CA Access Control

참조 안내서

r12.5

두 번째 버전

본 문서 및 관련 컴퓨터 소프트웨어 도움말 프로그램(이하 "문서"라고 함)은 귀하에게 정보를 제공하기 위한 것이며 CA 는 언제든 이를 변경하거나 철회할 수 있습니다.

CA 의 사전 서면 동의 없이 본 문서의 전체 혹은 일부를 복사, 전송, 재생산, 공개, 수정 또는 복제할 수 없습니다. 본건 문서는 CA 의 기밀 및 재산적 정보이며 귀하와 CA 사이에 체결된 별도의 보안 유지 동의에 따른 허가가 없는 한 귀하는 이 문서를 공개하거나 다른 용도로 사용할 수 없습니다.

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

본건 문서의 사본 인쇄 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 파기되었음을 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 제한 사항, 이익 손실, 투자 손실, 사업 중단, 영업권 또는 데이터 손실을 포함하여 이에 국한되지 않고, 본 문서의 사용에 따른 직간접적 손실 또는 손해에 대해 CA 가 발생 가능한 이 사실을 명백히 인지한 경우일지라도 사용자나 제 3 자에게 법적 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 문서의 제작자는 CA 입니다.

"제한된 권한"과 함께 제공됨. 미국 정부에 의한 사용, 복제 또는 공개는 FAR 12.212, 52.227-14 및 52.227-19(c)(1) - (2)항 및 DFARS 252.227-7014(b)(3)항의 적용을 받습니다.

Copyright © 2009 CA. All rights reserved. 이 문서에서 언급된 모든 상표, 상품명, 서비스 표시 및 로고는 각 해당 회사의 소유입니다.

CA 제품 참조

이 문서는 다음 CA 제품을 참조합니다.

- CA Access Control Premium Edition
- CA Access Control
- CA Single Sign-On(CA SSO)
- CA Top Secret®
- CA ACF2™
- CA Audit
- CA Network and Systems Management(CA NSM, 이전 이름: Unicenter NSM 및 Unicenter TNG)
- CA Software Delivery(이전 이름: Unicenter Software Delivery)
- 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
기울임꼴	반드시 입력해야 하는 정보
대괄호([ ]) 사이	선택적 피연산자
중괄호({ }) 사이	필수 피연산자 집합

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

예제: 명령 표기 규칙

다음 코드는 이 안내서에서 명령 규칙이 사용되는 방식을 보여 줍니다.

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

설명:

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

기술 지원팀에 문의

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

설명서 변경 사항

두 번째 버전

이 설명서의 두 번째 버전은 r12.5 GA 때 제공되었습니다.

이 버전에서 다음 항목이 추가 또는 업데이트되었습니다.

- ChangeEncryptionMethod 유틸리티 - 암호화 방법 변경 (페이지 29) - 업데이트된 항목에서 새 고려 사항에 대해 설명합니다.
- policydeploy -restore 함수 - 모든 정책 복원 (페이지 88) - 업데이트된 항목에서 끝점에서 정책을 복원하기 위해 CA Access Control 이 따르는 새 프로세스에 대해 설명합니다.
- secons -v 함수 - Windows 에서 계측 런타임 설정 제어 (페이지 146) - 새 항목에서 새 secons -v 유틸리티에 대해 설명합니다.
- uxconsole -register - Active Directory 에 UNIX 컴퓨터 등록 (페이지 226) - 업데이트된 항목에서 호스트 이름에 대한 제한 사항에 대해 설명합니다.
- UNAB 충돌 파일 (페이지 399) - 새 항목에서 UNAB 충돌 파일의 필드에 대해 설명합니다.
- FsiDrv (페이지 414) - 업데이트된 항목에서 SystemBypassRestricted 레지스트리 항목에 대해 자세히 설명합니다.
- Instrumentation (페이지 418) - 업데이트된 항목에서 이 키와 그 하위 키의 레지스트리 항목에 대해 자세히 설명합니다.
- endpoint management (페이지 453) - 업데이트 항목에서 이 하위 키의 레지스트리 항목에 대해 자세히 설명합니다.
- SeoSD 키 - 레지스트리 설정 (페이지 460) - 업데이트된 항목에서 SurrogateInterceptionMode 레지스트리 값의 변경된 기능에 대해 설명합니다.
- UNAB 사용된 포트 (페이지 582) - 새 항목에서 UNAB 가 사용하는 기본 포트에 대해 설명합니다.

첫 번째 버전

설명서의 첫 번째 버전은 r12.5 에서 제공되었습니다. 이 버전에서 설명서의 r12.0 SP1 릴리스에 다음 사항이 업데이트되었습니다.

- 유틸리티 (페이지 27) - 업데이트된 장에서 다음과 같은 새 유틸리티 및 업데이트된 유틸리티를 설명합니다.
  - acpwd 유틸리티 - 권한 있는 계정 암호 체크 인 및 체크 아웃 (페이지 27)
  - acuxchkey 유틸리티 - 암호화 키 설정 변경 (페이지 28)
  - dmsmgr -cleanup 함수-사용하지 않는 노드 제거 (페이지 45)
  - policydeploy 유틸리티-엔터프라이즈 정책 배포 관리 (페이지 76)
  - report_agent.sh 스크립트 - 보고서 에이전트 구성 (페이지 93)
  - secons -kt 함수 - UNIX 에서 커널 테이블 표시 (페이지 134)
  - secons -ktc 함수 - UNIX 에서 커널 캐시 테이블 삭제, 활성화, 비활성화 (페이지 144)
  - UXpreinstall 유틸리티 - 시스템 호환성 검사 (페이지 230)
  - uxconsole -manage - 사용자 및 그룹 정보 표시 및 편집 (페이지 222)
  - uxconsole -register - Active Directory 에 UNIX 컴퓨터 등록 (페이지 226)
  - uxconsole -migrate - UNIX 사용자 및 그룹을 Active Directory 로 마이그레이션 (페이지 224)
  - seauxd 데몬 (페이지 243)
- 구성 파일 (페이지 251) - 업데이트된 장에서 새 구성 파일 및 변경된 구성 파일을 설명합니다.
- 레지스트리 항목 (페이지 401) - 업데이트된 장에서 새로 추가되거나 변경된 CA Access Control 구성 설정을 설명합니다.
- 사용된 포트 (페이지 579) - 업데이트된 장에서 CA Access Control 구성 요소가 사용하는 포트에 대한 최신 정보를 설명합니다.
- 보고 데이터베이스 스키마 (페이지 583) - 업데이트된 장에서 보고 데이터베이스 스키마에 대한 최신 정보를 설명합니다.

목차

제 1 장: 소개 25

안내서 정보 25
안내서 사용자 25

제 2 장: 유틸리티 27

acpwd Utility - 권한 있는 계정 암호 체크 인 및 체크 아웃 27
acuxchkey 유틸리티 - 암호화 키 설정 변경 28
ChangeEncryptionMethod 유틸리티 - 암호화 방법 변경 29
dbmgr 유틸리티 30
- dbmgr -create 함수-데이터베이스 작성 31
- dbmgr -dump 함수-데이터베이스 정보 표시 33
- dbmgr -export 함수-데이터베이스를 정의하는 스크립트 작성 36
- dbmgr -migrate 함수-데이터를 플랫 파일로 복사 37
- dbmgr -util 함수-기존 데이터베이스 관리 39
- dbmgr -backup 함수 - 데이터베이스 백업 41
- dbmgr -restore 함수-데이터베이스 복원 41

defclass 유틸리티-사용자 정의 자산 유형을 클래스로 정의 42
DictImport 유틸리티-사전 파일 가져오기 42
dmsmgr 유틸리티 43
- dmsmgr -create 함수-DMS 또는 DH 작성 43
- dmsmgr -remove 함수-DMS 또는 DH 제거 45
- dmsmgr -cleanup 함수-사용하지 않는 노드 제거 45
- dmsmgr -config 함수-고급 정책 관리 구성 46
- dmsmgr -restore 기능 - DMS 또는 DH 복원 47

eacpg_gen 유틸리티-모범 사례 정책 정의 48
eACoexist 유틸리티-트러스트된 공존 프로그램 검색 및 등록 51
- 공존 유틸리티 작동 방법 52
- response.ini - 공존 유틸리티 구성 66

eACSigUpdate 유틸리티-STOP 서명 파일 교체 67
eACSyncLockout 유틸리티-계정 잠금 동기화 68
exporttngdb 유틸리티-Unicenter Security 데이터 마이그레이션 69
issec 유틸리티-CA Access Control 데몬 상태 표시 69
ldap2seos 스크립트-CA Access Control 에 추가하기 위해 LDAP 에서 사용자 추출 70
seos2ldap 스크립트-CA Access Control 사용자를 LDAP 로 내보내기 72
migopts 유틸리티-Unicenter Security 설정 변환 74

ntimport 유틸리티-Windows 사용자 및 그룹 가져오기 74
policydeploy 유틸리티-엔터프라이즈 정책 배포 관리 76
policydeploy -assign Function - 정책 할당 또는 할당 취소 77
policydeploy -delete 함수 - 정책 삭제 79
policydeploy -deploy 함수 - 정책 배포 또는 배포 취소 81
policydeploy -fix Function - 배포 작업 다시 실행 82
policydeploy -getrules Function - 배포 스크립트 보기 83
policydeploy -join Function - 호스트를 호스트 또는 호스트 그룹에서 조인 또는 제거 84
policydeploy -migrate 함수 - PMD 를 고급 정책 관리로 마이그레이션 85
policydeploy -reset Function - 정책 배포 다시 설정 88
policydeploy -restore Function - 모든 정책 복원 88
policydeploy -store 함수 - 정책 저장 89
policydeploy -upgrade 함수 - 정책 버전 업그레이드 또는 다운그레이드 92
report_agent.sh 스크립트 - 보고서 에이전트 구성 93
seaudit 유틸리티-감사 로그 레코드 표시 95
sebuildla 유틸리티-Lookaside 데이터베이스 작성 102
sechkey 유틸리티 106
대칭 키 모드의 sechkey 유틸리티 106
PKI 모드의 sechkey 유틸리티 110
seclassadm 유틸리티-CA Access Control 클래스 관리 112
secompas 유틸리티-암호 비교 115
secons 유틸리티 117
secons 유틸리티-UNIX 에서 CA Access Control 종료 관리 118
secons 유틸리티-CA Access Control 추적 관리 121
secons 유틸리티-동시 로그인 옵션 관리 122
secons 유틸리티-UNIX 에서 리소스 캐싱 관리 123
secons 유틸리티-Windows 에서 CA Access Control 종료 128
secons -acee 함수 - Windows 에서 ACEE 레코드 표시 128
secons -checkSID 함수-Windows 에서 재사용된 계정 확인 130
secons -i 함수-UNIX 에서 런타임 통계 표시 131
secons -i 함수-Windows 에서 런타임 통계 표시 133
secons -kt 함수 - UNIX 에서 커널 테이블 표시 134
secons -ktc 함수 - UNIX 에서 커널 캐시 테이블 삭제, 활성화, 비활성화 144
secons -refIP 함수-네트워크 리소스의 IP 주소 새로 고침 145
secons -rl 함수-UNIX 에서 구성 설정 다시 로드 145
secons -v 함수 - Windows 에서 계측 런타임 설정 제어 146
secons -whoami 함수 - 사용자 이름 및 보안 자격 증명 표시 149
secrepsw 유틸리티-정책 모델 및 섀도 파일 작성 150
sedbpchk 유틸리티-데이터베이스 백업 151
seerrlog 유틸리티-오류 로그 레코드 표시 153
segrace 유틸리티-사용자 로그인 정보 표시 154
segrace 유틸리티-UNIX 에서 사용자 로그인 설정 표시 154

segrace 유틸리티-Windows 에서 사용자 로그인 설정 표시 155
segracex 유틸리티-UNIX 에서 암호 만료 검사 156
SegraceW 유틸리티-Windows 에서 암호 만료 검사 158
seini 유틸리티-구성 파일 관리 159
selang 유틸리티-CA Access Control 명령줄 실행 162
seldapcred 유틸리티-자격 증명 암호화 및 저장 165
seload 유틸리티-CA Access Control 로드 및 시작 166
selock 유틸리티-X 터미널 화면 잠금 167
selockcom 유틸리티-selock 유틸리티 제어 170
selogmix 유틸리티-감사 로그 파일의 분할 및 병합 171
semsgtool 유틸리티-메시지 파일 유지 관리 173
senable 유틸리티-비활성 사용자 계정 활성화 176
senone 유틸리티-권한 없는 사용자로서 명령 실행 177
SEOS_load 유틸리티-CA Access Control 차단 모듈 로드 178
sepass 유틸리티-암호 설정 또는 교체 179
sepmd 유틸리티 182
sepmd 유틸리티-구독자 및 업데이트 파일 관리 183
sepmd 유틸리티-이중 컨트롤 관리 187
sepmd 유틸리티-PMDB 백업 188
sepmd 유틸리티-정책 모델 로그 파일 관리 191
sepmd 유틸리티-PMDB 관리 192
sepmd 유틸리티 - PMDB 복원 193
sepmdadm 유틸리티-PMDB 정의 만들기 194
sepropadm 유틸리티-데이터베이스 속성 관리 198
sepurgdb 유틸리티-정의되지 않은 레코드에 대한 데이터베이스 참조 제거 199
sereport 유틸리티 보고서 구성 200
sereport 유틸리티-UNIX 에서 HTML 보고서 작성 203
sereport 유틸리티-Windows 에서 HTML 보고서 작성 204
seretrust 유틸리티(UNIX)-프로그램 다시 트러스트 및 파일 보호를 위한 명령 생성 205
serevu 유틸리티-실패한 로그인 시도 처리 207
sessfgate 유틸리티-Unicenter Security 요청을 CA Access Control 로 라우팅 209
sesu 유틸리티 - 사용자 전환 210
sesudo 유틸리티 212
sesudo 유틸리티-UNIX 에서 다른 사용자로서 명령 실행 213
sesudo 유틸리티-Windows 에서 다른 사용자로서 명령 실행 214
seuidpgm 유틸리티-트러스트된 프로그램 추출 215
seversion 유틸리티-CA Access Control 프로그램 모듈 버전 정보 표시 218
sewhoami 유틸리티 - UNIX 에서 CA Access Control 사용자 이름 및 보안 자격 증명 표시 219
uninstall_AC 유틸리티-원격 컴퓨터에서 CA Access Control 제거 221
uxconsole -manage - 사용자 및 그룹 관리 222
uxconsole -migrate - UNIX 사용자 및 그룹을 Active Directory 로 마이그레이션 224

uxconsole -register - Active Directory 에 UNIX 컴퓨터 등록 226
UxImport 유틸리티-UNIX 운영 체제에서 정보 추출 227
UXpreinstall 유틸리티 - 시스템 호환성 검사 230
서비스 및 데몬 세부 사항 232
sepmdd 데몬 (UNIX) 232
sepmdd 서비스(Windows) 237
seagent 데몬 242
seauxd 데몬 243
seosd 데몬 243
selogrcd 데몬-감사 레코드 수집 245
selogrd 데몬-감사 레코드 송신 246
seostngd 데몬 248
seoswd Daemon 249

제 3 장: 구성 파일 251

accommon.ini 파일 251
communication 251
global 253
ReportAgent 253
seos.ini 초기화 파일 256
crypto 258
demons 260
Dependency 261
devcalc 261
lang 262
ldap 266
logmgr 267
message 270
mfsd 270
OS_User 271
package 272
pam_seos 272
passwd 274
pmd 281
policyfetcher 285
PUPMAgent 286
seauxd 287
segrace 289
seini 289
selock 290
selogrd 290

seos 295
SEOS_syscall 304
seosd 313
seosdb 331
seoswd 332
serevu 335
sesu 336
sesudo 337
standalone 338
tng 338
pmd.ini 파일 339
endpoint_management 340
lang 340
logmgr 341
passwd 343
pmd 343
seos 349
lang.ini 파일 349
general 350
history 350
newres 351
newusr 352
properties 353
unix 355
trcfilter.init 356
audit.cfg 파일 - 감사 레코드 필터링 357
auditrouteflt.cfg 파일 - 감사 레코드 라우팅 필터링 366
감사 로그 라우트 구성 파일 selogrd.cfg 374
uxauth.ini 파일 384
ad 385
agent 386
global 392
logmgr 392
map 395
message 396
migrate 396
passwd 398
register 399
UNAB 충돌 파일 399

제 4 장: 레지스트리 항목 401

CA Access Control 레지스트리 401
AccessControl 401
Agent 405
Applications 405
Client 406
Common 407
crypto 409
Dependency 411
devcalc 411
Exits 412
FsiDrv 414
Instrumentation 418
lang 441
logmgr 키 - 레지스트리 설정 442
message 445
OS_user 446
passwd 447
Pmd 448
policyfetcher 454
PUPMAgent 455
Report 457
ReportAgent 키 - 레지스트리 설정 458
SeOSD 키 - 레지스트리 설정 460
SeOSWD 467
(STOP) 468
Tracer 469
UCTNG 469
WebService 470
추가적인 레지스트리 키 472

부록 A: 감사 로그 레코드 475

감사 레코드 475
감사 레코드의 이벤트 유형을 식별하는 방법 476
감사 이벤트 유형 478
로그인 이벤트 478
로그아웃 이벤트 481
로그인 계정 사용 이벤트 483
로그인 계정 사용 안 함 이벤트 485
암호 시도 이벤트 488
리소스 액세스 이벤트 490

언트러스트 메시지 이벤트 493
인바운드 네트워크 연결 이벤트 496
아웃바운드 네트워크 연결 이벤트 498
보안 데이터베이스 관리 이벤트 501
시작 이벤트 504
종료 이벤트 505
암호 확인 이벤트 508
사용자에 대한 추적 메시지 510
로그인 및 로그아웃 이벤트의 권한 부여 단계 코드 513
2 - 사용자 개체 가져오기 513
3 - 로그인 터미널 원본에 대한 터미널 검사 513
5 - 사용자 일시 중지 검사 514
6 - 사용자 만료 검사 514
7 - 사용자 요일-시간 검사 514
8 - 암호 유효성 검사 514
9 - 사용자 유예 로그인 검사 514
10 - 유예 로그인이 없어 암호가 만료됨 514
11 - 사용자 ACEE 작성 515
12 - 사용자 비활성화 기간(일) 검사 515
13 - 사용자 로그인이 너무 많습니다. 515
14 - 활성 HOLIDAY 검사 515
15 - 로그인 응용 프로그램(LOGINAPPL) 검사 515
16 - 사용자 그룹 요일-시간 검사 515
17 - 네이티브 환경에 의해 시도가 거부되었습니다. 516
18 - 도메인 제한이 없는 사용자 516
19 - 거부할 이유가 없음 - 로그인 허용 516
20 - '논리' 사용자 검사 516
49 - 마지막 프로세스가 종료된 후 로그아웃이 검색되었습니다. 516
리소스 액세스 이벤트의 권한 부여 단계 코드 517
50 - 리소스의 보안 LABEL 검사 517
51 - 리소스의 보안 LEVEL 검사 517
52 - 리소스 범주 검사 517
53 - 리소스 DAYTIME 검사 517
54 - 리소스 OWNER 검사 517
55 - 리소스 ACL 검사 518
56 - 리소스 그룹 ACL 검사 518
57 - 리소스 ACL 에 있는 사용자 그룹 518
58 - 리소스 그룹 ACL 에 있는 사용자 그룹 518
59 - 리소스 UACC 검사 518
61 - 리소스의 OPERATOR 인 사용자 518
62 - 보호되지 않은 리소스의 클래스에 대한 UACC 검사 519
63 - 프로그램 조건부 액세스 519

64 - 리소스 ACL 의사용자 '*' 519
65 - 리소스의 AUDITOR 인 사용자 519
69 - 액세스를 허용한 단계가 없습니다. 519
70 - 리소스 그룹의 OWNER 검사 519
75 - 리소스 그룹 ACL 에 있는 사용자 '*' 520
76 - 리소스 거부 ACL 검사 520
77 - 리소스 그룹 거부 ACL 검사 520
78 - 리소스 거부 ACL 에 있는 사용자 그룹 520
79 - 리소스 그룹 거부 ACL 에 있는 사용자 그룹 520
80 - 리소스 거부 ACL 에 있는 사용자 '*' 520
81 - 리소스 그룹 거부 ACL 에 있는 사용자 '*' 521
82 - 리소스 그룹 DAYTIME 검사 521
86 - 사용자에 대한 리소스 일정 ACL 검사 521
87 - 사용자에 대한 리소스 그룹 일정 ACL 검사 521
88 - 사용자 그룹에 대한 리소스 일정 ACL 검사 521
89 - 사용자 그룹에 대한 리소스 그룹 일정 ACL 검사 521
90 - 리소스 일정 ACL 에 있는 사용자 * 522
91 - 리소스 그룹 일정 ACL 에 있는 사용자 * 522
92 - 보호된 리소스의 경로 이름 바꾸기 시도 522
200 - 클래스 검사가 활성화되지 않았습니다. 522
201 - 사용자 정보 로드 522
202 - 경고 모드의 리소스 522
203 - 리소스에 대한 액세스가 MAXIMUM_ALLOWED 입니다. 523
202 - 경고 모드의 클래스 523
210 - 특수 커널 모듈 로드 검사 523
250 - 언트러스트된 프로그램 실행 523
251 - 거부 가능한 매개 변수 사용 523
252 - an _abspath 사용자가 상대 경로를 지정했습니다. 523
253 - 허용된 sesudo 작업 524
254 - sesudo 명령 실패 524
440 - 잘못된 일정이 검색되었습니다. 524
441 - 일정에 액세스할 수 없습니다. 524
1050 - 기본 레코드 보안 레이블 검사 524
1051 - 기본 레코드 보안 수준 검사 524
1052 - 기본 레코드 범주 검사 525
1053 - 기본 레코드 요일 및 시간 검사 525
1054 - 기본 레코드 OWNER 검사 525
1055 - 사용자에 대한 기본 레코드 ACL 검사 525
1056 - 사용자에 대한 기본 레코드 그룹 ACL 검사 525
1057 - 사용자 그룹에 대한 기본 레코드 ACL 검사 525
1058 - 사용자 그룹에 대한 기본 레코드 그룹 ACL 검사 526
1059 - 기본 레코드 범용 액세스 검사 526
1061 - 기본 레코드 OPERATOR 특성 검사 526

1062 - 기본 레코드 클래스 전역 범용 액세스 526
1063 - 기본 레코드 프로그램 조건부 액세스 526
1064 - _default 레코드 ACL 에 있는 사용자 '*' 527
1069 - 기본 레코드에 대한 액세스 권한을 부여하는 규칙이 없습니다. 527
1202 - 경고 모드의 기본 레코드 527
1250 - 기본 레코드가 언트러스트로 설정되었습니다 527
언트러스트 메시지 이벤트의 권한 부여 단계 코드 527
0 - Watchdog 파일을 검사하는 동안 일반적인 오류가 발생했습니다. 527
1 - PROGRAM 또는 SECFILE 의 Stat 정보가 변경되었습니다. 528
4 - PROGRAM 또는 SECFILE 의 CRC 검사가 변경되었습니다. 528
5 - PROGRAM 또는 SECFILE 의 파일에 대해 stat 명령을 실행할 수 없습니다. 528
7 - PROGRAM 또는 SECFILE 의 MD5 서명이 변경되었습니다. 528
8 - PROGRAM 또는 SECFILE 의 SHA1 서명이 변경되었습니다. 528
인바운드 네트워크 연결 이벤트의 권한 부여 단계 코드 529
150 - 클래스 테이블 검사 529
153 - inetacl 에 있는 HOST 항목 별표 529
156 - HOST 항목 inetacl 529
157 - HOST 클래스 UACC 530
159 - HOST 항목 서비스 범위 ACL 530
163 - 서비스에 대한 액세스 권한을 부여하는 규칙이 없습니다. 530
164 - HOST 그룹 inetacl 530
165 - HOST 그룹 서비스 범위 ACL 530
166 - inetacl 에 있는 HOST 그룹 별표 530
167 - HOSTNET(네트워크 또는 IP 마스크/일치) inetacl 531
168 - HOSTNET(네트워크 또는 IP 마스크/일치) 서비스 범위 531
169 - HOSTNET(네트워크 또는 IP 마스크/일치) inetacl 별표 531
170 - HOSTNP(호스트 이름 패턴) inetacl 531
171 - HOSTNP(호스트 이름 패턴) 서비스 범위 531
172 - HOSTNP(호스트 이름 패턴) inetacl 별표 531
173 - HOST 항목 요일 & 시간 제한 532
174 - HOST 그룹 요일 & 시간 제한 532
175 - HOSTNET(네트워크 또는 IP 마스크/일치) 요일 및 시간 제한 532
176 - HOSTNP(호스트 이름 패턴) 요일 및 시간 제한 532
177 - HOST_default 요일 및 시간 제한 532
178 - HOST_default inetacl 532
179 - HOST_default 서비스 범위 532
180 - HOST_default 서비스 별표 533
404 - TCP 서비스 ACL 에 있는 HOST 항목 533
405 - TCP 서비스 ACL 에 있는 GHOST 항목 533
406 - TCP 서비스 ACL 에 있는 HOSTNET 항목 533
407 - TCP 서비스 ACL 에 있는 HOSTNP 항목 533
아웃바운드 네트워크 연결 이벤트의 권한 부여 단계 코드 534

400 - 클래스 TCP 의 _default 서비스 534
401 - TCP 서비스의 클래스 UACC 534
402 - TCP 서비스의 요일 및 시간 제한 534
403 - TCP 서비스의 ACL 읽기 단계 534
408 - TCP 서비스의 기본 액세스 534
409 - TCP 서비스의 CACL 읽기 단계 535
410 - TCP 서비스 CACL 에 있는 USER 의 HOST 항목 535
411 - TCP 서비스 CACL 에 있는 USER 의 GHOST 항목 535
412 - TCP 서비스 CACL 에 있는 USER 의 HOSTNET 항목 535
413 - TCP 서비스 CACL 에 있는 USER 의 HOSTNP 항목 535
414 - TCP 서비스 CACL 에 있는 GROUP 의 HOST 항목 535
415 - TCP 서비스 CACL 에 있는 GROUP 의 GHOST 항목 536
416 - TCP 서비스 CACL 에 있는 GROUP 의 HOSTNET 항목 536
417 - TCP 서비스 CACL 에 있는 GROUP 의 HOSTNP 항목 536
418 - TCP 서비스 CACL 에 있는 사용자 '*'의 HOST 항목 536
419 - TCP 서비스 CACL 에 있는 사용자 '*'의 GHOST 항목 536
420 - TCP 서비스에 있는 사용자 '*'의 HOSTNET 항목 537
421 - TCP 서비스 CACL 에 있는 사용자 '*'의 HOSTNP 항목 537
보안 데이터베이스 관리 이벤트의 권한 부여 단계 코드 537
300 - 정의되지 않은 CA Access Control 사용자 537
301 - 마지막 ADMIN 사용자를 삭제하려고 합니다. 537
302 - 루트 사용자를 삭제하려고 합니다. 538
303 - 사용자가 암호를 변경하려고 합니다. 538
304 - 감사자가 아닌 사용자가 감사 모드를 설정하려고 합니다. 538
305 - ADMIN 사용자에 대해 허용된 명령 538
306 - Showuser (myself) , Showxusr 허용 538
307 - 사용자가 소유하지 않은 범주를 설정하려고 합니다. 538
308 - 사용자가 소유하지 않은 보안 레이블을 설정하려고 합니다. 539
309 - 사용자가 자신의 보안 수준보다 높은 보안 수준을 설정하려고 합니다. 539
310 - ADMIN 이 아닌 사용자가 사용자 모드를 설정하려고 합니다. 539
311 - 개체 소유자에 대해 허용된 명령 539
312 - 네이티브 파일 소유자는 CA Access Control 로 정의할 수 있습니다. 539
313 - GROUP-ADMIN 사용자에 대해 허용된 명령 539
314 - GROUP-ADMIN 사용자는 그룹에 가입/가입 취소시킬 수 있습니다. 540
315 - GROUP-AUDITOR/ADMIN 은 그룹을 나열할 수 있습니다. 540
316 - 감사자는 모든 개체를 나열할 수 있습니다. 540
317 - OPERATOR 는 모든 개체를 나열할 수 있습니다. 540
318 - GROUP-AUDITOR 는 그룹 범위 내의 개체를 나열할 수 있습니다. 540
319 - GROUP-OPERATOR 는 그룹 범위 내의 개체를 나열할 수 있습니다. 540
320 - CLASS-ADMIN 사용자에 대해 허용된 명령 540
321 - 액세스 권한을 가진 PWMANAGER/ADMIN 에 대해 허용된 명령 541
322 - 이 작업을 허용하는 규칙이 없습니다. 541

324 - 사용자는 sepass 를 사용하여 암호를 변경할 수 있습니다. 541
326 - 사용자가 직접 '로그인 정보'를 작성했습니다. 541
327 - GROUP-PWMANAGER 에 대해 허용된 명령 541
329 - PWMANAGER 가 사용자를 활성화했습니다. 541
330 - DOMAIN 변경에 허용된 명령 541
331 - PWMANAGER 에 대해 허용된 명령 542
332 - PWMANAGER 에 대해 허용된 네이티브 플래그 변경 542
333 - PWMANAGER 는 '다음 로그온할 때 반드시 암호 변경' 특성을 변경할 수 있습니다. 542
334 - GROUP-PWMANAGER 에 대해 허용된 명령 542
335 - PWMANAGER 는 '로그인 정보'를 편집할 수 있습니다. 542
336 - 감사자 사용자에 대해 허용된 명령 542
337 - 데이터베이스 정보와 명령을 조정하지 못했습니다. 543
338 - 암시적 요청에 따라 명령 생성 543
339 - SEOS_syscall 모듈 언로드 준비 검사 543
종료 이벤트의 권한 부여 단계 코드 543
451 - OPERATOR 인 사용자 543
452 - ADMIN 또는 SPECIAL 인 사용자 543
453 - _seagent 는 CA Access Control 을 종료할 수 있습니다. 544
460 - 사용자가 CA Access Control 을 종료할 수 없습니다. 544
암호 확인 이벤트의 권한 부여 단계 코드 544
0 - 암호 품질을 확인했습니다. 544
1 - 암호가 너무 짧습니다. 544
2 - 암호에 사용자 이름이 포함되어 있습니다. 544
3 - 암호에 소문자가 너무 적습니다. 545
4 - 암호에 대문자가 너무 적습니다. 545
5 - 암호에 숫자가 너무 적습니다. 545
6 - 암호에 다른 문자가 너무 적습니다. 545
7 - 암호에 동일한 문자의 중복이 너무 많습니다. 545
8 - 현재 암호와 같습니다. 545
9 - 이미 사용된 암호입니다. 다른 암호를 선택하십시오. 545
10 - 암호에 영문자가 너무 적습니다. 546
11 - 암호에 영숫자가 너무 적습니다. 546
12 - 암호가 최근에 변경되어 현재 다시 변경할 수 없습니다. 546
13 - 암호가 이전 암호에 포함되어 있거나 그 반대입니다. 546
16 - 암호가 너무 깁니다. 546
20 - 암호가 일치하지 않습니다. 546
21 - 미리 정의된 금지 문자를 포함할 수 없습니다. 546
22 - 이미 사용된 암호입니다. 547
23 - 암호가 이전 암호에 포함되어 있거나 그 반대입니다. 547
24 - 암호가 사전 파일에 있습니다. 547
100 - 잘못된 인수 547
사용자에 대한 추적 메시지의 권한 부여 단계 코드 547

994 - 정보 메시지 548
995 - 내부 리소스에 대한 무단 액세스 548
996 - 내부 리소스에 대한 권한 있는 액세스 548
997 - 사용자가 setuid\setgid 디렉터리를 실행할 수 있습니다. 548
998 - 권한 부여가 '감사 모드 전용'으로 구성되어 있습니다. 548
999 - 리소스가 보호되지 않습니다. 규칙이 있는지 확인하십시오. 549
레코드가 작성된 이유를 지정하는 사유 코드 549
0 - 작업 로그에 대한 특정 요청이 없습니다. 549
2 - 사용자 감사 모드에 로깅이 필요합니다. 549
3 - 리소스 감사 모드에 로깅이 필요합니다. 549
4 - 경고 모드의 리소스 549
5 - CA Access Control serevu 유틸리티에서 감사를 요청했습니다. 549
7 - 아웃바운드 연결 레코드 550
8 - CA Access Control pam 지원 UNIX 로그인 실패 550
9 - CALENDAR 클래스의 Daytime 제한 검사 550
10 - 작업 로그에 대한 특정 요청 550
11 - CA Access Control secons 유틸리티에서 감사를 요청했습니다. 550

부록 B: 추적 메시지 551

규칙 551
메시지 551

부록 C: 문자열 일치 575

와일드카드 식 575
와일드카드 일치 575
문자 목록 575
예: 와일드카드 일치 576

부록 D: 사용된 포트 579

UNIX 사용된 포트 579
Windows 사용된 포트 580
서버 구성 요소에 사용되는 포트 581
UNAB 사용된 포트 582

부록 E: 보고 데이터베이스 스키마 583

스키마 도표 583
그룹 584
정책 관리 585

리소스 586
공유 속성 587
스냅숏 ..... 오류! 책갈피가 정의되어 있지 않습니다.
사용자 589
테이블 590
ACL 테이블 열 596
ACRPTDB_VERSION 테이블 열 600
CATEGORY 테이블 열 601
CONFIG 테이블 열 601
CONFIG_ENTRY 테이블 열 602
DAYTIME 테이블 열 603
DEPLOYMENT_RESULT_MESSAGE 테이블 열 603
DEPLOYMENT_TASK 테이블 열 604
DEPLOYMENT_TASK_GROUP 테이블 열 607
DISTRIBUTION_HOST 테이블 열 609
EFFECTIVE_POLICY 테이블 열 610
GROUPAUDIT 테이블 열 611
GROUPINFO 테이블 열 611
GROUPMEMBER 테이블 열 616
GROUPREVACL 테이블 열 616
GROUPS 테이블 열 619
HOLDATE 테이블 열 620
HOSTINFO 테이블 열 620
INETACL 테이블 열 621
INSERVRNGE 테이블 열 623
LOCAL_PMD_SUBSCRIBER 테이블 열 624
LOGINAPPL 테이블 열 625
MEMBEROF 테이블 열 628
MEMBERS 테이블 열 628
NODE 테이블 열 629
NODE_ADDRESS 테이블 열 630
NODE_ALIAS 테이블 열 631
NODE_DEVIATION 테이블 열 631
NODE_SUBSCRIPTION_STATUS 테이블 열 632
PASSWDRULES 테이블 열 633
POLICY 테이블 열 635
POLICY_DEVIATION 테이블 열 636
POLICY_GROUP 테이블 열 638
POLICY_GROUP_DEPENDENCY 테이블 열 639
POLICY_GROUP_NODE_ASSIGNMENT Table 테이블 열 640
POLICY_RULESET 테이블 열 641
POLICY_STATUS 테이블 열 642

POLICYMODELINFO 테이블 열 644
RAUDIT 테이블 열 645
RESAC 테이블 열 645
RESINFO 테이블 열 650
RULESET 테이블 열 653
RULESET_COMMAND 테이블 열 654
SEOS 테이블 열 655
SEOSSYSCALL 테이블의 열 661
SNAPSHOTINFO 테이블 열 662
SPECIALPGMTYPE 테이블 열 663
SYSCALL 테이블의 열 664
SYSCALLUSERSPECIALPGM 표의 열 664
UACC 테이블 열 665
USERAC 테이블 열 666
USERACAUDIT 테이블 열 675
USERACMODE 테이블 열 676
USERGRP 테이블 열 676
USERINFO 테이블 열 678
USERLIST 테이블 열 680
USERREVACL 테이블 열 681
관계 684
CONFIG_ENTRY_CON 관계의 부모 테이블 687
DEPTASK_RESULTMSG_CON 관계의 부모 테이블 687
GROUPMEMBER_FK 관계의 부모 테이블 688
GROUPREVACL_FK 관계의 부모 테이블 688
USERGRP_GROUP_CON 관계의 부모 테이블 689
MEMBEROF_FK 관계의 부모 테이블 689
PASSWDRULES_FK 관계의 부모 테이블 690
USERLIST_FK 관계의 부모 테이블 690
GROUPAUDIT_FK 관계의 부모 테이블 691
SNAPSHOTINFO_FK 관계의 부모 테이블 691
NODE_ALIAS_FK 관계의 부모 테이블 691
NODE_SUBSCRIPTION_PUBLISHER 관계의 부모 테이블 692
NODE_EFFECTIVE_POLICY_CON 관계의 부모 테이블 692
NODE_SUBSCRIPTION_SUBSCRIBER 관계의 부모 테이블 693
NODE_POLICY_STATUS_CON 관계의 부모 테이블 693
NODE_DEPTASKGRP_CON 관계의 부모 테이블 694
NODE_ADDRESS_FK 관계의 부모 테이블 694
NODE_NODE_DEVIATION_CON 관계의 부모 테이블 695
NODE_DEPTASK_CON 관계의 부모 테이블 695
POLICY_POLICY_STATUS_CON 관계의 부모 테이블 696
LATESTFIN_POLICYGRP_CON 관계의 부모 테이블 696

POLICY_EFFECTIVE_POLICY_CON 관계의 부모 테이블 697
POLICY_POLICY_DEVIATION_CON 관계의 부모 테이블 697
POLICY_RULESET_POLICY_CON 관계의 부모 테이블 698
LATEST_POLICYGRP_CON 관계의 부모 테이블 698
POLICY_DEPTASK_CON 관계의 부모 테이블 699
POLICYGRP_DEPTASK_CON 관계의 부모 테이블 699
POLICYGRP_DEPTASKGRP_CON 관계의 부모 테이블 700
POLICY_GROUP_DEP_ON_CON 관계의 부모 테이블 700
POLICY_GROUP_DEP_CON 관계의 부모 테이블 701
PMD_SUBSC_CON 관계의 부모 테이블 701
POLICYGRP_NODASS_POL_CON 관계의 부모 테이블 702
POLICY_GROUP_CON 관계의 부모 테이블 702
POLICY_CON 관계의 부모 테이블 703
RULESET_CON 관계의 부모 테이블 703
POLICYGRP_NODASS_NOD_CON 관계의 부모 테이블 704
NODE_CON 관계의 부모 테이블 704
GROUP_RESOURCE_ACL_CON 관계의 부모 테이블 705
RESINFO_USERREVACL_COND_CON 관계의 부모 테이블 705
UACC_CON 관계의 부모 테이블 706
SPECIALPGMTYPE_CON 관계의 부모 테이블 706
RESAC_CON 관계의 부모 테이블 707
RAUDIT_CON 관계의 부모 테이블 707
MEMBERS_PARENT_CON 관계의 부모 테이블 708
RESINFO_DEPTASKGRP_CON 관계의 부모 테이블 708
RESINFO_DEPTASK_CON 관계의 부모 테이블 709
LOGINAPPL_CON 관계의 부모 테이블 709
INSERVRNGE_CON 관계의 부모 테이블 710
NODEGRP_DEPTASKGRP_CON 관계의 부모 테이블 710
RESINFO_GRPREVACL_COND_CON 관계의 부모 테이블 711
RESINFO_HOST_CON 관계의 부모 테이블 711
GROUPS_GROUP_CON 관계의 부모 테이블 712
INETACL_CON 관계의 부모 테이블 712
HOLDATE_CON 관계의 부모 테이블 713
GROUPS_MEMBER_CON 관계의 부모 테이블 713
ACL_CON 관계의 부모 테이블 714
MEMBERS_CHILD_CON 관계의 부모 테이블 714
USER_RESOURCE_ACL_CON 관계의 부모 테이블 715
RULESET_RULESET_POLICY_CON 관계의 부모 테이블 715
RULESET_COMMAND_CON 관계의 부모 테이블 716
SEOS_DH_FK 관계의 부모 테이블 716
DAYTIME_CON 관계의 부모 테이블 716
SEOS_CON 관계의 부모 테이블 717
SEOSSYSCALL_CON 관계의 부모 테이블 717

NAPSHOT_CONFIG_CON 관계의 부모 테이블 718
SYSCALL_CON 관계의 부모 테이블 718
SYSCALLUSERSPECIALPGM 관계의 부모 테이블..... 719
CATEGORY_CON 관계의 부모 테이블..... 719
GROUPINFO_CON 관계의 부모 테이블..... 720
SNAPSHOTINFO_CON 관계의 부모 테이블 720
RESINFO_CON 관계의 부모 테이블 720
POLICYMODEL_CON 관계의 부모 테이블..... 721
USERACAUDIT_FK 관계의 부모 테이블 721
USERACMODE_FK 관계의 부모 테이블..... 722
USERGRP_FK 관계의 부모 테이블 722
USERINFO_SUSPEND_USERAC_CON 관계의 부모 테이블..... 723
USER_DEPTASK_CHECKER_CON 관계의 부모 테이블 723
USER_DEPTASK_MAKER_CON 관계의 부모 테이블..... 724
USERREVACL_FK 관계의 부모 테이블..... 724
USERAC_CON 관계의 부모 테이블 725

제 1 장: 소개

이 장은 아래의 주제를 포함하고 있습니다.

안내서 정보 (페이지 25)
안내서 사용자 (페이지 25)

안내서 정보

이 안내서는 CA Access Control 유틸리티, 구성 파일, 상태 코드, 메시지 등에 대한 정보를 제공합니다. 이 안내서는 또한 엔터프라이즈 관리 및 보고 기능과 고급 정책 관리 기능을 제공하는 CA Access Control Premium Edition 과 함께 제공됩니다.

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

안내서 사용자

이 안내서는 명령을 실행하거나 CA Access Control 로 보호되는 환경을 유지 관리 및 구성하는 보안 및 시스템 관리자용으로 작성되었습니다.

제 2 장: 유틸리티

CA Access Control 에는 많은 유틸리티가 있습니다. 편리한 개요를 제공하기 위해 이 장에서는 유틸리티를 알파벳순으로 설명합니다.

acpwd Utility - 권한 있는 계정 암호 체크 인 및 체크 아웃

CA Access Control 끝점에서 권한 있는 계정 암호를 가져오려면 PUPM 에이전트를 사용하십시오. 명령줄을 사용하여 PUPM 에이전트를 실행하면 CA Access Control 엔터프라이즈 관리에 연결하여 권한 있는 계정 암호를 체크 아웃 및 체크 인할 수 있습니다.

이 명령의 형식은 다음과 같습니다.

```
acpwd -checkin|-checkout -account name -ep name -eptype type -container name [-nologo]
-help
```

-checkin

권한 있는 계정 암호 체크 인 프로세스를 실행합니다.

-checkout

권한 있는 계정 암호 체크 아웃 프로세스를 실행합니다.

-account name

체크 아웃 또는 체크 인할 권한 있는 계정 암호를 정의합니다.

-ep name

권한 있는 계정이 있는 끝점의 이름을 정의합니다.

-eptype type

끝점의 유형을 지정합니다.

옵션: Windows Agentless, SSH 장치, MS SQL, OS 400, Oracle, PeopleSoft

예: Windows Agentless

-container name

계정이 있는 컨테이너의 이름을 정의합니다.

-nologo

출력에 추가 정보 없이 암호만 표시하도록 지정합니다.

-help

도움말 파일을 표시합니다.

acuxchkey 유틸리티 - 암호화 키 설정 변경

acuxchkey 유틸리티를 사용하여 암호화 키 및 메시지 큐 설정을 변경합니다. 이 명령의 형식은 다음과 같습니다.

```
acuxchkey -t -pwd password
```

-t

메시지 큐 변경 옵션을 지정합니다.

-pwd

메시지 큐 암호를 정의합니다.

예: 메시지 큐 암호 변경

메시지 큐 암호를 변경하려면 다음 명령을 사용하십시오.

```
eu +reportagent epassword (<tibco password>)
```

참고: 메시지 큐 암호를 변경한 다음에는 이 메시지 큐를 사용하는 모든 끝점에 새 암호를 전파해야 합니다.

예: 배포 서버 통신 설정 변경

이 예는 SSL 을 사용하도록 배포 서버 설정을 변경하는 방법을 설명합니다.

```
env config

editres CONFIG accommon.ini section (communication) token (Distribution_Server) value
("ssl://<DS Host>:7243")
```

ChangeEncryptionMethod 유틸리티 - 암호화 방법 변경

UNIX 에 해당

ChangeEncryptionMethod 유틸리티는 암호화 방법을 변경합니다.

참고: 이 유틸리티는 스크립트 파일로 제공되며 lbin 디렉터리에 있습니다.

이 유틸리티를 실행하면 다음 암호화 방법 중 하나를 선택할 수 있습니다.

- 기본값
- AES(128 비트, 192 비트 또는 256 비트)
- DES
- TRIPLEDES
- SCRAMBLE

암호화 방법을 지정하지 않으면 지정하라는 메시지가 표시됩니다. 이 유틸리티는 시스템에서 기존 정책 모델을 검색하고 "sepmd -de pmd_name"을 실행하여 정책 모델의 암호를 해독한 후 libcrypt 를 새 공유 라이브러리인 libaes128, libaes192, libaes256, libdes, libtripledes 또는 libscramble 에 연결하여 암호화 방법을 변경합니다.

참고: 이 유틸리티를 실행하려면 CA Access Control 이 실행되고 있어야 합니다. 암호화 방법을 변경하기 위해 CA Access Control 을 일시적으로 종료할 것인지를 묻는 스크립트 메시지가 표시됩니다.

중요! CA Access Control 엔터프라이즈 관리 서버와 CA Access Control 끝점에서 동일한 암호화 방법을 사용하는지 확인하십시오. 기존 CA Access Control 끝점의 암호화 방법을 변경하도록 선택하면 모든 암호 내역이 손실됩니다.

이 명령의 형식은 다음과 같습니다.

```
ChangeEncryptionMethod.sh [DES|TRIPLEDES|SCRAMBLE|AES128|AES192|AES256]
```

dbmgr 유틸리티

dbmgr 유틸리티를 사용하면 CA Access Control 데이터베이스 파일을 만들고 관리하고 유지 관리할 수 있습니다.

참고: 이 유틸리티는 이전 버전의 dbdump, rdbdump, dbutil, secredb, sedb2scr 및 semigrate 유틸리티를 대체합니다.

중요! 이 유틸리티는 문제 해결을 위해 기술 지원자의 안내를 받는 경우에만 사용하십시오. 도움이 필요하면 기술 지원 부서(http://www.ca.com/worldwide)에 문의하십시오.

dbmgr 유틸리티를 실행하려면 ADMIN, AUDITOR 또는 SERVER 특성을 가지고 있어야 합니다.

이 유틸리티는 여러 작업을 처리하며 다음과 같은 관련 함수를 가지고 있습니다.

작업	함수
데이터베이스 작성 (페이지 31)	`dbmgr -create`
데이터베이스 정보 표시 (페이지 33)	`dbmgr -dump`
데이터베이스를 정의하는 스크립트 작성 (페이지 36)	`dbmgr -export`
데이터베이스 데이터를 플랫 파일로 복사 (페이지 37)	`dbmgr -migrate`
기존 데이터베이스 관리 (페이지 39)	`dbmgr -util`
데이터베이스 백업 (페이지 41)	`dbmgr -backup`
데이터베이스 복원 (페이지 41)	`dbmgr -restore`

dbmgr -create 함수-데이터베이스 작성

dbmgr -create 함수는 새로운 빈 데이터베이스를 생성합니다. 이 함수는 설치 시에만 또는 데이터베이스나 PMDB 를 작성하고자 하는 경우에만 사용하십시오. CA Access Control 은 현재 디렉터리에 데이터베이스를 작성합니다.

참고: 사용자 정의 클래스를 새 데이터베이스에 추가하려면 먼저 새 데이터베이스를 작성한 후 seclassadm 유틸리티를 실행하십시오.

이 명령의 형식은 다음과 같습니다.

```
dbmgr {-create|-c} {-c[q]|-h} [-d] [-f filename] \
    [-n] [-o] [-t terminalNames] \
    [-u userName [,userName...]] [-ux userName [,userName...]]\
    [-v] [-w] [-k] [-n pathName]
```

-create|-c

dbmgr 유틸리티의 데이터베이스 작성 함수를 실행합니다.

-c

새 데이터베이스 작성 여부를 묻는 메시지를 표시합니다.

-cq

작성 여부를 묻지 않고 새 데이터베이스를 작성합니다.

-h

이 함수에 대한 도움말을 표시합니다.

-d

데이터베이스 레이아웃 문서를 인쇄합니다. 인쇄된 문서에는 구조에 대한 전체 설명 및 데이터베이스에서 사용된 속성 형식이 있습니다.

-f filename

표준 출력 장치 대신 출력을 내보낼 파일을 지정합니다.

-k

데이터베이스 작성이 완료되면 공존 유틸리티를 실행하도록 지정합니다.

-n pathName

(UNIX 전용). 백업할 CA Access Control 데이터베이스의 전체 경로 이름을 정의합니다.

새 데이터베이스를 생성하면 기본적인 클래스 체계가 생성됩니다. seclassadm 유틸리티를 사용하여 데이터베이스에 새 클래스를 추가하면 데이터베이스 디렉터리에 있는 파일에 클래스 정보가 저장됩니다. 정책 모델 데이터베이스와 같은 특정 데이터베이스를 해당 클래스 스키마와 함께 백업하려면 -n 옵션을 사용하여 위치를 지정하십시오. 그러면 해당 위치에서 사용자 정의 클래스 정보를 가져옵니다. -n 옵션을 지정하지 않으면 데이터베이스가 생성되는 로컬 디렉터리에서 클래스 정보 파일을 검색합니다. 로컬 디렉터리에서 클래스 정보 파일을 찾지 못하면 활성 CA Access Control 보안 데이터베이스 디렉터리에서 파일을 가져옵니다.

-o

Unicenter TNG 클래스를 기존 데이터베이스에 추가합니다.

-t terminalName

데이터베이스에서 작성할 터미널 목록을 쉼표로 구분하여 정의합니다. 슈퍼 사용자는 이러한 터미널에서 로컬 데이터베이스를 관리할 수 있습니다.

-u userName [,userName...]

데이터베이스에 작성할 사용자 목록을 쉼표로 구분하여 정의합니다. 이러한 사용자는 CA Access Control 보안 관리자로 정의됩니다.

-t 옵션을 지정하면 이러한 사용자는 정의된 터미널로부터 로컬 데이터베이스를 관리할 권한을 갖게 됩니다.

-ux 매개 변수를 참조하십시오.

-xu userName [,userName...]

CA Access Control 보안 관리자로 정의할 엔터프라이즈 사용자 목록을 쉼표로 구분하여 정의합니다.

-t 옵션을 지정하면 이러한 사용자는 정의된 터미널로부터 로컬 데이터베이스를 관리할 권한을 갖게 됩니다.

작성된 사용자가 없는 상태에서 dbmgr -create 를 사용하면 ADMIN, AUDITOR 및 IGN_HOL 특성과 함께 UNIX 의 root 또는 Windows 의 Administrator 에 해당하는 사용자가 데이터베이스에 작성됩니다.

-v

진행률이 표시되지 않도록 합니다.

-w

Unicenter TNG 클래스를 포함하는 새 데이터베이스를 작성합니다.

참고: -v 옵션과 -d 옵션은 함께 사용할 수 없습니다.

예: Windows 에서 새 데이터베이스 작성

시스템 프롬프트 c:\temp>에 다음 명령을 입력합니다.

```
dbmgr -c -c -u user1 -t myterminal.company.com
```

데이터베이스를 작성하도록 선택하면 c:\temp 디렉터리에 새 데이터베이스가 작성됩니다. 데이터베이스에 user1 사용자가 작성되는데, 이 사용자는 ADMIN, AUDITOR 및 IGN_HOL 특성을 가지며 myterminal.company.com 터미널로부터 데이터베이스를 관리할 수 있습니다.

예: UNIX 에서 새 데이터베이스 작성

\tmp\db 디렉터리에 다음 명령을 입력합니다.

```
dbmgr -c -cq -d -f dbLayout
```

\tmp\db 디렉터리에 새 데이터베이스가 작성됩니다. 또한 데이터베이스 레이아웃 문서를 포함하는 파일(dbLayout)이 작성됩니다. 기본적으로 데이터베이스에 사용자 root 가 작성되고 ADMIN, AUDITOR 및 IGN_HOL 특성이 이 root 에 할당됩니다.

추가 정보:

seclassadm 유틸리티-CA Access Control 클래스 관리 (페이지 112)
eACoexist 유틸리티-트러스트된 공존 프로그램 검색 및 등록 (페이지 51)

dbmgr -dump 함수-데이터베이스 정보 표시

dbmgr -dump 함수는 데이터베이스의 레코드에 대해 보고합니다. -r 스위치를 포함할 경우, 이 함수는 인증 데몬이 현재 사용하는 데이터베이스에서 작동됩니다. 다음 작업을 수행하려면 이 함수를 사용하십시오.

- 지정된 클래스의 레코드에 대한 정보 표시
- 지정된 클래스의 단일 레코드에 대한 정보 표시
- 클래스의 모든 레코드에 대한 정보 표시(지정된 레코드 제외)
- 클래스 목록 및 속성 정의 생성
- 사용자가 속한 그룹 목록 생성
- 특정 클래스의 레코드 목록 생성

이 함수는 CA Access Control 데몬이 실행되고 있지 않다고 간주하며, 이 함수는 데이터베이스가 있는 디렉터리에서 이 함수를 호출해야 합니다. -r 스위치를 사용하는 경우 CA Access Control 데몬이 실행 중이어야 하고 실행하는 사용자에게 ADMIN, AUDITOR 또는 SERVER 특성이 있어야 합니다. 이 함수를 실행하려면 데이터베이스 파일에 대해 읽기 및 쓰기 권한이 있어야 합니다.

이 명령의 형식은 다음과 같습니다.

```
dbmgr {-dump|-d} [-h] [-r] [-f fileName] \
    [c] [fc] [g user] [l class] [p class] [fp class] \
    [d class [props|@fileName] \
    [dn class [props|@fileName] \
    [e class record [props|@fileName] \
    [en class record [props|@fileName] \
    [o class record [props|@fileName] \
    [on class record [props|@fileName]
```

-dump|-d

dbmgr 유틸리티의 데이터베이스 덤프 함수를 실행합니다.

-f fileName

표준 출력 장치 대신에 지정한 파일로 직접 출력합니다.

-h

이 함수에 대한 도움말을 표시합니다.

-r

현재 권한 부여 데몬에 사용되는 데이터베이스에 대한 정보를 표시합니다.

이 옵션을 생략할 경우 dbmgr 은 현재 디렉터리의 데이터베이스에 대한 정보를 표시합니다.

-c

데이터베이스의 정의된 모든 클래스 이름을 나열합니다.

d class [props|@fileName]

특정 클래스의 모든 레코드에 대한 선택된 속성 값을 표시합니다. class 매개 변수는 클래스를 지정합니다. props 매개 변수는 사용자가 값을 표시하고자 하는 속성 목록을 공백으로 구분하여 정의합니다.

파일에서 속성 목록을 읽으려면 "at" 기호(@)로 시작하여 파일의 전체 경로 이름을 지정하십시오. 파일에 나열되는 각 속성은 별도의 행에 나타나야 합니다.

속성을 지정하지 않으면 모든 속성의 값이 나열됩니다.

dn class [props|@fileName]

d 옵션과 같지만, 알 수 없는 값을 갖는 속성은 표시되지 않습니다.

e class record [props|@fileName]

지정한 레코드 한 개를 제외하고 특정 클래스의 모든 레코드에 대한 선택된 속성 값을 표시합니다. class 매개 변수는 클래스를 지정합니다. record 매개 변수는 목록에서 생략할 레코드 이름을 지정합니다. props 매개 변수는 사용자가 값을 표시하고자 하는 속성 목록을 공백으로 구분하여 정의합니다.

파일에서 속성 목록을 읽으려면 "at" 기호(@)로 시작하여 파일의 전체 경로 이름을 지정하십시오. 파일에 나열되는 각 속성은 별도의 행에 나타나야 합니다.

속성을 지정하지 않으면 모든 속성의 값이 나열됩니다.

en class record [props|@fileName]

e 옵션과 같지만, 알 수 없는 값을 갖는 속성은 표시되지 않습니다.

fc

데이터베이스에 있는 모든 클래스에 대한 모든 클래스 정보를 나열합니다.

fp class

지정한 클래스의 속성에 대한 모든 속성 정보를 나열합니다.

g user

지정한 사용자가 속한 그룹을 나열합니다.

l class

지정된 클래스에 있는 레코드를 모두 나열합니다.

o class record property / on class record property

특정 클래스의 레코드 한 개에 대한 선택된 속성 값을 표시합니다. class 매개 변수는 클래스를 지정합니다. record 매개 변수는 레코드를 지정합니다. props 매개 변수는 사용자가 값을 표시하고자 하는 속성 목록을 공백으로 구분하여 정의합니다.

파일에서 속성 목록을 읽으려면 "at" 기호(@)로 시작하여 파일의 전체 경로 이름을 지정하십시오. 파일에 나열되는 각 속성은 별도의 행에 나타나야 합니다.

속성을 지정하지 않으면 모든 속성의 값이 나열됩니다.

o class record property / on class record property

o 옵션과 같지만, 알 수 없는 값을 갖는 속성은 표시되지 않습니다.

p class

지정된 클래스의 속성 이름을 나열합니다.

참고: -r 및 -f 를 제외하고 다른 한 옵션만 지정할 수 있습니다.

dbmgr -export 함수-데이터베이스를 정의하는 스크립트 작성

dbmgr -export 함수는 다른 스테이션에 있는 데이터베이스를 복제하며, 기존 데이터베이스를 정의하는 데 필요한 selang 명령으로 구성된 스크립트를 생성합니다.

참고: 데이터베이스 파일이 동일한 바이트 순서를 사용하지 않는 경우, UNIX 의 cp 나 tar 또는 Windows 의 복사와 같은 기본 명령을 사용하여 아키텍처 간에 데이터베이스 파일을 복사할 수 없습니다. 예를 들어, Sparc 기반 컴퓨터와 Intel 기반 컴퓨터는 각각 서로 다른 바이트 순서를 사용하므로, 두 컴퓨터 간에 데이터베이스를 복사할 수 없습니다.

중요! 실행하기 전에 스크립트를 검토하십시오.

이 명령의 형식은 다음과 같습니다.

```
dbmgr {-export|-e} {-l|-r} [-c className] [-f fileName]
```

-export|-e

dbmgr 유틸리티의 데이터베이스 내보내기 함수를 실행합니다.

-h

이 함수에 대한 도움말을 표시합니다.

-l

현재 디렉터리의 데이터베이스를 내보냅니다.

참고: 이 옵션은 CA Access Control 데몬이 실행되고 있지 않은 것으로 가정합니다. 데몬이 실행 중인 경우에는 데몬에서 사용 중인 데이터베이스가 아닌 다른 데이터베이스에서 작업하고 있다고 가정합니다.

-r

현재 CA Access Control 에서 사용되고 있는 데이터베이스를 내보냅니다. ADMIN 또는 SERVER 특성을 가지고 있어야 하며 CA Access Control 데몬이 실행되고 있어야 합니다.

-c className

데이터베이스에서 내보내고자 하는 클래스의 목록을 공백으로 구분하여 정의합니다.

-f fileName

표준 출력 장치 대신에 지정한 파일로 직접 출력합니다. 그러면 selang 을 사용하여 파일에서 명령을 읽도록 지시하여 파일에서 새 데이터베이스를 작성할 수 있습니다.

dbmgr -migrate 함수-데이터를 플랫 파일로 복사

dbmgr -migrate 함수는 기존 데이터베이스에 있는 사용자 및 프로그램 레코드의 데이터를 플랫 파일(바이너리 형식)에 복사합니다. 또한 플랫 파일의 데이터를 새 데이터베이스로 복사할 수 있습니다. 데이터를 가져올 데이터베이스는 버전 1.21 이상이어야 합니다.

플랫 파일을 새 데이터베이스에 복사하는 경우 플랫 파일 작성에 사용한 이 함수의 동일한 버전을 사용하십시오. 여러 버전이 있는 경우 최신 버전을 사용하는 것이 좋습니다.

참고: 데이터를 이전 데이터베이스에서 새 데이터베이스로 복사한 후에는 보안을 위해 이전 데이터베이스, 새 데이터베이스 작성에 사용된 스크립트 및 이 함수로 만든 플랫 파일을 삭제하십시오.

중요! 이 함수를 사용하기 전에 항상 데이터베이스의 백업을 작성합니다.

이 명령의 형식은 다음과 같습니다.

```
dbmgr {migrate|-m} {-r|-w|-h} [-s] filename \
    [-v versionNumber] [-f fileName]
```

-migrate|-m

dbmgr 유틸리티의 데이터베이스 마이그레이션 함수를 실행합니다.

filename

데이터를 복사할 플랫 파일을 정의합니다.

-f filename

표준 출력 장치 대신에 지정한 파일로 직접 출력합니다.

-h

이 함수에 대한 도움말을 표시합니다.

-r

현재 디렉터리의 데이터베이스를 읽고 특정 데이터를 플랫 파일 filename 으로 복사합니다.

-s

데이터베이스를 직접 읽지 않고 CA Access Control 서버를 사용하여 데이터베이스의 정보를 읽습니다. 이 옵션은 -r 스위치와 함께 사용할 경우에만 유효합니다.

이 옵션을 사용하려면 터미널에 대한 관리자 권한과 R(읽기) 및 W(쓰기) 액세스 권한이 있어야 합니다.

이 옵션을 지정하지 않으면 현재 디렉터리의 데이터베이스에서 읽기 또는 쓰기가 수행됩니다.

-v versionNumber

이전 버전에서 작성된 플랫 파일을 읽습니다. 이 옵션은 -w 명령어만 유효합니다. 파일 이름 뒤에 이 옵션을 입력하고 버전 번호를 제공하십시오.

-w

플랫 파일 filename 을 읽고 현재 디렉터리의 데이터베이스로 데이터를 복사합니다.

예: 기존 데이터베이스에서 새 데이터베이스로 데이터 복사

다음 단계는 기존 데이터베이스에서 새 데이터베이스로 데이터를 복사하는 방법을 설명합니다. 이전 데이터베이스는 /tmp/old_db 디렉터리에 있다고 가정합니다. 새 데이터베이스는 ACInstallDir/seosdb 디렉터리에 있다고 가정합니다. 여기서 ACInstallDir 은 CA Access Control 이 설치된 디렉터리입니다.

참고: 이 절차는 UNIX 경로 이름을 사용하여 작성되지만, 경로 이름을 적절히 수정하면 Windows 에서도 사용할 수 있습니다.

1. 슈퍼 사용자로 로그인합니다.
2. CA Access Control 데몬이 실행되고 있으면 다음 명령을 사용하여 종료합니다.

   ```
   secons -s
   ```

3. 이전 데이터베이스를 다른 위치 또는 백업 매체에 복사하여 이전 데이터베이스의 백업을 작성합니다.
4. 데이터베이스를 /tmp/old_db 로 복사한 다음, 이전 데이터베이스에서 dbmgr 유틸리티를 실행하여 이전 데이터베이스를 복제하는 스크립트를 생성합니다.

   ```
   cd /tmp/old_db
   /opt/CA/AccessControl/bin/dbmgr -export -l -f lang_script
   ```

5. 다음과 같이 새 데이터베이스를 작성합니다.

```
cd /opt/CA/AccessControl/seosdb
/opt/CA/AccessControl/bin/dbmgr -c -cq
```

6. 이전 단계에서 생성된 스크립트를 실행하여 다음과 같이 새 데이터베이스를 작성합니다.

```
cd /opt/CA/AccessControl/seosdb
/opt/CA/AccessControl/bin/selang -l /tmp/old_db/lang_script
```

7. dbmgr 유틸리티를 실행하여 이전 데이터베이스의 데이터를 포함하는 플랫 파일을 다음과 같이 작성합니다.

```
cd /tmp/old_db
/opt/CA/AccessControl/bin/dbmgr -migrate -r flat_file
```

8. 플랫 파일의 데이터를 다음과 같이 새 데이터베이스로 로드합니다.

```
cd /opt/CA/AccessControl/seosdb
/opt/CA/AccessControl/bin/dbmgr -migrate -w /tmp/old_db/flat_file
```

dbmgr -util 함수-기존 데이터베이스 관리

dbmgr -util 함수는 데이터베이스에서 관리 및 유지 관리 작업을 수행합니다. 현재 CA Access Control 이 실행되고 있지 않다고 가정합니다. 데이터베이스가 위치한 디렉터리에서 이 함수를 호출하십시오.

-util 옵션은 매개 변수 filename 에 의해 지정된 로컬 데이터베이스를 관리하고 처리하기 위해 사용됩니다. 데이터베이스 파일은 .dat 확장자를 가지며 DBIO 파일이어야 합니다. 데이터베이스 인덱스 파일(확장자가 .001 인 파일)은 -util 옵션과 함께 사용할 수 없습니다.

이 명령의 형식은 다음과 같습니다.

```
dbmgr {-util|-u} [-h] \
    [-all filename] \
    [-build filename] \
    [-check] \
    [-close] \
    [-dump filename] \
    [-dup src dst] \
    [-fast] \
    [-free filename] \
    [-index filename] \
    [-key filename] \
    [-load db ascii \
    [-scan filename] \
    [-scana filename] \
    [-stat filename] \
    [-verify] \
    [-f fileName]
```

-util-u

dbmgr 유틸리티의 데이터베이스 관리 및 유지 관리 함수를 실행합니다.

-all filename

모든 인덱스 검사를 수행합니다. -index 및 -free 옵션을 지정하는 것과 동일합니다.

-build filename

데이터 레코드를 기반으로 DBIO 인덱스를 작성합니다.

-check

(UNIX 전용). 모든 데이터베이스 파일의 모든 인덱스 항목에 대해 신속하게 온전성 검사(sanity check) 및 일관성 검사를 수행합니다.

-close

열려 있는 데이터베이스를 닫습니다.

-dump filename

표준 출력 장치에 ASCII 로 데이터 파일을 덤프합니다.

-dup src dst

파일 헤더를 기반으로 DBIO 파일을 복제합니다.

-f fileName

표준 출력 장치 대신에 지정한 파일로 직접 출력합니다.

-fast

모든 데이터베이스 파일의 모든 인덱스 항목에 대해 신속하게 온전성 검사(sanity check)를 수행합니다.

-free filename

사용 가능한 인덱스를 검사합니다.

-index filename

인덱스의 일관성을 검사합니다.

-key filename

인덱스 파일을 순차적으로 검색합니다.

-load db ascii

ASCII 파일을 로드하여 DBIO 파일로 변환합니다.

-scan filename

데이터베이스를 순서대로 검사합니다.

-scana filename

삭제된 레코드를 포함하여 데이터베이스를 순서대로 검사합니다.

-stat filename

데이터베이스 파일의 헤더 정보를 나열합니다.

-verify

(UNIX 전용). 미리 정의된 특정 개체가 데이터베이스에 있는지 확인합니다. 예를 들어, 모든 클래스에 대해 SEOS, ADMIN 및 UACC 가 있는지 확인합니다.

dbmgr -backup 함수 - 데이터베이스 백업

dbmgr -backup 함수는 지정된 디렉터리에 CA Access Control 데이터베이스의 온라인 백업을 작성합니다. 이 함수는 CA Access Control 데몬의 실행 여부와 관계없이 사용할 수 있습니다.

이 명령의 형식은 다음과 같습니다.

```
dbmgr {-backup|-b} backup_directory
```

-backup|-b

dbmgr 유틸리티의 데이터베이스 백업 함수를 실행합니다.

backup_directory

백업 디렉터리를 정의합니다. 이 디렉터리는 원격 컴퓨터에 둘 수 없습니다. 디렉터리가 없으면 자동으로 작성됩니다.

dbmgr -restore 함수-데이터베이스 복원

UNIX 에 해당

dbmgr -restore 함수는 지정한 디렉터리에서 CA Access Control 데이터베이스의 온라인 복원을 수행합니다. 이 함수는 CA Access Control 데몬의 실행 여부와 관계없이 사용할 수 있습니다.

이 명령의 형식은 다음과 같습니다.

```
dbmgr {-restore|-r} restore_directory
```

-restore|-r

dbmgr 유틸리티의 데이터베이스 복원 함수를 실행합니다.

restore_directory

복원하려는 데이터베이스가 있는 디렉터리를 정의합니다.

defclass 유틸리티-사용자 정의 자산 유형을 클래스로 정의

CA Access Control 은 각 CA Access Control 데이터베이스 및 정의된 모든 새 PMDB 에 있는 기본 Unicenter TNG 자산 유형을 정의합니다. defclass 스크립트는 사용자 정의된 보안 자산 유형을 CA Access Control 데이터베이스에 CA Access Control 클래스로서 정의합니다.

참고: Unicenter 통합을 선택하면 설치 프로그램이 자동으로 이 스크립트를 실행합니다. 이것은 새 PMDB 가 작성될 때마다 수동으로 호출되어야 합니다.

이 명령의 형식은 다음과 같습니다.

```
defclass
```

참고: UNIX 에서 이 유틸리티는 스크립트 파일로 제공되며, 이 유틸리티를 실행하려면 .sh 확장자를 지정해야 합니다. 이 유틸리티는 Unicenter 통합이 활성화된 경우에만 사용할 수 있습니다. Unicenter 통합은 기본적으로 비활성화되어 있습니다.

DictImport 유틸리티-사전 파일 가져오기

DictImport 유틸리티는 사전 파일을 준비하여 CA Access Control 데이터베이스로 가져옵니다. CA Access Control 을 설치한 후에는 암호 보호를 설정할 수 있도록 사전 파일을 CA Access Control 데이터베이스로 가져와서 활성화해야 합니다.

DictImport 유틸리티는 use_dbdict 암호 규칙을 db 로 설정하고 DICTIONARY 클래스 및 PASSWORD 클래스를 활성화합니다.

참고: PASSWORD 클래스가 활성화되어 있지 않으면 중앙 집중화된 사전이 비활성화됩니다.

이 명령의 형식은 다음과 같습니다.

```
DictImport [-h] [-o selangFilename] [-f dictionaryFilename]
```

참고: 이 유틸리티는 스크립트 파일로 제공되며 lbin 디렉터리에 있습니다.

-f dictionaryFilename

지정된 파일에서 사전 단어를 모두 가져오는 selang 명령을 생성합니다. 이 옵션을 생략하면 구성 설정의 값을 기반으로 사전 파일이 정의됩니다.

-h

이 유틸리티에 대한 도움말을 표시합니다.

-o selangFilename

selang 명령을 지정된 파일에 씁니다. 이 옵션을 생략하면 표준 출력 장치에 selang 명령이 기록됩니다.

dmsmgr 유틸리티

dmsmgr 유틸리티를 사용하면 고급 정책 관리 인프라를 관리할 수 있습니다. 인프라 구성 요소에는 CA Access Control 끝점, DMS(Deployment Map Server) 및 DH(배포 호스트)가 포함됩니다.

이 유틸리티는 여러 작업을 처리하며 다음과 같은 관련 함수를 가지고 있습니다.

작업	함수
DMS 또는 DH 작성 (페이지 43)	`dmsmgr -create`
DMS 또는 DH 제거 (페이지 45)	`dmsmgr -remove`
DMS 데이터베이스에서 사용하지 않는 노드 제거 (페이지 45)	`dmsmgr -cleanup`
고급 정책 관리 구성 (페이지 46)	`dmsmgr -config`
DMS 또는 DH 복원 (페이지 47)	`dmsmgr -restore`

dmsmgr -create 함수-DMS 또는 DH 작성

dmsmgr -create 함수는 CA Access Control 이 설치된 컴퓨터에 DMS 또는 DH 를 작성합니다.

참고: 설치하는 동안에 DMS 또는 DH 를 작성할 수도 있습니다.

참고: 이 유틸리티를 실행하는 사용자에게는 항상 작성된 DMS 또는 DH 에 대한 관리 권한이 부여됩니다.

이 명령의 형식은 다음과 같습니다.

```
dmsmgr -create -auto [-admin user [,user...]] [-xadmin user [,user...]] \
[-desktop hosts]

dmsmgr -create -dms name \
[-admin user [,user...]] [-xadmin user [,user...]] \
[-desktop hosts] [-subscriber dh-names]

dmsmgr -create -dh name [-parent dms_name@hostname] \
[-admin user [,user...]] [-xadmin user [,user...]] \
[-desktop hosts]
```

-admin user [,user...]]

(선택 사항) 내부 사용자를 작성된 DMS 또는 DH 의 관리자로 정의합니다.

-auto

DMS 및 DH 를 기본 이름(DMS__, DH__ 및 DH__WRITER)으로 작성합니다.

DMS 와 DH 그리고 이들 사이의 필수 연결을 손쉽게 작성하려면 이 옵션을 사용하십시오.

-desktop hosts

(선택 사항) 작성된 DMS 또는 DH 가 있는 컴퓨터에 대해 TERMINAL 액세스 권한을 갖는 컴퓨터의 목록을 쉼표로 구분하여 정의합니다.

참고: 지정하든 안 하든, 이 유틸리티를 실행하는 터미널에는 항상 작성된 DMS 또는 DH 에 대한 관리 권한이 부여됩니다.

-dh name

로컬 호스트에 지정된 name 으로 DH 를 작성합니다.

참고: 이 옵션을 사용하여 DH 를 작성하는 경우, DH 가 이미 구독되어 있고 이전에 전송된 정책이 없더라도 CA Access Control 에서는 DMS 와 DH 를 동기화해야 함을 사용자에게 알리는 메시지를 표시합니다. 이 메시지는 수행해야 하는 단계를 미리 알려주는 것이며 실제 상황을 나타내는 것이 아닐 수 있습니다. 필수 단계를 모두 완료한 경우 이를 무시해도 됩니다.

-dms name

로컬 호스트에 지정된 name 으로 DMS 를 작성합니다.

-parent dms_name@hostname

(선택 사항) 작성된 DH 가 끝점 알림을 전송할 DMS 를 정의합니다. DMS 는 DMS_name@hostname 형식으로 지정하십시오.

-subscriber dh_names

(선택 사항) 작성된 DMS 가 정책을 업데이트할 DH PMDB 의 목록을 쉼표로 구분하여 정의합니다. 각 DH 는 DH_name@hostname 형식으로 지정하십시오.

-xadmin user [,user...]]

(선택 사항) 엔터프라이즈 사용자를 작성된 DMS 또는 DH 의 관리자로 정의합니다.

dmsmgr -remove 함수-DMS 또는 DH 제거

dmsmgr -remove 함수는 CA Access Control 이 설치된 컴퓨터에서 DMS 또는 DH 를 제거합니다.

이 명령의 형식은 다음과 같습니다.

```
dmsmgr -remove {-dms|dh} name
```

```
dmsmgr -remove -auto
```

-auto

기본 DMS 및 DH 를 로컬 호스트에서 제거합니다.

이들은 설치 중에 또는 dmsmgr -create -auto 를 사용할 때 기본적으로 작성된 DMS 및 DH 데이터베이스입니다.

-dh name

지정된 name DH 를 로컬 호스트에서 제거합니다.

-dms name

지정된 name DMS 를 로컬 호스트에서 제거합니다.

dmsmgr -cleanup 함수-사용하지 않는 노드 제거

dmsmgr -cleanup 함수는 DMS 또는 DH 데이터베이스에서 사용하지 않는 노드를 제거합니다. 이들은 지정한 시간 동안 사용 가능하지 않던 CA Access Control 노드를 나타내는 HNODE 개체입니다.

참고: 일상적인 유지 관리 절차로서 DMS 및 DH 에서 이런 사용하지 않는 노드를 정리해야 합니다.

이 명령의 형식은 다음과 같습니다.

```
dmsmgr -cleanup {-hnode|-deployment} -days number {-dms|-dh} name
```

```
dmsmgr -cleanup -policy name -vcount number {-dms|dh} name
```

-hnode

number 일보다 오래 사용할 수 없었던 CA Access Control 노드에 해당하는 HNODE 개체를 제거합니다.

-deployment

number 일보다 오래된 DEPLOYMENT 개체를 제거합니다.

-policy name

지정된 정책에 속하며 number 버전보다 오래된 POLICY 개체(정책 버전)를 제거합니다.

-dh name

사용하지 않는 노드를 제거하고자 하는 DH 의 이름을 정의합니다.

-dms name

사용하지 않는 노드를 제거하고자 하는 DMS 의 이름을 정의합니다.

-vcount

유지할 버전 수를 정의합니다.

dmsmgr -config 함수-고급 정책 관리 구성

dmsmgr -config 함수는 고급 정책 관리를 구성합니다.

이 명령의 형식은 다음과 같습니다.

```
dmsmgr -config[-] [host_name] {-endpoint|-dhname names|-drname names}
```

-config[-]

고급 정책 관리를 구성하거나 구성을 제거합니다.

-dhname names

쉼표로 구분된 배포 호스트 목록과 함께 사용할 끝점을 구성합니다.

-drname names

쉼표로 구분된 재해 복구 배포 호스트 목록과 함께 사용할 끝점을 구성합니다.

-endpoint

고급 정책 관리를 위한 끝점을 구성합니다.

host_name

host_name 에서 구성을 수행합니다. 호스트가 지정되어 있지 않으면 로컬 컴퓨터에서 구성을 수행합니다.

dmsmgr -restore 기능 - DMS 또는 DH 복원

dmsmgr -restore 기능은 백업 파일에서 DMS 또는 DH 를 복원합니다. CA Access Control 이 실행 중이거나 중지되었을 때 기존 DMS 위에 또는 새 디렉터리로 DMS 또는 DH 를 복원할 수 있습니다.

이 명령의 형식은 다음과 같습니다.

```
dmsmgr -restore -dms name -source path\
[-replica name|-parent name] [-subscriber dhname[,dhname...]]\
[-admin user[,user...]] [-xadmin user[,user...]]

dmsmgr -restore -dh name -source path\
[-parent name] [-admin user[,user...]]\
[-xadmin user[,user...]] [-desktop host[,host...]]
```

-admin user[,user...]

(UNIX) 내부 사용자를 복원된 DMS 또는 DH 의 관리자로 정의합니다.

-desktop host[, host...]

(선택 사항) 복원된 DH 가 있는 컴퓨터에 대해 TERMINAL 액세스 권한을 갖는 컴퓨터의 목록을 정의합니다.

참고: 지정 여부에 관계없이 이 유틸리티를 실행하는 터미널에는 복원된 DH 에 대한 관리 권한이 항상 부여됩니다.

-dh name

로컬 호스트에 복원된 DH 의 이름을 정의합니다.

-dms name

로컬 호스트에 복원된 DMS 이름을 정의합니다.

-parent name

(선택 사항) 구독자 부모의 이름을 정의합니다. 재해 복구 배포에서 CA Access Control 을 설정한 경우 재해 복구 DMS 또는 DH 를 복원하려면 이 매개 변수를 사용하십시오. 재해 복구 DMS 를 복원하는 경우에는 프로덕션 DMS 의 이름을 지정하고, DH 를 복원하는 경우에는 부모 DMS 의 이름을 지정하십시오. 부모는 name@hostname 형식으로 지정하십시오.

-replica name

(선택 사항) 재해 복구 DMS 의 이름을 정의합니다. 재해 복구 배포에서 CA Access Control 을 설정한 경우 프로덕션 DMS 를 복원하려면 이 매개 변수를 사용하십시오. 재해 복구 DMS 이름은 DMS_name@hostname 형식으로 지정하십시오.

-source path

복원할 백업 파일이 있는 디렉터리를 정의합니다.

-subscriber dh_name[, dh_name...]

(선택 사항) 복원된 DMS 가 정책 업데이트를 보낼 DH 의 목록을 쉼표로 구분하여 정의합니다. 각 DH 는 DH_name@hostname 형식으로 지정하십시오.

-xadmin user[,user...]

(UNIX) 엔터프라이즈 사용자를 복원된 DMS 또는 DH 의 관리자로 정의합니다.

eacpg_gen 유틸리티-모범 사례 정책 정의

eacpg_gen 을 정책 생성기라고도 합니다. 이 메뉴 방식의 유틸리티는 CA Access Control 응용 프로그램에 대한 정책을 정의할 수 있는 손쉬운 방법을 제공합니다. 정책 생성기는 CA Access Control 규칙이 없는 테스트 시스템에서 사용할 수 있습니다. 정책 생성기의 목적은 중요한 전자 자산에 보안 모범 사례를 적용하여 엔터프라이즈 응용 프로그램 및/또는 운영 체제와 해당 기밀 데이터를 보호하는 것입니다.

"기본 거부(default-deny)" 패러다임과 함께 응용 프로그램 셀이 작성됩니다. 이러한 정책은 UNIX chroot() jail 의 개념과 유사합니다. 인터넷에 연결된 응용 프로그램에 대해 그러한 정책이 생성되면 해당 응용 프로그램을 사용하는 호스트 절충의 위험이 크게 줄어듭니다.

응용 프로그램 셀은 응용 프로그램을 차단하는 ACL(Access Control List - 액세스 제어 목록) 규칙입니다. eacpg_gen 은 각 응용 프로그램에 대해 다수의 응용 프로그램 셀을 생성합니다. 응용 프로그램 셀은 특정 리소스에 대해서만 액세스를 적용합니다. 셀 정책으로 보호되는 프로세스는 정책에서 특별히 액세스가 허용되지 않은 리소스에 액세스할 수 없습니다. 따라서 잠재적인 공격자가 디스크의 인증되지 않은 영역에 쓰거나 인증되지 않은 바이너리를 실행하는 것을 막을 수 있습니다.

참고: 이 유틸리티를 실행하기 전에 secadmin 및 그룹 secadmins 가 데이터베이스에 있는지 확인하십시오.

정책 생성에는 몇 가지 주요 단계가 있습니다.

- 초기화
- 응용 프로그램 조사
- 응용 프로그램 테스트
- 정책 생성

- 정책 적용
- 정책 테스트

이 명령의 형식은 다음과 같습니다.

```
eacpg_gen \
    [-u user] \
    [-g group] \
    [-p path] \
    [-o owner] \
    [-w wheel] \
    [-m machine] \
    [-a] \
    [-s file] \
    [-# step] \
    [-x]
```

-u user

프로세스를 실행할 사용자를 지정합니다.

-g group

프로세스를 소유할 그룹 이름을 지정합니다.

-p path

프로그램에 대한 전체 경로를 지정합니다.

-o owner

정책 소유자를 지정합니다.

-w wheel

'secadmins' 그룹으로서 설정합니다(권장).

-m machine

컴퓨터 이름을 지정합니다.

-a

생성된 규칙의 적용 여부를 설정합니다.

-s file

정책 규칙을 저장하기 위한 전체 경로와 파일 이름을 지정합니다.

-# step 1-2

2 로 설정해야 합니다.

-x

경고 모드와 실패 모드 간에 전환됩니다.

예: 정책 생성기 실행

1. (초기화). 정책 생성기를 실행합니다.

   ```
   eacpg_gen
   ```

2. 시스템을 경고 모드에 두려면 프롬프트에 **y** 를 입력합니다.
3. 정책 생성기에 실행 파일에 대한 전체 경로를 제공합니다. 예를 들면 다음과 같습니다.

   ```
   /work/WebServers/apache_1.3.26/bin/htppd
   ```

4. 기본 사용자 이름을 그대로 사용합니다.
5. 기본 그룹 이름을 그대로 사용합니다.
6. 정보가 정확한지 확인하려면 프롬프트에 **y** 를 입력합니다.

   (응용 프로그램 조사). 정책 생성기가 정책을 만들 대상 프로세스에 대한 데이터를 수집하기 시작합니다.

7. 화면 정보를 확인하고 Enter 키를 누릅니다.
8. (응용 프로그램 테스트). 응용 프로그램을 시작합니다. 예:

   ```
   ./apachectl start
   ```

9. 응용 프로그램을 중지합니다. 예:

   ```
   ./apachectl stop
   ```

   참고: 응용 프로그램을 시작하고 중지한 이후의 이 시점이 응용 프로그램을 다시 시작하고 일반 사용 데이터를 수집하기에 가장 적합합니다. 이 조사가 실행되는 기간은 원하는 대로 설정할 수 있습니다. 더 오래 실행할수록 정책 생성기에서 더 많은 데이터를 수집하며, 그 결과 더 정확한 정책이 나오게 됩니다. 데이터를 충분히 수집했다고 생각되면 다음 단계로 진행하십시오.

10. (정책 생성). filename.txt 를 입력하고 Enter 키를 눌러 정책을 파일에 저장합니다.
11. (정책 적용). 정책을 적용하려면 **y** 를 입력합니다.

12. 시스템을 Fail 모드에 두고 정책 적용을 시작하려면 **y** 를 입력합니다.
13. (정책 테스트). 정책을 테스트합니다.

    다음은 evil.html 이라는 이름의 파일에 대한 정책 테스트를 보여주는 샘플 화면입니다.

```
Linux:/srv/www/htdocs: #telnet localhost 80
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
GET /evil.html
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>403 Forbidden</TITLE>
<HEAD><BODY>
<H1>Forbidden</H1>
You don't have permission to access /evil.html
on the server. <P>
<HR>
<ADDRESS>Apache/1.3.26 Server at linux.local Port 80</ADDRESS>
</BODY></HTML>
Connection closed by foreign host.
Linux:/srv/www/htdocs# []
```

    정책이 적용되었으므로 더 이상 evil.html 파일을 사용할 수 없습니다. 그 이유는 이 파일이 일반 사용 프로필의 범위를 벗어났기 때문입니다.

eACoexist 유틸리티-트러스트된 공존 프로그램 검색 및 등록

Windows 에 해당

eACoexist 유틸리티는 로컬 시스템에 공존하는 모든 프로그램을 검색합니다(예: CA Anti-Virus). 검색된 프로그램이 트러스트되는 경우 CA Access Control 에서 SPECIALPGM 규칙을 사용하여 프로그램을 등록합니다. 특수 프로그램 규칙은 해당 프로그램에 대한 액세스 유형을 정의하며 액세스 허용 시 CA Access Control 이 해당 프로그램을 바이패스하도록 합니다.

이 명령의 형식은 다음과 같습니다.

```
eACoexist [plug-in-path]
```

plug-in-path

(선택 사항) 공존 프로그램에서 사용할 공존 플러그인이 들어 있는 폴더의 경로를 정의합니다.

경로를 정의하지 않으면 공존 플러그인이 저장되어 있는 기본 경로(ACInstallDir/Coexistence)가 사용됩니다.

추가 정보:

공존 유틸리티 작동 방법 (페이지 52)
response.ini - 공존 유틸리티 구성 (페이지 66)

공존 유틸리티 작동 방법

CA Access Control 이 제공하는 공존 유틸리티(eACoexist)를 사용하면 로컬 컴퓨터에 있는 다른 프로그램과의 잠재적 충돌을 해결할 수 있습니다. CA Access Control 에서 이러한 잠재적 충돌을 해결하기 위해 수행하는 작업을 이해하고 충돌 해결 방법에 영향을 줄 수 있으려면 유틸리티 작동 방법을 이해해야 합니다.

공존 유틸리티는 실행 시 다음 작업을 수행합니다.

1. 다음 조건 중 하나가 적용되는지 확인합니다.
   a. CA Access Control 이 실행되고 있지 않습니다.
   b. 사용자가 ADMIN 특성을 가집니다.

   두 조건이 적용되지 않으면 유틸리티가 종료됩니다.
2. 다음과 같이 response.ini 파일을 찾습니다.
   - 유틸리티가 설치 중에 실행되는 경우 media_drive:\Coexistence_architecture 경로가 사용됩니다.
   - CA Access Control 이 컴퓨터에 설치되어 있으면 다음 레지스트리 키 값이 사용됩니다.

     ```
     HKLM\SOFTWARE\ComputerAssociates\AccessControl\AccessControl\SeOSD\Response
     File
     ```

   이 파일이 없으면 유틸리티가 종료됩니다.
3. 다음과 같이 공존 플러그인 디렉터리를 찾습니다.
   - 유틸리티를 실행하고 명령줄에서 매개 변수를 전달하면 이 매개 변수가 플러그인 경로로 사용됩니다.
   - 유틸리티가 설치 중에 실행되는 경우 media_drive:\Coexistence_architecture 경로가 사용됩니다.
   - 매개 변수 없이 유틸리티를 실행하면 다음 레지스트리 키 값에 "\Coexistence" 문자열이 연결됩니다.

     ```
     HKLM\SOFTWARE\ComputerAssociates\AccessControl\AccessControl\SeOSPath
     ```

   디렉터리가 없거나 공존 플러그인이 디렉터리에 없으면 유틸리티가 종료됩니다.

4. 검색 프로세스를 실행합니다.

   이 작업을 위해 유틸리티는 다음과 같이 공존 플러그인 디렉터리에 있는 실행 파일을 열거하고 하나씩 실행합니다.

   a. 플러그인 실행 결과를 %windir%\EACDiscovery.ini 에 저장합니다.

      참고: 플러그인 검색 프로세스가 성공적으로 완료되면 이 파일은 자동으로 삭제됩니다.

   b. 출력 파일 EACDiscovery.ini 가 있는지 확인합니다.

      이 파일이 없으면 유틸리티가 계속해서 다음 플러그인을 실행합니다.

   c. EACDiscovery.ini 의 각 제품 섹션에 대해 섹션(제품) 이름과 버전 값을 연결하고 응답 파일에 일치하는 섹션이 있는지 확인합니다.

      참고: response.ini 파일에는 각 공존 프로그램에 대한 섹션이 포함되어 있습니다. 섹션 이름이 버전 번호와 함께 표시되면(예: eTrust Audit-1.5) 유틸리티는 지정한 버전에 대해서만 작업을 수행합니다.

   d. 일치하는 섹션이 응답 파일에 있으면 다음과 같이 해당 섹션의 Act-Utility-0 값으로 설정된 작업을 실행합니다.

      - **1** - 검색된 제품이 CA Access Control 과 호환되지 않는다는 경고를 표시합니다.
      - **2** - 검색된 제품의 서비스를 중지합니다.

        유틸리티는 검색된 제품의 서비스를 EACDiscovery.ini 파일에서 검색합니다.
      - **3** - 2 와 동일하지만 CA Access Control 설치 중에 수행됩니다.
      - **4** - 검색된 제품의 서비스를 시작합니다.

        유틸리티는 검색된 제품의 서비스를 EACDiscovery.ini 파일에서 검색합니다.
      - **5** - 검색된 제품의 프로세스에 대해 트러스트된 프로그램 규칙(SPECIALPGM)을 만들고 CA Access Control 을 시작합니다.

        유틸리티는 검색된 제품의 프로세스를 EACDiscovery.ini 파일에서 검색합니다. 이 파일에서 해당 프로그램 유형(pgmtype)도 검색합니다. 그런 다음 CA Access Control 이 시작될 때 실행하는 임시 스크립트 파일(ACInstallDir\Data\discoveryscp)을 만듭니다.
      - **6** - 2 와 동일하지만 CA Access Control 제거 중에 수행됩니다.

      참고: 각 섹션에 작업이 두 개 이상 포함될 수 있습니다. 예를 들어 순서대로 실행되는 Act-Utility-0, Act-Utility-1 및 Act-Utility-2 가 있을 수 있습니다.

추가 정보:

Policy Manager 플러그인 작동 방법 (페이지 54)
BrightStor 플러그인 작동 방법 (페이지 55)
Dr. Watson 플러그인 작동 방법 (페이지 56)
eTrust AV 플러그인 작동 방법 (페이지 57)
Scout 플러그인 작동 방법 (페이지 58)
Unicenter 플러그인 작동 방법 (페이지 58)
Asset Management 플러그인 작동 방법 (페이지 59)
Windows 플러그인 작동 방법 (페이지 60)
eTrust Audit 플러그인 작동 방법 (페이지 60)
eTrust Audit80 플러그인 작동 방법 (페이지 62)
F-Secure Antivirus 플러그인 작동 방법 (페이지 63)
McAfee Antivirus 플러그인 작동 방법 (페이지 64)
Windows Modules Installer 플러그인 작동 방법 (페이지 64)
Services and Controller 플러그인 작동 방법 (페이지 65)
리소스 호스팅 하위 시스템 플러그 인이 작동하는 방법 (페이지 65)

Policy Manager 플러그인 작동 방법

공존 유틸리티는 CA Access Control 설치가 시작되기 전에 다음과 같이 Policy Manager 플러그인을 실행하여 컴퓨터에서 Policy Manager 레지스트리 키와 실행 파일을 검색합니다.

- 다음 레지스트리 키를 쿼리하여 존재하는지 확인합니다.

  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\SeAM.Exe

  레지스트리 키가 있으면 플러그인은 다음을 수행합니다.

  - Path 항목의 값을 읽습니다.
  - 다음과 같은 실행 파일 경로 이름을 반환합니다.

    FilePathFromRegistry\Bin\SeAM.exe
  - CA Access Control 설치 중에 호환성 경고를 표시합니다.

    이것은 응답 파일에 정의된 기본 작업입니다. Policy Manager 플러그인은 기본적으로 트러스트된 프로그램(SPECIALPGM) 규칙을 추가하지 않습니다.

참고: 응답 파일에 따라 공존 유틸리티가 미리 지정된 단계에서 수행하는 기본 작업(CA Access Control 설치 전, CA Access Control 설치 후 등에 수행할 작업)이 결정됩니다. 또한 Policy Manager 응용 프로그램은 CA Access Control 과 함께 더 이상 제공되지 않습니다.

BrightStor 플러그인 작동 방법

공존 유틸리티는 CA Access Control 설치가 끝날 때 및 유틸리티가 실행될 때마다 다음과 같이 BrightStor 플러그인을 실행하여 컴퓨터에서 CA BrightStor 레지스트리 키와 실행 파일을 검색합니다.

1. 다음 레지스트리 키를 쿼리하여 존재하는지 확인합니다.

   ```
   HKLM\SOFTWARE\ComputerAssociates\BrightStor ARCserve
   Backup\UniversalClientAgent\Common
   HKLM\SOFTWARE\ComputerAssociates\Cheetah\UniversalClientAgent\Common
   HKLM\SOFTWARE\ComputerAssociates\BrightStor Enterprise
   Backup\UniversalClientAgent\Common
   ```

   첫 번째 레지스트리 키가 있으면 플러그인은 다음을 수행합니다.

   - Path 항목의 값을 읽습니다.
   - 다음과 같은 실행 파일 경로 이름을 반환합니다.

     ```
     FilePathFromRegistry\UnivAgent.exe
     ```

   - DCM 유형의 SPECIALPGM 리소스를 만듭니다.

     이것은 응답 파일에 정의된 기본 작업입니다.

2. 1 단계에서 레지스트리 키를 찾을 수 없는 경우 플러그인은 다음 레지스트리 키를 쿼리하여 존재하는지 확인합니다.

   ```
   HKLM\SOFTWARE\ComputerAssociates\BrightStor ARCserve Backup\Base\Path
   HKLM\SOFTWARE\ComputerAssociates\Cheetah\Base\Path
   HKLM\SOFTWARE\ComputerAssociates\BrightStor Enterprise Backup\Base\Path
   ```

   첫 번째 레지스트리 키가 있으면 플러그인은 다음을 수행합니다.

   - HOME 항목의 값을 읽습니다.
   - 다음과 같은 실행 파일 경로 이름을 반환합니다.

     ```
     FilePathFromRegistry\carunjob.exe
     ```

   - DCM 유형의 SPECIALPGM 리소스를 만듭니다.

     이것은 응답 파일에 정의된 기본 작업입니다.

3. 2 단계에서도 레지스트리 키를 찾을 수 없는 경우 플러그인은 다음 레지스트리 키를 쿼리하여 존재하는지 확인합니다.

   ```
   HKLM\SOFTWARE\ComputerAssociates\ARCserveIT\Base\Path
   ```

   레지스트리 키가 있으면 플러그인은 다음을 수행합니다.

   - HOME 항목의 값을 읽습니다.
   - 다음과 같은 실행 파일 경로 이름을 반환합니다.

     ```
     FilePathFromRegistry\ASRunJob.exe
     ```

- DCM 유형의 SPECIALPGM 리소스를 만듭니다.

  이것은 응답 파일에 정의된 기본 작업입니다.

4. 다음 레지스트리 키를 쿼리하여 존재하는지 확인합니다.

   ```
   HKLM\SOFTWARE\ComputerAssociates\CA BAOF\CurrentVersion
   HKLM\SOFTWARE\ComputerAssociates\BrightStor Backup Agent for Open
   Files\CurrentVersion
   ```

   첫 번째 레지스트리 키가 있으면 플러그인은 다음을 수행합니다.

   - ServicePath 항목의 값을 읽습니다.
   - ServicePathFromRegistry 에 대해 DCM 유형의 SPECIALPGM 리소스를 만듭니다.

     이것은 응답 파일에 정의된 기본 작업입니다.

참고: 응답 파일에 따라 공존 유틸리티가 미리 지정된 단계에서 수행하는 기본 작업(CA Access Control 설치 전, CA Access Control 설치 후 등에 수행할 작업)이 결정됩니다.

Dr. Watson 플러그인 작동 방법

공존 유틸리티는 CA Access Control 설치가 끝날 때 및 유틸리티가 실행될 때마다 다음과 같이 Dr. Watson 플러그인을 실행하여 컴퓨터에서 Dr. Watson 실행 파일을 검색합니다.

- 다음 경로 이름을 쿼리하여 존재하는지 확인합니다.

  ```
  %windir%\system32\drwtsn32.exe
  ```

  파일이 있으면 플러그인은 DCM 유형의 SPECIALPGM 리소스를 만듭니다.

  이것은 응답 파일에 정의된 기본 작업입니다.

참고: 응답 파일에 따라 공존 유틸리티가 미리 지정된 단계에서 수행하는 기본 작업(CA Access Control 설치 전, CA Access Control 설치 후 등에 수행할 작업)이 결정됩니다.

eTrust AV 플러그인 작동 방법

공존 유틸리티는 CA Access Control 설치가 끝날 때 및 유틸리티가 실행될 때마다 다음과 같이 eTrust AV 플러그인을 실행하여 컴퓨터에서 CA Antivirus 레지스트리 키와 실행 파일을 검색합니다.

1. 다음 레지스트리 키 항목 값을 읽습니다.

   ```
   HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\InocIT.Exe\Path
   HKLM\SOFTWARE\ComputerAssociates\eTrustITM\CurrentVersion\Path\Home
   ```

   항목 중 하나에서 값이 반환되면 플러그인은 다음과 같은 DCM 유형의 SPECIALPGM 리소스를 만듭니다.

   - FilePathFromRegistry\InoRT.exe
   - FilePathFromRegistry\InoTask.exe
   - FilePathFromRegistry\InocIT.exe
   - FilePathFromRegistry\ShellScn.exe

   이것은 응답 파일에 정의된 기본 작업입니다.

2. 다음 레지스트리 키 항목 값을 읽습니다.

   ```
   HKLM\SOFTWARE\ComputerAssociates\ScanEngine\Path\Engine
   ```

   항목에서 값이 반환되면 플러그인은 다음과 같은 DCM 유형의 SPECIALPGM 리소스를 만듭니다.

   ```
   FilePathFromRegistry\InoCmd32.exe
   ```

참고: 응답 파일에 따라 공존 유틸리티가 미리 지정된 단계에서 수행하는 기본 작업(CA Access Control 설치 전, CA Access Control 설치 후 등에 수행할 작업)이 결정됩니다.

Scout 플러그인 작동 방법

공존 유틸리티는 CA Access Control 설치가 끝날 때 및 유틸리티가 실행될 때마다 다음과 같이 Scout 플러그인을 실행하여 컴퓨터에서 SurfControl Web Filter for Windows 레지스트리 키와 실행 파일을 검색합니다.

- 다음 레지스트리 키를 쿼리하여 존재하는지 확인합니다.

  `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\Scscout.Exe`

  레지스트리 키가 있으면 플러그인은 다음을 수행합니다.

  - Path 항목의 값을 읽습니다.
  - 다음과 같은 실행 파일 경로 이름을 반환합니다.

    `FilePathFromRegistry\scoutsvc.exe`
  - DCM 유형의 SPECIALPGM 리소스를 만듭니다.

    이것은 응답 파일에 정의된 기본 작업입니다.

참고: 응답 파일에 따라 공존 유틸리티가 미리 지정된 단계에서 수행하는 기본 작업(CA Access Control 설치 전, CA Access Control 설치 후 등에 수행할 작업)이 결정됩니다.

Unicenter 플러그인 작동 방법

공존 유틸리티는 CA Access Control 설치가 끝날 때 및 유틸리티가 실행될 때마다 다음과 같이 Unicenter 플러그인을 실행하여 컴퓨터에서 CA Unicenter 레지스트리 키와 실행 파일을 검색합니다.

1. CAUENV.dll 을 사용하여 CA Unicenter 디렉터리의 경로(UniPath)를 검색합니다.
2. 다음과 같은 DCM 유형의 SPECIALPGM 리소스를 만듭니다.
   - UniPath\Bin\sfauditd.exe
   - UniPath\Bin\secdos2.exe
   - UniPath\Bin\caulgnd.exe
   - UniPath\Bin\sccommit.exe
   - UniPath\Bin\dsbulist.exe
   - UniPath\Bin\fmpost.exe
   - UniPath\Bin\catlbl.exe
   - UniPath\Bin\caanal.exe
   - UniPath\Bin\cascan.exe
   - UniPath\Bin\causamd.exe

- UniPath\Bin\acbrows.exe
- UniPath\Bin\secadmin.exe
- UniPath\Bin\dsbufcrt.exe
- UniPath\Bin\cnvpwd.exe
- UniPath\Bin\fmeng.exe
- UniPath\Bin\fmmscan.exe
- UniPath\Bin\cadevscn.exe
- UniPath\AGENTS\Bin\prfagent.exe
- UniPath\AGENTS\Bin\msexchagnt.exe

참고: 응답 파일에 따라 공존 유틸리티가 미리 지정된 단계에서 수행하는 기본 작업(CA Access Control 설치 전, CA Access Control 설치 후 등에 수행할 작업)이 결정됩니다.

Asset Management 플러그인 작동 방법

공존 유틸리티는 CA Access Control 설치가 끝날 때 및 유틸리티가 실행될 때마다 다음과 같이 Asset Management 플러그인을 실행하여 컴퓨터에서 Unicenter DSM 서비스를 검색합니다.

1. "CA Unicenter NSM Systems Performance Agent for UAM" 서비스 실행 파일의 디렉터리 경로(ServicePath)를 추출합니다.
2. 다음과 같은 REGISTRY 유형의 SPECIALPGM 리소스를 만듭니다.

   ```
   ServicePath\agents\bin\hpacbcol.exe
   ```

3. "caf" 서비스 실행 파일의 디렉터리 경로(ServicePath)를 추출합니다.
4. 다음과 같은 REGISTRY 유형의 SPECIALPGM 리소스를 만듭니다.

   ```
   ServicePath\PMAgent\agents\bin\hpacbcol.exe
   ```

또한 공존 유틸리티는 CA Access Control 설치가 끝날 때 및 유틸리티가 실행될 때마다 다음과 같이 Asset Management 플러그인을 실행하여 컴퓨터에서 Unicenter Asset Management Version 4 서비스를 검색합니다.

1. "CA Unicenter NSM Systems Performance Agent for UAM" 서비스 실행 파일의 디렉터리 경로(ServicePath)를 추출합니다.
2. 다음과 같은 REGISTRY 유형의 SPECIALPGM 리소스를 만듭니다.

   ```
   ServicePath\agents\bin\hpacbcol.exe
   ```

또한 공존 유틸리티는 CA Access Control 설치가 끝날 때 및 유틸리티가 실행될 때마다 다음과 같이 Asset Management 플러그인을 실행하여 컴퓨터에서 Unicenter DSM r11 서비스를 검색합니다.

1. "caf" 서비스 실행 파일의 디렉터리 경로(ServicePath)를 추출합니다.
2. 다음과 같은 REGISTRY 유형의 SPECIALPGM 리소스를 만듭니다.

   ```
   ServicePath\PMAgent\agents\bin\hpacbcol.exe
   ```

참고: 응답 파일에 따라 공존 유틸리티가 미리 지정된 단계에서 수행하는 기본 작업(CA Access Control 설치 전, CA Access Control 설치 후 등에 수행할 작업)이 결정됩니다.

Windows 플러그인 작동 방법

공존 유틸리티는 CA Access Control 설치가 끝날 때 및 유틸리티가 실행될 때마다 다음과 같이 Windows 플러그인을 실행하여 컴퓨터에서 Windows 서비스와 레지스트리 키를 검색합니다.

1. "WinMgmt" 서비스 실행 파일의 디렉터리 경로(ServicePath)를 추출합니다.
2. 다음과 같은 REGISTRY 유형의 SPECIALPGM 리소스를 만듭니다.

   ```
   ServicePath
   ```

   이것은 응답 파일에 정의된 기본 작업입니다.
3. 다음과 같은 PBF 유형의 SPECIALPGM 리소스를 만듭니다.

   ```
   %windir%\System32\cidaemon.exe
   ```

   이것은 응답 파일에 정의된 기본 작업입니다.

참고: 응답 파일에 따라 공존 유틸리티가 미리 지정된 단계에서 수행하는 기본 작업(CA Access Control 설치 전, CA Access Control 설치 후 등에 수행할 작업)이 결정됩니다.

eTrust Audit 플러그인 작동 방법

공존 유틸리티는 CA Access Control 설치가 시작되기 전에 다음과 같이 eTrust Audit 플러그인을 실행하여 컴퓨터에서 eTrust Audit Version 1.5 레지스트리 키와 파일을 검색합니다.

1. 다음 레지스트리 키를 쿼리하여 존재하는지 확인합니다.

   ```
   HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\acdistagn.exe
   ```

   성공하면 `%PathFromRegistry%`로 지정된 "Path" 값을 추출합니다.

   레지스트리 키가 있으면 플러그인은 다음을 수행합니다.

   - Path 항목의 값을 읽습니다.

- 다음과 같은 실행 파일 경로 이름을 반환합니다.

  ```
  FilePathFromRegistry\bin\acactmgr.exe
  FilePathFromRegistry\bin\SeLogRcd.exe
  FilePathFromRegistry\bin\acdistagn.exe
  FilePathFromRegistry\acdistsrv.exe
  FilePathFromRegistry\acfwrecd.exe
  FilePathFromRegistry\acrecorderd.exe
  FilePathFromRegistry\aclogrd.exe
  FilePathFromRegistry\portmap.exe
  FilePathFromRegistry\SeLogRec.exe
  FilePathFromRegistry\SeLogRd.exe
  FilePathFromRegistry\snmprec.exe
  ```

  이것은 응답 파일에 정의된 기본 작업입니다. eTrust Audit 플러그인은 기본적으로 트러스트된 프로그램(SPECIALPGM) 규칙을 추가하지 않습니다.

2. 다음 서비스를 중지합니다.
   - "eAudit Action Manager"
   - "eAudit Distribution Agent"
   - "eAudit Log Router"
   - "eAudit Recorder"
   - "eAudit Redirector"
   - "eAudit Portmap"

   eTrust Audit 최신 버전이 설치되어 있으면 다음 서비스를 중지합니다.
   - "eTrust Audit Action Manager"
   - "eTrust Audit Collector"
   - "eTrust Audit Distribution Agent"
   - "eTrust Audit Distribution Server"
   - "eTrust Audit FW-1 Recorder"
   - "eTrust Audit Generic Recorder"
   - "eTrust Audit Log Router"
   - "eTrust Audit Portmap"
   - "eTrust Audit Recorder"
   - "eTrust Audit Redirector"
   - "eTrust Audit SNMP Recorder"
3. CA Access Control 설치가 완료되면 동일한 서비스를 다시 시작합니다.

또한 공존 유틸리티는 eTrust Audit 플러그인을 실행하여 다음을 수행합니다.

- CA Access Control 을 제거할 때 eTrust Audit 서비스를 중지합니다.
- CA Access Control 제거가 완료된 후 eTrust Audit 서비스를 시작합니다.

참고: 응답 파일에 따라 공존 유틸리티가 미리 지정된 단계에서 수행하는 기본 작업(CA Access Control 설치 전, CA Access Control 설치 후 등에 수행할 작업)이 결정됩니다.

eTrust Audit80 플러그인 작동 방법

공존 유틸리티는 CA Access Control 설치가 끝날 때 및 유틸리티가 실행될 때마다 다음과 같이 eTrust Audit80 플러그인을 실행하여 컴퓨터에서 eTrust Audit r8 레지스트리 키와 파일을 검색합니다.

- 다음 레지스트리 키를 쿼리하여 존재하는지 확인합니다.

  HKLM\SOFTWARE\ComputerAssociates\eTrust Audit\Paths

  성공하면 %PathFromRegistry%로 지정된 "Path" 값을 추출합니다.

  레지스트리 키가 있으면 플러그인은 다음을 수행합니다.

  - RootPath 항목의 값을 읽습니다.
  - 다음과 같은 DCM 유형의 SPECIALPGM 리소스를 만듭니다.

    FilePathFromRegistry\bin\acactmgr.exe
    FilePathFromRegistry\bin\SeLogRcd.exe
    FilePathFromRegistry\bin\acdistagn.exe
    FilePathFromRegistry\acdistsrv.exe
    FilePathFromRegistry\acfwrecd.exe
    FilePathFromRegistry\acrecorderd.exe
    FilePathFromRegistry\aclogrd.exe
    FilePathFromRegistry\portmap.exe
    FilePathFromRegistry\SeLogRec.exe
    FilePathFromRegistry\SeLogRd.exe
    FilePathFromRegistry\snmprec.exe

    이것은 응답 파일에 정의된 기본 작업입니다.

참고: 응답 파일에 따라 공존 유틸리티가 미리 지정된 단계에서 수행하는 기본 작업(CA Access Control 설치 전, CA Access Control 설치 후 등에 수행할 작업)이 결정됩니다.

F-Secure Antivirus 플러그인 작동 방법

공존 유틸리티는 다음과 같이 F-Secure Antivirus 플러그인을 실행하여 컴퓨터에서 F-Secure Anti-Virus 레지스트리 키와 파일을 검색합니다.

- CA Access Control 설치가 시작되기 전에 플러그인에서 F-Secure Anti-Virus 서비스를 중지합니다.
- CA Access Control 설치가 완료되면 플러그인은 다음 레지스트리 키를 쿼리하여 존재하는지 확인합니다.

  ```
  HKLM\SOFTWARE\Data Fellows\F-Secure\Anti-Virus
  ```

  성공하면 %PathFromRegistry%로 지정된 "Path" 값을 추출합니다.

  레지스트리 키가 있으면 플러그인은 다음을 수행합니다.

  - Path 항목의 값을 읽습니다.
  - 다음과 같은 DCM 유형의 SPECIALPGM 리소스를 만듭니다.

    ```
    FilePathFromRegistry\fssm32.exe
    FilePathFromRegistry\fsgk32st.exe
    ```

    이것은 응답 파일에 정의된 기본 작업입니다. eTrust Audit 플러그인은 기본적으로 트러스트된 프로그램(SPECIALPGM) 규칙을 추가하지 않습니다.
- 공존 유틸리티가 실행될 때마다 플러그인은 다음을 수행합니다.

  a. F-Secure Anti-Virus 서비스를 중지합니다.

  b. 이 항목의 앞부분에서 설명한 대로 CA Access Control 설치가 완료될 때 만드는 것과 동일한 SPECIALPGM 리소스를 만듭니다.

  c. F-Secure Anti-Virus 서비스를 다시 시작합니다.

참고: 응답 파일에 따라 공존 유틸리티가 미리 지정된 단계에서 수행하는 기본 작업(CA Access Control 설치 전, CA Access Control 설치 후 등에 수행할 작업)이 결정됩니다.

McAfee Antivirus 플러그인 작동 방법

공존 유틸리티는 CA Access Control 설치가 끝날 때 및 유틸리티가 실행될 때마다 다음과 같이 McAfee VirusScan 플러그인을 실행하여 컴퓨터에서 McAfee VirusScan 서비스를 검색합니다.

1. "McShield" 서비스 실행 파일의 디렉터리 경로(ServicePath)를 추출합니다.
2. 다음과 같은 DCM 유형의 SPECIALPGM 리소스를 만듭니다.

   `ServicePath`

   이것은 응답 파일에 정의된 기본 작업입니다.

참고: 응답 파일에 따라 공존 유틸리티가 미리 지정된 단계에서 수행하는 기본 작업(CA Access Control 설치 전, CA Access Control 설치 후 등에 수행할 작업)이 결정됩니다.

Windows Modules Installer 플러그인 작동 방법

공존 유틸리티는 CA Access Control 설치가 끝날 때 및 유틸리티가 실행될 때마다 다음과 같이 Windows Modules Installer 플러그인을 실행하여 컴퓨터에서 Windows Modules Installer 서비스를 검색합니다.

1. "TrusterInstaller" 서비스 실행 파일의 디렉터리 경로(ServicePath)를 추출합니다.
2. 다음과 같은 PBF 유형의 SPECIALPGM 리소스를 만듭니다.

   `ServicePath`

   이것은 응답 파일에 정의된 기본 작업입니다.

참고: 응답 파일에 따라 공존 유틸리티가 미리 지정된 단계에서 수행하는 기본 작업(CA Access Control 설치 전, CA Access Control 설치 후 등에 수행할 작업)이 결정됩니다.

Services and Controller 플러그인 작동 방법

공존 유틸리티는 CA Access Control 설치가 끝날 때 및 유틸리티가 실행될 때마다 다음과 같이 Services and Controller 플러그인을 실행하여 컴퓨터에서 Windows 서비스 관리 실행 파일을 검색합니다.

1. 운영 체제 버전이 Windows Vista 이상인지 확인합니다.

   OS 가 이전 Windows 버전이면 플러그인이 종료됩니다.

2. 다음과 같은 KILL 유형의 SPECIALPGM 리소스를 만듭니다.

   ```
   %windir%\system32\services.exe
   ```

   이것은 응답 파일에 정의된 기본 작업입니다.

참고: 응답 파일에 따라 공존 유틸리티가 미리 지정된 단계에서 수행하는 기본 작업(CA Access Control 설치 전, CA Access Control 설치 후 등에 수행할 작업)이 결정됩니다.

리소스 호스팅 하위 시스템 플러그 인이 작동하는 방법

CA Access Control 설치 프로세스는 CA Access Control 설치 중 리소스 호스팅 하위 시스템을 실행하고, 공존 유틸리티는 사용자가 실행할 때 리소스 호스트 호스팅 하위 시스템을 실행합니다. 리소스 호스팅 하위 시스템 플러그 인은 다음과 같이 컴퓨터에서 클러스터 서비스 요소를 검색합니다.

1. 운영 체제가 Windows Server 2008 이상인지 확인합니다.

   OS 가 이전 Windows 버전이면 플러그인이 종료됩니다.

2. 컴퓨터에 클러스터 서비스 요소가 설치되어 있는지 확인합니다.

   클러스터 서비스 요소가 설치되어 있지 않으면 플러그 인이 종료됩니다.

3. 다음과 같은 PBF 유형의 SPECIALPGM 리소스를 만듭니다.

   ```
   system_drive:\Windows\Cluster\rhs.exe
   ```

참고: 응답 파일에 따라 공존 유틸리티가 미리 지정된 단계에서 수행하는 기본 작업(CA Access Control 설치 전, CA Access Control 설치 후 등에 수행할 작업)이 결정됩니다.

response.ini - 공존 유틸리티 구성

Windows 에 해당

응답 파일은 공존 유틸리티(eACoexist)에 실행 시 수행할 작업을 지정합니다. 응답 파일에는 공존 유틸리티가 실행하는 모든 플러그인에 대한 미리 정의된 작업 집합이 포함되어 있습니다. 응답 파일을 편집하여 기본 플러그인 작업을 변경할 수 있습니다.

참고: 응답 파일 경로 이름은 SeOSD 섹션의 응답 파일 구성 설정에 지정됩니다. 이 파일은 기본적으로 ACInstallDir\Data\response.ini 입니다.

이 파일의 형식은 다음과 같습니다.

```
[섹션 이름]
Act-Stage-#=Action
...
```

섹션 이름

공존 플러그인과 일치하는 섹션의 이름을 정의합니다.

공존 유틸리티는 이 섹션에 정의된 작업에 따라 플러그인을 실행합니다.

Act-Stage-#=Action#

미리 지정된 단계에서 플러그인이 수행할 작업을 정의합니다.

단계

플러그인이 작업을 수행하는 미리 지정된 단계를 다음과 같이 지정합니다.

- **BeginInstall** - CA Access Control 설치가 시작되기 전에 플러그인이 지정된 작업을 수행합니다.
- **EndInstall** - CA Access Control 설치가 완료된 후 플러그인이 지정된 작업을 수행합니다.
- **Utility** - 공존 유틸리티를 실행할 때 플러그인이 지정된 작업을 수행합니다.
- **BeginUninstall** - CA Access Control 제거가 시작되기 전에 플러그인이 지정된 작업을 수행합니다.
- **EndUninstall** - CA Access Control 제거가 완료된 후 플러그인이 지정된 작업을 수행합니다.

#

이 단계에서 플러그인이 작업을 실행하는 순서를 지정합니다.

동작

플러그인이 수행해야 하는 작업을 정의하는 숫자를 다음과 같이 지정합니다.

- **1** - CA Access Control 이 검색된 제품과 호환되지 않는다고 경고합니다.
- **2** - CA Access Control 설치 중에 서비스를 중지합니다.
- **3** - 서비스를 중지합니다.
- **4** - 서비스를 시작합니다.
- **5** - SPECIALPGM 규칙을 만듭니다.
- **6** - CA Access Control 제거 중에 서비스를 중지합니다.

예: Dr. Watson 플러그인 동작

이 예에서는 Dr. Watson 공존 플러그인이 컴퓨터에서 Dr. Watson 프로그램을 검색한 경우 기본적으로 수행하는 기본 동작을 표시합니다.

```
[DrWatson]
Act-EndInstall-0=5
Act-Utility-0=5
```

이 섹션에서는 CA Access Control 설치가 완료된 후 플러그인이 실행될 때 프로그램에 대한 SPECIALPGM 규칙을 만들도록 지정합니다. 또한 유틸리티를 실행할 때도 동일한 작업을 수행하도록 지정합니다.

eACSigUpdate 유틸리티-STOP 서명 파일 교체

Windows 에 해당

eACSigUpdate 유틸리티는 로컬 STOP(스택 오버플로 보호) 서명 파일을 다른 컴퓨터에서 업데이트한 파일과 교체합니다.

참고: eACSigUpdate 유틸리티는 CA Access Control 이 시작될 때 자동으로 실행된 다음, 서명 파일 브로커나 부모 정책 모델이 정의되는 경우 규칙적인 간격으로 실행됩니다.

이 명령의 형식은 다음과 같습니다.

```
eACSigUpdate hostname target_file
```

hostname

이 컴퓨터로 복사하고자 하는 업데이트된 STOP 서명 파일이 있는 호스트 컴퓨터의 이름을 정의합니다.

참고: 이 명령을 사용하려면 원격 호스트에서 관리 권한이 있어야 합니다.

target_file

새 서명 파일의 전체 경로와 이름을 정의합니다. 이는 지정한 호스트에서 검색되는 서명의 위치와 이름입니다.

eACSyncLockout 유틸리티-계정 잠금 동기화

Windows 에 해당

eACSyncLockout 유틸리티는 계정 잠금을 CA Access Control 데이터베이스와 동기화합니다. 즉, 계정을 잠그면 CA Access Control 데이터베이스에 있는 해당 사용자의 레코드가 일시 중단됩니다. 이 유틸리티는 암호 동기화가 설정되어 있고 또한 유틸리티를 실행하는 사용자가 ADMIN 속성을 가지고 있는 경우에만 적용됩니다.

이 명령의 형식은 다음과 같습니다.

```
eACSyncLockout -start [-u username] [-p password]
```

```
eACSyncLockout -stop|-remove|-debug
```

-p password

설치하고 시작할 서비스에 대해 사용자 암호를 정의합니다. -p 를 지정하지 않으면 사용자에게 암호가 없는 것으로 간주됩니다.

-remove

서비스를 중지하고 제거합니다. 다음번에 컴퓨터를 부팅할 때 서비스가 서비스 제어 관리자에 나타나지 않습니다.

-start

서비스를 설치하고 시작합니다. -u 를 지정하지 않으면 현재 사용자의 컨텍스트에서 서비스가 설치 및 시작됩니다.

-stop

서비스를 중지합니다.

-u user

서비스의 설치 및 시작을 위한 사용자 컨텍스트를 정의합니다.

exporttngdb 유틸리티-Unicenter Security 데이터 마이그레이션

exporttngdb 프로그램은 현재 Unicenter Security 데이터를 로컬 CA Access Control 데이터베이스나 PMDB 로 마이그레이션합니다.

참고: 두 개의 스크립트, 즉 uni_migrate_master.sh 와 uni_migrate_node.sh 가 이 프로그램을 자동으로 실행합니다. 두 스크립트는 모두 마스터 컴퓨터에서 실행되지만 uni_migrate_master.sh 스크립트가 이 프로그램을 먼저 호출하여 전역 Unicenter Security 데이터를 전역 PMDB 로 마이그레이션합니다. uni_migrate_node.sh 스크립트는 이 프로그램을 호출하여 로컬 Unicenter Security 데이터를 로컬 SeOS DB 로 마이그레이션합니다.

이 명령의 형식은 다음과 같습니다.

```
exporttngdb
```

issec 유틸리티-CA Access Control 데몬 상태 표시

UNIX 에 해당

issec 유틸리티는 CA Access Control 보안 데몬의 상태를 표시합니다. 옵션을 지정하지 않을 경우 다음 정보가 나타납니다.

- CA Access Control 버전 및 설치 디렉터리
- CA Access Control 커널 확장 상태
- 세 가지 주요 CA Access Control 데몬("seosd", "agent" 및 "watchdog") 상태
- CA Access Control 데몬("serevu", "selogrd" 및 "selogrcd") 상태
- PMDB 데몬 상태 및 이름
- seos.ini 파일의 [daemons] 섹션에서 지정한 데몬의 상태

이 명령의 형식은 다음과 같습니다.

```
issec [-b] [-k] [-h]
```

-b

주요 데몬("seosd", "agent" 및 "watchdog")의 상태 및 PID 를 표시합니다.

-k

CA Access Control 커널 확장이 로드되었는지 확인합니다.

-h

이 유틸리티에 대한 도움말을 표시합니다.

ldap2seos 스크립트-CA Access Control 에 추가하기 위해 LDAP 에서 사용자 추출

UNIX 에 해당

ldap2seos 유틸리티는 서버 호스트에 있는 LDAP 데이터베이스에서 사용자를 추출하여 CA Access Control 데이터베이스에 추가합니다.

중요! LDAP 사용자 저장소가 운영 체제에 의해 사용되는 경우, 즉 엔터프라이즈 사용자 저장소인 경우에는 CA Access Control 에서 LDAP 사용자를 가져오지 않고 직접 사용할 수 있습니다. ldap2seos 유틸리티 대신 CA Access Control 의 이 기능을 사용해 보십시오.

ldap2seos 유틸리티는 LDAP 서버에서 정의된 사용자 정보를 추출합니다. 추출된 정보는 데이터베이스에 사용자를 추가하기 위해 selang 명령을 실행하는 데 자동으로 사용됩니다. 생성된 명령도 표준 출력으로 인쇄되고 /tmp/ldap2seos.tcl.log 라는 파일에 자동으로 저장됩니다.

이 유틸리티를 사용하려면 TCL 셸 환경에 액세스할 수 있어야 합니다. ldap2seos 스크립트는 TCL 셸 경로가 /usr/local/bin/tclsh 라고 가정합니다. TCL 셸이 다른 위치에 있으면 스크립트의 첫 번째 행을 변경하십시오.

유틸리티가 제대로 작동하려면 CA Access Control 이 실행되고 있어야 합니다. 이 유틸리티는 데이터베이스를 업데이트하므로 반드시 ADMIN 권한이 있는 사용자가 실행해야 합니다. 또한 이 사용자는 LDAP 데이터베이스 설정에서 검색 쿼리를 만들 권한이 있어야 합니다.

이 스크립트의 형식은 다음과 같습니다.

```
ldap2seos [options]
```

-accfld account-field

CA Access Control 에 대한 사용자 ID 를 포함하는 LDAP 필드 이름을 지정합니다.

UNIX 사용자 ID 가 [LDAP userid] 필드에 있으면 이 옵션은 필요 없습니다.

UNIX 사용자 ID 가 userid 필드가 아닌 LDAP 필드에 할당되면 LDAP 필드를 account-field 로 지정하고 LDAP userid 필드는 무시됩니다.

참고: 스크립트에서 userid 를 찾지 못하면 사용자가 CA Access Control 데이터베이스로 업로드되지 않습니다.

-b base-entry

LDAP 데이터베이스에서 사용자를 가져오는 기본 항목을 지정합니다. 항목은 LDAP 데이터베이스 내에서 유효해야 합니다. 기본 항목을 생략하면 LDAP 는 기본값 항목을 사용하여 사용자에게 제공합니다.

-d dn

LDAP 에 또 다른 사용자로 인증하기 위해 -w 스위치와 함께 사용되는 항목 이름을 지정합니다. 주로 LDAP 에 admin 사용자로 로그인하기 위해 필요합니다.

-f filename

LDAP 서버에서 검색된 데이터를 일시적으로 저장할 수 있는 파일을 지정합니다.

-h

유틸리티에 대한 도움말을 표시합니다. 화면에는 ldap2seos 용도 및 옵션에 대한 목록 및 설명이 표시됩니다.

-h ldap-host

LDAP 데이터베이스가 있는 호스트의 이름을 지정합니다. 기본값은 로컬 호스트입니다.

-l ldap-dir

bin 하위 디렉터리에 있을 것으로 가정되는 명령줄 유틸리티를 포함하고 있는 디렉터리를 지정합니다. 기본값은 /usr/local/ldap 입니다.

-p port

연결하는 데 사용되는 LDAP 포트를 지정합니다. 기본값은 389 포트입니다.

-u

-h 와 동일하며 도움말을 표시합니다. 화면에는 ldap2seos 용도 및 옵션에 대한 목록 및 설명이 표시됩니다.

-w bindpasswd

사용자 암호를 지정합니다. LDAP 데이터베이스에 액세스하기 위해 인증이 필요할 때 -d 옵션과 함께 사용합니다.

예: 사용자 정보 추출

다음 명령은 호스트 myhost.mysite.co.na 의 LDAP 데이터베이스에서 사용자 정보를 추출하여 CA Access Control 데이터베이스에 추가합니다.

```
ldap2seos -h myhost.mysite.com
```

seos2ldap 스크립트-CA Access Control 사용자를 LDAP 로 내보내기

seos2ldap 는 데이터베이스의 CA Access Control 사용자를 서버 호스트의 LDAP 데이터베이스로 내보냅니다. 이 유틸리티는 CA Access Control 데이터베이스에서 적절한 사용자 정보를 추출합니다. 그런 다음 선택한 서버의 LDAP 데이터베이스로 정보를 전송합니다. 추출된 정보는 LDIF 파일을 만드는 데 사용됩니다. 지정한 사용자는 LDAP 데이터베이스에 추가됩니다. 응답은 /tmp/seos2ldap.tcl.log 라는 파일에 자동으로 저장됩니다.

이 유틸리티를 사용하려면 TCL 셸 환경에 액세스할 수 있어야 합니다. ldap2seos 스크립트는 TCL 셸 경로가 /usr/local/bin/tclsh 라고 가정합니다. TCL 셸이 다른 위치에 있으면 스크립트의 첫 번째 행을 변경하십시오.

유틸리티가 제대로 작동하려면 CA Access Control 이 실행되고 있어야 합니다. 이 유틸리티는 데이터베이스에서 정보를 읽으므로 반드시 ADMIN 권한이 있는 사용자가 실행해야 합니다. 또한 이 사용자는 LDAP 데이터베이스 설정에서 변경할 권한이 있어야 합니다.

사용하려고 선택한 LDAP 데이터베이스의 항목 스키마는 Netscape 서버의 스키마와 유사해야 합니다. Netscape 스키마를 변경하거나 다른 유형의 LDAP 서버를 사용하려는 경우 그에 따라 seos2ldap 예제 스크립트를 편집해야 합니다.

CA Access Control 데이터베이스 사용자가 LDAP 데이터베이스에 이미 있으면 이 사용자는 추가되지 않습니다. 오류 메시지가 표시되지만 내보내기 프로세스는 계속됩니다.

이 스크립트의 형식은 다음과 같습니다.

```
seos2ldap [options]
```

-b base-entry

LDAP 데이터베이스에서 사용자 정보를 저장하는 기본 항목을 지정합니다. 항목은 LDAP 데이터베이스 내에서 유효해야 합니다. 기본 항목을 생략하면 기본 항목을 제공하라는 메시지가 LDAP 에 표시됩니다.

-d dn

LDAP 에 또 다른 사용자로 인증하기 위해 -w 스위치와 함께 사용하는 항목 이름을 저정합니다. 이 옵션은 LDAP 에 admin 사용자로 로그인하는 데 필요합니다.

-f filename

LDAP 서버에서 검색된 데이터를 일시적으로 저장할 수 있는 파일을 지정합니다.

-h

유틸리티에 대한 도움말을 표시합니다. 화면에는 ldap2seos 용도 및 옵션에 대한 목록 및 설명이 표시됩니다.

-h ldap-host

LDAP 데이터베이스가 있는 호스트의 이름을 지정합니다. 기본값은 로컬 호스트입니다.

-l ldap-dir

bin 하위 디렉터리에 있을 것으로 가정되는 명령줄 유틸리티를 포함하고 있는 디렉터리를 지정합니다. 기본값은 /usr/local/ldap 입니다.

-noprompt

기본 항목 프롬프트를 취소합니다. 기본 LDAP 항목을 지정하기 위해 -b base-entry 플래그를 사용하지 않은 경우에는 기본적으로 기본 항목에 대해 seos2ldap 프롬프트가 표시됩니다. 이 플래그는 프롬프트를 무시합니다.

-p port

연결하는 데 사용되는 LDAP 포트를 정의합니다. 기본값은 389 포트입니다.

-u

-h 와 동일하며 도움말을 표시합니다. 화면에는 ldap2seos 용도 및 옵션에 대한 목록 및 설명이 표시됩니다.

-w bindpasswd

사용자 암호를 정의합니다. LDAP 데이터베이스에 액세스하기 위해 인증이 필요할 때 -d 옵션과 함께 사용하십시오.

예: 사용자 정보 내보내기

다음 명령은 CA Access Control 데이터베이스에서 사용자 정보를 추출하고 SeOS_user_dump 라는 LDIF 파일을 생성합니다. 이 명령은 myhost.mysite.com 호스트의 LDAP 데이터베이스에 레코드를 추가합니다. 나중에 LDIF 파일을 편집하여 LDAP 를 수동으로 업데이트할 수 있습니다.

```
seos2ldap -h myhost.mysite.com
```

migopts 유틸리티-Unicenter Security 설정 변환

migopts 유틸리티는 현재 Unicenter Security 환경 설정을 로컬 CA Access Control 데이터베이스 또는 PMDB 의 전역 설정으로 변환합니다.

참고: Unicenter 통합을 선택하면 설치 프로그램이 자동으로 이 스크립트를 실행합니다. 이것은 새 PMDB 가 작성될 때마다 수동으로 호출되어야 합니다.

이 명령의 형식은 다음과 같습니다.

```
migopts [options]
```

-d pmdName

로컬 CA Access Control 데이터베이스(기본값)가 아닌 가져온 PMDB 를 업데이트하도록, selang 명령을 실행하기 전에 CA Access Control **hosts** 명령을 작성합니다.

-f fileName

selang -c 명령을 실행 스크립트 파일로 생성합니다.

-l logfileName

로그 메시지를 완전히 지정된 파일 이름에 기록합니다.

ntimport 유틸리티-Windows 사용자 및 그룹 가져오기

Windows 에 해당

ntimport 유틸리티는 Windows 운영 체제 데이터베이스에서 Windows 사용자 및 그룹을 추출하여 로컬 데이터베이스로 가져옵니다. 또한 사용자 및 그룹을 로컬 CA Access Control 데이터베이스에 추가하기 위해 필요한 Windows 명령을 작성합니다.

중요! CA Access Control 에서는 Windows 사용자 및 그룹을 데이터베이스로 가져올 필요 없이 직접 사용할 수 있습니다. ntimport 유틸리티 대신 CA Access Control 의 이 기능을 사용해 보십시오. 이 유틸리티는 CA Access Control 에서 Windows 사용자 및 그룹을 직접 사용할 수 있기 전에 개발되었습니다.

생성된 명령은 표준 출력에 표시됩니다. selang 유틸리티에 대한 입력으로 사용할 파일을 작성하려면 -f 옵션을 사용하십시오.

이 명령의 형식은 다음과 같습니다.

```
ntimport {-a|{[-u] [-g] [-c]}} [-d] [-U] \
    [-D] [-f filename] [-o owner] [-p pmdb] \
    [-pa pmdb] [-r remote-host] [-v]
```

-a

-c, -g 및 -u 스위치의 모든 작업을 수행합니다.

-c

사용자를 해당 기본 그룹에 조인하는 데 필요한 selang 명령을 생성합니다.

-d

도메인을 접두사로 하여 사용자와 그룹을 가져옵니다.

-D

첫 번째 사용 가능한 도메인 컨트롤러에서 사용자 및 그룹 정보를 검색합니다.

-f filename

지정된 파일로 출력을 리디렉션합니다.

-g

Windows 에서 로컬 데이터베이스로 그룹을 가져오기 위해 필요한 selang 명령을 생성합니다.

-o owner

가져온 각 레코드에 대한 소유 규칙을 설정합니다. 관리자가 자동으로 모든 레코드의 소유자가 되지 않도록 하려면 이 플래그를 사용하십시오. Owner 는 ntimport 가 정의한 모든 레코드의 소유권이 할당될 사용자 또는 그룹의 이름입니다.

-p pmdb

사용자와 그룹을 pmdb 의 AC 환경으로 가져오기 위한 명령을 생성합니다.

-pa pmdb

사용자와 그룹을 pmdb 의 AC 및 네이티브 환경으로 가져오기 위한 명령을 생성합니다.

-pn pmdb

사용자와 그룹을 pmdb 의 네이티브 환경으로 가져오기 위한 명령을 생성합니다.

-r remote-host

지정한 원격 호스트에서 사용자 및 그룹 정보를 검색합니다.

-u

Windows 데이터베이스에서 로컬 데이터베이스로 사용자를 가져오기 위해 필요한 selang 명령을 생성합니다. 40 자보다 긴 이름은 잘립니다.

-U

사용자에 대한 surrogate 규칙을 가져오는 데 필요한 selang 명령을 생성합니다.

-v

사용자에게 진행 상태 정보를 제공합니다. 여러 사용자 또는 그룹이 있을 때 프로그램의 진행 상태를 확인하려면 이 플래그를 사용하십시오.

policydeploy 유틸리티-엔터프라이즈 정책 배포 관리

policydeploy 유틸리티는 여러 규칙 정책(고급 정책 관리)을 관리합니다. 이 유틸리티를 사용해 정책 버전을 DMS 노드에 저장하거나, 호스트와 호스트 그룹에 정책을 할당 및 할당 취소하거나, 저장된 정책을 직접 배포 또는 배포 취소하거나, 배포된 정책을 최신 버전으로 업그레이드할 수 있습니다.

이 유틸리티는 여러 작업을 처리하며 다음과 같은 함수가 있습니다.

작업	함수
정책 할당 또는 할당 취소 (페이지 77)	policydeploy -assign
정책 삭제 (페이지 79)	policydeploy -delete
정책 배포 (페이지 81)	policydeploy -deploy
정책 배포 취소 (페이지 81)	policydeploy -undeploy
배포 태스크 다시 실행 (페이지 82)	policydeploy -fix
배포 스크립트 보기 (페이지 83)	policydeploy -getrules

작업	함수
호스트 그룹에서 호스트 조인 또는 제거 (페이지 84)	policydeploy -join
PMD 를 고급 정책 관리로 마이그레이션 (페이지 85)	policydeploy -migrate
정책 배포 다시 설정 (페이지 88)	policydeploy -reset
모든 정책 복원 (페이지 88)	policydeploy -restore
정책 복원 (페이지 89)	policydeploy -store
정책 버전 업그레이드 (페이지 92)	policydeploy -upgrade
정책 버전 다운그레이드 (페이지 92)	policydeploy -downgrade

policydeploy -assign Function - 정책 할당 또는 할당 취소

이 함수는 지정된 정책을 하나 이상의 호스트 또는 호스트 그룹에 할당 또는 할당 취소합니다.

이 함수의 형식은 다음과 같습니다.

```
policydeploy -assign[-] name -hnode|-ghnode list [-dms list]
```

-assign name

지정된 정책을 하나 이상의 호스트 또는 호스트 그룹에 할당 또는 할당 취소합니다.

-assign- name

지정된 정책을 하나 이상의 호스트 또는 호스트 그룹에서 할당 취소합니다.

-dms list

(선택 사항) 사용할 DMS 노드의 목록을 쉼표로 구분하여 지정합니다. 정책을 배포하거나 배포 취소할 때 이러한 DMS 노드에 작업이 보고됩니다. 정책을 저장할 때 이러한 DMS 노드에 정책이 저장됩니다.

이 옵션으로 DMS 노드를 지정하지 않으면 로컬 CA Access Control 데이터베이스에 지정된 DMS 노드의 목록이 사용됩니다. 데이터베이스에서 DMS 노드의 목록을 지정하려면, dmsmgr 을 사용하여 새 DMS 를 만든 후 다음 selang 명령을 작성해야 합니다.

```
so dms+(new_dms_name)
```

참고: 설치 중 DMS 노드를 지정하지 않았거나 끝점에서 등록된 DMS 를 바꾸거나 추가하려는 경우 동일한 명령을 작성해야 합니다. 그러나 설치 중 고급 정책 관리 서버를 만들도록 지정하면 DMS 가 데이터베이스에 추가되므로 위 명령을 직접 실행할 필요가 없습니다.

-ghnode list

정책에 할당하고자 하는 호스트 그룹(GHNODE 개체)의 목록을 쉼표로 구분하여 정의합니다.

-hnode list

정책에 할당하고자 하는 호스트(HNODE 개체)의 목록을 쉼표로 구분하여 정의합니다.

예: IIS 5 보호 정책 할당

다음 예에서는 IIS(Internet Information Services) 5 웹 서버의 보안을 위해 정책을 할당하는 방법을 설명합니다. 정책과 IIS5 정책의 최신(네 번째) 버전을 검토하고 이 정책을 IIS5Servers 라는 호스트 그룹에 할당합니다. IIS5 정책은 crDMS@cr_host.company.com DMS 노드에 저장되어 있습니다.

1. 다음과 같이 selang 을 사용하여 DMS 에 연결합니다.

   ```
   hosts crDMS@cr_host.company.com
   ```

   이제 selang 을 통해 DMS 를 조회할 수 있습니다.

2. 정책의 완료된 최신 버전을 모르는 경우 다음 selang 명령을 실행하여 정책의 모든 버전을 찾습니다.

   ```
   sr GPOLICY IIS5
   ```

   selang 창에 할당할 수 있는(완료된) 최신 정책 버전인 최종 정책을 비롯하여 IIS5 정책의 속성이 나열됩니다.

3. 다음 selang 명령을 실행하여 정책 배포 및 배포 취소 스크립트를 확인합니다.

   ```
   sr RULESET IIS5#04
   ```

   selang 창에 IIS5 정책의 네 번째 버전과 관련된 배포 및 배포 취소 규칙을 비롯하여 IIS5#04 RULESET 개체가 표시됩니다.

4. 명령줄 프롬프트에서 다음과 같이 policydeploy 유틸리티를 실행합니다.

   ```
   policydeploy -assign IIS5 -ghnode IIS5Servers
   ```

   이 유틸리티를 실행하면 IIS5 정책이 IIS5Servers 논리 호스트 그룹의 모든 호스트에 할당된 다음 IIS5 정책의 네 번째 버전이 이 호스트에 배포됩니다.

예: IIS 5 보호 정책 할당 취소

다음 예에서는 앞에서 정책을 할당했던 웹 서버에서 할당된 IIS 5 정책을 할당 취소하는 방법을 설명합니다.

명령줄 프롬프트에서 다음과 같이 policydeploy 유틸리티를 실행합니다.

```
policydeploy -assign- IIS5 -ghnode IIS5Servers
```

이 유틸리티를 실행하면 IIS5 정책이 IIS5Servers 논리 호스트 그룹의 모든 호스트에서 할당 취소된 다음 이 호스트에 배포된 IIS5 정책이 배포 취소됩니다.

policydeploy -delete 함수 - 정책 삭제

이 함수는 지정된 정책 또는 정책 버전을 삭제합니다.

참고: 호스트 또는 호스트 그룹에 할당되었거나, 호스트 또는 호스트 그룹에 배포되었거나, 실패로 인해 상태가 "배포 취소됨"이거나, DMS 에 상태가 있는 정책 또는 정책 버전은 삭제할 수 없습니다. 정책 또는 정책 버전을 삭제하기 전에 모든 호스트 및 호스트 그룹에서 정책 또는 정책 버전을 배포 취소 또는 할당 취소해야 합니다. 또한 다른 정책에 필수적인 정책은 삭제할 수 없습니다. 삭제하기 전에 정책에 대한 모든 종속성을 제거하십시오.

이 함수의 형식은 다음과 같습니다.

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

-delete name[#xx]

지정된 정책 또는 정책 버전을 삭제합니다.

-dms list

(선택 사항) 사용할 DMS 노드의 목록을 쉼표로 구분하여 지정합니다. 정책을 배포하거나 배포 취소할 때 이러한 DMS 노드에 작업이 보고됩니다. 정책을 저장할 때 이러한 DMS 노드에 정책이 저장됩니다.

이 옵션으로 DMS 노드를 지정하지 않으면 로컬 CA Access Control 데이터베이스에 지정된 DMS 노드의 목록이 사용됩니다. 데이터베이스에서 DMS 노드의 목록을 지정하려면, dmsmgr 을 사용하여 새 DMS 를 만든 후 다음 selang 명령을 작성해야 합니다.

```
so dms+(new_dms_name)
```

참고: 설치 중 DMS 노드를 지정하지 않았거나 끝점에서 등록된 DMS 를 바꾸거나 추가하려는 경우 동일한 명령을 작성해야 합니다. 그러나 설치 중 고급 정책 관리 서버를 만들도록 지정하면 DMS 가 데이터베이스에 추가되므로 위 명령을 직접 실행할 필요가 없습니다.

예: IIS 5 보호 정책 삭제

다음 예는 할당 취소된 IIS 5 정책을 DMS 에서 삭제하는 방법에 대해 설명합니다. 이 예에서 정책 IIS5 는 어떠한 호스트 또는 호스트 그룹에도 할당되지 않았으며 crDMS@cr_host.company.com DMS 노드에 저장되어 있습니다.

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

```
policydeploy -delete IIS5
```

IIS5 정책이 crDMS@cr_host.company.com DMS 노드에서 삭제됩니다.

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.

policydeploy -deploy 함수 - 정책 배포 또는 배포 취소

이 함수는 호스트에 정책을 할당하거나 호스트에서 정책의 할당을 취소하지 않고 지정된 끝점에서 정책을 배포 및 배포 취소합니다.

이 함수의 형식은 다음과 같습니다.

```
policydeploy { -deploy name[#xx] | -undeploy name[#xx] } {-nodelist hnode_list | -root dbs} [-dms list]
```

-deploy name[#xx]

지정한 저장 정책 버전을 정의된 끝점에 직접 배포할 것인지(정책을 호스트에 할당하지 않은 채)를 묻는 메시지를 표시합니다. 정책의 최신 저장 버전을 배포하려면 정책 버전 번호를 생략하십시오.

-dms list

(선택 사항) 사용할 DMS 노드의 목록을 쉼표로 구분하여 지정합니다. 정책을 배포하거나 배포 취소할 때 이러한 DMS 노드에 작업이 보고됩니다. 정책을 저장할 때 이러한 DMS 노드에 정책이 저장됩니다.

이 옵션으로 DMS 노드를 지정하지 않으면 로컬 CA Access Control 데이터베이스에 지정된 DMS 노드의 목록이 사용됩니다. 데이터베이스에서 DMS 노드의 목록을 지정하려면, dmsmgr 을 사용하여 새 DMS 를 만든 후 다음 selang 명령을 작성해야 합니다.

```
so dms+(new_dms_name)
```

참고: 설치 중 DMS 노드를 지정하지 않았거나 끝점에서 등록된 DMS 를 바꾸거나 추가하려는 경우 동일한 명령을 작성해야 합니다. 그러나 설치 중 고급 정책 관리 서버를 만들도록 지정하면 DMS 가 데이터베이스에 추가되므로 위 명령을 직접 실행할 필요가 없습니다.

-nodelist hnode_list

작업을 수행하고자 하는 호스트(HNODE 개체)의 목록을 쉼표로 구분하여 정의합니다.

-root dbs

정책을 배포 또는 배포 취소해야 할 데이터베이스의 목록을 쉼표로 구분하여 정의합니다.

참고: 루트 데이터베이스가 정책 모델 부모이면 해당 구독 데이터베이스 전체에서 정책이 배포 또는 배포 취소됩니다. 루트 데이터베이스가 CA Access Control 끝점이면 지정된 데이터베이스에서만 정책이 배포 또는 배포 취소됩니다. 이 옵션은 r8 SP1 데이터베이스 및 PMDB 와의 이전 버전과의 호환성을 위해 사용됩니다.

-undeploy name[#xx]

정의된 끝점에서 지정된 정책 버전 name#xx 를 직접 배포 취소하고자 하는지(정책 할당 취소 없이)를 묻는 메시지를 표시합니다.

정책의 최신 저장 버전을 배포 취소하려면 정책 버전 번호를 생략하십시오.

policydeploy -fix Function - 배포 작업 다시 실행

이 함수는 지정된 배포 작업 또는 패키지를 수정하고 작업 또는 패키지를 다시 배포합니다.

이 함수의 형식은 다음과 같습니다.

```
policydeploy -fix {-task list | -package list} [-dms list]
```

-dms list

(선택 사항) 사용할 DMS 노드의 목록을 쉼표로 구분하여 지정합니다. 정책을 배포하거나 배포 취소할 때 이러한 DMS 노드에 작업이 보고됩니다. 정책을 저장할 때 이러한 DMS 노드에 정책이 저장됩니다.

이 옵션으로 DMS 노드를 지정하지 않으면 로컬 CA Access Control 데이터베이스에 지정된 DMS 노드의 목록이 사용됩니다. 데이터베이스에서 DMS 노드의 목록을 지정하려면, dmsmgr 을 사용하여 새 DMS 를 만든 후 다음 selang 명령을 작성해야 합니다.

```
so dms+(new_dms_name)
```

참고: 설치 중 DMS 노드를 지정하지 않았거나 끝점에서 등록된 DMS 를 바꾸거나 추가하려는 경우 동일한 명령을 작성해야 합니다. 그러나 설치 중 고급 정책 관리 서버를 만들도록 지정하면 DMS 가 데이터베이스에 추가되므로 위 명령을 직접 실행할 필요가 없습니다.

-fix

지정된 배포 작업 또는 패키지를 수정하고 다시 배포합니다.

-package list

배포 패키지(GDEPLOYMENT)의 목록을 쉼표로 구분하여 정의합니다.

-task list

배포 작업의 목록을 쉼표로 구분하여 정의합니다.

policydeploy -getrules Function - 배포 스크립트 보기

이 함수를 사용하면 지정된 정책 버전에 대한 배포 취소 스크립트와 selang 배포를 볼 수 있습니다.

```
policydeploy -getrules name[#xx] -ds file1 -uds file2 [-dms list]
```

-dms list

(선택 사항) 사용할 DMS 노드의 목록을 쉼표로 구분하여 지정합니다. 정책을 배포하거나 배포 취소할 때 이러한 DMS 노드에 작업이 보고됩니다. 정책을 저장할 때 이러한 DMS 노드에 정책이 저장됩니다.

이 옵션으로 DMS 노드를 지정하지 않으면 로컬 CA Access Control 데이터베이스에 지정된 DMS 노드의 목록이 사용됩니다. 데이터베이스에서 DMS 노드의 목록을 지정하려면, dmsmgr 을 사용하여 새 DMS 를 만든 후 다음 selang 명령을 작성해야 합니다.

```
so dms+(new_dms_name)
```

참고: 설치 중 DMS 노드를 지정하지 않았거나 끝점에서 등록된 DMS 를 바꾸거나 추가하려는 경우 동일한 명령을 작성해야 합니다. 그러나 설치 중 고급 정책 관리 서버를 만들도록 지정하면 DMS 가 데이터베이스에 추가되므로 위 명령을 직접 실행할 필요가 없습니다.

