

SiteMinder

정책 서버 설치 안내서

12.52 SP1



도움말 시스템 및 전자적으로 배포된 매체를 포함하는 본 문서(이하 "문서")는 최종 사용자에게 정보를 제공하기 위한 것이며, CA는 언제든지 본 문서를 변경 또는 철회할 수 있습니다. 본 문서는 CA의 재산적 정보이며 CA의 사전 서면 동의 없이 본 문서의 전체 혹은 일부를 복사, 전송, 재생, 공개, 수정 또는 복제할 수 없습니다.

CA 소프트웨어의 라이선스를 허여받은 사용자들은 본인 및 그 직원들의 해당 소프트웨어와 관련된 내부적인 사용을 위해 1부의 문서 사본을 만들 수 있습니다. 단, 이 경우 복사본에는 CA 저작권 표시 및 문구 일체가 기재되어야 합니다.

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

CA는 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. CA는 본 시스템의 사용으로 인해 발생하는 직, 간접 손실이나 손해(수익의 손실, 사업 중단, 영업권 또는 데이터 손실 포함)에 대해서는 (상기 손실이나 손해에 대해 사전에 명시적으로 통지를 받은 경우라 하더라도) 귀하나 제 3자에게 책임을 지지 않습니다.

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

본 문서는 CA에서 제작되었습니다.

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

Copyright © 2014 CA. All rights reserved. 이 문서에서 언급된 모든 상표, 상호, 서비스 표시 및 로고는 각 해당 회사의 소유입니다.

CA Technologies 제품 참조

이 문서는 다음 CA Technologies 제품을 참조합니다 :

- CA Directory
- SiteMinder
- CA Business Intelligence

CA 에 문의

기술 지원팀에 문의

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

설명서 변경 사항

SiteMinder 의 이전 릴리스에서 발견된 문제로 인해 다음과 같은 내용이 12.52 SP1 설명서에서 업데이트되었습니다.

- [보고서 서버 다시 시작](#) (페이지 504) - LD_LIBRARY_PATH 변수의 값이 업데이트되었습니다.
- [정책 저장소 스키마 파일 편집](#) (페이지 170) - Novell eDirectory 정책 저장소를 구성하는 데 사용된 정책 저장소 체계 파일을 편집하기 위한 명령이 업데이트되었습니다.
- [Linux 에서 Korn 셸\(ksh\) 패키지가 필요함](#) (페이지 66) - 정책 서버 설치에서 이 패키지가 필요하다는 설명이 추가되었습니다.
- [감사 저장소 스키마 만들기](#) (페이지 413) - DB2 지침이 수정되었습니다. 전체 어설션 자체가 아니라 각 어설션의 NULL 키워드만 제거하십시오.
- [MBCS URL 을 지원하는 인증 체계](#) (페이지 657) - 인쇄 오류가 수정되었습니다. 이 업데이트는 CQ171840 을 해결합니다.
- [Microsoft SQL Server 정보](#) (페이지 40) - SiteMinder 스키마가 데이터베이스에 이미 있는 경우 생성 권한이 있는 관리자에 대한 자격 증명이 필요 없다는 설명이 추가되었습니다.
- [정책 저장소를 구성하는 방법\(MySQL\)](#) (페이지 311) - 유니코드 문자를 지원하는 새로운 스키마 파일을 포함하여 이 항목과 [SiteMinder 스키마 만들기](#) (페이지 312) 항목이 수정되었습니다. 이 업데이트는 CQ178545 을 해결합니다.
- JCE(Java Cryptographic Extension)를 위해 패치 필요 - 이 항목에서는 Java 에서 제공하는 암호화 알고리즘을 사용하기 위해 업데이트가 필요한 파일을 설명합니다. CQ 174929 를 해결합니다.
- [필요한 Linux 라이브러리](#) (페이지 24) - 64 비트 Red Hat 6.x 에 필요한 모든 RPM 패키지는 32 비트 패키지라는 내용의 참고가 추가되었습니다. 이 업데이트는 CQ 177043 을 해결합니다.
- [Oracle Directory Server 를 정책 저장소로 구성](#) (페이지 198) - smlldapsetup 명령 정의가 변경되었습니다. 이 업데이트는 CQ 177321 을 해결합니다.
- [Oracle 정책 저장소 구성](#) (페이지 359), [MySQL 정책 저장소 구성](#) (페이지 310), [SQL Server 정책 저장소 구성](#) (페이지 326) - 더 이상 지원되지 않는 DataDirect 6.0 드라이버 지침이 DataDirect 7.1 드라이버에 대한 지침으로 바뀌어 업데이트되었습니다. CQ 177973 을 해결합니다.

- [Microsoft SQL Server 정보](#) (페이지 40) - 데이터베이스에 CA SiteMinder 스키마가 이미 있는 경우 마법사가 생성 권한이 있는 데이터베이스 관리자의 자격 증명을 요구하지 않는다는 참고가 추가되었습니다. CQ 176984 를 해결합니다.
- [Oracle Virtual Directory 를 정책 저장소로 구성하는 방법](#) (페이지 240) - Oracle Virtual Directory 를 정책 저장소로 구성하는 방법을 설명하는 섹션이 추가되었습니다. CQ 174391 을 해결합니다.
- [Oracle Unified Directory 를 정책 저장소로 구성하는 방법](#) (페이지 224) - Oracle Unified Directory 를 정책 저장소로 구성하는 방법을 설명하는 섹션이 추가되었습니다. CQ 172420 을 해결합니다.
- [SiteMinder 에 대한 Oracle 데이터 원본 구성](#) (페이지 367) - SCAN(Single Client Access Name) 기능을 사용하여 Oracle Real Application Cluster 11g R2 에 대한 데이터 원본을 생성하는 방법을 설명하는 내용이 추가되었습니다. CQ 171215 를 해결합니다.
- [필요한 Linux 라이브러리](#) (페이지 24) - 필요한 Linux 라이브러리의 전체 목록이 추가되었고 "관리 UI 설치 요구 사항" 장에 항목이 포함되었습니다. CQ 169427 및 171403 을 해결합니다. STAR 이슈 21343328-04 및 21436925-1 을 해결합니다.
- [정책 저장소 스키마 만들기](#) (페이지 203) - 여러 단계에 명령이 추가되었습니다. RTC 결함 117824 를 해결합니다.

이 안내서의 두 번째 에디션에는 다음과 같은 변경된 사항이 포함되어 있습니다.

설명서에서만 변경된 내용

- [콘솔 모드에서 구성 마법사 실행](#) (페이지 89) - 콘솔 모드에서 고급 인증 서버를 활성화하기 위한 단계가 추가되었습니다. 설명서는 12.52 SP1 에서 업데이트되었습니다. 이 변경 사항은 CQ 182427 및 STAR 21708422-1 을 해결합니다.
- [필요한 Linux 라이브러리](#) (페이지 24) - ncurses 패키지의 요구 사항에 대한 설명이 추가되었습니다. 설명서는 12.52 SP1 에서 업데이트되었습니다. 이 변경 사항은 CQ 184220 을 해결합니다.

목차

제 1 장: 정책 서버 설치 요구 사항 19

Windows	19
UNIX	20

제 2 장: 관리 UI 설치 요구 사항 23

Windows UI 호스트 시스템 요구 사항 확인	23
UNIX UI 호스트 시스템 요구 사항 확인	23
필요한 Linux 라이브러리	24

제 3 장: 보고서 서버 설치 요구 사항 27

시스템 요구 사항	27
Windows	27
UNIX	27
Solaris 필수 패치 클러스터	28
Red Hat 필수 패치 클러스터	28
보고서 데이터베이스 요구 사항	29
연결 요구 사항	29

제 4 장: Windows 시스템에 정책 서버 설치 31

설치 로드맵	32
Windows 에서 정책 서버 설치 전 고려 사항	33
Windows 에서 정책 서버 설치 방법	33
정책 서버 구성 요소 고려 사항	34
정책 저장소 고려 사항	35
FIPS 고려 사항	36
설치 관리자에 필요한 정보 수집	37
정책 서버 설치 관리자 실행	43
SNMP 이벤트 트래핑이 사용되도록 설정	45
정책 서버 설치 문제 해결	46
정책 서버 구성 마법사	46
구성 마법사를 사용하는 방법	47
정책 서버 다시 설치	54
Windows 에서 정책 서버 제거 방법	54

Path 변수에 JRE 설정	55
에이전트 호스트 파일에서 정책 서버 참조 제거	55
모든 SiteMinder 프로세스 중지	56
정책 서버 제거	56
남은 항목 제거	57
남은 서비스 제거	57
스크립팅 인터페이스	58

제 5 장: UNIX 시스템에 정책 서버 설치 59

설치 로드맵	60
Solaris 10 영역 지원	61
전역 영역 지원	61
스파스 루트 영역 지원	62
전체 루트 영역 지원	62
정책 서버 설치를 준비하는 방법	63
필요한 Linux 라이브러리	64
Linux 에서 Korn 셸(ksh) 패키지가 필요함	66
새 UNIX 계정 만들기	66
UNIX 시스템 매개 변수 수정	67
지역화 변수 설정 해제	68
LANG 환경 변수 설정 해제	68
UNIX 에서 정책 서버 설치 전 고려 사항	68
UNIX 에서 정책 서버 설치 방법	69
정책 서버 구성 요소 고려 사항	70
정책 저장소 고려 사항	70
FIPS 고려 사항	72
설치 관리자에 필요한 정보 수집	73
GUI 모드에서 정책 서버 설치	79
콘솔 모드에서 정책 서버 설치	82
Security-Enhanced Linux 에 예외 추가	84
SNMP 데몬 다시 시작	84
정책 서버 설치 문제 해결	85
자동 시작 구성	85
정책 서버 구성 마법사	86
구성 마법사를 사용하는 방법	87
UNIX 에서 정책 서버 제거 방법	90
에이전트 호스트 파일에서 정책 서버 참조 제거	90
PATH 변수에 JRE 설정	91
모든 SiteMinder 프로세스 중지	91

정책 서버 제거	91
IWS 에서 SiteMinder 참조 제거	93
StartServletExec 에서 SiteMinder 참조 제거	94
남은 항목 제거	94

제 6 장: SiteMinder 데이터를 저장하도록 LDAP 디렉터리 서버 구성 95

정책 또는 키 저장소로 LDAP 디렉터리 서버 사용	95
설치 로드맵	96
중요 고려 사항	97
기본 정책 저장소 개체 고려 사항	98
CA Directory 를 정책 저장소로 구성	99
디렉터리 서버 정보 수집	99
정책 저장소를 구성하는 방법	100
CA Directory 를 세션 저장소로 사용	114
세션 저장소를 구성하는 방법	114
Active Directory 를 정책 저장소로 구성	119
디렉터리 서버 정보 수집	120
정책 저장소를 구성하는 방법	121
Active Directory ObjectCategory 인덱싱 특성 지원	131
ObjectCategory 특성 지원이 사용되거나 사용되지 않도록 설정	132
Domino Directory Server 를 정책 저장소로 구성	132
Domino Directory Server 를 정책 저장소로 구성하는 방법	133
IBM Tivoli Directory Server 를 정책 저장소로 구성	144
디렉터리 서버 정보 수집	144
정책 저장소를 구성하는 방법	145
Microsoft Active Directory LDS 를 정책 저장소로 구성	155
Active Directory LDS 사전 요구 사항	156
디렉터리 서버 정보 수집	156
정책 저장소를 구성하는 방법	157
Novell eDirectory 를 정책 저장소로 구성	167
Novell eDirectory 에서 정책 저장소 개체의 제한 사항	168
디렉터리 서버 정보 수집	168
정책 저장소를 구성하는 방법	169
OpenLDAP 을 정책 저장소로 구성	180
디렉터리 서버 정보 수집	181
정책 저장소를 구성하는 방법	181
Oracle Directory Server 를 정책 저장소로 구성	198
디렉터리 서버 정보 수집	198
정책 저장소를 구성하는 방법	199

Oracle Internet Directory 를 정책 저장소로 구성	211
디렉터리 서버 정보 수집	212
정책 저장소를 구성하는 방법	212
Oracle Unified Directory 를 정책 저장소로 구성하는 방법	224
디렉터리 서버 정보 수집	225
Oracle Unified Directory 인스턴스를 구성하는 방법	226
데이터베이스 생성 방법	230
정책 서버를 정책 저장소에 연결	232
SiteMinder 슈퍼 사용자 암호 설정	233
정책 저장소 데이터 정의 가져오기	234
기본 정책 저장소 개체 가져오기	235
고급 인증 서버를 사용하도록 설정	237
관리 UI 등록 준비	237
Oracle Virtual Directory 를 정책 저장소로 구성하는 방법	240
디렉터리 서버 정보 수집	241
SiteMinder 스키마 파일을 사용하여 OVD 로컬 스키마 확장	243
기존 정책 저장소에 연결하기 위해 Oracle Virtual Directory 어댑터 생성	244
정책 서버를 정책 저장소에 연결	246
SiteMinder 슈퍼 사용자 암호 설정	247
고급 인증 서버를 사용하도록 설정	248
정책 서버를 다시 시작합니다.	248
관리 UI 등록 준비	249
Red Hat Directory Server 를 정책 저장소로 구성	251
디렉터리 서버 정보 수집	252
정책 저장소를 구성하는 방법	252
Siemens DirX 를 정책 저장소로 구성	262
디렉터리 서버 정보 수집	263
정책 저장소를 구성하는 방법	263
별도의 키 저장소 구성	274
Microsoft Active Directory 를 키 저장소로 구성	274
Microsoft AD LDS 를 키 저장소로 구성	279
Oracle Directory Server Enterprise Edition 을 키 저장소로 구성	285
Oracle Internet Directory Server 를 키 저장소로 구성	292
Red Hat Directory Server 를 키 저장소로 구성	296

제 7 장: 관계형 데이터베이스에 SiteMinder 데이터 저장소 구성 301

관계형 데이터베이스를 정책 또는 키 저장소로 사용	302
설치 로드맵	302
중요 고려 사항	304

기본 정책 저장소 개체 고려 사항	304
관계형 데이터베이스의 스키마 파일	305
IBM DB2 스키마 파일	306
MySQL 스키마 파일	307
SQL Server 스키마 파일	308
PostgreSQL Server 스키마 파일	309
Oracle 스키마 파일	310
MySQL 정책 저장소 구성	310
데이터베이스 정보 수집	311
정책 저장소를 구성하는 방법	311
SQL Server 정책 저장소 구성	326
데이터베이스 정보 수집	327
정책 저장소를 구성하는 방법	328
PostgreSQL 서버 정책 저장소를 구성하는 방법	344
PostgreSQL 데이터베이스 정보 수집	345
PostgreSQL 용 SiteMinder 스키마 만들기	346
Windows 에서 PostgreSQL 데이터 원본 만들기	347
UNIX 에서 PostgreSQL 데이터 원본 만들기	348
PostgreSQL Server 유선 프로토콜 드라이버 구성	349
정책 서버를 데이터베이스에 연결	351
SiteMinder 슈퍼 사용자 암호 설정	352
정책 저장소 데이터 정의 가져오기	353
기본 정책 저장소 개체 가져오기	354
고급 인증 서버를 사용하도록 설정	356
정책 서버를 다시 시작합니다.	356
관리 UI 등록 준비	357
Oracle 정책 저장소 구성	359
Oracle 10g 데이터베이스에 대한 사전 요구 사항	360
Oracle 12c 데이터베이스에 대한 사전 요구 사항	362
데이터베이스 정보 수집	362
정책 저장소를 구성하는 방법	365
IBM DB2 정책 저장소 구성	385
데이터베이스 정보 수집	386
정책 저장소를 구성하는 방법	387
IBM DB2 에서 세션 정보를 저장하는 방법	400
세션 저장소 스키마 만들기	400
정책 서버를 데이터베이스에 연결	401
정책 서버를 다시 시작합니다.	402
MySQL 에 세션 정보를 저장하는 방법	402
세션 저장소 스키마 만들기	403

정책 서버를 데이터베이스에 연결	403
정책 서버를 다시 시작합니다.....	404
Oracle 에서 세션 정보를 저장하는 방법	405
세션 저장소 스키마 만들기	405
정책 서버를 데이터베이스에 연결	406
정책 서버를 다시 시작합니다.....	407
SQL Server 에서 세션 정보를 저장하는 방법	408
세션 저장소 스키마 만들기	408
정책 서버를 데이터베이스에 연결	409
정책 서버를 다시 시작합니다.....	410
PostgreSQL 에 세션 정보를 저장하는 방법	410
세션 저장소 스키마 만들기	410
정책 서버를 데이터베이스에 연결	411
정책 서버를 다시 시작합니다.....	412
IBM DB2 에서 감사 로그를 저장하는 방법	412
감사 저장소 스키마 만들기	413
정책 서버를 데이터베이스에 연결	414
정책 서버를 다시 시작합니다.....	415
MySQL 에서 감사 로그를 저장하는 방법	415
감사 로그 스키마 만들기	416
정책 서버를 데이터베이스에 연결	416
정책 서버를 다시 시작합니다.....	418
Oracle 에서 감사 로그를 저장하는 방법	418
감사 로그 스키마 만들기	419
정책 서버를 데이터베이스에 연결	419
정책 서버를 다시 시작합니다.....	421
SQL Server 에서 감사 로그를 저장하는 방법	421
감사 로그 스키마 만들기	421
정책 서버를 데이터베이스에 연결	422
정책 서버를 다시 시작합니다.....	423
PostgreSQL 에서 감사 로그를 저장하는 방법	423
감사 로그 스키마 만들기	424
정책 서버를 데이터베이스에 연결	424
정책 서버를 다시 시작합니다.....	426
IBM DB2 에서 키 정보를 저장하는 방법	426
키 저장소 스키마 만들기	427
정책 서버를 데이터베이스에 연결	427
정책 서버를 다시 시작합니다.....	428
MySQL 에서 키 정보를 저장하는 방법	429
키 저장소 스키마 만들기	429

정책 서버를 데이터베이스에 연결	430
정책 서버를 다시 시작합니다.....	431
Oracle 에서 키 정보를 저장하는 방법	431
키 저장소 스키마 만들기	432
정책 서버를 데이터베이스에 연결	432
정책 서버를 다시 시작합니다.....	434
SQL Server 에서 키 정보를 저장하는 방법	434
키 저장소 스키마 만들기	434
정책 서버를 데이터베이스에 연결	435
정책 서버를 다시 시작합니다.....	436
PostgreSQL 에서 키 정보를 저장하는 방법	436
키 저장소 스키마 만들기	437
정책 서버를 데이터베이스에 연결	437
정책 서버를 다시 시작합니다.....	438
샘플 사용자 디렉터리	439
IBM DB2 샘플 사용자 디렉터리 구성	439
MySQL 샘플 사용자 디렉터리 구성.....	440
Oracle 샘플 사용자 디렉터리 구성.....	440
SQL Server 샘플 사용자 디렉터리 구성	441

제 8 장: 관리 UI 설치 443

UI 와 정책 서버 사이의 트러스트 관계	443
관리 UI 설치 검사 목록 완료	443
관리 UI 설치 방법.....	444
설치 관리자에 필요한 정보 수집	445
관리 UI 등록 창 재설정.....	445
관리 UI 설치 방법	448
관리 UI 설치 문제 해결.....	452
관리 UI 등록 방법.....	453
FIPS 환경 변수 만들기	453
응용 프로그램 서버 시작	454
관리 UI 등록	455
응용 프로그램 서버 중지	457
관리자 자격 증명	458
(선택 사항) 고가용성을 위해 추가 관리 UI 설치 및 구성	458
관리 UI 에 대한 추가 정책 서버 연결	459
관리 UI 등록 도구 실행.....	459
등록 정보 수집	462
정책 서버에 대한 연결 구성	462

기본 정책 서버 연결 수정	463
정책 서버 연결 삭제	464
(선택 사항) 관리 UI 제거	464
UNIX 에서 관리 UI 제거	465
웹 에이전트 설치를 위한 정책 서버 준비	466

제 9 장: 보고서 설치 469

설치 로드맵	469
보고서 설치 검사 목록	470
보고서 서버	471
보고서 데이터베이스 및 감사 데이터베이스	473
보고서 데이터베이스 및 감사 데이터베이스	475
보고 고려 사항	477
보고서 설치 작동 방식	478
보고서 서버 설치 방법	479
설치 관리자에 필요한 정보 수집	479
보고서 서버 설치	483
보고서 서버 설치 문제 해결	493
보고서 템플릿 설치 방법	493
설치 관리자에 필요한 정보 수집	494
보고서 템플릿 설치	494
작업 서버 서비스 시간 만료 값 늘리기	497
보고서 서버 등록 방법	499
클라이언트 이름 및 암호 만들기	500
등록 정보 수집	502
정책 서버에 보고서 서버 등록	503
보고서 서버 다시 시작	504
관리 UI 에 대한 연결 구성	506
감사 데이터베이스 구성 방법	507
관리 UI 에 감사 데이터베이스 등록	508
감사 데이터베이스와 보고서 서버의 연결	510
보고서 서버 시작	510
보고서 서버 중지	512
보고서 제거 방법	513
Windows 에서 보고서 서버 구성 마법사 제거	514
UNIX 에서 보고서 서버 구성 마법사 제거	514
Windows 에서 보고서 서버 제거	515
UNIX 에서 보고서 서버 제거	516
Windows 항목 제거	517

UNIX 항목 제거.....	517
보고서 데이터베이스 테이블 제거.....	518
보고서 서버와 관리 UI 의 연결 삭제.....	518
보고서 서버 다시 설치.....	518

제 10 장: OneView 모니터 구성 519

OneView 모니터 개요.....	519
OneView 모니터에 대한 시스템 요구 사항.....	520
OneView 모니터 구성.....	520
OneView 모니터 GUI 와 IIS 웹 에이전트를 동일한 컴퓨터에 구성할 경우의 제한 사항.....	521
Windows/IIS 에 OneView 모니터 GUI 를 구성하는 방법.....	521
Windows 에 ServletExec 를 설치하기 위한 사전 요구 사항.....	522
Windows IIS 에 ServletExec 설치.....	522
ServletExec 설치 후 IIS 사용자에게 권한 설정.....	523
UNIX/Sun Java System 에 OneView 모니터 GUI 를 구성하는 방법.....	523
ServletExec 설치를 위한 사전 요구 사항.....	523
Sun Java System 6.0 에서 서블릿이 사용되지 않도록 설정.....	524
UNIX/Sun Java System 에 ServletExec/AS 설치.....	524
OneView 모니터 서비스 시작.....	526
OneView 모니터 GUI 액세스.....	526
정책 서버 클러스터 모니터링.....	527

제 11 장: SNMP 지원 529

SNMP 지원 개요.....	529
Windows 및 UNIX 시스템에 대한 SNMP 사전 요구 사항.....	531
Windows 사전 요구 사항.....	531
UNIX 시스템 사전 요구 사항.....	532
Windows 에 SNMP 에이전트 구성.....	532
Windows 에서 SNMP 이벤트 트래핑을 구성하는 방법.....	533
UNIX 시스템에 SNMP 에이전트 구성.....	535
UNIX 시스템에서 SNMP 이벤트 트래핑을 구성하는 방법.....	535
Red Hat Enterprise Linux Advanced Server 에 대해 SNMP Gets 테스트.....	537

제 12 장: 기존 응용 프로그램 서버에 관리 UI 설치 539

관리 UI 설치 요구 사항.....	539
관리 UI 시스템 요구 사항.....	539
응용 프로그램 서버 요구 사항.....	541
UI 와 정책 서버 사이의 트러스트 관계.....	544

관리 UI 설치 검사 목록	545
관리 UI 설치 방법	546
필요한 Linux 라이브러리	546
응용 프로그램 서버 정보 수집	548
관리 UI 설치	549
관리 UI 등록 방법	553
관리 UI 등록 창 재설정	554
FIPS 환경 변수 만들기	557
응용 프로그램 서버 시작	558
관리 UI 등록	559
응용 프로그램 서버 중지	561
관리자 자격 증명	562
관리 UI 고가용성	563
Windows 에서 관리 UI 제거	563
UNIX 에서 관리 UI 제거	564

제 13 장: 문제 해결 567

정책 서버 문제 해결	567
Solaris 의 NETE_PS_ALT_CONF_FILE 환경 변수	567
설치 후 정책 서버가 시작되지 않음	568
프로필 파일에 SiteMinder 환경 변수가 설정되지 않음	568
Winsock 오류 10054 메시지	569
SiteMinder 라이선스 작업	569
영어가 아닌 입력 문자에 정크 문자가 포함됨	571
설치 제거 시 Java 오류 메시지	572
Adobe Acrobat Reader 가 설치되지 않음	573
Active Directory 를 사용자 저장소로 사용할 경우의 문제	573
"AE failed to load library 'smjavaapi'." (AE 에서 'smjavaapi' 라이브러리를 로드하지 못했습니다.)	
시스템 오류	574
정책 저장소 문제 해결	574
많은 수의 개체가 포함된 정책 저장소	574
SSL initialization failed: error -8174 (security library: bad database.)	575
ODBC 정책 저장소를 가져올 때 UserDirectory 오류가 발생하고 가져오기가 실패함	576
OneView 모니터 문제 해결	577
수정된 UNIX/Sun Java System 웹 서버 구성 파일의 문제 수정	577
/sitemindermonitor 에 대한 Windows/IIS 가상 경로가 없음	578
관리 UI 문제 해결	579
관리 UI 가 중단되어 응답하지 않음	579
처리되지 않은 예외가 발생하고 WebSphere 가 중단됨	579

정책 서버 연결을 등록할 수 없음	580
API 오류가 나타남	580
파일에 등록 기록이 없다는 오류가 나타남	581
등록 파일이 잘못되었다는 오류가 나타남	583
시간 만료 없이 등록이 실패함	584
관리 UI 등록 로그를 찾을 수 없음	585
시간 만료 오류가 발생하고 검색이 실패함	585
기본 로깅 파일을 찾을 수 없음	587
기본 로그 파일에 충분한 정보가 없음	587
보고서 서버 문제 해결	588
보고서 서버 설치 시 문자와 관련된 오류가 발생하고 설치가 실패함	588
보고서 서버 설치 관리자에서 파일 누락 오류가 표시됨	589
설치 제거에서 응용 프로그램을 닫으라는 메시지가 표시됨	589
감사 기반 보고서에 결과가 반환되지 않음	590
정책 분석 보고서를 실행할 수 없음	590
관리 UI 에서 파일 누락 오류가 표시됨	591

제 14 장: 무인 설치 593

무인 설치 소개	593
무인 설치 지침	593
기본 속성 파일	593
정책 서버 속성 파일	594
관리 UI 속성 파일	594
보고 기능 속성 파일	595
정책 서버 무인 설치 실행 방법	595
정책 서버 설치 관리자 속성 파일 수정	596
정책 서버 설치 관리자 실행	607
정책 서버 설치 문제 해결	609
무인 정책 서버 설치 중지	610
관리 UI 무인 설치 실행 방법	610
필수 구성 요소 설치 관리자 속성 파일 수정	611
관리 UI 설치 관리자 속성 파일 수정	612
관리 UI 설치 관리자 실행	615
보고서 서버 무인 설치 실행 방법	617
Windows 의 보고서 서버 응답 파일 수정	618
UNIX 의 보고서 서버 응답 파일 수정	636
SiteMinder 보고서 서버 구성 마법사 속성 파일 수정	649
보고서 서버 설치 관리자 실행	649
보고서 템플릿 설치	652

부록 A: 다국어 환경의 정책 서버 구성 653

다국어 환경의 정책 서버	653
정책 서버 설치 전 계획 고려 사항	653
멀티바이트 문자를 지원하는 정책 서버 구성 요소	654
멀티바이트 문자 URL 지원	655
다국어 문자를 지원하는 SiteMinder 데이터 저장소 구성	658
SQL Server 에 다국어 SiteMinder 데이터 저장소 구성	658
Oracle 에 다국어 SiteMinder 데이터 저장소 구성	658
SQL Server 에서 유니코드를 지원하는 사용자 저장소 구성	660
Oracle 에 일본어 사용자 저장소 구성	661

부록 B: 수정된 환경 변수 663

수정된 Windows 환경 변수	663
수정된 UNIX 환경 변수	664

제 1 장: 정책 서버 설치 요구 사항

Windows

정책 서버를 설치하는 Windows 시스템은 다음과 같은 최소 시스템 요구 사항을 충족해야 합니다.

- **CPU**-x86 또는 x64
- **메모리** - 2 GB 시스템 RAM
참고: 정책 서버 처리에는 2 GB RAM 이 권장됩니다. 정책 서버 호스트 시스템에서 사용할 수 있는 RAM 크기는 4 GB 이상을 권장합니다.
- **사용 가능한 디스크 공간:**
 - 설치 위치의 사용 가능한 디스크 공간 4 GB
 - 시스템의 임시 파일 위치에 3 GB 의 사용 가능한 공간 필요
참고: 이러한 요구 사항은 약 1,000 개의 정책을 포함하는 중간 규모의 정책 데이터베이스를 기준으로 합니다.
- **JDK** - JDK 와 함께 제공되는 필수 JRE 가 정책 서버 호스트 시스템에 설치되어 있는지 확인합니다.
- **JCE** - 최신 "Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction" 패치가 필요합니다. 운영 플랫폼에 맞는 JCE 패키지를 찾으려면 Oracle 웹 사이트를 방문하십시오.
패치를 시스템의 다음 파일에 적용하십시오.
 - local_policy.jar
 - US_export_policy.jar이러한 파일은 `jre_home\lib\security` 디렉터리에 있습니다.
`jre_home`
이 변수는 Java Runtime Environment 설치 위치를 지정합니다.

- **LDAP 디렉터리 서버 또는 관계형 데이터베이스** - 정책 저장소로 지원
LDAP 디렉터리 서버를 사용하고 있는지 아니면 관계형 데이터베이스를 사용하고 있는지 확인합니다.

참고: 지원되는 CA 및 타사 구성 요소의 목록에 대해서는 기술 지원 사이트의 SiteMinder 12.5.2 SP1 Platform Support Matrix(플랫폼 지원표)를 참조하십시오.

UNIX

정책 서버를 설치하는 UNIX 시스템은 다음과 같은 최소 시스템 요구 사항을 충족해야 합니다.

- **CPU**

- **Solaris** - UltraSparc 440MHz 이상
- **Red Hat**-x86 또는 x64

참고: Red Hat 운영 체제는 성능을 위해 엔트로피를 사용합니다.
구성 요소를 설치하기 전에 엔트로피를 늘리십시오. 그렇지 않으면 설치하는 데 시간이 오래 걸릴 수 있으며 관리 UI 응답이 런타임 중에 느려질 수 있습니다.

다음 명령을 사용하십시오.

```
mv /dev/random /dev/random.org  
ln -s /dev/urandom /dev/random
```

- **메모리** - 2 GB 시스템 RAM

참고: 정책 서버 처리에는 2 GB RAM 이 권장됩니다. 정책 서버 호스트 시스템에서 사용할 수 있는 RAM 크기는 4 GB 이상을 권장합니다.

- **사용 가능한 디스크 공간:**

- 사용 가능한 디스크 공간 4 GB
- /tmp 에 사용 가능한 디스크 공간 3 GB

참고: 일반적으로 정책 서버의 일상적인 작업을 위해서는 /tmp 에 10 MB 의 사용 가능한 디스크 공간이 있어야 합니다. 정책 서버에서는 /tmp 아래에 파일과 명명된 파이프를 생성합니다. 경로는 변경할 수 없습니다.

- **JRE** - 정책 서버를 설치하는 시스템에 필요한 JRE 버전이 설치되어 있는지 확인합니다.

- **JCE** - Java 암호화 알고리즘을 사용하려면 최신 JCE(Java Cryptography Extension) Unlimited Strength Jurisdiction 패치가 필요합니다. 운영 플랫폼에 맞는 JCE 패키지를 찾으려면 Oracle 웹 사이트를 방문하십시오. 패치를 시스템의 다음 파일에 적용하십시오.
 - local_policy.jar
 - US_export_policy.jar

이러한 파일은 *jre_home/lib/security* 디렉터리에 있습니다.

jre_home

이 변수는 Java Runtime Environment 설치 위치를 지정합니다.

- **LDAP 디렉터리 서버 또는 관계형 데이터베이스** - 정책 저장소로 지원 LDAP 디렉터리 서버를 사용하고 있는지 아니면 관계형 데이터베이스를 사용하고 있는지 확인합니다.

참고: 지원되는 CA 및 타사 구성 요소의 목록에 대해서는 기술 지원 사이트의 SiteMinder 12.52 SP1 Platform Support Matrix(플랫폼 지원표)를 참조하십시오.

제 2 장: 관리 UI 설치 요구 사항

Windows UI 호스트 시스템 요구 사항 확인

독립 실행형 설치를 위한 Windows 관리 UI 호스트 시스템은 다음과 같은 최소 시스템 요구 사항을 충족해야 합니다.

- **CPU** - x86 또는 x64, 1.2 GHz 이상
- **메모리** - 1 GB 시스템 RAM. 권장 크기는 2 GB 입니다.
- **사용 가능한 디스크 공간**-840 MB
- **임시 디렉터리 공간**-3 GB
- **화면 해상도**-관리 UI 를 올바르게 표시하려면 256 색 이상을 지원하는 1024 x 768 이상의 해상도가 필요합니다.

운영 체제 및 기타 필수 타사 구성 요소가 지원되는지 여부를 확인하려면 플랫폼 지원표를 사용하십시오.

UNIX UI 호스트 시스템 요구 사항 확인

독립 실행형 설치를 위한 UNIX 관리 UI 호스트 시스템은 다음과 같은 최소 시스템 요구 사항을 충족해야 합니다.

- **CPU**
 - Solaris - UltraSparc, 440 MHz 이상
 - Red Hat Linux - x86 또는 x64, 700 MHz 이상

참고: Red Hat 6 운영 체제는 성능을 위해 엔트로피를 사용합니다. 구성 요소를 설치하기 전에 엔트로피를 늘리십시오. 그렇지 않으면 설치하는 데 시간이 오래 걸릴 수 있으며 관리 UI 응답이 런타임 중에 느려질 수 있습니다.

다음 명령을 사용하십시오.

```
mv /dev/random /dev/random.org  
ln -s /dev/urandom /dev/random
```

- **메모리** - 1 GB 시스템 RAM. 권장 크기는 2 GB 입니다.

- 사용 가능한 디스크 공간-840 MB
- 임시 디렉터리 공간-3 GB
- 화면 해상도-관리 UI 를 올바르게 표시하려면 256 색 이상을 지원하는 1024 x 768 이상의 해상도가 필요합니다.

운영 체제 및 기타 필수 타사 구성 요소가 지원되는지 여부를 확인하려면 플랫폼 지원표를 사용하십시오.

필요한 Linux 라이브러리

Linux 운영 환경에서 작동하는 구성 요소의 경우 특정 라이브러리 파일이 필요합니다. 올바른 라이브러리를 설치하지 못하면 다음과 같은 오류가 발생할 수 있습니다.

```
java.lang.UnsatisfiedLinkError
```

이 구성 요소의 Linux 버전을 설치, 구성 또는 업그레이드하는 경우 호스트 시스템에 다음 패키지가 필요합니다.

Red Hat 5.x:

- compat-gcc-34-c++-3.4.6-patch_version.i386
- libstdc++-4.x.x-x.el5.i686.rpm
- libidn.so.11.rpm
- ncurses

Red Hat 6.x:

- libstdc++-4.x.x-x.el6.i686.rpm
- libidn-1.18-2.el6.i686
- libXext.i686.rpm
- libXrender.i686.rpm
- libXtst.i686.rpm
- libidn.so.11.rpm
- ncurses

또한 Red Hat 6.x(64 비트)의 경우:

64 비트 Red Hat 6.x 에 필요한 모든 RPM 패키지는 32 비트 패키지입니다.

- libXau-1.0.5-1.el6.i686.rpm
- libxcb-1.5-1.el6.i686.rpm
- compat-db42-4.2.52-15.el6.i686.rpm
- compat-db43-4.3.29-15.el6.i686.rpm
- libX11-1.3-2.el6.i686.rpm
- libXrender-0.9.5-1.el6.i686.rpm
- libexpat.so.1(expat-2.0.1-11.el6_2.i686.rpm 에서 제공)
- libfreetype.so.6(freetype-2.3.11-6.el6_2.9.i686.rpm 에서 제공)
- libfontconfig.so.1(fontconfig-2.8.0-3.el6.i686.rpm 에서 제공)
- libICE-1.0.6-1.el6.i686.rpm
- libuuid-2.17.2-12.7.el6.i686.rpm
- libSM-1.1.0-7.1.el6.i686.rpm
- libXext-1.1-3.el6.i686.rpm
- compat-libstdc++-33-3.2.3-69.el6.i686.rpm
- compat-db-4.6.21-15.el6.i686.rpm
- libXi-1.3-3.el6.i686.rpm
- libXtst-1.0.99.2-3.el6.i686.rpm
- libXft-2.1.13-4.1.el6.i686.rpm
- libXt-1.0.7-1.el6.i686.rpm
- libXp-1.0.0-15.1.el6.i686.rpm

- libstdc++.i686.rpm
- compat-libtermcap.rpm
- libidn.i686.rpm
- ncurses

제 3 장: 보고서 서버 설치 요구 사항

시스템 요구 사항

다음 단원에서는 보고서 서버를 설치하기 위한 최소 시스템 요구 사항에 대해 자세히 설명합니다.

참고: 지원되는 CA 및 타사 구성 요소의 목록에 대해서는 기술 지원 사이트의 SiteMinder 12.52 SP1 Platform Support Matrix(플랫폼 지원표)를 참조하십시오.

Windows

보고서 서버를 설치하려는 Windows 시스템은 다음과 같은 최소 시스템 요구 사항을 충족해야 합니다.

- **CPU** - Intel® Pentium™ 4 클래스 프로세서, 2.0 GHz
- **메모리** - 2 GB RAM
- **사용 가능한 디스크 공간** - 10 GB

참고: 이 요구 사항은 보고서 서버를 설치하는 데 필요한 공간을 의미합니다. 즉, 보고서 저장에 필요한 디스크 공간까지 고려한 요구 사항이 아닙니다.

- **임시 디렉터리 공간** - 1 GB
- **화면 해상도** - 관리 UI 에서 보고서를 올바르게 표시하려면 256 색 이상을 지원하는 1024 x 768 이상의 해상도가 필요합니다.

UNIX

보고서 서버를 설치하려는 UNIX 시스템은 다음과 같은 최소 시스템 요구 사항을 충족해야 합니다.

- **CPU**
 - (Solaris) SPARC v8plusSparc
 - (Red Hat Linux) Intel Pentium 4 클래스 프로세서, 2.0 GHz
- **메모리** - 2 GB RAM

- **사용 가능한 디스크 공간 - 10 GB**

참고: 이 요구 사항은 보고서 서버를 설치하는 데 필요한 공간을 의미합니다. 즉, 보고서 저장에 필요한 디스크 공간까지 고려한 요구 사항이 아닙니다.

- **임시 디렉터리 공간 - 1 GB**

- **화면 해상도** - 관리 UI 에서 보고서를 올바르게 표시하려면 256 색 이상을 지원하는 1024 x 768 이상의 해상도가 필요합니다.

Solaris 필수 패치 클러스터

보고서 서버에는 특정 Solaris 패치 클러스터가 필요합니다. 보고서 서버를 설치하기 전에 Solaris 시스템을 업데이트하십시오.

중요! 필수 패치를 설치하지 않으면 보고서 서버 설치가 실패합니다.

참고: Solaris 패치 클러스터에 대한 자세한 내용은 *정책 서버 릴리스* 정보를 참조하십시오.

Red Hat 필수 패치 클러스터

보고서 서버에는 특정 Red Hat 패치 클러스터가 필요합니다. 보고서 서버를 설치하기 전에 Red Hat 시스템을 업데이트하십시오.

중요! 필수 패치를 설치하지 않으면 보고서 서버 설치가 실패합니다.

참고: Red Hat 패치 클러스터에 대한 자세한 내용은 *정책 서버 릴리스* 정보를 참조하십시오.

보고서 데이터베이스 요구 사항

보고서 서버에서 보고서를 실행하려면 보고서 데이터베이스가 필요합니다. 보고서 서버 설치 관리자는 보고서 데이터베이스로 사용하기 위해 포함된 버전의 Sun Microsystems MySQL™ (MySQL)을 설치할 수 있습니다.

포함된 버전의 MySQL 을 설치하지 않을 경우 다음과 같은 지원되는 버전을 사용할 수 있습니다.

- Microsoft® SQL Server® (SQL Server)
- Oracle®

중요! 보고서 서버는 CA 제품 간에 공유할 수 있는 CA 공용 구성 요소입니다. 따라서 SiteMinder 가 아닌 다른 제품이 지원하는 데이터베이스 유형 및 버전으로 보고서 데이터베이스를 구성할 수 있습니다. 지원되는 데이터베이스 유형 및 버전 목록에 대해서는 "SiteMinder 12.52 SP1 Platform Support Matrix"(SiteMinder 12.52 SP1 플랫폼 지원표)를 참조하십시오.

연결 요구 사항

보고서 서버가 다음과 통신하려면 드라이버가 필요합니다.

- SQL Server 또는 Oracle 보고서 데이터베이스

참고: 포함된 버전의 MySQL 을 사용할 경우에는 보고서 데이터베이스 연결 요구 사항이 없습니다.

- SiteMinder 감사 저장소

지원되는 Microsoft SQL Server 드라이버나 Oracle Net 클라이언트가 보고서 서버 호스트 시스템에 설치되어 있어야 합니다.

참고: 지원되는 CA 및 타사 구성 요소의 목록에 대해서는 기술 지원 사이트의 SiteMinder 12.52 SP1 Platform Support Matrix(플랫폼 지원표)를 참조하십시오.

제 4 장: Windows 시스템에 정책 서버 설치

이 섹션은 다음 항목을 포함하고 있습니다.

[설치 로드맵](#) (페이지 32)

[Windows 에서 정책 서버 설치 전 고려 사항](#) (페이지 33)

[Windows 에서 정책 서버 설치 방법](#) (페이지 33)

[SNMP 이벤트 트래핑이 사용되도록 설정](#) (페이지 45)

[정책 서버 설치 문제 해결](#) (페이지 46)

[정책 서버 구성 마법사](#) (페이지 46)

[정책 서버 다시 설치](#) (페이지 54)

[Windows 에서 정책 서버 제거 방법](#) (페이지 54)

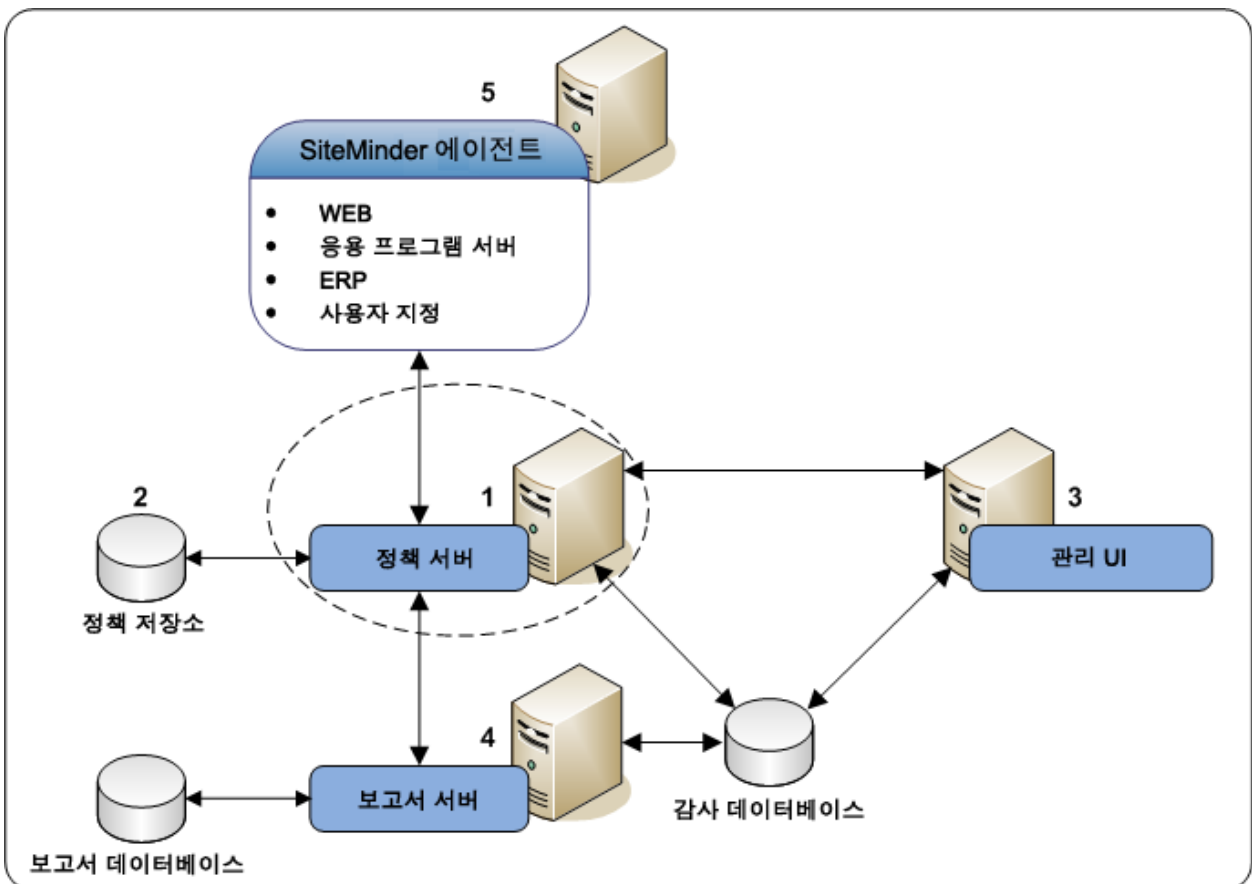
[스크립팅 인터페이스](#) (페이지 58)

설치 로드맵

다음 다이어그램에서는 샘플 SiteMinder 설치를 보여 주고 각 구성 요소를 설치 및 구성하는 순서를 나열합니다. 다음 사항을 고려하십시오.