-ds file1

배포 규칙을 포함하는 파일의 경로 이름을 지정합니다. 이들이 정책 구성에 필요한 명령입니다. -getrules 옵션을 사용하면 이 파일이 작성됩니다.

중요! 정책 배포에서는 사용자 암호를 설정하는 명령을 지원하지 않으므로 배포 스크립트 파일에 이러한 명령을 포함시키지 마십시오. 네이티브 selang 명령은 지원되지만 위반 보고서에는 표시되지 않습니다.

-getrules name[#xx]

지정한 정책 버전에 대해 selang 배포 및 배포 취소 스크립트를 검색합니다. 정책 버전을 지정하지 않으면 최신 정책 버전에 명령이 적용됩니다.

-uds file2

정책의 배포 취소를 위해 필요한 규칙이 포함된 파일의 경로 이름을 정의합니다. 이들이 정책 배포 취소에 필요한 명령입니다. -getrules 옵션을 사용하면 이 파일이 작성됩니다.

CA Access Control 이 정책을 배포 취소할 때 저장되어 있는 정책 배포 취소 스크립트가 없으면 CA Access Control 은 정책 제거를 위해 필요한 명령을 계산합니다.

예: IIS 5 보호 정책과 관련된 배포 스크립트 보기

다음 예에서는 IIS(Internet Information Services) 5 웹 서버 보안을 위한 정책의 배포 및 배포 취소와 관련된 selang 스크립트를 보는 방법에 대해 설명합니다. 정책의 이름은 myPolicy 입니다.

selang 스크립트를 보려면 다음 명령을 실행하십시오.

```
policydeploy -getrules myPolicy -ds c:\folder\deployRules.txt -uds undeployRules.txt
```

policydeploy -join Function - 호스트를 호스트 또는 호스트 그룹에서 조인 또는 제거

이 함수는 호스트를 호스트 그룹에 조인하거나 호스트 그룹에서 호스트를 제거합니다.

이 함수의 형식은 다음과 같습니다.

```
policydeploy -join[-] hnode_name -ghnode name [-dms list]
```

-dms list

(선택 사항) 사용할 DMS 노드의 목록을 쉼표로 구분하여 지정합니다. 정책을 배포하거나 배포 취소할 때 이러한 DMS 노드에 작업이 보고됩니다. 정책을 저장할 때 이러한 DMS 노드에 정책이 저장됩니다.

이 옵션으로 DMS 노드를 지정하지 않으면 로컬 CA Access Control 데이터베이스에 지정된 DMS 노드의 목록이 사용됩니다. 데이터베이스에서 DMS 노드의 목록을 지정하려면, dmsmgr 을 사용하여 새 DMS 를 만든 후 다음 selang 명령을 작성해야 합니다.

```
so dms+(new_dms_name)
```

참고: 설치 중 DMS 노드를 지정하지 않았거나 끝점에서 등록된 DMS 를 바꾸거나 추가하려는 경우 동일한 명령을 작성해야 합니다. 그러나 설치 중 고급 정책 관리 서버를 만들도록 지정하면 DMS 가 데이터베이스에 추가되므로 위 명령을 직접 실행할 필요가 없습니다.

-ghnode name

수행할 작업에 대한 호스트 그룹의 이름을 정의합니다.

-join hnode_name

지정된 호스트를 호스트 그룹에 추가합니다.

-join- hnode_name

지정된 호스트를 호스트 그룹에서 제거합니다.

policydeploy -migrate 함수 - PMD 를 고급 정책 관리로 마이그레이션

이 함수는 PMD 를 고급 정책 관리로 마이그레이션합니다. PMD 를 고급 정책 관리로 마이그레이션할 때는 PMD 에 있는 규칙에서 정책을 만들고, DMS 에서 호스트와 호스트 그룹을 만들고, 정책을 호스트 그룹에 할당하게 됩니다.

이 함수의 형식은 다음과 같습니다.

```
policydeploy -migrate pmdName@hostName [-dms name] [-policydir directory] \
[-exportfilter "class, class..."] [-hgcreate] [-pcreate name] [-addpmdfilter]\
[-unsubs] [-delete] [-auto]
```

pmdName@hostName

마이그레이션할 PMD 의 이름을 정의합니다.

-dms name

(선택 사항) PMD 에 있는 규칙이 마이그레이션될 DMS 의 이름을 정의합니다. DMS 이름을 지정하지 않으면 로컬 호스트에 있는 CA Access Control 데이터베이스에서 DMS 이름이 검색됩니다.

참고: DMS 이름을 지정하지 않았을 때 로컬 호스트에 있는 CA Access Control 데이터베이스에 여러 개의 DMS 이름이 지정되어 있는 경우 PMD 에 있는 규칙이 지정된 모든 DMS 로 마이그레이션됩니다.

-policydir directory

(선택 사항) 정책 파일이 저장된 디렉터리를 정의합니다. 디렉터리를 지정하지 않으면 정책 파일이 현재 작업 디렉터리에 저장됩니다.

-exportfilter "class, class..."

(선택 사항) PMD 데이터베이스에서 내보낼 CA Access Control 클래스를 지정합니다. 어떤 클래스도 지정하지 않으면 PMD 데이터베이스에 있는 모든 클래스를 내보냅니다.

다음 사항이 -exportfilter 매개 변수에 적용됩니다.

- 특정 클래스의 리소스를 수정하는 규칙을 내보내고, 이 클래스에 해당 리소스 그룹이 있는 경우 CA Access Control 은 이 리소스 그룹에 있는 리소스를 수정하는 규칙도 또한 내보냅니다.
- 특정 리소스 그룹에 있는 리소스를 수정하는 규칙을 내보내면 CA Access Control 은 이 리소스 그룹의 구성원 리소스를 수정하는 규칙도 또한 내보냅니다.
- 클래스에 PACL 이 있는 특정 클래스의 리소스를 수정하는 규칙을 내보내면 CA Access Control 은 PROGRAM 클래스에 있는 리소스를 수정하는 규칙도 또한 내보냅니다.
- 클래스에 CALACL 이 있는 특정 클래스의 리소스를 수정하는 규칙을 내보내면 CA Access Control 은 CALENDAR 클래스에 있는 리소스를 수정하는 규칙도 또한 내보냅니다.
- 특정 클래스에 있는 리소스를 수정하는 규칙을 내보내고, 해당 클래스에 있는 리소스 중 하나가 CONTAINER 리소스 그룹의 구성원인 경우 CA Access Control 은 CONTAINER 클래스에 있는 리소스를 수정하고 각 CONTAINER 리소스 그룹의 구성원인 리소스를 수정하는 규칙을 내보냅니다.

-hgcreate

(선택 사항) pmdName 에 해당하는 DMS 에 호스트 그룹(HNODE 개체)을 만들고, pmdName 의 끝점 구독자에 해당하는 DMS 에 호스트(HNODE 개체)를 만들고, 호스트를 호스트 그룹에 조인합니다.

-pcreate name

(선택 사항) pmdName 에서 내보낸 정책 파일에 있는 규칙을 포함하는 DMS 에 POLICY 개체를 만들고, pmdName 에 해당하는 DMS 에 있는 호스트 그룹에 POLICY 개체를 할당합니다. name 을 할당하면 만들어진 POLICY 개체의 이름이 name_POLICY#1 이 됩니다. 이름을 지정하지 않으면 만들어진 POLICY 개체의 이름은 pmdName_POLICY#01 이 됩니다.

-addpmdfilter

(선택 사항) 필터 파일을 pmdName 에 적용합니다. 필터 파일의 이름은 filter.flt 가 되며 pmdName 과 같은 디렉터리에 저장됩니다.

참고: 필터 파일을 사용하여 암호 PMD 를 만들 수 있습니다. 필터 파일은 단지 사용자 암호 명령이 pmdName 의 구독자로 전달되게 합니다.

-unsubs

(선택 사항) pmdName 에서 끝점 구독자를 구독 취소합니다.

-delete

(선택 사항) policydeploy -migrate 함수의 실행이 완료된 후에 pmdName 을 삭제합니다.

-auto

(선택 사항) -hgcreate 및 -pcreate 옵션을 모두 실행하도록 지정합니다. 이 옵션은 다음을 수행합니다.

- pmdName 에 있는 규칙을 내보냅니다.
- pmdName 에 해당하는 DMS 에 있는 호스트 그룹(GHNODE 개체)을 만듭니다.
- pmdName 의 끝점 구독자에 해당하는 DMS 에 있는 호스트(HNODE 개체)를 만듭니다.
- 호스트를 호스트 그룹에 조인합니다.
- pmdName 에서 내보낸 정책 파일에 있는 규칙을 포함하는 DMS 에 POLICY 개체를 만듭니다.
- pmdName 에 해당하는 DMS 에 있는 호스트 그룹에 POLICY 개체를 할당합니다.

예: 규칙 마이그레이션 및 호스트 그룹 만들기

이 예제는 호스트 A 에 있는 마스터 PMD 에서 호스트 B 에 있는 DMS__로 규칙을 마이그레이션하고, 정책 파일을 C:\Data\policies_MasterPMD_hostA 디렉터리에 저장하고, DMS__에 MasterPMD 란 이름으로 호스트 그룹을 만들고, 마스터 PMD 의 끝점 구독자에 해당하는 DMS__에 호스트를 만들고, 호스트를 MasterPMD 호스트 그룹에 조인합니다.

```
policydeploy -migrate MasterPMD@hostA -dms DMS__@hostB -policydir
"C:\Data\policies_MasterPMD_hostA" -hgcreate
```

policydeploy -reset Function - 정책 배포 다시 설정

이 함수는 끝점에서 정책 배포를 다시 설정합니다. CA Access Control 은 끝점에서 모든 유효한 정책을 배포 취소하고, 모든 고급 정책 관리 속성을 삭제하고, 호스트 상태를 재설정합니다.

이 함수의 형식은 다음과 같습니다.

```
policydeploy -reset hnode_name [-dms list]
```

-dms list

(선택 사항) 사용할 DMS 노드의 목록을 쉼표로 구분하여 지정합니다. 정책을 배포하거나 배포 취소할 때 이러한 DMS 노드에 작업이 보고됩니다. 정책을 저장할 때 이러한 DMS 노드에 정책이 저장됩니다.

이 옵션으로 DMS 노드를 지정하지 않으면 로컬 CA Access Control 데이터베이스에 지정된 DMS 노드의 목록이 사용됩니다. 데이터베이스에서 DMS 노드의 목록을 지정하려면, dmsmgr 을 사용하여 새 DMS 를 만든 후 다음 selang 명령을 작성해야 합니다.

```
so dms+(new_dms_name)
```

참고: 설치 중 DMS 노드를 지정하지 않았거나 끝점에서 등록된 DMS 를 바꾸거나 추가하려는 경우 동일한 명령을 작성해야 합니다. 그러나 설치 중 고급 정책 관리 서버를 만들도록 지정하면 DMS 가 데이터베이스에 추가되므로 위 명령을 직접 실행할 필요가 없습니다.

-reset hnode_name

지정된 끝점에서 정책 배포를 재설정합니다.

policydeploy -restore Function - 모든 정책 복원

이 함수는 지정된 호스트에서 모든 정책의 배포를 취소한 다음, 모든 배포 작업을 실행을 위해 호스트로 다시 전달함으로써 호스트에 배포해야 할 모든 정책을 복원(직접 재배포)합니다.

중요! 호스트에 이미 몇몇 정책이 적용되었으면 실행 전에 호스트 상태가 재설정되지 않으므로 복원이 실패합니다. 대신 policydeploy -reset 함수를 사용하십시오.

이 함수의 형식은 다음과 같습니다.

```
policydeploy -restore hnode_name [-dms list]
```

-dms list

(선택 사항) 사용할 DMS 노드의 목록을 쉼표로 구분하여 지정합니다. 정책을 배포하거나 배포 취소할 때 이러한 DMS 노드에 작업이 보고됩니다. 정책을 저장할 때 이러한 DMS 노드에 정책이 저장됩니다.

이 옵션으로 DMS 노드를 지정하지 않으면 로컬 CA Access Control 데이터베이스에 지정된 DMS 노드의 목록이 사용됩니다. 데이터베이스에서 DMS 노드의 목록을 지정하려면, dmsmgr 을 사용하여 새 DMS 를 만든 후 다음 selang 명령을 작성해야 합니다.

```
so dms+(new_dms_name)
```

참고: 설치 중 DMS 노드를 지정하지 않았거나 끝점에서 등록된 DMS 를 바꾸거나 추가하려는 경우 동일한 명령을 작성해야 합니다. 그러나 설치 중 고급 정책 관리 서버를 만들도록 지정하면 DMS 가 데이터베이스에 추가되므로 위 명령을 직접 실행할 필요가 없습니다.

-restore hnode_name

지정된 호스트에 배포해야 할 모든 정책을 복원(직접 재배포)합니다.

policydeploy -store 함수 - 정책 저장

이 함수는 지정된 정책을 명령에서 지정된 DMS 노드에 저장하거나 로컬 CA Access Control 데이터베이스에 저장합니다. -silent 옵션을 사용하지 않은 경우, 메시지가 표시되면 이 작업을 확인해야 합니다.

지정한 정책의 이전 버전이 DMS 에 저장되어 있지 않으면 정책의 버전 1 이 작성됩니다(name#01). 이 정책의 이전 버전이 있으면 정책의 새 버전이 작성됩니다(name#last_version+1). 저장하는 정책 버전은 자동으로 완료됩니다. 정책을 업데이트하려면 수정된 필수 정책 배포 및 배포 취소 규칙이 포함된 새 정책 버전을 저장해야 합니다.

이 함수의 형식은 다음과 같습니다.

```
policydeploy -store name -ds file1 [-uds file2] [-dms list] [-desc description] [-prereq
list] [-silent]
```

-desc description

(선택 사항) 정책에 대한 비즈니스 설명을 정의합니다.

-dms list

(선택 사항) 사용할 DMS 노드의 목록을 쉼표로 구분하여 지정합니다. 정책을 배포하거나 배포 취소할 때 이러한 DMS 노드에 작업이 보고됩니다. 정책을 저장할 때 이러한 DMS 노드에 정책이 저장됩니다.

이 옵션으로 DMS 노드를 지정하지 않으면 로컬 CA Access Control 데이터베이스에 지정된 DMS 노드의 목록이 사용됩니다. 데이터베이스에서 DMS 노드의 목록을 지정하려면, dmsmgr 을 사용하여 새 DMS 를 만든 후 다음 selang 명령을 작성해야 합니다.

```
so dms+(new_dms_name)
```

참고: 설치 중 DMS 노드를 지정하지 않았거나 끝점에서 등록된 DMS 를 바꾸거나 추가하려는 경우 동일한 명령을 작성해야 합니다. 그러나 설치 중 고급 정책 관리 서버를 만들도록 지정하면 DMS 가 데이터베이스에 추가되므로 위 명령을 직접 실행할 필요가 없습니다.

-ds file1

배포 규칙을 포함하는 파일의 경로 이름을 지정합니다. 이들이 정책 구성에 필요한 명령입니다. -getrules 옵션을 사용하면 이 파일이 작성됩니다.

중요! 정책 배포에서는 사용자 암호를 설정하는 명령을 지원하지 않으므로 배포 스크립트 파일에 이러한 명령을 포함시키지 마십시오. 네이티브 selang 명령은 지원되지만 위반 보고서에는 표시되지 않습니다.

-prereq list

(선택 사항) 이 정책을 배포하기 전에 배포해야 하는 정책의 목록을 쉼표로 구분하여 정의합니다.

중요! 의존적인 정책을 배포하려고 할 때 필수 정책이 배포되어 있지 않으면 배포 작업의 상태가 Pending Prerequisite 로 변경되며 모든 필수 정책이 배포된 후 배포가 다시 시작됩니다. 마찬가지로, 다른 배포된 정책의 전제 조건이 되는 정책을 배포 취소하려고 하면, 배포 작업의 상태가 Pending Dependents 로 변경되며 모든 의존적인 정책이 배포 취소된 후 배포가 다시 시작됩니다.

-silent

(선택 사항) 요청한 작업에 대해 확인 메시지를 표시하지 않습니다.

-store name

지정된 정책을 지정된 DMS 노드에 저장하거나 로컬 CA Access Control 데이터베이스에 저장합니다.

참고: 정책 이름에는 #(해시) 문자를 포함할 수 없습니다. 이 문자는 정책 버전 번호를 나타내기 위해 예약되어 있으며 자동으로 추가됩니다.

-uds file2

정책의 배포 취소를 위해 필요한 규칙이 포함된 파일의 경로 이름을 정의합니다. 이들이 정책 배포 취소에 필요한 명령입니다. -getrules 옵션을 사용하면 이 파일이 작성됩니다.

CA Access Control 이 정책을 배포 취소할 때 저장되어 있는 정책 배포 취소 스크립트가 없으면 CA Access Control 은 정책 제거를 위해 필요한 명령을 계산합니다.

예: IIS 5 보호 정책 저장

다음 예에서는 IIS(Internet Information Services) 5 웹 서버의 보안을 위한 정책을 저장하는 방법을 설명합니다. 이 과정은 이 정책을 DMS 에 처음 저장하는 경우에 해당합니다.

참고: 이 예에서 selang 명령은 Windows 운영 체제의 리소스에 사용되지만 동일한 절차가 UNIX 에도 적용됩니다.

1. 다음 IIS 스크립트를 사용하여 IIS5.selang 이란 이름으로 파일을 저장합니다.

   ```
   # IIS5 deployment script
   eu inet_pers owner(nobody)
   er FILE c:\InetPub\wwwroot\* defaccess(none) owner(nobody)
   authorize FILE c:\InetPub\wwwroot\* uid(inet_pers) access(all)
   er FILE c:\InetPub\wwwroot\scripts defaccess(none) owner(nobody)
   er FILE *.asp defaccess(none) owner(nobody)
   authorize FILE *.asp uid(inet_pers) via(pgm(inetinfo.exe)) access(read, execute)
   ```

   이러한 명령은 IIS 5 보호 정책을 배포하는 데 필요한 명령입니다.

2. 다음 스크립트를 사용하여 IIS5_rm.selang 이란 이름으로 파일을 저장합니다.

   ```
   # IIS5 undeployment script
   ru inet_pers
   rr FILE c:\InetPub\wwwroot\*
   rr FILE c:\InetPub\wwwroot\scripts
   rr FILE *.asp
   ```

   이러한 명령은 1 단계에서 작성한 IIS 5 보호 정책의 배포를 취소하는 데 필요한 명령입니다.

3. 명령 프롬프트 창을 연 다음 policydeploy 유틸리티를 실행합니다.

   ```
   policydeploy -store IIS5 -ds IIS5.selang -uds IIS5_rm.selang -desc "IIS5 web server security policy" -silent
   ```

   이렇게 하면 DMS 에 정책 IIS5(GPOLICY 개체)와 첫 번째 정책 버전(IIS5#01 POLICY 개체)이 IIS5.selang 및 IIS5_rm.selang 에 정의된 스크립트와 함께 저장됩니다.

policydeploy -upgrade 함수 - 정책 버전 업그레이드 또는 다운그레이드

이 함수는 정의된 호스트에서 가장 최근의 완료된 버전으로 정책을 업그레이드하거나 정의된 호스트에서 지정된 버전으로 정책을 다운그레이드합니다.

이 함수의 형식은 다음과 같습니다.

```
policydeploy {-upgrade name | -downgrade name#xx} [-nodelist hnode_list|-ghnode name] [-list] [-dms name]
```

-dms list

(선택 사항) 사용할 DMS 노드의 목록을 쉼표로 구분하여 지정합니다. 정책을 배포하거나 배포 취소할 때 이러한 DMS 노드에 작업이 보고됩니다. 정책을 저장할 때 이러한 DMS 노드에 정책이 저장됩니다.

이 옵션으로 DMS 노드를 지정하지 않으면 로컬 CA Access Control 데이터베이스에 지정된 DMS 노드의 목록이 사용됩니다. 데이터베이스에서 DMS 노드의 목록을 지정하려면, dmsmgr 을 사용하여 새 DMS 를 만든 후 다음 selang 명령을 작성해야 합니다.

```
so dms+(new_dms_name)
```

참고: 설치 중 DMS 노드를 지정하지 않았거나 끝점에서 등록된 DMS 를 바꾸거나 추가하려는 경우 동일한 명령을 작성해야 합니다. 그러나 설치 중 고급 정책 관리 서버를 만들도록 지정하면 DMS 가 데이터베이스에 추가되므로 위 명령을 직접 실행할 필요가 없습니다.

-downgrade name#xx

정의된 호스트에서 정책을 지정된 정책 버전으로 다운그레이드합니다.

-ghnode name

수행할 작업에 대한 호스트 그룹의 이름을 정의합니다.

-list

(선택 사항) 지정된 배포 정책 버전(지정된 버전이 아님)이 있는 호스트를 나열합니다. -upgrade 를 사용하면 암시적으로 지정된 버전이 사용 가능한 최신 버전입니다.

-nodelist hnode_list

작업을 수행하고자 하는 호스트(HNODE 개체)의 목록을 쉼표로 구분하여 정의합니다.

-upgrade name

정의된 호스트에서 지정한 정책을 최신 완료 버전으로 업그레이드합니다.

예: IIS 5 보호 정책 업그레이드

다음 예에서는 정책을 업그레이드하는 방법에 대해 설명합니다. 먼저 배포를 검토하여 배포된 이 정책의 최신 버전이 없는 호스트를 확인합니다.

1. 명령줄 프롬프트에서 다음과 같이 policydeploy 유틸리티를 실행합니다.

   ```
   policydeploy -upgrade IIS5 -list
   ```

   이 유틸리티를 실행하면 배포된 IIS5 정책의 이전 버전이 포함된 호스트가 나열됩니다.

2. 이러한 호스트를 모두 최신 정책 버전으로 업그레이드합니다.

   ```
   policydeploy -upgrade IIS5
   ```

예: IIS 5 보호 정책 다운그레이드

다음 예에서는 정책을 다운그레이드하는 방법에 대해 설명합니다. 먼저 배포를 검토하여 이전 버전의 배포된 정책이 포함된 호스트를 확인합니다.

1. 명령줄 프롬프트에서 다음과 같이 policydeploy 유틸리티를 실행합니다.

   ```
   policydeploy -downgrade IIS5#3 -list
   ```

   이 유틸리티를 실행하면 버전 3 이상의 배포된 IIS5 정책 버전이 포함된 호스트가 나열됩니다.

2. 이러한 호스트를 모두 세 번째 정책 버전으로 다운그레이드합니다.

   ```
   policydeploy -downgrade IIS5#3
   ```

report_agent.sh 스크립트 - 보고서 에이전트 구성

UNIX 에 해당

report_agent.sh 스크립트를 사용하면 설치 후에 보고서 에이전트 데몬을 구성할 수 있습니다. CA Access Control 을 설치할 때 지정한 보고서 에이전트 구성 설정을 변경해야 하는 경우 report_agent.sh 스크립트를 사용합니다.

report_agent.sh 스크립트는 ACSharedDir/lbin 에 있습니다. 기본적으로 이 디렉터리는 /opt/CA/AccessControlShared/lbin 입니다.

이 명령의 형식은 다음과 같습니다.

```
report_agent start
report_agent stop
report_agent config -server hostname [-proto {ssl|tcp}] [-port port_number] [-rqueue
queue_name] \
[-schedule <time@day[,day2,...]>] [-audit] [-bak] [-silent]
```

config

나머지 매개 변수가 보고서 에이전트 데몬을 구성하도록 지정합니다.

start

보고서 에이전트를 시작합니다.

stop

보고서 에이전트를 중지합니다.

-server hostname

배포 서버 호스트 이름의 이름을 정의합니다. -port 옵션의 입력과 결합할 경우 스크립트에서 배포 서버 URL 을 구성하고 ReportAgent 섹션의 report_server 구성 설정을 지정합니다.

-audit

끝점 감사 데이터를 배포 서버로 보낼지 여부를 지정합니다. ReportAgent 섹션의 reportagent_enabled 구성 설정이 지정됩니다.

-bak

타임스탬프가 지정된 감사 파일 백업을 유지하도록 지정합니다. logmgr 섹션 구성 설정 Backup_Date 가 yes 로 설정되고 audit_max_files 가 50 으로 설정됩니다.

-port port_number

배포 서버와 통신하는 데 사용할 포트 번호를 정의합니다. -server 옵션의 입력과 결합할 경우 스크립트에서 보고서 서버 URL 을 구성하고 ReportAgent 섹션의 report_server 구성 설정을 지정합니다.

-proto

연결 프로토콜(TCP 또는 SSL)을 지정합니다. ReportAgent 섹션의 use_ssl 구성 설정이 지정됩니다.

-rqueue queue_name

보고서 에이전트가 로컬 데이터베이스의 스냅숏과 PMDB 를 보내는 큐의 이름을 정의합니다. 이 옵션은 ReportAgent 섹션의 send_queue 구성 설정을 설정합니다.

-schedule <time@day[,day2,...]>

보고서를 생성할 시간과 보고서를 배포 서버로 보낼 시간을 정의합니다.

-silent

확인 메시지를 표시하지 않도록 지정합니다.

예: 보고서 에이전트 구성

이 예에서는 queue/snapshots 라는 큐와 SSL 을 통한 포트 7243 을 사용하여 rscomp.com 의 배포 서버로 데이터베이스 스냅숏을 보내도록 보고서 에이전트를 설정합니다. 또한 감사 데이터를 배포 서버로 보내도록 설정하고 감사 로그 파일에 대한 백업 설정을 지정합니다.

```
report_agent.sh config -server rscomp.com -proto ssl -port 7243 -rqueue queue/snapshots
-audit
```

배포 에이전트를 구성했으면 보고서 서버에 필요한 올바른 암호(공유 암호)를 사용하여 +reportagent 사용자를 업데이트해야 합니다. 이렇게 하려면 다음을 입력합니다.

```
eu +reportagent epassword(Shared_Secret) nonnative
```

추가 정보:

ReportAgent (페이지 253)

seaudit 유틸리티-감사 로그 레코드 표시

seaudit 유틸리티는 CA Access Control 감사 로그 파일의 레코드를 표시합니다. seaudit 유틸리티를 실행하려면 AUDITOR 특성이 있어야 합니다. 암호를 포함하는 감사 레코드를 표시할 때 seaudit 는 암호 텍스트 대신 일련의 별표(***)를 입력하여 암호를 보호합니다.

참고: 명령 스위치와 옵션에 문자열 일치를 사용할 수 있습니다. 일부 UNIX 셸은 마스크 인수를 자동으로 확장합니다. 따라서 이러한 셸에서 seaudit 를 호출하는 경우 별표 또는 물음표 앞에 백슬래시(\)를 입력하여 셸이 마스크를 처리하지 않도록 해야 합니다.

이 명령의 형식은 다음과 같습니다.

```
seaudit switch [options]
```

switch

유틸리티에 대한 작업 모드를 정의합니다. 다음 중 하나가 될 수 있습니다.

-a | -all

추적 기능으로 감사 로그에 전송된 사용자 추적 레코드를 제외한 모든 레코드를 표시합니다.

참고: UNIX 에 사용 가능한 연결된 TCP 레코드도 표시되지 않습니다. 이러한 레코드를 표시하려면 -c 옵션도 지정해야 합니다.

-h | -help

이 유틸리티에 대한 도움말을 표시합니다.

{-i | -inet} host service

지정된 서비스의 지정된 호스트에서 받은 TCP 요청의 INET 감사 레코드를 표시합니다. host 와 service 는 seaudit 에서 검색하는 호스트 및 서비스 세트를 식별하는 마스크입니다.

UNIX 에서 연결된 네트워크 ID(포트 번호)와 함께 TCP 레코드를 나열하려면 -c 플래그를 추가하십시오. 예:

```
seaudit -i -c myhost telnet
```

{-l | -login} user1, user2, ... terminal

지정된 터미널에서 쉼표로 구분된 지정 사용자에 대한 LOGIN 레코드를 표시합니다.

user 와 terminal 은 모두 마스크입니다.

UNIX 에서 이것은 또한 사용자를 활성화하고 비활성화할 때 serevu 가 작성한 레코드 및 잘못된 암호를 입력할 때 권한 부여 데몬이 작성한 레코드를 표시합니다.

{-r | -resource} class resource user1, user2, ...

쉼표로 구분된 지정 사용자의 지정 리소스에 대한 지정 클래스의 일반 리소스 감사를 표시합니다.

- class 는 액세스된 리소스가 속한 클래스를 식별하는 마스크입니다.
- resource 는 액세스된 리소스의 이름을 식별하는 마스크입니다.
- user 는 리소스를 액세스한 사용자 이름의 마스크입니다.

-s | -start

CA Access Control 시작 및 종료 메시지를 표시합니다.

-St | -Stat message_number

(UNIX 전용). watchdog 메시지 번호의 설명을 표시합니다.

-t | -table

로그 코드의 표를 표시합니다.

-tr

활동이 추적되는 모든 사용자의 추적 레코드를 표시합니다.

참고: 추적 레코드에는 기본적으로 로그인 세션 ID 열이 표시됩니다. 이 열을 표시하지 않으려면 -format 옵션을 사용합니다.

-trr resource

지정된 리소스의 추적 레코드를 표시합니다.

-tru {uid1|user1}, {uid1|user2}, ...

숫자 uid 또는 사용자 이름이 지정된 사용자의 추적 레코드를 표시합니다.

-u command class record user

데이터베이스 업데이트 감사 레코드를 표시합니다.

- command 는 검색할 selang 명령 세트를 식별하는 마스크입니다.
- class 는 검색할 클래스를 식별하는 마스크입니다.
- record 는 검색할 레코드를 식별하는 마스크입니다.
- user 는 명령을 실행한 사용자를 식별하는 마스크입니다.

-w

watchdog 감사 레코드를 표시합니다.

옵션

유틸리티의 정보 표시 방법을 변경하는 선택적인 한정자를 정의합니다. 다음 중 하나 이상이 될 수 있습니다.

-c

(UNIX 전용). 연결된 INET 레코드를 표시합니다. 이러한 레코드는 세션 ID 추적을 위해 생성된 레코드이며, 성공적인 TCP 연결의 포트 번호를 나열합니다.

예를 들어, 사용자(user1)가 comp1 에서 comp2 로(두 곳에 모두 CA Access Control 이 설치됨) Telnet 세션을 엽니다. Telnet 세션 중에 로그인한 사용자(user1 이외의 사용자일 수 있음)의 자격 증명과 함께 comp1 에 승인을 보내도록 comp2 의 CA Access Control 을 구성할 수 있습니다. comp1 은 이 승인을 받으면 TCP-CONNECTED 레코드(세션 설정 레코드)를 작성합니다. 이후 -c 옵션으로 이 레코드를 표시할 수 있습니다.

-detail

각 레코드에 대한 자세한 정보를 표시합니다.

-delim delimiter

첫 번째 필드 앞과 나머지 필드들 사이에 사용할 구분 기호를 정의합니다. 예를 들어, 다음 명령을 사용하면 필드가 인용 부호 안에 표시되고 쉼표로 구분됩니다.

seaudit -a -delim \",\"

-delim2 delimiter

(UNIX 전용). 구분 기호가 첫 번째 필드 앞에 나타나지 않는다는 점만 제외하고 -delim 옵션과 같습니다.

-ed date

종료 날짜를 지정합니다. 이 날짜 이후에 기록된 레코드는 표시되지 않습니다.

다음 두 방법 중 하나로 date 를 지정할 수 있습니다.

- dd-mm-yyyy 형식 사용
- today 문자열을 사용하여 날짜를 오늘로 설정

문자열 today 뒤에 -(빼기 기호)와 숫자를 사용할 수도 있습니다. 이렇게 하면 날짜가 오늘부터 지정한 일 수 이전의 날짜로 정의됩니다. 예를 들어, today-3 은 날짜가 3 일 전임을 의미합니다.

-et time

종료 시간을 지정합니다. 이 시간 이후에 기록된 레코드는 표시되지 않습니다.

다음 두 방법 중 하나로 time 을 지정할 수 있습니다.

- 24 시간 형식 hh:mm 사용
- now 문자열을 사용하여 시간을 지금으로 설정

  문자열 now 뒤에 -(빼기 기호)와 숫자를 사용할 수도 있습니다. 이렇게 하면 시간이 지금부터 지정한 분 수 이전의 시간으로 정의됩니다. 예를 들어, now-60 을 지정하면 시간이 60 분(1 시간) 전을 의미합니다. 특정 날짜 내의 시간 프레임을 설명하려면 -sd, -ed 또는 둘 모두와 함께 이 옵션을 사용하십시오.

-f | -failure

액세스 실패를 표시하지 않도록 지정합니다.

{-fn | -file} fileName

검색할 감사 로그 파일의 이름을 지정합니다.

-format release

출력 형식이 CA Access Control 릴리스용으로 만든 것처럼 보이도록 지정합니다.

release - 릴리스 번호를 정의합니다. 유효한 값:

- **80sp1** - r8 SP1 의 출력에는 최신 릴리스에 있는 유효한 UID 열이 포함되지 않았습니다.
- **12** - r12.0 의 출력에는 암호 변경 레코드를 표시하는 기능이 포함되지 않았습니다. 추적 레코드에 대해 r12.0 의 출력에는 또한 로그인 세션 ID 정보가 포함되지 않았습니다.

-g | -grant

성공적인(허용된) 액세스를 표시하지 않도록 지정합니다.

-gn | -grantnotify

성공적인(허용된) 액세스를 표시하지 않도록 지정합니다(알림 레코드 제외).

-logout

(UNIX 전용) 로그아웃 레코드를 표시하지 않도록 지정합니다.

-millennium

(UNIX 전용) 연도가 두 개의 숫자 대신 네 개의 숫자로 표시되도록 지정합니다.

-n | -netaddr

TCP/IP 레코드에 호스트 이름 대신 인터넷 주소가 표시되도록 지정합니다.

-notify

NOTIFY 감사 레코드를 표시하지 않도록 지정합니다.

{-o | -origin} host

지정한 호스트에서 시작된 레코드만 표시하도록 지정합니다.

이 옵션은 selogrcd 로그 라우트 수집 데몬에서 작성된 통합 감사 파일에서 레코드를 검색할 경우에만 적용됩니다.

-pwa

(UNIX 전용) 암호 시도 레코드를 표시하지 않도록 지정합니다.

-sd date

시작 날짜를 지정합니다. 이 날짜 이전에 기록된 레코드는 표시되지 않습니다.

다음 두 방법 중 하나로 date 를 지정할 수 있습니다.

- dd-mm-yyyy 형식 사용
- today 문자열을 사용하여 날짜를 오늘로 설정

문자열 today 뒤에 -(빼기 기호)와 숫자를 사용할 수도 있습니다. 이렇게 하면 날짜가 오늘부터 지정한 일 수 이전의 날짜로 정의됩니다. 예를 들어, today-3 은 날짜가 3 일 전임을 의미합니다.

sessionid

사용자 로그인 세션 ID 정보가 포함된 열을 표시하도록 지정합니다. 이 열은 기본적으로 숨겨져 있습니다.

참고: r12.0 SP1 이상 버전에서 제공되는 끝점에만 이 옵션을 사용할 수 있습니다.

-st time

시작 시간을 지정합니다. 이 시간 이전에 기록된 레코드는 표시되지 않습니다.

다음 두 방법 중 하나로 time 을 지정할 수 있습니다.

- 24 시간 형식 hh:mm 사용
- now 문자열을 사용하여 시간을 지금으로 설정

문자열 now 뒤에 -(빼기 기호)와 숫자를 사용할 수도 있습니다. 이렇게 하면 시간이 지금부터 지정한 분 수 이전의 시간으로 정의됩니다. 예를 들어, now-60 을 지정하면 시간이 60 분(1 시간) 전을 의미합니다. 특정 날짜 내의 시간 프레임을 설명하려면 -sd, -ed 또는 둘 모두와 함께 이 옵션을 사용하십시오.

-v | -servnum

서비스 이름 대신 포트 번호가 표시되도록 지정합니다.

-warn

경고 레코드를 표시하지 않도록 지정합니다.

예제

- 2004 년 1 월 3 일 이후의 모든 감사 레코드를 나열하려면 다음 명령을 사용합니다.

  ```
  seaudit -a -sd 04-Jan-2004
  ```

- 2004 년 1 월 3 일 모든 터미널에서 사용자 root 의 실패한 로그인을 나열하려면 다음 명령을 사용합니다.

  ```
  seaudit -sd 04-Jan-2004 -ed 04-Jan-2004 -l root * -g
  ```

- 클래스 FILE 의 모든 리소스에 대한 사용자 John 의 모든 액세스를 나열하려면 다음 명령을 사용합니다.

  ```
  seaudit -r FILE * John
  ```

- 17:00(첫째 날) 및 08:00(다음 날) 사이에 기록된 모든 감사 레코드를 모든 날짜에 대해 나열하려면 다음 명령을 사용합니다.

  ```
  seaudit -a -st 17:00 -et 08:00
  ```

- 08:00 및 17:00 사이에 기록된 모든 감사 레코드를 나열하려면 다음 명령을 사용합니다.

  ```
  seaudit -a -st 08:00 -et 17:00
  ```

- 단일 사용자의 로그인 및 리소스 액세스에 대한 모든 경고 레코드를 나열하려면 다음 명령을 사용합니다.

  ```
  seaudit -login * * -resource * * * -grant -failure -logout -pwa
  ```

- 두 사용자의 모든 로그인 레코드를 나열하려면 다음 명령을 사용합니다.

  ```
  seaudit -login "user1, user2"
  ```

- 어제부터의 모든 감사 레코드를 나열하려면 다음 명령을 사용합니다.

  ```
  seaudit -a -sd today-1 -ed today-1
  ```

- UID 244 의 단일 사용자가 파일에 액세스를 시도한 활동을 추적하는 모든 감사 레코드를 나열하려면 다음 명령을 사용합니다.

  ```
  seaudit -tru 244 -trr FILE
  ```

- 두 사용자의 활동을 추적하는 모든 감사 레코드를 나열하려면 다음 명령을 사용합니다.

  ```
  seaudit -tru "user1, 244"
  ```

추가 정보:

감사 레코드의 이벤트 유형을 식별하는 방법 (페이지 476)
감사 이벤트 유형 (페이지 478)

sebuildla 유틸리티-Lookaside 데이터베이스 작성

UNIX 에 해당

sebuildla 유틸리티는 CA Access Control 데몬인 seosd 에 의해 사용되는 lookaside 데이터베이스를 작성합니다. seosd 데몬은 이 데이터베이스를 사용하여 UNIX UID 를 사용자 이름으로, GID 를 그룹 이름으로, 호스트 IP 주소를 호스트 이름으로, 서비스 포트를 포트 이름으로 변환합니다. 이 데이터베이스에는 번호-이름 변환만 포함되어 있습니다. 또한 sebuildla 를 사용하면 LDAP DIT(디렉터리 정보 트리)의 정보를 lookaside 데이터베이스에 추가할 수 있습니다.

중요! sebuildla 및 필수 LDAP 구성 설정을 설정하려면 LDAP 에 대해 잘 알고 있고 ldapsearch 명령을 실행할 수 있어야 합니다. ldap(1), ldapsearch(1)에 대한 man 페이지와 LDAP 클라이언트 설명서에서 설정 정보를 검토하는 것이 좋습니다. sebuildla 를 사용하여 lookaside 데이터베이스를 작성하기 전에, ookaside_path 구성 설정에서 lookaside 데이터베이스의 전체 경로를 지정하십시오.

처음 lookaside 데이터베이스를 작성할 때 다음 명령을 사용합니다.

```
sebuildla a
```

이렇게 하면 모든 구성 요소가 생성됩니다. 데이터베이스의 단일 파일은 관련 스위치를 사용하여 나중에 업데이트될 수 있습니다.

CA Access Control 을 NIS, NIS+ 또는 DNS 서버에 설치한 경우 관련 makefile 에서 sebuildla 유틸리티를 호출해야 합니다.

참고: 기본적으로 lookaside 데이터베이스 파일(groupdb.la, hostdb.la, servdb.la 및 userdb.la)은 sebuildla 프로그램을 사용한 액세스가 아닌 모든 사용자 액세스에 대해 보호됩니다.

sebuildla 유틸리티는 /etc 파일 및 NIS 와 같은 시스템의 확인 메커니즘을 스캔하여 lookaside 데이터베이스를 작성합니다.

- sebuildla 는 사용한 도메인 이름을 가져오기 위해 /etc/resolv.conf 를 읽습니다.

  참고: CA Access Control 에서 호스트 이름을 정규화된 이름에 대해 확인하려면 resolv.conf 파일에 도메인 또는 검색 구성 옵션이 정의되어 있어야 합니다. resolv.conf 파일에 대한 자세한 내용은 이 파일의 man 페이지를 참조하십시오.

- sebuildla 는 시스템 확인 옵션을 사용하여 lookasaide 데이터베이스를 작성합니다. 일반적으로 이 옵션은 네트 캐시 데몬입니다.

- CA Access Control 은 네트 캐시 데몬이나 다른 모든 시스템 확인(resolution) 옵션에 대해 /etc/nsswitch.conf 파일을 사용하여 데이터 검색 위치를 결정합니다.

예를 들어, /etc/nsswitch.conf 파일에 호스트에 대한 다음 행이 포함되어 있으면 먼저 로컬 컴퓨터의 파일(/etc/hosts)에서 정보를 검색한 다음 DNS 와 NIS 에서 차례로 정보를 검색합니다.

```
hosts:    files dns nis
```

파일에 다음 행이 대신 포함되어 있으면 로컬 컴퓨터의 파일에서만 정보를 검색합니다. lookaside 데이터베이스에는 /etc/hosts 에 있는 호스트만 포함됩니다.

```
hosts:    files
```

참고: 호스트가 정규화된 이름을 가진 경우 sebuildla 는 이 이름을 사용합니다.

컴퓨터 구성의 차이 때문에 sebuildla 가 로컬 환경의 이름을 모두 나열하지 않을 수도 있습니다. 이런 경우 sebuildla 를 사용하여 목록 파일에서 필요한 항목을 모두 로드할 수 있습니다. 이렇게 하려면 각 개체 이름이 있는 목록 파일을 각 행에 작성하십시오. 유틸리티는 이 목록 파일을 읽고 필요에 따라 목록 파일의 모든 개체를 관련 lookaside 데이터베이스에 추가합니다. sebuildla 는 중복 개체를 무시합니다.

다음 표에서는 sebuildla 가 각 lookaside 데이터베이스를 작성하기 위해 사용하는 파일을 나열합니다.

개체 위치	추가 위치
ACInstallDir/ladb/userlist	사용자 lookaside 데이터베이스
ACInstallDir/ladb/grouplist	그룹 lookaside 데이터베이스
ACInstallDir/ladb/hostlist	호스트 lookaside 데이터베이스
ACInstallDir/ladb/servlist	서비스 lookaside 데이터베이스

ACInstallDir/ladb 디렉터리에 있는 파일의 형식에서:

- sebuildla 는 비어 있는 행이나 느낌표(!), 숫자 기호(#) 또는 세미콜론(;)으로 시작하는 행은 무시합니다.
- 항목을 확인할 수 있는 경우 다른 행은 sebuildla 가 관련 lookaside 데이터베이스에 추가하는 항목을 나타냅니다.
- 사용자, 그룹, 호스트 또는 서비스 이름은 행의 첫 번째에 있어야 합니다.

dbmgr -dump -r 을 사용하여 목록 파일을 작성할 수 있습니다. 예를 들어, 로컬 데이터베이스의 HOST 클래스에 정의된 호스트 목록을 작성하려면 다음 명령을 입력합니다.

```
dbmgr -dump r l HOST > /opt/CA/AccessControl/ladb/hostlist
```

l 스위치는 가져오는 각 호스트 항목의 FQDN 을 DNS 서버에 쿼리하는 대신, 기본 도메인의 모든 호스트 목록에 대한 DNS 요청 한 개를 수행합니다. 신속한 로드 옵션은 DNS 가 설치된 경우에만 적용됩니다. 기본 도메인의 호스트 이름만 유효한 전체 이름이 되고 유효한 전체 이름으로 남아 있게 됩니다. 시스템 메커니즘에서 검색한 호스트 이름이 유효한 전체 이름이 아니거나 기본 도메인에 없는 호스트 이름은 유효하지 않은 전체 이름으로 남아 있게 됩니다. 호스트 목록 파일에서 로드된 호스트 이름 중에서 유효하지 않은 전체 호스트 이름은 삭제됩니다.

이 명령의 형식은 다음과 같습니다.

```
sebuildla switch [options]
```

switch

유틸리티에 대한 작업 모드를 지정합니다. 다음 중 하나가 될 수 있습니다.

-a

모든 lookaside 데이터베이스 파일을 생성합니다.

-e

DNS 를 제외한 호스트 lookaside 데이터베이스 파일을 생성합니다.

-g

그룹 lookaside 데이터베이스 파일을 생성합니다.

-h

DNS 를 포함한 호스트 lookaside 데이터베이스 파일을 생성합니다.

-help

이 유틸리티에 대한 도움말을 표시합니다.

-n

LDAP DIT 에서 정보를 수집하여 주 사용자 데이터 원본(-u 스위치)으로부터 작성한 사용자 lookaside 데이터베이스에 추가합니다. 이 스위치는 반드시 -u 스위치나 -a 스위치와 함께 사용해야 하므로, LDAP DIT 가 추가 사용자 데이터를 제공하고 시스템의 명명 서비스로서 사용되지 않을 때 가장 유용합니다.

이 스위치를 사용하기 전에 다음 단계를 따르십시오.

a. CA Access Control 에 대해 seos.ini 파일 토큰(ldap_base, ldap_hostname 및 ldap_userdn)을 설정하여 LDAP 서비스를 찾습니다.

b. seldapcred 유틸리티를 실행하여 암호화된 LDAP 암호를 저장합니다.

c. (선택 사항) 환경에 대해 ldap_port 및 ldap_timeout 토큰을 설정합니다.

   LDAP 서비스에서 정보를 검색하는 데 걸리는 시간은 LDAP 서비스의 속도 및 DIT 에 저장된 사용자 데이터 양에 따라 다릅니다. 이러한 부분을 설명하기 위해 seos.ini 파일의 [seos] 섹션에서 ldap_timeout 토큰을 조정할 수 있습니다.

d. (선택 사항) 비표준 스키마를 사용하는 경우 ldap_uid_attr, ldap_uidNumber_attr 및 ldap_user_class 토큰을 설정합니다.

-s

서비스 lookaside 데이터베이스 파일을 생성합니다.

-u

사용자 lookaside 데이터베이스 파일을 생성합니다.

참고: LDAP 서비스에서 수집한 사용자 데이터를 추가하기 위해 -n 스위치를 -u 스위치와 함께 지정할 수 있습니다.

-G

그룹 lookaside 데이터베이스 파일의 내용을 나열합니다.

-H [IPv4 | IPv6]

호스트 lookaside 데이터베이스 파일의 내용을 나열합니다.

-S

서비스 lookaside 데이터베이스 파일의 내용을 나열합니다.

-U

사용자 lookaside 데이터베이스 파일의 내용을 나열합니다.

옵션

유틸리티의 정보 표시 방법을 변경하는 선택적인 한정자를 지정합니다. 다음 중 하나 이상이 될 수 있습니다.

-l

목록 파일만 사용하여 lookaside 데이터베이스를 로드합니다. 이 옵션은 시스템의 확인(resolution) 메커니즘을 제외합니다.

-f

h 스위치를 사용하여 lookaside 데이터베이스(호스트만)를 신속하게 로드합니다.

추가 정보:

seos.ini 초기화 파일 (페이지 256)

sechkey 유틸리티

CA Access Control 암호화를 관리하고 이를 통해 CA Access Control 관리 통신을 보호하려면 sechkey 유틸리티를 사용하십시오.

대칭 암호화를 위한 암호화 키를 설정하기 위해 이 유틸리티를 사용할 수 있으며, PKI 암호화에 대해 사용할 수도 있습니다.

대칭 키를 사용하는 경우 키의 기본값을 변경하는 것이 좋습니다. PKI 를 사용하는 경우 기본 인증서 및 관련된 기본 개인 키를 변경하는 것이 좋습니다.

어떤 암호화를 사용하든, CA Access Control 을 설치 또는 업그레이드한 후에는 사이트의 모든 컴퓨터에서 키를 변경하십시오. 이렇게 하면 권한이 없는 사용자가 시스템에 액세스하는 것을 막을 수 있습니다.

대칭 키 모드의 sechkey 유틸리티

sechkey 는 CA Access Control 데이터베이스에서 암호화 키를 변경함으로써 대칭 키를 관리합니다.

대칭 암호화 키의 길이는 55 자입니다. sechkey 는 키 길이가 이보다 길면 자동으로 자르고 짧으면 자동으로 늘입니다.

sechkey 는 UNIX 와 Windows 에서 다르게 작동합니다.

- Windows 에서는 사용자가 암호화 키를 변경하면 sechkey 가 CA Access Control 데이터베이스의 모든 프로그램에서 키를 즉시 변경합니다.

- UNIX 에서는 sechkey 유틸리티를 사용하여 한 프로그램에 대해 암호화 키를 변경하고 다른 프로그램에서는 키를 변경하지 않을 수 있습니다.

로컬 컴퓨터에서 CA Access Control 암호화 키를 변경하거나 설정하려면 먼저 CA Access Control 을 종료해야 합니다.

UNIX 에서는 원격 컴퓨터에 대해 새 키 또는 변경된 키를 지정할 수 있습니다. 이렇게 하려면 로컬 컴퓨터와 원격 컴퓨터에서 모두 CA Access Control 이 실행되고 있어야 합니다. CA Access Control 을 다시 시작할 때 원격 컴퓨터에서 변경 사항이 적용됩니다.

중요! Windows 와 UNIX 에서 모두 통신 문제를 피하려면 모든 컴퓨터의 모든 프로그램에 대해 동일한 암호화 키를 사용하십시오.

sechkey 는 libcrypt 키를 변경할 때 컴퓨터에 설치된 각 정책 모델의 암호화된 각 레코드에 대해 다음 단계를 수행합니다.

1. 정책 모델 파일에서 암호화된 레코드를 해독합니다.
2. 키를 변경합니다.
3. 모든 레코드를 다시 암호화합니다.

또한 CA Access Control API 를 사용하여 CA Access Control 과 통신하는 프로그램을 작성할 때마다 새 프로그램의 통신이 동일한 키로 암호화됩니다.

sechkey 유틸리티-UNIX 에서 대칭 암호화 키 변경

UNIX 에 해당

sechkey 유틸리티는 CA Access Control 프로그램에 대한 CA Access Control 암호화 키를 변경합니다.

이 명령의 형식은 다음과 같습니다.

```
sechkey {oldkey | -d} {newkey | -d | -n} [-nopmd | -r hostname]

sechkey -k newkey

sechkey -c

sechkey [-e {ca | -sub} [-in <input>] [-out <output>] -priv <CA priv path>

sechkey -t [-server] -pwd <password>
```

-d

원래 키를 지정합니다.

-h

이 유틸리티에 대한 도움말을 표시합니다.

newkey

새 암호화 키를 지정합니다.

-n

현재 키를 사용하는 프로그램을 나열하며, 다른 키로 변경하지 않습니다.

-nopmd

키를 변경하며, 새 키를 사용하여 정책 모델 업데이트 파일을 업데이트하지 않습니다.

oldkey

변경할 현재 암호화 키를 지정합니다.

-r hostname

암호화 키를 변경할 원격 컴퓨터의 이름을 지정합니다.

이 옵션을 사용하려면 로컬 시스템과 원격 시스템에서 모두 CA Access Control 이 실행되고 있어야 합니다. 이 매개 변수는 실제로 키를 변경하지 않는 대신 다음에 seload -c 를 사용하여 원격 시스템에서 CA Access Control 을 시작할 때 키가 변경되도록 정보를 저장합니다. 자세한 내용은 이 장의 seload 명령을 참조하십시오.

-k

변경할 selogrd 암호화 키를 지정합니다. 암호화 키는 새 파일에 저장되거나 이전 파일에서 업데이트됩니다.

-c

selogrd 암호화 키를 지웁니다. 기본 키는 키 파일에 저장됩니다.

참고: 저장된 키 자체는 기본 암호화 방법으로 암호화됩니다.

-e

암호화 키 생성을 지정합니다.

-ca

CA 개인 키 및 인증서를 정의합니다.

-sub

주체 개인 키 및 인증서를 정의합니다.

-in <input>

암호화 세부 정보를 포함하는 입력 파일의 전체 경로 이름을 지정합니다.

-out <output>

출력 파일에 중복 암호화 세부 정보를 지정합니다.

-priv <CA priv path>

CA 개인 키의 전체 경로 이름을 지정합니다. 이 옵션은 -ca 를 사용할 때 출력 매개 변수로 사용되고 -sub 를 사용할 때 입력 변수로 사용됩니다.

-t

메시지 큐 서버 암호를 정의합니다.

-server

메시지 큐 서버 암호를 지정합니다.

-pwd <password>

새 메시지 큐 서버 암호를 정의합니다.

예: 시스템에서 아직도 기본 암호화 키를 사용하는지 확인

시스템에서 아직도 기본 암호화 키를 사용하는지 확인하려면 다음 명령을 입력합니다.

```
sechkey -d -n
```

sechkey 유틸리티-Windows 에서 대칭 암호화 키 변경

Windows 에 해당

대칭 모드에서 sechkey 유틸리티는 CA Access Control 에 대한 CA Access Control 암호화 키를 변경합니다. 매개 변수를 지정하지 않으면 새 암호화 키를 입력하라는 메시지가 표시됩니다.

이 명령의 형식은 다음과 같습니다.

```
sechkey [-d]| [-h] |[-s registry-path] [-e {ca | -sub} [-in <input>] [-out <output>]
-priv <CA priv path> [-t [server[ -pwd <password>]
```

-d

CA Access Control 과 함께 제공된 원래 암호화 키를 복원합니다.

-h

이 유틸리티에 대한 도움말을 표시합니다.

-s registry-path

CA Access Control 프로그램에 대한 암호화 키를 저장할 레지스트리 루트 경로를 지정합니다.

-e

암호화 키 생성을 지정합니다.

-ca

CA 개인 키 및 인증서를 정의합니다.

-sub

주체 개인 키 및 인증서를 정의합니다.

-in <input>

암호화 세부 정보를 포함하는 입력 파일의 전체 경로 이름을 지정합니다.

-out <output>

출력 파일에 중복 암호화 세부 정보를 지정합니다.

-priv <CA priv path>

CA 개인 키의 전체 경로 이름을 지정합니다. 이 옵션은 -ca 를 사용할 때 출력 매개 변수로 사용되고 -sub 를 사용할 때 입력 변수로 사용됩니다.

-t

메시지 큐 서버 암호를 정의합니다.

-server

메시지 큐 서버 암호를 지정합니다.

-pwd <password>

새 메시지 큐 서버 암호를 정의합니다.

PKI 모드의 sechkey 유틸리티

PKI 모드에서 sechkey 유틸리티는 PKI 인증서 및 관련 개인 키를 작성합니다.

PKI 모드에서 sechkey 를 실행하면 CA Access Control 보안 데몬이 활성화됩니다. 이는 보안 데몬이 활성화되지 않는 대칭 암호화 모드의 sechkey 와 반대됩니다.

이 명령의 형식은 다음과 같습니다.

```
sechkey -e {-ca|-sub [-priv privfilepath]} [-in infilepath] [-out outfilepath]
```

-e

sechkey 가 PKI 인증서를 작성하도록 지정합니다.

-ca

sechkey 가 CA 인증서로 사용되는 자체 서명된 인증서를 작성하도록 지정합니다.

sechkey 는 [crypto] 토큰 ca_certificate 에 의해 정의된 PEM 파일에 인증서 및 개인 키를 저장합니다.

-sub

sechkey 가 제목 인증서를 작성하도록 지정합니다.

sechkey 는 [crypto] 토큰 subject_certificate 에 의해 정의된 PEM 파일에 인증서 및 개인 키를 저장합니다.

-priv 를 지정하지 않으면, 인증서와 관련된 개인 키를 포함하는 파일이 [crypto] 토큰 private_key 에 의해 정의됩니다.

-priv privfilepath

인증서와 관련된 개인 키를 포함하는 파일을 지정합니다. 이 옵션은 -sub 옵션과 함께 사용할 경우에만 유효합니다.

-in infilepath

인증서 정보를 포함하는 입력 파일을 지정합니다. -in 을 지정하지 않으면, sechkey 는 표준 입력에서 정보를 읽습니다.

인증서를 작성하려면 sechkey 에 다음 정보가 필요합니다.

- 일련 번호
- 제목
- 첫 번째 날(인증서의 첫 번째 유효한 날)
- 마지막 날(인증서의 마지막 유효한 날)

sechkey 는 다음 정보를 사용할 수 있지만 이러한 정보가 필수 사항은 아닙니다.

- 전자 메일
- URI(종종 URL 이라고 함)
- DNS 이름
- IP 주소

-out outfilepath

인증서 정보를 저장할 출력 파일을 지정합니다. 이것은 입력 정보의 사본입니다. -out 을 지정하지 않으면, sechkey 는 입력 정보를 복제하지 않습니다.

예: sechkey -e 에 대한 입력

입력 인증서 정보의 예는 다음과 같습니다.

```
SERIAL: 00-15-58-C3-5E-4B
SUBJECT: CN=192.168.0.1
NOTBEFORE: "12/31/08"
NOTAFTER: "12/31/09"
E-MAIL: john.smith@example.com
URI: http://www.example.com
DNS: 168.192.0.100
IP: 168.192.0.1
```

seclassadm 유틸리티-CA Access Control 클래스 관리

seclassadm 유틸리티는 CA Access Control 클래스를 관리하며 새로운 사용자 정의 클래스를 로컬 데이터베이스에 추가합니다. CA Access Control 이 실행되고 있지 않을 때 데이터베이스가 있는 디렉터리에서 이 유틸리티를 호출하십시오(또는 -p 옵션 사용).

참고: seclassadm 을 실행하면 새 클래스 정보를 사용하여 seosdb 디렉터리에 파일이 작성됩니다. CreateNewClasses 구성 설정이 yes(기본값)로 설정되어 있는 경우 dbmgr -c 를 사용하여 새 데이터베이스를 생성하면 새 데이터베이스에 사용자 정의 클래스가 생성됩니다.

이 명령의 형식은 다음과 같습니다.

```
seclassadm -add className [-a access] [{-|+}c] [-d access] \
    [-f] [-g] [-o] [-p db_pathname] [-t]

seclassadm -del className

seclassadm -upd className {-|+}c [-p db_pathname]
```

-add class-name

기존 데이터베이스에 새 리소스 클래스를 추가합니다. 여기서 class-name 은 새 클래스의 이름입니다.

대문자인 클래스 이름은 CA Access Control 에서 예약되어 있습니다. 클래스를 추가할 때 소문자를 적어도 한 개는 사용해야 합니다. 클래스 이름은 최대 79 자까지 지정할 수 있습니다.

새 클래스를 작성한 후 selang setoptions 명령을 사용하여 클래스를 활성화해야 합니다.

-del class-name

지정된 리소스 클래스를 데이터베이스에서 삭제합니다.

-upd class-name

지정된 리소스 클래스를 데이터베이스에서 업데이트합니다.

-a access

클래스에 대한 액세스 모드를 지정합니다. access 문자열은 허용되는 액세스를 나타냅니다. 각 액세스 모드는 임의의 순서로 나열된 단일 문자 코드로 표시됩니다. 문자열에는 공백 또는 알파벳 문자가 아닌 다른 문자는 들어갈 수 없습니다. 유효한 액세스 모드는 다음과 같습니다.

약자	설명
C	control
D	delete
E	create
F	filescan
M	chmod
O	chown
R	read
S	security
T	utime
U	update
V	rename
W	write
X	execute

-d access

클래스에 대한 기본 액세스 모드를 지정합니다. 이는 사용자가 액세스 권한을 지정하지 않은 채 authorize 명령을 실행할 때 CA Access Control 이 사용자에게 할당하는 액세스 모드입니다. authorize 명령이 사용하는 이 암시적 액세스는 리소스에 할당된 기본 액세스와 같지 않습니다. 사용 가능한 액세스 모드는 -a 옵션으로 나열할 수 있습니다.

-f

이름이 모두 대문자인 경우에도 CA Access Control 에서 새 클래스 이름을 허용하도록 지정합니다.

참고: 기본적으로 seclassadm 유틸리티는 이름을 모두 대문자로 만들도록 허용하지 않습니다. CA Access Control 대문자 이름은 미리 정의된 CA Access Control 클래스용으로 예약되어 있습니다.

-g

새 클래스를 기존 클래스의 구성원 그룹화 리소스로 지정합니다. 기존 클래스와 새 그룹 클래스 사이의 관계는 데이터베이스의 클래스와 해당 그룹 클래스(예: TERMINAL 및 GTERMINAL) 사이의 관계와 같습니다. 기존 클래스의 구성원을 그룹화하는 리소스는 대문자 G 로 시작해야 합니다. 즉, 기존 클래스와 동일한 이름을 갖지만 접두사 G로 시작합니다.

-o

새 클래스에 대한 _default 레코드를 생성하고 기본 액세스 권한을 설정합니다.

-p db_pathname

로컬 데이터베이스의 전체 경로 이름을 지정합니다.

기본적으로 유틸리티는 현재 디렉터리의 데이터베이스에 대해 작동합니다. 데이터베이스가 있는 다른 디렉터리를 정의하려면 이 옵션을 사용하십시오.

-t

이것이 Unicenter TNG 클래스임을 지정합니다.

예: 데이터베이스에 새 클래스 추가

다음의 예는 데이터베이스에 클래스를 추가하기 위해 seclassadm 유틸리티를 사용하는 방법을 보여줍니다.

- dbfield 라는 이름으로 리소스 클래스를 추가하려면 다음 명령을 사용합니다.

  ```
  seclassadm -add dbfield
  ```

- READ 액세스 권한만 있는 report 라는 이름으로 리소스 클래스를 추가하려면 다음 명령을 사용합니다.

  ```
  seclassadm -add report -d R -a R
  ```

- READ, WRITE 및 MODIFY 권한이 있고 기본값이 READ 인(지정되지 않은 경우) batch-jobs 라는 이름으로 리소스를 추가하려면 다음 명령을 사용합니다.

  ```
  seclassadm -add batch_jobs -d R -a RWM
  ```

- 액세스 실행 및 암시적 액세스 실행을 가지고 있으며 개체가 DEPTA 클래스의 리소스 그룹인 새 클래스를 추가하려면 다음 명령을 입력합니다.

  ```
  seclassadm -add DEPTA -d X -a X -g -f
  ```

secompas 유틸리티-암호 비교

UNIX 에 해당

secompas 유틸리티는 CA Access Control 데이터베이스의 암호를 UNIX 암호 파일의 암호와 비교합니다.

CA Access Control 데이터베이스의 각 사용자에 대해 유틸리티는 한 행을 출력합니다. 이 행에는 사용자 이름과 사용자가 UNIX 에서 정의되지 않았는지, 사용자가 CA Access Control 에 암호를 가지고 있지 않은지 또는 암호가 일치하는지를 나타내는 메시지가 포함됩니다. 이 유틸리티는 또한 비교한 총 사용자 수 및 암호가 일치하지 않는 사용자 수를 표시합니다. 양쪽 환경에 암호가 모두 존재하며 동일하지 않은 경우에만 이 합계에 추가됩니다. 사용자가 환경에 정의되지 않았거나 환경에 암호가 없는 경우 secompas 는 일치하지 않는 암호 수에 합치지 않습니다.

secompas 유틸리티는 암호 비교를 위해 /etc/passwd 파일, 섀도 암호 파일 및 NIS/NIS+ 암호 맵을 사용합니다.

참고: 이 유틸리티를 사용하려면 ADMIN 특성을 가지고 있어야 합니다.

이 명령의 형식은 다음과 같습니다.

```
secompas [-db] [-ok] [-ux]
```

-db

CA Access Control 데이터베이스에 암호를 가지고 있지 않은 사용자를 표시하지 않도록 지정합니다.

-h

이 유틸리티에 대한 도움말을 표시합니다.

-ok

CA Access Control 데이터베이스와 UNIX 에 동일한 암호를 가지고 있는 사용자를 표시하지 않도록 지정합니다(암호 일치).

-ux

UNIX 에 존재하지 않는 사용자를 표시하지 않도록 지정합니다.

예: 유틸리티 출력

다음 예는 유틸리티의 샘플 출력을 보여줍니다.

```
Checking root        : No password in Access Control database.
Checking tst_001      : Undefined in UNIX.
Checking tst_002      : No password in UNIX password file
Checking tst_003      : *** PASSWORDS DO NOT MATCH. ***
Checking tst_004      : *** NO MATCH - UNIX DISABLED ***
Checking tst_005      : OK

Total of 6 users found in database.
2 unmatched password(s) found. (1 UNIX DISABLED).
```

다음은 위의 출력에 있는 각 행을 설명한 것입니다.

```
Checking root        : No password in Access Control database.
```

사용자 root 가 CA Access Control 데이터베이스에서 정의되지 않았거나 사용자가 데이터베이스에서 정의되었지만 암호를 가지고 있지 않습니다.

```
Checking tst_001      : Undefined in UNIX.
```

사용자 tst_001 이 CA Access Control 데이터베이스에서는 정의되었지만 UNIX 에서는 정의되지 않았습니다.

```
Checking tst_002      : No password in UNIX password file
```

사용자 tst_002 가 UNIX 에서 정의되었지만 암호를 가지고 있지 않습니다.

```
Checking tst_003      : *** PASSWORDS DO NOT MATCH. ***
```

CA Access Control 암호가 사용자 tst_003 의 UNIX 암호와 일치하지 않습니다.

```
Checking tst_004      : *** NO MATCH - UNIX DISABLED ***
```

tst_004 사용자 계정이 UNIX 환경에서 비활성화되었습니다. secompas 는 /etc/passwd 파일에 있는 암호 앞의 별표(*)로 비활성화된 사용자 계정을 식별합니다.

```
Checking tst_005      : OK
```

CA Access Control 암호가 사용자 tst_005 의 UNIX 암호와 일치합니다.

secons 유틸리티

secons 유틸리티는 CA Access Control 보안 콘솔입니다. 이 유틸리티를 사용하여 다음 작업을 수행할 수 있습니다.

- UNIX 의 경우:
  - 런타임 통계 표시 (페이지 131)
  - 동시 로그인 옵션 관리 (페이지 122)
  - CA Access Control 추적 관리 (페이지 121)
  - 리소스 캐싱 관리 (페이지 123)
  - CA Access Control 종료 관리 (페이지 118)
  - 구성 설정 다시 로드 (페이지 145)
  - 커널 테이블 표시 (페이지 134)
  - 커널 캐시 테이블 삭제, 활성화, 비활성화 (페이지 144)
- Windows 의 경우:
  - 계측 런타임 설정 제어 (페이지 146)
  - 런타임 통계 표시 (페이지 133)
  - ACEE 레코드 표시 (페이지 128)
  - 동시 로그인 옵션 관리 (페이지 122)
  - CA Access Control 추적 관리 (페이지 121)
  - 네트워크 리소스의 IP 주소 새로 고침 (페이지 145)
  - 재사용된 계정 확인 (페이지 130)
  - CA Access Control 종료 (페이지 128)
  - 사용자 이름 및 보안 자격 증명 표시 (페이지 149)

secons 유틸리티는 보안 관리자와 기타 사용자에서 모두 사용할 수 있지만, ADMIN 특성을 가지고 있지 않은 사용자는 일부 옵션만 사용할 수 있습니다. 이러한 옵션은 다음과 같습니다.

-m(추적 관리), -d-, -d+, -ds(로그인 관리) 및 -whoami(사용자의 자격 증명).

secons 유틸리티-UNIX 에서 CA Access Control 종료 관리

UNIX 에 해당

secons 유틸리티는 CA Access Control 및 관련 데몬을 종료합니다. 이 유틸리티를 사용하면 어떤 프로세스가 아직도 CA Access Control 코드를 실행 중인지 확인할 수 있습니다.

ADMIN 또는 OPERATOR 로 정의된 사용자만 CA Access Control 을 종료할 수 있습니다. 원격 컴퓨터에서 CA Access Control 을 종료하려면, 사용자는 해당 원격 컴퓨터에서 ADMIN 또는 OPERATOR 로 정의되어 있어야 합니다.

이 명령의 형식은 다음과 같습니다.

```
secons [-s [hosts | ghosts]] \
    [-S [{selogrd | selogrcd | serevu}]] \
    [-sc] [-scl] [-sk]
```

-s [hosts | ghosts]

공백으로 구분하여 정의된 원격 호스트 목록에서 CA Access Control 데몬을 종료합니다. 호스트를 지정하지 않으면 CA Access Control 이 로컬 호스트에서 종료됩니다.

ghost 레코드의 이름을 입력하여 호스트 그룹을 정의할 수 있습니다. 원격 터미널에서 이 옵션을 사용하면 유틸리티가 암호 확인을 요청합니다. 원격 컴퓨터와 로컬 컴퓨터에서 모두 관리자 권한이 필요할 뿐만 아니라 원격 호스트 데이터베이스에 로컬 컴퓨터에 대한 쓰기 권한이 있어야 합니다.

-S [{selogrd | selogrcd | serevu}]

사용자가 데몬을 정의하지 않은 경우, CA Access Control 데몬을 종료하고 활성 데몬 selogrd, selogrcd 및 serevu 를 종료하려고 시도합니다. seos.ini 파일의 [daemons] 섹션에 있는 selogrd, selogrcd 또는 serevu 토큰이 yes 로 설정되어 있는 경우, 실행 중인 CA Access Control 주 데몬으로 종료 요청을 전송하거나 CA Access Control 이 이미 종료된 경우 지정한 데몬으로 종료 신호를 전송합니다.

사용자가 데몬을 정의하면 secons 는 CA Access Control 데몬을 종료하지 않습니다. seos.ini 파일의 [daemons] 섹션에 있는 해당 토큰이 yes 로 설정되어 있으면, 실행 중인 CA Access Control 주 데몬으로 종료 요청을 전송하거나 CA Access Control 이 이미 종료된 경우 해당 데몬으로 종료 신호를 전송합니다.

-sc[l]

아직도 CA Access Control 코드를 실행 중인 프로세스를 표시합니다.

CA Access Control 의 최상위에 로드된 응용 프로그램에 CA Access Control 에 연결된 open 시스템 호출(syscall)이 있는 경우 CA Access Control 을 언로드할 수 없습니다. 어떤 프로세스가 아직도 CA Access Control 코드를 실행 중인지 알게 되면 해당 프로세스를 종료하고 CA Access Control 커널 모듈을 언로드할 수 있습니다. 커널을 언로드하기 전에 UNIX exit 를 사용하여 이러한 프로세스를 자동으로 종료한 다음, 커널이 언로드된 후에 이들을 다시 시작할 수 있습니다.

-sc 출력은 두 개의 열로 구성된 표를 표시하는데, 첫 번째 열에는 시스템 호출 번호가 있고 두 번째 열에는 프로세스 식별자가 있습니다.

-scl 옵션은 또한 아직도 CA Access Control 코드를 실행 중인 프로세스에 대한 PPID(Parent Process ID - 부모 프로세스 ID), UID, 시간 및 프로그램 이름 정보를 표시합니다. 시간 정보를 보면 CA Access Control 에 대한 프로세스의 후크(hook) 시간을 알 수 있습니다. 시간이 비교적 짧으면 후크가 일시적인 것일 수 있습니다.

또한 CA Access Control 이 실행 중인 동안에도 이를 실행하여 언로드 문제를 일으킬 수 있는 요인을 미리 예측할 수 있습니다. 그러나 경우에 따라(예: accept 명령) CA Access Control 코드는 언로드 중에 후크를 제거합니다. 이는 CA Access Control 실행 중에 보이는 활성 후크 중 일부는 실제로 언로드에 영향을 미치지 않음을 의미합니다.

참고: 기본적으로 CA Access Control 은 CA Access Control 에서 차단한 시스템 호출을 모니터링합니다. CA Access Control 이 시스템 호출을 모니터링하지 않도록 하려면 seos.ini 파일에서 syscall_monitor 토큰을 0(비활성)으로 설정해야 합니다.

-sk

CA Access Control 데몬을 모두 종료하고 언로드할 CA Access Control 커널 확장을 준비합니다.

예: CA Access Control 종료

- CA Access Control 데몬을 종료하려면 다음을 입력하십시오.

  ```
  secons -s
  ```

- 원격 호스트 HOST1 과 HOST2 에서 CA Access Control 데몬을 종료하려면 다음을 입력하십시오.

  ```
  secons -s HOST1 HOST2
  ```

예: 아직도 CA Access Control 코드를 실행 중인 프로세스에 대한 정보 표시

- 아직도 CA Access Control 코드를 실행 중인 프로세스에 대한 기본 정보를 표시하려면 다음을 입력하십시오.

  ```
  secons -sc
  ```

  수신하는 출력은 다음과 유사합니다.

  ```
  CA Access Control secons vX.X.X.xxx - Console utility
  Copyright (c) YYYY CA. All rights reserved.
  Active system calls:

  syscall   5 - PID:  27477
  ```

- 아직도 CA Access Control 코드를 실행 중인 프로세스에 대한 자세한 정보를 표시하려면 다음을 입력하십시오.

  ```
  secons -scl
  ```

  수신하는 출력은 다음과 유사합니다.

  ```
  CA Access Control secons vX.X.X.xxx - Console utility
  Copyright (c) YYYY CA. All rights reserved.
  Active system calls:

  -Syscall 102 - PID:  2105 PPID:    1 UID:    0 TIME:   4d-4h PROGRAM NAME:
  /usr/sbin/vsftpd
   Syscall   5 - PID: 24269 PPID:  4289 UID:    0 TIME:  2d-21h PROGRAM NAME:
  /bin/bash
  ```

  출력 줄 앞의 대시(-)는 CA Access Control 이 이 후크로 인해 언로드 문제가 발생할 가능성이 낮다고 평가한다는 것을 의미합니다. 이 명령을 사용할 때 CA Access Control 은 또한 CA Access Control 의 언로드가 성공할 가능성이 있는지 여부를 기록하는 감사 로그에 이 줄을 추가합니다. 예를 들어, 다음 감사 레코드는 secons -scl 을 실행하고 CA Access Control 의 언로드를 방해할 가능성이 있는 블로킹 시스템 호출이 하나 이상 있을 때 생성됩니다.

  ```
  10 Nov 2008 05:47:22 F CHECK      root      Scan     339  0 SEOS_syscall    unload
  ```

secons 유틸리티-CA Access Control 추적 관리

secons 유틸리티는 CA Access Control 추적을 관리합니다. 추적 기능을 사용하면 운영 체제 이벤트를 모니터링할 수 있습니다. CA Access Control 은 운영 체제 이벤트를 보고하는 메시지를 파일에 누적합니다. 나중에 이러한 메시지를 표시할 수 있습니다.

이 명령의 형식은 다음과 같습니다.

```
secons [-t+] [-t-] [-tt] [-ts] [-tc] [-tv [size] [-file fileName]]
```

```
secons -m message
```

-m message

추적 파일에 텍스트 메시지를 추가합니다.

-t+

추적을 활성화합니다. 그러면 CA Access Control 엔진(seosd)이 작업 및 동작을 지정하는 메시지를 추적 파일에 덤프합니다.

-t-

추적을 비활성화합니다. 그러면 CA Access Control 엔진(seosd)이 메시지를 추적 파일에 덤프하는 것이 중지됩니다.

-tc

추적 파일을 지우고 파일에서 모든 레코드를 제거합니다.

참고: seosd 의 실행 여부와 상관없이 이 옵션을 사용할 수 있습니다.

-ts

현재 추적 상태를 표시합니다.

-tt

추적 상태를 전환합니다.

-tv [size] [-file fileName]

실시간 추적 출력을 표시합니다. 유틸리티는 추적 파일의 최종 sizeKB(기본적으로 2KB)를 표시하고, 파일에 추가된 새 추적 메시지가 표시되도록 세션을 열어둡니다. 이는 UNIX tail -f 명령과 유사합니다.

이 작업을 중지하려면 Ctrl+C 를 사용하십시오.

참고: seosd 의 실행 여부와 상관없이 이 옵션을 사용할 수 있습니다. 연도를 네 개의 숫자(기본값, yes)로 표시할지 두 개의 숫자로 표시할지를 선택하려면 full_year 구성 설정을 사용하십시오.

size

표시할 파일의 부분에 대한 크기를 킬로바이트로 지정합니다(끝에서 시작). 전체 추적 파일을 표시하려면 0 을 지정하십시오. 이 옵션을 지정하지 않으면 기본값인 2KB 가 사용됩니다.

-file fileName

ACInstallDir/log/seosd.trace 대신 fileName 을 읽습니다.

secons 유틸리티-동시 로그인 옵션 관리

secons 유틸리티는 동시 로그인 옵션을 관리합니다. 한 사용자가 두 번 이상 로그인하지 못하도록 CA Access Control 을 구성할 수 있습니다. 이러한 기능을 통해 침입자는 이미 로그인되어 있는 사용자 계정에 로그인할 수 없습니다.

이 명령의 형식은 다음과 같습니다.

```
secons [-d+] [-d-] [-ds] [-l+] [-l-] [-ls] \
       [-u+ userName] [-u- userName] [-us userName]
```

-d+

명령을 실행하는 사용자의 동시 로그인을 활성화합니다.

-d-

명령을 실행하는 사용자의 동시 로그인을 비활성화합니다. 이 명령을 사용하면 로컬 컴퓨터에 대한 사용자의 모든 동시 로그인이 비활성화됩니다.

참고: 사용자의 .login 또는 .cshrc 파일에 이 명령을 추가하여 동시 로그인을 비활성화할 수도 있습니다.

-ds

명령을 실행하는 사용자의 동시 로그인 설정을 표시합니다.

-l+

시스템 전체에서 동시 로그인을 활성화합니다.

참고: 기본적으로 CA Access Control 은 로그인을 활성화하지만 유지 관리를 위해 시스템이 종료되는 경우 특정 기간에 대한 로그인을 비활성화할 수 있습니다.

-l-

시스템 전체에서 동시 로그인을 비활성화합니다.

-ls

시스템 전체의 로그인 상태를 표시합니다.

-u+ userName

정의한 사용자에 대한 동시 로그인을 활성화합니다.

-u- userName

정의한 사용자에 대한 동시 로그인을 비활성화합니다.

-us userName

정의한 사용자에 대한 동시 로그인 설정을 표시합니다.

secons 유틸리티-UNIX 에서 리소스 캐싱 관리

UNIX 에 해당

secons 유틸리티는 UNIX 에서 리소스 캐싱(파일 캐시)을 관리합니다. 캐시, 즉 런타임 테이블은 FILE 클래스에 있는 리소스의 권한 부여 요청에 대한 이전의 응답(승인 또는 거부)을 "기억"합니다. 동일한 권한 부여가 요청되면 캐시 메모리 테이블에 저장된 최근 응답을 통해 해당 요청에 대해 응답합니다.

이 명령의 형식은 다음과 같습니다.

```
secons [-C+] [-C-] [-CA value] [-CC interval] [-CD] \
    [-CF value] [-CI init_value] [-CP interval] -CU value]
```

-C+

파일 권한 부여 캐시를 활성화합니다.

-C-

파일 권한 부여 캐시를 비활성화합니다.

-CA value

테이블의 최대 권한 부여 레코드 수를 지정합니다.

기본값: 80

제한: 1 과 800 사이의 숫자

-CC interval

캐시 정리 간격(분)을 지정합니다.

기본값: 60

제한: 0 보다 큰 숫자

-CD

캐시 테이블을 표준 출력에 표시합니다.

-CF value

테이블의 최대 파일 레코드 수를 지정합니다.

기본값: 20

제한: 1 과 200 사이의 숫자

-CI init_value

캐시 테이블의 새 레코드에 대한 초기 우선 순위 값을 지정합니다.

기본값: 10

-CP interval

캐시 우선 순위 컴퓨팅 간격을 지정합니다.

기본값: 1(레코드 하나)

제한: 1 과 10 사이의 숫자

-CU value

테이블의 최대 사용자 레코드 수를 지정합니다.

기본값: 50

제한: 1 과 500 사이의 숫자

예: 캐시 설정 변경

다음 예는 캐시에 있는 파일, 사용자 및 권한 부여 레코드의 최대 수가 60 이 되도록 캐시 설정을 변경하는 방법을 보여줍니다.

```
secons -CF 60 -CU 60 -CA 60
```

예: 캐시 테이블 표시

다음 예는 secons -CD 명령의 출력을 보여줍니다.

```
==============================================================================
        FILE CACHE (configuration, statistics, and dispatcher data)
------------------------------------------------------------------------------
sizes(bytes)     tables:            | max records:     | intervals
cache  head     files   users   auth  | files users auths |clean prio
------------------------------------------------------------------------------
40244   44      5600    4200   30400 |  20   50   80   |  60  1
==============================================================================
table  |statistics      | priority   |min | rec  | average     |pri |init
name   |  hits misses (ok)| maxim  minim|ind | used | usage  life |fact|prio
------------------------------------------------------------------------------
files  |   5    1  83% |  0     0  |  0 |  1  |          |    |
users  |   5    1  83% | 10     2  |  0 |  1  |  0     0  |  1 | 10
auths  |   4    2  66% |  2        |  0 |  2  |          |    |
==============================================================================
FILE TABLE
------------------------------------------------------------------------------
No  type   pid priority user                        file name
------------------------------------------------------------------------------
0   EXPL   372     0    0                          /etc/shadow
==============================================================================
USER TABLE
------------------------------------------------------------------------------
No   user name    prio   life   used   UID  EUID  RUID auth prev(file)next
------------------------------------------------------------------------------
0    root         2      2      7    0    0    0    0   50(  0)  50
==============================================================================
AUTHORIZATION RESULT TABLE  (R - Result: 'P'-permit, 'D'-deny ...)
------------------------------------------------------------------------------
No  R ACEE acc  Log stage prv(usr)nxt time     terminal  program
------------------------------------------------------------------------------
0   P   6  read  0  00036 80(  0)  1   07:48:25         /usr/bin/login
==============================================================================
```

다음은 위의 출력에 대한 설명입니다.

출력은 5 개의 부분으로 구성됩니다.

- 캐시 구성. 다음 필드를 포함합니다.
  - 캐시 크기(바이트)
  - 캐시 헤더 크기(바이트)
  - 파일 표 크기(바이트)
  - 사용자 표 크기(바이트)
  - 결과 표 크기(바이트)
  - 최대 파일 레코드 수
  - 최대 사용자 레코드 수
  - 최대 결과 레코드 수
  - 통계: 표의 적중 횟수
- 파일 레코드 테이블. 다음 필드를 포함합니다.
  - 레코드 시퀀스 번호
  - 파일 유형(EXPLICIT, IMPLICIT)
  - 프로세스 ID 번호
  - 사용자 우선 순위의 합계인 레코드 우선 순위
  - 사용자 표의 해당 사용자 레코드 번호
  - 파일 이름
- 사용자 테이블. 다음 필드를 포함합니다.
  - 레코드 시퀀스 번호
  - 사용자 이름
  - 레코드 우선 순위
  - 레코드 수명 카운터
  - 레코드 사용 카운터
  - 사용자 ID 및 사용자 유효 ID(실제로 보안 ID 에서 사용됨)
  - 권한 부여 표의 해당 권한 부여 레코드 번호
  - 사용자 체인의 이전 사용자 레코드 번호
  - 해당 파일 레코드 번호
  - 사용자 체인의 다음 사용자 레코드

- 권한 부여 결과 테이블. 다음 필드를 포함합니다.
  - 터미널
  - 단계
  - 권한이 부여된 단계
  - 결과 - 권한 부여 결과(P 또는 D)
  - ACEE 번호
  - 액세스 유형
  - 로깅 옵션 플래그 값
  - 결정된 단계 번호
  - 레코드 체인의 이전 권한 부여 레코드 번호
- 해당 사용자 레코드 번호
  - 레코드 체인의 다음 권한 부여 레코드 번호
  - 통계: 표에서의 누락된 레코드 수
  - 권한 부여 클래스
  - 프로그램 이름(via 매개 변수 사용)
  - 알림 문자열
  - 업데이트 시간(GMT)
- 디스패처 데이터. 다음 필드를 포함합니다.
  - 통계: 표에서 누락된 레코드 수
  - 통계: 표의 적중 횟수
  - 표의 최대 우선 순위
  - 표의 최소 우선 순위
  - 최소 우선 순위를 가진 항목 수
  - 사용된 레코드 수
  - 평균 사용(사용자 표에 대해서만)
  - 평균 수명(사용자 표에 대해서만)
  - 우선 순위 계산 요소(사용자 표에 대해서만)
  - 레코드 우선 순위 초기 값(사용자 표에 대해서만)

secons 유틸리티-Windows 에서 CA Access Control 종료

Windows 에 해당

secons 유틸리티는 로컬 스테이션 또는 하나 이상의 원격 스테이션에서 CA Access Control 엔진 및 기타 모든 CA Access Control 서비스를 종료합니다.

ADMIN 또는 OPERATOR 로 정의된 사용자만 CA Access Control 을 종료할 수 있습니다. 원격 컴퓨터에서 CA Access Control 을 종료하려면, 사용자는 해당 원격 컴퓨터에서 ADMIN 또는 OPERATOR 로 정의되어 있어야 합니다.

이 명령의 형식은 다음과 같습니다.

```
secons -s [hosts | ghosts]
```

-s [hosts | ghosts]

공백으로 구분하여 정의된 원격 호스트에서 CA Access Control 서비스를 종료합니다. 호스트를 지정하지 않으면 CA Access Control 이 로컬 호스트에서 종료됩니다.

ghost 레코드의 이름을 입력하여 호스트 그룹을 정의할 수 있습니다. 원격 터미널에서 이 옵션을 사용하면 유틸리티가 암호 확인을 요청합니다. 원격 컴퓨터와 로컬 컴퓨터에서 모두 관리자 권한이 필요할 뿐만 아니라 원격 호스트 데이터베이스에 로컬 컴퓨터에 대한 쓰기 권한이 있어야 합니다.

secons -acee 함수 - Windows 에서 ACEE 레코드 표시

Windows 에 해당

secons 유틸리티를 사용하면 권한 부여 엔진에서 접근자를 캐시하는 ACEE(Accessor Element Entry) 테이블을 모니터링할 수 있습니다. ACEE 는 다음 사용자에 대한 정보를 저장합니다.

- **로그인한 사용자** - 운영 체제에 로그인한 사용자입니다. 이 사용자 유형의 특정 ACEE 특성은 다음과 같습니다.
  - 로그인 세션 ID
  - 로그인 세션 유형
- **관리 사용자** - LCA 연결을 사용하여 CA Access Control 관리 응용 프로그램에 로그인한 사용자입니다. (예: selang).
- **권한 부여 API 사용자** - SEOSROUTE_* API 에서 참조된 사용자입니다.

- **SPECIALPGM 논리적 사용자** - 적어도 하나의 SPECIALPGM 레코드에서 참조되고 있는 사용자입니다. 이 사용자 유형의 특정 ACEE 특성은 다음과 같습니다.
  - SPECIALPGM 레코드와의 ACEE 연관
- **기본 제공 사용자** - CA Access Control 에 기본적으로 포함된 사용자입니다. 예: _undefined

참고: CA Access Control 관리자만 이 명령을 사용할 수 있습니다.

이 명령의 형식은 다음과 같습니다.

```
secons -acee [handle | all | list]
```

all

모든 ACEE 레코드를 표시합니다.

handle

표시할 ACEE 핸들을 정의합니다.

list

모든 ACEE 레코드의 요약 목록을 표시합니다(자세한 전체 내용 없이).

예: ACEE 레코드 표시

- 다음 예는 ACEE 에 핸들 목록을 표시합니다.

  ```
  secons -acee list
  ```

  secons 는 다음과 유사합니다.

  ```
  ACEE handle '0' represents 'Logged on User': NT AUTHORITY\ANONYMOUS LOGON (OS User)
  ACEE handle '1' represents 'Logged on User': NT AUTHORITY\NETWORK SERVICE (OS User)
  ACEE handle '2' represents 'Logged on User': COMP1-SRV-X86\John
  ACEE handle '3' represents 'Logged on User': NT AUTHORITY\LOCAL SERVICE (OS User)
  ACEE handle '4' represents 'Logged on User': NT AUTHORITY\SYSTEM (OS User)
  ACEE handle '5' represents 'Management User': COMP1-SRV-X86\John
  ACEE handle '6' represents 'SPECIALPGM Logical User': logicaluser
  ```

- 다음 예는 ACEE 에 핸들 6 을 표시합니다.

  ```
  secons -acee 6
  ```

  secons 는 다음과 유사합니다.

  ```
  ACEE handle '6' represents 'SPECIALPGM Logical User': logicaluser
  ACEE was created at: Wed Feb 20 17:35:52 2008
  ACEE was last accessed at: Wed Feb 20 17:35:52 2008
  ACEE user role is: Regular
  ACEE audit mode is: Failure, Login Success, Login Failure; Originated from User
  definition
  ACEE user is a member of 0 'CA Access Control' groups
  ACEE user is associated with 1 SPECIALPGM records
     1. C:\WINDOWS\system32\calc.exe
  ```

secons -checkSID 함수-Windows 에서 재사용된 계정 확인

Windows 에 해당

secons 유틸리티는 각 엔터프라이즈 계정(XUSER 및 XGROUP 리소스)의 SID(Security IDentifier - 보안 식별자)를 기본 Windows 계정 SID 와 비교하고, 재사용된 계정의 백업을 작성합니다. CA Access Control 권한 부여는 SID 를 기반으로 하는데 CA Access Control 접근자 리소스의 SID 가 기본 계정 SID(재사용된 계정)와 다르므로, 유틸리티는 새 계정(이전 계정과 동일한 이름)을 만들고 SID (accountName) 명명 규칙을 사용하여 사용하지 않는 리소스를 백업합니다.

참고: 재사용된 엔터프라이즈 저장 계정에 대한 자세한 내용은 Windows 용 끝점 관리 안내서를 참조하십시오.

이 명령의 형식은 다음과 같습니다.

```
secons -checkSID {-groups | -users} [accountName [,accountName...]]
```

-groups

secons 가 엔터프라이즈 그룹 레코드를 검사하도록 지정합니다.

-users

secons 가 엔터프라이즈 사용자 레코드를 검사하도록 지정합니다.

accountName

secons 가 검색해야 할 사용자 또는 그룹 이름을 지정합니다. accountName 을 생략하면, secons 는 모든 그룹 또는 사용자를 검색합니다.

secons -i 함수-UNIX 에서 런타임 통계 표시

UNIX 에 해당

secons 유틸리티는 시스템 동작에 대한 CA Access Control 런타임 통계를 표시합니다. 네트워크 연결 요청, 감사 및 오류 로그 큐의 크기, 캐시된 테이블의 크기, 데이터베이스의 크기 및 데이터베이스 각 부분의 레코드 수를 알아보려면 이 정보를 사용하십시오.

이 명령의 형식은 다음과 같습니다.

```
secons -i
```

-i

런타임 통계를 서식 있는 텍스트로 표시합니다.

예: 런타임 데이터 표시

다음 예는 secons -i 명령의 출력을 보여줍니다.

```
Runtime Statistics:
        --------------------
        INet statistics:
            Requests denied  : 0
            Requests granted : 17
            Errors found     : 0
        Queues size:
            Audit log: 0
            Error log: 0
        Cached tables info:
            ACEE handles     :    11
            Protected clients :    0
            Trusted programs  :    77
            Untrusted programs:    3
        Database info: (Record count & first free ID)
            Classes    :   235 ( CID    0x00f0 )
            Properties :  4829 ( PID    0x1346 )
            Objects    :   842 ( OID 0x0000035a )
            PropVals   :  4109 ( N/A )
```

다음은 위의 출력에 있는 각 행을 설명한 것입니다.

```
INet statistics:
    Requests denied  : 0
    Requests granted : 17
    Errors found     : 0
```

CA Access Control 에서 수행한 네트워크 액세스 권한 부여의 통계를 표시합니다. 이러한 행은 네트워크 요청에 대해 권한을 부여하는 동안 거부, 승인 및 오류 수를 요약하여 보여줍니다.

```
Queues size:
    Audit log: 0
    Error log: 0
```

CA Access Control 은 파일 잠금 상태로 로깅을 작성하므로 특정 이벤트는 메모리에 보관되었다가 잠시 후 로그 파일에 기록될 수 있습니다. 이러한 값이 10 을 초과하면 오류가 CA Access Control 로깅 기능을 방해할 수 있습니다.

```
Cached tables info:
    ACEE handles     :    11
    Protected clients :    0
    Trusted programs  :    77
    Untrusted programs:    3
```

CA Access Control 이 사용하는 캐시된 테이블의 크기에 대한 정보를 표시합니다.

- ACEE(Accessor Element Entry)는 기록된 프로세스를 포함하는 표입니다.
- 보호된 클라이언트는 캐시된 클라이언트 수를 나열합니다. 일반적으로 이 값은 0 입니다.
- 트러스트된 프로그램은 메모리에 캐시된 PROGRAM 클래스의 항목 수를 나열합니다. 일반적으로 모든 프로그램은 트러스트된 것으로 캐시되어야 합니다.
- 언트러스트된 프로그램은 언트러스트된 상태의 프로그램 수를 표시합니다.

```
Database info: (Record count & first free ID)
    Classes    :   235 ( CID    0x00f0 )
    Properties :  4829 ( PID    0x1346 )
    Objects    :   842 ( OID 0x0000035a )
    PropVals   :  4109 ( N/A )
```

데이터베이스 크기에 대한 일반 정보와 데이터베이스의 각 부분에 있는 레코드 수입니다.

secons -i 함수-Windows 에서 런타임 통계 표시

Windows 에 해당

secons 유틸리티는 CA Access Control 런타임 통계 및 내부 카운터를 표시합니다. 다음을 알아보려면 이 통계 시스템 동작 정보를 사용하십시오.

- 각 차단 유형에 대해 트리거된 이벤트의 수
- 캐시에 저장된 이벤트의 수와 완전히 권한 부여된 이벤트의 수를 비교하여 얻은 각 커널 캐시의 효율성

참고: 작업량이 많을 때 감사 큐가 증가하는 것은 정상입니다. 하지만 작업 로드가 정상으로 돌아왔을 때 큐 크기는 감소해야 합니다.

이 명령의 형식은 다음과 같습니다.

```
secons -i [-reset]
```

-i

런타임 통계를 서식 있는 텍스트로 표시합니다.

-reset

(선택 사항) 런타임 카운터를 0 으로 재설정합니다.

예: 런타임 데이터 표시

다음은 secons -i 명령의 출력에서 자동으로 채워지지 않는 정보를 설명합니다.

데이터베이스 런타임 데이터

CA Access Control 데이터베이스에 있는 클래스, 개체, 속성의 수와 마지막으로 생성된 클래스, 개체, 속성의 ID, 그리고 속성 값의 수를 표시합니다.

이 정보를 사용하여 데이터베이스의 크기를 평가하십시오. 사용하는 개체 및 속성이 많을수록 데이터베이스의 크기가 커집니다.

커널 런타임 데이터

각 커널 캐시(파일, 레지스트리, 서로게이트)에 대한 작성 시간, 크기 및 효율성을 표시합니다. 효율성은 감사 이벤트 수와 총 이벤트 수의 비율입니다. 나머지 차단 이벤트는 권한 부여 프로세스를 따릅니다.

이 정보를 사용하여 각 커널 캐시의 수요 및 효율성을 평가하십시오.

커널 감사 정보

현재 커널 감사 큐 크기와 도달한 최대 크기 및 도달 시간을 표시합니다.

이 정보를 사용하여 감사 큐 동작을 평가하십시오. 감사 큐가 FsiDrv\MaxAuditRecordLimit CA Access Control 레지스트리 항목에 설정된 최대 큐 크기를 초과하지 않도록 해야 합니다. 이 제한 크기에 도달하면 큐의 항목이 소진되도록 CA Access Control 에서 감사 이벤트가 더 느리게 생성됩니다.

사용자 모드 적용 런타임 데이터

차단된 파일, 레지스트리, 로그온, 중지 및 Windows 서비스 이벤트를 전체 적용 모드에서 표시합니다. 권한 부여 엔진에 의해 권한 부여되는 이벤트 수와, 권한 부여 프로세스에서 각 클래스에 대해 소비한 최대 및 평균 시간을 볼 수 있습니다.

이 정보를 사용하여 실제 업무 시스템에서 발생하는 문제를 해결하십시오. 여기에는 CA Access Control 을 종료하지 않고도 얻을 수 있는 귀중한 최초 데이터가 포함되어 있습니다.

사용자 모드 감사 런타임 데이터

감사 이벤트에 대한 정보(캐시에 저장된 차단된 이벤트)를 표시합니다.

이 정보를 사용하여 사용자 모드 감사 큐 동작을 모니터링하십시오. 최대 감사 큐가 지속적으로 증가하는 경우 CA Access Control 이 감사 로그 파일에 기록할 수 있도록 하십시오. 시스템의 디스크 공간이 모자라거나 파일에 대한 기본 액세스 권한이 없는 경우 CA Access Control 이 파일에 기록하지 못할 수 있습니다.

참고: 작업량이 많을 때 감사 큐가 증가하는 것은 정상입니다. 하지만 작업 로드가 정상으로 돌아왔을 때 큐 크기는 감소해야 합니다.

secons -kt 함수 - UNIX 에서 커널 테이블 표시

UNIX 에 해당

secons 유틸리티는 커널 테이블을 표시합니다.

이 명령의 형식은 다음과 같습니다.

```
secons -kt tableNumber
```

-kt

지정된 커널 테이블을 표시합니다.

tableNumber

표시할 커널 테이블을 지정합니다. tableNumber 는 다음 값 중 하나여야 합니다.

1

SpecPgm 커널 테이블을 표시하도록 지정합니다.

2

TrustPg 커널 테이블을 표시하도록 지정합니다.

3

LoginPg 커널 테이블을 표시하도록 지정합니다.

4

DBfiles 커널 테이블을 표시하도록 지정합니다.

5

FRegExp 커널 테이블을 표시하도록 지정합니다.

6

DCMfile 커널 테이블을 표시하도록 지정합니다.

7

AC PID 커널 테이블을 표시하도록 지정합니다.

8

InoCach 커널 테이블을 표시하도록 지정합니다.

참고: Linux 에는 해당되지 않습니다.

9

F cache 커널 테이블을 표시하도록 지정합니다.

10

NetwDCM 커널 테이블을 표시하도록 지정합니다.

11

MntDirs 커널 테이블을 표시하도록 지정합니다.

12

F inode 커널 테이블을 표시하도록 지정합니다.

13

STOPbyp 커널 테이블을 표시하도록 지정합니다.

참고: STOP 이 활성화되지 않은 경우 이 커널 테이블을 표시할 수 없습니다.

14

STOPexp 커널 테이블을 표시하도록 지정합니다.

참고: STOP 이 활성화되지 않은 경우 이 커널 테이블을 표시할 수 없습니다.

15

Family 커널 테이블을 표시하도록 지정합니다.

16

DbgProt 커널 테이블을 표시하도록 지정합니다.

17

TCPport 커널 테이블을 표시하도록 지정합니다.

18

TCPoutp 커널 테이블을 표시하도록 지정합니다.

19

ProcSrv 커널 테이블을 표시하도록 지정합니다.

예: DBfiles 커널 테이블 표시

다음 예제는 DBfiles 커널 테이블을 표시할 때의 예제 출력을 보여 줍니다.

```
secons -kt 4
DBfiles
file    ID      i-node  device  program name
1       29      280391  356515  /opt/CA/AccessControl/seosdb/seos_ids.dat
2       3       0       0       /opt/CA/AccessControl/etc/privpgms.init
```

커널 테이블

커널 테이블은 CA Access Control 성능 향상을 돕기 위해 자주 액세스하는 정보를 나열합니다. 커널 테이블을 사용하면 커널 테이블에 나열된 이벤트의 허용, 거부, 확인 이벤트를 CA Access Control 이 검사할 필요가 없으므로 성능이 향상됩니다.

CA Access Control 에는 다음과 같은 유형의 커널 테이블이 포함되어 있습니다.

- 캐시 테이블 - 이전 리소스 액세스 요청, 확인된 inode 수, 허용된 들어오는 TCP 요청의 결과를 나열합니다.
- 보호된 리소스 테이블 - 액세스가 요청될 때 CA Access Control 이 CA Access Control 엔진으로 항상 권한 부여 요청을 보내는 대상 리소스를 나열합니다.

- 바이패스 테이블 - 액세스가 요청될 때 CA Access Control 이 CA Access Control 엔진으로 권한 부여 요청을 보내지 않고 액세스를 허용할 수 있는 대상 리소스를 나열합니다.
- 프로세스 테이블 - 시스템에서 실행되고 있는 모든 프로세스에 대한 정보를 나열합니다.

다음 테이블은 각 커널 테이블에 대한 정보를 제공합니다.

테이블 이름	유형	나열	열 이름	구성 설정
SpecPgm	보호된 리소스	SPECIALPGM 클래스에 있는 모든 개체	flags; user; oid; i-node; device; program	SPECIALPGM 클래스 레코드
TrustPg	보호된 리소스	PROGRAM 클래스에 있는 모든 개체	flags; i-node; device; program	PROGRAM 클래스 레코드
LoginPg	보호된 리소스	LOGINAPPL 클래스에 있는 모든 개체	flags; i-node; device; program name	LOGINAPPL 클래스 레코드
DBfiles	보호된 리소스	FILE 클래스에 있는 모든 개체	file ID; i-node; device; program	FILE 클래스 레코드 **참고:** 이 테이블의 최대 레코드 수는 seos.ini 파일의 SEOS_syscall 섹션에 있는 max_regular_file_rules 에 의해 정의됩니다.
FRegExp	보호된 리소스	FILE 클래스에 정의된 일반 파일 액세스 규칙	fid; expression	FILE 클래스 레코드의 일반 규칙에 의해 정의됩니다. **참고:** 이 테이블의 최대 레코드 수는 seos.ini 파일의 SEOS_syscall 섹션에 있는 max_general_file_rules 에 의해 정의됩니다.

테이블 이름	유형	나열	열 이름	구성 설정
DCMfile	바이패스	GAC 를 사용하여 정의하는 '호출 안 함' 파일	fid; user; type; access	GAC.init 파일
ACpids	바이패스	CA Access Control 데몬에 대한 프로세스 ID	pid; service; contractID	-
InoCach	캐시	캐시된 inode	i-node; device; priority; entry	seos.ini 파일의 SEOS_syscall 섹션에 있는 cache_enabled
F cache	캐시	캐시 파일 액세스 권한 부여 결과	file ID; access; acee; answer; phash; prio	-
NetwDCM	캐시	캐시된, 허용된 들어오는 TCP 연결	peer; port; local port; flag; prio	seos.ini 파일의 seosd 섹션에 있는 UseNetworkCache
MntDirs	보호된 리소스	마운트하지 못하도록 CA Access Control 이 보호하는 디렉터리	dir ID; i-node; device; mount point	-
F inode	보호된 리소스	FILE 클래스에 있는 개체의 Inode 및 장치 번호	file ID; i-node; device; links	-
STOPbyp	바이패스	CA Access Control 이 STOP 보호를 제공하지 않는 PROGRAM 클래스의 개체	i-node; device; program	STOP 이 활성화되면 이 테이블에 있는 개체에는 pgmtype(STOP) 속성의 SPECIALPGM 레코드가 있습니다.
STOPexp	바이패스	CA Access Control 이 STOP 보호를 제공하지 않는 PROGRAM 클래스에 있는	priority; n-chars; expression	STOP 이 활성화되면 이 테이블에 있는 개체는 pgmtype(STOP)

테이블 이름	유형	나열	열 이름	구성 설정
		개체를 정의하는 정규식입니다.		속성의 SPECIALPGM 레코드의 일반 규칙에 의해 정의됩니다.
Family	바이패스	CA Access Control 데몬	service; pid; contractID	-
DbgProt	보호된 리소스	디버깅하지 못하도록 CA Access Control 이 보호하는 CA Access Control 바이너리	pid; access; name in proc	-
TCPport	바이패스	seos_syscall 이 seosd 로 이벤트를 전달하지 않는 포트	TCP port	seos.ini 파일의 seosd 섹션에 있는 bypass_TCPIP
TCPoutp	바이패스	seos_syscall 이 seosd 로 나가는 연결 이벤트를 전달하지 않는 포트	TCP port	seos.ini 파일의 seosd 섹션에 있는 bypass_outgoing_TCPIP
ProcServ	프로세스	시스템에서 실행되고 있는 모든 프로세스는 대한 정보를 나열합니다.	#n; pid; ppid; acee; flags; uid; euid; zone; arg0; ACuser **참고:** 이 테이블에는 secons 유틸리티로 표시되지 않는 더 많은 내부 열이 있습니다.	-

커널 테이블 열 이름

다음 목록은 커널 테이블 열 이름을 설명합니다.

#n

커널 테이블에서 항목 번호입니다.

access

CA Access Control 이 허용하는 액세스 유형 또는 사용자가 요청한 액세스 유형을 정의합니다. 값은 액세스 유형의 합계입니다.

1-read
2-write
4-chown
8-chmod
16-rename
32-unlink
64-utimes
128-chattr
256-link
512-chdir
1024-create

acee

액세스 요청을 하는 사용자의 ACEE 를 정의합니다.

ACuser

사용자의 CA Access Control 사용자 이름을 정의합니다.

answer

액세스 요청에 대한 CA Access Control 의 응답(허용 또는 거부)를 정의합니다. 유효한 값:

0–거부

1–허용

arg0

프로그램이 실행될 때 인수 번호 0 에 정의된 대로 프로그램을 정의합니다.

contractID

(Solaris 10 에만 해당) 계약 프로세스 ID 를 정의합니다.

device

파일이 있는 논리 디스크를 정의합니다.

dir ID

디렉터리 ID 를 정의합니다.

entry

inode 의 문자열 값을 정의합니다.

euid

유효한 사용자 ID 를 정의합니다.

expression

항목이 적용되는 리소스를 지정하는 식(문자열 일치에 사용되는 텍스트 패턴)을 정의합니다.

fid 또는 file ID

CA Access Control 이 파일을 식별하기 위해 사용하는 파일 ID 를 정의합니다.

flags

항목에 대한 비트 마스크를 정의합니다.

i-node

inode 번호를 정의합니다.

links

파일의 하드 링크 번호를 정의합니다.

Local port

들어오는 TCP 연결을 허용하는 로컬 호스트의 포트를 정의합니다.

mount point

마운트하지 못하도록 보호할 디렉터리의 위치를 정의합니다.

n-chars

식에서 문자의 수를 정의합니다.

name in proc

/proc 파일 시스템의 프로세스 이름을 정의합니다.

참고: /proc 파일 시스템에서 각 프로세스는 파일로 나타나며 파일 이름은 프로세스 번호입니다.

oid

개체 ID 를 정의합니다.

peer

피어 호스트 주소를 정의합니다.

phash

경로 문자열의 해시 값을 정의합니다.

pid

프로세스 ID 를 정의합니다.

port

들어오는 TCP 연결이 시작된 포트를 정의합니다.

ppid

부모 프로세스 ID 를 정의합니다.

prio 또는 priority

커널 테이블에서 항목의 우선 순위를 정의합니다. 커널 테이블이 꽉 차면 CA Access Control 이 커널 테이블에 새 항목을 기록할 때 우선 순위가 낮은 항목이 제거됩니다.

program 또는 program name

프로그램의 이름을 정의합니다.

service

CA Access Control 서비스(데몬)의 이름을 정의합니다.

TCP port

항목이 적용되는 TCP 포트를 정의합니다.

type

보호되는 파일 유형을 정의합니다.

uid 또는 user

사용자 ID 를 정의합니다.

zone

(Solaris 10 에만 해당) 영역 ID 를 정의합니다.

참고: 이 열의 값은 Solaris 10 컴퓨터가 아닌 경우 항상 0 입니다.

캐시 테이블

커널 캐시 테이블에는 다음과 같은 세 가지 유형이 있습니다.

- **F cache** - 파일 캐시 테이블은 이전 권한 부여 요청의 결과를 캐시합니다.

  동일한 권한 부여 요청을 받으면 CA Access Control 은 이 파일 캐시 테이블에 저장된 마지막 응답을 사용하여 이 요청에 응답합니다.

  참고: 파일 캐시 테이블은 매 30 분마다, 그리고 CALENDAR, CONTAINER, FILE, GFILE, GROUP, HOLIDAY, PROGRAM, SECLABEL, SECLEVEL, SHIFT, USER 클래스에서 레코드가 변경될 때마다 삭제됩니다.

- **InoCach** - inode 캐시 테이블은 확인된 inode 번호를 캐시합니다.

  CA Access Control 이 inode 번호를 파일 이름으로 확인해야 하는 경우 파일 시스템을 확인하기 전기 InoCach 테이블을 먼저 확인합니다.

- **NetwDCM** - 이 네트워크 캐시 테이블은 허용된 들어오는 TCP 요청을 저장합니다.

  CA Access Control 이 네크워크 캐시에 있는 요청과 동일한 들어가는 TCP 요청을 받으면 CA Access Control 은 이 요청을 자동으로 허용합니다.

secons 유틸리티를 사용하여 커널 캐시 테이블을 표시하고, 삭제하고, 활성화하고, 비활성화할 수 있습니다.

보호된 리소스 테이블

CA Access Control 이 권한 부여 요청을 차단할 때는 액세스가 요청된 대상 리소스가 커널의 보호된 리소스 테이블에 나열되어 있는지 확인합니다.

리소스가 보호된 리소스 테이블에 나열되어 있으면 CA Access Control 은 항상 권한 부여 요청을 CA Access Control 엔진으로 보냅니다. 리소스가 보호된 리소스 테이블에 나열되어 있지 않으면 CA Access Control 은 권한 부여 요청을 엔진에 보내는 대신 커널에서 액세스 요청을 확인할 수 있습니다.

바이패스 테이블

CA Access Control 이 권한 부여 요청을 차단할 때는 액세스가 요청된 대상 리소스가 커널의 바이패스 테이블에 나열되어 있는지 확인합니다.

리소스가 바이패스 테이블에 나열되어 있는 경우 CA Access Control 은 해당 액세스 요청을 승인합니다. 리소스가 바이패스 테이블에 나열되어 있지 않은 경우 CA Access Control 은 추가적인 액세스 검사를 위해 이 요청을 CA Access Control 권한 부여 엔진으로 전달합니다.

secons -ktc 함수 - UNIX 에서 커널 캐시 테이블 삭제, 활성화, 비활성화

UNIX 에 해당

secons 유틸리티는 커널 캐시 테이블을 삭제, 활성화, 비활성화합니다.

이 명령의 형식은 다음과 같습니다.

```
secons -ktc optionNumber
```

-ktc

커널 캐시 테이블을 삭제. 활성화, 비활성화하도록 지정합니다.

optionNumber

수행할 작업을 지정합니다. optionNumber 는 다음 중 하나여야 합니다.

1

F cache 테이블을 삭제합니다.

2

F cache 테이블을 활성화합니다.

3

F cache 테이블을 비활성화합니다.

4

NetwDCM 테이블을 삭제합니다.

5

NetwDCM 테이블을 활성화합니다.

6

NetwDCM 테이블을 비활성화합니다.

7

F inode 테이블을 삭제합니다.

참고: Linux 에는 해당되지 않습니다.

8

F inode 테이블을 활성화합니다.

참고: Linux 에는 해당되지 않습니다.

9

F inode 테이블을 비활성화합니다.

참고: Linux 에는 해당되지 않습니다.

예: F cache 테이블 삭제

다음 예제는 F cache 테이블을 삭제합니다.

```
secons -ktc 1
```

secons -refIP 함수-네트워크 리소스의 IP 주소 새로 고침

Windows 에 해당

secons 유틸리티는 데이터베이스 네트워크 리소스의 IP 주소를 새로 고칩니다. 특정 호스트에서 새로 고침을 수행하려면 해당 호스트의 DNS 를 이미 새로 고친 상태여야 합니다. DNS 를 수동으로 새로 고치려면 다음 Windows 명령을 사용하십시오.

```
ipconfig /flushdns
```

이 명령의 형식은 다음과 같습니다.

```
secons -refIP [hosts]
```

-refIP [hosts]

(Windows 전용) CA Access Control 이 네트워크 리소스의 IP 주소를 새로 고칠 호스트의 목록을 쉼표로 구분하여 정의합니다. 호스트를 나열하지 않으면 로컬 네트워크 리소스를 새로 고칩니다.

이 옵션을 사용하면 CA Access Control 리소스를 현재 IP 주소로 업데이트할 수 있는데, 이는 IP 주소가 동적으로 할당되는 DHCP 환경에서 특히 유용합니다.

secons -rl 함수-UNIX 에서 구성 설정 다시 로드

UNIX 에 해당

secons 유틸리티는 seos.ini 파일을 다시 로드합니다. 이 기능을 이용하면 CA Access Control 을 종료하지 않고도 구성 설정을 업데이트할 수 있습니다.

이 명령의 형식은 다음과 같습니다.

```
secons -rl
```

-rl

(UNIX 전용) CA Access Control 을 종료하지 않은 채 seos.ini 구성 파일을 다시 로드하고 설정을 업데이트합니다.

secons -v 함수 - Windows 에서 계측 런타임 설정 제어

Windows 에 해당

secons 유틸리티는 CA Access Control 계측 런타임 설정을 제어합니다. 이 유틸리티를 사용하여 외부 DLL 라이브러리를 활성 프로세스로 로드하고 CA Access Control 계측 플러그인의 런타임 추적 구성을 수정할 수 있습니다. 이 명령을 실행하려면 ADMIN 또는 OPERATOR 특성이 있어야 합니다.

이 명령은 DLL 라이브러리를 로드하기 위해 다음 형식을 사용합니다.

```
secons -v target load "dll_name"
```

이 명령은 CA Access Control 계측 플러그인에서 추적을 활성화 또는 비활성화하기 위해 다음 형식을 사용합니다.

```
secons -v target trace plugin_name
{trace:enable|trace:disable}:{file:"tracefile_path"|debug}
```

참고: CA Access Control 은 추적이 올바로 구성될 때까지 추적을 시작하지 않습니다.

이 명령은 CA Access Control 계측 플러그인에서 추적을 구성하기 위해 다음 형식을 사용합니다.

```
secons -v target trace plugin_name trace:option:{sources:{1 | 4} | filtering:value
| filecyclic:{0 | 1} | filelimit:value }
```

debug

명령이 디버그 출력 채널에 대한 추적을 활성화 또는 비활성화하도록 지정합니다.

file:"tracefile_path"

CA Access Control 이 추적을 기록하는 파일에 대한 전체 경로를 정의합니다.

참고: trace:disable 매개 변수를 지정하는 경우 CA Access Control 은 파일 "tracefile_path" 매개 변수에 대해 지정하는 모든 값을 무시합니다.

filecyclic:{0 | 1}

순환 파일 추적을 사용할지 여부를 지정합니다. 순환 파일 추적을 활성화하는 경우 추적 파일의 크기가 지정된 최대 크기에 도달하면 CA Access Control 은 추적 파일의 처음으로 돌아가 추적을 계속 기록합니다.

이 매개 변수에는 다음과 같은 값이 있습니다.

0-순환 파일 추적 사용 안 함

1-순환 파일 추적 사용

filelimit:value

추적 파일의 최대 크기(바이트)를 정의합니다. 값 0 은 추적 파일에 최대 크기 제한이 없음을 의미합니다.

filtering:value

지정된 계측 플러그인에 대한 추적을 필터링하는 bitwise 필터 마스크를 정의합니다. CA Access Control 은 필터링된 이벤트를 추적 파일에 기록하지 않습니다.

참고: 필터링을 사용하지 않도록 지정하려면(즉, CA Access Control 이 모든 이벤트를 추적에 기록) 0xFFFFFFFF 값을 사용하십시오. 이 매개 변수의 다른 모든 값은 지정하는 플러그인에 따라 다릅니다.

load "dll_name"

지정된 DLL 을 대상 프로세스로 로드하도록 지정합니다. DLL 운영 환경 및 대상 프로세스 운영 환경은 동일해야 합니다. 예를 들어, 대상 프로세스로 32 비트 프로세스를 지정하는 경우 DLL 도 32 비트여야 합니다.

중요! DLL 은 ACInstallDir\bin 폴더에 있어야 합니다.

sources:{1 | 4}

CA Access Control 이 추적을 출력할 위치를 지정합니다.

이 매개 변수에는 다음과 같은 값이 있습니다.

1-파일에 출력

4-디버그 API 추적에 출력

target

대상 프로세스를 정의합니다. 이 매개 변수는 다음 값 중 하나를 갖습니다.

all_32bit

명령을 컴퓨터에서 실행 중인 모든 32 비트 프로세스로 보내도록 지정합니다.

all_64bit

명령을 컴퓨터에서 실행 중인 모든 64 비트 프로세스로 보내도록 지정합니다.

PID

대상 프로세스의 프로세스 ID 를 정의합니다. 대상 프로세스는 컴퓨터에서 실행되고 있어야 합니다.

process_name

대상 프로세스의 이름의 식별하는 마스크를 정의합니다. 대상 프로세스는 컴퓨터에서 실행되고 있어야 합니다. 예를 들어, 이 매개 변수에 대해 cmd.exe 를 지정하고 컴퓨터에서 3 개의 cmd.exe 인스턴스가 실행 중인 경우 CA Access Control 은 명령을 3 개 프로세스 모두에 적용합니다.

trace plugin_name

module_name 이란 이름의 CA Access Control 계측 플러그인(예: cainstrm 또는 stopplg)에 대한 런타임 추적 구성을 수정하도록 지정합니다.

참고: 플러그인의 DLL 이름을 지정해야 합니다. 계측 플러그인을 업그레이드하고 플러그인의 DLL 이름이 변경되는 경우 명령에 새 DLL 이름을 지정해야 합니다. 예를 들어, cainstrm 플러그인을 업그레이드하고 이 플러그인의 업그레이드된 DLL 이름이 cainstrm2.dll 인 경우 cainstrm2 를 plugin_name 으로 지정해야 합니다.

trace:disable

대상 플러그인에서 추적을 사용하도록 지정합니다.

trace:enable

대상 플러그인에서 추적을 사용하지 않도록 지정합니다.

참고: 이 매개 변수는 런타임에 추적 사용 플래그의 상태를 변경합니다. CA Access Control 은 추적이 올바로 구성될 때까지 추적을 시작하지 않습니다.

trace:option

대상 플러그인에서 추적을 구성하도록 지정합니다.

예: 디버그 출력 채널에서 추적 활성화

다음 명령은 컴퓨터에서 실행 중인 32 비트 프로세스에 있는 stopplg 플러그인의 모든 파일에 대해 추적 사용 플래그의 상태를 런타임에 변경합니다. CA Access Control 은 추적이 올바로 구성될 때까지 추적을 시작하지 않습니다.

```
secons -v all_32bit trace stopplg trace:enable:debug
```

예: 플러그인에 추적 필터링 마스크 적용

다음 명령은 PID 362 프로세스에 있는 cainstrm 플러그인의 모든 파일에 대해 추적 필터링 마스크를 적용합니다.

```
secons –v 362 trace "cainstrm trace:option:filtering:4294967295"
```

secons -whoami 함수 - 사용자 이름 및 보안 자격 증명 표시

Windows 에 해당

secons 유틸리티는 CA Access Control 권한 부여 엔진에 알려진 대로 사용자 이름을 표시합니다. 이것은 ACEE(Accessor Element Entry) 테이블에 저장된 정보입니다. ACEE 는 다음 사용자에 대한 정보를 저장합니다.

- **로그인한 사용자** - 운영 체제에 로그인한 사용자입니다. 이 사용자 유형의 특정 ACEE 특성은 다음과 같습니다.
  - 로그인 세션 ID
  - 로그인 세션 유형
- **관리 사용자** - LCA 연결을 사용하여 CA Access Control 관리 응용 프로그램에 로그인한 사용자입니다. (예: selang).
- **권한 부여 API 사용자** - SEOSROUTE_* API 에서 참조된 사용자입니다.
- **SPECIALPGM 논리적 사용자** - 적어도 하나의 SPECIALPGM 레코드에서 참조되고 있는 사용자입니다. 이 사용자 유형의 특정 ACEE 특성은 다음과 같습니다.
  - SPECIALPGM 레코드와의 ACEE 연관
- **기본 제공 사용자** - CA Access Control 에 기본적으로 포함된 사용자입니다. 예: _undefined

이 명령의 형식은 다음과 같습니다.

```
secons -whoami
```

예: 사용자 이름 및 보안 자격 증명 표시

다음 예는 CA Access Control 권한 부여 엔진에 알려진 대로 사용자 이름 및 보안 자격 증명을 표시합니다.

```
secons -whoami
```

secons 는 다음과 유사합니다.

```
ACEE handle '2' represents 'Logged on User': COMP1-SRV-X86\John
ACEE was created at: Wed Feb 20 17:34:47 2008
ACEE was last accessed at: Wed Feb 20 17:36:49 2008
ACEE user role is: Auditor, Administrator
ACEE audit mode is: Failure, Login Success, Login Failure; Originated from User definition
ACEE user is a member of 0 'CA Access Control' groups
ACEE's Logon session ID is: 0:68737
ACEE's Logon session type is: Interactive
```

추가 정보:

sewhoami 유틸리티 - UNIX 에서 CA Access Control 사용자 이름 및 보안 자격 증명 표시 (페이지 219)

secrepsw 유틸리티-정책 모델 및 섀도 파일 작성

UNIX 에 해당

secrepsw 유틸리티는 /etc/passwd 파일에 있는 모든 사용자에 대해 암호 레코드를 작성합니다. 이 유틸리티는 UNIX 환경에서 작동하는 PMDB 에 정의된 사용자를 관리하는 데 필요하며 섀도 파일을 작성 및 제거하기도 합니다.

참고: 이 유틸리티는 lbin 디렉터리에 있으며 루트 사용자만 사용할 수 있습니다. 이 유틸리티를 사용하기 전에 pmd.ini 파일에서 섀도 토큰을 yes 로 변경해야 합니다.

이 명령의 형식은 다음과 같습니다.

```
secrepsw [-h] [-c] [-r PolicyModel] [-s PolicyModel]
```

-c

로컬 컴퓨터에 있는 /etc/passwd 및 /etc/shadow 파일에서 새 정책 모델 암호 파일을 작성합니다.

-h

이 유틸리티에 대한 도움말을 표시합니다.

-r PolicyModel

정책 모델 섀도 파일의 사용자 이름과 암호를 다시 원래의 정책 모델 암호 파일(passwd)로 전송합니다.

-s PolicyModel

정책 모델 암호 파일(passwd)의 사용자 이름과 암호를 정책 모델 섀도 파일로 전송합니다.

sedbpchk 유틸리티-데이터베이스 백업

UNIX 에 해당

sedbpchk 유틸리티는 데이터베이스의 백업 복사본을 작성합니다. 또한 런타임 데이터베이스를 임시 위치에 복사하고, 임시 데이터베이스에서 다양한 데이터베이스 무결성 검사를 수행하며, 데이터베이스가 검사를 통과할 경우 임시 데이터베이스를 백업 위치로 복사합니다.

데이터베이스가 무결성 테스트를 통과하지 못하면 sedbpchk 는 복사본을 만드는 동안 업데이트가 데이터베이스에 적용되었는지 여부를 확인하려고 시도합니다. 업데이트가 있는 경우 데이터베이스가 손상되었다고 간주할 수는 없습니다.

데이터베이스를 복사하는 동안 어떤 업데이트도 없는 경우에는 데이터베이스가 손상되었을 가능성이 높습니다. 이런 경우 시스템 관리자에게 메일 메시지가 전송되어 시스템 관리자는 백업 디렉터리를 사용하여 손상된 런타임 데이터베이스를 다시 정의할 수 있습니다.

참고: 이 스크립트는 잘못된 정보를 제공할 수 있습니다. 데이터베이스가 손상되지 않은 경우에도 데이터베이스가 손상되었다고 결론을 내릴 수는 있습니다. 그러나 데이터베이스가 손상되지 않았다는 결론은 항상 맞습니다.

이 스크립트를 실행하려면 root 및 ADMIN 권한이 있어야 합니다. sedbpchk 를 사용하기 전에 ACInstallDir/lbin 에 있는 sedbpchk.sh 스크립트를 검토하여 다음 필드의 값이 사이트의 요구에 맞는지 확인하는 것이 좋습니다.

MAIL_TO

데이터베이스가 손상되었다는 통지를 보내는 사용자의 이름을 지정합니다.

RETRIES

데이터베이스의 손상이 의심스러운 경우 유틸리티가 통보를 보내기 전에 해당 데이터베이스를 검사하는 횟수를 지정합니다.

ACInstallDir

CA Access Control 설치 디렉터리의 위치를 지정합니다.

SE_BINDIR

CA Access Control 바이너리 파일 디렉터리의 위치를 지정합니다.

SE_DB_DIR

CA Access Control 런타임 데이터베이스 디렉터리의 위치를 지정합니다.

SE_BCKDIR

백업 데이터베이스 디렉터리의 위치를 지정합니다.

SE_TMPDIR

임시 데이터베이스 디렉터리의 위치를 지정합니다.

참고: 이 유틸리티는 스크립트 파일로 제공되며, 이를 실행하려면 .sh 확장자를 지정해야 합니다.

이 명령의 형식은 다음과 같습니다.

```
sedbpchk
```

seerrlog 유틸리티-오류 로그 레코드 표시

UNIX 에 해당

seerrlog 유틸리티는 CA Access Control 오류 로그에 레코드를 표시합니다. 사용자는 오류 로그 파일에 대한 읽기 권한이 있거나 오류 로그 파일을 읽을 수 있는 그룹(구성 설정 error_group 에 정의된 그룹)의 구성원이어야 합니다.

이 명령의 형식은 다음과 같습니다.

```
seerrlog [-h] [-s date] [-e date] [-d] [-f filename]
```

-s date

목록의 시작 날짜를 지정합니다. 정의된 날짜부터 기록된 레코드를 나열합니다.

제한: 날짜 형식은 dd-mm-yyyy 를 사용해야 합니다.

-e date

목록의 종료 날짜를 지정합니다. 정의된 날짜까지 작성된 레코드를 나열합니다.
제한: 날짜 형식은 dd-mm-yyyy 를 사용해야 합니다.

-d

오류에 대한 세부 정보를 인쇄하지 않도록 지정합니다.

-h

이 유틸리티에 대한 도움말을 표시합니다.

-f filename

읽을 오류 로그 파일을 지정합니다.

기본적으로 seerrlog 는 ACInstallDir/log/seos.error 파일을 읽습니다. 이 파일은 데이터베이스에서 정의할 수 없으며, 이 파일에 기록할 수 있는 것은 CA Access Control 뿐입니다.

예제

- 2006 년 1 월 3 일부터 기록된 모든 오류 레코드를 나열하려면 다음과 같이 지정하십시오.

  ```
  seerrlog -s 03-Jan-2006
  ```

- 2006 년 1 월 3 일과 2007 년 1 월 1 일 사이에 기록된 모든 오류 레코드를 나열하려면 다음과 같이 지정하십시오.

  ```
  seerrlog -s 03-Jan-2006 -e 01-Jan-2007
  ```

segrace 유틸리티-사용자 로그인 정보 표시

segrace 명령줄 유틸리티는 사용자에게 남은 유예 로그인 횟수, 사용자의 기존 암호가 만료되기까지 남은 일 수 또는 사용자가 마지막으로 로그온한 날짜, 시간 및 터미널을 표시합니다.

참고: 사용자의 유예 로그인 속성에 대한 자세한 내용은 해당 OS 에 대한 끝점 관리 안내서를 참조하십시오.

segrace 를 실행하려면 시스템 관리자는 먼저 다음 명령을 입력하여 CA Access Control 암호 검사를 활성화해야 합니다.

```
setoptions class+(PASSWORD)
```

지금부터 사용자 암호가 변경될 때마다 데이터베이스에 설정된 암호 품질 규칙을 기준으로 새 암호가 검사됩니다.

segrace 유틸리티-UNIX 에서 사용자 로그인 설정 표시

UNIX 에 해당

segrace 유틸리티는 사용자에 대한 로그인 설정을 표시합니다. 사용자가 로그인할 때마다 segrace 명령을 실행하는 것이 좋습니다. 이렇게 하려면 /etc/profile 및 /etc/csh.login(또는 Solaris 의 경우 /etc/.login)에 명령줄을 추가하십시오.

segrace 의 유예 로그인 수를 계산하려면 sepass 유틸리티를 사용하여 암호를 변경해야 합니다. 사용자에게 남은 유예 로그인이 없으면 segrace 는 사용자에게 암호 변경을 요구하는 sepass 유틸리티를 호출합니다. seos.ini 파일의 segrace 섹션에 있는 sepass_command 토큰에 다른 유틸리티를 지정하여 사이트에서 sepass 유틸리티 대신 실행할 명령을 결정할 수도 있습니다.

이 명령의 형식은 다음과 같습니다.

```
segrace [-h] [-d days] [-l] [-p] [userName]
```

-d days

사용자의 현재 암호가 만료되기까지 남은 일 수를 표시합니다. days 매개 변수에 지정한 일 수가 CA Access Control 옵션의 간격 값보다 크거나 같은 경우에만 일 수가 표시됩니다. days 매개 변수를 생략하면 segrace 는 기본값인 7 일을 사용합니다. 이 옵션은 sepass 를 사용하여 사용자 암호를 변경한 경우에만 적용됩니다.

-h

이 유틸리티에 대한 도움말을 표시합니다.

-l

사용자가 마지막으로 로그인한 날짜와 시간 및 해당 터미널을 표시합니다.

-p

사용자 암호가 만료될 때 새 암호를 입력하라는 메시지를 표시합니다.

userName

요청자에게 ADMIN 특성이 있는 경우 사용자 이름을 지정하면 segrace 는 지정한 사용자에 대한 필수 로그인 정보를 표시합니다.

사용자 이름을 지정하지 않을 경우, segrace 는 현재 사용자에 대한 로그인 세부사항을 표시합니다.

추가 정보:

sepass 유틸리티-암호 설정 또는 교체 (페이지 179)

segrace 유틸리티-Windows 에서 사용자 로그인 설정 표시

Windows 에 해당

segrace 유틸리티는 사용자에 대한 로그인 설정을 표시합니다. 이 유틸리티는 독립형 모듈로 원격 컴퓨터에서 실행될 수 있습니다.

참고: 매개 변수 없이 segrace 를 호출하는 경우 사용자에게 남은 유예 로그인이 없으면 segrace 에서 아무 것도 표시하지 않습니다.

이 명령의 형식은 다음과 같습니다.

```
segrace [-h] [-d days] [-l] [-p] [-s host] [userName]
```

-d days

warning days 매개 변수를 서버에 구성된 기본값과 다르게 설정합니다.

-h

이 유틸리티에 대한 도움말을 표시합니다.

-l

사용자가 마지막으로 로그인한 날짜와 시간 및 해당 터미널을 표시합니다.

-p

암호가 warning days 기간 내에 만료될 예정이거나 사용자에게 유예 로그인 수가 있는 경우 암호 경고에 대한 메시지가 나타납니다.

-s host

CA Access Control 데이터베이스를 사용할 원격 서버 이름을 지정합니다.

userName

사용자 이름이 지정되고 ADMIN 특성을 가진 경우 segrace 는 지정된 사용자에게 필요한 데이터를 표시합니다.

사용자 이름을 지정하지 않을 경우, segrace 는 현재 사용자에 대한 로그인 세부사항을 표시합니다.

segracex 유틸리티-UNIX 에서 암호 만료 검사

UNIX 에 해당

segracex 유틸리티는 X-Windows 환경에서 새 암호를 설정합니다. segracex 유틸리티는 사용자 암호의 만료 여부를 검사합니다. 암호가 만료된 경우 segracex 는 사용자가 암호를 변경할 수 있는 창을 표시합니다.

segracex 유틸리티는 사용자가 데스크톱 환경에 로그인한 후에 호출하는 사용자 초기화 스크립트에 연결되도록 설계되었습니다.

이 유틸리티는 사용자의 CA Access Control 유예 로그인 특성을 검사합니다. 사용자의 남은 유예 로그인 수가 다음과 같은 경우:

- 0 인 경우, segracex 는 사용자에게 강제로 암호를 변경하도록 합니다.
- 남은 유예 로그인 수가 양수이지만 사용자 또는 전역 유예 설정(있을 경우)의 유예 매개 변수(매개 변수가 하나인 경우)에 지정된 값보다 작은 경우, segracex 는 사용자에게 암호 변경을 권장합니다.
- 남은 유예 로그인 수가 사용자 또는 전역 유예 설정(있을 경우)의 유예 매개 변수에 지정된 값보다 크거나 같은 경우, segracex 는 어떤 작업도 수행하지 않습니다.

암호를 변경하면 segracex 는 사용자에게 이전 암호를 입력하라는 메시지를 표시합니다. 그런 다음 사용자에게 새 암호를 입력하라는 메시지가 나타납니다.

- CA Access Control 암호 검사가 활성화되면 segracex 는 새 암호가 데이터베이스에 설정된 암호 규칙을 따르는지 확인합니다. 새 암호가 등급 검사를 통과할 경우 사용자에게 새 암호를 입력하라는 메시지가 다시 나타납니다.
- 암호 검사가 비활성화된 경우 사용자에게 새 암호를 입력하라는 메시지가 다시 나타납니다.

  새 암호를 두 번 입력하면 첫 번째 입력한 암호와 두번째 입력한 암호가 비교됩니다. 두 개의 암호가 같지 않을 경우 새 암호를 묻는 메시지가 다시 나타납니다.

두 개의 새 암호가 일치할 경우 암호는 다음과 같은 방법으로 업데이트됩니다.

- 로컬 호스트 암호 파일(/etc/passwd 와 보안 파일) 및 로컬 데이터베이스가 업데이트됩니다.
- seos.ini 파일의 [seos] 섹션에 있는 passwd_pmd 또는 parent_pmd 토큰에 값이 정의되어 있으면 해당 PMDB 가 업데이트됩니다. 그 후에 PMDB 는 UNIX 환경과 데이터베이스에 있는 해당 구독자에게 이 업데이트를 전파합니다. seos.ini 파일의 [passwd] 섹션에서 nis_env 토큰에 nis 또는 nisplus 값이 입력된 경우 NIS 또는 NIS+ 서버가 업데이트됩니다. 암호가 마스터 NIS 서버에 설정되면 NIS 암호 맵이 자동으로 다시 구성됩니다.

색상 및 글꼴과 같은 사용자 정의 가능한 리소스는 segracex 파일에 있습니다. CA Access Control 의 표준 설치 중에 이 파일은 다음 디렉터리에 저장됩니다.

- Sun Solaris 를 제외한 모든 플랫폼:

  /usr/lib/X11/app-defaults

- Sun Solaris 플랫폼:

  /usr/lib/openwin/app-defaults

CA Access Control 상표가 있는 아이콘은 BigTradeMark_BW.xpm 파일에 있으며, 설치 후에 이 파일을 ACInstallDir/data/segracex 디렉터리에 저장해야 합니다.

이 명령의 형식은 다음과 같습니다.

```
segracex [-user userName]
```

userName

요청자가 ADMIN 특성을 가지고 있는 경우 사용자 이름을 지정하면 segracex 는 지정한 사용자에 대해 작업을 수행합니다.

사용자 이름을 지정하지 않으면 segracex 는 현재 사용자에 대해 작업을 수행합니다.

SegraceW 유틸리티-Windows 에서 암호 만료 검사

Windows 에 해당

이 Windows GUI grace 유틸리티는 사용자의 암호가 만료되었는지 여부 및/또는 사용자에게 유예 로그인 수가 있는지 여부를 확인합니다. 만료된 경우 SegraceW 는 사용자가 암호를 바꿀 수 있는 창을 표시합니다.

SegraceW 를 CA Access Control 환경이 아닌 다른 환경에서 독립형 모듈로 실행할 수 있습니다. 이렇게 하면 이 유틸리티를 도메인에 있는 임의의 워크스테이션에 적용할 수 있습니다.

SegraceW 는 먼저 주 도메인 컨트롤러(NT 4.0 환경)에 연결하려고 시도하며, 시도한 연결이 실패할 경우에만 백업 도메인 컨트롤러를 찾습니다. Windows 2000 버전 이상 환경에서 SegraceW 는 발견하는 첫 번째 도메인 컨트롤러에 연결을 시도합니다.

참고: SegraceW 실행 옵션에 원격 호스트가 명시적으로 지정되어 있으면 SegraceW 는 이 원격 호스트에만 연결합니다.

SegraceW 유틸리티는 도메인 컨트롤러의 NETLOGON 공유에 위치한 로그인 배치 파일로부터 호출되도록 설계되었습니다.

SegraceW 유틸리티는 사용자의 암호가 만료되었는지 여부 및/또는 사용자에게 유예 로그인 수가 있는지 여부를 확인합니다.

사용자의 유예 로그인 수 특성이 존재할 경우:

- 사용자의 남은 유예 로그인의 수가 0 이면 SegraceW 는 사용자에게 암호 변경을 강요합니다.
- 사용자의 남은 유예 로그인의 수가 양수이면 SegraceW 는 사용자에게 암호 변경을 권장합니다.

사용자에게 유예 로그인 수가 없을 경우 SegraceW 는 암호 만료 상태를 확인합니다.

- 서버에 구성된 warning days 매개 변수 값보다 큰 시간대에 암호가 만료될 경우, SegraceW 는 어떤 작업도 수행하지 않습니다.
- 서버에 구성된 warning days 매개 변수 값보다 작거나 같은 시간대에 암호가 만료될 경우, SegraceW 는 사용자에게 암호를 변경하도록 권장합니다.
- 암호가 만료된 경우 SegraceW 는 사용자에게 암호를 변경하도록 요구합니다.

암호를 변경할 때 SegraceW 는 사용자에게 기존 암호, 새 암호, 새 암호 확인을 입력하도록 요청하는 "암호 변경" 메시지를 표시합니다.

확인 검사를 통과하면 암호는 도메인 컨트롤러의 SAM 데이터베이스에서 업데이트됩니다.

이 명령의 형식은 다음과 같습니다.

```
segracew [-d] [-s remoteHost]
```

-d

warning days 매개 변수를 서버에서 구성된 기본값과 다르게 설정합니다.

-s remoteHost

정보 검색을 위해 지정한 원격 호스트에 연결합니다.

seini 유틸리티-구성 파일 관리

UNIX 에 해당

seini 유틸리티는 모든 호스트에 대한 CA Access Control 데이터베이스 및 초기화 파일을 관리합니다. 모든 호스트에 대해 seini 유틸리티는 다음 작업을 수행할 수 있습니다.

- CA Access Control 데이터베이스의 경로를 표시합니다.
- 초기화(.ini) 파일 경로 표시
- 초기화 파일의 토큰 내용 표시
- 초기화 파일의 특정 섹션에서 특정 토큰 값 설정
- 초기화 파일의 특정 섹션에서 특정 토큰 삭제

또한 seini 유틸리티는 다른 .ini 파일의 모든 토큰을 표시합니다. 초기화 파일 이름은 .ini 확장자로 끝나야 합니다. WRITE 및 ADMIN 권한을 가지고 있으면 원격 호스트에서 .ini 파일 관련 작업을 수행할 수 있습니다.

스위치를 지정하지 않은 경우 seini 는 데이터베이스 및 seos.ini 파일의 경로를 표시합니다.

참고: seosd 가 실행되고 있지 않거나 데이터베이스의 규칙에서 특별히 허용하는 경우에만 seini 유틸리티는 seos.ini 파일을 업데이트할 수 있습니다.

seini 는 seos.ini 파일에 특정 토큰을 포함하여 지능형 토큰 및 섹션 검색을 수행할 수 있습니다. 이 기능은 완전 일치 또는 부분 일치(오차 범위 25% 이내)를 찾을 때까지 각 토큰이나 섹션을 지정된 토큰이나 섹션과 비교하여 맞춤법 오류를 검사합니다. 관련 토큰 또는 섹션을 찾을 경우 seini 는 지정된 작업을 수행하고, 그렇지 않은 경우에는 오류 메시지를 표시합니다.

참고: 지능형 검색 기능은 seini 유틸리티를 호출하는 호스트에서만 작동합니다.

이 명령의 형식은 다음과 같습니다.

```
seini [-d] [host]

seini [-i] [host]

seini [-H host] \
    {[-f [host.]section.token [ini_file]] | \
    [-r [host.]section.token [ini_file]] | \
    [-s [host.]section.token value [ini_file]] | \
    [-sn [host.]section.token value [ini_file]]}
```

-d [host]

원격 호스트의 데이터베이스 경로를 표시합니다. 호스트를 지정하지 않은 경우 seini 는 로컬 호스트 경로를 표시합니다.

-f [host.]section.token [ini_file]

지정한 호스트의 지정한 환경 파일 섹션에 있는 토큰 값을 표시합니다. seini 가 지정한 섹션이나 토큰을 찾을 수 없으면 빈 행이 나타납니다. 호스트, 섹션 및 토큰 이름을 마침표(.)로 구분해야 합니다. ini_file 을 지정하지 않으면 CA Access Control 은 seos.ini 파일에서 섹션과 토큰을 검색합니다. 로컬 컴퓨터에 대한 정보를 표시하려면 host 매개 변수를 생략하십시오.

-g section

정의된 섹션에 토큰 목록을 표시합니다.

-h

이 유틸리티에 대한 도움말을 표시합니다.

-H [host]

-f, -r, -s 및 -sn 플래그와 함께 사용할 원격 호스트를 지정합니다.

-i [host]

초기화 파일 seos.ini 의 경로 이름을 표시합니다. 호스트를 지정하지 않은 경우 seini 는 로컬 호스트의 경로 이름을 표시합니다.

-r [host.]section.token [ini_file]

지정한 호스트의 환경 파일 섹션에서 토큰을 삭제합니다. ini_file 을 지정하지 않으면 CA Access Control 은 seos.ini 파일에서 토큰을 삭제합니다.

로컬 컴퓨터에 대한 정보를 삭제하려면 섹션과 토큰 이름만 지정하면 됩니다.

-s [host.]section.token value [ini_file]

지정한 호스트의 환경 파일 섹션에 있는 토큰 값을 설정합니다. ini_file 매개 변수를 지정하지 않으면 CA Access Control 은 seos.ini 파일에 값을 설정합니다. 원격 호스트를 지정한 경우 섹션이나 토큰이 없으면 CA Access Control 은 해당 섹션이나 토큰을 작성합니다.

로컬 컴퓨터에 섹션 또는 토큰을 작성하려면 -sn 스위치를 사용하십시오.

-sn [host.]section.token newValue [ini_file]

지정한 호스트의 환경 파일 섹션에 있는 토큰 값을 설정합니다. ini_file 매개 변수를 지정하지 않으면 CA Access Control 은 seos.ini 파일에 값을 설정합니다. 로컬 호스트를 지정한 경우 섹션이나 토큰이 없으면 CA Access Control 은 해당 섹션이나 토큰을 작성합니다.

원격 컴퓨터에 섹션 또는 토큰을 작성하려면 -s 스위치를 사용하십시오.

예: seini 사용

- seos.ini 초기화 파일이 로컬 컴퓨터의 어느 위치에 있는지 찾으려면 다음 명령을 사용합니다.

  ```
  seini -i
  ```

- [seosd] 섹션에서 trace 구성 설정의 값을 찾으려면 다음 명령을 사용합니다.

  ```
  seini -f seosd.trace_file
  ```

- [seosd] 섹션에서 trace_to 구성 설정의 값을 설정하려면 다음 명령을 사용합니다.

  ```
  seini -s seosd.trace_to file
  ```

  명령 출력은 다음과 같습니다.

  seosd.trace_to 토큰이 file(이전에는 file,stop)로 설정됩니다.

selang 유틸리티-CA Access Control 명령줄 실행

selang 유틸리티는 CA Access Control 데이터베이스 및 네이티브 환경에 대한 액세스를 제공하는 명령 셸을 호출합니다. 명령 셸 내에서 selang 명령을 작성함으로써 동적으로 데이터베이스가 업데이트됩니다.

참고: -o 옵션을 사용하지 않으면 명령 실행 결과는 표준 출력으로 전송됩니다.

UNIX 에서 이 명령의 형식은 다음과 같습니다.

```
selang [{-c command|-f file}] [{-d path|-p pmdb}] [-o file] [-r file] [-s] \
[-u user pass]
selang [-l] [-o file] [-r file] [-s] [-u user pass]
```

Windows 에서 이 명령의 형식은 다음과 같습니다.

```
selang [{-c command|-f file}] [{-d path|-p pmdb}] [-o file] [-r file] [-s] [-v]
selang [-l] [-o file] [-r file] [-s] [-v]
```

-c command

실행할 selang 명령을 지정합니다. selang 은 명령을 실행한 후 종료됩니다.

command 에 공백이 포함되어 있으면 전체 문자열 앞뒤에 따옴표를 입력하십시오. 예:

```
selang -c "showusr rosa"
```

-d path

selang 명령이 정의된 경로에서 데이터베이스를 업데이트하도록 지정합니다.

참고: 로컬 데이터베이스만 지정할 수 있습니다.

-f file

터미널의 표준 입력이 아닌 정의된 파일로부터 selang 명령을 읽도록 지정합니다.

selang 은 입력 파일의 명령을 실행하므로 실행 중인 명령의 행 수가 화면에 나타납니다. selang 프롬프트는 화면에 나타나지 않습니다. selang 은 file 에서 명령을 실행한 후 종료됩니다.

-h

이 유틸리티에 대한 도움말을 표시합니다.

-l

selang 이 기본 로컬 데이터베이스를 업데이트하도록 지정합니다. 이 데이터베이스는 대개 ACInstallDir/seosdb 이며, 여기서 ACInstallDir 은 CA Access Control 이 설치된 디렉터리입니다.

이 옵션을 -d 또는 -p 와 함께 지정할 필요는 없습니다.

참고: 이 옵션은 selang 을 대체합니다. 이 옵션은 seosd 가 실행되고 있지 않을 경우에만 유효하며 슈퍼 사용자만 실행할 수 있습니다.

-o file

selang 출력이 지정한 파일에 기록되도록 지정합니다. selang 을 호출할 때마다 새로운 빈 파일이 생성됩니다. 기존 파일의 이름을 지정하면 selang 은 파일에 있는 현재 정보를 덮어씁니다.

-p pmdb

selang 명령이 정의된 PMDB 의 데이터베이스를 업데이트하도록 지정합니다. 이 데이터베이스는 로컬 스테이션, 즉 PMDB 하위 디렉터리에 있습니다. 데이터베이스에 대한 변경 사항은 구독자에게 전파되지 않습니다.

참고: 이 옵션은 sepmdd 또는 seosd 가 지정된 PMDB 에서 실행되고 있으면 유효하지 않으며, hosts 명령을 사용하는 것과는 다릅니다.

중요! 이 모드에서 전파가 필요한 사항은 변경하지 마십시오. 업데이트 시 기본 모드를 사용하면 CA Access Control 은 기본 호스트 파일만 업데이트합니다(CA Access Control 구성 옵션에 정의되어 있는 대로).

-r file

selang 이 정의된 파일에서 명령을 읽도록 지정합니다. 파일은 세미콜론 또는 줄 바꾸기 문자로 구분된 일반 selang 구문의 명령으로 구성되어야 합니다. selang 은 file 의 명령을 실행한 후 사용자에게 입력하라는 메시지를 표시합니다.

이 옵션에서 파일이 정의되어 있지 않으면 selang 은 홈 디렉터리의 .selangrc 파일을 사용합니다.

-s

selang 이 저작권 메시지를 표시하지 않은 채 자동 모드에서 열리도록 지정합니다.

-u user pass

(UNIX 전용) selang 을 실행하기 위한 사용자 이름과 암호를 지정합니다.

이 옵션을 사용하려면 seos.ini 파일에서 check_password 토큰을 yes 로 설정해야 합니다. 그러면 selang -u 를 실행할 때 CA Access Control 에서 "암호를 입력하십시오."라는 메시지가 표시됩니다. 로그인은 세 번 시도할 수 있습니다.

seos.ini 파일의 [lang] 섹션에 있는 no_check_password_users 토큰에는 로그인 중 selang 에 대한 암호 검사를 바이패스하는 사용자 목록이 있습니다.