- 정책 서버 호스트 시스템이 최소 시스템 요구 사항을 충족하는지 확인합니다. 정책 서버를 설치하기 전에 확인하는 것이 좋습니다.
- 점선으로 둘러싸인 부분은 정책 서버입니다. 지금 이 구성 요소를 설치합니다.

그림 1: 설치 로드맵



Windows 에서 정책 서버 설치 전 고려 사항

정책 서버를 설치하기 전에 다음 사항을 고려하십시오.

- **관리자 권한** - 정책 서버를 설치하려면 로컬 관리자 권한이 있는 Windows 계정이 필요합니다.
- **시스템 경로 길이** - 시스템 경로 길이가 1024 자를 초과하면 정책 서버 설치가 실패합니다. 이러한 제한은 포함되거나 제외되는 SiteMinder 추가 디렉터리에 모두 적용됩니다.

참고: 최상의 결과를 얻기 위해 사전 SiteMinder 시스템 경로를 약 700 자로 자르는 것이 좋습니다.

- **(Windows 2008) 방화벽 설정** - 정책 서버를 Windows 2008 에 설치하는 경우 다음 포트에서 인바운드 연결을 허용하도록 Windows 방화벽 설정을 업데이트해야 합니다.
 - 44441
 - 44442
 - 44443

이러한 포트는 기본 정책 서버 계정 설정, 인증 및 권한 부여 포트입니다. 정책 서버를 설치한 후 이러한 포트를 변경할 경우 각 포트에서 인바운드 연결을 허용하도록 해야 합니다.

참고: 자세한 내용은 Microsoft 설명서를 참조하십시오.

- **환경 변수** - 정책 서버 설치에서는 환경 변수를 수정합니다.

Windows 에서 정책 서버 설치 방법

정책 서버를 설치하려면 다음 절차를 완료하십시오.

1. 정책 서버 구성 요소 고려 사항을 검토합니다.
2. 정책 저장소 고려 사항을 검토합니다.
3. FIPS 고려 사항을 검토합니다.
4. 정책 서버 설치 관리자에 필요한 정보를 수집합니다.
5. 정책 서버 설치 관리자를 실행합니다.

6. (선택 사항) SNMP 를 구성한 경우 SNMP 이벤트 트래핑이 사용되도록 설정합니다.
7. (선택 사항) 정책 서버 설치 관리자를 사용하여 정책 저장소를 구성하지 않을 경우 수동으로 정책 저장소를 구성합니다.

추가 정보:

[정책 서버 다시 설치](#) (페이지 54)

정책 서버 구성 요소 고려 사항

정책 서버 외에도 설치 관리자를 통해 다음 구성 요소를 설치 및 구성할 수 있습니다. 정책 서버를 설치하기 전에 다음 사항을 검토하십시오.

- OneView 모니터

OneView 모니터를 통해 SiteMinder 구성 요소를 모니터링할 수 있습니다.

참고: OneView 모니터를 구성하려면 지원되는 Java SDK 및 ServletExec/AS 가 필요합니다.

- 정책 저장소

참고: 키 저장소 및 인증서 데이터 저장소는 자동으로 구성되고 정책 저장소와 같은 곳에 배치됩니다.

- SNMP

정책 서버를 설치하기 전에 Windows 운영 체제에 SNMP 서비스(마스터 OS 에이전트)가 설치되었는지 확인하십시오.

참고: SNMP 서비스 설치에 대한 자세한 내용은 Windows 온라인 도움말 시스템을 참조하십시오.

- 감사 로그

감사 로그를 관계형 데이터베이스 또는 텍스트 파일에 저장할 수 있습니다. 정책 서버를 설치하면 감사 로깅이 ODBC 가 아닌 텍스트 파일로 기본 설정됩니다.

참고: 지원되는 CA 및 타사 구성 요소의 목록에 대해서는 기술 지원 사이트의 SiteMinder 12.52 SP1 Platform Support Matrix(플랫폼 지원표)를 참조하십시오.

정책 저장소 고려 사항

정책 서버 설치 관리자 또는 정책 서버 구성 마법사를 실행하기 전에 다음 사항을 고려하십시오.

- 정책 서버 설치 관리자와 정책 서버 구성 마법사는 다음 저장소 중 하나를 정책 저장소로 자동 구성할 수 있습니다.
 - Microsoft AD LDS(Active Directory Lightweight Directory Services)

참고: AD LDS 를 정책 저장소로 구성하기 위한 사전 요구 사항을 충족했는지 확인하십시오.
 - Oracle® Directory Enterprise Edition(이전의 Sun Java™ System Directory Server)

중요! 정책 서버 설치 관리자와 정책 서버 구성 마법사는 SSL 연결을 사용하여 연결되는 정책 저장소를 자동으로 구성할 수 없습니다.
 - Microsoft SQL Server®
 - Oracle RDBMS
- (RDB 정책 저장소) 정책 서버 설치 관리자 또는 정책 서버 구성 마법사는 특정 데이터베이스 정보를 사용하여 정책 저장소 데이터 원본을 생성합니다. 정책 서버는 이 데이터 원본을 기반으로 정책 저장소와 통신합니다. 다음 사항을 고려하십시오.
 - 데이터 원본의 이름은 CA SiteMinder DSN 입니다.
 - 설치 관리자는 데이터 원본을 Microsoft ODBC 데이터 원본 관리자 도구에서 "시스템 DSN" 탭 아래에 저장합니다.
- (RDB 정책 저장소) 정책 저장소를 호스트할 데이터베이스 서버가 UTF-8 형식으로 개체를 저장하도록 구성되었는지 확인하십시오. 이렇게 구성하면 정책 저장소가 손상되지 않도록 방지됩니다.
 - (Oracle) 데이터베이스가 UTF-8 형식으로 개체를 저장하도록 구성되었는지 확인하십시오. 대부분의 Oracle 문자 집합에서 유니코드가 지원됩니다. UTF-8 형식으로 개체를 저장하도록 데이터베이스를 구성하는 방법에 대한 자세한 내용은 공급업체별 설명서를 참조하십시오.
 - (SQL Server) 데이터베이스가 기본 데이터 정렬(SQL_Latin1_General_CP1_CI_AS)을 사용하여 구성되었는지 확인하십시오. 대/소문자를 구분하는 데이터 정렬을 사용하면 예기치 않은 동작이 발생할 수 있습니다. 기본 데이터 정렬을 사용하여 개체를 저장하도록 데이터베이스를 구성하는 방법에 대한 자세한 내용은 공급업체별 설명서를 참조하십시오.

- 인증서 데이터 원본은 자동으로 정책 저장소와 함께 배치됩니다.
- 지원되는 다른 디렉터리 서버 또는 관계형 데이터베이스는 정책 서버를 설치한 후 정책 저장소로 수동으로 구성해야 합니다. 정책 저장소를 수동으로 구성하는 방법은 이 문서에 자세히 설명되어 있습니다.

추가 정보:

[관계형 데이터베이스에 SiteMinder 데이터 저장소 구성](#) (페이지 301)

FIPS 고려 사항

정책 서버는 인증된 FIPS(Federal Information Processing Standard) 140-2 호환 암호화 라이브러리를 사용합니다. FIPS 는 AES(Advanced Encryption Standard)를 충족하는 암호화 모듈을 인가하는 데 사용되는 미국 정부의 컴퓨터 보안 표준입니다. 이러한 라이브러리는 SiteMinder 환경에서 중요한 데이터를 암호화하는 데 FIPS 호환 알고리즘만 사용하는 경우 FIPS 작동 모드를 제공합니다.

다음 FIPS 작동 모드 중 하나에서 정책 서버를 설치할 수 있습니다.

참고: 정책 서버가 작동하는 FIPS 모드는 시스템에 따라 다릅니다. 자세한 내용은 [기술 지원 사이트](#)의 "SiteMinder 12.52 SP1 Platform Support Matrix"(SiteMinder 12.52 SP1 플랫폼 지원표)를 참조하십시오.

- **FIPS 호환성 모드**-설치 중의 기본 FIPS 작동 모드는 FIPS 호환성 모드입니다. FIPS 호환성 모드에서는 환경이 기존 SiteMinder 알고리즘을 사용하여 중요한 데이터를 암호화하며 이전 버전의 SiteMinder 와 호환됩니다.
 - 사용자 환경에서 FIPS 호환 알고리즘을 사용하는 것은 선택 사항입니다.
 - 조직에서 FIPS 호환 알고리즘을 사용할 필요가 없는 경우 정책 서버를 FIPS 호환성 모드에서 설치하십시오. 추가 구성이 필요하지 않습니다.
- **FIPS 마이그레이션 모드** - FIPS 마이그레이션 모드를 사용하면 FIPS 호환성 모드에서 실행 중인 12.52 SP1 환경을 FIPS 전용 모드로 전환할 수 있습니다.

FIPS 마이그레이션 모드에서는 FIPS 호환 알고리즘만 사용하도록 12.52 SP1 환경을 마이그레이션할 때 12.52 SP1 정책 서버가 계속해서 기존 SiteMinder 암호화 알고리즘을 사용합니다.

FIPS 호환 알고리즘만 사용하도록 기존 환경을 구성 중인 경우 정책 서버를 FIPS 마이그레이션 모드에서 설치하십시오.

- **FIPS 전용 모드** - FIPS 전용 모드의 환경에서는 FIPS 호환 알고리즘만 사용하여 중요한 데이터를 암호화합니다.

기존 환경이 12.52 SP1 버전으로 업그레이드되고 FIPS 호환 알고리즘만 사용하도록 구성되는 경우 정책 서버를 FIPS 전용 모드에서 설치하십시오.

중요! FIPS 전용 모드에서 실행되는 12.52 SP1 환경은 FIPS 를 완전히 지원하지 않는 버전, 즉 r12.0 이전 버전의 SiteMinder 와 함께 운용될 수 없습니다. 이 제한은 모든 에이전트, 이전 버전의 에이전트 API 를 사용하는 사용자 지정 소프트웨어, PM API 나 정책 서버에서 노출하는 기타 API 를 사용하는 사용자 지정 소프트웨어에 적용됩니다. 필요한 FIPS 지원을 받으려면 이러한 모든 소프트웨어를 각 SDK 의 12.52 SP1 버전과 다시 연결하십시오.

참고: FIPS 호환 알고리즘만 사용하도록 환경을 마이그레이션하는 방법에 대한 자세한 내용은 *업그레이드 안내서*를 참조하십시오.

설치 관리자에 필요한 정보 수집

정책 서버 설치 관리자가 정책 서버와 선택적 구성 요소를 설치하는 데는 특정 정보가 필요합니다.

필요한 정보

정책 서버 설치 관리자 또는 구성 마법사를 실행하기 전에 다음과 같은 필요한 정보를 수집하십시오. 필요한 정보 워크시트를 사용하여 값을 기록할 수 있습니다.

- **Java 버전** - 정책 서버에서 사용할 지원되는 Java Runtime Environment 버전을 식별합니다. UNIX 에서는 JAVA_HOME 시스템 변수가 JRE 의 위치로 설정되었는지 확인하십시오. JAVA_HOME 시스템 변수가 잘못 설정된 경우 설치 관리자가 JRE 를 찾지 못합니다.

- **정책 서버 설치 위치** - 설치 관리자가 정책 서버를 설치할 위치를 확인합니다.

기본값: C:\Program Files\CA

- **SiteMinder 암호화 키 값** - 암호화 키 값을 확인합니다. 암호화 키는 정책 서버와 정책 저장소 간에 전송되는 데이터를 보호하는 대/소문자 구분 영숫자 키입니다. 정책 저장소를 공유하는 모든 정책 서버는 동일한 암호화 키를 사용해야 합니다. 보안을 강화하기 위해 긴 암호화 키를 정의하십시오.

제한: 6 자~24 자

- **고급 인증 서버 암호화 키 값** - 암호화 키 값을 확인합니다. 대/소문자 구분 영숫자 값을 사용합니다. 이 키는 정책 서버와 고급 인증 서버(CA SiteMinder for Secure Proxy Server 에서 실행) 간에 전송되는 데이터를 보호합니다. CA SiteMinder for Secure Proxy Server 와 모든 정책 서버에는 동일한 키가 필요합니다. 보안을 강화하기 위해 긴 암호화 키를 정의하십시오.

제한: 6 자~24 자

Active Directory LDS 서버 정보

Microsoft Active Directory LDS 를 정책 저장소로 구성하려면 다음과 같은 필요한 정보를 수집하십시오.

- **시스템 IP 주소** - 디렉터리 서버 호스트 시스템의 IP 주소를 식별합니다.
- **포트 번호** - 디렉터리 서버가 수신 대기하는 포트 번호를 식별합니다.
- **응용 프로그램 파티션의 루트 DN** - 디렉터리 서버에서 정책 저장소 스키마 데이터를 설치해야 하는 응용 프로그램 파티션의 루트 DN 위치를 식별합니다.

예: dc=ca,dc=com

- **관리자 도메인 이름** - 디렉터리 관리자의 guid 값을 포함한 전체 도메인 이름을 식별합니다.

예: CN=user1,CN=people,CN=Configuration,CN=guid

- **관리자 암호** - 디렉터리 관리자의 암호를 식별합니다.

- **대체 사용자 계정** - 기본적으로 SiteMinder 는 관리자 계정을 사용하여 디렉터리 서버와 통신합니다. 하지만 다른 사용자 계정을 이용하여 정책 저장소를 관리할 수 있습니다. 대체 사용자 계정을 사용하여 정책 저장소를 관리하도록 SiteMinder 를 구성하려면 완전한 관리자 DN 및 암호를 식별합니다.

참고: 이 사용자는 특성을 수정하고 암호를 변경하는 데 필요한 권한이 있어야 합니다.

- **SiteMinder 슈퍼 사용자 암호** - 기본 SiteMinder 슈퍼 사용자 계정은 최대 권한을 가집니다. 기본 슈퍼 사용자 계정의 암호를 확인합니다. 기본 계정의 이름은 다음과 같습니다.

siteminder

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: 일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 대신, 기본 슈퍼 사용자 계정을 사용하여 처음으로 관리 UI 에 액세스한 후 슈퍼 사용자 권한이 있는 관리자를 생성하십시오.

Oracle Directory Server 정보

Oracle Directory Server 를 정책 저장소로 작동하도록 구성하려면 다음과 같은 필요한 정보를 수집하십시오.

- **시스템 IP 주소** - Oracle Directory Server 호스트 시스템의 IP 주소를 확인합니다.
- **디렉터리 인스턴스 포트 번호** - Oracle Directory Server 인스턴스의 포트 번호를 확인합니다.

기본값: 389

- **루트 DN** - Oracle Directory Server 의 루트 DN 을 식별합니다.

예: o=yourorg.com

- **관리자 계정** - LDAP 관리자 계정의 사용자 이름(바인딩 DN)을 식별합니다.

예: cn=Directory Manager

- **관리자 암호** - Oracle Directory Server 관리자의 암호를 식별합니다.

- **대체 LDAP 관리자** - 기본적으로 SiteMinder 는 LDAP 관리자 계정을 사용하여 LDAP 서버와 통신합니다. 하지만 다른 LDAP 사용자 계정을 이용하여 정책 저장소를 관리할 수 있습니다. 이러한 방식으로 SiteMinder 를 구성하려면 완전한 관리자 DN 및 암호를 식별합니다.

참고: 이 사용자는 특성을 수정하고 암호를 변경하는 데 필요한 권한이 있어야 합니다.

- **SiteMinder 슈퍼 사용자 암호** - 기본 SiteMinder 슈퍼 사용자 계정은 최대 권한을 가집니다. 기본 슈퍼 사용자 계정의 암호를 확인합니다. 기본 계정의 이름은 다음과 같습니다.

siteminder

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: 일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 대신, 기본 슈퍼 사용자 계정을 사용하여 처음으로 관리 UI 에 액세스한 후 슈퍼 사용자 권한이 있는 관리자를 생성하십시오.

Microsoft SQL Server 정보

Microsoft SQL Server 를 정책 저장소로 구성하려면 다음과 같은 필요한 정보를 수집하십시오.

데이터베이스 서버 이름

데이터베이스 호스트 시스템의 IP 주소 또는 이름을 식별합니다.

참고: IPv6 지원에 대한 자세한 내용은 "SiteMinder Platform Support Matrix"(SiteMinder 플랫폼 지원표)를 참조하십시오.

데이터베이스 이름

정책 저장소로 작동할 데이터베이스의 이름 또는 명명된 인스턴스를 식별합니다.

데이터베이스 포트

데이터베이스가 수신 대기하는 포트를 식별합니다.

데이터베이스 관리자 사용자 이름 및 암호

다음 작업을 수행할 수 있는 권한이 있는 관리자 계정의 이름과 암호를 식별합니다.

- 스키마 만들기
- 개체 생성, 읽기, 수정 및 삭제

참고: 데이터베이스에 SiteMinder 스키마가 이미 있는 경우 마법사는 **create** 권한이 있는 데이터베이스 관리자의 자격 증명을 요구하지 않습니다. 자세한 내용은 [SQL Server 정책 저장소 구성](#) (페이지 326)을 참조하십시오.

SiteMinder 슈퍼 사용자 암호

기본 SiteMinder superuser 계정은 최대 권한을 갖습니다. 기본 슈퍼 사용자 계정의 암호를 확인합니다. 기본 계정의 이름은 다음과 같습니다.

siteminder

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: 일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 대신, 기본 슈퍼 사용자 계정을 사용하여 처음으로 관리 UI 에 액세스한 후 슈퍼 사용자 권한이 있는 관리자를 생성하십시오.

Oracle RDBMS 정보

Oracle RDBMS 를 정책 저장소로 구성하려면 다음과 같은 필요한 정보를 수집하십시오.

데이터베이스 서버 이름

데이터베이스 호스트 시스템의 IP 주소 또는 이름을 식별합니다.

참고: IPv6 지원에 대한 자세한 내용은 "SiteMinder Platform Support Matrix"(SiteMinder 플랫폼 지원표)를 참조하십시오.

데이터베이스 서비스 이름

정책 저장소로 작동할 데이터베이스의 서비스 이름을 식별합니다.

데이터베이스 포트

데이터베이스가 수신 대기하는 포트를 식별합니다.

데이터베이스 관리자 사용자 이름

다음 작업을 수행할 수 있는 권한이 있는 관리자 계정의 이름을 식별합니다.

- 스키마 만들기
- 개체 생성, 읽기, 수정 및 삭제

데이터베이스 관리자 암호

관리자 계정의 암호를 식별합니다.

SiteMinder 슈퍼 사용자 암호

기본 SiteMinder superuser 계정은 최대 권한을 갖습니다. 기본 슈퍼 사용자 계정의 암호를 확인합니다. 기본 계정의 이름은 다음과 같습니다.

siteminder

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: 일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 대신, 기본 슈퍼 사용자 계정을 사용하여 처음으로 관리 UI 에 액세스한 후 슈퍼 사용자 권한이 있는 관리자를 생성하십시오.

OneView 모니터 정보

OneView 모니터 정보는 OneView 모니터를 구성하려는 경우에만 수집하면 됩니다.

OneView 모니터를 구성하려면 다음과 같은 필요한 정보를 수집하십시오. OneView 모니터 정보 워크시트를 사용하여 값을 기록할 수 있습니다.

- **JDK 경로** - 필요한 JDK 버전의 경로를 식별합니다.
- **ServletExec 설치 디렉터리** - ServletExec 설치 디렉터리를 식별합니다.
- **ServletExec 포트 번호** - ServletExec 인스턴스의 포트 번호를 확인합니다.
- **Sun Java System 관리자 디렉터리** - 다음 정보를 확인합니다.

- Sun Java System 이 설치된 위치
- Sun Java System Web Server 가 설치된 위치

예: `/sunjavasystem_home/location`

sunjavasystem_home

Sun Java System 이 설치된 위치를 지정합니다.

location

Sun Java System Web Server 가 설치된 위치를 지정합니다.

- **여러 ServletExec 인스턴스** - ServletExec 인스턴스가 여러 개 있는 경우 OneView 모니터 GUI 를 구성할 인스턴스를 결정합니다.

정책 서버 설치 관리자 실행

기술 지원 사이트의 설치 미디어를 사용하여 정책 서버를 설치하십시오.

참고: 설치 미디어 이름의 목록에 대해서는 *정책 서버 릴리스 정보*를 참조하십시오.

다음 단계를 수행하십시오.

1. 시스템이 Windows 요구 사항을 충족하는지 확인합니다.
2. 실행 중인 응용 프로그램을 모두 종료합니다.
3. 사용 중인 Windows 버전에 적절한 단계를 수행합니다.
 - **Windows 2008 및 Windows 7:** *installation_media* 를 마우스 오른쪽 단추로 클릭하고 "관리자 권한으로 실행"을 선택합니다.
 - **기타 Windows 버전:** *installation_media* 를 두 번 클릭합니다.

installation_media

정책 서버 설치 실행 파일의 이름을 지정합니다.

설치 관리자가 시작됩니다.

4. 수집된 시스템 및 구성 요소 정보를 사용하여 정책 서버를 설치하고 정책 서버 구성 요소를 구성합니다. 설치 관리자를 실행할 때는 다음 사항을 고려하십시오.
 - FIPS 작동 모드를 선택하라는 메시지가 표시됩니다. 선택할 FIPS 모드에 대한 자세한 내용은 [FIPS 고려 사항](#) (페이지 36)을 참조하십시오.
 - 구성 요소를 선택하라는 메시지가 표시되면 정책 저장소를 자동으로 구성하지 않으려는 경우에는 "정책 저장소" 확인란의 선택을 취소하십시오. 정책 저장소로 자동 구성될 수 있는 저장소에 대한 자세한 내용은 [정책 저장소 고려 사항](#) (페이지 35)을 참조하십시오.
 - 정책 저장소를 초기화하는 경우 기본 SiteMinder 사용자 계정에 대한 암호를 입력하라는 메시지가 표시됩니다. 기본 계정 이름은 다음과 같습니다.
`siteminder`
 - 기본 인증 기관 인증서를 인증서 데이터 저장소에 설치하라는 메시지가 표시됩니다. 설치 후에 추가 인증서와 개인 키를 인증서 데이터 저장소에 추가할 수 있습니다.
 - IPv6 주소를 사용하는 경우에는 항목을 대괄호로 묶으십시오.
예: [2001:db8::1428:57ab]
 - 고급 인증 서버에 대한 암호화 키를 생성하십시오. 사용하는 환경의 모든 정책 서버에서 동일한 키를 사용하십시오.

5. 설치 설정을 검토하고 "설치"를 클릭합니다.

정책 서버 및 선택한 모든 구성 요소가 설치되고 구성됩니다.

6. (선택 사항) 설치 관리자를 사용하여 정책 저장소를 구성하지 않은 경우 정책 저장소를 수동으로 구성하십시오.

참고: 설치 도중 문제가 발생하는 경우

`siteminder_home\siteminder\install_config_info` 에서 설치 로그 파일과 정책 저장소 상세 정보 파일을 찾을 수 있습니다.

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

SNMP 이벤트 트래핑이 사용되도록 설정

이 작업은 선택적 단계입니다. 정책 서버를 설치할 때 SNMP 트래핑을 구성한 경우에만 이 기능이 사용되도록 설정하면 됩니다.

참고: 이 절차를 완료하기 전에 Windows 시스템에 SNMP 서비스가 설치되어 있는지 확인하십시오.

SNMP 이벤트 트래핑이 사용되도록 설정하려면 XPSConfig 유틸리티를 사용하여 이벤트 처리기 라이브러리(eventsnmp.dll)를 XPSAudit 목록으로 설정하십시오. eventsnmp.dll 의 기본 위치는 `policy_server_home\bin` 입니다.

`policy_server_home`

정책 서버 설치 위치를 지정합니다.

참고: XPSConfig 유틸리티를 사용하여 이벤트 처리기 라이브러리를 설정하는 방법에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

SNMP 이벤트 트래핑 구성을 마치려면 `snmptrap.conf` 파일을 구성하십시오. 필요한 SNMP 필수 구성 요소 및 절차에 대한 자세한 내용은 "SNMP 지원"을 참조하십시오.

추가 정보:

[SNMP 지원 개요](#) (페이지 529)

정책 서버 설치 문제 해결

다음 파일을 사용하여 정책 서버 설치 문제를 해결하십시오.

- **CA_SiteMinder_Policy_Server_release_InstallLog.log**

이 설치 로그에는 설치 중에 발생한 오류, 심각하지 않은 오류, 경고, 성공의 수를 보여 주는 요약 섹션이 포함됩니다. 개별 설치 작업이 해당 상태와 함께 표시됩니다.

release

정책 서버 릴리스를 지정합니다.

위치: *siteminder_home*\siteminder\install_config_info

- **ca-ps-details.log**

정책 저장소 로그는 정책 저장소 상태 정보를 제공합니다.

위치: *siteminder_home*\siteminder\install_config_info

- **smps.log**

정책 서버를 시작하면 **smps.log** 가 생성됩니다. 정책 서버가 성공적으로 설치되었을 경우 이 로그에는 다음과 같은 줄이 포함됩니다.

[Info] Journaling thread started, will delete commands older than 60 minutes.

위치: *siteminder_home*\siteminder\log

siteminder_home

정책 서버 설치 경로를 지정합니다.

정책 서버 구성 마법사

정책 서버를 설치한 후 정책 서버 구성 마법사를 사용하여 다음 구성 요소를 구성 또는 재구성합니다.

- 정책 저장소 하나
- SNMP 지원
- OneView 모니터 UI

참고: 정책 서버 구성 마법사를 사용하여 정책 서버 **FIPS** 작업 모드를 변경할 수는 없습니다. 정책 서버 **FIPS** 작업 모드 변경에 대한 자세한 내용은 *SiteMinder 업그레이드 안내서*를 참조하십시오.

중요! OneView 모니터 UI 또는 SNMP 에 대해 Oracle iPlanet 웹 서버 인스턴스를 구성한 경우 마법사를 사용하여 새 인스턴스를 구성하지 마십시오. 새로운 웹 서버 인스턴스를 구성하면 기존 웹 서버 인스턴스가 실패할 수 있습니다.

추가 정보:

[정책 저장소 고려 사항](#) (페이지 35)

구성 마법사를 사용하는 방법

정책 서버 구성 마법사를 사용하려면 다음 절차를 완료하십시오.

1. [정책 저장소 고려 사항](#) (페이지 35)을 검토합니다.
2. 정책 저장소로 다음 저장소 중 하나를 구성하거나 OneView 모니터 UI 를 구성하려는 경우 마법사에서 필요한 정보를 수집합니다.
 - Active Directory LDS
 - Oracle Directory Server
 - SQL Server
 - Oracle RDBMS
3. 마법사를 실행합니다.

구성 마법사에 필요한 정보 수집

정책 서버 구성 마법사가 정책 서버 구성 요소를 구성하는 데는 특정 정보가 필요합니다.

참고: 정책 서버 설치 마법사 또는 정책 서버 구성 마법사를 사용하여 정책 서버 구성 요소를 설치하거나 구성하기 전에 정보를 수집 및 기록하는 데 유용한 설치 워크시트가 제공됩니다. 두 마법사를 실행하기 전에 이 워크시트를 인쇄하여 필요한 정보를 기록할 수 있습니다.

Active Directory LDS 서버 정보

Microsoft Active Directory LDS 를 정책 저장소로 구성하려면 다음과 같은 필요한 정보를 수집하십시오.

- **시스템 IP 주소** - 디렉터리 서버 호스트 시스템의 IP 주소를 식별합니다.
- **포트 번호** - 디렉터리 서버가 수신 대기하는 포트 번호를 식별합니다.
- **응용 프로그램 파티션의 루트 DN** - 디렉터리 서버에서 정책 저장소 스키마 데이터를 설치해야 하는 응용 프로그램 파티션의 루트 DN 위치를 식별합니다.

예: dc=ca,dc=com

- **관리자 도메인 이름** - 디렉터리 관리자의 guid 값을 포함한 전체 도메인 이름을 식별합니다.

예: CN=user1,CN=people,CN=Configuration,CN=guid

- **관리자 암호** - 디렉터리 관리자의 암호를 식별합니다.
- **대체 사용자 계정** - 기본적으로 SiteMinder 는 관리자 계정을 사용하여 디렉터리 서버와 통신합니다. 하지만 다른 사용자 계정을 이용하여 정책 저장소를 관리할 수 있습니다. 대체 사용자 계정을 사용하여 정책 저장소를 관리하도록 SiteMinder 를 구성하려면 완전한 관리자 DN 및 암호를 식별합니다.

참고: 이 사용자는 특성을 수정하고 암호를 변경하는 데 필요한 권한이 있어야 합니다.

- **SiteMinder 슈퍼 사용자 암호** - 기본 SiteMinder 슈퍼 사용자 계정은 최대 권한을 가집니다. 기본 슈퍼 사용자 계정의 암호를 확인합니다. 기본 계정의 이름은 다음과 같습니다.

siteminder

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: 일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 대신, 기본 슈퍼 사용자 계정을 사용하여 처음으로 관리 UI 에 액세스한 후 슈퍼 사용자 권한이 있는 관리자를 생성하십시오.

Oracle Directory Server 정보

Oracle Directory Server 를 정책 저장소로 작동하도록 구성하려면 다음과 같은 필요한 정보를 수집하십시오.

- **시스템 IP 주소** - Oracle Directory Server 호스트 시스템의 IP 주소를 확인합니다.
- **디렉터리 인스턴스 포트 번호** - Oracle Directory Server 인스턴스의 포트 번호를 확인합니다.

기본값: 389

- **루트 DN** - Oracle Directory Server 의 루트 DN 을 식별합니다.

예: o=yourorg.com

- **관리자 계정** - LDAP 관리자 계정의 사용자 이름(바인딩 DN)을 식별합니다.

예: cn=Directory Manager

- **관리자 암호** - Oracle Directory Server 관리자의 암호를 식별합니다.

- **대체 LDAP 관리자** - 기본적으로 SiteMinder 는 LDAP 관리자 계정을 사용하여 LDAP 서버와 통신합니다. 하지만 다른 LDAP 사용자 계정을 이용하여 정책 저장소를 관리할 수 있습니다. 이러한 방식으로 SiteMinder 를 구성하려면 완전한 관리자 DN 및 암호를 식별합니다.

참고: 이 사용자는 특성을 수정하고 암호를 변경하는 데 필요한 권한이 있어야 합니다.

- **SiteMinder 슈퍼 사용자 암호** - 기본 SiteMinder 슈퍼 사용자 계정은 최대 권한을 가집니다. 기본 슈퍼 사용자 계정의 암호를 확인합니다. 기본 계정의 이름은 다음과 같습니다.

siteminder

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: 일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 대신, 기본 슈퍼 사용자 계정을 사용하여 처음으로 관리 UI 에 액세스한 후 슈퍼 사용자 권한이 있는 관리자를 생성하십시오.

Microsoft SQL Server 정보

Microsoft SQL Server 를 정책 저장소로 구성하려면 다음과 같은 필요한 정보를 수집하십시오.

데이터베이스 서버 이름

데이터베이스 호스트 시스템의 IP 주소 또는 이름을 식별합니다.

참고: IPv6 지원에 대한 자세한 내용은 "SiteMinder Platform Support Matrix"(SiteMinder 플랫폼 지원표)를 참조하십시오.

데이터베이스 이름

정책 저장소로 작동할 데이터베이스의 이름 또는 명명된 인스턴스를 식별합니다.

데이터베이스 포트

데이터베이스가 수신 대기하는 포트를 식별합니다.

데이터베이스 관리자 사용자 이름 및 암호

다음 작업을 수행할 수 있는 권한이 있는 관리자 계정의 이름과 암호를 식별합니다.

- 스키마 만들기
- 개체 생성, 읽기, 수정 및 삭제

참고: 데이터베이스에 SiteMinder 스키마가 이미 있는 경우 마법사는 **create** 권한이 있는 데이터베이스 관리자의 자격 증명을 요구하지 않습니다. 자세한 내용은 [SQL Server 정책 저장소 구성](#) (페이지 326)을 참조하십시오.

SiteMinder 슈퍼 사용자 암호

기본 SiteMinder superuser 계정은 최대 권한을 갖습니다. 기본 슈퍼 사용자 계정의 암호를 확인합니다. 기본 계정의 이름은 다음과 같습니다.

siteminder

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: 일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 대신, 기본 슈퍼 사용자 계정을 사용하여 처음으로 관리 UI에 액세스한 후 슈퍼 사용자 권한이 있는 관리자를 생성하십시오.

Oracle RDBMS 정보

Oracle RDBMS를 정책 저장소로 구성하려면 다음과 같은 필요한 정보를 수집하십시오.

데이터베이스 서버 이름

데이터베이스 호스트 시스템의 IP 주소 또는 이름을 식별합니다.

참고: IPv6 지원에 대한 자세한 내용은 "SiteMinder Platform Support Matrix"(SiteMinder 플랫폼 지원표)를 참조하십시오.

데이터베이스 서비스 이름

정책 저장소로 작동할 데이터베이스의 서비스 이름을 식별합니다.

데이터베이스 포트

데이터베이스가 수신 대기하는 포트를 식별합니다.

데이터베이스 관리자 사용자 이름

다음 작업을 수행할 수 있는 권한이 있는 관리자 계정의 이름을 식별합니다.

- 스키마 만들기
- 개체 생성, 읽기, 수정 및 삭제

데이터베이스 관리자 암호

관리자 계정의 암호를 식별합니다.

SiteMinder 슈퍼 사용자 암호

기본 SiteMinder superuser 계정은 최대 권한을 갖습니다. 기본 슈퍼 사용자 계정의 암호를 확인합니다. 기본 계정의 이름은 다음과 같습니다.

siteminder

제한:

- 암호는 적어도 6자보다 길어야 하며 24자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: 일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 대신, 기본 슈퍼 사용자 계정을 사용하여 처음으로 관리 UI에 액세스한 후 슈퍼 사용자 권한이 있는 관리자를 생성하십시오.

OneView 모니터 정보

OneView 모니터 정보는 OneView 모니터를 구성하려는 경우에만 수집하면 됩니다.

OneView 모니터를 구성하려면 다음과 같은 필요한 정보를 수집하십시오. OneView 모니터 정보 워크시트를 사용하여 값을 기록할 수 있습니다.

- **JDK 경로** - 필요한 JDK 버전의 경로를 식별합니다.
- **ServletExec 설치 디렉터리** - ServletExec 설치 디렉터리를 식별합니다.
예: `/usr/local/NewAtlanta/ServletExecAS`
- **ServletExec 포트 번호** - ServletExec 인스턴스의 포트 번호를 확인합니다.
- **Sun Java System 관리자 디렉터리** - 다음 정보를 확인합니다.

- Sun Java System 이 설치된 위치
- Sun Java System Web Server 가 설치된 위치

예: `/sunjavasystem_home/location`

sunjavasystem_home

Sun Java System 이 설치된 위치를 지정합니다.

location

Sun Java System Web Server 가 설치된 위치를 지정합니다.

- **여러 ServletExec 인스턴스** - ServletExec 인스턴스가 여러 개 있는 경우 OneView 모니터 GUI 를 구성할 인스턴스를 결정합니다.

구성 마법사 실행

구성 마법사를 실행하려면

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. `siteminder_home\siteminder\install_config_info` 로 이동하여 `ca-ps-config.exe` 를 두 번 클릭합니다.

정책 서버 구성 마법사가 시작됩니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

중요! 이 마법사를 Windows Server 2008 에서 실행하는 경우 관리자 권한을 사용하여 실행 파일을 실행하십시오. 관리자로 시스템에 로그인한 경우에도 이 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

3. 수집한 시스템 및 구성 요소 정보를 사용하여 정책 저장소와 개별 구성 요소를 구성합니다.

참고: LDAP 인스턴스를 초기화할지 묻는 메시지가 나타나면 새 정책 저장소 인스턴스를 구성하려는 경우에만 해당 작업을 수행합니다.

4. 설치 설정을 검토하고 "설치"를 클릭합니다.

선택한 구성 요소가 정책 서버와 작동하도록 구성됩니다.

참고: 이 과정은 몇 분 정도 걸립니다.

5. "Done"(완료)을 클릭하고 시스템을 재부팅합니다.

선택한 구성 요소가 구성되었습니다.

참고: 문제가 발생할 경우

`siteminder_home\siteminder\install_config_info` 에서 정책 서버 설치 로그 파일과 정책 저장소 상세 정보 파일을 찾아 검토하십시오.

siteminder_home

정책 서버 설치 경로를 지정합니다.

추가 정보:

[정책 서버 설치 문제 해결](#) (페이지 46)

정책 서버 다시 설치

기존 정책 서버 위에 동일 버전의 정책 서버를 다시 설치하면 손실된 응용 프로그램 파일을 복원하거나 정책 서버의 기본 설치 설정을 복원할 수 있습니다.

정책 서버를 다시 설치하려면

1. 정책 서버 관리 콘솔을 사용하여 정책 서버를 중지합니다.
참고: 정책 서버 중지 및 시작에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.
2. 정책 서버 관리 콘솔을 닫습니다.
3. 정책 서버를 설치합니다.
4. 정책 서버 관리 콘솔을 사용하여 정책 서버를 시작합니다.

Windows 에서 정책 서버 제거 방법

정책 서버를 제거하려면 다음 절차를 완료하십시오.

1. Path 시스템 변수에 JRE 를 설정합니다.
2. 정책 서버 관리 콘솔의 모든 인스턴스를 종료합니다.
3. 에이전트 호스트 파일에서 정책 서버 참조를 제거합니다.
4. 정책 서버를 제거합니다.

Path 변수에 JRE 설정

정책 서버, 웹 에이전트 및 SDK 를 제거할 때는 path 변수에 JRE 를 설정하여 제거 프로그램이 중지되고 다음 오류 메시지 중 하나가 발생하지 않도록 하십시오.

- "Could not find a valid Java virtual machine to load. You need to reinstall a supported Java virtual machine." (로드할 유효한 Java Virtual Machine 을 찾을 수 없습니다. 지원되는 Java Virtual Machine 을 다시 설치해야 합니다.)
- "No Java virtual machine could be found from your PATH environment variable. You must install a VM prior to running this program." (PATH 환경 변수에서 Java Virtual Machine 을 찾을 수 없습니다. 이 프로그램을 실행하기 전에 VM 을 설치해야 합니다.)

path 변수에 JRE 를 설정하려면

1. Windows 제어판을 엽니다.
2. "시스템"을 두 번 클릭합니다.
3. "환경 변수" 대화 상자에서 PATH 시스템 변수에 JRE 의 위치를 추가합니다.

에이전트 호스트 파일에서 정책 서버 참조 제거

정책 서버를 제거한 후 웹 에이전트에서 예기치 못한 결과가 발생하지 않도록 SmHost.conf 파일에서 정책 서버 참조를 제거하십시오.

정책 서버 참조를 제거하려면

1. `web_agent_home/config` 로 이동합니다.

web_agent_home

웹 에이전트의 설치 디렉터리를 지정합니다.

2. 텍스트 편집기에서 SmHost.conf 파일을 엽니다.

3. "policyserver="로 시작하는 행을 삭제합니다.

참고: 이 행에는 제거할 정책 서버의 IP 주소 및 포트 번호가 포함되어 있습니다.

4. SmHost.conf 를 저장합니다.

이제 SmHost.conf 파일은 제거할 정책 서버를 더 이상 참조하지 않습니다.

모든 SiteMinder 프로세스 중지

정책 서버를 제거하려면 먼저 정책 서버 파일이 안전하게 제거되도록 모든 SiteMinder 프로세스를 중지하십시오.

다음 단계를 수행하십시오.

1. Windows 시스템에 로그인합니다.
2. "관리 도구"에서 "서비스"를 엽니다.
3. 아래로 스크롤하여 SiteMinder 정책 서버 서비스를 찾아 "중지"를 선택합니다.

모든 SiteMinder 프로세스가 중지됩니다.

정책 서버 제거

시스템에서 더 이상 필요하지 않을 경우 정책 서버를 제거하십시오.

다음 단계를 수행하십시오.

1. Windows 제어판을 열고 프로그램 목록으로 이동합니다.
2. CA SiteMinder 정책 서버를 마우스 오른쪽 단추로 클릭합니다.
3. "제거/변경"을 클릭합니다.
4. 마법사의 지시를 따릅니다.

참고: 공유 파일을 제거할지 묻는 메시지가 표시되면 "No to All"(모두 아니요)을 클릭합니다.

5. 필요한 경우 시스템을 재부팅합니다.

정책 서버가 제거되었습니다.

남은 항목 제거

정책 서버를 제거한 후에는 다음과 같은 폴더, 파일, 레지스트리 설정 및 가상 디렉터리를 수동으로 제거하십시오.

- **Windows 시스템**

- `siteminder_home\bin`
- `siteminder_home\install_config_info`
- `C:\Program Files\ZeroG Registry\com.zerog.registry.xml`

중요! 정책 서버를 다시 설치하기 전에 모든 항목을 제거하십시오.

- **AdventNet 소프트웨어 레지스트리 항목** - 정책 서버를 설치하기 전에 AdventNet 소프트웨어가 시스템에 없는 경우에만 AdventNet 소프트웨어 레지스트리 항목을 삭제합니다. 이 레지스트리 항목은 `HKEY_LOCAL_MACHINE\SOFTWARE\Advent,Inc` 에 있습니다.
- **IIS 가상 디렉터리** - IIS Microsoft 관리 콘솔을 사용하여 다음 SiteMinder 가상 디렉터를 삭제합니다.
 - 'SiteMinder'
 - 'SiteMinderCgi'
 - 'SiteMinderMonitor'
 - 'netegrity_docs'

남은 서비스 제거

정책 서버를 제거하고 컴퓨터를 재부팅한 후에도 다음 서비스가 제거되지 않고 남아 있을 수 있습니다.

- SiteMinder 건전성 모니터 서비스
- SiteMinder 정책 서버
- SNMP 에이전트

남은 서비스를 수동으로 제거하려면

1. 각 서비스를 중지합니다.
2. 필요에 따라 다음 Windows 레지스트리 키를 제거합니다.

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<Registry_Key_Name>`

Registry_Key_Name

제거할 서비스의 레지스트리 키 이름을 지정합니다.

- SMServMon(SiteMinder 건전성 모니터 서비스)
- SMPolicySrv(SiteMinder 정책 서버)
- Agent Service(SNMP 에이전트)

남은 서비스가 제거됩니다.