참고: check_password 토큰이 no 로 설정되어 있는 경우 selang 은 암호를 요구하지 않습니다.

-v

(Windows 전용) 출력할 명령줄을 작성합니다.

참고:

- -h 를 사용하면 모든 다른 옵션은 무시됩니다.
- -c 옵션은 -f 옵션과 함께 사용할 수 없습니다.
- -d 옵션은 -p 옵션과 함께 사용할 수 없습니다.
- -d 나 -p 를 지정하는 경우에는 -l 을 지정할 필요가 없습니다.

seldapcred 유틸리티-자격 증명 암호화 및 저장

UNIX 에 해당

seldapcred 유틸리티는 사용자가 제공하는 자격 증명을 암호화 및 저장합니다. 이 자격 증명은 LDAP 설정 CA Access Control 유틸리티(예: sebuildla)가 LDAP DIT(Directory Information Tree - 디렉터리 정보 트리)의 데이터를 검색하는 데 사용합니다. seos.ini 파일의 [seos] 섹션에 있는 ldap_userdn 토큰의 값과 함께 사용하면 유틸리티가 LDAP 서비스에 대해 인증을 받을 수 있습니다. 단순한 인증의 경우, 자격 증명은 ldap_userdn 값에 해당하는 암호입니다. SASL 인증의 경우, 자격 증명은 다른 의미 체계를 갖습니다.

seldapcred 유틸리티는 암호화된 자격 증명을 ACInstallDir/etc/ldapcred.dat 에 기록합니다.

이 명령의 형식은 다음과 같습니다.

```
seldapcred [-h] [-w [credential]]
```

-h

이 유틸리티에 대한 도움말을 표시합니다.

-w [credential]

seldapcred 에서 암호화 및 저장하도록 할 자격 증명을 지정합니다. seldapcred 유틸리티에 입력을 제공하지 않으면 이 값을 입력하라는 메시지가 표시됩니다. 이런 방식으로 대화형 모드를 사용하면 자격 증명이 다른 사용자에게 노출되는 것을 막을 수 있습니다.

추가 정보:

sebuildla 유틸리티-Lookaside 데이터베이스 작성 (페이지 102)

seload 유틸리티-CA Access Control 로드 및 시작

UNIX 에 해당

seload 유틸리티는 UNIX 커널에 대한 CA Access Control 확장을 로드하고 CA Access Control 데몬을 시작합니다. seload 유틸리티는 CA Access Control 데몬을 로컬과 원격으로 로드합니다. 또한 UNIX 커널에 대한 CA Access Control 확장이 지정한 호스트에 로드되어 있는지를 확인합니다. seosd 가 실행되고 있지 않으면 seload 는 지정한 호스트에서 데몬을 시작합니다. -r 스위치와 매개 변수를 생략하면 seosd 데몬은 로컬 호스트에서 실행됩니다.

seload 에 seosd, selogrd, selogrcd 또는 serevu 데몬 중 하나를 원격 호스트에서 로드하도록 지시할 수 있습니다. 이 프로세스는 토큰에 따라 달라집니다.

CA Access Control 이 서버 스테이션의 부트 시퀀스에 있으면 seload 를 사용하십시오.

참고:

- CA Access Control 이 설치되어 있으면 CA Access Control 에서 지원하는 모든 운영 체제의 샘플 초기화 파일은 ACInstallDir/samples/system.init 디렉터리에 있습니다. CA Access Control 을 시스템 초기화 중에 시작하려면 이러한 파일을 사용하십시오.
- seload 유틸리티를 실행하려면 se_loadtest 실행 파일이 ACInstallDir/lbin 에 있어야 합니다. 여기서 ACInstallDir 은 설치 디렉터리입니다. 이 프로그램은 UNIX 커널에 대한 CA Access Control 확장이 로드되어 있는지를 확인합니다.
- 원격으로 작업할 때 seload 유틸리티는 다음 조건에 해당되어야 합니다.
  - rseloadd 실행 파일은 CA Access Control dir/lbin 에 있습니다. 이 프로그램은 원격 호스트에서 실행되고 seload 를 활성화합니다.
  - /etc/services 파일에 seosload 서비스가 포함되어 있어야 합니다. CA Access Control 설치 중에 이 파일을 추가해야 합니다.
  - /etc/inetd.conf 파일에 rseloadd 프로그램이 포함되어 있어야 합니다. CA Access Control 설치 중에 이 프로그램을 추가할 수 있습니다.

이 명령의 형식은 다음과 같습니다.

```
seload [-c] [-nopmd] [-r host [daemon]]
```

-c

sechkey -r 명령을 사용하여 설정된 암호화 키를 변경합니다.

-nopmd

-nopmd 스위치와 함께 -c 스위치를 지정하면 seload 는 새 키를 사용하여 정책 모델 업데이트 파일을 업데이트하지 않습니다.

-r host [daemon]

seosd 데몬과 seos.ini 파일의 [daemons] 섹션에 지정된 다른 모든 데몬을 로드합니다.

daemon 을 지정하면 seload 는 seos.ini 토큰을 무시하고 해당 데몬만 시작합니다. 데몬의 전체 경로를 제공해야 합니다.

[daemons] 섹션의 seos.ini 토큰은 값을 지정하는 경우에만 사용됩니다. 이 토큰에는 기본값이 없습니다. 값을 지정할 경우 seload 는 지정된 유틸리티 또는 프로그램의 표준 값을 토큰에 있는 값으로 대체합니다. 예를 들어, selogrd 값을 yes 로 지정할 경우 seload 는 seosd 데몬을 시작한 후 자동으로 selogrd 데몬을 시작합니다.

selock 유틸리티-X 터미널 화면 잠금

UNIX 에 해당

selock 유틸리티는 일정 시간 동안 컴퓨터를 사용하지 않을 때 X 터미널 또는 스테이션을 항상 보호합니다. selock 은 다음과 같은 세 가지 작업 모드를 지원합니다.

- 모니터 모드
- 절전 모드
- 잠금 모드

selock 의 기본 설정은 저장 및 잠금 모드의 결합입니다.

참고: selock 을 사용하여 유휴 상태 스테이션을 잠그는 방법에 대한 자세한 내용은 UNIX 용 끝점 관리 안내서를 참조하십시오.

이 명령의 형식은 다음과 같습니다.

```
selock [-delay period] [-display hostname:display#.screen#] [-fodelay factor] \
    [-folevels levels] [-idelay seconds] [-lock-timeout minutes] \
    [-pixmapFile fileName] [-pw-timeout seconds]
```

-delay period

시스템 아이콘이 화면에서 사라져 다른 위치로 이동하기까지 화면의 한 위치에 나타나는 시간을 지정합니다. 이것은 표준 화면 보호기 활동으로, 화면이 타는 것을 방지합니다. 시간은 밀리초 단위로 입력됩니다.

이 기간을 정의하지 않으면 기본값인 5000000(5 백만)이 사용됩니다.

-display hostname:display#.screen#

잠글 화면 표시 모니터를 지정합니다. 디스플레이 및 화면 개수는 시스템의 X-session 목록에서 찾을 수 있습니다. 여기에 정의된 대체 디스플레이 모니터를 현재 실행하고 있는 사용자로부터 권한을 받아야 합니다.

이 옵션을 정의하지 않으면 유틸리티가 디스플레이를 잠급니다.

-fodelay factor

각 페이드 아웃 수준이 화면에 표시되는 시간을 수정합니다. 이를 통해 사용자는 수준 수를 늘리지 않고도 각 단계에 걸리는 시간을 연장할 수 있습니다. 기본값은 10 입니다.

-folevels levels

시스템 아이콘의 페이드 아웃(fade-out) 단계 수를 지정합니다. 페이드 아웃 수준 수를 증가시키면 천천히 사라지지만 아이콘이 페이드 아웃되려면 더 오랜 시간이 걸립니다. 기본적으로 유틸리티는 20 개의 페이드 아웃 단계를 사용합니다.

-help

다양한 selock 옵션을 설명하는 도움말 화면을 표시합니다.

-idelay seconds

로그인한 후 모니터링이 시작되기까지 경과되는 시간(초)을 지정합니다. selock 이 .login 셸에 포함되어 있으면 사용자가 처음 로그인한 후 시스템이 구성되기까지 이러한 지연 시간이 필요합니다. 기본값은 30 초입니다.

-lock-timeout minutes

transparent=off 이면 selock 이 잠금 모드로 변경하기까지 절전 모드를 유지하는 시간(분)을 지정합니다.

transparent 가 on 으로 설정된 경우, 잠금 모드로 변경되기 전에 selock 이 모니터 모드에서 보내는 시간(분)을 지정합니다.

기본값 0 은 절전 모드를 바이패스하고 바로 잠금 모드를 실행합니다.

-pixmapFile fileName

transparent=on 인 경우 화면이 잠길 때 selock 이 배경에 표시하는 XPM 파일을 지정합니다.

-pw-timeout seconds

암호 대화 상자가 화면에 표시되는 시간을 지정합니다. 기본값은 30 초입니다. 너무 큰 숫자를 입력하면 X-server 에 문제가 발생할 수 있으므로 주의하십시오. 지정한 기간 내에 암호가 올바로 입력되지 않으면 암호 입력 대화 상자가 닫히고 selock 은 잠금 모드를 유지합니다.

-segrace {on|off}

selock 이 사용자와 암호를 식별한 후 segracex 를 호출하도록 지정합니다. 그러나 사용자 ID 와 암호가 unlocking_user 토큰(seos.ini 의 [selock] 섹션에 있음)에 이름이 나타나는 사용자에게 속하는 경우 selock 은 segrace 를 호출하지 않습니다. 기본값은 off 입니다.

참고: segracex 유틸리티는 사용자의 암호 만료 여부를 확인합니다. 암호가 만료된 경우에는 사용자가 새 암호를 선택할 수 있는 대화 상자가 나타납니다. 자세한 내용은 "segrace 유틸리티-UNIX 에서 사용자 로그인 설정 표시"를 참조하십시오.

-timeout minutes

selock 이 모니터 모드에서 절전 모드로 전환하기까지의 사용자 비활성 기간을 지정합니다. 기본값은 10 분입니다.

-transparent {on|off}

selock 이 잠금 모드에 있을 때 화면 내용을 그대로 표시할지 여부를 지정합니다. on 을 지정하면 진행 중인 프로세스의 화면 표시와 업데이트가 계속됩니다. 화면이 잠겼음을 나타내기 위해 selock 은 -pixmapFile 옵션으로 지정된 파일 내용을 표시하여 배경을 변경합니다. 기본값은 off 입니다.

-user user-name

잠금 모드에서 사용자 활동이 탐지될 때 암호 대화 상자에 암호를 입력하도록 요구되는 사용자를 지정합니다. 기본값은 현재 사용자 이름입니다. 사용자 옵션에서 지정한 사용자에 상관없이 root 의 암호가 사용됩니다.

-workhours (hh:mm-hh:mm)

사용자가 화면 잠금을 해제할 수 있는 기간을 지정합니다. 지정된 기간 전후에는 키보드나 마우스를 사용하더라도 "암호" 대화 상자가 나타나지 않습니다.

기본값은 00:00-24:00 이므로, 사용자는 항상 화면 잠금을 해제할 수 있습니다.

-xmin pixels

시스템 아이콘이 움직일 때마다 가로로 이동하는 최소 거리(픽셀)를 지정합니다. 기본값은 100 입니다.

-xmax pixels

시스템 아이콘이 움직일 때마다 가로로 이동하는 최대 거리(픽셀)를 지정합니다. 기본값은 300 입니다.

-ymin pixels

시스템 아이콘이 움직일 때마다 세로로 이동하는 최소 거리(픽셀)를 지정합니다. 기본값은 80 입니다.

-ymax pixels

시스템 아이콘이 움직일 때마다 세로로 이동하는 최대 거리(픽셀)를 지정합니다. 기본값은 250 입니다.

추가 정보:

segrace 유틸리티-UNIX 에서 사용자 로그인 설정 표시 (페이지 154)

selockcom 유틸리티-selock 유틸리티 제어

UNIX 에 해당

selockcom 유틸리티는 현재의 활성 selock 프로세스를 제어합니다. 잠금, 저장 및 모니터 모드 간의 전환뿐만 아니라 selock 다시 시작 및 중지 기능이 있습니다.

참고: selock 이 로드되면 selock 과 기본 화면 보호기 간의 경쟁 또는 중복 상태를 방지하기 위해 터미널의 기본 화면 보호기가 비활성화됩니다. selockcom exit 스위치를 사용하여 selock 을 중지하면 터미널에서 어떤 화면 보호기도 활성화되지 않습니다. 표준 X 명령인 xset s on 을 사용하여 selock 또는 터미널의 기본 화면 보호기를 다시 시작할 수 있습니다. xset 명령에 대한 자세한 내용은 UNIX 설명서를 참조하십시오.

이 명령의 형식은 다음과 같습니다.

```
selockcom {-activate|-deactivate|-exit|-restart|-lock} \
    [-display hostname:display#.screen#]
```

-activate

미리 정의된 시간 초과 기간이 경과될 때까지 기다리지 않고 selock 을 모니터 모드에서 절전 모드로 전환합니다. 키보드가 잠기고 화면에 CA Access Control 로고가 나타납니다.

-deactivate

selock 을 다시 모니터 모드로 전환합니다. 이 스위치는 selock 프로세스에 대한 사용자 입력을 시뮬레이트합니다. 현재 selock 이 잠금 모드에 있으면 암호 대화 상자가 나타납니다. 모니터 모드로 돌아가려면 암호를 입력합니다. selock 이 절전 모드에 있으면 모니터 모드로 돌아갑니다.

-exit

selock 프로세스를 종료합니다. 또한 sigterm 신호를 보내 selock 을 종료할 수도 있습니다. 마지막 방법으로 sigkill 신호(kill -9)를 사용할 수도 있습니다. 이 방법을 사용할 경우 selock 은 완전하게 종료되지 않으므로 일반적으로 사용하지 마십시오. 가상 루트 창 관리자를 실행하는 경우 kill -9 를 사용하여 창 관리자를 강제로 다시 시작하여 가상 창을 복원할 수 있습니다.

-restart

selock 프로세스를 종료한 후 이전 호출과 동일한 명령 라인 옵션을 사용하여 즉시 다시 시작합니다. 이것은 selock 을 마지막으로 호출한 이후 데이터베이스가 변경된 경우 리소스 데이터베이스를 다시 읽어들이는 데 적합한 방법입니다.

-lock

현재의 lock-timeout 값에 관계없이 selock 을 잠금 모드로 전환합니다.

-display hostname:display#.screen#

지정한 화면 표시에서 작동하는 selock 프로세스를 제어하도록 selockcom 에 지시합니다. 이 옵션을 사용하면 원격 터미널에서도 selock 을 제어할 수 있습니다.

시스템의 X-session 목록에 있는 디스플레이 및 화면 번호를 찾을 수 있습니다. 이렇게 하려면 지정된 디스플레이 모니터를 현재 실행 중인 사용자로부터 권한을 받아야 합니다. 사용자의 디스플레이를 잠그려고 한다는 것을 기본적으로 가정합니다.

selogmix 유틸리티-감사 로그 파일의 분할 및 병합

UNIX 에 해당

selogmix 유틸리티는 CA Access Control 감사 로그 파일을 분할 및 병합합니다.

이 명령의 형식은 다음과 같습니다.

```
selogmix {-s|-m} [-fn fileName] [-l fileName1 fileName2] \
    [-c weight1:weight2] [-t days] [-d] [-i]
```

-c weight1:weight2

파일 분할 시 파일 크기의 상관 관계를 지정합니다. 여기서 weight1 은 첫 번째 파일의 상대적 가중치를 나타내고 weight2 는 두 번째 파일의 상대적 가중치를 나타냅니다. 이 옵션을 생략하면 selogmix 는 1 대 1 상관 관계를 사용합니다.

-d

selogmix 를 디버그 모드로 실행하도록 지정합니다. 이 모드에서 selogmix 는 모든 설정을 표시합니다.

-fn fileName

분할할 감사 로그 파일의 이름과 병합 후 생성되는 파일 이름을 지정합니다. 이 옵션을 생략할 경우 selogmix 는 seos.ini 파일의 [logmgr] 섹션에 있는 audit_log 토큰에서 지정된 파일 이름을 사용합니다.

-h

이 유틸리티에 대한 도움말을 표시합니다.

-i

selogmix 를 대화식 모드로 실행하도록 지정합니다. 이 모드에서 selogmix 는 기존 파일을 덮어쓰기 전에 확인 메시지를 표시하지만 다른 모드에서는 확인 절차 없이 덮어씁니다.

-l fileName1 fileName2

병합 또는 분할 작업에 사용되는 파일을 지정합니다.

이 옵션에 대한 파일 이름도 지정해야 합니다. 병합의 경우 병합할 두 개의 파일 이름을 지정하고, 분할의 경우 두 개의 대상 파일을 지정합니다. 이 옵션을 생략하면 selogmix 는 seos.ini 파일의 audit_log 토큰에서 지정된 파일 이름을 사용하고 1 과 2 를 파일 이름 끝에 추가합니다.

-m

두 개의 감사 로그 파일을 병합합니다.

-s

지정한 감사 로그 파일을 분할합니다.

-t days

일 수를 지정합니다. 파일 분할 시에만 이 옵션을 사용할 수 있습니다. 별도의 파일에 저장할 로깅 끝부터의 일 수를 지정합니다. 이 옵션을 생략하면 selogmix 는 마지막 로깅 일 하루만 분리합니다.

예제

- 표준 로그 파일을 동일한 크기의 두 파일로 분할하려면 다음 명령을 사용합니다.

  ```
  selogmix -s
  ```

  원본 감사 파일의 이름은 ACInstallDir/log/seos.audit 로 지정됩니다.

  분할된 새 파일의 이름은 각각 ACInstallDir/log/seos.audit1 과 ACInstallDir/log/seos.audit2 로 지정됩니다.

- 로그 파일에서 마지막 2 일 동안의 레코드를 분리하려면 다음 명령을 사용합니다.

  ```
  selogmix -s -t 2
  ```

- 정의된 크기의 상관 관계를 사용하여 로그 파일 한 개를 파일 두 개로 분할하려면 다음 명령을 사용합니다.

  ```
  selogmix -s -c 1:2
  ```

- 지정한 두 파일을 지정한 이름을 가진 파일 한 개로 병합하려면 다음 명령을 사용합니다.

  ```
  selogmix -m -l seos.audit1 seos.audit2 -fn seos.audit.merge
  ```

추가 정보:

seaudit 유틸리티-감사 로그 레코드 표시 (페이지 95)

semsgtool 유틸리티-메시지 파일 유지 관리

semsgtool 유틸리티를 사용하면 다음을 수행할 수 있습니다.

- CA Access Control 메시지 파일에서 단일 메시지 표시
- 메시지의 전체 섹션 나열
- 각 섹션에 대해 ASCII 파일 하나씩, 전체 파일을 ASCII 파일로 덤프
- 새 메시지 파일 작성
- 메시지를 새 메시지로 변경
- 하위 문자열을 포함하여 메시지 나열
- 메시지 파일 유효성 검사

semsgtool 을 실행할 때마다 하나의 명령만 지정할 수 있습니다.

메시지 파일의 기본 위치는 ACInstallDir/data/seos.msg 입니다.

참고: CA Access Control 메시지 파일은 섹션 및 메시지 번호로 구성되어 있습니다. 각 섹션에는 서로 다른 CA Access Control 모듈 또는 하위 모듈에 대한 메시지가 수록되어 있습니다.

이 명령의 형식은 다음과 같습니다.

```
semsgtool {-build|-b} asciiSourceFile OutputMessageFile

semsgtool {-change|-c} [messageFile] {0xerror-code|section# msg#} new-message

semsgtool {-dump|-d} messageFile

semsgtool {-list|-l} [messageFile] sectionNumber

semsgtool {-number|-n} [messageFile] subString

semsgtool {-show|-s} [messageFile] [0xerror-code|section# msg#]

semsgtool {-validate|-v} [messageFile]
```

-build|-b

ASCII 소스 파일에서 새 CA Access Control 메시지 파일을 생성합니다.

-number|-n

정의된 문자열을 포함하는 메시지를 메시지 파일에 나열합니다.

-change|-c

messageFile.new 라는 새 메시지 파일을 작성합니다. 이 파일에서, 지정된 메시지는 정의된 수정 문자열을 포함합니다.

-dump|-d

메시지 파일의 각 섹션별로 한 파일씩 메시지 파일을 몇 개의 파일에 덤프합니다. 이 명령은 나중에 새 CA Access Control 메시지 파일을 작성하기 위해 사용될 수 있는 ASCII 원본 파일을 작성합니다.

-h

이 유틸리티에 대한 도움말을 표시합니다.

-list|-l

메시지 파일의 지정된 섹션에 있는 모든 메시지를 나열합니다.

-show|-s

특정 메시지 코드와 연결된 메시지를 표시합니다.

-validate|-v

(Windows 전용) 중복 메시지와 할당된 제한 값을 초과하는 메시지를 검사하는 방법으로 메시지의 유효성을 검사합니다.

0xerror-code

표시 또는 변경하려는 메시지에 대해 오류 코드의 16 진수를 정의합니다.

asciiSourceFile

semsgtool 이 새 메시지 파일을 작성할 원본 파일을 ASCII 형식으로 정의합니다.

messageFile

메시지 파일의 이름을 정의합니다. 이 옵션을 생략하면 semsgtool 은 구성 설정에 지정된 메시지 파일을 사용합니다.

OutputMessageFile

작성할 새 메시지 파일의 이름을 정의합니다.

section# msg#

표시 또는 변경하려는 메시지에 대해 오류 코드의 섹션 번호 및 메시지 번호를 정의합니다.

sectionNumber

모든 메시지를 나열하려는 섹션의 섹션 번호를 정의합니다.

예제

- 오류 코드 0x205 와 관련된 메시지를 나열하려면 다음 명령을 입력합니다.

  ```
  semsgtool -s seos.msg 0x205
  ```

- 섹션 512 의 메시지를 나열하려면 다음 명령을 입력합니다.

  ```
  semsgtool -l seos.msg 512
  ```

- 수정된 CA Access Control 메시지 파일을 작성하려면 다음 단계를 따르십시오.

  1. 수정된 메시지와 함께 새 메시지 파일을 작성합니다.

     ```
     semsgtool -c 0x2501 "This is the new message"
     ```

     새 메시지 파일인 seos.msg.new 가 수정된 메시지와 함께 작성됩니다.

  2. 새 파일을 CA Access Control 메시지 파일로 복사합니다.

     ```
     copy seos.msg.new seos.msg
     ```

     수정된 메시지와 함께 새 메시지 파일을 이전 seos.msg 파일 위에 복사합니다.

- 오류 코드 0x205 와 관련된 메시지를 표시하려면 다음 명령을 입력합니다.

  ```
  semsgtool -s 0x205
  ```

senable 유틸리티-비활성 사용자 계정 활성화

UNIX 에 해당

senable 유틸리티를 통해 PMDB 를 포함하여 사용자를 비활성화한 위치에서 비활성화된 사용자의 로그인을 활성화합니다. 예를 들어, 서버 데몬에 의해 또는 사용자의 일시 중지 날짜나 만료 날짜에 도달하여 사용자가 비활성화되었을 수 있습니다.

사용자 계정을 활성화한 후 senable 는 새 사용자 암호를 확인하는 sepass 유틸리티를 호출합니다. 가장 최근 암호를 복원하려면 -n 옵션을 사용하십시오.

senable 유틸리티는 로컬 /etc/passwd 파일에서 계정을 삭제하여 정의되지 않은 사용자 계정을 활성화합니다.

원격으로 senable 을 실행하려면 원격 스테이션에 액세스할 수 있도록 WRITE 권한을 부여하는 규칙에서 명시적으로 로컬 터미널 요구를 지정해야 합니다. 그렇지 않으면 해당 위치에서 CA Access Control 을 관리할 수 없습니다.

참고: 원격 관리 제한 사항에 대한 자세한 내용은 UNIX 용 끝점 관리 안내서를 참조하십시오.

이 명령의 형식은 다음과 같습니다.

```
senable [-host hostname] userNames [-n]
```

-host hostname

비활성화된 상태에서 활성화할 계정이 있는 호스트를 선택합니다.

-host 옵션을 사용하려면 두 개의 호스트에서 ADMIN 또는 PWMANAGER 속성을 가지고 있어야 합니다.

- 비활성에서 활성으로 계정을 변경할 호스트
- senable 명령을 입력하는 호스트

-h

이 유틸리티에 대한 도움말을 표시합니다.

-n

비대화식 방법으로 명령을 실행합니다. 이 옵션을 사용하면 senable 은 sepass 를 호출하지 않고 가장 최근에 사용한 암호를 복원합니다.

userNames

비활성에서 활성으로 변경할 계정에 대해 사용자 이름을 공백으로 구분하여 정의합니다.

추가 정보:

serevu 유틸리티-실패한 로그인 시도 처리 (페이지 207)

senone 유틸리티-권한 없는 사용자로서 명령 실행

UNIX 에 해당

senone 유틸리티는 권한을 가진 사용자가 권한 없는 사용자 프로세스로 작성한 명령을 실행합니다.

참고: 언트러스트된 프로그램을 테스트하는 권한이 부여된 사용자만 이 유틸리티를 사용해야 합니다.

senone 유틸리티를 호출하면 권한 부여 데몬의 프로세스 자격 증명이 삭제됩니다. 그런 다음 senone 은 CA Access Control 에 정의되지 않은 사용자의 자격 증명을 사용하여 셸을 실행합니다. 이때부터 해당 셸 내에서 호출된 모든 프로그램은 비 CA Access Control 사용자의 인증서를 사용하여 실행됩니다. senone 은 호출자의 사용자 ID 를 변경하지 않으므로 사용자의 UNIX 권한은 변경되지 않습니다.

중요! root 로 로그인한 사용자는 언트러스트된 프로그램을 실행하지 않는 것이 좋습니다. 언트러스트된 프로그램을 senone 과 함께 실행할 때도 예상치 못한 문제가 발생할 수 있습니다.

명령을 지정하지 않고 senone 을 호출하면 senone 은 /etc/passwd 에 정의된 사용자의 셸을 실행합니다.

이 명령의 형식은 다음과 같습니다.

```
senone [command]
```

-h

이 유틸리티에 대한 도움말을 표시합니다.

command

senone 이 권한 없는 사용자로서 실행하도록 할 명령을 지정합니다.

추가 정보:

sesu 유틸리티 - 사용자 전환 (페이지 210)
sewhoami 유틸리티 - UNIX 에서 CA Access Control 사용자 이름 및 보안 자격 증명 표시 (페이지 219)

SEOS_load 유틸리티-CA Access Control 차단 모듈 로드

UNIX 에 해당

SEOS_load 유틸리티는 동적 CA Access Control 커널 모듈(SEOS_syscall)을 제어합니다. CA Access Control 유틸리티를 실행하기 전에 먼저 차단 모듈을 로드해야 합니다.

참고: 커널을 로드 및 언로드하기 전후에 UNIX exit 를 사용하여 프로그램을 자동으로 실행할 수 있습니다.

스트림 지원 플랫폼에서 이 유틸리티는 seos.ini 파일의 [SEOS_syscall] 섹션에 있는 SEOS_use_streams 토큰에 따라 CA Access Control 모듈을 스트림에 로드합니다. 토큰을 yes 로 설정하면 이 모듈이 스트림으로 푸시됩니다.

이 명령의 형식은 다음과 같습니다.

```
SEOS_load [-i|-k|-s|-u]
```

-i

(HP-UX 및 Sun Solaris 플랫폼 전용) CA Access Control 커널 확장에 대한 정보를 표시합니다.

-k

(HP-UX 및 Sun Solaris 플랫폼 전용) CA Access Control 모듈을 스트림으로 전송하지 않고 커널에 로드합니다.

-s

(HP-UX 및 Sun Solaris 플랫폼 전용) CA Access Control 커널 모듈을 스트림에 삽입합니다. 이 옵션은 seos.ini 파일의 SEOS_syscall 섹션에 있는 SEOS_use_streams 토큰을 무시합니다.

-u

커널에서 CA Access Control 커널 확장을 언로드한 다음 스트림에서 모듈을 제거합니다.

참고: CA Access Control 의 위에 로드된 응용 프로그램이 CA Access Control 에 의해 연결된 개방형 시스템 호출(syscall)을 가지고 있는 경우에는 CA Access Control 을 언로드할 수 없습니다. 이러한 프로세스를 찾으려면 secons -sc 또는 secons -scl 을 사용하십시오. 그러면 이러한 프로세스를 종료하고 CA Access Control 커널 모듈을 언로드할 수 있습니다. 또는 커널을 언로드하기 전에 UNIX exit 를 사용하여 이러한 프로세스를 자동으로 종료하고, 커널 언로드 이후 프로세스를 다시 시작할 수 있습니다.

sepass 유틸리티-암호 설정 또는 교체

UNIX 에 해당

sepass 유틸리티는 로컬 호스트, 정책 모델, NIS 또는 NIS+ 서버에서 상황에 따라 새 암호를 설정하거나 기존 암호를 교체합니다.

sepass 유틸리티는 사용자 암호를 변경합니다. 권한 있는 사용자는 sepass 를 사용하여 다른 사용자의 암호를 변경할 수도 있습니다. 암호를 변경할 때 sepass 는 이전 암호를 묻습니다.

참고: seosd 가 실행되고 있지 않으면 sepass 는 기본 암호 프로그램을 실행합니다. 기본 암호 프로그램은 seos.ini 파일의 passwd 섹션에 있는 DefaultPasswdCmd 토큰에서 지정됩니다. 암호는 암호화된 형식으로 네트워크에서 저장되고 전송됩니다.

이 명령의 형식은 다음과 같습니다.

```
sepass [-d] [-l] [-p] [-s policy_model@hostname] \
    [-g number] [-x] [userName]
```

-d

업데이트에 성공한 스테이션, setoptions class+(PASSWORD)를 활성화하지 않은 경우 암호 품질이 검사되지 않은 스테이션 등 암호 업데이트와 관련된 모든 정보를 표시합니다. 이 스위치는 디버그 시 유용합니다.

-g number

userName 에 대한 유예 로그인 수를 정의합니다.

-h

이 유틸리티에 대한 도움말을 표시합니다.

-l

로컬 암호 파일(대개 /etc/passwd)에서 보안 파일 및 로컬 데이터베이스인 로컬 스테이션에서만 암호를 교체합니다.

NIS/NIS+ 환경에서는 일반적으로 클라이언트의 /etc/passwd 파일에 사용자를 정의하지 않으므로 클라이언트 스테이션의 암호는 업데이트되지 않습니다.

NIS/NIS+ 서버 스테이션에서 암호가 로컬로 업데이트되고 NIS/NIS+에 의해 전파됩니다.

이 스위치와 -p 및 -s 스위치는 동시에 사용할 수 없습니다.

-p

스위치에 지정된 호스트의 PMDB 와 원격 스테이션에서만 암호를 변경합니다. 이 스위치와 -l 및 -s 스위치는 동시에 사용할 수 없습니다.

-s policy_model@hostname

스위치에 지정된 호스트의 PMDB 와 로컬 스테이션에 대해 암호를 교체합니다. 이 스위치와 -l 및 -p 스위치는 동시에 사용할 수 없습니다.

-x

사용자 username 이 암호를 변경한 것처럼 암호를 교체합니다. 이 스위치는 데이터베이스의 마지막 변경 시간과 날짜를 업데이트합니다. 유예 로그인은 종료됩니다.

참고: root 사용자가 변경한 것처럼 root 암호를 변경할 수 있으려면 RootPwAsOwn 을 적절하게 설정해야 합니다. seos.ini 토큰에 대한 자세한 내용은 참조 안내서를 참조하십시오.

username

(선택 사항) 암호 sepass 가 변경된 사용자의 이름을 지정합니다. 이 옵션을 생략하면 자신의 암호가 설정됩니다.

예제

다음 예는 다양한 상황에서 sepass 를 사용하는 방법을 설명합니다.

- 로컬 호스트에서 사용자 자신의 암호를 변경하려면 다음 명령을 입력합니다.

  ```
  sepass -l
  ```

  참고: 사이트에 정의된 PMDB 가 없을 경우 -l 스위치를 생략할 수 있습니다. 사이트에서 PMDB 를 사용 중인 경우 -l 스위치를 생략하면 PMDB 의 모든 구독자 데이터베이스에서 암호가 변경됩니다. NIS/NIS+ 클라이언트에서 이 스위치는 암호를 변경하지 않지만 NIS/NIS+ 서버에서는 암호가 변경된 후 전파됩니다.

- 자신을 제외한 다른 사람의 암호를 로컬 호스트에서만 변경하려면 다음 명령을 입력합니다.

  ```
  sepass -l username
  ```

  username 이 /etc/passwd 파일, 해당 UNIX 보안 파일 및 데이터베이스에 있어야 합니다.

  NIS/NIS+ 클라이언트에서 sepass 스위치를 사용하면 암호가 변경되지 않습니다. NIS/NIS+ 서버에서는 암호가 변경된 후 전파됩니다.

- NIS 를 사용하지 않는 사이트의 여러 스테이션에서 사용자 암호를 변경하려면 다음 단계를 따르십시오.

  1. PMDB 를 생성합니다.

     참고: PMDB 작성에 대한 자세한 내용은 UNIX 용 끝점 관리 안내서를 참조하십시오.

  2. 상세 내역을 구독자 컴퓨터로 배포해야 하는 모든 사용자를 PMDB 의 UNIX 및 CA Access Control 환경에 둘 다 추가합니다.

  3. 업데이트된 암호를 수신할 모든 스테이션을 PMDB 에 구독시킵니다.

  4. 모든 구독자에서 seos.ini 파일의 [seos] 섹션에 있는 토큰을 사용 중인 PMDB 의 이름으로 설정합니다. 예:

     ```
     passwd_pmd = PMD1@morocco
     parent_pmd = PMD1@casablanca
     ```

  5. 다음 명령을 입력합니다.

     ```
     sepass username
     ```

     sepass 실행이 완료되면 모든 구독자 데이터베이스에서 사용자 암호가 변경됩니다.

sepmd 유틸리티

sepmd 유틸리티는 정책 모델 관리 유틸리티입니다.

이 유틸리티를 사용하여 다음 작업을 수행할 수 있습니다.

- 구독자 및 업데이트 파일 관리
- 관리자 이중 제어
- 정책 모델 로그 파일 관리
- PMDB 관리
- PMDB 백업
- PMDB 복원

참고: 정책 모델이 있는 호스트에서 sepmd 유틸리티를 실행해야 합니다.

추가 정보:

sepmd 유틸리티-구독자 및 업데이트 파일 관리 (페이지 183)
sepmd 유틸리티-이중 컨트롤 관리 (페이지 187)
sepmd 유틸리티-PMDB 백업 (페이지 188)
sepmd 유틸리티-정책 모델 로그 파일 관리 (페이지 191)
sepmd 유틸리티-PMDB 관리 (페이지 192)

sepmd 유틸리티 - PMDB 복원 (페이지 193)

sepmd 유틸리티-구독자 및 업데이트 파일 관리

유틸리티는 구독자를 작성, 제거 및 할당합니다.

이 명령의 형식은 다음과 같습니다.

```
sepmd {-C|-de|-l|-L|-p|-R} pmd

sepmd {-n|-r|-u} pmd subscriber

sepmd -s pmd subscriber offset

sepmd -sm pmd mf_subscriber mf_type mf_sysid mf_admin offset

sepmd -t pmd {auto|offset}
```

-C

업데이트 파일의 모든 명령과 해당 오프세트를 표시합니다. 오프셋은 파일 내 업데이트의 위치를 나타냅니다. 다른 데이터베이스 또는 PMDB 를 구독할 때 이를 지정할 수 있습니다.

-de

(UNIX 전용) 암호화된 updates.dat 파일의 정보를 해독합니다. UseEncryption PMDB 구성 설정을 yes 로 설정할 때 이 파일에 대한 데이터 암호화가 발생합니다.

-l

정책 모델의 구독자를 나열합니다.

-L

정책 모델과 해당 상태(오류 수, 가용성, 오프셋, 동기화 모드 및 전파될 다음 명령 등)를 나열합니다. 업데이트 파일에는 정책 모델이 전파해야 하거나 전파한 모든 업데이트가 있습니다. 오프셋은 구독자에게 전송해야 하는 다음 업데이트의 위치를 표시합니다. 최초 오프셋과 최종 오프셋도 모두 나타납니다.

-n

새 구독자를 생성한 후 소급하여 정책 모델에 업데이트합니다. 구독자 업데이트에 적용되는 일반 규칙은 -s 옵션에 대한 설명을 참조하십시오.

참고: 이 옵션은 LOGINAPPL(UNIX 전용) 및 SPECIALPGM 개체를 포함하여 전체 PMDB 의 내용을 새 구독자에게 전송합니다. 구독자의 개체가 부모 항목의 개체와 다를 경우 이러한 개체를 필터링할 수 있습니다.

-n 으로 추가된 구독자는 sync 로 표시되어 동기화 모드에 있음을 나타내고, 모든 PMDB 규칙을 수신합니다. 구독자가 모든 규칙을 수신하면, 구독자는 동기화 모드에서 해제되어 정식 구독자가 됩니다. -n 옵션은 처리하는 데 시간이 걸릴 수 있습니다. 여러 개의 업데이트가 있거나 업데이트가 충돌하는 경우, 최종 업데이트가 사용됩니다.

중요! sepmd -n 을 사용하여 CA Access Control 끝점 또는 PMDB 를 다른 PMDB 에 구독시킬 때, 새 구독자에 이미 있는 정책(POLICY 개체 이름)을 새 부모 PMDB 에 포함해서는 안 됩니다. 구독자로부터 기존의 각 정책을 배포 취소한 다음, POLICY 개체 및 연결된 RULESET 개체를 구독자로부터 삭제해야 합니다. 그런 다음 새 부모 PMDB 를 구독해야 합니다.

UNIX 에서 seos.ini 파일의 send_unix_env 토큰을 yes 로 설정하면 -n 옵션을 사용하여 정책 모델 암호 및 그룹 파일의 내용을 전송할 수도 있습니다. dbmgr -export -l 을 통해 데이터베이스를 확인하여, 전달되는 명령을 명확히 알아두는 것이 좋습니다.

-p

상주하는 정책 모델 및 해당 상태를 나열합니다.

-r

sepmdd 에 의해 유지 관리되는 사용할 수 없는 구독자 목록에서 구독자를 제거하여, 구독자가 업데이트를 즉시 사용할 수 있게 합니다. 일반적으로 구독자가 종료되어 정책 모델로부터 업데이트를 받을 수 없는 경우 sepmdd 는 특정 기간이 경과해야만 해당 구독자에게 업데이트를 보내려고 시도합니다. 그러나 이 옵션을 지정할 경우 sepmdd 는 대기 기간을 건너뛰고 구독자에게 즉시 업데이트를 보내려고 시도합니다.

-R

실제 오프셋과 함께 모든 구독자를 업데이트합니다.

-s

다른 데이터베이스 또는 PMDB를 정책 모델에 구독합니다. 호스트를 정책 모델에 구독시키려면 호스트가 작동하고 있어야 하며, 해당 호스트에서 CA Access Control 이 실행되고 있어야 합니다. 또한 PMDB 는 구독한 호스트의 상위 PMDB 이어야 합니다. parent_pmd 구독자의 구성 설정과 이 관계를 만들어야 합니다. 이 구성 설정에는 호스트를 구독시킬 PMDB 의 이름이 포함되어 있어야 합니다.

또 다른 정책 모델에 정책 모델을 구독하는 경우

- 구독한 정책 모델의 pmd.ini 파일에 있는 parent_pmd 토큰에 구독된 정책 모델(상위 정책 모델)의 이름이 있어야 합니다.
- 구독된 정책이 있는 호스트에서 CA Access Control 이 실행되고 있어야 합니다.

PMDB에는 상위 데이터베이스가 하나만 있어야 합니다. 상위 정책 모델이 둘 이상인 정책 모델을 설정하기로 결정하는 경우, 상위 정책 모델 목록이 들어 있는 파일 이름을 parent_pmd 토큰에 제공해야 합니다. 그러나 두 개 이상의 상위 데이터베이스를 설정하는 것은 여러 출처로부터 신뢰할 수 없는 지시사항을 받아 데이터베이스에 정보를 입력할 수 있으므로 권장되지 않습니다.

-sm

메인프레임 구독자를 정책 모델에 할당합니다.

-t

업데이트 파일에서 항목을 삭제하여 파일을 자릅니다.

참고: UNIX 에서 force_auto_truncate PMDB 구성 설정이 'no'로 설정된 경우 sepmd -t 는 업데이트 파일을 자르지 않습니다. 토큰이 yes 로 설정되어 있으면 정책 모델에 구독자가 없는 경우에도 업데이트 파일이 잘립니다.

- 오프셋(수동 절단)을 사용하는 경우 -L 옵션과 함께 sepmd 를 실행하여 오프셋을 찾을 수 있습니다.

  참고: 파일을 자르려면 시작 오프셋에서 차감하여 유도된 오프셋이 아닌 -L 매개 변수에 제공된 실제 오프셋을 사용해야 합니다.

- 자동을 사용하는 경우 sepmd 는 첫 번째 비전파 항목의 오프셋을 계산하고 이전 항목을 모두 삭제합니다. 자동을 사용하면 -L 매개 변수와 함께 유틸리티를 실행하는 단계가 저장됩니다.

구독자가 지정된 오프셋 전에 모든 업데이트를 더 적게 받을 경우 sepmd 는 오류 메시지를 표시하고 파일을 자르지 않습니다. 파일을 자르려면 다음 작업을 수행하십시오.

- 업데이트되지 않은 호스트 구독 취소
- 파일 자르기
- 정책 모델에 호스트 다시 구독

이 작업을 수행할 경우 구독자는 정책 모델로부터 하나 이상의 업데이트를 받을 수 없습니다. 구독자의 오프셋은 업데이트 파일의 최종 오프셋으로 변경됩니다.

-u

정책 모델 예약 요청(구독) 목록에서 구독자를 제거합니다.

auto

전파되지 않은 첫 번째 항목의 오프셋을 계산하고 그 앞의 모든 항목을 삭제하도록 sepmd 에 지시합니다.

offset

-s 또는 -sm 옵션과 함께 사용할 경우, 새로 추가된 구독자가 업데이트 수신을 시작할 지점을 업데이트 파일 내에 지정합니다.

-t 옵션과 함께 사용할 경우, 업데이트 파일의 시작 부분에서 특정 구독자 위치까지의 거리를 지정합니다.

유효한 업데이트 오프셋을 보려면 -C 옵션을 사용하십시오. 업데이트의 중간 지점에 오프셋을 지정하면 오프셋이 앞으로 이동하여 다음 업데이트의 시작 지점에 오게 됩니다. 잘못된 오프셋(첫 번째 오프셋보다 작고 마지막 오프셋보다 큼)을 지정하면 오류 메시지가 나타납니다.

pmd

정책 모델의 이름을 지정합니다.

subscriber

구독자 스테이션이나 구독자 PMDB 의 호스트를 지정합니다.

sepmd 유틸리티-이중 컨트롤 관리

UNIX 에 해당

sepmd 유틸리티는 이중 컨트롤 트랜잭션을 관리합니다. sepmd 유틸리티는 각 트랜잭션이 작성될 때 고유한 ID 번호를 제공합니다.

참고: 이중 컨트롤에 대한 자세한 내용은 UNIX 용 끝점 관리 안내서를 참조하십시오.

이중 컨트롤을 사용할 때 PMDB 의 이름은 maker 여야 하며 is_maker_checker 구성 설정은 PMDB 및 CA Access Control 에 대해 모두 값 yes 를 가져야 합니다.

이 명령의 형식은 다음과 같습니다.

```
sepmd -m {l|la|lo}

sepmd -m {d|r} transactionId

sepmd -m p transactionId code
```

-m d

트랜잭션을 삭제합니다. 트랜잭션은 PMDB 에서 구현되기 전에 승인되어야 하는 하나 이상의 명령입니다. 트랜잭션을 작성한 사용자만 트랜잭션을 삭제할 수 있습니다.

-m l

명령을 호출한 사용자의 처리되지 않은 트랜잭션(Checker 대기 중)을 나열합니다. 각 트랜잭션은 ID 번호, Maker 이름(트랜잭션을 작성한 사용자로, 여기서는 명령을 호출한 동일한 사용자) 및 설명과 함께 나열됩니다.

-m la

모든 Maker 의 처리되지 않은 모든 트랜잭션을 나열합니다. 각 트랜잭션은 ID 번호, Maker 이름 및 설명과 함께 나열됩니다.

-m lo

명령을 호출한 사용자의 트랜잭션을 제외하고 모든 Maker 의 처리되지 않은 트랜잭션(Checker 대기 중)을 나열합니다.

-m p

트랜잭션을 처리합니다. Checker(트랜잭션을 생성한 Maker 를 제외한 모든 admin 사용자)가 ID 번호를 입력하면 지정한 트랜잭션의 모든 명령이 목록에 나타납니다.

이 옵션은 다음과 같은 경우에는 작동하지 않습니다.

- 트랜잭션의 명령 중 하나 이상이 명령을 호출한 사용자에 속해 있는 경우
- 다른 Checker 가 트랜잭션을 잠근 경우
- 명령을 호출한 사용자가 트랜잭션을 작성한 경우. 이때 Maker 는 자신의 트랜잭션에 대한 Checker 역할을 수행할 수 없습니다.
- 지정한 트랜잭션 ID 가 존재하지 않는 경우
- 명령을 호출한 사용자가 Checker 권한이 없는 경우

-m r

트랜잭션을 검색하거나 잠급니다.

- 트랜잭션을 작성한 사용자(Maker)인 경우 이 매개 변수는 처리되지 않은 특정 트랜잭션을 검색합니다. 트랜잭션을 검색한 후 해당 트랜잭션을 적합한 파일로 전송하고 선택한 ASCII 편집기(vi, emacs 등)를 사용하여 트랜잭션을 업데이트할 수 있습니다.
- Maker 가 아닌 사용자(Checker)인 경우 이 매개 변수는 처리하기 전에 트랜잭션을 잠급니다. 잠긴 트랜잭션은 변경할 수 없습니다.

transacationID

트랜잭션이 작성될 때 sepmdd 가 트랜잭션에 부여하는 고유 식별 번호를 지정합니다.

코드

트랜잭션을 처리할 때 Checker 가 수행해야 할 일을 지정하는 숫자 코드를 지정합니다.

0

트랜잭션을 거부합니다. 이 경우 트랜잭션의 모든 명령이 삭제되고 PMDB 에서 변경이 구현되지 않습니다.

1

트랜잭션에 권한을 부여합니다. 이 경우 명령이 PMDB 에서 즉시 구현됩니다.

2

나중에 또는 다른 Checker 에 의해 처리될 수 있도록 트랜잭션 잠금을 해제합니다.

sepmd 유틸리티-PMDB 백업

sepmd 유틸리티를 사용하면 정책 모델 데이터베이스를 백업할 수 있습니다.

이 명령의 형식은 다음과 같습니다.

```
sepmd {-bl|-ul} pmd
```

```
sepmd -bd pmd destination
```

```
sepmd -bh pmd destination backup_host
```

-bd

destination 디렉터리에 pmd 를 백업합니다.

-bh

계층에 있는 정책 모델에 대해 destination 디렉터리에 pmd 를 백업합니다. 즉, backup_host 호스트로 백업을 이동해도 구독이 유효하도록 백업은 PMDB 구독자를 수정합니다.

-bl

구독자에게 명령을 전파하지 않도록 pmd 를 잠급니다.

정책 모델에 구독자가 있으며 백업이 진행되는 동안 업데이트가 허용되지 않도록 하려면 이 옵션을 사용하십시오.

-ul

잠긴 pmd 의 잠금을 해제합니다.

backup_host

백업 호스트를 이동할 대상 호스트의 이름을 정의합니다.

destination

PMDB 파일을 백업할 대상 디렉터리 이름을 정의합니다.

pmd

정책 모델 데이터베이스를 정의합니다. 이 데이터베이스는 _pmd_directory_ 구성 설정에서 지정한 위치에 저장됩니다.

예: PMDB 백업

다음 명령은 myPMDB 라는 이름의 PMDB 를 /tmp/my_pmdb 디렉터리에 백업합니다.

```
sepmd -bd pmdb /tmp/my_pmdb
```

이제 필요한 대로 PMDB 를 관리할 수 있습니다.

```
selang -d /tmp/my_pmdb
```

예: 구독자와 함께 PMDB 백업

다음 명령은 구독자가 있는 PMDB 를 백업한 후 PMDB 를 다른 호스트로 이동하는 방법을 보여줍니다.

1. PMDB 를 잠급니다.

   ```
   sepmd -bl mainPMDB
   ```

   CA Access Control 은 업데이트를 송신 또는 수신하지 못하도록 PMDB 를 잠급니다.

2. PMDB 를 백업합니다.

   ```
   sepmd -bh mainPMDB /tmp/my_pmdb host63
   ```

   CA Access Control 은 PMDB 를 /tmp/my_pmdb 에 백업합니다.

   UNIX 에서 CA Access Control 은 사용자가 지정한 백업 호스트 이름과 함께 subscribers.dat 를 업데이트합니다.

   Windows 에서 CA Access Control 은 pmd.reg 파일을 작성합니다. 이 파일은 사용자가 지정한 새 호스트에 맞게 변경된 Parent_Pmd 구성 설정의 값이 포함된 pmd 레지스트리 설정의 덤프입니다.

3. PMDB 의 잠금을 해제합니다.

   ```
   sepmd -ul mainPMDB
   ```

   CA Access Control 은 PMDB 의 잠금을 해제합니다.

4. PMDB 백업을 새 호스트로 전송합니다.

   참고: 새 호스트는 현재 컴퓨터와 동일한 OS 및 CA Access Control 버전을 가지고 있어야 합니다.

5. (Windows 전용) mainPMDB.reg 파일을 새 호스트의 레지스트리로 가져옵니다.

   이제 정상적인 방법으로 PMDB 를 계속 사용할 수 있습니다.

sepmd 유틸리티-정책 모델 로그 파일 관리

sepmd 유틸리티는 정책 모델 로그 파일을 관리합니다. 정책 모델 로그 파일은 정책 모델 데이터베이스 활동에 대한 상세한 감사 추적 기능을 제공합니다. 예:

```
Wed Nov  4 10:08:02 2003 pmdb1:Processing list request for missouri.yourco.com
Wed Nov  4 10:08:02 2003 pmdb1:Processing list request for oregon.yourco.com
Wed Nov  4 10:09:14 2003 pmdb1:Empty request
Wed Nov  4 10:09:15 2003 pmdb1:Processing shutdown request
Wed Nov  4 10:09:15 2003 pmdb1:Delete filters
Wed Nov  4 10:10:04 2003 pmdb1:Opened error logs
Wed Nov  4 10:10:04 2003 pmdb1:Try to load filters
Wed Nov  4 10:10:04 2003 pmdb1:Filters file : nis_filter.dat
```

처음으로 sepmdd 를 실행하면 자동으로 정책 모델 로그 파일이 작성됩니다.

UNIX 에서는 pmd_log_level PMDB 구성 설정을 사용하여 PMDB 기록 내용을 제어할 수 있습니다.

- **0**-어떠한 항목도 기록하지 않습니다.
- **1**-오류 메시지만 나열합니다.
- **2**-오류 및 정보 메시지를 나열합니다(기본값).

참고: 로그 파일의 경고 메시지는 파일 크기 제한이 초과되었음을 알려줍니다. 로그 파일의 크기를 늘리려면 구성 설정을 사용하십시오.

이 명령의 형식은 다음과 같습니다.

```
sepmd {-sl|-kl|-dl|-cl} pmd
```

-cl

정책 모델 로그 파일의 내용을 지웁니다.

-dl

정책 모델 로그 파일을 표시합니다.

-kl

정책 모델 로그 파일을 사용할 수 없게 합니다.

-sl

정책 모델 로그 파일을 사용할 수 있게 합니다.

pmd

정책 모델의 이름을 지정합니다.

sepmd 유틸리티-PMDB 관리

sepmd 유틸리티는 UNIX 에서 정책 모델을 중지 또는 시작하며, 정책 모델에 영향을 주는 구성 설정을 다시 로드하기도 합니다.

참고: UNIX 에서와는 달리 Windows 에서는 sepmd 가 정책 모델 서비스를 중지 또는 시작하지 않습니다. 대신 정책 모델을 활성화 및 비활성화합니다.

sepmd 를 사용하여 정책 모델을 시작하거나 쿼리하려면 정책 모델에 ADMIN 권한이 있어야 합니다.

이 명령의 형식은 다음과 같습니다.

```
sepmd {-c|-e|-k|-S} pmd
```

```
sepmd -tm seconds
```

-c

정책 모델 오류 로그를 지웁니다.

-e

정책 모델 오류 로그를 표시합니다.

-k

UNIX 에서, 정책 모델 데몬을 안전하게 종료합니다. Windows 에서, 정책 모델 서비스를 비활성화합니다.

참고: UNIX 에서 정책 모델 데몬을 종료하기 위해 kill 명령을 사용하지 마십시오.

-ri

UNIX 에서, sepmdd 가 실행되고 있는 동안 정책 모델 및 CA Access Control 구성 파일(각각 pmd.ini 와 seos.ini)을 다시 로드합니다. 1 분 이상의 간격으로만 이 옵션을 사용할 수 있습니다. 이 옵션은 parent_pmd, _retry_timeout_, _min_retries_ 및 _shutoff_time_ 토큰에서 구성 변경 사항을 검사합니다.

Windows 에서, 정책 모델 정보를 레지스트리에서 호스트로 다시 로드합니다. 데이터를 변경했으며 호스트 PMDB 로 전송되었는지 확인하려면 이 스위치를 사용하십시오.

-S

UNIX 에서, 정책 모델 데몬을 시작합니다. Windows 에서, 정책 모델 서비스를 활성화합니다.

실행할 다른 명령이 없는 경우 데몬을 시작하기 위해 이 옵션을 사용하십시오.

-tm seconds

(Windows 전용) 실행된 요청에 대해 초기 시간 제한 간격(초)을 설정합니다.

pmd

정책 모델의 이름을 지정합니다.

sepmd 유틸리티 - PMDB 복원

sepmd 는 로컬 호스트에서 PMDB 를 복원합니다. PMDB 를 복원하기 위해 사용하는 백업 파일은 복원 호스트와 동일한 플랫폼, 운영 체제, CA Access Control 버전을 실행하는 호스트에서 가져와야 합니다. CA Access Control 은 복원 호스트에서 반드시 실행 중이어야 합니다.

참고: 다른 터미널에서 PMDB 를 백업 및 복원하는 경우 PMDB 는 복원된 PMDB 데이터베이스에서 터미널 리소스를 자동으로 업데이트하지 않습니다. 복원된 PMDB 에 새 터미널 리소스를 추가해야 합니다. 새 터미널 리소스를 추가하려면 복원된 PMDB 를 중단하고, selang -p pmdb 명령을 실행한 다음 복원된 PMDB 시작하십시오.

이 명령의 형식은 다음과 같습니다.

```
sepmd -restore pmd [-source path] [-admins user[,user...]]\
[-xadmins user[,user...]] [-parent_pmd name[,name...]]
```

-restore

localhost 에서 PMDB 를 복원합니다.

-admins user[,user...]

(UNIX) 내부 사용자를 복원된 PMDB 의 관리자로 정의합니다.

-parent_pmd name[,name...]

(선택 사항) 복원된 PMDB 의 부모 PMDB 의 이름을 정의합니다. 부모 PMDB 이름은 pmdb@host 형식으로 지정하십시오.

pmd

복원할 PMDB 의 이름을 정의합니다.

-source(path)

(선택 사항) 백업 파일이 있는 디렉터리를 정의합니다. 원본 디렉터리를 지정하지 않으면 기본 위치에 있는 파일에서 PMDB 가 복원됩니다. 기본 위치는 _pmd_backup_directory_ 토큰에 정의됩니다.

기본값: (UNIX) ACInstallDir/data/policies_backup/pmdName

기본값: (Windows) ACInstallDir\data\policies_backup\pmdName

-xadmins user[,user...]

(UNIX) 엔터프라이즈 사용자를 복원된 PMDB 의 관리자로 정의합니다.

sepmdadm 유틸리티-PMDB 정의 만들기

UNIX 에 해당

sepmdadm 유틸리티는 PMDB 를 실행하기 위해 필요한 정의를 만듭니다. sepmdadm 유틸리티는 PMDB 정의, PMDB 와 상위 및 하위 PMDB 간의 관계 정의 및 구독자 스테이션 정의에 필요한 CA Access Control 및 UNIX 명령으로 구성된 스크립트입니다. 기본적으로 root 사용자는 PMDB 의 관리자 및 감사자(Auditor)로 정의됩니다. 원격 셸을 통해 실행할 수도 있지만 로컬에서 sepmdadm 유틸리티를 실행해야 합니다. sepmdadm 을 사용하여 새 PMDB 를 작성할 때 후속 작업으로 PMDB 에 대해 구독자를 지정하고 UID 와 GID 를 동기화할 수 있습니다.

이 유틸리티는 대화형 또는 비대화형 모드에서 실행할 수 있습니다.

- 비대화형 모드에서 인수를 명령줄에 입력하십시오. 유틸리티는 수신한 값에 따라 PMDB 와 PMDB 계층을 작성합니다.
- 대화식 모드에서는 명령 라인에 인수를 입력하지 않습니다. sepmdadm 유틸리티는 사용자에게 원하는 모드가 대화식 모드인지 확인합니다. 사용자가 "y"를 입력하면 유틸리티는 계속해서 사용자에게 옵션 값을 묻는 메시지를 표시합니다.

새 PMDB 를 sepmdadm 으로 작성할 때 정책 모델의 구독자인 스테이션을 식별합니다. 그러나 스테이션을 구독한 PMDB 이름을 사용하여 각 구독자의 seos.ini 파일에 있는 parent_pmd 토큰도 업데이트해야 합니다. 그렇지 않으면 구독자는 PMDB 에서 업데이트를 수신하지 않습니다.

여러 개의 스테이션을 동일한 PMDB 에 구독하고 한 PMDB 스테이션을 또 다른 스테이션에 구독하면 PMDB 계층을 작성할 수 있습니다.

이 명령의 형식은 다음과 같습니다.

```
sepmdadm options
```

--admin name

PMDB 의 CA Access Control 관리자를 정의합니다.

--auditor name

PMDB 의 CA Access Control 감사자를 정의합니다.

-c | --clean pmdbName

지정한 정책 모델을 제거합니다. 이 옵션은 정책 모델 데몬을 종료하고, 데이터베이스로부터 파일 보호를 제거하며, 정책 모델 디렉터리 및 디렉터리 내 모든 내용을 삭제합니다.

이 옵션은 --noconfirm 옵션과 함께 사용할 수 없습니다.

--desktop hostname

관리자가 로컬 호스트에 있는 PMDB 를 관리할 수 있는 스테이션을 지정합니다. 스테이션을 지정하지 않을 경우 관리자는 로컬 호스트의 PMDB 만 관리할 수 있습니다.

--group_fname fileName

NIS 에서 그룹 파일의 위치를 정의합니다.

-h | --help

도움말 화면을 표시합니다.

-i | --interactive

sepmdadm 을 대화식 모드로 실행합니다.

-l

sepmdadm 이 로컬 모드에서 실행되도록 지정합니다. 즉, CA Access Control 이 실행되고 있지 않을 때 PMDB 를 작성할 수 있습니다.

참고: 이 옵션을 지정하지 않은 경우 CA Access Control 을 실행하여 sepmdadm 을 사용해야 합니다.

--nis | --NIS

정책 모델에서 NIS 설치를 수행합니다. PMDB 가 NIS 서버에 설치된 경우 이 옵션을 사용해야 합니다.

--noconfirm

사용자에게 응답을 요구하는 메시지를 표시하지 않도록 지정합니다. 이 옵션은 비대화형 모드의 shell 스크립트 내에서 sepmdadm 을 호출하는 경우 유용합니다.

--parentpmd pmdbName

이 PMDB 가 subscribed 된 부모 PMDB 의 이름을 지정합니다. 이 매개 변수를 -subsconfig 매개 변수와 함께 사용할 경우 sepmdadm 은 seos.ini 파일의 parent_pmd 토큰을 업데이트합니다. 이 매개 변수를 -subsconfig 매개 변수 없이 사용할 경우 sepmdadm 은 pmd.ini 파일의 parent_pmd 토큰을 업데이트합니다.

참고: 다중 부모 정책 모델을 정의하려는 경우 인용 부호를 사용해야 합니다. 예를 들어, 정책 모델을 만든 후 상위 정책 모델을 정의하려면 다음 명령을 사용하십시오.

```
sepmdadm --pmdname subs2 --admin abc123 --admin root --auditors abc123 --desktop
pcp36949 \
--parentpmd "aa@pcp36949,bb@pcp36949"
```

--passwd_fname fileName

NIS 에서 passwd 파일의 위치를 정의합니다.

--passwdpmd pmdbName

sepass 가 암호 업데이트를 보내는 PMDB 를 지정합니다. 이 옵션은 seos.ini 파일의 [seos] 섹션에 있는 passwd_pmd 토큰을 업데이트합니다.

참고: 이 매개 변수는 -subsconfig 스위치를 사용할 경우에만 사용할 수 있습니다.

멀티 수준의 정책 모델을 작성할 때 암호 변경사항을 PMDB 시스템의 모든 수준으로 전파할 수 있도록 이 매개 변수를 피라미드 구조의 맨 위에 있는 PMDB 로 설정하십시오.

--pmdname pmdbName

생성되는 PMDB 의 이름을 지정합니다.

--pwmanager name

PMDB 의 CA Access Control 암호 관리자를 지정합니다.

--seosdir directory

CA Access Control 이 설치된 디렉터리를 지정합니다. CA Access Control 이 기본 디렉터리에 설치되지 않은 경우에만 이 옵션을 사용하십시오.

--subsconfig

로컬 스테이션을 구독자로 지정합니다. 이 매개 변수를 사용할 때 --parentpmd pmdbName 및 --passwdpmd pmdbName 매개 변수를 지정하여 seos.ini 파일의 관련 토큰을 업데이트해야 합니다.

참고: 구독자를 구성할 때 이러한 매개 변수는 -subsconfig 옵션 뒤에 나와야 합니다.

--subscriber name

이 PMDB 의 구독자를 지정합니다. PMDB 또는 스테이션이 구독자가 될 수 있습니다.

--xadmin name

PMDB 의 엔터프라이즈 사용자 관리자를 정의합니다.

--xauditor name

PMDB 의 엔터프라이즈 사용자 감사자를 정의합니다.

--xpwmanager name

PMDB 의 엔터프라이즈 사용자 암호 관리자를 지정합니다.

예: 명령줄을 사용하여 PMDB 작성

bigcentral 이라는 스테이션이 있다고 가정할 경우, 다른 스테이션이 구독하는 PMDB 를 유지 관리하려고 합니다. PMDB 를 bigcentral 에 작성하려면 sepmdadm 을 실행하십시오. 이 유틸리티는 ACInstallDir/bin 디렉터리에 있습니다.

구독자가 workstat1 및 workstat2 이고 관리자가 adm1 및 adm2 인 pmdb1 이라는 이름의 PMDB 를 bigcentral 에서 작성하려면 bigcentral 에서 다음 명령을 실행하십시오.

```
sepmdadm --pmdname pmdb1 --subscriber workstat1 --subscriber workstat2 \
    --xadmin adm1 --xadmin adm2
```

예: 구독자 스테이션을 PMDB 로 지시

PMDB 에 대한 구독자로 스테이션을 구성하려면 PMDB 스테이션에 구독자 이름을 지정하는 것으로는 부족하고 구독자 스테이션에서 적합한 과정을 수행해야 합니다.

명령줄을 사용하여 로컬 스테이션을 PMDB 에 구독하려면 -subsconfig 매개 변수 외에도 -parentpmd 및 -passwdpmd 매개 변수를 사용해야 합니다.

예를 들어 HOST2 에 위치한 pmdb2 라는 PMDB 와 HOST1 에 위치한 master1 이라는 암호 PMDB 에 로컬 스테이션을 구독하려면 다음 명령을 입력합니다.

```
sepmdadm -subsconfig -parentpmd pmdb2@HOST2 -passwdpmd master1@HOST1
```

sepropadm 유틸리티-데이터베이스 속성 관리

sepropadm 유틸리티는 데이터베이스에 속성을 추가하고 업데이트하며 삭제합니다. CA Access Control 이 실행되지 않는 동안 데이터베이스가 있는 디렉터리에서 이 유틸리티를 호출하십시오. sepropadm 유틸리티는 한 번에 하나의 속성만 추가할 수 있습니다.

중요! 이 유틸리티는 CA Access Control 기술 지원 담당자만 사용하도록 마련된 것입니다. CA Access Control 의 기술 지원 담당자가 인증하지 않은 설명 파일과 함께 sepropadm 유틸리티를 사용하지 마십시오.

이 명령의 형식은 다음과 같습니다.

```
sepropadm file
```

file

CA Access Control 지원 담당자가 제공한 설명 파일을 지정합니다. 설명 파일은 다음과 같은 형식을 사용합니다.

- 해시 기호(#)로 시작되는 한 행이 있어야 하며 설명 행 앞에 나와야 합니다.
- 세미콜론(;)으로 시작되는 라인은 주석으로 처리되지 않습니다.
- 새 이중 연결 OID 를 추가하기 위한 설명 줄은 다음 형식을 준수해야 합니다.

  CLASS=%s PROPERTY=%s TYPE=%d SIZE=%d FLAGES=%x
- 새 속성을 추가하기 위한 설명 줄은 다음 형식을 준수해야 합니다.

  CLASS=%s PROPERTY=%s TYPE=%d SIZE=%d FLAGS=%x LINK2CLASS=%s
- 속성을 삭제하기 위한 설명 줄은 다음 형식을 준수해야 합니다.

  CLASS=%s PROPERTY=%s
- 속성을 변경하기 위한 설명 줄은 다음 형식을 준수해야 합니다.

  CLASS=%s PROPERTY=%s TYPE=%d SIZE=%d FLAGES=%x REPLACE=YES

예: sepropadm 용 설명 파일

다음은 샘플 설명 파일입니다.

```
; Sample Patch File for the CA Access Control database
; Copyright 2004 Computer Associates International, Inc.
; ---------------------------------------------
; DO NOT USE THIS FILE UNLESS YOU KNOW HOW TO!
# seclassadm database add property patch utility
; Format is :
CLASS=PROGRAM PROPERTY=MD5 TYPE=31 SIZE=16 FLAGS=0
```

sepurgdb 유틸리티-정의되지 않은 레코드에 대한 데이터베이스 참조 제거

UNIX 에 해당

sepurgdb 유틸리티는 전체 데이터베이스에서 정의되지 않은 레코드에 대한 참조를 검색한 후 데이터베이스에서 검색된 참조를 삭제하여 데이터베이스 크기를 줄입니다.

중요! 안전을 위해 먼저 데이터베이스를 백업한 후 CA Access Control 데몬이 실행되고 있지 않을 때 이 유틸리티를 호출하십시오.

레코드를 삭제할 때 ACL 이나 그룹 멤버쉽 목록 등의 해당 레코드에 대한 참조는 처리 시간을 줄이기 위해 그대로 유지됩니다. CA Access Control 은 이전에 사용하지 않은 고유 ID 를 새 레코드에 할당하므로 이렇게 해도 문제가 발생하지 않습니다. 이 유틸리티는 디스크 공간을 비우기 위한 용도로만 사용해야 합니다.

sepurgdb 를 실행하려면 root 사용자여야 하며 데이터베이스 파일이 포함된 디렉터리에서 유틸리티를 호출해야 합니다. 데이터베이스 관리 시스템은 미리 할당된 디스크 공간을 사용합니다. 삭제 후에도 데이터베이스 파일의 크기는 일반적으로 크게 변경되지 않습니다. 데이터베이스 크기가 이후에 증가하더라도 사전 할당으로 인해 파일 크기는 크게 변경되지 않습니다.

이 명령의 형식은 다음과 같습니다.

```
sepurgdb FilePath [Username]
```

FilePath

유틸리티 로그 파일의 기본 이름을 지정합니다. sepurgdb 유틸리티는 다음의 두 로그 파일을 생성합니다.

FilePath.err

발생한 오류의 로그가 포함됩니다.

FilePath.log

수행한 작업의 로그가 포함됩니다.

참고: FilePath 에 빼기 기호(-)를 지정하여 두 개의 로그를 병합한 후 표준 출력으로 전송할 수 있습니다.

사용자 이름

(선택 사항) sepurgdb 가 USER 레코드를 위한 그룹 연결의 삭제된 소유자(더 이상 존재하지 않는 사용자)를 대체하기 위해 사용하는 사용자 이름을 지정합니다.

참고: 데이터베이스에 있는 사용자를 지정해야 합니다. 그렇지 않으면 이 옵션은 무시됩니다.

sereport 유틸리티 보고서 구성

sereport 유틸리티는 웹 브라우저에서 액세스할 수 있는 데이터베이스 HTML 보고서 및 정책 모델 정보를 제공합니다. sereport 는 권한 부여 엔진에 의해 사용되는 현재 데이터베이스에서 작동합니다.

유틸리티에 대해 sereport 옵션을 설정할 수 있습니다.

- UNIX 에서 sereport 는 사용자가 -f 옵션을 사용하여 지정한 구성 파일을 사용합니다.

  기본적으로 이 파일은 ACInstallDir/etc/sereport.cfg 입니다.

- Windows 에서 sereport 는 사용자가 구성할 수 있는 레지스트리를 사용합니다. sereport 에 대한 레지스트리 설정은 다음 키 아래에 정의됩니다.

  HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Report

다음 표에서는 생성할 수 있는 보고서, 설명, 해당 구성 파일 설정 또는 레지스트리 키를 보여줍니다.

보고서 번호	제목 및 설명	섹션\하위 키	토큰\항목
1	관리자 권한 사용자의 지정된 관리 권한을 표시합니다.	admin_report	▪ Hostname ▪ Objects_Pattern ▪ Report_place ▪ User_Mode
2	로그인 제한 사용자의 로그인 제한을 표시합니다.	disablelogins_report	▪ Hostname ▪ Objects_Pattern ▪ 속성 ▪ Report_place ▪ User_Mode

보고서 번호	제목 및 설명	섹션\하위 키	토큰\항목
3	유휴 계정 날짜별로 비활성 계정을 표시합니다. 계정에 로그인 정보가 없는 경우 작성 시간을 사용하여 유휴 일 수를 계산합니다.	dormant_report	▪ Hostname ▪ Objects_Pattern ▪ Report_place ▪ Dormant_account
4	마지막 로그인 사용자의 마지막 로그인 날짜를 표시합니다.	login_report	▪ Hostname ▪ Objects_Pattern ▪ Report_place ▪ User_Mode
5	암호 변경 지정한 기간(일) 내에 암호를 변경해야 하는 사용자 목록을 표시합니다.	passwd_report	▪ Days_to_change ▪ Hostname ▪ Objects_Pattern ▪ Report_place ▪ User_Mode
6	경고 모드 개체가 있는 리소스를 경고 모드로 표시합니다.	warning_report	▪ Class_Name ▪ Hostname ▪ Objects_Pattern ▪ Report_place
7	언트러스트된 프로그램 언트러스트된 모드로 프로그램을 표시합니다.	untrust_report	▪ Hostname ▪ Objects_Pattern ▪ Report_place
8	사용자의 액세스 권한 지정된 리소스에 대한 사용자의 액세스 권한을 표시합니다.	accessor_report	▪ 접근자 ▪ Class_Name ▪ Hostname ▪ Objects_Pattern ▪ Report_place
9	데이터베이스의 사용자/그룹 비교 모든 데이터베이스가 아닌 일부 데이터베이스에 정의되는 사용자 및 그룹을 표시합니다.	grp_usr_compare	▪ Hostname ▪ Objects_Pattern ▪ Report_place

보고서 번호	제목 및 설명	섹션\하위 키	토큰\항목
10	보호되는 리소스 비교 리소스가 지정된 데이터베이스에 정의되어 있는지 여부를 표시합니다.	res_compare	▪ Class_Name ▪ Hostname ▪ Objects_Pattern ▪ Report_place
11	액세스 권한 비교 정책 모델과 구독자 데이터베이스 사이에 리소스 제한의 차이점을 표시합니다.	acc_compare	▪ Class_Name ▪ Hostname ▪ Objects_Pattern ▪ Report_place
12	사용자의 정보 비교 정책 모델과 구독자 데이터베이스 사이의 사용자 지정 차이점을 표시합니다.	usr_compare	▪ Hostname ▪ Objects_Pattern ▪ 속성 ▪ Report_place
13	PMDB 와 구독자 비교 PMDB 에 존재하지만 구독자 데이터베이스에는 존재하지 않는 규칙을 Class_Name 및 Object_pattern 토큰에서 정의한 대로 표시합니다. 참고: PMDB 의 모든 규칙이 구독자 데이터베이스에 존재하는 경우 데이터베이스는 IDENTICAL 로 보고됩니다.	pmdb_compare	▪ Class_Name ▪ Hostname ▪ Objects_Pattern ▪ Report_place

Accessor

접근자 선택에 대한 패턴(마스크)을 지정합니다. 모든 접근자를 선택하려면 *를 사용합니다.

Class_Name

클래스 목록을 지정합니다.

Days_to_change

사용자에게 암호를 변경하도록 요청할 때까지 남은 일 수를 지정합니다.

Dormant_account

계정이 유휴 상태인 것으로 간주되는 기간을 지정합니다.

Hostname

데이터가 검색되는 호스트 목록을 지정합니다.

Objects_pattern

개체 선택을 위한 패턴(마스크)을 지정합니다. 모든 개체를 선택하려면 *를 사용합니다.

Properties

개체와 연결된 특성을 지정합니다.

Report_place

(UNIX 전용) 보고서가 인쇄되는 위치의 전체 경로를 지정합니다.

참고: Windows 에서는 명령의 -f 옵션을 사용하여 출력 위치를 정의할 수 있습니다.

User_Mode

사용자 모드 목록을 쉼표로 구분하여 지정합니다.

colors 섹션\키에서 다음의 추가 구성 설정을 찾을 수 있습니다.

title

보고서 제목의 색상을 지정합니다.

class_title

보고서 class_title 의 색상을 지정합니다.

background

(UNIX 전용) 제목 보고서의 배경색을 지정합니다. 배경 및 로고는 전체 경로로 작성되어야 합니다.

logo

로고를 작성합니다. 배경 및 로고는 전체 경로로 작성되어야 합니다.

sereport 유틸리티-UNIX 에서 HTML 보고서 작성

UNIX 에 해당

sereport 유틸리티는 웹 브라우저에서 액세스할 수 있는 데이터베이스 HTML 보고서 및 정책 모델 정보를 작성합니다. sereport 는 권한 부여 엔진에 의해 사용되는 현재 데이터베이스에서 작동합니다.

sereport 를 사용하려면 쿼리된 모든 데이터베이스에서 READ 권한이 필요합니다.

참고: 기본 구성 파일은 ACInstallDir/etc/sereport.cfg 입니다.

이 명령의 형식은 다음과 같습니다.

```
sereport [-f|-file pathname] -r|-report number [-host hostnames]
```

-f | -file pathname

(선택 사항) 구성 파일의 전체 경로를 지정합니다. 파일을 지정하지 않으면 기본 파일인 ACInstallDir/etc/sereport.cfg 가 사용됩니다.

-host hostnames

(선택 사항) 보고할 하나 이상의 호스트 이름을 지정합니다. 호스트를 지정하지 않으면 구성 파일의 호스트가 사용됩니다.

-r | report number

작성할 보고서 수를 지정합니다.

sereport 유틸리티-Windows 에서 HTML 보고서 작성

Windows 에 해당

sereport 유틸리티는 웹 브라우저에서 액세스할 수 있는 데이터베이스 HTML 보고서 및 정책 모델 정보를 작성합니다. sereport 는 권한 부여 엔진에 의해 사용되는 현재 데이터베이스에서 작동합니다.

sereport 를 사용하려면 쿼리된 모든 데이터베이스에서 READ 권한이 필요합니다.

이 명령의 형식은 다음과 같습니다.

```
sereport -f|-file pathname -r|-report number [-host hostnames]
```

-f | -file pathname

출력 파일(보고서)의 전체 경로 이름을 지정합니다.

참고: 지정한 파일의 내용은 HTML 형식으로 구성되므로 자동 파일 연결을 위해 .html 확장자를 지정해야 합니다.

-host hostnames

(선택 사항) 보고할 하나 이상의 호스트 이름을 지정합니다.

호스트를 지정하지 않으면 localhost 가 사용됩니다.

-r | report number

작성할 보고서 수를 지정합니다.

seretrust 유틸리티(UNIX)-프로그램 다시 트러스트 및 파일 보호를 위한 명령 생성

seretrust 유틸리티는 프로그램을 다시 트러스트하고 데이터베이스에 정의된 파일을 보호하기 위해 필요한 selang 명령을 생성합니다. seretrust 유틸리티는 트러스트된 것으로 정의되었지만 그 이후 변경된 SECFILE 및 PROGRAM 리소스의 상태를 보고합니다. seretrust 는 프로그램이 변경되었지만 Watchdog 이 아직 감지하지 못했는지 여부도 검사합니다. 즉, CA Access Control 데이터베이스에서는 이러한 프로그램이 아직도 트러스트된 상태로 표시된다는 의미입니다. 이러한 프로그램은 프로그램 내용 또는 시간 스탬프가 변경되었으며 프로그램이 다시 트러스트되어야 한다는 메모와 함께 seretrust 출력에 추가됩니다.

참고: UNIX 에서 setuid 및 setgid 비트가 포함된 프로그램은 inode 값을 포함한 전체 설명과 함께 데이터베이스에 저장됩니다. 백업에서 시스템을 복원하면 이러한 프로그램은 다른 inode 를 차지합니다. CA Access Control 은 inode 간의 불일치를 검색하고 트러스트된 모든 프로그램을 언트러스트된 상태로 표시합니다. seretrust 유틸리티는 데이터베이스에 정의된 트러스트된 프로그램을 찾아 inode 값을 업데이트함으로써 CA Access Control 을 호출할 때 트러스트된 프로그램이 트러스트된 상태를 유지하도록 합니다.

스위치를 지정하지 않은 경우 언트러스트된 프로그램과 언트러스트된 보안 파일만 처리됩니다.

이 명령의 형식은 다음과 같습니다.

```
seretrust [-a] [-l|-m|-p|-s] path
```

-a

트러스트된 객체와 언트러스트된 객체를 모두 처리합니다.

-h

이 유틸리티에 대한 도움말을 표시합니다.

-l

현재 디렉터리에 있는 데이터베이스에서 프로그램 및 파일에 대한 정보를 추출합니다.

이 옵션을 생략하면 seretrust 는 CA Access Control 이 사용하는 데이터베이스를 처리합니다.

-m

모든 커널 모듈에 대한 서명을 계산합니다. 커널 모듈 레코드의 서명 속성이 유효하지 않으면 seretrust 는 커널 모듈이 트러스트된 상태를 유지하도록 올바른 서명으로 레코드를 업데이트합니다. 서명은 Linux 커널 모듈에 대해서만 사용됩니다.

-p

PROGRAM 클래스의 레코드만 처리합니다.

-s

SECFILE 클래스의 레코드만 처리합니다.

path

다시 트러스트해야 하는 프로그램 및 보안 파일을 검색하기 위한 기본 경로를 지정합니다.

유틸리티는 지정된 디렉터리 및 모든 하위 디렉터리를 처리합니다.

예: 언트러스트된 프로그램 및 보안 파일을 다시 트러스트

다음 예는 seretrust 유틸리티를 사용하여 프로그램 및 보안 파일을 다시 트러스트하는 방법을 보여줍니다.

참고: 다음 예는 UNIX 에서의 샘플 명령 출력을 보여주는 것이지만 Windows 에서도 유틸리티는 동일한 작업을 수행합니다.

프로그램 및 보안 파일을 다시 트러스트하려면 다음 단계를 따르십시오.

1. CA Access Control 데이터베이스 관리자로서 다음 seretrust 명령을 입력합니다.

   ```
   seretrust > retrust_script
   ```

   옵션을 지정하지 않았으므로 유틸리티는 트러스트된 프로그램과 보안 파일을 모두 처리합니다. 또한 기본 경로를 지정하지 않았으므로 루트 경로를 사용합니다.

   seretrust 는 화면에 다음 정보를 표시합니다.

   ```
   Retrusting PROGRAMs & SPECFILEs, Base path = /
   Total of 0 entries retrusted. (Class=SECFILE)
   Total of 16 entities retrusted. (class=PROGRAM)
   ```

   다음은 seretrust 가 작성할 수 있는 스크립트 파일의 내용입니다.

   ```
   chres PROGRAM ("/usr/bin/chgrpmem") trust
   chres PROGRAM ("/usr/bin/chie") trust
   chres PROGRAM ("/usr/bin/crontab") trust
   chres PROGRAM ("/usr/bin/cu") trust
   chres PROGRAM ("/usr/bin/ecs") trust
   chres PROGRAM ("/usr/bin/newgrp") trust
   chres PROGRAM ("/usr/bin/rmquedev") trust
   chres PROGRAM ("/usr/bin/rsh") trust
   chres PROGRAM ("/usr/bin/sysck") trust
   chres PROGRAM ("/usr/bin/uuname") trust
   chres PROGRAM ("/usr/lib/methods/showled") trust
   chres PROGRAM ("/usr/lib/mh/post") trust
   chres PROGRAM ("/usr/lib/mh/slocal") trust
   chres PROGRAM ("/usr/lpp/X11/bin/xlock") trust
   chres PROGRAM ("/usr/lpp/X11/bin/xterm") trust
   chres PROGRAM ("/usr/sbin/chvirprt") trust
   ```

2. 프로그램과 파일을 다시 트러스트하려면 seretrust 가 작성한 selang 스크립트 파일을 실행하십시오.

   ```
   selang -f retrust_script
   ```

serevu 유틸리티-실패한 로그인 시도 처리

UNIX 에 해당

serevu 유틸리티는 지정된 기간 동안 지정한 횟수만큼 로그인에 실패한 사용자를 처리합니다. 지정한 사양에 따라 사용자를 비활성화하거나 기록 또는 무시할 수 있습니다. 기본적으로 이 유틸리티는 로컬 스테이션의 UNIX 환경에 있는 사용자를 비활성화합니다. 이러한 사용자가 로컬에 존재하지 않는 경우 serevu 는 NIS 정보를 확인하여 사용자를 찾습니다.

passwd_pmd 구성 설정에 값을 설정한 경우 CA Access Control 은 적절한 PMDB 를 업데이트합니다. 그러면 PMDB 는 해당 구독자에게 업데이트를 전파합니다. passwd_pmd 토큰에 값을 설정하지 않은 경우 CA Access Control 은 parent_pmd 구성 설정의 값을 사용합니다. 그러면 구성 설정은 해당 구독자에게 업데이트를 전파합니다.

참고: serevu 유틸리티가 제대로 작동하려면 사용자 root 에게 /etc/passwd 파일에 대한 쓰기 액세스 권한이 있어야 합니다. serevu 구성 파일에서 원격 컴퓨터를 정의할 경우 원격 컴퓨터에 대한 로그인 권한도 부여해야 합니다.

이 명령의 형식은 다음과 같습니다.

```
serevu {daemon|nodeamon} [-f nn] \
    [-d {nn[S|m|h|d|w]|FOREVER}] \
    [{-s|-t} nn[S|m|h|d|w]]
```

daemon

유틸리티를 데몬으로 실행합니다. 이것이 기본값입니다.

nodaemon

유틸리티를 일반 프로세스로 실행합니다.

-d

사용자 로그인이 비활성화되는 기간을 지정합니다. 기본적으로 이 값은 초 단위입니다.

참고: 사용자 계정이 비활성화되는 기간은 각 serevu 스캔 간격과 같거나 그 이상이어야 합니다. 사용자 계정이 비활성화되는 기간은 각 serevu 스캔 간격의 배수여야 합니다.

-f

실패한 로그인 횟수를 지정합니다. serevu 유틸리티는 지정한 기간 동안 이 횟수의 로그인 시도에 실패한 사용자 계정을 비활성화합니다.

참고: 실패한 로그인의 횟수(def_fail_count 구성 설정의 값으로도 정의 가능)는 항상 시스템에 설정된 실패한 로그인 시도 허용 값과 동일하게 지정하는 것이 좋습니다. 예를 들어, Solaris 에서는 이에 대한 시스템 값이 RETRIES 에 의해 /etc/default/login 에 설정됩니다. 자세한 내용은 해당 운영 체제 설명서를 참조하십시오.

-h

이 유틸리티에 대한 도움말을 표시합니다.

-s

now 에서 시작하여 뒤로 가도록 기간을 지정합니다. serevu 는 이 기간 내에 실패한 로그인을 검색합니다.

기본값: 300 초(구성 설정).

-t

연속적인 serevu 검사 사이에 필요한 기간을 지정합니다.

기본값: 120 초(구성 설정).

FOREVER

-d 옵션과 함께 사용하면 시간을 무제한으로 지정합니다. 이 매개 변수를 사용하는 경우 사용자 로그인이 영구적으로 비활성화됩니다.

nn[s|m|h|d|w]

-d, -s 및 -t 옵션과 함께 사용하면 옵션에 대한 시간을 지정합니다.

s

nn - 초(기본값).

m

nn - 분.

h

nn - 시간.

d

nn -일.

w

nn -주.

sessfgate 유틸리티-Unicenter Security 요청을 CA Access Control 로 라우팅

Unicenter Security API 를 메시지 큐에서 CA Access Control 로 라우팅하고 형식을 변경합니다. UNIX 의 Unicenter Security API 는 모두 메시지 큐로 전달됩니다. sessfgate 유틸리티는 메시지 큐를 통해 전송된 API 요청을 처리하고, 형식이 다시 지정되었거나 다시 라우팅된 요청을 CA Access Control 로 라우팅합니다. 그런 다음 CA Access Control 의 반환 코드를 Unicenter TNG 코드로 변환합니다.

게이트웨이를 활성화하려면 Unicenter 통합 설치 과정을 실행해야 합니다. Unicenter 통합을 설치하면 ACInstallDir/tng/bin 디렉터리에 sessfgate 프로그램이 설치됩니다. 여기서 ACInstallDir 은 CA Access Control 을 설치한 디렉터리입니다(기본적으로 /opt/CA/AccessControl). Unicenter Security 가 종료되고 CA Access Control 이 시작되면 sessfgate 는 SSF 대신 API 요청을 승인합니다.

이 명령의 형식은 다음과 같습니다.

```
sessfgate [-i|-s|-l] -t
```

-I

게이트웨이를 시작하도록 지정합니다.

-s

게이트웨이를 중지하도록 지정합니다.

-l

상태를 지정합니다.

-t

추적 파일(로그 파일 = /opt/CA/AccessControl/log/sessftrace.log)을 실행하거나 실행하지 않습니다.

참고: Unicenter TNG 를 실행하기 전에 seload 를 실행할 경우 다음 명령을 사용하여 sessfagte 를 수동으로 시작해야 합니다.

```
ACInstallDir/tng/bin/sessfagte -I
```

여기서 ACInstallDir 은 CA Access Control 을 설치한 디렉터리입니다.

sesu 유틸리티 - 사용자 전환

sesu 유틸리티를 사용하면 임시로 다른 사용자로 전환할 수 있습니다. 이 유틸리티는 UNIX su 명령의 CA Access Control 버전입니다. 하지만 sesu 유틸리티를 사용하면 대상 사용자의 암호를 입력하지 않고도 사용자를 전환할 수 있습니다. 권한 부여 프로세스는 SURROGATE 클래스에 정의된 CA Access Control 액세스 규칙 및 (선택적으로) 명령을 실행하는 사용자의 암호에 기반합니다.

sesu 유틸리티는 seos.ini 파일의 sesu 섹션에 있는 토큰을 사용합니다. 이 유틸리티는 또한 다음의 특수 파일을 사용합니다.

- /etc/passwd
- /etc/group
- /etc/shells

부주의한 사용을 방지하기 위해 파일 시스템에서 sesu 는 누구도 실행할 수 없도록 설정되어 있습니다. 이 프로그램을 사용하려면 보안 관리자가 프로그램을 실행할 수 있도록 설정하고 setuid 를 root 로 설정해야 합니다.

중요! sesu 유틸리티를 사용하기 전에 모든 사용자를 CA Access Control 데이터베이스에 정의하고 sesu 사전 요구 사항을 설정하십시오. 이렇게 하면 CA Access Control 에 정의되지 않은 사용자에게 전체 시스템이 개방되는 사고를 방지할 수 있습니다.

참고:

- CA Access Control 권한 부여 서버를 찾을 수 없으면 이 유틸리티는 시스템의 표준 su 명령을 실행합니다.
- sesu.old_sesu 구성 토큰이 'no'로 설정되면 이 유틸리티는 시스템의 표준 su 명령을 실행합니다.
- /etc/shells 가 있지만 현재 셸을 정의하지 않는 경우 sesu 는 root 로의 대체를 허용하지 않습니다.

이 유틸리티의 형식은 다음과 같습니다.

```
sesu [-] [username] [-l] [-s shell] [-c command]
```

-

환경을 대상 사용자의 환경으로 설정합니다.

참고: 이 옵션은 Linux 의 -l 옵션과 동일합니다.

-c command

지정된 명령을 실행한 후 종료됩니다.

명령에 공백이 포함되는 경우 명령을 인용 부호로 묶으십시오.

-h

이 유틸리티에 대한 도움말을 표시합니다.

-l

(Linux 만 해당). 여는 셸을 로그인 셸로 지정합니다.

-s shell

(Linux 만 해당). 사용자의 암호 입력으로 열리는 셸 대신 다른 셸이 열리도록 합니다.

이 셸은 /etc/shells 파일에 지정되어 있어야 합니다.

username

세션과 연결된 ID 를 지정된 대상 사용자 username 의 ID 로 변경합니다.

username 을 지정하지 않으면 sesu 는 기본적으로 root 로 변경합니다.

예제

- 다음 명령은 UID 를 root 로 변경합니다. 환경은 명령을 실행한 사용자의 환경으로 유지됩니다.

  ```
  sesu
  ```

- 다음 명령은 UID 를 root 로 변경합니다. 이 유틸리티는 환경을 root 의 환경으로 변경합니다.

  ```
  sesu -
  ```

- 다음 명령은 사용자 John 으로 전환합니다.

  ```
  sesu John
  ```

- 다음 명령은 사용자 Carol 을 서로게이트하고 /home/carol 디렉터리에서 지정된 명령(ls -la)을 실행합니다.

  ```
  sesu - Carol -c "ls -la /home/carol"
  ```

- 다음 명령은 사용자 Angelo 로 전환하고 bash 셸을 사용하며, 이 셸을 로그인 셸로 엽니다.

  ```
  sesu Angelo -l -s /bin/bash
  ```

  참고: 이 명령은 Linux 에서만 유효합니다.

sesudo 유틸리티

sesudo 유틸리티는 다른 사용자의 권한으로 사용자 한 명에 대한 명령을 실행합니다. 이를 통해 관리자 권한이 필요한 작업을 일반 사용자가 수행할 수 있습니다.

이런 방식으로 명령 실행에 대한 사용자 권한을 관리하는 규칙은 SUDO 클래스의 액세스 규칙으로 정의되어 있습니다. SUDO 클래스의 레코드에는 명령 스크립트가 있으며 sesudo 로 해당 스크립트를 실행할 수 있는 사용자와 실행할 수 없는 사용자를 모두 지정할 수 있습니다.

sesudo 유틸리티-UNIX 에서 다른 사용자로서 명령 실행

UNIX 에 해당

sesudo 유틸리티는 다른 사용자의 권한으로 사용자 한 명에 대한 명령을 실행합니다. sesudo 유틸리티는 다른 사용자(대상 사용자)의 권한을 빌려 한 개 이상의 명령을 실행합니다. 이 유틸리티를 통해 일반 사용자는 mount 명령과 같은 슈퍼 사용자 권한이 필요한 작업을 수행할 수 있습니다.

이런 방식으로 명령 실행에 대한 사용자 권한을 관리하는 규칙은 SUDO 클래스의 액세스 규칙으로 정의되어 있습니다. SUDO 클래스의 레코드에는 명령 스크립트가 있으며 sesudo 로 해당 스크립트를 실행할 수 있는 사용자와 실행할 수 없는 사용자를 모두 지정할 수 있습니다.

sesudo 가 실행될 때마다 다음 값 중 하나를 반환합니다.

-2

대상 사용자가 없거나 명령이 중단됨

-1

암호 오류

0

실행 성공

10

매개 변수 사용 관련 문제

11

syscall 이 로드되지 않았습니다.

20

대상 사용자 오류

22

syscall 이 로드되었지만 데몬이 실행되고 있지 않습니다.

30

권한 부여 오류

이 명령의 형식은 다음과 같습니다.

```
sesudo {-h|-list|record [params]}
```

-h

도움말 화면을 표시합니다.

-list

실행 가능한 sesudo 명령을 나열합니다. 이는 CA Access Control 데이터베이스에 정의된, 실행 권한이 있는 SUDO 레코드입니다.

record

sesudo 유틸리티를 사용해 실행하려는 명령에 대해 보안 관리자가 제공한 SUDO 클래스 레코드의 이름을 지정합니다.

params

(선택 사항) 실행 중인 명령에 보내려는 매개 변수를 지정합니다.

sesudo 유틸리티-Windows 에서 다른 사용자로서 명령 실행

Windows 에 해당

sesudo 유틸리티는 다른 사용자의 권한으로 사용자 한 명에 대한 명령을 실행합니다. sesudo 유틸리티는 다른 사용자(대상 사용자)의 권한을 빌려 한 개 이상의 명령을 실행합니다. 이 유틸리티를 통해 일반 사용자는 mount 명령과 같은 슈퍼 사용자 권한이 필요한 작업을 수행할 수 있습니다.

이런 방식으로 명령 실행에 대한 사용자 권한을 관리하는 규칙은 SUDO 클래스의 액세스 규칙으로 정의되어 있습니다. SUDO 클래스의 레코드에는 명령 스크립트가 있으며 sesudo 로 해당 스크립트를 실행할 수 있는 사용자와 실행할 수 없는 사용자를 모두 지정할 수 있습니다.

이 명령의 형식은 다음과 같습니다.

```
sesudo {-h|-list|-do record [params]}
```

-h

도움말 화면을 표시합니다.

-list

실행 가능한 sesudo 명령을 나열합니다. 이는 CA Access Control 데이터베이스에 정의된, 실행 권한이 있는 SUDO 레코드입니다.

-do record [params]

sesudo 가 다른 사용자로서 명령을 실행하도록 지정합니다.

record

sesudo 유틸리티를 사용해 실행하려는 명령에 대해 보안 관리자가 제공한 SUDO 클래스 레코드의 이름을 지정합니다.

params

(선택 사항) 실행 중인 명령에 보내려는 매개 변수를 지정합니다.

seuidpgm 유틸리티-트러스트된 프로그램 추출

UNIX 에 해당

seuidpgm 유틸리티는 Set-User-ID 비트 또는 Set-Group-ID 비트가 설정된 모든 프로그램을 추출합니다. seuidpgm 은 파일 시스템을 탐색하고 PROGRAM 클래스에 이 프로그램을 추가하기 위해 selang 명령을 작성합니다.

seuidpgm 은 selang 명령 언어의 명령을 생성하고 표준 출력에 씁니다. selang 유틸리티에 대한 파이프라인을 사용하거나 출력을 파일로 리디렉션할 수 있습니다. 출력을 편집하여 원치 않는 프로그램을 제거하거나 다른 프로그램을 추가할 수 있으므로 출력을 파일로 리디렉션하는 것이 좋습니다. 시스템에서 원치 않는 setuid 프로그램을 검색하려면 이 절차를 사용하십시오.

참고: seuidpgm 유틸리티를 실행하기 전에 UxImport 유틸리티를 실행하여 사용자 및 그룹을 정의하는 것이 좋습니다. 그러나 UxImport 를 실행하지 않은 경우 -g 옵션 및 -u 옵션과 seuidpgm 를 함께 사용하여 사용자 및 그룹을 정의할 수 있습니다.

seuidpgm 은 명령줄에 지정된 경로를 통해 시작 경로의 모든 하위 디렉터리로 이동하여 실행됩니다. 여러 개의 시작 경로를 사용할 수 있습니다.

원하는 개수의 옵션을 지정할 수 있습니다. 둘 이상의 옵션을 지정하는 경우 공백으로 옵션을 구분하십시오.

프로그램이 setuid 프로그램이고 쓰기 액세스를 가진 경우 seuidpgm 은 프로그램을 다른 모든 setuid 프로그램처럼 처리하지만 표준 오류로 경고를 전송합니다.

참고: PROGRAM 클래스 레코드 제어 방법에 대한 자세한 내용은 UNIX 용 끝점 관리 안내서를 참조하십시오.

이 명령의 형식은 다음과 같습니다.

```
seuidpgm option startDir ... [-x excludeDir]
```

-d

UNIX 의 파일 권한을 분석하여 허용된 파일 액세스 권한을 확인하는 대신 defaccess 를 EXEC 으로 설정하여 PROGRAM 클래스에 setuid 및 setgid 프로그램에 대한 항목을 자동으로 생성합니다. 특정 setuid 또는 setgid 프로그램이 다른 프로그램을 실행하는 경우도 있습니다. 이 옵션을 포함하지 않으면 프로그램이 setuid 또는 setgid 프로그램을 실행하려고 해도 실행할 수 없습니다.

이 옵션을 사용하는 것이 좋습니다.

-f

FILE 클래스와 PROGRAM 클래스 둘 다에 대한 규칙을 생성합니다.

-g

setgid 프로그램에 대한 GROUP 레코드를 생성합니다.

참고: UxImport 를 실행하지 않은 경우에만 이 옵션을 사용하십시오.

-l

하드 링크 또는 심볼 링크가 있는 프로그램에 대해 단일 허용을 작성합니다.

root 디렉터리가 아닌 일부 디렉터리에서만 파일 시스템을 스캔하고 -l 옵션을 포함하려면 명령행에서 여러 시작 경로를 사용하십시오. 그렇지 않으면 -l 옵션이 무효가 될 수 있습니다.

-n

NFS 를 통과하지 않습니다.

이 옵션을 사용하는 것이 좋습니다.

-o

파일 이름을 표준 출력에 쓰지만 selang 명령을 생성하지는 않습니다.

-p

마운트 테이블에서 마운트된 파일 시스템의 setuid 를 허용하는 경우에만 NFS 디렉터리의 setuid 프로그램을 활성화합니다.

-q

자동 모드로 유틸리티를 실행합니다. 오류 메시지가 표준 오류로 전송되지 않습니다.

-s

PROGRAM 클래스의 항목을 생성하는 대신 SECFILE 클래스에 setuid/setgid 프로그램에 대한 항목을 생성합니다.

-u

setuid 프로그램에 대한 USER 레코드를 생성합니다.

참고: UxImport 를 실행하지 않은 경우에만 이 옵션을 사용하십시오.

-x excludeDir

트리에서 디렉터리를 제외합니다. 지정된 디렉터리는 setuid 및 setgid 프로그램을 검색하지 않습니다. 이 옵션은 명령줄에 지정된 마지막 옵션이어야 합니다. path 는 제외할 디렉터리의 전체 경로입니다. 둘 이상의 디렉터리를 제외하려면 각 디렉터리에 대해 -x 옵션을 반복하십시오.

startDir

트러스트된 프로그램을 검색할 상위 디렉터리의 목록을 공백으로 구분하여 지정합니다.

예제

- 다음 명령은 set-user-id 또는 set-group-id 가 설정된 상태에서 모든 프로그램을 추가하는 selang 명령을 인쇄하고, defaccess 실행 권한으로 NFS 를 경유하지 않고 자동 모드에서 중복된 이름이나 동일한 inode 를 검사합니다. 프로그램은 /usr 디렉터리와 해당 하위 디렉터리, /var 디렉터리와 해당 하위 디렉터리, /etc 디렉터리와 해당 하위 디렉터리에서 스캔합니다. 출력은 홈 디렉터리의 seprogs.seos 파일로 전송됩니다.

```
seuidpgm -dlqn /usr /var /etc > ~/seprogs.seos
```

출력 형식은 다음과 유사해야 합니다.

```
## ************************************************
## seuidpgm List Sun Feb 9 14:24:16 1997
# Start Path= /usr
# ************************************************
nr PROGRAM /usr/lpp/bos/inst_root/lpp/inu_LOCK defaccess(EXEC)
nr PROGRAM /usr/lpp/X11/bin/xlock defaccess(EXEC)
nr PROGRAM /usr/bin/setsenv defaccess(EXEC)
nr PROGRAM /usr/bin/shell defaccess(EXEC)
nr PROGRAM /usr/bin/su defaccess(EXEC)
nr PROGRAM /usr/bin/sysck defaccess(EXEC)
nr PROGRAM /usr/bin/tcbck defaccess(EXEC)
nr PROGRAM /usr/bin/usrck defaccess(EXEC)
nr PROGRAM /usr/bin/vmstat defaccess(EXEC)
```

- 다음 명령은 /home 디렉터리를 제외한 모든 하위 디렉터리와 root 디렉터리를 스캔합니다.

  ```
  seuidpgm -qln / -x /home
  ```

추가 정보:

UxImport 유틸리티-UNIX 운영 체제에서 정보 추출 (페이지 227)
selang 유틸리티-CA Access Control 명령줄 실행 (페이지 162)
seoswd Daemon (페이지 249)
seosd 데몬 (페이지 243)

seversion 유틸리티-CA Access Control 프로그램 모듈 버전 정보 표시

UNIX 에 해당

seversion 유틸리티는 CA Access Control 모듈의 버전과 관련된 정보를 표시합니다. 다음 데이터를 표시할 수 있습니다.

- 전역 및 마이너 버전 번호
- 모듈이 컴파일된 날짜 및 시간
- 모듈이 컴파일된 스테이션

이 명령의 형식은 다음과 같습니다.

```
seversion [-a|-l|-g|-h|-m|-s|-5] module
```

-a

요청된 정보를 테이블 형식으로 표시합니다.

-g

제목을 생략하고 전역 버전 번호만 표시합니다.

-h

이 유틸리티에 대한 도움말을 표시합니다.

-l

포함된 라이브러리 정보를 표시합니다.

-m

제목을 생략하고 보조 버전 번호만 표시합니다.

-s

SHA1 서명을 표시하고 제목은 생략합니다.

-5

제목을 생략하고 MD5 서명을 표시합니다.

이 옵션은 FIPS 전용 모드가 아닌 동안에만 적용됩니다.

모듈

버전 번호를 표시할 모듈의 파일 이름을 지정합니다.

예제

sesudo 유틸리티의 버전 정보를 표시하려면 다음 명령을 입력합니다.

```
seversion /opt/CA/AccessControl/bin/seosd
```

FIPS 모드가 아닌 동안 다음과 유사한 메시지가 화면에 나타납니다.

```
CA Access Control seversion vX.X.X.xxx - Display module's version
Copyright (c) YYYY CA. All rights reserved.
Running under: Linux
File name: /opt/CA/AccessControl/bin/seosd
Version  : major.minor.sp.build
Created  : MMM DD YYYY hh:mm:ss
OS info  : i86PC
SHA1     : 10068CC6A70195B84AF896682CCBA1A4B7B43CD1
MD5:     : 1F9BD56CA523A33FFBC47551ECE093E5
```

sewhoami 유틸리티 - UNIX 에서 CA Access Control 사용자 이름 및 보안 자격 증명 표시

UNIX 에 해당

sewhoami 유틸리티는 CA Access Control 권한 부여 데몬에 알려진 대로 사용자 이름을 표시합니다. sewhoami 는 UNIX 시스템에서 제공하는 whoami 유틸리티와 유사하지만 표시하는 정보는 다르며 종종 더 유용합니다.

- 사용자가 su 명령을 실행하고 UNIX whoami 유틸리티를 실행할 경우 su 명령을 실행한 후 획득한 사용자 ID 에 따라 사용자 이름을 표시합니다.
- 사용자가 su 명령을 실행한 후 CA Access Control sewhoami 유틸리티를 실행하면 해당 사용자의 원래 로그인 ID 가 표시되며 권한 부여 정보도 표시됩니다.

이 명령의 형식은 다음과 같습니다.

```
sewhoami [-a|-d]
```

-a

사용자의 자격 증명, 즉 사용자 ACEE 의 내용을 표시합니다.

참고: ACEE 에 대한 자세한 내용은 UNIX 용 끝점 관리 안내서를 참조하십시오.

-d

사용자와 연결된 ACEE 핸들과 데이터베이스에 있는 해당 핸들의 이름을 표시합니다.

예: UNIX 에서 CA Access Control 사용자 이름 및 보안 자격 증명 표시

다음 예는 CA Access Control 권한 부여 데몬에 알려진 대로 사용자 이름 및 보안 자격 증명을 표시합니다.

```
sewhoami -a
```

루트 사용자인 경우 sewhoami 출력은 다음 예와 유사합니다.

```
root
ACEE 콘텐츠
 사용자 이름 : root
 ACEE 핸들 : 52
 그룹 연결 테이블:
 그룹 이름 연결 모드
 ================== ==============================
 adm 일반
 bin 일반
 daemon 일반
 disk 일반
 root 일반
 seosaudt 일반
 sys 일반
 wheel 일반
범주 : <없음>
프로필 그룹 : <없음>
보안 레이블 : <없음>
사용자의 감사 모드 : Failure LoginSuccess LoginFailure
사용자의 보안 수준 : 0
원본 터미널 : <알 수 없음>
ACEE 의 프로세스 개수 : 19
사용자 모드 : 관리 감사자
ACEE 의 작성 시간 : 화 5 월 17 14:53:07 2009
```

사용자 이름이 "test"이고 루트 사용자가 아닌 경우 sewhoami 출력은 다음 예와 유사합니다.

```
test
ACEE 콘텐츠
 사용자 이름 : test
 ACEE 핸들 : 65
 그룹 연결 테이블:
 그룹 이름 연결 모드
 ================== ==============================
 seosaudt 일반
 사용자 일반
범주 : <없음>
프로필 그룹 : secadmin
보안 레이블 : <없음>
사용자의 감사 모드 : Failure LoginSuccess LoginFailure
사용자의 보안 수준 : 0
원본 터미널 : localhost.localdomain
ACEE 의 프로세스 개수 : 2
사용자 모드 : 관리 감사자
ACEE 의 작성 시간 : 수 5 월 18 15:34:53 2009
```

추가 정보:

secons -whoami 함수 - 사용자 이름 및 보안 자격 증명 표시 (페이지 149)

uninstall_AC 유틸리티-원격 컴퓨터에서 CA Access Control 제거

UNIX 에 해당

uninstall_AC 유틸리티는 명령을 실행하는 스테이션에서 CA Access Control 의 전부 또는 일부를 제거합니다. 기본값(-all)은 스테이션에서 전체 제품을 제거합니다.

참고: 제거하기 전에 CA Access Control 커널 확장을 언로드해야 합니다.

이 명령의 구문은 다음과 같습니다.

```
uninstall_AC [-all | -admin] [-f] [-force] [-h] [-ignore_dep] [-d path] [-fn file]
```

-admin

스테이션에서 Security Administrator 및 seauditx 와 같은 관리 도구만 제거합니다.

참고: 이제 admin 패키지는 CA Access Control 에 포함되어 있지 않습니다. 이 옵션은 CA Access Control 의 이전 버전을 제거하는 데 사용됩니다.

-all

스테이션에서 전체 제품을 제거합니다.

-d path

CA Access Control 이 설치된 디렉터리를 정의합니다.

참고: CA Access Control 이 기본 디렉터리(/opt/CA/AccessControl)에 설치되어 있으면 이 옵션을 지정할 필요가 없습니다.

-f

CA Access Control 을 자동 모드에서 제거합니다.

-fn file

제거가 완료된 후 지정된 파일을 실행합니다.

-force

커널 확장 언로드 프로세스가 실패하더라도 강제로 제거를 수행합니다.

-h

이 유틸리티에 대한 도움말을 표시합니다.

-ignore_dep

제거 중에 다른 제품과의 종속성을 검사하지 않도록 지정합니다.

예: 컴퓨터에서 CA Access Control 을 완전히 제거

이 컴퓨터에서 CA Access Control 을 완전히 제거하려면(기본 디렉터리에 설치된 경우) 다음 명령을 입력합니다.

```
uninstall_AC
```

uxconsole -manage - 사용자 및 그룹 관리

UNIX 에 해당

로컬 또는 엔터프라이즈 사용자 및 그룹의 정보를 나열, 표시, 편집하려면 이 명령을 사용하십시오.

이 명령의 형식은 다음과 같습니다.

```
uxconsole -manage -find {-user|-group} filter

uxconsole -manage -show {-user|-group} filter

uxconsole -manage -edit -a admin -w password -user name [-uid uid] [-gid gid] [-gecos
gecos] [-homedir dir] [-login shell]
```

```
uxconsole –manage –edit –a admin -w password –group name [-gid gid] [-gecos gecos]
[-members list]
```

-find

로컬 및 엔터프라이즈 사용자 또는 그룹의 목록을 표시하도록 지정합니다.

-show

특정 계정 또는 그룹의 세부 정보를 표시하도록 지정합니다.

-edit

계정 또는 그룹을 편집하도록 지정합니다.

filter

사용자 또는 그룹의 하위 집합을 반환하는 와일드카드를 정의합니다.

-a admin

관리자 계정의 이름을 정의합니다.

-w pass

관리자 계정의 암호를 정의합니다.

-user

편집할 사용자 계정을 정의합니다.

-group

편집할 그룹을 정의합니다.

-uid

사용자 계정 UID 를 지정합니다.

-gid

그룹 UID 를 지정합니다.

-gecos

사용자에 대한 일반 설명(예: 사용자의 전체 이름)을 포함하는 문자열을 정의합니다.

-homedir

UNIX 컴퓨터에서 계정 홈 디렉터리를 정의합니다.

-login

계정 로그인 셸을 정의합니다.

-members

그룹 구성원 목록 이름을 정의합니다.

uxconsole -migrate - UNIX 사용자 및 그룹을 Active Directory 로 마이그레이션

UNIX 에 해당

이 migrate 명령을 사용하여 UNIX 호스트에서 Active Directory 로 사용자 및 그룹을 마이그레이션합니다. 마이그레이션 프로세스는 로컬 사용자와 그룹을 Active Directory 로 마이그레이션한 다음 로컬 계정을 비활성화하려고 시도합니다.

이 명령의 형식은 다음과 같습니다.

```
uxconsole -migrate -scope {l|n|a} [-users] [-groups] {-mode {p|f} | -input file}
[-emulate] [-admin name -pw passwd] [-v {number}]
```

-migrate

UNIX 사용자 마이그레이션 옵션을 정의합니다.

-scope l|n|a

마이그레이션 범위를 지정합니다.

- l - 로컬 사용자와 그룹만 마이그레이션합니다.
- n - NIS\NIS+ 서버에서 NIS 사용자와 그룹을 마이그레이션합니다.
- a - 로컬 및 NIS/NIS+ 사용자와 그룹을 마이그레이션합니다.

기본값: l

-user

(선택 사항) 사용자만 Active Directory 로 마이그레이션되도록 지정합니다.

참고: 지정하지 않으면 사용자는 Active Directory 로 마이그레이션되지 않습니다.

-group

(선택 사항) 그룹만 Active Directory 로 마이그레이션되도록 지정합니다.

참고: 지정하지 않으면 그룹은 Active Directory 로 마이그레이션되지 않습니다.

-mode p|f

마이그레이션 모드를 지정합니다.

옵션: partial, full

기본값: f

-input file

계정 맵 파일의 전체 경로를 정의합니다.

참고: 마이그레이션 프로세스 중 발견된 사용자 계정의 충돌을 해결하려면 매핑 파일을 사용하십시오. 다음 필드 및 매개 변수를 사용하여 CSV 형식으로 맵 파일을 만드십시오.

유형 <USER|GROUP>, UNIX 이름 <사용자 이름>, 필요한 작업 <KEEPLOCAL|MIGRTE|MAP>, AD 이름 <AD 매핑된 이름>

예: 유형-user, UNIX 이름- uxuser, 필요한 작업- migrate, AD 이름- aduser

-emulate

마이그레이션 프로세스가 에뮬레이션 모드에서 실행되도록 지정합니다.

참고: 에뮬레이션 모드에서 uxconsole -migrate 명령을 실행하면 사용자가 Active Directory 로 마이그레이션되지 않습니다. 에뮬레이션 모드에서 uxconsole 은 사용자 및 그룹 ID 의 가능한 충돌에 대해 보고하는 저널 파일을 만듭니다. UNIX 와 Active Directory 사용자 및 그룹 ID 사이의 충돌을 해결하려면 에뮬레이션 모드를 사용하십시오.

-admin name

Active Directory 에서 사용자 속성을 등록하고, 만들고, 업데이트하는 데 사용된 Active Directory 관리자를 지정합니다.

참고: 관리자 자격 증명을 제공하지 않고 -migrate 명령을 실행하면 UNAB 가 UNIX 특성을 추가하지 않으며 Active Directory 에 계정 또는 그룹을 추가하지 않습니다. Active Directory 관리자 자격 증명을 제공하지 않으면 마이그레이션 중에 발견된 충돌을 해결할 수 없습니다.

-w passwd

Active Directory 관리자의 계정 암호를 지정합니다.

-v number

세부 정보 표시 수준을 지정합니다.

범위: 1-5

기본값: 5

uxconsole -register - Active Directory 에 UNIX 컴퓨터 등록

UNIX 에 해당

이 명령을 사용하여 Active Directory 에 UNIX 호스트를 등록합니다. 이렇게 하면 UNAB 구성 프로세스를 완료하고 Active Directory 사용자 계정을 사용하여 UNIX 호스트에 로그인할 수 있습니다.

Active Directory 를 사용하는 경우 컴퓨터 개체의 이름에 포함된 문자 수에 NetBIOS 기반 제한이 있으므로 도메인 이름 접미사를 제외한 UNIX 컴퓨터의 호스트 이름은 15 자 이하여야 합니다. UNIX 컴퓨터의 호스트 이름에 포함된 문자가 15 자를 초과하는 경우 등록이 실패합니다. 예를 들어, UNIX 컴퓨터 이름 engineering-dept-sol2 는 15 자보다 많은 문자를 포함하므로 이 호스트 이름을 등록할 수 없습니다. UNIX 컴퓨터 이름 eng-dept-sol2.example.com 은 도메인 이름(eng-dept-sol2)을 제외한 호스트 이름에 15 미만의 문자가 포함되어 있으므로 이 호스트 이름을 등록할 수 있습니다. UNIX 컴퓨터의 호스트 이름을 표시하려면 hostname 명령을 실행하십시오.

참고: 동일한 컴퓨터에 이 명령을 여러 번 실행할 수 있습니다. 예를 들어, keytab 파일이 삭제된 경우 Active Directory 에 대한 UNAB 호스트 등록을 복원하기 위해 이 명령을 실행할 수 있습니다.

이 명령의 형식은 다음과 같습니다.

```
uxconsole {-register | -unregister} [-a admin] [-w pass] [-d domain] [-v level] [-n]
[-o container] [-s server] [port #] [-h]
```

-register

Active Directory 가 UNAB 를 등록하도록 지정합니다.

-unregister

Active Directory 가 UNAB 의 등록을 취소하도록 지정합니다.

-a admin

관리자 계정 이름을 정의합니다.

-w pass

관리자 계정 암호를 정의합니다.

-d domain

Active Directory 가 속한 도메인 이름을 정의합니다.

-v level

설치 중 사용할 세부 정보 표시 수준을 정의합니다.

-n

설치 과정의 끝에 uxauthd 에이전트를 실행할지 여부를 지정합니다.

-o container

UNIX 컴퓨터가 등록되는 Active Directory 컨테이너 이름을 정의합니다.

-s server

Active Directory 서버 이름을 정의합니다.

-port #

Active Directory 수신 대기 포트 번호를 정의합니다.

-h

프로그램 도움말을 표시합니다.

UxImport 유틸리티-UNIX 운영 체제에서 정보 추출

UNIX 에 해당

uximport 유틸리티는 정의된 사용자, 그룹, 터미널, 호스트 및 TCP 서비스에 대한 정보를 UNIX 운영 체제에서 추출합니다. NIS 가 설치되어 있으며 시스템이 올바르게 구성된 경우 NIS 에서 정보를 추출합니다. 또한 DNS 지원도 제공합니다. 설치 과정 중에 uximport 를 사용해야 합니다.

uximport 는 추출된 정보를 자동으로 처리하여 사용자와 그룹을 CA Access Control 데이터베이스에 추가하는 데 사용할 수 있는 selang 명령을 생성합니다. 생성된 명령은 표준 출력에 인쇄됩니다. 파일로 리디렉션 또는 selang 유틸리티에 대한 파이프라인을 사용합니다.

이 명령의 형식은 다음과 같습니다.

```
UxImport switches [options]
```

-a

사용자, 그룹 및 호스트를 가져오고 사용자를 기본 그룹에 포함시키는 데 필요한 selang 명령을 생성합니다.

-c

사용자를 기본 그룹에 명시적으로 포함시키는 데 필요한 selang 명령을 생성합니다.

참고: -g 스위치를 사용하여 그룹을 가져올 경우에도 CA Access Control 는 명시적으로 링크된 그룹에 사용자를 조인하는 명령을 생성합니다.

-g

UNIX 및 NIS 의 그룹을 CA Access Control 데이터베이스로 가져오는 데 필요한 selang 명령을 생성합니다.

-h

UNIX, NIS 및 DNS 의 호스트를 CA Access Control 데이터베이스로 가져오는 데 필요한 selang 명령을 생성합니다. uximport 는 /etc/hosts 파일과 NIS 에서 호스트 정보를 추출하고 HOST 리소스를 작성합니다. /etc/hosts 파일 또는 NIS 에서 추출된 각 호스트 항목에 대해 적합한 newres 명령이 작성되고 TCP 서비스를 수신할 수 있는 권한이 해당 호스트에 할당됩니다.

또한 DNS 는 -d 옵션과 함께 지원됩니다. 일부 컴퓨터에서 지정된 DNS 데몬이 실행 중인 경우 /etc/hosts 파일과 NIS 의 정보는 무시됩니다. Solaris 의 경우 수집되는 정보는 /etc/nsswitch.conf 파일의 시스템 구성에 따라 결정됩니다.

-t

UNIX 및 NIS 의 터미널 규칙을 CA Access Control 데이터베이스로 가져오는 데 필요한 selang 명령을 생성합니다.

uximport 는 /etc/hosts 파일과 NIS 에서 호스트 정보를 추출하고 TERMINAL 리소스를 작성합니다. /etc/hosts 파일에 있거나 NIS 에서 추출된 각 항목에 대한 newres TERMINAL 명령이 생성되고 터미널에서 로그인할 수 있는 권한이 부여됩니다.

또한 DNS 는 -d 옵션과 함께 지원됩니다. 일부 컴퓨터에서 지정된 DNS 데몬이 실행 중인 경우 /etc/hosts 파일과 NIS 의 정보는 무시됩니다. Solaris 의 경우 수집되는 정보는 /etc/nsswitch.conf 파일의 시스템 구성에 따라 결정됩니다.

-T

UNIX 및 NIS 의 TCP 서비스를 CA Access Control 데이터베이스로 가져오는 데 필요한 selang 명령을 생성합니다. 이름은 UNIX 의 GECOS 에 따라 설정되며 40 자보다 길면 잘립니다.

-u

UNIX 및 NIS 의 사용자를 CA Access Control 데이터베이스로 가져오는 데 필요한 selang 명령을 생성합니다. 실제 사용자 이름은 UNIX 의 GECOS 에 따라 설정되며 40 자보다 길면 잘립니다.

옵션

-d

가져올 호스트 및 터미널 목록을 생성하는 데 DNS 를 사용하도록 지정합니다. -h 또는 -t 스위치와 함께 사용해야 합니다.

-f

동일한 이름이 여러 번 사용되면 중복 항목에 대한 검색을 건너뜁니다. 이 옵션은 표준 uximport 프로세스를 사용하지 않으므로 많은 사용자와 그룹을 신속하게 가져오고 메모리를 절약할 수 있습니다. -f 옵션은 호스트에 적용되지 않으므로 -u, -g, -a 스위치 중 하나를 함께 사용해야 합니다. -c 스위치를 -f 옵션과 함께 사용하는 경우에도 이러한 스위치 중 하나를 사용해야 합니다.

조인 및 서로게이트 규칙은 작성 레코드와 함께 인쇄됩니다.

-G

그룹에 대한 SURROGATE 클래스 규칙을 작성합니다. uximport 는 정의한 각 그룹에 대한 SURROGATE 클래스에 레코드를 추가하여 SURROGATE 요청을 보호된 리소스로 만듭니다. 또한 root 가 각 그룹을 서로게이트할 수 있도록 규칙을 추가합니다.

-gr n

모든 사용자의 유예 로그인 횟수를 지정하여 사용자가 n 번의 로그인 후 암호를 변경하도록 합니다. 이렇게 하면 USER 레코드의 PASSWD_L_C 속성이 업데이트됩니다.

-o owner

각 레코드에 대한 소유권 규칙을 설정합니다. 이 옵션을 사용하여 root 가 자동으로 모든 레코드의 소유자가 되지 않도록 하는 것이 좋습니다. owner 는 uximport 에서 정의된 모든 레코드의 소유권이 할당될 사용자나 그룹의 이름입니다.

참고: 이 옵션을 별도의 인수로 지정하고 뒤에 owner 를 입력해야 합니다.

-pr groupname

프로필 그룹을 사용자에게 할당합니다. 이 옵션을 지정하면 CA Access Control 은 사용자 프로필을 작성할 때 이 그룹을 사용하고, 지정하지 않으면 주 UNIX 그룹을 사용합니다.

-r

실패 후 검색을 계속하도록 지정합니다.

-s

사용자 및 그룹에 대한 사용자 ID 교체(SURROGATE) 클래스 규칙을 생성합니다. uximport 함수는 정의된 모든 그룹에 대한 SURROGATE 레코드를 추가함으로써 그룹에 대한 SURROGATE 요청을 보호된 리소스로 만듭니다.

-U

사용자에 대한 SURROGATE 클래스 규칙을 작성합니다. uximport 는 정의한 각 사용자에 대한 SURROGATE 클래스에 레코드를 추가하여 SURROGATE 요청을 보호된 리소스로 만듭니다. 또한 root 가 각 사용자를 서로게이트할 수 있도록 규칙을 추가합니다.

-v

프로그램 상태를 표시합니다(상세 모드). 사이트에 여러 사용자, 그룹 또는 호스트가 있는 경우 프로그램의 진행 상태를 확인할 수 있도록 이 옵션을 사용하는 것이 좋습니다.

예제

다음 명령은 UNIX 및 NIS 데이터베이스에서 모든 사용자, 그룹 및 호스트 정보를 추출합니다. 그런 다음 해당 레코드를 데이터베이스에 추가하는 selang 명령을 작성하면 uximport 는 SURROGATE 클래스 레코드를 작성하고 진행 상태를 표시합니다. 출력은 홈 디렉터리의 uxinfo.seos 파일로 전달됩니다.

```
UxImport -a -s -v > ~/uxinfo.seos
```

추가 정보:

seerrlog 유틸리티-오류 로그 레코드 표시 (페이지 153)
selang 유틸리티-CA Access Control 명령줄 실행 (페이지 162)
seuidpgm 유틸리티-트러스트된 프로그램 추출 (페이지 215)

UXpreinstall 유틸리티 - 시스템 호환성 검사

UNIX 에 해당

uxpreinstall 유틸리티는 운영 체제에 대해 설치된 버전, 패치, 라이브러리, 모듈을 조회합니다. 그런 다음 이 유틸리티는 DNS 서버를 조회하고 LDAP 및 Kerberos 서비스를 검색하여 도메인 이름을 파악합니다. LDAP 서비스를 사용하여 이 유틸리티는 Active Directory 에서 정보를 조회하고 사용 가능한 포트를 검색합니다.

또한 이 유틸리티는 사용자 인증 실패를 방지하기 위해 로컬 호스트와 Active Directory 도메인 사이의 시간 불일치를 검사합니다.

프로세스의 마지막에 uxpreinstall 유틸리티는 발견한 결과를 표시하며, 이 결과에 따라 오류가 있으면 사용자가 이러한 오류를 수정할 수 있습니다.

참고: UNAB 설치 중 uxpreinstall 유틸리티는 자동으로 실행되어 시스템 호환성을 검사합니다. 오류가 발견되면 설치가 취소됩니다.

이 명령의 형식은 다음과 같습니다.

```
uxpreinstall [-a user] [-w passwd] [-d domain] [-v level] [-h]
```

-a user

Active Directory 에 로깅하기 위해 사용할 사용자 계정을 정의합니다.

기본값: Administrator

-w passwd

사용자 계정의 암호를 정의합니다.

-d domain

Active Directory 가 설치된 도메인 이름을 정의합니다.

-v level

세부 정보 표시 수준을 정의합니다.

옵션: 0-5

기본값: 0

-h

유틸리티 도움말을 표시하고 종료하도록 지정합니다.

예: uxpreinstall 유틸리티 실행

이 예제는 administrator 자격 증명을 사용하여 세부 정보 표시 수준 1 로 Active Directory 도메인 domain.com 에 대해 uxpreinstall 유틸리티를 실행합니다.

```
/opt/CA/uxauth/bin/uxpreinstall -a administrator -w admin -d domain.com -v 1
```

예: uxpreinstall 유틸리티 보고서

이 예제에서는 uxpreinstall 유틸리티 보고서를 통해 사용하는 시스템이 시스템 요구 사항에 얼마나 부합하는지를 파악하는 방법을 보여줍니다.

```
OS detected: Linux 2.6.5-7.244-default
Succeeded to get the Active Directory DSE from <adserver.mydomain.com:389>
Clock skew is 6 seconds
Significant clock skew can cause user authentication failure
Kerberos preauthentication for <myuser1> succeeded
AD Schema version 31 (Windows Server 2003 R2)
```

이 예제 보고서에서 다음과 같은 정보를 알 수 있습니다. 운영 체제: 로컬 호스트 Linux 2.6.5-7.244-default 에서 실행 중, Active Directory 가 설치된 도메인 이름과 포트: <adserver.mydomain.com:389>, 시간 불일치: Clock skew is 6 seconds, Kerberos 서비스: Kerberos preauthentication for <administrator> succeeded, Active Directory 가 설치된 Active Directory 스키마 버전 및 운영 체제 버전: AD Schema version 31 (Windows Server 2003 R2)

서비스 및 데몬 세부 사항

이 단원에는 모든 CA Access Control 데몬 및 서비스에 대한 완전한 참조가 알파벳순으로 포함되어 있습니다.

sepmdd 데몬(UNIX)

정책 모델 데몬입니다.

sepmdd 데몬은 PMDB 데몬입니다. sepmdd 데몬은 다음 기능을 수행합니다.

- 정책 모델의 CA Access Control 및 UNIX 데이터베이스를 관리합니다.
- 구독자의 데이터베이스를 관리합니다.
- 변경 사항을 PMDB 에서 구독자 데이터베이스로 전파

sepmdd 데몬은 ACInstallDir/lbin 디렉터리에서 찾을 수 있습니다. 이 데몬은 PMDB 가 아직 작성되지 않은 경우 PMDB 를 시작합니다.

구문

```
sepmdd policyModel
```

매개 변수

policyModel

정책 모델의 이름입니다.

기타 파일

다른 특수 파일은 사용하지 않습니다.

참고:

selang 을 사용하고 정책 모델을 대상으로 선택하면(pmd@hostname 호스트 사용) sepmdd 에 대한 쿼리는 여러 구독자 데이터베이스가 아닌 PMDB 에 적용됩니다.

- PMDB 는 구독자 자신이 될 수 없습니다. PMDB 가 자신으로 구독되는 경우, 정책 모델이 차단하거나 네트워크가 과부화되어 처리 중인 디스크를 채웁니다.
- UNIX 환경에서 selang 으로 정책 모델을 업데이트할 때 newusr 명령에 둘 이상의 사용자를 지정할 수 없으며 newgrp 명령에 둘 이상의 그룹을 지정할 수 없습니다.
- selang 에서 UNIX 파일 특성을 업데이트할 때 정책 모델은 명령이 구독자에게 전달되었음을 알리는 메시지를 생성합니다.
- 정책 모델 관련 작업을 수행할 때 사용자는 UNIX 파일 특성의 상태를 쿼리할 수 없습니다.
- _shutoff_timeout_의 값을 0 으로 설정하면 sepmdd 데몬은 수동으로 종료할 때까지 무제한으로 실행됩니다. 정책 모델 데몬을 종료하려면 sepmd -k 명령을 사용합니다.

추가 정보:

sepmd 유틸리티 (페이지 182)
sepmdadm 유틸리티-PMDB 정의 만들기 (페이지 194)
seagent 데몬 (페이지 242)

sepmdd 작동 방법

CA Access Control 에이전트인 seagent 가 sepmdd 를 시작하므로 명시적으로 sepmdd 를 실행할 필요가 없습니다. UNIX 에서 sepmdd 데몬은 CA Access Control 에 대한 논리적 사용자 ID "_seagent"와 사용자 ID root 를 사용하여 실행됩니다. sepmdd 를 실행할 다른 논리적 사용자를 지정할 수 없습니다.

PMDB 는 공용 디렉터리에 저장됩니다. 정책 모델이 있는 스테이션에서 seos.ini 파일의 [pmd] 섹션에 있는 _pmd_directory_ 토큰을 사용하여 일반 디렉터리의 이름을 지정합니다. 각 정책 모델은 공용 디렉터리의 하위 디렉터리에 위치합니다. 정책 모델 이름은 모델이 위치하는 하위 디렉터리의 이름입니다.

sepmdd 가 시작되면 구독자 데이터베이스를 업데이트해야 하는지 확인한 후 필요에 따라 데이터베이스를 업데이트합니다. 시작 프로세스 후 sepmdd 는 사용자 요청을 기다리고, 이러한 사용자 요청은 정책 모델 관리 프로그램인 sepmd 및 selang 유틸리티가 seagent 를 사용하여 전송합니다.

sepmdd 가 요청을 수신하면 해당 요청을 PMDB 에 적용하고 그 결과를 사용자에게 다시 보냅니다. 요청을 전파해야 하는 경우 sepmdd 는 업데이트를 구독자 데이터베이스에 전파합니다.

sepmdd 데몬은 _QD_timeout_ 토큰에 지정된 기간 동안 구독자 데이터베이스를 업데이트하려고 시도합니다. 최대 시간이 경과하고 데몬이 구독자를 업데이트할 수 없는 경우 해당 구독자를 건너뛰고 목록의 나머지 구독자를 업데이트합니다. 구독자 목록의 최초 검사를 완료하면 sepmdd 는 두번째 검사를 수행합니다. 여기서는 첫번째 검사에서 업데이트에 실패한 구독자를 업데이트하려고 시도합니다. 두번째 검사 중에는 연결 시스템 호출 시간(약 90 초)이 만료될 때까지 구독자를 업데이트합니다.

참고: _QD_timeout_ 토큰은 seos.ini 파일과 pmd.ini 파일에 모두 있을 수 있습니다. 이 경우 sepmdd 는 pmd.ini 파일의 값을 사용합니다.

두번째 검사 동안 구독자가 유효하지 않으면 sepmdd 는 30 분마다 업데이트를 전송하려고 시도합니다. 이 간격을 수정하려면 _retry_timeout_ 토큰을 설정하십시오. 업데이트를 받은 순서대로 전송해야 하므로 sepmdd 는 구독자 데이터베이스가 사용 가능할 때까지 후속 업데이트를 보내지 않습니다.

구독자 데이터베이스의 seos.ini 파일에 있는 [pmd] 섹션에서 pull_option 토큰을 yes 로 설정하면 구독자 데이터베이스가 즉시 업데이트됩니다. seagent 는 컴퓨터의 모든 정책 모델에 대해 호스트를 사용할 수 있고 해당 구독자 PMDB 가 작동되고 있음을 부모 정책 모델에 알리며, sepmdd 는 즉시 업데이트를 전송합니다.

sepmdd 는 구독자 데이터베이스 업데이트에 실패할 때마다 정책 모델 오류 로그에 경고 메시지를 기록합니다. 정책 모델 오류 로그에 대한 자세한 내용은 UNIX 용 끝점 관리 안내서를 참조하십시오.

CA Access Control 은 구독자가 정책 모델에서 추가되거나 삭제될 때 완전한 권한을 가진 구독자가 되려고 합니다.

사용할 수 없는 구독자 목록에서 구독자를 제거하려면 다음 명령을 입력합니다.

```
sepmd -r policyModel subscriber
```

구독자 데이터베이스가 PMDB 와 다른 경우 발생할 수 있는 것처럼 구독자 데이터베이스가 업데이트를 거부하는 경우, sepmdd 는 오류 메시지를 정책 모델 오류 로그에 기록한 후 계속 진행합니다.

오류 로그를 보려면 PMDB 가 위치하는 호스트에 다음 명령을 입력합니다.

```
sepmd -e policyModel
```

일정한 비활성 기간 후에 sepmdd 가 자동으로 종료되도록 설정할 수 있습니다. 그러나 sepmdd 는 기본적으로 자체 종료되지 않습니다. sepmdd 를 자체 종료하려면 _shutoff_time_ 토큰을 0 보다 큰 값으로 설정하십시오. 이 값은 sepmdd 가 자체 종료되기 전에 허용되는 비활성 시간(분)을 나타냅니다. 수동으로 sepmdd 를 종료하려면 다음을 입력합니다.

```
sepmd -k policyModel
```

중요! sepmdd 를 수동으로 종료할 때는 PMDB 가 손상될 수 있으므로 UNIX 명령 kill -9 를 사용하지 마십시오.

UID/GID 동기화

사용자 이름 대신 UID 로 사용자를 참조하는 메시지를 받을 수 있으므로 각 사용자의 UID 를 아는 것이 중요합니다. 그러나 PMDB 를 사용하는 경우 새 사용자의 UID 가 할당되는 방법에 주의하지 않으면 각 구독자 컴퓨터에서 사용자가 다른 UID 를 받을 수 있습니다. 사용자는 각 구독자 컴퓨터마다 다른 UID 를 수신할 수 있으므로 대신 각 사용자가 어디서든 동일한 UID 를 가지는 것이 가장 좋으며 GID 에서도 마찬가지입니다. UNIX 용 끝점 관리 안내서의 UID/GID 동기화를 참조하십시오.

필터 메커니즘

PMDB 에서 하위 구독자 스테이션을 선택적으로 업데이트할 수도 있습니다. 구독자 스테이션으로 전송할 레코드를 정의하려면 pmd.ini 파일의 필터 토큰에 필터 파일을 지정합니다. 구독자 스테이션의 업데이트는 필터 파일을 통과한 레코드로 제한됩니다.

필터 파일은 행마다 6 개의 필드가 있는 행으로 구성되고, 각 필드에는 다음 정보가 포함됩니다.

- 허용되거나 금지된 액세스 형식. 가능한 값은 AUTHORIZE_DELETE, AUTHORIZE_MODIFY, CREATE, DELETE, DEPLOY, EDIT, FILESCAN, GET, SEOS_ACCS_READ, JOIN_DELETE, JOIN_MODIFY, MODIFY, READ, START 또는 UNDEPLOY 입니다.
- 적용되는 환경. 가능한 값은 AC, CONFIG, UNIX, NT 또는 NATIVE 입니다.
- 레코드 클래스. 가능한 값은 사용자 정의 클래스를 포함한 CA Access Control 의 모든 클래스입니다.
- 규칙이 적용되는 클래스 내 개체. 예를 들어 User1, AuditGroup, 또는 TTY1 입니다.
- 레코드가 허용하거나 취소한 속성. 예를 들어 사용자 레코드 필터 행의 OWNER 와 FULL_NAME 은 이러한 사용자 속성을 갖는 명령이 필터링됨을 의미합니다. 각 속성을 정확히 입력해야 합니다.
- 해당 레코드를 구독자 스테이션으로 전달해야 하는지 여부. 가능한 값은 PASS 또는 NOPASS 입니다.

"가능한 모든 값"을 의미하는 별표를 필드에서 사용할 수 있습니다. 여러 행에 동일한 레코드가 포함되어 있는 경우 적용 가능한 첫 번째 행이 사용됩니다.

필터 파일의 각 행에서 공백은 필드를 구분하고, 필드에 여러 개의 값이 있는 경우 세미콜론으로 값을 구분합니다. "#"으로 시작하는 행은 주석 행으로 간주합니다. 빈 줄은 허용되지 않습니다. 다음은 필터 파일 행의 예입니다.

CREATE	**AC**	**USER**	*****	**FULL-NAME;OBJ_TYPE**	**NOPASS**
액세스 access	환경	class	레코드 이름 (* =모두)	properties	처리

예를 들어 이 행이 포함된 파일 이름이 TTY1_FILTER 이고 정책 모델 TTY1 의 pmd.ini 파일에는 line filter=/opt/CA/AccessControl/TTY1_FILTER 가 있다고 가정합니다. 정책 모델 TTY1 은 FULL_NAME 및 OBJ_TYPE(admin, auditor 등)으로 새 CA Access Control 사용자를 작성하는 레코드를 전송하지 않습니다. 별표는 "이름에 상관 없다"는 의미입니다.

다음은 각 액세스 값과 관련된 selang 명령입니다.

액세스	selang 명령
AUTHORIZE_DELETE	authorize-
AUTHORIZE_MODIFY	authorize
CREATE	newres, newusr, newgrp, newfile
DELETE	rmres, rmusr, rmgrp, rmfile, join- (UNIX)
DEPLOY	deploy
EDIT	editres, editusr, editgrp, editfile
FILESCAN	search
GET	get devcalc
JOIN_DELETE	join-
JOIN_MODIFY	join
MODIFY	chres, chusr, chgrp, chfile, join (UNIX)
READ	list
START	start devcalc
UNDEPLOY	deploy- (배포 취소)

CA Access Control 은 규칙의 유효성을 검사하지 않으므로 규칙에 잘못된 값을 입력하면 규칙은 어떤 업데이트 트랜잭션과도 일치하지 않습니다.

sepmdd 서비스(Windows)

sepmdd 는 PMDB 서비스입니다. 이 서비스는 다음 기능을 수행합니다.

- 정책 모델의 CA Access Control 및 Windows 데이터베이스 관리
- 구독자 데이터베이스 관리
- 변경 내용을 PMDB 에서 구독자 데이터베이스로 전파

SeOSAgent 는 sepmdd 서비스를 시작합니다. sepmdd 를 명시적으로 실행할 필요는 없습니다. Sepmdd 는 Windows 에서 서비스 'CA Access Control 정책 모델'로서 실행됩니다. 각 정책 모델의 두 가지 가능한 상태는 Started 및 Stopped 입니다.

PMDB 는 공용 디렉터리에 저장됩니다. HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\Pmd 하위 키의 _pmd_directory_ 레지스트리 값은 공용 디렉터리의 이름을 지정합니다.

각 정책 모델은 공용 디렉터리의 하위 디렉터리에 위치합니다. 정책 모델 이름은 모델이 위치하는 하위 디렉터리의 이름입니다.

sepmdd 가 시작되면 구독자 데이터베이스를 업데이트해야 하는지 확인한 후 필요에 따라 업데이트합니다. 이러한 시작 프로세스 후에 sepmdd 서비스는 사용자 요청을 기다립니다. 사용자 요청은 정책 모델 관리 유틸리티 sepmd 및 CA Access Control 에이전트를 사용하는 selang 에 의해 전송됩니다.

요청이 수신되면 sepmdd 는 해당 요청을 PMDB 에 적용하고 그 결과를 사용자에게 다시 전송합니다. 요청을 전파해야 하는 경우 sepmdd 는 업데이트를 구독자 데이터베이스에 전파합니다.

sepmdd 서비스는 30 초 동안 구독자 데이터베이스 업데이트를 시도합니다. 시간이 경과되더라도 서비스가 구독자 업데이트에 성공하지 못하면 해당하는 특정 구독자를 건너뛰고 목록에 있는 나머지 구독자를 업데이트합니다. 구독자 목록의 최초 검사를 완료하면 sepmdd 는 두번째 검사를 수행합니다. 여기서는 첫번째 검사에서 업데이트에 실패한 구독자를 업데이트하려고 시도합니다. 두번째 검사 중에는 연결 시스템 호출 시간(약 90 초)이 만료될 때까지 구독자를 업데이트합니다.

두번째 검사 동안 구독자가 유효하지 않으면 sepmdd 는 30 분마다 업데이트를 전송하려고 시도합니다.

업데이트를 받은 순서대로 전송해야 하므로 sepmdd 는 구독자 데이터베이스가 사용 가능할 때까지 후속 업데이트를 보내지 않습니다.

sepmdd 는 구독자 데이터베이스를 업데이트하는 데 실패할 때마다 정책 모델 오류 로그에 경고 메시지가 기록됩니다.

필터 메커니즘

PMDB 에서 구독자 스테이션을 선택적으로 업데이트하도록 지정하려는 경우, 구독자 스테이션으로 전송되는 레코드를 정의하려면 레지스트리 키 문자열 값을 필터 파일로 설정하십시오. 구독자 스테이션의 업데이트는 필터 파일을 통과한 레코드로 제한됩니다.

다음은 그 예입니다.

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\Pmd\PolicyModelName\
Filter
```

필터 파일은 행마다 6 개의 필드가 있는 행으로 구성되고, 필드에는 다음 정보가 있습니다.

허용되거나 금지된 액세스 형식

유효한 값: AUTHORIZE_DELETE, AUTHORIZE_MODIFY, CREATE, DELETE, DEPLOY, EDIT, FILESCAN, GET, SEOS_ACCS_READ, JOIN_DELETE, JOIN_MODIFY, MODIFY, READ, START, UNDEPLOY.

적용되는 환경

유효한 값: AC, CONFIG, UNIX, NT, NATIVE.

레코드 클래스

유효한 값은 사용자 정의 클래스를 포함한 CA Access Control 의 모든 클래스입니다.

규칙이 적용되는 클래스 내 개체

예: User1, AuditGroup, COM2

레코드가 허용하거나 취소한 속성

예를 들어 사용자 레코드 필터 행에 GROUPS 와 FULLNAME 을 포함하는 것은 이러한 사용자 속성을 갖는 명령이 필터링됨을 의미합니다. 나타나는 대로 정확히 각 속성을 입력해야 합니다.

해당 레코드를 구독자 스테이션으로 전달할지 여부

유효한 값: PASS, NOPASS

참고: "가능한 모든 값"을 의미하는 별표를 필드에서 사용할 수 있습니다. 두 개 이상의 행이 동일한 레코드를 포함할 경우, 첫 번째 적용 가능한 행이 사용됩니다.

필터 파일의 각 행에서 공백은 필드를 구분하고, 두 개 이상의 값을 갖는 필드에서는 값을 세미콜론(;)으로 구분합니다. "#"으로 시작하는 행은 주석 행으로 간주합니다. 빈 줄은 허용되지 않습니다. 다음은 필터 파일 행의 예입니다.

CREATE	AC	USER	*	FULLNAME;OBJ_TYPE	NOPASS
액세스 access	환경	class	레코드 이름 (* =모두)	properties	처리

예를 들어, 이 행을 가진 파일 이름이 Printer1_Filter.flt 이고 레지스트리 키 HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\Pmd\PM-\Filter 가 "C:\Program Files\CA\AccessControl\data\Printer1_Filter.flt" 행을 포함할 경우, 정책 모델 PM-1 은 FULLNAME 및 OBJ_TYPE(admin, auditor 등)을 가진 새 CA Access Control 사용자를 작성하는 레코드는 전송하지 않습니다. 별표는 "이름에 상관 없다"는 의미입니다.

다음은 각 액세스 값과 관련된 selang 명령입니다.

액세스	**selang 명령**
AUTHORIZE_DELETE	authorize-
AUTHORIZE_MODIFY	authorize
CREATE	newres, newusr, newgrp, newfile
DELETE	rmres, rmusr, rmgrp, rmfile, join- (UNIX)
DEPLOY	deploy
EDIT	editres, editusr, editgrp, editfile
FILESCAN	search
GET	get devcalc
JOIN_DELETE	join-
JOIN_MODIFY	join
MODIFY	chres, chusr, chgrp, chfile, join (UNIX)
READ	list
START	start devcalc
UNDEPLOY	deploy- (배포 취소)

참고: CA Access Control 은 규칙의 유효성을 검사하지 않으므로 규칙에 잘못된 값을 입력하면 규칙은 어떤 업데이트 트랜잭션과도 일치하지 않습니다.

레지스트리 하위 키

각 PMDB 는 다음 아래에 자체 레지스트리 하위 키를 가지고 있습니다.
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\Pmd

이 하위 키에는 PMDB 의 활동을 정의하고 결정하는 값이 있습니다. sepmdd 유틸리티는 필요한 최소한의 항목으로 하위 키를 작성합니다(이전에 존재하지 않은 경우).

참고: PMDB 레지스트리 항목에 대한 자세한 내용은 참조 안내서를 참조하십시오.

참고

- selang 을 사용하고 정책 모델을 대상으로 선택한 경우(pmd@hostname 호스트 사용), sepmdd 에 대한 쿼리는 여러 구독자의 데이터베이스가 아닌 PMDB 에 적용됩니다.
- PMDB 는 구독자 자신이 될 수 없습니다. PMDB 가 자신으로 구독되는 경우, 정책 모델이 차단하거나 네트워크가 과부화되어 처리 중인 디스크를 채웁니다.
- selang 을 사용하여 정책 모델을 업데이트하기 위해 UNIX 환경에서 작업 중일 때 newusr 명령으로 둘 이상의 사용자를 지정할 수 없습니다.
- selang 을 사용하여 정책 모델을 업데이트하기 위해 UNIX 환경에서 작업 중일 때 newgrp 명령으로 둘 이상의 그룹을 지정할 수 없습니다.
- selang 에서 UNIX 파일 특성을 업데이트할 때 정책 모델은 명령이 구독자에게 전달되었음을 알리는 메시지를 생성합니다.
- 정책 모델에 대한 작업을 수행할 경우, Windows 파일 특성의 상태를 쿼리할 수 없습니다.
- sepmdd 서비스는 -k 옵션으로 비활성화될 때까지 무한대로 활성 상태를 유지합니다.

추가 정보:

seagent 데몬 (페이지 242)
sepmd 유틸리티 (페이지 182)
sepmdadm 유틸리티-PMDB 정의 만들기 (페이지 194)

seagent 데몬

UNIX 에 해당

seagent 데몬은 원격 스테이션에서 요청을 받아 로컬 CA Access Control 및 UNIX 데이터베이스나 PMDB 에 적용합니다. 또한 Watchdog 데몬 seoswd 가 실행 중인지 확인한 후 실행 중이 아닌 경우에는 해당 데몬을 재시작합니다.

참고: CA Access Control(seload)을 로드하면 seagent 가 시작됩니다. 이 데몬은 독립적으로 작동하지 않으며 seagent 명령을 사용하여 시작할 수 없습니다.

Seagent 는 seoslang 및 seoslang2 TCP 서비스에서 연결을 대기합니다(기본값은 각각 8890 및 8891). 연결 요청이 도착하면 seagent 는 하위 프로세스를 나누어 연결 상의 통신을 처리하고 새 연결을 계속 기다립니다.

seagent 의 하위 프로세스는 클라이언트에서 요청을 가져오고 가져온 요청을 로컬 데이터베이스에 적용합니다.

또한 에이전트는 다음과 같은 작업을 수행합니다.

- UNIX 사용자 파일 /etc/passwd, 시스템의 섀도 암호 파일 및 UNIX 그룹 파일 /etc/group 업데이트
- 업데이트 전송 시 정책 모델 데몬 경고
- 중단된 구독자 스테이션을 업데이트할 수 있을 때 로컬 호스트의 상위 정책 모델과 컴퓨터의 정책 모델 경고

CA Access Control 은 8890 및 8891 포트만 사용합니다. 이러한 포트를 변경하지 않는 것이 좋습니다.

seagent 는 RPC 메커니즘을 사용하므로 로컬 컴퓨터에서 포트 매퍼가 실행되고 있어야 합니다. 포트 매퍼에 대한 자세한 내용은 시스템 설명서를 참조하십시오.

이 명령의 형식은 다음과 같습니다.