스크립팅 인터페이스

명령줄 인터페이스를 사용하여 정책 저장소를 구성하고 관리하는 Perl 스크립트를 작성할 수 있습니다. 설치 프로그램은 Perl 전체 버전을 설치하고 인터페이스 파일을 *siteminder_installation/CLI* 디렉터리에 저장합니다.

siteminder_installation

SiteMinder 가 설치된 위치를 지정합니다.

예: `/home/smuser/siteminder/CLI`

명령줄 인터페이스를 사용하려면 컴퓨터의 PATH 환경 변수에서 다음 디렉터리가 컴퓨터의 다른 Perl bin 디렉터리 앞에 있는지 확인하십시오.

예: `/home/smuser/siteminder/CLI/bin`

참고: 스크립팅 인터페이스에 대한 자세한 내용은 *Programming Guide for Perl*(Perl 프로그래밍 안내서)을 참조하십시오.

제 5 장: UNIX 시스템에 정책 서버 설치

이 섹션은 다음 항목을 포함하고 있습니다.

[설치 로드맵](#) (페이지 60)

[Solaris 10 영역 지원](#) (페이지 61)

[정책 서버 설치를 준비하는 방법](#) (페이지 63)

[UNIX 에서 정책 서버 설치 전 고려 사항](#) (페이지 68)

[UNIX 에서 정책 서버 설치 방법](#) (페이지 69)

[정책 서버 설치 문제 해결](#) (페이지 85)

[자동 시작 구성](#) (페이지 85)

[정책 서버 구성 마법사](#) (페이지 86)

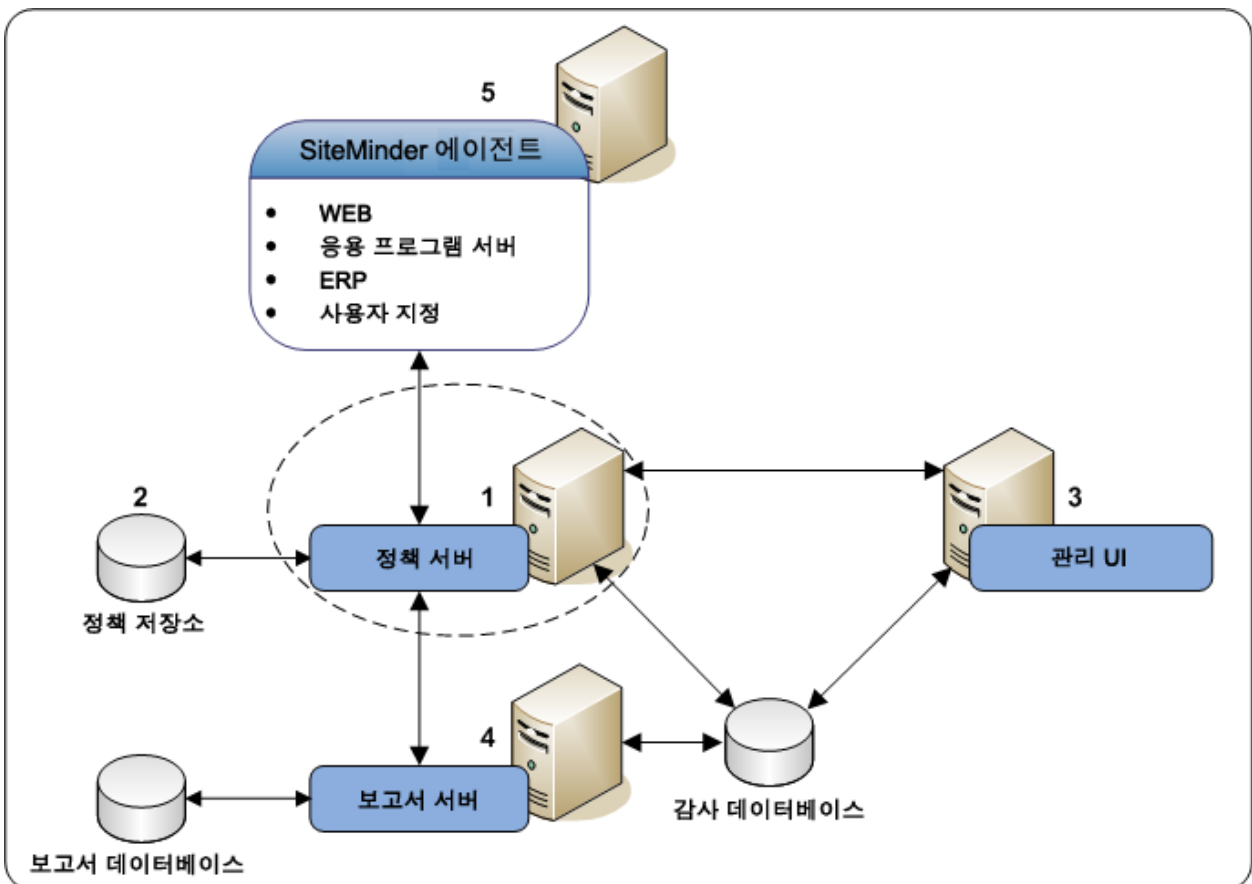
[UNIX 에서 정책 서버 제거 방법](#) (페이지 90)

설치 로드맵

다음 다이어그램에서는 샘플 SiteMinder 설치를 보여 주고 각 구성 요소를 설치 및 구성하는 순서를 나열합니다. 다음 사항을 고려하십시오.

- 정책 서버 호스트 시스템이 최소 시스템 요구 사항을 충족하는지 확인합니다. 정책 서버를 설치하기 전에 확인하는 것이 좋습니다.
- 점선으로 둘러싸인 부분은 정책 서버입니다. 지금 이 구성 요소를 설치합니다.

그림 2: 설치 로드맵



Solaris 10 영역 지원

다음은 SiteMinder 정책 서버가 지원되는 영역입니다.

- 전역 영역
- 스파스 루트 영역
- 전체 루트 영역

Solaris 10 환경에서 정책 서버를 하나 이상 실행하려는 경우 다음 시나리오를 고려하십시오.

전역 영역 지원

전역 영역 구성을 사용하면 모든 영역에서 단일 정책 서버 인스턴스만 구현할 수 있습니다. 구체적인 사항은 다음과 같습니다.

- 전역 영역에서 단일 정책 서버 인스턴스만 지원됩니다.
- 전역 영역에 다른 정책 서버 인스턴스가 있으면 스파스 루트 영역에서는 정책 서버 인스턴스가 지원되지 않습니다.
- 전역 영역에 다른 정책 서버 인스턴스가 있으면 전체 루트 영역에서는 정책 서버 인스턴스가 지원되지 않습니다.

예: 전역 영역 지원

스파스 루트 또는 전체 루트 영역 1 (정책 서버가 지원되지 않음)	스파스 루트 또는 전체 루트 영역 2 (정책 서버가 지원되지 않음)	스파스 루트 또는 전체 루트 영역 3 (정책 서버가 지원되지 않음)
전역 영역 (정책 서버 1)		

참고: 하지만 웹 에이전트는 어느 영역에서나 동시에 실행될 수 있습니다.

스파스 루트 영역 지원

스파스 루트 영역 구성을 사용할 경우 여러 스파스 루트 영역에서 여러 정책 서버 인스턴스를 실행할 수 있습니다. 구체적인 사항은 다음과 같습니다.

- 각 스파스 루트 영역에서 정책 서버 인스턴스가 하나씩만 지원됩니다.
- 각 스파스 루트 영역 또는 전체 루트 영역에 정책 서버 인스턴스가 하나씩만 있는 경우에 한해 스파스 루트 영역과 전체 루트 영역에서 동시 정책 서버 인스턴스가 지원됩니다.
- 정책 서버 인스턴스를 전역 영역과 스파스 루트 영역에서 동시에 실행할 수는 없습니다.

예: 스파스 루트 영역 지원

스파스 루트 영역 1 (정책 서버 1)	스파스 루트 영역 2 (정책 서버 2)	스파스 루트 영역 3 (정책 서버 3)	스파스 루트 영역 1 (정책 서버 4)
전역 영역 (정책 서버가 지원되지 않음)			

참고: 하지만 웹 에이전트는 어느 영역에서나 동시에 실행될 수 있습니다.

전체 루트 영역 지원

전체 루트 영역 구성을 사용할 경우 여러 전체 루트 영역에서 여러 정책 서버 인스턴스를 실행할 수 있습니다. 구체적인 사항은 다음과 같습니다.

- 각 전체 루트 영역에서 정책 서버 인스턴스가 하나씩만 지원됩니다.
- 각 전체 루트 영역 또는 스파스 루트 영역에 정책 서버 인스턴스가 하나씩만 있는 경우에 한해 전체 루트 영역과 스파스 루트 영역에서 동시 정책 서버 인스턴스가 지원됩니다.
- 정책 서버 인스턴스를 전역 영역과 전체 루트 영역에서 동시에 실행할 수는 없습니다.

예: 전체 루트 영역 지원

스파스 루트 영역 1 (정책 서버 1)	스파스 루트 영역 2 (정책 서버 2)	스파스 루트 영역 3 (정책 서버 3)	스파스 루트 영역 1 (정책 서버 4)
전역 영역 (정책 서버가 지원되지 않음)			

참고: 하지만 웹 에이전트는 어느 영역에서나 동시에 실행될 수 있습니다.

정책 서버 설치를 준비하는 방법

UNIX 시스템에서 정책 서버를 설치하기 전에 해당하는 경우 다음 단계를 완료하십시오.

1. 정책 서버 호스트 시스템이 최소 운영 체제 패치 요구 사항을 충족하는지 확인합니다. 자세한 내용은 *정책 서버 릴리스 정보*를 참조하십시오.
2. (Red Hat Linux) Red Hat 운영 체제는 성능을 위해 엔트로피를 사용합니다. 구성 요소를 설치하기 전에 엔트로피를 늘리십시오. 엔트로피가 충분하지 않으면 설치를 완료하는 데 시간이 매우 오래 걸릴 수 있습니다. 다음 명령을 사용하십시오.

```
mv /dev/random /dev/random.org
ln -s /dev/urandom /dev/random
```

3. (Linux) 필요한 Linux 라이브러리가 정책 서버 호스트 시스템에 설치되었는지 확인하십시오.
4. 새로운 UNIX 계정을 생성합니다.
5. UNIX 시스템 매개 변수를 수정합니다.
6. 지역화 변수를 설정하지 않습니다.
7. LANG 환경 변수를 설정하지 않습니다.

필요한 Linux 라이브러리

Linux 운영 환경에서 작동하는 구성 요소의 경우 특정 라이브러리 파일이 필요합니다. 올바른 라이브러리를 설치하지 못하면 다음과 같은 오류가 발생할 수 있습니다.

```
java.lang.UnsatisfiedLinkError
```

이 구성 요소의 Linux 버전을 설치, 구성 또는 업그레이드하는 경우 호스트 시스템에 다음 패키지가 필요합니다.

Red Hat 5.x:

- `compat-gcc-34-c++-3.4.6-patch_version.i386`
- `libstdc++-4.x.x-x.el5.i686.rpm`
- `libidn.so.11.rpm`
- `ncurses`

Red Hat 6.x:

- libstdc++-4.x.x-x.el6.i686.rpm
- libidn-1.18-2.el6.i686
- libXext.i686.rpm
- libXrender.i686.rpm
- libXtst.i686.rpm
- libidn.so.11.rpm
- ncurses

또한 Red Hat 6.x(64 비트)의 경우:

64 비트 Red Hat 6.x 에 필요한 모든 RPM 패키지는 32 비트 패키지입니다.

- libXau-1.0.5-1.el6.i686.rpm
- libxcb-1.5-1.el6.i686.rpm
- compat-db42-4.2.52-15.el6.i686.rpm
- compat-db43-4.3.29-15.el6.i686.rpm
- libX11-1.3-2.el6.i686.rpm
- libXrender-0.9.5-1.el6.i686.rpm
- libexpat.so.1(expat-2.0.1-11.el6_2.i686.rpm 에서 제공)
- libfreetype.so.6(freetype-2.3.11-6.el6_2.9.i686.rpm 에서 제공)
- libfontconfig.so.1(fontconfig-2.8.0-3.el6.i686.rpm 에서 제공)
- libICE-1.0.6-1.el6.i686.rpm
- libuuid-2.17.2-12.7.el6.i686.rpm
- libSM-1.1.0-7.1.el6.i686.rpm
- libXext-1.1-3.el6.i686.rpm
- compat-libstdc++-33-3.2.3-69.el6.i686.rpm
- compat-db-4.6.21-15.el6.i686.rpm
- libXi-1.3-3.el6.i686.rpm
- libXtst-1.0.99.2-3.el6.i686.rpm
- libXft-2.1.13-4.1.el6.i686.rpm
- libXt-1.0.7-1.el6.i686.rpm
- libXp-1.0.0-15.1.el6.i686.rpm

- libstdc++.i686.rpm
- compat-libtermcap.rpm
- libidn.i686.rpm
- ncurses

Linux 에서 Korn 셸(ksh) 패키지가 필요함

Linux 플랫폼에서 정책 서버를 설치 및 업그레이드하는 중에 ksh Korn 셸이 필요합니다. 사용하는 Linux 환경에 대한 적절한 버전이 설치되어 있는지 확인하십시오.

Red Hat 5.x 32 비트

ksh-20100621-12.el5.i386.rpm

Red Hat 5.x 64 비트

ksh-20100621-12.el5.x86_64.rpm

Red Hat 6.x 32 비트

ksh-20100621-16.el6.i686.rpm

Red Hat 6.x 64 비트

ksh-20100621-16.el6.x86_64.rpm

새 UNIX 계정 만들기

ksh 로 기본 셸을 사용하여 UNIX 계정을 생성합니다. 다음과 같이 계정 이름을 지정합니다.

smuser

중요! 다음 웹 서버에서는 설치 관리자를 사용하여 OneView 모니터 UI 를 구성하지 마십시오.

- Oracle iPlanet
- Linux 의 Apache

설치 관리자가 웹 서버의 구성 파일을 수정합니다. 새로운 UNIX 계정에는 필요한 루트 권한이 없습니다.

정책 서버를 설치한 후 정책 서버 구성 마법사를 루트로 사용하여 OneView 모니터 UI 를 구성하십시오.

UNIX 시스템 매개 변수 수정

부하가 있는 상태에서 정책 서버를 배치하면 대량의 소켓과 파일을 엽니다. 기본 제한 매개 변수가 이러한 부하에 적절하지 않을 경우 대량의 소켓과 파일은 문제가 될 수 있습니다. 관련 문제를 방지하려면 기본 제한 매개 변수를 수정하십시오.

기본 제한 매개 변수를 보려면 셸 창에서 다음 명령을 입력하십시오.

```
ulimit -a
```

다음 예와 비슷한 메시지가 표시됩니다.

```
$ ulimit -a
time(seconds)                unlimited
file(blocks)                  unlimited
data(kbytes)                   2097148
stack(kbytes)                  8192
coredump(blocks)               unlimited
nofiles(descriptor s)         256
vmemory(kbytes)                unlimited
```

이 예에서 **nofiles** 매개 변수는 **256** 으로 설정되었습니다. 이 매개 변수는 이 셸과 하위 셸에서 할당된 총 파일 수(소켓 + 파일 설명자)입니다. 이 매개 변수가 충분히 높지 않으면 정책 서버에서 수많은 소켓 오류를 반환합니다. 가장 일반적인 소켓 오류는 **10024** 오류, 즉 "열린 파일이 너무 많습니다." 오류입니다.

부하가 있는 적절한 정책 서버 작업에 대해 `nofiles` 매개 변수 값을 늘리십시오. 다음 명령을 실행하여 이 값을 변경할 수 있습니다.

```
ulimit -n
```

예를 들어 값을 `1024` 로 설정하려면 다음 명령을 `smuser` 계정의 프로필 파일에 추가합니다.

```
ulimit -n 1024
```

정책 서버는 서버 연결 수가 무제한인 `smuser` 계정의 `nofiles` 매개 변수의 영향을 받습니다.

지역화 변수 설정 해제

때때로 `LC_*` 변수는 `smuser` 계정의 프로필 파일에 기본 설정됩니다. `LC_*` 환경 변수를 사용할 수는 없습니다. 정책 서버를 설치하기 전에 설정을 해제합니다.

`LC_*` 환경 변수 설정을 해제하려면 `smuser` 계정의 프로필 파일을 열고 설정 해제하십시오.

LANG 환경 변수 설정 해제

`LANG` 환경 변수는 허용되지 않습니다. 정책 서버를 설치하기 전에 설정을 해제합니다.

이 변수를 설정 해제하려면 `smuser` 계정의 프로필에 `unset LANG` 명령을 추가하십시오.

UNIX 에서 정책 서버 설치 전 고려 사항

정책 서버를 설치하기 전에 다음 사항을 고려하십시오.

- **/tmp 의 사용 가능한 공간** - 정책 서버를 설치하려면 `/tmp` 디렉터리에 3 GB 의 사용 가능한 공간이 있어야 합니다.

- **시스템 경로 길이** - 시스템 경로 길이가 1024 자를 초과하면 정책 서버 설치가 실패합니다. 이러한 제한은 포함되거나 제외되는 SiteMinder 추가 디렉터리에 모두 적용됩니다.
참고: 최상의 결과를 얻기 위해 설치 경로가 700 자를 초과하지 않는 위치에 SiteMinder 를 설치하는 것이 좋습니다.
- **텔넷 또는 기타 터미널 애플리케이션 소프트웨어** - 텔넷 또는 기타 터미널 애플리케이션 소프트웨어를 사용하여 정책 서버를 설치하려는 경우 콘솔창을 사용하여 설치를 완료합니다. GUI 모드에서 설치하면 Java 예외가 발생하고 설치 관리자가 종료됩니다.
- **Exceed X-windows 응용 프로그램** - Exceed X-windows 응용 프로그램을 사용하여 정책 서버 설치 관리자 또는 정책 서버 구성 마법사(ca-ps-config.bin)를 실행하면 창의 텍스트가 잘릴 수 있습니다. 이러한 제한은 Exceed 에서 사용할 수 없는 글꼴 때문에 발생하며 정책 서버 설치 또는 구성에 아무런 영향을 주지 않습니다.
- **환경 변수** - 정책 서버 설치에서는 환경 변수를 수정합니다.

UNIX 에서 정책 서버 설치 방법

정책 서버를 설치하려면 다음 단계를 완료하십시오.

1. 정책 서버 구성 요소 고려 사항을 검토합니다.
2. 정책 저장소 고려 사항을 검토합니다.
3. FIPS 고려 사항을 검토합니다.
4. 정책 서버 설치 관리자에 필요한 정보를 수집합니다.
5. 정책 서버 설치 관리자를 실행합니다.
6. (Linux) Security-Enhanced Linux 가 활성화되어 있으면 SiteMinder 관련 예외를 추가합니다.
7. (선택 사항) SNMP 를 구성한 경우 SNMP 데몬을 다시 시작합니다.

정책 서버 구성 요소 고려 사항

정책 서버 외에도 설치 관리자를 통해 다음 구성 요소를 설치 및 구성할 수 있습니다. 정책 서버를 설치하기 전에 다음 사항을 검토하십시오.

- OneView 모니터 UI

OneView 모니터를 통해 SiteMinder 구성 요소를 모니터링할 수 있습니다.

참고: OneView 모니터를 사용하려면 지원되는 Java SDK 및 ServletExec/AS 가 시스템에 설치되어 있어야 합니다.

- SNMP

SNMP 지원을 활성화하기 위해 다음 항목이 있어야 합니다.

- 루트 사용자의 암호
- 네이티브 SunSolstice 마스터 에이전트

- 정책 저장소

참고: 키 저장소와 인증서 데이터 저장소는 정책 저장소와 함께 자동으로 구성되고 배치됩니다.

- 감사 로그

감사 로그를 관계형 데이터베이스 또는 텍스트 파일에 저장할 수 있습니다. 정책 서버를 설치하면 감사 로깅이 ODBC 가 아닌 텍스트 파일로 기본 설정됩니다.

참고: 지원되는 CA 및 타사 구성 요소의 목록에 대해서는 기술 지원 사이트의 SiteMinder 12.52 SP1 Platform Support Matrix(플랫폼 지원표)를 참조하십시오.

정책 저장소 고려 사항

정책 서버 설치 관리자 또는 정책 서버 구성 마법사를 실행하기 전에 다음 사항을 고려하십시오.

- 정책 서버 설치 관리자와 정책 서버 구성 마법사는 다음 저장소 중 하나를 정책 저장소로 자동 구성할 수 있습니다.

- Microsoft AD LDS(Active Directory Lightweight Directory Services)

참고: AD LDS 를 정책 저장소로 구성하기 위한 사전 요구 사항을 충족했는지 확인하십시오.

- Oracle® Directory Enterprise Edition(이전의 Sun Java™ System Directory Server)

중요! 정책 서버 설치 관리자와 정책 서버 구성 마법사는 **SSL 연결을 사용하여 연결되는 정책 저장소를 자동으로 구성할 수 없습니다.**

- Microsoft SQL Server®
- Oracle RDBMS

- (RDB 정책 저장소) 정책 서버 설치 관리자 또는 정책 서버 구성 마법사는 특정 데이터베이스 정보를 사용하여 정책 저장소 데이터 원본을 생성합니다. 정책 서버는 이 데이터 원본을 기반으로 정책 저장소와 통신합니다. 다음 사항을 고려하십시오.

- 데이터 원본의 이름은 **CA SiteMinder DSN** 입니다.
- 설치 관리자는 데이터 원본을 *siteminder_home/db* 에 있는 *system_odbc.ini* 파일에 저장합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

- (RDB 정책 저장소) 정책 저장소를 호스트할 데이터베이스 서버가 **UTF-8** 형식으로 개체를 저장하도록 구성되었는지 확인하십시오. 이렇게 구성하면 정책 저장소가 손상되지 않도록 방지됩니다.
 - (Oracle) 데이터베이스가 **UTF-8** 형식으로 개체를 저장하도록 구성되었는지 확인하십시오. 대부분의 Oracle 문자 집합에서 유니코드가 지원됩니다. **UTF-8** 형식으로 개체를 저장하도록 데이터베이스를 구성하는 방법에 대한 자세한 내용은 공급업체별 설명서를 참조하십시오.
 - (SQL Server) 데이터베이스가 기본 데이터 정렬(**SQL_Latin1_General_CP1_CI_AS**)을 사용하여 구성되었는지 확인하십시오. 대/소문자를 구분하는 데이터 정렬을 사용하면 예기치 않은 동작이 발생할 수 있습니다. 기본 데이터 정렬을 사용하여 개체를 저장하도록 데이터베이스를 구성하는 방법에 대한 자세한 내용은 공급업체별 설명서를 참조하십시오.
- 인증서 데이터 원본은 자동으로 정책 저장소와 함께 배치됩니다.
- 지원되는 다른 디렉터리 서버 또는 관계형 데이터베이스는 정책 서버를 설치한 후 정책 저장소로 수동으로 구성해야 합니다. 정책 저장소를 수동으로 구성하는 방법은 이 문서에 자세히 설명되어 있습니다.

추가 정보:

[관계형 데이터베이스에 SiteMinder 데이터 저장소 구성](#) (페이지 301)

FIPS 고려 사항

정책 서버는 인증된 FIPS(Federal Information Processing Standard) 140-2 호환 암호화 라이브러리를 사용합니다. FIPS는 AES(Advanced Encryption Standard)를 충족하는 암호화 모듈을 인가하는 데 사용되는 미국 정부의 컴퓨터 보안 표준입니다. 이러한 라이브러리는 SiteMinder 환경에서 중요한 데이터를 암호화하는 데 FIPS 호환 알고리즘만 사용하는 경우 FIPS 작동 모드를 제공합니다.

다음 FIPS 작동 모드 중 하나에서 정책 서버를 설치할 수 있습니다.

참고: 정책 서버가 작동하는 FIPS 모드는 시스템에 따라 다릅니다. 자세한 내용은 [기술 지원 사이트](#)의 "SiteMinder 12.52 SP1 Platform Support Matrix"(SiteMinder 12.52 SP1 플랫폼 지원표)를 참조하십시오.

- **FIPS 호환성 모드**-설치 중의 기본 FIPS 작동 모드는 FIPS 호환성 모드입니다. FIPS 호환성 모드에서는 환경이 기존 SiteMinder 알고리즘을 사용하여 중요한 데이터를 암호화하며 이전 버전의 SiteMinder와 호환됩니다.
 - 사용자 환경에서 FIPS 호환 알고리즘을 사용하는 것은 선택 사항입니다.
 - 조직에서 FIPS 호환 알고리즘을 사용할 필요가 없는 경우 정책 서버를 FIPS 호환성 모드에서 설치하십시오. 추가 구성이 필요하지 않습니다.
- **FIPS 마이그레이션 모드** - FIPS 마이그레이션 모드를 사용하면 FIPS 호환성 모드에서 실행 중인 12.52 SP1 환경을 FIPS 전용 모드로 전환할 수 있습니다.

FIPS 마이그레이션 모드에서는 FIPS 호환 알고리즘만 사용하도록 12.52 SP1 환경을 마이그레이션할 때 12.52 SP1 정책 서버가 계속해서 기존 SiteMinder 암호화 알고리즘을 사용합니다.

FIPS 호환 알고리즘만 사용하도록 기존 환경을 구성 중인 경우 정책 서버를 FIPS 마이그레이션 모드에서 설치하십시오.

- **FIPS 전용 모드** - FIPS 전용 모드의 환경에서는 FIPS 호환 알고리즘만 사용하여 중요한 데이터를 암호화합니다.

기존 환경이 12.52 SP1 버전으로 업그레이드되고 FIPS 호환 알고리즘만 사용하도록 구성되는 경우 정책 서버를 FIPS 전용 모드에서 설치하십시오.

중요! FIPS 전용 모드에서 실행되는 12.52 SP1 환경은 FIPS 를 완전히 지원하지 않는 버전, 즉 r12.0 이전 버전의 SiteMinder 와 함께 운용될 수 없습니다. 이 제한은 모든 에이전트, 이전 버전의 에이전트 API 를 사용하는 사용자 지정 소프트웨어, PM API 나 정책 서버에서 노출하는 기타 API 를 사용하는 사용자 지정 소프트웨어에 적용됩니다. 필요한 FIPS 지원을 받으려면 이러한 모든 소프트웨어를 각 SDK 의 12.52 SP1 버전과 다시 연결하십시오.

참고: FIPS 호환 알고리즘만 사용하도록 환경을 마이그레이션하는 방법에 대한 자세한 내용은 *업그레이드 안내서*를 참조하십시오.

설치 관리자에 필요한 정보 수집

정책 서버 설치 관리자가 정책 서버와 선택적 구성 요소를 설치하는 데는 특정 정보가 필요합니다.

필요한 정보

정책 서버 설치 관리자 또는 구성 마법사를 실행하기 전에 다음과 같은 필요한 정보를 수집하십시오.

- **JRE 위치** - 설치 관리자에서 지원되는 JRE 를 찾을 수 있는 폴더를 식별합니다. JRE 가 PATH 변수에 올바르게 설정되었는지 확인합니다. JRE 가 PATH 변수에 올바르게 설정되어 있지 않으면 설치 관리자가 JRE 를 찾을 수 없습니다.
- **정책 서버 설치 위치** - 설치 관리자에서 정책 서버를 설치해야 하는 위치를 확인합니다.

- **암호화 키 값** - 암호화 키 값을 확인합니다. 암호화 키는 정책 서버와 정책 저장소 간에 전송되는 데이터를 보안하는 대/소문자 구분 영숫자 키입니다. 정책 저장소를 공유하는 모든 정책 서버는 동일한 암호화 키를 사용해야 합니다. 보안을 강화하기 위해 긴 암호화 키를 정의하십시오.

제한: 6 자~24 자

- **고급 인증 서버 암호화 키 값** - 암호화 키 값을 확인합니다. 암호화 키는 정책 서버와 고급 인증 서버(CA SiteMinder for Secure Proxy Server 실행) 간에 전송되는 데이터를 보호하는 대/소문자 구분 영숫자 키입니다. CA SiteMinder for Secure Proxy Server 와 모든 정책 서버는 동일한 키를 공유합니다. 보안을 강화하기 위해 긴 암호화 키를 정의하십시오.

제한: 6 자~24 자

Active Directory LDS 서버 정보

Microsoft Active Directory LDS 를 정책 저장소로 구성하려면 다음과 같은 필요한 정보를 수집하십시오.

- **시스템 IP 주소** - 디렉터리 서버 호스트 시스템의 IP 주소를 식별합니다.
- **포트 번호** - 디렉터리 서버가 수신 대기하는 포트 번호를 식별합니다.
- **응용 프로그램 파티션의 루트 DN** - 디렉터리 서버에서 정책 저장소 스키마 데이터를 설치해야 하는 응용 프로그램 파티션의 루트 DN 위치를 식별합니다.

예: dc=ca,dc=com

- **관리자 도메인 이름** - 디렉터리 관리자의 guid 값을 포함한 전체 도메인 이름을 식별합니다.

예: CN=user1,CN=people,CN=Configuration,CN=guid

- **관리자 암호** - 디렉터리 관리자의 암호를 식별합니다.

- **대체 사용자 계정** - 기본적으로 SiteMinder 는 관리자 계정을 사용하여 디렉터리 서버와 통신합니다. 하지만 다른 사용자 계정을 이용하여 정책 저장소를 관리할 수 있습니다. 대체 사용자 계정을 사용하여 정책 저장소를 관리하도록 SiteMinder 를 구성하려면 완전한 관리자 DN 및 암호를 식별합니다.

참고: 이 사용자는 특성을 수정하고 암호를 변경하는 데 필요한 권한이 있어야 합니다.

- **SiteMinder 슈퍼 사용자 암호** - 기본 SiteMinder 슈퍼 사용자 계정은 최대 권한을 가집니다. 기본 슈퍼 사용자 계정의 암호를 확인합니다. 기본 계정의 이름은 다음과 같습니다.

siteminder

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: 일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 대신, 기본 슈퍼 사용자 계정을 사용하여 처음으로 관리 UI 에 액세스한 후 슈퍼 사용자 권한이 있는 관리자를 생성하십시오.

Oracle Directory Server 정보

Oracle Directory Server 를 정책 저장소로 작동하도록 구성하려면 다음과 같은 필요한 정보를 수집하십시오.

- **시스템 IP 주소** - Oracle Directory Server 호스트 시스템의 IP 주소를 확인합니다.
- **디렉터리 인스턴스 포트 번호** - Oracle Directory Server 인스턴스의 포트 번호를 확인합니다.

기본값: 389

- **루트 DN** - Oracle Directory Server 의 루트 DN 을 식별합니다.

예: o=yourorg.com

- **관리자 계정** - LDAP 관리자 계정의 사용자 이름(바인딩 DN)을 식별합니다.

예: cn=Directory Manager

- **관리자 암호** - Oracle Directory Server 관리자의 암호를 식별합니다.

- **대체 LDAP 관리자** - 기본적으로 SiteMinder 는 LDAP 관리자 계정을 사용하여 LDAP 서버와 통신합니다. 하지만 다른 LDAP 사용자 계정을 이용하여 정책 저장소를 관리할 수 있습니다. 이러한 방식으로 SiteMinder 를 구성하려면 완전한 관리자 DN 및 암호를 식별합니다.

참고: 이 사용자는 특성을 수정하고 암호를 변경하는 데 필요한 권한이 있어야 합니다.

- **SiteMinder 슈퍼 사용자 암호** - 기본 SiteMinder 슈퍼 사용자 계정은 최대 권한을 가집니다. 기본 슈퍼 사용자 계정의 암호를 확인합니다. 기본 계정의 이름은 다음과 같습니다.

siteminder

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: 일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 대신, 기본 슈퍼 사용자 계정을 사용하여 처음으로 관리 UI 에 액세스한 후 슈퍼 사용자 권한이 있는 관리자를 생성하십시오.

Microsoft SQL Server 정보

Microsoft SQL Server 를 정책 저장소로 구성하려면 다음과 같은 필요한 정보를 수집하십시오.

데이터베이스 서버 이름

데이터베이스 호스트 시스템의 IP 주소 또는 이름을 식별합니다.

참고: IPv6 지원에 대한 자세한 내용은 "SiteMinder Platform Support Matrix"(SiteMinder 플랫폼 지원표)를 참조하십시오.

데이터베이스 이름

정책 저장소로 작동할 데이터베이스의 이름 또는 명명된 인스턴스를 식별합니다.

데이터베이스 포트

데이터베이스가 수신 대기하는 포트를 식별합니다.

데이터베이스 관리자 사용자 이름 및 암호

다음 작업을 수행할 수 있는 권한이 있는 관리자 계정의 이름과 암호를 식별합니다.

- 스키마 만들기
- 개체 생성, 읽기, 수정 및 삭제

참고: 데이터베이스에 SiteMinder 스키마가 이미 있는 경우 마법사는 **create** 권한이 있는 데이터베이스 관리자의 자격 증명을 요구하지 않습니다. 자세한 내용은 [SQL Server 정책 저장소 구성](#) (페이지 326)을 참조하십시오.

SiteMinder 슈퍼 사용자 암호

기본 SiteMinder superuser 계정은 최대 권한을 갖습니다. 기본 슈퍼 사용자 계정의 암호를 확인합니다. 기본 계정의 이름은 다음과 같습니다.

siteminder

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: 일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 대신, 기본 슈퍼 사용자 계정을 사용하여 처음으로 관리 UI 에 액세스한 후 슈퍼 사용자 권한이 있는 관리자를 생성하십시오.

Oracle RDBMS 정보

Oracle RDBMS 를 정책 저장소로 구성하려면 다음과 같은 필요한 정보를 수집하십시오.

데이터베이스 서버 이름

데이터베이스 호스트 시스템의 IP 주소 또는 이름을 식별합니다.

참고: IPv6 지원에 대한 자세한 내용은 "SiteMinder Platform Support Matrix"(SiteMinder 플랫폼 지원표)를 참조하십시오.

데이터베이스 서비스 이름

정책 저장소로 작동할 데이터베이스의 서비스 이름을 식별합니다.

데이터베이스 포트

데이터베이스가 수신 대기하는 포트를 식별합니다.

데이터베이스 관리자 사용자 이름

다음 작업을 수행할 수 있는 권한이 있는 관리자 계정의 이름을 식별합니다.

- 스키마 만들기
- 개체 생성, 읽기, 수정 및 삭제

데이터베이스 관리자 암호

관리자 계정의 암호를 식별합니다.

SiteMinder 슈퍼 사용자 암호

기본 SiteMinder superuser 계정은 최대 권한을 갖습니다. 기본 슈퍼 사용자 계정의 암호를 확인합니다. 기본 계정의 이름은 다음과 같습니다.

siteminder

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: 일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 대신, 기본 슈퍼 사용자 계정을 사용하여 처음으로 관리 UI 에 액세스한 후 슈퍼 사용자 권한이 있는 관리자를 생성하십시오.

OneView 모니터 정보

OneView 모니터 정보는 OneView 모니터를 구성하려는 경우에만 수집하면 됩니다.

OneView 모니터를 구성하려면 다음과 같은 필요한 정보를 수집하십시오. OneView 모니터 정보 워크시트를 사용하여 값을 기록할 수 있습니다.

- **JDK 경로** - 필요한 JDK 버전의 경로를 식별합니다.
- **ServletExec 설치 디렉터리** - ServletExec 설치 디렉터리를 식별합니다.
- **ServletExec 포트 번호** - ServletExec 인스턴스의 포트 번호를 확인합니다.
- **Sun Java System 관리자 디렉터리** - 다음 정보를 확인합니다.

- Sun Java System 이 설치된 위치
- Sun Java System Web Server 가 설치된 위치

예: `/sunjavasystem_home/location`

sunjavasystem_home

Sun Java System 이 설치된 위치를 지정합니다.

location

Sun Java System Web Server 가 설치된 위치를 지정합니다.

- **여러 ServletExec 인스턴스** - ServletExec 인스턴스가 여러 개 있는 경우 OneView 모니터 GUI 를 구성할 인스턴스를 결정합니다.

GUI 모드에서 정책 서버 설치

기술 지원 사이트의 설치 미디어를 사용하여 정책 서버를 설치합니다. 다음 사항을 고려하십시오.

- 실행 권한이 있는지 확인합니다. 설치 미디어에 대한 실행 권한을 추가하려면 다음 명령을 실행하십시오.

```
chmod +x installation_media
```

installation_media

정책 서버 설치 관리자 실행 파일을 지정합니다.

- 여러 서브넷에서 정책 서버 설치 관리자를 실행하면 설치 관리자가 충돌할 수 있습니다. 이 문제를 방지하려면 정책 서버를 호스트 시스템에 직접 설치하십시오.

다음 단계를 수행하십시오.

1. 모든 포그라운드 응용 프로그램을 종료합니다.
2. 셸을 열고 설치 미디어를 탐색합니다.
3. 다음 명령을 입력합니다.

```
./ca-ps-12.5-cr-unix_version
```

cr

누적 릴리스 번호를 지정합니다. 기본 r12.5 릴리스에는 누적 릴리스 번호가 포함되지 않습니다.

unix_version

UNIX 버전(sol 또는 linux)을 지정합니다.

설치 관리자가 시작됩니다.

참고: 설치 미디어 이름의 목록에 대해서는 *정책 서버 릴리스 정보*를 참조하십시오.

4. 수집한 시스템 및 구성 요소 정보를 사용하여 정책 서버를 설치합니다.

설치 관리자를 실행할 때 다음 사항을 고려하십시오.

- 이 시스템에서 처음으로 정책 서버를 설치하는 경우 **OneView** 모니터 UI 를 구성하지 마십시오. 설치 관리자가 **OneView** 모니터 UI 를 호스트할 웹 서버의 구성 파일을 수정합니다. smuser 계정에는 필요한 루트 권한이 없습니다. 정책 서버를 설치한 후 정책 서버 구성 마법사를 루트로 사용하여 **OneView** 모니터 UI 를 구성하십시오.
- **FIPS** 작동 모드를 선택하라는 메시지가 표시됩니다. 선택할 **FIPS** 모드에 대한 자세한 내용은 [FIPS 고려 사항](#) (페이지 72)을 참조하십시오.
- 정책 저장소를 수동으로 구성하는 경우 구성 요소를 선택할 때 정책 저장소 옵션의 선택을 취소하십시오. 정책 저장소로 자동 구성될 수 있는 저장소에 대한 자세한 내용은 [정책 저장소 고려 사항](#) (페이지 70)을 참조하십시오.

- 정책 저장소를 초기화하는 경우 기본 SiteMinder 사용자 계정에 대한 암호를 입력하라는 메시지가 표시됩니다. 기본 계정 이름은 다음과 같습니다.

siteminder

- 기본 CA(인증 기관) 인증서를 인증서 데이터 저장소에 설치하라는 메시지가 표시됩니다. 설치 후에 추가 인증서와 개인 키를 인증서 데이터 저장소에 추가할 수 있습니다.
- IPv6 주소를 사용하는 경우에는 항목을 대괄호로 묶으십시오.

예:

[2001:db8::1428:57ab]

- 경로 정보를 잘라내서 마법사에 붙여 넣은 경우 문자를 입력하여 "다음" 단추가 사용되도록 설정합니다.

5. 설치 설정을 검토하고 "설치"를 클릭합니다.

정책 서버 및 선택한 모든 구성 요소가 설치되고 구성됩니다.

참고: 설치하는 몇 분 정도 걸릴 수 있습니다.

6. "Done"(완료)을 클릭합니다.

설치 관리자가 닫힙니다.

7. (선택 사항) 설치 관리자를 사용하여 정책 저장소를 구성하지 않은 경우 정책 저장소를 수동으로 구성합니다.

참고: 설치 도중 문제가 발생할 경우

`siteminder_home/siteminder/install_config_info` 에서 설치 로그 파일과 정책 저장소 상세 정보 파일을 찾아 검토하십시오.

추가 정보:

[정책 서버 설치 문제 해결](#) (페이지 85)

콘솔 모드에서 정책 서버 설치

기술 지원 사이트의 설치 미디어를 사용하여 정책 서버를 설치합니다. 다음 사항을 고려하십시오.

- 실행 권한이 있는지 확인합니다. 설치 미디어에 대한 실행 권한을 추가하려면 다음 명령을 실행하십시오.

```
chmod +x installation_media
```

installation_media

정책 서버 설치 관리자 실행 파일을 지정합니다.

- 여러 서브넷에서 정책 서버 설치 관리자를 실행하면 설치 관리자가 충돌할 수 있습니다. 이 문제를 방지하려면 정책 서버를 호스트 시스템에 직접 설치하십시오.

다음 단계를 수행하십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. 셸을 열고 설치 미디어를 탐색합니다.
3. 다음 명령을 실행합니다.

```
./ca-ps-12.5-cr-unix_version -i console
```

cr

누적 릴리스 번호를 지정합니다. 기본 r12.5 릴리스에는 누적 릴리스 번호가 포함되지 않습니다.

unix_version

UNIX 버전(sol 또는 linux)을 지정합니다.

설치 관리자가 시작됩니다.

참고: 설치 미디어 이름의 목록에 대해서는 *정책 서버 릴리스 정보*를 참조하십시오.

4. 수집한 시스템 및 구성 요소 정보를 사용하여 정책 서버를 설치합니다.
정보를 입력할 때 다음 사항을 고려하십시오.

- 이 시스템에서 처음으로 정책 서버를 설치하는 경우 **OneView** 모니터 UI 를 구성하지 마십시오. 설치 관리자가 **OneView** 모니터 UI 를 호스트할 웹 서버의 구성 파일을 수정합니다. smuser 계정에는 필요한 루트 권한이 없습니다. 정책 서버를 설치한 후 정책 서버 구성 마법사를 루트로 사용하여 **OneView** 모니터 UI 를 구성하십시오.

- FIPS 작동 모드를 선택하라는 메시지가 표시됩니다. 선택할 FIPS 모드에 대한 자세한 내용은 [FIPS 고려 사항](#) (페이지 72)을 참조하십시오.
- 구성할 구성 요소를 선택하라는 메시지가 표시됩니다. 여러 항목을 입력하는 경우 쉼표(,)로 구분하십시오. 아무 기능도 선택하지 않으려면 쉼표만 입력합니다.
- 정책 저장소를 수동으로 구성하는 경우 정책 저장소를 선택하지 마십시오. 정책 저장소로 자동 구성될 수 있는 저장소에 대한 자세한 내용은 [정책 저장소 고려 사항](#) (페이지 70)을 참조하십시오.
- 정책 저장소를 초기화하는 경우 기본 SiteMinder 사용자 계정에 대한 암호를 입력하라는 메시지가 표시됩니다. 기본 계정 이름은 다음과 같습니다.

siteminder

- 기본 CA(인증 기관) 인증서를 인증서 데이터 저장소에 설치하라는 메시지가 표시됩니다. 설치 후에 추가 인증서와 개인 키를 인증서 데이터 저장소에 추가할 수 있습니다.
- IPv6 주소를 사용하는 경우에는 항목을 대괄호로 묶으십시오.

예:

[2001:db8::1428:57ab]

- 새 정책 저장소 인스턴스를 구성하는 경우에만 정책 저장소를 초기화하십시오.

5. 설치 설정을 검토하고 Enter 키를 누릅니다.

정책 서버 및 선택한 모든 구성 요소가 설치되고 구성됩니다.

참고: 설치하는 몇 분 정도 걸릴 수 있습니다.

6. Enter 키를 누릅니다.

설치 관리자가 닫힙니다.

7. (선택 사항) 설치 관리자를 사용하여 정책 저장소를 구성하지 않은 경우 정책 저장소를 수동으로 구성합니다.

참고: 설치 도중 문제가 발생할 경우

`siteminder_home/siteminder/install_config_info` 에서 설치 로그 파일과 정책 저장소 상세 정보 파일을 찾아 검토하십시오.

추가 정보:

[정책 서버 설치 문제 해결](#) (페이지 85)

Security-Enhanced Linux 에 예외 추가

Security-Enhanced Linux 가 정책 서버 호스트 시스템에서 활성화된 경우 SiteMinder 예외를 환경에 추가하십시오. 예외를 추가하면 Security-Enhanced Linux 에서 텍스트 재배포 거부를 방지할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 셸을 열고 다음 명령을 실행합니다.

```
chcon -t textrel_shlib_t /siteminder_home/lib/*  
siteminder_home
```

정책 서버 설치 경로를 지정합니다.

3. 다음 명령을 실행합니다.

```
chcon -t textrel_shlib_t /JDK_home/lib/i386/*  
JDK_home
```

필요한 JDK 설치 경로를 지정합니다.

4. 다음 명령을 실행합니다.

```
chcon -t textrel_shlib_t /JDK_home/lib/i386/server/*  
JDK_home
```

필요한 JDK 설치 경로를 지정합니다.

SiteMinder 관련 예외가 추가되었습니다.

SNMP 데몬 다시 시작

정책 서버 설치 중 SNMP 를 구성한 경우에만 SNP 데몬을 다시 시작하면 됩니다.

SNMP 데몬을 다시 시작하려면

1. `S76snmpdx stop in /etc/rc3.d` 를 입력합니다.
SNMP 데몬이 중지됩니다.
2. `S76snmpdx start in /etc/rc3.d` 를 입력합니다.
SNMP 데몬이 시작됩니다.

정책 서버 설치 문제 해결

다음 파일을 사용하여 정책 서버 설치 문제를 해결하십시오.

- **CA_SiteMinder_Policy_Server_release_InstallLog.log**

이 설치 로그에는 설치 중에 발생한 오류, 심각하지 않은 오류, 경고, 성공의 수를 보여 주는 요약 섹션이 포함됩니다. 개별 설치 작업이 해당 상태와 함께 표시됩니다.

release

정책 서버 릴리스를 지정합니다.

위치: `siteminder_home\siteminder\install_config_info`

- **ca-ps-details.log**

정책 저장소 로그는 정책 저장소 상태 정보를 제공합니다.

위치: `siteminder_home\siteminder\install_config_info`

- **smps.log**

정책 서버를 시작하면 `smps.log` 가 생성됩니다. 정책 서버가 성공적으로 설치되었을 경우 이 로그에는 다음과 같은 줄이 포함됩니다.

[Info] Journaling thread started, will delete commands older than 60 minutes.

위치: `siteminder_home\siteminder\log`

siteminder_home

정책 서버 설치 경로를 지정합니다.

자동 시작 구성

UNIX 시스템이 재부팅될 때 정책 서버가 자동으로 다시 시작되도록 자동 시작을 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. S98M 스크립트에서 모든 "nete_ps_root" 문자열을 SiteMinder 설치 디렉터리의 명시적 경로로 바꿉니다.

예: /export/ca/siteminder

2. 디렉터리를 SiteMinder 설치 디렉터리로 변경합니다.

3. su 를 입력하고 Enter 키를 누릅니다.

참고: suse 명령을 사용하지 마십시오.

암호를 묻는 메시지가 표시됩니다.

4. 루트 암호를 입력하고 Enter 키를 누릅니다.

5. \$ cp S98sm /etc/rc2.d 를 입력하고 Enter 키를 누릅니다.

UNIX 시스템이 재부팅되면 s98sm 이 자동으로 stop-all 및 start-all 실행 파일을 호출하여 정책 서버를 중지했다가 시작합니다.

참고: 로컬 LDAP 디렉터리 서버를 정책 저장소로 사용할 경우에는 정책 서버를 자동으로 시작하기 전에 LDAP 디렉터리가 자동으로 시작되도록 구성해야 합니다.

정책 서버 구성 마법사

정책 서버를 설치한 후 정책 서버 구성 마법사를 사용하여 다음 구성 요소를 구성 또는 재구성합니다.

- 정책 저장소 하나
- SNMP 지원
- OneView 모니터 UI

참고: 정책 서버 구성 마법사를 사용하여 정책 서버 FIPS 작업 모드를 변경할 수는 없습니다. 정책 서버 FIPS 작업 모드 변경에 대한 자세한 내용은 *SiteMinder 업그레이드 안내서*를 참조하십시오.

중요! OneView 모니터 UI 또는 SNMP 에 대해 Oracle iPlanet 웹 서버 인스턴스를 구성한 경우 마법사를 사용하여 새 인스턴스를 구성하지 마십시오. 새로운 웹 서버 인스턴스를 구성하면 기존 웹 서버 인스턴스가 실패할 수 있습니다.

추가 정보:

[정책 저장소 고려 사항](#) (페이지 35)

구성 마법사를 사용하는 방법

정책 서버 구성 마법사를 사용하려면 다음 절차를 완료하십시오.

1. 구성 마법사 요구 사항을 검토합니다.
2. [정책 저장소 고려 사항](#) (페이지 70)을 검토합니다.
3. 정책 저장소로 다음 저장소 중 하나를 구성하거나 OneView 모니터 UI 를 구성하려는 경우 [마법사에서 필요한 정보를 수집합니다](#) (페이지 47).
 - Active Directory LDS
 - Oracle Directory Server
 - SQL Server
 - Oracle RDBMS
4. 마법사를 실행합니다.

구성 마법사 요구 사항

정책 서버 구성 마법사를 사용하기 전에 다음 요구 사항을 충족해야 합니다.

- 정책 서버 구성 마법사를 사용하려면 /tmp 에 150 MB 이상의 사용 가능한 공간이 있어야 합니다.
- 로컬 관리자 권한이 있는 UNIX 사용자로 마법사를 실행합니다.
- 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

GUI 모드에서 구성 마법사 실행

정책 서버 구성 마법사를 실행하여 각각의 정책 서버 구성 요소를 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. SiteMinder 설치 디렉터리의 ksh 셸에서 다음 스크립트를 실행합니다.

```
./ca_ps_env.ksh
```

참고: 마침표 사이에는 공백이 있어야 합니다(.).

3. 셸을 열고 다음 명령을 실행합니다.

```
./ca-ps-config.bin gui
```

구성 마법사가 시작됩니다.

4. 수집한 시스템 및 구성 요소 정보를 사용하여 정책 저장소와 개별 구성 요소를 구성합니다.

참고: 새로운 정책 저장소 인스턴스를 구성할 때만 정책 저장소 인스턴스를 초기화하십시오.

5. 설치 설정을 검토하고 "설치"를 클릭합니다.

선택한 구성 요소가 정책 서버와 작동하도록 구성됩니다.

참고: 설치에는 몇 분 정도 걸릴 수 있습니다.

6. "Done"(완료)을 클릭합니다.

선택한 구성 요소가 구성됩니다.

참고: 문제가 발생할 경우

`siteminder_home/siteminder/install_config_info` 에서 설치 로그 파일과 정책 저장소 상세 정보 파일을 찾아 검토하십시오.

추가 정보:

[정책 서버 설치 문제 해결](#) (페이지 85)

콘솔 모드에서 구성 마법사 실행

정책 서버 구성 마법사를 실행하여 각각의 정책 서버 구성 요소를 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. SiteMinder 설치 디렉터리의 ksh 셸에서 다음 스크립트를 실행합니다.

```
./ca_ps_env.ksh
```

참고: 마침표 사이에는 공백이 있어야 합니다(.).

3. 셸을 열고 다음 명령을 실행합니다.

```
./ca-ps-config.bin -i console
```

구성 마법사가 시작됩니다.

4. 수집한 시스템 및 구성 요소 정보를 사용하여 정책 저장소와 개별 구성 요소를 구성합니다.

참고:

- 새로운 정책 저장소 인스턴스를 구성할 때만 정책 저장소 인스턴스를 초기화하십시오.
- 고급 인증 서버를 구성하려면 구성 선택 목록의 위에 있는 "없음"을 선택하고 고급 인증 서버에 대한 마스터 암호화 키를 입력하십시오.

5. 설치 설정을 검토하고 Enter 키를 누릅니다.

선택한 구성 요소가 정책 서버와 작동하도록 구성됩니다.

참고: 설치하는 몇 분 정도 걸릴 수 있습니다.

6. Enter 키를 누릅니다.

설치 관리자가 닫힙니다. 선택한 구성 요소가 구성됩니다.

참고: 문제가 발생할 경우

`siteminder_home/siteminder/install_config_info` 에서 설치 로그 파일과 정책 저장소 상세 정보 파일을 찾아 검토하십시오.

추가 정보:

[정책 서버 설치 문제 해결](#) (페이지 85)

UNIX 에서 정책 서버 제거 방법

정책 서버를 제거하려면 다음 절차를 완료하십시오.

1. 정책 서버 관리 콘솔의 모든 인스턴스를 종료합니다.

참고: 정책 서버 관리 콘솔을 종료하는 방법에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

2. 경로 변수에서 JRE 를 설정합니다.
3. 에이전트 호스트 파일에서 정책 서버 참조를 제거합니다.
4. 모든 SiteMinder 프로세스를 중지합니다.
5. 정책 서버를 제거합니다.
6. IWS 에서 SiteMinder 참조를 제거합니다.
7. ServletExec/AS 에서 SiteMinder 참조를 제거합니다.
8. 남은 항목을 제거합니다.

에이전트 호스트 파일에서 정책 서버 참조 제거

정책 서버를 제거한 후 웹 에이전트에서 예기치 못한 결과가 발생하지 않도록 SmHost.conf 파일에서 정책 서버 참조를 제거하십시오.

정책 서버 참조를 제거하려면

1. `web_agent_home/config` 로 이동합니다.

web_agent_home

웹 에이전트의 설치 디렉터리를 지정합니다.

2. 텍스트 편집기에서 SmHost.conf 파일을 엽니다.
3. "policyserver="로 시작하는 행을 삭제합니다.

참고: 이 행에는 제거할 정책 서버의 IP 주소 및 포트 번호가 포함되어 있습니다.

4. SmHost.conf 를 저장합니다.

이제 SmHost.conf 파일은 제거할 정책 서버를 더 이상 참조하지 않습니다.

PATH 변수에 JRE 설정

정책 서버, 웹 에이전트, SDK 또는 설명서를 제거할 때는 PATH 변수에 JRE 를 설정하여 제거 프로그램이 중지되고 오류 메시지가 발생하지 않도록 하십시오.

PATH 변수에 JRE 를 설정하려면

1. 다음 명령을 실행합니다.

```
PATH=$PATH:<JRE>/bin
```

JRE

JRE 의 위치를 지정합니다.

2. 다음 명령을 실행합니다.

```
export PATH
```

PATH 변수에 JRE 가 설정됩니다.

모든 SiteMinder 프로세스 중지

정책 서버 파일이 안전하게 제거되도록 SiteMinder 프로세스를 모두 중지하십시오.

모든 SiteMinder 프로세스를 중지하려면

1. smuser 계정으로 UNIX 시스템에 로그인합니다.
2. /siteminder 디렉터리에 있는 stop-all 을 실행합니다.

모든 SiteMinder 프로세스가 중지됩니다.

정책 서버 제거

시스템에서 더 이상 필요하지 않을 경우 정책 서버를 제거하십시오.

참고: 이 구성 요소를 제거하기 위해 설치 디렉터리를 수동으로 제거하지 마십시오. 제거용 셸 스크립트를 실행해야 합니다. 설치 디렉터리만 제거한 경우 관련 레지스트리가 남아 있게 됩니다. 이 호스트 시스템에 이 구성 요소를 다시 설치하려고 하면 이러한 항목으로 인해 설치가 실패할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버를 설치한 사용자로 정책 서버 호스트 시스템에 로그인합니다.

참고: 정책 서버를 설치한 사용자는 필요한 SiteMinder 스크립트를 제공해야 합니다. 로그인 시 SiteMinder 스크립트를 제공하지 않거나 다른 사용자로 로그인한 경우 다음 스크립트를 제공하십시오.

```
smprofile.ksh
ca_ps_env.ksh
```

2. 콘솔 창에서 다음 디렉터리로 변경합니다.

```
siteminder_home/siteminder/install_config_info/ca-ps-uninstall
siteminder_home
```

정책 서버 설치 경로를 지정합니다.

3. 다음 명령을 실행합니다.

```
./uninstall
제거 프로그램이 표시됩니다.
```

4. Enter 키를 누릅니다.

상태 표시기에 진행률이 표시됩니다.

5. 디렉터리를 SiteMinder 설치 디렉터리 상위 디렉터리로 변경합니다.

예: SiteMinder 설치 디렉터리가 /export/smuser/ca/siteminder 이면 다음으로 이동합니다.

```
/export/smuser/ca
```

6. 다음 명령을 입력하고 Enter 키를 누릅니다.

```
$ rm -rf siteminder
SiteMinder 설치 디렉터리가 제거됩니다.
```

7. HOME 디렉터리에서 다음 파일을 엽니다.

```
.profile
```

8. smprofile.ksh 가 포함된 행을 찾아 삭제합니다.

예:

```
./export/smuser/siteminder/smprofile.ksh
```

9. 파일을 저장합니다.

정책 서버가 제거되었습니다.

IWS 에서 SiteMinder 참조 제거

정책 서버를 제거한 후 IWS 에서 수동으로 SiteMinder 참조를 제거하십시오.
SiteMinder 참조는 obj.conf 파일과 magnus.conf 파일에 남아 있습니다.

IWS 에서 SiteMinder 참조를 제거하려면

1. 웹 서버 구성에 대한 액세스 및 수정 권한이 있는 계정으로 로그인합니다.

2. Solaris 명령줄에서 다음 위치로 이동합니다.

```
<SunJavaSystem_home>/https-<hostname>/config
```

obj.conf 및 magnus.conf 파일은 config 폴더에 있습니다.

3. obj.conf 를 열고 다음 행을 제거합니다.

```
NameTrans fn="assign-name" from="/servlet/*" name="<ServletExec_instance name>"
NameTrans fn="assign-name" from="*.jsp*" name="<ServletExec_instance name>"
NameTrans fn="pfx2dir" from="/sitemindermonitor"
dir="/<siteminder_installation>/monitor"
NameTrans fn="pfx2dir" from="/sitemindercgi"
dir="/<siteminder_installation>/admin" name="cgi"
NameTrans fn="pfx2dir" from="/siteminder"
dir="/<siteminder_installation>/admin"
NameTrans fn="pfx2dir" from="/netegrity_docs"
dir="/netegrity/netegrity_documents"
<Object name="<ServletExec_instance name>">
Service fn="ServletExecService" group="<ServletExec_instance name>"
</Object>
```

4. obj.conf 파일을 저장한 후 닫습니다.

5. magnus.conf 를 열고 다음 행을 제거합니다.

```
Init fn="init-cgi" SM_ADM_UDP_PORT="44444" SM_ADM_TCP_PORT="44444"
Init fn="load-modules"
shlib="/<Servlet_Exec_Install>/bin/ServletExec_Adapter.so"
funcs="ServletExecInit,ServletExecService"
Init fn="ServletExecInit" <ServletExec_instance
name>.instances="<IP_Address>:<port_number>"
```

6. magnus.conf 를 저장한 후 닫습니다.

7. 웹 서버를 다시 시작합니다.

SiteMinder 참조가 IWS 에서 제거되었습니다.

IWS 에 더 이상 SiteMinder 참조가 표시되지 않습니다.

StartServletExec 에서 SiteMinder 참조 제거

StartServletExec 에서 참조를 제거하려면

1. ServletExec 구성에 대한 액세스 및 수정 권한이 있는 계정으로 로그인합니다.
2. Solaris 명령줄에서 `/usr/NewAtlanta/ServletExecAS/ServletExec_instance name` 폴더로 이동합니다.
3. StartServletExec 스크립트에서 다음 행을 제거합니다.

```
CLASSPATH=${NA_LIB}/servlet-api.jar:${NA_LIB}/jsp-  
api.jar:${NA_LIB}/ServletExec60.jar:${NA_LIB}/ServletExecAdmin.jar:${NA_LIB}/  
el-  
api.jar:${NA_LIB}/jasper-el.jar:${JL}/tools.jar:${NA_LIB}/jstl.jar:${NA_LIB}/  
appserv-  
jstl.jar:${NA_LIB}/activation.jar:${NA_LIB}/mail.jar:${HOMEDIRPATH}/classes:/  
siteminder_home/monitor/  
smmonui.jar:/siteminder_home/lib/smconapi.jar:/siteminder_home/lib/smmonclien  
tapi.jar  
$SENAME $HOMEDIR $MIMEFILE $DOCR00TDIR -allow 127.0.0.1 -port $PORT $SEOPTS"  
$SENAME $HOMEDIR $MIMEFILE $DOCR00TDIR -allow 127.0.0.1 -port $PORT $SEOPTS -addl  
"/sitemindermonitor=/siteminder_home/monitor"
```

siteminder_home

정책 서버 설치 경로를 지정합니다.

4. StartServletExec 스크립트를 저장한 후 닫습니다.
 5. ServletExec 를 다시 시작합니다.
- 제거가 완료되었습니다.

남은 항목 제거

정책 서버를 제거한 후에도 시스템에 `com.zerog.registry.xml` 파일이 남아 있습니다. 이 파일을 제거하십시오.

다음 중 하나에서 이 파일을 찾을 수 있습니다.

- `$HOME/.com.zerog.registry.xml`
- `/var/.com.zerog.registry.xml`

제 6 장: SiteMinder 데이터를 저장하도록 LDAP 디렉터리 서버 구성

이 섹션은 다음 항목을 포함하고 있습니다.

- [정책 또는 키 저장소로 LDAP 디렉터리 서버 사용 \(페이지 95\)](#)
- [설치 로드맵 \(페이지 96\)](#)
- [중요 고려 사항 \(페이지 97\)](#)
- [기본 정책 저장소 개체 고려 사항 \(페이지 98\)](#)
- [CA Directory 를 정책 저장소로 구성 \(페이지 99\)](#)
- [CA Directory 를 세션 저장소로 사용 \(페이지 114\)](#)
- [Active Directory 를 정책 저장소로 구성 \(페이지 119\)](#)
- [Domino Directory Server 를 정책 저장소로 구성 \(페이지 132\)](#)
- [IBM Tivoli Directory Server 를 정책 저장소로 구성 \(페이지 144\)](#)
- [Microsoft Active Directory LDS 를 정책 저장소로 구성 \(페이지 155\)](#)
- [Novell eDirectory 를 정책 저장소로 구성 \(페이지 167\)](#)
- [OpenLDAP 을 정책 저장소로 구성 \(페이지 180\)](#)
- [Oracle Directory Server 를 정책 저장소로 구성 \(페이지 198\)](#)
- [Oracle Internet Directory 를 정책 저장소로 구성 \(페이지 211\)](#)
- [Oracle Unified Directory 를 정책 저장소로 구성하는 방법 \(페이지 224\)](#)
- [Oracle Virtual Directory 를 정책 저장소로 구성하는 방법 \(페이지 240\)](#)
- [Red Hat Directory Server 를 정책 저장소로 구성 \(페이지 251\)](#)
- [Siemens DirX 를 정책 저장소로 구성 \(페이지 262\)](#)
- [별도의 키 저장소 구성 \(페이지 274\)](#)

정책 또는 키 저장소로 LDAP 디렉터리 서버 사용

SiteMinder 정책 저장소는 모든 정책 관련 정보를 저장하는 리포지토리입니다. SiteMinder 설치 환경의 모든 정책 서버는 정책 저장소 데이터를 직접적으로 또는 복제를 통해 공유해야 합니다. SiteMinder 는 관리자가 정책 저장소 데이터를 한 저장소에서 다른 저장소로 이동할 수 있는 도구와 함께 설치됩니다.

정책 서버를 설치할 때 다음 디렉터리 서버 중 하나를 정책 저장소로 자동 구성할 수 있습니다.

- Microsoft AD LDS(Active Directory Lightweight Directory Services)
- Oracle Directory Server(이전의 Sun Java System Directory Server)

정책 서버를 사용하여 정책 저장소를 자동으로 구성하지 않을 경우 정책 서버를 설치한 후 정책 저장소를 수동으로 구성할 수 있습니다. 또한 정책 서버를 설치한 후 정책 서버 관리 콘솔을 사용하여 정책 서버를 기존 정책 저장소에 연결할 수 있습니다.

참고: 지원되는 CA 및 타사 구성 요소의 목록에 대해서는 기술 지원 사이트의 SiteMinder 12.52 SP1 Platform Support Matrix(플랫폼 지원표)를 참조하십시오.

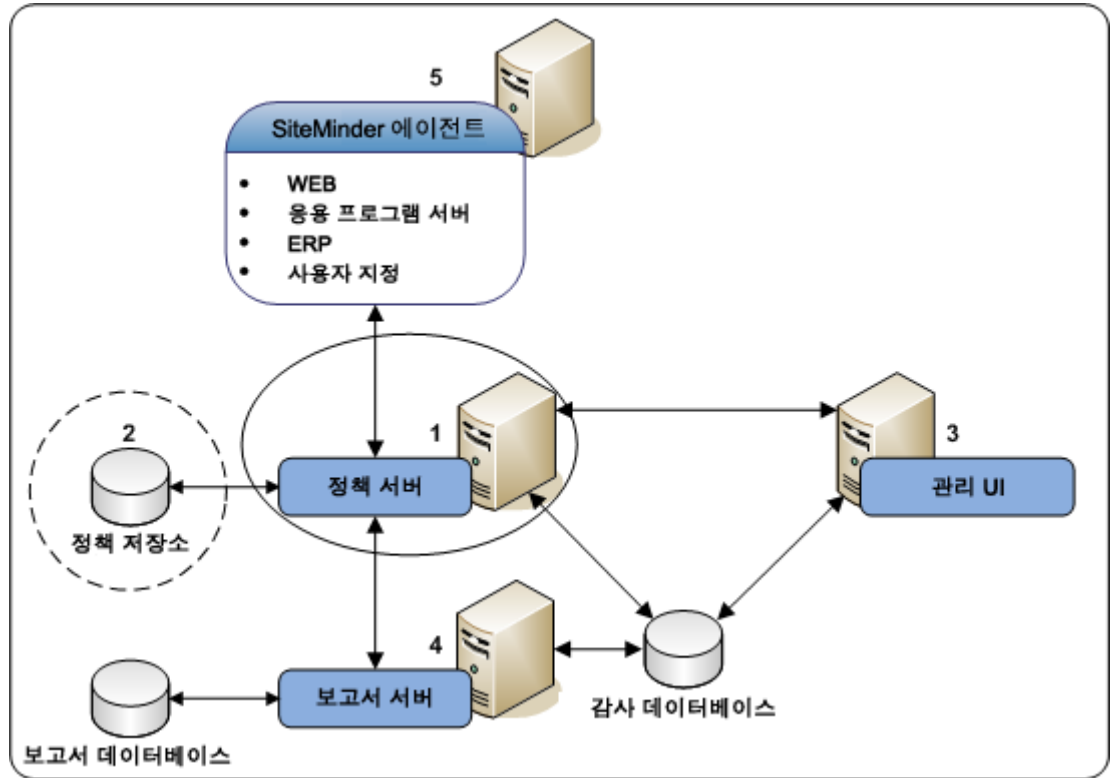
설치 로드맵

다음 다이어그램에서는 샘플 SiteMinder 설치를 보여 주고 각 구성 요소를 설치 및 구성하는 순서를 나열합니다.

- 실선으로 둘러싸인 부분은 정책 서버입니다. 이 정책 서버는 정책 저장소를 구성하기 전에 필요합니다. 정책 서버가 환경에 포함되어 있지 않은 경우 계속하기 전에 설치해야 합니다.
- 점선으로 둘러싸인 부분은 정책 저장소입니다. 지금 이 구성 요소를 구성합니다.

다음 그림은 단일 정책/키 저장소 인스턴스를 보여 줍니다. 그림에는 표시되지 않았지만 환경에서 각 정책 및 키 저장소에 별도의 인스턴스를 사용할 수 있습니다.

수식1: 설치 로드맵



중요 고려 사항

정책 저장소 손상을 방지하려면 정책 저장소가 있는 서버가 개체를 UTF-8 형식으로 저장하도록 구성되었는지 확인하십시오. 개체를 UTF-8 형식으로 저장하도록 서버를 구성하는 방법에 대한 자세한 내용은 해당 서버의 설명서를 참조하십시오.

기본 정책 저장소 개체 고려 사항

정책 저장소를 구성할 때 다음 기본 정책 저장소 개체 파일을 사용할 수 있습니다.

- smpolicy.xml
- smpolicy-secure.xml

두 파일 모두에 정책 저장소에 필요한 기본 개체가 포함되어 있습니다.

- 정책 서버 구성 마법사를 사용하여 정책 저장소를 자동으로 구성하는 경우 마법사는 smpolicy.xml 만 사용합니다.
- smpolicy-secure.xml 을 사용하려면 정책 저장소를 수동으로 구성해야 합니다.

두 파일 모두에서 기본 보안 설정을 제공합니다. 이러한 설정은 관리 UI 에서 제공하는 기본 ACO(에이전트 구성 개체) 템플릿에서 사용할 수 있습니다.

smpolicy-secure 파일은 보다 제한적인 기본 보안 설정을 제공합니다. smpolicy.xml 을 선택해도 보다 제한적인 기본 보안 설정을 사용할 수 있습니다. 관리 UI 를 사용하면 기본 ACO 설정을 수정할 수 있습니다.

다음 표에는 두 파일의 보안 설정이 요약되어 있습니다.

매개 변수 이름	smpolicy 값	smpolicy-secure 값
BadCssChars	값이 없음	<, >, ', ;,), (, &, +, %00
BadQueryChars	값이 없음	<, >, ', ;,), (, &, +, %00
BadUrlChars	//, ./, /., /*, *, ~, \, %00-%1f, %7f-%ff, %25	smpolicy.smdif 값과 다음 값: <, >, ', ;,), (, &, +
EnableCookieProvider	예	아니요
IgnoreExt	.class, .gif, .jpg, .jpeg, .png, .fcc, .scc, .sf cc, .ccc, .ntc	모든 smpolicy 값
LimitCookieProvider	아니요	예

매개 변수 이름	smpolicy 값	smpolicy-secure 값
ValidTargetDomain	이 파일에는 이 매개 변수가 없습니다.	이 매개 변수에는 기본값이 없습니다. 올바른 리디렉션 도메인을 제공하십시오. 예: validtargetdomain=".example.com"

CA Directory 를 정책 저장소로 구성

CA Directory 는 정책 저장소로 작동할 수 있습니다. 단일 디렉터리 서버 인스턴스가 다음 기능을 수행할 수 있습니다.

- 정책 저장소
- 키 저장소

단일 디렉터리 서버를 사용하면 관리 태스크를 간소화할 수 있습니다. 다음 단원에서는 정책 데이터 및 암호화 키를 저장하도록 단일 디렉터리 서버 인스턴스를 구성하는 방법에 대한 지침을 제공합니다. 구현에 필요할 경우 별도의 키 저장소를 구성할 수 있습니다.

디렉터리 서버 정보 수집

CA Directory 를 정책 저장소로 구성하려면 특정 디렉터리 서버 정보가 필요합니다. 정책 저장소를 구성하기 전에 다음 정보를 수집하십시오. 정책 저장소 워크시트를 사용하여 값을 기록할 수 있습니다.

- **호스트 정보** - CA Directory 가 실행되는 시스템의 정규화된 호스트 이름 또는 IP 주소를 확인합니다.
- **DSA 포트 번호** - DSA 가 수신 대기하는 포트를 확인합니다.
- **기본 DN** - LDAP 트리에서 정책 저장소 개체가 정의되는 노드의 고유 이름을 확인합니다.
- **관리 DN** - SiteMinder 가 DSA 에서 개체를 관리하는 데 사용하는 계정의 LDAP 사용자 이름을 확인합니다.
- **관리 암호** - 관리 사용자의 암호를 확인합니다.

정책 저장소를 구성하는 방법

CA Directory 를 정책 저장소로 구성하려면 다음 절차를 완료하십시오.

1. [정책 저장소에 대한 DSA 를 생성합니다](#) (페이지 100).
2. [정책 저장소 스키마를 생성합니다](#) (페이지 101).
3. [DSA 를 엽니다](#) (페이지 103).
4. [정책 저장소 데이터에 대한 기본 트리 구조를 생성합니다](#) (페이지 104).
5. [DSA 에 대한 슈퍼 사용자 관리자를 생성합니다](#) (페이지 105).
6. [정책 서버를 정책 저장소에 연결합니다](#) (페이지 105).
7. [SiteMinder 슈퍼 사용자 암호를 설정합니다](#) (페이지 106).
8. [CA Directory 캐시 구성을 확인합니다](#) (페이지 108).
9. [정책 저장소 데이터 정의를 가져옵니다](#) (페이지 109).
10. [기본 정책 저장소 개체를 가져옵니다](#) (페이지 109).
11. [관리 UI 등록을 준비합니다](#) (페이지 111).

정책 저장소의 DSA 만들기

다음 명령을 실행하여 DSA 를 생성합니다.

```
dxnewdsa DSA_Name port "o=DSA_Name,c=country_code"
```

DSA_Name

DSA 의 이름을 지정합니다.

port

DSA 가 수신 대기하는 포트를 지정합니다.

o=DSA_Name,c=country_code

DSA 접두사를 지정합니다.

예: "o=psdsa,c=US"

dxnewdsa 유틸리티가 새 DSA 를 시작합니다.

참고: DSA 가 자동으로 시작되지 않으면 다음을 실행하십시오.

```
dxserver start DSA_Name
```


정책 저장소 스키마 만들기

디렉터리 서버가 정책 저장소로 작동할 수 있도록 정책 저장소 스키마를 생성하십시오.

중요! 기본적으로 CA Directory 구성 파일은 읽기 전용입니다. 지침에 따라 수정해야 할 CA Directory 파일이 있는 경우 쓰기가 가능하도록 권한을 업데이트해야 합니다. 파일을 업데이트한 후 다시 읽기 전용으로 권한을 되돌릴 수 있습니다. 또한 CA Directory 에서 제공하는 모든 default.xxx 파일은 CA Directory 업그레이드 중 덮어쓰여집니다. 읽기 전용 파일을 수정할 때는 주의하십시오.

다음 단계를 수행하십시오.

1. 다음 파일을 CA Directory *DXHOME*\config\schema 디렉터리에 복사합니다.

- netegrity.dxc
- etrust.dxc

DXHOME

Directory Server 설치 경로를 지정합니다.

참고: netegrity.dxc 파일은 정책 서버와 함께 *siteminder_home*\eTrust 에 설치됩니다. etrust.dxc 파일은 정책 서버와 함께 *siteminder_home*\xps\db 에 설치됩니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

- Windows %*DXHOME*%
- Unix/Linux: \$*DXHOME*

2. default.dxc 스키마 파일을 복사한 후 이름을 바꿔 SiteMinder 스키마 파일을 생성합니다.

참고: default.dxc 스키마 파일은 *DXHOME*\config\schema\default.dxc 에 있습니다.

예: default.dxc 스키마 파일을 복사하고 복사본의 이름을 smdsa.dxc 로 바꿉니다.

3. 새 SiteMinder 스키마 파일의 맨 아래에 다음 행을 추가합니다.

```
#CA Schema
source "netegrity.dxc";
source "etrust.dxc";
```

4. DSA 의 DXI 파일(*DSA_Name.dxi*)을 편집하여 스키마를 *default.dxc* 에서 새 SiteMinder 스키마 파일로 변경합니다.

DSA_Name

정책 저장소에 대해 생성한 DSA 의 이름을 나타냅니다.

참고: DXI 파일은 *DXHOME\config\servers* 에 있습니다.

5. DSA 의 DXI 파일 끝에 다음 행을 추가합니다.

■ **r12**

```
# cache configuration
set max-cache-size = 100;
set cache-attrs = all-attributes;
set cache-load-all = true;
set ignore-name-bindings = true;
```

참고: max-cache-size 항목은 총 캐시 크기(MB)입니다. CA Directory Server 의 사용 가능한 총 메모리와 정책 저장소의 전체 크기에 따라 이 값을 조정하십시오.

■ **r12 SP1 이상**

```
# cache configuration
set ignore-name-bindings = true;
```

6. DSA 의 기본 제한 DXC 파일(*default.dxc*)을 복사하여 SiteMinder DXC 파일을 생성합니다.

예: 기본 DXC 파일을 복사한 후 복사본 *smdsa.dxc* 의 이름을 바꿉니다.

참고: 기본 DXC 파일은 *DXHOME\dxserver\config\limits* 에 있습니다.

7. 새 DXC 파일의 설정을 다음과 일치하도록 편집합니다.

```
# size limits
set max-users = 1000;
set credits = 5;
set max-local-ops = 1000;
set max-op-size = 4000;
set multi-write-queue = 20000;
```

참고: 크기 제한 설정을 편집하면 캐시 크기 오류가 CA Directory 로그 파일에 표시되지 않습니다.

중요! multi-write-queue 설정은 텍스트 기반 구성에서만 사용됩니다.
DXmanager 를 사용하여 DSA 를 설치한 경우에는 이 설정을 생략하십시오.

8. DXC 파일을 저장합니다.
9. DSA 의 DXI 파일(*DSA_Name.dxi*)을 편집하여 제한 구성을 default.dxc 에서 새 SiteMinder 제한 파일로 변경합니다.

예: 제한 구성을 default.dxc 에서 smdsa.dxc 로 변경합니다.

DSA_Name

정책 저장소에 대해 생성한 DSA 의 이름을 나타냅니다.

참고: DSA 의 DXI 파일은 DXHOME\config\servers 에 있습니다.
DXmanager 를 사용하여 DSA 를 생성한 경우 기존 제한 파일의 이름은 dxmanager.dxc 로 지정됩니다.

10. DSA 사용자 권한으로 다음 명령을 사용하여 DSA 를 중지했다가 다시 시작합니다.

```
dxserver stop DSA_Name
dxserver start DSA_Name
```

DSA_Name

DSA 의 이름을 지정합니다.

정책 저장소 스키마가 생성되었습니다.

DSA 열기

디렉터리 서버를 보여 주는 뷰를 생성하여 개체를 관리할 수 있습니다.

다음 단계를 수행하십시오.

1. 데이터베이스가 익명 로그인을 허용하도록 구성되어 있는지 확인합니다.
2. JXplorer GUI 를 시작합니다.
3. 연결 아이콘을 선택합니다.
연결 설정이 표시됩니다.

4. "Host Name"(호스트 이름) 필드에 *host_name_or_IP_address* 를 입력합니다.

host_name_or_IP_address

CA Directory 가 실행되는 시스템의 호스트 이름 또는 IP 주소를 지정합니다.

5. "Port number"(포트 번호) 필드에 *port_number* 를 입력합니다.

port_number

DSA 가 수신 대기하는 포트를 지정합니다.

6. "Base DN"(기본 DN) 필드에 *o=DSA_Name,c=country_code* 를 입력합니다.

예: *o=psdsa,c=US*

7. "Level"(수준) 목록에서 "Anonymous"(익명)를 선택하고 "Connect"(연결)를 클릭합니다.

DSA 뷰가 표시됩니다.

정책 저장소 데이터의 기본 트리 구조 만들기

정책 저장소 데이터를 보관할 기본 트리 구조를 생성할 수 있습니다. 조직 단위를 만드는 데는 JXplorer GUI 를 사용합니다.

다음 단계를 수행하십시오.

1. DSA 의 루트 요소를 선택합니다.
2. 루트 요소 아래에 다음 이름의 조직 단위를 생성합니다.
Netegrity
3. Netegrity 아래에 다음 이름의 조직 단위(루트 요소)를 생성합니다.
SiteMinder
4. SiteMinder 아래에 다음 이름의 조직 단위(루트 요소)를 생성합니다.
PolicySvr4
5. PolicySvr4 아래에 다음 이름의 조직 단위(루트 요소)를 생성합니다.
XPS

기본 트리 구조가 생성되었습니다.

DSA 에 대한 슈퍼 사용자 관리자 만들기

SiteMinder 가 DSA 에 액세스하는 데 사용할 수 있는 관리자 계정이 없을 경우에만 슈퍼 사용자 관리자를 생성해야 합니다. 정책 서버에서 정책 저장소를 연결하는 데 이 정보가 필요합니다.

다음 단계를 수행하십시오.

1. JXplorer GUI 를 사용하여 DSA 에 액세스합니다.
2. SiteMinder 가 정책 저장소에 액세스하는 데 사용할 수 있는 관리자를 생성합니다.

참고: 다음 개체 유형을 사용하여 사용자를 생성하십시오.

inetOrgPerson

3. 관리자 DN 과 암호를 기록합니다. 정책 서버를 정책 저장소에 연결할 때 이 자격 증명을 사용합니다.

예:

dn:cn=admin,o=yourcompany,c=in

정책 서버를 정책 저장소에 연결

정책 서버가 정책 저장소에 액세스할 수 있도록 정책 서버를 정책 저장소에 연결하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.

중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "데이터" 탭을 클릭합니다.
3. "데이터베이스" 목록에서 다음 값을 선택합니다.

정책 저장소

4. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

5. "LDAP 정책 저장소" 그룹 상자에서 다음 설정을 구성합니다.

- LDAP IP 주소
- 관리자 사용자 이름
- 암호
- 암호 확인
- 루트 DN

참고: "도움말"을 클릭하면 필드, 컨트롤 및 해당되는 요구 사항에 대한 설명을 볼 수 있습니다.

6. "적용"을 클릭합니다.

7. "LDAP 연결 테스트"를 클릭하여 정책 서버에서 정책 저장소에 액세스할 수 있는지 여부를 확인합니다.

8. "데이터베이스" 목록에서 다음 값을 선택합니다.

키 저장소

9. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

10. 다음 옵션을 선택합니다.

정책 저장소 데이터베이스 사용

11. "확인"을 클릭합니다.

SiteMinder 슈퍼 사용자 암호 설정

기본 SiteMinder 관리자 계정의 이름은 다음으로 지정됩니다.

siteminder

이 계정에는 최대 권한이 있습니다.

일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 다음과 같은 경우에 기본 슈퍼 사용자를 사용합니다.

- 관리 UI 에 처음 액세스할 경우
- SiteMinder 유틸리티를 처음 관리할 경우
- 슈퍼 사용자 권한이 있는 다른 관리자를 생성할 경우

다음 단계를 수행하십시오.

1. smreg 유틸리티를 *siteminder_home*\bin 에 복사합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

참고: 이 유틸리티는 정책 서버 설치 키트의 최상위 수준에 있습니다.

2. 다음 명령을 실행합니다.

```
smreg -su password
```

password

기본 SiteMinder 관리자의 암호를 지정합니다.

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: Oracle 정책 저장소를 구성하는 경우 암호의 대/소문자를 구분합니다. 다른 모든 정책 저장소에서는 암호의 대/소문자를 구분하지 않습니다.

3. *siteminder_home*\bin 에서 smreg 를 삭제합니다. smreg 를 삭제하면 이전 암호를 모르는 다른 사람은 암호를 변경할 수 없게 됩니다.

기본 SiteMinder 관리자 계정의 암호가 설정되었습니다.

CA Directory 캐시 구성 확인

DXconsole 을 사용하여 DXcache 설정이 활성화되었는지 확인할 수 있습니다.

참고: 기본적으로 DxConsole 은 localhost 에서만 액세스할 수 있습니다. set dsa 명령을 사용하여 DxConsole 에서 원격 시스템의 연결을 수락하도록 구성하는 방법에 대한 자세한 내용은 *Directory Configuration Guide*(디렉터리 구성 안내서)를 참조하십시오.

다음 단계를 수행하십시오.

1. 명령 프롬프트에서 다음 명령을 입력하여 텔넷을 통해 DSA DXConsole 포트에 연결합니다.

```
telnet DSA_Host DXconsole_Port
```

DSA_Host

DSA 를 호스트하는 시스템의 호스트 이름 또는 IP 주소를 지정합니다.

참고: localhost 에 있을 경우 **localhost** 를 입력합니다. 호스트 이름 또는 IP 주소를 입력하면 연결이 실패합니다.

DXConsole_Port

DXconsole 가 수신 대기하는 포트를 지정합니다. 이 값은 다음 파일에서 console-port 매개 변수에 표시됩니다.

```
DXHOME\config\knowledge\DSA_Name.dxc
```

기본값: DXconsole 포트는 DSA 포트+1 의 값으로 설정됩니다.

예: DSA 가 포트 19389 에서 실행되면 DXconsole 포트는 19390 입니다.

DSA 관리 콘솔이 표시됩니다.

2. 다음 명령을 입력합니다.

```
get cache;
```

DSA 관리 콘솔은 현재 DSA DXcache 설정을 보여 주고 디렉터리 캐시 상태를 지정합니다.

3. 다음 명령을 입력합니다.

```
logout;
```

DXconsole 을 닫고 시스템 프롬프트로 돌아갑니다.

정책 저장소 데이터 정의 가져오기

정책 저장소 데이터 정의 가져오기를 사용하여 정책 저장소에서 생성하고 저장할 수 있는 개체의 유형을 정의합니다.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home*\xps\dd 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

```
XPSDDInstall SmMaster.xdd
```

XPSDDInstall

필수 데이터 정의를 가져옵니다.

기본 정책 저장소 개체 가져오기

기본 정책 저장소 개체 가져오기를 사용하여 관리 UI 및 정책 서버에서 사용할 정책 저장소를 구성합니다.

다음 사항을 고려하십시오.

- *siteminder_home*\bin 에 대한 쓰기 액세스 권한이 있는지 확인하십시오. 가져오기 유틸리티에서 정책 저장소 개체를 가져오려면 이 권한이 필요합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

- Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 `siteminder_home\db` 로 이동합니다.

2. 다음 파일 중 하나를 가져옵니다.

- `smpolicy.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy.xml -npass
```

- `smpolicy-secure.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy-secure.xml -npass
```

npass

암호를 사용할 필요가 없음을 지정합니다. 기본 정책 저장소 개체에 암호화된 데이터가 포함되지 않습니다.

두 파일 모두 기본 정책 저장소 개체를 포함합니다. 이러한 개체는 기본 ACO(에이전트 구성 개체) 템플릿의 기본 보안 설정을 포함합니다. `smpolicy-secure` 파일은 보다 제한적인 보안 설정을 제공합니다. 자세한 내용은 [기본 정책 저장소 개체 고려 사항](#) (페이지 98)을 참조하십시오.

- 옵션 팩 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport ampolicy.xml -npass
```

- 페더레이션 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

정책 저장소 개체를 가져왔습니다.

참고: `smpolicy.xml` 을 가져오면 SiteMinder 에서 별도로 라이선스가 제공되는 레거시 페더레이션 및 웹 서비스 변수 기능을 사용할 수 있게 됩니다. 웹 서비스 변수 기능을 사용하려면 CA 고객 담당자에게 라이선스 정보에 대해 문의하십시오.

고급 인증 서버를 사용하도록 설정

정책 서버를 구성하는 과정에서 고급 인증 서버를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 구성 마법사를 시작합니다.
2. 마법사의 첫 번째 화면에서 모든 확인란을 **선택 취소**한 상태로 둡니다.
3. "다음"을 클릭합니다.
4. 고급 인증 서버에 대한 마스터 암호화 키를 생성합니다.

참고: 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

5. 정책 서버 구성 마법사의 나머지 과정을 완료합니다.
고급 인증 서버가 사용되도록 설정되었습니다.

관리 UI 등록 준비

기본 SiteMinder 슈퍼 사용자 계정(siteminder)을 사용하여 관리 UI 에 최초로 로그인합니다. 최초 로그인 시 관리 UI 를 정책 서버에 등록하여 두 구성 요소 간에 트러스트 관계를 생성해야 합니다.

등록을 준비하려면 XPSRegClient 유틸리티를 사용하여 슈퍼 사용자 계정 이름과 암호를 제공합니다. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 트러스트 관계를 설정할 수 있는지 확인합니다.

다음 사항을 고려하십시오.

- 자격 증명을 제공한 때부터 **24 시간** 이내에 최초 관리 UI 로그인 이루어져야 합니다. 관리 UI 설치를 하루 안에 수행할 계획이 아니면 관리 UI 를 설치하기 전에 다음 단계를 완료하십시오.
- (UNIX) XPSRegClient 를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c  
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

기본 SiteMinder 슈퍼 사용자 계정(siteminder)의 암호를 지정합니다.

참고: 암호를 지정하지 않으면 XPSRegClient 에서 암호를 입력하고
확인하라는 메시지가 표시됩니다.

-adminui-setup

관리 UI 가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 관리 UI 를 설치할 때부터 정책 서버에 로그인하고 정책
서버와의 트러스트 관계를 생성할 때까지 할당된 시간을
지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록
요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 15

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI 를 등록할 때 허용되는 시도 실패 횟수를
지정합니다. 관리 UI 에 최초로 로그인할 때 올바르게 않은
SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수
있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을
삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error_path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: `stderr`

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

XPSRegClient 가 정책 서버에 관리자 자격 증명을 제공합니다. 정책 서버에서는 관리 UI 에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

CA Directory 를 세션 저장소로 사용

CA Directory 를 세션 저장소로 구성할 수 있습니다.

참고: 지원되는 버전에 대한 자세한 내용은 "12.52 SP1 SiteMinder Platform Support Matrix"(12.52 SP1 SiteMinder 플랫폼 지원표)를 참조하십시오.

세션 저장소를 구성하는 방법

CA Directory 를 세션 저장소로 구성하려면 다음 태스크를 수행하십시오.

1. 세션 저장소 스키마 파일을 가져옵니다.
2. 세션 저장소에 대한 DSA 를 생성합니다.
3. 세션 저장소 관리 사용자 및 루트 DN 을 추가합니다.
4. 세션 저장소 스키마를 생성합니다.
5. 정책 서버를 세션 저장소에 연결합니다.

세션 저장소 스키마 파일 가져오기

필요한 모든 세션 저장소 스키마 파일이 정책 서버와 함께 설치됩니다. SiteMinder 관리자에게 문의하여 다음 파일을 요청하십시오.

netegrity.dxc

DSA 세션 저장소 스키마를 생성합니다. 이 스키마를 통해 DSA 가 SiteMinder 사용자의 세션 정보를 저장하고 검색할 수 있습니다.

이 파일은 *siteminder_home\etTrust* 에 있습니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

세션 저장소에 대한 DSA 만들기

DSA 를 생성하고 용도를 세션 저장소 전용으로 한정합니다. 전용 DSA 를 사용하면 세션 저장소 성능을 최대화할 수 있습니다.

다음 단계를 수행하십시오.

1. CA Directory 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 데이터 DSA 를 생성합니다.