```
seagent
```

추가 정보:

seoswd Daemon (페이지 249)
sepmdd 데몬 (UNIX) (페이지 232)

seauxd 데몬

UNIX 에 해당

seauxd 데몬은 Unicenter 달력 업데이트를 관리하는 CA Access Control 보조 데몬입니다.

seauxd 를 활성화하려면 TNG_calendars 구성 설정을 "yes"로 설정하십시오.

seauxd 데몬은 초기화 설정에 따라 seosd 데몬에 의해 시작됩니다. seauxd 데몬은 다음 기능을 수행합니다.

- seosd 의 분석 요청
- Unicenter TNG 달력 검색-이 기능을 활성화하려면 seos.ini 파일의 [seauxd] 섹션에서 TNG_calendars 토큰을 yes 로 설정하십시오. 이 기능이 활성화되면 seosd 는 Unicenter TNG 일정(Calendar)을 seauxd 로 전송합니다. seauxd 데몬은 Unicenter TNG 를 호출하고 각 일정(Calendar)의 상태를 업데이트하며 업데이트된 일정(Calendar) 목록을 seosd 로 반환합니다.

seos.ini 의 [seauxd] 섹션에는 seauxd 데몬을 미세 조정할 수 있는 여러 개의 토큰이 있습니다.

seosd 데몬

UNIX 에 해당

CA Access Control 권한 부여 데몬입니다. seosd 실행 파일은 CA Access Control 주 데몬입니다. 데몬은 제어 TTY 와 부모 프로세스 둘 다에서 연결이 끊어진 프로세스를 말합니다. CA Access Control 데몬은 리소스에 대한 액세스를 승인 또는 거부하는 데 필요한 런타임 결정을 내립니다.

root 만 seosd 를 호출할 수 있고 ADMIN 또는 OPERATOR 특성을 가진 사용자만 이 유틸리티를 종료할 수 있습니다.

CA Access Control 데몬은 데이터베이스를 열고 읽고 업데이트합니다. CA Access Control 데몬이 실행되고 있는 동안에는 다른 프로세스가 이 데이터베이스에 액세스할 수 없습니다. 또한 CA Access Control 데몬은 CA Access Control 감사 파일 및 추적 파일과 같은 중요한 파일과 CA Access Control 바이너리 파일(선택 사항)에 대한 쓰기, 삭제 또는 이름 변경 액세스 권한을 차단합니다.

seosd 실행 파일은 다음 조건 중 하나 이상에 해당되는 경우에만 데몬이 됩니다.

- 추적 메시지가 화면으로 전송되지 않습니다. 즉 seos.ini 파일의 trace_to 토큰을 file, file,stop 또는 none 으로 설정했습니다.
- 유틸리티를 호출할 때 인수(-d 를 제외)를 명령줄에 지정하지 않습니다.

이러한 조건에 모두 해당되지 않을 경우 seosd 는 사용자가 호출한 터미널에 연결된 일반 프로세스를 유지합니다.

시작 중에 seosd 는 다음 프로세스도 호출합니다.

- seagent, CA Access Control agent 데몬.
- seoswd, CA Access Control watchdog 데몬.

CA Access Control 데몬은 이러한 데몬도 실행되고 있어야만 완전히 초기화됩니다. 초기화된 후 세 개의 데몬은 핸드쉐이킹 프로토콜 유형을 유지 관리하여 데몬이 제대로 작동하는지 확인합니다. 이러한 데몬 중 하나가 없는 경우 해당 데몬은 다른 두 개의 데몬 중 하나에 의해 자동으로 다시 시작됩니다.

이 명령의 형식은 다음과 같습니다.

```
seosd [-d|argument]
```

참고: 인수 없이 seosd 를 입력하면 seosd 는 데몬으로서 실행됩니다.

argument

무시됩니다. 그러나 인수를 지정하면 seosd 는 일반 프로세스로 실행됩니다.

-d

seosd 를 데몬으로서 실행하고 trace_file 에 대한 추적을 강제로 수행합니다.

selogrcd 데몬-감사 레코드 수집

UNIX 에 해당

CA Access Control 로그 라우팅 시스템을 위한 "수집기" 데몬입니다.

참고: selogrcd 는 IPv6 전용 환경에서 작동하지 않습니다.

CA Access Control 로그 라우팅 데몬인 selogrd 와 selogrcd 는 시스템 관리자가 원하는 감사 로그 레코드에 편리하게 선택적으로 액세스할 수 있게 해줍니다.

selogrcd 유틸리티는 수집 데몬입니다. 이 데몬은 여러 위성 시스템에서 보낸 선택된 감사 로그 레코드를 수집하여 감사 수집 파일에 저장합니다. 기본 파일은 ACInstallDir/log/seos.collect.audit 입니다.

두 개의 토큰이 감사 수집(Collection) 파일 관리를 향상시킵니다. 두 토큰은 모두 seos.ini 파일의 [selogrd] 섹션에 있습니다.

- Caudit_size 토큰을 사용하여 감사 수집 파일의 최대 크기를 지정합니다. 파일이 이 크기에 도달하면 CA Access Control 은 백업 파일을 생성하고 새 파일을 엽니다.
- CbackUp_Date 토큰을 사용하여 감사 수집 파일에 대한 자동 백업 간격 및 시간 스탬프를 지정합니다.

selogrcd 에 USR1 신호를 전송하여 새 감사 파일을 시작하도록 할 수 있습니다. selogrcd 프로세스 ID 가 있으면 다음과 같이 kill 명령을 사용하여 USR1 신호를 전송합니다.

```
kill -USR1 processID
```

USR1 신호를 받으면 selogrcd 는 기존 감사 파일의 이름을 ACInstallDir/log/seos.collect.bak 으로 변경하고 새 감사 파일을 작성합니다. 크론(cron) 작업을 사용하여 정기적으로 이 작업을 수행할 수도 있습니다. 이 작업을 수행하는 샘플 스크립트는 ACInstallDir/samples/selogrcd 디렉터리에 있습니다.

참고: CA Access Control 과 함께 제공된 API 를 사용하는 프로그램을 사이트에서 작성하여 selogrcd 데몬의 기능을 확장할 수 있습니다. 자세한 내용은 SDK 안내서를 참조하십시오.

이 명령의 형식은 다음과 같습니다.

```
selogrcd [-d] [-l lock-file-name]
```

-d

디버그 모드를 지정합니다. 이 모드에서 selogrcd 는 데몬이 되지 않으며 터미널로 디버그 정보를 전송합니다.

-h

이 유틸리티에 대한 도움말을 표시합니다.

-l lock-file-name

사용할 잠금 파일의 이름(lock-file-name)을 지정합니다. 기본적으로 selogrcd 는 ACInstallDir/lock/selogrcd 파일을 사용합니다.

참고: selogrd 가 다른 로그 파일(예: PMDB 로그 파일)에 대해 작동하도록 설정하면, 잠금 파일은 PMDB 이름 또는 selogrd command (페이지 246)에 대한 매개 변수로 사용된 데이터 파일 이름을 기반으로 하는 확장자를 갖습니다.

selogrd 데몬-감사 레코드 송신

UNIX 에 해당

CA Access Control 로그 라우팅 시스템의 에미터(emitter) 데몬입니다.

참고: selogrd 는 IPv6 전용 환경에서 작동하지 않습니다.

CA Access Control 로그 라우팅 데몬인 selogrd 와 selogrcd 는 시스템 관리자가 원하는 감사 로그 레코드에 편리하게 선택적으로 액세스할 수 있게 해줍니다.

selogrd 유틸리티는 송신기 데몬입니다. 이 데몬은 선택된 로컬 감사 로그 레코드를 여러 대상 호스트로 분배하고, 감사 로그 레코드를 전자 메일 메시지, ASCII 파일 또는 사용자 창으로 형식을 변경하며, 감사된 이벤트에 따라 알림 메시지를 보냅니다.

참고: 먼저 CA Access Control 데몬을 실행해야만 로그 라우팅 데몬이 CA Access Control 이벤트에 대한 의미 있는 정보를 수집할 수 있습니다. CA Access Control 데몬이 실행되고 있지 않으면 selogrd 는 이전 감사 레코드만 라우트합니다.

로그 라우팅 데몬은 구성 파일을 사용하여 각 감사 로그 레코드가 전송되는 위치, 로그 레코드가 작성되는 형식 및 라우트되는 레코드를 확인합니다. 기본적으로 selogrd 는 ACInstallDir/log/selogrd.cfg 감사 로그 라우트 구성 파일을 사용합니다. selogrd 및 selogrcd 에 사용되는 구성 파일의 이름과 기타 전역 환경 변수는 CA Access Control 초기화 파일인 seos.ini 에서 지정됩니다.

selogrd 데몬은 주기적으로 다시 시작하고 구성 파일을 읽습니다. 또한 selogrd 데몬을 지정된 시간에 다시 시작하도록 지정할 수 있습니다. 이렇게 하려면 다음 HUP 신호를 보내야 합니다.

```
kill -HUP processID
```

processID

selogrd 프로세스 ID 를 정의합니다. 이것을 찾으려면 UNIX ps 명령을 사용하하십시오. 자세한 내용은 UNIX 설명서를 참조하십시오.

selogrd 유틸리티는 CA Access Control 에서 작업하는 프로그래머에게 API 액세스를 제공합니다. 프로그래머는 LogRoute API 를 사용하여 CA Access Control 감사 로그 시스템에 자체 옵션을 통합함으로써 현재의 로그 라우팅 기능에서 제공하지 않는 내부 경보를 지원할 수 있습니다. 또한 Logroute API 를 통해 프로그래머는 로그 라우팅 데몬을 사용하여 자신의 프로그램에 함수를 제공할 수 있습니다. 모든 CA Access Control API 에 대한 자세한 내용은 SDK 개발자 안내서를 참조하십시오.

이 명령의 형식은 다음과 같습니다.

```
selogrd [-audit fileName] [-config fileName] [-d] \
    [-data fileName] [-pmdb policy-model-name]
```

-audit fileName

seos.ini 에 나열된 파일 대신 입력 감사 파일용으로 사용할 감사 파일을 정의합니다.

-config fileName

seos.ini 에 나열된 파일 대신 구성 파일용으로 사용할 구성 파일을 정의합니다.

-d

디버그 메시지를 인쇄하도록 지정합니다.

-data fileName

seos.ini 에 나열된 파일 대신 라우팅 프로세스 정보 저장을 위해 사용할 데이터 파일을 정의합니다.

-h

이 유틸리티에 대한 도움말을 표시합니다.

-pmdb policy-model-name

PMDB 의 감사 데이터를 라우트할 위치를 selogrd 에 지시합니다. 명령은 selogrd 에 사용자가 명령으로 지정한 PMDB 에서 PMDB 의 pmd.ini 파일에 있는 audit_log 토큰에 지정된 감사 파일로 감사 데이터를 보낼 것을 지시합니다.

기본적으로 selogrd 는 정책 모델 이름으로 구성된 데이터 파일 및 잠금 파일을 사용합니다. 명령줄에 데이터 파일이나 잠금 파일을 지정하거나 둘 다를 지정하면 이러한 파일은 기본값을 무시합니다. 잠금 파일 이름과 데이터 파일 이름은 스테이션의 감사 데이터를 라우트하는 selogrd 의 이름과 달라야 합니다. selogrd 는 12 자의 정책 모델 이름만 지원할 수 있습니다.

PMDB 에서 전송된 감사 데이터는 policy-model-name@station-name 이름을 가진 스테이션에서 제공된 것처럼 수집된 감사 파일에 나타납니다.

추가 정보:

감사 로그 라우트 구성 파일 selogrd.cfg (페이지 374)

seostngd 데몬

UNIX 에 해당

Unicenter TNG 를 위한 CA Access Control 동기화 데몬입니다.

Unicenter Security 와 CA Access Control 은 전체 마이그레이션이 실행되기 전에 엔터프라이즈 IT 환경 관리를 공동으로 수행합니다. 관리 작업을 수행하기 위해 여러 개의 제품 도구를 함께 사용하는 복잡성을 줄이기 위해 동기화 데몬을 제공합니다.

이 데몬을 seostngd 라고 합니다. CA Access Control 은 CAICCI(CA Common Communication Interface)를 통해 PMDB(정책 모델 데이터베이스) 업데이트를 seostngd 로 전송합니다. 데몬은 CAICCI 에서 업데이트를 받은 후 메시지를 해당 cautil 명령으로 변환하여 Unicenter Security 데이터베이스를 이러한 전역 데이터로 업데이트합니다.

현재 Unicenter TNG 프로세스에서 다른 Unicenter TNG 클라이언트 설치를 여전히 업데이트할 수 있습니다. Unicenter Security 데이터베이스와 동일한 컴퓨터(일반적으로 Unicenter TNG 마스터 컴퓨터라고 함)에서 seostngd 를 실행해야 합니다. CA Access Control 도 동일한 컴퓨터에서 실행되고 있어야 합니다.

이 명령의 형식은 다음과 같습니다.

```
seostngd

seostngd {-stop|-shut}
```

seoswd Daemon

UNIX 에 해당

CA Access Control watchdog 데몬입니다.

watchdog(seoswd)은 데이터베이스에 트러스트된 프로그램으로 정의된 프로그램의 파일 정보와 디지털 서명을 모니터합니다. 이 모니터링 작업은 시스템 로드를 최소화하여 백그라운드에서 수행됩니다. CA Access Control 에이전트 데몬인 seagent 가 자동으로 seoswd 를 시작합니다.

seoswd 데몬은 다음 기능을 수행합니다.

- 데이터베이스의 PROGRAM 클래스에 정의한 프로그램을 모니터합니다. 특정 프로그램이 수정된 것을 탐지하면 watchdog 은 CA Access Control 데몬인 seosd 에 통보합니다. 그러면 seosd 데몬은 프로그램을 언트러스트된 상태로 표시합니다. seosd 데몬은 언트러스트된 프로그램의 실행을 허용하지 않습니다. 또한 seosd 데몬은 데이터베이스에서 프로그램 상태를 언트러스트된 상태로 표시하고 감사 레코드를 작성합니다.
- 보안 파일로 정의되는 파일을 모니터합니다. 이러한 파일은 데이터베이스의 SECFILE 클래스에 정의됩니다.
- seosd 를 모니터하여 실행되고 있는지 확인합니다. seosd 에서 문제가 탐지되면 watchdog 은 seosd 를 자동으로 다시 시작합니다.
- seoswd 데몬은 seosd 가 응답하지 않음을 감지하면 시스템 로그 syslogd 를 사용하여 보안 관리자에게 알립니다. 모든 시스템 로그 메시지는 AUTH 기능으로 제출됩니다. 시스템 로그 기능에 대한 자세한 내용은 syslogd 및 syslog.conf 절의 시스템 주 페이지를 참조하십시오.
- 여러 가지 이벤트를 CA Access Control 에 보고하고 변경된 프로그램 및 보안 파일에 대한 감사 레코드를 작성합니다.
- 트러스트된 프로그램과 보안 파일에 대한 간격 및 고정 스캔 스케줄을 지정할 수 있습니다.
- watchdog 은 SIGHUP 을 제외한 모든 신호를 무시하므로, seosd 를 먼저 종료하지 않으면 seoswd 데몬을 종료할 수 없습니다. 그러나 kill -SIGHUP pid 명령을 실행할 경우 watchdog 은 데이터베이스의 보안 파일과 트러스트된 모든 프로그램을 스캔합니다.

Watchdog 스캐닝 메커니즘을 설정할 수 있는 방법에는 두 가지가 있습니다.

1. 시작 시간을 결정한 다음 지정된 간격으로 스캔을 반복하십시오.

   예를 들어 Watchdog 은 트러스트된 프로그램을 검사할 때 PgmTestStartTime 에서 첫 번째 검색을 시작하고 모든 트러스트된 프로그램을 검사합니다. 다시 검색은 이전 검색을 시작한지 PgmTestInterval 초 후에 발생합니다.

2. 지정된 시간에 스캔하십시오.

참고: 두 경우 모두 Watchdog 은 각 검색 중에 미리 지정된 휴식 기간(PgmRest 초) 동안 주기적으로 작동을 중지합니다. 시스템 부하를 막기 위해 Watchdog 이 중지됩니다.

한 메커니즘을 사용할지 또는 둘 다를 동시에 사용할지를 선택할 수 있습니다. 예를 들어 12:00 에 시작하여 13:00 와 17:30 에 검색할 뿐만 아니라 4 시간마다 검색합니다.

트러스트된 프로그램과 보안 파일의 일상적인 검색 방법에는 위에서 언급한 메커니즘뿐 아니라, HUP 신호를 보내어 요구 시 일회성 검색을 수행하는 방법도 있습니다(토큰 SignalMinInterval 참조).

인수 없이 seoswd 를 호출하면 seoswd 는 데몬으로 실행됩니다. -d 인수를 사용하여 seoswd 를 호출하면 seoswd 는 데몬으로 실행되지만 호출한 터미널에 대한 모든 디버그 정보를 표시합니다.

추가 정보:

seuidpgm 유틸리티-트러스트된 프로그램 추출 (페이지 215)

제 3 장: 구성 파일

이 장은 아래의 주제를 포함하고 있습니다.

accommon.ini 파일 (페이지 251)
seos.ini 초기화 파일 (페이지 256)
pmd.ini 파일 (페이지 339)
lang.ini 파일 (페이지 349)
trcfilter.init (페이지 356)
audit.cfg 파일 - 감사 레코드 필터링 (페이지 357)
auditrouteflt.cfg 파일 - 감사 레코드 라우팅 필터링 (페이지 366)
감사 로그 라우트 구성 파일 selogrd.cfg (페이지 374)
uxauth.ini 파일 (페이지 384)
UNAB 충돌 파일 (페이지 399)

accommon.ini 파일

accommon.ini 구성 파일에는 보고서 에이전트의 초기화 프로세스를 제어하는 토큰과 일반 통신 설정(예: CA Access Control 엔터프라이즈 관리에 대한 UNAB 등록 설정)을 제어하는 토큰이 포함되어 있습니다. accommon.ini 파일은 다음 섹션으로 구분되어 있습니다.

섹션	설명
communication	일반 통신 설정을 제어하는 토큰을 포함하고 있습니다.
global	CA Access Control 전역 설정을 포함하고 있습니다.
ReportAgent	보고서 에이전트 설정을 제어하는 토큰을 포함하고 있습니다.

communication

[communication] 섹션에서 이 토큰은 통신 및 암호화 옵션을 제어합니다.

Distribution_Server

배포 서버 URL 을 정의합니다. 목록에서 쉼표로 구분하여 여러 배포 서버를 정의할 수 있습니다.

예: tcp://ds.comp.com:7222, tcp://ds_dr.comp.com:7222

기본값: 없음

endpoint_to_server_queue

끝점이 CA Access Control 엔터프라이즈 관리로 정보를 보내기 위해 사용하는 메시지 큐의 이름을 정의합니다.

기본값: ac_endpoint_to_server

server_to_endpoint_broadcast_queue

CA Access Control 엔터프라이즈 관리가 모든 끝점으로 메시지를 브로드캐시트하기 위해 사용하는 메시지 큐의 이름을 정의합니다.

기본값: ac_server_to_endpoint_broadcast

server_to_endpoint_queue

CA Access Control 엔터프라이즈 관리가 끝점으로 메시지를 보내기 위해 사용하는 메시지 큐의 이름을 정의합니다.

기본값: ac_server_to_endpoint

ssl_custom

호스트 이름 확인자 함수 사용 여부를 지정합니다.

제한: 0 - 호스트 이름 확인자 함수 사용 안 함, 1 - 호스트 이름 확인자 함수 사용

기본값: 0

ssl_hostname

SSL 호스트 이름을 정의합니다.

기본값: none

ssl_identity

보고서 에이전트의 ID 를 정의합니다.

제한: 인증서 데이터를 포함하는 파일의 전체 경로 이름

기본값: none

ssl_issuer

SSL 연결에 대한 발급자 인증서를 정의합니다.

제한: 인증서 데이터를 포함하는 파일의 전체 경로 이름

기본값: none

ssl_key

보고서 에이전트 개인 키를 정의합니다.

제한: 개인 키를 포함하는 파일의 전체 경로 이름.

기본값: none

ssl_noverifyhost

호스트 인증서 확인을 사용할지 여부를 지정합니다.

제한: 0 - 호스트 인증서 확인 사용 안 함, 1 - 호스트 인증서 확인 사용

기본값: 0

ssl_noverifyhostname

호스트 이름 확인을 사용할지 여부를 지정합니다.

제한: 0 - 호스트 이름 확인 사용 안 함, 1 - 호스트 이름 확인 사용

기본값: 0

ssl_trace

SSL 추적을 사용할지 여부를 지정합니다.

제한: 0 - SSL 추적 사용 안 함, 1 - SSL 추적 사용

기본값: 0

ssl_trusted

SSL 연결에 대한 트러스트된 인증서를 정의합니다.

제한: 인증서 데이터를 포함하는 파일의 전체 경로 이름

기본값: none

global

[global] 섹션에서 토큰은 CA Access Control 끝점의 동작을 제어합니다.

accommon_path

accommon 디렉터리의 전체 경로 이름을 지정합니다.

기본값: /opt/CA/AccessControlShared/

ReportAgent

[ReportAgent] 섹션에서 토큰은 보고서 에이전트 데몬("ReportAgent")의 동작을 제어합니다.

audit_enabled

끝점 감사 데이터를 배포 서버로 보낼지 여부를 지정합니다.

값: 0 - 아니요, **1** - 예

기본값: 0

audit_filter

보고서 에이전트가 외부 소스(예: CA Enterprise Log Manager)로 라우팅하는 감사 레코드에 대한 필터링 규칙이 포함된 파일의 전체 경로 이름을 정의합니다. 이 파일에 따라 보고서 에이전트가 라우팅하는 레코드가 결정됩니다.

기본값: ACSharedDir/etc/auditrouteflt.cfg

audit_queue

보고서 에이전트가 끝점 감사 데이터를 보내는 큐의 이름을 정의합니다.

기본값: queue/audit

audit_read_chunk

보고서 에이전트가 감사 파일을 한 번 읽을 때 수집하는 최대 감사 레코드 수를 정의합니다.

제한: 양의 정수

기본값: 300

audit_send_chunk

보고서 에이전트가 각 연결에서 배포 서버로 보내는 최대 감사 레코드 수를 정의합니다. 보고서 에이전트는 수집한 감사 레코드 수가 이 개수에 도달하면 해당 레코드를 배포 서버로 보냅니다.

제한: 양의 정수

기본값: 1800

audit_sleep

보고서 에이전트가 감사 보고서 생성 사이에 수면하는 시간 간격을 정의합니다.

제한: 초 수를 나타내는 양의 정수

기본값: 10

audit_timeout

보고서 에이전트가 끝점 감사 데이터를 배포 서버로 보내야 하는 주기를 정의합니다. 마지막 전송 이후로 이 시간이 경과하면 보고서 에이전트는 수집한 레코드 수가 audit_send_chunk 값보다 적어도 감사 데이터를 배포 서버로 보냅니다.

제한: 초 수를 나타내는 양의 정수

기본값: 300

Debug

보고서 에이전트가 디버그 정보를 로깅하는지 여부를 지정합니다.

로깅하도록 지정(1)하면 보고서 에이전트는 다음을 로깅합니다.

- CA Access Control 는 ACSharedDir/log/ReportAgent.log 에 보고합니다.
- UNAB 는 ACSharedDir/log/unab2xml.log 에 보고(uxauthd)합니다.
- CA Enterprise Log Manager 는 ACSharedDir/log/audit2elm.log 에 보고합니다.

제한: 0: 보고서 에이전트가 디버그 정보를 로깅하지 않습니다. 1: 보고서 에이전트가 디버그 정보를 로깅합니다.

기본값: 0

interval

CA Access Control 이 보고서를 생성하여 배포 서버로 보내는 간격(분)을 정의합니다.

예약 설정은 간격 시작 시간과 작업 요일을 정의합니다. 보고서 에이전트가 예약된 발생보다 나중에 시작되는 경우 예약부터 계산된 다음 간격과 정의된 이후 간격마다 예약된 요일에 보고서를 보냅니다.

예: schedule=8:30@Mon,Tue,Wed 및 interval=5 가 있고 보고서 에이전트가 화요일 오전 8:47 에 로드되는 경우 보고서 에이전트는 오전 8:50 에 보고서를 생성하여 보냅니다. 이 시간이 예약된 시작 시간부터 5 분 간격을 사용하여 계산된 가장 빠른 주기입니다.

값: 0 - 간격 없음(예약된 발생만 사용); 양의 정수 - 간격으로 사용할 분 수

기본값: 0

reportagent_enabled

로컬 컴퓨터에서 보고를 활성화할지 여부를 지정합니다(1).

기본값: 0

schedule

보고서가 생성되어 배포 서버로 전송되는 시기를 정의합니다.

이 설정은 time@day[,day2][...] 형식으로 지정할 수 있습니다.

예를 들어 "19:22@Sun,Mon"을 지정하면 일요일과 월요일마다 오후 7:22 에 보고서가 생성됩니다.

기본값: 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

send_queue

보고서 에이전트가 로컬 데이터베이스의 스냅숏과 PMDB 를 보내는 배포 서버의 보고 큐 이름을 정의합니다.

기본값: queue/snapshots

추가 정보:

auditrouteflt.cfg 파일 - 감사 레코드 라우팅 필터링 (페이지 366)

seos.ini 초기화 파일

UNIX 에 해당

seos.ini 파일에는 CA Access Control 이 사용하는 다양한 설치 및 초기화 토큰이 들어 있습니다. 각 토큰은 다음 형식으로 파일 안에서 한 행을 차지합니다.

```
token = value
```

특정 유틸리티, 데몬 또는 기타 CA Access Control 의 기능에 해당하는 토큰을 포함하는 행은 섹션에 그룹화되어 있습니다. 각 섹션은 대괄호 안에서 섹션 이름을 제공하는 헤더 행으로 시작합니다. 모든 토큰은 섹션에 속합니다. 예를 들어 다음 행은 serevu 유틸리티를 관리하는 섹션을 시작합니다.

```
[serevu]
```

설치한 seos.ini 파일은 CA Access Control 에 의해 보호되며 CA Access Control 을 실행하는 동안에는 업데이트할 수 없습니다. 기본적으로 CA Access Control 에서 정의된 이 파일은 READ 권한을 가지고 있는데, 그 이유는 많은 유틸리티가 처리 중에 이 파일에 액세스하기 때문입니다. 유틸리티에서 seos.ini 파일을 읽을 수 없으면 오류가 발생합니다.

CA Access Control 이 실행되고 있는 동안 권한이 부여된 사용자가 파일을 업데이트할 수 있도록 하려면 다음 selang 명령을 입력하십시오.

```
newres FILE /opt/CA/AccessControl/seos.ini owner(authUser)
```

여기에서 authUser 는 권한이 부여된 사용자의 이름입니다. 이 명령은 authUser를 파일의 소유자로 설정하고, 파일의 소유자로서 authUser가 항상 파일을 업데이트할 수 있도록 합니다.

CA Access Control 끝점 관리 또는 seini 유틸리티를 사용하여 초기화 파일의 토큰을 읽고 추가하고 수정하고 삭제할 수 있습니다.

참고: seosd 가 실행되고 있지 않거나 데이터베이스의 규칙에서 특별히 허용하는 경우에만 seini 유틸리티는 seos.ini 파일을 업데이트할 수 있습니다.

secons -rl 명령을 사용하면 eosd 데몬을 다시 시작하지 않고도 업데이트된 토큰과 함께 seos.ini 파일을 다시 로드할 수 있습니다.

다음 표는 seos.ini 파일의 모든 섹션을 보여 줍니다.

섹션	설명
crypto	암호화 모듈 라이브러리 설정.
demons	seload 유틸리티가 자동으로 실행하는 CA Access Control 데몬 목록.
Dependency	사용자가 정의한 대로, CA Access Control 을 포함된 구성 요소로 사용하는 제품 목록.
devcalc	정책 위반 계산기(devcalc) 설정.
lang	CA Access Control 관리 인터페이스(selang) 설정.
ldap	LDAP 샘플 exit 에 대한 LDAP 서버 설정.
logmgr	로깅 기능 설정.
message	메시지 파일 설정.
-mfsd	메인프레임 동기화 데몬("mfsd") 설정.
OS_user	엔터프라이즈 사용자 저장 사용 설정.
package	설치된 CA Access Control 패키지 목록.
pam_seos	PAM(플러그형 인증 모듈) 프로그래밍 인터페이스 설정.
passwd	암호 대체 및 사용자 관련 서비스 설정
pmd	일반 정책 모델 데이터베이스 설정.
policyfetcher	Policy fetcher 데몬("policyfetcher") 설정.
pupmagent	PUPM 데몬(pupmagent) 설정
seauxd	Unicenter 달력 업데이트를 위한 보조 데몬(seauxd) 설정
segrace	사용자 로그인 정보 유틸리티(segrace) 설정.
seini	구성 파일 관리 유틸리티(seini) 특성.

섹션	설명
selock	데스크톱 비활성 보호 유틸리티(selock) 설정.
selogrd	로그 라우팅 데몬("selogrd" 및 "selogrcd") 설정.
seos	전역 구성 설정.
SEOS_syscall	SEOS_syscall 커널 모듈 설정.
seosd	권한 부여 데몬("seosd") 설정.
seosdb	데이터베이스 검사 및 재구축 설정.
seoswd	Watchdog 데몬("seoswd") 설정.
serevu	실패한 로그인 시도 확인 유틸리티(serevu) 유틸리티 설정.
sesu	CA Access Control 스위치 사용자 유틸리티(sesu) 설정.
sesudo	CA Access Control 대체 사용자 do 유틸리티(sesudo) 유틸리티 설정.
standalone	독립형 컴퓨터 관리 설정.
tng	Unicenter 와 CA Access Control 통합 설정.

crypto

[crypto] 섹션에서 토큰은 암호화 모듈과 관련된 부분을 제어합니다.

ca_certificate

CA(인증 기관) 데이터베이스에 대한 전체 경로 이름을 정의합니다.

기본값: ACInstallDir/data/crypto/def_root.pem

communication_mode

SSL(Secure Socket Layer) 프로토콜의 활성화 여부를 지정합니다.

이것을 ssl_only 로 설정하면 SSL V2, SSL V3 및 TLS 연결만 활성화됩니다. 즉, 이 컴퓨터는 SSL 을 지원하지 않는 컴퓨터와 통신할 수 없으며, 따라서 SSL 을 지원하지 않는 Access Control 이전 버전을 실행하는 컴퓨터와 통신할 수 없습니다.

fips_only 토큰이 1 로 설정되어 있으면 실제 통신 모드는 FIPS 모드(즉, TLS)에서 ssl_only 로 설정되며 communication_mode 토큰은 무시됩니다.

유효한 값:

- all_modes
- ssl_only
- non_ssl

기본값: non_ssl

CAPKIHOME

CAPKI 의 설치 디렉터리를 정의합니다.

기본값: /opt/CA/SharedComponents/CAPKI

fips_only

이 토큰은 CA Access Control 이 FIPS 전용 모드에서 작동할지 여부를 제어합니다. 이 모드에서는 FIPS 이외의 모든 기능이 비활성화됩니다.

유효한 값:

1 CA Access Control 이 FIPS 전용 모드에서 작동합니다.

0 CA Access Control 이 비 FIPS 모드에서 작동합니다.

기본값: 0

LIBRARY_PATH

ETPKI 암호화 라이브러리의 디렉터리를 정의합니다.

기본값: ACInstallDir/lib/etpki

private_key

제목 개인 키에 대한 전체 경로 이름을 정의합니다.

기본값: ACInstallDir/data/crypto/sub.key

ssl_port

CA Access Control 클라이언트와 서비스 간의 SSL 통신용 포트를 정의합니다.

기본값: 5249

subject_certificate

제목 인증서에 대한 전체 경로 이름을 정의합니다.

기본값: ACInstallDir/data/crypto/sub.pem

demons

[daemons] 섹션에서 각 토큰은 seload 유틸리티가 CA Access Control 설치 디렉터리에서 특정 프로그램을 실행할지 여부와 실행할 경우 실행 방법을 지정합니다. 각 토큰 이름은 CA Access Control 데몬 이름에 해당하거나 프로그램 별칭이며, 각 토큰에 여러 값을 할당할 수 있습니다.

program-name

다음 두 가지 가능성 중 하나를 지정합니다.

- 다음 값과 일치할 데몬이나 다른 프로그램의 이름:
  - yes 값과 일치하면 seload 는 기본 매개 변수를 사용하여 프로그램을 실행합니다.
  - no 값과 일치하면 seload 는 프로그램을 실행하지 않습니다.
  - 매개 변수 집합과 일치하면 seload 는 이러한 매개 변수를 사용하여 프로그램을 실행합니다.

  예를 들어 기본 매개 변수를 사용하여 CA Access Control 설치 디렉터리에서 serevu 를 실행하려면 다음을 입력하십시오.

  ```
  serevu=yes
  ```

  실행 중인 serevu 를 종료하려면 다음을 입력합니다. 이것은 serevu 토큰을 전혀 사용하지 않는 것과 같습니다.

  ```
  serevu=no
  ```

  지정된 매개 변수를 사용하여 CA Access Control 설치 디렉터리에서 serevu 를 실행하려면 다음을 입력하십시오.

  ```
  serevu=-f -d -t 1m -s 5m
  ```

- 데몬 또는 다른 프로그램의 절대 경로 이름과 일치할 더미 문자열. 선택적으로 그 뒤에 매개 변수를 사용할 수 있는데 seload 는 이 매개 변수에 따라 프로그램을 실행합니다.

  예를 들어 /opt/CA/AccessControl/bin 디렉터리에 있는 serevu 유틸리티를 실행하려면 지정된 매개 변수와 함께 다음을 입력하십시오.

  ```
  run_it=/opt/CA/AccessControl/bin/serevu -f 3 -d 6m -t 1m
  ```

  여러 프로그램에 대한 세부 사항을 포함시키려면 각 프로그램에 대해 토큰을 한 번만 사용합니다.

기본값: no

참고: seosd 데몬은 지정할 필요가 없습니다. seload 는 seosd 데몬이 실행되고 있는지를 항상 확인합니다.

Dependency

[Dependency] 섹션에서 각 사용자가 정의한 토큰은 CA Access Control 을 사용하는 제품을 포함된 구성 요소로 지정합니다.

product-name

CA Access Control 을 사용하는 제품을 포함된 구성 요소로 지정합니다. 유효한 값:

0 - 포함된 제품이 아닙니다.

1 - 포함된 CA Access Control 제품입니다.

기본값: 기본 제품이 지정되어 있지 않습니다.

devcalc

[devcalc] 섹션에서 토큰은 정책 위반 계산기와 관련된 부분을 제어합니다.

dms_command_retry_interval

각 DMS 알림 명령 재시도 사이의 시간(초)을 정의합니다.

기본값: 60

init_ac_db

더 이상 사용되지 않습니다.

max_dms_command_retry

포기하기 전까지 DMS 에 업데이트 알림을 보내는 정책 위반 계산기의 최대 재시도 횟수를 정의합니다.

기본값: 3

max_lines_request

get devcalc selang 명령이 정책 위반 데이터 파일로부터 한 번에 반환하는 최대 줄 수를 정의합니다. 그 후에 추가 행을 검색하려면 다음 명령을 사용해야 합니다.

```
get devcalc params("offset=X")
```

X

이전 get devcalc 출력에 의해 반환되는 줄 오프셋을 정의합니다.

기본값: 50

lang

[lang] 섹션에서 토큰은 selang, 보안 관리자 및 seadm 같은 selang 명령어 프로그램에서 사용하는 특성을 지정합니다.

check_password

selang 이 사용자에게 암호를 지정하도록 요청할지 여부를 결정합니다. 유효한 값:

no-selang 이 암호를 요청하지 않습니다.

yes-사용자에게 암호를 입력하라는 메시지가 표시됩니다.

기본값: no

exit_timeout

CA Access Control 이 허용하는 최대 exit 프로그램 실행 시간(초)을 지정합니다. 이 시간이 지나면 CA Access Control 이 exit 프로그램을 종료합니다.

기본값: 15

exits_dir

ACInstallDir/lbin/install_exits.sh 셸 스크립트로 exit 가 설치될 대상 디렉터리를 지정합니다.

기본값: ACInstallDir/exits

exits_source_dir

ACInstallDir/install_exits.sh 셸 스크립트로 exit 가 설치될 원본 디렉터리를 지정합니다.

기본값: ACInstallDir/exits-src

help_path

lang 도움말 파일이 위치한 디렉터리를 지정합니다.

기본값: ACInstallDir/data/langhelp

language

CA Access Control 의 설치 언어를 정의합니다(내부용).

기본값: English

max_groups_buffsize

보안 관리자가 데이터베이스와 통신할 때 사용하는 버퍼 크기(KB)를 지정합니다. 이 토큰은 UNIX 업데이트를 적용해야 할 때 사용합니다.

기본값: 128

no_check_password_users

암호를 입력하라는 메시지를 표시하지 않을 사용자를 지정합니다.

이 토큰은 check_password 토큰을 **yes** 로 설정한 경우에만 관련이 있습니다.

유효한 값은 쉼표로 구분된 사용자 목록입니다.

기본값: 없음

passwd_copy

사용자 정보를 변경한 후 임시 파일을 다시 원본 파일로 복사할 때 컴퓨터 암호 파일(/etc/passwd) 또는 PMDB 암호 파일(/PMDB_Directory/policies/pmdb/ passwd)의 업데이트 방법을 지정합니다. 유효한 값은 다음과 같습니다.

fast_copy - 파일 정보를 복사합니다.

rename - 새 파일을 가리키도록 디렉터리를 변경합니다.

기본값: fast_copy

post_group_exit

UNIX 환경에서 그룹 명령을 실행한 후 호출할 exit 프로그램의 경로를 지정합니다.

기본값: ACInstallDir/exits/lang_exit.sh

post_user_exit

UNIX 환경에서 사용자 명령을 실행한 후 호출할 exit 프로그램의 경로를 지정합니다.

기본값: ACInstallDir/exits/lang_exit.sh

pre_group_exit

UNIX 환경에서 그룹 명령을 실행하기 전 호출할 exit 프로그램의 경로를 지정합니다.

기본값: ACInstallDir/exits/lang_exit.sh

pre_user_exit

UNIX 환경에서 사용자 명령을 실행하기 전 호출할 exit 프로그램의 경로를 지정합니다.

기본값: ACInstallDir/exits/lang_exit.sh

query_size

데이터베이스 쿼리에 나열할 최대 레코드 수를 지정합니다.

기본값: 100

RecvTimeOut

시간이 초과되기 전에 selang 이 정보를 받기 위해 대기할 최대 시간(초)을 지정합니다.

값을 0 으로 설정하면 시간 초과 값이 설정되지 않습니다.

기본값: 60

SendTimeOut

시간이 초과되기 전에 selang 이 정보를 보내기 위해 대기할 최대 시간(초)을 지정합니다.

값을 0 으로 설정하면 시간 초과 값이 설정되지 않습니다.

기본값: 60

SetBlockRun

프로그램이 트러스트되었는지 확인하고 언트러스트된 프로그램의 실행을 차단할지 여부를 지정합니다. 실행 차단은 프로그램이 setuid 인지 일반 프로그램인지에 관계없이 수행됩니다.

올바른 값은 다음과 같습니다.

yes-viapgm 권한 부여 규칙으로 정의된 모든 프로그램에서 blockrun 속성이 yes 로 설정됩니다.

no-viapgm 권한 부여 규칙으로 정의된 모든 프로그램에서 blockrun 속성이 no 로 설정됩니다.

suid-모든 setuid 프로그램에서는 blockrun 속성이 yes 로 설정되고, 다른 모든 프로그램에서는 blockrun 속성이 no 로 설정됩니다.

기본값: yes

swap_deletion_order

"ru userName unix" 명령(사용자 삭제)이 selang 에서 실행되는 순서를 정의합니다. 일반적으로 이 명령은 AC 환경에서 먼저 실행된 후 UNIX 환경에서 실행됩니다. 경우에 따라(예: 그룹 관리자가 사용자 삭제) 이 순서를 바꿀 수 있습니다.

유효한 값:

no - UNIX 환경보다 AC 환경에서 먼저 사용자를 제거합니다.

yes - AC 환경보다 UNIX 환경에서 먼저 사용자를 제거합니다.

기본값: no

timeout

클라이언트가 seosd 데몬의 응답을 기다리는 최대 시간을 지정합니다(단위: 초). seosd 가 이 시간 동안 응답하지 않는 경우 오류 메시지를 보내 seosd 가 응답하지 않음을 알립니다. 그러면 클라이언트는 seosd 연결 시도를 중지합니다.

기본값: 90

use_old_commands

이전 ACF2 호환성 명령(ag, lg, rg, lu, au 등)의 비활성화 여부를 지정합니다.

기본값: 1(이전 명령 지원)

use_unix_file_owner

UNIX 환경의 파일 소유자가 파일을 CA Access Control 에 대해 정의할 수 있는지 여부를 지정합니다. 값이 yes 이면 UNIX 환경의 파일 소유자는 newres 또는 newfile 명령을 사용하여 파일을 CA Access Control 에 대해 정의할 수 있습니다.

파일이 이미 CA Access Control 에 대해 정의되어 있으면, 일반적인 CA Access Control 권한 부여 규칙에 따라 데이터베이스에서 해당 매개 변수를 변경할 수 있도록 허용된 경우가 아니면 사용자는 매개 변수를 변경할 수 없습니다.

유효한 값은 yes 와 no 입니다.

기본값: no

ldap

[ldap] 섹션에서 토큰은 LDAP 서버 및 입력 데이터를 찾는 데 사용하는 특성을 지정합니다. 이러한 매개 변수는 ACInstallDir/samples/ldap/exits/S50CREATE_Ldap_u.sh 에 있는 ldap 샘플 exit 프로그램에서만 사용됩니다.

base_entry

기본 항목 요소로 사용되는 LDAP 디렉터리 트리의 지점을 지정합니다.

예를 들어, o=organization_name, c=country_name 을 사용할 수 있습니다.

기본값: 토큰이 설정되지 않음

host

LDAP 서버의 호스트 이름을 지정합니다.

기본값: 토큰이 설정되지 않음(localhost)

path

LDAP 클라이언트 기본 디렉터리를 지정합니다.

기본값: 토큰이 설정되지 않음(/usr/local/ldap)

port

LDAP 서버 포트를 지정합니다(선택 사항).

기본값: 토큰이 설정되지 않음(389)

logmgr

[logmgr] 섹션에서 토큰은 로그인 기능의 동작을 제어합니다.

audit_back

감사 로그 백업 파일의 이름을 지정합니다. CA Access Control 만 이 파일에 쓸 수 있습니다. 사용자는 이 파일에 대해 READ 권한만 가질 수 있습니다.

기본값: ACInstallDir/log/seos.audit.bak

audit_group

감사 로그를 읽을 수 있는 그룹을 지정합니다. 이 토큰을 **none** 으로 설정하면 root 사용자만 감사 로그를 읽을 수 있습니다. CA Access Control 은 이 토큰의 값을 확인하지 않습니다. 따라서 사용자가 잘못된 그룹 이름을 입력하면 CA Access Control 은 감사 로그 파일에 어떤 그룹 권한도 할당하지 않습니다.

기존 감사 로그 파일의 그룹 소유권을 변경하려면 다음 단계를 수행합니다.

selang 명령 chgrp 을 사용하여 파일의 그룹 소유권을 설정합니다.

다음 명령을 입력하여 UNIX 허용 권한을 변경합니다.

```
chmod 640 ACInstallDir/log/seos.audit
```

기본값: 없음.

audit_log

감사 로그 파일의 이름을 지정합니다. 이 파일이 audit_size 에 지정된 크기에 도달하면 CA Access Control 은 파일을 닫고, 파일 이름을 audit_back 에 있는 이름으로 변경하고, 새 감사 로그를 작성합니다. CA Access Control 만 이 파일에 쓸 수 있습니다. 사용자는 이 파일에 대해 READ 권한만 가질 수 있습니다.

기본값: ACInstallDir/log/seos.audit

audit_max_files

CA Access Control 이 날짜 트리거된 백업을 수행할 때 누적하는 감사 로그 백업 파일의 최대 개수를 정의합니다. BackUp_Date 구성 설정이 none 이외의 값으로 설정된 경우 CA Access Control 은 날짜 트리거된 백업 파일을 계속 누적합니다. 이 구성 설정을 사용하면 CA Access Control 이 감사 로그 백업에 사용하는 디스크 공간을 줄일 수 있습니다. 감사 로그 백업 파일의 수가 설정한 제한에 도달하면 CA Access Control 은 새 백업 파일을 만들 때 가장 오래된 백업 파일을 삭제합니다.

값:

- **0** - 모든 감사 로그 백업 파일 유지
- n - 0 보다 큰 양의 정수

참고: 중복 감사 로그 백업 파일은 CA Access Control 에서 자동으로 보호되기 때문에 수동으로 제거할 수 없습니다. 또한 감사 보고가 사용되면 CA Access Control 은 보고서 에이전트가 프로세스를 완료할 때까지 백업 파일을 삭제하지 않습니다.

기본값: 0

audit_size

감사 로그 파일의 최대 크기(KB)를 지정합니다.

최소값: 50 KB

기본값: 1024

참고: 감사 파일 크기가 2 GB 를 초과하면 CA Access Control 은 감사 레코드를 감사 파일에 기록하는 것을 중단합니다.

BackUp_Date

CA Access Control 이 백업을 수행하는 기준을 설정합니다.

유효한 값은 none, yes, daily, weekly 및 monthly 입니다.

yes 를 지정하면 CA Access Control 은 크기 제한 토큰인 audit_size 에 따라 백업을 수행하고 파일에 타임스탬프를 설정합니다.

none 을 지정하면 CA Access Control 은 audit_size 토큰에 따라 백업을 수행하지만 파일에 타임스탬프를 설정하지는 않습니다.

daily, **weekly** 또는 **monthly** 를 지정하면 CA Access Control 은 처음으로 감사 로그 백업 파일을 만들 때 타임스탬프를 추가합니다. 현재 날짜가 타임스탬프를 지난 경우 CA Access Control 은 자동으로 백업 파일을 만들고 그 파일에 타임스탬프를 설정합니다.

그러나 감사 로그 파일의 크기가 audit_size 토큰의 값을 처음으로 초과하면 CA Access Control 은 타임스탬프를 발행하지 않고 백업 파일을 작성합니다.

기본값: 없음

error_back

오류 로그 백업 파일의 이름을 지정합니다.

기본값: ACInstallDir/log/seos.error.bak

error_group

오류 로그 파일을 읽을 수 있는 그룹을 지정합니다. 이 토큰을 **none** 으로 설정하면 root 사용자만 오류 로그 파일을 읽을 수 있습니다. CA Access Control 은 이 토큰의 값을 확인하지 않습니다. 따라서 사용자가 잘못된 그룹 이름을 입력하면 CA Access Control 은 오류 로그 파일에 어떤 그룹 권한도 할당하지 않습니다.

기존 오류 로그 파일의 그룹 소유권을 변경하려면 다음 단계를 수행합니다.

selang 명령 chgrp 을 사용하여 파일의 그룹 소유권을 설정합니다.

다음 명령을 입력하여 UNIX 허용 권한을 변경합니다.

```
chmod 640 ACInstallDir/log/seos.audit
```

기본값: 없음

error_log

오류 로그 파일의 이름을 지정합니다. 이 파일이 erro_size 에 지정된 크기에 도달하면 CA Access Control 은 파일을 닫고, 파일 이름을 error_back 에 있는 이름으로 변경하고, 새 오류 로그를 작성합니다. CA Access Control 만 이 파일에 쓸 수 있습니다.

기본값: ACInstallDir/log/seos.error

error_size

오류 로그 파일의 최대 크기(KB)를 정의합니다.

제한: 최소값 50KB.

기본값: 50

irecorder_audit

IR API 라이브러리가 로컬 보안 데몬 감사 이벤트 외에 기존 PMD 의 감사 이벤트도 라우트할지 여부를 지정합니다.

"all" - 로컬 보안 데몬 감사 이벤트 외에 정책 모델의 감사 이벤트도 라우트합니다.

"localhost" - 로컬 보안 데몬의 감사 이벤트만 라우트합니다.

기본값: all

logconnected

TCP-CONNECTED 레코드가 감사 로그를 작성하지 못하게 합니다.

이 기능을 사용하려면 logconnected 를 No 로 설정합니다.

기본값: 없음

추가 정보:

seaudit 유틸리티-감사 로그 레코드 표시 (페이지 95)
seerrlog 유틸리티-오류 로그 레코드 표시 (페이지 153)

message

[message] 섹션에서 토큰은 메시지 유틸리티 semsgtool 의 동작을 제어합니다.

filename

대부분의 메시지를 제공하는 파일의 위치와 이름을 지정하고 이러한 메시지는 입력한 selang 명령에 대한 응답으로 나타납니다.

기본값: ACInstallDir/data/seos.msg

mfsd

[mfsd] 섹션에서 토큰은 메인프레임 동기화 데몬 옵션을 정의합니다.

mfsd_trace_file

CA Access Control 메인프레임 동기화 데몬 mfsd 추적 메시지가 기록될 파일의 위치를 지정합니다.

이 토큰을 **no** 로 설정하면 추적 파일이 생성되지 않습니다.

기본값: ACInstallDir/log/mfsd.trace

OS_User

[OS_User] 섹션의 토큰은 엔터프라이즈 사용자 및 엔터프라이즈 그룹에 대해 CA Access Control 이 사용하는 설정을 정의합니다.

create_user_in_db

CA Access Control 에 대해 정의되지 않은 사용자의 XUSER 레코드를 CA Access Control 이 작성할지 여부 및 해당 사용자의 로그인 시간을 지정합니다.

참고: 이 설정은 엔터프라이즈 사용자(osuser_enabled 가 1 로 설정됨)를 사용할 경우에만 적용됩니다.

유효한 값:

0 - CA Access Control 이 자동으로 XUSER 레코드를 작성하지 않습니다.

1 - CA Access Control 이 자동으로 XUSER 레코드를 작성합니다.

기본값: 1

osuser_enabled

엔터프라이즈 사용자 및 그룹의 활성화 여부를 지정합니다.

유효한 값:

0 - 엔터프라이즈 사용자 및 그룹의 사용이 비활성화됩니다.

1 - 엔터프라이즈 사용자 및 그룹의 사용이 활성화됩니다.

기본값: 0

UserCache_groups_max

런타임 사용자 캐시 테이블에 사용할 그룹의 최대 수를 정의합니다.

기본값: 1000

UserCache_max

런타임 사용자 캐시 테이블에 사용할 항목의 최대 수를 정의합니다.

기본값: 16000

UserCache_timeout

런타임 사용자 캐시 테이블에서 레코드가 제거되기 전의 간격(분)을 정의합니다.

기본값: 60

verify_osuser

CA Access Control 이 엔터프라이즈 사용자 레코드(XUSER)를 작성하기 전에 엔터프라이즈 저장소에 사용자가 있는지를 확인할지 여부를 지정합니다.

유효한 값:

1 - 엔터프라이즈 사용자 저장소에 사용자가 정의되어 있는 경우에만 CA Access Control 이 엔터프라이즈 사용자 레코드를 작성합니다.

0 - CA Access Control 은 항상 엔터프라이즈 사용자 레코드를 작성합니다.

기본값: 0

package

[package] 섹션에서 토큰은 사용자가 설치할 패키지를 지정합니다.

Client, Server, Admin, Mfsd, Tng, Stop, Api

지정한 패키지를 설치하도록 선택했는지 여부를 나타냅니다.

기본값: no

pam_seos

[pam_seos] 섹션에서 토큰은 프로그래밍 인터페이스 PAM(Pluggable Authentication Module)을 완전히 사용할 수 있도록 도와 줍니다.

참고: [pam_seos] 섹션은 HP-UX 11.00 과 Sun Solaris 7.1 이상에서만 사용할 수 있습니다.

api_update_lastaccterm

API 라이브러리가 SEOS_VerifyCreate 를 통해 사용자의 마지막 액세스 시간 및 날짜를 업데이트할지 여부를 지정합니다.

유효한 값:

0 - 마지막 액세스 시간 및 날짜가 업데이트되지 않습니다.

1 - 마지막 액세스 시간 및 날짜가 업데이트됩니다.

기본값: 토큰이 설정되지 않음(0)

bypass_services

PAM 이 바이패스하는 서비스를 정의합니다.

기본값: ftp,vsftpd

call_segrace

모든 로그인으로 segrace 유틸리티를 자동으로 호출할지 여부를 지정합니다.

유효한 값은 yes 와 no 입니다.

기본값: no

debug_mode_for_user

사용자에게 로그인 거부 이유를 알려줄지 여부를 지정합니다.

유효한 값은 yes 와 no 입니다.

기본값: no

failed_login_file

실패한 로그인 감사 파일 pam_seos 의 위치를 지정합니다.

기본값: ACInstallDir/pam_seos_failed_logins.log

PamPassUserInfo

pam_seos 가 사용자 정보를 seosd 로 보낼지 여부를 지정합니다. CA Access Control 에 정보가 없는 엔터프라이즈 사용자를 사용할 때 필요합니다. 엔터프라이즈 사용자를 사용하지 않는 경우(osuser_enabled = no) 이 설정을 0 으로 지정하십시오.

값: 0 - 사용자 정보를 보내지 않음, **1** - 사용자 정보를 보냄

기본값: 0

process_failed_logins

사용자 암호를 인증하고 실패한 로그인을 처리하기 위해 pam_seos 가 pam_authenticate 를 호출하도록 지정합니다.

pam_authenticate 를 두 번 호출하지 않으려면 이 값을 0 으로 설정하십시오.

값: 0 - CA Access Control PAM 모듈에서 pam_authenticate 를 호출하지 않습니다. **1** - CA Access Control PAM 모듈에서 pam_authenticate 를 호출합니다.

기본값: 1

serevu_use_pam_seos

serevu 가 시스템 파일 대신 pam_seos 로그인 오류 로그 파일을 사용해야 하는지 여부를 지정합니다.

이 기능을 사용하면 serevu 의 정확성이 높아집니다.

기본값: HP-UX Itanium(IA64) 및 Linux 에서는 yes, 기타 운영 체제에서는 no.

passwd

[passwd] 섹션에서 토큰은 암호 대체 및 기타 사용자 관련 서비스를 정의합니다.

AllowedGidRange

사용자가 추가, 업데이트 및 삭제할 수 있는 GID 의 범위를 지정합니다. 이 범위를 벗어난 값은 CA Access Control 이 업데이트할 수 없는 예약된 GID 를 나타냅니다.

참고: 하나의 정수만 지정하는 경우 1 부터 지정된 정수 사이의 모든 정수가 예약된 GID 입니다. 상한값보다 높은 숫자를 지정하면 기본 상한값(30000)이 적용됩니다. 음수를 지정하면 기본 하한값(1)이 적용됩니다.

제한: 1 ~ 2147483647

기본값: 100,30000

AllowedUidRange

사용자가 추가, 업데이트 및 삭제할 수 있는 UID 의 범위를 지정합니다. 이 범위를 벗어난 값은 CA Access Control 이 업데이트할 수 없는 예약된 UID 를 나타냅니다.

참고: 하나의 정수만 지정하는 경우 1 부터 지정된 정수 사이의 모든 정수가 예약된 UID 입니다. 상한값보다 높은 숫자를 지정하면 기본 상한값(30000)이 적용됩니다. 음수를 지정하면 기본 하한값(1)이 적용됩니다.

제한: 1 ~ 2147483647

기본값: 100,30000

AllowRootProp

sepass -p 또는 sepass -s 를 사용하여 변경한 루트 암호를 정책 모델로 전송할지 여부를 지정합니다. 그런 다음에는 PMD 가 해당 구독자에게 암호를 전파합니다.

유효한 값은 yes 와 no 입니다.

기본값: no

change_pam

로컬 호스트가 LDAP 데이터베이스에서 암호 인증 및 변경을 위해 PAM 을 사용할지 여부를 지정합니다.

기본값: no

Check_Adm_Rules

ADMIN 사용자에 대해 암호 규칙을 적용할지 여부를 지정합니다.

기본값: no

Check_All_User_Rules

selang 이 모든 사용자에 대해 암호 규칙을 확인해야 하는지 여부를 지정합니다.

유효한 값은 yes 와 no 입니다.

이 토큰을 yes 로 설정하면 selang 은 모든 사용자에 대해 암호 규칙을 확인합니다.

이 토큰을 no 로 설정하면 selang 은 암호를 변경하는 사용자에 대해서만 암호 규칙을 확인합니다.

기본값: no

CreateHashedPasswdDatabase

(DEC UNIX 전용). 사용자 레코드를 작성, 업데이트 또는 제거하는 각 CA Access Control 명령을 사용한 이후 또는 sepass 유틸리티를 사용하여 각 사용자 암호를 변경한 이후 exit 스크립트를 실행할지 여부를 지정합니다.

참고: 자세한 사용 지침은 ACInstallDir/samples/exits-src/USER_POST 디렉터리의 추가 정보 파일을 참조하십시오.

기본값: no

DefaultHome

시스템의 기본 홈 디렉터리를 지정합니다. 사용자의 홈 디렉터리는 지정한 시스템 홈 디렉터리의 하위 디렉터리입니다. 예를 들어, 시스템 홈 디렉터리가 /home 인 경우 새 사용자의 홈 디렉터리는 /home/username 입니다. 이 토큰의 값을 지정하면 지정된 값은 클라이언트의 lang.ini 파일에 있는 값을 무시합니다. nohomedir 을 지정하면 홈 디렉터리는 자동으로 설정되지 않습니다.

기본값: /home

DefaultPasswdCmd

기본 암호 프로그램을 지정합니다. 지정하는 경우 sepass 가 시작될 때, 그리고 seosd 가 실행되지 않을 때 이 암호 프로그램이 사용됩니다.

기본값: /bin/passwd

DefaultPgroup

값을 입력하지 않는 경우 CA Access Control 이 새 UNIX 사용자에게 할당할 주 그룹을 지정합니다.

기본값: 기타

DefaultShell

값을 입력하지 않는 경우 CA Access Control 이 새 UNIX 사용자에게 할당할 기본 셸을 지정합니다. 이 토큰의 값을 지정하면 지정된 값은 클라이언트의 lang.ini 파일에 있는 값을 무시합니다.

기본값: /bin/sh(HP-UX 에서는 /sbin/sh)

Dictionary

암호로 사용할 수 없는 단어가 포함된 파일의 전체 경로 이름을 정의합니다.

참고: 이 파일을 사용하려면 사전 형식 암호 규칙(use_dbdict)을 file 로 설정하고 UseDict 설정을 yes 로 설정해야 합니다. 사전 형식을 db 로 설정한 경우 사용할 수 없는 암호를 CA Access Control 로부터 가져오며 이 설정은 무시됩니다. 이 값은 UNIX 에서 기본값입니다.

기본값: /usr/dict/words

GeneratePasswd

sepass 가 직접 새 암호를 생성하는지 여부를 지정합니다.

유효한 값은 yes 와 no 입니다.

이 토큰을 **no** 로 설정하면 사용자에게 새 암호를 입력하라는 메시지가 나타납니다.

기본값: no

HomeDirUpd

사용자의 주 그룹이 변경될 때 CA Access Control 이 사용자 홈 디렉터리의 그룹 소유권을 업데이트할지 여부를 지정합니다.

유효한 값은 **yes** 와 **no** 입니다.

기본값: yes

nis_env

로컬 호스트가 NIS 인지 NIS+ 클라이언트인지를 지정합니다.

유효한 값은 no, nis 또는 nisplus 입니다.

기본값: no

NisPlus_server

이 스테이션이 NIS+ 서버인지 여부를 지정합니다.

유효한 값은 yes 와 no 입니다.

토큰 값이 yes 이면 CA Access Control 은 암호 변경을 NIS+ 암호 변경으로 간주합니다.

기본값: no

only_local

sepass 의 기본 설정에 -l 플래그가 포함되는지 여부를 결정합니다.

유효한 값은 yes 와 no 입니다.

이 토큰을 yes 로 설정하면 sepass 는 로컬 즉, 로컬 암호 파일(일반적으로 /etc/passwd), 보안 파일 및 로컬 데이터베이스에서만 암호를 변경합니다.

기본값: no

only_pmdb

sepass 의 기본 설정에 -p 플래그가 포함되는지 여부를 지정합니다. 토큰 값이 yes 이면 지정된 호스트의 PMDB 에서만 암호를 변경하도록 sepass 에 지시합니다.

이러한 데이터베이스가 정의되지 않은 경우 sepass 는 아무 작업도 하지 않습니다.

기본값: no

passwd_distribution_encryption_mode

정책 모델 서비스의 일부로서 암호를 배포할 때 사용자 암호를 암호화하기 위해 사용할 방법을 지정합니다.

유효한 값:

1 - 호환성 모드: 긴 암호를 사용하지 않는 CA Access Control 시스템 간에 암호를 배포하는 데 사용합니다. 여기에는 r12.0 보다 이전 버전의 CA Access Control 을 실행하는 모든 컴퓨터가 포함됩니다.

2 - MD5 모드: 긴 암호를 사용하며 Linux 를 실행하는 CA Access Control 시스템 간에 암호를 배포하는 데 사용합니다.

3 - 양방향 모드: 긴 암호를 사용하는 임의의 CA Access Control 시스템 사이에서 암호화된 메시지에 포함된 일반 텍스트로 안전하게 암호를 배포하는 데 사용합니다.

기본값: 1

passwd_format

암호 변경이 NT 호스트에 전파되는지 여부를 나타냅니다.

이 토큰을 **NT** 로 설정하면 관리하는 호스트 중 하나가 NT 호스트임을 의미합니다.

기본값: 없음

passwd_local_encryption_method

사용자 암호를 로컬에 저장할 때 이러한 암호를 암호화하기 위해 사용할 방법을 지정합니다.

유효한 값:

crypt - 암호의 첫 8 자만 (DES 키로서) 사용하는 표준 단방향 UNIX 암호화. crypt 를 지정하면 긴 암호 사용이 비활성화됩니다.

md5 - 길이 제한이 없는 암호를 암호화할 수 있는 MD5 해시 함수. md5 를 지정하면 긴 암호 사용이 활성화됩니다.

기본값: crypt

PromptOldPassword

sepass 가 /opt/CA/AccessControl/ bin/segrace 를 통해 호출될 때 로컬 사용자에게 이전 암호를 묻는 메시지를 표시할지 여부를 지정합니다. 이때 전체 경로를 사용해야 합니다.

이 토큰을 **yes** 로 설정하면 사용자에게 이전 암호를 입력하라는 메시지가 표시됩니다.

기본값: yes

quiet_mode

sepass 가 정책 모델로의 암호 전파에 대한 메시지와 저작권 고지 사항을 표시할지 여부를 지정합니다.

기본값: no

RootPwAsOwn

권한 있는 사용자가 sepass 를 사용하여 마치 루트 사용자처럼 루트 암호를 변경할 수 있는지 여부를 지정합니다(-x 옵션 사용).

유효한 값:

yes-권한 있는 사용자가 sepass 를 사용하여 마치 루트 사용자처럼 루트 암호를 변경할 수 있습니다. 권한 있는 사용자가 자기 자신으로서(관리상 변경) 루트 암호를 변경할 수는 없습니다.

no-권한 있는 사용자가 sepass 를 사용하여 자기 자신으로서만(관리상 변경) 루트 암호를 변경할 수 있습니다.

예를 들어, 이 토큰이 yes 로 설정된 경우 권한 있는 사용자는 다음 명령을 사용하여 루트 암호를 변경할 수 있습니다.

```
sepass -x root
```

동일한 사용자가 다음 명령을 사용하여 루트 암호를 변경할 수는 없습니다.

```
sepass root
```

이 토큰이 no 로 설정된 경우 반대 상황이 적용됩니다.

기본값: no

SaveGroupAttrs

이전 그룹 파일 소유자, 그룹 및 모드가 UNIX 환경에서 그룹 업데이트 이후 예약되었는지 여부를 지정합니다.

유효한 값은 yes 와 no 입니다.

이 토큰을 **no** 로 설정하면 새로운 값은 각각 0, 0, 644 로 설정됩니다.

기본값: no

SavePasswdAttrs

이전 암호 파일 소유자, 그룹 및 모드가 UNIX 환경에서 사용자 업데이트 이후 예약되었는지 여부를 지정합니다.

유효한 값은 yes 와 no 입니다.

이 토큰을 **no** 로 설정하면 새로운 값은 각각 0, 0, 644 로 설정됩니다.

기본값: no

Shadow_Admin_Change

(AIX 플랫폼 전용). 관리자가 selang 에서 또는 sepass 를 사용하여 암호를 변경하는 경우 ADMCHG 플래그가 /etc/security/passwd 파일의 사용자 항목에 추가될지 여부를 지정합니다.

기본값: no

UIDAlgorithm

새 사용자를 추가할 때 사용할 자동 UID 알고리즘을 지정합니다. 이 알고리즘을 다른 값으로 설정하면 이전 프로세스가 선택됩니다. 새 알고리즘은 64KB 이상의 UID 번호를 제공하며 일반적으로 속도가 더 빠릅니다.

기본값: new

UseDict

암호를 확인할 때 Dictionary 설정으로 설정한 dictionary 파일을 사용할지 여부를 지정합니다.

참고: 또한, 사전 파일을 사용하려면 사전 형식 암호 규칙(use_dbdict)을 file 로 설정해야 합니다. 사전 형식을 db 로 설정한 경우 사용할 수 없는 암호를 CA Access Control 로부터 가져오며 이 설정은 무시됩니다.

기본값: no

YpGrpCmd

NIS 그룹 맵 생성에 사용할 명령을 지정합니다.

기본값: make group

YpMakeDir

NIS 맵을 생성할 때 사용할 makefile 디렉터리의 이름을 지정합니다.

기본값: /var/yp

YpPassCmd

NIS 암호 맵 생성에 사용할 명령을 지정합니다.

기본값: make passwd

YpServerGroup

NIS 그룹 맵을 만들 그룹 파일을 지정합니다.

기본값: /etc/group

YpServerPasswd

NIS 암호 맵을 만들 암호 파일을 지정합니다.

기본값: /etc/passwd

YpServerSecure

NIS 암호 맵 작성에 사용된 암호가 들어 있는 보안 파일의 이름을 지정합니다.

기본값: 플랫폼에 따라 다름:

- IBM AIX: /etc/security/passwd
- HP-UX: /.secure/etc/passwd
- Sun Solaris: /etc/shadow

YpTimeOut

새 클라이언트(selang, Security Administrator 등)가 ypbind 테스트(로컬 호스트와 NIS 서버의 연결 여부를 결정하는 테스트)를 실행할 수 있는 시간을 지정합니다(단위: 초). 시간이 만료되면 클라이언트는 종료되고 오류 메시지가 나타납니다.

기본값 영(**0**)은 ypbind 테스트가 수행되지 않음을 의미입니다.

기본값: 0

추가 정보:

sepass 유틸리티-암호 설정 또는 교체 (페이지 179)

pmd

[pmd] 섹션에서 토큰은 PMDB 특성을 결정합니다.

참고: seos.ini 이외에도 각 정책 모델에는 pmd.ini 라는 구성 파일이 있습니다.

_min_retries_

사용할 수 없는 구독자에게 큐에 있는 다음번 업데이트를 다시 보내기 위해 sepmdd 가 시도해야 하는 최소 횟수를 지정합니다. sepmdd 는 보내지 못한 업데이트를 위해 구독자 목록을 처음부터 끝까지 돌며, 사용할 수 없는 구독자에게 업데이트를 다시 보낼 수 없으면 매회 카운터를 늘립니다. 이 토큰에 지정된 최소 시도 횟수 이후 구독자는 사용할 수 없는 상태로 표시됩니다.

기본값: 4

_pmd_directory_

PMDB 가 있는 디렉터리를 지정합니다. 이름에는 최대 70 자의 영숫자를 사용할 수 있습니다. 디렉터리의 전체 경로를 지정합니다. 각 정책 모델은 pmdDirectory/pmdName 디렉터리에 위치합니다.

기본값: ACInstallDir/policies

_PMD_DIRECTORY_

_pmd_directory_와 동일

_PMD_EXEC

정책 모델 데몬의 이름을 정의합니다.

기본값: sepmdd

_QD_timeout_

구독자 목록의 첫 번째 스캔 중에 sepmdd 데몬이 구독자 데이터베이스를 업데이트하는 동안 대기하는 최대 시간(초)을 지정합니다. 시간이 경과되어도 데몬이 구독자 업데이트에 성공하지 못하면 해당하는 특정 구독자를 건너뛰고 목록에 있는 나머지 구독자를 업데이트합니다.

구독자 목록의 첫 스캔이 완료되면 sepmdd 는 첫 스캔 중에 업데이트하지 못한 구독자를 업데이트하는 두 번째 스캔을 수행합니다. 두번째 검사 중에는 연결 시스템 호출 시간(약 90 초)이 만료될 때까지 구독자를 업데이트합니다.

기본값: 3

_retry_timeout_

_min_retries_에 지정된 최소 시도 횟수를 수행한 후, 사용할 수 없는 구독자에게 업데이트를 다시 보내려고 시도하기까지 기다려야 하는 시간(분)을 지정합니다. 이 토큰에 정의된 시간(분)이 경과한 후 구독자는 사용 가능한 것으로 표시됩니다.

다음을 수행할 때까지 구독자는 사용할 수 없는 상태로 표시됩니다.

- 구독자는 수동으로 해제됩니다.
- sepmdd 는 수동으로 종료되고 다시 시작됩니다. sepmdd 는 다음의 경우 다시 시작됩니다.
  - 언어 기능이 연결을 시도하는 경우
  - 부모 PMDB 가 업데이트를 보내고자 하는 경우
  - 구독자가 pull 옵션을 트리거한 경우 이는 CA Access Control 이 구독자에서 시작될 때 선택적으로 발생합니다.

- 사용할 수 없는 구독자에 의해 pull 옵션이 트리거되었습니다.

참고: 데몬을 다시 시작하는 데에는 시간이 걸리며 그로 인해 전체 전파 프로세스의 속도가 느려질 수 있으므로 sepmdd 를 너무 자주 종료하는 것은 바람직하지 못합니다. 안정성 문제가 있을 수 있으므로 sepmdd 를 항상 실행 상태로 두는 것도 바람직하지 못합니다. 그러나 이는 추측일 뿐입니다.

기본값: 30 분

_shutoff_time_

sepmdd 가 종료되기 전 활동 시간(분)을 지정합니다. 토큰 값이 0 이면 sepmdd 가 종료되지 않습니다.

기본값: 0

ClientOperationTimeout

클라이언트가 정책 모델의 응답을 기다리는 시간 만료 기간(초)을 정의합니다.

기본값: 60

is_maker_checker

이중 컨트롤을 사용할지 여부를 지정합니다.

유효한 값은 yes 와 no 입니다.

토큰 값이 **yes** 이면 데이터베이스를 직접 업데이트할 수 없고 PMDB 를 통해서만 가능하며, 두 관리자인 Maker 와 Checker 가 공동으로 업데이트를 수행해야 합니다.

기본값: 토큰이 설정되지 않음(no)

pass_auth

원격 암호 변경 시 sepass 가 호출자의 암호를 확인할지 여부를 지정합니다. sepass 유틸리티는 사용자가 입력한 이전 암호와 로컬 prodname 데이터베이스에 저장된 암호를 항상 비교합니다. 이 토큰을 yes 로 설정하면 sepass 는 또한 sepass 를 실행하는 사용자가 입력한 이전 암호를 원격 prodname 데이터베이스(대개 pmdb)에 저장된 사용자 자신의 암호와 비교합니다. 즉, sepass 사용자는 다른 사용자의 암호를 변경할 때에도 자신의 암호를 입력해야 합니다.

값: yes, no

기본값: yes

pull_option

구독자 데이터베이스를 사용할 수 있게 되는 즉시 업데이트할지 여부를 지정합니다.

유효한 값은 yes 와 no 입니다.

토큰 값이 **yes** 이면, 구독자 스테이션이 사용 가능해지는 즉시 seagent 는 컴퓨터에 있는 로컬 호스트와 정책 모델 모두의 부모 정책 모델에 메시지를 전송합니다. 그러면 sepmdd 는 30 분 간격으로 이루어지는 재시도를 기다리지 않고 즉시 구독자를 업데이트합니다.

기본값: yes

send_unix_env

sepmd -n 옵션이 정책 모델 암호 파일과 그룹 파일의 내용을 보내는지 여부를 지정합니다.

유효한 값은 yes 와 no 입니다.

yes-sepmd -n 옵션이 정책 모델 암호 파일과 그룹 파일의 내용을 전송합니다.

no-sepmd -n 옵션이 정책 모델 암호 파일과 그룹 파일의 내용을 전송하지 **않습니다.**

기본값: yes

ShutdownWaitingTimeout

구성 요소가 정상 종료될 때까지 정책 모델이 대기하는 시간 만료 기간(초)을 정의합니다. 정책 모델 구성 요소가 정상 종료되지 않으면 정책 모델이 강제 종료됩니다.

기본값: 60

synch_uid

새 UNIX 사용자를 작성할 때 CA Access Control 이 구독자로 하여금 부모 정책 모델 호스트와 동일한 UID 를 사용하도록 할 것인지를 지정합니다.

기본값: Yes

updates_in_chunk

정책 모델이 루프의 각 주기에서 각각의 구독자에게 전달하는 최대 명령 수를 정의합니다.

기본값: 20

추가 정보:

sepmd 유틸리티 (페이지 182)

policyfetcher

[policyfetcher] 섹션에서 토큰은 policy fetcher 데몬("policyfetcher")의 동작을 제어합니다.

check_deployment_tasks

policyfetcher 가 배포 호스트에서 새 배포 작업(DEPLOYMENT 리소스)을 검사하는 빈도(초)를 정의합니다.

기본값: 600(10 분마다)

제한: 최소값 60

deploy_timeout

policyfetcher 가 끝점에서 배포 또는 배포 취소 작업이 완료될 때까지 기다리는 시간(초)을 정의합니다.

기본값: 900

dh_command_retry_interval

각 DH 알림 명령 재시도 사이의 시간(초)을 정의합니다.

기본값: 30

endpoint_heartbeat

policyfetcher 가 배포 호스트(DH)에 하트비트를 전송하는 빈도를 정의합니다. 이 빈도는 check_deployment_task 설정의 요소이며, policyfetcher 가 하트비트를 전송하기 전에 배포 작업을 검사할 횟수를 결정합니다. 예를 들어 check_deployment_task 가 기본값인 600 초(10 분)로 설정되어 있을 때 이 값을 6 으로 설정하면, policyfetcher 는 3600 초(1 시간)마다 한 번씩 하트비트를 전송합니다.

하트비트를 보낸 이후에 policyfetcher 는 또한 위반 계산기(start devcalc 명령)를 실행하고 위반 계산이 완료될 때까지 60 초 동안 기다립니다. 60 초가 지나면 policyfetcher 는 로컬 끝점 정보가 DH 정보와 동일한지 계속 검사합니다.

기본값: 10

max_dh_command_retry

policyfetcher 가 포기하기 전까지 DH 에서 업데이트 알림을 받기 위해 재시도하는 최대 횟수를 정의합니다.

기본값: 3

max_dh_retry_cycles

policyfetcher 가 재해 복구 HD 로 이동하기 전까지 프로덕션 DH 에서 업데이트 알림을 받기 위해 재시도하는 최대 사이클 수를 정의합니다.

기본값: 3

policy_verification

작업을 실행하기 전에 policyfetcher 데몬이 백업 CA Access Control 데이터베이스에서 새 배포 작업을 확인할지 여부를 지정합니다.

유효한 값:

1 - 정책 확인 실행

0 - 정책 확인 사용 안 함

기본값: 0

policyfetcher_enabled

policyfetcher 데몬 실행 여부를 지정합니다.

유효한 값:

1 - policyfetcher 를 실행합니다.

0 - policyfetcher 를 비활성화합니다.

기본값: 0

PUPMAgent

[PUPMAgent] 섹션에서 토큰은 권한 있는 사용자 암호 관리(PUPM) 에이전트의 기능을 결정합니다.

ActivitySendCountThreshold

누적되는 캐시된 이벤트의 최대 수를 지정합니다. 캐시된 이벤트으 수가 지정된 값에 도달하면 PUPM 에이전트는 CA Access Control 엔터프라이즈 관리에 이벤트를 보냅니다.

제한: 1–8192

기본값: 1024

참고: 값으로 0 을 지정하면 CA Access Control 은 이 매개 변수의 기본값을 사용합니다. 8192 보다 큰 값을 지정하면 CA Access Control 은 이 매개 변수에 대해 값 8192 를 사용합니다.

ActivitySendTimeInterval

캐시된 작업 로그 메시지를 CA Access Control 엔터프라이즈 관리로 보내는 간격(분)을 지정합니다.

제한: 양의 정수

기본값: 10

참고: 값으로 0 을 지정하면 CA Access Control 은 이 매개 변수의 기본값을 사용합니다.

InterfaceName

통신 인터페이스 이름, 즉 PUPM 에이전트가 요청을 처리하기 위해 사용하는 UNIX 소켓 이름을 정의합니다. 소켓 파일은 /opt/CA/AccessControl/data/PUPMAgent 디렉터리에 있습니다.

기본값: PUPMAgentInterface

OperationMode

PUPM 에이전트 작업 모드를 지정합니다.

제한: 0 - PUPM 에이전트가 비활성화되고 실행되지 않음, 1 - PUPM 에이전트가 활성화되고 실행됨, 2 - PUPM 에이전트가 활성화되고, 실행되고, 데이터를 추적 파일에 로깅함

기본값: 0

seauxd

[seauxd] 섹션에서 토큰은 Unicenter TNG 일정의 사용 및 새로 고침 간격을 결정하며 이름 확인(name resolution)을 관리하는 데 유용합니다.

client_request_timeout

확인 요청을 유지할 시간 간격(초)을 지정합니다.

기본값: 120

file_time_check

/etc/passwd 에서 변경을 확인할 시간 간격(초)을 지정합니다.

0 으로 지정하면 검사가 이루어지지 않습니다.

기본값: 10

init_delay

seauxd 가 시작될 때까지 대기할 시간(초)을 지정합니다.

기본값: 10

log_file_name

보조 로그 파일의 이름을 지정합니다. 위치는 SEOSPATH/log 입니다.

기본값: seauxd.log

log_file_size

보조 로그 파일의 최대 크기(KB)를 지정합니다. 이 크기를 초과하면 파일 크기가 0 이 되면서 잘립니다.

기본값: 100

log_level

사용할 로깅 수준을 지정합니다.

올바른 값은 다음과 같습니다.

0-Minimum info
1-ERR
2-WARN + ERR
3-NOTIC + WARN + ERR
4-DEBUG + INFO + WARN + ERR

기본값: 0

req_poll_timeout

입력 요청을 대기하는 시간 간격(밀리초)을 지정합니다.

기본값: 200

respawn_seauxd_delay

seauxd 가 종료되는 경우 seosd 가 이를 다시 생성하는 데 걸리는 최소 시간을 초 단위로 정의합니다.

기본값: 60

TNG_cal_lib

Unicenter TNG 일정이 있는 공유 라이브러리의 이름을 지정합니다.

기본값: libcalendar

TNG_calendars

Unicenter TNG 일정을 사용하여 시간 간격 설정 시 리소스를 제한할지 여부를 지정합니다.

기본값: NO

TNG_lib_path

CA Access Control 이 Unicenter TNG 달력을 포함하는 공유 라이브러리를 찾기 위한 경로를 지정합니다.

기본값: /opt/CA/Calib

TNG_refresh_interval

CA Access Control 이 Unicenter TNG 에서 활성 달력 정보를 검색하기 위한 새로 고침 간격을 분 단위로 지정합니다.

기본값: 10

trace_cnt

추적 파일에 횟수를 적성할지 여부를 지정합니다.

유효한 값은 yes 와 no 입니다.

기본값: no

segrace

[segrace] 섹션에서 토큰은 segrace 유틸리티의 특성을 결정합니다.

sepass_command

사용자에게 유예 로그인이 남아 있지 않은 경우 실행되는 CA Access Control 암호 변경 명령의 위치를 지정합니다.

기본값: ACInstallDir/sepass

추가 정보:

segrace 유틸리티-사용자 로그인 정보 표시 (페이지 154)

seini

[seini] 섹션에서 토큰은 seini 지능형 검색 기능의 특성을 결정합니다.

get_error_warning

지능 검색 기능에 대한 오류 및 경고 메시지 표시 여부를 지정합니다.

기본값: yes

perform_action

seini 가 지능 검색 기능으로 찾은 토큰이나 섹션에서 해당 작업을 수행하는지 여부를 지정합니다.

유효한 값은 yes 와 no 입니다.

이 토큰을 **yes** 로 설정하면 추가 지능형 검색에 의해 발견된 섹션과 토큰은 요청된 seini 동작에 사용됩니다.

기본값: no

use_intelligent_search

seini 유틸리티를 호출할 때 지능 검색을 수행할지 여부를 지정합니다.

기본값: no

추가 정보:

seini 유틸리티-구성 파일 관리 (페이지 159)

selock

[selock] 섹션에서 토큰은 selock 유틸리티의 동작을 제어합니다.

unlocking_user

소유자 이외에 잠긴 화면의 잠금을 해제할 수 있는 사용자의 이름을 지정합니다.

기본값: root

추가 정보:

selock 유틸리티-X 터미널 화면 잠금 (페이지 167)

selogrd

[selogrd] 섹션에서 토큰은 로그 라우팅 데몬인 selogrd 와 selogrcd 의 동작을 제어합니다.

Caudit_size

selogrcd 가 백업 파일을 작성하고 새 파일을 열기 전, 감사 수집 파일의 최대 크기(KB)를 지정합니다.

최소값은 50 KB 입니다.

기본값: 1024

CBackUp_Date

selogrcd 가 백업을 수행하는 기준을 설정합니다.

유효한 값은 none, yes, daily, weekly 및 monthly 입니다.

yes 로 설정하면 CA Access Control 은 크기 제한 토큰인 Caudit_size 에 따라 백업을 수행하고 파일에 타임스탬프를 설정합니다.

none 으로 설정하면 CA Access Control 은 Caudit_size 토큰에 따라 백업을 수행하지만 파일에 타임스탬프를 설정하지는 않습니다.

daily, **weekly** 또는 **monthly** 로 설정하면 selogrcd 는 파일을 처음 생성할 때 타임스탬프를 추가합니다. 현재 날짜가 타임스탬프를 지난 경우 CA Access Control 은 자동으로 백업 파일을 만들고 그 파일에 타임스탬프를 설정합니다.

그러나 파일 크기가 처음부터 Caudit_size 토큰의 값을 초과하면 CA Access Control 은 타임스탬프를 발행하지 않고 백업 파일을 작성합니다.

기본값: 없음

ChangeLogFactor

로그 파일이 백업 파일로 변경되었는지 여부를 테스트하기 전에 토큰 간격 값에 적용할 요소를 지정합니다. 예를 들어, interval 토큰과 ChangeLogFactor 토큰이 모두 5 로 설정되어 있으면(기본값), CA Access Control 은 로그 파일이 백업 파일로 변경되었는지를 확인하기 전에 25 초 동안 기다립니다.

기본값: 5

CipherName

UseEncryption 토큰이 eTrust 로 설정된 경우 selogrd 에서 사용하는 암호화 함수가 포함된 파일 이름을 지정합니다.

이 파일은 ACInstallDir/lib/ 디렉터리에 있어야 합니다.

CipherName 은 공유 개체 파일에 대한 심볼 링크입니다.

기본값: adcipher

CollectFile

감사 수집기 데몬 selogrcd 가 수집된 감사 레코드를 저장하는 파일 이름을 지정합니다.

기본값: ACInstallDir/log/seos.collect.audit

CollectFileBackup

selogrcd 가 USR1 신호를 받을 때 수집된 감사 레코드의 파일을 백업하고 이름을 바꿀 때 사용하는 이름을 지정합니다.

기본값: ACInstallDir/log/seos.collect.bak

ConsolePort

통신을 위한 포트 번호 또는 이름을 지정합니다. 이는 동일한 호스트에서 selogrcd 와 secmon 을 모두 실행하려는 경우에만 필요합니다.

지정하는 경우, seolgrd - secmon 통신은 지정된 포트를 사용하여 수행됩니다. 지정하지 않는 경우, 이들은 ServicePort 토큰에 지정된 포트를 사용합니다. 이 토큰도 비어 있는 경우 RPC 포트매퍼를 사용하여 동적으로 포트를 할당합니다. 로그 라우팅 데몬은 UDP 를 사용하여 통신하므로 서비스 이름은 UDP 포트여야 합니다.

토큰 값이 숫자이면 데몬은 지정된 포트 번호에 바인딩됩니다.

토큰 값이 서비스 이름(문자열)이면 /etc/services 또는 NIS 서비스 맵을 사용하여 포트 번호를 확인합니다.

기본값: 토큰이 설정되지 않음(ServicePort 토큰에서 가져오는 값)

DataFile

대상 라우팅 정보가 지정한 대상으로 전달되기 전에 작성되는 파일 이름을 지정합니다.

기본값: ACInstallDir/log/logroute.dat

Interval

selogrd 데몬에서 지정한 로그 파일의 각 폴링 간 시간 간격(초)을 지정합니다.

기본값: 5

KeyFile

감사 암호화 키를 보유하는 파일 이름을 지정합니다.

selogrd 가 CA Access Control 감사 암호화를 수행할 때 이 키를 사용합니다. 키 파일의 위치는 ACInstallDir/lib 디렉터리입니다.

sechkey 유틸리티로 이 키를 변경할 수 있습니다.

기본값: adcipher.bin

Mailer

selogrd 가 전자 메일을 보낼 때 사용하는 프로그램의 이름을 지정합니다.

참고: 이 옵션은 UseSmtpMail 토큰을 yes 로 설정한 경우에만 적용됩니다.

기본값: /bin/mail

MaxErrorSending

문제 수가 이 토큰 값을 초과한 후에만 selogrd 가 감사 레코드를 selogrcd 로 보내지 못했다는 오류 메시지를 syslog 에 보낼지 여부를 지정합니다.

기본값은 1 이며, selogrd 가 selogrcd 로 보내지 못할 때마다 오류 메시지를 syslog 에 보냅니다.

기본값: 1

MaxSeqNoSleep

중지되지 않고 selogrd 가 스캔된 로그 레코드의 최대 수를 지정합니다.

기본값: 50

RefuseUnencrypted

selogrcd 가 암호화되지 않은 감사를 허용할지 여부를 지정합니다. UseEncryption 토큰과 함께 사용되며, UseEncryption 이 **no** 로 설정된 경우 중복됩니다. 따라서 selogrcd 가 암호화를 사용하는 경우에만 유효합니다.

유효한 값:

yes- 암호화되지 않은 감사를 거부합니다.

no- 암호화된 감사와 암호화되지 않은 감사를 모두 허용합니다.

기본값: no

RouteFile

로그 라우팅 구성 파일의 이름을 지정합니다. selogrd 유틸리티의 -config 옵션에 의해 무시되지 않는 한 이 파일이 사용됩니다.

기본값: ACInstallDir/log/selogrd.cfg

SavePeriod

보낸 레코드 수에 대한 정보를 저장하는 시간 간격(분)을 지정합니다.

기본값: 2

sendmail_header_format

selogrd 가 보내는 메일 헤더의 사용자 이름 형식을 결정합니다.

참고: 이 토큰 값은 selogrd 가 메일을 전송할 수 없는 경우에만 변경하십시오. (예를 들어, syslog 의 selogrd 에서 4634 오류가 발생된 경우).

올바른 값은 다음과 같습니다.

1-사용자 이름 형식이 SmtpMailFrom 입니다.

예: eTrust_Admin

2-사용자 이름 형식이 SmtpMailFrom@hostname 입니다. 여기서 hostname 은 selogrd 가 실행되는 호스트입니다.

예: eTrust_Admin@machine

기본값: 1

ServicePor

로그 라우팅 기능이 사용해야 하는 이름 또는 포트 번호를 지정합니다.

지정하는 경우, selogrd 와 selogrcd 는 지정된 포트를 사용합니다. 지정하지 않는 경우, selogrd 와 selogrcd 는 RPC 포트매퍼를 사용하여 동적으로 포트를 할당합니다.

토큰에 값이 있으면 selogrd 와 selogrcd 가 지정된 포트를 사용하고, 그렇지 않으면 selogrd 와 selogrcd 가 RPC portmapper 를 사용하여 동적으로 UDP 포트를 할당합니다. 로그 라우팅 데몬은 UDP 를 사용하여 통신하므로 서비스 이름은 UDP 포트여야 합니다.

토큰 값이 숫자이면 데몬은 지정된 포트 번호에 바인딩됩니다.

토큰 값이 서비스 이름(문자열)이면 /etc/services 또는 NIS 서비스 맵을 사용하여 포트 번호를 확인합니다.

UDP 포트/서비스만 지정할 수 있습니다.

기본값: 토큰이 설정되지 않음(selogrd 와 selogrcd 는 RPC 포트매퍼를 사용하여 동적으로 포트를 할당함)

SmtpMailFrom

UseSmtpMail 의 보내는 사람 ID 를 지정합니다.

기본값: eTrust Admin

SmtpMailServer

원격 메일 서버 호스트 주소를 지정합니다. UseSmtpMail 을 yes 로 설정한 경우 이 토큰을 사용합니다. 이 토큰을 지정하지 않은 경우에는 로컬 컴퓨터가 메일 서버로 간주됩니다.

기본값: (공백 - 로컬 서버)

SmtpTimeLimit

시간이 초과되기 전에 메일 서버가 응답할 때까지 selogrd 가 대기하는 시간 제한(초)을 지정합니다.

기본값: 100

tec_conf_file

selogrd 데몬이 TEC 이벤트 생성을 위해 사용하는 구성 파일 이름을 지정합니다.

기본값: /etc/tecad_seos.conf

UseEncryption

암호화 유형을 결정합니다.

올바른 값은 다음과 같습니다.

native-selogrd 가 CA Access Control 표준 암호화를 사용합니다.

eTrust-selogrd 가 adcipher 를 통해 감사 로그 암호화를 사용합니다.

no-selogrd 가 암호화를 사용하지 않습니다.

기본값: no

UseSmtpMail

DM 기능을 사용할지 이전 메일러를 사용할지 여부를 결정합니다.

기본값: yes

추가 정보:

seaudit 유틸리티-감사 로그 레코드 표시 (페이지 95)
selogrcd 데몬-감사 레코드 수집 (페이지 245)
selogrd 데몬-감사 레코드 송신 (페이지 246)

seos

[seos] 섹션에서 토큰은 CA Access Control 이 사용하는 전역 설정을 결정합니다.

admin_data

Security Administrator ruler 및 기타 구성 파일을 저장할 디렉터리를 지정합니다.

기본값: ACInstallDir/data

auth_login

로그인 권한 방법을 결정합니다. 유효한 값:

Native-로그인은 UNIX passwd 또는 섀도 파일과 비교하여 사용자 암호를 검사합니다.

eTrust-Native 환경에 사용자가 없을 경우 CA Access Control 데이터베이스와 비교하여 사용자 암호를 검사합니다.

PAM-Native 환경에 사용자가 없을 경우 PAM 모듈을 통해 로그인을 검사합니다. 이것은 PAM 을 지원하는 컴퓨터에서만 지원됩니다. LDAP 정의 사용자와 같은 사용자를 확인하는 데 PAM 을 사용합니다.

기본값: Native

auth_module_names

기본 인증 외부에서 인증을 받을 수 있는 언어 클라이언트 모듈을 정의합니다. 이 토큰은 인증 전 lca API 호출 내부에서 클라이언트에 의해 설정됩니다. 이 토큰을 변경하면 기본 모드 이외의 모드에서 인증되는 다른 클라이언트에 영향을 줄 수 있습니다.

기본값 없음.

fast_create_db

PMDB 가 고속 데이터베이스 복사 장치를 사용하는지 여부를 지정합니다.

유효한 값:

no-기존 장치를 사용합니다.

yes-고속 데이터베이스 복사 장치를 사용합니다.

기본값: yes

full_year

4 자리 또는 마지막 2 자리를 사용하여 연도를 표시하는 형식을 지정합니다.

예를 들어 토큰을 yes 로 설정하면 00 대신 2000 이 표시됩니다.

올바른 값은 다음과 같습니다.

yes-4 자리 숫자

no-2 자리 숫자

이 토큰은 secons -tv, dbmgr -d 및 seaudit 유틸리티에 의해 생성된 결과에 영향을 줍니다.

기본값: yes(4 자리 숫자)

ldap_base

CA Access Control LDAP 사용 유틸리티(예: sebuildla)에서 사용하는 사용자 데이터 쿼리를 위한 검색 기준의 고유 이름을 LDAP DIT(디렉터리 정보 트리)에서 정의합니다.

예를 들면 직접 입력하는 대신 다음 형식을 사용할 수 있습니다.

```
o=organization_name,c=country_name
```

기본값: 토큰이 설정되지 않음

중요! sebuildla 및 필수 LDAP 구성 설정을 설정하려면 LDAP 에 대해 잘 알고 있고 ldapsearch 명령을 실행할 수 있어야 합니다. ldap(1), ldapsearch(1)에 대한 man 페이지와 LDAP 클라이언트 설명서에서 설정 정보를 검토하는 것이 좋습니다.

ldap_hostname

CA Access Control LDAP 사용 유틸리티를 위해 LDAP 서버가 실행되고 있는 호스트 이름의 목록을 공백으로 구분하여 정의합니다.

기본값: 토큰이 설정되지 않음(localhost)

ldap_certdb_path

Netscape 스타일의 인증서 데이터베이스가 있는 디렉터리를 정의합니다.

이는 LDAP over SSL 용 Netscape LDAP SDK API(Solaris)를 사용하는 플랫폼에서 sebuildla 에 필요합니다. sebuildla 가 작동하려면 유효한 LDAP 서버용 인증서가 인증서 데이터베이스에 반드시 포함되어 있어야 합니다.

참고: sebuildla 는 서버 인증과 함께 LDAP over SSL 을 사용합니다(즉, 클라이언트 인증 없음). 안전한 서비스 설정에 대한 자세한 내용은 해당 PKI 툴킷 설명서를 참조하십시오.

기본값: /.netscape

ldap_keydb

주요 데이터베이스 파일의 이름을 정의합니다.

참고: AIX 주요 데이터베이스는 임의의 이름을 가질 수 있으므로 이 설정은 AIX 전용입니다. 이는 구현 버전에 따라 certX.db 및 keyY.db 와 같은 이름을 갖기 때문에 이름 검색을 위해 ldap_certdb_path 만 필요한 Netscape 보안 데이터베이스와 반대됩니다.

기본값: 토큰이 설정되지 않음

ldap_method

CA Access Control 이 LDAP 서비스에 액세스하기 위해 LDAP 사용 유틸리티에 대해 사용하는 바인딩 방법을 지정합니다.

기본적으로 sebuildla 는 모든 보안 메커니즘과 함께 간단한 인증을 사용합니다. 간단한 인증에서는 ldap_userdn 및 해당 자격 증명이 LDAP 서버로 전달됩니다. sebuildla 는 사용자 자격 증명을 ACInstallDir/etc 의 ldapcred.dat 에 암호화된 형식으로 저장합니다. 이 두 매개 변수는 LDAP 서버에 필요한 계정 및 암호 조합과 유사합니다.

참고: SASL 또는 TLSv.1/SSL 에 대해서는 해당 LDAP 서버 설명서를 참조하십시오. 특정 ldap_method 설정을 적용하려면 sebuildla 가 실행되는 컴퓨터에 배포된 LDAP 클라이언트에서 해당 메커니즘이 지원 및 구성되어야 합니다. 즉, TLS/SSL 작동과 함께 유효한 인증서가 서버와 클라이언트에 모두 설치되어 있어야 합니다.

유효한 값:

0-표준 LDAP

1-SASL(RFC 2222)

2-LDAPS(LDAP over SSL - 서버 인증 전용.)

참고: 사용 방법에 따라 ldap_userdn 토큰 및 해당 자격 증명의 설정 방법이 결정됩니다(seldapcred 유틸리티를 통해).

기본값: 0

ldap_port

CA Access Control LDAP 사용 유틸리티에 대한 LDAP 서버 포트를 정의합니다. LDAP 서버가 표준 LDAP 포트(389)를 사용하지 않는 경우에만 이 토큰을 변경해야 합니다.

기본값: 토큰이 설정되지 않음(389)

ldap_query_size

각 배치 쿼리에서 sebuildla 가 검색할 LDAP 의 최대 수를 정의합니다.

LDAP 서버 측 크기 제한 매개 변수를 변경하고 싶지 않을 경우에만 이것을 사용하십시오. 일반적으로 sebuildla 는 한 인스턴스에서 모든 데이터를 검색하려고 시도합니다. 사용자 항목이 많을 경우 이 작업은 서버 크기 제한을 초과하여 LDAP 작동 오류를 일으킬 수 있습니다. ldap_query_size 를 설정하는 경우 sebuildla 는 모든 항목을 검색할 필요가 없으므로 작동 오류가 발생하지 않습니다. 총 사용자 항목 수가 ldap_query_size 또는 서버 측 크기 제한보다 큰 경우, 검색되는 항목 수는 이 두 설정 중 낮은 숫자와 일치합니다.

중요! 배치 쿼리를 활성화하면 sebuildla 성능에 영향을 줄 수 있습니다. LDAP 환경의 DIT(디렉터리 정보 트리)에 많은 사용자 데이터(수천 개의 항목)가 있는 경우에만 이 설정을 사용하는 것이 좋습니다.

참고: 서버 측 LDAP 컨트롤(예: OpenLDAP 서버(slapd) sizelimit 매개 변수)에 대한 자세한 내용은 해당 LDAP 서버 설명서를 참조하십시오.

ldap_timeout

LDAP 서비스를 작성하고 LDAP 검색 결과를 얻을 때 연결이 종료되기 전에 CA Access Control LDAP 사용 유틸리티가 기다리는 최대 시간(초)을 정의합니다. LDAP 서비스에서 정보를 검색하는 데 걸리는 시간은 LDAP 서비스의 속도 및 DIT 에 저장된 사용자 데이터 양에 따라 다릅니다. 이러한 부분을 설명하려면 이 토큰을 사용하십시오.

참고: 검색 결과가 잘리지 않도록 하려면 서버 측 LDAP 컨트롤을 조정해야 할 수 있습니다. 예를 들면 OpenLDAP 서버(slapd)에 대해 sizelimit 매개 변수를 조정해야 합니다. 자세한 내용은 해당 LDAP 서버 설명서를 참조하십시오.

기본값: 토큰이 설정되지 않음(15 초)

ldap_uid_attr

LDAP DIT 에서 사용자 이름을 포함하고 있는 특성의 이름을 정의합니다. RFC 2307(LDAP 를 네트워크 정보 서비스로 사용하기 위한 접근법)에서는 uid 를 이 특성으로 미리 지정하는데, 이것이 이 토큰의 기본값입니다. CA Access Control LDAP 사용 유틸리티가 LDAP DIT 에 대해 작동하도록 하려면 이 토큰을 비표준 스키마로 변경하십시오.

기본값: 토큰이 설정되지 않음(uid)

ldap_uidNumber_attr

LDAP DIT 에서 UID 번호를 포함하고 있는 특성의 이름을 정의합니다. RFC 2307 에서는 uidNumber 를 이 특성으로 미리 지정하는데, 이것이 이 토큰의 기본값입니다. CA Access Control LDAP 사용 유틸리티가 LDAP DIT 에 대해 작동하도록 하려면 이 토큰을 비표준 스키마로 변경하십시오.

기본값: 토큰이 설정되지 않음(uidNumber)

ldap_user_class

LDAP DIT 에서 사용자 데이터를 포함하고 있는 개체 클래스의 이름을 정의합니다. RFC 2307 에서는 posixAccount 를 이 개체 클래스로 미리 지정하는데, 이것이 이 토큰의 기본값입니다. CA Access Control LDAP 사용 유틸리티가 LDAP DIT 에 대해 작동하도록 하려면 이 토큰을 비표준 스키마로 변경하십시오.

기본값: 토큰이 설정되지 않음(posixAccount)

ldap_userdn

CA Access Control LDAP 사용 유틸리티가 LDAP DIT 에서 사용자 데이터를 검색하기 위해 사용하는 LDAP 사용자의 고유 이름(DN)을 정의합니다. RFC 2307 을 기반으로, CA Access Control 은 DIT 에 있는 ou=People 수준의 uid 및 uidNumber 특성에서 사용자 데이터를 찾고자 합니다. 보안상의 이유로, 이 사용자(ldap_userdn)에게는 이 데이터에 대한 액세스 권한만 부여하는 것이 좋습니다.

DIT 에 대한 익명 액세스가 허용되는 경우 이 토큰을 비워 둘 수 있습니다. 그렇지 않은 경우 LDAP 서비스에 대해 인증을 받으려면 CA Access Control LDAP 사용 유틸리티에 대해 이 토큰을 설정하고 seldapcred 유틸리티를 실행해야 합니다. seldapcred 가 재사용을 위해 암호화된 자격 증명을 파일에 저장하므로 이 작업은 한 번만 수행하면 됩니다.

예를 들면 이 토큰을 다음과 같이 설정하십시오.

```
ldap_userdn = uid=user1,ou=People,dc=myCompany,dc=com
```

기본값: 토큰이 설정되지 않음

ldap_verbose

sebuildla 의 사용자 데이터 입수와 관련된 LDAP 작업의 자세한 설명 표시를 활성화할지 여부를 지정합니다.

sebuildla 에서 LDAP 데이터 검색을 설정하거나 문제 해결을 수행할 때 이 설정을 사용하십시오.

유효한 값은 **0**-비활성, 0 이외의 정수-활성입니다.

기본값: 0

locale

CA Access Control 데몬 및 유틸리티의 언어를 결정합니다. CA Access Control 은 여러 언어로 작동할 수 있습니다.

지원되는 언어는 C, 일본어, 중국어 간체, 중국어 번체입니다.

전체 언어 목록은 /etc/ca/localeX/calocmap.txt 를 참조하십시오. Linux 에서는 ACInstallDir/data/localeX/locale/calocmap.txt 를 참조하십시오.

기본값: C

pam_enabled

SOLARIS, HP-UX 및 LINUX 에만 해당.

로컬 호스트가 인증 및 암호 변경을 위해 LDAP 데이터베이스에서 PAM 사용을 활성화할지 여부를 지정합니다.

이를 위해 로컬 호스트는 PAM 라이브러리가 동적으로 로드되는지를 확인합니다(시스템에 라이브러리가 있어야 함).

유효한 값은 'no'와 'yes'입니다.

기본값: yes

parent_pmd

이 컴퓨터에서 업데이트를 허용하는 PMDB(정책 모델 데이터베이스)의 목록을 쉼표로 구분하여 정의합니다. 로컬 CA Access Control 데이터베이스는 이 목록에 지정되지 않은 PMDB 에서 오는 업데이트를 거부합니다.

줄로 구분된 PMDB 목록이 포함된 파일 경로를 지정할 수도 있습니다.

로컬 CA Access Control 데이터베이스가 모든 PMDB 에서 오는 업데이트를 허용하도록 하려면 이 토큰을 "_NO_MASTER_"로 설정하십시오.

이 토큰을 설정하지 않으면 로컬 CA Access Control 데이터베이스는 어떤 PMDB 에서 오는 업데이트도 허용하지 않습니다.

각 PMDB 는 pmd_name@hostname 형식으로 지정됩니다.

예:

```
parent_pmd = pmd1@host1,pmd2@host1,pmd3@host2
parent_pmd = /opt/CA/AccessControl/parent_pmdbs_file
```

기본값: 토큰이 설정되지 않음(데이터베이스는 어떤 PMDB 에서 오는 업데이트도 허용하지 않음).

passwd_pmd

sepass 가 암호 업데이트를 보내는 PMDB 를 지정합니다.

이 토큰을 설정하지 않으면 parent_pmd 토큰 값을 상속합니다.

형식은 pmd_name@hostname 입니다.

parent_pmd 와 passwd_pmd 토큰은 동일한 값을 가질 수 있습니다. parent_pmd 및 passwd_pmd 토큰의 값이 동일하지 않으면 passwd_pmd 데이터베이스는 자신의 업데이트를 parent_pmd 데이터베이스로 보내 배포되도록 합니다. 따라서 parent_pmd 데이터베이스는 passwd_pmd 데이터베이스의 자식(구독자)이어야 합니다.

기본값 없음.

ReverseIpLookup

seagent 가 연결된 클라이언트를 식별하는 방법을 제어합니다.

올바른 값은 다음과 같습니다.

yes-seagent 가 열려 있는 클라이언트 소켓의 IP 주소를 찾습니다.

no-seagent 가 클라이언트에서 받은 호스트 이름을 사용하고 호스트 이름을 확인하지 않습니다. TERMINAL 클래스를 비활성화해도 동일한 효과를 얻을 수 있습니다.

기본값: yes

secondary_pmd

기본 대상(passwd_pmd)에 정의되지 않은 사용자의 암호 교체를 위한 보조 대상으로 사용된 PMDB 를 지정합니다.

형식은 pmd_name@hostname 입니다.

기본값 없음.

SEOSPATH

CA Access Control 이 설치된 디렉터리를 지정합니다.

마운트된 NFS 파일 시스템의 디렉터리만 아니라면 어떤 디렉터리건 CA Access Control 을 설치할 수 있습니다.

기본값: ACInstallDir

SyncUnixFilePerms

CA Access Control 이 ACL 허용 권한을 ACL 및 기본 UNIX 시스템(있는 경우)의 다른 사용 권한과 동기화해야 하는지 여부를 지정합니다.

올바른 값은 다음과 같습니다.

no-UNIX 파일 사용 권한을 CA Access Control ACL 과 동기화하지 않습니다.

warn-ACL 사용 권한을 동기화하지 않지만 CA Access Control 및 UNIX 의 사용 권한이 충돌하는 경우 경고를 표시합니다.

traditional-CA Access Control ACL 에 따라 그룹 및 소유자의 rwx 사용 권한을 변경하고 다른 모든 경우에는 경고를 표시합니다.

acl-ACL 을 지원하는 플랫폼에서 CA Access Control ACL 에 따라 기본 파일 시스템 ACL 을 변경합니다.

force-traditional 또는 acl(ACL 을 지원하는 플랫폼의 경우)과 동일하게 작동하지만 defaccess 를 "다른" 사용 권한에 강제로 매핑하기도 합니다.

참고: HP-UX 및 Sun Solaris 2.5 이상에서는 파일 시스템 ACL 을 지원합니다. 다른 플랫폼 및 운영 체제 버전에서는 파일의 기존 사용 권한 모드만 지원됩니다.

기본값: no

TNG_Environment

특수한 Unicenter TNG 클래스 및 리소스로 데이터베이스를 만드는지 여부를 지정합니다.

올바른 값은 다음과 같습니다.

0-특수한 Unicenter TNG 클래스 없이 데이터베이스를 작성합니다.

1-특수한 모든 Unicenter TNG 클래스로 데이터베이스를 작성합니다.

기본값: 0

TNGDir

Unicenter TNG 가 설치되는 디렉터리를 지정합니다.

유효한 값은 기본 Unicenter TNG 디렉터리 또는 .uniprodloc 입니다.

기본값 없음

TRUEPATH

CA Access Control 이 실제로 있는 디렉터리를 지정합니다. CA Access Control 디렉터리는 다른 실제 위치에 대한 심볼 링크일 수 있습니다. 이 토큰은 CA Access Control 이 설치된 실제 위치를 가리킵니다.

기본값: ACInstallDir

use_rpc_protocol

RPC portmapper 가 필요한지 여부를 결정합니다. 이전(1.43)의 CA Access Control 프로토콜을 사용하려면 RPC 포트매퍼가 필요합니다. 기존 프로토콜은 NIS+ 암호 변경을 지원하는 데 필요합니다.

토큰은 old_protocol 토큰을 교체합니다.

올바른 값은 다음과 같습니다.

yes-RPC 포트매퍼를 사용하여 포트를 할당합니다.

no-ServicePort 토큰으로 지정한 포트를 사용합니다.

기본값: no

추가 정보:

sebuildla 유틸리티-Lookaside 데이터베이스 작성 (페이지 102)
seldapcred 유틸리티-자격 증명 암호화 및 저장 (페이지 165)
sepass 유틸리티-암호 설정 또는 교체 (페이지 179)

SEOS_syscall

[SEOS_syscall] 섹션에서 토큰은 SEOS_syscall 커널 모듈에 의해 사용됩니다.

bypass_NFS

SEOS 이벤트에서 NFS 파일을 바이패스할지 여부를 결정합니다.

올바른 값은 다음과 같습니다.

0-NFS 파일을 바이패스하지 않습니다.
1-NFS 파일을 바이패스합니다.

기본값: 0

bypass_realpath

권한 부여에 대해 실제 파일 경로 확인을 바이패스할지 여부를 지정합니다.

이 설정을 (1)로 지정하면 CA Access Control 은 권한 부여에 대해 파일 경로를 확인하지 않습니다. 이렇게 하면 파일 이벤트 처리 속도가 빨라지지만 이 링크를 통한 파일 액세스에 대해 일반 규칙이 시행되지 않습니다.

예제: 이 설정이 사용되고 링크를 통해 사용자가 이 디렉터리에 있는 파일을 액세스하는 경우 /realpath/files/*에 대한 액세스 거부 규칙은 고려되지 않습니다. 링크에 대한 일반 규칙도 필요합니다(/alternatepath/*).

기본값: 0

cache_enabled

파일에 대한 액세스 권한을 결정하기 위해 전체 경로 확인에 캐싱을 사용할지 여부를 지정합니다.

올바른 값은 다음과 같습니다.

0-캐싱 없음.
1-캐싱 사용.

기본값: 0

cache_rate

캐시를 전체 경로 확인에 사용하는 경우 사용되는 캐시율을 결정합니다.

값이 클수록 캐시가 더 잘 됩니다.

기본값: 1000

call_tripAccept_from_seload

CA Access Control 이 시작한 이후 seload 명령에서 tripAccept 를 호출할지 여부를 결정하고, tripAccept 가 호출되는 경우 tripAccept 가 연결하여 포트의 수신기를 활성화해야 하는 TCP/IP 포트의 쉼표로 구분된 목록을 정의합니다.

유효한 값은 임의의 TCP/IP 포트 번호입니다. 또한,

0-seload 에서 tripAccept 를 호출하지 않습니다.

제한: 0-64000

기본값: 0

cdserver_conn_res

UnixWare 의 fiwput 루틴에서 T_CONN_RES 스트림 메시지를 우선 순위가 높은 메시지로 처리할지 여부를 결정합니다.

유효한 값:

1-fiwput 루틴에서 T_CONN_RES 스트림 메시지를 우선 순위가 높은 메시지로 처리합니다.

0-fiwput 루틴에서 T_CONN_RES 스트림 메시지를 우선 순위가 낮은 메시지로 처리합니다.

기본값: 0(UnixWare 에서는 1 이어야 함)

debug_protect

CA Access Control 이 실행되는 동안 프로그램 디버깅을 허용할지 여부를 결정합니다.

올바른 값은 다음과 같습니다.

0-디버깅을 허용합니다.
1-디버깅을 허용하지 않습니다.

기본값: 1

DESCENDENT_dependent

SEOS 데몬의 후손이 SEOS 서비스를 등록할 수 있는지 여부를 결정합니다.

올바른 값은 다음과 같습니다.

0-아무나 SEOS 서비스를 등록할 수 있습니다.
1-하위 데몬만 SEOS 서비스를 등록할 수 있습니다.

기본값: 0

exec_read_enabled

CA Access Control 커널이 스크립트 실행을 식별할지 여부를 지정합니다.

올바른 값은 다음과 같습니다.

0-CA Access Control 커널이 스크립트 실행을 식별하지 않습니다.

1-CA Access Control 커널이 스크립트 실행을 식별합니다.

기본값: 0

참고: PUPM 에이전트가 끝점에 설치된 경우 기본값은 1 입니다. 활성화된 경우 PUPM 에이전트는 스크립트를 PROGRAM 리소스로 정의하지 않고 PUPM 에이전트 파일(acpwd)을 사용하는 명명된 셸 스크립트를 식별할 수 있습니다.

file_bypass

CA Access Control 이 데이터베이스에 정의되지 않은 파일에 대한 액세스를 검사할지 여부를 나타냅니다. 기본적으로 CA Access Control 은 데이터베이스에 정의되지 않은 파일을 검사하지 않습니다.

올바른 값은 다음과 같습니다.

-1-모든 파일을 검사하지는 않습니다.
0-모든 파일을 검사합니다.

기본값: -1

GAC_root

사용자가 root 인 경우 파일에 GAC 캐싱을 사용할지 여부를 결정합니다. 기본적으로 GAC 는 사용자가 루트일 경우 사용되지 않습니다.

올바른 값은 다음과 같습니다.

0-root 사용자에 대해 캐싱 없음.
1-root 사용자에 대해 캐싱 사용.

기본값: 0

HPUX11_SeOS_Syscall_number

HP-UX 의 SEOS_syscall 과 통신하는 기본 syscall 번호를 결정합니다.

유효한 값은 sysent 에서 사용되지 않은 syscall 항목 번호입니다.

기본값: 254

kill_signal_mask

보호할 신호를 정의합니다.

유효한 값은 SEOS 이벤트에서 원하는 모든 신호를 포함하는 마스크입니다.

기본값: SIGKILL, SIGSTOP 또는 SIGTERM 이벤트. 실제 값은 플랫폼에 따라 다릅니다.

- HP-UX: 0x804100
- Sun Solaris: 0x404100
- IBM AIX 및 Digital DEC UNIX: 0x14100
- Linux: 0x44100

link_protect

심볼 링크 보호 여부를 결정합니다.

올바른 값은 다음과 같습니다.

0-링크가 보호되지 않습니다.
1-링크가 보호됩니다.

기본값: 0

max_generic_file_rules

데이터베이스에서 허용되는 일반 파일 규칙의 최대 개수를 정의합니다.

참고: 너무 큰 수를 사용하면 다른 플랫폼에서 잘못된 동작이 발생할 수 있습니다. 도움이 필요하면 기술 지원 부서(http://www.ca.com/worldwide)에 문의하십시오.

유효한 값은 511 보다 큰(<) 수입니다.

참고: 이 토큰은 AIX, HP, Linux 및 Solaris 에서만 지원됩니다.

기본값: 512

max_regular_file_rules

데이터베이스에 허용되는 파일 규칙의 최대 개수를 정의합니다.

참고: 너무 큰 수를 사용하면 다른 플랫폼에서 잘못된 동작이 발생할 수 있습니다. 도움이 필요하면 기술 지원 부서(http://www.ca.com/worldwide)에 문의하십시오.

유효한 값은 4095 보다 큰(<) 수입니다.

참고: 이 토큰은 AIX, HP, Linux 및 Solaris 에서만 지원됩니다.

기본값: 4096

mount_protect

CA Access Control 이 사용하는 디렉터리에 대해 마운트 및 언마운트를 허용할지 여부를 결정합니다.

올바른 값은 다음과 같습니다.

0-마운트를 허용합니다.
1-마운트를 허용하지 않습니다.

기본값: 1

proc_bypass

파일이 프로세스 파일 시스템(/proc)에 속하는 경우 파일 액세스를 확인할지 여부를 결정합니다. 올바른 값은 다음과 같습니다.

0-토큰이 무시됩니다.

다음은 액세스에 대한 요약입니다.

1-read
2-write
4-chown
8-chmod
16-rename
32-unlink
64-utimes
128-chattr
256-link
512-chdir
1024-create

기본값: 0

s68_reboot_string

더 이상 사용되지 않습니다.

s68_reboot_sys

더 이상 사용되지 않습니다.

SEOS_network_intercept_type

사용할 네트워크 차단 유형을 지정합니다(HP-UX 전용).

참고: 또한 SEOS_use_streams = yes 로 설정해야 합니다.

유효한 값:

0 - TCP 후크

1 - 스트림

기본값: 1

중요! 이 토큰을 직접 수정하지 마십시오. 도움이 필요하면 기술 지원 부서(http://www.ca.com/worldwide)에 문의하십시오.

SEOS_streams_attach

CA Access Control 이 실행 중인 STREAMS 에 첨부될지 여부를 지정합니다.

이 설정을 변경할 경우 CA Access Control 의 보호에 대해 이미 네트워크에서 수신 대기하고 있는 데몬을 다시 시작해야 합니다.

참고: 이 설정은 Solaris 9 또는 그 이전 버전에만 적용됩니다.

기본값: yes

SEOS_unload_enabled

SEOS_syscall 커널 모듈을 언로드할 수 있는지 여부를 결정합니다.

올바른 값은 다음과 같습니다.

0-언로드를 허용하지 않습니다.
1-언로드를 허용합니다.

기본값: 1

SEOS_use_ioctl

CA Access Control 커널 모듈 통신 방법을 지정합니다(ioctl 또는 시스템 호출).

사용 가능한 모든 시스템 호출 번호가 운영 체제에 의해 사용되고 있을 경우 ioctl 통신 방법을 사용할 수 있습니다.

Values: 0-시스템 호출, **1**-ioctl

기본값: 0

중요! 이 토큰을 직접 수정하지 마십시오. 도움이 필요하면 기술 지원 부서(http://www.ca.com/worldwide)에 문의하십시오.

SEOS_use_streams

네트워크 차단에 스트림 하위 시스템을 사용할지(SEOS_load 에서 모듈을 스트림으로 푸시할지) 여부를 결정합니다.

이 설정은 HP-UX 및 Sun Solaris 버전 8 과 9 에서만 사용됩니다.

기본값: no

silent_admin

유지 관리 사용자의 사용자 ID 를 정의합니다. 보안이 중단되고 silent_deny 가 yes 일 경우 이 사용자의 활동이 허용됩니다. 유지 관리 사용자를 정의하려면 사용자의 숫자 UNIX UID 를 사용하십시오.

기본값: 0(root 의 사용자 ID)

silent_deny

보안이 중단될 때 모든 이벤트를 거부할지 여부를 결정합니다.

올바른 값은 다음과 같습니다.

yes-자동 거부가 활성화됩니다(유지 관리 모드).

no-자동 거부가 비활성화됩니다.

기본값: no

STAT_intercept

stat 시스템 호출이 발생할 때 파일 액세스를 검사할지 여부를 지정합니다.

1(파일 액세스 검사)을 지정하면 CA Access Control 은 읽기 권한이 없는 사용자가 감사 로그의 파일 및 레코드 읽기에 대해 정보를 얻는 작업을 수행하는 것을 허용하지 않습니다. 이것을 0 으로 설정하면 모든 사용자가 파일 정보를 얻을 수 있습니다.

값: 0(파일 액세스를 검사하지 않음), 1(파일 액세스를 검사함).

기본값: 0

STOP_enabled

스택 오버플로 공격을 방지하는 STOP 기능을 사용할지 여부를 결정합니다.

올바른 값은 다음과 같습니다.

0-해제합니다.
1-설정합니다.

기본값: 0

synchronize_fork

포크 동기화를 관리하는 방법을 결정합니다.

HP-UX 플랫폼에서

1-부모로부터의 포크 보고
2-자식으로부터의 포크 보고

다른 플랫폼에서

1-동기화 없이 부모가 보고
2-동기화와 함께 부모가 보고(Linux 에서는 지원되지 않음)

제한: 1 보다 작은 값은 1 로 해석됩니다. 1 보다 큰 값은 2 로 해석됩니다.

참고: 다른 플랫폼에서는 예상치 못한 결과가 발생할 수 있으므로 이 설정을 수정하지 마십시오. 도움이 필요하면 기술 지원 부서(http://www.ca.com/worldwide)에 문의하십시오.

기본값: 1

syscall_monitor_enabled

CA Access Control 이 CA Access Control 코드를 실행하는 프로세스를 모니터링할지 여부를 지정합니다. 모니터링을 활성화하는 경우(기본값) secons -sc 또는 secons -scl 을 사용하여 이러한 프로세스를 볼 수 있습니다.

유효한 값:

0-비활성

1-활성

기본값: 토큰이 설정되지 않음(1)

threshold_time

차단된 시스템 호출이 위험 내용으로 간주되기 전에 차단될 수 있는 기간(초)을 정의합니다. 프로세스가 이 시간보다 오랜 기간 동안 차단되면 CA Access Control 에서 SEOS_syscall 모듈 언로드가 실패할 수 있다고 보고합니다.

참고: 이 값은 CA Access Control 에서 제공하는 언로드 준비 보고서에 영향을 줍니다. 자세한 내용은 엔터프라이즈 관리 안내서를 참조하십시오.

기본값: 60

trace_enabled

SEOS_syscall 순환 추적 버퍼 사용 여부를 결정합니다.

올바른 값은 다음과 같습니다.

0-추적 사용 안 함.
1-추적 사용함.

기본값: 0

use_tripAccept

차단된 시스템 허용 호출을 깨우기 위해 SEOS_syscall 을 언로드할 때 tripAccept 유틸리티를 사용할지 여부를 결정합니다. 이렇게 하면 모듈이 언로드된 후 SEOS_syscall 코드가 실행되지 않습니다.

유효한 값은 yes 와 no 입니다.

기본값: yes

seosd

[seosd] 섹션에서 토큰은 권한 부여 데몬의 동작과 성능 향상을 위한 캐시 유틸리티의 동작을 결정합니다.

bypass_filenames

seos 이벤트에서 제외할 파일 이름 목록이 들어 있는 파일을 지정합니다.

예: bypass_filenames = /opt/CA/AccessControl/bin/bypass_filenames

기본값: 토큰이 설정되지 않음

bypass_nfs_port

nfs 가 사용하는 포트(포트 2049)가 CONNECT 에 대해 바이패스되는지 여부를 지정합니다. 바이패스는 NFS 기능의 올바른 작동을 위해 존재합니다.

이 토큰의 값을 no 로 변경하면 이 포트에 대해 바이패스가 발생하지 않습니다. 이 경우 이러한 바이패스를 대체할 수 있는 필수 CA Access Control 규칙을 제공해야 합니다. 다음은 그러한 규칙의 예입니다. 아래 내용을 있는 그대로 사용해서는 안 됩니다.

```
nr hostnet all mask (0.0.0.0) match(0.0.0.0)
nr TCP 2049 owner(nobody) defaccess(none)
authorize TCP 2049 hostnet(all) access(w) uid(root)
nr TCP nfsd owner(nobody) defaccess(none)
authorize TCP nfsd hostnet(all) access(w) uid(root)
```

참고: 이 토큰의 값을 no 로 설정하고도 올바른 CA Access Control 규칙을 제공하지 않으면 NFS 작동이 중지됩니다.

기본값: yes

bypass_outgoing_TCPIP

seos_syscall 이 seosd 로 나가는 연결 이벤트를 전달하지 않을, 쉼표로 구분된 포트 목록을 정의합니다.

기본값: 토큰이 설정되지 않음

bypass_suid_for_login

더미 SUID 시스템 호출을 무시할 로그인 프로그램의 경로를 지정합니다.

이 경로는 samba 같이 많은 더미 SUID 시스템 호출을 생성하는 일부 로그인 프로그램의 경우에 사용됩니다. 이러한 시스템 호출은 사용자 로깅의 정확한 인식을 방해할 수 있습니다.

기본값: 없음

bypass_suid_program

여러 su 명령을 허용합니다. 일부 플랫폼에서 시스템의 su 바이너리는 다음과 같은 비표준 방식으로 작동합니다. root 가 아닌 사용자에 대한 su 명령을 요청하면 요청된 사용자에 대해 su 를 실행하기 전에 root 에 대해 su 를 실행합니다.

root 사용자에 대해 CA Access Control 서로게이트 보호 기능이 설정되어 있으면 root 가 아닌 사용자에 대한 su 명령이 성공적으로 실행되지 않을 수 있습니다.

이러한 플랫폼의 root 사용자에 대한 서로게이트 보호를 사용하고 root 가 아닌 사용자에 대해서도 개입 없이 su 를 사용하려면 시스템의 su 바이너리에 대한 실제 경로를 포함하도록 bypass_suid_program 토큰을 설정합니다.

기본값: 없음

bypass_system_files

CA Access Control 권한 부여 엔진이 /etc/passwd 및 /etc/group 시스템 파일에 대한 읽기 액세스를 바이패스할지 여부를 결정합니다.

유효한 값:

yes-시스템 파일에 대한 읽기 액세스를 바이패스합니다.

no-시스템 파일에 대한 읽기 액세스를 바이패스하지 않습니다.

기본값: yes

bypass_TCPIP

seos_syscall 이 seosd 로 이벤트를 전달하지 않을 하나 이상의 포트를 쉼표로 구분하여 추가할 수 있습니다.

구문은 bypass_TCPIP=port1[,port2,portx]입니다.

기본값: 토큰이 설정되지 않음

bypass_xdm_ports

xdm 이 사용하는 포트(포트 6000-6010)가 CONNECT 에 대해 바이패스되는지 여부를 지정합니다. 바이패스는 xdm 기능의 올바른 작동을 위해 존재합니다.

이 토큰의 값을 no 로 변경하면 이러한 포트에 대해 바이패스가 발생하지 않습니다. 이 경우 이러한 바이패스를 대체할 수 있는 필수 CA Access Control 규칙을 제공해야 합니다. 다음은 그러한 규칙의 예입니다. 아래 내용을 있는 그대로 사용해서는 안 됩니다.

```
nr hostnet all mask (0.0.0.0) match(0.0.0.0)
nr TCP X-Win owner(nobody) defaccess(none)
authorize TCP X_Win hostnet(all) access(r)
authorize TCP X_Win hostnet(all) access(w) uid(root)
authorize TCP X_Win hostnet(all) access(w) gid(mygroup)
nr TCP 6000 owner(nobody) defaccess(none)
authorize TCP 6000 hostnet(all) access(r)
authorize TCP 6000 hostnet(all) access(w) uid(root)
authorize TCP 6000 hostnet(all) access(w) gid(mygroup)
```

참고: 이 토큰의 값을 no 로 설정하고도 올바른 CA Access Control 규칙을 제공하지 않으면 xdm 작동이 중지됩니다. 이 토큰의 값이 yes 이고 나가는 연결이 포트 6000-6010 을 통해 설정된 경우 해당 감사 레코드의 클래스 이름은 TERMINAL 입니다.

기본값: yes

cron_program

seosd 에서 cron 로그인 확인 기능을 향상시킵니다.

시스템의 cron 바이너리에 대한 실제 경로를 포함하도록 cron_program 토큰을 설정합니다.

기본값: 없음

dbdir

CA Access Control 데이터베이스의 위치를 지정합니다.

기본값: ACInstallDir/seosdb

device_file

/dev 에서 모든 장치를 스캔할지 여부를 지정합니다.

이 토큰의 값을 Yes 로 설정한 경우 tty 가 표준 목록에 없으면 CA Access Control 은 /dev 에 있는 장치를 모두 검색합니다.

qplib 는 표준 장치에서 tty 이름을 확인합니다.

참고: tty 이름 목록에 장치를 추가할 수 있습니다.

기본값: no

dns_server

기본 서버에서 다른 서버로 확인하는 호스트를 변경하는 데 사용되는 DNS 서버 이름을 지정합니다.

일반적으로 이 토큰은 DNS 캐싱 옵션이 활성화되면 사용됩니다.

기본값: 없음

domain_names

seosd 가 정규화된 이름을 작성하기 위해 권한 부여용으로 받은 짧은 호스트 이름에 추가하는 도메인 이름 목록을 지정합니다. 따라서 이러한 이름은 관련 HOST, CONNECT 또는 TERMINAL 클래스에서 권한을 부여할 수 있습니다.

seosd 는 전체 이름을 식별하기 위해 domain_names 목록의 도메인 이름을 짧은 이름에 추가하여 권한을 부여합니다.

seosd 는 먼저 짧은 이름만 사용하여 해당 데이터베이스에서 관련 규칙을 찾습니다. 짧은 이름에 일치하는 레코드를 찾지 못하면 일치하는 레코드를 찾을 때까지 domain_names 토큰에 지정된 각 도메인 이름을 하나씩 추가합니다.

예를 들어 domain_names 에 다음 목록을 할당한다고 가정합니다.

domain_names= market.com, journey.com, total.com

다음은 데이터베이스에서 규칙으로 정의되지 않은 acme 라는 구독자가 요청할 때 seosd 가 일치하는 프로세스를 처리하는 방법입니다.

acme (not found in database)
acme.market.com (not found)
acme.journey.com (not found)
acme.total.com (found)

seosd 는 권한 부여를 위해 일치하는 첫 번째 레코드(이 예제에서는 acme.total.com)를 사용합니다.

기본값: /etc/resolv.conf 에 정의된 대로

EnablePolicyCache

권한 부여에 필요한 데이터베이스 값을 저장하는 데 런타임 테이블을 사용해야 하는지 여부를 결정합니다. 런타임 테이블은 seosd 가 시작될 때 메모리로 로드됩니다. 이렇게 하면 데이터베이스에 연결되지 않으므로 권한 부여 시간이 줄어듭니다.

유효한 값은 yes 와 no 입니다.

기본값: no

enf_register

seosd 가 Unicenter NSM ENF(Event Notification Facility)에 등록할지 여부를 결정합니다.

유효한 값은 다음과 같습니다.

yes-seosd 가 ENF 에 등록합니다.

no-seosd 가 ENF 에 등록하지 않습니다.

기본값: no

FileCache_auths

캐싱이 활성화된 경우 권한 부여 풀의 레코드 수를 지정합니다. 캐시할 수 있는 최대 권한 부여 레코드 수는 800 개입니다.

기본값: 80

FileCache_CleanInt

파일 캐시를 지우는 간격(분)을 지정합니다.

기본값: 60

FileCache_files

캐싱이 활성화된 경우 파일 풀의 레코드 수를 지정합니다. 캐시할 수 있는 최대 파일 레코드 수는 200 개입니다.

기본값: 20

FileCache_InitPrio

캐시 테이블에 있는 새 레코드의 초기 우선 순위 값을 지정합니다.

기본값: 10

FileCache_PriorInt

캐싱이 활성화된 경우 캐시 테이블의 우선 순위를 다시 계산하는 빈도를 지정합니다. 새 레코드를 저장할 때마다 하나로 계산됩니다.

기본값: 1

FileCache_users

캐싱이 활성화된 경우 사용자 풀의 레코드 수를 지정합니다. 캐시할 수 있는 최대 사용자 레코드 수는 500 개입니다.

기본값: 50

get_login_terminal

seosd 가 다른 방법으로 로그인 프로그램의 피어 주소를 찾으려고 하는지 여부를 결정합니다. 이 토큰은 ssh 와 같은 연결에 유용합니다.

유효한 값은 yes 와 no 입니다.

기본값: yes

grace_admin

관리자가 사용자의 암호를 변경할 때 설정되는 유예 로그인 수를 결정합니다.

기본값: 토큰이 설정되지 않음(1)

GroupidResolution

CA Access Control 이 그룹 이름에 대한 GID 번호를 확인하는 방법을 결정합니다.

올바른 값은 다음과 같습니다.

system-CA Access Control 이 시스템 호출을 사용하여 gid 번호를 변환합니다. 이 값은 독립 실행형, DNS 클라이언트 및 DNS 서버 스테이션에 사용할 수 있습니다. 이 표의 resolve_timeout 토큰을 참조하십시오.

cache-gid 번호와 그룹 이름은 모두 seosd 에 캐시됩니다. 이 방법을 사용하면 가장 빠르고 쉽게 변환할 수 있지만 런타임 중에 캐시를 업데이트할 수는 없습니다.

ladb-CA Access Control 이 lookaside 데이터베이스를 사용하여 gid 번호를 변환합니다. 관련 트랜잭션 테이블을 업데이트할 때마다 sebuildla 유틸리티를 실행하여 lookaside 데이터베이스를 다시 만들어야 합니다.

NIS 및 NIS+ 서버의 경우 캐시 또는 ladb 를 사용할 수 있습니다.

Sun Solaris 2.5 이상 및 HP-UX 11.x 의 경우 캐시 또는 ladb 를 사용할 수 있습니다.

모든 스테이션의 경우 ladb 값이 기본 설정됩니다.

기본값: 토큰이 설정되지 않음(system)

HostResolution

CA Access Control 이 호스트 이름에 대한 IP 주소를 확인하는 방법을 결정합니다.

올바른 값은 다음과 같습니다.

system-CA Access Control 이 시스템 호출을 사용하여 IP 주소를 변환합니다. 이 값은 독립 실행형 컴퓨터, NIS/NIS+ 클라이언트, DNS 클라이언트 스테이션에 사용할 수 있습니다. 이 표의 resolve_timeout 토큰을 참조하십시오.

cache-호스트 이름 및 해당 IP 주소는 seosd 에 캐시됩니다. 이 방법을 사용하면 가장 빠르고 쉽게 변환할 수 있지만 런타임 중에 캐시를 업데이트할 수는 없습니다.

ladb-CA Access Control 이 lookaside 데이터베이스를 사용하여 IP 주소를 변환합니다. 관련 트랜잭션 테이블을 업데이트할 때마다 sebuildla 유틸리티를 실행하여 lookaside 데이터베이스를 다시 만들어야 합니다.

NIS, NIS+ 및 DNS 서버의 경우 캐시 또는 ladb 를 사용할 수 있습니다. ladb 값이 기본 설정됩니다.

기본값: 토큰이 설정되지 않음(system)

IsolatedDaemon

파일 설명자 stdin, stdout 및 stderr 이 데몬이 되면 seosd 가 이러한 파일 설명자를 닫을지 여부를 지정합니다.

올바른 값은 다음과 같습니다.

yes-이러한 파일 설명자가 데몬이 될 때 seosd 가 파일 설명자를 닫습니다.

no-이러한 파일 설명자가 데몬이 될 때 seosd 가 파일 설명자를 닫지 않습니다.

기본값: no

kill_ignore

seosd 가 CA Access Control 의 주요 세 가지 데몬 중 하나로 전달된 "kill -9" 명령을 무시(거부)할지 여부를 지정합니다. 올바른 값은 다음과 같습니다.

yes-kill 명령을 무시합니다. 이것이 기본값입니다.

no-kill 명령이 seosd 를 종료합니다.

기본값: yes

login_parent_check

하위 프로세스가 로그인한 경우 상위 프로세스에서 로그인 시퀀스를 계속할지 시퀀스를 중지하고 하위 프로세스에서 로그인을 상속할지를 지정합니다.

유효한 값은 0 과 1 입니다.

0 이면 상위 프로세스가 로그인 시퀀스를 계속합니다.

1 이면 상위 프로세스가 로그인 시퀀스를 중단하고 하위 프로세스에서 로그인을 상속합니다.

기본값: 토큰이 설정되지 않음(0)

lookaside_allowdupuid

sebuildla 가 중복된 UID 를 등록할지 여부를 결정합니다.

유효한 값:

yes-중복된 UID 를 등록합니다.

no-중복된 UID 의 경우 하나의 UID 만 등록합니다.

참고: 중복된 UID 는 UNIX OS 에서 변동을 일으킬 수 있습니다.

기본값: no

lookaside_path

lookaside 데이터베이스가 위치할 디렉터리를 지정합니다. sebuildla 유틸리티를 실행하기 전에 이 디렉터리를 만듭니다.

참고: lookaside 데이터베이스 파일은 sebuildla 유틸리티를 사용하여 작성 및 업데이트됩니다.

기본값: ACInstallDir/ladb

MultiLoginPgm

다중 로그인을 수행하는 프로그램의 이름과 전체 경로를 정의하며, 이러한 특수 로그인 응용 프로그램에 대해 올바른 로그인 시퀀스를 검색하는 데 사용됩니다.

MultiLoginPgm 은 로그인 응용 프로그램 이름 및 전체 경로입니다.

기본값: 토큰이 설정되지 않음(none)

network_cache_timeout

네트워크 캐시가 사용되는 경우 네트워크 캐시 테이블을 지우는 시간 간격(분)을 지정합니다. 저장 및 허용된 들어오는 TCP 요청에 대해 제한 시간을 설정하려면 이 토큰을 사용하십시오.

참고: 네트워크 캐시 사용에 대한 자세한 내용은 UNIX 용 끝점 관리 안내서를 참조하십시오.

기본값: 10

nfs_devices

NFS 주요 장치 번호가 있는 파일 이름과 경로를 지정합니다. 전체 파일 경로를 지정합니다.

CA Access Control 은 장치 및 inode 번호 또는 이름을 사용하여 프로그램을 얻지 못하면 이 파일을 사용합니다. 파일에는 모든 플랫폼의 주요 장치 번호에 대한 NFS 기본값이 들어 있습니다. 이 기본값은 시스템마다 다를 수 있습니다. 시스템에 대한 번호를 찾으려면 UNIX getmajor() 함수와 함께 간단한 프로그램을 사용합니다. 그런 다음 찾은 번호를 포함하도록 nfsdevs.init 파일 또는 이 토큰으로 이름을 지정한 파일을 편집합니다.

참고: NFS 시스템을 마운트하고 다시 마운트할 때마다 nfsdevs.init 파일을 업데이트해야 합니다. 또한 장치의 처음 4 자리 숫자만 사용할 수도 있습니다. 이러한 숫자는 시스템을 마운트 해제하고 다시 마운트할 때도 변경되지 않은 상태로 유지됩니다.

기본값: ACInstallDir/etc/nfsdevs.init

protect_bin

seosd 가 CA Access Control 바이너리 파일을 보호할지 여부를 지정합니다. 다음 값 중 하나를 지정합니다.

yes-이러한 액세스를 허용하는 규칙이 정의되지 않은 경우 seosd 가 CA Access Control 바이너리 파일을 보호합니다.

참고: FILE 레코드에 대한 _default 액세스가 없으면 yes 를 지정하지 마십시오. 왜냐하면 모든 /opt/CA/AccessControl/bin 파일에 FILE 레코드가 없으면 파일에 액세스할 수 없어 CA Access Control 을 사용할 수 없기 때문입니다.

no-seosd 가 CA Access Control 바이너리 파일을 보호하지 않습니다.

기본값: no

resolve_rebind

제한 시간 오류 발생 후 seosd 가 NIS 서버에 대한 연결을 다시 설정하는지 여부를 지정합니다.

기본값을 변경하지 않는 것이 좋습니다.

기본값: yes

resolve_timeout

seosd 가 주소에 대한 IP, 사용자 이름에 대한 사용자 ID, 그룹 이름에 대한 그룹 ID 또는 서비스 이름에 대한 서비스 포트 번호를 확인하는 최대 시간(초)을 지정합니다.

이 값은 다음과 같은 두 가지 경우에 적용됩니다.

seosd 가 시스템 확인을 사용하는 경우. HostResolution, ServiceResolution, UseridResolution 및 GroupidResolution 토큰을 참조하십시오.

under_NIS_server 토큰을 no 로 설정한 경우

지정한 시간이 확인 없이 만료되면 seosd 는 지정한 IP, ID 및 포트에 대한 확인이 없는 것으로 간주합니다.

값을 0 으로 설정하면 제한 시간이 없습니다.

기본값: 5

rt_priority

seosd 에 실시간 우선 순위가 있는지 여부를 결정합니다.

유효한 값은 yes 와 no 입니다.

이 토큰을 yes 로 설정하면 seosd 에 실시간 우선 순위가 있습니다.

기본값: yes

ServiceResolution

CA Access Control 이 TCP 포트 번호를 서비스 이름으로 변환하는 방법을 결정합니다.

올바른 값은 다음과 같습니다.

system-CA Access Control 이 시스템 호출을 사용하여 TCP 포트 번호를 변환합니다. 이 값은 독립 실행형 컴퓨터, NIS/NIS+ 클라이언트, DNS 클라이언트, DNS 서버 스테이션에 사용할 수 있습니다. 이 표의 resolve_timeout 토큰을 참조하십시오.

cache-서비스 이름 및 해당 TCP 포트 번호가 seosd 에서 캐시됩니다. 이 방법을 사용하면 가장 빠르고 쉽게 변환할 수 있지만 런타임 중에 캐시를 업데이트할 수는 없습니다.

ladb-CA Access Control 이 lookaside 데이터베이스를 사용하여 TCP 포트 번호를 변환합니다. 관련 트랜잭션 테이블을 업데이트할 때마다 sebuildla 유틸리티를 실행하여 lookaside 데이터베이스를 다시 만들어야 합니다.

NIS 및 NIS+ 서버의 경우 캐시 또는 ladb 를 사용합니다.

기본값: system

sim_login_timeout

CA Access Control 이 ACEE(Accessor Element Entry) 테이블에서 사용되지 않는 시뮬레이션된 로그인 사용자 항목을 제거하기 전의 제한 시간(분)을 정의합니다.

CA Access Control 은 ACEE 에서 발견되는 정보에 액세스해야 할 경우 시뮬레이션된 로그인을 수행하여 ACEE 항목을 작성합니다.

기본값: 60

special_check

커널 모듈 로딩에 대한 파일 경로 검사의 활성화 여부를 지정합니다. 활성화되면 CA Access Control 은 로드할 커널 모듈이 KMODULE 레코드의 filepath 속성과 일치하는지(비 Linux 시스템) 또는 KMODULE 레코드의 서명과 일치하는지(Linux 시스템)를 검사합니다.

기본값: no

terminal_default_ignore

관리 액세스의 권한을 부여할 때 _default TERMINAL 및 특정 TERMINAL 레코드의 defaccess 값을 고려할지 여부를 결정합니다.

유효한 값은 yes 와 no 입니다.

yes-관리 액세스가 _default 및 특정 TERMINAL 레코드의 defaccess 값을 무시합니다. 이런 경우에는 관리 액세스에 관련된 특정 TERMINAL 레코드에 대한 명시적 권한 부여 규칙이 필요합니다.

no-관리 액세스는 _default 인지 특정 값인지에 따라 관련된 모든 TERMINAL 레코드의 defaccess 값을 고려합니다.

기본값: yes

terminal_search_order

이름으로 정의된 TERMINAL 과 IP 주소로 정의된 TERMINAL 중 seosd 가 어떤 것에 대한 검사를 먼저 시도할지를 지정합니다.

유효한 값:

name - IP 주소에 앞서 이름으로 TERMINAL 을 검사합니다.

ip - 이름에 앞서 IP 주소로 TERMINAL 을 검사합니다.

참고: TERMINAL 클래스는 와일드카드로 정의된 일반 규칙을 지원합니다(IP 주소 또는 호스트 이름 패턴 일치). 일반 규칙은 항상 특수(전체 이름) 규칙 이후에 검사됩니다. 예를 들어 이 값을 ip 로 설정하면 seosd 는 전체 IP 주소 일치, 전체 호스트 이름 일치, IP 주소 패턴 일치, 호스트 이름 패턴 일치 순서로 TERMINAL 리소스를 찾습니다.

기본값: name

trace_file

추적 메시지를 요청한 경우 추적 메시지를 보낼 파일 이름을 지정합니다.

기본값: ACInstallDir/log/seosd.trace

trace_file_type

추적 파일을 이진 형식으로 작성할지 텍스트 형식으로 작성할지를 결정합니다.

올바른 값은 다음과 같습니다.

binary-추적 파일을 이진 형식으로 작성합니다. 이 옵션을 지정하면 이 파일에서 사용하는 공간이 줄어듭니다.

text-추적 파일을 텍스트 형식으로 작성합니다.

seosd 데몬은 이 토큰의 값을 확인하고 추적 파일의 내용과 비교합니다. 토큰 값이 추적 파일의 형식과 일치하지 않으면 seosd 는 추적 파일을 해당 이름으로 저장하고 확장명 .backup 을 추가합니다.

기본값: text

trace_filter

추적 메시지를 필터링하는 데 사용하는 필터 데이터가 들어 있는 파일 이름과 경로를 지정합니다.

기본값: ACInstallDir/data/language/etc/trcfilter.init

trace_space_saver

파일 시스템에 남아 있는 사용 가능한 공간(KB)을 지정합니다. 사용 가능한 공간이 이 숫자보다 작으면 CA Access Control 은 추적을 비활성화합니다.

참고: 나중에 더 많은 공간을 사용할 수 있게 되더라도 추적이 자동으로 활성화되지 않습니다.

기본값: 5120

trace_to

추적 메시지의 대상을 지정합니다.

올바른 값은 다음과 같습니다.

file-trace_file 토큰이 지정한 파일로 CA Access Control 이 추적 메시지를 보냅니다. 추적을 사용하지 않으려면 secons -t- 명령을 사용합니다. 자세한 내용은 이 테이블의 trace_file 토큰을 참조하십시오.

file, stop-CA Access Control 이 데몬 초기화 중에 추적 메시지를 생성합니다. 데몬이 초기화되면 추적 메시지 생성이 중지됩니다.

none-CA Access Control 이 추적 메시지를 생성하지 않습니다. 이것은 CA Access Control 을 설치 및 구현한 후의 정상적인 설정입니다.

참고: 토큰을 **file** 이나 **file,stop** 으로 설정하면 secons 명령을 -t 옵션과 함께 사용하여 CA Access Control 추적을 활성화하거나 비활성화할 수 있습니다.

기본값: file, stop

UpdSurrogLogin

CA Access Control 이 서로게이트 로그인에서 사용자의 마지막 액세스 시간을 업데이트할지 여부를 지정합니다.

유효한 값:

1 - CA Access Control 이 서로게이트 로그인에서 사용자의 마지막 액세스 시간을 업데이트합니다.

0 - CA Access Control 이 서로게이트 로그인에서 사용자의 마지막 액세스 시간을 업데이트하지 않습니다.

Undef_ForPacl

PACL 의 접근자 이름에 별표(*)가 있을 때 seosd 가 정의되지 않은 사용자를 검사할지 여부를 결정합니다.

올바른 값은 다음과 같습니다.

1-seosd 는 별표가 있는 정의되지 않은 사용자를 PACL 에 포함하지 않습니다.

0-seosd 는 별표가 있는 정의되지 않은 사용자를 PACL 에 포함합니다.

기본값: 0

under_NIS_server

seosd 가 시스템 이름 확인 대신 내부 이름 확인을 사용하는지 여부를 결정합니다.

올바른 값은 다음과 같습니다.

yes-seosd 는 시작 시 메모리 또는 lookaside 데이터베이스(use_lookaside 토큰 참조)에 사용자, 그룹, 호스트 및 포트 정보를 모두 보관합니다.

이 설정은 NIS, NIS+ 및 DNS 서버 컴퓨터와 Sun Solaris 2.5 이상, HP-UX 11.x, IBM AIX 4.3.x, 및 IRIX 6.5 같은 운영 체제에 필요합니다.

중요! 컴퓨터가 NIS 서버이거나 앞서 언급한 운영 체제 중 하나인 경우 이 토큰을 비활성화하면 시스템이 중지됩니다.

no-seosd 가 시스템 이름 확인을 사용하며 resolve_timeout 토큰이 적용됩니다.

참고: 이 토큰에는 설치 중에 자동으로 값이 할당됩니다.

이 토큰은 이전 버전과의 호환성을 위해서만 유지됩니다. 새 CA Access Control 을 설치하거나 버전 2 이상을 설치하는 경우에는 HostResolution, ServiceResolution, UseridResolution 및 GroupidResolution 토큰을 대신 사용하십시오.

기본값: 설치 중 할당됨

use_lookaside

seosd 가 사용자, 그룹, 호스트 및 포트 정보를 lookaside 데이터베이스나 메모리에 저장하는지 여부를 결정합니다.

참고: 이 토큰은 under_NIS_server 토큰과 함께 사용되며, under_NIS_server 토큰이 yes 로 설정되지 않은 경우에는 관련이 없습니다.

올바른 값은 다음과 같습니다.

yes-seosd 는 사용자, 그룹, 호스트 및 서비스 세부 사항에 대해 lookaside 데이터베이스를 사용합니다. lookaside 데이터베이스는 sebuildla 유틸리티에 의해 구축되며 언제든지 이 유틸리티를 사용하여 새로 고칠 수 있습니다.

lookaside 데이터베이스의 위치는 lookaside_path 토큰으로 설정합니다.

no-seosd 는 시작 시 사용자, 그룹, 호스트 및 서비스 정보를 모두 캐시하여 모든 변환이 메모리에서 이루어질 수 있도록 합니다. 캐시를 새로 고치도록 seosd 를 매일 다시 시작하는 것이 좋습니다.

이 토큰은 이전 버전과의 호환성을 위해서만 유지됩니다. 새 CA Access Control 을 설치하거나 버전 2 이상을 설치하는 경우에는 HostResolution, ServiceResolution, UseridResolution 및 GroupidResolution 토큰을 대신 사용하십시오.

기본값: no

use_nfs_devices

NFS 장치 사용 여부를 결정합니다. 유효한 값은 yes 또는 no 입니다.

기본값: Yes

use_standard_functions

NIS 환경에서 sebuildla 가 사용자 검색을 위해 표준 시스템 함수 getpwent 를 호출할지 ypcat passwd 및 cat /etc/passwd 명령의 출력을 구문 분석할지를 결정합니다.

유효한 값:

yes-표준 시스템 함수 getpwent 를 사용합니다.

no-ypcat passwd 및 cat /etc/passwd 명령의 출력을 구문 분석합니다.

기본값: yes

use_trusted_script

seosd 에서 트러스트된 스크립트 메커니즘을 사용할지 여부를 지정합니다.

트러스트된 스크립트 메커니즘을 사용할 경우 셸 스크립트 내에서 호출된 프로그램은 셸 스크립트 이름을 내부 CA Access Control 테이블에 보관합니다.

즉, 스크립트가 PACL 에 사용된 경우에는 이러한 프로그램이 해당 권한을 상속합니다. 또한 CA Access Control 을 통해 이러한 프로그램을 보호할 수 없습니다.

트러스트된 스크립트의 첫 번째 줄은 #!로 시작합니다.

트러스트된 스크립트 메커니즘을 사용하지 **않는** 경우 이들 프로그램은 원래 이름대로 내부 CA Access Control 테이블에 등록됩니다.

기본값: yes

UseFileCache

성능 향상을 위해 파일 레코드에 캐시 도구를 사용할지 여부를 지정합니다.

기본값: yes

UseNetworkCache

CA Access Control 이 들어오는 허용된 TCP 요청을 캐시할지 여부를 결정합니다.

참고: 네트워크 캐시 사용에 대한 자세한 내용은 UNIX 용 끝점 관리 안내서를 참조하십시오.

유효한 값은 yes 와 no 입니다.

기본값: no

UseridResolution

CA Access Control 이 UID 번호를 사용자 이름으로 변환하는 방식을 지정합니다.

올바른 값은 다음과 같습니다.

system-CA Access Control 이 시스템 호출을 사용하여 uid 번호를 변환합니다. 이 값은 독립 실행형 컴퓨터, NIS/NIS+ 클라이언트, DNS 클라이언트, DNS 서버 스테이션에 사용할 수 있습니다.

cache-사용자 이름 및 해당 uid 번호는 seosd 에서 캐시됩니다. 이 방법을 사용하면 가장 빠르고 쉽게 변환할 수 있지만 런타임 중에 캐시를 업데이트할 수는 없습니다.

ladb-CA Access Control 이 lookaside 데이터베이스를 사용하여 uid 번호를 변환합니다. 관련 트랜잭션 테이블을 업데이트할 때마다 sebuildla 유틸리티를 실행하여 lookaside 데이터베이스를 다시 만들어야 합니다.

NIS 및 NIS+ 서버, Sun Solaris 2.5 이상이나 HP-UX 11.x 운영 체제의 경우 캐시 또는 ladb 를 사용해야 합니다.

기본값: system

watchdog_refresh

각 파일이 처리되는 동안 권한이 있는 프로그램과 보안된 파일을 스캔하도록 seosd 가 Watchdog 을 새로 고치는지 여부를 결정합니다.

올바른 값은 다음과 같습니다.

yes-seosd 가 Watchdog 을 새로 고칩니다.

no-seosd 가 Watchdog 을 새로 고치지 않습니다.

기본값: no

seosdb

[seosdb] 섹션에서 토큰은 데이터베이스 검사 및 재구축을 관리합니다.

CheckAlways

CA Access Control 을 초기화할 때 데이터베이스의 손상을 확인해야 하는지 여부를 결정합니다.

유효한 값은 yes 와 no 입니다.

기본값: yes

CheckProgram

데이터베이스를 확인하는 데 내부 코드 대신 사용할 대체 명령의 전체 경로 및 매개 변수를 지정합니다. 이 명령은 데이터베이스가 유효한 경우에는 0 을 반환하고, 데이터베이스를 수정해야 하는 경우에는 0 이외의 숫자를 반환합니다.

기본값: 토큰이 설정되지 않음(프로그램을 실행하지 않음. dbmgr -u -fast 를 사용하는 경우에도 동일.)

CreateNewClasses

seclassadm 유틸리티로 만든 새 클래스를 데이터베이스에 추가할 수 있는지 여부를 지정합니다.

유효한 값은 yes 와 no 입니다.

기본값: yes

CreateNewProps

CA Access Control sepropadm 유틸리티가 새 데이터베이스 속성을 만들 때 새 속성에 대한 데이터를 파일에 저장할지 여부를 지정합니다.

유효한 값은 yes 와 no 입니다.

이 값이 yes 이면 sepropadm 은 새 속성에 대한 데이터를 파일에 저장하고 나중에 dbmgr -c 유틸리티가 새 CA Access Control 데이터베이스를 생성하면 dbmgr 은 이 파일을 사용하여 데이터베이스에 이러한 속성을 추가합니다.

기본값: yes

RebuildAlways

CA Access Control 초기화 시 CA Access Control 데이터베이스를 항상 재구축해야 할지 여부를 나타냅니다.

유효한 값은 yes 와 no 입니다.

기본값: no

RebuildProgram

데이터베이스를 수정하는 데 내부 코드 대신 사용할 대체 명령의 전체 경로 및 매개 변수를 지정합니다.

기본값: 토큰이 설정되지 않음(프로그램 실행 안 함. dbmgr -u -build all 을 사용하는 경우와 동일)

seoswd

[seoswd] 섹션에서 토큰은 Watchdog 의 동작을 결정합니다.

IgnoreScanInterval

특정 간격으로 프로그램과 파일을 스캔할지 여부를 지정합니다.

토큰 값이 no 이면 watchdog 이 간격을 스캔하고 yes 이면 특정 간격으로 스캔하지 않습니다.

참고: PgmTestTime 또는 SecFileTestTime 토큰으로 검색 시간을 지정하지 않고 이 토큰을 yes 로 설정하면 watchdog 이 트러스트된 프로그램이나 보안된 파일을 각각 검색하지 않습니다.

기본값: no

PgmRest

마지막 이벤트 이후부터 프로그램을 다시 확인하기 전까지의 기간(초)을 지정합니다. 프로그램은 시스템 오버로드를 방지하기 위해 중지됩니다.

기본값: 10

PgmTestInterval

트러스트된 프로그램을 다시 스캔하는 시간 간격(초)을 지정합니다.

참고: 값이 하루(86400 초)와 같거나 하루보다 크면 IgnoreScanInterval 의 기본값은 yes 가 됩니다.

기본값: 18000(5 시간)

PgmTestStartTime

트러스트된 프로그램에 대한 첫 번째 검색 시작 시간을 지정합니다(형식: hh:mm).

이 토큰을 설정하지 않으면 Watchdog 은 시작 후 바로 첫 번째 스캔을 수행합니다.

기본값 없음.

PgmTestTime

트러스트된 프로그램에 대한 정기 검색 시간을 지정합니다(형식: hh:mm). 둘 이상의 스캔 시간을 공백으로 구분하여 지정할 수 있습니다.

참고: 검색 시간을 지정하지 않고 IgnoreScanInterval 토큰을 yes 로 설정하면 Watchdog 은 트러스트된 프로그램을 검색하지 않습니다.

기본값 없음.

RefreshParams

seos.ini 토큰의 Watchdog 에서 연속적으로 읽는 시간 간격(초)을 지정합니다.

기본값: 86400(1 일)

SecFileRest

마지막 이벤트 이후부터 보안된 파일을 다시 확인하기 전까지의 기간(초)을 지정합니다. 시스템 부하를 막기 위해 Watchdog 이 중지됩니다.

참고: 검색 시간을 지정하지 않고 IgnoreScanInterval 토큰을 yes 로 설정하면 seoswd 는 보안 파일을 검색하지 않습니다.

기본값: 10

SecFileTestInterval

보안된 파일을 다시 스캔하는 시간 간격(초)을 지정합니다.

기본값: 36000(10 시간)

SecFileTestStartTime

보안이 설정된 파일에 대한 첫 번째 검색 시작 시간을 지정합니다(형식: hh:mm).

값을 지정하지 않으면 Watchdog 은 CA Access Control 데몬이 시작된 후 바로 첫 검색을 수행합니다.

기본값 없음.

SecFileTestTime

보안이 설정된 파일에 대한 정기 검색 시간을 지정합니다(형식: hh:mm). 둘 이상의 스캔 시간을 공백으로 구분하여 지정할 수 있습니다.

기본값 없음.

SeosAYT

Watchdog 이 데몬 seosd 를 검사하는 시간 간격(초)을 지정합니다.

중요! 잘못된 값을 사용하면 CA Access Control 작동에 큰 문제가 생길 수 있으니 이 토큰을 직접 수정하지 마십시오. 도움이 필요하면 기술 지원 부서(http://www.ca.com/worldwide)에 문의하십시오.

기본값: 60

SignalMinInterval

시스템 오버로드를 방지하기 위해 HUP 신호가 요구 시 한 번 스캔을 트리거한 후 스캔 사이의 간격(초)을 지정합니다.

참고: 요구 시 검색은 트러스트된 프로그램과 보안 파일에서 모두 수행됩니다.

기본값: 60

UnTrustMissing

파일이 삭제되었거나 관련 NFS 파티션이 마운트되지 않은 경우처럼 Watchdog 이 프로그램이나 파일을 찾을 수 없는 경우에도 프로그램이나 파일을 언트러스트할지 여부를 결정합니다.

올바른 값은 다음과 같습니다.

yes-손실된 파일을 언트러스트합니다.

no-손실된 파일을 언트러스트하지 않습니다.

기본값: yes

VerifyCtime

CA Access Control Watchdog 이 트러스트된 프로그램과 보안 파일의 마지막 파일 상태 변경 시간을 확인할지 여부를 지정합니다.

유효한 값은 yes 또는 no 입니다.

기본값: no

serevu

[serevu] 섹션에서 토큰은 serevu 유틸리티의 특성을 결정합니다.

config_file

serevu 구성 파일의 위치를 지정합니다.

기본값: ACInstallDir/etc/serevu.cfg

def_diff_time

serevu 가 실패한 로그인에 대해 관련 시스템 로그를 스캔하는 동안 시간 간격을 지정합니다.

값을 초(즉 300) 또는 분(즉 5m)으로 지정합니다.

예를 들어 토큰을 300 으로 설정하면 serevu 는 이전 300 초 동안 발생한 실패한 로그인을 검색합니다.

이 값은 def_sleep_time 토큰 값의 배수가 되는 것이 좋습니다.

기본값: 5m(5 분)

def_disable_time

실패한 로그인 시도가 너무 많아 사용자 계정이 비활성화되는 시간을 지정합니다.

값을 초(즉 300) 또는 분(즉 5m)으로 지정합니다.

기본값: 6m(6 분)

def_fail_count

def_diff_time 토큰의 기간당 각 사용자에게 지정된 실패한 로그인 횟수를 지정합니다.

지정된 기간 동안 적어도 이 횟수 이상 로그인에 실패한 사용자는 비활성화됩니다.

참고: 로그인 실패 횟수는 시스템에 설정된 로그인 시도 실패 허용 값과 항상 동일한 것이 좋습니다. 예를 들어 Sun Solaris 에서는 /etc/default/login 파일의 RETRIES 토큰을 사용하여 시스템 값을 설정합니다.

Solaris 에서는 기본값이 5, HP-UX 및 AIX 에서는 3 입니다. 자세한 내용은 운영 체제 설명서를 참조하십시오.

기본값: 5

def_sleep_time

연속적인 serevu 검사 간격을 지정합니다.

값은 초(2 초) 또는 분(2 분)으로 지정됩니다.

기본값: 2m(2 분)

save_disable_path

serevu 가 중단될 때 비활성화된 사용자 계정 목록의 위치를 지정합니다.

기본값: ACInstallDir/log/serevu_disable.users

추가 정보:

serevu 유틸리티-실패한 로그인 시도 처리 (페이지 207)

sesu

[sesu] 섹션에서 토큰은 다른 사용자의 암호를 입력하지 않고 그 사용자로 로그인하는 동작을 제어합니다.

AlwaysTargetShell

대상 셸(SysV 스타일) 또는 호출자 셸(BSD 스타일) 중에서 사용할 셸을 결정합니다. yes 로 설정하면 CA Access Control 은 대상 사용자 셸을 사용합니다.

유효한 값은 yes 와 no 입니다.

기본값: no

FilterEnv

대상 사용자가 root 인 경우 sesu 가 셸에 전달하지 않는 환경 변수 목록을 지정합니다. 변수 이름은 공백 및 탭으로 분리됩니다.

기본값 없음.

old_sesu

기존 sesu 유틸리티를 사용할지 새 sesu 유틸리티를 사용할지 여부를 결정합니다.

올바른 값은 다음과 같습니다.

yes-이전 버전에 있던 기존 sesu 유틸리티를 사용합니다.

no-새 sesu 유틸리티가 SystemSu 토큰에 정의된 기본 su 프로그램을 호출하여 su 와 sesu 의 일관성을 유지합니다. SystemSu 토큰이 유효하지 않은 경우 sesu 는 이전 메커니즘으로 되돌립니다.

참고: 이 토큰을 no 로 설정하면 토큰 경로, AlwaysTargetShell, sys_env_file 및 FilterEnv 가 무시됩니다.

기본값: yes

Path

sesu 가 PATH 환경 변수를 설정할 때 사용하는 값을 지정합니다. 이 토큰을 설정하지 않으면 sesu 가 PATH 변수를 설정하지 않습니다.

기본값 없음.

request_target_password

old_sesu 토큰이 no 로 설정되고 대상 사용자가 비 root 사용자에 대해 sesu 를 실행할 때 대상 사용자의 암호를 요청할지 여부를 지정합니다.

기본값: yes

sys_env_file

sesu 세션에 대한 환경 변수 값이 들어 있는 ASCII 파일을 지정합니다. 이 토큰은 "-" 매개 변수를 사용하는 sesu(sesu-)를 시작할 때만 적용됩니다. 파일의 각 행 형식은 variable = value 입니다.

기본값: 없음(기본값이 /etc/environment 인 IBM AIX 제외)

SystemSu

/bin/su 프로그램의 위치를 지정합니다. 기본 위치가 아닌 곳에서 프로그램을 사용하려면 이 토큰을 업데이트합니다. sesu 가 권한 부여 데몬을 찾을 수 없는 경우 이 토큰에 지정된 프로그램을 실행합니다.

참고: AIX 에서는 시스템 su 바이너리를 sesu 바이너리 대신 sesu 래퍼에 대한 심볼 링크로 바꾸십시오.

기본값: /bin/su

UseInvokerPassword

sesu 를 사용하려면 호출자가 암호를 지정해야 하는지 여부를 결정합니다. 토큰 값이 no 이면 sesu 에 암호가 필요하지 않습니다.

기본값: no

추가 정보:

sesu 유틸리티 - 사용자 전환 (페이지 210)

sesudo

[sesudo] 섹션에서 토큰은 sesudo 유틸리티의 특성을 결정합니다.

echo_command

sesudo 가 명령을 실행하기 전에 그 명령을 표시하는지 여부를 결정합니다. 명령을 에코하려면 토큰 값을 yes 로 설정합니다.

기본값: No

echo_success

sesudo 명령이 성공적으로 실행되면 sesudo 이 터미널에 성공 메시지를 인쇄할지 여부를 결정합니다.

유효한 값은 yes 와 no 입니다.

기본값: yes

추가 정보:

sesudo 유틸리티 (페이지 212)

standalone

[standalone] 섹션에서 토큰은 독립 실행형 컴퓨터를 사용하여 관리할 옵션을 지정합니다.

full_login_check

독립 실행형 컴퓨터에 로그인하여 사이트를 관리할지 여부를 지정합니다.

유효한 값은 0 과 1 입니다.

이 토큰을 1 로 설정하면 컴퓨터에 로그인하는 것으로 간주합니다.

기본값: 0

tng

[tng] 섹션에서 토큰은 CA Access Control 을 Unicenter TNG 환경에 통합하는 동작을 제어합니다.

defsesid

특정 세션 그룹 ID 가 정의되지 않은 사용자의 기본 세션 그룹 ID 를 지정합니다.

세션 그룹은 CA SSO 에 의해 사용됩니다.

기본값: CAUNICENTER

ssf_numsubp

sessfgate 데몬이 들어오는 SSF 요청 처리를 시작하는 데 필요한 하위 프로세스의 수를 지정합니다.

기본값: 1

sso_applname

CA SSO 의 CA-Ticket 기능을 사용하는 사이트의 경우, data/keymgmt 폴더의 seos 홈 디렉터리에 있는 keymgmt 파일과 반드시 일치하는 8 자리 문자열을 지정합니다. 이러한 파일 이름은 SSO_APPLNAME_key 에 있습니다.

예를 들어 UNICENTR 의 기본값을 가져오는 경우 파일 이름은 UNICENTR_key 가 됩니다.

기본값: UNICENTR

pmd.ini 파일

UNIX 에 해당

pmd.ini 파일에는 CA Access Control 이 PMDB 를 작성 및 유지 관리할 때 사용하는 다양한 설치 및 초기화 설정이 포함되어 있습니다. 이 파일은 여러 섹션으로 구성되어 있으며 각 섹션에는 여러 설정이 포함되어 있습니다.

섹션	설명
endpoint_management	정책 모델 끝점 관리 설정
lang	정책 모델로 작업하기 위한 CA Access Control 관리 인터페이스(selang) 설정.
logmgr	PMDB 로깅 기능 설정.
passwd	사용자 및 암호 데이터 설정.
pmd	정책 모델 데몬("sepmdd") 설정.
seos	일반 PMDB 설정.

endpoint_management

[endpoint_management] 섹션은 정책 모델의 끝점 관리 설정을 정의하는 매개 변수를 수록하고 있습니다.

debug_mode

CA Access Control 이 DMS 디렉터리(1)의 endpoint_management.log 파일에 디버그 메시지를 기록할지 여부를 지정합니다.

제한: 0,1

기본값: 0(디버깅 사용 안 함)

참고: 로그 파일은 ACInstallDir/log/endpoint_management.log 에 있습니다.

operation_mode

CA Access Control 메시지 큐를 통한 중앙 (DMS) 끝점 관리를 사용할지 여부를 지정합니다.

제한: 0,1

기본값: 1(사용됨)

lang

[lang] 섹션에는 CA Access Control 언어 프로그램(selang)이 PMDB 를 작성 및 유지 관리할 때 사용하는 매개 변수가 포함되어 있습니다.

pre_user_exit

CA Access Control 이 UNIX 사용자 데이터베이스를 업데이트하기 위한 언어 명령을 실행하기 전에 실행될 exit 프로그램의 경로를 지정합니다.

post_user_exit

CA Access Control 이 UNIX 사용자 데이터베이스를 업데이트하기 위한 언어 명령을 실행한 후에 실행될 exit 프로그램의 경로를 지정합니다.

pre_group_exit

CA Access Control 이 UNIX 그룹 데이터베이스를 업데이트하기 위한 언어 명령을 실행하기 전에 실행될 exit 프로그램의 경로를 지정합니다.

post_group_exit

CA Access Control 이 UNIX 그룹 데이터베이스를 업데이트하기 위한 언어 명령을 실행한 후에 실행될 exit 프로그램의 경로를 지정합니다.

logmgr

[logmgr] 섹션은 PMDB 로그인 기능에 사용할 매개 변수를 포함합니다.

audit_back

PMDB 감사 백업 파일 이름을 지정합니다.

기본값: pmd_audit.bak

audit_log

PMDB 감사 로그 파일의 이름을 지정합니다.

기본값: pmd_audit

audit_group

PMDB 감사 파일을 읽을 수 있는 그룹을 지정합니다. 그룹을 지정하지 않으면 root 사용자만 감사 파일을 읽을 수 있습니다. CA Access Control 은 이 토큰의 값을 확인하지 않습니다. 따라서 사용자가 잘못된 그룹 이름을 입력하면 CA Access Control 은 감사 로그 파일에 어떤 그룹 권한도 할당하지 않습니다.

기존 감사 로그 파일의 그룹 소유권을 변경하려면 다음을 수행합니다.

1. selang 명령 chgrp 을 사용하여 파일의 그룹 소유권을 설정합니다.
2. 다음을 입력하여 UNIX 권한을 변경합니다.

```
chmod 640 /opt/CA/AccessControl/log/seos.audit
```

audit_size

PMDB 감사 로그 파일의 크기(KB)를 지정합니다. 50 KB 보다 작은 크기를 지정하지 않습니다.

기본값: 50KB

error_back

PMDB 오류 백업 파일 이름을 지정합니다.

기본값: pmd_error.bak

error_log

PMDB 오류 로그 파일 이름을 지정합니다.

기본값: pmd_error

error_group

PMDB 오류 파일을 읽을 수 있는 그룹을 지정합니다. 그룹을 지정하지 않으면 root 사용자만 오류 파일을 읽을 수 있습니다. CA Access Control 은 이 토큰의 값을 확인하지 않습니다. 따라서 사용자가 잘못된 그룹 이름을 입력하면 CA Access Control 은 오류 로그 파일에 어떤 그룹 권한도 할당하지 않습니다.

기존 오류 로그 파일의 그룹 소유권을 변경하려면 다음을 수행합니다.

1. selang 명령 chgrp 을 사용하여 파일의 그룹 소유권을 설정합니다.
2. 다음을 입력하여 UNIX 권한을 변경합니다.

```
chmod 640 /opt/CA/AccessControl/log/seos.error
```

error_size

PMDB 오류 로그 파일(error_log 로 정의)의 최대 크기(KB)를 정의합니다.

제한: 최소값 50KB.

기본값: 50

max_log_size

PMDB 일반 로그 파일의 크기(KB)를 지정합니다.

기본값: 50KB

pmd_log_level

PMDB 로그 파일에 기록되는 메시지를 확인합니다.

올바른 값은 다음과 같습니다.

0-어떠한 항목도 기록하지 않습니다.

1-오류 메시지만 나열합니다.

2-오류 및 정보 메시지를 나열합니다.

기본값: 2

use_syslog

정책 모델 데몬이 syslog 메시지를 작성할지 여부를 결정합니다.

기본값: yes

passwd

[passwd] 섹션은 UID 와 GID 의 매개 변수를 포함합니다.

AllowedGidRange

예약된 수를 지정합니다.

첫 번째 숫자보다 작고 두 번째 숫자보다 큰 정수는 CA Access Control 이 업데이트할 수 없는 예약된 GID 입니다.

참고: 하나의 정수만 지정하는 경우 1 부터 지정된 정수 사이의 모든 정수가 예약된 GID 입니다. 상한값보다 높은 숫자를 지정하면 기본 상한값(30000)이 적용됩니다. 음수를 지정하면 기본 하한값(1)이 적용됩니다.

제한: 1 ~ 2147483647

기본값: 100,30000

AllowedUidRange

예약된 수를 지정합니다.

첫 번째 숫자보다 작고 두 번째 숫자보다 큰 정수는 CA Access Control 이 업데이트할 수 없는 예약된 UID 입니다.

참고: 하나의 정수만 지정하는 경우 1 부터 지정된 정수 사이의 모든 정수가 예약된 UID 입니다.

기본값: 100,30000

pmd

[pmd] 섹션은 PMDB 를 빌드하고 유지 관리할 때 sepmdd 데몬이 사용하는 특성을 포함합니다.

_min_retries_

사용할 수 없는 구독자에게 큐에 있는 다음번 업데이트를 다시 보내기 위해 sepmdd 가 시도해야 하는 최소 횟수를 지정합니다. sepmdd 는 보내지 못한 업데이트를 위해 구독자 목록을 처음부터 끝까지 돌며, 사용할 수 없는 구독자에게 업데이트를 다시 보낼 수 없으면 매회 카운터를 늘립니다. 이 토큰에 지정된 최소 시도 횟수 이후 구독자는 사용할 수 없는 상태로 표시됩니다.

기본값: 4

_QD_timeout_

구독자 목록의 첫 번째 스캔 중에 sepmdd 데몬이 구독자 데이터베이스를 업데이트하는 동안 대기하는 최대 시간(초)을 지정합니다. 시간이 경과되어도 데몬이 구독자 업데이트에 성공하지 못하면 해당하는 특정 구독자를 건너뛰고 목록에 있는 나머지 구독자를 업데이트합니다.

구독자 목록의 첫 스캔이 완료되면 sepmdd 는 첫 스캔 중에 업데이트하지 못한 구독자를 업데이트하는 두 번째 스캔을 수행합니다. 두번째 검사 중에는 연결 시스템 호출 시간(약 90 초)이 만료될 때까지 구독자를 업데이트합니다.

기본값: 3

_retry_timeout_

_min_retries_에 지정된 최소 시도 횟수를 수행한 후, 사용할 수 없는 구독자에게 업데이트를 다시 보내려고 시도하기까지 기다려야 하는 시간(분)을 지정합니다. 이 토큰에 정의된 시간(분)이 경과한 후 구독자는 사용 가능한 것으로 표시됩니다.

다음을 수행할 때까지 구독자는 사용할 수 없는 상태로 표시됩니다.

- 구독자는 수동으로 해제합니다.
- sepmdd 는 수동으로 종료되고 다시 시작됩니다. sepmdd 는 다음의 경우 다시 시작됩니다.
  - 언어 기능이 연결을 시도하는 경우
  - 부모 PMDB 가 업데이트를 보내고자 하는 경우
  - 구독자가 pull 옵션을 트리거한 경우 이는 CA Access Control 이 구독자에서 시작될 때 선택적으로 발생합니다.
- 사용할 수 없는 구독자에 의해 pull 옵션이 트리거됨.

참고: 데몬을 다시 시작하는 데에는 시간이 걸리며 그로 인해 전체 전파 프로세스의 속도가 느려질 수 있으므로 sepmdd 를 너무 자주 종료하는 것은 바람직하지 못합니다. 안정성 문제가 있을 수 있으므로 sepmdd 를 항상 실행 상태로 두는 것도 바람직하지 못합니다. 그러나 이는 추측일 뿐입니다.

기본값: 30 분

_shutoff_time_

sepmdd 가 종료되기 전 활동 시간(분)을 지정합니다. 토큰 값이 0 이면 sepmdd 가 종료되지 않습니다.

기본값: 0

always_propagate

이 토큰을 no 로 설정하면 정책 모델에 의해 실행되지 않은 명령은 구독자로 전파되지 않습니다.

기본값 없음.

exclude_file

제외 파일을 지정합니다.

제외 파일에는 수신하는 정책 모델 업데이트에서 제외해야 하는 호스트 이름(각 줄에 하나씩)이 있습니다.

기본값: empty

exclude_localhost

구독자로서 수신하는 업데이트에서 로컬 호스트를 제외하도록 pmdb 에 지시합니다.

가능한 값: yes, no.

기본값: no

exclude_method

구독자가 제외될 때 업데이트 파일에서 오프셋 승격을 활성화/비활성화합니다.

값:

"pmdwait"-오프셋 승격을 수행하지 않음

기타-"bypass"

기본값: pmdwait

필터

필터 파일의 이름을 지정합니다.

force_auto_truncate

정책 모델에 대한 구독자가 없는 경우에도 CA Access Control 이 업데이트 파일을 자를지 여부를 지정합니다.

사용자가 수동으로(sepmd -t) 업데이트 파일을 자를 수 있으며, CA Access Control 역시 자동 자르기를 트리거하는 이벤트를 정의하는 별도의 구성 설정(trigger_auto_truncate)을 기반으로 자동으로 파일을 자릅니다.

참고: 정책 모델에 대한 모든 구독자가 "동기화되지 않은" 경우 정책 모델은 실제로 구독자를 갖지 못합니다.

기본값: yes

group_file_name

새로운 UNIX 그룹에 대한 그룹 파일 이름을 지정합니다. sepmdd 는 새로운 UNIX 그룹의 그룹 항목을 이 파일에 저장합니다.

기본값: group

is_maker_checker

이중 컨트롤을 사용할지 여부를 지정합니다. 이 토큰의 올바른 값은 yes 및 no 입니다.

yes 를 선택하면 PMDB 를 직접 업데이트할 수 없고 트랜잭션을 통해서만 업데이트할 수 있으며, 한 관리자가 입력하는 각 트랜잭션을 다른 관리자가 처리해야 PMDB 에서 명령을 구현할 수 있습니다.

기본값: no

password_file_name

새로운 UNIX 사용자에 대한 암호 파일의 이름을 지정합니다. sepmdd 는 새로운 UNIX 사용자의 암호 항목을 이 파일에 저장합니다.

기본값: passwd

replicate_pmd

이 정책 모델에 대한 백업 역할을 하는 정책 모델의 이름입니다.

이 토큰에는 기본값이 없습니다.

토큰이 설정되어 있지 않으면 정책 모델은 백업되지 않습니다.

send_unix_env

sepmd 가 정책 모델 암호 파일 및 그룹 파일의 내용을 보내는지 여부를 나타냅니다.

이 토큰을 **yes** 로 설정하면 sepmd -n 옵션은 정책 모델 암호 파일과 그룹 파일의 내용을 전송합니다.

이 토큰을 **no** 로 설정하면 sepmd -n 옵션은 정책 모델 암호 파일 및 그룹 파일의 내용을 전송하지 않습니다.

기본값: yes

synch_uid

sepmdd 가 정책 모델과 구독이자 사이의 UID 를 동기화하려는지 여부를 결정합니다. 이 토큰의 올바른 값은 yes 및 no 입니다.

이 토큰을 **no** 로 설정하면 sepmdd 는 UID 동기화를 시도하지 않습니다. 각 구독이자 호스트의 첫 번째 사용 가능한 UID 가 사용자에게 할당됩니다.

이 토큰을 **yes** 로 설정하면 sepmdd 는 UID 동기화를 시도합니다. 예를 들어, PMDB 에서 1000 이라는 UID 를 가진 새 UNIX 사용자가 작성된 경우 sepmdd 가 이 UID 를 구독자에게 전달합니다. UID 1000 을 구독이자 중 한 명이 이미 사용하고 있는 경우 해당 구독자에 대한 업데이트가 실패합니다.

PMDB 에 전송된 원본 명령이 사용자의 UID 를 지정하지 않으면 sepmdd 가 UID 를 동기화하려고만 합니다. 원본 명령이 UID 를 지정한 경우 지정된 UID 가 모든 구독자에게 전달됩니다.

기본값: yes

TNG_Environment

특수한 TNG 클래스 및 리소스로 데이터베이스를 만들지 여부를 지정합니다.

유효한 값:

"0"은 특수한 TNG 클래스 없이 데이터베이스를 작성합니다.

"1"은 특수한 모든 TNG 클래스로 데이터베이스를 작성합니다.

기본값: 0

transaction_lib

maker-checker 정책 경로를 지정합니다.

기본값: 없음

trigger_auto_truncate

업데이트 파일의 자동 자르기를 트리거하는 정책 모델 업데이트 파일의 크기(MB)를 정의합니다.

하한값보다 낮은 값을 사용하면 CA Access Control 은 기본값을 사용합니다. 상한값보다 높은 값을 사용하면 CA Access Control 은 상한값을 사용합니다.

제한: 1 - 2000MB

기본값: 1024 MB

update_while_processing

정책 모델이 들어오는 이벤트를 처리하는 동안 구독자에게 명령을 전파하는 빈도를 정의합니다.

이 빈도는 updates_in_chunk 설정의 요소이며, PMD 가 줄에 있는 다음 구독자에게 한 세트의 명령을 전송하기 전에 얼마나 많은 명령을 처리할지를 결정합니다. 예를 들어, 이 빈도를 3 으로 설정하고 updates_in_chunk 를 10 으로 설정하면 PMD 는 줄에 있는 다음 구독자에게 명령(10) 세트를 한 번 전달하기 전에 30 개의 명령을 처리합니다. 값 0 은 들어오는 이벤트를 처리하는 동안 PMD 가 명령을 전파하지 않음을 의미합니다.

기본값: 1

updates_in_chunk

정책 모델이 루프의 각 주기에서 각각의 구독자에게 전달하는 최대 명령 수를 결정합니다.

기본값: 20

UseEncryption

파일에 저장된 업데이트 정보를 암호화할지 여부를 지정합니다.

기본값: no

UseShadow

PMDB 네이티브 환경을 참조하는 경우 섀도 파일을 사용할지 여부를 결정합니다.

기본값: no

YpServerSecure

NIS 암호 맵을 구축하는 데 사용되는 암호 섀도 파일(NIS 서버의 보안 파일) 이름을 지정합니다. UseShadow 를 yes 로 설정한 경우에만 이 토큰이 적합합니다.

기본값: /etc/shadow

seos

다음은 CA Access Control 이 사용하는 전역 설정을 포함하는 [seos] 섹션의 토큰에 대한 설명입니다.

parent_pmd

이 PMDB 에서 업데이트를 허용하는 PMDB(정책 모델 데이터베이스)의 목록을 쉼표로 구분하여 정의합니다. 이 PMDB 는 이 목록에 지정되지 않은 다른 PMDB 에서 오는 업데이트를 거부합니다.

줄로 구분된 PMDB 목록이 포함된 파일 경로를 지정할 수도 있습니다.

이 PMDB 가 모든 PMDB 에서 오는 업데이트를 허용하도록 하려면 이 토큰을 "_NO_MASTER_"로 설정하십시오.

이 토큰을 설정하지 않으면 이 PMDB 는 어떤 PMDB 에서 오는 업데이트도 허용하지 않습니다.

각 PMDB 는 pmd_name@hostname 형식으로 지정됩니다.

예:

```
parent_pmd = pmd1@host1,pmd2@host1,pmd3@host2
parent_pmd = /opt/CA/AccessControl/parent_pmdbs_file
```

기본값: 토큰이 설정되지 않음(PMDB 는 어떤 PMDB 에서 오는 업데이트도 허용하지 않음).

lang.ini 파일

UNIX 에 해당

이 섹션에서는 selang 유틸리티에서 사용되는 lang.ini 파일의 토큰에 대해 설명합니다.

lang.ini 파일은 다음 섹션으로 구성되어 있습니다.

general

두 가지 유형(새 리소스와 새 사용자) 이상의 리소스에 모두 적용되는 기본 매개 변수가 있습니다.

history

selang 기록 메커니즘에 대한 기본 매개 변수가 있습니다.

newres

새 리소스 레코드의 속성에 할당되는 기본 값이 있습니다. 명시적으로 다른 값을 설정하지 않으면 기본값이 할당됩니다.

newusr

새 사용자 레코드의 속성에 할당되는 기본값이 있습니다. 명시적으로 다른 값을 설정하지 않으면 기본값이 할당됩니다.

properties

사용자 정의 속성에 대한 사용자 정의 속성 값(예: 파일 위치)을 지정하는 토큰이 있습니다. 이 토큰에는 기본값이 없으므로, 명시적으로 기본값을 설정해야 합니다.

unix

새 사용자가 selang 명령 셸에서 UNIX 로 정의될 때 할당되는 기본값이 있습니다. 명시적으로 다른 값을 설정하지 않으면 기본값이 할당됩니다.

general

[general] 섹션에는 두 가지 유형 이상의 리소스에 적용되는 기본 매개 변수가 있습니다.

defaultOwner

새 레코드에 할당된 소유자의 이름입니다.

값을 지정하지 않을 경우, 새 레코드의 작성자가 소유자로 할당됩니다.

history

[history] 섹션에는 selang 기록 메커니즘에 대한 기본 매개 변수가 있습니다.

HistFile

기록 목록의 명령이 저장된 파일 이름입니다. 명령 목록은 각 세션을 시작할 때 로드됩니다.

기본값 없음(세션 종료 시 기록 목록이 저장되지 않음)

HistSize

기록 메커니즘에 의해 저장되는 명령 개수(10 과 100 사이의 양수)입니다.

기본값: 30

newres

[newres] 섹션에는 newres 명령이 할당하는 기본값이 포함됩니다. newres 명령은 데이터베이스에 새 리소스 레코드를 생성합니다. 이 섹션의 각 토큰은 newres 매개 변수를 나타냅니다. lang.ini 파일에 없는 매개 변수에는 CA Access Control 에 하드 코딩된 기본값이 할당됩니다. 토큰에 대한 값을 지정하지 않을 경우 테이블에 지정된 기본값이 적용됩니다.

DefaultAudit

새 리소스의 기본 감사 모드입니다. 유효한 값은 none, all, success, failure 입니다.

기본값: failure

DefaultDay

리소스에 적용되는 기본 날짜 제한사항입니다. 유효한 값: anyday, weekdays, mon, tue, wed, thu, fri, sat, sun

기본값: anyday

DefaultNotify

리소스 레코드에 대한 경고 메시지가 전송되는 기본 전자 메일 주소입니다.

기본값 없음(알림 메시지가 전달되지 않음)

DefaultTime

리소스에 적용되는 기본 시간 제한사항입니다. 유효한 값: anytime, startTime:endTime.

기본값: anytime

DefaultWarning

기본적으로 경고 모드가 활성화되었는지 여부입니다. 유효한 값은 yes, no 입니다.

기본값: no

newusr

[newusr] 섹션에는 데이터베이스에 새 사용자 레코드를 생성하는 newusr 명령에 의해 할당된 기본값이 수록되어 있습니다. 이 섹션의 각 토큰은 newusr 매개 변수를 나타냅니다. lang.ini 파일에 없는 매개 변수에는 CA Access Control 에 하드 코딩된 기본값이 할당됩니다. 토큰에 대한 값을 지정하지 않을 경우 테이블에 지정된 기본값이 적용됩니다.

DefaultAudit

새 사용자에 대한 기본 감사 모드입니다. 유효한 값: none, all, success, failure, loginsuccess loginfailure

기본값: failure loginfailure loginsuccess

DefaultDay

시스템에 로그인할 때 사용자에게 적용되는 기본 요일 제한입니다. 유효한 값: anyday, weekdays, mon, tue, wed, thu, fri, sat, sun

기본값: anyday

DefaultExpire

사용자 레코드에 대한 기본 만료 날짜입니다. 유효한 값: expire[dd/mm/yy], expire-.

기본값: expire-

DefaultLocation

사용자가 근무하는 기본 위치입니다.

기본값 없음

DefaultNotify

사용자가 로그인할 때 알림 메시지가 전달되는 기본 전자 메일 주소입니다.

기본값 없음(알림 메시지가 전달되지 않음)

DefaultOrg

사용자가 근무하는 조직입니다.

기본값 없음

DefaultOrgUnit

사용자가 근무하는 조직 단위입니다.

기본값 없음

DefaultTime

시스템에 로그인할 때 사용자에게 적용되는 기본 시간 제한입니다. 유효한 값: anytime, startTime:endTime.

기본값: anytime

properties

"properties" 섹션에는 사용자 정의 속성에 적용되는 매개 변수가 있습니다.

UserDefinedTokensFile

사용자 정의 속성에 대한 상황별 정보가 포함된 정의 파일의 경로입니다.

기본값: 없음

UserDefinedAttributesFile

사용자 정의 속성에 대한 속성 정보가 포함된 정의 파일의 경로입니다.

기본값: 없음

사용자 정의 속성

이 섹션에는 sepropadm 유틸리티에 대한 보충 내용이 포함되어 있습니다. 이 섹션은 sepropadm 으로 생성된 데이터베이스 속성을 인식하는 데 사용되는 selang 컨텍스트를 정의합니다. sepropadm 이 사용하는 형식과 유사한 형식을 사용하는 두 개의 정의 파일이 이 작업을 수행합니다. 두 파일의 위치는 이 섹션의 토큰 두 개에 지정됩니다.

참고: 정의 파일이 selang 에 의해 로드되기 전에 sepropadm 유틸리티를 사용하여 데이터베이스에서 속성을 정의해야 합니다. 정의 파일은 초기화 단계 중에 selang 이 실행되면 자동으로 로드됩니다.

해당 정의 파일과 데이터베이스에서 모두 이러한 속성을 정의하면 selang 명령에서도 다른 CA Access Control 정의 속성처럼 이러한 속성을 사용할 수 있습니다.

중요! 공급업체의 기술 지원 담당자가 인증하지 **않은** 설명 파일을 sepropadm 유틸리티와 함께 사용하지 **마십시오.**

추가 정보:

sepropadm 유틸리티-데이터베이스 속성 관리 (페이지 198)

정의 파일

selang 은 새 사용자 정의 속성을 인식하기 위해 초기화 중에 두 개의 *.def 파일인 토큰 파일과 속성 파일을 로드합니다.

토큰 파일

사용자 정의 토큰 파일

공급업체의 기술 지원 담당자가 제공하는 정의 파일입니다. 설명 파일의 형식은 다음과 같습니다.

세미콜론(;)으로 시작되는 행은 주석이고 처리되지 않습니다.

해시 기호(#)로 시작하는 행이 한 개는 있어야 합니다. 설명 줄 앞에 와야 합니다.

설명 줄은 다음과 같은 서식으로 확인됩니다.

```
TOKEN=%s DOMAIN=%d CLASS=%d COMMAND=%d
```

다음은 예제 정의 토큰 파일입니다.

```
; Sample Token Definition File for user defined properties
; Copyright 2004 Computer Associates International, Inc.
; ---------------------------------------------
; DO NOT USE THIS FILE UNLESS YOU KNOW HOW TO!
# token definition file
; Format is :
TOKEN=EMAIL DOMAIN=1 CLASS=USER COMMAND=206
TOKEN=NOEMAIL DOMAIN=1 CLASS=USER COMMAND=206
TOKEN=EMAIL DOMAIN=1 CLASS=USER COMMAND=218
TOKEN=AGE DOMAIN=1 CLASS=USER COMMAND=206
TOKEN=AGE DOMAIN=1 CLASS=USER COMMAND=218
TOKEN=NOAGE DOMAIN=1 CLASS=USER COMMAND=206
TOKEN=TERMLOCATION DOMAIN=1 CLASS=TERMINAL COMMAND=217
TOKEN=NOTERMLOCATION DOMAIN=1 CLASS=TERMINAL COMMAND=205
TOKEN=TERMLOCATION DOMAIN=1 CLASS=TERMINAL COMMAND=205
```

특성 파일

사용자 정의 특성 파일

공급업체의 기술 지원 담당자가 제공하는 정의 파일입니다. 설명 파일의 형식은 다음과 같습니다.

세미콜론(;)으로 시작되는 행은 주석이고 처리되지 않습니다.

해시 기호(#)로 시작하는 행이 한 개는 있어야 합니다. 설명 줄 앞에 와야 합니다.

설명 줄은 다음과 같은 서식으로 확인됩니다.

```
PROPERTY=%s TYPE=%d FLAGS=%x
```

다음은 예제 정의 특성 파일입니다.

```
; Sample Attributes Definition File for user defined properties
; Copyright 2004 Computer Associates International, Inc.
; ----------------------------------------------
; DO NOT USE THIS FILE UNLESS YOU KNOW HOW TO!
# attributes definition file
; Format is :
PROPERTY=EMAIL TYPE=306 FLAGS=8000
PROPERTY=EMAIL TYPE=5 FLAGS=8000
PROPERTY=AGE TYPE=306 FLAGS=8000
PROPERTY=AGE TYPE=5 FLAGS=8000
PROPERTY=TERMLOCATION TYPE=306 FLAGS=8000
PROPERTY=TERMLOCATION TYPE=5 FLAGS=8000
```

중요! 공급업체의 기술 지원 담당자가 인증하지 **않은** 정의 파일을 selang 유틸리티와 함께 사용하지 **마십시오.**

unix

[unix] 섹션에는 UNIX 에 사용자를 추가할 때 newusr 명령이 할당하는 기본값이 포함됩니다. 이 섹션의 각 토큰은 unix 매개 변수의 인수를 나타냅니다. lang.ini 파일에 없는 UNIX 인수에는 CA Access Control 에 하드 코딩된 기본값이 할당됩니다.

DefaultPGroup

새 사용자에게 할당된 기본 그룹입니다. 서버의 seos.ini 파일에서 기본 셸을 지정하면, 그 값이 여기에 지정된 값보다 우선합니다.

기본값: 기타

DefaultShell

새 사용자의 기본 셸입니다. 서버의 seos.ini 파일에서 기본 셸을 지정하면, 그 값이 여기에 지정된 값보다 우선합니다.

기본값: /bin/sh

DefaultHome

시스템의 기본 홈 디렉터리입니다. 서버의 seos.ini 파일에서 기본 셸을 지정하면, 그 값이 여기에 지정된 값보다 우선합니다. 사용자의 홈 디렉터리는 지정한 시스템 홈 디렉터리의 하위 디렉터리입니다. 예를 들어, 시스템 홈 디렉터리가 /home 인 경우 새 사용자의 홈 디렉터리는 /home/username 입니다. 서버의 seos.ini 파일에서 홈 디렉터리 상위 경로를 지정하면, 그 값이 여기에 지정된 값보다 우선합니다.

이전 버전에 익숙한 사용자를 위해 DefaultHome 토큰이 HomeDirPrefix 를 대체합니다.

기본값: /home

trcfilter.init

UNIX 에 해당

CA Access Control 데몬은 trcfilter.init 초기화 파일도 사용합니다.

이 선택적 파일에는 CA Access Control 추적 메시지를 필터링하기 위한 필터 마스크를 지정하는 항목이 들어 있습니다. 파일의 각 행은 정규 표현식을 포함합니다. 메시지가 추적 파일로 전송되면 seosd 는 메시지가 trcfilter.init 파일의 항목 중 하나와 일치하는지 여부를 확인합니다. trcfilter.init 파일에 지정된 표현식과 모두 일치하지 않을 경우에만 추적 메시지를 파일에 씁니다.

예를 들어, 다음 trcfilter.init 파일은 "INFO" 또는 "WATCHDOG"으로 시작하는 모든 메시지를 삭제합니다. 이러한 메시지는 추적 파일에 기록되지 않습니다.

```
WATCHDOG*
INFO*
```

참고: 이 파일은 사용자 추적에 의해 생성된 감사 레코드를 필터링하지 않습니다. 이러한 감사 레코드를 필터링하려면 audit.cfg 파일을 편집하십시오.

audit.cfg 파일 - 감사 레코드 필터링

audit.cfg 파일은 감사 파일로 전송되지 않는 레코드를 정의하여 호스트의 감사 레코드를 필터링합니다. 각 줄은 감사 정보를 필터링하는 하나의 규칙을 나타냅니다.

기본적으로 audit.cfg 파일은 ACInstallDir/etc 디렉터리(UNIX) 또는 ACInstallDir\data 디렉터리(Windows)에 있습니다. seos.ini 파일의 [logmgr] AuditFiltersFile 토큰(UNIX) 또는 logmgr 레지스트리 키의 AuditFiltersFile 항목(Windows)을 편집하여 audit.cfg 파일의 위치를 변경할 수 있습니다.

audit.cfg 파일을 사용하여 각각 다른 구문으로 다음 감사 이벤트 유형의 레코드를 필터링할 수 있습니다.

- 리소스 액세스
- 네트워크 연결
- 로그인 및 로그아웃 이벤트
- 보안 데이터베이스 관리
- 사용자에 대한 추적 메시지

참고: 각 구문 유형에서 열에 표시된 *는 "모든 값"을 나타냅니다.

리소스 액세스 이벤트 필터 구문

리소스 액세스 이벤트에 속하는 감사 레코드는 다음과 같은 필터 형식을 갖습니다.

```
ClassName;ObjectName;UserName;ProgramPath;Access;AuthorizationResult
```

ClassName

액세스한 개체가 속하는 클래스의 이름을 정의합니다.

참고: 클래스 이름은 대문자로 입력해야 합니다.

ObjectName

액세스한 개체의 이름을 정의합니다.

UserName

접근자의 이름을 정의합니다.

ProgramPath

개체를 액세스하는 데 사용된 프로그램의 이름을 정의합니다.

Access

개체에 대해 요청된 액세스를 정의합니다.

참고: 다음 값은 감사 레코드를 필터링하기 위해 audit.cfg 파일에 사용하는 이 매개 변수의 값입니다. 경우에 따라 audit.cfg 파일에 있는 이 매개 변수의 값은 CA Access Control 에서 해당 이벤트에 대해 감사 레코드에 쓰는 값과 다릅니다. 이러한 차이는 각 값의 설명 뒤에 나와 있습니다. 다음 목록에 표시된 대로 대/소문자를 구분하여 매개 변수를 입력해야 합니다.

값:

*****

모든 유형의 액세스를 나타내는 와일드카드입니다.

Chdir

디렉터리 변경 - 접근자가 개체를 다른 디렉터리로 이동하도록 요청했습니다.

Chmod

모드 변경 - 접근자가 개체 모드를 변경하도록 요청했습니다.

Chgrp

(UNIX) 그룹 변경 - 접근자가 개체가 속하는 그룹을 변경하도록 요청했습니다.

Chown

소유자 변경 - 접근자가 개체의 소유자를 변경하도록 요청했습니다.

Connect

사용자를 그룹에 가입 - 접근자가 새 사용자를 그룹에 추가하도록 요청했습니다.

참고: Connect 값은 Join 값과 같습니다.

Control

(UNIX) 제어 - 접근자가 개체에 대한 Chown, Chmod, Utime, Sec, Chdir 및 Update 액세스를 요청했습니다.

Cre

만들기 - 접근자가 개체를 만들도록 요청했습니다.

Crrdwr

만들기, 읽기 및 쓰기 - 접근자가 개체에 대한 만들기, 읽기 및 쓰기 권한을 요청했습니다.

참고: CA Access Control 는 이 값을 해당 감사 레코드에 CrRdWrite 로 씁니다.

Crread

만들기 및 읽기 - 접근자가 개체에 대한 만들기 및 읽기 권한을 요청했습니다.

참고: CA Access Control 는 이 값을 해당 감사 레코드에 CrRead 로 씁니다.

Crwrite

만들기 및 쓰기 - 접근자가 개체에 대한 만들기 및 쓰기 권한을 요청했습니다.

참고: CA Access Control 는 이 값을 해당 감사 레코드에 CrWrite 로 씁니다.

Del

삭제 - 접근자가 개체를 삭제하도록 요청했습니다.

참고: CA Access Control 는 이 값을 해당 감사 레코드에 Erase 로 씁니다.

Filereplace

만들기 및 지우기 - 접근자가 개체에 대한 만들기 및 지우기 권한을 요청했습니다.

참고: CA Access Control 는 이 값을 해당 감사 레코드에 Replace 로 씁니다.

Filescan

파일 검사 - 접근자가 개체에 대한 나열 권한을 요청했습니다.

참고: CA Access Control 는 이 값을 해당 감사 레코드에 Scan 으로 씁니다.

Join

사용자를 그룹에 가입 - 접근자가 새 사용자를 그룹에 추가하도록 요청했습니다.

참고: Join 값은 Connect 값과 같습니다.

Kill

종료 - 접근자가 프로세스를 종료하도록 요청했습니다.

Modify

수정 - 접근자가 개체에 대한 수정 권한을 요청했습니다.

OwnGrp

소유자 변경 및 그룹 변경 - 접근자가 개체에 대한 Chown 및 Chgrp 권한을 요청했습니다.

PW

암호 - 접근자가 암호를 변경하도록 요청했습니다.

참고: CA Access Control 는 이 값을 해당 감사 레코드에 Password 로 씁니다.

R

읽기 - 접근자가 개체에 대한 읽기 권한을 요청했습니다.

참고: (UNIX) STAT_intercept 가 1 로 설정된 경우 이 매개 변수에 stat 차단이 포함됩니다.

Rename

파일 이름 변경 - 접근자가 개체의 파일 이름을 변경하도록 요청했습니다.

Sec

ACL 변경 - 접근자가 개체의 ACL 을 편집하도록 요청했습니다.

참고: CA Access Control 는 이 값을 해당 감사 레코드에 ACL 로 씁니다.

Update

읽기, 쓰기 및 실행 - 접근자가 개체에 대한 읽기, 쓰기 및 실행 권한을 요청했습니다.

참고: Update 값은 접근자가 개체에 대한 읽기 및 쓰기 권한을 요청한 이벤트도 필터링합니다.

Utime

(UNIX) 시간 변경 - 접근자가 개체의 수정 시간을 변경하도록 요청했습니다.

참고: CA Access Control 는 이 값을 해당 감사 레코드에 Utimes 로 씁니다.

W

쓰기 - 접근자가 개체에 대한 쓰기 권한을 요청했습니다.

X

실행 - 접근자가 개체를 실행하도록 요청했습니다.

참고: 일부 클래스에 유효하지 않은 값도 있습니다. 예를 들어 FILE 클래스의 개체에는 kill 동작을 사용할 수 없으므로 kill 은 FILE 클래스에 유효하지 않은 값입니다. 규칙을 작성할 때 클래스에 유효하지 않은 값을 입력하면 CA Access Control 에서 파일을 읽을 때 해당 규칙을 무시합니다.

AuthorizationResult

권한 부여 결과를 정의합니다.

값: P(허용됨), D(거부됨), *

네트워크 연결 이벤트 필터 구문

네트워크 연결 이벤트에 속하는 감사 레코드는 다음과 같은 필터 형식을 갖습니다.

```
{HOST|TCP};ObjectName;HostName;ProgramPath;Access;AuthorizationResult
```

HOST

규칙에서 HOST 클래스의 개체에 의해 생성된 레코드, 즉 들어오는 TCP 연결을 필터링하도록 지정합니다.

TCP

규칙에서 TCP 클래스의 개체에 의해 생성된 레코드, 즉 서비스 이벤트와의 연결을 필터링하도록 지정합니다.

ObjectName

액세스한 개체의 이름을 정의합니다. ObjectName 은 서비스 이름이나 포트 이름일 수 있습니다.

HostName

호스트의 이름을 정의합니다. HostName 은 HOST 클래스의 객체여야 합니다.

ProgramPath

로그인 프로그램 유형을 정의합니다.

(Windows) 나가는 연결에 대해 이 매개 변수는 연결 설정을 시도하는 프로세스의 프로그램 경로를 정의합니다.

참고: 이 매개 변수는 들어오는 연결 이벤트에는 의미가 없습니다. 들어오는 연결 이벤트에 의해 생성된 감사 레코드를 필터링하려면 이 매개 변수에 대해 *를 사용합니다.

Access

시도된 연결 유형을 정의합니다.

값:

- (HOST) *
- (TCP) R(들어오는 연결), W(나가는 연결), *

AuthorizationResult

권한 부여 결과를 정의합니다.

값: P(허용됨), D(거부됨), *

로그인 및 로그아웃 이벤트 필터 구문

로그인 또는 로그아웃 이벤트에 속하는 감사 레코드는 다음과 같은 필터 형식을 갖습니다.

```
LOGIN;UserName;UserId;TerminalName;LoginProgram;AuthorizationResultOrLoginType
```

LOGIN

규칙에서 로그인 및 로그아웃 이벤트에 의해 생성된 감사 레코드를 필터링하도록 지정합니다.

UserName

접근자의 이름을 정의합니다.

UserId

접근자의 기본 사용자 ID 를 정의합니다.

TerminalName

이벤트가 발생한 터미널을 정의합니다.

LoginProgram

로그인 또는 로그아웃을 시도한 프로그램의 이름을 정의합니다.

AuthorizationResultorLoginType

권한 부여 결과를 정의합니다.

값:

*****

모든 유형의 권한 부여 결과를 나타내는 와일드카드입니다.

D

로그인 시도가 거부되었습니다.

P

로그인 시도가 허용되었습니다.

O

(UNIX) 접근자가 로그아웃했습니다.

-I

(UNIX) serevu 데몬이 접근자의 계정을 해지했습니다.

E

(UNIX) serevu 데몬이 접근자의 계정을 설정했습니다.

A

(UNIX) serevu 데몬 또는 "PAM(플러그형 인증 모듈)"이 잘못된 암호를 사용한 사용자의 로그인 시도를 감사했습니다.

참고: Windows 에서는 로그아웃 이벤트를 기록하지 않습니다.

보안 데이터베이스 관리 이벤트 필터 구문

보안 데이터베이스 관리 이벤트에 속하는 감사 레코드는 다음과 같은 필터 형식을 갖습니다.

```
ADMIN;ClassName;ObjectName;UserName;EffectiveUserName;TerminalName;Command;Comman
dResult
```

ADMIN

규칙에서 관리자가 수행한 이벤트에 의해 생성된 감사 레코드를 필터링하도록 지정합니다.

ClassName

관리자가 명령을 실행하는 클래스를 정의합니다.

ObjectName

관리자의 명령이 업데이트한 개체를 정의합니다.

UserName

명령을 실행한 사용자의 이름을 정의합니다.

EffectiveUserName

(UNIX) 규칙이 적용되는 유효 사용자의 이름을 정의합니다.

(Windows) 규칙이 적용되는 기본 사용자의 이름을 정의합니다.

TerminalName

이벤트가 발생한 터미널을 정의합니다.

Command

관리자가 실행한 selang 명령을 정의합니다.

CommandResult

권한 부여 또는 명령 결과를 정의합니다.

값: S(명령 성공), F(명령 실패), D(명령 거부), *

사용자에 대한 추적 메시지 이벤트 필터 구문

사용자에 대한 추적 메시지 이벤트에 속하는 감사 레코드는 다음과 같은 필터 형식을 갖습니다.

```
TRACE;TracedClassName;TracedObjectName;RealUserName;EffectiveUserName;ACUserName;
AuthorizationResult;TraceMessage
```

TRACE

규칙에서 사용자 추적 레코드를 필터링하도록 지정합니다.

TracedClassName

사용자가 액세스를 시도한 개체 클래스의 이름을 정의합니다.

참고: 클래스 이름은 대문자로 입력해야 합니다.

TracedObjectName

사용자가 액세스를 시도한 개체의 이름을 정의합니다.

RealUserName

(UNIX) 추적 레코드를 생성한 실제 사용자의 이름을 정의합니다.

(Windows) 추적 레코드를 생성한 기본 사용자의 이름을 정의합니다.

EffectiveUserName

(UNIX) 추적 레코드를 생성한 유효 사용자의 이름을 정의합니다.

(Windows) 추적 레코드를 생성한 기본 사용자의 이름을 정의합니다. 이 매개 변수는 RealUserName 매개 변수와 같습니다. 이 매개 변수에는 *를 사용합니다.

ACUserName

CA Access Control 에서 이벤트 권한 부여를 위해 선택한 사용자 이름을 정의합니다.

AuthorizationResult

권한 부여 결과를 정의합니다.

값: P(허용됨), D(거부됨), *

TraceMessage

생성된 추적 메시지를 정의합니다.

예: 네트워크 연결 이벤트 필터링

- 이 예에서는 들어오는 성공한 텔넷 연결에 의해 생성된 ca.com 호스트의 모든 감사 레코드를 필터링합니다.

  ```
  HOST;telnet;ca.com;*;*;P
  ```

- 이 예에서는 들어오고 나가는 거부된 로그인 TCP 연결에 의해 생성된 ca.com 호스트의 모든 감사 레코드를 필터링합니다.

  ```
  TCP;login;ca.com;*;*;D
  ```

- 이 예에서는 나가는 텔넷 연결에 의해 생성된 ca.com 호스트의 모든 감사 레코드를 필터링합니다.

  ```
  TCP;telnet;ca.com;*;W;*
  ```

예: 로그인 또는 로그아웃 이벤트 필터링

- 이 예에서는 루트가 허용된 계정에 로그인할 때 생성된 모든 감사 레코드를 필터링합니다.

  ```
  LOGIN;root;*;*;*;P
  ```

- 이 예에서는 루트가 시스템의 CRON 프로그램으로 인해 성공적으로 로그인할 때 생성된 모든 감사 레코드를 필터링합니다.

  ```
  LOGIN;root;*;*;SBIN_CRON;P
  ```

- 이 예에서는 _CRONJOB_ 프로세스가 루트 사용자를 로그아웃할 때 생성된 모든 감사 레코드를 필터링합니다.

  ```
  LOGIN;root;*;_CRONJOB_;*;O
  ```

예: 보안 데이터베이스 관리 이벤트 필터링

이 예에서는 admin01 에 의한 성공한 FILE 관리 명령에 의해 생성된 모든 감사 레코드를 필터링합니다.

```
ADMIN;FILE'*;admin01;*;*;*;S
```

예: 사용자에 대한 추적 메시지 이벤트 필터링

이 예에서는 유효 사용자가 루트이고, 루트가 FILE 클래스의 개체에 액세스할 때 생성된 모든 사용자 추적 레코드를 필터링합니다.

```
TRACE;FILE;*;*;root;*;*
```

예: 감사 필터 정책

- 이 예에서는 감사 필터링 정책이 어떻게 표시되는지 보여 줍니다.

  ```
  env config
  er config audit.cfg line+("FILE;*;*;R;P")
  ```

- 이 정책은 audit.cfg 파일에 다음 줄을 씁니다.

  ```
  FILE;*;*;R;P
  ```

- 이 줄에서는 접근자가 파일 리소스를 읽기 위한 액세스를 허용한 시도를 기록하는 레코드를 감사합니다.

auditrouteflt.cfg 파일 - 감사 레코드 라우팅 필터링

auditrouteflt.cfg 파일은 CA Access Control 에서 배포 서버로 보내지 않아야 하는 레코드를 정의하여 감사 레코드 라우팅을 필터링합니다. 각 줄은 감사 정보를 필터링하는 하나의 규칙을 나타냅니다. 파일 경로 이름은 ReportAgent 섹션의 audit_filter 구성 설정에 의해 정의됩니다.

참고: 필터링된 감사 이벤트는 로컬 감사 파일에 기록되지만 CA Access Control 은 이 이벤트를 배포 서버의 메시지 큐로 보내지 않습니다. 로컬 감사 파일에서 감사 메시지를 필터링하려면 logmgr 섹션의 AuditFiltersFile 구성 설정(기본적으로 audit.cfg)에 의해 정의된 파일의 필터 규칙을 수정합니다.

auditrouteflt.cfg 파일을 사용하여 각각 다른 구문으로 다음 감사 이벤트 유형의 레코드를 필터링할 수 있습니다.

- 리소스 액세스
- 네트워크 연결
- 로그인 및 로그아웃 이벤트
- 보안 데이터베이스 관리
- 사용자에 대한 추적 메시지

참고: 각 구문 유형에서 열에 표시된 *는 "모든 값"을 나타냅니다.

리소스 액세스 이벤트 필터 구문

리소스 액세스 이벤트에 속하는 감사 레코드는 다음과 같은 필터 형식을 갖습니다.

```
ClassName;ObjectName;UserName;ProgramPath;Access;AuthorizationResult
```

ClassName

액세스한 개체가 속하는 클래스의 이름을 정의합니다.

참고: 클래스 이름은 대문자로 입력해야 합니다.

ObjectName

액세스한 개체의 이름을 정의합니다.

UserName

접근자의 이름을 정의합니다.

ProgramPath

개체를 액세스하는 데 사용된 프로그램의 이름을 정의합니다.

Access

개체에 대해 요청된 액세스를 정의합니다.

값:

*****

모든 유형의 액세스를 나타내는 와일드카드입니다.

Chdir

디렉터리 변경 - 접근자가 개체를 다른 디렉터리로 이동하도록 요청했습니다.

Chmod

모드 변경 - 접근자가 개체 모드를 변경하도록 요청했습니다.

Chgrp

(UNIX) 그룹 변경 - 접근자가 개체가 속하는 그룹을 변경하도록 요청했습니다.

Chown

소유자 변경 - 접근자가 개체의 소유자를 변경하도록 요청했습니다.

Cre

만들기 - 접근자가 새 개체를 만들도록 요청했습니다.

Del

삭제 - 접근자가 개체를 삭제하도록 요청했습니다.

Join

사용자를 그룹에 가입 - 접근자가 새 사용자를 그룹에 추가하도록 요청했습니다.

Kill

종료 - 접근자가 프로세스를 종료하도록 요청했습니다.

R

읽기 - 접근자가 개체에 대한 읽기 권한을 요청했습니다.

참고: (UNIX) STAT_intercept 가 1 로 설정된 경우에는 이 매개변수에 stat 차단이 포함됩니다.

Rename

파일 이름 변경 - 접근자가 개체의 파일 이름을 변경하도록 요청했습니다.

Sec

ACL 변경 - 접근자가 개체의 ACL 을 편집하도록 요청했습니다.

Utime

(UNIX) 시간 변경 - 접근자가 개체의 수정 시간을 변경하도록 요청했습니다.

W

쓰기 - 접근자가 개체에 대한 쓰기 권한을 요청했습니다.

X

실행 - 접근자가 개체를 실행하도록 요청했습니다.

참고: 일부 클래스에 유효하지 않은 값도 있습니다. 예를 들어 FILE 클래스의 개체에는 kill 동작을 사용할 수 없으므로 kill 은 FILE 클래스에 유효하지 않은 값입니다. 규칙을 작성할 때 클래스에 유효하지 않은 값을 입력하면 CA Access Control 에서 파일을 읽을 때 해당 규칙을 무시합니다.

AuthorizationResult

권한 부여 결과를 정의합니다.

값: P(허용됨), D(거부됨), *

네트워크 연결 이벤트 필터 구문

네트워크 연결 이벤트에 속하는 감사 레코드는 다음과 같은 필터 형식을 갖습니다.

```
{HOST|TCP};ObjectName;HostName;ProgramPath;Access;AuthorizationResult
```

HOST

규칙에서 HOST 클래스의 개체에 의해 생성된 레코드, 즉 들어오는 TCP 연결을 필터링하도록 지정합니다.

TCP

규칙에서 TCP 클래스의 개체에 의해 생성된 레코드, 즉 서비스 이벤트와의 연결을 필터링하도록 지정합니다.

ObjectName

액세스한 개체의 이름을 정의합니다. ObjectName 은 서비스 이름이나 포트 이름일 수 있습니다.

HostName

호스트의 이름을 정의합니다. HostName 은 HOST 클래스의 객체여야 합니다.

ProgramPath

로그인 프로그램 유형을 정의합니다.

(Windows) 나가는 연결에 대해 이 매개 변수는 연결 설정을 시도하는 프로세스의 프로그램 경로를 정의합니다.

참고: 이 매개 변수는 들어오는 연결 이벤트에는 의미가 없습니다. 들어오는 연결 이벤트에 의해 생성된 감사 레코드를 필터링하려면 이 매개 변수에 대해 *를 사용합니다.

Access

시도된 연결 유형을 정의합니다.

값:

- (HOST) *
- (TCP) R(들어오는 연결), W(나가는 연결), *

AuthorizationResult

권한 부여 결과를 정의합니다.

값: P(허용됨), D(거부됨), *

로그인 및 로그아웃 이벤트 필터 구문

로그인 또는 로그아웃 이벤트에 속하는 감사 레코드는 다음과 같은 필터 형식을 갖습니다.

```
LOGIN;UserName;UserId;TerminalName;LoginProgram;AuthorizationResultOrLoginType
```

LOGIN

규칙에서 로그인 및 로그아웃 이벤트에 의해 생성된 감사 레코드를 필터링하도록 지정합니다.

UserName

접근자의 이름을 정의합니다.

UserId

접근자의 기본 사용자 ID 를 정의합니다.

TerminalName

이벤트가 발생한 터미널을 정의합니다.

LoginProgram

로그인 또는 로그아웃을 시도한 프로그램의 이름을 정의합니다.

AuthorizationResultorLoginType

권한 부여 결과를 정의합니다.

값:

*****

모든 유형의 권한 부여 결과를 나타내는 와일드카드입니다.

D

로그인 시도가 거부되었습니다.

P

로그인 시도가 허용되었습니다.

O

(UNIX) 접근자가 로그아웃했습니다.

-I

(UNIX) serevu 데몬이 접근자의 계정을 해지했습니다.

E

(UNIX) serevu 데몬이 접근자의 계정을 설정했습니다.

A

(UNIX) serevu 데몬 또는 "PAM(플러그형 인증 모듈)"이 잘못된 암호를 사용한 사용자의 로그인 시도를 감사했습니다.

참고: Windows 에서는 로그아웃 이벤트를 기록하지 않습니다.

보안 데이터베이스 관리 이벤트 필터 구문

보안 데이터베이스 관리 이벤트에 속하는 감사 레코드는 다음과 같은 필터 형식을 갖습니다.

```
ADMIN;ClassName;ObjectName;UserName;EffectiveUserName;TerminalName;Command;Comman
dResult
```

ADMIN

규칙에서 관리자가 수행한 이벤트에 의해 생성된 감사 레코드를 필터링하도록 지정합니다.

ClassName

관리자가 명령을 실행하는 클래스를 정의합니다.

ObjectName

관리자의 명령이 업데이트한 개체를 정의합니다.

UserName

명령을 실행한 사용자의 이름을 정의합니다.

EffectiveUserName

(UNIX) 규칙이 적용되는 유효 사용자의 이름을 정의합니다.

(Windows) 규칙이 적용되는 기본 사용자의 이름을 정의합니다.

TerminalName

이벤트가 발생한 터미널을 정의합니다.

Command

관리자가 실행한 selang 명령을 정의합니다.

CommandResult

권한 부여 또는 명령 결과를 정의합니다.

값: S(명령 성공), F(명령 실패), D(명령 거부), *

사용자에 대한 추적 메시지 이벤트 필터 구문

사용자에 대한 추적 메시지 이벤트에 속하는 감사 레코드는 다음과 같은 필터 형식을 갖습니다.

```
TRACE;TracedClassName;TracedObjectName;RealUserName;EffectiveUserName;ACUserName;
AuthorizationResult;TraceMessage
```

TRACE

규칙에서 사용자 추적 레코드를 필터링하도록 지정합니다.

TracedClassName

사용자가 액세스를 시도한 개체 클래스의 이름을 정의합니다.

참고: 클래스 이름은 대문자로 입력해야 합니다.

TracedObjectName

사용자가 액세스를 시도한 개체의 이름을 정의합니다.

RealUserName

(UNIX) 추적 레코드를 생성한 실제 사용자의 이름을 정의합니다.

(Windows) 추적 레코드를 생성한 기본 사용자의 이름을 정의합니다.

EffectiveUserName

(UNIX) 추적 레코드를 생성한 유효 사용자의 이름을 정의합니다.

(Windows) 추적 레코드를 생성한 기본 사용자의 이름을 정의합니다. 이 매개 변수는 RealUserName 매개 변수와 같습니다. 이 매개 변수에는 *를 사용합니다.

ACUserName

CA Access Control 에서 이벤트 권한 부여를 위해 선택한 사용자 이름을 정의합니다.

AuthorizationResult

권한 부여 결과를 정의합니다.

값: P(허용됨), D(거부됨), *

TraceMessage

생성된 추적 메시지를 정의합니다.

예: 네트워크 연결 이벤트 필터링

- 이 예에서는 들어오는 성공한 텔넷 연결에 의해 생성된 ca.com 호스트의 모든 감사 레코드를 필터링합니다.

  ```
  HOST;telnet;ca.com;*;*;P
  ```

- 이 예에서는 들어오고 나가는 거부된 로그인 TCP 연결에 의해 생성된 ca.com 호스트의 모든 감사 레코드를 필터링합니다.

  ```
  TCP;login;ca.com;*;*;D
  ```

- 이 예에서는 나가는 텔넷 연결에 의해 생성된 ca.com 호스트의 모든 감사 레코드를 필터링합니다.

  ```
  TCP;telnet;ca.com;*;W;*
  ```

예: 로그인 또는 로그아웃 이벤트 필터링

- 이 예에서는 루트가 허용된 계정에 로그인할 때 생성된 모든 감사 레코드를 필터링합니다.

  ```
  LOGIN;root;*;*;*;P
  ```

- 이 예에서는 루트가 시스템의 CRON 프로그램으로 인해 성공적으로 로그인할 때 생성된 모든 감사 레코드를 필터링합니다.

  ```
  LOGIN;root;*;*;SBIN_CRON;P
  ```

- 이 예에서는 _CRONJOB_ 프로세스가 루트 사용자를 로그아웃할 때 생성된 모든 감사 레코드를 필터링합니다.

  ```
  LOGIN;root;*;_CRONJOB_;*;O
  ```

예: 보안 데이터베이스 관리 이벤트 필터링

이 예에서는 admin01 에 의한 성공한 FILE 관리 명령에 의해 생성된 모든 감사 레코드를 필터링합니다.

```
ADMIN;FILE'*;admin01;*;*;*;S
```

예: 사용자에 대한 추적 메시지 이벤트 필터링

이 예에서는 유효 사용자가 루트이고, 루트가 FILE 클래스의 개체에 액세스할 때 생성된 모든 사용자 추적 레코드를 필터링합니다.

```
TRACE;FILE;*;*;root;*;*
```

예: 감사 필터 정책

이 예에서는 감사 필터링 정책이 어떻게 표시되는지 보여 줍니다.

```
env config
er config auditrouteflt.cfg line+("FILE;*;*;R;P")
```

이 정책은 auditrouteflt.cfg 파일에 다음 줄을 씁니다.

```
FILE;*;*;R;P
```

이 줄에서는 접근자가 파일 리소스를 읽기 위한 액세스를 허용한 시도를 기록하는 레코드를 감사합니다.

감사 로그 라우트 구성 파일 selogrd.cfg

UNIX 에 해당

다음은 구성 파일의 형식과 자세한 설명입니다.

```
section-name-1
routing-method destination
[{include|exclude} match-field(match-pattern) ...]
...
.
section-name-2
routing-method destination
[{include|exclude} match-field(match-pattern) ...]
...
.
...
```

감사 레코드 지정

구성 파일은 다양한 대상으로 라우트할 것이 아닌, 라우트할 감사 레코드 목록입니다. 감사 레코드를 지정하기 위해 하나 이상의 특수 필드 내용을 설명합니다. 표준 UNIX 패턴 일치(* 및 ?) 와일드카드를 사용할 수 있습니다.

예를 들어, 사용자 이름이 dbms 글자로 시작하는 사용자를 처리하는 레코드를 지정하려면 다음 명령을 입력합니다.

```
User(dbms*)
```

이 예제는 dbms1, dbms_mgr 등과 같은 이름을 가진 사용자를 일치시킵니다.

동일한 사용자를 지정하지만 각 사용자의 로그인 시도를 처리하는 레코드만 지정하려면 다음 명령을 입력합니다.

```
User(dbms*) Class(LOGIN)
```

참고: 한 행이 둘 이상의 필드와 관련해서 레코드를 지정할 경우 모든 해당 필드와 일치하는 레코드만 지정합니다.

레코드를 지정하는 동일한 행의 시작에서 레코드의 포함 또는 제외 여부를 지정합니다. 예를 들어, 라우팅에 이러한 레코드를 포함하려면 다음 명령을 입력합니다.

```
include User(dbms*) Class(LOGIN).
```

이러한 유형의 행 형식은전체적으로 다음과 같습니다.

```
[{include|exclude} match-field(match-pattern) ... .]
```

여기서 "..."은 첫 번째 match-field(match-pattern) 쌍 뒤에 다른 쌍이 올 수 있음을 의미합니다.

다음 중 원하는 항목을 match-field(match-pattern)로 사용할 수 있습니다.

Access(access-type)

필요한 액세스 유형에 사용됩니다. 여기서 access-type 은 다음 중 하나입니다.

ACL, Chdir, Chgrp, Chmod, Chown, Connect, Control, Create, Erase, Exec, Kill, Modify, Owngrp, Password, Read, Rename, Replace, Update, Utimes 및 Write

Class(LOGIN)

로그인 레코드에 사용됩니다.

Class(LOGOUT)

로그아웃 레코드에 사용됩니다.

Class(PWCHANGE)

암호 관리에 사용됩니다.

Class(HOST)

TCP/IP 레코드에 사용됩니다.

Class(UPDATE CA Access Control-class)

데이터베이스 관리에 대해 사용됩니다. CA Access Control 클래스는 임의의 접근자 또는 리소스 클래스(예: USER, GROUP, FILE, HOSTNP...)이거나 일치시킬 클래스 이름의 패턴입니다. 따라서 모든 데이터베이스 관리를 위해 UPDATE *를 지정할 수 있습니다.

Class(CA Access Control-class)

보호된 리소스에 대한 액세스에 사용됩니다. 예를 들어, Class(FILE)는 파일 액세스 시도를 보고하는 레코드를 나타냅니다.

*를 사용하여 Class(CA Access Control-class)와 Class(UPDATE CA Access Control-class)를 Class(*CA Access Control-class)로 결합할 수 있습니다. 예를 들어, Class(*FILE)를 지정하는 것은 Class(FILE)와 Class(UPDATE FILE)를 모두 지정하는 것과 같습니다. 이것은 파일 액세스 시도와 FILE 클래스의 레코드 업데이트 시도를 모두 나타냅니다.

Code(return-code)

발생한 이벤트를 나타내는 CA Access Control 반환 코드에 대해 사용됩니다. return-code 는 다음 값을 가질 수 있습니다. 이 단원의 "예제 1"을 참조하십시오.

A-잘못된 암호를 반복해서 입력했기 때문에 로그인 시도가 실패했습니다.

D-접근자의 권한이 부족해서 CA Access Control 이 리소스에 대한 액세스를 거부했거나, 로그인을 허용하지 않았거나, 데이터베이스의 업데이트를 허용하지 않았습니다.

E-Serevu 가 비활성화된 사용자 계정을 활성화했습니다.

F-데이터베이스 업데이트 시도가 실패했습니다.

I-Serevu 가 사용자 계정을 비활성화했습니다.

M-실행된 명령이 데몬을 시작했거나 종료했습니다.

O-사용자가 로그아웃했습니다.

P-CA Access Control 이 리소스에 대한 액세스를 허용했거나 로그인을 허용했습니다.

S-데이터베이스가 업데이트되었습니다.

T-사용자의 모든 작업을 추적 중이므로 감사 레코드가 작성되었습니다.

U-트러스트된 프로그램(setuid 또는 setgid)이 변경되었으므로 더 이상 트러스트되지 않습니다.

W-리소스에 대한 액세스가 리소스에 대한 액세스 규칙을 위반했습니다. 그러나 리소스에 경고 모드가 설정되어 있으므로 CA Access Control 이 액세스를 허용했습니다.

Host(host-name)

TCP/IP 연결에 관련된 호스트에 사용됩니다.

Object(resource-name)

사용자가 액세스를 시도 중인 리소스에 사용됩니다.

Reason(reason-number)

감사 레코드가 작성되는 이유에 사용됩니다.

Service(service-name)

텔넷 또는 ftp 와 같은 원격 호스트에서 요청된 서비스 이름에 사용됩니다.

Source Host(hostname)

통합된 감사에 레코드를 제공하는 호스트 이름에 사용됩니다.

Stage(stage-number)

액세스가 승인 또는 거부된 단계에 대해 사용됩니다. 참조 안내서의 단계 코드 목록을 참조하십시오.

Terminal(terminal-name)

액세스 또는 관리를 시도 중인 터미널에 사용됩니다.

Uid(uid-number)

액세스 또는 관리를 시도 중인 사용자의 uid 에 사용됩니다.

User(username)

액세스 또는 관리를 시도 중인 사용자에 사용됩니다. 여기서 username 은 이름 또는 패턴입니다.

참고: 일부 변수는 패턴으로서 지정되기 쉽지만, 모든 변수(단계 번호 등도 포함)에 대해 패턴을 사용할 수 있습니다.

추가 행으로 미세 조정

사양을 미세 조정하기 위해 기준을 동시에 다르게 지정하여 필터링할 수 있습니다. 다른 행 다음에 include/exclude 행만 하나 추가하십시오. 예:

```
include User(dbms*) Class(*LOGIN*).
exclude Terminal(console_*).
```

예제에서는 이름이 dbms 로 시작하는 사용자의 모든 로그인 시도와, 이름이 console_로 시작하지 않으며 터미널에 있는 사용자의 모든 로그인 시도를 지정합니다.

대상 지정

include 및 exclude 행의 시퀀스 위에 다른 행을 추가하여 포함 중인 감사 레코드의 라우팅 대상을 지정합니다. 예:

```
mail weekwatch
include User(dbms*) Class(*LOGIN*).
exclude Terminal(console_*).
```

이 예제는 이름이 dbms 로 시작하고 console_로 시작하지 않는 이름을 가진 터미널을 사용하는 사용자의 모든 로그인 시도에 대한 리포트가 전자 메일 주소 weekwatch 로 전송되도록 지정합니다.

이러한 유형의 행은 다음과 같이 로그 라우트 구성 파일의 형식으로 나타납니다.

```
routing-method destination
```

다음 방법 중 하나를 사용할 수 있습니다.

mail address

감사 레코드를 전자 메일로 전송하는 데 사용됩니다. address 는 대상 주소입니다. 여기서 address 는 대상 주소입니다. user@host 형식이 아닌 경우, 로컬 사용자 목록 및 NIS 메일 별칭 맵에 대해 검사됩니다.

참고: address 가 사용자 이름 및 해당 사용자의 계정이 감사되는 서로게이트 요청인 경우 감사 레코드는 끊임없이 누적됩니다.

screen username

selogrd 가 감사 레코드를 전달할 때 해당 사용자가 현재 호스트에 로그인된 경우, 지정된 사용자의 화면에 감사 레코드를 표시합니다. 사용자가 로그인되지 않은 경우 표시는 연기되지 않고 취소됩니다.

cons hostname

지정된 호스트에서 secmon 유틸리티의 Security Administrator GUI 에 감사 레코드를 보냅니다. 해당 호스트를 사용할 수 없는 경우 디스플레이는 연기되지 않고 종료됩니다.

file textfilename

지정된 ASCII 파일에 감사 레코드를 기록합니다. 여기서 textfilename 은 절대 경로 이름이어야 하고 selogrd 는 파일에 대한 액세스 권한을 가지고 있어야 합니다.

host hostname

지정된 호스트의 감사 로그 수집기로 감사 레코드를 보냅니다. 해당 호스트를 사용할 수 없는 경우 selogrd 는 나중에 다시 시도합니다.

notify mail 또는 notify default

감사 레코드 자체가 지정하는 주소에 감사 레코드를 전송합니다.

notify screen

감사 레코드 자체가 지정하는 사용자 화면에 감사 레코드를 표시합니다. 사용자가 로그온되지 않은 경우 디스플레이는 연기되지 않고 취소됩니다.

syslog 우선 순위

지정된 로그 우선 순위로 syslog 에 감사 레코드를 보내려면

- **LOG_EMERG** - 시스템을 사용할 수 없습니다.
- **LOG_ALERT** - 작업을 즉시 수행해야 합니다.
- **LOG_CRIT** - 중요 조건입니다.
- **LOG_ERR** - 오류 조건입니다.
- **LOG_WARNING** - 경고 조건입니다.
- **LOG_NOTICE** - 정상이지만 중요한 조건입니다.
- **LOG_INFO** - 정보용입니다.
- **LOG_DEBUG** - 디버그 수준 메시지입니다.

uni hostname

지정된 호스트의 Unicenter TNG 이벤트 관리자로 감사 레코드를 보냅니다. 또한 ACInstallDir/lib 디렉터리에 있는 uni.so 공유 라이브러리를 로드하도록 selogrd 를 설정해야 합니다. 지정된 호스트에 설치된 Unicenter TNG 를 찾고 사용자가 이 작업을 수행하도록 선택한 경우 설치 시 이 작업을 수행합니다.

행의 올바른 순서

include 및 exclude 행을 올바르게 구분하여 적합한 순서로 배열하는 것이 중요합니다.

- 단일 복합 필터로 처리할 행(또는 단일 행)의 각 순서 앞에 제목 행을 입력하고 점 하나로 구성된 종료 행으로 끝내야 합니다. 예는 다음과 같습니다.

  dbms login from non-console

  ```
  mail weekwatch
  ```

  include User(dbms*) Class(*LOGIN*).

  ```
  exclude Terminal(console_*).
  .
  ```

제목 행과 종료 행을 포함한 전체 시퀀스를 파일의 한 섹션이라고 합니다.

- include 및 exclude 행이 모두 동일한 섹션의 동일한 감사 레코드와 일치할 경우 마지막 일치는 다른 모든 항목을 무시합니다.
- 특정 감사 레코드와 일치하는 행이 없으면 섹션이 첫 번째 행이 해당 레코드의 결정 행이 됩니다. 첫 번째 행이 include 행이면 일치하는 행이 없을 경우 해당 레코드가 제외됩니다. 첫 번째 행이 exclude 행이면 일치하는 행이 없을 경우 해당 레코드가 라우팅에 포함됩니다.
- 섹션에 include 및 exclude 행이 없는 경우 라우팅할 모든 감사 레코드를 포함합니다.

섹션 공존 방법

섹션의 행은 함께 작동하여 레코드의 전송 여부와 상관 없이 단일 결정을 내리는 반면, 구성 파일의 다른 섹션은 완전히 독립적으로 작동합니다. 한 섹션에서 감사 레코드를 전송했는지 여부는 다른 섹션에 의한 동일한 감사 레코드의 전송 여부에 영향을 미치지 않습니다.

둘 이상의 대상에 감사 레코드의 동일한 선택을 전송할 수 있으며, 동일한 대상은 둘 이상의 감사 레코드 선택을 수신할 수 있습니다.

구성 파일에서 모든 섹션의 include 및 exclude 행은 합해서 64 행을 넘지 않아야 합니다.

설명 포함

설명 행을 구성 파일에 추가하려면 세미콜론으로 행을 시작하십시오.

예제 1

다음은 설명이 뒤에 나오는 예제 구성 파일입니다.

```
; Product : CA Access Control
; Module  : selogrd
; Purpose : route table for audit log routing daemon
;
;-----------------------------------------------------
 Rule#1
 mail jones@admhost
 include     Class(*LOGIN*) Code(D).
 .
 Rule#2
 mail smith
 include     Class(*SURROGATE*) Object(USER.root*).
 .
 Rule#3
 host venus
 exclude     Class(UPDATE SU*).
 .
 Rule#4
 host venus
 include     Class(*PROGRAM*) Object(/usr/bin/ps).
 .
```

처음 5 개 행은 설명 행입니다.

다음 네 개의 행은 첫 번째 섹션을 구성하고 Rule#1 로 명명됩니다. 이러한 행은 로그인 요청이 거부될 때마다 로그 레코드를 jones@admhost 주소로 전송하도록 selogrd 에게 지시합니다(코드 D 는 거부를 보고함).

```
Rule#1
mail jones@admhost
include     Class(*LOGIN*) Code(D).
.
```

다음 섹션 이름은 Rule#2 입니다. 이 섹션은 사용자가 su 명령을 사용하여 루트 계정을 입력할 때마다 로그 레코드를 smith 주소로 전송하도록 selogrd 에게 지시합니다(SURROGATE 클래스의 개체는 su 명령의 대상임).

```
Rule#2
mail smith
include     Class(*SURROGATE*) Object(USER.root*).
.
```

다음 섹션 이름은 Rule#3 입니다. 이 섹션은 클래스 이름이 SU 글자로 시작하지 않으면(일치 클래스는 SURROGATE 및 SUDO 임) 사용자가 데이터베이스를 관리할 때마다 venus 호스트의 수집기로 로그 레코드를 보내도록 selogrd 에게 지시합니다.

```
Rule#3
host venus
exclude     Class(UPDATE SU*).
```

마지막 섹션 이름은 Rule#4 입니다. 이 섹션은 사용자가 ps 명령을 사용할 때마다 venus 호스트의 수집기로 로그 레코드를 보내도록 selogrd 에게 지시합니다.

```
(Code 1 8pt) Rule#4
host venus
include     Class(*PROGRAM*) Object(/usr/bin/ps).
.
```

예제 2

다음 구성 파일은 모든 감사 레코드를 loghost 스테이션의 수집기로 전송합니다.

```
 ; Product : CA Access Control
 ; Module  : selogrd
 ; Purpose : route table for audit log routing daemon
 ;
 ;-----------------------------------------------------
  Rule#1
  host loghost
  .
```

반환 코드

구성 파일에 있는 각 유형의 레코드를 한 개 이상의 CA Access Control 반환 코드와 연결할 수 있습니다. 전체 반환 코드 목록을 보려면 이 섹션의 "감사 레코드 지정"에서 code(return-code)의 설명을 참조하십시오. 다음 표는 레코드 유형 및 관련 반환 코드를 설명합니다.

레코드 유형	클래스 또는 이벤트	연결된 반환 코드
로그인	LOGIN	D, P, W
	LOGINDISABLE	I
	LOGINENABLE	E
로그아웃	LOGOUT	O
TCP/IP	HOST	D, P
리소스 클래스	클래스 이름	D, P, W
Watchdog	PROGRAM	U
	SECFILE	U
암호 관리	PWCHANGE	D, F, S
다운	SHUTDOWN	D, S
Start	START	S
CA Access Control 데이터베이스 관리	UPDATE	D, F, S

uxauth.ini 파일

UNIX 에 해당

uxauth.ini 구성 파일에는 UNAB 의 기능을 제어하는 여러 토큰이 수록되어 있습니다. UNAB 구성 파일은 다음과 같이 UNAB 기능을 제어하는 여러 토큰의 섹션으로 구분되어 있습니다.

섹션	설명
ad	설치 중 입력한 매개 변수와 함께 Active Directory 토큰을 포함하고 있습니다.
agent	여러 UNAB 매개 변수를 제어하는 토큰을 포함하고 있습니다.
global	UNAB 일반 설정을 제어하는 토큰을 포함하고 있습니다.

섹션	설명
logmgr	UNAB 로깅 유틸리티가 사용하는 토큰을 포함하고 있습니다.
map	Active Directory 특성 이름을 지정하는 토큰을 포함하고 있습니다.
message	UNAB 가 메시지 파일을 정의하기 위해 사용하는 토큰을 포함하고 있습니다.
migrate	마이그레이션 프로세스 중 UNAB 가 사용하는 토큰을 포함하고 있습니다.
passwd	마이그레이션 프로세스 중 UNAB 가 암호 변경을 제어하기 위해 사용하는 토큰을 포함하고 있습니다.
register	UNAB 등록 기능을 제어하는 토큰을 포함하고 있습니다.

ad

[ad] 섹션은 설치 중 입력한 매개 변수와 함께 Active Directory 토큰을 포함하고 있습니다.

ad_domain

Active Directory 도메인의 이름을 정의합니다.

ad_gc_port

Active Directory 글로벌 카탈로그 서비스가 사용하는 포트를 지정합니다.

기본값: 3268

base_dn

Active Directory 서버의 base_dn 을 정의합니다.

computer_container

Active Directory 에서 UNIX 호스트의 위치를 정의합니다.

기본값: cn=Computers

group_container

Active Directory 에서 UNIX 그룹의 위치를 정의합니다.

기본값: cn=Users

ldap_port

Active Directory LDAP 서비스가 사용하는 포트를 정의합니다.

기본값: 389

user_container

Active Directory 에서 UNIX 사용자의 위치를 정의합니다.

기본값: cn=Users

agent

[agent] 섹션에는 여러 UNAB 매개 변수를 제어하는 토큰이 수록되어 있습니다.

ac_registration_interval

UNAB 를 CA Access Control 끝점에 등록하는 간격(초)을 정의합니다. 값 0 은 등록이 없음을 지정합니다.

기본값: 60

참고: UNAB 는 CA Access Control 이 UNIX 호스트에 설치된 경우에만 끝점에 등록을 시도합니다.

ad_group_deny_gid_list

로그인할 수 없는 Active Directory 그룹의 GID 를 쉼표로 구분하여 정의합니다.

예: ad_group_deny_gid_list = 11,14

ad_group_minimal_gid

로그인할 수 있는 Active Directory 그룹의 최소 GID 를 정의합니다.

ad_user_deny_uid_list

로그인할 수 없는 Active Directory 사용자의 UID 를 쉼표로 구분하여 정의합니다.

예: ad_user_deny_uid_list = 12,37

ad_user_minimal_uid

로그인할 수 있는 Active Directory 사용자의 최소 UID 를 정의합니다.

debug_backup

디버그 메시지 파일을 백업할지 여부를 지정합니다.

제한: yes, no

기본값: yes

debug_backup_file

백업 디버그 메시지 파일의 이름을 정의합니다. 파일에 대한 전체 경로 이름을 사용하지 않으면 UNAB 는 파일을 InstallDir/log/debug/ 디렉터리에 만듭니다.

기본값: agent_debug.back

debug_file

UNAB 가 디버그 메시지를 기록하는 파일 이름을 정의합니다. 파일에 대한 전체 경로 이름을 사용하지 않으면 UNAB 는 이 파일을 InstallDir/log/debug/ 디렉터리에 만듭니다.

기본값: agent_debug

debug_level

디버그 파일에서 디버그 메시지의 수준을 지정합니다.

제한: disabled, high, medium, low

- disabled: 파일에 디버그 메시지를 기록하지 않음
- high: 파일에 HIGH 수준의 디버그 메시지를 기록
- medium: 파일에 HIGH 및 MEDIUM 수준의 디버그 메시지를 기록
- low: 파일에 HIGH, MEDIUM, LOW 수준의 디버그 메시지를 기록

기본값: disabled

debug_zones

하위 모듈(영역)에 대한 디버그 메시지를 로깅할지 여부를 지정합니다. 여러 영역에 대한 디버그 메시지를 기록하려면 영역 값의 합계를 지정하십시오.

제한: -1, 1, 2, 4, 8, 16, 또는 양수 값의 합계

- 영역 -1: 모든 영역에 대한 디버그 메시지를 기록
- 영역 1: "일반" 영역에 대한 디버그 메시지를 기록
- 영역 2: "전체" 통신 영역에 대한 디버그 메시지를 기록
- 영역 4: "스케줄러" 영역에 대한 디버그 메시지를 기록
- 영역 8: PAM 통신 영역에 대한 디버그 메시지를 기록
- 영역 16: NSS 통신 영역에 대한 디버그 메시지를 기록

예: 영역 "일반" 및 "스케줄러"에 대한 디버그 메시지를 로깅하려면 debug_zones 의 값을 5 로 지정하십시오.

기본값: -1

default_login_access

사용자 및 그룹에 대한 액세스를 정의하는 규칙이 없는 경우의 기본 액세스 모드를 지정합니다.

제한: 0 - 액세스 없음, 1 - 액세스 허용

기본값: 0

groups_allow_file

로컬 groups.allow 파일의 위치를 정의합니다.

기본값: /opt/CA/uxauth/etc/groups.allow

groups_deny_file

로컬 groups.deny 파일의 위치를 정의합니다.

기본값: /opt/CA/uxauth/etc/groups.deny

heartbeat_send_interval

CA Access Control 배포 호스트에 하트비트를 보내는 간격(초)을 정의합니다.

기본값: 3600

ldap_connection_lifetime

사용이 없는 LDAP 연결을 유지할 최대 기간(초)을 정의합니다. 0 으로 설정하면 UNAB 는 LDAP 작업 후 즉시 연결을 끊습니다.

기본값: 60

LIC98Dir

CA 라이선스 라이브러리의 위치를 정의합니다.

기본값: /opt/CA/SharedComponents/ca_lic

login_name_type

매핑된 사용자가 자신의 UNIX 사용자 이름 또는 엔터프라이즈 사용자 이름을 사용하여 로그인할 수 있는지 여부를 지정합니다.

제한: 1 - UNIX 로그인 이름, 2 - 엔터프라이즈 로그인 이름

기본값: 1

message_read_interval

CA Access Control 정책 큐를 읽는 간격(초)을 지정합니다.

기본값: 60

message_read_timeout

CA Access Control 정책 큐를 읽는 시간 간격(밀리초)을 정의합니다.

기본값: 1

nss_cache_update_grp_mode

그룹 캐시 업데이트 방법을 지정합니다.

제한: 0 - 업데이트 안 함, 1 - 증분 업데이트, 2 - 전체 업데이트

기본값: 1

nss_cache_update_interval

사용자 및 그룹 캐시를 업데이트하는 간격(초)을 정의합니다.

기본값: 60

nss_cache_update_startup

에이전트가 시작되는 동안 NSS 사용자와 그룹 캐시를 업데이트하는 방법을 지정합니다.

제한: 0 - 업데이트 안 함, 1 - 증분 업데이트, 2 - 전체 업데이트

기본값: 1

nss_cache_update_usr_mode

사용자 캐시 업데이트 방법을 지정합니다.

제한: 0 - 업데이트 안 함, 1 - 증분 업데이트, 2 - 전체 업데이트

기본값: 1

ntp_server

NTP 서버의 이름 또는 IP 주소를 정의합니다.

기본값: 없음

offline_logon

Active Directory 를 사용할 수 없을 때 사용자가 계속 UNIX 호스트에 액세스할 수 있는지 여부를 지정합니다.

제한: no - 오프라인 연결 비활성화, yes - 오프라인 연결 활성화

기본값: yes

offline_logon_max_fail

오프라인 로그온 시도의 최대 실패 횟수를 정의합니다.

기본값: 5

offline_logon_period

마지막 성공한 온라인 인증 이후 오프라인 인증이 허용되는 최대 기간(일)을 정의합니다.

기본값: 30

report_user_mapped_name

사용자가 매핑된 모드에 있을 때 보고서와 감사 파일에 표시되는 사용자 이름을 지정합니다.

제한: no - UNIX 사용자 이름과 함께 보고서가 표시됨, yes - 사용자 매핑된 이름과 함께 보고서가 표시됨

기본값: no

tgt_renew_interval

TGT(Tickect Granting Ticket) 갱신 간격(초)을 정의합니다.

기본값: 14400

tgt_renewable_lifetime

TGT(Tickect Granting Ticket) 갱신 최대 간격(일)을 정의합니다.

기본값: 30

time_sync_interval

시계 동기화 간격(초)을 정의합니다.

기본값: 300

use_local_policy

로컬 로그인 정책(.allow 및 .deny 파일)을 사용할지 여부를 지정합니다.

제한: no - 엔터프라이즈 로그인 정책만 사용, yes - 엔터프라이즈 로그인 정책을 사용한 다음 로컬 로그인 정책을 사용

기본값: no

use_time_sync

시계 동기화 옵션을 지정합니다.

제한: no - 수동 동기화, yes - 자동 동기화

기본값: no

use_wingrp

UNAB 가 Active Directory 그룹을 CA Access Control 사용을 위해 데이터베이스에 저장할지 여부를 지정합니다.

제한: no, yes

기본값: yes

users_allow_file

로컬 users.allow 파일의 위치를 정의합니다.

기본값: /opt/CA/uxauth/etc/users.allow

users_deny_file

로컬 users.deny 파일의 위치를 정의합니다.

기본값: /opt/CA/uxauth/etc/users.deny

wingrp_update_interval

UNAB Active Directory 그룹 데이터베이스를 업데이트하는 간격(초)을 정의합니다.

기본값: 60

windgrp_update_mode

UNAB Active Directory 그룹 데이터베이스를 업데이트하는 방법을 지정합니다.

제한: 0 - 업데이트 안 함, 1 - 증분 업데이트, 2 - 전체 업데이트

기본값: 1

wingrp_update_startup

UNAB 가 시작되는 동안 Active Directory 그룹 데이터베이스를 업데이트하는 방법을 지정합니다.

제한: 0 - 업데이트 안 함, 1 - 증분 업데이트, 2 - 전체 업데이트

기본값: 1

working_threads

에이전트에서 실행 중인 스레드의 수를 정의합니다.

기본값: 64

global

[global] 섹션에는 UNAB 일반 설정을 제어하는 매개 변수가 포함되어 있습니다.

활성화

호스트 활성화 수준을 지정합니다.

제한: 0, 1, 2

- 0 - 등록되지 않음
- 1 - 등록됨(로컬 사용자 저장소에 정의된 사용자만 로그인 허용)
- 2 - 활성화됨(로컬 사용자 저장소에 정의되었거나 .allow 파일 또는 UNAB 로그인 정책에 정의된 사용자의 로그인 허용)

기본값: 0

CASHCOMP

CA 공유 구성 요소 설치 디렉터리의 경로를 지정합니다.

기본값: /opt/CA/SharedComponents

integration_mode

UNAB 설치 방법을 지정합니다.
제한: 1 - 부분 통합, 2 - 전체 통합

참고: UNIX 사용자 저장소를 유지하려는 경우 부분 통합 (1)을 지정하십시오.

기본값: 2

product_path

UNAB 설치 디렉터리의 이름을 정의합니다.

기본값: /opt/CA/uxauth

logmgr

[logmgr] 섹션은 UNAB 로깅 유틸리티가 사용하는 토큰을 수록하고 있습니다.

audit_back

백업 파일의 전체 경로와 이름을 정의합니다.

기본값: /opt/CA/uxauth/log/uxauth.audit.bak

audit_group

감사 로그 파일을 읽도록 허용된 그룹의 이름을 지정합니다.

제한: none, group_name

- None - 그룹의 액세스를 허용하지 않고 root 만 감사 로그 파일을 읽을 수 있습니다.
- group_name - 감사 로그 파일을 읽을 수 있는 그룹의 이름을 정의합니다.

참고: UNAB 가 감사 로그 파일을 만든 이후에 이 토큰 값을 변경하는 경우 selang 명령을 사용하여 로그를 읽을 수 있도록 파일 그룹 소유권 및 그룹 권한을 설정해야 합니다. 이 토큰 값을 설정한 이후에 만든 모든 파일은 지정하는 권한을 갖게 됩니다.

기본값: none

audit_log

감사 로그 파일의 전체 경로 이름을 정의합니다.

기본값: /opt/CA/uxauth/log/uxauth.audit

audit_max_files

지정된 각 백업 모드에 대해 저장할 감사 로그 파일의 최대 개수를 정의합니다. 백업 감사 로그 파일의 최대 개수에 도달하면 UNAB 는 새 백업 파일을 작성할 때 가장 오래된 백업 파일을 삭제합니다. 값 0 은 UNAB 가 누적 백업 파일을 유지하도록 지정합니다.

기본값: 0

audit_size

감사 로그 파일의 최대 크기(KB)를 정의합니다.

참고: 이 토큰에 지정할 수 있는 최소값은 50 KB 입니다.

기본값: 1024

BackUp_Date

감사 로그 파일을 백업하는 간격을 지정합니다.

제한: none, yes, daily, weekly, monthly

- none - 감사 로그 파일이 백업되지 않습니다.
- yes - 감사 파일이 audit_size 토큰에 지정된 크기에 도달하면 감사 로그 파일 백업이 수행됩니다.
- daily - 매일 감사 로그 파일 백업이 수행됩니다.
- weekly - 매주 감사 로그 파일 백업이 수행됩니다.
- monthly - 매월 감사 로그 파일 백업이 수행됩니다.

참고: 이 토큰에 daily, weekly, monthly를 지정하면 UNAB는 시작할 때 타임스탬프를 작성하고, 현재 날짜가 지정된 간격을 지나면 감사 로그 파일을 백업하고, 타임스탬프를 백업 파일의 이름에 추가합니다. 하지만 현재 날짜가 지정된 간격을 지나기 전에 감사 로그 파일의 크기가 audit_size 토큰에 지정된 크기에 도달하면 UNAB는 감사 로그 파일을 백업하지만 백업 파일의 이름에 타임스탬프를 추가하지는 않습니다. 이 토큰에 yes를 지정한 경우 타임스탬프는 백업 파일의 이름에 항상 추가됩니다.

기본값: none

error_back

오류 로그 파일 백업 복사본의 전체 경로 이름을 정의합니다.

기본값: /opt/CA/uxauth/log/uxauth.error.bak

error_group

오류 로그 파일을 읽도록 허용된 그룹의 이름을 지정합니다.

제한: none, group_name

- None - 그룹의 액세스를 허용하지 않고 root만 오류 로그 파일을 읽을 수 있습니다.
- group_name - 오류 로그 파일을 읽을 수 있는 그룹의 이름을 정의합니다.

참고: UNAB가 오류 로그 파일을 만든 이후에 이 토큰 값을 변경하는 경우 selang 명령을 사용하여 로그를 읽을 수 있도록 파일 그룹 소유권 및 그룹 권한을 설정해야 합니다. 이 토큰 값을 설정한 이후에 만든 모든 파일은 지정하는 권한을 갖게 됩니다.

기본값: none

error_log

오류 로그 파일의 전체 경로 이름을 정의합니다.

기본값: /opt/CA/uxauth/log/uxauth.error

error_size

오류 로그 파일의 최대 크기(KB)를 지정합니다.

참고: 이 토큰에 지정할 수 있는 최소값은 50 KB 입니다.

기본값: 50

map

[map] 섹션에는 UNAB 가 Active Directory 특성 이름을 지정하기 위해 사용하는 토큰이 수록되어 있습니다.

group_gid_attr_name

UNIX 그룹 ID 를 나타내는 Active Directory 특성 이름을 지정합니다.

기본값: gidNimber

group_member_attr_name

그룹 구성원을 나열하는 Active Directory 특성 이름을 지정합니다.

제한: member, memberUid

기본값: member

group_nest_level

UNAB 가 Active Directory 에서 사용자의 구성원 자격을 찾기 위해 사용하는 중첩된 그룹 쿼리의 수준을 지정합니다.

기본값: 1

user_gecos_attr_name

UNIX 사용자 gecos 를 나타내는 Active Directory 특성 이름을 지정합니다.

기본값: gecos

user_gid_attr_name

UNIX 그룹 ID 를 나타내는 Active Directory 특성 이름을 지정합니다.

기본값: gidNumber

user_homedir_attr_name

UNIX 사용자 홈 디렉터리를 나타내는 Active Directory 특성 이름을 지정합니다.

기본값: unixHomeDirectory

user_loginshell_attr_name

UNIX 사용자 로그인 셸을 나타내는 Active Directory 특성 이름을 지정합니다.

기본값: loginShell

user_uid_attr_name

UNIX 사용자 ID 를 나타내는 Active Directory 특성 이름을 지정합니다.

기본값: uidNumber

message

[message] 섹션은 메시지 파일을 정의하기 위해 UNAB 가 사용하는 토큰을 수록하고 있습니다.

filename

메시지 파일의 전체 경로 이름을 정의합니다.

기본값: /opt/CA/uxauth/data/uxauth.msg

migrate

[migrate] 섹션은 마이그레이션 프로세스 중 UNAB 가 사용하는 토큰을 수록하고 있습니다.

conflicts_file

마이그레이션 충돌 파일의 전체 경로 이름을 정의합니다.

기본값: /opt/CA/uxauth/log/migrate.conflicts

create_ad_groups

Active Directory 에 동일한 그룹이 없는 경우 마이그레이션 중에 새 Active Directory 그룹을 만들지 여부를 지정합니다.

제한: yes, no

기본값: yes

disable_mapped_user

부분 마이그레이션된(매핑된) 사용자의 UNIX 암호를 비활성화할지 여부를 지정합니다.

제한: yes, no

기본값: yes

ignore_gecos_conflict

마이그레이션 프로세스 중에 UNAB 가 발견하는 gecos 사용자 특성 관련 충돌을 무시할지 여부를 정의합니다.

제한: yes, no

기본값: yes

is_gid_migration_a_prerequisite

사용자를 마이그레이션하려면 사용자의 주 그룹을 반드시 마이그레이션해야 하는지 여부를 지정합니다.

제한: yes, no

기본값: no

journal

마이그레이션 저널 파일의 전체 경로 이름을 정의합니다.

기본값: /opt/CA/uxauth/log/migrate.journal

minimal_gid

마이그레이션 프로세스 중에 Active Directory 로 마이그레이션될 최소 그룹 ID 를 정의합니다. 더 작은 GID 의 그룹은 마이그레이션되지 않습니다.

기본값: 101

minimal_uid

마이그레이션 프로세스 중에 Active Directory 로 마이그레이션될 최소 사용자 ID 를 정의합니다. 더 작은 UID 의 사용자는 마이그레이션되지 않습니다.

기본값: 101

remove_migrated_user

마이그레이션 후 로컬 사용자 계정을 제거할지 여부를 지정합니다.

제한: yes, no

기본값: yes

try_to_map_on_conflict

전체 마이그레이션 프로세스가 실패하는 경우 충돌하는 계정을 매핑할지 여부를 지정합니다.

제한: yes, no

기본값: yes

passwd

[passwd] 섹션은 마이그레이션 프로세스 중 UNAB 가 암호 변경을 제어하기 위해 사용하는 토큰을 포함하고 있습니다.

YpGrpCmd

NIS 그룹 맵을 생성하는 명령을 정의합니다.

기본값: make group

YpMakeDir

NIS 맵을 만들 때 사용된 makefile 디렉터리를 정의합니다.

기본값: /var/vp

YpPassCmd

NIS 암호 맵을 생성하는 명령을 정의합니다.

기본값: make passwd

YpServerGroup

NIS 서버에 있는 그룹 파일의 전체 경로 이름을 정의합니다.

기본값: /etc/group

YpServerPasswd

NIS 서버에 있는 암호 파일의 전체 경로 이름을 정의합니다.

기본값: /etc/passwd

YpServerSecure

운영 체제의 암호 파일에 대한 전체 경로 이름을 정의합니다.

기본값: /etc/shadow

register

[register] 섹션에는 UNAB 등록 기능을 제어하는 토큰이 수록되어 있습니다.

start_uxauthd

설치 프로세스의 마지막에 uxactivate 유틸리티를 실행할지 여부를 지정합니다.

제한: yes, no

기본값: yes

verbose

설치 중 사용할 세부 정보 표시 수준을 정의합니다.

기본값: 0

UNAB 충돌 파일

UNAB 충돌 파일은 Active Directory 로 사용자 및 그룹의 마이그레이션을 시도한 이후에 생성됩니다. 이 파일에는 마이그레이션 프로세스 중 UNAB 에서 발견된 충돌 정보가 수록되어 있습니다. 이 파일을 검토하여 이 파일에서 보고된 충돌을 해결하십시오.

이 파일에는 다음과 같은 필드가 있습니다.

유형,이름,상태,다음에 매핑됨:,충돌,UID,홈 디렉터리,GID,소속 그룹,구성원,GECOS

유형

마이그레이션할 엔터티의 유형을 표시합니다.

제한: user, group

이름

엔터티의 이름을 표시합니다.

상태

엔터티 마이그레이션 상태를 표시합니다.

제한: Keeplocal, Migrate, Map

다음에 매핑됨:

로컬 계정이 매핑된 Active Directory 계정 이름을 표시합니다.

충돌

마이그레이션 중 발견된 충돌을 표시합니다.

UID

사용자 ID 를 표시합니다.

홈 디렉터리

사용자 홈 디렉터리를 표시합니다.

GID

그룹 ID 를 표시합니다.

소속 그룹

사용자가 속한 그룹을 표시합니다.

구성원

그룹의 구성원인 사용자의 목록을 표시합니다.

GECOS

GECOS 정보를 표시합니다.

제 4 장: 레지스트리 항목

이 장은 아래의 주제를 포함하고 있습니다.

CA Access Control 레지스트리 (페이지 401)
추가적인 레지스트리 키 (페이지 472)

CA Access Control 레지스트리

CA Access Control 은 다음 레지스트리 키 아래에 레지스트리 항목을 작성합니다. 이를 CA Access Control 끝점 관리 원격 구성의 ACROOT 라고 합니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl

주 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

CurrentVersion

제품의 현재 버전 및 빌드를 정의합니다.

Encryption Package

대칭 암호화 구현을 위해 사용되는 DLL 의 전체 경로 이름을 정의합니다.

기본값: ACInstallDir\bin\defenc.dll

AccessControl

CA Access Control 이 사용하는 일반 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\AccessControl

AccessControl 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

AccessControl Services

CA Access Control 서비스 이름 목록 및 실행 파일을 정의합니다.

기본값: "SeOSAgent;SeOS Agent", "SeSudo;SeOS TD", "seoswd;SeOS Watchdog"

admin_default_check

원격 터미널 리소스에 대한 defaccess 속성이 all 로 설정되어 있거나 _default 터미널 리소스에 대한 액세스가 허용되는 경우에도 CA Access Control 서버에 대한 로그인 액세스를 CA Access Control 이 거부할지 여부를 지정합니다.

이전 버전과의 호환을 위해 유지됩니다.

기본값: 0(액세스가 거부되지 않음)

AdminInst

내부 사용자 전용.

auth_login

관리 목적을 위해 사용자를 인증하는 방법을 지정합니다.

유효한 값:

native - 기본 운영 체제 사용자의 경우 OS 에 대해 사용자 암호를 확인합니다.

eTrus - 기본 운영 체제에 없는 사용자의 경우 CA Access Control 데이터베이스에 대해 사용자 암호를 확인합니다.

기본값: native

auth_module_names

기본 인증 외부에서 인증할 수 있는 언어 클라이언트 모듈 목록입니다. 클라이언트 모듈 이름은 인증 전에 클라이언트에 의해 Ica API 호출 내부에 설정됩니다. 이 레지스트리 값을 변경하면 비기본 모드에서 인증하는 다른 클라이언트에 영향을 미칠 수 있습니다.

기본값: 없음

CPF_TARGETS

CPF 서비스와 통신하는 대상 메인프레임 CPF 시스템(원격 CPF 대상 노드) 목록입니다.

기본값: ACF2 TOP RACF

GenerateMemDump

CA Access Control 이 CA Access Control 서비스의 코드 예외를 처리할 때 메모리 덤프를 작성할지 여부를 지정합니다(1). CA Access Control 은 ACInstallDir\bin\serviceProcessName.PID.dmp(예: SeOSAgent.5704.dmp)에 메모리 덤프를 작성합니다.

참고: 메모리 덤프는 커널 모드용이 아니라 사용자 모드 전용입니다.

기본값: 1

eACPipePrefix

새 파이프 서버와 파이프 클라이언트가 사용할 파이프 이름의 일부에 대한 값입니다. 시스템에 CA Access Control 의 이전 클라이언트가 설치된 경우, 이러한 클라이언트가 작동하려면 이 값이 반드시 필요합니다. 또는 이 값을 더 안전한 파이프 이름으로 변경하십시오.

기본값: SEOS

eACPipeTranslator

더 이상 사용되지 않습니다.

Emulate

더 이상 사용되지 않습니다.

full_year

secons -tv, seaudit 및 dbmgr 유틸리티를 사용할 때 연도를 2 자리 숫자(값= no)로 표시할 것인지 4 자리 숫자(값=yes)로 표시할지를 지정합니다.

기본값: yes

parent_pmd

워크스테이션이 pmdb@host 형식으로 구독하는 PMDB 입니다. 이것은 로컬 데이터베이스를 업데이트할 수 있는 유일한 정책 모델입니다.

값을 설정하지 않으면 워크스테이션이 PMDB 에서 오는 업데이트를 허용하지 않습니다. 항목을 _NO_MASTER_로 설정하면 모든 PMDB 가 이 워크스테이션을 업데이트할 수 있습니다.

기본값 없음.

passwd_pmd

정책 모델에서 암호를 바꿀 대상이며, 형식은 pmdb@host 입니다.

parent_pmd 및 passwd_pmd 레지스트리 값은 같은 값을 가질 수 있습니다. parent_pmd 및 passwd_pmd 레지스트리 값이 같지 않으면 passwd_pmd 데이터베이스가 해당 업데이트를 parent_pmd 데이터베이스로 보내 배포합니다. parent_pmd 데이터베이스는 passwd_pmd 데이터베이스의 구독자여야 합니다.

이 값을 설정하지 않으면 parent_pmd 레지스트리 키의 값을 상속합니다.

기본값 없음.

ReverseIpLookup

해당 터미널로부터 사용자 로그인을 허용할지를 결정하기 위해 클라이언트 IP 주소를 확인하는 방법을 제어합니다.

유효한 값:

yes-열려 있는 클라이언트 소켓의 IP 주소를 조회하고 그에 따라 로그인을 허용합니다.

no-클라이언트에서 수신한 그대로 호스트 이름을 사용하며 어떤 호스트 이름도 확인하지 않습니다. TERMINAL 클래스를 비활성화해도 동일한 효과를 얻을 수 있습니다.

기본값: yes

secondary_pmd

암호 교체의 보조 대상으로 사용하는 정책 모델 데이터베이스입니다.

기본값 없음.

SeOSPath

CA Access Control 이 설치된 디렉터리입니다.

SplashEnable

대화형(GINA) 로그인 프로세스 중에 보호 메시지를 활성화하거나 비활성화하는 토글 키입니다. 이 메시지는 CA Access Control 이 컴퓨터를 보호한다고 사용자에게 알려줍니다. 값이 1 이면 메시지가 활성화되었음을 나타내고, 값이 0 이면 메시지가 비활성화되었음을 나타냅니다.

기본값: 1

TNG_Environment

Unicenter 통합을 활성화하거나 비활성화하는 토글 키입니다.

기본값: 0

TrustedServices

트러스트된 프로그램 목록입니다.

기본값 없음.

UseFsiDrv

드라이버 로드를 활성화하거나 비활성화하는 토글 키입니다.

기본값: 1

에이전트

CA Access Control 이 사용하는 에이전트 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Agent

에이전트 키 항목(및 모든 하위 키)은 내부에서만 사용됩니다.

응용 프로그램

CA Access Control 이 사용하는 응용 프로그램 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Applications

Applications 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

OperationMode

제어된 응용 프로그램 모드의 활성화 여부를 지정합니다(1).

이 값은 1 로 설정해야 합니다.

기본값: 1

<Application_Name>

CA Access Control 이 사용하는 특정 응용 프로그램 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Applications\Application_Name

각 Applications\Application_Name 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

ApplicationName

제어된 프로세스의 이름을 정의합니다.

전체 경로 이름은 device:\path\name.exe 형식으로 지정해야 합니다.

기본값: No

Arguments

응용 프로그램을 시작할 때 CA Access Control 이 사용하는 인수를 정의합니다.

기본값: ""(인수 없음)

Desktop

워크스테이션 및 세션 이름을 정의합니다.

기본값: "WinSta0\\default"(주)

OperationMode

응용 프로그램의 활성화 여부를 지정합니다(1).

기본값: 1

RestartApplication

응용 프로그램이 닫히거나 종료된 후 응용 프로그램을 다시 시작할지 여부를 지정합니다(1).

기본값: 1

StartAplication

Watchdog 이 깨어날 때 CA Access Control 이 응용 프로그램을 시작할지 여부를 지정합니다(1).

기본값: 1

WorkingDirectory

응용 프로그램이 시작되는 작업 디렉터리를 정의합니다.

기본값: ACInstallDir\bin

클라이언트

CA Access Control 이 사용하는 클라이언트 응용 프로그램 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Client
```

Client 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

ConnectTo

CA Access Control 클라이언트 관리 응용 프로그램(예: selang)이 기본적으로 연결되는 호스트 이름을 정의합니다.

기본값: localhost

Standalone

CA Access Control 이 사용하는 독립형 클라이언트 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Client\Standalone

Client\Standalone 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

full_login_check

CA Access Control 서버가 추가적인 사용자 속성(grace 및 max_login)을 확인하고 독립형 응용 프로그램의 연결 요청 중에 로그인을 수행할 수 있게 해주는 토글 키입니다.

암호가 곧 만료될 경우 이 값은 원격 암호를 변경하는 데 도움이 됩니다.

값을 1 로 설정하면 확인 기능이 활성화됩니다.

기본값: 0

Common

CA Access Control 은 다음 키 아래에서 일반 구성 요소에서 사용되는 설정을 유지 관리합니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Common

Common 키는 어떠한 레지스트리 항목도 포함하지 않습니다. 여기에는 일반 구성 요소에 대한 레지스트리 하위 키가 수록되어 있습니다.

communication

CA Access Control 이 사용하는 메시지 큐 서버 통신 설정은 다음 키에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\common\communication

통신 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

certificate

SSL 연결을 위한 인증서 파일을 정의합니다.

제한: 인증서 데이터를 포함하는 파일의 전체 경로 이름

Distribution_Server

배포 서버 URL 을 정의합니다. 목록에서 쉼표로 구분하여 여러 배포 서버를 정의할 수 있습니다.

예: tcp://ds.comp.com:7222, tcp://ds_dr.comp.com:7222

기본값: 없음

endpoint_to_server_queue

끝점이 CA Access Control 엔터프라이즈 관리로 정보를 보내기 위해 사용하는 메시지 큐의 이름을 정의합니다.

기본값: ac_endpoint_to_server

server_to_endpoint_broadcast_queue

CA Access Control 엔터프라이즈 관리가 모든 끝점으로 메시지를 브로드캐시트하기 위해 사용하는 메시지 큐의 이름을 정의합니다.

기본값: ac_server_to_endpoint_broadcast

server_to_endpoint_queue

CA Access Control 엔터프라이즈 관리가 끝점으로 메시지를 보내기 위해 사용하는 메시지 큐의 이름을 정의합니다.

기본값: ac_server_to_endpoint

ssl_custom

호스트 이름 확인자 함수 사용 여부를 지정합니다.

제한: 0 - 호스트 이름 확인자 함수 사용 안 함, 1 - 호스트 이름 확인자 함수 사용

기본값: 0

ssl_hostname

SSL 호스트 이름을 정의합니다.

기본값: none

ssl_identity

보고서 에이전트의 ID 를 정의합니다.

제한: 인증서 데이터를 포함하는 파일의 전체 경로 이름

기본값: none

ssl_issuer

SSL 연결에 대한 발급자 인증서를 정의합니다.

제한: 인증서 데이터를 포함하는 파일의 전체 경로 이름

기본값: none

ssl_key

보고서 에이전트 개인 키를 정의합니다.

제한: 개인 키를 포함하는 파일의 전체 경로 이름.

기본값: none

ssl_noverifyhost

호스트 인증서 확인을 사용할지 여부를 지정합니다.

제한: 0 - 호스트 인증서 확인 사용 안 함, 1 - 호스트 인증서 확인 사용

기본값: 0

ssl_noverifyhostname

호스트 이름 확인을 사용할지 여부를 지정합니다.

제한: 0 - 호스트 이름 확인 사용 안 함, 1 - 호스트 이름 확인 사용

기본값: 0

ssl_trace

SSL 추적을 사용할지 여부를 지정합니다.

제한: 0 - SSL 추적 사용 안 함, 1 - SSL 추적 사용

기본값: 0

ssl_trusted

SSL 연결에 대한 트러스트된 인증서를 정의합니다.

제한: 인증서 데이터를 포함하는 파일의 전체 경로 이름

기본값: none

crypto

CA Access Control 이 사용하는 암호화 모듈 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\crypto
```

crypto 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

ca_certificate

CA(인증 기관) 데이터베이스에 대한 전체 경로 이름을 정의합니다.

기본값: ACInstallDir\data\crypto\def_root.pem

communication_mode

SSL(Secure Socket Layer) 프로토콜의 활성화 여부를 지정합니다.

이것을 ssl_only 로 설정하면 SSL V2, SSL V3 및 TLS 연결만 활성화됩니다. 즉, 이 컴퓨터는 SSL 을 지원하지 않는 컴퓨터와 통신할 수 없으며, 따라서 SSL 을 지원하지 않는 Access Control 이전 버전을 실행하는 컴퓨터와 통신할 수 없습니다.

fips_only 토큰이 1 로 설정되어 있으면 실제 통신 모드는 FIPS 모드(즉, TLS)에서 ssl_only 로 설정되며 communication_mode 토큰은 무시됩니다.

유효한 값:

- all_modes
- ssl_only
- non_ssl

기본값: non_ssl

fips_only

이 토큰은 CA Access Control 이 FIPS 전용 모드에서 작동할지 여부를 제어합니다. 이 모드에서는 FIPS 이외의 모든 기능이 비활성화됩니다.

유효한 값:

1 CA Access Control 이 FIPS 전용 모드에서 작동합니다.

0 CA Access Control 이 비 FIPS 모드에서 작동합니다.

기본값: 0

private_key

제목 개인 키에 대한 전체 경로 이름을 정의합니다.

기본값: ACInstallDir\data\crypto\sub.key

ssl_port

CA Access Control 클라이언트와 서비스 간의 SSL 통신용 포트를 정의합니다.

기본값: 5249

subject_certificate

제목 인증서에 대한 전체 경로 이름을 정의합니다.

기본값: ACInstallDir\data\crypto\sub.pem

Dependency

CA Access Control 이 사용하는 종속성 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Dependency
```

CA Access Control 구성 요소 모듈이 다른 제품의 포함된 구성 요소로 설치되면 이 레지스트리 키의 모든 하위 키는 CA Access Control 에 종속적인 제품의 이름이 됩니다. CA Access Control 을 업그레이드하거나 제거하면, CA Access Control 은 이 레지스트리를 확인하고 프로세스를 계속할 수 있는지 중단해야 하는지를 결정합니다.

devcalc

CA Access Control 이 사용하는 위반 계산기 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\devcalc
```

devcalc 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

dms_cmd_retry_interval

각 DMS 알림 명령 재시도 사이의 시간(초)을 정의합니다.

기본값: 60

init_ac_db

더 이상 사용되지 않습니다.

max_dms_cmd_retry

포기하기 전까지 DMS 에 업데이트 알림을 보내는 정책 위반 계산기의 최대 재시도 횟수를 정의합니다.

기본값: 3

max_lines_request

get devcalc selang 명령이 정책 위반 데이터 파일로부터 한 번에 반환하는 최대 줄 수를 정의합니다. 그 후에 추가 행을 검색하려면 다음 명령을 사용해야 합니다.

```
get devcalc params("offset=X")
```

X

이전 get devcalc 출력에 의해 반환되는 줄 오프셋을 정의합니다.

기본값: 50

Exits

CA Access Control 이 사용하는 에이전트 종료 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Exits

Exits 레지스트리 키에는 레지스트리 항목이 포함되어 있지 않습니다. 여기에는 모든 에이전트 종료에 대한 레지스트리 하위 키가 포함되어 있습니다.

AuthenticatePassword

CA Access Control 이 사용하는 암호 인증 에이전트 종료 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Exits\AuthenticatePassword

Exits\AuthenticatePassword 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

사용

암호 규칙 실행 에이전트 종료를 활성화하거나 비활성화하는 토글 키입니다. 값이 0 이면 종료를 비활성화하고, 다른 값은 종료를 활성화합니다

기본값: 0

EnforcePasswordControl

CA Access Control 클라이언트를 사용하여 암호 규칙을 적용하기 위한 조건입니다.

0 - 암호 규칙 적용 없음

1 - 일반 사용자가 자신의 암호를 변경할 때 암호 규칙 적용이 활성화됨

2 - 관리자 또는 암호 관리자가 타인 또는 자신의 암호를 변경할 때 암호 규칙 적용이 활성화됨

3 - 값 1 과 2 과 모두 해당됨

기본값: 1

Engine

CA Access Control 이 사용하는 CA Access Control 엔진(seos) 에이전트 종료 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Exits\Engine
```

Exits\Engine 레지스트리 키는 기본적으로 레지스트리 항목을 포함하고 있지 않습니다.

Remote Grace Info

CA Access Control 이 사용하는 원격 유예 정보 에이전트 종료 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Exits\Remote Grace Info
```

Exits\Remote Grace Info 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

DefaultWarningDays

segrace\SegraceW 유틸리티의 사용자에게 암호 만료 경고를 표시하는 기본 날짜 수를 정의합니다. 이것은 유틸리티 중 하나가 적용되고 있으며 사용자의 암호가 만료될 날짜 수가 이 레지스트리 값에 지정된 날짜 수보다 적게 남았을 경우 사용자에게 경고 메시지를 표시한다는 의미입니다.

기본값: 7

Remote Shutdown

CA Access Control 이 사용하는 원격 종료 에이전트 종료 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Exits\Remote Shutdown

Exits\Remote Shutdown 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

Path

원격 종료 DLL 의 전체 경로 이름입니다.

기본값: \bin\remshut.dll

Prefix

원격 종료 DLL 에서 사용되는 정의된 접두사입니다.

기본값: SD

FsiDrv

CA Access Control 이 사용하는 드라이버 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\FsiDrv

FsiDrv 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

AcceptEmptyDomainLogin

더 이상 사용되지 않습니다.

AudiRefreshPeriod

동일한 소스에서 발생하는 두 개의 연속 감사 이벤트 사이의 최소 시간(초)을 정의합니다. CA Access Control 은 이 기간 내에 동일한 소스에서 발생하는 연속 이벤트에 대해 감사 메시지를 기록하지 않습니다.

기본값: 0(모든 감사 이벤트를 기록함)

BatchOplockStatus

전체 파일의 배치 OpLocks(조건적 잠금)를 비활성화할지 여부를 지정합니다. 비활성화된 경우(값이 0) 드라이버는 파일 액세스에 대한 모든 감사 정보를 수집하지만 이 경우 성능이 저하됩니다. 0 이 아닌 값은 배치 OpLocks 가 정기적으로 작동하도록(활성화되도록) 유지하지만, 관련된 파일에 액세스하려는 시도가 포함되지 않을 수 있는 불완전한 감사 정보를 제공할 수 있습니다.

참고: 새 설정을 사용하려면 드라이버를 다시 로드해야 합니다. 이때 CA Access Control 을 중지(secons -s)한 후 드라이버를 언로드(net stop seosdrv)하십시오.

기본값: 1(활성화됨)

BypassDriversCount

무시 목록에 추가할 드라이버의 수를 정의합니다.

유형: REG_DWORD

기본값: 0

DriverName_drvNumber

무시하려는 드라이버의 이름(예: thisdrv.sys)을 정의합니다.

drvNumber 는 0 에서 BypassDriversCount - 1 까지의 숫자입니다. 무시할 각 드라이버에 대해 하나의 레지스트리 항목을 만들고, 정의한 드라이버의 수가 BypassDriversCount 에 정의되어 있는지 확인해야 합니다.

유형: REG_SZ

제한: 49 자

DynamicSysThreadDetection

시스템 스레드를 생성하는 다른 제품(예: Trend Micro™ PC-cillin Antivirus)에서 생성된 모든 커널 모드 스레드를 CA Access Control 이 추적하도록 지정합니다.

참고: 이 레지스트리 값을 활성화하면 성능이 저하될 수 있습니다. 이 레지스트리 값을 활성화하기 전에 우선 CA 에 문의하는 것이 좋습니다. 도움이 필요하면 기술 지원 부서(http://www.ca.com/worldwide)에 문의하십시오.

유형: REG_DWORD

기본값: 0(비활성)

directory

드라이버의 위치입니다.

기본값: system_drive\Windows_path\system32\drivers

FileCacheDisabled

일반 파일 캐시를 활성화하거나 비활성화하는 토글 키입니다.

기본값: 0

FileCacheRefreshPeriod

동일한 위치로부터 전송되는 두 개의 감사 메시지 간의 최소 시간 간격을 정의한 값(밀리초)입니다.

예를 들어, 변수를 3000 으로 설정할 경우 파일 감사 이벤트의 최소 간격은 3 초가 됩니다.

기본값: 3000

LoopHoleProtectionDisabled

CA Access Control 의 핸들을 닫을 수 있는 Process Monitor(procmon.exe)와 같은 응용 프로그램으로부터 CA Access Control 을 보호하는 루프홀 보호를 비활성화할지 여부를 지정합니다.

값: 0 - 루프홀 보호 활성화, **1** - 루프홀 보호 비활성화.

기본값: 0

참고: 이 키는 32 비트 Windows 환경에 적용됩니다.

MaxAuditRecordLimit

감사 큐 제한을 정의합니다. 큐 길이가 이 제한을 초과하면 CA Access Control 은 감사 이벤트를 생성하는 스레드의 속도를 늦춰 큐에서 새 이벤트를 읽어 로그 파일에 쓰는 속도가 큐에 새 이벤트 항목이 추가되는 속도보다 빠르게 합니다.

참고: CA Access Control 이 읽는 것보다 새 항목이 큐에 추가되는 속도가 빠르면 시스템 메모리가 부족해질 수 있습니다.

기본값: 200

MaxTimeoutLimit

CA Access Control 에서 드라이버 무시를 트리거하는 연속 제한 시간 초과 횟수를 정의합니다. 이 횟수에 도달하면 엔진이 이벤트를 처리할 준비가 되었음을 알릴 때까지 드라이버가 권한 부여 요청을 권한 부여 엔진에 전달하지 않습니다.

이 값을 0 으로 하면 드라이버 무시가 트리거되지 않습니다.

기본값: 5

QueueTimeout

seosd 의 응답을 기다리는 최대 시간(초)입니다.

기본값: 10

QueueTimeoutAnswer

제한 시간 후 드라이버의 응답입니다.

기본값: 0(Deny)

RegistryCacheDisabled

일반 레지스트리 캐시를 활성화하거나 비활성화하는 토글 키입니다.

기본값: 0

RegistryCacheRefreshPeriod

동일한 위치로부터 전송되는 두 개의 감사 메시지 간의 최소 시간 간격을 정의한 값(밀리초)입니다.

예를 들어, 변수를 3000 으로 설정할 경우 레지스트리 감사 이벤트의 최소 간격은 3 초가 됩니다.

기본값: 3000

SilentModeAdmins

유지 관리 모드(SilentModeEnabled =1)에서 컴퓨터를 관리할 수 있는 사용자 이름을 줄로 구분하여 나열하는 목록입니다.

기본값 없음

SilentModeEnabled

유지 관리 모드의 활성화 여부를 결정합니다(1).

기본값: 0(비활성)

SystemBypassRestricted

CA Access Control 가 시스템 프로세스에 대한 액세스 검사를 바이패스할지 여부를 지정합니다. 기본적으로 CA Access Control 은 시스템 프로세스를 트러스트된 것으로 간주하지 않으며 시스템 프로세스에 대한 액세스 검사를 바이패스하지 않습니다.

값: 0 - 액세스 검사 바이패스, **1** - 액세스 검사 바이패스하지 않음

기본값: 1

Instrumentation

CA Access Control 이 사용하는 cainstrm.dll 동작 설정(로드된 모든 플러그인에 적용됨)은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation
```

Instrumentation 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

Active

cainstrm.dll 의 활성화 여부를 지정합니다(1).

값을 0 으로 지정하면 cainstrm.dll 은 로드되지만 cainstrm.dll 이 플러그인을 처리하지는 않습니다.

유형: REG_DWORD

기본값: 1

ApplyOnProcess

기기가 적용되는 프로세스의 목록을 정의합니다.

서비스의 이름 또는 전체 경로 이름을 정의할 수 있습니다. 이름은 대/소문자를 구분하지 않습니다. 예: "services.exe", "\system32\services.exe", "c:\windows\system32\services.exe".

유형: REG_MULTI_SZ

기본적으로 이 토큰은 설정되지 않습니다(기기가 모든 프로세스에 적용됨).

ExcludeProcess

기기를 적용하지 않을 프로세스 목록을 정의합니다.

참고: 이 항목은 ApplyOnProcess 가 설정되지 않은 경우에만 유효합니다.

유형: REG_MULTI_SZ

기본적으로 이 토큰은 설정되지 않습니다.

OperationMode

cainstrm.dll 이 메모리로 플러그인을 로드할지 여부를 지정합니다(1).

유형: REG_DWORD

기본값: 1

RunTimeInstrumentationDisabled

런타임에 CA Access Control 계측 정책을 지정합니다.

유형: REG_DWORD

제한: 0 - 런타임 계층 사용, 1 - 런타임 계측 사용 안 함

기본값: 1

RunTimeInstrumentationIncludeList

런타임 계측을 적용할 프로세스의 목록의 정의합니다.

유형: REG_MULTI_SZ

기본값: empty

TraceDbgEnable

cainstrm 모듈의 상태 플래그를 추적할지 여부, 즉 DbgView 또는 커널 디버거 추적을 사용할지 여부를 지정합니다.

유형: RED_DWORD

제한: 0 - false, 1 - true

기본값: 0

TraceFileIsCyclic

추적 파일의 유형을 지정합니다.

유형: REG_DWORD

제한: 0 - 추적 파일이 순환 아님, 1 - 추적 파일이 순환

기본값: 0

TraceFileSizeLimit

추적 파일의 최대 크기(바이트)를 정의합니다. 값 0 은 추적 파일에 최대 크기 제한이 없음을 의미합니다.

유형: REG_DWORD

기본값: 0

TraceFilteringMask

각 플러그인에 대한 필터링 마스크를 정의합니다. 이 레지스트리 값의 지원되는 값은 레지스트리 값을 정의하는 소프트웨어 구성 요소의 상태에 따라 변경됩니다. 두 값은 미리 정의되어 있습니다. 0 - 모든 정보가 필터링됩니다(정보 표시 안 함), 0x0ffffffff - 정보가 필터링되지 않습니다(모든 정보 표시).

유형: REG_DWORD

기본값: 0

참고: 이 레지스트리 값을 변경하기 전에 우선 CA 에 문의하는 것이 좋습니다.

TraceFolderPath

추적 파일의 전체 경로 이름을 정의합니다.

유형: REG_SZ

기본값: 0

TraceOutputMask

추적 출력 채널(디버그, 스트림, 파일, ETW)에 대한 필터링 마스크를 정의합니다. 추적이 파일, DbgView 디버거 채널, WinDbg 디버거 채널로 출력되도록 지정할 수 있습니다. 값이 0 이면 출력을 비활성화합니다.

유형: REG_DWORD

기본값: 0

참고: 이 레지스트리 값을 변경하기 전에 우선 CA 에 문의하는 것이 좋습니다.

UnloadIfNoPlugins

현재 프로세스에 할당된 플러그인이 없을 때 cainstrm.dll 이 자동으로 언로드될지 여부를 지정합니다(1).

값을 0 으로 지정하면 cainstrm.dll 은 로드되지만 cainstrm.dll 이 플러그인을 처리하지는 않습니다.

유형: REG_DWORD

기본값: 1

PluginManagement

CA Access Control 이 사용하는 동적 플러그인 로드 및 언로드 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\
Instrumentation\PluginManagement
```

Instrumentation\PluginManagement 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

Active

플러그인 동적 로딩의 활성화 여부를 지정합니다(1).

유형: REG_DWORD

기본값: 1

Altitude

체인에서 동적 관리 스텁의 순서를 정의합니다.

유형: REG-DWORD

기본값: 0x0fffffff(예약된 값)

ApplyOnDLL

읽기 전용 값입니다.

기본값: Kernel32.dll

ApplyOnProcess

동적 로딩이 적용되는 프로세스의 목록을 정의합니다.

서비스의 이름 또는 전체 경로 이름을 정의할 수 있습니다. 이름은 대/소문자를 구분하지 않습니다. 예: "services.exe", "\system32\services.exe", "c:\windows\system32\services.exe".

유형: REG_MULTI_SZ

기본적으로 이 토큰은 설정되지 않습니다(동적 로딩이 모든 플러그인에 적용됨).

ExcludeProcess

동적 로딩을 적용하지 않을 프로세스 목록을 정의합니다.

참고: 이 항목은 ApplyOnProcess 가 설정되지 않은 경우에만 유효합니다.

유형: REG_MULTI_SZ

기본적으로 이 토큰은 설정되지 않습니다.

OperationMode

수정하지 마십시오.

유형: REG_DWORD

기본값: 1

LoadLibraryA

내부 사용자 전용.

LoadLibraryExA

내부 사용자 전용.

LoadLibraryExW

내부 사용자 전용.

OperationMode

내부 사용자 전용.

PluginName

읽기 전용 값입니다.

기본값: ACInstallDir\bin\cainstrm.dll

PlugIns

CA Access Control 이 사용하는 플러그인 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\PlugIns
```

Instrumentation\PlugIns 레지스트리 키에는 레지스트리 항목이 포함되어 있지 않습니다. 여기에는 로드된 모든 플러그인에 대한 레지스트리 하위 키가 포함되어 있습니다.

CMDPlg

CA Access Control 이 사용하는 CMD 플러그인 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\PlugIns\CMDPlg

Instrumentation\PlugIns\CMDPlg 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

Altitude

플러그인 로딩 순서를 정의합니다.

제한: 1-1000(이 제한을 벗어나는 값은 내부용으로 예약되어 있음)

유형: REG_DWORD

기본값: 5

ApplyOnDLL

현재 플러그인을 적용할 DLL 이름(모듈)을 정의합니다.

유형: REG_SZ

기본값: Kernel32.dll

ApplyOnProcess

현재 플러그인을 적용할 프로세스를 정의합니다.

서비스 이름, 파일 이름 또는 전체 경로 이름을 제공할 수 있습니다. 예: "services.exe", "\system32\services.exe", "c:\windows\system32\services.exe".

유형: REG_MULTI_SZ

기본값: CMD.exe

ExcludeProcess

플러그인을 적용하지 않을 프로세스를 정의합니다.

참고: 이 항목은 ApplyOnProcess 가 설정되지 않은 경우에만 유효합니다.

유형: REG_MULTI_SZ

기본적으로 이것은 비어 있습니다.

OperationMode

메모리로 플러그인을 로드할지 여부를 지정합니다(1).

유형: REG_DWORD

기본값: 1

PluginName

플러그인에 대한 DLL(Dynamic Link Library)의 이름을 정의합니다.

유형: REG_SZ

기본값: ACInstallDir\bin\CMDPlg.dll

ServiceTimeOut

seosd 와의 트랜잭션을 기다리는 최대 시간 간격(밀리초)을 정의합니다.

참고: 제한 시간이 만료되면 요청이 승인됩니다.

유형: REG_DWORD

기본값: BB8(십진수 3000)

TraceDbgEnable

cainstrm 모듈의 상태 플래그를 추적할지 여부, 즉 DbgView 또는 커널 디버거 추적을 사용할지 여부를 지정합니다.

유형: RED_DWORD

제한: 0 - false, 1 - true

기본값: 0

TraceFileEnable

파일에 대한 추적을 활성화합니다.

유형: REG_DWORD

기본값: 0(비활성)

TraceFileIsCyclic

추적 파일의 유형을 지정합니다.

유형: REG_DWORD

제한: 0 - 추적 파일이 순환 아님, 1 - 추적 파일이 순환

기본값: 0

TraceFileSizeLimit

추적 파일의 최대 크기(바이트)를 정의합니다. 값 0 은 추적 파일에 최대 크기 제한이 없음을 의미합니다.

유형: REG_DWORD

기본값: 0

TraceFilteringMask

각 플러그인에 대한 필터링 마스크를 정의합니다. 이 레지스트리 값의 지원되는 값은 레지스트리 값을 정의하는 소프트웨어 구성 요소의 상태에 따라 변경됩니다. 두 값은 미리 정의되어 있습니다. 0 - 모든 정보가 필터링됩니다(정보 표시 안 함), 0x0ffffffff - 정보가 필터링되지 않습니다(모든 정보 표시).

유형: REG_DWORD

기본값: 0

참고: 이 레지스트리 값을 변경하기 전에 우선 CA 에 문의하는 것이 좋습니다.

TraceFolderPath

추적 파일의 전체 경로 이름을 정의합니다.

유형: REG_SZ

기본값: 0

TraceOutputMask

추적 출력 채널(디버그, 스트림, 파일, ETW)에 대한 필터링 마스크를 정의합니다. 추적이 파일, DbgView 디버거 채널, WinDbg 디버거 채널로 출력되도록 지정할 수 있습니다. 값이 0 이면 출력을 비활성화합니다.

유형: REG_DWORD

기본값: 0

참고: 이 레지스트리 값을 변경하기 전에 우선 CA 에 문의하는 것이 좋습니다.

TraceReadParamsSec

추적 매개 변수를 업데이트하기 위한 시간 간격을 정의합니다. WinServicePlg.dll 은 TraceReadParamsSec 마다 업데이트 추적 매개 변수를 읽습니다.

유형: REG_DWORD

기본값: 60

OCIPlg

CA Access Control 이 사용하는 OCI 플러그인 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\PlugIns\OCIPlg

Instrumentation\PlugIns\OCIPlg 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

Altitude

플러그인 로딩 순서를 정의합니다.

제한: 1-1000(이 제한을 벗어나는 값은 내부용으로 예약되어 있음)

유형: REG_DWORD

기본값: 5

ApplyOnDLL

현재 플러그인을 적용할 DLL 이름(모듈)을 정의합니다.

유형: REG_SZ

기본값: OCI.dll

ApplyOnProcess

현재 플러그인을 적용할 프로세스를 정의합니다.

서비스 이름, 파일 이름 또는 전체 경로 이름을 제공할 수 있습니다. 예: "services.exe", "\system32\services.exe", "c:\windows\system32\services.exe".

유형: REG_MULTI_SZ

기본적으로 이 토큰은 설정되지 않습니다(플러그인이 모든 프로세스에 적용됨).

ExcludeProcess

플러그인을 적용하지 않을 프로세스를 정의합니다.

참고: 이 항목은 ApplyOnProcess 가 설정되지 않은 경우에만 유효합니다.

유형: REG_MULTI_SZ

기본적으로 이것은 비어 있습니다.

OperationMode

메모리로 플러그인을 로드할지 여부를 지정합니다(1).

유형: REG_DWORD

기본값: 0

PluginName

플러그인에 대한 DLL(Dynamic Link Library)의 이름을 정의합니다.

유형: REG_SZ

기본값: ACInstallDir\bin\OCIPlg.dll

ServiceTimeOut

seosd 와의 트랜잭션을 기다리는 최대 시간 간격(밀리초)을 정의합니다.

참고: 제한 시간이 만료되면 요청이 승인됩니다.

유형: REG_DWORD

기본값: BB8(십진수 3000)

TraceDbgEnable

cainstrm 모듈의 상태 플래그를 추적할지 여부, 즉 DbgView 또는 커널 디버거 추적을 사용할지 여부를 지정합니다.

유형: RED_DWORD

제한: 0 - false, 1 - true

기본값: 0

TraceFileEnable

파일에 대한 추적을 활성화합니다.

유형: REG_DWORD

기본값: 0(비활성)

TraceFileIsCyclic

추적 파일의 유형을 지정합니다.

유형: REG_DWORD

제한: 0 - 추적 파일이 순환 아님, 1 - 추적 파일이 순환

기본값: 0

TraceFileSizeLimit

추적 파일의 최대 크기(바이트)를 정의합니다. 값 0 은 추적 파일에 최대 크기 제한이 없음을 의미합니다.

유형: REG_DWORD

기본값: 0

TraceFilteringMask

각 플러그인에 대한 필터링 마스크를 정의합니다. 이 레지스트리 값의 지원되는 값은 레지스트리 값을 정의하는 소프트웨어 구성 요소의 상태에 따라 변경됩니다. 두 값은 미리 정의되어 있습니다. 0 - 모든 정보가 필터링됩니다(정보 표시 안 함), 0x0ffffffff - 정보가 필터링되지 않습니다(모든 정보 표시).

유형: REG_DWORD

기본값: 0

참고: 이 레지스트리 값을 변경하기 전에 우선 CA 에 문의하는 것이 좋습니다.

TraceFolderPath

추적 파일의 전체 경로 이름을 정의합니다.

유형: REG_SZ

기본값: 0

TraceOutputMask

추적 출력 채널(디버그, 스트림, 파일, ETW)에 대한 필터링 마스크를 정의합니다. 추적이 파일, DbgView 디버거 채널, WinDbg 디버거 채널로 출력되도록 지정할 수 있습니다. 값이 0 이면 출력을 비활성화합니다.

유형: REG_DWORD

기본값: 0

참고: 이 레지스트리 값을 변경하기 전에 우선 CA 에 문의하는 것이 좋습니다.

TraceReadParamsSec

추적 매개 변수를 업데이트하기 위한 시간 간격을 정의합니다. WinServicePlg.dll 은 TraceReadParamsSec 마다 업데이트 추적 매개 변수를 읽습니다.

유형: REG_DWORD

기본값: 60

ODBCPlg

CA Access Control 이 사용하는 PUPM 에이전트 ODBC 플러그인 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\PlugIns\ODBCPlg

Instrumentation\PlugIns\ODBCPlg 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

Altitude

플러그인 로딩 순서를 정의합니다.

제한: 1-1000(이 제한을 벗어나는 값은 내부용으로 예약되어 있음)

유형: REG_DWORD

기본값: 5

ApplyOnDLL

현재 플러그인을 적용할 DLL 이름(모듈)을 정의합니다.

유형: REG_MULTI_SZ

기본값: ODBC32.dll

ApplyOnProcess

현재 플러그인을 적용할 프로세스를 정의합니다.

서비스 이름, 파일 이름 또는 전체 경로 이름을 제공할 수 있습니다. 예: "services.exe", "\system32\services.exe", "c:\windows\system32\services.exe".

유형: REG_MULTI_SZ

기본적으로 이 토큰은 설정되지 않습니다(플러그인이 모든 프로세스에 적용됨).

ExcludeProcess

플러그인을 적용하지 않을 프로세스를 정의합니다.

참고: 이 항목은 ApplyOnProcess 가 설정되지 않은 경우에만 유효합니다.

유형: REG_MULTI_SZ

기본적으로 이것은 비어 있습니다.

OperationMode

메모리로 플러그인을 로드할지 여부를 지정합니다(1).