```
dxnewdsa dsa_name port prefix
```

dsa_name

세션 저장소 DSA 의 이름을 지정합니다.

port

세션 저장소가 요청을 수신 대기하는 포트를 지정합니다.

prefix

네임스페이스 접두사를 지정합니다. LDAP 구문을 사용하여 접두사를 지정합니다.

예: 세션 저장소에 대한 데이터 DSA 를 생성합니다.

```
dxnewdsa smsessionstore 1234 o=forwardinc,c=us
```

참고: Forward, Inc.는 설명용으로만 사용되는 가상의 회사 이름으로, 실제 회사를 가리키지 않습니다.

세션 저장소 관리 사용자 및 루트 DN 추가

정책 서버에는 다음 사항이 필요합니다.

- DSA 에 있는 사용자의 전체 고유 이름(DN)과 암호. 정책 서버에서는 이 자격 증명을 사용하여 세션 저장소를 관리합니다.
- 세션 정보를 쓸 수 있는 루트 DN

다음 단계를 수행하십시오.

1. 다음 방법 중 *하나*로 익명 인증을 사용하여 DSA 에 액세스합니다.
 - JXplorer 도구를 사용합니다.
 - CA Directory [명령줄 인터페이스](#)를 사용합니다.
2. SiteMinder 의 세션 저장소 관리에 사용할 수 있는 사용자를 생성합니다.
 - 다음 개체 클래스만 포함하는 사용자를 생성해야 합니다.
inetOrgPerson
 - 자격 증명을 기록합니다. 정책 서버를 세션 저장소 DSA 에 연결하려면 이 자격 증명에 필요합니다.
3. JXplorer 연결을 해제합니다.
4. JXplorer 를 시작합니다.
5. 앞서 생성한 관리 사용자의 전체 DN 을 사용하여 DSA 에 로그인하여 DSA 에 액세스할 수 있는지 확인합니다.
예: cn=admin,o=forwardinc,c=us
6. 세션 저장소의 루트 DN 으로 사용할 조직 단위를 수동으로 생성합니다.
예: ou=sessionstore
7. JXplorer 연결을 해제합니다.

참고: 세션 저장소에 대한 권한 없는 액세스를 방지하도록 익명 인증을 비활성화하는 것이 좋습니다.

세션 저장소 스키마 만들기

DSA 에서 SiteMinder 사용자의 세션 정보를 저장하고 검색하려면 스키마가 필요합니다.

다음 단계를 수행하십시오.

1. CA Directory 호스트 시스템에 로그인합니다.
2. 다음 명령을 사용하여 DSA 를 중지합니다.
dxserver stop DSA_Name
3. DXHOME\config\schema 에 SiteMinder 세션 저장소 스키마 파일(netegrity.dxc)을 추가합니다.
4. DXHOME\config\schema 로 이동합니다.

5. DSA 의 기본 스키마 파일(default.dxc)을 복사하여 읽기 전용 특성을 제거한 다음 이름을 변경하여 세션 저장소 스키마를 생성합니다.

예: default.dxc 를 복사한 후 복사본의 이름을 smsession.dxc 로 바꿉니다.

6. 세션 저장소 스키마 파일을 편집합니다.

- a. 파일 맨 아래에 다음 행을 추가합니다.

```
#CA Schema
source "netegrity.dxc";
```

- b. 파일을 저장합니다.

- c. 읽기 전용 특성을 적용합니다.

7. DXHOME\dxserver\config\limits 로 이동합니다.

8. 기본 제한 파일(default.dxc)을 복사하여 읽기 전용 특성을 제거한 다음 이름을 변경하여 세션 저장소 제한 파일을 생성합니다.

예: default.dxc 를 복사한 후 복사본의 이름을 smsession.dxc 로 바꿉니다.

9. 세션 저장소 기본 제한 파일을 편집합니다.

- a. max-local-ops 특성을 다음 값과 일치하도록 편집합니다.

```
set max-op-size = 1000;
```

이 특성은 size limits 섹션에 있으며 상한을 나타냅니다. 세션 저장소는 검색 쿼리당 1,000 개 이상의 개체를 반환하지 않아야 합니다.

- b. 파일을 저장합니다.

- c. 읽기 전용 특성을 적용합니다.

10. DXHOME\config\servers 로 이동하여 세션 저장소 초기화 파일(DSA_name.dxi)을 엽니다.

DSA_name

세션 저장소 DSA 의 이름을 지정합니다.

11. 세션 저장소 초기화 파일을 편집합니다.

- a. 스키마 참조를 default.dxc 에서 세션 저장소 스키마 파일로 편집합니다.

이 참조는 schema 섹션에 있습니다.

예: default.dxc 를 smsession.dxc 로 변경합니다.

- b. 서비스 제한 참조를 `default.dxc` 에서 세션 저장소 제한 파일로 편집합니다.

이 참조는 `service limits` 섹션에 있습니다.

예: `default.dxc` 를 `smsession.dxc` 로 변경합니다.

- c. `set-cache index` 특성을 다음 설정과 일치하도록 편집합니다.

```
set cache-index-all-except = smVariableValue,smsessionblob;
```

참고: `cache index all` 특성을 다음 특성보다 먼저 설정해야 합니다.

```
set lookup-cache = true;
```

이 특성은 `grid configuration` 섹션에 있습니다.

- d. (선택 사항) 다음 특성을 압축하여 메모리에 더 많은 세션 개체를 저장합니다.

`smVariableValue`

- e. (선택 사항) 트랜잭션 로깅을 비활성화하여 성능을 향상시킵니다.

중요! 트랜잭션 로깅을 비활성화할 경우 데이터 복구에 미치는 영향을 고려하십시오. 자세한 내용은 **CA Directory** 설명서를 참조하십시오.

- 12. 다음 명령을 사용하여 **DSA** 를 시작합니다.

```
dxserver start DSA_Name
```

세션 저장소 스키마가 생성됩니다.

정책 서버를 세션 저장소에 연결

SiteMinder 가 세션 저장소를 관리할 수 있도록 정책 서버를 세션 저장소 **DSA** 에 연결합니다.

다음 단계를 수행하십시오.

- 1. 정책 서버 관리 콘솔을 엽니다.

중요! **Windows Server 2008** 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 **SiteMinder** 구성 요소의 릴리스 정보를 참조하십시오.

- 2. "데이터" 탭을 클릭합니다.
- 3. "데이터베이스" 목록에서 "세션 저장소"를 선택합니다.

4. "저장소" 목록에서 "CA Directory"를 선택합니다.
 5. "세션 저장소 사용" 옵션을 선택합니다.
 6. "LDAP 세션 저장소" 섹션 아래에서 다음 작업을 수행하십시오.
 - a. 세션 저장소 DSA 의 IP 주소와 포트를 입력합니다.
 - b. 세션 저장소 DSA 의 루트 DN 을 입력합니다.
예: ou=sessionstore,o=fowardinc,c=us
 - c. DSA 의 관리 사용자에게 대한 전체 DN 을 입력합니다.
예: cn=admin,o=forwardinc,c=us
 - d. 관리 사용자의 암호를 입력합니다.
 7. "LDAP 연결 테스트"를 클릭하여 연결을 확인합니다.
 8. "확인"을 클릭합니다.
- SiteMinder 가 세션 저장소를 관리하도록 구성됩니다.

Active Directory 를 정책 저장소로 구성

Active Directory 는 정책 저장소로 작동할 수 있습니다. 단일 디렉터리 서버 인스턴스가 다음 기능을 수행할 수 있습니다.

- 정책 저장소
- 키 저장소

단일 디렉터리 서버를 사용하면 관리 태스크를 간소화할 수 있습니다. 다음 단위에서는 정책 데이터 및 암호화 키를 저장하도록 단일 디렉터리 서버 인스턴스를 구성하는 방법에 대한 지침을 제공합니다. 구현에 필요할 경우 별도의 키 저장소를 구성할 수 있습니다.

참고: Active Directory 가 SSL 을 통해 정책 서버와 통신할 경우 SSL 클라이언트 인증서에 SubjectDN 의 CN 이 포함되어야 합니다. SSL 클라이언트 인증서에 이 정보가 포함되지 않으면 정책 서버가 작동하지 않습니다.

디렉터리 서버 정보 수집

LDAP 디렉터리 서버를 정책 저장소로 구성하거나 기존 정책 저장소를 업그레이드하려면 특정 디렉터리 서버 정보가 필요합니다. 시작하기 전에 다음 정보를 수집하십시오. 정책 저장소 워크시트를 사용하여 값을 기록할 수 있습니다.

호스트 정보

디렉터리 서버의 정규화된 호스트 이름 또는 IP 주소를 지정합니다.

포트 정보

(선택 사항) 비표준 포트를 지정합니다.

기본값: 636(SSL) 및 389(비 SSL)

관리 DN

LDAP 트리에서 정책 저장소 루트 개체 아래의 개체에 대한 생성, 읽기, 수정 및 삭제 권한이 있는 사용자의 LDAP 사용자 이름을 지정합니다.

관리 암호

관리 DN 의 암호를 지정합니다.

정책 저장소 루트 DN

LDAP 트리에서 정책 저장소 개체가 정의될 노드의 고유 이름을 지정합니다.

SSL 클라이언트 인증서

SSL 클라이언트 인증서 데이터베이스 파일이 있는 디렉터리의 경로 이름을 지정합니다.

제한: SSL 에만 해당

정책 저장소를 구성하는 방법

Active Directory 디렉터리 서버를 정책 저장소로 구성하려면 다음 절차를 완료하십시오.

1. (선택 사항) 해당하는 경우 공급업체별 소프트웨어를 사용하여 LDAP 디렉터리 서버 인스턴스를 생성합니다.
2. (선택 사항) 해당하는 경우 공급업체별 소프트웨어를 사용하여 다음 권한이 있는 사용자를 생성합니다.

- create
- 읽기
- 수정
- 삭제

LDAP 트리에서 정책 저장소 루트 개체 아래에 이 사용자를 생성합니다.

3. 정책 서버를 디렉터리 서버에 연결합니다.
4. 정책 저장소 스키마를 생성합니다.
5. SiteMinder 슈퍼 사용자 암호를 설정합니다.
6. 정책 저장소 데이터 정의를 가져옵니다.
7. 기본 정책 저장소 개체를 가져옵니다.
8. 정책 서버를 다시 시작합니다.
9. 관리 UI 등록을 준비합니다.

정책 서버를 정책 저장소에 연결

정책 서버가 정책 저장소에 액세스할 수 있도록 정책 서버를 정책 저장소에 연결하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.

중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자 권한으로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "데이터" 탭을 클릭합니다.

3. "데이터베이스" 목록에서 다음 값을 선택합니다.

정책 저장소

4. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

5. "LDAP 정책 저장소" 그룹 상자에서 다음 설정을 구성합니다.

- LDAP IP 주소
- 관리자 사용자 이름
- 암호
- 암호 확인
- 루트 DN

참고: "도움말"을 클릭하면 필드, 컨트롤 및 해당되는 요구 사항에 대한 설명을 볼 수 있습니다.

6. "적용"을 클릭합니다.

7. "LDAP 연결 테스트"를 클릭하여 정책 서버에서 정책 저장소에 액세스할 수 있는지 여부를 확인합니다.

8. "데이터베이스" 목록에서 다음 값을 선택합니다.

키 저장소

9. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

10. 다음 옵션을 선택합니다.

정책 저장소 데이터베이스 사용

11. "확인"을 클릭합니다.

정책 저장소 스키마 만들기

디렉터리 서버가 정책 저장소로 작동하고 SiteMinder 개체를 저장할 수 있도록 정책 저장소 스키마를 생성하십시오.

중요! Active Directory 스키마는 루트 도메인이 소유합니다. 따라서 모든 스키마 변경은 스키마 마스터를 포함하는 루트 도메인 컨트롤러에서 SchemaAdmins 권한이 있는 계정을 사용하여 수행해야 합니다. 자식 도메인(복제본)에서 스키마를 변경할 수 없습니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에서 다음 명령을 실행합니다.

```
smlldapsetup ldgen -ffile_name
file_name
```

생성하려는 LDIF 파일의 이름을 지정합니다.

SiteMinder 스키마를 사용하여 LDIF 파일이 생성됩니다.

2. 다음 명령을 실행합니다.

```
smlldapsetup ldmod -ffile_name
file_name
```

생성한 LDIF 의 이름을 지정합니다.

유틸리티에서 정책 저장소 스키마를 가져옵니다.

3. `policy_server_home\xps\db` 로 이동하고 다음 파일을 엽니다.

```
ActiveDirectory.ldif
```

4. 수동으로 <RootDN>의 각 인스턴스를 정책 저장소 개체 위치가 아닌 정책 저장소 스키마 위치를 나타내는 DN 으로 바꿉니다.

예: 다음 루트 DN 은 정책 저장소 개체를 나타냅니다.

```
ou=policystore,dc=domain,dc=com
```

<RootDN>의 각 인스턴스를 다음 DN 으로 바꾸십시오.

```
dc=domain,dc=com
```

5. 다음 명령을 실행합니다.

```
smlldapsetup ldmod  
-fpolicy_server_home\xps\db\ActiveDirectory.ldif
```

policy_server_home

정책 서버 설치 경로를 지정합니다.

정책 저장소 스키마가 확장됩니다. 정책 저장소 스키마를 생성했습니다.

SiteMinder 슈퍼 사용자 암호 설정

기본 SiteMinder 관리자 계정의 이름은 다음으로 지정됩니다.

siteminder

이 계정에는 최대 권한이 있습니다.

일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 다음과 같은 경우에 기본 슈퍼 사용자를 사용합니다.

- 관리 UI 에 처음 액세스할 경우
- SiteMinder 유틸리티를 처음 관리할 경우
- 슈퍼 사용자 권한이 있는 다른 관리자를 생성할 경우

다음 단계를 수행하십시오.

1. smreg 유틸리티를 *siteminder_home*\bin 에 복사합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

참고: 이 유틸리티는 정책 서버 설치 키트의 최상위 수준에 있습니다.

2. 다음 명령을 실행합니다.

```
smreg -su password
```

password

기본 SiteMinder 관리자의 암호를 지정합니다.

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: Oracle 정책 저장소를 구성하는 경우 암호의 대/소문자를 구분합니다. 다른 모든 정책 저장소에서는 암호의 대/소문자를 구분하지 않습니다.

3. *siteminder_home\bin* 에서 *smreg* 를 삭제합니다. *smreg* 를 삭제하면 이전 암호를 모르는 다른 사람은 암호를 변경할 수 없게 됩니다.

기본 SiteMinder 관리자 계정의 암호가 설정되었습니다.

정책 저장소 데이터 정의 가져오기

정책 저장소 데이터 정의 가져오기를 사용하여 정책 저장소에서 생성하고 저장할 수 있는 개체의 유형을 정의합니다.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home\bin* 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

```
XPSDDInstall SmMaster.xdd
```

XPSDDInstall

필수 데이터 정의를 가져옵니다.

기본 정책 저장소 개체 가져오기

기본 정책 저장소 개체 가져오기를 사용하여 관리 UI 및 정책 서버에서 사용할 정책 저장소를 구성합니다.

다음 사항을 고려하십시오.

- *siteminder_home\bin* 에 대한 쓰기 액세스 권한이 있는지 확인하십시오. 가져오기 유틸리티에서 정책 저장소 개체를 가져오려면 이 권한이 필요합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

- Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home\db* 로 이동합니다.

2. 다음 파일 중 하나를 가져옵니다.

- *smpolicy.xml* 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy.xml -npass
```

- *smpolicy-secure.xml* 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy-secure.xml -npass
```

npass

암호를 사용할 필요가 없음을 지정합니다. 기본 정책 저장소 개체에 암호화된 데이터가 포함되지 않습니다.

두 파일 모두 기본 정책 저장소 개체를 포함합니다. 이러한 개체는 기본 ACO(에이전트 구성 개체) 템플릿의 기본 보안 설정을 포함합니다. *smpolicy-secure* 파일은 보다 제한적인 보안 설정을 제공합니다. 자세한 내용은 [기본 정책 저장소 개체 고려 사항](#) (페이지 98)을 참조하십시오.

- 옵션 팩 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport ampolicy.xml -npass
```

- 페더레이션 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

정책 저장소 개체를 가져왔습니다.

참고: *smpolicy.xml* 을 가져오면 SiteMinder 에서 별도로 라이선스가 제공되는 레거시 페더레이션 및 웹 서비스 변수 기능을 사용할 수 있게 됩니다. 웹 서비스 변수 기능을 사용하려면 CA 고객 담당자에게 라이선스 정보에 대해 문의하십시오.

고급 인증 서버를 사용하도록 설정

정책 서버를 구성하는 과정에서 고급 인증 서버를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 구성 마법사를 시작합니다.
2. 마법사의 첫 번째 화면에서 모든 확인란을 **선택 취소**한 상태로 둡니다.
3. "다음"을 클릭합니다.
4. 고급 인증 서버에 대한 마스터 암호화 키를 생성합니다.

참고: 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

5. 정책 서버 구성 마법사의 나머지 과정을 완료합니다.
고급 인증 서버가 사용되도록 설정되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 **stop-all** 명령 다음에 **start-all** 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

관리 UI 등록 준비

기본 SiteMinder 슈퍼 사용자 계정(siteminder)을 사용하여 관리 UI 에 최초로 로그인합니다. 최초 로그인 시 관리 UI 를 정책 서버에 등록하여 두 구성 요소 간에 트러스트 관계를 생성해야 합니다.

등록을 준비하려면 XPSRegClient 유틸리티를 사용하여 슈퍼 사용자 계정 이름과 암호를 제공합니다. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 트러스트 관계를 설정할 수 있는지 확인합니다.

다음 사항을 고려하십시오.

- 자격 증명을 제공한 때부터 24 시간 이내에 최초 관리 UI 로그인이 이루어져야 합니다. 관리 UI 설치를 하루 안에 수행할 계획이 아니면 관리 UI 를 설치하기 전에 다음 단계를 완료하십시오.
- (UNIX) XPSRegClient 를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

기본 SiteMinder 슈퍼 사용자 계정(siteminder)의 암호를 지정합니다.

참고: 암호를 지정하지 않으면 XPSRegClient 에서 암호를 입력하고 확인하라는 메시지가 표시됩니다.

-adminui-setup

관리 UI 가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 관리 UI 를 설치할 때부터 정책 서버에 로그인하고 정책 서버와의 트러스트 관계를 생성할 때까지 할당된 시간을 지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록 요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 15

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI 를 등록할 때 허용되는 시도 실패 횟수를 지정합니다. 관리 UI 에 최초로 로그인할 때 올바르게 않은 SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수 있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을 삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error_path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: stderr

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

XPSRegClient 가 정책 서버에 관리자 자격 증명을 제공합니다. 정책 서버에서는 관리 UI 에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

Active Directory ObjectCategory 인덱싱 특성 지원

다른 LDAP 호환 디렉터리와 달리 Active Directory 는 기본적으로 objectClass 특성을 사용하여 정책 저장소 개체를 인덱싱하지 않고 대신 objectCategory 특성을 기준으로 개체를 인덱싱합니다. 검색 성능을 개선하려면 objectClass 를 인덱싱 가능한 특성으로 구성하거나(Active Directory 설명서 참조) 정책 서버에서 objectCategory 지원이 사용되도록 설정하면 됩니다.

ObjectCategory 특성 지원이 사용되거나 사용되지 않도록 설정

Windows 의 경우:

다음 단계를 수행하십시오.

1. Windows 레지스트리 편집기를 실행합니다.
2. HKLM\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\DS\LDAPProvider 키를 찾습니다.
 - a. 지원이 사용되도록 설정하려면 EnableObjectCategory 값을 1 로 설정합니다.
 - b. 지원이 사용되지 않도록 설정하려면 EnableObjectCategory 값을 0 으로 설정합니다.

참고: 기본값은 0 입니다.

UNIX 의 경우:

다음 단계를 수행하십시오.

1. 텍스트 편집기에서 <siteminder_installation>/registry 에 있는 SiteMinder sm.registry 파일을 엽니다.
2. 다음 키를 찾습니다.
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider.
 - a. 지원이 사용되도록 설정하려면 EnableObjectCategory 값을 1 로 설정합니다.
 - b. 지원이 사용되지 않도록 설정하려면 EnableObjectCategory 값을 0 으로 설정합니다.

참고: 기본값은 0 입니다.

Domino Directory Server 를 정책 저장소로 구성

Domino Directory Server 는 정책 저장소로 작동할 수 있습니다. 단일 디렉터리 서버 인스턴스가 다음 기능을 수행할 수 있습니다.

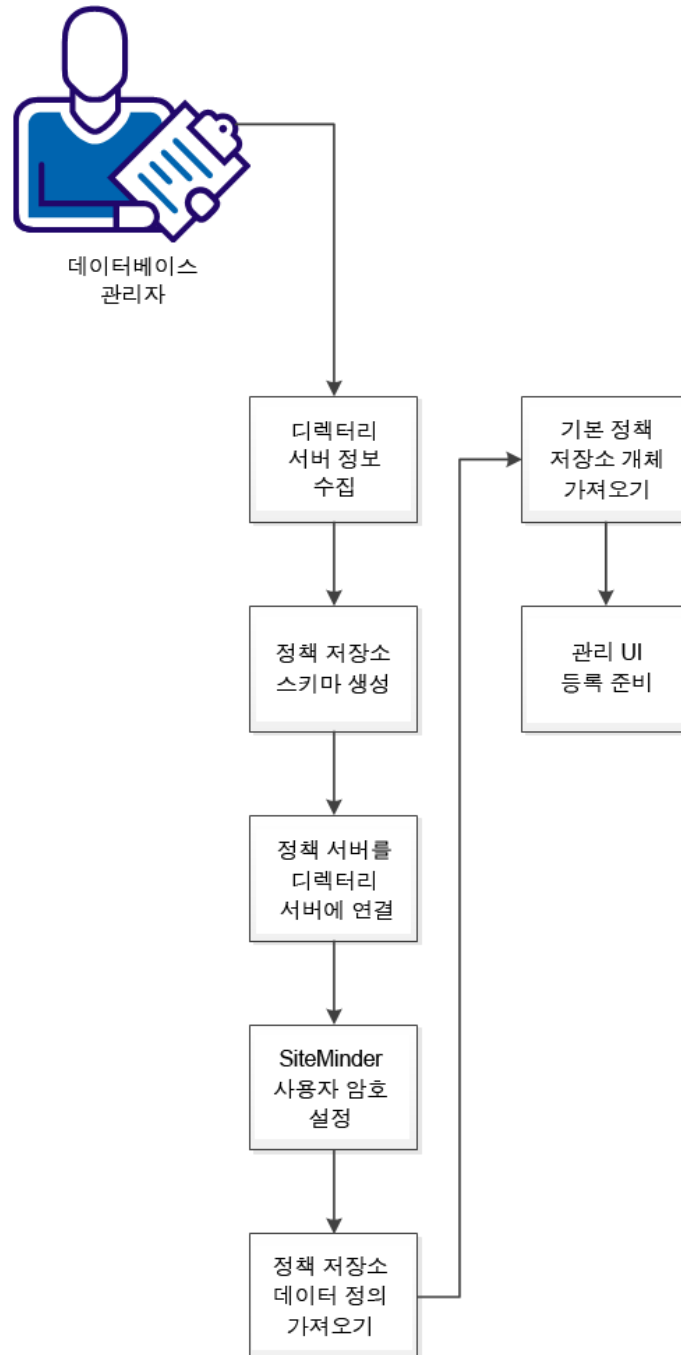
- 정책 저장소
- 키 저장소

단일 디렉터리 서버를 사용하면 관리 태스크를 간소화할 수 있습니다. 다음 단원에서는 정책 데이터 및 암호화 키를 저장하도록 단일 디렉터리 서버 인스턴스를 구성하는 방법에 대한 지침을 제공합니다. 구현에 필요할 경우 별도의 키 저장소를 구성할 수 있습니다.

Domino Directory Server 를 정책 저장소로 구성하는 방법

이 시나리오에서는 데이터베이스 관리자가 Domino Directory Server 버전 8.5 를 SiteMinder 정책 저장소로 구성하는 방법을 설명합니다.

이 구성 프로세스에는 몇 가지 독립 절차가 포함됩니다. 다음 그림은 워크플로를 보여 줍니다.



Domino Directory Server 버전 8.5 를 SiteMinder 정책 저장소로 구성하려면 다음 단계를 수행하십시오.

1. [디렉터리 서버 정보를 수집합니다](#) (페이지 120).
2. [정책 저장소 스키마를 생성합니다](#) (페이지 136).
3. [정책 서버를 디렉터리 서버에 연결합니다](#) (페이지 105).
4. [SiteMinder 슈퍼 사용자 암호를 설정합니다](#) (페이지 106).
5. [정책 저장소 데이터 정의를 가져옵니다](#) (페이지 109).
6. [기본 정책 저장소 개체를 가져옵니다](#) (페이지 109).
7. [관리 UI 등록을 준비합니다](#) (페이지 111).

디렉터리 서버 정보 수집

LDAP 디렉터리 서버를 정책 저장소로 구성하거나 기존 정책 저장소를 업그레이드하려면 특정 디렉터리 서버 정보가 필요합니다. 시작하기 전에 다음 정보를 수집하십시오. 정책 저장소 워크시트를 사용하여 값을 기록할 수 있습니다.

호스트 정보

디렉터리 서버의 정규화된 호스트 이름 또는 IP 주소를 지정합니다.

포트 정보

(선택 사항) 비표준 포트를 지정합니다.

기본값: 636(SSL) 및 389(비 SSL)

관리 DN

LDAP 트리에서 정책 저장소 루트 개체 아래의 개체에 대한 생성, 읽기, 수정 및 삭제 권한이 있는 사용자의 LDAP 사용자 이름을 지정합니다.

관리 암호

관리 DN 의 암호를 지정합니다.

정책 저장소 루트 DN

LDAP 트리에서 정책 저장소 개체가 정의될 노드의 고유 이름을 지정합니다.

SSL 클라이언트 인증서

SSL 클라이언트 인증서 데이터베이스 파일이 있는 디렉터리의 경로 이름을 지정합니다.

제한: SSL에만 해당

정책 저장소 스키마 만들기

Domino Directory Server 가 정책 저장소로 작동할 수 있도록 정책 저장소 스키마를 생성하십시오.

다음 단계를 수행하십시오.

1. Domino Directory Service 를 중지합니다.
2. Domino Directory Server 에서 다음 파일의 백업 복사본을 생성합니다.
`domino_home\data\schema.nsf`
3. 정책 서버에서 다음 파일을 찾습니다.
`policy_server_home\db\tier2\IBM_Lotus_Domino_DirectoryServer\schema.nsf`
4. 3 단계의 파일을 Domino Directory Server 의 다음 폴더로 복사합니다.
`domino_home\data`
5. Domino Directory Service 를 시작합니다.
6. Domino Directory Server 에서 `schema.nsf` 파일을 엽니다.
7. 모든 xps 및 SiteMinder 개체와 특성이 있는지 확인합니다.
8. LDAP 브라우저를 사용하여 Domino LDAP 디렉터리에 연결합니다.
9. SiteMinder 에 대한 다음 기본 DN 을 생성합니다.
`Netegrity/SiteMinder/PolicySvr4`
10. Domino Directory Service 를 다시 시작합니다.
11. 서비스를 콘솔 모드로 엽니다.
12. 다음 명령을 사용하여 디렉터리의 인덱스를 업데이트합니다.
`load updall -r`
13. Domino Directory Service 를 다시 시작합니다.

정책 서버를 정책 저장소에 연결

정책 서버가 정책 저장소에 액세스할 수 있도록 정책 서버를 정책 저장소에 연결하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.

중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "데이터" 탭을 클릭합니다.
3. "데이터베이스" 목록에서 다음 값을 선택합니다.

정책 저장소

4. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

5. "LDAP 정책 저장소" 그룹 상자에서 다음 설정을 구성합니다.

- LDAP IP 주소
- 관리자 사용자 이름
- 암호
- 암호 확인
- 루트 DN

참고: "도움말"을 클릭하면 필드, 컨트롤 및 해당되는 요구 사항에 대한 설명을 볼 수 있습니다.

6. "적용"을 클릭합니다.
7. "LDAP 연결 테스트"를 클릭하여 정책 서버에서 정책 저장소에 액세스할 수 있는지 여부를 확인합니다.
8. "데이터베이스" 목록에서 다음 값을 선택합니다.

키 저장소

9. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

10. 다음 옵션을 선택합니다.

정책 저장소 데이터베이스 사용

11. "확인"을 클릭합니다.

SiteMinder 슈퍼 사용자 암호 설정

기본 SiteMinder 관리자 계정의 이름은 다음으로 지정됩니다.

siteminder

이 계정에는 최대 권한이 있습니다.

일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다.
다음과 같은 경우에 기본 슈퍼 사용자를 사용합니다.

- 관리 UI 에 처음 액세스할 경우
- SiteMinder 유틸리티를 처음 관리할 경우
- 슈퍼 사용자 권한이 있는 다른 관리자를 생성할 경우

다음 단계를 수행하십시오.

1. smreg 유틸리티를 *siteminder_home*\bin 에 복사합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

참고: 이 유틸리티는 정책 서버 설치 키트의 최상위 수준에 있습니다.

2. 다음 명령을 실행합니다.

smreg -su *password*

password

기본 SiteMinder 관리자의 암호를 지정합니다.

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: Oracle 정책 저장소를 구성하는 경우 암호의 대/소문자를 구분합니다. 다른 모든 정책 저장소에서는 암호의 대/소문자를 구분하지 않습니다.

3. *siteminder_home\bin* 에서 **smreg** 를 삭제합니다. **smreg** 를 삭제하면 이전 암호를 모르는 다른 사람은 암호를 변경할 수 없게 됩니다.
기본 SiteMinder 관리자 계정의 암호가 설정되었습니다.

정책 저장소 데이터 정의 가져오기

정책 저장소 데이터 정의 가져오기를 사용하여 정책 저장소에서 생성하고 저장할 수 있는 개체의 유형을 정의합니다.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home\bin* 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

```
XPSSDIInstall SmMaster.xdd
```

XPSSDIInstall

필수 데이터 정의를 가져옵니다.

기본 정책 저장소 개체 가져오기

기본 정책 저장소 개체 가져오기를 사용하여 관리 UI 및 정책 서버에서 사용할 정책 저장소를 구성합니다.

다음 사항을 고려하십시오.

- *siteminder_home\bin* 에 대한 쓰기 액세스 권한이 있는지 확인하십시오. 가져오기 유틸리티에서 정책 저장소 개체를 가져오려면 이 권한이 필요합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

- Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 `siteminder_home\db` 로 이동합니다.

2. 다음 파일 중 하나를 가져옵니다.

- `smpolicy.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy.xml -npass
```

- `smpolicy-secure.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy-secure.xml -npass
```

npass

암호를 사용할 필요가 없음을 지정합니다. 기본 정책 저장소 개체에 암호화된 데이터가 포함되지 않습니다.

두 파일 모두 기본 정책 저장소 개체를 포함합니다. 이러한 개체는 기본 ACO(에이전트 구성 개체) 템플릿의 기본 보안 설정을 포함합니다. `smpolicy-secure` 파일은 보다 제한적인 보안 설정을 제공합니다. 자세한 내용은 [기본 정책 저장소 개체 고려 사항](#) (페이지 98)을 참조하십시오.

- 옵션 팩 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport ampolicy.xml -npass
```

- 페더레이션 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

정책 저장소 개체를 가져왔습니다.

참고: `smpolicy.xml` 을 가져오면 SiteMinder 에서 별도로 라이선스가 제공되는 레거시 페더레이션 및 웹 서비스 변수 기능을 사용할 수 있게 됩니다. 웹 서비스 변수 기능을 사용하려면 CA 고객 담당자에게 라이선스 정보에 대해 문의하십시오.

고급 인증 서버를 사용하도록 설정

정책 서버를 구성하는 과정에서 고급 인증 서버를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 구성 마법사를 시작합니다.
2. 마법사의 첫 번째 화면에서 모든 확인란을 **선택 취소**한 상태로 둡니다.
3. "다음"을 클릭합니다.
4. 고급 인증 서버에 대한 마스터 암호화 키를 생성합니다.

참고: 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

5. 정책 서버 구성 마법사의 나머지 과정을 완료합니다.
고급 인증 서버가 사용되도록 설정되었습니다.

관리 UI 등록 준비

기본 SiteMinder 슈퍼 사용자 계정(siteminder)을 사용하여 관리 UI 에 최초로 로그인합니다. 최초 로그인 시 관리 UI 를 정책 서버에 등록하여 두 구성 요소 간에 트러스트 관계를 생성해야 합니다.

등록을 준비하려면 XPSRegClient 유틸리티를 사용하여 슈퍼 사용자 계정 이름과 암호를 제공합니다. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 트러스트 관계를 설정할 수 있는지 확인합니다.

다음 사항을 고려하십시오.

- 자격 증명을 제공한 때부터 **24 시간** 이내에 최초 관리 UI 로그인 이루어져야 합니다. 관리 UI 설치를 하루 안에 수행할 계획이 아니면 관리 UI 를 설치하기 전에 다음 단계를 완료하십시오.
- (UNIX) XPSRegClient 를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c  
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

기본 SiteMinder 슈퍼 사용자 계정(siteminder)의 암호를 지정합니다.

참고: 암호를 지정하지 않으면 XPSRegClient 에서 암호를 입력하고
확인하라는 메시지가 표시됩니다.

-adminui-setup

관리 UI 가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 관리 UI 를 설치할 때부터 정책 서버에 로그인하고 정책
서버와의 트러스트 관계를 생성할 때까지 할당된 시간을
지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록
요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 15

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI 를 등록할 때 허용되는 시도 실패 횟수를
지정합니다. 관리 UI 에 최초로 로그인할 때 올바르게 않은
SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수
있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을
삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error_path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: `stderr`

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

XPSRegClient 가 정책 서버에 관리자 자격 증명을 제공합니다. 정책 서버에서는 관리 UI 에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

IBM Tivoli Directory Server 를 정책 저장소로 구성

IBM Tivoli Directory Server 는 정책 저장소로 작동할 수 있습니다. 단일 디렉터리 서버 인스턴스가 다음 기능을 수행할 수 있습니다.

- 정책 저장소
- 키 저장소

단일 디렉터리 서버를 사용하면 관리 태스크를 간소화할 수 있습니다. 다음 단원에서는 정책 데이터 및 암호화 키를 저장하도록 단일 디렉터리 서버 인스턴스를 구성하는 방법에 대한 지침을 제공합니다. 구현에 필요할 경우 별도의 키 저장소를 구성할 수 있습니다.

디렉터리 서버 정보 수집

LDAP 디렉터리 서버를 정책 저장소로 구성하거나 기존 정책 저장소를 업그레이드하려면 특정 디렉터리 서버 정보가 필요합니다. 시작하기 전에 다음 정보를 수집하십시오. 정책 저장소 워크시트를 사용하여 값을 기록할 수 있습니다.

호스트 정보

디렉터리 서버의 정규화된 호스트 이름 또는 IP 주소를 지정합니다.

포트 정보

(선택 사항) 비표준 포트를 지정합니다.

기본값: 636(SSL) 및 389(비 SSL)

관리 DN

LDAP 트리에서 정책 저장소 루트 개체 아래의 개체에 대한 생성, 읽기, 수정 및 삭제 권한이 있는 사용자의 LDAP 사용자 이름을 지정합니다.

관리 암호

관리 DN 의 암호를 지정합니다.

정책 저장소 루트 DN

LDAP 트리에서 정책 저장소 개체가 정의될 노드의 고유 이름을 지정합니다.

SSL 클라이언트 인증서

SSL 클라이언트 인증서 데이터베이스 파일이 있는 디렉터리의 경로 이름을 지정합니다.

제한: SSL에만 해당

정책 저장소를 구성하는 방법

IBM Directory Server 를 정책 저장소로 구성하려면 다음 단계를 완료하십시오.

1. 필수 정보를 수집했는지 확인합니다.
2. 디렉터리 항목과 루트 노드를 생성합니다.
3. 정책 서버를 정책 저장소에 연결합니다.
4. 정책 저장소 스키마를 생성합니다.
5. SiteMinder 슈퍼 사용자 암호를 설정합니다.
6. 정책 저장소 데이터 정의를 가져옵니다.
7. 기본 정책 저장소 개체를 가져옵니다.
8. 정책 서버를 다시 시작합니다.
9. 관리 UI 등록을 준비합니다.

디렉터리 항목 및 루트 노드 만들기

IBM Tivoli Directory Server Web Administration Tool 을 사용하여 디렉터리 항목 및 루트 노드를 생성할 수 있습니다.

참고: 해당하는 경우 IBM Tivoli Directory Server Configuration Tool 을 사용하여 서버 접미사를 생성하거나 로드하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 데이터의 루트 DN 에 대한 디렉터리 항목을 생성합니다.

예:

`ou=Nete`

2. 루트 DN 아래에 다음 루트 노드를 생성합니다.

예:

`ou=Netegrity,ou=SiteMinder,ou=PolicySvr4,ou=XPS`

정책 서버를 정책 저장소에 연결

정책 서버가 정책 저장소에 액세스할 수 있도록 정책 서버를 정책 저장소에 연결하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.

중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "데이터" 탭을 클릭합니다.
3. "데이터베이스" 목록에서 다음 값을 선택합니다.

정책 저장소

4. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

5. "LDAP 정책 저장소" 그룹 상자에서 다음 설정을 구성합니다.

- LDAP IP 주소
- 관리자 사용자 이름

- 암호
- 암호 확인
- 루트 DN

참고: "도움말"을 클릭하면 필드, 컨트롤 및 해당되는 요구 사항에 대한 설명을 볼 수 있습니다.

6. "적용"을 클릭합니다.
7. "LDAP 연결 테스트"를 클릭하여 정책 서버에서 정책 저장소에 액세스할 수 있는지 여부를 확인합니다.
8. "데이터베이스" 목록에서 다음 값을 선택합니다.
키 저장소
9. "저장소" 목록에서 다음 값을 선택합니다.
LDAP
10. 다음 옵션을 선택합니다.
정책 저장소 데이터베이스 사용
11. "확인"을 클릭합니다.

정책 저장소 스키마 만들기

디렉터리 서버가 정책 저장소로 작동하고 SiteMinder 개체를 저장할 수 있도록 정책 저장소 스키마를 생성하십시오.

다음 단계를 수행하십시오.

1. IBM 디렉터리 서버 구성 도구를 사용하여 디렉터리 서버에 액세스합니다.
2. `policy_server_home\IBMDirectoryServer` 로 이동합니다.
`policy_server_home`
정책 서버 설치 경로를 지정합니다.
3. IBM 디렉터리 서버 구성 도구를 사용하여 `V3.siteminderrelease` 스키마 파일을 스키마 구성의 "Manage Schema Files"(스키마 파일 관리) 섹션에 추가합니다.
`release`
SiteMinder 릴리스를 지정합니다.
4. `policy_server_home\xps\db` 로 이동합니다.

5. 다음 파일을 찾습니다.
`IBMDirectoryServer.ldif`
6. IBM 디렉터리 서버 구성 도구를 사용하여 이 파일을 스키마 구성의 "Manage Schema Files"(스키마 파일 관리) 섹션에 추가합니다.
7. 디렉터리 서버를 다시 시작합니다.
정책 저장소 스키마가 생성되었습니다.

SiteMinder 슈퍼 사용자 암호 설정

기본 SiteMinder 관리자 계정의 이름은 다음으로 지정됩니다.

`siteminder`

이 계정에는 최대 권한이 있습니다.

일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다.
다음과 같은 경우에 기본 슈퍼 사용자를 사용합니다.

- 관리 UI 에 처음 액세스할 경우
- SiteMinder 유틸리티를 처음 관리할 경우
- 슈퍼 사용자 권한이 있는 다른 관리자를 생성할 경우

다음 단계를 수행하십시오.

1. `smreg` 유틸리티를 `siteminder_home\bin` 에 복사합니다.

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

참고: 이 유틸리티는 정책 서버 설치 키트의 최상위 수준에 있습니다.

2. 다음 명령을 실행합니다.

`smreg -su password`

`password`

기본 SiteMinder 관리자의 암호를 지정합니다.

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: Oracle 정책 저장소를 구성하는 경우 암호의 대/소문자를 구분합니다. 다른 모든 정책 저장소에서는 암호의 대/소문자를 구분하지 않습니다.

3. *siteminder_home*\bin 에서 *smreg* 를 삭제합니다. *smreg* 를 삭제하면 이전 암호를 모르는 다른 사람은 암호를 변경할 수 없게 됩니다.

기본 SiteMinder 관리자 계정의 암호가 설정되었습니다.

정책 저장소 데이터 정의 가져오기

정책 저장소 데이터 정의 가져오기를 사용하여 정책 저장소에서 생성하고 저장할 수 있는 개체의 유형을 정의합니다.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home*\xps\dd 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

```
XPSDDInstall SmMaster.xdd
```

XPSDDInstall

필수 데이터 정의를 가져옵니다.

기본 정책 저장소 개체 가져오기

기본 정책 저장소 개체 가져오기를 사용하여 관리 UI 및 정책 서버에서 사용할 정책 저장소를 구성합니다.

다음 사항을 고려하십시오.

- *siteminder_home\bin* 에 대한 쓰기 액세스 권한이 있는지 확인하십시오. 가져오기 유틸리티에서 정책 저장소 개체를 가져오려면 이 권한이 필요합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

- Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 `siteminder_home\db` 로 이동합니다.

2. 다음 파일 중 하나를 가져옵니다.

- `smpolicy.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy.xml -npass
```

- `smpolicy-secure.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy-secure.xml -npass
```

npass

암호를 사용할 필요가 없음을 지정합니다. 기본 정책 저장소 개체에 암호화된 데이터가 포함되지 않습니다.

두 파일 모두 기본 정책 저장소 개체를 포함합니다. 이러한 개체는 기본 ACO(에이전트 구성 개체) 템플릿의 기본 보안 설정을 포함합니다. `smpolicy-secure` 파일은 보다 제한적인 보안 설정을 제공합니다. 자세한 내용은 [기본 정책 저장소 개체 고려 사항](#) (페이지 98)을 참조하십시오.

- 옵션 팩 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport ampolicy.xml -npass
```

- 페더레이션 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

정책 저장소 개체를 가져왔습니다.

참고: `smpolicy.xml` 을 가져오면 SiteMinder 에서 별도로 라이선스가 제공되는 레거시 페더레이션 및 웹 서비스 변수 기능을 사용할 수 있게 됩니다. 웹 서비스 변수 기능을 사용하려면 CA 고객 담당자에게 라이선스 정보에 대해 문의하십시오.