유형: REG_DWORD

기본값: 0

PluginName

플러그인에 대한 DLL(Dynamic Link Library)의 이름을 정의합니다.

유형: REG_SZ

기본값: ACInstallDir\bin\ODBCPlg.dll

ServiceTimeOut

seosd 와의 트랜잭션을 기다리는 최대 시간 간격(밀리초)을 정의합니다.

참고: 제한 시간이 만료되면 요청이 승인됩니다.

유형: REG_DWORD

기본값: BB8(십진수 3000)

TraceDbgEnable

cainstrm 모듈의 상태 플래그를 추적할지 여부, 즉 DbgView 또는 커널 디버거 추적을 사용할지 여부를 지정합니다.

유형: RED_DWORD

제한: 0 - false, 1 - true

기본값: 0

TraceFileEnable

파일에 대한 추적을 활성화합니다.

유형: REG_DWORD

기본값: 0(비활성)

TraceFileIsCyclic

추적 파일의 유형을 지정합니다.

유형: REG_DWORD

제한: 0 - 추적 파일이 순환 아님, 1 - 추적 파일이 순환

기본값: 0

TraceFileSizeLimit

추적 파일의 최대 크기(바이트)를 정의합니다. 값 0 은 추적 파일에 최대 크기 제한이 없음을 의미합니다.

유형: REG_DWORD

기본값: 0

TraceFilteringMask

각 플러그인에 대한 필터링 마스크를 정의합니다. 이 레지스트리 값의 지원되는 값은 레지스트리 값을 정의하는 소프트웨어 구성 요소의 상태에 따라 변경됩니다. 두 값은 미리 정의되어 있습니다. 0 - 모든 정보가 필터링됩니다(정보 표시 안 함), 0x0ffffffff - 정보가 필터링되지 않습니다(모든 정보 표시).

유형: REG_DWORD

기본값: 0

참고: 이 레지스트리 값을 변경하기 전에 우선 CA 에 문의하는 것이 좋습니다.

TraceFolderPath

추적 파일의 전체 경로 이름을 정의합니다.

유형: REG_SZ

기본값: 0

TraceOutputMask

추적 출력 채널(디버그, 스트림, 파일, ETW)에 대한 필터링 마스크를 정의합니다. 추적이 파일, DbgView 디버거 채널, WinDbg 디버거 채널로 출력되도록 지정할 수 있습니다. 값이 0 이면 출력을 비활성화합니다.

유형: REG_DWORD

기본값: 0

참고: 이 레지스트리 값을 변경하기 전에 우선 CA 에 문의하는 것이 좋습니다.

TraceReadParamsSec

추적 매개 변수를 업데이트하기 위한 시간 간격을 정의합니다. WinServicePlg.dll 은 TraceReadParamsSec 마다 업데이트 추적 매개 변수를 읽습니다.

유형: REG_DWORD

기본값: 60

RunAsPlg

CA Access Control 이 사용하는 RunAs 플러그인 설정은 다음 키에 있습니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\PlugIns\RunAsPlg

Instrumentation\PlugIns\RunAsPlg 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

Altitude

플러그인 로딩 순서를 정의합니다.

제한: 1-1000(이 제한을 벗어나는 값은 내부용으로 예약되어 있음)

유형: REG_DWORD

기본값: 5

ApplyOnDLL

현재 플러그인을 적용할 DLL 이름(모듈)을 정의합니다.

유형: REG_MULTI_SZ

기본값: advapi32.dll

ApplyOnProcess

현재 플러그인을 적용할 프로세스를 정의합니다.

서비스 이름, 파일 이름 또는 전체 경로 이름을 제공할 수 있습니다. 예: "services.exe", "\system32\services.exe", "c:\windows\system32\services.exe".

유형: REG_MULTI_SZ

기본값: runas.exe, explorer.exe

ExcludeProcess

플러그인을 적용하지 않을 프로세스를 정의합니다.

참고: 이 항목은 ApplyOnProcess 가 설정되지 않은 경우에만 유효합니다.

유형: REG_MULTI_SZ

기본적으로 이것은 비어 있습니다.

OperationMode

메모리로 플러그인을 로드할지 여부를 지정합니다(1).

유형: REG_DWORD

기본값: 0

PluginName

플러그인에 대한 DLL(Dynamic Link Library)의 이름을 정의합니다.

유형: REG_SZ

기본값: ACInstallDir\bin\RunAsPlg.dll

ServiceTimeOut

seosd 와의 트랜잭션을 기다리는 최대 시간 간격(밀리초)을 정의합니다.

참고: 제한 시간이 만료되면 요청이 승인됩니다.

유형: REG_DWORD

기본값: BB8(십진수 3000)

TraceDbgEnable

cainstrm 모듈의 상태 플래그를 추적할지 여부, 즉 DbgView 또는 커널 디버거 추적을 사용할지 여부를 지정합니다.

유형: RED_DWORD

제한: 0 - false, 1 - true

기본값: 0

TraceFileEnable

파일에 대한 추적을 활성화합니다.

유형: REG_DWORD

기본값: 0(비활성)

TraceFileIsCyclic

추적 파일의 유형을 지정합니다.

유형: REG_DWORD

제한: 0 - 추적 파일이 순환 아님, 1 - 추적 파일이 순환

기본값: 0

TraceFileSizeLimit

추적 파일의 최대 크기(바이트)를 정의합니다. 값 0 은 추적 파일에 최대 크기 제한이 없음을 의미합니다.

유형: REG_DWORD

기본값: 0

TraceFilteringMask

각 플러그인에 대한 필터링 마스크를 정의합니다. 이 레지스트리 값의 지원되는 값은 레지스트리 값을 정의하는 소프트웨어 구성 요소의 상태에 따라 변경됩니다. 두 값은 미리 정의되어 있습니다. 0 - 모든 정보가 필터링됩니다(정보 표시 안 함), 0x0ffffffff - 정보가 필터링되지 않습니다(모든 정보 표시).

유형: REG_DWORD

기본값: 0

참고: 이 레지스트리 값을 변경하기 전에 우선 CA 에 문의하는 것이 좋습니다.

TraceFolderPath

추적 파일의 전체 경로 이름을 정의합니다.

유형: REG_SZ

기본값: 0

TraceOutputMask

추적 출력 채널(디버그, 스트림, 파일, ETW)에 대한 필터링 마스크를 정의합니다. 추적이 파일, DbgView 디버거 채널, WinDbg 디버거 채널로 출력되도록 지정할 수 있습니다. 값이 0 이면 출력을 비활성화합니다.

유형: REG_DWORD

기본값: 0

참고: 이 레지스트리 값을 변경하기 전에 우선 CA 에 문의하는 것이 좋습니다.

TraceReadParamsSec

추적 매개 변수를 업데이트하기 위한 시간 간격을 정의합니다. WinServicePlg.dll 은 TraceReadParamsSec 마다 업데이트 추적 매개 변수를 읽습니다.

유형: REG_DWORD

기본값: 60

StopPlg

CA Access Control 이 사용하는 STOP(스택 오버플로 보호) 플러그인 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\PlugIns\StopPlg
```

Instrumentation\PlugIns\StopPlg 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

Active

플러그인의 활성화 여부를 지정합니다(1).

유형: REG_DWORD

기본값: 1

Altitude

플러그인 로딩 순서를 정의합니다.

제한: 1-1000(이 제한을 벗어나는 값은 내부용으로 예약되어 있음)

유형: REG_DWORD

기본값: 5

ApplyOnDLL

현재 플러그인을 적용할 DLL 이름(모듈)을 정의합니다.

유형: REG_MULTI_SZ

기본값: Kernel32.dll

ApplyOnProcess

현재 플러그인을 적용할 프로세스를 정의합니다.

서비스 이름, 파일 이름 또는 전체 경로 이름을 제공할 수 있습니다. 예: "services.exe", "\system32\services.exe", "c:\windows\system32\services.exe".

유형: REG_MULTI_SZ

기본적으로 이 토큰은 설정되지 않습니다(플러그인이 모든 프로세스에 적용됨).

ExcludeProcess

플러그인을 적용하지 않을 프로세스를 정의합니다.

참고: 이 항목은 ApplyOnProcess 가 설정되지 않은 경우에만 유효합니다.

유형: REG_MULTI_SZ

기본적으로 이것은 비어 있습니다.

OperationMode

메모리로 플러그인을 로드할지 여부를 지정합니다(1).

유형: REG_DWORD

기본값: 1

PluginName

플러그인에 대한 DLL(Dynamic Link Library)의 이름을 정의합니다.

유형: REG_SZ

기본값: ACInstallDir\bin\StopPlg.dll

STOPClientTraceEnabled

STOP 클라이언트 모듈이 추적 로깅을 활성화할지 여부를 지정합니다.

유형: REG_DWORD

기본값: 0(비활성)

STOPClientTraceModulePath

STOP 클라이언트 모듈 추적 로깅 모듈의 전체 경로 이름을 정의합니다.

유형: REG_SZ

기본값: ACInstallDir\bin\STOPClientTrace.dll

STOPSEHHandlingModeDisabled

SEH 기반 악용에 대한 STOP 확장 검사를 활성화할지 여부를 지정합니다.

유형: REG_DWORD

기본값: 1(비활성)

TraceDbgEnable

cainstrm 모듈의 상태 플래그를 추적할지 여부, 즉 DbgView 또는 커널 디버거 추적을 사용할지 여부를 지정합니다.

유형: RED_DWORD

제한: 0 - false, 1 - true

기본값: 0

TraceFileIsCyclic

추적 파일의 유형을 지정합니다.

유형: REG_DWORD

제한: 0 - 추적 파일이 순환 아님, 1 - 추적 파일이 순환

기본값: 0

TraceFileSizeLimit

추적 파일의 최대 크기(바이트)를 정의합니다. 값 0 은 추적 파일에 최대 크기 제한이 없음을 의미합니다.

유형: REG_DWORD

기본값: 0

TraceFilteringMask

각 플러그인에 대한 필터링 마스크를 정의합니다. 이 레지스트리 값의 지원되는 값은 레지스트리 값을 정의하는 소프트웨어 구성 요소의 상태에 따라 변경됩니다. 두 값은 미리 정의되어 있습니다. 0 - 모든 정보가 필터링됩니다(정보 표시 안 함), 0x0ffffffff - 정보가 필터링되지 않습니다(모든 정보 표시).

유형: REG_DWORD

기본값: 0

참고: 이 레지스트리 값을 변경하기 전에 우선 CA 에 문의하는 것이 좋습니다.

TraceFolderPath

추적 파일의 전체 경로 이름을 정의합니다.

유형: REG_SZ

기본값: 0

TraceOutputMask

추적 출력 채널(디버그, 스트림, 파일, ETW)에 대한 필터링 마스크를 정의합니다. 추적이 파일, DbgView 디버거 채널, WinDbg 디버거 채널로 출력되도록 지정할 수 있습니다. 값이 0 이면 출력을 비활성화합니다.

유형: REG_DWORD

기본값: 0

참고: 이 레지스트리 값을 변경하기 전에 우선 CA 에 문의하는 것이 좋습니다.

WinServicePlg

CA Access Control이 사용하는 Windows 서비스 보호 플러그인 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\WinServicePlg
```

Instrumentation\PlugIns\WinServicePlg 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

Active

플러그인의 활성화 여부를 지정합니다(1).

유형: REG_DWORD

기본값: 1

Altitude

플러그인 로딩 순서를 정의합니다.

제한: 1-1000(이 제한을 벗어나는 값은 내부용으로 예약되어 있음)

유형: REG_DWORD

기본값: 5

ApplyOnDLL

현재 플러그인을 적용할 DLL 이름(모듈)을 정의합니다.

유형: REG_MULTI_SZ

기본값: Rpcrt4.dll

ApplyOnProcess

현재 플러그인을 적용할 프로세스를 정의합니다.

서비스 이름, 파일 이름 또는 전체 경로 이름을 제공할 수 있습니다. 예: "services.exe", "\system32\services.exe", "c:\windows\system32\services.exe".

유형: REG_MULTI_SZ

기본값: Services.exe

ExcludeProcess

플러그인을 적용하지 않을 프로세스를 정의합니다.

참고: 이 항목은 ApplyOnProcess가 설정되지 않은 경우에만 유효합니다.

유형: REG_MULTI_SZ

기본적으로 이것은 비어 있습니다.

OperationMode

메모리로 플러그인을 로드할지 여부를 지정합니다(1).

유형: REG_DWORD

기본값: 1

PluginName

플러그인에 대한 DLL(Dynamic Link Library)의 이름을 정의합니다.

유형: REG_SZ

기본값: ACInstallDir\bin\WinServicePlg.dll

ServiceTimeOut

seosd 와의 트랜잭션을 기다리는 최대 시간 간격(밀리초)을 정의합니다.

참고: 제한 시간이 만료되면 요청이 승인됩니다.

유형: REG_DWORD

기본값: BB8(십진수 3000)

TraceDbgEnable

cainstrm 모듈의 상태 플래그를 추적할지 여부, 즉 DbgView 또는 커널 디버거 추적을 사용할지 여부를 지정합니다.

유형: RED_DWORD

제한: 0 - false, 1 - true

기본값: 0

TraceFileEnable

파일에 대한 추적을 활성화합니다.

유형: REG_DWORD

기본값: 0(비활성)

TraceFileIsCyclic

추적 파일의 유형을 지정합니다.

유형: REG_DWORD

제한: 0 - 추적 파일이 순환 아님, 1 - 추적 파일이 순환

기본값: 0

TraceFileName

TraceFileEnable 이 true 일 때 추적에 사용할 전체 파일 이름을 지정합니다.

유형: REG_MULTI_SZ

기본값: Rpcrt4.dll

TraceFileSizeLimit

추적 파일의 최대 크기(바이트)를 정의합니다. 값 0 은 추적 파일에 최대 크기 제한이 없음을 의미합니다.

유형: REG_DWORD

기본값: 0

TraceFilteringMask

각 플러그인에 대한 필터링 마스크를 정의합니다. 이 레지스트리 값의 지원되는 값은 레지스트리 값을 정의하는 소프트웨어 구성 요소의 상태에 따라 변경됩니다. 두 값은 미리 정의되어 있습니다. 0 - 모든 정보가 필터링됩니다(정보 표시 안 함), 0x0ffffffff - 정보가 필터링되지 않습니다(모든 정보 표시).

유형: REG_DWORD

기본값: 0

참고: 이 레지스트리 값을 변경하기 전에 우선 CA 에 문의하는 것이 좋습니다.

TraceFolderPath

추적 파일의 전체 경로 이름을 정의합니다.

유형: REG_SZ

기본값: 0

TraceOutputMask

추적 출력 채널(디버그, 스트림, 파일, ETW)에 대한 필터링 마스크를 정의합니다. 추적이 파일, DbgView 디버거 채널, WinDbg 디버거 채널로 출력되도록 지정할 수 있습니다. 값이 0 이면 출력을 비활성화합니다.

유형: REG_DWORD

기본값: 0

참고: 이 레지스트리 값을 변경하기 전에 우선 CA 에 문의하는 것이 좋습니다.

TraceReadParamsSec

추적 매개 변수를 업데이트하기 위한 시간 간격을 정의합니다. WinServicePlg.dll 은 TraceReadParamsSec 마다 업데이트 추적 매개 변수를 읽습니다.

유형: REG_DWORD

기본값: 1E(30 decimal)

lang

CA Access Control 이 사용하는 관리 언어(selang) 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\lang
```

lang 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

help_path

lang 도움말 파일이 있는 디렉터리입니다.

기본값: ACInstallDir\data\help

HandleHomeDir

기본 사용자 계정에 대한 HOME_DIR 속성을 업데이트하고 홈 디렉터리를 작성할지 여부를 결정하는 값입니다.

값이 0 으로 설정되면 사용자의 속성 HOME_DIR 만 업데이트됩니다. 값이 1 로 설정되면 사용자의 속성이 업데이트되고 홈 디렉터리가 파일 시스템에 실제로 작성됩니다.

query_size

데이터베이스 쿼리에 나열되는 레코드의 최대 수입니다.

기본값: 100

SetBlockRun

프로그램이 트러스트되었는지 확인하고 언트러스트된 프로그램의 실행을 차단할지 여부를 지정합니다.

유효한 값:

yes-viapgm 권한 부여 규칙으로 정의된 모든 프로그램에서 blockrun 속성이 yes 로 설정됩니다.

no-viapgm 권한 부여 규칙으로 정의된 모든 프로그램에서 blockrun 속성이 no 로 설정됩니다.

기본값: Yes

SpaceReplace

내부 사용자 전용. 이 키는 항상 비어 있어야 합니다.

logmgr 키 - 레지스트리 설정

CA Access Control 이 사용하는 로깅 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\logmgr

logmgr 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

audit_back

CA Access Control 감사 백업 파일의 이름입니다. CA Access Control 만 이 파일에 쓸 수 있습니다.

기본값 ACInstallDir\log\seos.audit.bak

audit_group

감사 로그를 읽을 수 있는 그룹입니다.

기본값: ComputerAssociates

audit_log

CA Access Control 감사 로그 파일의 이름입니다. 이 파일이 audit_size 에 지정된 크기에 도달하면 CA Access Control 은 파일을 닫고, 파일 이름을 audit_back 에 있는 이름으로 변경하고, 새 감사 로그를 작성합니다. CA Access Control 만 이 파일에 쓸 수 있습니다.

기본값: ACInstallDir\log\seos.audit

audit_max_files

CA Access Control 이 날짜 트리거된 백업을 수행할 때 누적하는 감사 로그 백업 파일의 최대 개수를 정의합니다. BackUp_Date 구성 설정이 none 이외의 값으로 설정된 경우 CA Access Control 은 날짜 트리거된 백업 파일을 계속 누적합니다. 이 구성 설정을 사용하면 CA Access Control 이 감사 로그 백업에 사용하는 디스크 공간을 줄일 수 있습니다. 감사 로그 백업 파일의 수가 설정한 제한에 도달하면 CA Access Control 은 새 백업 파일을 만들 때 가장 오래된 백업 파일을 삭제합니다.

값:

- **0** - 모든 감사 로그 백업 파일 유지
- n - 0 보다 큰 양의 정수

참고: 중복 감사 로그 백업 파일은 CA Access Control 에서 자동으로 보호되기 때문에 수동으로 제거할 수 없습니다. 또한 감사 보고가 사용되면 CA Access Control 은 보고서 에이전트가 프로세스를 완료할 때까지 백업 파일을 삭제하지 않습니다.

기본값: 0

audit_size

CA Access Control 감사 로그 파일의 최대 크기(KB)입니다. 50KB 보다 작게 지정하지 마십시오.

기본값: 10240

참고: 감사 파일 크기가 2 GB 를 초과하면 CA Access Control 은 감사 레코드를 감사 파일에 기록하는 것을 중단합니다.

AuditFiltersFile

AC 감사 필터 파일의 이름입니다.

기본값: ACInstallDir\data\audit.cfg

BackUp_Date

CA Access Control 이 백업을 수행하는 기준입니다. 다섯 개의 값(no, yes, daily, weekly 및 monthly) 중 하나를 지정할 수 있습니다.

no 를 지정하면 CA Access Control 은 audit_size 레지스트리 값에 따라 백업을 수행하지만 파일에 타임스탬프를 설정하지는 않습니다.

yes 를 지정하면 CA Access Control 은 크기 제한 레지스트리 값 audit_size 에 따라 백업을 수행하고 파일에 타임스탬프를 설정합니다.

daily, **weekly** 또는 **monthly** 를 지정하면 CA Access Control 은 처음으로 감사 로그 백업 파일을 만들 때 타임스탬프를 추가합니다. 현재 날짜가 타임스탬프를 지난 경우 CA Access Control 은 자동으로 백업 파일을 만들고 그 파일에 타임스탬프를 설정합니다.

그러나 감사 로그 파일의 크기가 audit_size 레지스트리 값을 처음으로 초과하면 CA Access Control 은 타임스탬프를 발행하지 않고 백업 파일을 작성합니다.

기본값: no

제한: 값을 모두 대문자로 지정하거나 모두 소문자로 지정해야 합니다.

error_back

CA Access Control 오류 백업 파일의 이름입니다.

기본값: ACInstallDir\Log\seos.error.bak

error_group

오류 로그 파일을 읽을 수 있는 그룹입니다.

이 값을 none 으로 설정하면, 관리자만 파일을 읽을 수 있습니다.

기본값: 없음

error_log

CA Access Control 오류 로그 파일의 이름입니다. 이 파일이 erro_size 에 지정된 크기에 도달하면 CA Access Control 은 파일을 닫고, 파일 이름을 error_back 에 있는 이름으로 변경하고, 새 오류 로그를 작성합니다. CA Access Control 만 이 파일에 쓸 수 있습니다.

기본값: ACInstallDir\log\seos.error

error_size

CA Access Control 오류 로그 파일의 최대 크기(KB)입니다.

기본값: 50

irecorder_audit

IR API 라이브러리가 로컬 보안 서비스 감사 이벤트 외에 기존 PMD 의 감사 이벤트도 라우트할지 여부를 지정합니다.

all - 로컬 보안 서비스 감사 이벤트 외에 정책 모델의 감사 이벤트도 라우트합니다.

localhost - 로컬 보안 서비스의 감사 이벤트만 라우트합니다.

기본값: all

SendAuditToNativeChannel

seosd 가 감사 이벤트를 CA Access Control 용 Windows 2008 이벤트 로그 채널로 보낼지 여부를 지정합니다(1).

기본값: 0(아니오)

SendAuditToNativeLog

seosd 가 감사 이벤트를 Windows 이벤트 로그로 보낼지 여부를 지정합니다(1).

기본값: 0(아니오)

message

CA Access Control 이 사용하는 메시징 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\message
```

message 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

filename

CA Access Control 명령에 대한 응답으로 나타나는 메시지의 대부분을 제공하는 파일의 이름입니다.

기본값: ACInstallDir\Data\SeOS.msg

WACFILENAME

CA Access Control Administrator GUI 에서 사용되는 메시지 파일의 이름입니다.

기본값: WAC.MSG

WACPATH

CA Access Control Administrator GUI 의 메시지 파일이 있는 디렉터리입니다.

기본값: ACInstallDir\Data\

OS_user

CA Access Control 이 사용하는 엔터프라이즈 사용자 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\OS_user
```

OS_user 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

create_user_in_db

CA Access Control 에 대해 정의되지 않은 사용자의 XUSER 레코드를 CA Access Control 이 작성할지 여부 및 해당 사용자의 로그인 시간을 지정합니다.

참고: 이 설정은 엔터프라이즈 사용자(osuser_enabled 가 1 로 설정됨)를 사용할 경우에만 적용됩니다.

유효한 값:

0 - CA Access Control 이 자동으로 XUSER 레코드를 작성하지 않습니다.

1 - CA Access Control 이 자동으로 XUSER 레코드를 작성합니다.

기본값: 1

osuser_enabled

엔터프라이즈 사용자 및 그룹의 활성화 여부를 지정합니다.

유효한 값:

0 - 엔터프라이즈 사용자 및 그룹의 사용이 비활성화됩니다.

1 - 엔터프라이즈 사용자 및 그룹의 사용이 활성화됩니다.

기본값: 0

passwd

CA Access Control 이 사용하는 암호 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\passwd

passwd 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

DefaultPgroup

내부 사용자 전용.

기본값: 기타

Dictionary

암호로 사용할 수 없는 단어가 포함된 파일의 전체 경로 이름을 정의합니다.

참고: 이 파일을 사용하려면 사전 형식 암호 규칙(use_dbdict)을 file 로 설정하고 UseDict 설정을 yes 로 설정해야 합니다. 사전 형식을 db 로 설정한 경우 사용할 수 없는 암호를 CA Access Control 로부터 가져오며 이 설정은 무시됩니다.

기본값: ACInstallDir\Data\words

EnforceViaeTrust

CA Access Control 을 통해서만 사용자 암호를 업데이트 또는 작성하도록 할지 여부를 지정합니다.

기본값: 0(CA Access Control 을 사용할 필요가 없음).

PasswordTimeOut

CA Access Control 암호 필터가 권한 부여 응답을 기다리는 최대 시간(밀리초)을 정의합니다.

기본값: 4000

PasswordTimeOutAnswer

권한 부여 프로세스가 지정된 제한 시간 내에 응답하지 않을 경우 LSA 로 다시 전송할 응답을 지정합니다.

0 으로 설정하면 암호 변경이 거부되고, 1 로 설정하면 암호 변경이 승인됩니다.

기본값: 0

UseDict

암호를 확인할 때 Dictionary 설정으로 설정한 dictionary 파일을 사용할지 여부를 지정합니다.

참고: 또한, 사전 파일을 사용하려면 사전 형식 암호 규칙(use_dbdict)을 file 로 설정해야 합니다. 사전 형식을 db 로 설정한 경우 사용할 수 없는 암호를 CA Access Control 로부터 가져오며 이 설정은 무시됩니다.

기본값: no

Pmd

CA Access Control 이 사용하는 일반 정책 모델 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd
```

Pmd 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

_pmd_directory_

PMDB 데이터베이스 파일이 있는 디렉터리를 정의합니다.

기본값: ACInstallDir\Data

ClientOperationTimeout

이 컴퓨터의 정책 모델 클라이언트가 정책 모델로부터의 응답을 기다리는 시간(초)을 정의합니다. 정책 모델이 이 시간 내에 응답하지 않으면 정책 모델 클라이언트는 이 정책 모델이 응답할 수 없다고 간주합니다.

기본값: 60

MaximumPolicyModels

작성할 수 있는 최대 정책 모델 수를 정의합니다.

기본값: 16

ShutdownWaitingTimeout

이 컴퓨터의 정책 모델이 해당 구성 요소가 완전하게 종료되기까지 기다리는 시간(밀리초)을 정의합니다. 정책 모델 구성 요소가 이 시간 내에 정상 종료되지 않으면 정책 모델이 구성 요소를 강제로 종료합니다.

기본값: 60000(1 분)

TCPReceiveTimeout

이 컴퓨터의 정책 모델이 구독자로부터 응답을 기다리는 시간(초)을 정의합니다. 정책 모델 구독자가 이 시간 내에 응답하지 않으면 정책 모델은 구독자에 대한 연결을 닫습니다.

기본값: 60

<PMDB_Name>

CA Access Control 이 사용하는 특정 정책 모델 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd\PMDB_Name

각 Pmd\PMDB_Name 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

_Min_Retries_

정책 모델 서비스(sepmdd)가 비활성화되기 전에 CA Access Control 이 사용할 수 없는 구독자에 액세스하기 위해 시도하는 최소 횟수를 정의합니다.

기본값: 4

_Retry_Timeout

사용할 수 없는 구독자에 액세스하기 위한 연속 시도 사이의 시간(분)을 정의합니다.

기본값: 30

_Shutoff_Time_

서비스가 중지되기 전에 sepmdd 가 기다리는 비활성 기간(분)을 정의합니다.

기본값: 1

Active_Policy

정책 모델 이름을 정의합니다.

Always_Propagate

오류가 있을 때 정책 모델이 명령을 전파할지 여부를 지정합니다. 기본적으로 정책 모델은 항상 전파를 위해 명령을 전송합니다. 이 값을 no 로 설정하면 정책 모델은 오류가 있을 때 명령을 전송하지 않습니다.

Auto_Truncate

업데이트 파일에서 잘린 전파된 항목을 활성화할지 여부를 지정합니다.

기본값: Yes

Filter

업데이트 파일에 대한 필터 파일의 전체 경로 이름을 정의합니다.

기본값 없음.

force_auto_truncate

정책 모델에 대한 구독자가 없는 경우에도 CA Access Control 이 업데이트 파일을 자를지 여부를 지정합니다.

사용자가 수동으로(sepmd -t) 업데이트 파일을 자를 수 있으며, CA Access Control 역시 자동 자르기를 트리거하는 이벤트를 정의하는 별도의 구성 설정(trigger_auto_truncate)을 기반으로 자동으로 파일을 자릅니다.

참고: 정책 모델에 대한 모든 구독자가 "동기화되지 않은" 경우 정책 모델은 실제로 구독자를 갖지 못합니다.

기본값: yes

Parent_pmd

이 PMDB 가 업데이트를 허용하는 부모 PMDB 의 이름을 정의합니다.

기본값 없음.

trigger_auto_truncate

업데이트 파일의 자동 자르기를 트리거하는 정책 모델 업데이트 파일의 크기(MB)를 정의합니다.

하한값보다 낮은 값을 사용하면 CA Access Control 은 기본값을 사용합니다. 상한값보다 높은 값을 사용하면 CA Access Control 은 상한값을 사용합니다.

유형: REG_DWORD

제한: 1 - 2000MB

기본값: 1024 MB

UseEncryption

updates.dat 파일에 저장된 업데이트 정보를 암호화할지 여부를 지정합니다.

기본값: no

logmgr

CA Access Control 이 사용하는 특정 정책 모델 로그 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd\PMDB_Name\logmgr
```

각 Pmd\PMDB_Name\logmgr 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

audit_back

정책 모델 감사 백업 파일의 이름을 정의합니다. CA Access Control 만 이 파일에 쓸 수 있습니다.

기본값: pmd_audit.bak

audit_group

감사 로그를 읽을 수 있는 그룹을 정의합니다.

기본값: Computer Associates

audit_log

정책 모델 감사 로그 파일의 이름을 정의합니다. 이 파일이 audit_size 에 지정된 크기에 도달하면 CA Access Control 은 파일을 닫고, 파일 이름을 audit_back 에 설정된 이름으로 변경하고, 새 감사 로그를 작성합니다. CA Access Control 만 이 파일에 쓸 수 있습니다.

기본값: pmd.audit

audit_size

정책 모델 감사 로그 파일의 최대 크기(KB)를 정의합니다. 50KB 보다 작은 값을 지정하지 마십시오.

기본값: 1024

error_back

정책 모델 오류 백업 파일의 이름을 정의합니다.

기본값: pmd_error.back

error_group

오류 로그 파일을 읽을 수 있는 그룹을 정의합니다.

이 값을 none 으로 설정하면, 관리자만 파일을 읽을 수 있습니다.

기본값: 없음

error_log

정책 모델 오류 로그 파일의 이름을 지정합니다. 이 파일이 erro_size 에 지정된 크기에 도달하면 CA Access Control 은 파일을 닫고, 파일 이름을 error_back 에 있는 이름으로 변경하고, 새 오류 로그를 작성합니다. CA Access Control 만 이 파일에 쓸 수 있습니다.

기본값: pmd.error

error_size

CA Access Control 오류 로그 파일의 최대 크기(KB)를 정의합니다.

기본값: 50

SendAuditToNativeChannel

해당 정책 모델에 대해 CA Access Control 이 정책 모델 감사 이벤트를 Windows 2008 이벤트 로그 채널로 보낼지 여부를 지정합니다. (1)

기본값: 0(아니오)

SendAuditToNativeLog

CA Access Control 이 정책 모델 감사 이벤트를 Windows 이벤트 로그로 보낼지 여부를 지정합니다. (1)

기본값: 0(아니오)

<DMS_Name>

CA Access Control 이 사용하는 특정 DMS 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd\DMS_Name
```

Pmd\DMS_Name 레지스트리 키에는 레지스트리 항목이 포함되어 있지 않습니다. 여기에는 DMS_Name 이란 이름의 DMS 에 대한 레지스트리 하위 키가 포함되어 있습니다.

endpoint_management

CA Access Control 이 사용하는 특정 DMS 끝점 관리 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd\
DMS_NAME\endpoint_management
```

dmsmgr 는 DMS 를 만들 때 이 키의 레지스트리 값을 정의합니다. 이 키는 호스트에 DMS 가 없는 경우 정의되지 않습니다.

각 Pmd\DMS_Name\endpoint_management 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

commands_to_exec_before_sleep

대기 상태가 되기 전에 루프에서 DMS 가 실행하는 끝점 명령의 수를 지정합니다.

기본값: 10

debug_mode

CA Access Control 이 DMS 디렉터리(1)의 endpoint_management.log 파일에 디버그 메시지를 기록할지 여부를 지정합니다.

제한: 0,1

기본값: 0(디버깅 사용 안 함)

참고: 로그 파일은 ACInstallDir\log\endpoint_management.log 에 있습니다.

operation_mode

CA Access Control 메시지 큐를 통한 중앙 (DMS) 끝점 관리를 사용할지 여부를 지정합니다.

제한: 0,1

기본값: 1(사용됨)

sleep_between_exec_commands

DMS 가 대기하는 시간(밀리초)을 지정합니다. DMS 가 대기 상태에서 돌아오면 commands_to_exec_before_sleep 레지스트리 값에 지정된 수의 끝점 명령을 수행합니다.

기본값: 100

policyfetcher

CA Access Control 이 사용하는 policyfetcher 서비스 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\policyfetcher
```

policyfetcher 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

check_deployment_tasks

policyfetcher 가 배포 호스트에서 새 배포 작업(DEPLOYMENT 리소스)을 검사하는 빈도(초)를 정의합니다.

기본값: 600(10 분마다)

deploy_timeout

policyfetcher 가 끝점에서 배포 또는 배포 취소 작업이 완료될 때까지 기다리는 시간(초)을 정의합니다.

기본값: 900

dh_command_retry_interval

각 DH 알림 명령 재시도 사이의 시간(초)을 정의합니다.

기본값: 30

endpoint_heartbeat

policyfetcher 가 배포 호스트(DH)에 하트비트를 전송하는 빈도를 정의합니다. 이 빈도는 check_deployment_task 설정의 요소이며, policyfetcher 가 하트비트를 전송하기 전에 배포 작업을 검사할 횟수를 결정합니다. 예를 들어 check_deployment_task 가 기본값인 600 초(10 분)로 설정되어 있을 때 이 값을 6 으로 설정하면, policyfetcher 는 3600 초(1 시간)마다 한 번씩 하트비트를 전송합니다.

하트비트를 보낸 이후에 policyfetcher 는 또한 위반 계산기(start devcalc 명령)를 실행하고 위반 계산이 완료될 때까지 60 초 동안 기다립니다. 60 초가 지나면 policyfetcher 는 로컬 끝점 정보가 DH 정보와 동일한지 계속 검사합니다.

기본값: 10

max_dh_command_retry

policyfetcher 가 포기하기 전까지 DH 에서 업데이트 알림을 받기 위해 재시도하는 최대 횟수를 정의합니다.

기본값: 3

max_dh_retry_cycles

policyfetcher 가 재해 복구 HD 로 이동하기 전까지 프로덕션 DH 에서 업데이트 알림을 받기 위해 재시도하는 최대 사이클 수를 정의합니다.

기본값: 3

policy_verification

작업을 실행하기 전에 policyfetcher 가 백업 CA Access Control 데이터베이스에서 새 배포 작업을 확인할지 여부를 지정합니다.

유효한 값:

1 - 정책 확인 실행

0 - 정책 확인 사용 안 함

기본값: 0

policyfetcher_enabled

policyfetcher 서비스를 실행할지 여부를 지정합니다.

유효한 값:

1 - policyfetcher 를 실행합니다.

0 - policyfetcher 를 비활성화합니다.

기본값: 0

PUPMAgent

CA Access Control 이 사용하는 PUPM 에이전트 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\PUPMAgent
```

PUPM 에이전트 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

ActivitySendCountThreshold

누적되는 캐시된 이벤트의 최대 수를 지정합니다. 캐시된 이벤트으 수가 지정된 값에 도달하면 PUPM 에이전트는 CA Access Control 엔터프라이즈 관리에 이벤트를 보냅니다.

제한: 1–8192

기본값: 1024

참고: 값으로 0 을 지정하면 CA Access Control 은 이 매개 변수의 기본값을 사용합니다. 8192 보다 큰 값을 지정하면 CA Access Control 은 이 매개 변수에 대해 값 8192 를 사용합니다.

ActivitySendTimeInterval

캐시된 작업 로그 메시지를 CA Access Control 엔터프라이즈 관리로 보내는 간격(분)을 지정합니다.

제한: 양의 정수

기본값: 10

참고: 값으로 0 을 지정하면 CA Access Control 은 이 매개 변수의 기본값을 사용합니다.

InterfaceName

요청을 처리하기 위해 PUPM 에이전트가 사용하는 인터페이스 이름을 정의합니다.

기본값: PUPMAgentInterface

OperationMode

PUPM 에이전트 작업 모드를 지정합니다.

제한: 0 - PUPM 에이전트가 비활성화되고 실행되지 않음, 1 - PUPM 에이전트가 활성화되고 실행됨, 2 - PUPM 에이전트가 활성화되고, 실행되고, 데이터를 추적 파일에 로깅함

기본값: 0

ProcessArgumentsReplacement

PUPM 에이전트가 프로세스 인수 대체를 지원하는지 여부를 지정합니다.

제한: 0,1

기본값: 0

참고: 프로세스 인수 대체를 지원하도록 선택하는 경우(즉, 이 레지스트리 항목의 값을 1 로 설정하는 경우) CMD 플러그인도 활성화해야 합니다. CMD 플러그인을 활성화하려면 다음 레지스트리 항목을 1 로 설정하십시오.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\plugins\CMDPlg\OperationMode

보고서

CA Access Control 이 사용하는 sereport 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Reports

Reports 레지스트리 키에는 레지스트리 항목이 포함되어 있지 않습니다. 여기에는 sereport 가 생성하는 모든 보고서에 대한 레지스트리 하위 키가 포함되어 있습니다.

참고: sereport 가 생성하는 보고서 각각의 레지스트리 항목에 대한 자세한 내용은 sereport 유틸리티 (페이지 200)를 참조하십시오.

색상

CA Access Control 이 사용하는 sereport 스타일 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Reports\colors

Reports\colors 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

background

내부 사용자 전용.

이 키는 변경하지 말고 그대로 두어야 합니다.

class_title

보고서 class_title 의 색상을 정의합니다.

기본값: green

logo

로고 파일의 전체 경로 이름을 정의합니다.

기본값: ACInstallDir\data\logo.jpg

title

보고서 제목의 색상을 정의합니다.

기본값: midnightblue

ReportAgent 키 - 레지스트리 설정

CA Access Control 이 사용하는 보고서 에이전트 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\ReportAgent

ReportAgent 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

audit_enabled

끝점 감사 데이터를 배포 서버로 보낼지 여부를 지정합니다.

값: 0 - 아니요, **1** - 예

기본값: 0

audit_filter

보고서 에이전트가 외부 소스(예: CA Enterprise Log Manager)로 라우팅하는 감사 레코드에 대한 필터링 규칙이 포함된 파일의 전체 경로 이름을 정의합니다. 이 파일에 따라 보고서 에이전트가 라우팅하는 레코드가 결정됩니다.

기본값: ACInstallDir\Data\AuditRouteFlt.cfg

audit_queue

보고서 에이전트가 끝점 감사 데이터를 보내는 큐의 이름을 정의합니다.

기본값: queue/audit

audit_read_chunk

보고서 에이전트가 감사 파일을 한 번 읽을 때 수집하는 최대 감사 레코드 수를 정의합니다.

제한: 양의 정수

기본값: 300

audit_send_chunk

보고서 에이전트가 각 연결에서 배포 서버로 보내는 최대 감사 레코드 수를 정의합니다. 보고서 에이전트는 수집한 감사 레코드 수가 이 개수에 도달하면 해당 레코드를 배포 서버로 보냅니다.

제한: 양의 정수

기본값: 1800

audit_sleep

보고서 에이전트가 감사 보고서 생성 사이에 수면하는 시간 간격을 정의합니다.

제한: 초 수를 나타내는 양의 정수

기본값: 10

audit_timeout

보고서 에이전트가 끝점 감사 데이터를 배포 서버로 보내야 하는 주기를 정의합니다. 마지막 전송 이후로 이 시간이 경과하면 보고서 에이전트는 수집한 레코드 수가 audit_send_chunk 값보다 적어도 감사 데이터를 배포 서버로 보냅니다.

제한: 초 수를 나타내는 양의 정수

기본값: 300

interval

CA Access Control 이 보고서를 생성하여 배포 서버로 보내는 간격(분)을 정의합니다.

예약 설정은 간격 시작 시간과 작업 요일을 정의합니다. 보고서 에이전트가 예약된 발생보다 나중에 시작되는 경우 예약부터 계산된 다음 간격과 정의된 이후 간격마다 예약된 요일에 보고서를 보냅니다.

예: schedule=8:30@Mon,Tue,Wed 및 interval=5 가 있고 보고서 에이전트가 화요일 오전 8:47 에 로드되는 경우 보고서 에이전트는 오전 8:50 에 보고서를 생성하여 보냅니다. 이 시간이 예약된 시작 시간부터 5 분 간격을 사용하여 계산된 가장 빠른 주기입니다.

값: 0 - 간격 없음(예약된 발생만 사용); 양의 정수 - 간격으로 사용할 분 수

기본값: 0

reportagent_enabled

로컬 컴퓨터에서 보고를 활성화할지 여부를 지정합니다(1).

기본값: 0

schedule

보고서가 생성되어 배포 서버로 전송되는 시기를 정의합니다.

이 설정은 time@day[,day2][...] 형식으로 지정할 수 있습니다.

예를 들어 "19:22@Sun,Mon"을 지정하면 일요일과 월요일마다 오후 7:22 에 보고서가 생성됩니다.

기본값: 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

send_queue

보고서 에이전트가 로컬 데이터베이스의 스냅숏과 PMDB 를 보내는 배포 서버의 보고 큐 이름을 정의합니다.

기본값: queue/snapshots

추가 정보:

auditrouteflt.cfg 파일 - 감사 레코드 라우팅 필터링 (페이지 366)

SeOSD 키 - 레지스트리 설정

CA Access Control 이 사용하는 일반 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\SeOSD

SeOSD 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

AuditCollectorInterfaceName

감사 수집기 구성 요소(seosd 에 포함됨)와 감사 수집기의 다른 클라이언트(커널) 사이에서 감사 인터페이스로 기능하는 파이프 이름을 정의합니다.

기본값: AuditCollector

AuditServerCacheSize

감사 캐시의 크기를 항목 수로 정의합니다.

기본값: 1024

CreateNewClasses

seclassadm 유틸리티로 작성한 새 클래스를 CA Access Control 데이터베이스에 추가할 수 있는지 여부를 지정하기 위한 키입니다.

기본값: yes

CreateNewProps

seclassadm 유틸리티로 작성한 새 속성을 데이터베이스에 추가할 수 있는지 여부를 결정합니다.

기본값: yes

dbdir

CA Access Control 데이터베이스가 있는 디렉터리입니다.

기본값: ACInstallDir\data\seosdb

DefLookupThreads

CA Access Control 이 SID 를 계정 이름으로 해석하기 위해 사용할 수 있는 스레드 수를 정의합니다.

기본값: 5

DefLookupTimeout

CA Access Control 이 SID 를 계정 이름으로 해석하려는 시도를 중단하는 제한 시간(밀리초)을 정의합니다.

기본값: 2000

domain_names

일치 목적을 위해 사용되는 접미사 이름의 목록입니다.

CA Access Control 은 짧은 호스트 이름에 이러한 접미사를 추가하여 정규화된 긴 호스트 이름을 만듭니다. 이런 이름은 관련 HOST, CONNECT 또는 TERMINAL 클래스에서 권한 부여될 수 있습니다. CA Access Control 은 전체 이름을 식별하기 위해 domain_names 목록에 있는 도메인 이름을 권한 부여 용도의 짧은 이름에 추가하려고 시도합니다. 클래스 HOSTNP 의 경우, CA Access Control 은 이 레지스트리에 나열된 모든 도메인 이름을 패턴과 일치시켜 실제 IP 주소로 해석합니다.

EnablePolicyCache

이 값은 권한 부여 엔진이 캐시된 레코드를 사용할지 아니면 데이터베이스의 레코드를 직접 사용할지를 제어합니다.

유효한 값:

no - 권한 부여 엔진이 데이터베이스 레코드를 사용합니다.

yes - 권한 부여 엔진이 캐시 레코드를 사용합니다.

기본값: no

EnvVarResolvingMode

(FILE, SECFILE, PROGRAM, PROCESS, SPECIALPGM, TERMINAL 또는 USER 클래스에 있는 개체에 대해) 포함된 환경 변수를 확인하는 메소드입니다. 예:

newfile %SystemRoot%\temp.txt.

0 을 선택할 경우 CA Access Control 은 모든 환경 변수를 확인하고, 오류 메시지가 사용자에게 전송되며, 개체는 작성되지 않습니다.

1 을 선택할 경우 CA Access Control 은 모든 환경 변수를 확인하고, 경고 메시지가 사용자에게 전송되며, 개체가 작성됩니다.

2 를 선택할 경우 CA Access Control 은 모든 환경 변수를 확인하고 개체는 메시지 없이 작성됩니다.

3 을 선택할 경우 CA Access Control 은 환경 변수를 확인하지 않습니다.

참고: PMDB 는 환경 변수가 없다고 가정하므로 확인 작업은 실행되지 않습니다.

GeneralInterceptionMode

전체 적용 모드(0) 또는 감사 전용 모드(1)의 사용 여부를 지정합니다.

기본값: 0

GraceCountForMessage

암호 변경 대화 상자가 나타나는 남은 유예 로그인의 수를 정의합니다.

참고: 이 항목은 LogonInterceptionMethod 항목이 1 로 설정된 경우에만 적용됩니다.

기본값: 0

HostResolutionMode

CA Access Control 에서 호스트 이름을 확인하는 데 사용하는 방법을 지정합니다.

값:

0 -- HOST 확인이 동시적(현재 동작)

1 -- HOST 확인이 비동시적('이벤트 로그' 보고 사용)

이 설정의 효과는 다음과 같습니다.

- 제어가 selang 으로 즉시 반환됩니다.
- HOST 레코드를 확인할 수 없으면 selang 메시지가 표시되지 않습니다(0 과 동일).
- 알림 메시지가 '이벤트 로그'에 기록됩니다.

2 -- HOST 확인이 비동시적('이벤트 로그' 보고 사용 안 함)

'1'과 동일하지만 알림 메시지가 기록되지 않습니다.

기본값: 0

HostResolutionRenewal

내부 캐시 새로 고침 시간입니다. 레지스트리 값은 네트워크 차단 권한 부여 이벤트에 의해 사용됩니다.

HostResolutionTimeout

권한 부여 엔진이 네트워크 차단 이벤트에 대해 역방향 IP 조회 요청을 기다리는 시간입니다.

LogonInterceptionMethod

더 이상 사용되지 않습니다.

LogonTimeOut

CA Access Control 이 포기하기 전에 하위 권한 부여 DLL(eACSubAuth.dll)과의 트랜잭션을 기다리는 시간(밀리초)을 정의합니다. 이 시간이 지나면 CA Access Control 은 LogonTimeOutAnswer 에 설정된 값으로 응답합니다.

기본값: 4000

LogonTimeOutAswer

CA Access Control 의 응답 없이 LogonTimeOut 설정이 경과할 경우 운영 체제에 대한 로그온 응답을 정의합니다.

기본값: 1(true)

MaximumDiscreteFILELimit

CA Access Control 데이터베이스에서 작성할 수 있는 개별 FILE 레코드의 수입니다.

최소값은 기본값이어야 하며, 이 값을 기본값보다 작게 설정하면 CA Access Control 은 최소값이 설정된 것처럼 작동합니다.

기본값: 4096

MaximumGenericFILELimit

CA Access Control 데이터베이스에서 작성할 수 있는 일반 FILE 레코드(이름 패턴 기반 레코드)의 수입니다.

최소값은 기본값이어야 하며, 이 값을 기본값보다 작게 설정하면 CA Access Control 은 최소값이 설정된 것처럼 작동합니다.

기본값: 512

RebuildSuspiciousDatabase

이 값은 데이터베이스가 이전 세션에서 올바르게 종료되지 않은 경우에만 실행됩니다.

값을 0 으로 설정할 경우 (시작 중에) 데이터베이스의 정확성이 발견 절차를 통해 검사됩니다. 데이터베이스에 문제가 있는 것으로 확인될 경우 데이터베이스는 재작성됩니다.

값을 1 로 설정할 경우 발견 절차 검사 기능을 건너뜁니다. 데이터베이스는 데이터베이스 무결성 검사에 따라 재작성됩니다.

기본값: 1

RefreshIPInterval

연속 자동 IP 새로 고침 요청 사이의 시간(분)입니다.

이 값을 0 으로 설정하면 IP 새로 고침이 자동으로 수행되지 않습니다. 1 과 30 사이의 값을 사용하면 CA Access Control 은 설정 가능한 최소 시간인 30 분을 값으로 사용합니다.

참고: 새로 고침 요청은 시간이 오래 걸리는 작업일 수 있습니다. 자세한 내용은 secons 유틸리티 -refIP 옵션을 참조하십시오.

기본값: 0

ResponseFile

eACOexist.exe 유틸리티가 사용하는 response.ini 가 있는 위치입니다.

sim_login_timeout

접근자 요소 항목 테이블에 있는 사용되지 않은 시뮬레이션된 로그인 사용자의 수명(분)입니다.

기본값: 60

sim_login_timeout

CA Access Control 이 ACEE(Accessor Element Entry) 테이블에서 사용되지 않는 시뮬레이션된 로그인 사용자 항목을 제거하기 전의 제한 시간(분)을 정의합니다.

CA Access Control 은 ACEE 에서 발견되는 정보에 액세스해야 할 경우 시뮬레이션된 로그인을 수행하여 ACEE 항목을 작성합니다.

기본값: 60

SusrauthReadParamsSec

추적 매개 변수의 업데이트 시간 간격을 정의합니다.

기본값: 30

SusrauthTraceDbgEnable

DbgView 또는 커널 디버거에 대한 추적을 활성화할지 여부를 지정합니다(1).

기본값: 0

SusrauthTraceFileEnable

추적 파일(SusrauthTraceFileName)에 대한 추적을 활성화할지 여부를 지정합니다(1).

기본값: 0

SusrauthTraceFileName

추적 파일의 전체 경로 이름을 정의합니다.

기본값 없음

SusrauthReadParamsSec

DbgView 또는 커널 디버거에 대한 추적을 활성화할지 여부를 지정합니다(1).

기본값: 0

SurrogateInterceptionMode

SURROGATE 클래스 차단 모드를 지정합니다.

유형: REG_DWORD

제한: 0 - 사용자 모드 차단: CA Access Control 이 RunAs 유틸리티에서 받은 가장 요청만 차단합니다. 1 - 커널 모드 차단: CA Access Control 이 모든 가장 요청을 차단합니다.

기본값: 0

TerminalSearchOrder

권한 부여 엔진이 권한 부여 프로세스 중에 검사해야 할 TERMINAL 레코드를 결정하는 방법을 지정합니다.

값:

name-권한 부여 엔진은 먼저 이름으로 TERMINAL 레코드를 찾아보고, 레코드가 발견되지 않으면 일치하는 IP 주소를 찾아봅니다.

nameonly-권한 부여 엔진은 이름으로 TERMINAL 레코드를 찾아보고, 레코드가 발견되지 않으면 검색을 중단합니다. IP 주소 형식으로 된 TERMINAL 레코드는 무시합니다.

IP-권한 부여 엔진은 먼저 IP 주소로 TERMINAL 레코드를 찾아보고, 레코드가 발견되지 않으면 일치하는 이름을 찾아봅니다.

참고: TERMINAL 클래스는 와일드카드로 정의된 일반 규칙을 지원합니다(IP 주소 또는 호스트 이름 패턴 일치). 일반 규칙은 항상 특수(전체 이름) 규칙 이후에 검사됩니다. 예를 들어 이 값을 ip 로 설정하면 seosd 는 전체 IP 주소 일치, 전체 호스트 이름 일치, IP 주소 패턴 일치, 호스트 이름 패턴 일치 순서로 TERMINAL 리소스를 찾습니다.

기본값: nameonly

trace_file

추적 메시지를 요청한 경우 추적 메시지를 보낼 파일의 이름입니다.

기본값: \Log\seosd.trace

trace_file_type

추적 파일의 유형입니다.

값을 변경하고 추적 파일이 이미 있는 경우 기존 추적 파일을 파일 이름 확장명 .backup 으로 저장한 다음 새 추적 파일을 지정한 형식으로 시작합니다.

기본값: text

trace_filter

추적 메시지를 필터링하는 데 사용하는 필터 데이터가 들어 있는 파일 이름입니다. 파일의 전체 경로를 지정합니다.

기본값: \Log\trcfilter.ini

trace_space_saver

파일 시스템에 남아 있는 사용 가능한 공간(KB)입니다. 사용 가능한 공간이 이 숫자보다 작으면 CA Access Control 은 추적을 비활성화합니다.

기본값: 5120

trace_to

추적 메시지의 대상입니다. none, file 또는 file,stop 으로 설정합니다.

none 을 선택할 경우 CA Access Control 은 추적 메시지를 생성하지 않습니다.

file 을 선택할 경우 CA Access Control 은 추적 메시지를 생성하고 CA Access Control 이 활성화되는 즉시 추적 메시지를 레지스트리 trace_file 에 나열된 파일로 전송합니다.

file,stop 을 선택할 경우 CA Access Control 은 서비스 초기화 기간 중에 추적 메시지를 생성합니다. 일단 서비스가 초기화되면 추적 메시지가 더 이상 생성되지 않습니다.

기본값: file,stop

SeOSWD

CA Access Control 이 사용하는 watchdog 설정은 다음 키 아래에 유지됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\SeOSWD
```

SeOSWD 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

PgmRest

마지막 이벤트 이후부터 프로그램을 다시 확인하기 전까지의 기간(초)을 지정합니다. 프로그램은 시스템 오버로드를 방지하기 위해 중지됩니다.

기본값: 10

PgmTestInterval

프로그램을 다시 검사하는 기간(초)입니다.

기본값: 18000

SecFileRest

마지막 이벤트 이후부터 보안된 파일을 다시 확인하기 전까지의 기간(초)을 지정합니다. 프로그램은 시스템 오버로드를 방지하기 위해 중지됩니다.

기본값: 10

SecFileTestInterval

보안 파일을 다시 검사하는 기간(초)입니다.

기본값: 36000

(STOP)

CA Access Control 이 사용하는 STOP(스택 오버플로 보호) 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\STOP

STOP 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

STOPIniFileName

STOP 초기화 파일의 전체 경로 및 이름을 정의합니다. 이 파일에는 STOP 이 활성화되는 함수의 목록이 포함되어 있습니다.

기본값: ACInstallDir\Data\stop.ini

STOPLearningModeEnabled

STOP 이 특수 학습 모드에서 실행될지 여부를 지정합니다. 이 모드에서는 인시던트가 기록되지만 항상 허용됩니다. 즉, 거부 인시던트가 적절히 기록되기는 하지만 계속해서 진행하도록 허용됩니다.

기본값: 0(비활성)

STOPLogFileName

STOP(스택 오버플로 보호)용 동적 인시던트 데이터베이스의 전체 경로 및 이름을 정의합니다.

기본값: ACInstallDir\Log\STOPRTEvents.dat

STOPServerTraceEnabled

STOP 서버 모듈이 추적 로깅을 활성화할지 여부를 지정합니다.

기본값: 0(비활성)

STOPSignatureBrokerName

STOP 서명 데이터베이스를 검색하는 데 사용되는 컴퓨터(정의된 경우)의 호스트 이름을 정의합니다.

기본값 없음.

STOPSignatureFileName

STOP 서명 파일(트러스트된 인시던트 데이터베이스)의 전체 경로 및 이름을 정의합니다.

기본값: ACInstallDir\Data\stopsignature.dat

STOPUpdateInterval

STOP 서명 데이터베이스를 업데이트하려는 두 개의 연속 시도 사이의 기간(분)을 정의합니다.

기본값: 60

STOPZeroSnapshotBypassEnabled

크기가 0 인 코드 스냅숏이 포함된 인시던트를 STOP 이 허용할지 여부를 지정합니다.

기본값: 0(허용하지 않음)

Tracer

CA Access Control 이 사용하는 추적 모듈 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Tracer

Tracer 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

TraceCfgFile

CA Access Control 모듈 추적을 위한 초기화된 구성 설정이 포함된 파일의 전체 경로를 정의합니다.

기본값: ACInstallDir\Data\tracer.ini

TraceEnabled

추적 메커니즘의 활성화 여부를 지정합니다.

기본값: 0(비활성)

UCTNG

CA Access Control 이 사용하는 Unicenter 통합 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\UCTNG

UCTNG 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

EvtManagerServer

Unicenter TNG 호스트의 이름을 정의합니다.

Integration

Unicenter TNG 와의 통합을 활성화하고 감사 데이터를 전송할지 여부를 지정합니다.

TNG_calendars

달력 기능의 활성화 여부를 지정합니다.

TNG_refresh_interval

달력 상태 새로 고침의 시간 간격을 정의합니다.

기본값: 10

WebService

CA Access Control 이 사용하는 웹 서비스 설정은 다음 키 아래에 유지됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\WebService

참고: WebService 레지스트리 키 및 관련 항목은 CA Access Control 끝점 관리 설치 시 추가됩니다.

WebService 레지스트리 키에는 다음 레지스트리 항목이 포함되어 있습니다.

auditFileCheckInterval

CA Access Control 웹 서비스가 감사 파일 크기가 정의된 한계에 도달했는지를 검사하는 시간 간격(초)을 정의합니다.

기본값: 60

auditFileMaxSize

CA Access Control 웹 서비스 감사 로그 파일의 최대 크기(KB)를 정의합니다.

파일이 이 크기에 도달하면 웹 서비스는 파일 이름을 "Backup_of_logFileName"으로 변경하고 새 감사 로그 파일을 작성합니다.

기본값: 20000

backLog

CA Access Control 웹 서비스가 유지 관리하는 요청 큐의 최대 크기를 정의합니다.

기본값: 100

logFileName

CA Access Control 웹 서비스 감사 로그 파일의 이름을 정의합니다.

이 값을 빈 문자열("")로 남겨두면, 사용자가 -debug 옵션으로 웹 서비스를 실행할 때 웹 서비스가 터미널에 로그 메시지를 보냅니다.

기본값: eACWS.log

machineName

CA Access Control 웹 서비스가 설치된 컴퓨터의 이름을 정의합니다.

maxRequestsQueue

소켓의 전역 요청 큐의 크기를 정의합니다.

기본값: 1000

maxThreads

CA Access Control 웹 서비스가 사용하는 스레드 수를 정의합니다.

기본값: 1

portNumber

CA Access Control 웹 서비스가 통신에 사용하는 포트를 정의합니다.

기본값: 5248

sessionTimeOut

작업이 없을 때 CA Access Control 웹 서비스가 세션을 종료하기 전의 시간(초)을 정의합니다.

기본값: 600

StandAloneService

CA Access Control 웹 서비스를 다른 Windows 서비스처럼 사용자가 시작 및 중지할 수 있는 독립형 서비스로 실행할지(1), 아니면 seosd 로 시작하고 secons 로 중지하는 서비스로 실행할지를 지정합니다.

기본값: 1

추가적인 레지스트리 키

다음 키와 값을 추가하거나 수정하여 CA Access Control 의 수행 방법을 변경할 수도 있습니다.

레지스트리 항목	유형	설명
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\drveng\Parameters\DisableFileInterception	REG_DWORD	파일 차단 연결의 비활성화 여부를 지정합니다(관련 함수가 부팅 시 초기화되지 않음). **값:** 1(비활성) **참고:** 이 레지스트리 항목이 없거나(기본값) 1 이외의 다른 값으로 설정되면 부팅 시 파일 차단이 초기화됩니다.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\drveng\Parameters\DisableLogonInterception	REG_DWORD	더 이상 사용되지 않습니다.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\drveng\Parameters\DisableNetworkInterception	REG_DWORD	네트워크 차단 연결의 비활성화 여부를 지정합니다(관련 함수가 부팅 시 초기화되지 않음). **값:** 1(비활성) **참고:** 이 레지스트리 항목이 없거나(기본값) 1 이외의 다른 값으로 설정되면 부팅 시 네트워크 차단이 시작됩니다.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\drveng\Parameters\DisableProcessInterception	REG_DWORD	프로세스 차단 연결의 비활성화 여부를 지정합니다(관련 함수가 부팅 시 초기화되지 않음). **값:** 1(비활성) **참고:** 이 레지스트리 항목이 없거나(기본값) 1 이외의 다른 값으로 설정되면 부팅 시 프로세스 차단이 초기화됩니다.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\drveng\Parameters\DisableRegistryInterception	REG_DWORD	레지스트리 차단 연결의 비활성화 여부를 지정합니다(관련 함수가 부팅 시 초기화되지 않음). **값:** 1(비활성) **참고:** 이 레지스트리 항목이 없거나(기본값) 1 이외의 다른 값으로 설정되면 부팅 시 레지스트리 차단이 초기화됩니다.

레지스트리 항목	유형	설명
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SeosDrv\Parameters\KernelBuffersSize	REG_DWORD	CA Access Control 커널 드라이버(seosdrv.sys)는 시작 시 기본적으로 다음 수식에 따라 내부에서 사용할 메모리를 할당합니다. number_of_buffers = amount_of_RAM 예를 들어, 256MB 의 RAM 에는 256 개의 버퍼가 할당됩니다. 각 버퍼 길이는 4096 바이트입니다. seos.drv 가 할당하는 버퍼 수를 제어하려면, 이 레지스트리 키를 작성하고 값을 할당할 버퍼 수로 설정하십시오. **참고:** 최소 버퍼 수는 32 입니다.
HKLM\SYSTEM\CurrentControlSet\SeosDrv\Parameters\EnableTMBypass	REG_DWORD	더 이상 사용되지 않습니다.
HKLM\SYSTEM\CurrentControlSet\SeosDrv\Parameters\TMDriverName	REG_SZ	더 이상 사용되지 않습니다.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\System\SeosDrv\EventMessageFile	REG_EXPAND_SZ	seosdrv.sys 드라이버의 경로 이름을 정의합니다. **기본값:** %SystemRoot%\System32\drivers\seosdrv.sys
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\System\SeosDrv\TypesSupported	REG_DWORD	지원되는 이벤트 유형의 비트 마스크를 정의하는 표준 Windows 항목입니다. **기본값:** 7
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\cainstrm\parameters\DllScanList	REG_SZ	cainstrm.sys 에 의한 주입을 트리거하는 DLL 의 쉼표로 구분된 이름별 목록을 정의합니다.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\cainstrm\parameters\DllScanListRefreshPeriod	REG_DWORD	cainstrm 레지스트리 항목을 검색하는 간격(초)을 정의합니다. **기본값**: 600

부록 A: 감사 로그 레코드

이 장은 아래의 주제를 포함하고 있습니다.

감사 레코드 (페이지 475)
감사 레코드의 이벤트 유형을 식별하는 방법 (페이지 476)
감사 이벤트 유형 (페이지 478)
로그인 및 로그아웃 이벤트의 권한 부여 단계 코드 (페이지 513)
리소스 액세스 이벤트의 권한 부여 단계 코드 (페이지 517)
언트러스트 메시지 이벤트의 권한 부여 단계 코드 (페이지 527)
인바운드 네트워크 연결 이벤트의 권한 부여 단계 코드 (페이지 529)
아웃바운드 네트워크 연결 이벤트의 권한 부여 단계 코드 (페이지 534)
보안 데이터베이스 관리 이벤트의 권한 부여 단계 코드 (페이지 537)
종료 이벤트의 권한 부여 단계 코드 (페이지 543)
암호 확인 이벤트의 권한 부여 단계 코드 (페이지 544)
사용자에 대한 추적 메시지의 권한 부여 단계 코드 (페이지 547)
레코드가 작성된 이유를 지정하는 사유 코드 (페이지 549)

감사 레코드

감사 로그의 각 레코드에는 열로 정렬된 데이터가 포함됩니다. 두 개의 열(날짜 및 타임스탬프)은 모든 레코드 유형에서 공통적으로 사용됩니다. 나머지 열과 해당 열에 포함되는 데이터는 감사 레코드 작성을 트리거한 이벤트 유형에 따라 달라집니다.

참고: 감사 로그 레코드에 대해 표시되는 열의 순서, 개수 및 내용은 감사 로그를 보는 방법에 따라 달라집니다. 일부 필드는 CA Access Control 끝점 관리, seaudit 출력 또는 자세한 seaudit 출력에 표시되지 않습니다. seaudit 유틸리티를 사용하는 경우 지정한 옵션에 따라 열의 개수, 순서 및 내용이 결정될 수도 있습니다.

감사 레코드의 이벤트 유형을 식별하는 방법

감사 레코드의 내용을 이해하려면 먼저 감사 레코드의 이벤트 유형을 식별해야 합니다. 이것은 레코드에 포함되는 데이터가 감사 레코드 작성을 트리거한 이벤트 유형에 따라 달라지기 때문입니다.

참고: 감사 로그 레코드에 대해 표시되는 열의 순서, 개수 및 내용은 감사 로그를 보는 방법에 따라 달라집니다. 일부 필드는 CA Access Control 끝점 관리, seaudit 출력 또는 자세한 seaudit 출력에 표시되지 않습니다. seaudit 유틸리티를 사용하는 경우 지정한 옵션에 따라 열의 개수, 순서 및 내용이 결정될 수도 있습니다.

감사 레코드의 이벤트 유형을 식별하려면

- CA Access Control 끝점 관리에서 감사 레코드를 보는 경우 감사 레코드가 속하는 이벤트 유형이 "감사 레코드 결과" 창의 첫 번째 열에 표시됩니다.

  감사 레코드에 대한 추가 정보를 표시하려면 첫 번째 열의 감사 이벤트 유형 링크를 클릭합니다.

- seaudit 출력에서 감사 레코드를 보는 경우 이벤트 유형을 확인하려면 자세한 출력(-detail 옵션)을 표시해야 합니다.

이벤트 유형을 식별하고 나면 메시지 정보의 나머지 내용을 해석할 수 있습니다.

예: CA Access Control 끝점 관리의 감사 레코드

다음 이미지에서는 CA Access Control 끝점 관리가 감사 이벤트를 어떻게 표시하는지를 보여 줍니다.

감사 레코드 결과 | 새로 고침

다음 필터로 필터링된 감사 레코드: '오늘의 레코드', 마지막 업데이트:09. 6. 12. 오전 10:53

표시: 10개 이벤트 / 페이지 | 1 - 10/74

이벤트	날짜	상태	클래스	사용자 이름	개체/리소스	터미널	프로그램
로그인 이벤트	2009. 6. 12. 오전 10시 52분 26초	허용됨		_dms		dhaas01-kor	_dh_module_
로그인 이벤트	2009. 6. 12. 오전 10시 42분 26초	허용됨		_dms		dhaas01-kor	_dh_module_
로그인 이벤트	2009. 6. 12. 오전 10시 32분 25초	허용됨		_dms		dhaas01-kor	_dh_module_
로그인 이벤트	2009. 6. 12. 오전 10시 22분 25초	허용됨		_dms		dhaas01-kor	_dh_module_
보안 DB 관리	2009. 6. 12. 오전 10시 22분 20초	성공	HNODE	_dms	dhaas01-kor	DMS__@dhaas01-kor	
로그인 이벤트	2009. 6. 12. 오전 10시 12분 20초	허용됨		_dms		dhaas01-kor	_dh_module_
로그인 이벤트	2009. 6. 12. 오전 10시 02분 20초	허용됨		_dms		dhaas01-kor	_dh_module_
로그인 이벤트	2009. 6. 12. 오전 9시 52분 20초	허용됨		_dms		dhaas01-kor	_dh_module_
로그인 이벤트	2009. 6. 12. 오전 9시 42분 20초	허용됨		_dms		dhaas01-kor	_dh_module_
로그인 이벤트	2009. 6. 12. 오전 9시 32분 19초	허용됨		_dms		dhaas01-kor	_dh_module_

1 - 10/74

예: 기본 seaudit 출력의 감사 레코드

다음 seaudit 출력 조각에서는 seaudit 유틸리티가 기본적으로 감사 이벤트를 어떻게 표시하는지를 보여 줍니다.

```
19 Dec 2008 16:46:47 P WINSERVICE  TM123VM-AC\Administrator Read   1059  2 VMTools
C:\WINDOWS\system32\services.exe TM123VM-AC
19 Dec 2008 16:46:52 P WINSERVICE  TM123VM-AC\Administrator Read   1059  2 VMTools
C:\WINDOWS\system32\services.exe TM123VM-AC
19 Dec 2008 16:46:53 P LOGIN      TM123VM-AC\Administrator  55  2 TM123VM-AC
C:\WINDOWS\system32\lsass.exe
19 Dec 2008 16:46:57 P WINSERVICE  TM123VM-AC\Administrator Read   1059  2 VMTools
C:\WINDOWS\system32\services.exe TM123VM-AC
19 Dec 2008 16:47:02 P WINSERVICE  TM123VM-AC\Administrator Read   1059  2 VMTools
C:\WINDOWS\system32\services.exe TM123VM-AC
19 Dec 2008 16:47:07 P WINSERVICE  TM123VM-AC\Administrator Read   1059  2 VMTools
C:\WINDOWS\system32\services.exe TM123VM-AC
19 Dec 2008 16:47:12 P WINSERVICE  TM123VM-AC\Administrator Read   1059  2 VMTools
C:\WINDOWS\system32\services.exe TM123VM-AC
19 Dec 2008 16:47:16 S UPDATE     GROUP    TM123VM-AC\Administrator 336  0 test
TM123VM-AC egtest audit-
19 Dec 2008 18:28:18 P LOGIN      TM123VM-AC\Administrator  55 10 TM123VM-AC
selang
19 Dec 2008 18:28:18 S UPDATE     TERMINAL  TM123VM-AC\Administrator 305  0
TM123VM-AC-SC1.ca.com TM123VM-AC er terminal TM123VM-AC-SC1.ca.com
```

위의 첫 번째 메시지에 대한 자세한 seaudit 출력은 다음과 같습니다.

```
19 Dec 2008 16:46:47 P WINSERVICE  TM123VM-AC\Administrator Read   1059  2 VMTools
C:\WINDOWS\system32\services.exe TW852VM-AC
```

이벤트 유형: 리소스 액세스

상태: 허용됨

클래스: WINSERVICE

리소스: VMTools

액세스: 읽기

사용자 이름: TM123VM-AC\Administrator

사용자 로그온 세션 ID: 00000000:05647d29

터미널: TM123VM-AC

프로그램: C:\WINDOWS\system32\services.exe

날짜: 19 Dec 2008

시간: 16:46

자세한 내용: 기본 레코드 범용 액세스 검사

감사 플래그: AC 데이터베이스 사용자

감사 이벤트 유형

CA Access Control 가 감사 로그에 저장하는 정보는 감사하는 이벤트 유형에 따라 결정됩니다.

CA Access Control 은 다음 이벤트 유형에 대한 감사 레코드를 기록합니다.

로그인 이벤트 (페이지 478)
로그아웃 이벤트 (페이지 481)
로그인 계정 사용 이벤트 (페이지 483)
로그인 계정 사용 안 함 이벤트 (페이지 485)
암호 시도 이벤트 (페이지 488)
리소스 액세스 이벤트 (페이지 490)
언트러스트 메시지 이벤트 (페이지 493)
인바운드 네트워크 연결 이벤트 (페이지 496)
아웃바운드 네트워크 연결 이벤트 (페이지 498)
보안 데이터베이스 관리 이벤트 (페이지 501)
시작 이벤트 (페이지 504)
종료 이벤트 (페이지 505)
암호 확인 이벤트 (페이지 508)
사용자에 대한 추적 메시지 (페이지 510)

로그인 이벤트

로그인 이벤트는 CA Access Control 또는 CA Access Control 로 보호된 호스트에 로그인하려는 시도에 대해 설명합니다.

이 이벤트의 감사 레코드 형식은 다음과 같습니다.

날짜 시간 상태 이벤트 사용자이름 세션 ID 자세한내용 원인 터미널 프로그램

날짜

이벤트가 발생한 날짜를 식별합니다.

형식: DD MMM YYYY

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 날짜 표시 형식을 지정합니다.

시간

이벤트가 발생한 시간을 식별합니다.

형식: HH:MM:SS

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 시간 표시 형식을 지정합니다.

상태

이벤트의 반환 코드를 나타냅니다.

값: 다음 중 하나일 수 있습니다.

- D(거부됨) - 권한이 부족하여 이벤트가 거부되었습니다.
- P(허용됨) - 이벤트가 허용되었습니다.
- W(경고) - 액세스 요청이 액세스 규칙을 위반하지만 경고 모드가 설정되어 이벤트가 허용되었습니다.

이벤트 유형

이 레코드가 속하는 이벤트 유형을 식별합니다.

참고: CA Access Control 끝점 관리에서는 이 필드를 간단하게 이벤트라고 합니다.

사용자 이름

이 이벤트를 트리거한 작업을 수행한 접근자의 이름을 식별합니다.

사용자 로그온 세션 ID

접근자의 세션 ID 를 식별합니다.

자세한 내용

CA Access Control 이 이 이벤트에 대해 수행할 작업을 결정한 단계를 나타냅니다.

참고: 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 권한 부여 단계 코드라고 합니다. 자세한 출력이나 CA Access Control 끝점 관리의 감사 레코드는 권한 부여 단계 코드와 연관된 메시지를 표시합니다. 전체 단계 코드 목록을 보려면 seaudit -t 를 실행하십시오.

원인

CA Access Control 이 감사 레코드를 작성한 이유를 나타냅니다.

참고: 자세한 seaudit 출력이나 CA Access Control 끝점 관리에는 이 필드가 표시되지 않습니다. 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 사유 코드라고 합니다. 전체 사유 코드 목록을 보려면 seaudit -t 를 실행하십시오.

터미널

접근자가 호스트에 연결하는 데 사용한 터미널의 이름을 식별합니다.

프로그램

이벤트를 트리거한 프로그램의 이름을 식별합니다. 즉, 접근자가 로그인하는 데 사용한 프로그램입니다. CA Access Control 관리 로그인의 경우에는 로그인한 CA Access Control 모듈(selang, 웹 서비스 등)입니다.

감사 플래그

접근자가 내부 사용자(CA Access Control 데이터베이스 사용자)인지 또는 엔터프라이즈 사용자인지를 나타냅니다.

참고: 접근자가 엔터프라이즈 사용자인 경우 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 "(OS 사용자)"라는 문자열을 표시합니다. 그렇지 않으면 이 필드는 비어 있습니다.

예: 로그인 이벤트 메시지

다음 감사 레코드는 자세한 seaudit 출력에서 가져온 것입니다.

```
28 Oct 2008 12:15:01 P LOGIN root 49047159:0000034b 59 2 _CRONJOB_ SBIN_CRON
이벤트 유형: 로그인 이벤트
상태: 허용됨
사용자 이름: root
터미널: _CRONJOB_
프로그램: SBIN_CRON
날짜: 28 Oct 2008
시간: 12:15
자세한 내용: 리소스 UACC 검사
사용자 로그온 세션 ID: 49047159:0000034b
감사 플래그: AC 데이터베이스 사용자
```

이 감사 레코드는 2008 년 10 월 28 일, 12:15:01 에 사용자 루트가 _CRONJOB_ 터미널에서 보호된 호스트에 로그인하여 SBIN_CRON 프로그램을 실행했음을 나타냅니다. 리소스의 기본 액세스 권한에서 이 작업이 허용되기 때문에 CA Access Control 에서 작업을 허용했습니다(권한 부여 단계 코드 59 - 리소스 UACC 검사). 접근자의 감사 모드에서 이 이벤트가 기록되도록 지정하기 때문에 CA Access Control 에서 이 이벤트를 기록했습니다(사유 코드 2 - 사용자 감사 모드에 로깅 필요).

추가 정보:

로그인 및 로그아웃 이벤트의 권한 부여 단계 코드 (페이지 513)
레코드가 작성된 이유를 지정하는 사유 코드 (페이지 549)

로그아웃 이벤트

UNIX 에 해당

로그아웃 이벤트는 CA Access Control 또는 CA Access Control 로 보호된 호스트에서 로그아웃하려는 시도에 대해 설명합니다.

참고: 로그아웃 이벤트는 UNIX 에서만 지원됩니다. CA Access Control 은 실제로 로그아웃을 차단하지 않습니다. 대신 세션의 마지막 프로세스가 종료될 때 로그아웃이 발생한다고 가정합니다.

이 이벤트의 감사 레코드 형식은 다음과 같습니다.

날짜 시간 상태 이벤트 사용자이름 세션 ID 자세한내용 원인 터미널

날짜

이벤트가 발생한 날짜를 식별합니다.

형식: DD MMM YYYY

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 날짜 표시 형식을 지정합니다.

시간

이벤트가 발생한 시간을 식별합니다.

형식: HH:MM:SS

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 시간 표시 형식을 지정합니다.

상태

사용자 로그아웃이 발생했음을 나타냅니다.

값: O(로그아웃)

이벤트 유형

이 레코드가 속하는 이벤트 유형을 식별합니다.

참고: CA Access Control 끝점 관리에서는 이 필드를 간단하게 이벤트라고 합니다.

사용자 이름

이 이벤트를 트리거한 작업을 수행한 접근자의 이름을 식별합니다.

사용자 로그온 세션 ID

접근자의 세션 ID 를 식별합니다.

자세한 내용:

로그아웃이 검색된 방법을 나타냅니다.

자세한 내용

CA Access Control 이 이 이벤트에 대해 수행할 작업을 결정한 단계를 나타냅니다.

참고: 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 권한 부여 단계 코드라고 합니다. 자세한 출력이나 CA Access Control 끝점 관리의 감사 레코드는 권한 부여 단계 코드와 연관된 메시지를 표시합니다. 전체 단계 코드 목록을 보려면 seaudit -t 를 실행하십시오.

원인

CA Access Control 이 감사 레코드를 작성한 이유를 나타냅니다.

참고: 자세한 seaudit 출력이나 CA Access Control 끝점 관리에는 이 필드가 표시되지 않습니다. 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 사유 코드라고 합니다. 전체 사유 코드 목록을 보려면 seaudit -t 를 실행하십시오.

터미널

접근자가 호스트에 연결하는 데 사용한 터미널의 이름을 식별합니다.

감사 플래그

접근자가 내부 사용자(CA Access Control 데이터베이스 사용자)인지 또는 엔터프라이즈 사용자인지를 나타냅니다.

참고: 접근자가 엔터프라이즈 사용자인 경우 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 "(OS 사용자)"라는 문자열을 표시합니다. 그렇지 않으면 이 필드는 비어 있습니다.

예: 로그아웃 이벤트 메시지

다음 감사 레코드는 자세한 seaudit 출력에서 가져온 것입니다.

```
29 Jan 2009 17:23:33 O LOGOUT root 49 2 computer.com
이벤트 유형: 로그아웃
상태: 로그아웃
사용자 이름: root
터미널: computer.com
날짜: 29 Jan 2009
시간: 17:23
자세한 내용: 마지막 프로세스 종료 후 로그아웃 검색
감사 플래그: AC 데이터베이스 사용자
```

이 감사 레코드는 2009 년 1 월 29 일에 CA Access Control 이 원격 터미널 computer.com 에서 작업 중인 사용자 루트의 마지막 세션 프로세스가 닫힌 것을 검색하여 사용자가 시스템에서 로그아웃했다고 가정함을 나타냅니다(권한 부여 단계 코드 49 - 마지막 프로세스가 종료된 후 로그아웃이 검색됨).

추가 정보:

로그인 및 로그아웃 이벤트의 권한 부여 단계 코드 (페이지 513)
레코드가 작성된 이유를 지정하는 사유 코드 (페이지 549)

로그인 계정 사용 이벤트

UNIX 에 해당

로그인 계정 사용 이벤트는 serevu 가 사용자 로그인을 활성화하는 이벤트에 대해 설명합니다.

이 이벤트의 감사 레코드 형식은 다음과 같습니다.

날짜 시간 상태 이벤트 사용자이름 자세한내용 원인 터미널 프로그램

날짜

이벤트가 발생한 날짜를 식별합니다.

형식: DD MMM YYYY

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 날짜 표시 형식을 지정합니다.

시간

이벤트가 발생한 시간을 식별합니다.

형식: HH:MM:SS

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 시간 표시 형식을 지정합니다.

상태

serevu 가 사용자 로그인을 활성화했음을 나타냅니다.

값: E(로그인 사용)

이벤트 유형

이 레코드가 속하는 이벤트 유형을 식별합니다.

참고: CA Access Control 끝점 관리에서는 이 필드를 간단하게 이벤트라고 합니다.

사용자 이름

이 이벤트를 트리거한 작업을 수행한 접근자의 이름을 식별합니다.

자세한 내용

CA Access Control 이 이 이벤트에 대해 수행할 작업을 결정한 단계를 나타냅니다.

참고: 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 권한 부여 단계 코드라고 합니다. 자세한 출력이나 CA Access Control 끝점 관리의 감사 레코드는 권한 부여 단계 코드와 연관된 메시지를 표시합니다. 전체 단계 코드 목록을 보려면 seaudit -t 를 실행하십시오.

원인

CA Access Control 이 감사 레코드를 작성한 이유를 나타냅니다.

참고: 자세한 seaudit 출력이나 CA Access Control 끝점 관리에는 이 필드가 표시되지 않습니다. 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 사유 코드라고 합니다. 전체 사유 코드 목록을 보려면 seaudit -t 를 실행하십시오.

터미널

접근자가 호스트에 연결하는 데 사용한 터미널의 이름을 식별합니다.

프로그램

이벤트를 트리거한 프로그램의 이름을 식별합니다.

감사 플래그

접근자가 내부 사용자(CA Access Control 데이터베이스 사용자)인지 또는 엔터프라이즈 사용자인지를 나타냅니다.

참고: 접근자가 엔터프라이즈 사용자인 경우 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 "(OS 사용자)"라는 문자열을 표시합니다. 그렇지 않으면 이 필드는 비어 있습니다.

예: 로그인 계정 사용 이벤트 메시지

다음 감사 레코드는 자세한 seaudit 출력에서 가져온 것입니다.

```
13 Jan 2009 17:05:00 E LOGINENABLE test10 5 computer.com serevu
```

이벤트 유형: 로그인 계정 사용

상태: 로그인 사용

사용자 이름: test1
자세한 내용: Stage code 0
터미널: computer.com
날짜: 13 Jan 2009
시간: 17:05
프로그램: serevu
감사 플래그: AC 데이터베이스 사용자

이 감사 레코드는 2009 년 1 월 13 일에 serevu 데몬이 test1 사용자가 computer.com 터미널에서 로그인할 수 있도록 허용했음을 나타냅니다. CA Access Control 은 serevu 데몬이 감사를 요청하여 이 이벤트를 기록했습니다(사유 코드 5 - CA Access Control serevu 유틸리티에서 감사를 요청함).

추가 정보:

로그인 및 로그아웃 이벤트의 권한 부여 단계 코드 (페이지 513)
레코드가 작성된 이유를 지정하는 사유 코드 (페이지 549)

로그인 계정 사용 안 함 이벤트

UNIX 에 해당

로그인 계정 사용 안 함 이벤트는 serevu 가 사용자 로그인을 비활성화하는 이벤트에 대해 설명합니다.

이 이벤트의 감사 레코드 형식은 다음과 같습니다.

날짜 시간 상태 이벤트 사용자이름 자세한내용 원인 터미널 프로그램

날짜

이벤트가 발생한 날짜를 식별합니다.

형식: DD MMM YYYY

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 날짜 표시 형식을 지정합니다.

시간

이벤트가 발생한 시간을 식별합니다.

형식: HH:MM:SS

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 시간 표시 형식을 지정합니다.

상태

serevu 가 사용자 로그인을 비활성화했음을 나타냅니다.

값: I(로그인 사용 안 함)

이벤트 유형

이 레코드가 속하는 이벤트 유형을 식별합니다.

참고: CA Access Control 끝점 관리에서는 이 필드를 간단하게 이벤트라고 합니다.

사용자 이름

이 이벤트를 트리거한 작업을 수행한 접근자의 이름을 식별합니다.

사용자 로그온 세션 ID

접근자의 세션 ID 를 식별합니다.

자세한 내용

CA Access Control 이 이 이벤트에 대해 수행할 작업을 결정한 단계를 나타냅니다.

참고: 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 권한 부여 단계 코드라고 합니다. 자세한 출력이나 CA Access Control 끝점 관리의 감사 레코드는 권한 부여 단계 코드와 연관된 메시지를 표시합니다. 전체 단계 코드 목록을 보려면 seaudit -t 를 실행하십시오.

원인

CA Access Control 이 감사 레코드를 작성한 이유를 나타냅니다.

참고: 자세한 seaudit 출력이나 CA Access Control 끝점 관리에는 이 필드가 표시되지 않습니다. 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 사유 코드라고 합니다. 전체 사유 코드 목록을 보려면 seaudit -t 를 실행하십시오.

터미널

접근자가 호스트에 연결하는 데 사용한 터미널의 이름을 식별합니다.

프로그램

이벤트를 트리거한 프로그램의 이름을 식별합니다.

감사 플래그

접근자가 내부 사용자(CA Access Control 데이터베이스 사용자)인지 또는 엔터프라이즈 사용자인지를 나타냅니다.

참고: 접근자가 엔터프라이즈 사용자인 경우 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 "(OS 사용자)"라는 문자열을 표시합니다. 그렇지 않으면 이 필드는 비어 있습니다.

예: 로그인 계정 사용 안 함 이벤트 메시지

다음 감사 레코드는 자세한 seaudit 출력에서 가져온 것입니다.

```
13 Jan 2009 16:53:26 I LOGINDISABLE test1 0 5 computer.com serevu
이벤트 유형: 로그인 계정 사용 안 함
상태: 로그인 사용 안 함
사용자 이름: test1
터미널: computer.com
날짜: 13 Jan 2009
시간: 16:53
프로그램: serevu
자세한 내용: 단계 코드 0
사용자 로그온 세션 ID: 496b629c:00000003
감사 플래그: AC 데이터베이스 사용자
```

이 감사 레코드는 2009 년 1 월 13 일에 serevu 데몬이 test1 사용자가 computer.com 터미널에서 로그인할 수 없도록 차단했음을 나타냅니다. CA Access Control 은 serevu 데몬이 감사를 요청하여 이 이벤트를 기록했습니다(사유 코드 5 - CA Access Control serevu 유틸리티에서 감사를 요청함).

추가 정보:

로그인 및 로그아웃 이벤트의 권한 부여 단계 코드 (페이지 513)
레코드가 작성된 이유를 지정하는 사유 코드 (페이지 549)

암호 시도 이벤트

UNIX 에 해당

암호 시도 이벤트는 잘못된 암호를 사용한 접근자의 로그인 시도에 대해 설명합니다.

이 이벤트의 감사 레코드 형식은 다음과 같습니다.

날짜 시간 상태 이벤트 사용자이름 자세한내용 원인 터미널 프로그램

날짜

이벤트가 발생한 날짜를 식별합니다.

형식: DD MMM YYYY

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 날짜 표시 형식을 지정합니다.

시간

이벤트가 발생한 시간을 식별합니다.

형식: HH:MM:SS

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 시간 표시 형식을 지정합니다.

상태

잘못된 암호 시도를 나타냅니다.

값: A(암호 시도)

이벤트 유형

이 레코드가 속하는 이벤트 유형을 식별합니다.

참고: CA Access Control 끝점 관리에서는 이 필드를 간단하게 이벤트라고 합니다.

사용자 이름

이 이벤트를 트리거한 작업을 수행한 접근자의 이름을 식별합니다.

자세한 내용

CA Access Control 이 이 이벤트에 대해 수행할 작업을 결정한 단계를 나타냅니다.

참고: 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 권한 부여 단계 코드라고 합니다. 자세한 출력이나 CA Access Control 끝점 관리의 감사 레코드는 권한 부여 단계 코드와 연관된 메시지를 표시합니다. 전체 단계 코드 목록을 보려면 seaudit -t 를 실행하십시오.

원인

CA Access Control 이 감사 레코드를 작성한 이유를 나타냅니다.

참고: 자세한 seaudit 출력이나 CA Access Control 끝점 관리에는 이 필드가 표시되지 않습니다. 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 사유 코드라고 합니다. 전체 사유 코드 목록을 보려면 seaudit -t 를 실행하십시오.

터미널

접근자가 호스트에 연결하는 데 사용한 터미널의 이름을 식별합니다.

프로그램

이벤트를 트리거한 프로그램의 이름을 식별합니다.

감사 플래그

접근자가 내부 사용자(CA Access Control 데이터베이스 사용자)인지 또는 엔터프라이즈 사용자인지를 나타냅니다.

참고: 접근자가 엔터프라이즈 사용자인 경우 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 "(OS 사용자)"라는 문자열을 표시합니다. 그렇지 않으면 이 필드는 비어 있습니다.

예: 암호 시도 이벤트 메시지

다음 감사 레코드는 자세한 seaudit 출력에서 가져온 것입니다.

```
13 Jan 2009 16:21:12 A LOGIN admin 17 8 localhost.localdomain login
이벤트 유형: 암호 시도
상태: 암호 시도
사용자 이름: admin
터미널: localhost.localdomain
날짜: 13 Jan 2009
시간: 16:21
프로그램: login
자세한 내용: 네이티브 환경에서 시도 거부
감사 플래그: AC 데이터베이스 사용자
```

이 감사 레코드는 2009 년 1 월 13 일에 사용자 admin 이 계정 암호를 변경하려고 했음을 나타냅니다. 이 시도는 로그인 실패로 인해 네이티브 환경에서 거부되었습니다(권한 부여 단계 코드 17 - 네이티브 환경에서 시도가 거부됨). pam _seos 모듈에서 이 이벤트를 기록했습니다(사유 코드 8 - CA Access Control pam 지원 UNIX 로그인 실패).

추가 정보:

로그인 및 로그아웃 이벤트의 권한 부여 단계 코드 (페이지 513)
레코드가 작성된 이유를 지정하는 사유 코드 (페이지 549)

리소스 액세스 이벤트

리소스 액세스 이벤트는 FILE, TERMINAL, PROGRAM 등의 리소스에 대한 액세스 시도를 설명합니다. 이 이벤트의 감사 레코드 데이터는 다른 레코드에 나타날 수 있습니다(예: 접근자가 TERMINAL 리소스에 액세스하는 LOGIN 이벤트). 이 경우의 이벤트 레코드는 LOGIN 유형이지만 레코드에 나타나는 감사 레코드 데이터는 리소스 액세스 이벤트 메시지 중 하나입니다.

이 이벤트의 감사 레코드 형식은 다음과 같습니다.

날자 시간 상태 클래스 사용자이름 세션 ID 액세스 자세한내용 원인 리소스 프로그램 터미널 유효 UID

날짜

이벤트가 발생한 날짜를 식별합니다.

형식: DD MMM YYYY

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 날짜 표시 형식을 지정합니다.

시간

이벤트가 발생한 시간을 식별합니다.

형식: HH:MM:SS

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 시간 표시 형식을 지정합니다.

상태

이벤트의 반환 코드를 나타냅니다.

값: 다음 중 하나일 수 있습니다.

- D(거부됨) - 권한이 부족하여 이벤트가 거부되었습니다.
- P(허용됨) - 이벤트가 허용되었습니다.
- W(경고) - 액세스 요청이 액세스 규칙을 위반하지만 경고 모드가 설정되어 이벤트가 허용되었습니다.

클래스

액세스되는 리소스가 속하는 클래스를 식별합니다.

사용자 이름

이 이벤트를 트리거한 작업을 수행한 접근자의 이름을 식별합니다.

사용자 로그온 세션 ID

접근자의 세션 ID 를 식별합니다.

액세스

이 이벤트를 트리거한 액세스 시도 유형을 식별합니다.

예: 읽기

참고: 액세스 값은 차단된 리소스가 속하는 클래스에 따라 달라집니다. 각 클래스의 액세스 권한에 대한 자세한 내용은 selang 참조 안내서를 참조하십시오.

자세한 내용

CA Access Control 이 이 이벤트에 대해 수행할 작업을 결정한 단계를 나타냅니다.

참고: 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 권한 부여 단계 코드라고 합니다. 자세한 출력이나 CA Access Control 끝점 관리의 감사 레코드는 권한 부여 단계 코드와 연관된 메시지를 표시합니다. 전체 단계 코드 목록을 보려면 seaudit -t 를 실행하십시오.

원인

CA Access Control 이 감사 레코드를 작성한 이유를 나타냅니다.

참고: 자세한 seaudit 출력이나 CA Access Control 끝점 관리에는 이 필드가 표시되지 않습니다. 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 사유 코드라고 합니다. 전체 사유 코드 목록을 보려면 seaudit -t 를 실행하십시오.

리소스

액세스 또는 업데이트되는 실제 리소스의 이름을 식별합니다.

프로그램

이벤트를 트리거한 프로그램의 이름을 식별합니다. 즉, 접근자가 리소스에 액세스하는 데 사용한 프로그램입니다.

유효 사용자 **ID**

(UNIX 전용) 기본 OS 유효 사용자 ID 의 ID 를 나타냅니다.

터미널

접근자가 호스트에 연결하는 데 사용한 터미널의 이름을 식별합니다. (UNIX 전용)

감사 플래그

접근자가 내부 사용자(CA Access Control 데이터베이스 사용자)인지 또는 엔터프라이즈 사용자인지를 나타냅니다.

참고: 접근자가 엔터프라이즈 사용자인 경우 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 "(OS 사용자)"라는 문자열을 표시합니다. 그렇지 않으면 이 필드는 비어 있습니다.

유효 사용자 이름

(UNIX 전용) 이 이벤트를 트리거한 기본 OS 유효 사용자의 이름을 식별합니다. 사용자가 다른 사용자를 대체(대리)하거나 setuid 프로그램을 실행하는 경우 이 이름은 사용자 이름과 다릅니다.

예: 리소스 액세스 이벤트 메시지

다음 감사 레코드는 자세한 seaudit 출력에서 가져온 것입니다.

```
18 Nov 2008 15:23:56 D FILE      admabc  4922ae61:00000132 Read     69  3 /tmp/one
/usr/local/bin/tcsh  localhost     admabc
이벤트 유형: 리소스 액세스
상태: 거부됨
클래스: FILE
리소스: /tmp/one
액세스: 읽기
사용자 이름: admabc
터미널: localhost
프로그램: /usr/local/bin/tcsh
날짜: 18 Nov 2008
시간: 15:23
자세한 내용: 액세스를 허용한 단계 없음
사용자 로그온 세션 ID: 4922ae61:00000132
감사 플래그: AC 데이터베이스 사용자
유효 사용자 이름: admabc
```

이 감사 레코드는 2008 년 11 월 18 일 15:23:56 에 사용자 admabc 가 로컬 컴퓨터에서 UNIX tcsh 셸 프로그램을 사용하여 보호된 /tmp/one 파일 리소스를 읽으려고 했음을 나타냅니다. CA Access Control 은 이 유형의 액세스 권한을 부여하는 규칙이 데이터베이스에 없으므로 이 작업을 거부했습니다(권한 부여 단계 코드 69 - 액세스를 허용한 단계가 없음). 리소스의 감사 모드에서 이 이벤트가 기록되도록 지정하기 때문에 CA Access Control 에서 이 이벤트를 기록했습니다(사유 코드 2 - 리소스 감사 모드에 로깅 필요).

추가 정보:

리소스 액세스 이벤트의 권한 부여 단계 코드 (페이지 517)

레코드가 작성된 이유를 지정하는 사유 코드 (페이지 549)

언트러스트 메시지 이벤트

언트러스트 이벤트는 CA Access Control Watchdog 이 이벤트에 대해 생성하는 경고 메시지를 설명합니다.

이 이벤트의 감사 레코드 형식은 다음과 같습니다.

날짜 시간 상태 클래스 모듈 자세한내용 메시지 ID/errno 파일

날짜

이벤트가 발생한 날짜를 식별합니다.

형식: DD MMM YYYY

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 날짜 표시 형식을 지정합니다.

시간

이벤트가 발생한 시간을 식별합니다.

형식: HH:MM:SS

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 시간 표시 형식을 지정합니다.

상태

언트러스트가 발생했음을 나타냅니다.

값: U(언트러스트)

클래스

Watchdog 메시지를 트리거한 리소스가 속하는 CA Access Control 클래스를 식별합니다.

값: PROGRAM 또는 SECFILE

모듈 이름

CA Access Control Watchdog 의 이름을 표시합니다.

값: seoswd

자세한 내용

언트러스트 이벤트가 발생한 이유를 나타냅니다.

참고: 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 언트러스트 사유 코드라고 합니다. 자세한 출력이나 CA Access Control 끝점 관리의 감사 레코드는 언트러스트 사유 코드와 연관된 메시지를 표시합니다. 전체 암호 품질 코드 목록을 보려면 seaudit -t 를 실행하십시오.

메지지 ID

(UNIX 전용) CA Access Control 에서 PROGRAM 또는 SECFILE 을 언트러스트한 이유를 나타냅니다.

참고: 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 상태 코드라고 하며 자세한 출력이나 CA Access Control 끝점 관리에는 표시되지 않습니다. 상태 코드의 의미를 이해하려면 seaudit -Stat untrust_code 를 실행합니다. 이 필드는 권한 부여 단계 코드가 1 인 경우에만 표시됩니다. 다른 모든 경우에서는 errno 필드가 대신 표시됩니다.

errno

errno 변수의 반환 값(오류 조건에 대한 오류 코드)을 나타냅니다.

값: 다음 중 하나일 수 있습니다.

0 - 오류가 없습니다. 이 값은 권한 부여 단계 코드가 1 인 경우에만 반환됩니다. 이 경우 errno 필드는 표시되지 않고 메시지 ID 필드가 대신 표시됩니다.

errno - 오류인 0 이 아닌 정수입니다.

참고: 오류의 의미를 확인하려면 UNIX 의 경우 로컬 컴퓨터에 있는 /usr/include/errno.h 또는 /usr/include/sys/errno.h 파일을 참조하십시오. Windows 의 경우 로컬 컴퓨터에서 net helpmsg errno 명령을 입력합니다.

파일

Watchdog 메시지를 트리거한 보호된 리소스의 전체 경로 이름을 식별합니다.

예: 언트러스트 메시지 이벤트 메시지

다음 감사 레코드는 자세한 seaudit 출력에서 가져온 것입니다.

```
18 Nov 2008 14:01:18 U PROGRAM     seoswd            1 11776 /tmp/testsuid
```

이벤트 유형: 언트러스트 메시지

클래스: PROGRAM

모듈 이름: seoswd

메시지 ID: 11776

날짜: 18 Nov 2008
시간: 14:01
파일: /tmp/testsuid
자세한 내용: 파일 시스템에서 변경된 시작 정보
감사 플래그: AC 데이터베이스 사용자

이 감사 레코드는 2008 년 11 월 15 일에 Watchdog 이 /tmp/testsuid 프로그램을 언트러스트(U) 상태로 표시했음을 나타냅니다. 파일 상태 정보가 수정되어 프로그램이 언트러스트되었습니다(언트러스트 사유 코드 1 - 파일 시스템에서 파일 정보가 변경됨).

예: seaudit -Stat 를 사용하여 프로그램이 언트러스트된 이유 확인(UNIX)

다음 seaudit -Stat 출력에서는 감사 레코드에 언급된 Watchdog 메시지 ID 에 대한 자세한 정보를 얻을 수 있는 방법을 보여 줍니다.

```
# seaudit -Stat 11776
CA Access Control seaudit v12.01.00.45 - Audit log lister
Copyright (c) 2008 CA. All rights reserved.

파일의 MODE 가 변경되었습니다.
파일의 INODE 가 변경되었습니다.
파일의 SIZE 가 변경되었습니다.
파일의 MTIME 이 변경되었습니다.
```

메시지 ID 를 사용하여 seaduit -Stat 명령을 실행하면 파일에 대한 변경 사항 목록이 표시됩니다. 이 예에서는 파일의 MODE, INODE, SIZE 및 MTIME 이 변경되었습니다. 따라서 CA Access Control 에서 이 파일을 언트러스트된 파일로 표시했습니다.

추가 정보:

언트러스트 메시지 이벤트의 권한 부여 단계 코드 (페이지 527)
레코드가 작성된 이유를 지정하는 사유 코드 (페이지 549)

인바운드 네트워크 연결 이벤트

인바운드 네트워크 연결 이벤트는 보호된 호스트로 들어오는 트래픽을 나타냅니다. 인바운드 네트워크 이벤트는 로컬 데이터베이스의 클래스 활성화에 따라 두 가지 형태로 감사됩니다. 두 감사 이벤트 유형은 모두 동일한 정보를 포함하지만 다른 보기를 사용합니다. 예를 들어 한 감사 이벤트에는 HOST 가 클래스 이름으로 포함되는 반면 다른 이벤트에서는 TCP 를 클래스 이름으로 표시합니다.

이 이벤트의 감사 레코드 형식은 다음과 같습니다.
날짜 시간 상태 이벤트 서비스 자세한내용 원인 호스트 프로그램

날짜

이벤트가 발생한 날짜를 식별합니다.

형식: DD MMM YYYY

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 날짜 표시 형식을 지정합니다.

시간

이벤트가 발생한 시간을 식별합니다.

형식: HH:MM:SS

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 시간 표시 형식을 지정합니다.

상태

이벤트의 반환 코드를 나타냅니다.

값: 다음 중 하나일 수 있습니다.

- D(거부됨) - 권한이 부족하여 이벤트가 거부되었습니다.
- P(허용됨) - 이벤트가 허용되었습니다.
- W(경고) - 액세스 요청이 액세스 규칙을 위반하지만 경고 모드가 설정되어 이벤트가 허용되었습니다.

이벤트 유형

이 레코드가 속하는 이벤트 유형을 식별합니다.

참고: CA Access Control 끝점 관리에서는 이 필드를 간단하게 이벤트라고 합니다.

호스트 이름

네트워크 트래픽이 시작된 호스트의 이름입니다.

프로그램

(UNIX 전용) 접근자가 실행하려고 시도한 프로그램의 이름을 식별합니다.

서비스

연결에 사용된 서비스의 이름을 식별합니다.

자세한 내용

CA Access Control 이 이 이벤트에 대해 수행할 작업을 결정한 단계를 나타냅니다.

참고: 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 권한 부여 단계 코드라고 합니다. 자세한 출력이나 CA Access Control 끝점 관리의 감사 레코드는 권한 부여 단계 코드와 연관된 메시지를 표시합니다. 전체 단계 코드 목록을 보려면 seaudit -t 를 실행하십시오.

원인

CA Access Control 이 감사 레코드를 작성한 이유를 나타냅니다.

참고: 자세한 seaudit 출력이나 CA Access Control 끝점 관리에는 이 필드가 표시되지 않습니다. 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 사유 코드라고 합니다. 전체 사유 코드 목록을 보려면 seaudit -t 를 실행하십시오.

예: 인바운드 네트워크 연결 이벤트 메시지

다음 감사 레코드는 자세한 seaudit 출력에서 가져온 것입니다.

```
17 Nov 2008 12:22:04 D HOST      telnet          173  3 computer.org.com
/usr/sbin/inetd
이벤트 유형: 인바운드 네트워크 연결
상태: 거부됨
호스트 이름: computer.org.com
서비스: 텔넷
프로그램: /usr/sbin/inetd/
날짜: 17 Nov 2008
시간: 12:22
자세한 내용: HOST 항목 일/시간 제한
감사 플래그: AC 데이터베이스 사용자
```

이 감사 레코드는 2008 년 11 월 17 일에 inetd 프로그램을 실행하기 위해 텔넷 서비스를 사용하여 computer.org.com 호스트에 액세스를 시도한 접근자가 보호된 호스트에 적용된 요일 및 시간 제한으로 인해 거부되었음을 나타냅니다(권한 부여 단계 코드 173 - HOST 항목 요일 및 시간 제한). 리소스의 감사 모드에서 이 이벤트가 기록되도록 지정하기 때문에 CA Access Control 에서 이 이벤트를 기록했습니다(사유 코드 2 - 리소스 감사 모드에 로깅 필요).

추가 정보:

인바운드 네트워크 연결 이벤트의 권한 부여 단계 코드 (페이지 529)
레코드가 작성된 이유를 지정하는 사유 코드 (페이지 549)

아웃바운드 네트워크 연결 이벤트

아웃바운드 네트워크 연결 이벤트는 보호된 호스트로의 아웃바운드 트래픽을 나타냅니다. 아웃바운드 네트워크 이벤트는 로컬 데이터베이스의 클래스 활성화에 따라 두 가지 형태로 감사됩니다. 두 감사 이벤트 유형은 모두 동일한 정보를 포함하지만 다른 보기를 사용합니다. 예를 들어 한 감사 이벤트에는 HOST 가 클래스 이름으로 포함되는 반면 다른 이벤트에서는 TCP 를 클래스 이름으로 표시합니다.

이 이벤트의 감사 레코드 형식은 다음과 같습니다.

날짜 시간 상태 클래스 서비스 사용자이름 자세한내용 원인 호스트 프로그램 터미널

날짜

이벤트가 발생한 날짜를 식별합니다.

형식: DD MMM YYYY

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 날짜 표시 형식을 지정합니다.

시간

이벤트가 발생한 시간을 식별합니다.

형식: HH:MM:SS

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 시간 표시 형식을 지정합니다.

상태

이벤트의 반환 코드를 나타냅니다.

값: 다음 중 하나일 수 있습니다.

- D(거부됨) - 권한이 부족하여 이벤트가 거부되었습니다.
- P(허용됨) - 이벤트가 허용되었습니다.
- W(경고) - 액세스 요청이 액세스 규칙을 위반하지만 경고 모드가 설정되어 이벤트가 허용되었습니다.

호스트 이름

대상 호스트의 이름을 식별합니다.

서비스

연결에 사용된 서비스의 이름을 식별합니다.

사용자 이름

이 이벤트를 트리거한 작업을 수행한 접근자의 이름을 식별합니다.

터미널

접근자가 호스트에 연결하는 데 사용한 터미널의 이름을 식별합니다.

프로그램

이벤트를 트리거한 프로그램의 이름을 식별합니다.

사용자 로그온 세션 **ID**

접근자의 세션 ID 를 식별합니다.

참고: 사용자 로그온 세션 ID 번호는 자세히 보기에만 표시됩니다. 사용자 로그온 세션 ID 필드는 TCP 또는 CONNECT 클래스 정의의 결과로 생성된 이벤트에만 추가됩니다.

자세한 내용

CA Access Control 이 이 이벤트에 대해 수행할 작업을 결정한 단계를 나타냅니다.

참고: 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 권한 부여 단계 코드라고 합니다. 자세한 출력이나 CA Access Control 끝점 관리의 감사 레코드는 권한 부여 단계 코드와 연관된 메시지를 표시합니다. 전체 단계 코드 목록을 보려면 seaudit -t 를 실행하십시오.

원인

CA Access Control 이 감사 레코드를 작성한 이유를 나타냅니다.

참고: 자세한 seaudit 출력이나 CA Access Control 끝점 관리에는 이 필드가 표시되지 않습니다. 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 사유 코드라고 합니다. 전체 사유 코드 목록을 보려면 seaudit -t 를 실행하십시오.

감사 플래그

접근자가 내부 사용자(CA Access Control 데이터베이스 사용자)인지 또는 엔터프라이즈 사용자인지를 나타냅니다.

참고: 접근자가 엔터프라이즈 사용자인 경우 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 "(OS 사용자)"라는 문자열을 표시합니다. 그렇지 않으면 이 필드는 비어 있습니다.

예: 아웃바운드 네트워크 연결 이벤트 메시지

다음 감사 레코드는 자세한 seaudit 출력에서 가져온 것입니다.

```
21 Jan 2009 15:37:43 D TCP      telnet    root     408  2 computer.org /usr/bin/telnet
computer.com
이벤트 유형: 아웃바운드 네트워크 연결
상태: 거부됨
호스트 이름: computer.org
서비스: 텔넷
프로그램: /usr/bin/telnet
사용자 이름: Administrator
터미널: computer.com
사용자 이름: root
날짜: 21 Jan 2009
시간: 15:37:43
자세한 내용: TCP 서비스의 기본 액세스
사용자 로그온 세션 ID: 4977248c:0000012a5248
감사 플래그: AC 데이터베이스 사용자
```

이 감사 레코드는 2009 년 1 월 21 일에 관리자가 텔넷 서비스를 통해 computer.org 터미널에서 computer.com 컴퓨터로 나가는 연결을 열었음을 나타냅니다. CA Access Control 은 TCP 레코드의 defaccess 속성 때문에 이 작업을 거부했습니다. (권한 부여 단계 코드 408 - TCP 서비스의 기본값). CA Access Control 은 접근자의 AUDIT_MODE 속성이 레코드 결과와 일치하여 이 이벤트를 기록했습니다. (사유 코드 2 - 사용자 감사 모드에 로깅 필요)

추가 정보:

아웃바운드 네트워크 연결 이벤트의 권한 부여 단계 코드 (페이지 534)
레코드가 작성된 이유를 지정하는 사유 코드 (페이지 549)

보안 데이터베이스 관리 이벤트

보안 데이터베이스 관리 이벤트는 CA Access Control 관리자 또는 적절한 권한을 가진 하위 관리자가 수행했으며 CA Access Control 에 의해 차단된 작업에 대해 설명합니다.

이 이벤트의 감사 레코드 형식은 다음과 같습니다.

날짜 시간 상태 이벤트 클래스 관리자 자세한내용 원인 개체 터미널 명령

날짜

이벤트가 발생한 날짜를 식별합니다.

형식: DD MMM YYYY

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 날짜 표시 형식을 지정합니다.

시간

이벤트가 발생한 시간을 식별합니다.

형식: HH:MM:SS

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 시간 표시 형식을 지정합니다.

상태

이벤트의 반환 코드를 나타냅니다.

값: 다음 중 하나일 수 있습니다.

- D(거부됨) - 권한이 부족하여 이벤트가 거부되었습니다.
- S(성공) - 이벤트가 허용되었습니다.
- F(실패) - 이벤트가 실패했습니다.

명령 유형

이 이벤트가 설명하는 데이터베이스 관리 명령의 유형을 식별합니다.

값은 다음 중 하나일 수 있습니다.

- **Add user** - newusr 명령
- **Add group** - newgrp 명령
- **Add resource** - newres 또는 newfile 명령
- **Modify user** - chusr 명령
- **Modify group** - chgrp 명령
- **Modify group membership** - join 명령

- **Modify resource** - chres 명령
- **Modify resource access** - authorize 명령
- **Remove user** - rmusr 명령
- **Remove group** - rmgrp 명령
- **Remove resource** - rmres 또는 rmfile 명령
- **Set options** - setoptions 명령
- **Add/Modify user** - editusr 명령
- **Add/Modify group** - editgrp 명령
- **Add/Modify resource** - editres 또는 editfile 명령
- **Administrative command** - 기타 명령

클래스

관리되는 리소스가 속하는 클래스를 식별합니다.

이벤트 유형

이 레코드가 속하는 이벤트 유형을 식별합니다.

참고: CA Access Control 끝점 관리에서는 이 필드를 간단하게 이벤트라고 합니다.

관리자

selang 명령을 실행한 관리 사용자의 이름을 식별합니다.

개체

관리되는 리소스의 이름을 식별합니다.

터미널

접근자가 호스트에 연결하는 데 사용한 터미널의 이름을 식별합니다.

참고: 명령이 부모 정책 모델에서 시작된 경우에는 이 필드에 정규화된 PMD 이름이 표시됩니다.

자세한 내용

CA Access Control 이 이 이벤트에 대해 수행할 작업을 결정한 단계를 나타냅니다.

참고: 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 권한 부여 단계 코드라고 합니다. 자세한 출력이나 CA Access Control 끝점 관리의 감사 레코드는 권한 부여 단계 코드와 연관된 메시지를 표시합니다. 전체 단계 코드 목록을 보려면 seaudit -t 를 실행하십시오.

원인

CA Access Control 이 감사 레코드를 작성한 이유를 나타냅니다.

참고: 자세한 seaudit 출력이나 CA Access Control 끝점 관리에는 이 필드가 표시되지 않습니다. 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 사유 코드라고 합니다. 전체 사유 코드 목록을 보려면 seaudit -t 를 실행하십시오.

명령

사용자가 실행한 selang 명령을 표시합니다.

감사 플래그

접근자가 내부 사용자(CA Access Control 데이터베이스 사용자)인지 또는 엔터프라이즈 사용자인지를 나타냅니다.

참고: 접근자가 엔터프라이즈 사용자인 경우 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 "(OS 사용자)"라는 문자열을 표시합니다. 그렇지 않으면 이 필드는 비어 있습니다.

예: 보안 데이터베이스 관리 이벤트 메시지

다음 감사 레코드는 자세한 seaudit 출력에서 가져온 것입니다.

```
05 Nov 2008 15:45:12 S UPDATE     FILE     DOMAIN_NAME\computer 305  0 dfdok
computer.com cr file dfdok defacc(r)
이벤트 유형: 보안 데이터베이스 관리
컴퓨터 유형: 리소스 수정
상태: 성공
관리자: DOMAIN_NAME\computer
클래스: FILE
개체: dfdok
터미널: computer.com
날짜: 05 Nov 2008
시간: 15:45
자세한 내용: ADMIN 사용자에 대해 명령 성공
명령: cr file dfdok defacc(r)
감사 플래그: AC 데이터베이스 사용자
```

이 감사 레코드는 2008 년 11 월 5 일에 CA Access Control 이 computer.com 터미널에서 보호된 호스트 로깅에 대해 cr file dfdok defacc(r) 명령을 실행하여 파일 업데이트를 시도한 관리자의 액세스를 거부했음을 나타냅니다(권한 부여 단계 코드 305 - ADMIN 사용자에 대해 허용된 명령).

추가 정보:

보안 데이터베이스 관리 이벤트의 권한 부여 단계 코드 (페이지 537)

레코드가 작성된 이유를 지정하는 사유 코드 (페이지 549)

시작 이벤트

CA Access Control 시작 이벤트는 CA Access Control 서비스(Windows) 또는 데몬(UNIX)의 시작 시퀀스에 대해 설명합니다.

이 이벤트의 감사 레코드 형식은 다음과 같습니다.

```
Date Time M Event Service
```

날짜

이벤트가 발생한 날짜를 식별합니다.

형식: DD MMM YYYY

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 날짜 표시 형식을 지정합니다.

시간

이벤트가 발생한 시간을 식별합니다.

형식: HH:MM:SS

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 시간 표시 형식을 지정합니다.

이벤트 유형

이 레코드가 속하는 이벤트 유형을 식별합니다.

참고: CA Access Control 끝점 관리에서는 이 필드를 간단하게 이벤트라고 합니다.

서비스

seosd - 기본 CA Access Control 데몬 또는 서비스입니다. seosd 데몬 또는 서비스는 CA Access Control 의 시작 및 종료 시퀀스를 제어합니다.

예: 데몬 시작 이벤트 메시지(UNIX)

다음 감사 레코드는 자세한 seaudit 출력에서 가져온 것입니다.

```
02 Nov 2008 15:41:06 M START                    seoswd
이벤트 유형: 데몬 시작
데몬: seoswd
날짜: 02 Nov 2008
```

시간: 15:41
감사 플래그: AC 데이터베이스 사용자

이 감사 레코드는 2008 년 11 월 2 일에 seoswd Watchdog 이 시작되었음을 나타냅니다.

예: 엔진 서비스 시작 이벤트 메시지(Windows)

다음 감사 레코드는 자세한 seaudit 출력에서 가져온 것입니다.

02 Nov 2008 15:34:48 M START seosd
이벤트 유형: Engine service start
엔진 서비스: seosd
날짜: 02 Nov 2008
시간: 15:34
감사 플래그: AC 데이터베이스 사용자

이 감사 레코드는 2008 년 11 월 2 일에 CA Access Control 을 시작하는 역할을 하는 seosd 서비스 엔진이 시작되었음을 나타냅니다.

종료 이벤트

CA Access Control 종료 이벤트는 관리자 또는 시스템 종료 권한을 가진 하위 관리자 사용자가 수행한 종료 프로세스에 대해 설명합니다.

이 이벤트의 감사 레코드 형식은 다음과 같습니다.

Date Time M Event UserName SessionID Details Service

날짜

이벤트가 발생한 날짜를 식별합니다.

형식: DD MMM YYYY

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 날짜 표시 형식을 지정합니다.

시간

이벤트가 발생한 시간을 식별합니다.

형식: HH:MM:SS

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 시간 표시 형식을 지정합니다.

이벤트 유형

이 레코드가 속하는 이벤트 유형을 식별합니다.

참고: CA Access Control 끝점 관리에서는 이 필드를 간단하게 이벤트라고 합니다.

사용자 이름

이 이벤트를 트리거한 작업을 수행한 접근자의 이름을 식별합니다.

사용자 로그온 세션 ID

접근자의 세션 ID 를 식별합니다.

참고: 사용자 로그온 세션 ID 번호는 자세히 보기에만 표시됩니다.

데몬(UNIX) / 엔진 서비스(Windows)

종료된 CA Access Control 데몬(UNIX) 또는 서비스(Windows)의 이름을 식별합니다.

값: seosd(CA Access Control 엔진)

자세한 내용

CA Access Control 이 이 이벤트에 대해 수행할 작업을 결정한 단계를 나타냅니다.

참고: 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 권한 부여 단계 코드라고 합니다. 자세한 출력이나 CA Access Control 끝점 관리의 감사 레코드는 권한 부여 단계 코드와 연관된 메시지를 표시합니다. 전체 단계 코드 목록을 보려면 seaudit -t 를 실행하십시오.

감사 플래그

접근자가 내부 사용자(CA Access Control 데이터베이스 사용자)인지 또는 엔터프라이즈 사용자인지를 나타냅니다.

참고: 접근자가 엔터프라이즈 사용자인 경우 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 "(OS 사용자)"라는 문자열을 표시합니다. 그렇지 않으면 이 필드는 비어 있습니다.

예: UNIX 의 종료 이벤트 메시지

다음 감사 레코드는 자세한 seaudit 출력에서 가져온 것입니다.

```
24 Sep 2008 15:40:46 M SHUTDOWN    root   452 seosd
이벤트 유형: 데몬 종료
사용자 이름: root
데몬: seosd
날짜: 24 Sep 2008
시간: 15:40:46
```

자세한 내용: 사용자가 ADMIN 또는 SPECIAL 입니다.
사용자 로그온 세션 ID: 48da26ce:00000142
감사 플래그: CA Access Control 데이터베이스 사용자

이 감사 이벤트는 2008 년 9 월 24 일에 루트 사용자가 CA Access Control 을 종료하려고 했으며 사용자에게 ADMIN 특성이 있으므로 이 작업이 허용되었음을 나타냅니다(권한 부여 단계 코드 452 - ADMIN 또는 SPECIAL 인 사용자).

예: Windows 의 종료 이벤트 메시지

다음 감사 레코드는 자세한 seaudit 출력에서 가져온 것입니다.

23 Dec 2008 12:56:20 D SHUTDOWN tst002 460 seosd
이벤트 유형: 엔진 서비스 종료
사용자 이름: tst002
엔진 서비스: seosd
날짜: 10 Feb 2009
시간: 12:56
자세한 내용: 사용자가 CA Access Control 을(를) 종료할 수 없습니다.

사용자 로그온 세션 ID: 00000000:04c240d5
감사 플래그: AC 데이터베이스 사용자

이 감사 레코드는 사용자 tst002 가 CA Access Control 을 종료할 수 없어 2008 년 12 월 23 일에 CA Access Control 종료가 거부되었음을 나타냅니다(권한 부여 단계 코드 460 - 사용자가 CA Access Control 을 종료할 수 없음).

추가 정보:

종료 이벤트의 권한 부여 단계 코드 (페이지 543)

암호 확인 이벤트

암호 확인 이벤트 유형 메시지는 사용자가 계정의 암호를 변경하지 못했음을 나타냅니다.

이 이벤트의 감사 레코드 형식은 다음과 같습니다.

날짜 시간 상태 이벤트 사용자이름 자세한내용 원인

날짜

이벤트가 발생한 날짜를 식별합니다.

형식: DD MMM YYYY

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 날짜 표시 형식을 지정합니다.

시간

이벤트가 발생한 시간을 식별합니다.

형식: HH:MM:SS

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 시간 표시 형식을 지정합니다.

이벤트 유형

이 레코드가 속하는 이벤트 유형을 식별합니다.

참고: CA Access Control 끝점 관리에서는 이 필드를 간단하게 이벤트라고 합니다.

상태

이벤트의 반환 코드를 나타냅니다.

값: F(실패) - 계정 암호를 변경하지 못했습니다.

사용자 이름

암호 시도가 적용된 사용자의 이름을 식별합니다.

자세한 내용

암호 변경 시도가 실패한 이유를 나타냅니다.

참고: 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 암호 품질 코드라고 합니다. 자세한 출력이나 CA Access Control 끝점 관리의 감사 레코드는 암호 품질 코드와 연관된 메시지를 표시합니다. 전체 암호 품질 코드 목록을 보려면 seaudit -t 를 실행하십시오.

원인

CA Access Control 이 감사 레코드를 작성한 이유를 나타냅니다.

참고: 자세한 seaudit 출력이나 CA Access Control 끝점 관리에는 이 필드가 표시되지 않습니다. 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 사유 코드라고 합니다. 전체 사유 코드 목록을 보려면 seaudit -t 를 실행하십시오.

감사 플래그

접근자가 내부 사용자(CA Access Control 데이터베이스 사용자)인지 또는 엔터프라이즈 사용자인지를 나타냅니다.

참고: 접근자가 엔터프라이즈 사용자인 경우 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 "(OS 사용자)"라는 문자열을 표시합니다. 그렇지 않으면 이 필드는 비어 있습니다.

예: 암호 확인 이벤트 메시지

다음 감사 레코드는 자세한 seaudit 출력에서 가져온 것입니다.

```
02 Dec 2008 10:23:47 F PASSWORD    test1       1 10
이벤트 유형: 암호 확인
상태: 실패
사용자 이름: test1
자세한 내용: 암호가 너무 짧습니다.
감사 플래그: AC 데이터베이스 사용자
```

이 감사 레코드는 2008 년 12 월 2 일에 사용자가 계정 암호를 변경하려고 했는데 암호가 암호 정책에 정의된 최소 필수 문자 수를 충족하지 않아 사용자 시도가 거부되었음을 나타냅니다(권한 부여 단계 코드 1 - 암호가 너무 짧음). CA Access Control 은 명시적 요청에 따라 이 이벤트 메시지를 기록했습니다(사유 코드 10 - 작업을 기록하라는 명시적 요청이 수신됨).

추가 정보:

암호 확인 이벤트의 권한 부여 단계 코드 (페이지 544)
레코드가 작성된 이유를 지정하는 사유 코드 (페이지 549)

사용자에 대한 추적 메시지

사용자 이벤트에 대한 추적 메시지는 보호된 리소스를 열거나 실행 또는 사용하려는 시도에 대해 설명합니다.

이 이벤트의 감사 레코드 형식은 다음과 같습니다.

날짜 시간 상태 이벤트 사용자이름 세션 ID 실제 UID 실제사용자이름 클래스 리소스 자세한내용 추적

날짜

이벤트가 발생한 날짜를 식별합니다.

형식: DD MMM YYYY

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 날짜 표시 형식을 지정합니다.

시간

이벤트가 발생한 시간을 식별합니다.

형식: HH:MM:SS

참고: CA Access Control 끝점 관리는 컴퓨터 설정에 따라 시간 표시 형식을 지정합니다.

상태

이벤트의 반환 코드를 나타냅니다.

값: 다음 중 하나일 수 있습니다.

- D(거부됨) - 권한이 부족하여 이벤트가 거부되었습니다.
- P(허용됨) - 이벤트가 허용되었습니다.
- W(경고) - 액세스 요청이 액세스 규칙을 위반하지만 경고 모드가 설정되어 이벤트가 허용되었습니다.

참고: 자세한 seaudit 출력에서는 이 필드에 추적 정보가 표시됩니다.

이벤트 유형

이 레코드가 속하는 이벤트 유형을 식별합니다.

참고: CA Access Control 끝점 관리에서는 이 필드를 간단하게 이벤트라고 합니다.

사용자 이름

이 이벤트를 트리거한 작업을 수행한 접근자의 이름을 식별합니다.

실제 사용자 ID

프로세스를 호출한 사용자의 사용자 ID 를 식별합니다.

실제 사용자 이름

추적된 작업을 수행하는 사용자 이름을 식별합니다.

사용자 로그온 세션 ID

접근자의 세션 ID 를 식별합니다.

유효 사용자 ID

(UNIX 전용) 기본 OS 유효 사용자 ID 의 ID 를 나타냅니다.

유효 사용자 이름

(UNIX 전용) 이 이벤트를 트리거한 기본 OS 유효 사용자의 이름을 식별합니다. 사용자가 다른 사용자를 대체(대리)하거나 setuid 프로그램을 실행하는 경우 이 이름은 사용자 이름과 다릅니다.

클래스

액세스되는 리소스가 속하는 클래스를 식별합니다.

리소스

액세스 또는 업데이트되는 실제 리소스의 이름을 식별합니다.

자세한 내용

CA Access Control 이 이 이벤트에 대해 수행할 작업을 결정한 단계를 나타냅니다.

참고: 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 숫자를 표시합니다. 이 숫자를 권한 부여 단계 코드라고 합니다. 자세한 출력이나 CA Access Control 끝점 관리의 감사 레코드는 권한 부여 단계 코드와 연관된 메시지를 표시합니다. 전체 단계 코드 목록을 보려면 seaudit -t 를 실행하십시오.

추적 정보

클래스, 리소스 및 해당 리소스에 대해 수행된 작업 또는 이 작업의 결과를 비롯한 추적 세부 정보를 표시합니다.

감사 플래그

접근자가 내부 사용자(CA Access Control 데이터베이스 사용자)인지 또는 엔터프라이즈 사용자인지를 나타냅니다.

참고: 접근자가 엔터프라이즈 사용자인 경우 자세하지 않은 seaudit 출력의 감사 레코드는 이 필드에 "(OS 사용자)"라는 문자열을 표시합니다. 그렇지 않으면 이 필드는 비어 있습니다.

예: UNIX 의 사용자에 대한 추적 메시지 이벤트 메시지

다음 감사 레코드는 자세한 seaudit 출력에서 가져온 것입니다.

```
03 Nov 2008 10:38:47 P TRACE      root      490daddd:00000140 john      108
FILE      /home/jon/file.txt  55  FILE   > Result: 'P' [stage=55 gstag=55 ACEEH=8
rv=0(/home/john/file.txt
```

이벤트 유형: 사용자에 대한 추적 메시지

날짜: 03 Nov 2008

시간: 10:38

자세한 내용: 리소스 ACL 검사

추적 정보: FILE > 결과: 'P' [stage=55 gstag=55 ACEEH=8 rv=0(/home/john/file.txt

클래스: FILE

리소스: /home/admin/file.txt

사용자 이름: root

실제 사용자 ID: 108

실제 사용자 이름: john

유효 사용자 ID: 108

유효 사용자 이름: root

사용자 로그온 세션 ID: 490daddd:00000140

감사 플래그: AC 데이터베이스 사용자

이 감사 레코드는 2008 년 11 월 3 일에 관리자가 FILE 클래스에 속하는 리소스에 액세스를 시도하여 추적 메시지가 기록되었음을 나타냅니다. 액세스된 리소스의 ACL 에 따라 관리자 액세스가 허용되었습니다(권한 부여 단계 코드 55 - 리소스 ACL 검사).

예: Windows 의 사용자에 대한 추적 메시지 이벤트 메시지

다음 감사 레코드는 자세한 seaudit 출력에서 가져온 것입니다.

```
10 Nov 2008 10:14:53 P TRACE      MACHINE\Administrator 00000000:172ef9ef MACHINE\john
MACHINE\john WINSERVICE  _default   1059  WINSERVICE >
(C:\WINDOWS\system32\services.exe) 결과: 'P' [stage=1059 gstag=1059 ACEEH=6   rv=0x0
(WebClient)]                    이유?  기본 레코드 범용 액세스 검사
```

이벤트 유형: 사용자에 대한 추적 메시지

날짜: 10 Nov 2008

시간: 10:14

자세한 내용: 기본 레코드 범용 액세스 검사

추적 정보: WINSERVICE > (C:\WINDOWS\system32\services.exe) 결과: 'P' [stage=1059 gstag=1059 ACEEH=6 rv=0x0 (WebClient)] 이유? 기본 레코드 범용 액세스 검사

클래스: WINSERVICE

리소스: _default

사용자 이름: MACHINE\Administrator

실제 사용자 이름: MACHINE\john

사용자 로그온 세션 ID: 00000000:172ef9ef
감사 플래그: AC 데이터베이스 사용자

이 감사 레코드는 2008 년 11 월 10 일에 관리자가 WINSERVICE 클래스에 속하는 _default 리소스에 액세스를 시도하여 추적 메시지가 트리거되었음을 나타냅니다. 레코드 범용 액세스 검사로 인해 관리자 액세스가 허용되었습니다(권한 부여 단계 코드 1059 - 기본 레코드 범용 액세스 검사).

추가 정보:

사용자에 대한 추적 메시지의 권한 부여 단계 코드 (페이지 547)
레코드가 작성된 이유를 지정하는 사유 코드 (페이지 549)

로그인 및 로그아웃 이벤트의 권한 부여 단계 코드

로그인 및 로그아웃 이벤트의 권한 부여 단계 코드에서는 CA Access Control 이 로그인 또는 로그아웃 이벤트에 대해 수행할 작업을 결정한 단계를 설명합니다.

추가 정보:

로그인 이벤트 (페이지 478)
로그아웃 이벤트 (페이지 481)
로그인 계정 사용 이벤트 (페이지 483)
로그인 계정 사용 안 함 이벤트 (페이지 485)
암호 시도 이벤트 (페이지 488)

2 - 사용자 개체 가져오기

CA Access Control 에서 사용자 모드, 터미널 또는 로그인 프로그램과 같은 사용자 정보를 로드할 수 없어 로그인 시도가 실패했음을 나타냅니다. 데이터베이스가 손상되었거나 CA Access Control 이 올바르게 시작되지 않은 경우 CA Access Control 은 감사 로그에 이 메시지를 쓸 수 있습니다.

3 - 로그인 터미널 원본에 대한 터미널 검사

CA Access Control 이 TERMINAL 클래스 규칙에 따라 로그인을 허용 또는 거부했음을 나타냅니다.

5 - 사용자 일시 중지 검사

사용자 계정이 일시 중지되어 CA Access Control 에서 로그인을 거부했음을 나타냅니다.

6 - 사용자 만료 검사

사용자 계정이 사용자 프로필에 정의된 대로 만료되어 CA Access Control 에서 로그인을 거부했음을 나타냅니다.

7 - 사용자 요일-시간 검사

사용자가 CA Access Control 데이터베이스에 대해 허용된 요일과 시간 외의 시간에 로그인을 시도하여 CA Access Control 에서 로그인을 거부했음을 나타냅니다.

8 - 암호 유효성 검사

UNIX 에 해당

CA Access Control 이 사용자 암호를 검사하여 암호 규칙을 준수하는지 확인했음을 나타냅니다. 사용자 암호가 CA Access Control 데이터베이스 암호 규칙을 준수하지 않아 로그인 시도가 실패한 경우 CA Access Control 에서 이 메시지를 감사 로그에 쓸 수 있습니다.

9 - 사용자 유예 로그인 검사

사용자 계정의 유예 로그인 시도 횟수가 모두 사용되어 CA Access Control 에서 로그인을 거부했음을 나타냅니다.

10 - 유예 로그인이 없어 암호가 만료됨

암호가 만료되어 CA Access Control 에서 로그인을 거부했음을 나타냅니다. 사용자가 암호 간격 제한 내에 이 암호를 변경하지 않았으며, 사용자 프로필 그룹 정의와 CA Access Control 전역 정의에 모두 암호 만료 후의 유예 횟수가 구성되어 있지 않습니다.

11 - 사용자 ACEE 작성

CA Access Control 에서 사용자에 대한 ACEE 를 성공적으로 생성했음을 나타냅니다.

12 - 사용자 비활성화 기간(일) 검사

사용자가 허용되는 비활성 간격을 초과하는 기간 동안 비활성 상태이므로 CA Access Control 에서 로그인을 거부했음을 나타냅니다. 허용되는 비활성 간격은 사용자 프로필이나 전역 CA Access Control 설정에서 정의됩니다.

13 - 사용자 로그인이 너무 많습니다.

사용자가 서로 다른 터미널에서 허용되는 최대 동시 로그인 수를 초과하여 CA Access Control 에서 로그인을 거부했음을 나타냅니다. 허용되는 최대 동시 로그인 수는 사용자 프로필이나 전역 CA Access Control 설정의 'Maxlogins' 속성 값에 정의됩니다.

14 - 활성 HOLIDAY 검사

사용자가 제한된 휴일 날짜에 로그인을 시도하여 CA Access Control 에서 로그인을 거부했음을 나타냅니다. 제한된 휴일 날짜는 HOLIDAY 클래스에 정의됩니다.

15 - 로그인 응용 프로그램(LOGINAPPL) 검사

UNIX 에 해당

LOGINAPPL 클래스 규칙으로 인해 CA Access Control 에서 로그인을 거부했음을 나타냅니다.

16 - 사용자 그룹 요일-시간 검사

사용자가 사용자 또는 사용자 그룹 중 하나에 대해 허용된 요일과 시간 외의 시간에 로그인을 시도하여 CA Access Control 에서 로그인을 거부했음을 나타냅니다.

17 - 네이티브 환경에 의해 시도가 거부되었습니다.

UNIX 에 해당

네이티브 환경 설정으로 인해 로그인 시도가 실패했음을 나타냅니다. CA Access Control PAM 모듈에 의해 기록됩니다.

18 - 도메인 제한이 없는 사용자

Windows 에 해당

사용자가 도메인 이름을 제공하지 않아 CA Access Control 에서 로그인을 거부했음을 나타냅니다.

19 - 거부할 이유가 없음 - 로그인 허용

로그인 권한 부여에 TERMINAL 개체가 할당되어 있는 경우 로그인 시도가 모든 검사 단계를 통과하여 CA Access Control 에서 로그인을 허용했음을 나타냅니다.

참고: 이 이벤트 상태 메시지가 표시되는 경우 터미널 이름이 지정되지 않은 CA Access Control 권한 부여 API 에서 로그인 권한 부여가 트리거되었음을 나타낼 수 있습니다.

20 - '논리' 사용자 검사

CA Access Control 은 '논리' 사용자(logical 속성이 설정된 사용자)의 로그인을 허용하지 않으므로 CA Access Control 에서 로그인을 거부했음을 나타냅니다.

49 - 마지막 프로세스가 종료된 후 로그아웃이 검색되었습니다.

UNIX 에 해당

CA Access Control 에서 마지막 프로세스가 종료된 후 발생하는 사용자 로그아웃 이벤트를 검색했음을 나타냅니다.

리소스 액세스 이벤트의 권한 부여 단계 코드

리소스 액세스 이벤트의 권한 부여 단계 코드에서는 CA Access Control 이 리소스 액세스 이벤트에 대해 수행할 작업을 결정한 단계를 설명합니다.

추가 정보:

리소스 액세스 이벤트 (페이지 490)

50 - 리소스의 보안 LABEL 검사

리소스에 액세스하는 사용자에 대해 다음 중 하나가 적용되어 CA Access Control 에서 리소스에 대한 액세스를 거부했음을 나타냅니다.

- 리소스 보안 레이블의 보안 수준이 사용자 보안 레이블보다 더 높습니다.
- 사용자에게 보안 레이블이 없습니다.

51 - 리소스의 보안 LEVEL 검사

리소스에 액세스하는 사용자에 대해 다음 중 하나가 적용되어 CA Access Control 에서 리소스에 대한 액세스를 거부했음을 나타냅니다.

- 리소스의 보안 수준이 사용자보다 더 높습니다.
- 사용자에게 보안 수준이 없습니다.

52 - 리소스 범주 검사

사용자에게 할당되지 않은 보안 범주가 리소스에 할당되어 CA Access Control 에서 리소스에 대한 액세스를 거부했음을 나타냅니다.

53 - 리소스 DAYTIME 검사

사용자가 리소스에 대해 허용된 요일과 시간 외의 시간에 액세스를 시도하여 CA Access Control 에서 리소스에 대한 액세스를 거부했음을 나타냅니다.

54 - 리소스 OWNER 검사

액세스하는 사용자가 리소스를 소유하고 있으므로 CA Access Control 에서 리소스에 대한 액세스를 허용했음을 나타냅니다.

55 - 리소스 ACL 검사

리소스 ACL 에 사용자가 나열되므로 CA Access Control 에서 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

56 - 리소스 그룹 ACL 검사

리소스 그룹 ACL 에 사용자가 나열되므로 CA Access Control 에서 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

57 - 리소스 ACL 에 있는 사용자 그룹

사용자 그룹 ACL 에 리소스 중 적어도 하나가 나열되므로 CA Access Control 에서 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

58 - 리소스 그룹 ACL 에 있는 사용자 그룹

리소스 그룹 ACL 에 사용자 그룹 중 적어도 하나가 나열되므로 CA Access Control 에서 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

59 - 리소스 UACC 검사

리소스의 기본 설정으로 인해 CA Access Control 에서 리소스에 대한 액세스를 허용했음을 나타냅니다.

61 - 리소스의 OPERATOR 인 사용자

사용자에게 OPERATOR 특성이 있으므로 CA Access Control 에서 리소스에 대한 액세스를 허용했음을 나타냅니다. OPERATOR 특성을 사용하면 사용자가 FILE 리소스에 대한 read 및 chdir 액세스와 관련해서 권한 부여 절차를 바이패스할 수 있습니다.

참고: UNIX 에서 CA Access Control 은 추적 파일에만 이 메시지를 쓰고 감사 로그 파일에는 메시지를 쓰지 않습니다.

62 - 보호되지 않은 리소스의 클래스에 대한 UACC 검사

CA Access Control 에서 리소스 클래스의 defaccess 값을 기준으로 CA Access Control 데이터베이스에 레코드가 없는 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

63 - 프로그램 조건부 액세스

리소스 PACL 에 프로그램과 사용자 또는 사용자 그룹 중 하나가 나열되므로 CA Access Control 에서 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

64 - 리소스 ACL 의사용자 '*'

리소스 ACL 에 별표(*)가 포함되어 있으므로 CA Access Control 에서 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

참고: 별표는 정의된 모든 사용자를 지정합니다.

65 - 리소스의 AUDITOR 인 사용자

사용자에게 AUDITOR 특성이 있으므로 CA Access Control 에서 감사 파일에 대한 액세스를 허용했음을 나타냅니다. AUDITOR 특성을 사용하면 사용자가 read 및 chdir 액세스 요청과 관련해서 권한 부여 절차를 바이패스할 수 있습니다.

참고: CA Access Control 은 추적 파일에만 이 메시지를 쓰고 감사 로그 파일에는 메시지를 쓰지 않습니다.

69 - 액세스를 허용한 단계가 없습니다.

사용자가 리소스에 액세스할 수 있도록 허용하는 규칙이 없으므로 CA Access Control 에서 리소스에 대한 액세스를 거부했음을 나타냅니다.

70 - 리소스 그룹의 OWNER 검사

리소스에 액세스하려는 사용자가 리소스 그룹 중 하나의 소유자이므로 CA Access Control 에서 리소스에 대한 액세스를 허용했음을 나타냅니다.

75 - 리소스 그룹 ACL 에 있는 사용자 '*'

리소스 그룹 ACL 에 별표(*)가 포함되어 있으므로 CA Access Control 에서 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

참고: 별표는 정의된 모든 사용자를 지정합니다.

76 - 리소스 거부 ACL 검사

리소스 NACL 에 사용자가 나열되므로 CA Access Control 에서 리소스에 대한 액세스를 거부했음을 나타냅니다.

77 - 리소스 그룹 거부 ACL 검사

리소스 그룹 NACL 에 사용자가 나열되므로 CA Access Control 에서 리소스에 대한 액세스를 거부했음을 나타냅니다.

78 - 리소스 거부 ACL 에 있는 사용자 그룹

리소스 NACL 에 사용자 그룹 중 적어도 하나가 나열되므로 CA Access Control 에서 리소스에 대한 액세스를 거부했음을 나타냅니다.

79 - 리소스 그룹 거부 ACL 에 있는 사용자 그룹

리소스 그룹 NACL 에 사용자 그룹 중 적어도 하나가 나열되므로 CA Access Control 에서 리소스에 대한 액세스를 거부했음을 나타냅니다.

80 - 리소스 거부 ACL 에 있는 사용자 '*'

리소스 NACL 에 별표(*)가 포함되어 있으므로 CA Access Control 에서 리소스에 대한 액세스를 거부했음을 나타냅니다.

참고: 별표는 정의된 모든 사용자를 지정합니다.

81 - 리소스 그룹 거부 ACL 에 있는 사용자 '*'

리소스 그룹 NACL 에 별표(*)가 포함되어 있으므로 CA Access Control 에서 리소스에 대한 액세스를 거부했음을 나타냅니다.

참고: 별표는 정의된 모든 사용자를 지정합니다.

82 - 리소스 그룹 DAYTIME 검사

사용자가 리소스 그룹에 대해 허용된 요일과 시간 외의 시간에 리소스 액세스를 시도하여 CA Access Control 에서 리소스에 대한 액세스를 거부했음을 나타냅니다.

86 - 사용자에 대한 리소스 일정 ACL 검사

사용자가 리소스 CALACL 에 의해 허용 또는 거부된 시간에 리소스 액세스를 시도하여 CA Access Control 에서 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

87 - 사용자에 대한 리소스 그룹 일정 ACL 검사

사용자가 리소스 그룹 CALACL 에 의해 허용 또는 거부된 시간에 리소스 액세스를 시도하여 CA Access Control 에서 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

88 - 사용자 그룹에 대한 리소스 일정 ACL 검사

사용자가 리소스 CALACL 에 나열된 그룹 중 하나의 구성원이어서 허용 또는 승인된 시간에 리소스 액세스를 시도하여 CA Access Control 에서 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

89 - 사용자 그룹에 대한 리소스 그룹 일정 ACL 검사

사용자가 리소스 CALACL 에 나열된 그룹 중 하나의 구성원이어서 허용 또는 승인된 시간에 사용자 그룹이 리소스 액세스를 시도하여 CA Access Control 에서 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

90 - 리소스 일정 ACL 에 있는 사용자 *

리소스 CALACL 에 별표(*)가 포함되어 있으므로 CA Access Control 에서 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

참고: 별표는 정의된 모든 사용자를 지정합니다.

91 - 리소스 그룹 일정 ACL 에 있는 사용자 *

리소스 그룹 CALACL 에 별표(*)가 포함되어 있으므로 CA Access Control 에서 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

참고: 별표는 정의된 모든 사용자를 지정합니다.

92 - 보호된 리소스의 경로 이름 바꾸기 시도

Windows 에 해당

CA Access Control 에서 보호된 파일 또는 레지스트리 항목의 이름을 바꾸는 요청을 거부했음을 나타냅니다.

200 - 클래스 검사가 활성화되지 않았습니다.

리소스 클래스가 비활성 상태이므로 CA Access Control 에서 리소스에 대한 액세스를 허용했음을 나타냅니다.

참고: 리소스 클래스가 비활성 상태이면 setoptions list 명령을 실행할 때 클래스 활동이 'No'로 표시됩니다.

201 - 사용자 정보 로드

사용자 정보를 검색하지 못해 CA Access Control 에서 요청을 승인할 수 없음을 나타냅니다.

202 - 경고 모드의 리소스

리소스가 경고 모드에 있으므로 CA Access Control 에서 리소스에 대한 액세스를 허용했음을 나타냅니다.

203 - 리소스에 대한 액세스가 MAXIMUM_ALLOWED 입니다.

Windows 에 해당

허용된 경우 CA Access Control 에서 레지스트리 핸들에 대해 최대 액세스 권한을 할당했음을 나타냅니다.

거부된 경우 CA Access Control 에서 레지스트리 핸들에 대한 액세스를 차단했음을 나타냅니다.

202 - 경고 모드의 클래스

리소스 클래스가 경고 모드에 있으므로 CA Access Control 에서 리소스에 대한 액세스를 허용했음을 나타냅니다.

210 - 특수 커널 모듈 로드 검사

UNIX 에 해당

CA Access Control 에서 KMODULE 클래스 정의를 기준으로 커널 모듈의 로드나 언로드를 허용 또는 거부했음을 나타냅니다.

250 - 언트러스트된 프로그램 실행

CA Access Control 에서 언트러스트된 프로그램 실행을 거부했음을 나타냅니다.

251 - 거부 가능한 매개 변수 사용

명령 구문에 SUDO 레코드가 금지 항목으로 정의하는 매개 변수가 포함되어 있으므로 CA Access Control 에서 sesudo 명령 실행을 거부했음을 나타냅니다.

252 - an _abspath 사용자가 상대 경로를 지정했습니다.

UNIX 에 해당

프로그램을 실행하려는 사용자가 '_abspath' 그룹의 구성원이므로 CA Access Control 에서 상대 경로에 의해 지정된 프로그램 실행을 거부했음을 나타냅니다.

253 - 허용된 sesudo 작업

CA Access Control 에서 sesudo 명령 실행을 허용했음을 나타냅니다.

254 - sesudo 명령 실패

UNIX 에 해당

운영 체제에서 sesudo 명령이 실행되지 못했음을 나타냅니다.

440 - 잘못된 일정이 검색되었습니다.

일정 정보를 가져오는 동안 오류가 발생하여 CA Access Control 에서 액세스를 거부했음을 나타냅니다. 예를 들어 메모리 문제가 발생하거나 일정 테이블이 손상되었습니다.

441 - 일정에 액세스할 수 없습니다.

액세스된 리소스와 연관된 일정 개체의 정의에서 현재 액세스를 허용하지 않으므로 CA Access Control 에서 액세스를 거부했음을 나타냅니다.

1050 - 기본 레코드 보안 레이블 검사

리소스에 액세스하는 사용자에 대해 다음 중 하나가 적용되어 CA Access Control 에서 기본 레코드에 대한 액세스를 거부했음을 나타냅니다.

- 리소스 보안 레이블의 보안 수준이 사용자 보안 레이블보다 더 높습니다.
- 사용자에게 보안 레이블이 없습니다.

1051 - 기본 레코드 보안 수준 검사

리소스에 액세스하는 사용자에 대해 다음 중 하나가 적용되어 CA Access Control 에서 기본 리소스에 대한 액세스를 거부했음을 나타냅니다.

- 리소스의 보안 수준이 사용자보다 더 높습니다.
- 사용자에게 보안 수준이 없습니다.

1052 - 기본 레코드 범주 검사

사용자에게 할당되지 않은 보안 범주가 리소스에 할당되어 CA Access Control 에서 기본 리소스에 대한 액세스를 거부했음을 나타냅니다.

1053 - 기본 레코드 요일 및 시간 검사

사용자가 리소스에 대해 허용된 요일과 시간 외의 시간에 액세스를 시도하여 CA Access Control 에서 기본 리소스에 대한 액세스를 거부했음을 나타냅니다.

1054 - 기본 레코드 OWNER 검사

액세스하는 사용자가 기본 리소스를 소유하고 있으므로 CA Access Control 에서 기본 리소스에 대한 액세스를 허용했음을 나타냅니다.

1055 - 사용자에 대한 기본 레코드 ACL 검사

리소스 ACL 에 사용자가 나열되거나 나열되지 않으므로 CA Access Control 에서 기본 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

1056 - 사용자에 대한 기본 레코드 그룹 ACL 검사

리소스 그룹 ACL 에 사용자가 나열되거나 나열되지 않으므로 CA Access Control 에서 기본 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

1057 - 사용자 그룹에 대한 기본 레코드 ACL 검사

CA Access Control 에서 기본 리소스에 대한 read 또는 chdir 액세스를 허용했음을 나타냅니다.

참고: CA Access Control 은 추적 파일에만 이 메시지를 쓰고 감사 로그 파일에는 메시지를 쓰지 않습니다.

1058 - 사용자 그룹에 대한 기본 레코드 그룹 ACL 검사

리소스 그룹 ACL 에 사용자 그룹이 나열되거나 나열되지 않으므로 CA Access Control 에서 기본 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

1059 - 기본 레코드 범용 액세스 검사

리소스의 기본 설정으로 인해 CA Access Control 에서 기본 리소스에 대한 액세스를 허용했음을 나타냅니다.

1061 - 기본 레코드 OPERATOR 특성 검사

사용자에게 OPERATOR 특성이 있으므로 CA Access Control 에서 기본 리소스에 대한 액세스를 허용했음을 나타냅니다. OPERATOR 특성을 사용하면 사용자가 read 및 chdir 액세스 요청과 관련해서 권한 부여 절차를 바이패스할 수 있습니다.

참고: CA Access Control 은 추적 파일에만 이 메시지를 쓰고 감사 로그 파일에는 메시지를 쓰지 않습니다.