고급 인증 서버를 사용하도록 설정

정책 서버를 구성하는 과정에서 고급 인증 서버를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 구성 마법사를 시작합니다.
2. 마법사의 첫 번째 화면에서 모든 확인란을 **선택 취소**한 상태로 둡니다.
3. "다음"을 클릭합니다.
4. 고급 인증 서버에 대한 마스터 암호화 키를 생성합니다.

참고: 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

5. 정책 서버 구성 마법사의 나머지 과정을 완료합니다.
고급 인증 서버가 사용되도록 설정되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 **stop-all** 명령 다음에 **start-all** 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

관리 UI 등록 준비

기본 SiteMinder 슈퍼 사용자 계정(siteminder)을 사용하여 관리 UI 에 최초로 로그인합니다. 최초 로그인 시 관리 UI 를 정책 서버에 등록하여 두 구성 요소 간에 트러스트 관계를 생성해야 합니다.

등록을 준비하려면 XPSRegClient 유틸리티를 사용하여 슈퍼 사용자 계정 이름과 암호를 제공합니다. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 트러스트 관계를 설정할 수 있는지 확인합니다.

다음 사항을 고려하십시오.

- 자격 증명을 제공한 때부터 24 시간 이내에 최초 관리 UI 로그인이 이루어져야 합니다. 관리 UI 설치를 하루 안에 수행할 계획이 아니면 관리 UI 를 설치하기 전에 다음 단계를 완료하십시오.
- (UNIX) XPSRegClient 를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

기본 SiteMinder 슈퍼 사용자 계정(siteminder)의 암호를 지정합니다.

참고: 암호를 지정하지 않으면 XPSRegClient 에서 암호를 입력하고 확인하라는 메시지가 표시됩니다.

-adminui-setup

관리 UI 가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 관리 UI 를 설치할 때부터 정책 서버에 로그인하고 정책 서버와의 트러스트 관계를 생성할 때까지 할당된 시간을 지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록 요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 15

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI 를 등록할 때 허용되는 시도 실패 횟수를 지정합니다. 관리 UI 에 최초로 로그인할 때 올바르게 않은 SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수 있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을 삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error_path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: stderr

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

XPSRegClient 가 정책 서버에 관리자 자격 증명을 제공합니다. 정책 서버에서는 관리 UI에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

Microsoft Active Directory LDS 를 정책 저장소로 구성

Microsoft Active Directory LDS 는 정책 저장소로 작동할 수 있습니다. 단일 디렉터리 서버 인스턴스가 다음 기능을 수행할 수 있습니다.

- 정책 저장소
- 키 저장소

단일 디렉터리 서버를 사용하면 관리 태스크를 간소화할 수 있습니다. 다음 단원에서는 정책 데이터 및 암호화 키를 저장하도록 단일 디렉터리 서버 인스턴스를 구성하는 방법에 대한 지침을 제공합니다. 구현에 필요할 경우 별도의 키 저장소를 구성할 수 있습니다.

참고: 정책 서버 구성 마법사를 사용하여 이 유형의 LDAP 디렉터리를 정책 저장소로 자동 구성할 수 있습니다.

Active Directory LDS 사전 요구 사항

구성 파티션의 관리 사용자만 정책 저장소 스키마를 가져올 수 있습니다. 이 사용자는 구성 파티션은 물론 정책 저장소 파티션을 비롯한 모든 응용 프로그램 파티션에 대한 관리 권한을 가져야 합니다.

다음 단계를 수행하십시오.

1. ADSI Edit 콘솔을 엽니다.
2. 구성 파티션의 다음 항목으로 이동합니다.
`cn=directory service, cn=windows nt, cn=services, cn=configuration, cn={guid}`
3. msDS-Other-Settings 특성을 찾습니다.
4. 다음 새 값을 msDS-Other-Settings 특성에 추가합니다.
`ADAMAllowADAMSecurityPrincipalsInConfigPartition=1`
5. 구성 및 정책 저장소 응용 프로그램 파티션에서 다음을 수행합니다.
 - a. CN=Administrators, CN=Roles 로 이동합니다.
 - b. CN=Administrators 의 속성을 엽니다.
 - c. 구성원 특성을 편집합니다.
 - d. "DN 추가"를 클릭하고 구성 파티션에 생성한 사용자의 전체 DN 을 붙여 넣습니다.
 - e. 생성한 사용자의 속성으로 이동하고 다음 개체의 값을 확인합니다.
`msDS-UserAccountDisabled`
값이 false 로 설정되었는지 확인합니다.

이 관리 사용자는 구성 파티션은 물론 정책 저장소 파티션을 비롯한 모든 응용 프로그램 파티션에 대한 권한을 가집니다.

디렉터리 서버 정보 수집

Active Directory LDS 를 정책 저장소로 구성하려면 특정 디렉터리 서버 정보가 필요합니다. 정책 저장소를 구성하기 전에 다음 정보를 수집하십시오.

- **호스트 정보** - 디렉터리 서버 호스트 시스템의 정규화된 이름 또는 IP 주소를 확인합니다.
- **포트 정보** - 디렉터리 서버가 비표준 포트에서 수신 대기하는지 여부를 확인합니다. 포트 정보를 제공하지 않으면 정책 저장소를 구성하는 데 사용하는 SiteMinder 유틸리티에서 기본적으로 포트 389(비 SSL) 및 636(SSL)을 지정합니다.
- **관리 DN** - 디렉터리 서버 관리자의 guid 값을 포함한 전체 도메인 이름을 확인합니다.
예: CN=user1,CN=People,CN=Configuration,CN,{guid}
- **관리자 암호** - 디렉터리 서버 관리자의 암호를 확인합니다.
- **응용 프로그램 파티션의 루트 DN** - 디렉터리 서버에서 정책 저장소 스키마 데이터를 설치해야 하는 응용 프로그램 파티션의 루트 DN 위치를 식별합니다.
- (선택 사항) **SSL 클라이언트 인증서** - 디렉터리 연결이 SSL 을 통해 이루어지는 경우 SSL 클라이언트 인증서 데이터베이스가 있는 디렉터리의 경로를 확인합니다.

정책 저장소를 구성하는 방법

Active Directory LDS 를 정책 저장소로 구성하려면 다음 절차를 완료하십시오.

1. Active Directory LDS 사전 요구 사항이 충족되었는지 확인합니다.
2. 필수 정보를 수집했는지 확인합니다.
3. 정책 서버를 디렉터리 서버에 연결합니다.
4. 정책 저장소 스키마를 생성합니다.
5. SiteMinder 슈퍼 사용자 암호를 설정합니다.
6. 정책 저장소 데이터 정의를 가져옵니다.
7. 기본 SiteMinder 개체를 가져옵니다.
8. 정책 서버를 다시 시작합니다.
9. 관리 UI 등록을 준비합니다.

정책 서버를 정책 저장소에 연결

정책 서버가 정책 저장소에 액세스할 수 있도록 정책 서버를 정책 저장소에 연결하십시오.

참고: 정책 서버는 프록시 개체를 사용하여 AD LDS 정책 저장소에 바인딩할 수 있습니다. 프록시 개체는 AD LDS 에 생성되며 해당 계정의 보안 식별자를 통해 Active Directory 계정과 연결됩니다. 프록시 개체를 사용하여 AD LDS 인스턴스에 바인딩하는 방법에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오. 프록시 개체를 사용하여 정책 서버 연결을 구성하고 암호 정책을 사용할 계획이라면 SSL 에 대해 AD LDS 를 구성해야 합니다.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.

중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "데이터" 탭을 클릭합니다.
3. "데이터베이스" 목록에서 다음 값을 선택합니다.

정책 저장소

4. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

5. "LDAP 정책 저장소" 그룹 상자에서 다음 설정을 구성합니다.

- LDAP IP 주소
- 관리자 사용자 이름
디렉터리 서버 관리자의 guid 값을 포함한 전체 도메인 이름을 지정합니다.
- 암호

- 암호 확인
- 루트 DN

AD LDS 서버에서 응용 프로그램 파티션의 기존 루트 DN 위치를 지정합니다. 기존 루트 DN 위치는 정책 저장소 스키마를 가져오는 위치입니다.

참고: "도움말"을 클릭하면 필드, 컨트롤 및 해당되는 요구 사항에 대한 설명을 볼 수 있습니다.

6. "적용"을 클릭합니다.
7. "LDAP 연결 테스트"를 클릭하여 정책 서버에서 정책 저장소에 액세스할 수 있는지 여부를 확인합니다.
8. "데이터베이스" 목록에서 다음 값을 선택합니다.
키 저장소
9. 다음 옵션을 선택합니다.
정책 저장소 데이터베이스 사용
10. "확인"을 클릭합니다.

정책 저장소 스키마 만들기

디렉터리 서버가 정책 저장소로 작동하고 SiteMinder 개체를 저장할 수 있도록 정책 저장소 스키마를 생성하십시오.

다음 단계를 수행하십시오.

1. 다음 명령을 실행합니다.

```
smldapsetup ldgen -ffile_name  
file_name
```

생성하려는 LDIF 파일의 이름을 지정합니다.

SiteMinder 스키마를 사용하여 LDIF 파일이 생성됩니다.

2. 다음 명령을 실행합니다.

```
smldapsetup ldmod -ffile_name  
file_name
```

생성한 LDIF 의 이름을 지정합니다.

smldapsetup 에서 정책 저장소 스키마를 가져옵니다.

3. *siteminder_home\mps\db* 로 이동하고 다음 파일을 엽니다.

ADLDS.ldif

siteminder_home

정책 서버 설치 경로를 지정합니다.

4. {guid}의 각 인스턴스를 괄호에 포함된 guid 의 실제 값으로 바꾸고 파일을 저장합니다.

예: {CF151EA3-53A0-44A4-B4AC-DA0EBB1FF200}

5. 다음 명령을 실행합니다.

```
smldapsetup ldmod -fsiteminder_home\mps\db\ADLDS.ldif
```

정책 저장소 스키마가 확장됩니다. 정책 저장소 스키마를 생성했습니다.

SiteMinder 슈퍼 사용자 암호 설정

기본 SiteMinder 관리자 계정의 이름은 다음으로 지정됩니다.

siteminder

이 계정에는 최대 권한이 있습니다.

일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 다음과 같은 경우에 기본 슈퍼 사용자를 사용합니다.

- 관리 UI 에 처음 액세스할 경우
- SiteMinder 유틸리티를 처음 관리할 경우
- 슈퍼 사용자 권한이 있는 다른 관리자를 생성할 경우

다음 단계를 수행하십시오.

1. smreg 유틸리티를 *siteminder_home\bin* 에 복사합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

참고: 이 유틸리티는 정책 서버 설치 키트의 최상위 수준에 있습니다.

2. 다음 명령을 실행합니다.

```
smreg -su password
```

password

기본 SiteMinder 관리자의 암호를 지정합니다.

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: Oracle 정책 저장소를 구성하는 경우 암호의 대/소문자를 구분합니다. 다른 모든 정책 저장소에서는 암호의 대/소문자를 구분하지 않습니다.

3. *siteminder_home\bin* 에서 *smreg* 를 삭제합니다. *smreg* 를 삭제하면 이전 암호를 모르는 다른 사람은 암호를 변경할 수 없게 됩니다.

기본 SiteMinder 관리자 계정의 암호가 설정되었습니다.

정책 저장소 데이터 정의 가져오기

정책 저장소 데이터 정의 가져오기를 사용하여 정책 저장소에서 생성하고 저장할 수 있는 개체의 유형을 정의합니다.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home\bin* 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

```
XPSDDInstall SmMaster.xdd
```

XPSDDInstall

필수 데이터 정의를 가져옵니다.

기본 정책 저장소 개체 가져오기

기본 정책 저장소 개체 가져오기를 사용하여 관리 UI 및 정책 서버에서 사용할 정책 저장소를 구성합니다.

다음 사항을 고려하십시오.

- *siteminder_home\bin* 에 대한 쓰기 액세스 권한이 있는지 확인하십시오. 가져오기 유틸리티에서 정책 저장소 개체를 가져오려면 이 권한이 필요합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

- Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 `siteminder_home\db` 로 이동합니다.
2. 다음 파일 중 하나를 가져옵니다.
 - `smpolicy.xml` 을 가져오려면 다음 명령을 실행합니다.
`XPSImport smpolicy.xml -npass`
 - `smpolicy-secure.xml` 을 가져오려면 다음 명령을 실행합니다.
`XPSImport smpolicy-secure.xml -npass`

npass

암호를 사용할 필요가 없음을 지정합니다. 기본 정책 저장소 개체에 암호화된 데이터가 포함되지 않습니다.

두 파일 모두 기본 정책 저장소 개체를 포함합니다. 이러한 개체는 기본 ACO(에이전트 구성 개체) 템플릿의 기본 보안 설정을 포함합니다. `smpolicy-secure` 파일은 보다 제한적인 보안 설정을 제공합니다. 자세한 내용은 [기본 정책 저장소 개체 고려 사항](#) (페이지 98)을 참조하십시오.

- 옵션 팩 기능을 가져오려면 다음 명령을 실행합니다.
`XPSImport ampolicy.xml -npass`
 - 페더레이션 기능을 가져오려면 다음 명령을 실행합니다.
`XPSImport fedpolicy-12.52 SP1.xml -npass`
- 정책 저장소 개체를 가져왔습니다.

참고: `smpolicy.xml` 을 가져오면 SiteMinder 에서 별도로 라이선스가 제공되는 레거시 페더레이션 및 웹 서비스 변수 기능을 사용할 수 있게 됩니다. 웹 서비스 변수 기능을 사용하려면 CA 고객 담당자에게 라이선스 정보에 대해 문의하십시오.

고급 인증 서버를 사용하도록 설정

정책 서버를 구성하는 과정에서 고급 인증 서버를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 구성 마법사를 시작합니다.
2. 마법사의 첫 번째 화면에서 모든 확인란을 *선택 취소*한 상태로 둡니다.
3. "다음"을 클릭합니다.
4. 고급 인증 서버에 대한 마스터 암호화 키를 생성합니다.

참고: 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

5. 정책 서버 구성 마법사의 나머지 과정을 완료합니다.
고급 인증 서버가 사용되도록 설정되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 **stop-all** 명령 다음에 **start-all** 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

관리 UI 등록 준비

기본 SiteMinder 슈퍼 사용자 계정(siteminder)을 사용하여 관리 UI 에 최초로 로그인합니다. 최초 로그인 시 관리 UI 를 정책 서버에 등록하여 두 구성 요소 간에 트러스트 관계를 생성해야 합니다.

등록을 준비하려면 XPSRegClient 유틸리티를 사용하여 슈퍼 사용자 계정 이름과 암호를 제공합니다. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 트러스트 관계를 설정할 수 있는지 확인합니다.

다음 사항을 고려하십시오.

- 자격 증명을 제공한 때부터 24 시간 이내에 최초 관리 UI 로그인이 이루어져야 합니다. 관리 UI 설치를 하루 안에 수행할 계획이 아니면 관리 UI 를 설치하기 전에 다음 단계를 완료하십시오.
- (UNIX) XPSRegClient 를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

기본 SiteMinder 슈퍼 사용자 계정(siteminder)의 암호를 지정합니다.

참고: 암호를 지정하지 않으면 XPSRegClient 에서 암호를 입력하고 확인하라는 메시지가 표시됩니다.

-adminui-setup

관리 UI 가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 관리 UI 를 설치할 때부터 정책 서버에 로그인하고 정책 서버와의 트러스트 관계를 생성할 때까지 할당된 시간을 지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록 요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 15

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI 를 등록할 때 허용되는 시도 실패 횟수를 지정합니다. 관리 UI 에 최초로 로그인할 때 올바르게 않은 SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수 있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을 삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error_path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: stderr

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

XPSRegClient 가 정책 서버에 관리자 자격 증명을 제공합니다. 정책 서버에서는 관리 UI 에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

Novell eDirectory 를 정책 저장소로 구성

Novell eDirectory 는 정책 저장소로 작동할 수 있습니다. 단일 디렉터리 서버 인스턴스가 다음 기능을 수행할 수 있습니다.

- 정책 저장소
- 키 저장소

단일 디렉터리 서버를 사용하면 관리 태스크를 간소화할 수 있습니다. 다음 단원에서는 정책 데이터 및 암호화 키를 저장하도록 단일 디렉터리 서버 인스턴스를 구성하는 방법에 대한 지침을 제공합니다. 구현에 필요할 경우 별도의 키 저장소를 구성할 수 있습니다.

시작하기 전에 다음이 설치되었는지 확인합니다.

- Novell Windows Login Client
- Windows, UNIX 및 Netware 시스템용 Novell ConsoleOne

Novell eDirectory 에서 정책 저장소 개체의 제한 사항

Novell eDirectory 에서 정책 저장소 개체로 작업할 때 다음 사항을 고려하십시오.

- 15 자 이하의 정책 저장소 루트 DN 을 사용합니다.
Novell eDirectory DN 은 256 자를 초과할 수 없습니다. 일부 SiteMinder 개체는 최대 241 자가 될 수 있습니다. 루트 DN 이 15 자보다 긴 경우 일부 개체는 256 바이트 제한을 초과할 수 있습니다.
- 정책 저장소가 Novell eDirectory 에 있으면 정책 저장소 개체의 이름은 64 자를 초과할 수 없습니다. eDirectory 에서는 특성 값을 64 보다 길게 설정할 수 없습니다. 이러한 제한은 특히 인증서 맵에 영향을 주는데, 대개 인증서 맵은 설계상 이름이 길기 때문입니다.
- 정책 서버는 Novell eDirectory 에 있는 정책 저장소에 대한 LDAP 참조를 지원하지 않습니다.

디렉터리 서버 정보 수집

LDAP 디렉터리 서버를 정책 저장소로 구성하거나 기존 정책 저장소를 업그레이드하려면 특정 디렉터리 서버 정보가 필요합니다. 시작하기 전에 다음 정보를 수집하십시오. 정책 저장소 워크시트를 사용하여 값을 기록할 수 있습니다.

호스트 정보

디렉터리 서버의 정규화된 호스트 이름 또는 IP 주소를 지정합니다.

포트 정보

(선택 사항) 비표준 포트를 지정합니다.

기본값: 636(SSL) 및 389(비 SSL)

관리 DN

LDAP 트리에서 정책 저장소 루트 개체 아래의 개체에 대한 생성, 읽기, 수정 및 삭제 권한이 있는 사용자의 LDAP 사용자 이름을 지정합니다.

관리 암호

관리 DN 의 암호를 지정합니다.

정책 저장소 루트 DN

LDAP 트리에서 정책 저장소 개체가 정의될 노드의 고유 이름을 지정합니다.

SSL 클라이언트 인증서

SSL 클라이언트 인증서 데이터베이스 파일이 있는 디렉터리의 경로 이름을 지정합니다.

제한: SSL 에만 해당

정책 저장소를 구성하는 방법

Novell eDirectory 를 정책 저장소로 구성하려면 다음 절차를 완료하십시오.

1. 정책 저장소 스키마 파일을 편집합니다.
2. 정책 서버를 정책 저장소에 연결합니다.
3. SiteMinder 슈퍼 사용자 암호를 설정합니다.
참고: 이미 SiteMinder 슈퍼 사용자 암호를 설정한 경우에는 이 단계를 수행할 필요가 없습니다.
4. 정책 저장소 스키마를 생성합니다.
5. 정책 저장소 데이터 정의를 가져옵니다.
6. 기본 정책 저장소 개체를 가져옵니다.
7. LDAP 서버를 새로 고칩니다.
8. 정책 서버를 다시 시작합니다.
9. 관리 UI 등록을 준비합니다.

정책 저장소 스키마 파일 편집

Novell 서버 DN 정보를 포함하도록 Novell 정책 저장소 스키마 파일을 편집합니다. Novell Client 에서 Novell 정책 저장소 스키마 파일을 편집합니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에서 *policy_server_home\bin* 으로 이동합니다.

policy_server_home

정책 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

```
ldapsearch -hhost -pport -bbasedn -ssub -Dadmin_DN -wAdminPwd  
objectclass=ncpServer dn
```

-hhost

디렉터리 서버의 정규화된 호스트 이름 또는 IP 주소를 지정합니다.

-pport

LDAP 디렉터리 서버가 수신 대기하는 포트를 지정합니다.

-bbasedn

검색에 대한 기본 DN 을 지정합니다.

-Dadmin_dn

디렉터리 서버에 바인딩할 수 있는 관리자 계정의 DN 을 지정합니다.

-wadmin_pw

관리자 계정의 암호를 지정합니다.

예:

```
ldapsearch -h192.168.1.47 -p389 -bo=nwqa47container -ssub  
-dcn=admin,o=nwqa47container -wpassword objectclass=ncpServer dn
```

Novell 서버 DN 이 열립니다.

3. *policy_server_hoe\novell* 로 이동합니다.
4. Novell 정책 저장소 스키마 파일을 엽니다.

5. 모든 <ncpsrvr> 변수를 Novell 서버 DN 에 대해 2 단계에서 찾은 값으로 바꿔 정책 저장소 스키마 파일을 수동으로 편집합니다.

예: Novell 서버 DN 값이 cn=servername,o=servercontainer 이면
<ncpsrvr>의 모든 인스턴스를 cn=servername,o=servercontainer 로 바꿉니다.

6. 정책 저장소 스키마 파일을 저장하고 닫습니다.

7. `policy_server_home\mps\db` 로 이동합니다.

8. 다음 Novell 정책 저장소 스키마 파일을 엽니다.

Novell.ldif

9. 모든 <ncpsrvr> 변수를 Novell 서버 DN 에 대해 2 단계에서 찾은 값으로 바꿔 정책 저장소 스키마 파일을 수동으로 편집합니다.

예: Novell 서버 DN 값이 cn=servername,o=servercontainer 이면
<ncpsrvr>의 모든 인스턴스를 cn=servername,o=servercontainer 로 바꿉니다.

Novell 정책 저장소 스키마 파일에 Novell 서버 DN 정보가 포함됩니다.

정책 서버를 정책 저장소에 연결

정책 서버가 정책 저장소에 액세스할 수 있도록 정책 서버를 정책 저장소에 연결하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.

중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자 권한으로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "데이터" 탭을 클릭합니다.
3. "데이터베이스" 목록에서 다음 값을 선택합니다.

정책 저장소

4. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

5. "LDAP 정책 저장소" 그룹 상자에서 다음 설정을 구성합니다.

- LDAP IP 주소
- 관리자 사용자 이름
- 암호
- 암호 확인
- 루트 DN

참고: "도움말"을 클릭하면 필드, 컨트롤 및 해당되는 요구 사항에 대한 설명을 볼 수 있습니다.

6. "적용"을 클릭합니다.

7. "LDAP 연결 테스트"를 클릭하여 정책 서버에서 정책 저장소에 액세스할 수 있는지 여부를 확인합니다.

8. "데이터베이스" 목록에서 다음 값을 선택합니다.

키 저장소

9. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

10. 다음 옵션을 선택합니다.

정책 저장소 데이터베이스 사용

11. "확인"을 클릭합니다.

정책 저장소 스키마 만들기

디렉터리 서버가 정책 저장소로 작동하고 SiteMinder 개체를 저장할 수 있도록 정책 저장소 스키마를 생성하십시오. `smldapsetup` 도구를 사용하여 정책 저장소 스키마를 추가할 수 있습니다.

다음 단계를 수행하십시오.

1. 다음 명령을 실행합니다.

```
smldapsetup ldmod -v  
-fpolicy_server_home\novell\Novell_Add_release.ldif  
-fpolicy_server_home
```

정책 서버 설치 경로를 지정합니다.

-v

추적을 설정하고 오류, 경고 및 설명 메시지를 출력합니다.

release

SiteMinder 릴리스를 지정합니다.

2. 다음 명령을 실행합니다.

```
smldapsetup ldmod -v -fpolicy_server_home\xps\db\Novell.ldif
```

정책 저장소 스키마가 생성되었습니다.

SiteMinder 슈퍼 사용자 암호 설정

기본 SiteMinder 관리자 계정의 이름은 다음으로 지정됩니다.

siteminder

이 계정에는 최대 권한이 있습니다.

일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 다음과 같은 경우에 기본 슈퍼 사용자를 사용합니다.

- 관리 UI 에 처음 액세스할 경우
- SiteMinder 유틸리티를 처음 관리할 경우
- 슈퍼 사용자 권한이 있는 다른 관리자를 생성할 경우

다음 단계를 수행하십시오.

1. smreg 유틸리티를 *siteminder_home\bin* 에 복사합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

참고: 이 유틸리티는 정책 서버 설치 키트의 최상위 수준에 있습니다.

2. 다음 명령을 실행합니다.

```
smreg -su password
```

password

기본 SiteMinder 관리자의 암호를 지정합니다.

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: Oracle 정책 저장소를 구성하는 경우 암호의 대/소문자를 구분합니다. 다른 모든 정책 저장소에서는 암호의 대/소문자를 구분하지 않습니다.

3. *siteminder_home*\bin 에서 *smreg* 를 삭제합니다. *smreg* 를 삭제하면 이전 암호를 모르는 다른 사람은 암호를 변경할 수 없게 됩니다.

기본 SiteMinder 관리자 계정의 암호가 설정되었습니다.

정책 저장소 데이터 정의 가져오기

정책 저장소 데이터 정의 가져오기를 사용하여 정책 저장소에서 생성하고 저장할 수 있는 개체의 유형을 정의합니다.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home*\xps\dd 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

```
XPSDDInstall SmMaster.xdd
```

XPSDDInstall

필수 데이터 정의를 가져옵니다.

기본 정책 저장소 개체 가져오기

기본 정책 저장소 개체 가져오기를 사용하여 관리 UI 및 정책 서버에서 사용할 정책 저장소를 구성합니다.

다음 사항을 고려하십시오.

- *siteminder_home\bin* 에 대한 쓰기 액세스 권한이 있는지 확인하십시오. 가져오기 유틸리티에서 정책 저장소 개체를 가져오려면 이 권한이 필요합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

- Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 `siteminder_home\db` 로 이동합니다.
2. 다음 파일 중 하나를 가져옵니다.
 - `smpolicy.xml` 을 가져오려면 다음 명령을 실행합니다.
`XPSImport smpolicy.xml -npass`
 - `smpolicy-secure.xml` 을 가져오려면 다음 명령을 실행합니다.
`XPSImport smpolicy-secure.xml -npass`

npass

암호를 사용할 필요가 없음을 지정합니다. 기본 정책 저장소 개체에 암호화된 데이터가 포함되지 않습니다.

두 파일 모두 기본 정책 저장소 개체를 포함합니다. 이러한 개체는 기본 ACO(에이전트 구성 개체) 템플릿의 기본 보안 설정을 포함합니다. `smpolicy-secure` 파일은 보다 제한적인 보안 설정을 제공합니다. 자세한 내용은 [기본 정책 저장소 개체 고려 사항](#) (페이지 98)을 참조하십시오.

- 옵션 팩 기능을 가져오려면 다음 명령을 실행합니다.
`XPSImport ampolicy.xml -npass`
- 페더레이션 기능을 가져오려면 다음 명령을 실행합니다.
`XPSImport fedpolicy-12.52 SP1.xml -npass`

정책 저장소 개체를 가져왔습니다.

참고: `smpolicy.xml` 을 가져오면 SiteMinder 에서 별도로 라이선스가 제공되는 레거시 페더레이션 및 웹 서비스 변수 기능을 사용할 수 있게 됩니다. 웹 서비스 변수 기능을 사용하려면 CA 고객 담당자에게 라이선스 정보에 대해 문의하십시오.

LDAP 서버 새로 고침

Novell eDirectory 에 변경 내용을 적용하려면 LDAP 서버를 새로 고치십시오. Novell Client 를 사용하여 LDAP 서버를 새로 고칠 수 있습니다.

다음 단계를 수행하십시오.

1. ConsoleOne 을 엽니다.

2. 디렉터리 트리에서 LDAP 서버를 두 번 클릭합니다.
3. "Refresh LDAP Server Now"(지금 LDAP 서버 새로 고침)를 클릭합니다.
LDAP 서버가 새로 고쳐집니다.

고급 인증 서버를 사용하도록 설정

정책 서버를 구성하는 과정에서 고급 인증 서버를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 구성 마법사를 시작합니다.
2. 마법사의 첫 번째 화면에서 모든 확인란을 *선택 취소한* 상태로 둡니다.
3. "다음"을 클릭합니다.
4. 고급 인증 서버에 대한 마스터 암호화 키를 생성합니다.

참고: 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

5. 정책 서버 구성 마법사의 나머지 과정을 완료합니다.
고급 인증 서버가 사용되도록 설정되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 `stop-all` 명령 다음에 `start-all` 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

관리 UI 등록 준비

기본 SiteMinder 슈퍼 사용자 계정(siteminder)을 사용하여 관리 UI 에 최초로 로그인합니다. 최초 로그인 시 관리 UI 를 정책 서버에 등록하여 두 구성 요소 간에 트러스트 관계를 생성해야 합니다.

등록을 준비하려면 XPSRegClient 유틸리티를 사용하여 슈퍼 사용자 계정 이름과 암호를 제공합니다. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 트러스트 관계를 설정할 수 있는지 확인합니다.

다음 사항을 고려하십시오.

- 자격 증명을 제공한 때부터 24 시간 이내에 최초 관리 UI 로그인이 이루어져야 합니다. 관리 UI 설치를 하루 안에 수행할 계획이 아니면 관리 UI 를 설치하기 전에 다음 단계를 완료하십시오.
- (UNIX) XPSRegClient 를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c  
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

기본 SiteMinder 슈퍼 사용자 계정(siteminder)의 암호를 지정합니다.

참고: 암호를 지정하지 않으면 XPSRegClient 에서 암호를 입력하고 확인하라는 메시지가 표시됩니다.

-adminui-setup

관리 UI 가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 관리 UI 를 설치할 때부터 정책 서버에 로그인하고 정책 서버와의 트러스트 관계를 생성할 때까지 할당된 시간을 지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록 요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 15

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI 를 등록할 때 허용되는 시도 실패 횟수를 지정합니다. 관리 UI 에 최초로 로그인할 때 올바르게 않은 SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수 있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을 삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error_path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: stderr

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

XPSRegClient 가 정책 서버에 관리자 자격 증명을 제공합니다. 정책 서버에서는 관리 UI 에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

OpenLDAP 을 정책 저장소로 구성

OpenLDAP 은 정책 저장소로 작동할 수 있습니다. 단일 디렉터리 서버 인스턴스가 다음 기능을 수행할 수 있습니다.

- 정책 저장소
- 키 저장소

단일 디렉터리 서버를 사용하면 관리 태스크를 간소화할 수 있습니다. 다음 단원에서는 정책 데이터 및 암호화 키를 저장하도록 단일 디렉터리 서버 인스턴스를 구성하는 방법에 대한 지침을 제공합니다. 구현에 필요할 경우 별도의 키 저장소를 구성할 수 있습니다.

디렉터리 서버 정보 수집

LDAP 디렉터리 서버를 정책 저장소로 구성하거나 기존 정책 저장소를 업그레이드하려면 특정 디렉터리 서버 정보가 필요합니다. 시작하기 전에 다음 정보를 수집하십시오. 정책 저장소 워크시트를 사용하여 값을 기록할 수 있습니다.

호스트 정보

디렉터리 서버의 정규화된 호스트 이름 또는 IP 주소를 지정합니다.

포트 정보

(선택 사항) 비표준 포트를 지정합니다.

기본값: 636(SSL) 및 389(비 SSL)

관리 DN

LDAP 트리에서 정책 저장소 루트 개체 아래의 개체에 대한 생성, 읽기, 수정 및 삭제 권한이 있는 사용자의 LDAP 사용자 이름을 지정합니다.

관리 암호

관리 DN 의 암호를 지정합니다.

정책 저장소 루트 DN

LDAP 트리에서 정책 저장소 개체가 정의될 노드의 고유 이름을 지정합니다.

SSL 클라이언트 인증서

SSL 클라이언트 인증서 데이터베이스 파일이 있는 디렉터리의 경로 이름을 지정합니다.

제한: SSL 에만 해당

정책 저장소를 구성하는 방법

OpenLDAP Directory Server 를 정책 저장소로 구성하려면 다음 절차를 완료하십시오.

1. sldap 구성 파일을 구성합니다.
2. 데이터베이스를 생성합니다.
3. 정책 서버를 디렉터리 서버에 연결합니다.
4. SiteMinder 슈퍼 사용자 암호를 설정합니다.

5. 정책 저장소 데이터 정의를 가져옵니다.
6. 기본 정책 저장소 개체를 가져옵니다.
7. 관리 UI 등록을 준비합니다.

Slapd 구성 파일 구성 방법

OpenLDAP Directory Server 를 정책 저장소로 사용하려면 먼저 추가 구성을 수행해야 합니다. 구성 단계는 다음과 같습니다.

1. SiteMinder 스키마 파일을 지정합니다.
2. 정책 저장소 인덱싱을 지정합니다.
3. 사용자 인증이 사용되도록 설정합니다.
4. 데이터베이스 지시문을 지정합니다.
5. 클라이언트 측 정렬 지원
6. 구성 파일을 테스트합니다.
7. OpenLDAP 서버를 다시 시작합니다.

SiteMinder 스키마 파일 지정

slapd 구성 파일(slapd.conf)의 include 섹션에 스키마 파일을 지정하여 추가 구성 정보를 읽는 slapd 프로세스(LDAP Directory Server 데몬)를 구성합니다. 포함되는 파일은 올바른 slapd 구성 파일 형식을 따라야 합니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. *siteminder_home/db/tier2/OpenLDAP* 로 이동하고 다음 파일을 OpenLDAP 설치 디렉터리의 schema 폴더에 복사합니다.
 - *openldap_attribute.schema*
 - *openldap_object.schema*

siteminder_home

정책 서버 설치 경로를 지정합니다.
3. *siteminder_home/xps/db* 로 이동하고 다음 파일을 OpenLDAP 설치 디렉터리의 schema 폴더에 복사합니다.
 - *openldap_attribute_XPS.schema*
 - *openldap_object_XPS.schema*

4. 다음 항목을 `slapd` 구성 파일의 `include` 섹션에 입력합니다.

```
....  
.....  
include /usr/local/etc/openldap/schema/openldap_attribute.schema  
include /usr/local/etc/openldap/schema/openldap_object.schema  
include /usr/local/etc/openldap/schema/openldap_attribute_XPS.schema  
include /usr/local/etc/openldap/schema/openldap_object_XPS.schema
```

참고: 이 절차에서는 OpenLDAP 서버가 `/usr/local/etc/openldap`에 있고 스키마 파일이 `schema` 하위 디렉터리에 있다고 가정합니다.

SiteMinder 스키마 파일이 지정되었습니다.

정책 저장소 인덱싱 지정

OpenLDAP 을 정책 저장소로 사용하려면 `slapd.conf` 파일에서 인덱싱을 지정하십시오.

다음 단계를 수행하십시오.

1. `slapd` 인스턴스를 중지합니다.
2. 텍스트 편집기에서 `slapd.conf` 파일을 엽니다.
3. 다음 행을 찾습니다.

```
# Indices to maintain
index objectClass eq
```

4. 파일에 새 행을 삽입하고 다음 행을 추가합니다.

```
index smAdminOID4 pres,eq
index smAuthDirOID4 pres,eq
index smAzDirOID4 pres,eq
index smcertmapOID4 pres,eq
index smIsRadius4 pres,eq
index smIsAffiliate4 pres,eq
index smParentRealmOID4 pres,eq
index smPasswordPolicyOID4 pres,eq
index smAgentGroupOID4 pres,eq
index smKeyManagementOID4 pres,eq
index smAgentOID4 pres,eq
index smAgentKeyOID4 pres,eq
index smRootConfigOID4 pres,eq
index smAGAgents4 pres,eq
index smDomainAdminOIDs4 pres,eq
index smDomainOID4 pres,eq
index smvariableoid5 pres,eq
index smNestedVariableOIDs5 pres,eq
index smvariabletypeoid5 pres,eq
index smActiveExprOID5 pres,eq
index smDomainUDs4 pres,eq
index smVariableOIDs5 pres,eq
index smusractiveexpoid5 pres,eq
index smPropertyOID5 pres,eq
index smPropertySectionOID5 pres,eq
index smPropertyCollectionOID5 pres,eq
index smFilterClass4 pres,eq
index smTaggedStringOID5 pres,eq
index smNoMatch5 pres,eq
index smTrustedHostOID5 pres,eq
index smIs4xTrustedHost5 pres,eq
index smDomainMode5 pres,eq
# index smImsEnvironmentOIDs5 pres,eq
```

```

index smSecretRolloverEnabled6 pres,eq
index smSecretGenTime6 pres,eq
index smSecretUsedTime6 pres,eq
index smSharedSecretPolicyOID6 pres,eq
index smFilterPath4 pres,eq
index smPolicyLinkOID4 pres,eq
index smIPAddress4 pres,eq
index smRealmOID4 pres,eq
index smSelfRegOID4 pres,eq
index smAzUserDirOID4 pres,eq
index smResourceType4 pres,eq
index smResponseAttrOID4 pres,eq
index smResponseGroupOID4 pres,eq
index smResponseOID4 pres,eq
index smRGResponses4 pres,eq
index smRGRules4 pres,eq
index smRuleGroupOID4 pres,eq
index smRuleOID4 pres,eq
index smSchemeOID4 pres,eq
index smisTemplate4 pres,eq
index smisUsedbyAdmin4 pres,eq
index smSchemeType4 pres,eq
index smUserDirectoryOID4 pres,eq
index smODBCQueryOID4 pres,eq
index smUserPolicyOID4 pres,eq
index smAgentTypeAttrOID4 pres,eq
index smAgentTypeOID4 pres,eq
index smAgentTypeperfcid4 pres,eq
index smAgentTypeType4 pres,eq
index smAgentCommandOID4 pres,eq
index smTimeStamp4 pres,eq
index smServerCommandOID4 pres,eq
index smAuthAzMapOID4 pres,eq
index xpsParameter pres,eq
index xpsValue pres,eq
index xpsNumber pres,eq
index xpsCategory pres,eq
index xpsGUID pres,eq
index xpsSortKey pres,eq
index xpsIndexedObject pres,eq

```

5. 파일을 저장하고 텍스트 편집기를 닫습니다.
6. 다음 명령을 실행합니다.

```
slapindex -f slapd.conf
```

7. slapd 인스턴스를 다시 시작합니다.

OpenLDAP 에 대한 정책 저장소 인덱싱이 지정되었습니다.

사용자 인증 활성화

사용자 인증을 활성화하면 지원되는 인증 체계로 리소스를 보호할 수 있습니다.

사용자 인증을 활성화하려면 다음을 **slapd** 구성 파일에 추가하십시오.

```
access to attrs=userpassword
by self write
by anonymous auth
by * none
```

데이터베이스 지시문 지정

slapd 구성 파일에서 추가 데이터베이스 지시문의 값을 지정해야 합니다.

지시문을 지정하려면 다음 항목을 편집하십시오.

database

지원되는 백엔드 유형을 지정합니다.

예: **bdb**

suffix

데이터베이스 접미사를 지정합니다.

예: **dc=example,dc=com**

rootdn

루트의 DN 을 지정합니다.

예: **cn=Manager,dc=example,dc=com**

rootpw

루트의 암호를 지정합니다.

directory

데이터베이스 디렉터리의 경로를 지정합니다.

예: **/usr/local/var/openldap-data**

참고: **slapd** 를 실행하려면 데이터베이스 디렉터리가 있어야 하고 **slapd** 프로세스에서만 이 디렉터리에 액세스할 수 있어야 합니다.

클라이언트 측 정렬 지원

지원되는 LDAP 디렉터리 중 OpenLDAP 만 서버 측 정렬을 지원하지 않습니다. OpenLDAP 을 사용할 때는 모든 정렬이 클라이언트 측에서 수행되어야 합니다. 이를 위해 시작 시 서버 측 페이지징을 사용하여 모든 XPS 개체를 가져와야 합니다.

클라이언트 측 정렬을 지원하려면 OpenLDAP 디렉터리 관리자가 slapd.conf 파일에서 다음 설정을 구성해야 합니다.

- 루트 DSE 를 읽을 수 있도록 설정합니다.

이렇게 하면 XPS 클라이언트가 OpenLDAP 디렉터리의 유형과 기능을 읽을 수 있습니다.

- 검색 작업에서 반환될 수 있는 최대 항목 수를 500 개 이상으로 설정합니다.

이렇게 하면 서버 측 페이지징으로 가져오는 XPS 개체를 500 개씩 나누어 가져올 수 있습니다.

- 단순 V2 바인딩을 허용합니다.

이렇게 하면 smconsole 이 단순 V2 바인딩을 사용하여 LDAP 연결을 테스트할 수 있습니다.

다음 단계를 수행하십시오.

1. slapd.conf 파일에 다음 행을 추가합니다.

```
access to *
by users read
by anonymous read
access to dn.base=ACL by users read
```

ACL

액세스 제어 목록이나 권한 목록을 지정합니다.

참고: ACL 을 지정하는 방법에 대한 자세한 내용은

<http://www.openldap.org/doc/admin24/access-control.html>(영문)을 참조하십시오.

2. slapd.conf 파일에서 sizelimit 지시문에 지정된 값이 500 이상인지 확인합니다.

```
sizelimit 500
```

참고: sizelimit 의 기본값은 500 입니다. 자세한 내용은 <http://www.openldap.org/doc/admin24/slapdconfig.html>(영문)을 참조하십시오.

3. slapd.conf 파일에 다음 행을 추가합니다.

```
allow bind_v2
```

클라이언트 측 정렬을 지원하도록 slapd.conf 파일이 구성되었습니다.

구성 파일 테스트

구성 파일을 테스트하면 형식이 올바른지 확인할 수 있습니다.

다음 단계를 수행하십시오.

1. 디렉토리를 OpenLDAP 서버 디렉토리로 변경합니다.
2. 다음 명령을 실행합니다.

```
./slapd
```

참고: 디버깅 수준(수준 0 포함)을 지정하지 않은 경우 slapd 는 자동으로 분기되어 제어 터미널에서 분리되고 백그라운드에서 실행됩니다.

3. 다음 명령을 실행합니다.

```
./slapd -Tt
```

slapd 구성 파일이 테스트됩니다.

OpenLDAP 서버를 다시 시작합니다.

OpenLDAP Directory Server 를 다시 시작하면 SiteMinder 스키마가 로드됩니다. 디렉터리 서버를 정책 저장소로 사용하려면 먼저 정책 서버에서 SiteMinder 스키마가 로드되어야 합니다.

다음 단계를 수행하십시오.

1. 다음 명령을 사용하여 디렉터리 서버를 중지합니다.

```
kill -INT 'cat path_of_var/run_directory/slapd.pid'
```

path_of_var/run_directory

데이터베이스 디렉터리의 경로를 지정합니다.

예: kill -INT 'cat /usr/local/var/run/slapd.pid'

2. 다음 명령을 사용하여 디렉터리 서버를 시작합니다.

```
./slapd
```

데이터베이스 생성 방법

다음 프로세스에서는 정책 저장소의 디렉터리 서버 데이터베이스를 생성하는 단계를 보여 줍니다.

1. 기본 트리 구조를 생성합니다.
2. 항목을 추가합니다.

기본 트리 구조 만들기

정책 저장소 개체를 저장할 기본 트리 구조를 생성할 수 있습니다.

루트 DN 아래에 다음 항목을 지정하십시오.

```
ou=Netegrity,ou=SiteMinder,ou=PolicySvr4,ou=XPS
```

기본 트리 구조가 생성되었습니다.

항목 추가

SiteMinder 에서 필요한 조직 및 조직 역할 정보를 갖도록 디렉터리 서버에 항목을 추가하십시오.

다음 단계를 수행하십시오.

1. LDIF 파일을 생성합니다.

예: 다음 예에는 `entries.ldif` 에 대한 조직 역할 항목과 조직 항목이 포함되어 있습니다.

```
# CA, example.com
dn: ou=Netegrity,dc= example,dc=com
ou: CA
objectClass: organizationalUnit
objectClass: top

# SiteMinder, CA, example.com
dn: ou=SiteMinder,ou=CA,dc= example,dc=com
ou: SiteMinder
objectClass: organizationalUnit
objectClass: top

# PolicySvr4, SiteMinder, CA, example.com
dn: ou=PolicySvr4,ou=SiteMinder,ou=CA,dc= example,dc=com
ou: PolicySvr4
objectClass: organizationalUnit
objectClass: top

# XPS, policysvr4, siteminder, ca, example.com
dn: ou=XPS,ou=policysvr4,ou=siteminder,ou=ca,dc= example,dc=com
ou: XPS
objectClass: organizationalUnit
objectClass: top
```

2. 다음 명령을 사용하여 항목을 추가합니다.

```
ldapadd -f <file_name.ldif> -D "cn=Manager,dc=example,dc=com"
-w<password>
```

정책 서버를 정책 저장소에 연결

정책 서버가 정책 저장소에 액세스할 수 있도록 정책 서버를 정책 저장소에 연결하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.

중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "데이터" 탭을 클릭합니다.
3. "데이터베이스" 목록에서 다음 값을 선택합니다.

정책 저장소

4. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

5. "LDAP 정책 저장소" 그룹 상자에서 다음 설정을 구성합니다.

- LDAP IP 주소
- 관리자 사용자 이름
- 암호
- 암호 확인
- 루트 DN

참고: "도움말"을 클릭하면 필드, 컨트롤 및 해당되는 요구 사항에 대한 설명을 볼 수 있습니다.

6. "적용"을 클릭합니다.
7. "LDAP 연결 테스트"를 클릭하여 정책 서버에서 정책 저장소에 액세스할 수 있는지 여부를 확인합니다.
8. "데이터베이스" 목록에서 다음 값을 선택합니다.

키 저장소

9. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

10. 다음 옵션을 선택합니다.

정책 저장소 데이터베이스 사용

11. "확인"을 클릭합니다.

SiteMinder 슈퍼 사용자 암호 설정

기본 SiteMinder 관리자 계정의 이름은 다음으로 지정됩니다.

siteminder

이 계정에는 최대 권한이 있습니다.

일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다.
다음과 같은 경우에 기본 슈퍼 사용자를 사용합니다.

- 관리 UI 에 처음 액세스할 경우
- SiteMinder 유틸리티를 처음 관리할 경우
- 슈퍼 사용자 권한이 있는 다른 관리자를 생성할 경우

다음 단계를 수행하십시오.

1. smreg 유틸리티를 *siteminder_home*\bin 에 복사합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

참고: 이 유틸리티는 정책 서버 설치 키트의 최상위 수준에 있습니다.

2. 다음 명령을 실행합니다.

smreg -su *password*

password

기본 SiteMinder 관리자의 암호를 지정합니다.

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: Oracle 정책 저장소를 구성하는 경우 암호의 대/소문자를 구분합니다. 다른 모든 정책 저장소에서는 암호의 대/소문자를 구분하지 않습니다.

3. *siteminder_home\bin* 에서 **smreg** 를 삭제합니다. **smreg** 를 삭제하면 이전 암호를 모르는 다른 사람은 암호를 변경할 수 없게 됩니다.
기본 SiteMinder 관리자 계정의 암호가 설정되었습니다.

정책 저장소 데이터 정의 가져오기

정책 저장소 데이터 정의 가져오기를 사용하여 정책 저장소에서 생성하고 저장할 수 있는 개체의 유형을 정의합니다.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home\xps\dd* 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

```
XPSDDInstall SmMaster.xdd
```

XPSDDInstall

필수 데이터 정의를 가져옵니다.

기본 정책 저장소 개체 가져오기

기본 정책 저장소 개체 가져오기를 사용하여 관리 UI 및 정책 서버에서 사용할 정책 저장소를 구성합니다.

다음 사항을 고려하십시오.

- *siteminder_home\bin* 에 대한 쓰기 액세스 권한이 있는지 확인하십시오. 가져오기 유틸리티에서 정책 저장소 개체를 가져오려면 이 권한이 필요합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

- Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 `siteminder_home\db` 로 이동합니다.

2. 다음 파일 중 하나를 가져옵니다.

- `smpolicy.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy.xml -npass
```

- `smpolicy-secure.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy-secure.xml -npass
```

npass

암호를 사용할 필요가 없음을 지정합니다. 기본 정책 저장소 개체에 암호화된 데이터가 포함되지 않습니다.

두 파일 모두 기본 정책 저장소 개체를 포함합니다. 이러한 개체는 기본 ACO(에이전트 구성 개체) 템플릿의 기본 보안 설정을 포함합니다. `smpolicy-secure` 파일은 보다 제한적인 보안 설정을 제공합니다. 자세한 내용은 [기본 정책 저장소 개체 고려 사항](#) (페이지 98)을 참조하십시오.

- 옵션 팩 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport ampolicy.xml -npass
```

- 페더레이션 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

정책 저장소 개체를 가져왔습니다.

참고: `smpolicy.xml` 을 가져오면 SiteMinder 에서 별도로 라이선스가 제공되는 레거시 페더레이션 및 웹 서비스 변수 기능을 사용할 수 있게 됩니다. 웹 서비스 변수 기능을 사용하려면 CA 고객 담당자에게 라이선스 정보에 대해 문의하십시오.

고급 인증 서버를 사용하도록 설정

정책 서버를 구성하는 과정에서 고급 인증 서버를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 구성 마법사를 시작합니다.
2. 마법사의 첫 번째 화면에서 모든 확인란을 **선택 취소**한 상태로 둡니다.
3. "다음"을 클릭합니다.
4. 고급 인증 서버에 대한 마스터 암호화 키를 생성합니다.

참고: 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

5. 정책 서버 구성 마법사의 나머지 과정을 완료합니다.
고급 인증 서버가 사용되도록 설정되었습니다.

관리 UI 등록 준비

기본 SiteMinder 슈퍼 사용자 계정(siteminder)을 사용하여 관리 UI 에 최초로 로그인합니다. 최초 로그인 시 관리 UI 를 정책 서버에 등록하여 두 구성 요소 간에 트러스트 관계를 생성해야 합니다.

등록을 준비하려면 XPSRegClient 유틸리티를 사용하여 슈퍼 사용자 계정 이름과 암호를 제공합니다. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 트러스트 관계를 설정할 수 있는지 확인합니다.

다음 사항을 고려하십시오.

- 자격 증명을 제공한 때부터 **24 시간** 이내에 최초 관리 UI 로그인 이루어져야 합니다. 관리 UI 설치를 하루 안에 수행할 계획이 아니면 관리 UI 를 설치하기 전에 다음 단계를 완료하십시오.
- (UNIX) XPSRegClient 를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c  
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

기본 SiteMinder 슈퍼 사용자 계정(siteminder)의 암호를 지정합니다.

참고: 암호를 지정하지 않으면 XPSRegClient 에서 암호를 입력하고
확인하라는 메시지가 표시됩니다.

-adminui-setup

관리 UI 가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 관리 UI 를 설치할 때부터 정책 서버에 로그인하고 정책
서버와의 트러스트 관계를 생성할 때까지 할당된 시간을
지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록
요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 15

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI 를 등록할 때 허용되는 시도 실패 횟수를
지정합니다. 관리 UI 에 최초로 로그인할 때 올바르게 않은
SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수
있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을
삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error_path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: `stderr`

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

XPSRegClient 가 정책 서버에 관리자 자격 증명을 제공합니다. 정책 서버에서는 관리 UI 에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

Oracle Directory Server 를 정책 저장소로 구성

Oracle Directory Server(이전의 Sun Java System Directory Server)는 정책 저장소로 작동할 수 있습니다. 단일 디렉터리 서버 인스턴스가 다음 기능을 수행할 수 있습니다.

- 정책 저장소
- 키 저장소

단일 디렉터리 서버를 사용하면 관리 태스크를 간소화할 수 있습니다. 다음 단원에서는 정책 데이터 및 암호화 키를 저장하도록 단일 디렉터리 서버 인스턴스를 구성하는 방법에 대한 지침을 제공합니다. 구현에 필요할 경우 별도의 키 저장소를 구성할 수 있습니다.

참고: 정책 서버 구성 마법사를 사용하여 이 유형의 LDAP 디렉터리를 정책 저장소로 자동 구성할 수 있습니다.

디렉터리 서버 정보 수집

LDAP 디렉터리 서버를 정책 저장소로 구성하거나 기존 정책 저장소를 업그레이드하려면 특정 디렉터리 서버 정보가 필요합니다. 시작하기 전에 다음 정보를 수집하십시오. 정책 저장소 워크시트를 사용하여 값을 기록할 수 있습니다.

호스트 정보

디렉터리 서버의 정규화된 호스트 이름 또는 IP 주소를 지정합니다.

포트 정보

(선택 사항) 비표준 포트를 지정합니다.

기본값: 636(SSL) 및 389(비 SSL)

관리 DN

LDAP 트리에서 정책 저장소 루트 개체 아래의 개체에 대한 생성, 읽기, 수정 및 삭제 권한이 있는 사용자의 LDAP 사용자 이름을 지정합니다.

관리 암호

관리 DN의 암호를 지정합니다.

정책 저장소 루트 DN

LDAP 트리에서 정책 저장소 개체가 정의될 노드의 고유 이름을 지정합니다.

SSL 클라이언트 인증서

SSL 클라이언트 인증서 데이터베이스 파일이 있는 디렉터리의 경로 이름을 지정합니다.

제한: SSL에만 해당

정책 저장소를 구성하는 방법

Oracle Directory Server Enterprise Edition(이전의 Sun Directory Server Enterprise Edition)을 정책 저장소로 구성하려면 다음 절차를 완료하십시오.

1. (선택 사항) 해당하는 경우 공급업체별 소프트웨어를 사용하여 LDAP 디렉터리 서버 인스턴스를 생성합니다.
2. (선택 사항) 해당하는 경우 공급업체별 소프트웨어를 사용하여 다음 권한이 있는 관리 사용자를 생성합니다.

- create
- 읽기
- 수정
- 삭제

LDAP 트리에서 정책 저장소 루트 개체 아래에 이 사용자를 생성합니다.

3. Oracle Directory Server 고려 사항을 검토합니다.
4. 정책 서버를 디렉터리 서버에 연결합니다.
5. 정책 저장소 스키마를 생성합니다.
6. SiteMinder 슈퍼 사용자 암호를 설정합니다.
7. 정책 저장소 데이터 정의를 가져옵니다.
8. 기본 SiteMinder 개체를 가져옵니다.
9. 정책 서버를 다시 시작합니다.
10. 관리 UI 등록을 준비합니다.

Oracle Directory Server Enterprise Edition 고려 사항

Oracle Directory Server Enterprise Edition 을 정책 저장소로 사용하는 경우 다음 사항을 고려하십시오.

smldapsetup 및 Oracle Directory Enterprise Edition

smldapsetup 유틸리티는 `ou=Netegrity`, `root` 하위 접미사 및 `PolicySvr4` 데이터베이스를 생성합니다.

root

정책 서버 관리 콘솔의 "데이터" 탭에서 "루트 DN" 필드에 지정한 디렉터리 루트입니다. 이 변수는 기존의 루트 접미사 또는 하위 접미사여야 합니다.

예: 루트 접미사가 `dc=netegrity,dc=com` 일 경우 smldapsetup 을 실행하면 디렉터리 서버에 다음 항목이 생성됩니다.

- 루트 접미사, `dc=netegrity,dc=com` 과 해당 `userRoot` 데이터베이스
- 하위 접미사, `ou=Netegrity,dc=netegrity,dc=com` 과 해당 `PolicySvr4` 데이터베이스

예: 정책 저장소를 `ou=apps,dc=netegrity,dc=com` 아래에 배치하려는 경우 `ou=apps,dc=netegrity,dc=com` 은 루트 접미사이거나 루트 접미사 `c=netegrity,dc=com` 의 하위 접미사여야 합니다.

하위 접미사일 경우 smldapsetup 을 실행하면 다음 항목이 생성됩니다.

- 루트 접미사, `dc=netegrity,dc=com` 과 해당 `userRoot` 데이터베이스
- 하위 접미사, `ou=apps,dc=netegrity,dc=com` 과 해당 `Apps` 데이터베이스
- 하위 접미사, `ou=Netegrity,ou=apps,dc=netegrity,dc=com` 과 해당 `PolicySvr4` 데이터베이스

참고: 루트 및 하위 접미사에 대한 자세한 내용은 Oracle [설명서](#)를 참조하십시오.

Oracle Directory Server Enterprise Edition 정책 저장소 복제

SiteMinder 12.52 SP1 는 UserRoot 및 PolicySvr4 데이터베이스를 생성합니다. PolicySvr4 데이터베이스에는 데이터베이스를 가리키는 접미사 매핑이 있습니다. 이 정책 저장소를 복제하려면 PolicySvr4 데이터베이스 디렉터리에 대해 복제 계약을 설정하십시오.

참고: 복제 계약에 대한 자세한 내용은 Oracle [설명서](#)를 참조하십시오.

복제 계약을 생성했으면 SiteMinder 인덱스를 복제하십시오.

다음 단계를 수행하십시오.

1. SiteMinder 인덱스를 생성합니다.

```
smldapsetup ldgen -x -findexes.ldif
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

2. 복제본 서버에서 인덱스를 설정합니다.

```
smldapsetup ldmod -x -findexes.ldif -hhost -preplicaport  
-dAdminDN -wAdminPW
```

host

복제본 호스트를 지정합니다.

replicaport

복제본 포트 번호를 지정합니다.

AdminDN

복제본 관리자 DN 을 지정합니다.

예: cn=directory manager

AdminPW

복제본 관리자 암호를 지정합니다.

SiteMinder 인덱스가 복제되었습니다.

정책 서버를 정책 저장소에 연결

정책 서버가 정책 저장소에 액세스할 수 있도록 정책 서버를 정책 저장소에 연결하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.

중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "데이터" 탭을 클릭합니다.
3. "데이터베이스" 목록에서 다음 값을 선택합니다.

정책 저장소

4. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

5. "LDAP 정책 저장소" 그룹 상자에서 다음 설정을 구성합니다.

- LDAP IP 주소
- 관리자 사용자 이름
- 암호
- 암호 확인
- 루트 DN

참고: "도움말"을 클릭하면 필드, 컨트롤 및 해당되는 요구 사항에 대한 설명을 볼 수 있습니다.

6. "적용"을 클릭합니다.
7. "LDAP 연결 테스트"를 클릭하여 정책 서버에서 정책 저장소에 액세스할 수 있는지 여부를 확인합니다.
8. "데이터베이스" 목록에서 다음 값을 선택합니다.

키 저장소

9. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

10. 다음 옵션을 선택합니다.

정책 저장소 데이터베이스 사용

11. "확인"을 클릭합니다.

정책 저장소 스키마 만들기

디렉터리 서버가 정책 저장소로 작동하고 SiteMinder 개체를 저장할 수 있도록 정책 저장소 스키마를 생성하십시오. 다음 디렉터리 서버 제품에 대해 이 절차를 사용하십시오.

- Oracle 10g, 11g(32 비트)
- Sun Java 시스템 6.1, 7.0

다음 사전 요구 사항을 수행하십시오.

- LDAP 인스턴스를 생성합니다.
- SiteMinder 관리 콘솔을 열고 "데이터" 탭을 클릭한 다음 LDAP 인스턴스의 정책 저장소 및 키 저장소 정보를 입력합니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에서 다음 명령을 실행합니다.

```
smlldapsetup ldgen -ffile_name  
file_name
```

생성하려는 LDIF 파일의 이름을 지정합니다.

SiteMinder 스키마를 사용하여 LDIF 파일이 생성됩니다.

2. 다음 명령을 실행합니다.

```
smldapsetup ldmod -ffile_name
```

file_name

생성한 LDIF 의 이름을 지정합니다.

3. 다음 명령을 실행합니다.

```
smldapsetup ldmod -fpolicy_server_home\xps\db\OracleDirectoryServer.ldif
```

policy_server_home

정책 서버 설치 경로를 지정합니다.

4. 디렉터리 서버의 관리자가 다음 명령을 실행합니다.

```
dsconf reindex -h localhost -p port_number -e "ou=Netegrity,root_dn"
```

5. 다음 ldif 파일을 편집합니다.

```
policy_server_home/xps/db/OracleDirectoryServerBrowse.ldif
```

6. 계속하기 전에 LDAP 디렉터리가 다음 경로를 포함하는지 확인하십시오(아래 루트 DN 을 사용하는 루트 DN 으로 교체).

```
ou=xps,ou=PolicySvr4,ou=siteminder,ou=netegrity,<루트 DN>\
```

7. LDIF 파일을 편집하여 앞 단계의 <root dn> 값을 <root dn> 값이 파일에 있는 두 위치에 배치합니다.

8. Policy_server_home/xps/db/OracleDirectoryServerBrowser.ldif. 다음 명령을 실행합니다.

```
smldapsetup ldmod -fOracleDirectoryServerBrowse.ldif -v
```

9. 데이터베이스를 중지하고 다음 명령을 사용하여 vlv 인덱스를 다시 인덱싱합니다.

```
dsadm stop Instance_Path
```

```
dsadm reindex -bl -t "Sort xpsSortKey" Instance_Path policysvr4
```

```
dsadm reindex -bl -t "Sort modifyTimestamp" Instance_Path policysvr4
```

```
dsadm reindex -b -t xpsNumber -t xpsValue -t xpsSortKey -t xpsCategory -t  
xpsParameter -t xpsIndexedObject -t xpsTombstone instance_path policysvr4
```

10. 다음 명령을 사용하여 데이터베이스를 시작합니다.

```
dsadm start Instance_Path
```

정책 저장소 스키마가 확장됩니다. 정책 저장소 스키마를 생성했습니다.

SiteMinder 슈퍼 사용자 암호 설정

기본 SiteMinder 관리자 계정의 이름은 다음으로 지정됩니다.

siteminder

이 계정에는 최대 권한이 있습니다.

일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 다음과 같은 경우에 기본 슈퍼 사용자를 사용합니다.

- 관리 UI 에 처음 액세스할 경우
- SiteMinder 유틸리티를 처음 관리할 경우
- 슈퍼 사용자 권한이 있는 다른 관리자를 생성할 경우

다음 단계를 수행하십시오.

1. smreg 유틸리티를 *siteminder_home*\bin 에 복사합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

참고: 이 유틸리티는 정책 서버 설치 키트의 최상위 수준에 있습니다.

2. 다음 명령을 실행합니다.

smreg -su *password*

password

기본 SiteMinder 관리자의 암호를 지정합니다.

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: Oracle 정책 저장소를 구성하는 경우 암호의 대/소문자를 구분합니다. 다른 모든 정책 저장소에서는 암호의 대/소문자를 구분하지 않습니다.

3. *siteminder_home*\bin 에서 smreg 를 삭제합니다. smreg 를 삭제하면 이전 암호를 모르는 다른 사람은 암호를 변경할 수 없게 됩니다.

기본 SiteMinder 관리자 계정의 암호가 설정되었습니다.

정책 저장소 데이터 정의 가져오기

정책 저장소 데이터 정의 가져오기를 사용하여 정책 저장소에서 생성하고 저장할 수 있는 개체의 유형을 정의합니다.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home*\xps\dd 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

```
XPSDDInstall SmMaster.xdd
```

XPSDDInstall

필수 데이터 정의를 가져옵니다.

기본 정책 저장소 개체 가져오기

기본 정책 저장소 개체 가져오기를 사용하여 관리 UI 및 정책 서버에서 사용할 정책 저장소를 구성합니다.

다음 사항을 고려하십시오.

- *siteminder_home*\bin 에 대한 쓰기 액세스 권한이 있는지 확인하십시오. 가져오기 유틸리티에서 정책 저장소 개체를 가져오려면 이 권한이 필요합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

- Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 `siteminder_home\db` 로 이동합니다.

2. 다음 파일 중 하나를 가져옵니다.

- `smpolicy.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy.xml -npass
```

- `smpolicy-secure.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy-secure.xml -npass
```

npass

암호를 사용할 필요가 없음을 지정합니다. 기본 정책 저장소 개체에 암호화된 데이터가 포함되지 않습니다.

두 파일 모두 기본 정책 저장소 개체를 포함합니다. 이러한 개체는 기본 ACO(에이전트 구성 개체) 템플릿의 기본 보안 설정을 포함합니다. `smpolicy-secure` 파일은 보다 제한적인 보안 설정을 제공합니다. 자세한 내용은 [기본 정책 저장소 개체 고려 사항](#) (페이지 98)을 참조하십시오.

- 옵션 팩 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport ampolicy.xml -npass
```

- 페더레이션 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

정책 저장소 개체를 가져왔습니다.

참고: `smpolicy.xml` 을 가져오면 SiteMinder 에서 별도로 라이선스가 제공되는 레거시 페더레이션 및 웹 서비스 변수 기능을 사용할 수 있게 됩니다. 웹 서비스 변수 기능을 사용하려면 CA 고객 담당자에게 라이선스 정보에 대해 문의하십시오.

고급 인증 서버를 사용하도록 설정

정책 서버를 구성하는 과정에서 고급 인증 서버를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 구성 마법사를 시작합니다.
2. 마법사의 첫 번째 화면에서 모든 확인란을 **선택 취소**한 상태로 둡니다.
3. "다음"을 클릭합니다.
4. 고급 인증 서버에 대한 마스터 암호화 키를 생성합니다.

참고: 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

5. 정책 서버 구성 마법사의 나머지 과정을 완료합니다.
고급 인증 서버가 사용되도록 설정되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 **stop-all** 명령 다음에 **start-all** 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

관리 UI 등록 준비

기본 SiteMinder 슈퍼 사용자 계정(siteminder)을 사용하여 관리 UI 에 최초로 로그인합니다. 최초 로그인 시 관리 UI 를 정책 서버에 등록하여 두 구성 요소 간에 트러스트 관계를 생성해야 합니다.

등록을 준비하려면 XPSRegClient 유틸리티를 사용하여 슈퍼 사용자 계정 이름과 암호를 제공합니다. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 트러스트 관계를 설정할 수 있는지 확인합니다.

다음 사항을 고려하십시오.

- 자격 증명을 제공한 때부터 24 시간 이내에 최초 관리 UI 로그인이 이루어져야 합니다. 관리 UI 설치를 하루 안에 수행할 계획이 아니면 관리 UI 를 설치하기 전에 다음 단계를 완료하십시오.
- (UNIX) XPSRegClient 를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

기본 SiteMinder 슈퍼 사용자 계정(siteminder)의 암호를 지정합니다.

참고: 암호를 지정하지 않으면 XPSRegClient 에서 암호를 입력하고 확인하라는 메시지가 표시됩니다.

-adminui-setup

관리 UI 가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 관리 UI 를 설치할 때부터 정책 서버에 로그인하고 정책 서버와의 트러스트 관계를 생성할 때까지 할당된 시간을 지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록 요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 15

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI 를 등록할 때 허용되는 시도 실패 횟수를 지정합니다. 관리 UI 에 최초로 로그인할 때 올바르게 않은 SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수 있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을 삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error_path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: stderr

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

XPSRegClient 가 정책 서버에 관리자 자격 증명을 제공합니다. 정책 서버에서는 관리 UI 에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

Oracle Internet Directory 를 정책 저장소로 구성

OID(Oracle Internet Directory)는 정책 저장소로 작동할 수 있습니다. 단일 디렉터리 서버 인스턴스가 다음 기능을 수행할 수 있습니다.

- 정책 저장소
- 키 저장소

단일 디렉터리 서버를 사용하면 관리 태스크를 간소화할 수 있습니다. 다음 단원에서는 정책 데이터 및 암호화 키를 저장하도록 단일 디렉터리 서버 인스턴스를 구성하는 방법에 대한 지침을 제공합니다. 구현에 필요할 경우 별도의 키 저장소를 구성할 수 있습니다.

디렉터리 서버 정보 수집

LDAP 디렉터리 서버를 정책 저장소로 구성하거나 기존 정책 저장소를 업그레이드하려면 특정 디렉터리 서버 정보가 필요합니다. 시작하기 전에 다음 정보를 수집하십시오. 정책 저장소 워크시트를 사용하여 값을 기록할 수 있습니다.

호스트 정보

디렉터리 서버의 정규화된 호스트 이름 또는 IP 주소를 지정합니다.

포트 정보

(선택 사항) 비표준 포트를 지정합니다.

기본값: 636(SSL) 및 389(비 SSL)

관리 DN

LDAP 트리에서 정책 저장소 루트 개체 아래의 개체에 대한 생성, 읽기, 수정 및 삭제 권한이 있는 사용자의 LDAP 사용자 이름을 지정합니다.

관리 암호

관리 DN의 암호를 지정합니다.

정책 저장소 루트 DN

LDAP 트리에서 정책 저장소 개체가 정의될 노드의 고유 이름을 지정합니다.

SSL 클라이언트 인증서

SSL 클라이언트 인증서 데이터베이스 파일이 있는 디렉터리의 경로 이름을 지정합니다.

제한: SSL에만 해당

정책 저장소를 구성하는 방법

OID를 정책 저장소로 구성하려면 다음 절차를 완료하십시오.

1. 필수 특성을 인덱싱합니다.
2. Oracle Internet Directory에서 도메인을 구성합니다.
3. 정책 서버를 디렉터리 서버에 연결합니다.
4. 정책 저장소 스키마를 생성합니다.
5. SiteMinder 슈퍼 사용자 암호를 설정합니다.

6. 정책 저장소 데이터 정의를 가져옵니다.
7. 기본 정책 저장소 개체를 가져옵니다.
8. 정책 서버를 다시 시작합니다.
9. 관리 UI 등록을 준비합니다.

필요한 특성 인덱싱

다음 특성을 인덱싱하면 기본 정책 저장소 개체를 가져올 때 오류가 발생하지 않습니다.

`modifyTimestamp`

다음 단계를 수행하십시오.

1. Oracle Internet Directory 호스트 시스템에 로그인합니다.
2. Oracle 카탈로그 명령줄 도구를 사용하여 다음 명령을 실행합니다.

```
oracle_home/ldap/bin/catalog connect=conn_str add=TRUE
attribute=modifyTimestamp
```

oracle_home

Oracle Internet Directory 설치 경로를 지정합니다.

conn_str

디렉터리 데이터베이스 연결 문자열을 지정합니다. `tnsnames.ora` 파일을 구성한 경우 이 파일에 지정된 `net` 서비스 이름을 입력합니다.

특성이 인덱싱되었습니다.

참고: 카탈로그 명령줄 도구에 대한 자세한 내용은 Oracle 설명서를 참조하십시오.

Oracle Internet Directory 에 도메인 구성

OID 를 정책 저장소로 구성하려면 먼저 OID 에 도메인을 생성하십시오.

다음 단계를 수행하십시오.

1. Oracle Data Manager(ODM)를 엽니다.
2. "Entry Management"(항목 관리)를 마우스 오른쪽 단추로 클릭하고 "Create"(만들기)를 선택합니다.
3. "Distinguished Name"(고유 이름) 값으로 **dc=dcbok** 를 입력합니다.

4. dc 값으로 **dc** 를 입력합니다.
5. 조직 단위를 생성합니다.
6. 조직 단위를 선택합니다.
7. "Distinguished Name"(고유 이름) 값으로 **ou=bok,dc=dcbok** 를 입력합니다.
8. ou 값으로 **bok** 를 입력합니다.
OID 도메인이 구성되었습니다.

정책 서버를 정책 저장소에 연결

정책 서버가 정책 저장소에 액세스할 수 있도록 정책 서버를 정책 저장소에 연결하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.

중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "데이터" 탭을 클릭합니다.
3. "데이터베이스" 목록에서 다음 값을 선택합니다.

정책 저장소

4. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

5. "LDAP 정책 저장소" 그룹 상자에서 다음 설정을 구성합니다.

- LDAP IP 주소
- 관리자 사용자 이름
- 암호
- 암호 확인
- 루트 DN

참고: "도움말"을 클릭하면 필드, 컨트롤 및 해당되는 요구 사항에 대한 설명을 볼 수 있습니다.

6. "적용"을 클릭합니다.
7. "LDAP 연결 테스트"를 클릭하여 정책 서버에서 정책 저장소에 액세스할 수 있는지 여부를 확인합니다.
8. "데이터베이스" 목록에서 다음 값을 선택합니다.
키 저장소
9. "저장소" 목록에서 다음 값을 선택합니다.
LDAP
10. 다음 옵션을 선택합니다.
정책 저장소 데이터베이스 사용
11. "확인"을 클릭합니다.

정책 저장소 스키마 만들기

디렉터리 서버가 정책 저장소로 작동하고 SiteMinder 개체를 저장할 수 있도록 정책 저장소 스키마를 생성하십시오.

다음 단계를 수행하십시오.

1. 다음 명령을 실행합니다.

```
smlldapsetup ldgen -ffile_name.ldif
-ffile_name
```

생성할 스키마 파일의 이름을 지정합니다.

2. 다음 명령을 실행합니다.

```
smlldapsetup ldmod -ffile_name.ldif
-ffile_name
```

생성한 스키마 파일의 이름을 지정합니다.

3. 다음 명령을 실행합니다.

```
ldapmodify -hhost -pport -dAdminDN -wAdminPW
-c -fsiteminder_home/xps/db/OID_10g.ldif
-Z -Pcert
```

참고: 스키마 파일은 버전별이지만 이 파일을 사용하여 지원되는 모든 OID 버전에 대한 정책 저장소 스키마를 가져올 수 있습니다.

-hhost

LDAP 디렉터리 서버의 IP 주소를 지정합니다.

예: 123.123.12.12

-pport

LDAP 디렉터리 서버의 포트 번호를 지정합니다.

예: 3500

-dAdminDN

LDAP 디렉터리 서버에 스키마를 생성할 수 있는 권한이 있는 LDAP 사용자의 이름을 지정합니다.

-wAdminPW

-d 옵션으로 지정된 관리자의 암호를 지정합니다.

-c

연속 모드(오류 시 중지되지 않음)를 지정합니다.

-fsiteminder_home

정책 서버 설치 경로를 지정합니다.

-Z

(선택 사항) SSL 암호화 연결을 지정합니다.

-P cert

(선택 사항) SSL 클라이언트 인증서 데이터베이스 파일(cert8.db)의 경로를 지정합니다.

예:

cert8.db 가 app/siteminder/ssl 에 있으면 다음을 지정합니다.

-Papp/siteminder/ssl

정책 저장소 스키마가 생성되었습니다.

SiteMinder 슈퍼 사용자 암호 설정

기본 SiteMinder 관리자 계정의 이름은 다음으로 지정됩니다.

siteminder

이 계정에는 최대 권한이 있습니다.

일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 다음과 같은 경우에 기본 슈퍼 사용자를 사용합니다.

- 관리 UI 에 처음 액세스할 경우
- SiteMinder 유틸리티를 처음 관리할 경우
- 슈퍼 사용자 권한이 있는 다른 관리자를 생성할 경우

다음 단계를 수행하십시오.

1. smreg 유틸리티를 *siteminder_home*\bin 에 복사합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

참고: 이 유틸리티는 정책 서버 설치 키트의 최상위 수준에 있습니다.

2. 다음 명령을 실행합니다.

smreg -su *password*

password

기본 SiteMinder 관리자의 암호를 지정합니다.

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: Oracle 정책 저장소를 구성하는 경우 암호의 대/소문자를 구분합니다. 다른 모든 정책 저장소에서는 암호의 대/소문자를 구분하지 않습니다.

3. *siteminder_home*\bin 에서 smreg 를 삭제합니다. smreg 를 삭제하면 이전 암호를 모르는 다른 사람은 암호를 변경할 수 없게 됩니다.

기본 SiteMinder 관리자 계정의 암호가 설정되었습니다.

정책 저장소 데이터 정의 가져오기

정책 저장소 데이터 정의 가져오기를 사용하여 정책 저장소에서 생성하고 저장할 수 있는 개체의 유형을 정의합니다.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home*\xps\dd 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

```
XPSDDInstall SmMaster.xdd
```

XPSDDInstall

필수 데이터 정의를 가져옵니다.

기본 정책 저장소 개체 가져오기

기본 정책 저장소 개체 가져오기를 사용하여 관리 UI 및 정책 서버에서 사용할 정책 저장소를 구성합니다.

다음 사항을 고려하십시오.

- *siteminder_home*\bin 에 대한 쓰기 액세스 권한이 있는지 확인하십시오. 가져오기 유틸리티에서 정책 저장소 개체를 가져오려면 이 권한이 필요합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

- Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home\db* 로 이동합니다.

2. 다음 파일 중 하나를 가져옵니다.

- *smpolicy.xml* 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy.xml -npass
```

- *smpolicy-secure.xml* 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy-secure.xml -npass
```

npass

암호를 사용할 필요가 없음을 지정합니다. 기본 정책 저장소 개체에 암호화된 데이터가 포함되지 않습니다.

두 파일 모두 기본 정책 저장소 개체를 포함합니다. 이러한 개체는 기본 ACO(에이전트 구성 개체) 템플릿의 기본 보안 설정을 포함합니다. *smpolicy-secure* 파일은 보다 제한적인 보안 설정을 제공합니다. 자세한 내용은 [기본 정책 저장소 개체 고려 사항](#) (페이지 98)을 참조하십시오.

- 옵션 팩 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport ampolicy.xml -npass
```

- 페더레이션 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

정책 저장소 개체를 가져왔습니다.

참고: *smpolicy.xml* 을 가져오면 SiteMinder 에서 별도로 라이선스가 제공되는 레거시 페더레이션 및 웹 서비스 변수 기능을 사용할 수 있게 됩니다. 웹 서비스 변수 기능을 사용하려면 CA 고객 담당자에게 라이선스 정보에 대해 문의하십시오.

고급 인증 서버를 사용하도록 설정

정책 서버를 구성하는 과정에서 고급 인증 서버를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 구성 마법사를 시작합니다.
2. 마법사의 첫 번째 화면에서 모든 확인란을 *선택 취소*한 상태로 둡니다.
3. "다음"을 클릭합니다.
4. 고급 인증 서버에 대한 마스터 암호화 키를 생성합니다.

참고: 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

5. 정책 서버 구성 마법사의 나머지 과정을 완료합니다.
고급 인증 서버가 사용되도록 설정되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 **stop-all** 명령 다음에 **start-all** 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

관리 UI 등록 준비

기본 SiteMinder 슈퍼 사용자 계정(siteminder)을 사용하여 관리 UI 에 최초로 로그인합니다. 최초 로그인 시 관리 UI 를 정책 서버에 등록하여 두 구성 요소 간에 트러스트 관계를 생성해야 합니다.

등록을 준비하려면 XPSRegClient 유틸리티를 사용하여 슈퍼 사용자 계정 이름과 암호를 제공합니다. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 트러스트 관계를 설정할 수 있는지 확인합니다.

다음 사항을 고려하십시오.

- 자격 증명을 제공한 때부터 24 시간 이내에 최초 관리 UI 로그인이 이루어져야 합니다. 관리 UI 설치를 하루 안에 수행할 계획이 아니면 관리 UI 를 설치하기 전에 다음 단계를 완료하십시오.
- (UNIX) XPSRegClient 를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

기본 SiteMinder 슈퍼 사용자 계정(siteminder)의 암호를 지정합니다.

참고: 암호를 지정하지 않으면 XPSRegClient 에서 암호를 입력하고 확인하라는 메시지가 표시됩니다.

-adminui-setup

관리 UI 가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 관리 UI 를 설치할 때부터 정책 서버에 로그인하고 정책 서버와의 트러스트 관계를 생성할 때까지 할당된 시간을 지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록 요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 15

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI 를 등록할 때 허용되는 시도 실패 횟수를 지정합니다. 관리 UI 에 최초로 로그인할 때 올바르게 않은 SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수 있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을 삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error_path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: stderr

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

XPSRegClient 가 정책 서버에 관리자 자격 증명을 제공합니다. 정책 서버에서는 관리 UI 에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

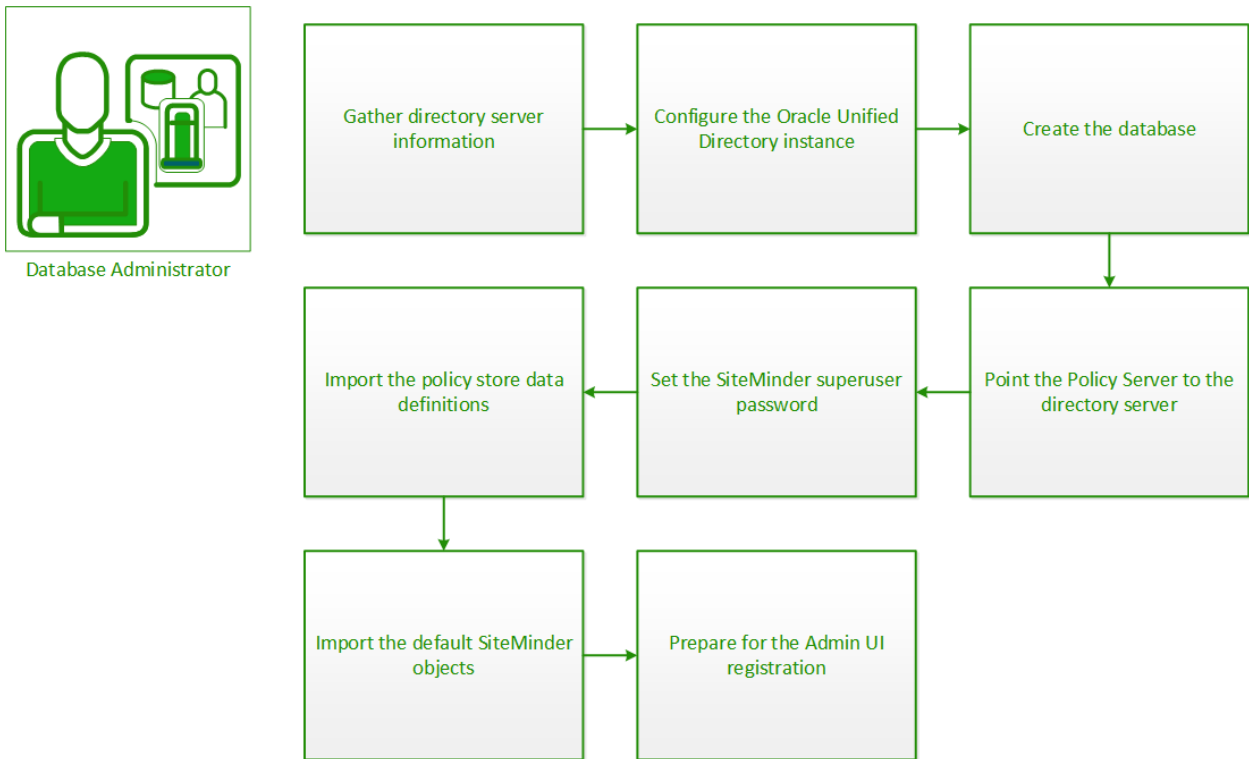
Oracle Unified Directory 를 정책 저장소로 구성하는 방법

OOD(Oracle Unified Directory)는 정책 저장소로서 기능할 수 있습니다. 단일 디렉터리 서버 인스턴스가 다음 기능을 수행할 수 있습니다.

- 정책 저장소
- 키 저장소

단일 디렉터리 서버를 사용하면 관리 태스크를 간소화할 수 있습니다. 이 시나리오는 정책 데이터 및 암호화 키를 저장하도록 단일 디렉터리 서버 인스턴스를 구성하는 방법을 설명합니다.

참고: 구현에 필요할 경우 별도의 키 저장소를 구성할 수 있습니다.



Oracle Unified Directory 를 정책 저장소로 구성하려면 다음 절차를 완료하십시오.

1. [디렉터리 서버 정보를 수집합니다.](#) (페이지 120)
2. [Oracle Unified Directory 인스턴스를 구성합니다.](#) (페이지 226).
3. [데이터베이스를 생성합니다.](#) (페이지 230).

4. [정책 서버를 디렉터리 서버에 연결합니다](#) (페이지 105).
5. [SiteMinder 슈퍼 사용자 암호를 설정합니다](#) (페이지 106).
6. [정책 저장소 데이터 정의를 가져옵니다](#) (페이지 109).
7. [기본 SiteMinder 개체를 가져옵니다](#) (페이지 109).
8. [관리 UI 등록을 준비합니다](#) (페이지 111).

디렉터리 서버 정보 수집

LDAP 디렉터리 서버를 정책 저장소로 구성하거나 기존 정책 저장소를 업그레이드하려면 특정 디렉터리 서버 정보가 필요합니다. 시작하기 전에 다음 정보를 수집하십시오. 정책 저장소 워크시트를 사용하여 값을 기록할 수 있습니다.

호스트 정보

디렉터리 서버의 정규화된 호스트 이름 또는 IP 주소를 지정합니다.

포트 정보

(선택 사항) 비표준 포트를 지정합니다.

기본값: 636(SSL) 및 389(비 SSL)

관리 DN

LDAP 트리에서 정책 저장소 루트 개체 아래의 개체에 대한 생성, 읽기, 수정 및 삭제 권한이 있는 사용자의 LDAP 사용자 이름을 지정합니다.

관리 암호

관리 DN의 암호를 지정합니다.

정책 저장소 루트 DN

LDAP 트리에서 정책 저장소 개체가 정의될 노드의 고유 이름을 지정합니다.

SSL 클라이언트 인증서

SSL 클라이언트 인증서 데이터베이스 파일이 있는 디렉터리의 경로 이름을 지정합니다.

제한: SSL에만 해당

Oracle Unified Directory 인스턴스를 구성하는 방법

Oracle Unified Directory 를 정책 저장소로 사용하려면 먼저 추가 구성을 수행해야 합니다. 구성 단계는 다음과 같습니다.

1. [Windows](#) (페이지 226) 또는 [UNIX](#) (페이지 227)에서 SiteMinder 스키마 파일을 지정합니다.
2. [Windows](#) (페이지 227) 또는 [UNIX](#) (페이지 229)에서 정책 저장소 인텍싱을 구성합니다.

Windows 에서 SiteMinder 스키마 파일을 지정합니다.

SiteMinder 스키마 파일을 지정합니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. `ps_home\db\tier2\OUD` 로 이동하여 다음 파일을 Oracle Unified Directory 설치 디렉터리의 스키마 폴더(`oud_instance\config\schema`)에 복사합니다.

`oud_sm_schema.ldif`

`ps_home`

정책 서버 설치 경로를 지정합니다.

`oud_instance`

Oracle Unified Directory 인스턴스의 이름을 지정합니다.

3. `ps_home\tps\db\schema_extension\db\OUD` 로 이동하여 다음 파일을 Oracle Unified Directory 설치 디렉터리의 스키마 폴더(`oud_instance\config\schema`)에 복사합니다.

`oud_XPS_schema.ldif`

SiteMinder 스키마 파일이 지정되었습니다.

UNIX 에서 SiteMinder 스키마 파일을 지정합니다.

SiteMinder 스키마 파일을 지정합니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. `ps_home/db/tier2/OUT` 로 이동하여 다음 파일을 Oracle Unified Directory 설치 디렉터리의 스키마 폴더(`oud_instance/config/schema`)에 복사합니다.

`oud_sm_schema.ldif`

`ps_home`

정책 서버 설치 경로를 지정합니다.

`oud_instance`

Oracle Unified Directory 인스턴스의 이름을 지정합니다.

3. `ps_home/xps/db/schema_extension/db/OUT` 로 이동하여 다음 파일을 Oracle Unified Directory 설치 디렉터리의 스키마 폴더(`oud_instance/config/schema`)에 복사합니다.

`oud_XPS_schema.ldif`

SiteMinder 스키마 파일이 지정되었습니다.

Windows 에서 프록시 저장소 인텍싱 구성

Oracle Unified Directory 를 정책 저장소로 사용하려면 Oracle Unified Directory 인스턴스 구성 파일(`oud_instance\config\config.ldif`)에서 인텍싱을 지정하십시오.

다음 단계를 수행하십시오.

1. Oracle Unified Directory 인스턴스를 중지합니다.
2. 텍스트 편집기에서 `oud_instance\config\config.ldif` 파일을 엽니다.

`oud_instance`

Oracle Unified Directory 인스턴스의 이름을 지정합니다.