1062 - 기본 레코드 클래스 전역 범용 액세스

CA Access Control 에서 리소스 클래스의 defaccess 값을 기준으로 CA Access Control 데이터베이스에 레코드가 없는 기본 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

1063 - 기본 레코드 프로그램 조건부 액세스

리소스 PACL 에 리소스에 액세스하는 프로그램이 나열되거나 나열되지 않으므로 CA Access Control 에서 기본 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

1064 - _default 레코드 ACL 에 있는 사용자 '*'

리소스 ACL 에 별표(*)가 포함되어 있으므로 CA Access Control 에서 기본 리소스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

참고: 별표는 정의된 모든 사용자를 지정합니다.

1069 - 기본 레코드에 대한 액세스 권한을 부여하는 규칙이 없습니다.

사용자가 리소스에 액세스할 수 있도록 허용하는 규칙이 없으므로 CA Access Control 에서 기본 리소스에 대한 액세스를 거부했음을 나타냅니다.

1202 - 경고 모드의 기본 레코드

리소스가 경고 모드에 있으므로 CA Access Control 에서 기본 리소스에 대한 액세스를 허용했음을 나타냅니다.

1250 - 기본 레코드가 언트러스트로 설정되었습니다.

CA Access Control 에서 언트러스트된 기본 프로그램 실행을 거부했음을 나타냅니다.

언트러스트 메시지 이벤트의 권한 부여 단계 코드

언트러스트 메시지 이벤트의 권한 부여 단계 코드에서는 CA Access Control 이 언트러스트 메시지 이벤트에 대해 수행할 작업을 결정한 단계를 설명합니다.

추가 정보:

언트러스트 메시지 이벤트 (페이지 493)

0 - Watchdog 파일을 검사하는 동안 일반적인 오류가 발생했습니다.

CA Access Control 이 파일 정보를 가져오는 동안 오류가 발생했음을 나타냅니다. 파일이 언트러스트되는 경우 CA Access Control 에서 감사 로그에 이 메시지를 쓸 수 있습니다. 자세한 내용은 시스템 로그를 참조하십시오.

1 - PROGRAM 또는 SECFILE 의 Stat 정보가 변경되었습니다.

PROGRAM 또는 SECFILE 클래스의 레코드에서 데이터가 변경되었음을 나타냅니다. 프로그램 또는 파일을 조작하려는 시도를 검색하면 CA Access Control 에서 감사 로그에 이 메시지를 쓸 수 있습니다. 프로그램 또는 파일에 대한 감사 이벤트, 시스템 로그 및 추적 레코드를 검사해야 합니다. 관리자가 프로그램 또는 파일을 변경한 경우 변경된 프로그램 또는 파일을 다시 트러스트합니다.

4 - PROGRAM 또는 SECFILE 의 CRC 검사가 변경되었습니다.

PROGRAM 또는 SECFILE 클래스의 레코드에 대한 CRC(순환 중복 검사)가 변경되었음을 나타냅니다. 프로그램 또는 파일에 대한 시스템 로그, 이벤트 로그 파일 및 추적 레코드를 검사해야 합니다.

5 - PROGRAM 또는 SECFILE 의 파일에 대해 stat 명령을 실행할 수 없습니다.

CA Access Control 이 지정된 파일에 대한 파일 정보를 검색하지 못했음을 나타냅니다. 다음 중 하나가 발생할 경우 CA Access Control 은 감사 로그에 이 메시지를 쓸 수 있습니다.

- 파일 이름 또는 디렉터리가 변경됨
- 파일 이름 또는 디렉터리가 존재하지 않음
- 파일의 액세스 권한
- 시스템 메모리 부족

가능한 오류 원인을 확인하려면 시스템 로그 파일을 검사합니다.

7 - PROGRAM 또는 SECFILE 의 MD5 서명이 변경되었습니다.

PROGRAM 또는 SECFILE 클래스의 레코드에 대한 MD5 서명이 변경되었음을 나타냅니다. 프로그램 또는 파일에 대한 시스템 로그 파일, 감사 메시지 및 추적 로그를 검사해야 합니다.

8 - PROGRAM 또는 SECFILE 의 SHA1 서명이 변경되었습니다.

PROGRAM 또는 SECFILE 클래스의 레코드에 대한 SHA1 서명이 변경되었음을 나타냅니다. 프로그램 또는 파일에 대한 시스템 로그 파일, 감사 메시지 및 추적 로그를 검사해야 합니다.

인바운드 네트워크 연결 이벤트의 권한 부여 단계 코드

인바운드 네트워크 연결 이벤트의 권한 부여 단계 코드에서는 CA Access Control 이 들어오는 네트워크 연결 이벤트에 대해 수행할 작업을 결정한 단계를 설명합니다.

추가 정보:

인바운드 네트워크 연결 이벤트 (페이지 496)

150 - 클래스 테이블 검사

CA Access Control 데이터베이스에서 클래스를 찾을 수 없음을 나타냅니다. CA Access Control 데이터베이스에 문제가 있는 경우 CA Access Control 에서 감사 로그에 이 메시지를 쓸 수 있습니다. 이 문제를 해결하려면 dbmgr 유틸리티를 사용하여 CA Access Control 데이터베이스를 다시 작성합니다.

중요! dbmgr 유틸리티는 문제를 해결하는 동안 지원 담당자의 안내가 있는 경우에만 사용합니다. 도움이 필요하면 기술 지원 부서(http://www.ca.com/worldwide)에 문의하십시오.

추가 정보:

dbmgr 유틸리티 (페이지 30)

153 - inetacl 에 있는 HOST 항목 별표

호스트 INETACL 에 별표(*)가 포함되어 있으므로 CA Access Control 에서 보호된 호스트의 연결을 허용 또는 거부했음을 나타냅니다.

참고: 별표는 0 개 이상의 문자 시퀀스를 지정하므로 INETACL 에 사용할 경우 모든 서비스와 일치합니다.

156 - HOST 항목 inetacl

호스트 INETACL 에 연결 서비스가 나열되므로 CA Access Control 에서 보호된 호스트의 연결을 허용 또는 거부했음을 나타냅니다.

157 - HOST 클래스 UACC

호스트 UACC 클래스에 대해 거부된 기본 액세스 권한 값으로 인해 CA Access Control 에서 보호된 호스트의 연결을 허용 또는 거부했음을 나타냅니다.

159 - HOST 항목 서비스 범위 ACL

연결 서비스가 호스트 INETACL 범위 내에 있으므로 CA Access Control 에서 보호된 호스트의 연결을 허용 또는 거부했음을 나타냅니다.

163 - 서비스에 대한 액세스 권한을 부여하는 규칙이 없습니다.

액세스를 허용하는 규칙을 찾지 못해 CA Access Control 에서 호스트의 연결을 거부했음을 나타냅니다. 해당 호스트에 대한 HOST 클래스 액세스 규칙을 검사해야 합니다.

164 - HOST 그룹 inetacl

GHOST 개체의 INETCAL 에 연결 서비스가 나열되므로 CA Access Control 에서 보호된 호스트의 연결을 허용 또는 거부했음을 나타냅니다.

165 - HOST 그룹 서비스 범위 ACL

연결 서비스가 호스트 그룹의 INETACL 범위 내에 있으므로 CA Access Control 에서 GHOST 호스트 그룹 개체의 구성원인 보호된 호스트의 연결을 허용 또는 거부했음을 나타냅니다.

166 - inetacl 에 있는 HOST 그룹 별표

호스트 그룹의 INETACL 에 별표(*)가 포함되어 있으므로 CA Access Control 에서 GHOST 호스트 그룹 개체의 구성원인 보호된 호스트의 연결을 허용 또는 거부했음을 나타냅니다.

참고: 별표는 0 개 이상의 문자 시퀀스를 지정하므로 INETACL 에 사용할 경우 모든 서비스와 일치합니다.

167 - HOSTNET(네트워크 또는 IP 마스크/일치) inetacl

HOSTNET 레코드의 INETACL 에 연결 서비스가 나열되므로 CA Access Control 에서 보호된 호스트의 연결을 허용 또는 거부했음을 나타냅니다.

168 - HOSTNET(네트워크 또는 IP 마스크/일치) 서비스 범위

연결 서비스가 호스트 HOSTNET 레코드 INETACL 범위 내에 있으므로 CA Access Control 에서 보호된 호스트의 연결을 허용 또는 거부했음을 나타냅니다.

169 - HOSTNET(네트워크 또는 IP 마스크/일치) inetacl 별표

HOSTNET 레코드 INETACL 에 별표(*)가 포함되어 있으므로 CA Access Control 에서 보호된 호스트의 연결을 허용 또는 거부했음을 나타냅니다.

참고: 별표는 0 개 이상의 문자 시퀀스를 지정하므로 INETACL 에 사용할 경우 모든 서비스와 일치합니다.

170 - HOSTNP(호스트 이름 패턴) inetacl

HOSTNP 레코드의 INETACL 에 연결 서비스가 나열되므로 CA Access Control 에서 보호된 호스트의 연결을 허용 또는 거부했음을 나타냅니다.

171 - HOSTNP(호스트 이름 패턴) 서비스 범위

연결 서비스가 호스트 HOSTNP 레코드 INETACL 범위 내에 있으므로 CA Access Control 에서 보호된 호스트의 연결을 허용 또는 거부했음을 나타냅니다.

172 - HOSTNP(호스트 이름 패턴) inetacl 별표

HOSTNP 레코드 INETACL 에 별표(*)가 포함되어 있으므로 CA Access Control 에서 보호된 호스트의 연결을 허용 또는 거부했음을 나타냅니다.

참고: 별표는 0 개 이상의 문자 시퀀스를 지정하므로 INETACL 에 사용할 경우 모든 서비스와 일치합니다.

173 - HOST 항목 요일 & 시간 제한

시도된 액세스가 HOST 레코드의 요일 및 시간 제한을 벗어났으므로 CA Access Control 에서 보호된 호스트에 대한 액세스를 거부했음을 나타냅니다.

174 - HOST 그룹 요일 & 시간 제한

GHOST 레코드의 요일 및 시간 제한으로 인해 CA Access Control 에서 보호된 호스트 그룹에 대한 액세스를 거부했음을 나타냅니다.

175 - HOSTNET(네트워크 또는 IP 마스크/일치) 요일 및 시간 제한

HOSTNET 레코드의 요일 및 시간 제한으로 인해 CA Access Control 에서 보호된 호스트에 대한 액세스를 거부했음을 나타냅니다.

176 - HOSTNP(호스트 이름 패턴) 요일 및 시간 제한

HOSTNP 레코드의 요일 및 시간 제한으로 인해 CA Access Control 에서 보호된 호스트에 대한 액세스를 거부했음을 나타냅니다.

177 - HOST_default 요일 및 시간 제한

HOST _default 레코드의 요일 및 시간 제한으로 인해 CA Access Control 에서 보호된 호스트에 대한 액세스를 거부했음을 나타냅니다.

178 - HOST_default inetacl

HOST _default INETACL 의 값으로 인해 CA Access Control 에서 보호된 호스트에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

179 - HOST_default 서비스 범위

연결 서비스가 HOST _default 레코드 INETACL 범위 내에 있으므로 CA Access Control 에서 보호된 호스트에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

180 - HOST_default 서비스 별표

HOST _default 레코드 INETACL 에 별표(*)가 포함되어 있으므로 CA Access Control 에서 보호된 호스트에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

참고: 별표는 0 개 이상의 문자 시퀀스를 지정하므로 INETACL 에 사용할 경우 모든 서비스와 일치합니다.

404 - TCP 서비스 ACL 에 있는 HOST 항목

TCP 레코드 ACL 에 HOST 가 나열되므로 CA Access Control 에서 HOST 의 액세스를 허용 또는 거부했음을 나타냅니다.

405 - TCP 서비스 ACL 에 있는 GHOST 항목

TCP 레코드 ACL 에 HOST 가 구성원으로 속해 있는 GHOST 가 나열되므로 CA Access Control 에서 HOST 의 액세스를 허용 또는 거부했음을 나타냅니다.

406 - TCP 서비스 ACL 에 있는 HOSTNET 항목

TCP 레코드 ACL 에 HOST 가 속해 있는 HOSTNET 네트워크가 나열되므로 CA Access Control 에서 HOST 의 액세스를 허용 또는 거부했음을 나타냅니다.

407 - TCP 서비스 ACL 에 있는 HOSTNP 항목

TCP 레코드 ACL 에 HOST 가 속해 있는 HOSTNP 집합이 나열되므로 CA Access Control 에서 HOST 의 액세스를 허용 또는 거부했음을 나타냅니다.

아웃바운드 네트워크 연결 이벤트의 권한 부여 단계 코드

아웃바운드 네트워크 연결 이벤트의 권한 부여 단계 코드에서는 CA Access Control 이 아웃바운드 네트워크 연결 이벤트에 대해 수행할 작업을 결정한 단계를 설명합니다.

추가 정보:

아웃바운드 네트워크 연결 이벤트 (페이지 498)

400 - 클래스 TCP 의 _default 서비스

연결 서비스에 대한 TCP 레코드의 _default 개체 권한으로 인해 CA Access Control 에서 보호된 호스트에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

401 - TCP 서비스의 클래스 UACC

UACC 클래스에 있는 TCP 개체의 값으로 인해 CA Access Control 에서 보호된 호스트에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

402 - TCP 서비스의 요일 및 시간 제한

TCP 레코드의 요일 및 시간 제한으로 인해 CA Access Control 에서 TCP 서비스에 대한 액세스를 거부했음을 나타냅니다.

403 - TCP 서비스의 ACL 읽기 단계

TCP 레코드의 ACL 읽기 속성으로 인해 CA Access Control 에서 TCP 서비스에 대한 액세스를 허용 또는 거부했음을 나타냅니다. 데이터베이스가 손상된 경우 CA Access Control 에서 감사 로그에 이 메시지를 쓸 수 있습니다.

408 - TCP 서비스의 기본 액세스

TCP 레코드의 defaccess 속성으로 인해 CA Access Control 에서 TCP 클래스 서비스에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

참고: 이 이벤트 메시지는 HOST 에 대한 인바운드 연결을 나타내기 위해 들어오는 TCP 이벤트에도 적용됩니다.

409 - TCP 서비스의 CACL 읽기 단계

TCP 레코드의 CACL 읽기 속성으로 인해 CA Access Control 에서 TCP 서비스에 대한 액세스를 거부했음을 나타냅니다. 데이터베이스가 손상된 경우 CA Access Control 에서 감사 로그에 이 메시지를 쓸 수 있습니다.

410 - TCP 서비스 CACL 에 있는 USER 의 HOST 항목

CA Access Control 에서 지정된 USER 또는 XUSER 의 HOST 개체에 대한 액세스를 허용 또는 거부했음을 나타냅니다. CA Access Control 은 TCP 서비스의 CACL 에 있는 액세스 규칙을 사용하여 액세스를 허용 또는 거부할지를 결정했습니다.

411 - TCP 서비스 CACL 에 있는 USER 의 GHOST 항목

CA Access Control 에서 지정된 USER 또는 XUSER 개체의 GHOST 개체에 대한 액세스를 허용 또는 거부했음을 나타냅니다. CA Access Control 은 TCP 서비스의 CACL 에 있는 액세스 규칙을 사용하여 액세스를 허용 또는 거부할지를 결정했습니다.

412 - TCP 서비스 CACL 에 있는 USER 의 HOSTNET 항목

CA Access Control 에서 지정된 USER 또는 XUSER 개체의 HOSTNET 개체에 대한 액세스를 허용 또는 거부했음을 나타냅니다. CA Access Control 은 TCP 서비스의 CACL 에 있는 액세스 규칙을 사용하여 액세스를 허용 또는 거부할지를 결정했습니다.

413 - TCP 서비스 CACL 에 있는 USER 의 HOSTNP 항목

CA Access Control 에서 지정된 USER 또는 XUSER 개체의 HOSTNP 개체에 대한 액세스를 허용 또는 거부했음을 나타냅니다. CA Access Control 은 TCP 서비스의 CACL 에 있는 액세스 규칙을 사용하여 액세스를 허용 또는 거부할지를 결정했습니다.

414 - TCP 서비스 CACL 에 있는 GROUP 의 HOST 항목

CA Access Control 에서 지정된 GROUP 또는 XGROUP 개체의 HOST 개체에 대한 액세스를 허용 또는 거부했음을 나타냅니다. CA Access Control 은 TCP 서비스의 CACL 에 있는 액세스 규칙을 사용하여 액세스를 허용 또는 거부할지를 결정했습니다.

415 - TCP 서비스 CACL 에 있는 GROUP 의 GHOST 항목

CA Access Control 에서 지정된 GROUP 또는 XGROUP 개체의 GHOST 개체에 대한 액세스를 허용 또는 거부했음을 나타냅니다. CA Access Control 은 TCP 서비스의 CACL 에 있는 액세스 규칙을 사용하여 액세스를 허용 또는 거부할지를 결정했습니다.

416 - TCP 서비스 CACL 에 있는 GROUP 의 HOSTNET 항목

CA Access Control 에서 지정된 GROUP 또는 XGROUP 개체의 HOSTNET 개체에 대한 액세스를 허용 또는 거부했음을 나타냅니다. CA Access Control 은 TCP 서비스의 CACL 에 있는 액세스 규칙을 사용하여 액세스를 허용 또는 거부할지를 결정했습니다.

417 - TCP 서비스 CACL 에 있는 GROUP 의 HOSTNP 항목

CA Access Control 에서 지정된 GROUP 또는 XGROUP 개체의 HOSTNP 개체에 대한 액세스를 허용 또는 거부했음을 나타냅니다. CA Access Control 은 TCP 서비스의 CACL 에 있는 액세스 규칙을 사용하여 액세스를 허용 또는 거부할지를 결정했습니다.

418 - TCP 서비스 CACL 에 있는 사용자 '*'의 HOST 항목

HOST 레코드 CACL 에 별표(*)가 포함되어 있으므로 CA Access Control 에서 사용자의 HOST 에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

참고: 별표는 정의된 모든 사용자를 지정합니다.

419 - TCP 서비스 CACL 에 있는 사용자 '*'의 GHOST 항목

GHOST 레코드 CACL 에 별표(*)가 포함되어 있으므로 CA Access Control 에서 사용자의 GHOST 클래스에 속해 있는 HOST 에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

참고: 별표는 정의된 모든 사용자를 지정합니다.

420 - TCP 서비스에 있는 사용자 '*'의 HOSTNET 항목

HOSTNET 레코드 CACL 에 별표(*)가 포함되어 있으므로 CA Access Control 에서 사용자의 HOSTNET 개체에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

참고: 별표는 정의된 모든 사용자를 지정합니다.

421 - TCP 서비스 CACL 에 있는 사용자 '*'의 HOSTNP 항목

HOSTNP 레코드 CACL 에 별표(*)가 포함되어 있으므로 CA Access Control 에서 사용자의 HOSTNET 개체에 대한 액세스를 허용 또는 거부했음을 나타냅니다.

참고: 별표는 정의된 모든 사용자를 지정합니다.

보안 데이터베이스 관리 이벤트의 권한 부여 단계 코드

보안 데이터베이스 관리 이벤트의 권한 부여 단계 코드에서는 CA Access Control 이 보안 데이터베이스 관리 이벤트에 대해 수행할 작업을 결정한 단계를 설명합니다.

추가 정보:

보안 데이터베이스 관리 이벤트 (페이지 501)

300 - 정의되지 않은 CA Access Control 사용자

CA Access Control 데이터베이스에서 액세스하는 사용자를 찾을 수 없으므로 CA Access Control 에서 시스템에 대한 액세스를 거부했음을 나타냅니다. 사용자 계정 프로필을 검사해야 합니다.

301 - 마지막 ADMIN 사용자를 삭제하려고 합니다.

CA Access Control 에서 다음 중 하나의 수행 요청을 거부했음을 나타냅니다.

- CA Access Control 데이터베이스에서 마지막 ADMIN 사용자 삭제
- ADMIN 속성이 할당된 유일한 사용자로부터 ADMIN 속성 제거

302 - 루트 사용자를 삭제하려고 합니다.

UNIX 에 해당

CA Access Control 에서 시스템 루트 계정 삭제 시도를 거부했음을 나타냅니다.

303 - 사용자가 암호를 변경하려고 합니다.

CA Access Control 에서 selang 명령을 사용하여 암호를 변경하려는 사용자 시도를 거부했음을 나타냅니다. UNIX 에서는 sepass 유틸리티를 사용하여 암호를 변경할 수 있습니다. Windows 에서는 네이티브 암호 관리 도구를 사용하여 암호를 변경할 수 있습니다.

304 - 감사자가 아닌 사용자가 감사 모드를 설정하려고 합니다.

사용자에게 AUDITOR 특성이 없으므로 CA Access Control 에서 레코드의 감사 모드를 변경하는 사용자 시도를 거부했음을 나타냅니다. 사용자가 레코드의 감사 모드를 변경할 수 있도록 하려면 사용자에게 AUDITOR 특성을 할당합니다.

305 - ADMIN 사용자에 대해 허용된 명령

작업을 요청하는 사용자에게 ADMIN 특성이 있으므로 CA Access Control 에서 작업을 허용했음을 나타냅니다.

306 - Showuser (myself) , Showxusr 허용

CA Access Control 에서 사용자 또는 외부 사용자가 CA Access Control 데이터베이스에 있는 해당 레코드의 속성을 표시할 수 있도록 허용했음을 나타냅니다.

참고: 이 메시지는 감사 레코드로 기록되지 않습니다.

307 - 사용자가 소유하지 않은 범주를 설정하려고 합니다.

보안 범주를 할당하려는 사용자가 해당 보안 범주를 소유하고 있지 않으므로 CA Access Control 에서 사용자의 보안 범주 할당 시도를 거부했음을 나타냅니다.

308 - 사용자가 소유하지 않은 보안 레이블을 설정하려고 합니다.

보안 레이블을 할당하려는 사용자가 해당 보안 레이블을 소유하고 있지 않으므로 CA Access Control 에서 사용자의 보안 레이블 할당 시도를 거부했음을 나타냅니다.

309 - 사용자가 자신의 보안 수준보다 높은 보안 수준을 설정하려고 합니다.

사용자의 보안 수준이 이 사용자가 할당하려는 보안 수준보다 낮으므로 CA Access Control 에서 사용자의 보안 수준 할당 시도를 거부했음을 나타냅니다.

310 - ADMIN 이 아닌 사용자가 사용자 모드를 설정하려고 합니다.

특성을 설정하려는 사용자에게 ADMIN 특성이 없으므로 CA Access Control 에서 관리 특성 설정 시도를 거부했음을 나타냅니다.

311 - 개체 소유자에 대해 허용된 명령

사용자가 레코드를 소유하고 있으므로 CA Access Control 에서 작업을 허용했음을 나타냅니다.

312 - 네이티브 파일 소유자는 CA Access Control 로 정의할 수 있습니다.

UNIX 에 해당

파일 소유자가 파일을 CA Access Control 로 정의했으므로 CA Access Control 에서 작업을 허용했음을 나타냅니다.

참고: 파일 소유자는 seos.ini 파일의 lang 섹션에 있는 use_unix_file_owner 토큰이 yes 로 설정된 경우 파일을 CA Access Control 로 정의할 수 있습니다.

313 - GROUP-ADMIN 사용자에 대해 허용된 명령

CA Access Control 에서 GROUP-ADMIN 특성을 가진 사용자가 그룹 내의 레코드를 수정할 수 있도록 허용했음을 나타냅니다.

314 - GROUP-ADMIN 사용자는 그룹에 가입/가입 취소시킬 수 있습니다.

CA Access Control 에서 GROUP-ADMIN 특성을 가진 사용자가 그룹에 사용자를 추가하거나 제거할 수 있도록 허용했음을 나타냅니다.

315 - GROUP-AUDITOR/ADMIN 은 그룹을 나열할 수 있습니다.

사용자에게 해당 그룹에 대한 GROUP-ADMIN 또는 GROUP-AUDITOR 특성이 있으므로 CA Access Control 에서 사용자가 그룹 내의 레코드 속성을 나열할 수 있도록 허용했음을 나타냅니다.

316 - 감사자는 모든 개체를 나열할 수 있습니다.

CA Access Control 에서 AUDITOR 특성을 가진 사용자가 데이터베이스의 데이터를 표시할 수 있도록 허용했음을 나타냅니다.

317 - OPERATOR 는 모든 개체를 나열할 수 있습니다.

CA Access Control 에서 OPERATOR 특성을 가진 사용자가 데이터베이스의 데이터를 표시할 수 있도록 허용했음을 나타냅니다.

318 - GROUP-AUDITOR 는 그룹 범위 내의 개체를 나열할 수 있습니다.

CA Access Control 에서 GROUP-AUDITOR 특성을 가진 사용자가 데이터베이스의 그룹 데이터를 표시할 수 있도록 허용했음을 나타냅니다.

319 - GROUP-OPERATOR 는 그룹 범위 내의 개체를 나열할 수 있습니다.

CA Access Control 에서 GROUP-OPERATOR 특성을 가진 사용자가 데이터베이스의 그룹 데이터를 표시할 수 있도록 허용했음을 나타냅니다.

320 - CLASS-ADMIN 사용자에 대해 허용된 명령

ADMIN 클래스의 ACL 에 나열된 사용자가 작업을 수행했으므로 CA Access Control 에서 작업을 허용했음을 나타냅니다.

321 - 액세스 권한을 가진 PWMANAGER/ADMIN 에 대해 허용된 명령

사용자에게 PWMANAGER 또는 ADMIN 특성이 있으므로 CA Access Control 에서 사용자의 암호 변경을 허용했음을 나타냅니다.

322 - 이 작업을 허용하는 규칙이 없습니다.

작업을 허용한 규칙이 없으므로 CA Access Control 에서 작업을 거부했음을 나타냅니다.

324 - 사용자는 sepass 를 사용하여 암호를 변경할 수 있습니다.

CA Access Control 에서 사용자가 sepass 유틸리티나 암호 정책 모델을 사용하여 암호를 변경할 수 있도록 허용했음을 나타냅니다.

326 - 사용자가 직접 '로그인 정보'를 작성했습니다.

CA Access Control 에서 사용자가 직접 로그인 정보를 작성할 수 있도록 허용했음을 나타냅니다.

327 - GROUP-PWMANAGER 에 대해 허용된 명령

명령을 실행한 사용자에게 GROUP-PWMANAGER 특성이 있으므로 CA Access Control 에서 명령을 허용했음을 나타냅니다.

329 - PWMANAGER 가 사용자를 활성화했습니다.

다른 사용자를 활성화한 사용자에게 PWMANAGER 특성이 있으므로 CA Access Control 에서 사용자가 다른 사용자를 활성화(다시 활성화)할 수 있도록 허용했음을 나타냅니다.

330 - DOMAIN 변경에 허용된 명령

Windows 에 해당

CA Access Control 에서 사용자가 DOMAIN 클래스를 변경할 수 있도록(예: 도메인에 새 컴퓨터 추가) 허용했음을 나타냅니다.

331 - PWMANAGER 에 대해 허용된 명령

명령을 실행한 사용자에게 PWMANAGER 특성이 있으므로 CA Access Control 에서 명령 실행을 허용했음을 나타냅니다.

332 - PWMANAGER 에 대해 허용된 네이티브 플래그 변경

Windows 에 해당

사용자에게 PWMANAGER 특성이 있으므로 CA Access Control 에서 사용자가 사용자 계정에 할당된 계정 플래그를 수정할 수 있도록 허용했음을 나타냅니다.

333 - PWMANAGER 는 '다음 로그온할 때 반드시 암호 변경' 특성을 변경할 수 있습니다.

Windows 에 해당

사용자에게 PWMANAGER 특성이 있으므로 CA Access Control 에서 사용자가 사용자 계정에 대해 '다음 로그온할 때 반드시 암호 변경' 특성을 수정할 수 있도록 허용했음을 나타냅니다.

334 - GROUP-PWMANAGER 에 대해 허용된 명령

명령을 실행한 사용자에게 GROUP-PWMANAGER 특성이 있으므로 CA Access Control 에서 명령을 허용했음을 나타냅니다.

335 - PWMANAGER 는 '로그인 정보'를 편집할 수 있습니다.

사용자에게 PWMANAGER 특성이 있으므로 CA Access Control 에서 사용자가 사용자 계정에 대해 '로그인 정보' 특성을 편집할 수 있도록 허용했음을 나타냅니다.

336 - 감사자 사용자에 대해 허용된 명령

사용자에게 AUDITOR 특성이 있으므로 CA Access Control 에서 사용자의 명령 실행을 허용했음을 나타냅니다.

337 - 데이터베이스 정보와 명령을 조정하지 못했습니다.

명령에 포함된 개체가 CA Access Control 데이터베이스에 없어 CA Access Control 에서 명령을 실행하지 않았음을 나타냅니다. 명령을 다시 실행하기 전에 명령 구문을 검사해야 합니다.

338 - 암시적 요청에 따라 명령 생성

CA Access Control 이 암시적 요청에 따라 명령을 만들었음을 나타냅니다.

339 - SEOS_syscall 모듈 언로드 준비 검사

UNIX 에 해당

접근자가 차단된 syscall 에서 실행 중인 프로세스가 있는지 확인하기 위해 'secons –scl' 명령을 실행하고 있음을 나타냅니다. CA Access Control 은 SEOS_syscall 모듈 언로드를 허용하지 않습니다.

종료 이벤트의 권한 부여 단계 코드

종료 이벤트의 권한 부여 단계 코드에서는 CA Access Control 이 종료 이벤트에 대해 수행할 작업을 결정한 단계를 설명합니다.

추가 정보:

종료 이벤트 (페이지 505)

451 - OPERATOR 인 사용자

종료 시퀀스를 실행한 사용자에게 OPERATOR 특성이 있으므로 CA Access Control 에서 종료 요청을 허용했음을 나타냅니다.

452 - ADMIN 또는 SPECIAL 인 사용자

종료 시퀀스를 실행한 사용자에게 ADMIN 특성이 할당되어 있으므로 CA Access Control 에서 종료 요청을 허용했음을 나타냅니다.

453 - _seagent 는 CA Access Control 을 종료할 수 있습니다.

UNIX 에 해당

_seagent 는 CA Access Control 을 종료할 수 있으므로 CA Access Control 에서 종료 요청을 허용했음을 나타냅니다.

460 - 사용자가 CA Access Control 을 종료할 수 없습니다.

요청하는 사용자가 CA Access Control 을 종료할 수 없으므로 CA Access Control 에서 종료 요청을 거부했음을 나타냅니다.

암호 확인 이벤트의 권한 부여 단계 코드

암호 확인 이벤트의 권한 부여 단계 코드에서는 CA Access Control 이 암호 확인 이벤트에 대해 수행할 작업을 결정한 단계를 설명합니다.

추가 정보:

암호 확인 이벤트 (페이지 508)

0 - 암호 품질을 확인했습니다.

사용자가 성공적으로 암호를 변경했으며 새 암호가 모든 암호 품질 규칙을 충족함을 나타냅니다.

1 - 암호가 너무 짧습니다.

새 암호의 길이가 최소 암호 길이에 대한 암호 정책을 준수하지 않아 암호 변경에 실패했음을 나타냅니다.

2 - 암호에 사용자 이름이 포함되어 있습니다.

새 암호에 사용자의 사용자 이름이 포함되어 암호 변경에 실패했음을 나타냅니다.

3 - 암호에 소문자가 너무 적습니다.

암호 정책에 정의된 최소값에 따라 새 암호에 포함된 소문자 개수가 충분하지 않아 암호 변경에 실패했음을 나타냅니다.

4 - 암호에 대문자가 너무 적습니다.

암호 정책에 정의된 최소값에 따라 새 암호에 포함된 대문자 개수가 충분하지 않아 암호 변경에 실패했음을 나타냅니다.

5 - 암호에 숫자가 너무 적습니다.

암호 정책에 정의된 최소값에 따라 새 암호에 포함된 숫자 개수가 충분하지 않아 암호 변경에 실패했음을 나타냅니다.

6 - 암호에 다른 문자가 너무 적습니다.

암호 정책에 정의된 최소값에 따라 새 암호에 포함된 다른 문자 개수가 충분하지 않아 암호 변경에 실패했음을 나타냅니다.

7 - 암호에 동일한 문자의 중복이 너무 많습니다.

암호 정책에 정의된 최대값에 따라 새 암호에 포함된 중복 문자가 너무 많아 암호 변경에 실패했음을 나타냅니다.

8 - 현재 암호와 같습니다.

새 암호가 현재 암호와 같아 암호 변경에 실패했음을 나타냅니다. 이전에 사용하지 않은 암호를 선택해야 합니다.

9 - 이미 사용된 암호입니다. 다른 암호를 선택하십시오.

새 암호가 이미 사용된 암호이므로 암호 변경에 실패했음을 나타냅니다. 이전에 사용하지 않은 암호를 선택해야 합니다.

10 - 암호에 영문자가 너무 적습니다.

암호 정책에 정의된 최소값에 따라 새 암호에 포함된 영문자 개수가 충분하지 않아 암호 변경에 실패했음을 나타냅니다.

11 - 암호에 영숫자가 너무 적습니다.

암호 정책에 정의된 최소값에 따라 새 암호에 포함된 영숫자 문자 개수가 충분하지 않아 암호 변경에 실패했음을 나타냅니다.

12 - 암호가 최근에 변경되어 현재 다시 변경할 수 없습니다.

암호가 최근에 변경되었으며 현재 변경할 수 없으므로 암호 변경에 실패했음을 나타냅니다. 암호 정책에 정의된 최소값에 따라 최소 암호 사용 기간이 경과한 후에만 암호를 변경해야 합니다.

13 - 암호가 이전 암호에 포함되어 있거나 그 반대입니다.

새 암호가 이전 암호를 포함하거나 이전 암호의 일부이므로 암호 변경에 실패했음을 나타냅니다. 새 암호가 이전 암호를 포함하지 않으며 이전 암호의 일부가 아니도록 해야 합니다.

16 - 암호가 너무 깁니다.

암호 정책에 정의된 최대값에 따라 새 암호가 너무 길어 암호 변경에 실패했음을 나타냅니다.

20 - 암호가 일치하지 않습니다.

새 암호가 암호 확인 필드에 입력된 암호와 일치하지 않아 암호 변경에 실패했음을 나타냅니다.

21 - 미리 정의된 금지 문자를 포함할 수 없습니다.

암호 정책에 따라 새 암호에 금지 문자가 포함되어 있어 암호 변경에 실패했음을 나타냅니다.

22 - 이미 사용된 암호입니다.

입력한 암호가 이미 사용되었으므로 CA Access Control 에서 액세스를 거부했음을 나타냅니다. 사용하는 새 암호가 암호 정책 규칙을 준수하는지 확인하십시오.

23 - 암호가 이전 암호에 포함되어 있거나 그 반대입니다.

사용한 암호가 이전 암호에 포함되어 있거나 이전 암호가 새 암호에 포함되어 있어 암호 변경에 실패했음을 나타냅니다. 이미 사용된 암호를 포함하지 않는 새 암호를 선택해야 합니다.

24 - 암호가 사전 파일에 있습니다.

새 암호가 DICTIONARY 클래스 또는 DICTIONARY 파일에 정의되어 있어 암호 변경에 실패했음을 나타냅니다. DICTIONARY 클래스 또는 DICTIONARY 파일에 정의되지 않은 암호를 선택해야 합니다.

100 - 잘못된 인수

잘못된 데이터가 권한 부여 엔진으로 전송되어 암호 변경에 실패했음을 나타냅니다.

다음 중 하나가 발생할 경우 CA Access Control 에서 감사 로그에 이 메시지를 쓸 수 있습니다.

- 메모리 문제
- CA Access Control 최신 업그레이드에 대한 여러 CA Access Control 모듈 버전 간의 불일치

혼합된 CA Access Control 환경이 없는지, 그리고 클라이언트와 서버가 같은 버전의 CA Access Control 을 사용하는지 확인하십시오. 도움이 필요하면 기술 지원 부서(http://www.ca.com/worldwide)에 문의하십시오.

사용자에 대한 추적 메시지의 권한 부여 단계 코드

사용자에 대한 추적 이벤트의 권한 부여 단계 코드에서는 CA Access Control 이 사용자 활동 이벤트에 대해 수행할 작업을 결정한 단계를 설명합니다.

추가 정보:

사용자에 대한 추적 메시지 (페이지 510)

994 - 정보 메시지

사용자가 추적 감사 레코드에 액세스했음을 나타냅니다.

참고: 이 메시지는 정보를 제공하기 위한 것이며 seaudit –tr 명령을 실행하여 볼 수 있습니다.

995 - 내부 리소스에 대한 무단 액세스

접근자가 내부적으로 보호된 FILE 리소스에 대한 무단 액세스를 시도했음을 나타냅니다. 예를 들어 seos.audit 레코드 등이 있습니다.

996 - 내부 리소스에 대한 권한 있는 액세스

CA Access Control 에서 내부 바이패스를 통해 리소스에 대한 액세스를 허용했음을 나타냅니다. 예를 들어 reading /etc/passwd 등이 있습니다.

997 - 사용자가 setuid\setgid 디렉터리를 실행할 수 있습니다.

UNIX 만 해당

접근자가 setuid\setgid 플래그 비트로 표시된 디렉터리를 실행하려고 했으므로 CA Access Control 에서 이벤트를 바이패스했음을 나타냅니다. 이 단계는 TRACE 레코드 메시지의 일부입니다.

998 - 권한 부여가 '감사 모드 전용'으로 구성되어 있습니다.

Windows 전용

CA Access Control 이 '감사 모드 전용'으로 작동하도록 설정되었음을 나타냅니다.

999 - 리소스가 보호되지 않습니다. 규칙이 있는지 확인하십시오.

CA Access Control 에서 보호되지 않은 리소스에 대한 액세스를 허용함을 나타냅니다.

레코드가 작성된 이유를 지정하는 사유 코드

레코드가 작성된 이유를 지정하는 사유 코드는 CA Access Control 이 이벤트에 대해 만들 감사 레코드를 결정한 단계를 설명합니다.

0 - 작업 로그에 대한 특정 요청이 없습니다.

작업 로그에 대한 특정 요청이 없으므로 CA Access Control 에서 기본적으로 이 작업을 기록했음을 나타냅니다.

2 - 사용자 감사 모드에 로깅이 필요합니다.

접근자의 감사 속성이나 해당 프로필이 레코드 결과와 일치하므로 CA Access Control 에서 작업을 기록했음을 나타냅니다. 예를 들어 AUDIT_MODE 속성 값이 FAILURE 로 설정된 사용자가 수행하는 작업은 보호된 리소스에 액세스하지 못한 경우에만 기록됩니다.

3 - 리소스 감사 모드에 로깅이 필요합니다.

리소스의 RAUDIT 속성이 레코드 결과와 일치하므로 CA Access Control 에서 작업을 기록했음을 나타냅니다.

4 - 경고 모드의 리소스

경고 속성이 리소스 또는 리소스의 클래스로 설정되어 CA Access Control 에서 이 작업을 기록했음을 나타냅니다.

5 - CA Access Control serevu 유틸리티에서 감사를 요청했습니다.

UNIX 에 해당

serevu 유틸리티에서 감사 레코드를 요청했으므로, 예를 들어 사용자의 로그인 시도가 실패할 경우 CA Access Control 에서 이 작업을 기록했음을 나타냅니다.

7 - 아웃바운드 연결 레코드

UNIX 에 해당

아웃바운드 연결에 성공하여 CA Access Control 에서 이 작업을 기록했음을 나타냅니다.

8 - CA Access Control pam 지원 UNIX 로그인 실패

UNIX 에 해당

CA Access Control PAM 모듈에서 감사를 요청했으므로, 예를 들어 암호 로그인 시도가 실패할 경우 CA Access Control 에서 이 작업을 기록했음을 나타냅니다.

9 - CALENDAR 클래스의 Daytime 제한 검사

CALENDAR 클래스의 daytime 제한 검사에 감사 레코드 로깅이 필요하므로 CA Access Control 에서 이 메시지를 기록했음을 나타냅니다.

10 - 작업 로그에 대한 특정 요청

CA Access Control 데몬 종료 시도 등의 작업 로그에 대한 특정 요청 때문에 CA Access Control 에서 이 작업을 기록했음을 나타냅니다.

11 - CA Access Control secons 유틸리티에서 감사를 요청했습니다.

UNIX 에 해당

Syscall 모니터 옵션이 실행되어(secons-scl) CA Access Control 에서 이 작업을 기록했음을 나타냅니다.

부록 B: 추적 메시지

이 장은 아래의 주제를 포함하고 있습니다.

규칙 (페이지 551)
메시지 (페이지 551)

규칙

모든 메시지는 맨 처음이 날짜 및 시간으로 시작되며, 그 뒤에 대문자로 된 이벤트 유형 단어와 :, ! 또는 > 등의 기호가 옵니다. 다음 표에는 각 기호의 의미가 설명되어 있습니다.

:

CA Access Control 이 이벤트 신호를 받았으며 동작을 수행했습니다.

>

CA Access Control 이 D(거부), P(허용) 또는 BYPASS 의 권한 부여 결정을 내렸습니다. 이벤트는 액세스 규칙을 해석할 필요가 없습니다(예: 동일한 UID 에 대한 setuid 요청을 현재 UID 로 해석).

!

CA Access Control 이 오류를 발견했습니다(예: 알 수 없는 프로세스에서 온 요청).

메시지

앞에서 설명한 기호는 이 절에서 설명하는 이벤트 인수 앞에 나옵니다.

ACTION : CA Access Control 에서 P=ppp 을(를) 중지했습니다.

CA Access Control 이 setuid 또는 로그인 요청을 거부하고 예방 조치로 요청 프로세스(ppp)를 중단했습니다.

경보입니다. Uid uuu 이(가) 시스템을 위반했습니다!!!

알 수 없는 프로세스가 fork, exec 또는 setuid 와 같은 요청을 했습니다. 이 프로세스는 CA Access Control 이 알지 못하는 프로세스이며, 프로세스에 할당된 UID 는 시스템의 다른 프로세스에 할당되어 있지 않습니다. 이것은 사용자가 CA Access Control 에 통보하지 않고 로그인했음을 의미합니다. 소프트웨어 버그로 인해 또는 CA Access Control 이 현재 프로세스 상태를 검색한 직후 초기화를 완료하기 전에 사용자가 로그인한 경우 이런 상황이 발생할 수 있습니다.

APIAUTH ! P=ppp U=uuu ChangePasswd(user) Error 0xerr

사용자 uuu 와 연결된 프로세스 ppp 가 user 의 암호를 변경하려고 합니다. 이 요청의 결과가 16 진수로 지정된 코드에 오류가 있습니다. semsgtool 유틸리티를 사용하여 오류의 원인을 파악하십시오.

APIAUTH ! P=ppp U=uuu CheckPasswd(user) Error 0xerr

사용자 uuu 와 연결된 프로세스 ppp 가 user 에 대한 새 암호의 유효성을 확인하려고 합니다. 이 요청의 결과가 16 진수로 지정된 코드에 오류가 있습니다. semsgtool 유틸리티를 사용하여 오류의 원인을 파악하십시오.

APIAUTH ! P=ppp U=uuu Error, Unknown API Service nnn

프로세스 ppp 가 응용 프로그램 인터페이스를 사용하며, 사용자 오류로 인해 CA Access Control 프로그래밍 인터페이스가 지원하지 않는 서비스 코드를 전달했습니다. 오류의 원인을 확인하고 소스를 수정하여 다시 컴파일합니다.

APIAUTH ! P=ppp U=uuu GeneralResourceProc 오류 nnn >description

UID uuu 로 실행되는 프로세스 ppp 가 일반 리소스에 액세스하려고 요청했지만 지정한 리소스를 확인할 수 없습니다. 지정한 클래스가 정의되어 있지 않거나, 사용자 오류로 인해 지정한 액세스를 알 수 없습니다. 코드를 확인하고 수정한 다음 다시 컴파일합니다.

APIAUTH ! P=ppp U=uuu in VerifyCreate only for ROOT

UID uuu 로 실행되는 프로세스 ppp 가 ACEE 를 생성하기 위해 VerifyCreate 요청을 실행했습니다. 이 작업은 UID 0(root)과 연결된 멀티 사용자 프로세스에만 허용됩니다.

지정된 프로세스가 멀티 사용자 프로세스로 실행되어야 하는 경우 root 권한을 사용하여 프로세스를 다시 실행하십시오. 그렇지 않은 경우 프로세스가 요청을 실행한 이유를 확인하십시오.

APIAUTH : P=ppp U=uuu in VerifyDelete only for ROOT

UID uuu 로 실행되는 프로세스 ppp 가 ACEE 를 제거하기 위해 VerifyDelete 요청을 실행했습니다. 이 작업은 UID 0(root)과 연결된 멀티 사용자 프로세스에만 허용됩니다.

지정된 프로세스가 멀티 사용자 프로세스로 실행되어야 하는 경우 root 권한을 사용하여 프로세스를 다시 실행하십시오. 그렇지 않은 경우 프로세스가 요청을 실행한 이유를 확인하십시오.

APIAUTH ! P=ppp U=uuu LoginProc 오류 nnn >description

UID uuu 로 실행되는 프로세스 ppp 가 사용자 로그인을 확인하려고 요청했습니다. CA Access Control 로그인 확인 절차가 실패했습니다. 공급업체의 기술 지원부에 문의하십시오.

APIAUTH ! P=ppp U=uuu NULL ACEE Error VerifyCreate (ACEEH=hhh)

서버 프로세스가 접근자의 로그인을 처리하는 동안 "server"로 표시된 사용자 프로세스가 ACEE 의 작성을 요청했습니다. 다음 이유 중 하나로 인해 NULL ACEE 결과가 나타납니다.

- 지정한 사용자가 CA Access Control 데이터베이스에 정의되어 있지 않습니다.
- VerifyCreate 요청 실행자가 모든 정보를 올바로 제공하지 않았습니다.
- 지정한 사용자의 로그인이 허용되지 않습니다.

APIAUTH ! P=ppp U=uuu NULL ACEE Error VerifyDelete (ACEEH=hhh)

사용자 uuu 와 연결되어 있으며 'server' 프로세스로 표시된 프로세스 ppp 가 사용자 로그오프 처리의 일부로 ACEE 핸들 hhh 의 삭제를 요청했습니다. 그러나 이 핸들과 연결된 ACEE 가 없으므로 CA Access Control 이 이 핸들을 삭제할 수 없습니다.

APIAUTH : ACEEH=1 인 P=ppp U=uuu 요청 > 새 ACEEH=hhh

UID uuu 로 실행되는 프로세스 ppp 가 일반 리소스에 대한 액세스를 요청했으며 ACEE 핸들 -1 을 제공했습니다. CA Access Control 은 요청 프로세스와 연결된 ACEE 핸들을 사용했습니다. 이 메시지는 리소스에 대한 액세스를 요청하는 단일 사용자 프로세스의 일반적인 메시지입니다. 수행해야 할 작업은 없습니다.

APIAUTH ! P=ppp U=uuu VerifyCreate(ACEEH=hhh) Error nnn

UID uuu 로 실행되는 프로세스 ppp 가 ACEE 를 생성하기 위해 VerifyCreate 요청을 실행했습니다. VerifyCreate 과정이 실패했습니다. 공급업체의 기술 지원부에 문의하십시오.

APIAUTH > P=ppp U=uuu VerifyCreate DENY (Result=[P/D/C]) string

다음 이유 중 하나로 인해 VerifyCreate 요청이 거부되었습니다.

- 지정된 사용자가 시간 또는 날짜 규칙으로 인해 로그인할 수 없습니다.
- 사용자가 지정된 터미널에서 작업할 수 없습니다.
- 지정된 암호(입력한 경우)가 올바르지 않습니다.
- 다음 메시지에서 설명하는 이유 중 하나에 해당됩니다.

APIAUTH > P=ppp U=uuu VerifyCreate OK (ACEEH=hhh)!

VerifyCreate 요청이 허용되었습니다. ACEE(Accessor Environment Element)가 저장소에 작성되었습니다. CA Access Control 은 호출 프로그램에 ACEEH(ACEE 핸들)를 반환했습니다. 지정한 사용자가 CA Access Control 에 정의되어 있지 않아 함수가 ACEEH -1 을 반환했습니다.

APIAUTH ! P=ppp U=uuu VerifyDelete(ACEEH=hhh) [OK | Error 0xerr]

사용자 uuu 와 연결되어 있으며 'server' 프로세스로 표시된 프로세스 ppp 가 사용자 로그오프 처리의 일부로 ACEE 핸들 hhh 의 삭제를 요청했습니다. VerifyDelete 요청의 결과는 OK 또는 오류입니다. 오류인 경우 오류 코드가 16 진수인 err 로 표시됩니다. semsgtool 유틸리티를 사용하여 오류의 속성을 확인하십시오.

APIAUTH > P=ppp U=uuu VerifyRequest(ACEEH=hhh, C=ccc, R=rrr, A=nnn) DENY (결과='D')Why ? detaileddenialreason

액세스 권한 xxx 를 사용하여 클래스 ccc 의 리소스 rrr 에 액세스하려는 요청이 거부되었습니다. ACEEH 가 -1 인 경우 거부는 범용 액세스 규칙에 따라 결정됩니다. ACEEH 가 -1 이 아닌 경우 거부는 지정된 핸들과 관련된 사용자에 따라 결정됩니다. 두번째 행은 거부의 이유를 상세히 제공합니다.

APIAUTH > P=ppp U=uuu VerifyRequest(ACEEH=hhh, C=ccc R=rrr, A=xxx) PASS

액세스 권한 xxx 를 사용하여 클래스 ccc 의 리소스 rrr 에 액세스하려는 요청이 승인되었습니다. ACEEH 가 -1 인 경우(사용자가 CA Access Control 에 정의되지 않음), 리소스에 대한 액세스 권한은 범용 액세스 규칙에 따라 결정됩니다. ACEEH 가 -1 이 아닌 경우 권한은 지정된 핸들과 연결된 사용자에 대한 액세스 규칙에 따라 결정됩니다.

CONNECT : P=ppp U=uuu ACEEH=hhh from ipip:port1 to socket 6000 host=iiii

UID uuu 와 연결된 프로세스 ppp 가 호스트 iiii(X-터미널 또는 스테이션)에서 창 열기를 요청했습니다.

참고: 포트 번호는 항상 6000 이고, 다른 모든 TCP/IP 연결 요청은 CA Access Control 에서 무시됩니다.

CONNECT > P=ppp U=uuu from ipip:port1 to socket 6000 host=iiii BYPASS

프로세스 ppp 에서 실행 중인 프로그램이 등록된 XDM 프로그램이기 때문에 CA Access Control 은 액세스 규칙을 해석하지 않고 CONNECT 요청을 바이패스했습니다.

CONNECT > 결과: [P/D/C] P=ppp ACEEH=hhh TERM=tttWhy ? detaileddecisiontext

CONNECT 결과는 D(거부) 또는 P(허용)입니다. 두번째 행은 결정의 이유를 제공합니다.

오류입니다. 포크할 수 없습니다. Errno nnn.

초기화 중에 CA Access Control 은 데몬이 되기 위해 포크를 여러 번 수행합니다. 포크 요청이 실패했으며 지정된 오류 번호가 나타납니다.

문제의 원인을 확인할 수 없으면 공급업체의 기술 지원부로 문의하십시오.

ERROR ! CA Access Control 에이전트에서 ddd 을(를) 실행하지 못했습니다.

엔진이 에이전트 데몬을 시작할 수 없습니다. seagent 실행 파일이 올바른 위치(일반적으로 ACInstallDir/bin/seagent)에 있는지 확인하십시오. 이 파일이 올바른 위치에 있으면 공급업체의 기술 지원 담당자에게 문제를 보고하십시오. 메시지 텍스트에서 ddd 는 CA Access Control 이 seagent 를 실행할 때 운영 체제로부터 받은 오류 번호입니다.

오류입니다. LOGIN 프로그램에 대한 메모리를 가져오지 못했습니다.ERROR ! NFS 장치에 대한 메모리를 가져오지 못했습니다.ERROR ! PRIV 프로그램에 대한 메모리를 가져오지 못했습니다.ERROR ! XDM 프로그램에 대한 메모리를 가져오지 못했습니다.

이러한 메시지는 심각한 메모리 부족을 나타냅니다. CA Access Control 을 실행하는 데 필요한 최소 메모리가 컴퓨터에 없거나 소프트웨어 버그가 발견되었습니다. 공급업체의 기술 지원부에 문의하십시오.

ERROR ! PROC 테이블에 대한 메모리를 가져오지 못했습니다.

seosd 는 시작된 후 실행 중인 모든 프로세스를 검색하여 각 실행 프로세스에 대한 모든 필요 정보를 확인합니다. seosd 가 이 작업 수행을 위한 메모리 할당에 실패했으므로 실행이 종료됩니다. 심각한 메모리 부족으로 인해 이 오류가 발생합니다.

오류입니다. 로그인 프로그램을 등록하지 못했습니다. programname

시작하는 동안 CA Access Control 은 로그인 프로그램으로 처리해야 하는 모든 실행 파일을 등록합니다. 로그인 프로그램 목록은 각 운영 체제 환경에 대한 CA Access Control 코드에 정의됩니다.

시작하는 동안 파일 시스템에서 지정된 programname 을 찾을 수 없습니다. CA Access Control 은 이 프로그램을 무시하며 작업이 계속 진행됩니다.

오류입니다. 권한 있는 프로그램을 등록하지 못했습니다. programname

시작하는 동안 CA Access Control 은 권한 있는 프로그램으로 처리해야 하는 모든 실행 파일을 등록합니다. 시작하는 동안 파일 시스템에서 지정된 programname 을 찾을 수 없습니다. CA Access Control 은 이 프로그램을 무시하며 작업이 계속 진행됩니다.

권한 있는 프로그램 목록은 각 운영 체제 환경에 대한 CA Access Control 코드에 정의됩니다.

오류입니다. XDM 프로그램을 등록하지 못했습니다. programname

시작하는 동안 CA Access Control 은 XDM 프로그램으로 처리해야 하는 모든 실행 파일을 등록합니다. XDM 프로그램 목록은 각 운영 체제 환경에 대한 CA Access Control 코드에 정의됩니다.

시작하는 동안 파일 시스템에서 지정된 programname 을 찾을 수 없습니다. CA Access Control 은 이 프로그램을 무시하며 작업이 계속 진행됩니다.

ERROR : FileDb 목록에 대한 메모리가 없습니다.

시작 중에 seosd 가 보호된 파일 목록을 저장할 메모리를 할당할 수 없습니다. 이것은 심각한 메모리 부족 때문일 수 있습니다. seosd 데몬이 종료됩니다.

오류입니다. GroupDb 목록에 대한 메모리가 없습니다.ERROR ! HostDb 목록에 대한 메모리가 없습니다.ERROR ! ServDb 목록에 대한 메모리가 없습니다.ERROR ! UserDb 목록에 대한 메모리가 없습니다.

이러한 메시지는 심각한 메모리 부족을 나타냅니다. CA Access Control 을 실행하는 데 필요한 최소 메모리가 컴퓨터에 없거나 소프트웨어 버그가 발견되었습니다. 공급업체의 기술 지원부에 문의하십시오.

ERROR ! PreMatureExec FORK Child=ppp Parent=PPP(으)로 가정합니다.

이 메시지는 프로세스 ID(ppp)가 seosd 에 알려지지 않은 EXEC system-call 을 실행했음을 나타냅니다. 일반적으로 이러한 메시지는 seosd 가 EXEC 요청 전의 FORK 시스템 호출에 대해 통지를 받지 못했음을 나타냅니다. 이것은 UNIX 커널에 대한 CA Access Control 확장인 SEOS_syscall 이 유지 관리해야 하는 직렬화 잠금에 문제가 있음을 의미할 수 있습니다.

메시지 텍스트의 ppp 가 seagent 의 pid 이면 이 메시지를 무시할 수 있습니다. 메시지가 두 번 이상 표시되면 공급업체의 기술 지원부에 문제를 보고하십시오.

오류입니다. P=ppp 을(를) 실행하지 못했습니다.

CA Access Control 이 EXEC 이벤트를 수신했지만 실행 파일의 inode 번호가 0 이었습니다. 이 메시지는 앞부분에 #! 셸 프로그램 선언 행이 없는 파일을 호출할 때 나타납니다. 수행해야 할 작업은 없습니다.

ERROR ! CA Access Control 파일 테이블을 설정하지 못했습니다.

seosd 가 파일 테이블(보호된 모든 CA Access Control 파일의 테이블)을 설정하려고 시도했습니다. 그러나 SEOS_syscall 이 이 요청을 거부했습니다. 대부분의 경우 커널의 메모리 부족 또는 seosd 와 SEOS_syscall 의 버전 불일치가 그 원인입니다. CA Access Control 파일 보호 기능이 계속해서 제대로 작동할 수 없습니다.

가능하면 버전 불일치를 해결하십시오. 다른 문제가 없는 경우 공급업체의 기술 지원부에 이 문제를 보고하십시오.

오류입니다. seosini_ShutDown rv=errorno

종료 중에 CA Access Control 에 오류가 발생했습니다. 공급업체의 기술 지원부에 오류를 보고하십시오.

ERROR ! 문자열이 너무 일반적인 'path'입니다.

newfile 또는 newres FILE 명령을 통해 파일 보호에 대한 포괄적인 규칙을 정의하려고 시도했습니다. 그러나 지정한 경로는 포괄적인 파일 액세스 규칙이 될 수 없습니다. 파일 규칙이 정의되어 있지 않습니다.

오류입니다. 알 수 없는 요청: 유형:ttt Pid=ppp, Buff=bbb

CA Access Control 이 시스템 호출로부터 요청을 수신했지만 요청 유형 ttt 는 인식이 불가능합니다. 이 문제는 CA Access Control 시스템 호출과 seosd 간의 소프트웨어 버전 불일치 또는 소프트웨어 오류로 인해 발생할 수 있습니다. 요청은 프로세스 ppp 로부터 전달되었고, bbb 는 요청 버퍼의 출력입니다. 공급업체의 기술 지원부에 문제를 보고하십시오.

EXEC : P=ppp U=uuu G=ggg (D=ddd I=iii) Pgm:ProgramName [연결: ipaddress]

CA Access Control 이 UID uuu 및 GID ggg 와 연결된 프로세스 ppp 로부터 프로그램 실행 이벤트를 수신했습니다. (ggg 값이 -1 이면 CA Access Control 이 해당 프로세스의 GID 를 등록하지 않았음을 나타냅니다.) 메시지 텍스트에서 ddd 와 iii 는 각각 파일의 장치 번호와 inode 입니다. Program-Name 은 프로그램을 호출할 때 사용되는 0 인수입니다. 지정한 프로그램은 일반 프로그램입니다(즉, setuid 또는 setgid 가 아님). 따라서 CA Access Control 은 데이터베이스 액세스 규칙 결정 메커니즘을 호출하지 않고 실행을 허용합니다. 프로세스가 연결되는 ip-address 를 추출할 수 있으면 CA Access Control 은 메시지 텍스트로 이 주소를 보고합니다.

EXEC sg: P=ppp U=uuu G=ggg (D=ddd I=iii) Pgm:ProgramName[연결: ipaddress]

CA Access Control 이 UID uuu 및 GID ggg 와 연결된 프로세스 ppp 로부터 프로그램 실행 이벤트를 수신했습니다. (ggg 값이 -1 이면 CA Access Control 이 해당 프로세스의 GID 를 등록하지 않았음을 나타냅니다.) 메시지 텍스트에서 ddd 와 iii 는 각각 파일의 장치 번호와 inode 입니다.Program-Name 은 프로그램을 호출할 때 사용된 0 인수입니다. 지정한 프로그램은 setgid 프로그램입니다. 따라서 CA Access Control 은 데이터베이스 액세스 규칙 결정 메커니즘을 호출하여 실행 허용 여부를 결정합니다. 프로세스가 연결되는 ip-address 를 추출할 수 있으면 CA Access Control 은 메시지 텍스트로 이 주소를 보고합니다.

EXECsu : P=ppp U=uuu G=ggg (D=ddd I=iii) Pgm:ProgramName[연결: ipaddress]

CA Access Control 이 UID uuu 및 GID ggg 와 연결된 프로세스 ppp 로부터 프로그램 실행 이벤트를 수신했습니다. (ggg 값이 -1 이면 CA Access Control 이 해당 프로세스의 GID 를 등록하지 않았음을 나타냅니다.) 메시지 텍스트에서 ddd 와 iii 는 각각 파일의 장치 번호와 inode 입니다. Program-Name 은 프로그램을 호출할 때 사용된 0 인수입니다. 지정한 프로그램은 setuid 프로그램입니다. 따라서 CA Access Control 은 데이터베이스 액세스 규칙 결정 메커니즘을 호출하여 실행 허용 여부를 결정합니다. 프로세스가 연결되는 ip-address 를 추출할 수 있으면 CA Access Control 은 메시지 텍스트로 이 주소를 보고합니다.

EXECsusg: P=ppp U=uuu G=ggg (D=ddd I=iii) Pgm:ProgramName[연결: ipaddress]

CA Access Control 이 UID uuu 및 GID ggg 와 연결된 프로세스 ppp 로부터 프로그램 실행 이벤트를 수신했습니다. (ggg 값이 -1 이면 CA Access Control 이 해당 프로세스의 GID 를 등록하지 않았음을 나타냅니다.) 메시지 텍스트에서 ddd 와 iii 는 각각 파일의 장치 번호와 inode 입니다. Program-Name 은 프로그램을 호출할 때 사용된 0 인수입니다. 지정한 프로그램은 setuid 및 setgid 프로그램입니다. 따라서 CA Access Control 은 데이터베이스 액세스 규칙 결정 메커니즘을 호출하여 실행 허용 여부를 결정합니다. 프로세스가 연결되는 ip-address 를 추출할 수 있으면 CA Access Control 은 메시지 텍스트로 이 주소를 보고합니다.

EXEC > P=ppp U=uuu (R=rrr E=eee S=sss) to (E=EEE) BYPASS

프로그램이 setuid, setgid 또는 둘 다이고 해당 프로그램의 실행이 액세스 규칙 결정 메커니즘을 호출했지만, 파일 EEE 의 소유자가 현재의 eee(유효한 UID)와 동일하기 때문에 CA Access Control 이 이 검사를 바이패스했습니다. 프로그램 실행은 프로세스의 권한 범위를 변경할 수 없습니다. 프로그램이 데이터베이스에 트러스트된 프로그램으로 정의되어 있고 수정되었거나 다른 방법으로 변경된 경우에는 프로그램 실행이 승인되지 않습니다.

EXEC > 결과: 'R' [stage=sss gstag=ggg ACEEH=hhh rv=rc]Why? DetailedDecisiontext

CA Access Control 이 사용자의 프로그램 실행 권한과 결과 R 을 검사했습니다. 여기서 R 은 D(거부) 또는 P(허용)입니다. 단계 sss 와 승인 단계 ggg 는 결정 흐름의 어떤 단계에서 결과가 결정되었는지 나타냅니다. ACEE 핸들 hhh 는 프로그램 접근자로 사용되었습니다. 결과가 'C'(검사)이면 CA Access Control 이 소프트웨어 오류로 인해 결정을 내리지 않았음을 의미합니다. 공급업체의 기술 지원부에 문의하고 반환 값 rc 를 알려 주십시오. Detailed-Decision-text 는 단계와 승인 단계에 대한 텍스트 설명입니다. 결과가 P 이면 프로그램이 성공적으로 실행됩니다. 결과가 D 이면 프로그램이 실행되지 않고 사용자가 권한 거부됨 메시지를 수신합니다.

EXECARGS: 'execution arguments'

EXEC syscall 로 인해 CA Access Control 이 전달된 모든 인수와 함께 실행된 명령줄을 표시합니다.

EXIT : 종료됩니다...

CA Access Control 이 종료 프로세스를 시작했으며 시스템 호출의 차단을 비활성화했습니다.

치명적 오류입니다. 위치: seosrt_InitDatabase (nnn) 계층 = nnn 단계 = nnn 반환 코드 = 0xnnn

CA Access Control 이 데이터베이스 I/O 루틴을 초기화할 수 없습니다. 이유는 다음과 같습니다.

- 디렉터리에 seos.ini 파일의 dbdir 토큰으로 식별되는 CA Access Control 데이터베이스가 없습니다.
- CA Access Control 을 호출하는 사용자가 root 가 아닙니다.
- 데이터베이스가 손상되었습니다.

문제를 해결할 수 없으면 공급업체의 기술 지원부로 문의하십시오.

FILE : P=ppp U=uuu (D=dev I=inode) acc : pathname

userid uuu 와 연결된 프로세스 ppp 가 보호된 CA Access Control 파일에 액세스하려고 시도했습니다. 메시지 텍스트에서 dev 와 inode 는 각각 액세스되는 파일의 장치 및 inode 입니다. acc 는 액세스 모드(READ, WRITE 등)이고 pathname 은 액세스되는 파일의 실제 경로 이름입니다.

FILE > 결과 'D' CA Access Control 파일 전용 'filename'

CA Access Control 만 이 파일에 액세스할 수 있기 때문에 파일 액세스 요청의 결과가 D(거부)입니다. 접근 규칙이 접근을 허용해도 CA Access Control 이 하드 코딩되어 이 파일에 대한 접근을 거부합니다.

FILE > 결과: 'R' [stage=sss gstag=gs ACEEH=hhh rv=rv (recordname)Why? detailedreasontext

파일 액세스 요청의 결과 R 은 D(거부) 또는 P(허용)입니다. 단계 sss 와 승인 단계 gs 는 두 번째 행의 "Why?" 뒤에 나오는 텍스트 문자열 이유에 매핑됩니다. 메시지 텍스트에서 hhh 는 요청의 접근자와 연결된 접근자 핸들이고 record-name 은 접근을 거부 또는 허용하는 결정을 트리거한 접근 규칙 레코드의 이름입니다.

FORK : P=ppp U=uuu G=ggg Child=cppp Pgm:ProgramName

CA Access Control 이 UID uuu 및 GID ggg 와 연결된 프로세스 ppp 의 포크 요청을 차단했습니다. child 프로세스 ID 는 cppp 입니다. Program-Name 은 부모 프로세스에서 실행 중인 프로그램으로, 처음에는 자식 프로세스에서도 실행됩니다. CA Access Control 은 포크 요청을 결코 거부하지 않으며 언제나 승인합니다. 포크 시스템 호출의 다른 형태인 vfork 와 kfork 도 포크 요청으로 보고됩니다.

GETCRED : P=ppp, 티켓으로 자격 증명을 가져옵니다.

이것은 정보 제공만을 위한 메시지로, ppp(일반적으로 정책 모델 데몬 sepmdd 의 프로세스 ID)가 특정 티켓 소유자(sepmdd 의 서비스를 요청한 클라이언트 프로세스)의 인증서를 요청했음을 나타냅니다. 자세한 내용은 부록의 GTICKET 설명과 "유틸리티 세부 정보" 장의 sepmdd 설명을 참조하십시오.

GPEERNAM: P=ppp, ADDR=addr, N=desc

CA Access Control 이 getpeername() 시스템 호출을 차단하여 현재 프로세스와 연결된 IP 주소를 확인했습니다. 이 시스템 호출은 항상 허용됩니다. 메시지 텍스트에서 ppp 는 getpeername() 호출을 작성한 프로세스 id 이고 addr 은 소켓 설명자 desc 와 연결된 IP 주소입니다.

GTICKET : P=ppp, 인증 티켓을 가져옵니다.

이것은 정보 제공만을 위한 메시지로, ppp 가 seosd 에 인증 티켓을 실행하도록 요청했음을 나타냅니다. 정책 모델 클라이언트인 sepmd 가 sepmdd 와 통신할 때마다 서버는 전달된 티켓을 통해 클라이언트를 식별합니다. 클라이언트는 소켓 통신을 사용하여 서버로 획득한 티켓을 보냅니다. 그러면, 서버는 이 티켓을 seosd 로 전달하여 GETCRED 요청을 받은 티켓 보유자의 자격 증명을 가져옵니다. 이런 방식으로 sepmdd 는 서비스를 요청하는 클라이언트를 식별합니다.

INET : P=ppp, 시작 ipaddress:localport 포트 portnumber

CA Access Control 이 TCP/IP 서비스 port-number 를 요청하는 원격 ip-address 에서 실행된 들어오는 인터넷 허용 요청을 차단했습니다.

INET > 결과: 'R' ipaddr>locport, stg=stage gtsg=gstageWHY ? DetailedReasonText

인터넷 요청의 결과 R 은 P(허용) 또는 D(거부)입니다. 메시지 텍스트에서 ip_addr 은 요청의 IP 주소입니다. Detailed-Reason-Text 는 요청 호스트에 대해 TCP/IP 서비스를 거부할지 허용할지 최종 결정을 내리는 단계가 어떤 결정 플로우 단계 및 허용 단계인지 나타내는 설명입니다.

정보 : fs-space 가 부족하여 추적이 자동으로 비활성화됩니다(space).

추적 파일이 위치하는 파일 시스템에 남아 있는 빈 공간의 양이 seos.ini 파일의 trace_space_saver 토큰에 지정된 임계값보다 낮은 경우 추적 기능은 자동으로 비활성화됩니다. 메시지 텍스트에서 space 는 파일 시스템에 남은 여유 공간의 양입니다.

정보 : fs freespace 를 가져올 수 없습니다(오류 번호=err).

추적 기능의 Auto Disable 기능은 파일 시스템의 빈 공간 양을 결정할 수 없습니다. 메시지 텍스트에서 err 은 UNIX statfs() 호출로부터 받은 오류 integer 입니다. 공급업체의 기술 지원부에 문제를 보고하십시오.

정보 : DB 쿼리

seosd 데몬이 CA Access Control 데이터베이스의 정보를 추출하라는 요청을 받았습니다.

정보 : DB 요청

seosd 데몬이 CA Access Control 데이터베이스의 데이터를 수정하거나 쿼리하라는 요청을 받았습니다.

정보 : 필터 마스크: 'mask'이(가) 등록되었습니다.

seosd 데몬은 trcfilter.init 파일에서 읽은 각 필터 마스크를 등록하므로, 마스크와 일치하는 메시지가 추적 파일에 전송되지 않습니다.

정보 : GroupList: nnn 개 항목이 등록되었습니다.

seosd 가 NIS 서버 아래에서 실행되면 시작 시 /etc/group 및 NIS 맵의 모든 그룹 항목을 캐시하므로 ypserv 프로세스와 TCP/IP 요청을 호출하지 않고 GID 를 그룹 이름으로 변환할 수 있습니다. 또한 이 메시지는 seos.ini 의 under_NIS_server 토큰이 YES 로 설정되어 있음을 나타냅니다. CA Access Control 이 실행되는 스테이션이 NIS 서버가 아니면 under_NIS_server 토큰을 NO 로 설정합니다. 메시지 텍스트에서 nnn 은 캐시된 그룹 항목의 수입니다.

정보 : HostList: nnn 개 항목이 등록되었습니다.

seosd 데몬은 시작할 때 /etc/hosts 로부터 모든 항목을 캐시합니다. 메시지 텍스트에서 nnn 은 캐시된 호스트 항목의 수입니다.

정보 : 로그인 프로그램: programname 이(가) 등록되었습니다.

seosd 데몬은 사용자가 시스템에 로그인하기 위해 사용하는 모든 프로그램을 인식해야 합니다. CA Access Control 은 로그인 프로그램이 호출한 setuid 시스템 호출을 setuid 요청이 아닌 로그인 요청으로 취급합니다. 메시지 텍스트에서 programname 은 등록된 로그인 프로그램의 전체 경로입니다. seosd 데몬은 CA Access Control 시작 코드에서 로그인 프로그램의 이름을 내부적으로 가져옵니다.

정보 : NFS Device Major %d 개 항목이 등록되었습니다.

Watchdog 이 트러스트된 프로그램에서 수행하는 검사에는 파일이 위치하는 장치 번호의 검사도 포함됩니다. 장치 번호가 부팅 후 다른 값을 갖게 되는 NFS 마운트 파일 시스템(특히, 자동 마운트 파일 시스템)에 파일이 위치할 경우, 검사를 수행한 후 오류가 발생할 수 있습니다. 따라서 CA Access Control 은 불안정한 마이너 장치 번호를 무시할 수 있도록 NFS 파일 시스템의 메이저 장치 번호를 등록합니다. CA Access Control 에는 각 환경의 NFS 마운트 파일 시스템에 대한 메이저 장치 번호 목록이 있습니다. 설치 시 CA Access Control 에서 인식되지 않는 네트워크 마운트 파일 시스템을 사용하는 경우, 메이저 장치 번호를 목록에 추가하는 방법을 알아보려면 공급업체의 기술 지원부에 문의하십시오. 메시지 텍스트에서 nnn 은 NFS 마운트된 파일 시스템으로 등록된 기본 장치 번호의 수입니다.

정보 : P=ppp 이(가) 종료되었습니다.

프로세스 ppp 가 종료되었습니다. seosd 는 이 프로세스 번호를 해당 ACEE(accessor environment element)와 분리합니다. 프로세스 ppp 가 해당 ACEE 와 연결된 마지막 프로세스이면(즉, 동일한 환경을 사용하는 다른 parent 프로세스나 하위 프로세스가 없음) 저장소에서 ACEE 가 제거됩니다. 이 메시지는 프로세스가 종료된 후 즉시 작성되지 않습니다. CA Access Control 이 "가비지 콜렉션"을 수행하여 내부 테이블의 프로세스 항목을 재사용할 때만 작성됩니다.

정보 : P=ppp 실행이 실패했습니다.

이 메시지는 CA Access Control 이 실행을 승인한 후 UNIX 가 이 요청을 거부했기 때문에 프로세스 ppp 가 마지막 EXEC syscall 을 실행하지 못했음을 나타냅니다. 따라서 CA Access Control 은 프로세스 ID 에서 프로그램이 실행되는 동안 프로세스와 연결된 이전 실행 파일의 값을 복원합니다. 대부분의 경우 프로세스는 종료됩니다. 이것을 오류라고 할 수는 없으므로 특별한 작업을 수행할 필요는 없습니다. 그러나 UNIX 도구를 사용하여 실행이 실패한 원인은 확인해야 합니다. 대부분의 경우 그 이유는 셸 스크립트의 첫 번째 행에 "#!/bin/sh" 헤더가 없기 때문입니다.

정보 : P=ppp 알 수 없는 TTY 유형 typename 입니다.

seosd 데몬이 프로세스 ppp 가 실제 TTY 를 사용 중인지 또는 의사(pseudo) TTY 를 사용 중인지 확인할 수 없습니다. 공급업체의 기술 지원부에 문의하십시오.

정보 : 권한 있는 프로그램: programname 이(가) 등록되었습니다.

seosd 데몬이 권한이 있는 일부 프로그램을 등록합니다. 이러한 프로그램은 사용자 ID 교체(SURROGATE) 클래스를 검사하지 않고 모든 사용자에 대해 setuid 를 수행할 수 있습니다. 흐름 요구 사항으로 인해 지금은 /bin/sendmail 만 권한이 있는 프로그램으로 만들 수 있습니다. 가능한 한 이 목록을 작게 유지해야 합니다. seoswd 가 권한이 있는 모든 프로그램을 모니터하여 트러스트된 상태를 계속 유지하는지 확인하는 것이 좋습니다. 메시지 텍스트에서 programname 은 등록된 프로그램의 전체 경로입니다.

정보 : 제한된 파일 테이블 nnn 개 항목이 설정되었습니다.

시작 중에 seosd 가 보호된 CA Access Control 파일 nnn 개 항목을 발견했으며 이 목록을 UNIX 커널의 CA Access Control 확장으로 전달했습니다. 이것은 정보 메시지일 뿐입니다.

정보 : SEOS_syscall UnRegister rc=nnn

종료 중에 seosd 가 커널로 등록 취소하여 다시 시작될 수 있게 합니다. 메시지 텍스트에서 nnn 은 반환 코드로, 0 이어야 합니다. 반환 코드가 0 이 아니면 공급업체의 기술 지원부에 문제를 보고하십시오.

정보 : ServList 가 nnn 개 항목에 등록되었습니다.

seosd 데몬은 시작할 때 /etc/services 의 모든 항목을 캐시합니다. 메시지 텍스트에서 nnn 은 캐시된 호스트 항목의 수입니다.

정보 : nnn portmapper 항목으로 등록된 ServList 입니다.

시작할 때 seosd 는 portmapper 가 확인한 nnn 개의 TCP/IP 서비스를 등록했습니다. 이것은 정보 메시지일 뿐입니다.

정보 : 사이트 설정

다른 CA Access Control 스테이션과의 통신을 담당하는 CA Access Control 데몬인 seagent 데몬이 원격 스테이션의 연결 요청을 seosd 로 전송했습니다.

정보 : PV C=ccc O=ooo P=ppp(으)로 설정합니다.

seoswd 데몬이 클래스 ccc의 객체 ooo에서 속성 ppp의 값을 설정했습니다.

정보 : UserList nnn 개 항목이 등록되었습니다.

seosd는 NIS 서버에서 실행될 때 모든 사용자 항목(/etc/passwd과 NIS 맵)을 캐시하므로, ypserv 프로세스와 TCP/IP 요청을 호출하지 않고 seosd가 UID를 사용자 이름으로 변환할 수 있습니다. 또한 이 메시지는 seos.ini의 under_NIS_server 토큰이 YES로 설정되었음을 나타냅니다. eTrust AC를 실행 중인 컴퓨터가 NIS 서버가 아닌 경우 seos.ini의 under_NIS_server 토큰을 NO로 설정하십시오. CA Access Control이 실행되고 있는 컴퓨터가 NIS 서버가 아니면 seos.ini 에서 under_NIS_server 토큰을 NO로 설정하십시오. 메시지 텍스트에서 nnn은 캐시된 사용자 항목의 수입니다.

정보 : XDM 프로그램: programname 이(가) 등록되었습니다.

XDM 프로그램은 X-Terminal에 userid 및 암호 상자를 표시하는 프로그램입니다. XDM 프로그램은 일반적으로 X-터미널에서 윈도우를 열 수 없는 수퍼유저 권한으로 실행됩니다. 하지만 XDM 프로그램은 지정할 사용자의 userid 및 암호가 있는 상자를 표시하기 위해 X-터미널에서 창을 열어야 합니다. 따라서 seosd는 CONNECT 요청을 작성하는 프로그램이 등록된 XDM 프로그램인 경우 터미널 검사를 바이패스합니다.

KILL : P=ppp U=uuu 에서 (nn)을(를) 제외하고 모두 중지: (proclist)

사용자 uuu와 연결된 프로세스 ppp가 proclist에 나열된 모든 프로세스 또는 목록에 있는 프로세스를 제외한 모든 프로세스를 강제 중단(kill)하려고 시도했습니다. 메시지 텍스트에서 nn은 대상 프로세스의 수입니다.

KILL > 결과 'R' [stage=sss gstag=gs rv=rr] ACEEH=hhhWhy? detailedreasontext

Kill 이벤트의 결과 R은 D(거부) 또는 P(허용)입니다. 메시지 텍스트에서 sss, gs 및 rr은 각각 CA Access Control 결정 루틴의 단계, 승인 단계 및 반환 값이고, hhh는 중지(kill) 이벤트와 연결된 접근자 핸들입니다. 단계 및 허용 단계 코드에서 파생된 detailed-reason-text가 두 번째 행에 나타납니다.

LOGIN : P=ppp 사용자=uuu 터미널=ttt

seosd 데몬은 터미널 ttt에서 프로세스 번호 ppp로 작업 중인 사용자 uuu의 로그인 요청을 차단했습니다. 로그인 결과 메시지가 이 메시지 뒤에 나와야 합니다.

LOGIN > 결과: 'R' [stage=stage gstag=gstage rv=nnn] ACEEH=hhh[Why ?detaileddenialreason]

로그인 요청의 결과 R 은 D(거부) 또는 P(허용)입니다. 메시지 텍스트에서 stage 와 gstage 는 로그인 요청을 허용 또는 거부하는 결정을 내린 CA Access Control 흐름의 단계를 나타내는 번호입니다. 로그인이 허용된 경우 hhh 는 현재 실행 프로세스와 연결된 ACEE 핸들입니다. 로그인이 거부되는 경우 hhh 는 -1 로 설정되고 detailed-denial-reason 이 두 번째 행에 나타납니다. detailed-denial-reason 이 리소스 액세스(예: "리소스 액세스를 허용하는 규칙이 없음")와 연결된 경우 관련 리소스는 사용자가 로그인 요청을 작성한 터미널이 됩니다.

LOGIN > 결과: ALL 에 대해 'D' 로그인이 비활성화되었습니다.

모든 사용자에 대한 로그인이 현재 비활성화되었기 때문에 로그인 요청이 거부되었습니다.

LOGIN > 결과: U=uuu 에 대해 'D' 로그인이 비활성화되었습니다.

특정 사용자에 대한 로그인이 현재 비활성화되었기 때문에 로그인 요청이 거부되었습니다. 그 이유는 사용자가 이미 로그인한 상태이기 때문일 수 있습니다.

MESSAGE : string

콘솔 요청에 의해 추적 파일에는 표시 메시지가 있습니다.

NEWPASS : 새 암호를 설정합니다.

sepass 유틸리티는 userid 에 대한 새 암호 설정을 요청했습니다.

PW_ATTCK: P=ppp make nnn attempts in sss seconds from terminal

seosd 데몬은 등록된 로그인 프로그램 중 하나를 실행하는 프로세스 ppp 가 사용자/암호 조합을 지정하기 위해 nnn 회 시도했다가 실패했음을 검색했습니다. CA Access Control 은 메시지 텍스트에 지정된 터미널에서 암호 추측 공격을 시도했다는 결론을 내리고 CA Access Control 감사 파일에 감사 레코드를 기록했습니다. PWATTACK 감사 레코드는 로그 라우팅 데몬("selogrcd" 및 "selogrd") 동작을 트리거할 수 있습니다.

RESTART : DBSERV 는 Watchdog (P=ppp)에 의해 다시 시작됩니다.

seoswd 데몬이 seosd 를 재시작했습니다. 메시지 텍스트에서 ppp 는 seosd 의 프로세스 ID 입니다.

SCONSOLE: UID 에 대해 로그인할 수 없음: uuu

CA Access Control 콘솔 유틸리티인 secons 가 userid uuu 의 로그인 요청을 비활성화하는 요청을 실행했습니다. 이 때부터 지정된 userid 의 로그인 요청은 거부됩니다.

SCONSOLE: U=uuu 에 대한 로그인을 비활성화했습니다.

secons 유틸리티가 userid uuu 의 로그인 요청을 비활성화하는 요청을 실행했습니다. 그러나 userid 에 대한 로그인은 이미 비활성화되어 있습니다.

SCONSOLE: U=uuu 에 대한 로그인을 다시 활성화했습니다.

secons 유틸리티가 userid uuu 의 로그인을 다시 활성화하는 요청을 실행했습니다. 그러나 이 userid 의 로그인이 이미 활성화되었습니다.

SCONSOLE: 로그인할 수 없습니다.

secons 유틸리티는 모든 사용자의 로그인을 비활성화하는 요청을 작성했습니다. 이 때부터 사용자의 로그인 요청이 거부됩니다.

SCONSOLE: 로그인할 수 있습니다.

secons 유틸리티는 모든 사용자의 로그인을 다시 활성화하는 요청을 작성했습니다. 이 때부터 로그인 요청이 허용됩니다.

SCONSOLE: U=uuu 에 대해 로그인이 다시 활성화되었습니다.

secons 유틸리티는 지정된 사용자의 로그인을 다시 활성화하는 요청을 작성했습니다. 이 때부터 지정된 사용자의 로그인 요청이 허용됩니다.

SCONSOLE: Disabled Logins 테이블에 더 이상 공간이 없습니다.

secons 유틸리티가 특정 사용자의 로그인을 비활성화하는 요청을 작성했습니다. 그러나 로그인 비활성화 테이블이 가득 찼습니다. 공급업체의 기술 지원부에 문의하십시오.

SCONSOLE: U=uuu 은(는) 작업할 수 없습니다.

OPERATIONS 속성이 없는 사용자가 비 OPERATIONS 사용자에게 허용되지 않는 secons 스위치 중 하나를 사용하려고 했습니다.

SCONSOLE: U=uuu 은(는) U=uuu2 에 대해 로그인을 활성화했습니다.

사용자 uuu 가 secons 를 통해 사용자 uuu2 의 로그인을 비활성화하려고 시도했습니다. 그러나 root 및 사용자 uuu2 만 uuu2 의 로그인을 비활성화할 수 있습니다.

SCONSOLE: U=uuu 에서 U=uuu2 에 대해 로그인을 다시 활성화할 수 없습니다.

사용자 uuu 가 secons 를 통해 사용자 uuu2 의 로그인을 다시 활성화하려고 시도했습니다. 그러나 root 및 uuu2 사용자만 uuu2 의 로그인을 다시 활성화할 수 있습니다.

SETGRPS : P=ppp to grouplist

프로세스 ppp 가 grouplist 에 지정된 그룹에 대해 setgroups system-call 을 실행했습니다.

SGID : P=ppp U=uuu G=ggg to GGG (GROUP.groupname) ACEEH=hhh D=devnum I=inode

UID uuu 및 GID ggg 의 권한으로 실행 중인 프로세스 ppp 가 GID GGG 에 대해 setgid 시스템 호출을 실행했습니다. CA Access Control 은 SURROGATE 클래스 및 개체 GROUP.groupname 을 사용하여 해당 프로세스의 권한을 검사하고, 요청에 대한 접근자 핸들로 hhh 를 사용합니다. 메시지 텍스트에서 devnum 및 inode 는 각각 실행 프로그램의 장치 및 inode 입니다. "SGID 결과" 메시지는 이 메시지 다음에 나와야 합니다.

SGID > P=ppp U=uuu (RG=rg EG=eg SG=sg) to (RG=trg EG=teg SG=tsg) () BYPASS

CA Access Control 이 SURROGATE 액세스 규칙을 검사하지 않고 setgid 요청을 승인했습니다. 메시지 텍스트에서 ppp 는 작성 프로세스 id 이고 uuu 는 프로세스와 연결된 userid 입니다. rg, eg, sg 는 프로세스의 유효한 실제 저장 GID 이고 trg, teg, tsg 는 setgid 요청이 작성된 유효한 실제 대상 저장 GID 입니다. 바이패스가 발생한 이유는 대부분 현재 실제 또는 저장 GID 가 대상 GID 와 동일하여 setgid 요청이 사용자의 보안 범위를 변경하지 않기 때문입니다.

SGID > 결과: 'R' [stage=stage gstag=gstage ACEEH=hhh]Why? detailedreasontext

CA Access Control 이 SURROGATE 액세스 규칙과 비교하여 setgid 요청을 검사했으며 결과 R 은 P(허용) 또는 D(거부)입니다. 접근자 핸들 hhh 를 대신하여 결정되었습니다. 메시지 텍스트에서 detailed-reason-text 는 거부 또는 허용 이유입니다.

종료 요청이 거부되었습니다. U=uuu 은(는) 서버를 SHUTDOWN 할 수 없습니다.

userid uuu 가 secons 를 사용하여 seosd 를 종료하려고 시도했습니다. 그러나 이 사용자의 프로필에 OPERATIONS 특성이 없습니다. 따라서 요청이 거부되었습니다.

SHUTDOWN: OPERATOR 의 요청에 따라 서버가 종료됩니다.

seosd 데몬은 권한 있는 사용자의 요청에 따라 종료를 시작했습니다.

SHUTDOWN: CA Access Control 데몬 daemonname P=ppp RV=nnn 을(를) 종료합니다.

CA Access Control 이 종료 프로세스 중에 데몬 ppp 를 종료했습니다. CA Access Control 은 seoswd 와 seagent 도 종료합니다.

STARTUP: CA Access Control 데몬 PID=ppp

seosd 데몬이 시작되었습니다. 해당 프로세스 ID 는 ppp 입니다.

STREAM c: P=ppp 닫기 Stream Id=iii

프로세스 ppp 가 스트림 ID iii 를 가진 스트림을 닫았습니다. CA Access Control 은 나중에 (특정 스트림 ID 를 위해 TCP/IP 요청이 처리되는 때에) 스트림을 소유한 프로세스 ID 를 파악하기 위해 모든 스트림 열기 및 스트림 닫기 작업을 추적합니다.

STREAM o: P=ppp 에서 Stream Id=iii 을(를) 엽니다.

프로세스 ppp 가 스트림 ID iii 를 가진 스트림을 열었습니다. CA Access Control 은 나중에 (특정 스트림 ID 를 위해 TCP/IP 요청이 처리되는 때에) 스트림을 소유한 프로세스 ID 를 파악하기 위해 모든 스트림 열기 및 스트림 닫기 작업을 추적합니다.

SUID > P=ppp U=uuu (R=r E=e S=s) ~ (R=tr E=te S=ts) (reason) BYPASS

CA Access Control 이 SURROGATE 액세스 규칙을 검사하지 않고 setuid 요청을 승인했습니다. 메시지 텍스트에서 ppp 는 작성 프로세스의 id 이고, uuu 는 프로세스와 연결된 userid 입니다. r, e, s 는 프로세스 ppp 의 실제 유효 저장 UID 이고 tr, te, ts 는 setgid 요청이 작성된 실제 유효 대상 저장 UID 입니다. 바이패스의 이유는 대부분 현재의 실제 UID 또는 저장된 UID 가 대상 UID 와 동일하여 setuid 요청이 사용자의 보안 범위를 변경하지 않기 때문입니다. setuid system-call 을 실행하는 프로그램이 권한이 있는 프로그램(이 경우 reason 은 For Priv 가 됨)이거나, 실행 프로그램이 실제 로그인 전후에 UID 를 여러 번 전환하는 로그인 프로그램(이 경우 reason 은 For Login 으로 지정됨)인 경우에도 바이패스가 발생할 수 있습니다.

SUID : P=ppp U=uuu (R=r E=e S=s) ~ USER.username (R=tr E=te S=ts)D=devnum I=inode

userid uuu 의 권한으로 실행 중인 프로세스 ppp 가 현재의 실제 UID, 유효한 UID 또는 저장된 UID 를 UID uuu 로 변경하기 위해 setuid 시스템 호출을 실행했습니다. CA Access Control 은 해당 요청의 SURROGATE 클래스와 USER.username 개체를 사용하여 프로세스의 권한을 검사합니다. 메시지 텍스트에서 devnum 및 inode 는 각각 실행 프로그램의 장치 및 inode 입니다. "SGID 결과" 메시지는 이 메시지 다음에 나와야 합니다.

SUID > 결과: 'R' [stage=stage gstag=gstage ACEEH=hhh rv=rv]Why? detailedreasontext

CA Access Control 이 SURROGATE 액세스 규칙과 비교하여 setuid 요청을 검사했으며 결과 R 은 P(허용) 또는 D(거부)입니다. 접근자 핸들 hhh 를 대신하여 결정되었습니다. 메시지 텍스트에서 detailed-reason-text 는 거부 또는 허용 이유입니다.

VERPASS : 암호를 확인합니다.

CA Access Control 이 사용자의 암호 유효성을 확인하라는 요청을 받았습니다.

WAKE_UP : 서버가 시작됩니다.

seosd 데몬이 초기화를 시작했습니다.

경고 : P=ppp ACEEH=hhh 을(를) 연결합니다.

CA Access Control 은 모든 포크 요청에 대해 프로세스와 접근자 핸들(ACEEH)을 연결합니다. 이 메시지는 핸들 hhh 가 -1 이거나 hhh 가 유효한 접근자 핸들이 아니어서 연결할 수 없음을 나타냅니다. 후자의 경우 공급업체의 기술 지원부에 문의하십시오.

경고 : P=ppp 을(를) 확인할 수 없습니다.

이 메시지는 알 수 없는 프로세스의 포크 요청을 나타내는 Unknown P= 메시지 뒤에 옵니다. CA Access Control 은 UNIX 가 해당 사용자와 연결하는 사용자가 누구인지 확인하려고 시도합니다. 이 확인 작업을 완료할 수 없으며, 프로세스가 이미 종료되었기 때문일 수 있습니다. 이런 경우에 해당되지 않으면 공급업체의 기술 지원부에 문의하십시오.

경고 : P=ppp ACEEH=hhh 을(를) 연결 해제합니다.

CA Access Control 은 종료된 모든 프로세스에 대해 프로세스와 접근자 핸들(ACEEH)을 분리합니다. 이 메시지는 핸들 hhh 가 -1 이거나 hhh 가 유효한 접근자 핸들이 아니어서 분리할 수 없음을 나타냅니다. 후자의 경우 공급업체의 기술 지원부에 문제를 보고하십시오.

경고 : P=ppp 이(가) NULL 이 아닌 항목에 대한 ExecArg 입니다.

이 경고는 CA Access Control 이 시스템에 알려지지 않은 새 프로세스를 발견했으며 해당 실행 프로그램을 알 수 없을 때 나타납니다. 대부분의 경우 메시지를 무시할 수 있습니다. 예상된 결과가 나타나지 않는 경우 공급업체의 기술 지원부에 문의하십시오.

경고 : P=ppp 인 ACEEH 를 가져오지 못했습니다.

CA Access Control 이 프로세스 ppp 의 권한을 검사하라는 요청을 받았지만 해당 프로세스에 유효한 접근자 핸들이 없었습니다. 그 이유는 대부분의 경우 프로세스와 연결된 사용자가 정의된 CA Access Control 사용자가 아니거나 프로세스가 CA Access Control 시스템에 알려져 있지 않기 때문입니다. 두 경우 모두 CA Access Control 은 이 프로세스에 범용 액세스 권한만 제공합니다. 예상된 결과가 나타나지 않는 경우 공급업체의 기술 지원부에 문의하십시오.

경고 : P=0 ???의 로그인

AIX 이외의 시스템에서 시작 중에 이 경보 메시지가 나타나면 무시할 수 있습니다. 정상 작업(seosd 가 시작되어 실행된 후) 중에 또는 AIX 에서 시작 중에 이 메시지가 나타나면 소프트웨어 오류를 나타내므로, 이 경우 공급업체의 기술 지원부에 문의해야 합니다.

경고 : CA Access Control 에서 P=ppp 을 중지하지 못했습니다. 이유=nnn

예방 조치로 CA Access Control 은 중요한 권한을 얻으려고 시도하여 루프홀을 생성할 수 있는 프로세스를 중지합니다. 이러한 이벤트는 권한 없는 UID(setuid 시스템 호출)를 서로게이트하려는 시도일 수 있습니다. CA Access Control 이 위반 프로세스를 중지하려고 했지만 실패했습니다. 실패 원인은 kill 시스템 호출에서 반환되는 원인 코드에서 자세히 설명합니다.

경고 : P=ppp 이(가) NULL 이 아닌 항목에 대한 터미널입니다.

이 경고는 CA Access Control 이 시스템에 알려지지 않은 새 프로세스를 발견했으며 해당 실행 프로그램을 알 수 없을 때 나타납니다. 대부분의 경우 메시지를 무시할 수 있습니다. 예상된 결과가 나타나지 않는 경우 공급업체의 기술 지원부에 문의하십시오.

경고 : 알 수 없는 P=ppp

이 메시지는 CA Access Control 에 알려지지 않은 프로세스에서 작성된 포크 요청을 나타냅니다. 이 메시지가 시작 중 seoswd 또는 seagent 에 대해 나타날 경우 메시지를 무시할 수 있습니다. 그 외의 경우에는 CA Access Control 이 해당 프로세스의 실제 권한을 확인할 수 없으므로 소프트웨어 오류를 암시할 수 있습니다. 후자의 경우 공급업체의 기술 지원부에 문의하십시오.

WATCHDOG: 여기 있는지 확인(AYT)

seoswd 데몬은 seosd 가 활동 중이고 예상된 응답을 반환하는지 확인하려고 했습니다. 메시지 텍스트에서 AYT 는 seoswd 의 "사용자 위치 확인" 질문입니다. 이 메시지는 무시할 수 있으며 무시해야 합니다. trcfilter.init 파일을 사용하여 메시지를 필터링하십시오. 메시지는 seoswd 가 정상적으로 작동하고 있음을 의미합니다.

WATCHDOG: Init initializationtext

seoswd 초기화 메시지로, 무시할 수 있습니다.

WATCHDOG: 로그 logtext

seoswd 데몬이 로그 요청을 작성했습니다. 로그 요청은 log-text 에 자세히 설명되어 있습니다.

WATCHDOG: SecFile operation result

seoswd 데몬이 보안 파일에 관한 정보를 추출하도록 요청했습니다. 메시지 텍스트에서 operation 은 GETFIRST 또는 GETNEXT 가 될 수 있습니다. 해당 정보가 추출되면 결과가 OK 가 되고 CA Access Control 데이터베이스에 더 이상 보안 파일이 없으면 NOFOUND 가 됩니다. 이 메시지는 보안 파일을 검색하는 seoswd 의 정상 동작을 나타냅니다.

WATCHDOG: 타이머

seoswd 데몬은 seos.ini 파일 설정에 따라 몇 초 간격으로 타이머 요청을 작성합니다. 메시지를 필터링할 수 있으며 trcfilter.init 파일을 사용하여 메시지를 필터링해야 합니다.

WATCHDOG: Trust Pgm: programname [OK | NOTOK]

seoswd 데몬이 지정한 프로그램을 트러스트된 프로그램으로 표시했습니다. 이것은 지정한 프로그램이 디지털 서명 테스트를 통과했음을 암시합니다. 메시지 텍스트에서 OK 는 트러스트 작업이 성공적으로 완료되었음을 의미하고 NOTOK 는 seoswd 가 이 프로그램을 트러스트된 프로그램으로 표시하지 못했음을 의미합니다. 손상된 데이터베이스로 인해 NOTOK 가 발생할 수 있으며, 이 경우 공급업체의 기술 지원부에 문의해야 합니다.

WATCHDOG: Untrust Pgm: programname [OK | NOTOK]

seoswd 데몬이 지정한 프로그램을 언트러스트된 프로그램으로 표시했습니다. 이것은 지정한 프로그램이 seoswd 의 디지털 서명 검사를 통과하지 못했음을 암시합니다. 메시지 텍스트에서 OK 는 언트러스트 작업이 성공적으로 완료되었음을 의미하고 NOTOK 는 seoswd 가 이 프로그램을 언트러스트된 프로그램으로 표시하지 못했음을 의미합니다. 손상된 데이터베이스로 인해 NOTOK 가 발생할 수 있으며, 이 경우 공급업체의 기술 지원부에 문의해야 합니다.

부록 C: 문자열 일치

이 장은 아래의 주제를 포함하고 있습니다.

와일드카드 식 (페이지 575)
예: 와일드카드 일치 (페이지 576)

와일드카드 식

이 절에서는 와일드카드 식 작성에 사용할 수 있는 구문에 대해 설명합니다.

CA Access Control 은 와일드카드 일치와 문자 목록을 사용하여 문자열 일치(globbing)를 수행합니다.

와일드카드 일치

CA Access Control 은 다음의 와일드카드 문자를 지원합니다.

문자	일치
* (별표)	0 개 이상의 임의 문자
? (물음표)	임의의 단일 문자

문자 목록

각괄호([ ])로 묶인 문자 목록에는 한 개 이상의 문자가 포함될 수 있습니다. CA Access Control 은 이러한 문자를 긍정 또는 부정 일치 기준으로 사용합니다.

문자 목록은 하나 이상의 문자로 구성될 수 있습니다. 이 목록 유형에서 CA Access Control 은 목록에 있는 임의의 한 문자를 일치시킵니다. 각괄호 안의 목록 앞에 캐럿(^)이 있으면 CA Access Control 은 목록에 없는 임의의 한 문자를 일치시킵니다.

범위는 일정한 범위의 문자를 지정하는 문자 목록 유형입니다. CA Access Control 은 목록의 모든 문자를 일치시킵니다(경계 포함). 목록 앞에 캐럿(^)이 있으면 CA Access Control 은 지정된 목록의 모든 문자를 제외합니다. 범위의 양쪽 끝을 모두 지정하거나 처음과 끝 문자만 지정할 수도 있습니다.

다음 표에는 사용할 수 있는 문자 목록이 설명되어 있습니다. 이 구문에 각괄호를 포함해야 한다는 것을 명심하십시오. ch1, ch2 및 chN 은 각각 한 문자를 나타냅니다.

목록	설명
[ch1ch2...chN**]**	CA Access Control 은 각괄호로 묶인 목록에 있는 임의의 한 문자를 일치시킵니다.
[^ch1ch2...chN**]**	CA Access Control 은 각괄호로 묶인 목록에 없는 임의의 한 문자를 일치시킵니다.
[ch1-ch2**]**	CA Access Control 은 범위(경계 포함)에 포함된 임의의 한 문자를 일치시킵니다.
[^ch1-ch2**]**	CA Access Control 은 범위(경계 포함)에 포함되지 않는 임의의 한 문자를 일치시킵니다.
[-ch2**]**	CA Access Control 은 지정한 문자(ch2)보다 작거나 같은 ASCII 값을 가진 임의의 한 문자를 일치시킵니다.
[^-ch2**]**	CA Access Control 은 지정한 문자(ch2)보다 크거나 같은 ASCII 값을 가진 임의의 한 문자를 일치시킵니다.
[ch1-**]**	CA Access Control 은 지정한 문자(ch1)보다 크거나 같은 ASCII 값을 가진 임의의 한 문자를 일치시킵니다.
[^ch1-**]**	CA Access Control 은 지정한 문자(ch1)보다 작거나 같은 ASCII 값을 가진 임의의 한 문자를 일치시킵니다.

예: 와일드카드 일치

한 문자를 다른 모든 한 문자와 일치하는 문자로 만들려면 다음과 같이 물음표(?)를 사용하십시오.

지정 값	일치 값
mmc?	mmc3, mmcx, mmc5
mmc?.t	mmc1.t, mmc2.t
mmc04.?	mmc04.a, mmc04.1

0 개 또는 하나 이상의 문자가 일치하려면 별표(*)를 사용하십시오.

지정 값	일치 값
i.c	main.c, list.c 등
st*.h	stdio.h, stdlib.h, string.h 등
*	지정한 클래스의 모든 레코드

목록에 있는 임의 문자가 일치하려면 다음 예제 중 하나를 따르십시오.

지정 값	일치 값
[abcgk]	a, b, c, g 또는 k
[^abcgk]	a, b, c, g 또는 k 를 제외한 임의 문자, 예:A, B, d, e, f 또는@
[a-z]	a 와 z 사이의 임의 문자(a 와 z 포함)
[^a-z]	"a"보다 작거나 "z"보다 큰 ASCII 값을 가진 임의 문자
[Z-]	Z 보다 큰 ASCII 값을 가진 모든 문자(예: a, b, \ 또는 ~)
[^-A]	A 보다 작지 않은 ASCII 값을 가진 모든 문자(예: B, a, c 또는 ~)

부록 D: 사용된 포트

이 장은 아래의 주제를 포함하고 있습니다.

UNIX 사용된 포트 (페이지 579)
Windows 사용된 포트 (페이지 580)
서버 구성 요소에 사용되는 포트 (페이지 581)
UNAB 사용된 포트 (페이지 582)

UNIX 사용된 포트

CA Access Control 은 UNIX 에서 기본적으로 다음의 TCP 포트를 사용합니다.

숫자	설명	수신자	전송자	설명
8891	CA Access Control 클라이언트 응용 프로그램	CA Access Control 에이전트	dbmgr(seosd 가 실행 중일 때), devcalc, dmsmgr, policydeploy, policyreport, sechkey(원격 컴퓨터를 관리할 때), secons, segrace, segracex, seini(원격 컴퓨터를 관리할 때), selang(seosd 가 실행 중일 때), senable, sepass, sereport, seretrust, serevu, sesu, sesudo, sewhoami, sepmdd(PMD)	/etc/services 파일 설정을 수정하면 기본 포트 번호를 변경할 수 있습니다. 이렇게 하려면 다음 행을 추가하고 CA Access Control 데몬을 다시 시작하십시오. `seoslang2 port-number/tcp`
5249	SSL 통신	CA Access Control 에이전트	**참고:** FIPS 를 준수하는 통신을 제공하는 구성 요소에 대해 알아보려면 릴리스 정보를 참조하십시오.	FIPS 140-2 준수
8892	원격 컴퓨터에서 seosd 시작	seosload	selaod	seload 가 원격 컴퓨터에서 데몬을 로드하면 원격 컴퓨터의 inetd(인터넷 서비스 데몬)가 rseloadd 프로그램을 실행합니다. 이 프로그램은 seload 를 로컬에서 실행하고 종료합니다. 또한 이

숫자	설명	수신자	전송자	설명
				포트에서 매개 변수를 수신합니다. /etc/services 파일 설정을 수정하면 기본 포트 번호를 변경할 수 있습니다. 이렇게 하려면 다음 행을 추가하고 CA Access Control 데몬을 다시 시작하십시오. `seosload port-number/tcp` **참고:** 이 포트로는 중요한 정보가 전송되지 않으므로 이 포트를 통한 통신은 암호화되지 않습니다.

Windows 사용된 포트

CA Access Control 은 Windows 에서 기본적으로 다음의 TCP 포트를 사용합니다.

숫자	설명	수신자	전송자	설명
8891	CA Access Control 클라이언트 응용 프로그램	CA Access Control 에이전트	selang.exe, sepmdd.exe(PMD), eACSigUpdate.exe, SegraceW.exe(유예 로그인 및 암호 설정), secons.exe(원격 종료 및 IP 주소 새로 고침), policydeploy.exe, devcalc.exe, policyfetcher.exe	%SystemRoot%\drivers\etc\services 파일 설정을 수정하면 기본 포트 번호를 변경할 수 있습니다. 이렇게 하려면 다음 행을 추가하고 CA Access Control 서비스를 다시 시작하십시오. `seoslang2 port-number/tcp`
5249	SSL 통신	CA Access Control 에이전트	**참고:** FIPS 를 준수하는 통신을 제공하는 구성 요소에 대해 알아보려면 릴리스 정보를 참조하십시오.	FIPS 140-2 준수

서버 구성 요소에 사용되는 포트

CA Access Control 은 서버 구성 요소에 대해 기본적으로 다음의 TCP 포트를 사용합니다.

숫자	설명	수신자	보낸 사람
7222	보고서 스냅숏	배포 서버	보고서 에이전트
7243	SSL 을 사용하는 보고서 스냅숏	배포 서버	보고서 에이전트
5248	로컬 웹 기반 인터페이스 통신	CA Access Control 웹 서비스	CA Access Control 끝점 관리, CA Access Control 엔터프라이즈 관리

이러한 포트 외에도 다음에서 포트를 열어야 합니다.

- 배포 서버 또는 CA Access Control 엔터프라이즈 관리가 별도의 컴퓨터에 있는 경우 이러한 대상과 통신하기 위해 중앙 데이터베이스 컴퓨터에서 포트를 열어야 합니다.
- 원격 컴퓨터에서 InfoView 응용 프로그램에 액세스하기 위해 보고서 포털(BusinessObjects) 컴퓨터에서(기본값: 8080).
- 원격 컴퓨터에서 웹 기반 인터페이스에 액세스하기 위해 CA Access Control 끝점 관리 및 CA Access Control 엔터프라이즈 관리 컴퓨터에서 포트(기본값: 18080)를 열어야 합니다.
- 원격 컴퓨터에서 웹 기반 인터페이스에 액세스하기 위해 Oracle 데이터베이스가 설치된 컴퓨터에서 포트(기본값: 8080 또는 SSL 의 경우 7443)를 열어야 합니다.
- CA Access Control 에이전트 포트를 통해 연결하기 위해 다음 구성 요소에 대한 고급 정책 관리 서버 구성 요소에서(기본값: SSL 에 대해 8891 또는 5249).
  - DMS 에서 DH 로
  - DH 에서 DMS 로
  - 원격 서버에서 policyfetcher 및 devcalc 를 DH 에

UNAB 사용된 포트

UNAB 는 UNIX 에서 기본적으로 다음의 TCP 포트를 사용합니다.

숫자	설명	수신자	보낸 사람
88	Kerberos 트래픽	Active Directory	UNAB
389	Kerberized LDAP	Active Directory	UNAB
445	Microsoft 디렉터리 서비스	Active Directory	UNAB
464	Kerberos kpasswd	Active Directory	UNAB
3268	전역 카탈로그	Active Directory	UNAB

UNAB 는 UNIX 에서 기본적으로 다음의 UDP 를 사용합니다.

숫자	설명	수신자	보낸 사람
53	DNS	Active Directory	UNAB
88	Kerberos 트래픽	Active Directory	UNAB
123	NTP	Active Directory	UNAB
389	Kerberized LDAP	Active Directory	UNAB

부록 E: 보고 데이터베이스 스키마

이 장은 아래의 주제를 포함하고 있습니다.

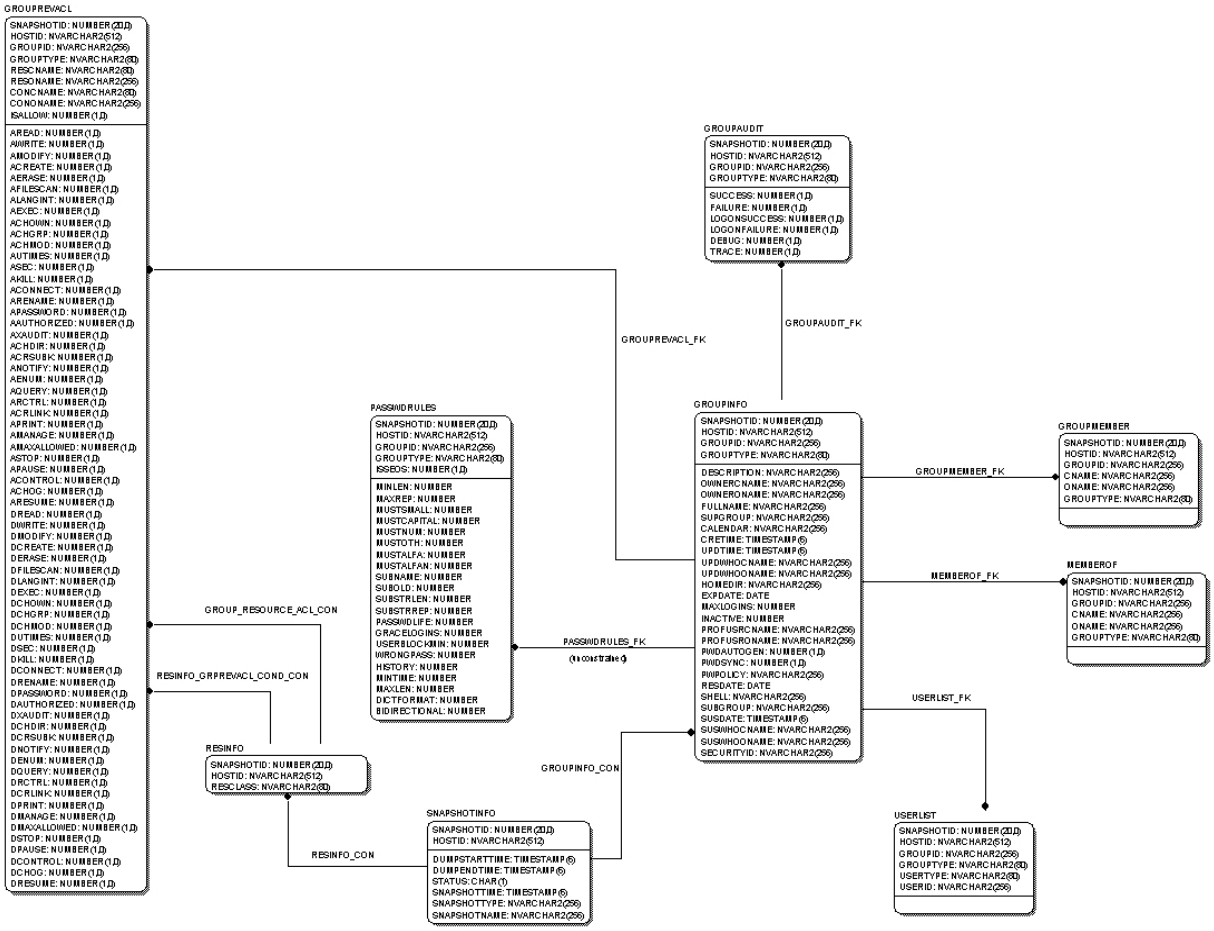
스키마 도표 (페이지 583)
테이블 (페이지 590)
관계 (페이지 684)

스키마 도표

다음 항목에서는 CA Access Control 보고 데이터베이스의 스키마에 대해 설명합니다.

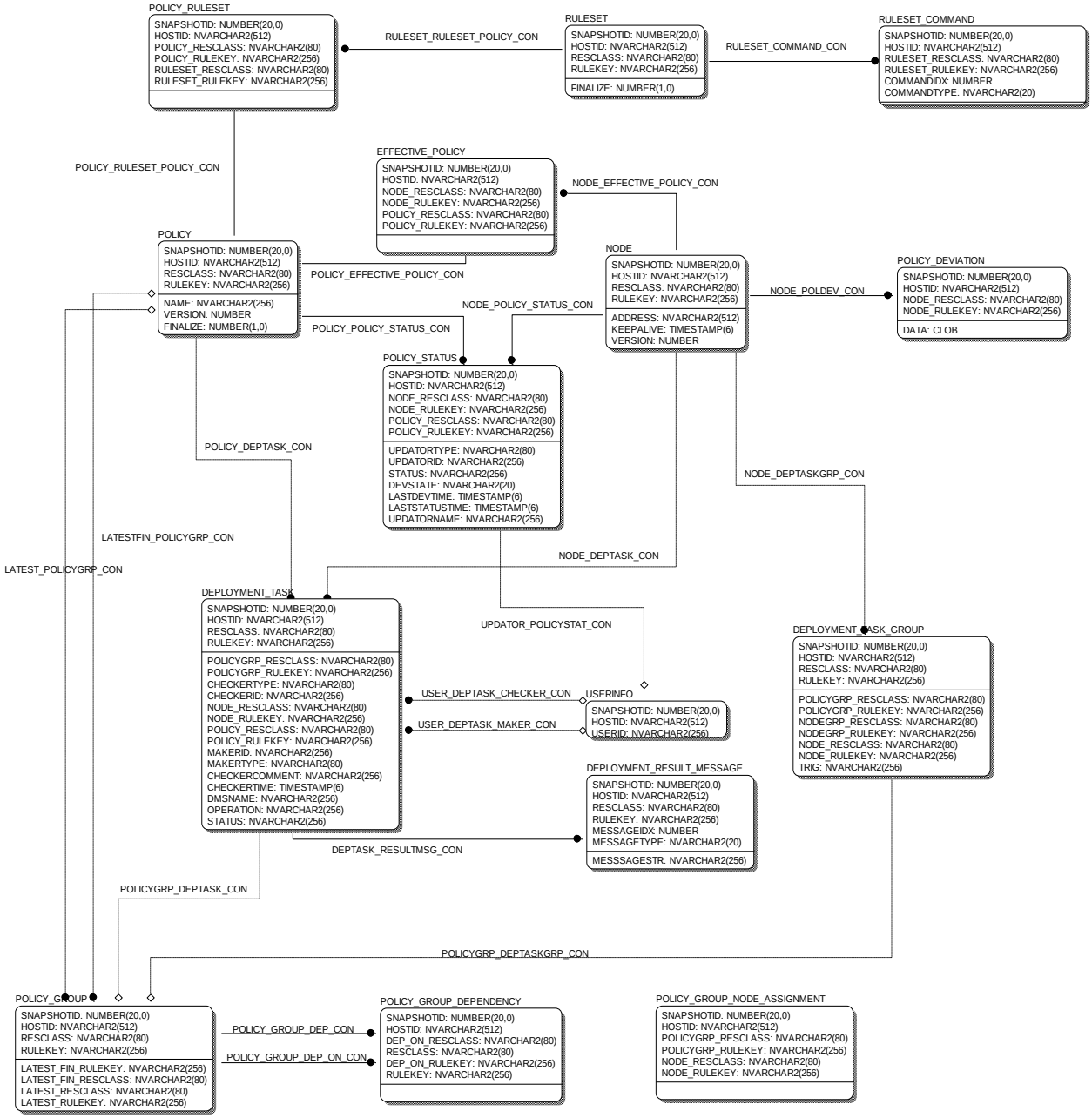
그룹

그룹 관련 테이블에 대한 도표입니다.



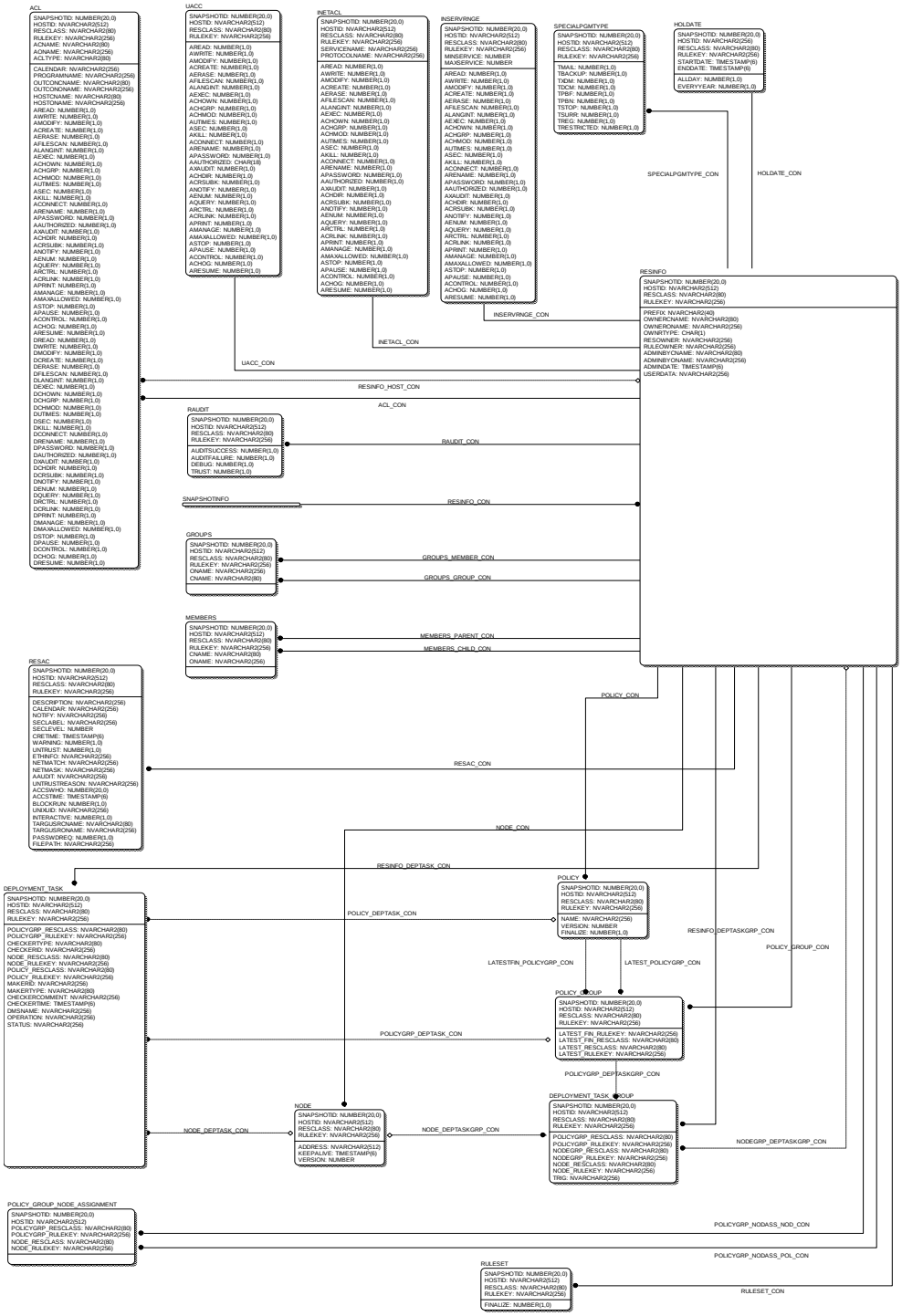
정책 관리

정책 관리 관련 테이블에 대한 도표입니다.



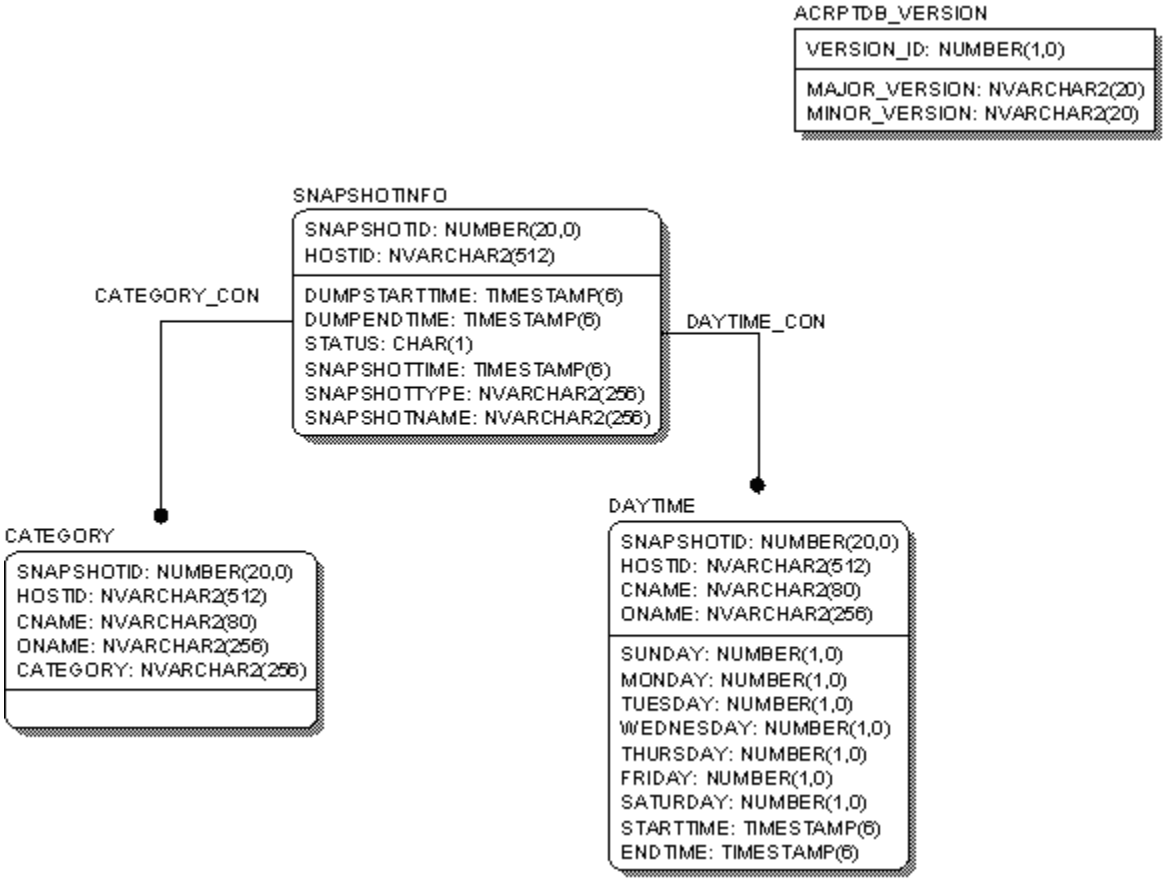
리소스

리소스 관련 테이블에 대한 도표입니다.



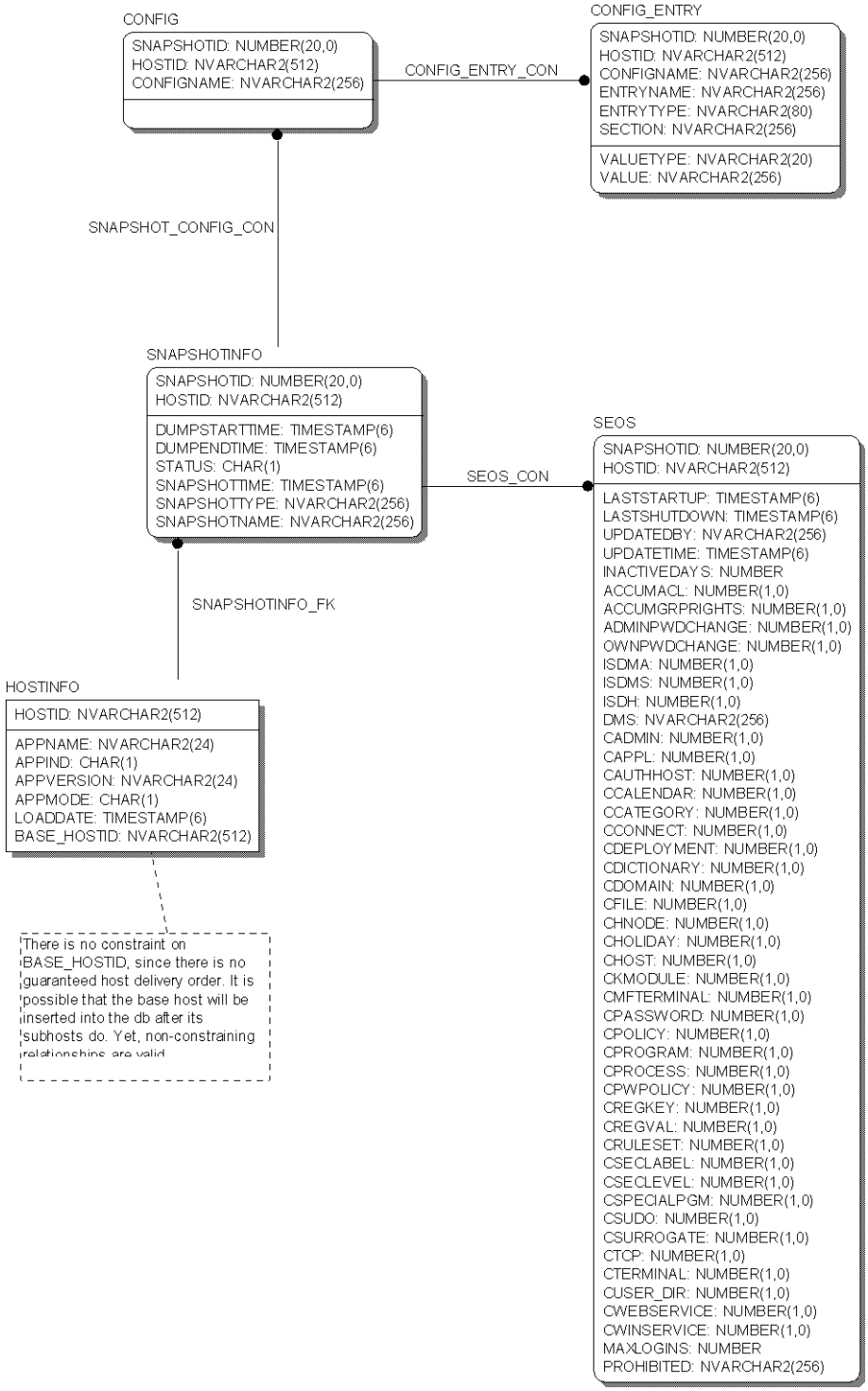
공유 속성

사용자, 그룹 및 리소스 개체의 공유 속성에 대한 도표입니다.



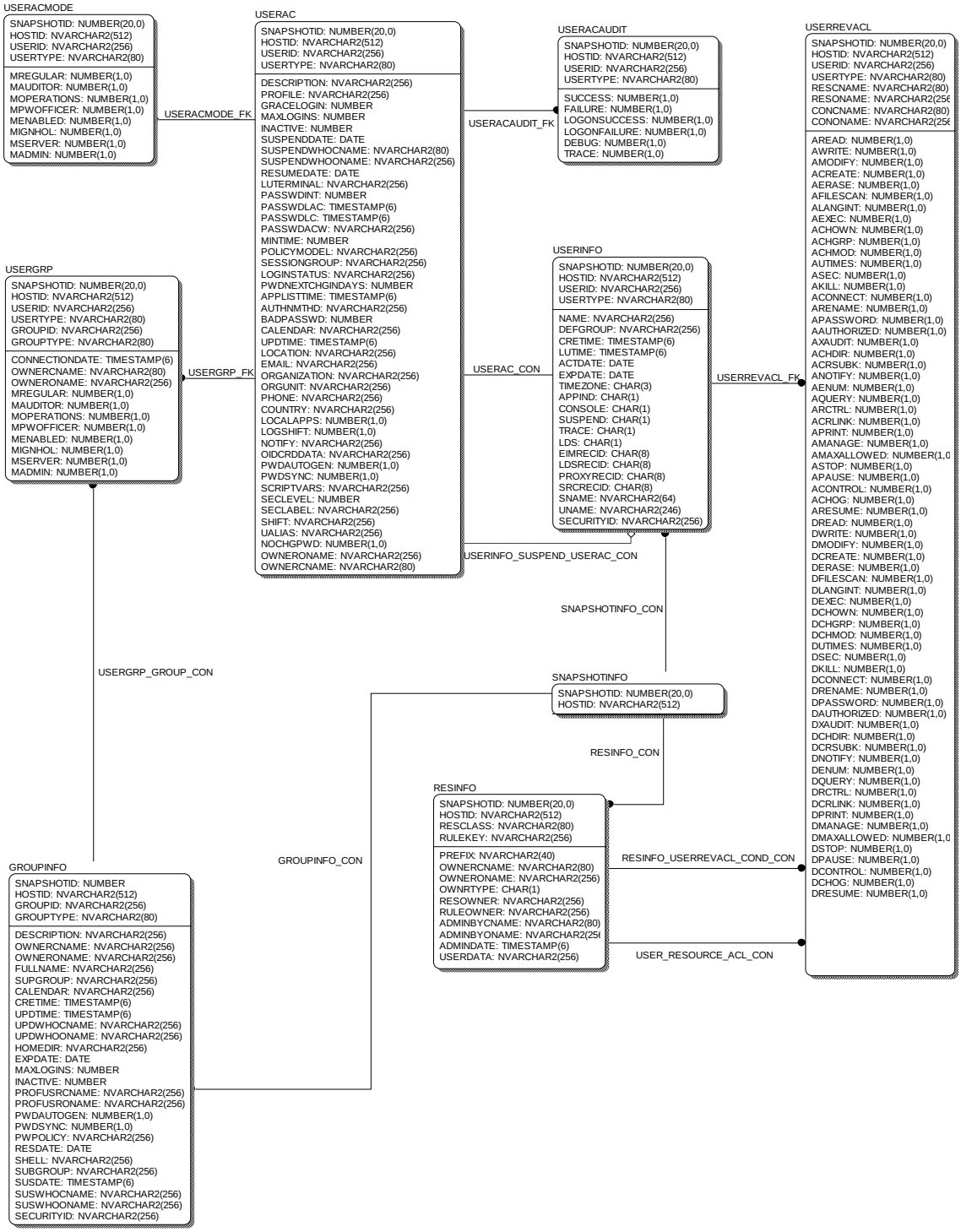
스냅숏

스냅숏 및 끝점 관련 테이블에 대한 도표입니다.



사용자

사용자 관련 테이블에 대한 도표입니다.



테이블

다음 표에서는 스키마에 있는 테이블 이름을 표시하고 각 테이블에 대해 간단히 설명합니다.

이름	설명
ACL	대부분의 CA Access Control 리소스에 대한 액세스 제어 목록입니다. 이 테이블은 CA Access Control 속성인 ACL, NACL, PACL, CACL, CALACL 을 결합합니다. ACL - 리소스에 액세스할 수 있는 권한이 있는 사용자 이름 및 그룹 이름과 각 이름에 부여된 액세스 수준을 포함하는 표준 액세스 제어 목록입니다. NACL - 리소스에 액세스할 수 있는 권한이 없는 사용자 이름 또는 그룹 이름을 포함하는 네거티브 액세스 제어 목록입니다. PACL - 액세스 프로그램에 따라 결정되는 프로그램 액세스 제어 목록입니다. 각 PACL 에는 사용자 이름과 그룹 이름, 액세스 수준, 특정 리소스에 액세스하기 위해 사용자가 실행해야 하는 프로그램이나 셸 스크립트의 이름이 있습니다. CACL - 조건부 액세스 제어 목록입니다. CALACL - 달력 액세스 제어, Unicenter® TNG 달력에 따라 달라지는 리소스 ACL 입니다. Axxxx 및 Dxxxx 열은 지원되는 모든 리소스 유형에 대해 지원되는 모든 허용(A) 및 거부(D) 권한을 나타냅니다. 몇몇 권한은 특정 리소스 유형에만 적용됩니다. 예를 들어 시작, 중지 및 일시 중지 권한은 프로세스와 서비스에만 적용되며 파일에는 적용될 수 없습니다.
ACRPTDB_VERSION	DB 스키마 업그레이드를 제어하는 데 사용되는 DB 스키마 버전입니다.
CATEGORY	리소스 개체 / 사용자 개체 / 그룹 개체에 대한 B1 기능(보안 범주)입니다.
CONFIG	0 개 이상의 구성 항목을 저장하는 CA Access Control 구성 저장소입니다(CONFIG_ENTRY 참조).
CONFIG_ENTRY	구성 저장소 내의 단일 구성 항목입니다.

이름	설명
DAYTIME	사용자가 리소스에 액세스할 수 있는 요일 및 시간을 지정합니다.
DEPLOYMENT_RESULT_MESSAGE	배포 작업의 결과 메시지입니다.
DEPLOYMENT_TASK	단일 노드에 단일 정책을 배포/배포 취소하는 작업인 단일 정책 배포 작업을 설명합니다.
DEPLOYMENT_TASK_GROUP	다음 배포 관련 작업 중 하나만 설명합니다. 1. 하나의 노드 그룹 하나의 노드 할당 2. 하나의 노드에 하나의 정책 그룹 할당 3. 하나의 노드 그룹에 하나의 정책 그룹 할당 표시된 것처럼 이 작업은 바이너리입니다. 여기서 첫 번째 연산자는 노드 또는 정책 그룹이고 두 번째 연산자는 노드 또는 노드 그룹입니다.
DISTRIBUTION_HOST	재해 복구 모드를 위한 배포 호스트입니다. CA Access Control SEOS 클래스의 DH 및 DHDR 속성 내에서 요소에 매핑됩니다.
EFFECTIVE_POLICY	노드 그룹, 정책 그룹 등을 통해 암시적 관계를 포함하여 정책 모델에서 어떤 정책과 어떤 노드가 관련되는지 참조합니다.
GROUPAUDIT	그룹 개체에 대한 감사 설정입니다.
GROUPINFO	그룹 개체 정보입니다.
GROUPMEMBER	그룹의 구성원이 되는 그룹입니다.
GROUPREVACL	그룹 역방향 ACL(예: 특정 조건에서 특정 리소스에 대해 그룹에 포함된 ACL)입니다. 모든 Axxx 및 Dxxxx(허용/거부) 열에 대한 자세한 내용은 ACL 표를 참조하십시오.
GROUPS	리소스 개체와 사용자 개체의 그룹 속성입니다. USER 레코드가 속하는 사용자 그룹(GROUP 레코드)의 목록입니다. 이 속성에는 사용자가 속해 있는 각 그룹의 사용자에게 할당된 모든 그룹 권한(예: 그룹 관리 권한(GROUP-ADMIN))도 포함되어 있습니다. 이 속성에 포함된 그룹 목록은 네이티브 환경 GROUPS 속성에 있는 목록과 다를 수도 있습니다.
HOLDATE	휴일 개체에 대한 휴일 정보입니다.
HOSTINFO	호스트 정보는 네트워크에 있는 CA Access Control

이름	설명
	끝점을 나타냅니다.
INETACL	INET-ACL - 인터넷 액세스 제어 목록입니다. 로컬 호스트가 클라이언트 호스트 그룹에 제공할 수 있는 서비스 및 해당 액세스 유형입니다. 액세스 제어 목록에 있는 각 요소는 다음 정보를 포함합니다. 1. 서비스 참조-서비스에 대한 참조(포트 번호 또는 이름)입니다. 모든 서비스를 지정하려면 별표(*)를 서비스 참조로 입력하십시오. 2. 허용된 액세스-클라이언트 호스트가 서비스에 대해 갖는 액세스의 유형입니다. 올바른 액세스 유형 및 액세스 유형이 부여하는 권한은 다음과 같습니다. - read-로컬 호스트가 호스트 그룹에 서비스를 제공할 수 있습니다. - none-로컬 호스트가 호스트 그룹에 서비스를 제공할 수 없습니다. 모든 Axxx 및 Dxxxx(허용/거부) 열에 대한 자세한 내용은 ACL 표를 참조하십시오.
INSERVRNGE	서비스 범위 ACL 입니다. INETACL 속성과 유사합니다. 이 속성은 로컬 호스트가 클라이언트 호스트의 그룹에 제공하는 서비스를 명시적으로 지정하는 대신 서비스의 범위를 지정합니다. 모든 Axxx 및 Dxxxx(허용/거부) 열에 대한 자세한 내용은 ACL 표를 참조하십시오.
LOCAL_PMD_SUBSCRIBER	정책 모델 구독 항목을 나타냅니다. 각 항목은 sepmd -L selang 명령에 의해 제공되는 개별 구독 항목에 매핑됩니다.
LOGINAPPL	LOGINAPPL 클래스는 로그인 응용 프로그램을 관리하고 검색합니다. 이 클래스를 사용하여 로그인 응용 프로그램을 정의하고 이 응용 프로그램을 사용하여 로그인을 제어하는 액세스 제어 규칙을 설정할 수 있습니다. 각 열의 설명에는 해당 CA Access Control 클래스, 속성 및 해당 값에 대한 참조가 포함되어 있습니다. 자세한 내용은 selang 참조 안내서를 참조하십시오.
MEMBEROF	이 그룹이 구성원인 그룹입니다.
MEMBERS	리소스 개체의 구성원 속성입니다.
NODE	정책 준수가 적용되는 CA Access Control 호스트를

이름	설명
	정의합니다. 노드 그룹은 단순 리소스 엔터티별로 표시됩니다(RESINFO/RESAC 참조). 노드와 노드 그룹의 관계는 다른 리소스와 마찬가지로 GROUPS/MEMBERS 메커니즘에 의해 처리됩니다(GROUPS/MEMBERS/RESINFO 테이블 참조)
NODE_ADDRESS	노드의 네트워크 주소 0 개 이상을 나타냅니다. CA Access Control HNODE 클래스의 HNODE_IP 속성에 매핑됩니다.
NODE_ALIAS	노드의 별칭 주소 0 개 이상을 나타냅니다. CA Access Control HNODE 클래스의 ALIAS 속성에 매핑됩니다.
NODE_DEVIATION	호스트 수준 위반 세부 정보입니다.
NODE_SUBSCRIPTION_STATUS	정책 배포 목적으로 다양한 HNODE 사이의 구독 관계와 상태를 설명합니다.
PASSWDRULES	암호 규칙을 지정합니다. 이 속성에는 CA Access Control 에서 암호 보호를 처리하는 방법을 결정하는 여러 필드가 있습니다. 규칙의 전체 목록은 USER 클래스의 수정 가능한 PROFILE 속성을 참조하십시오.
POLICY	노드의 준수 상태와 정책을 적용하는 데 필요한 작업을 설명합니다. 각 정책 엔터티는 다른 정책의 초기 버전이나 후속 버전을 나타냅니다. 초기 정책은 항상 단일 정책 그룹에 할당되고(POLICY_GROUP 테이블 참조) 해당 정책의 모든 후속 버전은 이 정책 그룹에 포함됩니다.
POLICY_DEVIATION	노드 유효 정책과의 위반(정책 위반)을 설명합니다.
POLICY_GROUP	동일한 초기 정책의 후속 버전인 모든 정책을 포함합니다.
POLICY_GROUP_DEPENDENCY	다른 정책 그룹에 따라 달라지는 정책 그룹을 설명합니다. 독립 정책 그룹은 이 테이블에 나타나지 않습니다.
POLICY_GROUP_NODE_ASSIGNMENT	정책 모델에서 어떤 정책이 어떤 노드(또는 노드 그룹)에 할당되는지 설명합니다. 정책이 노드에 할당되면 NODE_RESCLASS 가 HNODE 가 됩니다. 정책이 노드 그룹에 할당되면 NODE_RESCLASS 가 GHNODE 가 됩니다.

이름	설명
	이 테이블은 노드 및 노드 그룹 할당에 모두 사용됩니다. 정책 그룹과 노드(또는 노드 그룹)의 관계는 다른 리소스와 마찬가지로 GROUPS/MEMBERS 메커니즘에 의해 처리됩니다(GROUPS/MEMBERS/RESINFO 테이블 참조).
POLICY_RULESET	정책과 해당 규칙 집합 사이의 링크입니다.
POLICY_STATUS	정책과 관련된 각 노드에 대해 해당 정책 상태(예: 정책이 배포 또는 배포 취소되었는지 여부 등)를 설명합니다(EFFECTIVE_POLICY 참조).
POLICYMODELINFO	정책 모델 정보입니다. 특정 노드에 의해 다른 노드에 배포된 정책에 대한 상태가 포함됩니다.
RAUDIT	CA Access Control 이 감사 로그에 기록하는 액세스 이벤트의 유형입니다.
RESAC	CA Access Control 리소스 정보입니다.
RESINFO	CA Access Control 리소스 정보입니다.
RULESET	정책 배포/배포 취소의 일부로 실행되는 명령 집합입니다.
RULESET_COMMAND	단일 selang 명령으로, 대부분 규칙 집합으로 구성됩니다.
SEOS	옵션 정보를 설정합니다.
SEOSSYSCALL	(r12.0 SP1) CA Access Control 주 커널 모듈로, 주로 허용 또는 거부를 결정하기 위해 seosd 가 참조되는 OS 이벤트를 차단하기 위해 사용됩니다.
SNAPSHOTINFO	스냅숏 정보는 수집 시 단일 로컬 AC 데이터베이스(단일 호스트)에 있는 수집된 데이터를 모두 표시합니다.
SPECIALPGMTYPE	SPECIALPGM 클래스에 대한 특수 프로그램 유형입니다. AC 에서 자동으로 생성된 프로그램 정보입니다. Watchdog 은 이 속성에 저장된 정보를 자동으로 확인합니다. 이 정보가 변경되면 CA Access Control 은 해당 프로그램을 언트러스트된 것으로 정의합니다. 각 레코드는 CA Access Control SPECIALPGM 클래스의 단일 SPECIALPGMTYPE 속성을

이름	설명
	나타냅니다.
SYSCALL	(r12.0 SP1) CA Access Control 주 커널 모듈로, 주로 허용 또는 거부를 결정하기 위해 seosd 가 참조되는 OS 이벤트를 차단하기 위해 사용됩니다.
SYSCALLUSERSPECIALPGM	(r12.0 SP1) CA Access Control 주 커널 모듈로, 주로 허용 또는 거부를 결정하기 위해 seosd 가 참조되는 OS 이벤트를 차단하기 위해 사용됩니다.
UACC	기본 액세스 권한은 개체에 대한 액세스를 요청하는 모든 접근자에게 부여된 권한이지만, 개체의 액세스 제어 목록에는 없습니다. 데이터베이스에 정의되지 않은 사용자도 기본 액세스 권한을 받습니다. 모든 Axxx 및 Dxxxx(허용/거부) 열에 대한 자세한 내용은 ACL 표를 참조하십시오. 각 레코드는 다양한 CA Access Control 리소스 클래스의 UACC 속성을 나타냅니다. 모든 Axxx 및 Dxxxx(허용/거부) 열에 대한 자세한 내용은 ACL 표를 참조하십시오.
USERAC	CA Access Control 사용자 정보입니다. 이 테이블의 각 레코드는 USER/XUSER 클래스의 단일 CA Access Control 개체에 대한 AC 특정 속성을 나타납니다.
USERACAUDIT	CA Access Control 사용자 감사 설정입니다. 각 레코드는 CA Access Control USER/XUSER 클래스의 CA Access Control AUDIT_MODE 속성의 단일 항목을 나타냅니다.
USERACMODE	CA Access Control 사용자 모드(OBJ_TYPE)입니다. 각 레코드는 CA Access Control USER/XUSER 클래스의 CA Access Control OBJ_TYPE 속성의 단일 항목을 나타냅니다.
USERGRP	그룹에 대한 사용자 연결입니다. 각 레코드는 CA Access Control USER/XUSER 클래스의 CA Access Control GROUPS 속성의 단일 항목을 나타냅니다.
USERINFO	기본 사용자 정보입니다. 모든 사용자의 이 테이블에는 레코드가 있어야 합니다. 이 테이블은 사용자 정보의 다른 세그먼트를 나타내는 다른 USER 테이블의 부모입니다.

이름	설명
USERLIST	그룹 개체의 사용자 목록(구성원)입니다. 각 레코드는 CA Access Control GROUP/XGROUP 클래스의 CA Access Control USERLIST 속성의 단일 OID 항목을 나타냅니다.
USERREVACL	사용자 역방향 ACL(예: 특정 조건에서 특정 리소스에 대해 사용자에 포함된 ACL)입니다. 모든 Axxx 및 Dxxxx(허용/거부) 열에 대한 자세한 내용은 ACL 표를 참조하십시오. 각 레코드는 CA Access Control USER/XUSER 클래스의 CA Access Control REVACL 속성의 단일 항목을 나타냅니다.

ACL 테이블 열

다음 표에서는 ACL 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 ACL 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 ACL 레코드의 호스트 ID
RESCLASS	예	NVARCHAR2(80)	NOT NULL	이 ACL 레코드의 리소스 클래스 이름(예: FILE, PROCESS)
RULEKEY	예	NVARCHAR2(256)	NOT NULL	이 ACL 레코드의 리소스 개체 이름
ACNAME	예	NVARCHAR2(80)	NOT NULL	접근자 클래스 이름
AONAME	예	NVARCHAR2(256)	NOT NULL	액세스 개체 이름
ACLTYPE	예	NVARCHAR2(80)	NOT NULL	액세스 유형(예: R = 읽기, W = 쓰기)
ISALLOW	예	NUMBER(1,0)	NOT NULL	이 레코드에서 관련이 있는 열: Axxx(허용) 또는 Dxxx(거부) 특히 이 값은 allow-ACL 항목 또는 deny-ACL 항목입니다.
CONDHASH	예	NUMBER(20,0)	NOT NULL	ACLTYPE 에 따라 이 ACL 의

이름	PK 여부	데이터 유형	Null 옵션	설명
				해시된 조건 값을 나타냅니다. PACL 의 경우 PROGRAMNAME 필드의 해시를 나타냅니다. CACL 의 경우 OUTCONCNAME, OUTCONONAME, HOSTCNAME, HOSTONAME 의 해시입니다. CALACL 의 경우 CALENDAR 의 해시입니다. ACL 및 NACL 의 경우 0 입니다.
CALENDAR	아니요	NVARCHAR2 (256)	NULL	달력 이름(CALACL 레코드의 경우)
PROGRAMNAME	아니요	NVARCHAR2 (256)	NULL	프로그램 이름(PACL 레코드의 경우)
OUTCONCNAME	아니요	NVARCHAR2(80)	NULL	ACLTYPE=CACL 인 경우 이 필드는 나가는 연결 클래스 이름을 갖습니다. GROUP 또는 XGROUP 은 GROUPINFO 테이블에 관련 레코드가 있음을 의미합니다. USER 또는 XUSER 는 USERINFO 테이블에 관련 레코드가 있음을 의미합니다. 다른 ACLTYPE 값의 경우 이 필드는 NULL 이 됩니다.
OUTCONONAME	아니요	NVARCHAR2 (256)	NULL	ACLTYPE=CACL 인 경우 이 필드는 나가는 연결 개체 이름을 갖습니다. 다른 ACNAME 값의 경우 이 필드는 NULL 이 됩니다.
HOSTCNAME	아니요	NVARCHAR2(80)	NULL	ACLTYPE=CACL 인 경우 이 필드는 호스트 클래스 이름(즉, 'HOST')을 가지며 RESINFO 테이블의 해당

이름	PK 여부	데이터 유형	Null 옵션	설명
				레코드에 연계됩니다. 다른 ACNAME 값의 경우 이 필드는 NULL 이 됩니다.
HOSTONAME	아니요	NVARCHAR2 (256)	NULL	ACLTYPE=CACL 인 경우 이 필드는 호스트 개체 이름을 갖습니다. 다른 ACNAME 값의 경우 이 필드는 NULL 이 됩니다.
AREAD	아니요	NUMBER(1,0)	NULL	읽기 액세스
AWRITE	아니요	NUMBER(1,0)	NULL	쓰기 액세스
AMODIFY	아니요	NUMBER(1,0)	NULL	수정 액세스
ACREATE	아니요	NUMBER(1,0)	NULL	작성 액세스
AERASE	아니요	NUMBER(1,0)	NULL	지우기 액세스
AFILESCAN	아니요	NUMBER(1,0)	NULL	파일 검색 액세스
ALANGINT	아니요	NUMBER(1,0)	NULL	
AEXEC	아니요	NUMBER(1,0)	NULL	실행 액세스
ACHOWN	아니요	NUMBER(1,0)	NULL	소유자 변경 액세스
ACHGRP	아니요	NUMBER(1,0)	NULL	그룹 변경 액세스
ACHMOD	아니요	NUMBER(1,0)	NULL	Chmod 유틸리티 실행 액세스
AUTIMES	아니요	NUMBER(1,0)	NULL	파일/폴더 리소스 업데이트 시간을 업데이트하기 위한 액세스
ASEC	아니요	NUMBER(1,0)	NULL	
AKILL	아니요	NUMBER(1,0)	NULL	
ACONNECT	아니요	NUMBER(1,0)	NULL	연결 액세스
ARENAME	아니요	NUMBER(1,0)	NULL	이름 변경 액세스
APASSWORD	아니요	NUMBER(1,0)	NULL	
AAUTHORIZED	아니요	NUMBER(1,0)	NULL	
AXAUDIT	아니요	NUMBER(1,0)	NULL	
ACHDIR	아니요	NUMBER(1,0)	NULL	폴더 리소스를 현재 작업 디렉터리로 설정하기 위한 액세스

이름	PK 여부	데이터 유형	Null 옵션	설명
ACRSUBK	아니요	NUMBER(1,0)	NULL	
ANOTIFY	아니요	NUMBER(1,0)	NULL	알림 액세스
AENUM	아니요	NUMBER(1,0)	NULL	열거 액세스
AQUERY	아니요	NUMBER(1,0)	NULL	쿼리 액세스
ARCTRL	아니요	NUMBER(1,0)	NULL	
ACRLINK	아니요	NUMBER(1,0)	NULL	
APRINT	아니요	NUMBER(1,0)	NULL	인쇄 액세스
AMANAGE	아니요	NUMBER(1,0)	NULL	관리 액세스
AMAXALLOWED	아니요	NUMBER(1,0)	NULL	
ASTOP	아니요	NUMBER(1,0)	NULL	중지 액세스
APAUSE	아니요	NUMBER(1,0)	NULL	일시 중지 액세스
ACONTROL	아니요	NUMBER(1,0)	NULL	제어 액세스
ACHOG	아니요	NUMBER(1,0)	NULL	
ARESUME	아니요	NUMBER(1,0)	NULL	다시 시작 액세스
DREAD	아니요	NUMBER(1,0)	NULL	읽기 거부
DWRITE	아니요	NUMBER(1,0)	NULL	쓰기 거부
DMODIFY	아니요	NUMBER(1,0)	NULL	수정 거부
DCREATE	아니요	NUMBER(1,0)	NULL	작성 거부
DERASE	아니요	NUMBER(1,0)	NULL	지우기 거부
DFILESCAN	아니요	NUMBER(1,0)	NULL	
DLANGINT	아니요	NUMBER(1,0)	NULL	
DEXEC	아니요	NUMBER(1,0)	NULL	실행 거부
DCHOWN	아니요	NUMBER(1,0)	NULL	
DCHGRP	아니요	NUMBER(1,0)	NULL	
DCHMOD	아니요	NUMBER(1,0)	NULL	
DUTIMES	아니요	NUMBER(1,0)	NULL	
DSEC	아니요	NUMBER(1,0)	NULL	
DKILL	아니요	NUMBER(1,0)	NULL	종료 거부

이름	PK 여부	데이터 유형	Null 옵션	설명
DCONNECT	아니요	NUMBER(1,0)	NULL	연결 거부
DRENAME	아니요	NUMBER(1,0)	NULL	이름 변경 거부
DPASSWORD	아니요	NUMBER(1,0)	NULL	
DAUTHORIZED	아니요	NUMBER(1,0)	NULL	
DXAUDIT	아니요	NUMBER(1,0)	NULL	
DCHDIR	아니요	NUMBER(1,0)	NULL	
DCRSUBK	아니요	NUMBER(1,0)	NULL	
DNOTIFY	아니요	NUMBER(1,0)	NULL	알림 거부
DENUM	아니요	NUMBER(1,0)	NULL	열거 거부
DQUERY	아니요	NUMBER(1,0)	NULL	쿼리 거부
DRCTRL	아니요	NUMBER(1,0)	NULL	
DCRLINK	아니요	NUMBER(1,0)	NULL	
DPRINT	아니요	NUMBER(1,0)	NULL	
DMANAGE	아니요	NUMBER(1,0)	NULL	관리 거부
DMAXALLOWED	아니요	NUMBER(1,0)	NULL	
DSTOP	아니요	NUMBER(1,0)	NULL	중지 거부
DPAUSE	아니요	NUMBER(1,0)	NULL	일시 중지 거부
DCONTROL	아니요	NUMBER(1,0)	NULL	제어 거부
DCHOG	아니요	NUMBER(1,0)	NULL	
DRESUME	아니요	NUMBER(1,0)	NULL	다시 시작 거부

ACRPTDB_VERSION 테이블 열

다음 표에서는 ACRPTDB_VERSION 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
VERSION_ID	아니요	NUMBER(1,0)	NOT NULL	항상 1 이어야 합니다.
MAJOR_VERSION	아니요	NVARCHAR2(20)	NULL	주 버전

이름	PK 여부	데이터 유형	Null 옵션	설명
MINOR_VERSION	아니요	NVARCHAR2(20)	NULL	부 버전

CATEGORY 테이블 열

다음 표에서는 CATEGORY 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID
CNAME	예	NVARCHAR2(80)	NOT NULL	이 레코드의 클래스 이름
ONAME	예	NVARCHAR2(256)	NOT NULL	이 레코드의 개체 이름
CATEGORY	예	NVARCHAR2(256)	NOT NULL	이 레코드의 범주 이름. 리소스에 하나 이상의 보안 범주가 할당된 경우 사용자 보안 범주 목록이 리소스에 할당된 보안 범주를 모두 포함할 때만 사용자에게 리소스에 대한 액세스 권한이 부여됩니다.

CONFIG 테이블 열

다음 표에서는 CONFIG 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
CONFIGNAME	예	NVARCHAR2(256)	NOT NULL	이 레코드의 범주 이름. 리소스에 하나 이상의 보안 범주가 할당된 경우 사용자 보안 범주 목록이 리소스에 할당된 보안 범주를 모두 포함할 때만 사용자에게 리소스에 대한

이름	PK 여부	데이터 유형	Null 옵션	설명
				액세스 권한이 부여됩니다.

CONFIG_ENTRY 테이블 열

다음 표에서는 CONFIG_ENTRY 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
CONFIGNAME	예	NVARCHAR2(256)	NOT NULL	구성 저장소 이름
ENTRYID	예	NVARCHAR2(256)	NOT NULL	구성 항목 이름
ENTRYTYPE	예	NVARCHAR2(80)	NOT NULL	구성 항목 유형. 'section' 값은 이 항목의 VALUE 및 VALUETYPE 이 NULL 임을 의미합니다.
SECTION	아니요	NVARCHAR2(256)	NOT NULL	이 항목의 섹션 이름. ENRYTYPE=section 인 경우 이 필드는 섹션 이름과 같습니다. 그렇지 않으면 이 필드는 이 항목이 포함된 섹션 이름과 같아집니다.
ENTRYNAME	아니요	NVARCHAR2(256)	NULL	구성 항목 이름. 이 열은 토큰 요소의 AC 구성 NAME 속성에 매핑됩니다.
VALUETYPE	아니요	NVARCHAR2(20)	NULL	ENTRYTYPE 이 NULL 이 아닌 경우 이 항목의 값 유형
VALUE	아니요	NVARCHAR2(256)	NULL	ENTRYTYPE 이 NULL 이 아닌 경우 이 항목의 값

DAYTIME 테이블 열

다음 표에서는 DAYTIME 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID
CNAME	예	NVARCHAR2(80)	NOT NULL	이 레코드의 클래스 이름
ONAME	예	NVARCHAR2(256)	NOT NULL	이 레코드의 개체 이름
SUNDAY	아니요	NUMBER(1,0)	NULL	일요일에 액세스 허용
MONDAY	아니요	NUMBER(1,0)	NULL	월요일에 액세스 허용
TUESDAY	아니요	NUMBER(1,0)	NULL	화요일에 액세스 허용
WEDNESDAY	아니요	NUMBER(1,0)	NULL	수요일에 액세스 허용
THURSDAY	아니요	NUMBER(1,0)	NULL	목요일에 액세스 허용
FRIDAY	아니요	NUMBER(1,0)	NULL	금요일에 액세스 허용
SATURDAY	아니요	NUMBER(1,0)	NULL	토요일에 액세스 허용
STARTTIME	아니요	TIMESTAMP(6)	NULL	이 시작 시간 이후에 액세스 허용
ENDTIME	아니요	TIMESTAMP(6)	NULL	이 종료 시간 이전에 액세스 허용

DEPLOYMENT_RESULT_MESSAGE 테이블 열

다음 표에서는 DEPLOYMENT_RESULT_MESSAGE 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2 (512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
RESCLASS	예	NVARCHAR2 (80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC

이름	PK 여부	데이터 유형	Null 옵션	설명
				OID 의 CNAME 에 매핑됩니다.
RULEKEY	예	NVARCHAR2 (256)	NOT NULL	CA CA-ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
MESSAGEIDX	예	NUMBER	NOT NULL	메시지가 정렬됩니다. 이 열은 메시지 인덱스를 나타내므로 다른 메시지를 기준으로 메시지 위치를 설명합니다. AC 클래스 DEPLOYMENT 의 RESULT_MESSAGE AC 속성의 명령 인덱스 구성 요소에 매핑됩니다.
MESSSAGESTR	예	NVARCHAR2 (256)	NULL	메시지 본문. AC 클래스 DEPLOYMENT 의 RESULT_MESSAGE AC 속성의 명령 문자열 구성 요소에 매핑됩니다.

DEPLOYMENT_TASK 테이블 열

다음 표에서는 DEPLOYMENT_TASK 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2 (512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
RULEKEY	예	NVARCHAR2 (256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
POLICYGRP_RESCLASS	아니요	NVARCHAR2(80)	NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. DEPLOYMENT 클래스의 GPOLICY AC OID 속성의 CNAME 에 매핑됩니다.
POLICYGRP_RULEKEY	아니요	NVARCHAR2 (256)	NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. DEPLOYMENT 클래스의 GPOLICY AC OID 속성의 ONAME 에 매핑됩니다.
CHECKERTYPE	아니요	NVARCHAR2(80)	NULL	이 사용자의 AC 클래스: USER, XUSER. DEPLOYMENT 클래스의 CHECKER AC OID 속성의 CNAME 에 매핑됩니다.
CHECKERID	아니요	NVARCHAR2 (256)	NULL	이 시스템에서 해당 개체의 식별자입니다. DEPLOYMENT 클래스의 CHECKER AC OID 속성의 ONAME 에 매핑됩니다.
NODE_RESCLASS	아니요	NVARCHAR2(80)	NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. DEPLOYMENT 클래스의 HNODEY AC OID 속성의 CNAME 에 매핑됩니다.
NODE_RULEKEY	아니요	NVARCHAR2 (256)	NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret:

이름	PK 여부	데이터 유형	Null 옵션	설명
				이 리소스에 대해 소유된 리소스 마스크입니다. DEPLOYMENT 클래스의 HNODE AC OID 속성의 ONAME 에 매핑됩니다.
POLICY_RESCLASS	아니요	NVARCHAR2(80)	NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. DEPLOYMENT 클래스의 POLICY AC OID 속성의 CNAME 에 매핑됩니다.
POLICY_RULEKEY	아니요	NVARCHAR2 (256)	NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. DEPLOYMENT 클래스의 POLICY AC OID 속성의 ONAME 에 매핑됩니다.
MAKERID	아니요	NVARCHAR2 (256)	NULL	이 시스템에서 해당 개체의 식별자입니다. DEPLOYMENT 클래스의 AC OID 속성 MAKER 에 대한 ONAME 에 매핑됩니다.
MAKERTYPE	아니요	NVARCHAR2(80)	NULL	메이커 클래스. 값 USER 및 XUSER 는 메이커 레코드가 USERINFO 테이블에 있음을 의미합니다. GROUP 또는 XGROUP 은 메이커 레코드가 GROUPINFO 테이블에 있음을 의미합니다. DEPLOYMENT 클래스의 MAKER AC OID 속성의 CNAME 에 매핑됩니다.
CHECKERCOMMENT	아니요	NVARCHAR2 (256)	NULL	검사기에 의해 작성된 설명. DEPLOYMENT 클래스의 CHECKER_COMMENT AC 속성에 매핑됩니다.
CHECKERTIME	아니요	TIMESTAMP(6)	NULL	검사 타임스탬프.

이름	PK 여부	데이터 유형	Null 옵션	설명
				DEPLOYMENT 클래스의 CHECKER_TIME AC 속성에 매핑됩니다.
DMSNAME	아니요	NVARCHAR2 (256)	NULL	이 작업을 생성한 DMS 의 이름. DEPLOYMENT 클래스의 DMS_NAME AC 속성에 매핑됩니다.
OPERATION	아니요	NVARCHAR2 (256)	NULL	이 작업에서 수행해야 하는 작업: DEPLOY, UNDEPLOY. DEPLOYMENT 클래스의 OPERATION AC 속성에 매핑됩니다.
STATUS	아니요	NVARCHAR2 (256)	NULL	작업의 상태: SUCCESS, WARNING, FAIL, NOACTION. DEPLOYMENT 클래스의 STATUS AC 속성에 매핑됩니다.

DEPLOYMENT_TASK_GROUP 테이블 열

다음 표에서는 DEPLOYMENT_TASK_GROUP 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2 (512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.
RULEKEY	예	NVARCHAR2 (256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된

이름	PK 여부	데이터 유형	Null 옵션	설명
				리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
POLICYGRP_RESCLASS	아니요	NVARCHAR2(80)	NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. GDEPLOYMENT 클래스의 POLICY AC OID 속성의 CNAME 에 매핑됩니다.
POLICYGRP_RULEKEY	아니요	NVARCHAR2 (256)	NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. GDEPLOYMENT 클래스의 POLICY AC OID 속성의 ONAME 에 매핑됩니다.
NODEGRP_RESCLASS	아니요	NVARCHAR2(80)	NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. GDEPLOYMENT 클래스의 GHNODE AC OID 속성의 CNAME 에 매핑됩니다.
NODEGRP_RULEKEY	아니요	NVARCHAR2 (256)	NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. GDEPLOYMENT 클래스의 GHNODE AC OID 속성의 ONAME 에 매핑됩니다.
NODE_RESCLASS	아니요	NVARCHAR2(80)	NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. GDEPLOYMENT 클래스의 HNODE AC OID 속성의 CNAME 에 매핑됩니다.
NODE_RULEKEY	아니요	NVARCHAR2 (256)	NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된

이름	PK 여부	데이터 유형	Null 옵션	설명
				리소스 마스크입니다. GDEPLOYMENT 클래스의 HNODE AC OID 속성의 ONAME 에 매핑됩니다.
TRIG	아니요	NVARCHAR2 (256)	NULL	이 작업 그룹의 트리거: ASSIGN, UNASSIGN, DIRECTDEPLOY, DIRECTUNDEPLOY. GDEPLOYMENT 클래스의 TRIGGER AC 속성에 매핑됩니다.

DISTRIBUTION_HOST 테이블 열

다음 표에서는 DISTRIBUTION_HOST 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2 (512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
DH	예	NVARCHAR2 (256)	NOT NULL	DHTYPE 열 값에 따라 AC 클래스 SEOS 의 DH 또는 DHDR 속성 내에 있는 단일 요소에 매핑됩니다.
DHTYPE	예	NVARCHAR2 (20)	NOT NULL	DHTYPE 이 'DR'인 경우 DH 열은 AC 클래스 SEOS 의 DHDR 속성 내에 있는 단일 요소에 매핑됩니다. DHTYPE 이 'NORMAL'인 경우 이 열은 해당 클래스의 DH 속성에 매핑됩니다.

EFFECTIVE_POLICY 테이블 열

다음 표에서는 EFFECTIVE_POLICY 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2 (512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
NODE_RESCLASS	예	NVARCHAR2 (80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.
NODE_RULEKEY	예	NVARCHAR2 (256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
POLICY_RESCLASS	예	NVARCHAR2 (80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.
POLICY_RULEKEY	예	NVARCHAR2 (256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.

GROUPAUDIT 테이블 열

다음 표에서는 GROUPAUDIT 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2 (512)	NOT NULL	이 레코드의 호스트 ID
GROUPID	예	NVARCHAR2 (256)	NOT NULL	이 레코드의 그룹 ID(이름)
GROUPTYPE	예	NVARCHAR2 (80)	NOT NULL	그룹 클래스: GROUP, XGROUP 등. AC 그룹 OID 의 CNAME 에 매핑됩니다.
SUCCESS	아니요	NUMBER(1,0)	NULL	성공한 이벤트 감사
FAILURE	아니요	NUMBER(1,0)	NULL	실패한 이벤트 감사
LOGONSUCCESS	아니요	NUMBER(1,0)	NULL	성공한 로그온 감사
LOGONFAILURE	아니요	NUMBER(1,0)	NULL	실패한 로그온 감사
DEBUG	아니요	NUMBER(1,0)	NULL	디버그 모드 동안 로그
TRACE	아니요	NUMBER(1,0)	NULL	그룹에서 추적

GROUPINFO 테이블 열

다음 표에서는 GROUPINFO 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2 (512)	NOT NULL	이 레코드의 호스트 ID
GROUPID	예	NVARCHAR2 (256)	NOT NULL	이 레코드의 그룹 ID(이름) AC 그룹 OID 의 ONAME 에 매핑됩니다.
GROUPTYPE	예	NVARCHAR2(80)	NOT NULL	그룹 클래스: GROUP, XGROUP 등. AC 그룹 OID 의 CNAME 에 매핑됩니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
DESCRIPTION	아니요	NVARCHAR2 (256)	NULL	그룹 설명. AC 클래스 GROUP/XROUP 의 COMMENT AC 속성에 매핑됩니다.
OWNERCNAME	아니요	NVARCHAR2 (256)	NULL	소유자의 보안 수준, 보안 레이블 및 보안 범주 권한이 리소스에 액세스할 수 있을 만큼 충분한 경우 리소스 레코드의 소유자는 리소스에 제한 없이 액세스할 수 있습니다. 리소스 소유자는 항상 리소스 레코드를 업데이트 및 삭제할 수 있습니다. AC 클래스 GROUP/XGROUP 의 OWNER AC 속성의 CNAME 에 매핑됩니다.
OWNERONAME	아니요	NVARCHAR2 (256)	NULL	AC 클래스 GROUP/XGROUP 의 OWNER AC 속성의 ONAME 에 매핑됩니다.
FULLNAME	아니요	NVARCHAR2 (256)	NULL	그룹과 연관된 전체 이름. AC 클래스 GROUP/XGROUP 의 FULL_NAME AC 속성에 매핑됩니다.
SUPGROUP	아니요	NVARCHAR2 (256)	NULL	부모 그룹("상위" 그룹)의 이름입니다. AC 클래스 GROUP/XGROUP 의 SUPGROUP AC 속성에 매핑됩니다.
CALENDAR	아니요	NVARCHAR2 (256)	NULL	Unicenter TNG 의 시간 제한을 나타내는 Unicenter TNG 달력 개체를 지정합니다. AC 에서는 관리 용도로만 이러한 개체 목록을 유지하며 이 목록을 보호하지는 않습니다. AC 클래스 GROUP/XGROUP 의 CALENDAR AC 속성에 매핑됩니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
CRETIME	아니요	TIMESTAMP(6)	NULL	작성 시간. AC 클래스 GROUP/XGROUP 의 CREATE_TIME AC 속성에 매핑됩니다.
UPDTIME	아니요	TIMESTAMP(6)	NULL	레코드가 마지막으로 수정된 날짜 및 시간입니다.
UPDWHOCNAME	아니요	NVARCHAR2 (256)	NULL	레코드가 마지막으로 수정된 날짜 및 시간입니다. AC 클래스 GROUP/XROUP 의 UPDATE_TIME AC 속성에 매핑됩니다.
UPDWHOONAME	아니요	NVARCHAR2 (256)	NULL	AC 클래스 GROUP/XGROUP 의 UPDATE_WHO AC 속성의 ONAME 에 매핑됩니다.
HOMEDIR	아니요	NVARCHAR2 (256)	NULL	새 그룹 구성원에게 할당된 홈 디렉터리입니다. AC 클래스 GROUP/XGROUP 의 HOMEDIR AC 속성에 매핑됩니다.
EXPDATE	아니요	DATE	NULL	그룹 구성원 계정이 만료되는 날짜를 설정합니다. AC 클래스 GROUP/XROUP 의 EXPIRE_DATE AC 속성에 매핑됩니다.
MAXLOGINS	아니요	NUMBER	NULL	사용자가 동시에 로그인할 수 있는 최대 터미널 수를 설정합니다. 값 0 은 사용자가 터미널 수에 제한 없이 동시에 로그인할 수 있음을 의미합니다. AC 클래스 GROUP/XROUP 의 MAXLOGINS 속성에 매핑됩니다.
INACTIVE	아니요	NUMBER	NULL	시스템에서 사용자가 비활성 상태로 전환되기 전까지 대기하는 일 수를 지정합니다. AC 클래스 GROUP/XGROUP 의

이름	PK 여부	데이터 유형	Null 옵션	설명
				INACTIVE AC 속성에 매핑됩니다.
PROFUSRCNAME	아니요	NVARCHAR2 (256)	NULL	AC 클래스 GROUP/XGROUP 의 PROFUSR AC 속성의 CNAME 에 매핑됩니다.
PROFUSRONAME	아니요	NVARCHAR2 (256)	NULL	AC 클래스 GROUP/XGROUP 의 PROFUSR AC 속성의 ONAME 에 매핑됩니다.
PWDAUTOGEN	아니요	NUMBER(1,0)	NULL	응용 프로그램의 암호가 정책 서버에서 자동으로 생성되는지 여부를 나타냅니다. AC 클래스 GROUP/XGROUP 의 PWD_AUTOGEN AC 속성에 매핑됩니다.
PWDSYNC	아니요	NUMBER(1,0)	NULL	응용 프로그램의 암호가 사용자의 다른 응용 프로그램 암호와 동일할 수 있는지 여부를 나타냅니다. AC 클래스 GROUP/XGROUP 의 PWD_SYNC AC 속성에 매핑됩니다.
PWPOLICY	아니요	NVARCHAR2 (256)	NULL	응용 프로그램에 대한 암호 정책의 레코드 이름입니다. AC 클래스 GROUP/XGROUP 의 PWPOLICY AC 속성에 매핑됩니다.
RESDATE	아니요	DATE	NULL	suspend 매개 변수를 지정하여 비활성화된 사용자 레코드를 활성화합니다. AC 클래스 GROUP/XGROUP 의 RESUME_DATE AC 속성에

이름	PK 여부	데이터 유형	Null 옵션	설명
				매핑됩니다.
SHELL	아니요	NVARCHAR2 (256)	NULL	사용자가 login 또는 su 명령을 호출한 후 실행되는 초기 프로그램 또는 셸의 전체 경로를 지정합니다. AC 클래스 GROUP/XGROUP 의 SHELL AC 속성에 매핑됩니다.
SUBGROUP	아니요	NVARCHAR2 (256)	NULL	이 그룹이 부모인 그룹의 목록입니다. AC 클래스 GROUP/XGROUP 의 SUBGROUP AC 속성에 매핑됩니다.
SUSDATE	아니요	TIMESTAMP(6)	NULL	사용자 레코드를 비활성화하지만 데이터베이스에 정의된 상태를 유지합니다. AC 클래스 GROUP/XGROUP 의 SUSPEND_DATE AC 속성에 매핑됩니다.
SUSWHOCNAME	아니요	NVARCHAR2 (256)	NULL	중단 날짜를 활성화한 관리자의 클래스입니다. AC 클래스 GROUP/XGROUP 의 SUSPEND_WHO AC 속성의 CNAME 에 매핑됩니다.
SUSWHOONAME	아니요	NVARCHAR2 (256)	NULL	중단 날짜를 활성화한 관리자의 개체 이름입니다. AC 클래스 GROUP/XGROUP 의 SUSPEND_WHO AC 속성의 ONAME 에 매핑됩니다.
SECURITYID	아니요	NVARCHAR2 (256)	NULL	이 그룹 항목의 공급업체 특정 보안 ID 입니다. AC 클래스 XGROUP 의 SECURITY_ID AC 속성에 매핑됩니다.

GROUPMEMBER 테이블 열

다음 표에서는 GROUPMEMBER 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID
GROUPID	예	NVARCHAR2(256)	NOT NULL	이 레코드의 그룹 ID(이름)
CNAME	예	NVARCHAR2(256)	NOT NULL	구성원의 클래스 이름
ONAME	예	NVARCHAR2(256)	NOT NULL	구성원의 개체 이름
GROUPTYPE	예	NVARCHAR2(80)	NOT NULL	그룹 클래스: GROUP, XGROUP 등. AC 그룹 OID 의 CNAME 에 매핑됩니다.

GROUPREVACL 테이블 열

다음 표에서는 GROUPREVACL 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2 (512)	NOT NULL	이 레코드의 호스트 ID
GROUPID	예	NVARCHAR2 (256)	NOT NULL	이 레코드의 그룹 ID(이름)
GROUPTYPE	예	NVARCHAR2(80)	NOT NULL	그룹 클래스: GROUP, XGROUP 등. AC 그룹 OID 의 CNAME 에 매핑됩니다.
RESCNAME	예	NVARCHAR2(80)	NOT NULL	리소스 클래스 이름
RESONAME	예	NVARCHAR2 (256)	NOT NULL	리소스 개체 이름
CONCNAME	예	NVARCHAR2(80)	NOT NULL	조건 클래스 이름(즉, PROGRAM, HOST, CALENDAR). 비어 있지 않은 문자열은 RESINFO

이름	PK 여부	데이터 유형	Null 옵션	설명
				테이블에 조건 개체가 있음을 의미합니다. 하이픈 문자열('-')은 "조건 없음"을 의미합니다.
CONONAME	예	NVARCHAR2 (256)	NOT NULL	조건 개체 이름
ISALLOW	예	NVARCHAR2 (256)	NOT NULL	
AREAD	아니요	NUMBER(1,0)	NULL	
AWRITE	아니요	NUMBER(1,0)	NULL	
AMODIFY	아니요	NUMBER(1,0)	NULL	
ACREATE	아니요	NUMBER(1,0)	NULL	
AERASE	아니요	NUMBER(1,0)	NULL	
AFILESCAN	아니요	NUMBER(1,0)	NULL	
ALANGINT	아니요	NUMBER(1,0)	NULL	
AEXEC	아니요	NUMBER(1,0)	NULL	
ACHOWN	아니요	NUMBER(1,0)	NULL	
ACHGRP	아니요	NUMBER(1,0)	NULL	
ACHMOD	아니요	NUMBER(1,0)	NULL	
AUTIMES	아니요	NUMBER(1,0)	NULL	
ASEC	아니요	NUMBER(1,0)	NULL	
AKILL	아니요	NUMBER(1,0)	NULL	
ACONNECT	아니요	NUMBER(1,0)	NULL	
ARENAME	아니요	NUMBER(1,0)	NULL	
APASSWORD	아니요	NUMBER(1,0)	NULL	
AAUTHORIZED	아니요	NUMBER(1,0)	NULL	
AXAUDIT	아니요	NUMBER(1,0)	NULL	
ACHDIR	아니요	NUMBER(1,0)	NULL	
ACRSUBK	아니요	NUMBER(1,0)	NULL	
ANOTIFY	아니요	NUMBER(1,0)	NULL	
AENUM	아니요	NUMBER(1,0)	NULL	

이름	PK 여부	데이터 유형	Null 옵션	설명
AQUERY	아니요	NUMBER(1,0)	NULL	
ARCTRL	아니요	NUMBER(1,0)	NULL	
ACRLINK	아니요	NUMBER(1,0)	NULL	
APRINT	아니요	NUMBER(1,0)	NULL	
AMANAGE	아니요	NUMBER(1,0)	NULL	
AMAXALLOWED	아니요	NUMBER(1,0)	NULL	
ASTOP	아니요	NUMBER(1,0)	NULL	
APAUSE	아니요	NUMBER(1,0)	NULL	
ACONTROL	아니요	NUMBER(1,0)	NULL	
ACHOG	아니요	NUMBER(1,0)	NULL	
ARESUME	아니요	NUMBER(1,0)	NULL	
DREAD	아니요	NUMBER(1,0)	NULL	
DWRITE	아니요	NUMBER(1,0)	NULL	
DMODIFY	아니요	NUMBER(1,0)	NULL	
DCREATE	아니요	NUMBER(1,0)	NULL	
DERASE	아니요	NUMBER(1,0)	NULL	
DFILESCAN	아니요	NUMBER(1,0)	NULL	
DLANGINT	아니요	NUMBER(1,0)	NULL	
DEXEC	아니요	NUMBER(1,0)	NULL	
DCHOWN	아니요	NUMBER(1,0)	NULL	
DCHGRP	아니요	NUMBER(1,0)	NULL	
DCHMOD	아니요	NUMBER(1,0)	NULL	
DUTIMES	아니요	NUMBER(1,0)	NULL	
DSEC	아니요	NUMBER(1,0)	NULL	
DKILL	아니요	NUMBER(1,0)	NULL	
DCONNECT	아니요	NUMBER(1,0)	NULL	
DRENAME	아니요	NUMBER(1,0)	NULL	
DPASSWORD	아니요	NUMBER(1,0)	NULL	
DAUTHORIZED	아니요	NUMBER(1,0)	NULL	

이름	PK 여부	데이터 유형	Null 옵션	설명
DXAUDIT	아니요	NUMBER(1,0)	NULL	
DCHDIR	아니요	NUMBER(1,0)	NULL	
DCRSUBK	아니요	NUMBER(1,0)	NULL	
DNOTIFY	아니요	NUMBER(1,0)	NULL	
DENUM	아니요	NUMBER(1,0)	NULL	
DQUERY	아니요	NUMBER(1,0)	NULL	
DRCTRL	아니요	NUMBER(1,0)	NULL	
DCRLINK	아니요	NUMBER(1,0)	NULL	
DPRINT	아니요	NUMBER(1,0)	NULL	
DMANAGE	아니요	NUMBER(1,0)	NULL	
DMAXALLOWED	아니요	NUMBER(1,0)	NULL	
DSTOP	아니요	NUMBER(1,0)	NULL	
DPAUSE	아니요	NUMBER(1,0)	NULL	
DCONTROL	아니요	NUMBER(1,0)	NULL	
DCHOG	아니요	NUMBER(1,0)	NULL	
DRESUME	아니요	NUMBER(1,0)	NULL	

GROUPS 테이블 열

다음 표에서는 GROUPS 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2 (512)	NOT NULL	이 레코드의 호스트 ID
RESCLASS	예	NVARCHAR2(80)	NOT NULL	리소스 클래스 이름
RULEKEY	예	NVARCHAR2 (256)	NOT NULL	리소스 개체 이름
ONAME	예	NVARCHAR2 (256)	NOT NULL	그룹에 참여한 개체의 개체 이름
CNAME	예	NVARCHAR2(80)	NOT NULL	그룹에 참여한 개체의 클래스

이름	PK 여부	데이터 유형	Null 옵션	설명
				이름

HOLDATE 테이블 열

다음 표에서는 HOLDATE 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(256)	NOT NULL	이 레코드의 호스트 ID
RESCLASS	예	NVARCHAR2(80)	NOT NULL	리소스 클래스 이름(HOLIDAY 여야 함)
RULEKEY	예	NVARCHAR2(256)	NOT NULL	리소스 개체 이름
STARTDATE	예	TIMESTAMP(6)	NOT NULL	휴일 시작 날짜
ENDDATE	예	TIMESTAMP(6)	NOT NULL	휴일 끝 날짜
ALLDAY	예	NUMBER(1,0)	NULL	이 휴일은 하루 종일 계속됩니다.
EVERYYEAR	예	NUMBER(1,0)	NULL	이 휴일은 매년 발생합니다.

HOSTINFO 테이블 열

다음 표에서는 HOSTINFO 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
HOSTID	예	NVARCHAR2 (512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
APPNAME	아니요	NVARCHAR2(24)	NULL	보안 데이터가 포함된 보안 응용 프로그램 이름
APPIND	아니요	CHAR(1)	NULL	응용 프로그램 표시기. 이 레코드가 속한 응용 프로그램을 나타냅니다.
APPVERSION	아니요	NVARCHAR2(24)	NULL	보안 응용 프로그램 버전
APPMODE	아니요	CHAR(1)	NULL	이 레코드에 적용되는 처리

이름	PK 여부	데이터 유형	Null 옵션	설명
				모드
LOADDATE	아니요	TIMESTAMP(6)	NULL	보안 데이터베이스에서 보안 정보가 언로드된 날짜
BASE_HOSTID	아니요	NVARCHAR2 (512)	NULL	포함된 호스트 ID(있는 경우)

INETACL 테이블 열

다음 표에서는 INETACL 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
RESCLASS	예	NVARCHAR2(80)	NOT NULL	리소스 클래스 이름
RULEKEY	예	NVARCHAR2(256)	NOT NULL	리소스 개체 이름
SERVICENAME	예	NVARCHAR2(256)	NOT NULL	서비스 이름
PROTOCOLNAME	예	NVARCHAR2(256)	NOT NULL	프로토콜 이름
AREAD	아니요	NUMBER(1,0)	NULL	
AWRITE	아니요	NUMBER(1,0)	NULL	
AMODIFY	아니요	NUMBER(1,0)	NULL	
ACREATE	아니요	NUMBER(1,0)	NULL	
AERASE	아니요	NUMBER(1,0)	NULL	
AFILESCAN	아니요	NUMBER(1,0)	NULL	
ALANGINT	아니요	NUMBER(1,0)	NULL	
AEXEC	아니요	NUMBER(1,0)	NULL	
ACHOWN	아니요	NUMBER(1,0)	NULL	
ACHGRP	아니요	NUMBER(1,0)	NULL	
ACHMOD	아니요	NUMBER(1,0)	NULL	

이름	PK 여부	데이터 유형	Null 옵션	설명
AUTIMES	아니요	NUMBER(1,0)	NULL	
ASEC	아니요	NUMBER(1,0)	NULL	
AKILL	아니요	NUMBER(1,0)	NULL	
ACONNECT	아니요	NUMBER(1,0)	NULL	
ARENAME	아니요	NUMBER(1,0)	NULL	
APASSWORD	아니요	NUMBER(1,0)	NULL	
AAUTHORIZED	아니요	NUMBER(1,0)	NULL	
AXAUDIT	아니요	NUMBER(1,0)	NULL	
ACHDIR	아니요	NUMBER(1,0)	NULL	
ACRSUBK	아니요	NUMBER(1,0)	NULL	
ANOTIFY	아니요	NUMBER(1,0)	NULL	
AENUM	아니요	NUMBER(1,0)	NULL	
AQUERY	아니요	NUMBER(1,0)	NULL	
ARCTRL	아니요	NUMBER(1,0)	NULL	
ACRLINK	아니요	NUMBER(1,0)	NULL	
APRINT	아니요	NUMBER(1,0)	NULL	
AMANAGE	아니요	NUMBER(1,0)	NULL	
AMAXALLOWED	아니요	NUMBER(1,0)	NULL	
ASTOP	아니요	NUMBER(1,0)	NULL	
APAUSE	아니요	NUMBER(1,0)	NULL	
ACONTROL	아니요	NUMBER(1,0)	NULL	
ACHOG	아니요	NUMBER(1,0)	NULL	
ARESUME	아니요	NUMBER(1,0)	NULL	

INSERVRNGE 테이블 열

다음 표에서는 INSERVRNGE 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다.
RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. AC: 리소스 개체 이름입니다.
MINSERVICE	예	NUMBER	NOT NULL	최소 포트 번호
MAXSERVICE	예	NUMBER	NOT NULL	최대 포트 번호
AREAD	아니요	NUMBER(1,0)	NULL	
AWRITE	아니요	NUMBER(1,0)	NULL	
AMODIFY	아니요	NUMBER(1,0)	NULL	
ACREATE	아니요	NUMBER(1,0)	NULL	
AERASE	아니요	NUMBER(1,0)	NULL	
AFILESCAN	아니요	NUMBER(1,0)	NULL	
ALANGINT	아니요	NUMBER(1,0)	NULL	
AEXEC	아니요	NUMBER(1,0)	NULL	
ACHOWN	아니요	NUMBER(1,0)	NULL	
ACHGRP	아니요	NUMBER(1,0)	NULL	
ACHMOD	아니요	NUMBER(1,0)	NULL	
AUTIMES	아니요	NUMBER(1,0)	NULL	
ASEC	아니요	NUMBER(1,0)	NULL	

이름	PK 여부	데이터 유형	Null 옵션	설명
AKILL	아니요	NUMBER(1,0)	NULL	
ACONNECT	아니요	NUMBER(1,0)	NULL	
ARENAME	아니요	NUMBER(1,0)	NULL	
APASSWORD	아니요	NUMBER(1,0)	NULL	
AAUTHORIZED	아니요	NUMBER(1,0)	NULL	
AXAUDIT	아니요	NUMBER(1,0)	NULL	
ACHDIR	아니요	NUMBER(1,0)	NULL	
ACRSUBK	아니요	NUMBER(1,0)	NULL	
ANOTIFY	아니요	NUMBER(1,0)	NULL	
AENUM	아니요	NUMBER(1,0)	NULL	
AQUERY	아니요	NUMBER(1,0)	NULL	
ARCTRL	아니요	NUMBER(1,0)	NULL	
ACRLINK	아니요	NUMBER(1,0)	NULL	
APRINT	아니요	NUMBER(1,0)	NULL	
AMANAGE	아니요	NUMBER(1,0)	NULL	
AMAXALLOWED	아니요	NUMBER(1,0)	NULL	
ASTOP	아니요	NUMBER(1,0)	NULL	
APAUSE	아니요	NUMBER(1,0)	NULL	
ACONTROL	아니요	NUMBER(1,0)	NULL	
ACHOG	아니요	NUMBER(1,0)	NULL	
ARESUME	아니요	NUMBER(1,0)	NULL	

LOCAL_PMD_SUBSCRIBER 테이블 열

다음 표에서는 LOCAL_PMD_SUBSCRIBER 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID

이름	PK 여부	데이터 유형	Null 옵션	설명
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
SUBSCRIBER_HOSTID	예	NVARCHAR2(256)	NOT NULL	구독자 정책 모델. sepmd -L selang 명령 출력의 구독자 열에 매핑됩니다.
ERRORCOUNT	아니요	NUMBER	NULL	구독 오류 수. sepmd -L selang 명령 출력의 오류 열에 매핑됩니다.
STATUS	아니요	NVARCHAR2(256)	NULL	구독 상태 설명. sepmd -L selang 명령 출력의 플래그 열에 매핑됩니다.
OFFSET	아니요	NUMBER	NULL	배포된 정책 파일 내의 현재 구독 오프셋입니다. sepmd -L selang 명령 출력의 오프셋 열에 매핑됩니다.
NEXTCOMMAND	아니요	NVARCHAR2(256)	NULL	배포된 정책 파일 내의 현재 구독 명령입니다. sepmd -L selang 명령 출력의 다음 명령 열에 매핑됩니다.

LOGINAPPL 테이블 열

다음 표에서는 LOGINAPPL 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
LOGINHOW	아니요	NVARCHAR2(256)	NULL	로그인 방법(pseudo, normal, ...). AC 클래스 LOGINAPPL 의 LOGINHOW 속성에 매핑됩니다.
LOGINPATH	아니요	NVARCHAR2(256)	NULL	로그인 응용 프로그램의 전체 경로(또는 일반 경로)입니다. AC 클래스 LOGINAPPL 의 LOGINPATH 속성에 매핑됩니다.
FNFSPGM	아니요	NUMBER(1,0)	NULL	AC 클래스 LOGINAPPL 의 LOGINFLAG 속성의 로그인 플래그 NFSPGM 에 매핑됩니다.
FINOGRACE	아니요	NUMBER(1,0)	NULL	AC 클래스 LOGINAPPL 의 LOGINFLAG 속성의 로그인 플래그 nograce 에 매핑됩니다.
FINOGRACEROOT	아니요	NUMBER(1,0)	NULL	AC 클래스 LOGINAPPL 의 LOGINFLAG 속성의 로그인 플래그 nograceroot 에 매핑됩니다.
FNOLOGIN	아니요	NUMBER(1,0)	NULL	AC 클래스 LOGINAPPL 의 LOGINFLAG 속성의 로그인 플래그 nologin 에 매핑됩니다.
SSEID	아니요	NUMBER(1,0)	NULL	AC 클래스 LOGINAPPL 의 LOGINSEQUENCE 속성의 SEID 로그인 시퀀스에 매핑됩니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SSUID	아니요	NUMBER(1,0)	NULL	AC 클래스 LOGINAPPL 의 LOGINSEQUENCE 속성의 SUID 로그인 시퀀스에 매핑됩니다.
SSGID	아니요	NUMBER(1,0)	NULL	AC 클래스 LOGINAPPL 의 LOGINSEQUENCE 속성의 SGID 로그인 시퀀스에 매핑됩니다.
SSGRP	아니요	NUMBER(1,0)	NULL	AC 클래스 LOGINAPPL 의 LOGINSEQUENCE 속성의 SGRP 로그인 시퀀스에 매핑됩니다.
SFEID	아니요	NUMBER(1,0)	NULL	AC 클래스 LOGINAPPL 의 LOGINSEQUENCE 속성의 FEID 로그인 시퀀스에 매핑됩니다.
SFUID	아니요	NUMBER(1,0)	NULL	AC 클래스 LOGINAPPL 의 LOGINSEQUENCE 속성의 FUID 로그인 시퀀스에 매핑됩니다.
SFGID	아니요	NUMBER(1,0)	NULL	AC 클래스 LOGINAPPL 의 LOGINSEQUENCE 속성의 FGID 로그인 시퀀스에 매핑됩니다.
SFGRP	아니요	NUMBER(1,0)	NULL	AC 클래스 LOGINAPPL 의 LOGINSEQUENCE 속성의 FGRP 로그인 시퀀스에 매핑됩니다.
SN3EID	아니요	NUMBER(1,0)	NULL	AC 클래스 LOGINAPPL 의 LOGINSEQUENCE 속성의 N3EID 로그인 시퀀스에 매핑됩니다.
SN3UID	아니요	NUMBER(1,0)	NULL	AC 클래스 LOGINAPPL 의 LOGINSEQUENCE 속성의 N3UID 로그인 시퀀스에 매핑됩니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SN3GID	아니요	NUMBER(1,0)	NULL	AC 클래스 LOGINAPPL 의 LOGINSEQUENCE 속성의 N3GID 로그인 시퀀스에 매핑됩니다.
SN3GRP	아니요	NUMBER(1,0)	NULL	AC 클래스 LOGINAPPL 의 LOGINSEQUENCE 속성의 N3GRP 로그인 시퀀스에 매핑됩니다.

MEMBEROF 테이블 열

다음 표에서는 MEMBEROF 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID
GROUPID	예	NVARCHAR2(256)	NOT NULL	이 레코드의 그룹 ID(이름)
CNAME	예	NVARCHAR2(256)	NOT NULL	클래스 이름
ONAME	예	NVARCHAR2(256)	NOT NULL	개체 이름
GROUPTYPE	예	NVARCHAR2(80)	NOT NULL	그룹 클래스: GROUP, XGROUP 등. AC 그룹 OID 의 CNAME 에 매핑됩니다.

MEMBERS 테이블 열

다음 표에서는 MEMBERS 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는

이름	PK 여부	데이터 유형	Null 옵션	설명
				엔터티의 리소스 클래스입니다.
RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. AC: 리소스 개체 이름입니다.
CNAME	예	NVARCHAR2(80)	NOT NULL	구성원의 클래스 이름
ONAME	예	NVARCHAR2(256)	NOT NULL	구성원의 개체 이름

NODE 테이블 열

다음 표에서는 NODE 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.
RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
KEEPALIVE	예	TIMESTAMP(6)	NULL	마지막 keepalive 시간. AC 클래스 HNODE 의 HNODE_KEEP_ALIVE AC 속성에 매핑됩니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
VERSION	예	NUMBER	NULL	노드 버전. AC 클래스 HNODE 의 HNODE_VERSION AC 속성에 매핑됩니다.
ACID	예	NVARCHAR2(256)	NULL	고유한 AC 호스트 ID. AC 클래스 HNODE 의 ACID 속성에 매핑됩니다.

NODE_ADDRESS 테이블 열

다음 표에서는 NODE_ADDRESS 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.
RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
ADDRESS	예	NVARCHAR2(256)	NOT NULL	

NODE_ALIAS 테이블 열

다음 표에서는 NODE_ALIAS 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.
RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
ALIAS	예	NVARCHAR2(256)	NOT NULL	노드 별칭. AC 클래스 HNODE 의 ALIAS 속성 내에 있는 단일 문자열에 매핑됩니다.

NODE_DEVIATION 테이블 열

다음 표에서는 NODE_DEVIATION 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스

이름	PK 여부	데이터 유형	Null 옵션	설명
				클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.
RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
DATA	예	CLOB	NULL	원시 위반 데이터. DEVCALC 출력의 시작 부분에 있는 DEVCALC 헤더(즉, 첫 번째 POLICYSTART 태그 앞에 있는 모든 데이터)에 매핑됩니다.

NODE_SUBSCRIPTION_STATUS 테이블 열

다음 표에서는 NODE_SUBSCRIPTION_STATUS 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
PUBLISHERCNAME	예	NVARCHAR2(80)	NOT NULL	게시 노드 CNAME
SUBSCRIBERCNAME	예	NVARCHAR2(80)	NOT NULL	구독 노드 CNAME. AC 클래스 HNODE 의 SUBSCRIBER_STATUS 속성의 구독자 OID 구성 요소의 클래스 이름에 매핑됩니다.
PUBLISHERONAME	예	NVARCHAR2(256)	NOT NULL	게시 노드 ONAME

이름	PK 여부	데이터 유형	Null 옵션	설명
SUBSCRIBERONAME	예	NVARCHAR2(256)	NOT NULL	구독 노드 ONAME. 구독자 OID 의 개체 이름에 매핑됩니다.
STATUS	아니요	NVARCHAR2(256)	NULL	구독 상태. AC 클래스 HNODE 의 SUBSCRIBER_STATUS 속성의 Status 구성 요소에 매핑됩니다.
LASTSTATUSTIME	아니요	TIMESTAMP(6)	NULL	마지막 상태 업데이트 시간 AC 클래스 HNODE 의 SUBSCRIBER_STATUS 속성의 Last Status Time 구성 요소에 매핑됩니다.

PASSWDRULES 테이블 열

다음 표에서는 PASSWDRULES 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID
GROUPID	예	NVARCHAR2(256)	NOT NULL	이 레코드의 그룹 ID(이름)
GROUPTYPE	예	NVARCHAR2(80)	NOT NULL	그룹 클래스: GROUP, XGROUP 등. AC 그룹 OID 의 CNAME 에 매핑됩니다.
ISSEOS	예	NUMBER(1,0)	NOT NULL	이 passwdrules 레코드가 SEOS 테이블의 레코드와 관련이 있습니까? 이 레코드가 GROUPINFO 레코드가 아닌 SEOS 와 연관된 경우에만 ISSEOS 가 1 입니다. ISSEOS 가 1 이면 GROUPID 및 GROUPTYPE 은 비어 있습니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
MINLEN	아니요	NUMBER	NULL	최소 길이
MAXREP	아니요	NUMBER	NULL	최대 단일 문자 반복
MUSTSMALL	아니요	NUMBER	NULL	반드시 소문자 포함
MUSTCAPITAL	아니요	NUMBER	NULL	반드시 대문자 포함
MUSTNUM	아니요	NUMBER	NULL	반드시 숫자 포함
MUSTOTH	아니요	NUMBER	NULL	반드시 다른 문자 포함
MUSTALFA	아니요	NUMBER	NULL	반드시 #개 이상의 알파벳 문자 포함
MUSTALFAN	아니요	NUMBER	NULL	반드시 #개 이상의 영숫자 문자 포함
SUBNAME	아니요	NUMBER	NULL	사용자 이름의 하위 문자열이 아니어야 함
SUBOLD	아니요	NUMBER	NULL	이전 암호 하위 문자열이 아니어야 함
SUBSTRLEN	아니요	NUMBER	NULL	암호에서 반복 하위 문자열의 최대 길이
SUBSTRREP	아니요	NUMBER	NULL	하위 문자열의 최대 반복
PASSWDLIFE	아니요	NUMBER	NULL	기본 암호 변경 주기(일)
GRACELOGINS	아니요	NUMBER	NULL	암호 만료 후 유예 로그인 횟수
USERBLOCKMIN	아니요	NUMBER	NULL	암호에서 사용자를 차단할 시간(분)
WRONGPASS	아니요	NUMBER	NULL	EXPIRE 가 설정될 때까지 실패한 암호 시도 횟수
HISTORY	아니요	NUMBER	NULL	기록 길이
MINTIME	아니요	NUMBER	NULL	최소 변경 주기(일?)
MAXLEN	아니요	NUMBER	NULL	최대 길이
DICTFORMAT	아니요	NUMBER	NULL	사전 형식 선택
BIDIRECTIONAL	아니요	NUMBER	NULL	양방향 암호 암호화를 활성화 또는 비활성화합니다. 양방향 암호 암호화를 활성화하면 각각의

이름	PK 여부	데이터 유형	Null 옵션	설명
				새 암호가 암호화되며 나중에 일반 텍스트로 다시 암호를 해독할 수 있습니다. 이 암호화는 새 암호와 이전 암호(암호 기록) 사이에 보다 폭넓은 비교를 제공합니다. 양방향 암호화가 비활성화되면 단방향 암호 기록 암호화가 활성화되며 이전 암호를 해독할 수 없습니다.

POLICY 테이블 열

다음 표에서는 POLICY 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.
RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
NAME	예	NVARCHAR2(256)	NULL	정책의 논리적 이름. AC 클래스 POLICY 의 POLICY_BASE_NAME AC 속성에 매핑됩니다.
VERSION	예	NUMBER	NULL	정책 버전을 나타내는 정수입니다. 정책 버전은 1 부터 시작하는 연속 숫자입니다. AC 클래스 POLICY 의

이름	PK 여부	데이터 유형	Null 옵션	설명
				POLICY_VERSION AC 속성에 매핑됩니다.
FINALIZE	아니요	NUMBER(1,0)	NULL	정책이 완료되었는지 여부(즉, 배포 가능 여부)입니다. AC 클래스 POLICY 의 FINALIZE AC 속성에 매핑됩니다.
EXTENDED_ SIGNATURE	아니요	NVARCHAR2(256)	NULL	FIPS 140-2 준수 SHA1 정책 서명. AC 클래스 POLICY 의 EXTENDED_SIGNATURE 속성에 매핑됩니다.
SIGNATURE	아니요	NVARCHAR2(256)	NULL	정책 서명. AC 클래스 POLICY 의 SIGNATURE 속성에 매핑됩니다.

POLICY_DEVIATION 테이블 열

다음 표에서는 POLICY_DEVIATION 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
NODE_RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다.
NODE_RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. AC: 리소스 개체 이름입니다.
DEVIATION_INDEX	예	NUMBER	NOT NULL	각 정책에 대해 0 부터 시작하는 위반 행 시퀀스 번호입니다. DEVCALC 출력에서 가장 최근

이름	PK 여부	데이터 유형	Null 옵션	설명
				POLICYSTART 태그를 기준으로 이 위반 행의 줄 번호에 매핑됩니다.
DEVIATED_CLASS	아니요	NVARCHAR2(256)	NULL	위반 클래스. DEVCALC 출력에서 DIFF 줄의 두 번째 토큰에 매핑됩니다. null 값은 DEVCALC 출력의 값(*)에 매핑됩니다.
DEVIATED_OBJECT	아니요	NVARCHAR2(256)	NULL	위반 개체. DEVCALC 출력에서 DIFF 줄의 세 번째 토큰에 매핑됩니다. null 값은 DEVCALC 출력의 값(*)에 매핑됩니다.
DEVIATED_PROPERTY	아니요	NVARCHAR2(256)	NULL	위반 속성. DEVCALC 출력에서 DIFF 줄의 네 번째 토큰에 매핑됩니다. null 값은 DEVCALC 출력의 값(*)에 매핑됩니다.
DEVIATED_VALUE	아니요	NVARCHAR2(256)	NULL	위반 값. DEVCALC 출력에서 DIFF 줄의 다섯 번째 토큰에 매핑됩니다. null 값은 DEVCALC 출력의 값(*)에 매핑됩니다.
DEVIATION_DATA	아니요	CLOB	NULL	해당 유형을 알 수 있는(즉, 'UNKNOWN_%'가 아님) 위반 행의 경우 이 값이 DEVCALC 출력에서 DIFF 줄의 첫 번째 토큰에 매핑됩니다(예: 'DIFF'). 다른 위반 행의 경우 이 필드에 전체 DEVCALC 줄이 그대로 포함되어 있습니다.
DEVIATION_TYPE	아니요	NVARCHAR2(256)	NULL	A_B 형식의 위반 유형. 여기서, A = EXPECTED, UNEXPECTED 또는 UNKNOWN B = CLASS, OBJECT, PROPERTY, VALUE 또는

이름	PK 여부	데이터 유형	Null 옵션	설명
				GENERIC

POLICY_GROUP 테이블 열

다음 표에서는 POLICY_GROUP 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
RESCLASS	예	NVARCHAR2(80)	NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.
RULEKEY	예	NVARCHAR2(256)	NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
LATEST_FIN_RULEKEY	아니요	NVARCHAR2(256)	NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. GPOLICY 클래스의 LATEST_FINALIZED_VERSION OID AC 속성의 ONAME 에 매핑됩니다.
LATEST_FIN_RESCLASS	아니요	NVARCHAR2(80)	NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. GPOLICY

이름	PK 여부	데이터 유형	Null 옵션	설명
				클래스의 LATEST_FINALIZED_VERSION OID AC 속성의 CNAME 에 매핑됩니다.
LATEST_RESCLASS	아니요	NVARCHAR2(80)	NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. GPOLICY 클래스의 LATEST_VERSION OID AC 속성의 CNAME 에 매핑됩니다.
LATEST_RULEKEY	아니요	NVARCHAR2(256)	NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. GPOLICY 클래스의 LATEST_VERSION OID AC 속성의 ONAME 에 매핑됩니다.

POLICY_GROUP_DEPENDENCY 테이블 열

다음 표에서는 POLICY_GROUP_DEPENDENCY 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
DEP_ON_RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.
RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는

이름	PK 여부	데이터 유형	Null 옵션	설명
				엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.
DEP_ON_RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.

POLICY_GROUP_NODE_ASSIGNMENT Table 테이블 열

다음 표에서는 POLICY_GROUP_NODE_ASSIGNMENT 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
POLICYGRP_RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스

이름	PK 여부	데이터 유형	Null 옵션	설명
				AC OID 의 CNAME 에 매핑됩니다.
POLICYGRP_RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
NODE_RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다. 이 필드가 'HNODE'와 같은 경우 노드 할당이 됩니다. 이 필드가 'GHNODE'와 같으면 노드 그룹이 됩니다.
NODE_RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. AC: 리소스 개체 이름입니다.

POLICY_RULESET 테이블 열

다음 표에서는 POLICY_RULESET 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의

이름	PK 여부	데이터 유형	Null 옵션	설명
				시스템 식별자입니다.
POLICY_RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.
POLICY_RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
RULESET_RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.
RULESET_RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.

POLICY_STATUS 테이블 열

다음 표에서는 POLICY_STATUS 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
NODE_RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는

이름	PK 여부	데이터 유형	Null 옵션	설명
				엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.
NODE_RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
POLICY_RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.
POLICY_RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
UPDATORTYPE	예	NVARCHAR2(80)	NULL	이 사용자의 클래스: USER, XUSER
UPDATORID	예	NVARCHAR2(256)	NULL	이 시스템에서 해당 개체의 식별자입니다.
STATUS	아니요	NVARCHAR2(256)	NULL	정책 상태: APPROVED, REJECTED, PROCESSING.
DEVSTATE	아니요	NVARCHAR2(20)	NULL	위반 상태: UNSET, YES, NO
LASTDEVTIME	아니요	TIMESTAMP(6)	NULL	마지막 위반 계산 시간
LASTSTATUSTIME	아니요	TIMESTAMP(6)	NULL	상태가 설정된 마지막 시간
UPDATORNAME	아니요	NVARCHAR2(256)	NULL	정책 업데이터 이름. AC

이름	PK 여부	데이터 유형	Null 옵션	설명
				class POLICY 의 POLICY_STATUS 속성의 UpdatorName 구성원에 매핑됩니다.
UPDATORID	아니요	NVARCHAR2(256)	NULL	업데이터 개체 이름. AC 클래스 POLICY 의 POLICY_STATUS 속성의 Updator 구성원의 ONAME 구성 요소에 매핑됩니다.
UPDATORTYPE	아니요	NVARCHAR2(256)	NULL	업데이터 개체 이름. AC 클래스 POLICY 의 POLICY_STATUS 속성의 Updator 구성원의 CNAME 구성 요소에 매핑됩니다.

POLICYMODELINFO 테이블 열

다음 표에서는 POLICYMODELINFO 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
INITIAL_POLICY_OFFSET	아니요	NUMBER	NULL	로컬 노드의 경우 이 레코드는 sepmd -L selang 명령에 의해 제공된 초기 정책 오프셋에 매핑됩니다.
LAST_POLICY_OFFSET	아니요	NUMBER	NULL	로컬 노드의 경우 이 레코드는 sepmd -L selang 명령에 의해 제공된 마지막 정책 오프셋에 매핑됩니다.

RAUDIT 테이블 열

다음 표에서는 RAUDIT 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다.
RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. AC: 리소스 개체 이름입니다.
AUDITSUCCESS	예	NUMBER(1,0)	NULL	AC 가 리소스에 대한 인증된 액세스를 로깅합니다.
AUDITFAILURE	예	NUMBER(1,0)	NULL	AC 가 검색된 인증되지 않은 액세스 시도를 로깅합니다.
DEBUG	아니요	NUMBER(1,0)	NULL	디버그 모드 동안 로그
TRUST	아니요	NUMBER(1,0)	NULL	트러스트 이벤트 감사

RESAC 테이블 열

다음 표에서는 RESAC 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.
RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
DESCRIPTION	아니요	NVARCHAR2(256)	NULL	레코드 설명. 관련 AC 리소스 클래스의 COMMENT AC 속성에 매핑됩니다.
CALENDAR	아니요	NVARCHAR2(256)	NULL	Unicenter TNG 의 시간 제한을 나타내는 Unicenter TNG 달력 개체를 지정합니다. AC 에서는 관리 용도로만 이러한 개체 목록을 유지하며 이 목록을 보호하지는 않습니다. 관련 AC 리소스 클래스의 CALENDAR AC 속성에 매핑됩니다.
NOTIFY	아니요	NVARCHAR2(256)	NULL	리소스 레코드로 표시되는 리소스에 액세스할 때마다 AC 가 알림 메시지를 보내도록 합니다. 사용자 이름이나 전자 메일 주소를 입력하거나 별칭이 지정된 경우 메일 그룹의 전자 메일 주소를 입력하십시오. 관련 AC 리소스 클래스의 NOTIFY AC 속성에 매핑됩니다.
SECLABEL	아니요	NVARCHAR2(256)	NULL	특정 보안 수준과 0 개 이상의 보안 범주 사이의

이름	PK 여부	데이터 유형	Null 옵션	설명
				관계를 나타내는 보안 레이블입니다. 관련 AC 리소스 클래스의 SECLABEL AC 속성에 매핑됩니다.
SECLEVEL	아니요	NUMBER	NULL	보안 수준. 관련 AC 리소스 클래스의 SECLEVEL AC 속성에 매핑됩니다.
CRETIME	아니요	TIMESTAMP(6)	NULL	작성 시간. 관련 AC 리소스 클래스의 CREATE_TIME AC 속성에 매핑됩니다.
WARNING	아니요	NUMBER(1,0)	NULL	접근자의 권한이 리소스에 액세스할 만큼 충분하지 않은 경우에도 AC 가 리소스에 대한 액세스를 허용합니다. 그러나 AC 는 감사 로그에 경고 메시지를 기록합니다. 관련 AC 리소스 클래스의 WARNING AC 속성에 매핑됩니다.
UNTRUST	아니요	NUMBER(1,0)	NULL	프로그램이 트러스트되었는지 여부를 나타냅니다. 이 속성이 설정되면 아무도 프로그램을 실행할 수 없습니다. 이 속성이 설정되지 않으면 이 프로그램에 대해 데이터베이스에 나열된 다른 속성을 사용하여 사용자가 프로그램을 실행할 수 있는 권한이 있는지 여부가 결정됩니다. 트러스트된 프로그램이 변경되면 AC 는 이 속성을 자동으로 설정합니다. PROGRAM, SECFILE 및 HOST 같은 AC 리소스 클래스의 UNTRUST AC 속성에 매핑됩니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
ETHINFO	아니요	NVARCHAR2(256)	NULL	호스트의 이더넷 정보. AC 리소스 클래스 HOST 의 ETHINFO AC 속성에 매핑됩니다.
NETMATCH	아니요	NVARCHAR2(256)	NULL	IP 주소 일치. AC 리소스 클래스 HOSTNET 의 INMASKMATCH AC 속성의 NetworkMatch 구성 요소에 매핑됩니다.
NETMASK	아니요	NVARCHAR2(256)	NULL	IP 주소 마스크. AC 리소스 클래스 HOSTNET 의 INMASKMATCH AC 속성의 Mask 구성 요소에 매핑됩니다.
AAUDIT	아니요	NVARCHAR2(256)	NULL	eTrust AC 가 감사를 수행하는 작업 유형을 표시합니다. AC 리소스 클래스 ADMIN 의 AAUDIT AC 속성에 매핑됩니다.
UNTRUSTREASON	아니요	NVARCHAR2(256)	NULL	UNIX dbdump 전용. AC 리소스 클래스 PROGRAM, SECFILE 의 UNTRUSTREASON AC 속성에 매핑됩니다.
ACCSWHO	아니요	NUMBER(20,0)	NULL	액세스 개체 이름. 레코드에 마지막으로 액세스한 관리자입니다. AC 리소스 클래스 PROGRAM 의 ACCSWHO AC 속성에 매핑됩니다. Unix 의 경우 UID(숫자 값)가 포함됩니다. Windows 의 경우 사용자 이름이 포함됩니다.
ACCSTIME	아니요	TIMESTAMP(6)	NULL	액세스 개체 이름(UNIX 전용). 레코드에 마지막으로 액세스한 날짜 및 시간입니다. AC 리소스 클래스 PROGRAM 의 ACCSTIME AC 속성에

이름	PK 여부	데이터 유형	Null 옵션	설명
				매핑됩니다.
BLOCKRUN	아니요	NUMBER(1,0)	NULL	실행 차단. AC 리소스 클래스 PROGRAM 의 BLOCKRUN AC 속성에 매핑됩니다.
UNIXUID	아니요	NVARCHAR2(256)	NULL	UNIX UID. AC 리소스 클래스 SPECIALPGM 의 UNIXUID AC 속성에 매핑됩니다.
INTERACTIVE	아니요	NUMBER(1,0)	NULL	대화형. sesudo 를 통해 실행할 응용 프로그램이 서비스 응용 프로그램이 아닌 대화형 Windows 응용 프로그램(예: notepad.exe, cmd.exe)인 경우 이 스위치가 표시되어 있어야 합니다. sesudo 클라이언트 명령을 통해 대화형 응용 프로그램을 실행할 때 이 스위치가 '대화형'으로 표시되어 있지 않으면 이 응용 프로그램은 상호 작용하는 기능 없이 백그라운드로 실행됩니다. AC 리소스 클래스 SUDO 의 INTERACTIVE AC 속성에 매핑됩니다.
TARGUSRCNAME	아니요	NVARCHAR2(80)	NULL	명령 실행을 위해 SUDO 클래스에서 권한을 빌려갈 사용자의 이름을 지정합니다. 기본값은 SUDO 클래스의 관리자입니다. AC 리소스 클래스 SUDO 의 TARGUSR AC 속성의 CNAME 에 매핑됩니다(UNIX 전용).
TARGUSRONAME	아니요	NVARCHAR2(256)	NULL	AC 리소스 클래스 SUDO 의 TARGUSR AC

이름	PK 여부	데이터 유형	Null 옵션	설명
				속성의 ONAME 에 매핑됩니다(UNIX 전용).
PASSWDREQ	아니요	NUMBER(1,0)	NULL	암호 필요. 실행하기 전에 sesudo 명령이 대상 사용자 암호를 요청하는지 여부를 나타냅니다. AC 리소스 클래스 SUDO 의 PASSWDREQ AC 속성에 매핑됩니다(UNIX 전용).
FILEPATH	아니요	NVARCHAR2(256)	NULL	AC 리소스 클래스 KMODULE 의 FILEPATH AC 속성에 매핑됩니다.

RESINFO 테이블 열

다음 표에서는 RESINFO 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.
RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
PREFIX	아니요	NVARCHAR2(40)	NULL	CA ACF2 전용: 규칙 집합의 Prefix 필드

이름	PK 여부	데이터 유형	Null 옵션	설명
OWNERCNAME	아니요	NVARCHAR2(80)	NULL	이 리소스 소유자의 클래스입니다. 소유자의 보안 수준, 보안 레이블 및 보안 범주 권한이 리소스에 액세스할 수 있을 만큼 충분한 경우 리소스 레코드의 소유자는 리소스에 제한 없이 액세스할 수 있습니다. 리소스 소유자는 항상 리소스 레코드를 업데이트 및 삭제할 수 있습니다. 'GROUP' 또는 'XGROUP' 값은 GROUPINFO 테이블에 관련 레코드가 있음을 의미합니다. 'USER' 또는 'XUSER'는 USERINFO 테이블에 관련 레코드가 있음을 의미합니다. 관련 AC 리소스 클래스의 OWNER 속성의 CNAME 에 매핑됩니다.
OWNERONAME	아니요	NVARCHAR2(256)	NULL	이 리소스 소유자의 개체 이름입니다. 관련 AC 리소스 클래스의 OWNER 속성의 ONAME 에 매핑됩니다.
OWNRTYPE	아니요	CHAR(1)	NULL	이 리소스의 소유자가 사용자(U) 또는 역할(R)인지 나타냅니다. 관련 AC 리소스 클래스의 OWNER 속성의 CNAME 의 첫 번째 문자에 매핑됩니다.
RESOWNER	아니요	NVARCHAR2(256)	NULL	CA ACF2: 규칙 집합의 $RESOWNER 값. CA Top Secret: SMS RESOWNER.
RULEOWNER	아니요	NVARCHAR2(256)	NULL	CA ACF2 전용. 규칙 집합의 $OWNER 값입니다.
ADMINBYCNAME	아니요	NVARCHAR2(80)	NULL	CA ACF2 및 AC: 이 규칙 집합을 마지막으로 변경한

이름	PK 여부	데이터 유형	Null 옵션	설명
				관리자의 클래스입니다. 'GROUP' 또는 'XGROUP' 값은 GROUPINFO 테이블에 관련 레코드가 있음을 의미합니다. 'USER' 또는 'XUSER'는 USERINFO 테이블에 관련 레코드가 있음을 의미합니다. 관련 AC 리소스 클래스의 UPDATE_WHO 속성의 CNAME 에 매핑됩니다.
ADMINBYONAME	아니요	NVARCHAR2(256)	NULL	이 규칙 집합을 마지막으로 변경한 관리자의 개체 이름입니다. 관련 AC 리소스 클래스의 UPDATE_WHO 속성의 ONAME 에 매핑됩니다.
ADMINDATE	아니요	TIMESTAMP(6)	NULL	CA ACF2 및 AC. 이 규칙 집합을 마지막으로 변경한 날짜입니다. 관련 AC 리소스 클래스의 UPDATE_TIME AC 속성에 매핑됩니다.
USERDATA	아니요	NVARCHAR2(256)	NULL	CA ACF2 전용. 규칙 집합의 $USERDATA 값입니다.
ON_BEHALF_OF	아니요	NVARCHAR2(256)	NULL	유효한 사용자 ID. DEPLOYMENT, GDEPLOYMENT, HNODE, GHNODE, POLICY, GPOLICY, RULEKEY 같은 다양한 AC 클래스의 ON_BEHALF_OF AC 속성에 매핑됩니다.

RULESET 테이블 열

다음 표에서는 RULESET 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.
RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
FINALIZE	아니요	NUMBER(1,0)	NULL	이 규칙 집합이 완료되었는지 여부(즉, 배포 가능 여부)입니다. AC 클래스 RULESET 의 FINALIZE AC 속성에 매핑됩니다.
EXTENDED_SIGNATURE	아니요	NVARCHAR2(256)	NULL	FIPS 140-2 준수 SHA1 규칙 집합 서명. AC 클래스 RULESET 의 EXTENDED_SIGNATURE 속성에 매핑됩니다.
SIGNATURE	아니요	NVARCHAR2(256)	NULL	규칙 집합 서명. AC 클래스 RULESET 의 SIGNATURE 속성에 매핑됩니다.

RULESET_COMMAND 테이블 열

다음 표에서는 RULESET_COMMAND 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
RULESET_RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다. 리소스 AC OID 의 CNAME 에 매핑됩니다.
RULESET_RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. 리소스 AC OID 의 ONAME 에 매핑됩니다.
COMMANDIDX	예	NUMBER	NOT NULL	규칙 집합 명령이 정렬됩니다. 이 열은 명령 시퀀스에서 명령의 위치를 나타냅니다. AC 클래스 RULESET 의 RULESET_DO/UNDOCMDS AC 속성의 명령 인덱스 구성 요소에 매핑됩니다(자세한 내용은 COMMANDTYPE 열 참조).
COMMANDTYPE	예	NVARCHAR2(20)	NOT NULL	명령 유형: do, undo. 유형이 'do'인 경우 이 레코드는 AC 클래스 RULESET 의 RULESET_DOCMDS AC 속성 내부의 명령에 매핑됩니다. 유형이 'undo'인 경우 레코드는 대신

이름	PK 여부	데이터 유형	Null 옵션	설명
				RULESET_UNDOCMDS 속성에 매핑됩니다.
COMMANDSTR	예	NVARCHAR2(256)	NULL	명령 문자열. AC 클래스 RULESET 의 RULESET_DO/UNDOCMDS AC 속성의 명령 문자열 구성 요소에 매핑됩니다(자세한 내용은 COMMANDTYPE 열 참조).

SEOS 테이블 열

다음 표에서는 SEOS 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
LASTSTARTUP	아니요	TIMESTAMP(6)	NULL	호스트 마지막 시작 시간. AC 클래스 SEOS 의 STARTTIME AC 속성에 매핑됩니다.
LASTSHUTDOWN	아니요	TIMESTAMP(6)	NULL	호스트 마지막 종료 시간. AC 클래스 SEOS 의 ENDTIME AC 속성에 매핑됩니다.
UPDATEDBY	아니요	NVARCHAR2(256)	NULL	마지막 업데이트한 사람 개체 이름. AC 클래스 SEOS 의 UPDATE_WHO AC 속성의 ONAME 에 매핑됩니다.
UPDATETIME	아니요	TIMESTAMP(6)	NULL	마지막 업데이트 시간. AC 클래스 SEOS 의 UPDATE_TIME AC

이름	PK 여부	데이터 유형	Null 옵션	설명
				속성에 매핑됩니다.
INACTIVEDAYS	아니요	NUMBER	NULL	비활성 기간. AC 클래스 SEOS 의 INACT AC 속성에 매핑됩니다.
ACCUMACL	아니요	NUMBER(1,0)	NULL	ACL 및 PACL 누적. AC 클래스 SEOS 의 ACCPACL AC 속성에 매핑됩니다.
ACCUMGRPRIGHTS	아니요	NUMBER(1,0)	NULL	그룹 권한 누적. AC 클래스 SEOS 의 GRACCR AC 속성에 매핑됩니다.
ADMINPWDCHANGE	아니요	NUMBER(1,0)	NULL	관리자 암호 변경. AC 클래스 SEOS 의 CNG_ADMIN_PWD AC 속성에 매핑됩니다.
OWNPWDCHANGE	아니요	NUMBER(1,0)	NULL	직접 암호 변경. AC 클래스 SEOS 의 CNG_OWN_PWD AC 속성에 매핑됩니다.
ISDMA	아니요	NUMBER(1,0)	NULL	DMA 호스트인지 여부입니다. AC 클래스 SEOS 의 ISDMA AC 속성에 매핑됩니다.
ISDMS	아니요	NUMBER(1,0)	NULL	DMS 호스트인지 여부입니다. AC 클래스 SEOS 의 ISDMS AC 속성에 매핑됩니다.
ISDH	아니요	NUMBER(1,0)	NULL	DH(배포 호스트). AC 클래스 SEOS 의 ISDH AC 속성에 매핑됩니다.
DMS	아니요	NVARCHAR2(256)	NULL	DMS 호스트 이름. AC 클래스 SEOS 의 DMS AC 속성에 매핑됩니다.
CADMIN	아니요	NUMBER(1,0)	NULL	클래스 활성화: ADMIN. AC 클래스 SEOS 의 ADMIN AC 속성에 매핑됩니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
CAPPL	아니요	NUMBER(1,0)	NULL	클래스 활성화: APPL. AC 클래스 SEOS 의 APPL AC 속성에 매핑됩니다.
CAUTHHOST	아니요	NUMBER(1,0)	NULL	클래스 활성화: AUTHHOST. AC 클래스 SEOS 의 AUTHHOST AC 속성에 매핑됩니다.
CCALENDAR	아니요	NUMBER(1,0)	NULL	클래스 활성화: CALENDAR. AC 클래스 SEOS 의 CALENDAR AC 속성에 매핑됩니다.
CCATEGORY	아니요	NUMBER(1,0)	NULL	클래스 활성화: CATEGORY. AC 클래스 SEOS 의 CATEGORY AC 속성에 매핑됩니다.
CCONNECT	아니요	NUMBER(1,0)	NULL	클래스 활성화: CONNECT. AC 클래스 SEOS 의 CONNECT AC 속성에 매핑됩니다.
CDEPLOYMENT	아니요	NUMBER(1,0)	NULL	클래스 활성화: DEPLOYMENT. AC 클래스 SEOS 의 DEPLOYMENT AC 속성에 매핑됩니다.
CDICTIONARY	아니요	NUMBER(1,0)	NULL	클래스 활성화: DICTIONARY. AC 클래스 SEOS 의 DICTIONARY AC 속성에 매핑됩니다.
CDOMAIN	아니요	NUMBER(1,0)	NULL	클래스 활성화: DOMAIN. AC 클래스 SEOS 의 DOMAIN AC 속성에 매핑됩니다.
CFILE	아니요	NUMBER(1,0)	NULL	클래스 활성화: FILE. AC 클래스 SEOS 의 FILE AC 속성에 매핑됩니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
CHNODE	아니요	NUMBER(1,0)	NULL	클래스 활성화: HNODE. AC 클래스 SEOS 의 HNODE AC 속성에 매핑됩니다.
CHOLIDAY	아니요	NUMBER(1,0)	NULL	클래스 활성화: HOLIDAY. AC 클래스 SEOS 의 HOLIDAY AC 속성에 매핑됩니다.
CHOST	아니요	NUMBER(1,0)	NULL	클래스 활성화: HOST. AC 클래스 SEOS 의 HOST AC 속성에 매핑됩니다.
CKMODULE	아니요	NUMBER(1,0)	NULL	클래스 활성화: KMODULE. AC 클래스 SEOS 의 KMODULE AC 속성에 매핑됩니다.
CMFTERMINAL	아니요	NUMBER(1,0)	NULL	클래스 활성화: MFTERMINAL. AC 클래스 SEOS 의 MFTERMINAL AC 속성에 매핑됩니다.
CPASSWORD	아니요	NUMBER(1,0)	NULL	클래스 활성화: PASSWORD. AC 클래스 SEOS 의 PASSWORD AC 속성에 매핑됩니다.
CPOLICY	아니요	NUMBER(1,0)	NULL	클래스 활성화: POLICY. AC 클래스 SEOS 의 POLICY AC 속성에 매핑됩니다.
CPROGRAM	아니요	NUMBER(1,0)	NULL	클래스 활성화: PROGRAM. AC 클래스 SEOS 의 PROGRAM AC 속성에 매핑됩니다.
CPROCESS	아니요	NUMBER(1,0)	NULL	클래스 활성화: PROCESS. AC 클래스 SEOS 의 PROCESS AC 속성에 매핑됩니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
CPWPOLICY	아니요	NUMBER(1,0)	NULL	클래스 활성화: PWPOLICY. AC 클래스 SEOS 의 PWPOLICY AC 속성에 매핑됩니다.
CREGKEY	아니요	NUMBER(1,0)	NULL	클래스 활성화: REGKEY. AC 클래스 SEOS 의 REGKEY AC 속성에 매핑됩니다.
CREGVAL	아니요	NUMBER(1,0)	NULL	클래스 활성화: REGVAL. AC 클래스 SEOS 의 REGVAL AC 속성에 매핑됩니다.
CRULESET	아니요	NUMBER(1,0)	NULL	클래스 활성화: RULESET. AC 클래스 SEOS 의 RULESET AC 속성에 매핑됩니다.
CSECLABEL	아니요	NUMBER(1,0)	NULL	클래스 활성화: SECLABEL. AC 클래스 SEOS 의 SECLABEL AC 속성에 매핑됩니다.
CSECLEVEL	아니요	NUMBER(1,0)	NULL	클래스 활성화: SECLEVEL. AC 클래스 SEOS 의 SECLEVEL AC 속성에 매핑됩니다.
CSPECIALPGM	아니요	NUMBER(1,0)	NULL	클래스 활성화: SPECIALPGM. AC 클래스 SEOS 의 SPECIALPGM AC 속성에 매핑됩니다.
CSUDO	아니요	NUMBER(1,0)	NULL	클래스 활성화: SUDO. AC 클래스 SEOS 의 SUDO AC 속성에 매핑됩니다.
CSURROGATE	아니요	NUMBER(1,0)	NULL	클래스 활성화: SURROGATE. AC 클래스 SEOS 의 SURROGATE AC 속성에 매핑됩니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
CTCP	아니요	NUMBER(1,0)	NULL	클래스 활성화: TCP. AC 클래스 SEOS 의 TCP AC 속성에 매핑됩니다.
CTERMINAL	아니요	NUMBER(1,0)	NULL	클래스 활성화: TERMINAL. AC 클래스 SEOS 의 TERMINAL AC 속성에 매핑됩니다.
CUSER_DIR	아니요	NUMBER(1,0)	NULL	클래스 활성화: USER_DIR. AC 클래스 SEOS 의 USER_DIR AC 속성에 매핑됩니다.
CWEBSERVICE	아니요	NUMBER(1,0)	NULL	클래스 활성화: WEBSERVICE. AC 클래스 SEOS 의 WEBSERVICE AC 속성에 매핑됩니다.
CWINSERVICE	아니요	NUMBER(1,0)	NULL	Windows 전용: 클래스 활성화: WINSERVICE. AC 클래스 SEOS 의 WINSERVICE AC 속성에 매핑됩니다.
CDAYTIMERES	아니요	NUMBER(1,0)	NULL	UNIX 전용: 시간 제한 확인 여부입니다. AC 클래스 SEOS 의 DAYTIMERES AC 속성에 매핑됩니다.
CLOGINAPPL	아니요	NUMBER(1,0)	NULL	UNIX 전용. AC 클래스 SEOS 의 LOGINAPPL AC 속성에 매핑됩니다.
MAXLOGINS	아니요	NUMBER	NULL	유효한 최대 로그인 횟수. AC 클래스 SEOS 의 MAXLOGINS AC 속성에 매핑됩니다.
PROHIBITED	아니요	NVARCHAR2(256)	NULL	AC 클래스 SEOS 의 PROHIBITED AC 속성에 매핑됩니다.
ACID	아니요	NVARCHAR2(256)	NULL	고유한 AC 호스트 ID.

이름	PK 여부	데이터 유형	Null 옵션	설명
				AC 클래스 SEOS 의 ACID 속성에 매핑됩니다. 이 값은 NODE 테이블에서 동일한 ACID 를 가진 노드를 식별하는 데 사용됩니다.

SEOSSYSCALL 테이블의 열

다음 표에서는 SEOSSYSCALL 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
INTERCEPTEDSYSCALLS	아니요	NUMBER(20,0)	NULL	차단된 syscall 의 수
NONBLOCKINGSYSCALLS	아니요	NUMBER(1,0)	NULL	"위험"하지 않은 차단된 syscall 의 수
ISOVERFLOW	아니요	NUMBER(20,0)	NULL	할당된 버퍼가 너무 작은 경우 1
THRESHOLDTIME	아니요	NUMBER(20,0)	NULL	syscall 의 "위험한" 시간(초)
ALWAYSEXITSCRIPT	아니요	NUMBER(1,0)	NULL	SEOS_unload_int.always 가 존재하는 경우 1
OPTIONALEXITSCRIPT	아니요	NUMBER(1,0)	NULL	SEOS_unload_int.opt 가 존재하는 경우 1
USETRIPACCEPT	아니요	NUMBER(1,0)	NULL	use_tripAccept 토큰이 "yes"인 경우 1
TRIPACCEPT	아니요	NUMBER(1,0)	NULL	bin/tripAccept 가 존재하는 경우 1

이름	PK 여부	데이터 유형	Null 옵션	설명
NOVELLZMD	아니요	NUMBER(1,0)	NULL	/etc/init.d/novell-zmd 가 존재하는 경우 1
XM	아니요	NUMBER(1,0)	NULL	/usr/sbin/xm 이 존재하는 경우 1
NSCD	아니요	NUMBER(1,0)	NULL	/etc/init.d/nscd 가 존재하는 경우 1

SNAPSHOTINFO 테이블 열

다음 표에서는 SNAPSHOTINFO 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
DUMPSTARTTIME	아니요	TIMESTAMP(6)	NULL	스냅숏 시작 시간
DUMPENDTIME	아니요	TIMESTAMP(6)	NULL	스냅숏 종료 시간
STATUS	아니요	CHAR(1)	NULL	스냅숏 상태
SNAPSHOTTIME	아니요	TIMESTAMP(6)	NULL	
SNAPSHOTTYPE	아니요	NVARCHAR2(256)	NULL	
SNAPSHOTNAME	아니요	NVARCHAR2(256)	NULL	
OS	아니요	NVARCHAR2(100)	NULL	
ACVERSION	아니요	NVARCHAR2(50)	NULL	
ACVERSIONNUM1	아니요	NUMBER(20,0)	NULL	
ACVERSIONNUM2	아니요	NUMBER(20,0)	NULL	
ACVERSIONNUM3	아니요	NUMBER(20,0)	NULL	
ACVERSIONNUM4	아니요	NUMBER(20,0)	NULL	

SPECIALPGMTYPE 테이블 열

다음 표에서는 SPECIALPGMTYPE 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다.
RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. AC: 리소스 개체 이름입니다.
TMAIL	아니요	NUMBER(1,0)	NULL	
TBACKUP	아니요	NUMBER(1,0)	NULL	
TXDM	아니요	NUMBER(1,0)	NULL	
TDCM	아니요	NUMBER(1,0)	NULL	
TPBF	아니요	NUMBER(1,0)	NULL	
TPBN	아니요	NUMBER(1,0)	NULL	
TPROPAGATE	아니요	NUMBER(1,0)	NULL	(r12.0 SP1)
TSTOP	아니요	NUMBER(1,0)	NULL	
TSURR	아니요	NUMBER(1,0)	NULL	
TREG	아니요	NUMBER(1,0)	NULL	
TRESTRICTED	아니요	NUMBER(1,0)	NULL	

SYSCALL 테이블의 열

다음 표에서는 SYSCALL 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
PID	예	NUMBER(20,0)	NOT NULL	키: 프로세스 pid
PARENTPID	아니요	NUMBER(20,0)	NULL	부모 프로세스 ID
USERID	아니요	NUMBER(20,0)	NULL	실제 사용자 ID
GROUPID	아니요	NUMBER(20,0)	NULL	그룹 ID
INTERCEPTEDPGM	아니요	NVARCHAR2(256)	NULL	프로그램 이름
INTERCEPTEDTIME	아니요	NUMBER(20,0)	NULL	syscall 의 수명
SYSCALLNUM	아니요	NUMBER(20,0)	NULL	시스템 호출 번호
ISBLOCKING	아니요	NUMBER(1,0)	NULL	syscall 이 위험한 경우 1

SYSCALLUSERSPECIALPGM 표의 열

다음 표에서는 SYSCALLUSERSPECIALPGM 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
SAFEPGM	예	NVARCHAR2(256)	NOT NULL	

UACC 테이블 열

다음 표에서는 UACC 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
RESCLASS	예	NVARCHAR2(80)	NOT NULL	사용 권한이 적용되는 엔터티의 리소스 클래스입니다.
RULEKEY	예	NVARCHAR2(256)	NOT NULL	CA ACF2: 사용 권한이 발견된 규칙의 규칙 집합 키입니다. CA Top Secret: 이 리소스에 대해 소유된 리소스 마스크입니다. AC: 리소스 개체 이름입니다.
AREAD	아니요	NUMBER(1,0)	NULL	
AWRITE	아니요	NUMBER(1,0)	NULL	
AMODIFY	아니요	NUMBER(1,0)	NULL	
ACREATE	아니요	NUMBER(1,0)	NULL	
AERASE	아니요	NUMBER(1,0)	NULL	
AFILESCAN	아니요	NUMBER(1,0)	NULL	
ALANGINT	아니요	NUMBER(1,0)	NULL	
AEXEC	아니요	NUMBER(1,0)	NULL	
ACHOWN	아니요	NUMBER(1,0)	NULL	
ACHGRP	아니요	NUMBER(1,0)	NULL	
ACHMOD	아니요	NUMBER(1,0)	NULL	
AUTIMES	아니요	NUMBER(1,0)	NULL	
ASEC	아니요	NUMBER(1,0)	NULL	
AKILL	아니요	NUMBER(1,0)	NULL	
ACONNECT	아니요	NUMBER(1,0)	NULL	

이름	PK 여부	데이터 유형	Null 옵션	설명
ARENAME	아니요	NUMBER(1,0)	NULL	
APASSWORD	아니요	NUMBER(1,0)	NULL	
AAUTHORIZED	아니요	CHAR(18)	NULL	
AXAUDIT	아니요	NUMBER(1,0)	NULL	
ACHDIR	아니요	NUMBER(1,0)	NULL	
ACRSUBK	아니요	NUMBER(1,0)	NULL	
ANOTIFY	아니요	NUMBER(1,0)	NULL	
AENUM	아니요	NUMBER(1,0)	NULL	
AQUERY	아니요	NUMBER(1,0)	NULL	
ARCTRL	아니요	NUMBER(1,0)	NULL	
ACRLINK	아니요	NUMBER(1,0)	NULL	
APRINT	아니요	NUMBER(1,0)	NULL	
AMANAGE	아니요	NUMBER(1,0)	NULL	
AMAXALLOWED	아니요	NUMBER(1,0)	NULL	
ASTOP	아니요	NUMBER(1,0)	NULL	
APAUSE	아니요	NUMBER(1,0)	NULL	
ACONTROL	아니요	NUMBER(1,0)	NULL	
ACHOG	아니요	NUMBER(1,0)	NULL	
ARESUME	아니요	NUMBER(1,0)	NULL	

USERAC 테이블 열

다음 표에서는 USERAC 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
USERID	예	NVARCHAR2(256)	NOT NULL	이 레코드의 사용자 ID(이름). USER/XUSER 개체의 AC OID 에 매핑됩니다.
USERTYPE	예	NVARCHAR2(80)	NOT NULL	이 사용자의 AC 클래스: USER, XUSER.
DESCRIPTION	아니요	NVARCHAR2(256)	NULL	이 사용자의 설명. USER/XUSER 클래스의 COMMENT AC 속성에 매핑됩니다.
PROFILE	아니요	NVARCHAR2(256)	NULL	사용자의 프로필에 대한 경로를 지정하는 문자열입니다. 이 문자열은 로컬 절대 경로 또는 UNC 경로를 포함할 수 있습니다. USER/XUSER 클래스의 PROFILE AC 속성의 ONAME 에 매핑됩니다.
GRACELOGIN	아니요	NUMBER	NULL	암호가 만료된 후 사용자의 유예 로그인 횟수입니다. 유예 로그인 횟수를 초과하면 시스템에 대한 액세스가 거부되고 시스템 관리자에게 새 암호를 문의해야 합니다. USER/XUSER 클래스의 GRACELOGIN AC 속성에 매핑됩니다.
MAXLOGINS	아니요	NUMBER	NULL	사용자가 동시에 로그인할 수 있는 최대 터미널 수를 설정합니다. 값 0 은 사용자가 터미널 수에 상관없이 동시에 로그인할 수 있음을 의미합니다. USER/XUSER 클래스의 MAXLOGINS AC

이름	PK 여부	데이터 유형	Null 옵션	설명
				속성에 매핑됩니다.
INACTIVE	아니요	NUMBER	NULL	시스템에서 사용자가 비활성 상태로 전환되기 전까지 대기하는 일 수를 지정합니다. 지정된 일 수에 도달하면 사용자는 로그인할 수 없습니다. USER/XUSER 클래스의 INACTIVE AC 속성에 매핑됩니다.
SUSPENDDATE	아니요	DATE	NULL	사용자 레코드를 비활성화하지만 데이터베이스에 정의된 상태를 유지합니다. 사용자는 일시 중지된 사용자 계정을 사용하여 시스템에 로그인할 수 없습니다. USER/XUSER 클래스의 SUSPEND_DATE AC 속성에 매핑됩니다.
SUSPENDWHOCNAME	아니요	NVARCHAR2(80)	NULL	중단 날짜를 활성화한 관리자입니다. USER/XUSER 클래스의 SUSPEND_WHO AC 속성의 CNAME 에 매핑됩니다.
SUSPENDWHOONAME	아니요	NVARCHAR2(256)	NULL	이 시스템에서 해당 개체의 식별자입니다. USER/XUSER 클래스의 SUSPEND_WHO AC 속성의 ONAME 에 매핑됩니다.
RESUMEDATE	아니요	DATE	NULL	suspend 매개 변수를 지정하여 비활성화된 사용자 레코드를 활성화합니다. USER/XUSER 클래스의 RESUME_DATE AC

이름	PK 여부	데이터 유형	Null 옵션	설명
				속성에 매핑됩니다.
LUTERMINAL	아니요	NVARCHAR2(256)	NULL	터미널에서 마지막 업데이트한 시간. USER/XUSER 클래스의 LAST_ACC_TERM AC 속성에 매핑됩니다.
PASSWDINT	아니요	NUMBER	NULL	암호 설정 또는 변경 이후 시스템에 새 사용자 암호를 입력해야 하는 일 수를 설정합니다. USER/XUSER 클래스의 PASSWD_INT AC 속성에 매핑됩니다.
PASSWDLAC	아니요	TIMESTAMP(6)	NULL	관리자가 암호를 마지막으로 업데이트한 날짜 및 시간입니다. USER/XUSER 클래스의 PASSWD_L_A_C AC 속성에 매핑됩니다.
PASSWDLC	아니요	TIMESTAMP(6)	NULL	암호가 마지막으로 업데이트된 날짜 및 시간입니다. USER/XUSER 클래스의 PASSWD_L_C AC 속성에 매핑됩니다.
PASSWDACW	아니요	NVARCHAR2(256)	NULL	이 레코드의 사용자 암호를 마지막으로 변경한 ADMIN 사용자입니다. USER/XUSER 클래스의 PASSWD_A_C_W AC 속성에 매핑됩니다.
MINTIME	아니요	NUMBER	NULL	암호를 다시 변경하기 위해 대기해야 하는 최소 일 수입니다. USER/XUSER 클래스의 MIN_TIME AC 속성에 매핑됩니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
POLICYMODEL	아니요	NVARCHAR2(256)	NULL	사용자가 sepass 유틸리티를 사용하여 암호를 변경하면 eTrust AC 가 새 암호를 지정된 정책 모델(pmdbName)로 전파하도록 지정합니다. 암호는 다음 레지스트리 하위 키의 parent_pmd 또는 passwd_pmd 값에서 정의된 정책 모델로 전송되지 않습니다. HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrust AccessControl\eTrust AccessControl. USER/XUSER 클래스의 POLICYMODEL AC 속성에 매핑됩니다.
SESSIONGROUP	아니요	NVARCHAR2(256)	NULL	통합 사용자 인증에서 사용됩니다. 이 속성은 SSO 세션 그룹을 사용자에게 할당합니다. SESSION_GROUP 속성의 최대 길이는 16 자입니다. USER/XUSER 클래스의 SESSION_GROUP AC 속성에 매핑됩니다.
LOGINSTATUS	아니요	NVARCHAR2(256)	NULL	로그인 상태
PWDNEXTCHGINDAYS	아니요	NUMBER	NULL	암호 변경이 가능한 기간(일)
APPLISTTIME	아니요	TIMESTAMP(6)	NULL	USER/XUSER 클래스의 APPLIST_TIME AC 속성에 매핑됩니다.
AUTHNMTHD	아니요	NVARCHAR2(256)	NULL	인증 방법. USER/XUSER 클래스의 AUTHNMTHD AC

이름	PK 여부	데이터 유형	Null 옵션	설명
				속성에 매핑됩니다.
BADPASSWD	아니요	NUMBER	NULL	잘못된 암호 입력 횟수. USER/XUSER 클래스의 BADPASSWD AC 속성에 매핑됩니다.
CALENDAR	아니요	NVARCHAR2(256)	NULL	Unicenter TNG 의 시간 제한을 나타내는 Unicenter TNG 달력 개체를 지정합니다. AC 에서는 관리 용도로만 이러한 개체 목록을 유지하며 이 목록을 보호하지는 않습니다. USER/XUSER 클래스의 CALENDAR AC 속성에 매핑됩니다.
UPDTIME	아니요	TIMESTAMP(6)	NULL	레코드가 마지막으로 수정된 날짜 및 시간입니다. USER/XUSER 클래스의 UPDTIME AC 속성에 매핑됩니다.
LOCATION	아니요	NVARCHAR2(256)	NULL	사용자 위치. USER/XUSER 클래스의 LOCATION AC 속성에 매핑됩니다.
EMAIL	아니요	NVARCHAR2(256)	NULL	사용자의 전자 메일 주소. USER/XUSER 클래스의 EMAIL AC 속성에 매핑됩니다.
ORGANIZATION	아니요	NVARCHAR2(256)	NULL	사용자의 조직 이름. USER/XUSER 클래스의 ORGANIZATION AC 속성에 매핑됩니다.
ORGUNIT	아니요	NVARCHAR2(256)	NULL	사용자의 조직 단위. USER/XUSER 클래스의 ORG_UNIT AC 속성에 매핑됩니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
PHONE	아니요	NVARCHAR2(256)	NULL	사용자 전화 번호. USER/XUSER 클래스의 PHONE AC 속성에 매핑됩니다.
COUNTRY	아니요	NVARCHAR2(256)	NULL	사용자가 있는 국가를 지정합니다. 이 문자열은 X.500 명명 체계의 일부입니다. eTrust AC 는 권한 부여에 이 문자열을 사용하지 않습니다. USER/XUSER 클래스의 COUNTRY AC 속성에 매핑됩니다.
LOCALAPPS	아니요	NUMBER(1,0)	NULL	USER/XUSER 클래스의 LOCALAPPS AC 속성에 매핑됩니다.
LOGSHIFT	아니요	NUMBER(1,0)	NULL	근무 시간 이외에도 로그인을 허용할지 여부를 나타냅니다. AC 는 감사 로그에 이 이벤트에 대한 감사 레코드를 기록합니다. USER/XUSER 클래스의 LOGSHIFT AC 속성에 매핑됩니다.
NOTIFY	아니요	NVARCHAR2(256)	NULL	사용자가 로그인할 때마다 사용자에게 알립니다. 사용자 이름이나 전자 메일 주소를 입력하거나 별칭이 지정된 경우 메일 그룹의 전자 메일 주소를 입력하십시오. 알림 메시지의 수신자는 각 메시지에 설명된 인증되지 않은 액세스 시도에 대응하기 위해 자주 로그인해야 합니다. USER/XUSER 클래스의 NOTIFY AC

이름	PK 여부	데이터 유형	Null 옵션	설명
				속성에 매핑됩니다.
OIDCRDDATA	아니요	NVARCHAR2(256)	NULL	CA 통합 사용자 인증 및 CA Web Access Control 에서 사용됩니다. USER/XUSER 클래스의 OIDCRDDATA AC 속성에 매핑됩니다.
PWDAUTOGEN	아니요	NUMBER(1,0)	NULL	응용 프로그램의 암호가 정책 서버에서 자동으로 생성되는지 여부를 나타냅니다. USER/XUSER 클래스의 PWD_AUTOGEN AC 속성에 매핑됩니다.
PWDSYNC	아니요	NUMBER(1,0)	NULL	응용 프로그램의 암호가 사용자의 다른 응용 프로그램 암호와 동일할 수 있는지 여부를 나타냅니다. USER/XUSER 클래스의 PWD_SYNC AC 속성에 매핑됩니다.
SCRIPTVARS	아니요	NVARCHAR2(256)	NULL	CA 통합 사용자 인증 및 CA Web Access Control 에서 사용되며, 응용 프로그램별로 저장되는 응용 프로그램 스크립트의 변수 값이 수록된 변수 목록입니다. USER/XUSER 클래스의 SCRIPT_VARS AC 속성에 매핑됩니다.
SECLEVEL	아니요	NUMBER	NULL	사용자 레코드에 대한 보안 수준. USER/XUSER 클래스의 SECLEVEL AC 속성에 매핑됩니다.
SECLABEL	아니요	NVARCHAR2(256)	NULL	USER/XUSER 클래스의

이름	PK 여부	데이터 유형	Null 옵션	설명
				SECLABEL AC 속성의 ONAME 에 매핑됩니다.
SHIFT	아니요	NVARCHAR2(256)	NULL	CA 통합 사용자 인증 및 CA Web Access Control 에서 사용됩니다. USER/XUSER 클래스의 SHIFT AC 속성의 ONAME 에 매핑됩니다.
UALIAS	아니요	NVARCHAR2(256)	NULL	하나 이상의 인증 호스트에 정의된 특정 사용자의 모든 별칭입니다. CA 통합 사용자 인증 및 CA Web Access Control 에서 사용됩니다. USER/XUSER 클래스의 UALIAS AC 속성에 매핑됩니다.
NOCHGPWD	아니요	NUMBER(1,0)	NULL	UNIX 전용: 암호 변경 없음. AC 클래스 USER 의 NOCHNGPASS AC 속성에 매핑됩니다.
OWNERONAME	아니요	NVARCHAR2(256)	NULL	소유자 개체 이름. USER/XUSER 클래스의 OWNER AC 속성의 ONAME 에 매핑됩니다.
OWNERCNAME	아니요	NVARCHAR2(80)	NULL	소유자 클래스 이름. GROUP 또는 XGROUP 은 GROUPINFO 테이블에 소유자 레코드가 있음을 의미합니다. USER 또는 XUSER 는 USERINFO 테이블에 소유자 레코드가 있음을 의미합니다. USER/XUSER 클래스의 OWNER AC 속성의

이름	PK 여부	데이터 유형	Null 옵션	설명
				CNAME 에 매핑됩니다.

USERACAUDIT 테이블 열

다음 표에서는 USERACAUDIT 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
USERID	예	NVARCHAR2(256)	NOT NULL	이 레코드의 사용자 ID(이름)
USERTYPE	예	NVARCHAR2(80)	NOT NULL	이 사용자의 클래스: USER, XUSER
SUCCESS	아니요	NUMBER(1,0)	NULL	CA Access Control 은 성공적인 액세스를 로깅합니다.
FAILURE	아니요	NUMBER(1,0)	NULL	실패한 액세스 시도를 로깅합니다.
LOGONSUCCESS	아니요	NUMBER(1,0)	NULL	CA Access Control 은 성공적인 로그인을 로깅합니다.
LOGONFAILURE	아니요	NUMBER(1,0)	NULL	CA Access Control 은 실패한 로그인 시도를 기록합니다.
DEBUG	아니요	NUMBER(1,0)	NULL	디버그 이벤트 감사
TRACE	아니요	NUMBER(1,0)	NULL	추적 이벤트 감사

USERACMODE 테이블 열

다음 표에서는 USERACMODE 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
USERID	예	NVARCHAR2(256)	NOT NULL	이 레코드의 사용자 ID(이름)
USERTYPE	예	NVARCHAR2(80)	NOT NULL	이 사용자의 클래스: USER, XUSER
MREGULAR	아니요	NUMBER(1,0)	NULL	
MAUDITOR	아니요	NUMBER(1,0)	NULL	
MOPERATIONS	아니요	NUMBER(1,0)	NULL	
MPWOFFICER	아니요	NUMBER(1,0)	NULL	
MENABLED	아니요	NUMBER(1,0)	NULL	
MIGNHOL	아니요	NUMBER(1,0)	NULL	
MSERVER	아니요	NUMBER(1,0)	NULL	
MADMIN	아니요	NUMBER(1,0)	NULL	

USERGRP 테이블 열

다음 표에서는 USERGRP 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템

이름	PK 여부	데이터 유형	Null 옵션	설명
				식별자입니다.
USERID	예	NVARCHAR2(256)	NOT NULL	이 레코드의 사용자 ID(이름).
USERTYPE	예	NVARCHAR2(80)	NOT NULL	이 사용자의 클래스: USER, XUSER
GROUPID	예	NVARCHAR2(256)	NOT NULL	이 레코드의 그룹 ID(이름) AC 그룹 OID 의 ONAME 에 매핑됩니다.
GROUPTYPE	예	NVARCHAR2(80)	NOT NULL	그룹 클래스: GROUP, XGROUP 등. AC 그룹 OID 의 CNAME 에 매핑됩니다.
CONNECTIONDATE	아니요	TIMESTAMP(6)	NULL	연결 날짜
OWNERCNAME	아니요	NVARCHAR2(80)	NULL	소유자 클래스 이름. GROUP 또는 XGROUP 은 GROUPINFO 테이블에 소유자 레코드가 있음을 의미합니다. USER 또는 XUSER 는 USERINFO 테이블에 소유자 레코드가 있음을 의미합니다.
OWNERONAME	아니요	NVARCHAR2(256)	NULL	
MREGULAR	아니요	NUMBER(1,0)	NULL	
MAUDITOR	아니요	NUMBER(1,0)	NULL	
MOPERATIONS	아니요	NUMBER(1,0)	NULL	
MPWOFFICER	아니요	NUMBER(1,0)	NULL	
MENABLED	아니요	NUMBER(1,0)	NULL	
MIGNHOL	아니요	NUMBER(1,0)	NULL	
MSERVER	아니요	NUMBER(1,0)	NULL	
MADMIN	아니요	NUMBER(1,0)	NULL	

USERINFO 테이블 열

다음 표에서는 USERINFO 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
USERID	예	NVARCHAR2(256)	NOT NULL	이 시스템에서 해당 개체의 식별자입니다.
USERTYPE	예	NVARCHAR2(80)	NOT NULL	이 사용자의 클래스: USER, XUSER
NAME	아니요	NVARCHAR2(256)	NULL	보안 데이터베이스에 정의된 사용자 전체 이름. 이 열은 USER/XUSER 클래스의 FULL_NAME AC 속성에 매핑됩니다.
DEFGROUP	아니요	NVARCHAR2(256)	NULL	USS 의 사용자 기본 그룹. 이 열은 CA Top Secret 의 경우 DFLTGRP 필드이고 CA ACF2 의 경우 GROUP 필드입니다.
CRETIME	아니요	TIMESTAMP(6)	NULL	보안 데이터베이스에서 사용자가 생성된 시간입니다. 이 열은 USER/XUSER 클래스의 CREATE_TIME AC 속성에 매핑됩니다.
LUTIME	아니요	TIMESTAMP(6)	NULL	사용자가 시스템에 들어온 마지막 시간입니다. 이 열은 USER/XUSER 클래스의 LAST_ACC_TIME AC 속성에 매핑됩니다.
ACTDATE	아니요	DATE	NULL	CA ACF2 전용. 사용자 계정이 활성화된 날짜입니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
EXPDATE	아니요	DATE	NULL	사용자 계정이 만료되는 날짜입니다. 이 열은 USER/XUSER 클래스의 EXPIRE_DATE AC 속성에 매핑됩니다.
TIMEZONE	아니요	CHAR(3)	NULL	CPU 시간대와 관련된 ACID 의 실제 시간대입니다. 시간대 값은 -12 에서 +12 사이입니다.
APPIND	아니요	CHAR(1)	NULL	응용 프로그램 표시기. 이 레코드가 속한 응용 프로그램을 나타냅니다. TSS/ACF2 DB 스키마의 문자 ID 와 같습니다. 항상 'A'여야 합니다.
CONSOLE	아니요	CHAR(1)	NULL	CA ACF2: TSO 콘솔 기능에 액세스할 수 있습니다. CA Top Secret: TSS MODIFY 명령을 실행할 수 있습니다.
SUSPEND	아니요	CHAR(1)	NULL	사용자가 시스템에 액세스할 수 없게 합니다.
TRACE	아니요	CHAR(1)	NULL	모든 사용자 활동(시스템 출입, 리소스 액세스, 위반 등)을 기록하기 위해 활성화된 진단 추적입니다.
LDS	아니요	CHAR(1)	NULL	LDAP 동기화에 대해 활성화된 사용자입니다.
EIMRECID	아니요	CHAR(8)	NULL	레코드 식별자
LDSRECID	아니요	CHAR(8)	NULL	레코드 식별자
PROXYRECID	아니요	CHAR(8)	NULL	레코드 식별자
SRCRECID	아니요	CHAR(8)	NULL	사용자의 SOURCE 레코드 이름을 지정하는 데 사용됩니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAME	아니요	NVARCHAR2(64)	NULL	Lotus Notes z/OS UNIX 에서 CA Top Secret 또는 CA ACF2 사용자 ID 로 사용자 ID 를 매핑하는 데 사용됩니다.
UNAME	아니요	NVARCHAR2(246)	NULL	Novell Directory Services 에서 CA Top Secret 또는 CA ACF2 사용자 ID 로 사용자 ID 를 매핑하는 데 사용됩니다.
SECURITYID	아니요	NVARCHAR2(256)	NULL	이 사용자 항목의 공급업체 특정 보안 ID 입니다. 이 열은 XUSER 클래스의 SECURITY_ID AC 속성에 매핑됩니다.

USERLIST 테이블 열

다음 표에서는 USERLIST 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID.
GROUPID	예	NVARCHAR2(256)	NOT NULL	이 레코드의 그룹 ID(이름)
GROUPTYPE	예	NVARCHAR2(80)	NOT NULL	그룹 클래스: GROUP, XGROUP 등. AC 그룹 OID 의 CNAME 에 매핑됩니다.
USERTYPE	예	NVARCHAR2(80)	NOT NULL	사용자의 클래스 이름
USERID	예	NVARCHAR2(256)	NOT NULL	사용자의 개체 이름

USERREVACL 테이블 열

다음 표에서는 USERREVACL 테이블 열의 특성을 설명합니다.

이름	PK 여부	데이터 유형	Null 옵션	설명
SNAPSHOTID	예	NUMBER(20,0)	NOT NULL	이 레코드의 스냅숏 ID
HOSTID	예	NVARCHAR2(512)	NOT NULL	이 레코드의 호스트 ID. 레코드가 존재하는 시스템의 시스템 식별자입니다.
USERID	예	NVARCHAR2(256)	NOT NULL	이 시스템에서 해당 개체의 식별자입니다. USER/XUSER 개체의 AC OID 에 매핑됩니다.
USERTYPE	예	NVARCHAR2(80)	NOT NULL	이 사용자의 클래스: USER, XUSER
RESCNAME	예	NVARCHAR2(80)	NOT NULL	리소스 클래스 이름
RESONAME	예	NVARCHAR2(256)	NOT NULL	리소스 개체 이름
CONCNAME	예	NVARCHAR2(80)	NOT NULL	조건 클래스 이름(즉, PROGRAM, HOST, CALENDAR). 비어 있지 않은 문자열은 RESINFO 테이블에 조건 개체가 있음을 의미합니다. 빈 문자열은 조건 없음을 의미합니다.
CONONAME	예	NVARCHAR2(256)	NOT NULL	조건 개체 이름
AREAD	아니요	NUMBER(1,0)	NULL	
AWRITE	아니요	NUMBER(1,0)	NULL	
AMODIFY	아니요	NUMBER(1,0)	NULL	
ACREATE	아니요	NUMBER(1,0)	NULL	
AERASE	아니요	NUMBER(1,0)	NULL	
AFILESCAN	아니요	NUMBER(1,0)	NULL	
ALANGINT	아니요	NUMBER(1,0)	NULL	
AEXEC	아니요	NUMBER(1,0)	NULL	
ACHOWN	아니요	NUMBER(1,0)	NULL	

이름	PK 여부	데이터 유형	Null 옵션	설명
ACHGRP	아니요	NUMBER(1,0)	NULL	
ACHMOD	아니요	NUMBER(1,0)	NULL	
AUTIMES	아니요	NUMBER(1,0)	NULL	
ASEC	아니요	NUMBER(1,0)	NULL	
AKILL	아니요	NUMBER(1,0)	NULL	
ACONNECT	아니요	NUMBER(1,0)	NULL	
ARENAME	아니요	NUMBER(1,0)	NULL	
APASSWORD	아니요	NUMBER(1,0)	NULL	
AAUTHORIZED	아니요	NUMBER(1,0)	NULL	
AXAUDIT	아니요	NUMBER(1,0)	NULL	
ACHDIR	아니요	NUMBER(1,0)	NULL	
ACRSUBK	아니요	NUMBER(1,0)	NULL	
ANOTIFY	아니요	NUMBER(1,0)	NULL	
AENUM	아니요	NUMBER(1,0)	NULL	
AQUERY	아니요	NUMBER(1,0)	NULL	
ARCTRL	아니요	NUMBER(1,0)	NULL	
ACRLINK	아니요	NUMBER(1,0)	NULL	
APRINT	아니요	NUMBER(1,0)	NULL	
AMANAGE	아니요	NUMBER(1,0)	NULL	
AMAXALLOWED	아니요	NUMBER(1,0)	NULL	
ASTOP	아니요	NUMBER(1,0)	NULL	
APAUSE	아니요	NUMBER(1,0)	NULL	
ACONTROL	아니요	NUMBER(1,0)	NULL	
ACHOG	아니요	NUMBER(1,0)	NULL	
ARESUME	아니요	NUMBER(1,0)	NULL	
DREAD	아니요	NUMBER(1,0)	NULL	
DWRITE	아니요	NUMBER(1,0)	NULL	
DMODIFY	아니요	NUMBER(1,0)	NULL	
DCREATE	아니요	NUMBER(1,0)	NULL	

이름	PK 여부	데이터 유형	Null 옵션	설명
DERASE	아니요	NUMBER(1,0)	NULL	
DFILESCAN	아니요	NUMBER(1,0)	NULL	
DLANGINT	아니요	NUMBER(1,0)	NULL	
DEXEC	아니요	NUMBER(1,0)	NULL	
DCHOWN	아니요	NUMBER(1,0)	NULL	
DCHGRP	아니요	NUMBER(1,0)	NULL	
DCHMOD	아니요	NUMBER(1,0)	NULL	
DUTIMES	아니요	NUMBER(1,0)	NULL	
DSEC	아니요	NUMBER(1,0)	NULL	
DKILL	아니요	NUMBER(1,0)	NULL	
DCONNECT	아니요	NUMBER(1,0)	NULL	
DRENAME	아니요	NUMBER(1,0)	NULL	
DPASSWORD	아니요	NUMBER(1,0)	NULL	
DAUTHORIZED	아니요	NUMBER(1,0)	NULL	
DXAUDIT	아니요	NUMBER(1,0)	NULL	
DCHDIR	아니요	NUMBER(1,0)	NULL	
DCRSUBK	아니요	NUMBER(1,0)	NULL	
DNOTIFY	아니요	NUMBER(1,0)	NULL	
DENUM	아니요	NUMBER(1,0)	NULL	
DQUERY	아니요	NUMBER(1,0)	NULL	
DRCTRL	아니요	NUMBER(1,0)	NULL	
DCRLINK	아니요	NUMBER(1,0)	NULL	
DPRINT	아니요	NUMBER(1,0)	NULL	
DMANAGE	아니요	NUMBER(1,0)	NULL	
DMAXALLOWED	아니요	NUMBER(1,0)	NULL	
DSTOP	아니요	NUMBER(1,0)	NULL	
DPAUSE	아니요	NUMBER(1,0)	NULL	
DCONTROL	아니요	NUMBER(1,0)	NULL	
DCHOG	아니요	NUMBER(1,0)	NULL	

이름	PK 여부	데이터 유형	Null 옵션	설명
DRESUME	아니요	NUMBER(1,0)	NULL	

관계

FK 이름	설명
CONFIG_ENTRY_CON	항목 포함
DEPTASK_RESULTMSG_CON	메시지 포함
USERGRP_GROUP_CON	사용자 그룹
USERLIST_FK	사용자 포함
PASSWDRULES_FK	암호 규칙 포함
MEMBEROF_FK	그룹 포함
GROUPMEMBER_FK	구성원(그룹 유형) 포함
GROUPREVACL_FK	ACL 이 적용됨
GROUPAUDIT_FK	감사 포함
SNAPSHOTINFO_FK	스냅숏 포함
NODE_ALIAS_FK	
NODE_SUBSCRIPTION_PUBLISHER	
NODE_EFFECTIVE_POLICY_CON	정책이 적용됨
NODE_SUBSCRIPTION_SUBSCRIBER	
NODE_POLICY_STATUS_CON	정책 상태 포함
NODE_DEPTASKGRP_CON	작업 그룹 운영자
NODE_ADDRESS_FK	
NODE_NODE_DEVIATION_CON	위반 포함
NODE_DEPTASK_CON	작업에 의해 처리됨
POLICY_POLICY_STATUS_CON	노드의 상태 포함
LATESTFIN_POLICYGRP_CON	최근 완료된 정책 그룹
POLICY_EFFECTIVE_POLICY_CON	노드에 적용
POLICY_POLICY_DEVIATION_CON	
POLICY_RULEST_POLICY_CON	규칙 집합 포함

FK 이름	설명
LATEST_POLICYGRP_CON	그룹의 최신 정책
POLICY_DEPTASK_CON	작업에 의해 배포됨
POLICYGRP_DEPTASK_CON	작업에 의해 배포됨
POLICYGRP_DEPTASKGRP_CON	작업 그룹 운영자
POLICY_GROUP_DEP_ON_CON	정책 그룹에 따라 달라짐
POLICY_GROUP_DEP_CON	종속 정책 그룹 포함
PMDSUBC_CON	
POLICYGRP_NODASS_POL_CON	노드 할당 포함
POLICY_GROUP_CON	슈퍼클래스
POLICY_CON	슈퍼클래스
RULESET_CON	슈퍼클래스
POLICYGRP_NODASS_NOD_CON	정책 그룹에 할당된 리소스(NODE/GNODE)
NODE_CON	슈퍼클래스
HOLDATE_CON	슈퍼클래스
RESINFO_GRPREVACL_COND_CON	조건에 참여
RESINFO_HOST_CON	CACL 호스트
USER_RESOURCE_ACL_CON	사용자의 ACL 포함
UACC_CON	기본 액세스 포함
SPECIALPGMTYPE_CON	슈퍼클래스
GROUP_RESOURCE_ACL_CON	그룹에서 ACL 포함
GROUPS_GROUP_CON	컨테이너 구성원
RESAC_CON	CA Access Control 속성으로 확장됨
RAUDIT_CON	슈퍼클래스
MEMBERS_PARENT_CON	구성원 포함
INSERVRNGE_CON	슈퍼클래스
INETACL_CON	슈퍼클래스
MEMBERS_CHILD_CON	구성원 컨테이너
RESINFO_DEPTASKGRP_CON	슈퍼클래스
RESINFO_DEPTASK_CON	슈퍼클래스

FK 이름	설명
RESINFO_USERREVACL_COND_CON	조건에 참여(제약 조건 없음)
RESINFO_HOST_CON	CACL 호스트
GROUPS_MEMBER_CON	컨테이너 포함
LOGINAPPL_CON	
INSERVRNGE_CON	슈퍼클래스
NODEGRP_DEPTASK_CON	작업의 그룹 대상(노드 그룹)
ACL_CON	ACL 로 보호됨
USER_RESOURCE_ACL_CON	사용자의 ACL 포함
RULESET_RULESET_POLICY_CON	정책에 포함
RULESET_COMMAND_CON	명령 포함
SEOS_DH_FK	
SNAPSHOTINFO_CON	사용자 포함
SNAPSHOT_CONFIG_CON	구성 포함
SEOS_CON	옵션 포함
RESINFO_CON	리소스 포함
POLICYMODEL_CON	
CATEGORY_CON	범주 포함
DAYTIME_CON	주간 설정 포함
GROUPINFO_CON	그룹 포함
USERACMODE_FK	CA Access Control 모드 포함
USERACAUDIT_FK	CA Access Control 감사 포함
USERGRP_FK	그룹에 속함
USERREVACL_FK	ACL 이 적용됨
USERINFO_SUSPEND_USERAC_CON	사용자에 의한 일시 중단
USER_DEPTASK_CHECKER_CON	이 작업의 Checker
USER_DEPTASK_MAKER_CON	작업 Maker
USERAC_CON	CA Access Control 속성으로 확장됨

CONFIG_ENTRY_CON 관계의 부모 테이블

CONFIG 는 CONFIG_ENTRY_CON 의 부모 테이블입니다.

CONFIG_ENTRY_CON 관계의 자식 테이블

CONFIG_ENTRY 는 CONFIG_ENTRY_CON 의 자식 테이블입니다.

CONFIG_ENTRY_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
CONFIGNAME	CONFIGNAME

DEPTASK_RESULTMSG_CON 관계의 부모 테이블

DEPLOYMENT_TASK 는 DEPTASK_RESULTMSG_CON 의 부모 테이블입니다.

DEPTASK_RESULTMSG_CON 관계의 자식 테이블

DEPLOYMENT_RESULT_MESSAGE 는 DEPTASK_RESULT_MSG_CON 의 자식 테이블입니다.

DEPTASK_RESULTMSG_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

GROUPMEMBER_FK 관계의 부모 테이블

GROUPINFO 는 GROUPMEMBER_FK 의 부모 테이블입니다.

GROUPMEMBER_FK 관계의 자식 테이블

GROUPMEMBER 는 GROUPMEMBER_FK 의 자식 테이블입니다.

GROUPMEMBER_FK 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

GROUPREVACL_FK 관계의 부모 테이블

GROUPINFO 는 GROUPREVACL_FK 의 부모 테이블입니다.

GROUPREVACL_FK 관계의 자식 테이블

GROUPREVACL 은 GROUPREVACL_FK 의 자식 테이블입니다.

GROUPREVACL_FK 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

USERGRP_GROUP_CON 관계의 부모 테이블

GROUPINFO 는 USERGRP_GROUP_CON 의 부모 테이블입니다.

USERGRP_GROUP_CON 관계의 자식 테이블

USERGRP 는 USERGRP_GROUP_CON 의 자식 테이블입니다.

USERGRP_GROUP_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

MEMBEROF_FK 관계의 부모 테이블

GROUPINFO 는 MEMBEROF_FK 의 부모 테이블입니다.

MEMBEROF_FK 관계의 자식 테이블

MEMBEROF 는 MEMBEROF_FK 의 자식 테이블입니다.

MEMBEROF_FK 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

PASSWDRULES_FK 관계의 부모 테이블

GROUPINFO 는 PASSWDRULES_FK 의 부모 테이블입니다.

PASSWDRULES_FK 관계의 자식 테이블

PASSWDRULES 는 PASSWDRULES_FK 의 자식 테이블입니다.

PASSWDRULES_FK 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

USERLIST_FK 관계의 부모 테이블

GROUPINFO 는 USERLIST_FK 의 부모 테이블입니다.

USERLIST_FK 관계의 자식 테이블

USERLIST 는 USERLIST_FK 의 자식 테이블입니다.

USERLIST_FK 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

GROUPAUDIT_FK 관계의 부모 테이블

GROUPINFO 는 GROUPAUDIT_FK 의 부모 테이블입니다.

GROUPAUDIT_FK 관계의 자식 테이블

GROUPAUDIT 는 GROUPAUDIT_FK 의 자식 테이블입니다.

GROUPAUDIT_FK 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

SNAPSHOTINFO_FK 관계의 부모 테이블

HOSTINFO 는 SNAPSHOTINFO_FK 의 부모 테이블입니다.

SNAPSHOTINFO_FK 관계의 자식 테이블

SNAPSHOTINFO 는 SNAPSHOTINFO_FK 의 자식 테이블입니다.

SNAPSHOTINFO_FK 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
HOSTID	HOSTID

NODE_ALIAS_FK 관계의 부모 테이블

NODE 는 NODE_ALIAS_FK 의 부모 테이블입니다.

NODE_ALIAS_FK 관계의 자식 테이블

NODE_ALIAS 는 NODE_NODE_ALIAS_FK 의 자식 테이블입니다.

NODE_ALIAS_FK 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

NODE_SUBSCRIPTION_PUBLISHER 관계의 부모 테이블

NODE 는 NODE_SUBSCRIPTION_PUBLISHER 의 부모 테이블입니다.

NODE_SUBSCRIPTION_PUBLISHER 관계의 자식 테이블

NODE_SUBSCRIPTION_STATUS 는
NODE_SUBSCRIPTION_PUBLISHER 의 자식 테이블입니다.

NODE_SUBSCRIPTION_PUBLISHER 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	PUBLISHERCNAME
RULEKEY	PUBLISHERONAME

NODE_EFFECTIVE_POLICY_CON 관계의 부모 테이블

NODE 는 NODE_EFFECTIVE_POLICY_CON 의 부모 테이블입니다.

NODE_EFFECTIVE_POLICY_CON 관계의 자식 테이블

EFFECTIVE_POLICY 는 NODE_EFFECTIVE_POLICY_CON 의 자식 테이블입니다.

NODE_EFFECTIVE_POLICY_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

NODE_SUBSCRIPTION_SUBSCRIBER 관계의 부모 테이블

NODE 는 NODE_SUBSCRIPTION_SUBSCRIBER 의 부모 테이블입니다.

NODE_SUBSCRIPTION_SUBSCRIBER 관계의 자식 테이블

NODE_SUBSCRIPTION_STATUS 는 NODE_SUBSCRIPTION_SUBSCRIBER 의 자식 테이블입니다.

NODE_SUBSCRIPTION_SUBSCRIBER 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	SUBSCRIBERCNAME
RULEKEY	SUBSCRIBERONAME

NODE_POLICY_STATUS_CON 관계의 부모 테이블

NODE 는 NODE_POLICY_STATUS_CON 의 부모 테이블입니다.

NODE_POLICY_STATUS_CON 관계의 자식 테이블

POLICY_STATUS 는 NODE_POLICY_STATUS_CON 의 자식 테이블입니다.

NODE_POLICY_STATUS_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	NODE_RESCLASS
RULEKEY	NODE_RULEKEY

NODE_DEPTASKGRP_CON 관계의 부모 테이블

NODE 는 NODE_DEPTASKGRP_CON 의 부모 테이블입니다.

NODE_DEPTASKGRP_CON 관계의 자식 테이블

DEPLOYMENT_TASK_GROUP 은 NODE_DEPTASKGRP_CON 의 자식 테이블입니다.

NODE_DEPTASKGRP_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	NODE_RESCLASS
RULEKEY	NODE_RULEKEY

NODE_ADDRESS_FK 관계의 부모 테이블

NODE 는 NODE_ADDRESS_FK 의 부모 테이블입니다.

NODE_ADDRESS_FK 관계의 자식 테이블

NODE_ADDRESS 는 NODE_ADDDRESS_FK 의 자식 테이블입니다.

NODE_ADDRESS_FK 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

NODE_NODE_DEVIATION_CON 관계의 부모 테이블

NODE 는 NODE_NODE_DEVIATION_CON 의 부모 테이블입니다.

NODE_NODE_DEVIATION_CON 관계의 자식 테이블

NODE_DEVIATION 은 NODE_NODE_DEVIATION_CON 의 자식 테이블입니다.

NODE_NODE_DEVIATION_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	NODE_RESCLASS
RULEKEY	NODE_RULEKEY

NODE_DEPTASK_CON 관계의 부모 테이블

NODE 는 NODE_DEPTASK_CON 의 부모 테이블입니다.

NODE_DEPTASK_CON 관계의 자식 테이블

DEPLOYMENT_TASK 는 NODE_DEPTASK_CON 의 자식 테이블입니다.

NODE_DEPTASK_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	NODE_RESCLASS
RULEKEY	NODE_RULEKEY

POLICY_POLICY_STATUS_CON 관계의 부모 테이블

POLICY 는 POLICY_POLICY_STATUS_CON 의 부모 테이블입니다.

POLICY_POLICY_STATUS_CON 관계의 자식 테이블

POLICY_STATUS 는 POLICY_POLICY_STATUS_CON 의 자식 테이블입니다.

POLICY_POLICY_STATUS_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICY_RESCLASS
RULEKEY	POLICY_RULEKEY

LATESTFIN_POLICYGRP_CON 관계의 부모 테이블

POLICY 는 LATESTFIN_POLICYGRP_CON 의 부모 테이블입니다.

LATESTFIN_POLICYGRP_CON 관계의 자식 테이블

POLICY_GROUP 은 LATESTFIN_POLICYGRP_CON 의 자식 테이블입니다.

LATESTFIN_POLICYGRP_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	LATEST_FIN_RESCLASS
RULEKEY	LATEST_FIN_RULEKEY

POLICY_EFFECTIVE_POLICY_CON 관계의 부모 테이블

POLICY 는 POLICY_EFFECTIVE_POLICY_CON 의 부모 테이블입니다.

POLICY_EFFECTIVE_POLICY_CON 관계의 자식 테이블

POLICY_EFFECTIVE 는 POLICY_EFFECTIVE_POLICY_CON 의 자식 테이블입니다.

POLICY_EFFECTIVE_POLICY_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICY_RESCLASS
RULEKEY	POLICY_RULEKEY

POLICY_POLICY_DEVIATION_CON 관계의 부모 테이블

POLICY 는 POLICY_POLICY_DEVIATION_CON 의 부모 테이블입니다.

POLICY_POLICY_DEVIATION_CON 관계의 자식 테이블

POLICY_DEVIATION 은 POLICY_POLICY_DEVIATION_CON 의 자식 테이블입니다.

POLICY_POLICY_DEVIATION_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICY_RESCLASS
RULEKEY	POLICY_RULEKEY

POLICY_RULESET_POLICY_CON 관계의 부모 테이블

POLICY 는 POLICY_RULESET_POLICY_CON 의 부모 테이블입니다.

POLICY_RULESET_POLICY_CON 관계의 자식 테이블

POLICY_RULESET 는 POLICY_RULESET_POLICY_CON 의 자식 테이블입니다.

POLICY_RULESET_POLICY_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICY_RESCLASS
RULEKEY	POLICY_RULEKEY

LATEST_POLICYGRP_CON 관계의 부모 테이블

POLICY 는 LATEST_POLICYGRP_CON 의 부모 테이블입니다.

LATEST_POLICYGRP_CON 관계의 자식 테이블

POLICY_GROUP 은 LATEST_POLICYGRP_CON 의 자식 테이블입니다.

LATEST_POLICYGRP_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	LATEST_RESCLASS
RULEKEY	LATEST_RULEKEY

POLICY_DEPTASK_CON 관계의 부모 테이블

POLICY 는 POLICY_DEPTASK_CON 의 부모 테이블입니다.

POLICY_DEPTASK_CON 관계의 자식 테이블

DEPLOYMENT_TASK 는 POLICY_DEPTASK_CON 의 자식 테이블입니다.

POLICY_DEPTASK_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICY_RESCLASS
RULEKEY	POLICY_RULEKEY

POLICYGRP_DEPTASK_CON 관계의 부모 테이블

POLICY_GROUP 은 POLICYGRP_DEPTASK_CON 의 부모 테이블입니다.

POLICYGRP_DEPTASK_CON 관계의 자식 테이블

DEPLOYMENT_TASK 는 POLICYGRP_DEPTASK_CON 의 자식 테이블입니다.

POLICYGRP_DEPTASK_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICYGRP_RESCLASS
RULEKEY	POLICYGRP_RULEKEY

POLICYGRP_DEPTASKGRP_CON 관계의 부모 테이블

POLICY_GROUP 은 POLICYGRP_DEPTASKGRP_CON 의 부모 테이블입니다.

POLICYGRP_DEPTASKGRP_CON 관계의 자식 테이블

DEPLOYMENT_TASK_GROUP 은 POLICYGRP_DEPTASKGRP_CON 의 자식 테이블입니다.

POLICYGRP_DEPTASKGRP_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICYGRP_RESCLASS
RULEKEY	POLICYGRP_RULEKEY

POLICY_GROUP_DEP_ON_CON 관계의 부모 테이블

POLICY_GROUP 은 POLICY_GROUP_DEP_ON_CON 의 부모 테이블입니다.

POLICY_GROUP_DEP_ON_CON 관계의 자식 테이블

POLICY_GROUP_DEPENDENCY 는 POLICY_GROUP_DEP_ON_CON 의 자식 테이블입니다.

POLICY_GROUP_DEP_ON_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	DEP_ON_RESCLASS
RULEKEY	DEP_ON_RULEKEY

POLICY_GROUP_DEP_CON 관계의 부모 테이블

POLICY_GROUP 은 POLICY_GROUP_DEP_CON 의 부모 테이블입니다.

POLICY_GROUP_DEP_CON 관계의 자식 테이블

POLICY_GROUP_DEPENDENCY 는 POLICY_GROUP_DEP_CON 의 자식 테이블입니다.

POLICY_GROUP_DEP_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

PMD_SUBSC_CON 관계의 부모 테이블

POLICYMODELINFO 는 PMD_SUBSC_CON 의 부모 테이블입니다.

PMD_SUBSC_CON 관계의 자식 테이블

LOCAL_PMD_SUBSCRIBER 는 PMD_SUBSC_CON 의 자식 테이블입니다.

PMD_SUBSC_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

POLICYGRP_NODASS_POL_CON 관계의 부모 테이블

RESINFO 는 POLICYGRP_NODASS_POL_CON 의 부모 테이블입니다.

POLICYGRP_NODASS_POL_CON 관계의 자식 테이블

POLICY_GROUP_NODE_ASSIGNMENT 는
POLICYGRP_NODASS_POL_CON 의 자식 테이블입니다.

POLICYGRP_NODASS_POL_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	NODE_RESCLASS
RULEKEY	NODE_RULEKEY

POLICY_GROUP_CON 관계의 부모 테이블

RESINFO 는 POLICY_GROUP_CON 의 부모 테이블입니다.

POLICY_GROUP_CON 관계의 자식 테이블

POLICY_GROUP 은 POLICY_GROUP_CON 의 자식 테이블입니다.

POLICY_GROUP_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

POLICY_CON 관계의 부모 테이블

RESINFO 는 POLICY_CON 의 부모 테이블입니다.

POLICY_CON 관계의 자식 테이블

POLICY 는 POLICY_CON 의 자식 테이블입니다.

POLICY_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

RULESET_CON 관계의 부모 테이블

RESINFO 는 RULESET_CON 의 부모 테이블입니다.

RULESET_CON 관계의 자식 테이블

RULESET 는 RULESET_CON 의 자식 테이블입니다.

RULESET_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

POLICYGRP_NODASS_NOD_CON 관계의 부모 테이블

RESINFO 는 POLICYGRP_NODASS_NOD_CON 의 부모 테이블입니다.

POLICYGRP_NODASS_NOD_CON 관계의 자식 테이블

POLICY_GROUP_NODE_ASSIGNMENT 는
POLICYGRP_NODASS_NOD_CON 의 자식 테이블입니다.

POLICYGRP_NODASS_NOD_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICYGRP_RESCLASS
RULEKEY	POLICYGRP_RULEKEY

NODE_CON 관계의 부모 테이블

RESINFO 는 NODE_CON 의 부모 테이블입니다.

NODE_CON 관계의 자식 테이블

NODE 는 NODE_CON 의 자식 테이블입니다.

NODE_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

GROUP_RESOURCE_ACL_CON 관계의 부모 테이블

RESINFO 는 GROUP_RESOURCE_ACL_CON 의 부모 테이블입니다.

GROUP_RESOURCE_ACL_CON 관계의 자식 테이블

GROUPREVACL 은 GROUP_RESOURCE_ACL_CON 의 자식 테이블입니다.

GROUP_RESOURCE_ACL_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
RESCLASS	RESCNAME
RULEKEY	RESONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

RESINFO_USERREVACL_COND_CON 관계의 부모 테이블

RESINFO 는 RESINFO_USERREVACL_COND_CON 의 부모 테이블입니다.

RESINFO_USERREVACL_COND_CON 관계의 자식 테이블

USERREVACL 은 RESINFO_USERREVACL_COND_CON 의 자식 테이블입니다.

RESINFO_USERREVACL_COND_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
RESCLASS	CONCNAME
RULEKEY	CONONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

UACC_CON 관계의 부모 테이블

RESINFO 는 UACC_CON 의 부모 테이블입니다.

UACC_CON 관계의 자식 테이블

UACC 는 UACC_CON 의 자식 테이블입니다.

UACC_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

SPECIALPGMTYPE_CON 관계의 부모 테이블

RESINFO 는 SPECIALPGMTYPE_CON 의 부모 테이블입니다.

SPECIALPGMTYPE_CON 관계의 자식 테이블

SPECIALPGMTYPE 은 SPECIALPGMTYPE_CON 의 자식 테이블입니다.

SPECIALPGMTYPE_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

RESAC_CON 관계의 부모 테이블

RESINFO 는 RESAC_CON 의 부모 테이블입니다.

RESAC_CON 관계의 자식 테이블

RESAC 는 RESAC_CON 의 자식 테이블입니다.

RESAC_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

RAUDIT_CON 관계의 부모 테이블

RESINFO 는 RAUDIT_CON 의 부모 테이블입니다.

RAUDIT_CON 관계의 자식 테이블

RAUDIT 는 RAUDIT_CON 의 자식 테이블입니다.

RAUDIT_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

MEMBERS_PARENT_CON 관계의 부모 테이블

RESINFO 는 MEMBERS_PARENT_CON 의 부모 테이블입니다.

MEMBERS_PARENT_CON 관계의 자식 테이블

MEMBERS 는 MEMBERS_PARENT_CON 의 자식 테이블입니다.

MEMBERS_PARENT_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

RESINFO_DEPTASKGRP_CON 관계의 부모 테이블

RESINFO 는 RESINFO_DEPTASKGRP_CON 의 부모 테이블입니다.

RESINFO_DEPTASKGRP_CON 관계의 자식 테이블

DEPLOYMENT_TASK_GROUP 은 RESINFO_DEPTASKGRP_CON 의 자식 테이블입니다.

RESINFO_DEPTASKGRP_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

RESINFO_DEPTASK_CON 관계의 부모 테이블

RESINFO 는 RESINFO_DEPTASK_CON 의 부모 테이블입니다.

RESINFO_DEPTASK_CON 관계의 자식 테이블

DEPLOYMENT_TASK 는 RESINFO_DEPTASK_CON 의 자식 테이블입니다.

LOGINAPPL_CON 관계의 부모 테이블

RESINFO 는 LOGINAPPL_CON 의 부모 테이블입니다.

LOGINAPPL_CON 관계의 자식 테이블

LOGINAPPL 은 LOGINAPPL_CON 의 자식 테이블입니다.

LOGINAPPL_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

INSERVRNGE_CON 관계의 부모 테이블

RESINFO 는 INSERVRNGE_CON 의 부모 테이블입니다.

INSERVRNGE_CON 관계의 자식 테이블

INSERVRNGE 은 INSERVRNGE_CON 의 자식 테이블입니다.

INSERVRNGE_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

NODEGRP_DEPTASKGRP_CON 관계의 부모 테이블

RESINFO 는 NODEGRP_DEPTASKGRP_CON 의 부모 테이블입니다.

NODEGRP_DEPTASKGRP_CON 관계의 자식 테이블

DEPLOYMENT_TASK_GROUP 은 NODEGRP_DEPTASKGRP_CON 의 자식 테이블입니다.

NODEGRP_DEPTASKGRP_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	NODEGRP_RESCLASS
RULEKEY	NODEGRP_RULEKEY

RESINFO_GRPREVACL_COND_CON 관계의 부모 테이블

RESINFO 는 RESINFO_GRPREVACL_COND_CON 의 부모 테이블입니다.

RESINFO_GRPREVACL_COND_CON 관계의 자식 테이블

GROUPREVACL 은 RESINFO_GRPREVACL_COND_CON 의 자식 테이블입니다.

RESINFO_GRPREVACL_COND_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
RESCLASS	CONCNAME
RULEKEY	CONONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

RESINFO_HOST_CON 관계의 부모 테이블

RESINFO 는 RESINFO_HOST_CON 의 부모 테이블입니다.

RESINFO_HOST_CON 관계의 자식 테이블

ACL 은 RESINFO_HOST_CON 의 자식 테이블입니다.

RESINFO_HOST_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
RESCLASS	HOSTCNAME
RULEKEY	HOSTONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

GROUPS_GROUP_CON 관계의 부모 테이블

RESINFO 는 GROUPS_GROUP_CON 의 부모 테이블입니다.

GROUPS_GROUP_CON 관계의 자식 테이블

GROUPS 는 GROUPS_GROUP_CON 의 자식 테이블입니다.

GROUPS_GROUP_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
RESCLASS	CNAME
RULEKEY	ONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

INETACL_CON 관계의 부모 테이블

RESINFO 는 INETACL_CON 의 부모 테이블입니다.

INETACL_CON 관계의 자식 테이블

INETACL 은 INETACL_CON 의 자식 테이블입니다.

INETACL_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

HOLDATE_CON 관계의 부모 테이블

RESINFO 는 HOLDATE_CON 의 부모 테이블입니다.

HOLDATE_CON 관계의 자식 테이블

HOLDATE 은 HOLDATE_CON 의 자식 테이블입니다.

HOLDATE_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

GROUPS_MEMBER_CON 관계의 부모 테이블

RESINFO 는 GROUPS_MEMBER_CON 의 부모 테이블입니다.

GROUPS_MEMBER_CON 관계의 자식 테이블

GROUPS 는 GROUPS_MEMBER_CON 의 자식 테이블입니다.

GROUPS_MEMBER_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

ACL_CON 관계의 부모 테이블

RESINFO 는 ACL_CON 의 부모 테이블입니다.

ACL_CON 관계의 자식 테이블

ACL 은 ACL_CON 의 자식 테이블입니다.

ACL_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

MEMBERS_CHILD_CON 관계의 부모 테이블

RESINFO 는 MEMBERS_CHILD_CON 의 부모 테이블입니다.

MEMBERS_CHILD_CON 관계의 자식 테이블

MEMBERS 는 MEMBERS_CHILD_CON 의 자식 테이블입니다.

MEMBERS_CHILD_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
RESCLASS	CNAME
RULEKEY	ONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

USER_RESOURCE_ACL_CON 관계의 부모 테이블

RESINFO 는 USER_RESOURCE_ACL_CON 의 부모 테이블입니다.

USER_RESOURCE_ACL_CON 관계의 자식 테이블

USERREVACL 은 USER_RESOURCE_ACL_CON 의 자식 테이블입니다.

USER_RESOURCE_ACL_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
RESCLASS	RESCNAME
RULEKEY	RESONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

RULESET_RULESET_POLICY_CON 관계의 부모 테이블

RULESET 는 RULESET_RULESET_POLICY_CON 의 부모 테이블입니다.

RULESET_RULESET_POLICY_CON 관계의 자식 테이블

POLICY_RULESET 는 RULESET_RULESET_POLICY_CON 의 자식 테이블입니다.

RULESET_RULESET_POLICY_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RULESET_RESCLASS
RULEKEY	RULESET_RULEKEY

RULESET_COMMAND_CON 관계의 부모 테이블

RULESET 는 RULESET_COMMAND_CON 의 부모 테이블입니다.

RULESET_COMMAND_CON 관계의 자식 테이블

RULESET_COMMAND 는 RULESET_COMMAND_CON 의 자식 테이블입니다.

RULESET_COMMAND_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RULESET_RESCLASS
RULEKEY	RULESET_RULEKEY

SEOS_DH_FK 관계의 부모 테이블

SEOS 는 SEOS_DH_FK 의 부모 테이블입니다.

SEOS_DH_FK 관계의 자식 테이블

DISTRIBUTION_HOST 는 SEOS_DH_FK 의 자식 테이블입니다.

SEOS_DH_FK 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

DAYTIME_CON 관계의 부모 테이블

SNAPSHOTINFO 는 DAYTIME_CON 의 부모 테이블입니다.

DAYTIME_CON 관계의 자식 테이블

DAYTIME 은 CATEGORY_CON 의 자식 테이블입니다.

DAYTIME_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

SEOS_CON 관계의 부모 테이블

SNAPSHOTINFO 는 SEOS_CON 의 부모 테이블입니다.

SEOS_CON 관계의 자식 테이블

SEOS 는 SEOS_CON 의 자식 테이블입니다.

SEOS_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

SEOSSYSCALL_CON 관계의 부모 테이블

SNAPSHOTINFO 는 SEOSSYSCALL_CON 의 부모 테이블입니다.

SEOSSYSCALL_CON 관계의 자식 테이블

SEOSSYSCALL 은 SEOSSYSCALL_CON 의 자식 테이블입니다.

SEOSSYSCALL_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

NAPSHOT_CONFIG_CON 관계의 부모 테이블

SNAPSHOTINFO 는 NAPSHOT_CONFIG_CON 의 부모 테이블입니다.

NAPSHOT_CONFIG_CON 관계의 자식 테이블

CONFIG 는 SNAPSHOT_CONFIG_CON 의 자식 테이블입니다.

SNAPSHOT_CONFIG_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

SYSCALL_CON 관계의 부모 테이블

SEOSSYSCALL 은 SYSCALL_CONFIG_CON 의 부모 테이블입니다.

SYSCALL_CON 관계의 자식 테이블

SYSCALL 은 SYSCALL_CON 의 자식 테이블입니다.

SYSCALL_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID

부모 열 이름	자식 열 이름
HOSTID	HOSTID

SYSCALLUSERSPECIALPGM 관계의 부모 테이블

SEOSSYSCALL 은 SYSCALLUSERSPECIALPGM 의 부모 테이블입니다.

SYSCALLUSERSPECIALPGM 관계의 자식 테이블

SYSCALLUSERSPECIALPGM 은 SYSCALLUSERSPECIALPGM 의 자식 테이블입니다.

SYSCALLUSERSPECIALPGM 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

CATEGORY_CON 관계의 부모 테이블

SNAPSHOTINFO 는 CATEGORY_CON 의 부모 테이블입니다.

CATEGORY_CON 관계의 자식 테이블

CATEGORY 는 CATEGORY_CON 의 자식 테이블입니다.

CATEGORY_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

GROUPINFO_CON 관계의 부모 테이블

SNAPSHOTINFO 는 GROUPINFO_CON 의 부모 테이블입니다.

GROUPINFO_CON 관계의 자식 테이블

GROUPINFO 은 CATEGORY_CON 의 자식 테이블입니다.

GROUPINFO_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

SNAPSHOTINFO_CON 관계의 부모 테이블

SNAPSHOTINFO 는 SNAPSHOTINFO_CON 의 부모 테이블입니다.

SNAPSHOTINFO_CON 관계의 자식 테이블

USERINFO 는 SNAPSHOTINFO_CON 의 자식 테이블입니다.

SNAPSHOTINFO_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

RESINFO_CON 관계의 부모 테이블

SNAPSHOTINFO 는 RESINFO_CON 의 부모 테이블입니다.

RESINFO_CON 관계의 자식 테이블

RESINFO 은 RESINFO_CON 의 자식 테이블입니다.

RESINFO_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

POLICYMODEL_CON 관계의 부모 테이블

SNAPSHOTINFO 는 POLICYMODEL_CON 의 부모 테이블입니다.

POLICYMODEL_CON 관계의 자식 테이블

POLICYMODELINFO 은 POLICYMODEL_CON 의 자식 테이블입니다.

POLICYMODEL_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

USERACAUDIT_FK 관계의 부모 테이블

USERAC 는 USERACAUDIT_FK 의 부모 테이블입니다.

USERACAUDIT_FK 관계의 자식 테이블

USERACAUDIT 는 USERACAUDIT_FK 의 자식 테이블입니다.

USERACAUDIT_FK 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID

부모 열 이름	자식 열 이름
HOSTID	HOSTID
USERID	USERID
USERTYPE	USERTYPE

USERACMODE_FK 관계의 부모 테이블

USERAC 는 USERACMODE_FK 의 부모 테이블입니다.

USERACMODE_FK 관계의 자식 테이블

USERACMODE 는 USERACMODE_FK 의 자식 테이블입니다.

USERACMODE_FK 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
USERID	USERID
USERTYPE	USERTYPE

USERGRP_FK 관계의 부모 테이블

USERAC 는 USERGRP_FK 의 부모 테이블입니다.

USERGRP_FK 관계의 자식 테이블

USERGRP 는 USERGRP_FK 의 자식 테이블입니다.

USERGRP_FK 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID

부모 열 이름	자식 열 이름
HOSTID	HOSTID
USERID	USERID
USERTYPE	USERTYPE

USERINFO_SUSPEND_USERAC_CON 관계의 부모 테이블

USERINFO 는 USERINFO_SUSPEND_USERAC_CON 의 부모 테이블입니다.

USERINFO_SUSPEND_USERAC_CON 관계의 자식 테이블

USERAC 는 USERINFO_SUSPEND_USERAC_CON 의 자식 테이블입니다.

USERINFO_SUSPEND_USERAC_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
USERTYPE	SUSPENDWHOCNAME
USERID	SUSPENDWHOONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

USER_DEPTASK_CHECKER_CON 관계의 부모 테이블

USERINFO 는 USER_DEPTASK_CHECKER_CON 의 부모 테이블입니다.

USER_DEPTASK_CHECKER_CON 관계의 자식 테이블

DEPLOYMENT_TASK 는 USER_DEPTASK_CHECKER_CON 의 자식 테이블입니다.

USER_DEPTASK_CHECKER_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID

부모 열 이름	자식 열 이름
HOSTID	HOSTID
USERID	CHECKERID
USERTYPE	CHECKERTYPE

USER_DEPTASK_MAKER_CON 관계의 부모 테이블

USERINFO 는 USER_DEPTASK_MAKER_CON 의 부모 테이블입니다.

USER_DEPTASK_MAKER_CON 관계의 자식 테이블

DEPLOYMENT_TASK 는 USER_DEPTASK_CON 의 자식 테이블입니다.

USER_DEPTASK_MAKER_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
USERID	MAKERID
USERTYPE	MAKERTYPE

USERREVACL_FK 관계의 부모 테이블

USERINFO 는 USERREVACL_FK 의 부모 테이블입니다.

USERREVACL_FK 관계의 자식 테이블

USERREVACL 은 USERREVACL_FK 의 자식 테이블입니다.

USERREVACL_FK 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID

부모 열 이름	자식 열 이름
HOSTID	HOSTID
USERID	USERID
USERTYPE	USERTYPE

USERAC_CON 관계의 부모 테이블

USERINFO 는 USERAC_CON 의 부모 테이블입니다.

USERAC_CON 관계의 자식 테이블

USERAC 는 USERAC_CON 의 자식 테이블입니다.

USERAC_CON 관계의 마이그레이션된 열

다음 표에서는 부모 테이블과 자식 테이블의 열 사이 관계를 설명합니다.

부모 열 이름	자식 열 이름
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
USERID	USERID
USERTYPE	USERTYPE