3. 다음 행을 찾습니다.

```
dn: cn=Index,cn=userRoot,cn=Workflow Elements,cn=config
objectClass: top
objectClass: ds-cfg-branch
cn: Index
```

4. 파일에 새 행을 삽입한 후 다음 파일의 내용을 추가합니다.
 - `ps_home\db\tier2\OUD\oud_sm_indexes.ldif`
 - `ps_home\xps\db\schema_extension\db\OUD\oud_xps_index.ldif`
5. 파일을 저장하고 텍스트 편집기를 닫습니다.
6. 인덱스를 재작성하려면 `oud_instance\bat` 로 이동하여 다음 명령을 실행합니다.

```
rebuild-index.bat -b base_dn --rebuildAll -h hostname -p OUD_administration_port  
-D "cn=Directory Manager" -j <bindpasswordfile> -X -t 0 --completionNotify  
emailAddress
```

base_dn

인덱싱을 지원하는 백엔드의 기본 DN 을 지정합니다. 인덱스는 지정된 기본 DN 의 범위 내에서 작성됩니다.

hostname

디렉터리 서버의 정규화된 호스트 이름 또는 IP 주소를 지정합니다. 제공하지 않으면 localhost 가 기본값으로 사용됩니다.

OUD_administration_port

디렉터리 서버의 관리 포트를 지정합니다. 제공하지 않으면 기본 관리 포트(44444)가 사용됩니다.

bindpasswordfile

디렉터리 서버로 인증할 때 사용할 바인드 암호를 수록한 파일을 지정합니다.

completionNotify

태스크가 완료될 때 알릴 수신자의 전자 메일 주소를 지정합니다. 이 옵션은 하나의 명령에서 여러 번 지정할 수 있습니다.

7. 재작성 태스크가 완료된 후 Oracle Unified Directory 인스턴스를 다시 시작합니다.

Oracle Unified Directory 에 대한 정책 저장소 인덱싱이 지정되었습니다.

UNIX 에서 정책 저장소 인덱싱 지정

Oracle Unified Directory 를 정책 저장소로 사용하려면 Oracle Unified Directory 인스턴스 구성 파일(*oud_instance/config/config.ldif*)에서 인덱싱을 지정하십시오.

다음 단계를 수행하십시오.

1. Oracle Unified Directory 인스턴스를 중지합니다.
2. 텍스트 편집기에서 *oud_instance/config/config.ldif* 파일을 엽니다.

oud_instance

Oracle Unified Directory 인스턴스의 이름을 지정합니다.

3. 다음 행을 찾습니다.

```
dn: cn=Index,cn=userRoot,cn=Workflow Elements,cn=config
objectClass: top
objectClass: ds-cfg-branch
cn: Index
```

4. 파일에 새 행을 삽입한 후 다음 파일의 내용을 추가합니다.

- *ps_home/db/tier2/LOUD/oud_sm_indexes.ldif*
- *ps_home/xps/db/schema_extension/db/LOUD/oud_xps_index.ldif*

ps_home

정책 서버 설치 경로를 지정합니다.

5. 파일을 저장하고 텍스트 편집기를 닫습니다.
6. *oud_instance/bin* 으로 이동한 후 다음 명령을 실행하여 인덱스를 재작성합니다.

```
rebuild-index -b base_dn --rebuildAll -h hostname -p OUD_administration_port -D
"cn=Directory Manager" -j bindpasswordfile -X -t 0 --completionNotify
emailAddress
```

base_dn

인덱싱을 지원하는 백엔드의 기본 DN 을 지정합니다. 인덱스는 지정된 기본 DN 의 범위 내에서 작성됩니다.

hostname

디렉터리 서버의 정규화된 호스트 이름 또는 IP 주소를 지정합니다. 제공하지 않으면 *localhost* 가 기본값으로 사용됩니다.

OID_administration_port

디렉터리 서버의 관리 포트를 지정합니다. 제공하지 않으면 기본 관리 포트(4444)가 사용됩니다.

bindpasswordfile

디렉터리 서버로 인증할 때 사용할 바인드 암호를 수록한 파일을 지정합니다.

completionNotify

태스크가 완료될 때 알릴 수신자의 전자 메일 주소를 지정합니다. 이 옵션은 하나의 명령에서 여러 번 지정할 수 있습니다.

7. 재작성 태스크가 완료된 후 Oracle Unified Directory 인스턴스를 다시 시작합니다.

Oracle Unified Directory 에 대한 정책 저장소 인덱싱이 지정되었습니다.

데이터베이스 생성 방법

다음 프로세스에서는 정책 저장소의 디렉터리 서버 데이터베이스를 생성하는 단계를 보여 줍니다.

1. 기본 트리 구조를 생성합니다.
2. 항목을 추가합니다.

기본 트리 구조 만들기

정책 저장소 개체를 저장하기 위한 기본 트리 구조를 만들려면 루트 DN 아래에 다음 항목을 지정하십시오.

`ou=Netegrity,ou=SiteMinder,ou=PolicySvr4`

데이터베이스에 항목 추가

SiteMinder 에서 필요한 조직 및 조직 역할 정보를 갖도록 디렉터리 서버에 항목을 추가하십시오.

다음 단계를 수행하십시오.

1. LDIF 파일을 생성합니다.

예: 다음 예에는 `entries.ldif` 에 대한 조직 역할 항목과 조직 항목이 포함되어 있습니다.

```
# CA, example.com
dn: ou=Netegrity,dc= example,dc=com
ou: CA
objectClass: organizationalUnit
objectClass: top

# SiteMinder, CA, example.com
dn: ou=SiteMinder,ou=CA,dc= example,dc=com
ou: SiteMinder
objectClass: organizationalUnit
objectClass: top

# PolicySvr4, SiteMinder, CA, example.com
dn: ou=PolicySvr4,ou=SiteMinder,ou=CA,dc= example,dc=com
ou: PolicySvr4
objectClass: organizationalUnit
objectClass: top
```

2. 항목을 추가하려면 다음 명령을 실행하십시오.

```
ldapmodify -h hostname -p port -D bindDN -j pwd_file -a -f LDIF_file_name
```

hostname

디렉터리 서버의 정규화된 호스트 이름 또는 IP 주소를 지정합니다.

기본값: localhost

port

디렉터리 서버에 연결하는 포트를 지정합니다.

기본값: 389

BindDN

디렉터리 서버로 인증하기 위한 바인드 DN 을 지정합니다.

기본값: cn=Directory Manager

pwd_file

디렉터리 서버로 인증하기 위한 바인드 암호를 수록한 파일을 지정합니다.

LDIF_file_name

1 단계에서 만든 LDIF 파일을 지정합니다.

정책 서버를 정책 저장소에 연결

정책 서버가 정책 저장소에 액세스할 수 있도록 정책 서버를 정책 저장소에 연결하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.

중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자 권한으로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "데이터" 탭을 클릭합니다.
3. "데이터베이스" 목록에서 다음 값을 선택합니다.

정책 저장소

4. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

5. "LDAP 정책 저장소" 그룹 상자에서 다음 설정을 구성합니다.

- LDAP IP 주소
- 관리자 사용자 이름
- 암호

- 암호 확인
- 루트 DN

참고: "도움말"을 클릭하면 필드, 컨트롤 및 해당되는 요구 사항에 대한 설명을 볼 수 있습니다.

6. "적용"을 클릭합니다.
7. "LDAP 연결 테스트"를 클릭하여 정책 서버에서 정책 저장소에 액세스할 수 있는지 여부를 확인합니다.
8. "데이터베이스" 목록에서 다음 값을 선택합니다.
키 저장소
9. "저장소" 목록에서 다음 값을 선택합니다.
LDAP
10. 다음 옵션을 선택합니다.
정책 저장소 데이터베이스 사용
11. "확인"을 클릭합니다.

SiteMinder 슈퍼 사용자 암호 설정

기본 SiteMinder 관리자 계정의 이름은 다음으로 지정됩니다.

`siteminder`

이 계정에는 최대 권한이 있습니다.

일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 다음과 같은 경우에 기본 슈퍼 사용자를 사용합니다.

- 관리 UI 에 처음 액세스할 경우
- SiteMinder 유틸리티를 처음 관리할 경우
- 슈퍼 사용자 권한이 있는 다른 관리자를 생성할 경우

다음 단계를 수행하십시오.

1. `smreg` 유틸리티를 `siteminder_home\bin` 에 복사합니다.

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

참고: 이 유틸리티는 정책 서버 설치 키트의 최상위 수준에 있습니다.

2. 다음 명령을 실행합니다.

```
smreg -su password
```

password

기본 SiteMinder 관리자의 암호를 지정합니다.

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: Oracle 정책 저장소를 구성하는 경우 암호의 대/소문자를 구분합니다. 다른 모든 정책 저장소에서는 암호의 대/소문자를 구분하지 않습니다.

3. *siteminder_home*\bin 에서 smreg 를 삭제합니다. smreg 를 삭제하면 이전 암호를 모르는 다른 사람은 암호를 변경할 수 없게 됩니다.

기본 SiteMinder 관리자 계정의 암호가 설정되었습니다.

정책 저장소 데이터 정의 가져오기

정책 저장소 데이터 정의 가져오기를 사용하여 정책 저장소에서 생성하고 저장할 수 있는 개체의 유형을 정의합니다.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home*\xps\dd 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

```
XPSDDInstall SmMaster.xdd
```

XPSDDInstall

필수 데이터 정의를 가져옵니다.

기본 정책 저장소 개체 가져오기

기본 정책 저장소 개체 가져오기를 사용하여 관리 UI 및 정책 서버에서 사용할 정책 저장소를 구성합니다.

다음 사항을 고려하십시오.

- *siteminder_home\bin*에 대한 쓰기 액세스 권한이 있는지 확인하십시오. 가져오기 유틸리티에서 정책 저장소 개체를 가져오려면 이 권한이 필요합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

- Windows Server 2008에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home\db* 로 이동합니다.

2. 다음 파일 중 하나를 가져옵니다.

- *smpolicy.xml* 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy.xml -npass
```

- *smpolicy-secure.xml* 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy-secure.xml -npass
```

npass

암호를 사용할 필요가 없음을 지정합니다. 기본 정책 저장소 개체에 암호화된 데이터가 포함되지 않습니다.

두 파일 모두 기본 정책 저장소 개체를 포함합니다. 이러한 개체는 기본 ACO(에이전트 구성 개체) 템플릿의 기본 보안 설정을 포함합니다. *smpolicy-secure* 파일은 보다 제한적인 보안 설정을 제공합니다. 자세한 내용은 [기본 정책 저장소 개체 고려 사항](#) (페이지 98)을 참조하십시오.

- 옵션 팩 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport ampolicy.xml -npass
```

- 페더레이션 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

정책 저장소 개체를 가져왔습니다.

참고: *smpolicy.xml* 을 가져오면 SiteMinder 에서 별도로 라이선스가 제공되는 레거시 페더레이션 및 웹 서비스 변수 기능을 사용할 수 있게 됩니다. 웹 서비스 변수 기능을 사용하려면 CA 고객 담당자에게 라이선스 정보에 대해 문의하십시오.

고급 인증 서버를 사용하도록 설정

정책 서버를 구성하는 과정에서 고급 인증 서버를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 구성 마법사를 시작합니다.
2. 마법사의 첫 번째 화면에서 모든 확인란을 *선택 취소*한 상태로 둡니다.
3. "다음"을 클릭합니다.
4. 고급 인증 서버에 대한 마스터 암호화 키를 생성합니다.

참고: 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

5. 정책 서버 구성 마법사의 나머지 과정을 완료합니다.
고급 인증 서버가 사용되도록 설정되었습니다.

관리 UI 등록 준비

기본 SiteMinder 슈퍼 사용자 계정(siteminder)을 사용하여 관리 UI 에 최초로 로그인합니다. 최초 로그인 시 관리 UI 를 정책 서버에 등록하여 두 구성 요소 간에 트러스트 관계를 생성해야 합니다.

등록을 준비하려면 XPSRegClient 유틸리티를 사용하여 슈퍼 사용자 계정 이름과 암호를 제공합니다. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 트러스트 관계를 설정할 수 있는지 확인합니다.

다음 사항을 고려하십시오.

- 자격 증명을 제공한 때부터 24 시간 이내에 최초 관리 UI 로그인 이루어져야 합니다. 관리 UI 설치를 하루 안에 수행할 계획이 아니면 관리 UI 를 설치하기 전에 다음 단계를 완료하십시오.
- (UNIX) XPSRegClient 를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c  
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

기본 SiteMinder 슈퍼 사용자 계정(siteminder)의 암호를 지정합니다.

참고: 암호를 지정하지 않으면 XPSRegClient 에서 암호를 입력하고
확인하라는 메시지가 표시됩니다.

-adminui-setup

관리 UI 가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 관리 UI 를 설치할 때부터 정책 서버에 로그인하고 정책
서버와의 트러스트 관계를 생성할 때까지 할당된 시간을
지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록
요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 15

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI 를 등록할 때 허용되는 시도 실패 횟수를
지정합니다. 관리 UI 에 최초로 로그인할 때 올바르게 않은
SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수
있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을
삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error_path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: `stderr`

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

XPSRegClient 가 정책 서버에 관리자 자격 증명을 제공합니다. 정책 서버에서는 관리 UI 에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

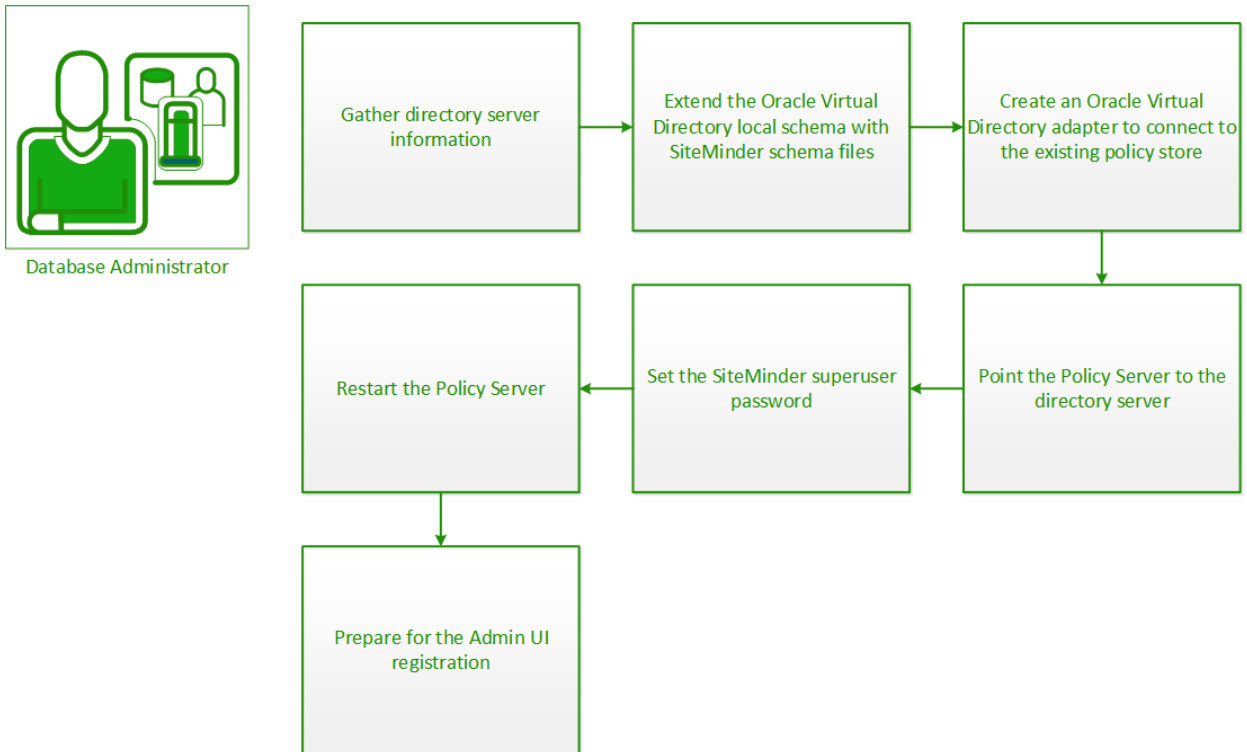
Oracle Virtual Directory 를 정책 저장소로 구성하는 방법

OVD(Oracle Virtual Directory)는 정책 저장소로서 기능할 수 있습니다. 단일 디렉터리 서버 인스턴스가 다음 기능을 수행할 수 있습니다.

- 정책 저장소
- 키 저장소

단일 디렉터리 서버를 사용하면 관리 태스크를 간소화할 수 있습니다. 이 시나리오는 정책 데이터 및 암호화 키를 저장하도록 단일 디렉터리 서버 인스턴스를 구성하는 방법을 설명합니다.

참고: 구현에 필요할 경우 별도의 키 저장소를 구성할 수 있습니다.



Oracle Virtual Directory 를 정책 저장소로 구성하려면 다음 절차를 수행하십시오.

1. [디렉터리 서버 정보를 수집합니다.](#) (페이지 120)
2. [SiteMinder 스키마 파일을 사용하여 Oracle Virtual Directory 로컬 스키마를 확장합니다.](#) (페이지 243).
3. [기존 정책 저장소에 연결하기 위해 Oracle Virtual Directory 어댑터를 만듭니다.](#) (페이지 244).
4. [정책 서버를 디렉터리 서버에 연결합니다.](#) (페이지 105).
5. [SiteMinder 슈퍼 사용자 암호를 설정합니다.](#) (페이지 106).
6. [정책 서버를 다시 시작합니다.](#) (페이지 128).
7. [관리 UI 등록을 준비합니다.](#) (페이지 111).

디렉터리 서버 정보 수집

LDAP 디렉터리 서버를 정책 저장소로 구성하거나 기존 정책 저장소를 업그레이드하려면 특정 디렉터리 서버 정보가 필요합니다. 시작하기 전에 다음 정보를 수집하십시오. 정책 저장소 워크시트를 사용하여 값을 기록할 수 있습니다.

호스트 정보

디렉터리 서버의 정규화된 호스트 이름 또는 IP 주소를 지정합니다.

포트 정보

(선택 사항) 비표준 포트를 지정합니다.

기본값: 636(SSL) 및 389(비 SSL)

관리 DN

LDAP 트리에서 정책 저장소 루트 개체 아래의 개체에 대한 생성, 읽기, 수정 및 삭제 권한이 있는 사용자의 LDAP 사용자 이름을 지정합니다.

관리 암호

관리 DN 의 암호를 지정합니다.

정책 저장소 루트 DN

LDAP 트리에서 정책 저장소 개체가 정의될 노드의 고유 이름을 지정합니다.

SSL 클라이언트 인증서

SSL 클라이언트 인증서 데이터베이스 파일이 있는 디렉터리의 경로 이름을 지정합니다.

제한: SSL에만 해당

SiteMinder 스키마 파일을 사용하여 OVD 로컬 스키마 확장

다음 SiteMinder 스키마 파일을 사용하여 Oracle Virtual Directory 를 확장합니다.

- ovd_sm_schema.ldif
- ovd_xps_schema.ldif

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. *siteminder_home/db/tier2/Oracle Virtual Directory* 로 이동하여 다음 파일을 OVD 호스트 시스템으로 복사합니다.

```
ovd_sm_schema.ldif
```

3. *siteminder_home/xps/db/schema_extension/db/Oracle Virtual Directory* 로 이동하여 다음 파일을 OVD 호스트 시스템으로 복사합니다.

```
ovd_xps_schema.ldif
```

4. Oracle Virtual Directory 호스트 시스템에 로그인합니다.
5. SiteMinder 스키마 파일을 사용하여 로컬 스키마를 확장하기 위해 디렉터리 서버의 관리자가 다음 명령을 실행합니다.

```
ldapmodify -h OVD_Host -p OVD_Port -D cn=Admin -w Admin_Password -v -a -f  
ovd_sm_schema.ldif
```

```
ldapmodify -h OVD_Host -p OVD_Port -D cn=Admin -w Admin_Password -v -a -f  
ovd_xps_schema.ldif
```

```
dsconf reindex -h localhost -p OVD_Port -e "ou=Netegrity,root_database"
```

OVD_Host

OVD 시스템 IP 주소 또는 정규화된 도메인 이름을 지정합니다.

OVD_Port

OVD 인스턴스가 실행되는 포트를 지정합니다.

cn=Admin

스키마를 수정할 권한이 있는 OVD 서버 관리자를 지정합니다.

Admin_Password

서버 관리자 암호를 지정합니다.

기존 정책 저장소에 연결하기 위해 Oracle Virtual Directory 어댑터 생성

기존 정책 저장소에 연결하기 위해 Oracle Virtual Directory LDAP 어댑터를 만들려면 Oracle Directory Services Manager 를 사용하십시오.

다음 단계를 수행하십시오.

1. Oracle Directory Services Manager 에 로그인합니다.
2. 태스크 선택 표시줄에서 "어댑터"를 선택합니다. "Adapter"(어댑터) 탐색 트리가 표시됩니다.
3. "Create Adapter"(어댑터 만들기) 단추를 클릭합니다. "New Adapter Wizard"(어댑터 새로 만들기 마법사)가 표시됩니다.
4. "Type"(유형) 화면에서 다음 값을 지정합니다.

Adapter Type(어댑터 유형)

"LDAP"를 선택하십시오.

Adapter Name(어댑터 이름)

LDAP 어댑터에 대한 고유 이름을 입력하십시오.

Adapter Template(어댑터 템플릿)

기존 정책 저장소의 디렉터리 유형에 해당하는 어댑터 템플릿을 선택하십시오.

5. "Next"(다음)를 클릭합니다.

6. "Connection"(연결) 화면에서 다음 값을 입력합니다(기타 다른 설정에 대해서는 기본값 선택).

Use DNS for Auto Discovery(자동 검색을 위해 DNS 사용)

"No"(아니요)를 선택합니다.

Host(호스트)

원격 호스트의 호스트 이름 또는 IP 주소를 입력하십시오.

Port(포트)

원격 호스트 인스턴스가 실행 중인 포트를 입력하십시오.

Server proxy Bind DN(서버 프록시 바인드 DN)

디렉터리 내용을 수정할 권한이 있는 디렉터리 사용자의 자격 증명을 입력하십시오.

Proxy Password(프록시 암호)

Secure proxy Bind DN(보안 프록시 바인드 DN) 필드에 지정된 사용자의 암호입니다.

7. "Next"(다음)를 클릭합니다.
8. "Connection Test"(연결 테스트) 화면에서 연결 상태가 "OK"인 경우 "Next"(다음)를 클릭합니다. 그렇지 않은 경우 "Back"(뒤로)를 클릭하여 연결 설정 문제를 해결하십시오.
9. "Namespace"(네임스페이스) 화면에서 다음 값을 입력합니다(기타 다른 설정에 대해서는 기본값 선택).

Remote Base:(원격 베이스:)

"Browse"(찾아보기)를 클릭하여 정책 데이터가 저장된 DN 을 찾아 선택하십시오.

Mapped Namespace(매핑된 네임스페이스)

정책 데이터를 매핑할 로컬 DN 을 입력하십시오.

10. 요약 정보를 검토한 다음 "Finish"(마침)를 클릭합니다.

정책 서버를 정책 저장소에 연결

정책 서버가 정책 저장소에 액세스할 수 있도록 정책 서버를 정책 저장소에 연결하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.

중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "데이터" 탭을 클릭합니다.
3. "데이터베이스" 목록에서 다음 값을 선택합니다.

정책 저장소

4. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

5. "LDAP 정책 저장소" 그룹 상자에서 다음 설정을 구성합니다.

- LDAP IP 주소
- 관리자 사용자 이름
- 암호
- 암호 확인
- DN

참고: "도움말"을 클릭하면 필드, 컨트롤 및 해당되는 요구 사항에 대한 설명을 볼 수 있습니다.

6. "적용"을 클릭합니다.
7. "LDAP 연결 테스트"를 클릭하여 정책 서버에서 정책 저장소에 액세스할 수 있는지 여부를 확인합니다.
8. "확인"을 클릭합니다.

SiteMinder 슈퍼 사용자 암호 설정

기본 SiteMinder 관리자 계정의 이름은 다음으로 지정됩니다.

siteminder

이 계정에는 최대 권한이 있습니다.

일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 다음과 같은 경우에 기본 슈퍼 사용자를 사용합니다.

- 관리 UI 에 처음 액세스할 경우
- SiteMinder 유틸리티를 처음 관리할 경우
- 슈퍼 사용자 권한이 있는 다른 관리자를 생성할 경우

다음 단계를 수행하십시오.

1. smreg 유틸리티를 *siteminder_home*\bin 에 복사합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

참고: 이 유틸리티는 정책 서버 설치 키트의 최상위 수준에 있습니다.

2. 다음 명령을 실행합니다.

```
smreg -su password
```

password

기본 SiteMinder 관리자의 암호를 지정합니다.

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: Oracle 정책 저장소를 구성하는 경우 암호의 대/소문자를 구분합니다. 다른 모든 정책 저장소에서는 암호의 대/소문자를 구분하지 않습니다.

3. *siteminder_home*\bin 에서 smreg 를 삭제합니다. smreg 를 삭제하면 이전 암호를 모르는 다른 사람은 암호를 변경할 수 없게 됩니다.

기본 SiteMinder 관리자 계정의 암호가 설정되었습니다.

고급 인증 서버를 사용하도록 설정

정책 서버를 구성하는 과정에서 고급 인증 서버를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 구성 마법사를 시작합니다.
2. 마법사의 첫 번째 화면에서 모든 확인란을 *선택 취소*한 상태로 둡니다.
3. "다음"을 클릭합니다.
4. 고급 인증 서버에 대한 마스터 암호화 키를 생성합니다.

참고: 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

5. 정책 서버 구성 마법사의 나머지 과정을 완료합니다.
고급 인증 서버가 사용되도록 설정되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 `stop-all` 명령 다음에 `start-all` 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

관리 UI 등록 준비

기본 SiteMinder 슈퍼 사용자 계정(siteminder)을 사용하여 관리 UI 에 최초로 로그인합니다. 최초 로그인 시 관리 UI 를 정책 서버에 등록하여 두 구성 요소 간에 트러스트 관계를 생성해야 합니다.

등록을 준비하려면 XPSRegClient 유틸리티를 사용하여 슈퍼 사용자 계정 이름과 암호를 제공합니다. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 트러스트 관계를 설정할 수 있는지 확인합니다.

다음 사항을 고려하십시오.

- 자격 증명을 제공한 때부터 24 시간 이내에 최초 관리 UI 로그인 이루어져야 합니다. 관리 UI 설치를 하루 안에 수행할 계획이 아니면 관리 UI 를 설치하기 전에 다음 단계를 완료하십시오.
- (UNIX) XPSRegClient 를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

기본 SiteMinder 슈퍼 사용자 계정(siteminder)의 암호를 지정합니다.

참고: 암호를 지정하지 않으면 XPSRegClient 에서 암호를 입력하고 확인하라는 메시지가 표시됩니다.

-adminui-setup

관리 UI 가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 관리 UI 를 설치할 때부터 정책 서버에 로그인하고 정책 서버와의 트러스트 관계를 생성할 때까지 할당된 시간을 지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록 요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 15

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI 를 등록할 때 허용되는 시도 실패 횟수를 지정합니다. 관리 UI 에 최초로 로그인할 때 올바르게 않은 SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수 있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을 삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error_path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: stderr

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

XPSRegClient 가 정책 서버에 관리자 자격 증명을 제공합니다. 정책 서버에서는 관리 UI에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

Red Hat Directory Server 를 정책 저장소로 구성

Red Hat Directory Server 는 정책 저장소로 작동할 수 있습니다. 단일 디렉터리 서버 인스턴스가 다음 기능을 수행할 수 있습니다.

- 정책 저장소
- 키 저장소

단일 디렉터리 서버를 사용하면 관리 태스크를 간소화할 수 있습니다. 다음 단원에서는 정책 데이터 및 암호화 키를 저장하도록 단일 디렉터리 서버 인스턴스를 구성하는 방법에 대한 지침을 제공합니다. 구현에 필요할 경우 별도의 키 저장소를 구성할 수 있습니다.

디렉터리 서버 정보 수집

LDAP 디렉터리 서버를 정책 저장소로 구성하거나 기존 정책 저장소를 업그레이드하려면 특정 디렉터리 서버 정보가 필요합니다. 시작하기 전에 다음 정보를 수집하십시오. 정책 저장소 워크시트를 사용하여 값을 기록할 수 있습니다.

호스트 정보

디렉터리 서버의 정규화된 호스트 이름 또는 IP 주소를 지정합니다.

포트 정보

(선택 사항) 비표준 포트를 지정합니다.

기본값: 636(SSL) 및 389(비 SSL)

관리 DN

LDAP 트리에서 정책 저장소 루트 개체 아래의 개체에 대한 생성, 읽기, 수정 및 삭제 권한이 있는 사용자의 LDAP 사용자 이름을 지정합니다.

관리 암호

관리 DN의 암호를 지정합니다.

정책 저장소 루트 DN

LDAP 트리에서 정책 저장소 개체가 정의될 노드의 고유 이름을 지정합니다.

SSL 클라이언트 인증서

SSL 클라이언트 인증서 데이터베이스 파일이 있는 디렉터리의 경로 이름을 지정합니다.

제한: SSL에만 해당

정책 저장소를 구성하는 방법

Red Hat Directory Server 를 정책 저장소로 구성하려면 다음 절차를 완료하십시오.

1. 정책 서버를 정책 저장소에 연결합니다.
2. 정책 저장소 스키마를 생성합니다.
3. SiteMinder 슈퍼 사용자 암호를 설정합니다.
4. 정책 저장소 데이터 정의를 가져옵니다.

5. 기본 정책 저장소 개체를 가져옵니다.
6. 정책 서버를 다시 시작합니다.
7. 관리 UI 등록을 준비합니다.

정책 서버를 정책 저장소에 연결

정책 서버가 정책 저장소에 액세스할 수 있도록 정책 서버를 정책 저장소에 연결하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.

중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "데이터" 탭을 클릭합니다.
3. "데이터베이스" 목록에서 다음 값을 선택합니다.

정책 저장소

4. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

5. "LDAP 정책 저장소" 그룹 상자에서 다음 설정을 구성합니다.

- LDAP IP 주소
- 관리자 사용자 이름
- 암호
- 암호 확인
- 루트 DN

참고: "도움말"을 클릭하면 필드, 컨트롤 및 해당되는 요구 사항에 대한 설명을 볼 수 있습니다.

6. "적용"을 클릭합니다.
7. "LDAP 연결 테스트"를 클릭하여 정책 서버에서 정책 저장소에 액세스할 수 있는지 여부를 확인합니다.
8. "데이터베이스" 목록에서 다음 값을 선택합니다.

키 저장소

9. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

10. 다음 옵션을 선택합니다.

정책 저장소 데이터베이스 사용

11. "확인"을 클릭합니다.

정책 저장소 스키마 만들기

디렉터리 서버가 정책 저장소로 작동하고 SiteMinder 개체를 저장할 수 있도록 정책 저장소 스키마를 생성하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.

2. 다음 명령을 실행합니다.

```
smldapsetup ldgen -fschema_file
```

schema_file

생성하려는 LDIF 파일의 이름을 지정합니다.

정책 저장소 스키마를 사용하여 LDIF 파일이 생성됩니다.

3. 다음 명령을 실행합니다.

```
smldapsetup ldmod -fschema_file
```

schema_file

생성한 LDIF 파일의 이름을 지정합니다.

정책 저장소 스키마를 가져옵니다.

4. 다음 단계를 완료합니다.

- a. 디렉터리 서버를 다시 시작합니다. 정책 저장소 스키마를 올바르게 저장하기 위해 디렉터리 서버를 다시 시작해야 합니다.
- b. 3 단계를 반복합니다. 디렉터리 서버를 다시 시작하면 정책 저장소 루트가 제거됩니다. 정책 저장소 루트를 생성하려면 정책 저장소 스키마를 다시 가져와야 합니다.

5. 다음 명령을 실행합니다.

```
smldapsetup ldmod
-fsiteminder_home/xps/db/RedHat_7_1.ldif
```

-fsiteminder_home

정책 서버 설치 경로를 지정합니다.

정책 저장소 스키마가 XPS 에 대해 확장됩니다.

정책 저장소 스키마가 생성되었습니다.

SiteMinder 슈퍼 사용자 암호 설정

기본 SiteMinder 관리자 계정의 이름은 다음으로 지정됩니다.

siteminder

이 계정에는 최대 권한이 있습니다.

일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다.
다음과 같은 경우에 기본 슈퍼 사용자를 사용합니다.

- 관리 UI 에 처음 액세스할 경우
- SiteMinder 유틸리티를 처음 관리할 경우
- 슈퍼 사용자 권한이 있는 다른 관리자를 생성할 경우

다음 단계를 수행하십시오.

1. smreg 유틸리티를 *siteminder_home*\bin 에 복사합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

참고: 이 유틸리티는 정책 서버 설치 키트의 최상위 수준에 있습니다.

2. 다음 명령을 실행합니다.

```
smreg -su password
```

password

기본 SiteMinder 관리자의 암호를 지정합니다.

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: Oracle 정책 저장소를 구성하는 경우 암호의 대/소문자를 구분합니다. 다른 모든 정책 저장소에서는 암호의 대/소문자를 구분하지 않습니다.

3. *siteminder_home*\bin 에서 *smreg* 를 삭제합니다. *smreg* 를 삭제하면 이전 암호를 모르는 다른 사람은 암호를 변경할 수 없게 됩니다.

기본 SiteMinder 관리자 계정의 암호가 설정되었습니다.

정책 저장소 데이터 정의 가져오기

정책 저장소 데이터 정의 가져오기를 사용하여 정책 저장소에서 생성하고 저장할 수 있는 개체의 유형을 정의합니다.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home*\xps\dd 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

```
XPSDDInstall SmMaster.xdd
```

XPSDDInstall

필수 데이터 정의를 가져옵니다.

기본 정책 저장소 개체 가져오기

기본 정책 저장소 개체 가져오기를 사용하여 관리 UI 및 정책 서버에서 사용할 정책 저장소를 구성합니다.

다음 사항을 고려하십시오.

- *siteminder_home*\bin 에 대한 쓰기 액세스 권한이 있는지 확인하십시오. 가져오기 유틸리티에서 정책 저장소 개체를 가져오려면 이 권한이 필요합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

- Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 `siteminder_home\db` 로 이동합니다.

2. 다음 파일 중 하나를 가져옵니다.

- `smpolicy.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy.xml -npass
```

- `smpolicy-secure.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy-secure.xml -npass
```

npass

암호를 사용할 필요가 없음을 지정합니다. 기본 정책 저장소 개체에 암호화된 데이터가 포함되지 않습니다.

두 파일 모두 기본 정책 저장소 개체를 포함합니다. 이러한 개체는 기본 ACO(에이전트 구성 개체) 템플릿의 기본 보안 설정을 포함합니다. `smpolicy-secure` 파일은 보다 제한적인 보안 설정을 제공합니다. 자세한 내용은 [기본 정책 저장소 개체 고려 사항](#) (페이지 98)을 참조하십시오.

- 옵션 팩 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport ampolicy.xml -npass
```

- 페더레이션 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

정책 저장소 개체를 가져왔습니다.

참고: `smpolicy.xml` 을 가져오면 SiteMinder 에서 별도로 라이선스가 제공되는 레거시 페더레이션 및 웹 서비스 변수 기능을 사용할 수 있게 됩니다. 웹 서비스 변수 기능을 사용하려면 CA 고객 담당자에게 라이선스 정보에 대해 문의하십시오.

고급 인증 서버를 사용하도록 설정

정책 서버를 구성하는 과정에서 고급 인증 서버를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 구성 마법사를 시작합니다.
2. 마법사의 첫 번째 화면에서 모든 확인란을 *선택 취소*한 상태로 둡니다.
3. "다음"을 클릭합니다.
4. 고급 인증 서버에 대한 마스터 암호화 키를 생성합니다.

참고: 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

5. 정책 서버 구성 마법사의 나머지 과정을 완료합니다.
고급 인증 서버가 사용되도록 설정되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 `stop-all` 명령 다음에 `start-all` 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

관리 UI 등록 준비

기본 SiteMinder 슈퍼 사용자 계정(siteminder)을 사용하여 관리 UI 에 최초로 로그인합니다. 최초 로그인 시 관리 UI 를 정책 서버에 등록하여 두 구성 요소 간에 트러스트 관계를 생성해야 합니다.

등록을 준비하려면 XPSRegClient 유틸리티를 사용하여 슈퍼 사용자 계정 이름과 암호를 제공합니다. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 트러스트 관계를 설정할 수 있는지 확인합니다.

다음 사항을 고려하십시오.

- 자격 증명을 제공한 때부터 24 시간 이내에 최초 관리 UI 로그인이 이루어져야 합니다. 관리 UI 설치를 하루 안에 수행할 계획이 아니면 관리 UI 를 설치하기 전에 다음 단계를 완료하십시오.
- (UNIX) XPSRegClient 를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c  
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

기본 SiteMinder 슈퍼 사용자 계정(siteminder)의 암호를 지정합니다.

참고: 암호를 지정하지 않으면 XPSRegClient 에서 암호를 입력하고 확인하라는 메시지가 표시됩니다.

-adminui-setup

관리 UI 가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 관리 UI 를 설치할 때부터 정책 서버에 로그인하고 정책 서버와의 트러스트 관계를 생성할 때까지 할당된 시간을 지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록 요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 15

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI 를 등록할 때 허용되는 시도 실패 횟수를 지정합니다. 관리 UI 에 최초로 로그인할 때 올바르게 않은 SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수 있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을 삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error_path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: stderr

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

XPSRegClient 가 정책 서버에 관리자 자격 증명을 제공합니다. 정책 서버에서는 관리 UI 에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

Siemens DirX 를 정책 저장소로 구성

Siemens DirX 는 정책 저장소로 작동할 수 있습니다. 단일 디렉터리 서버 인스턴스가 다음 기능을 수행할 수 있습니다.

- 정책 저장소
- 키 저장소

단일 디렉터리 서버를 사용하면 관리 태스크를 간소화할 수 있습니다. 다음 단원에서는 정책 데이터 및 암호화 키를 저장하도록 단일 디렉터리 서버 인스턴스를 구성하는 방법에 대한 지침을 제공합니다. 구현에 필요할 경우 별도의 키 저장소를 구성할 수 있습니다.

디렉터리 서버 정보 수집

LDAP 디렉터리 서버를 정책 저장소로 구성하거나 기존 정책 저장소를 업그레이드하려면 특정 디렉터리 서버 정보가 필요합니다. 시작하기 전에 다음 정보를 수집하십시오. 정책 저장소 워크시트를 사용하여 값을 기록할 수 있습니다.

호스트 정보

디렉터리 서버의 정규화된 호스트 이름 또는 IP 주소를 지정합니다.

포트 정보

(선택 사항) 비표준 포트를 지정합니다.

기본값: 636(SSL) 및 389(비 SSL)

관리 DN

LDAP 트리에서 정책 저장소 루트 개체 아래의 개체에 대한 생성, 읽기, 수정 및 삭제 권한이 있는 사용자의 LDAP 사용자 이름을 지정합니다.

관리 암호

관리 DN의 암호를 지정합니다.

정책 저장소 루트 DN

LDAP 트리에서 정책 저장소 개체가 정의될 노드의 고유 이름을 지정합니다.

SSL 클라이언트 인증서

SSL 클라이언트 인증서 데이터베이스 파일이 있는 디렉터리의 경로 이름을 지정합니다.

제한: SSL에만 해당

정책 저장소를 구성하는 방법

Siemens DirX 를 정책 저장소로 구성하려면 다음 절차를 완료하십시오.

1. 정책 저장소 스키마를 생성합니다.
2. 정책 서버를 정책 저장소에 연결합니다.
3. SiteMinder 슈퍼 사용자 암호를 설정합니다.
4. 정책 저장소 데이터 정의를 가져옵니다.

5. 기본 정책 저장소 개체를 가져옵니다.
6. 관리 UI 등록을 준비합니다.

정책 저장소 스키마 만들기

디렉터리 서버가 정책 저장소로 작동하고 **SiteMinder** 개체를 저장할 수 있도록 정책 저장소 스키마를 생성하십시오.

사전 요구 사항

특정 정책 저장소 작업에서는 **SiteMinder** 특성 검색이 필요합니다. **DirX** 디렉터리에서 검색 작업을 수행하기 위해 특성을 인덱싱해야 합니다.

기본적으로 **DirX** 디렉터리는 20 개의 특성을 인덱싱합니다. **SiteMinder** 에는 이 기본 제한보다 많은 특성이 있습니다. **DirX** 디렉터리에서 인덱싱할 수 있는 특성의 수를 최대로 늘립니다. 값을 800 으로 지정하는 것이 좋습니다.

특성 인덱싱 제한을 늘리려면 데이터베이스 프로필을 초기화하는 동안 다음 명령을 사용합니다.

```
dbamboot -Pdatabase_profile_name -aindexing_value
```

예:

```
dbamboot -Pprofile1 -a800
```

스키마 만들기

다음 단계를 수행하십시오.

1. 디렉터리 서버 호스트 시스템에 다음 디렉터리 구조를 생성합니다.

```
DirX_installation\scripts\security\CA\SiteMinder
```

DirX_installation

DirX 설치 경로를 지정합니다.

2. 정책 서버 호스트 시스템에 로그인합니다.
3. `siteminder_home\db\tier2\SiemensDirx` 로 이동하고 다음 파일을 `DirX_installation\scripts\security\CA\SiteMinder` 에 복사합니다.
 - `dirxabbr-ext.SiteMinderrelease`
 - `schema_ext_for_SiteMinderrelease.adm`
 - `bind.tcl`

- l-bind.cp
- GlobalVar.tcl

siteminder_home

정책 서버 설치 경로를 지정합니다.

release

SiteMinder 릴리스를 지정합니다.

4. *siteminder_home\xps\db\Siemens_DirX* 로 이동하고 다음 파일을 *DirX_installation\scripts\security\CA\SiteMinder* 에 복사합니다.
 - dirxabbr-ext.XPS
 - schema_ext_for_XPS.adm
5. 다음 파일의 이름을 바꿉니다.
 - schema_ext_for_SiteMinderrelease.adm 을 schema_ext_for_SiteMinder.adm 으로 바꿉니다.
 - dirxabbr-ext.SiteMinderrelease 를 dirxabbr-ext.SiteMinder 로 바꿉니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

release

SiteMinder 릴리스를 지정합니다.

6. 다음 파일을 *DirX_installation\client\conf* 에 복사합니다.
 - dirxabbr-ext.SiteMinder
 - dirxabbr-ext.XPS
7. DirX 서비스를 다시 시작합니다.
8. *DirX_installation\scripts\security\CA\SiteMinder* 로 이동하고 GlobalVar.tcl 파일을 편집하여 DirX 스크립트에서 참조하는 전역 변수를 업데이트합니다.

기본값:

- LDAP 포트: 389
- 루트 DN: o=My-Company
- 관리자 사용자 이름: cn=admin,o=My-Company
- 관리자 암호: dirx

9. 명령 프롬프트에서 *DirX_installation\scripts\security\CA\SiteMinder* 로 이동하고 다음 명령을 실행합니다.
 - `dirxadm schema_ext_for_siteminder.adm`
 - `dirxadm schema_ext_for_XPS.adm`
10. DirX 서비스를 다시 시작합니다.
11. DirX 가 설치된 시스템에서 `modifyTimestamp` 특성을 인덱싱합니다. 이 태스크를 수동으로 수행하거나 DirX Manager 를 통해 수행합니다.

DirX Manager 를 사용하는 단계는 다음과 같습니다.

 - a. DSA 에 리바인딩합니다.
 - b. 왼쪽 패널에서 "Schema"(스키마)를 클릭합니다
 - c. "Database"(데이터베이스)를 클릭합니다.
 - d. "Hide attributes with no index assigned"(인덱스가 할당되지 않은 특성 숨기기) 확인란의 선택을 취소합니다.
 - e. "편집"을 클릭합니다.
 - f. "Index"(인덱스) 행 아래에서 `modifyTimestamp` 특성을 선택합니다.
 - g. 변경 내용을 저장합니다.
 - h. 데이터베이스를 마우스 오른쪽 단추로 클릭하고 특성 인덱스의 일관성을 검사합니다.
12. DirX 관리 도구를 사용하여 다음 단계를 완료합니다.
 - a. DSA 에 리바인딩합니다.
 - b. 다음 기본 트리 구조를 생성합니다.
 - o=My-Company 아래에 ou=Netegrity 를 생성합니다.
 - ou=Netegrity 아래에 ou=SiteMinder 를 생성합니다.
 - ou=SiteMinder 아래에 ou=PolicySvr4 를 생성합니다.
 - ou=PolicySvr4 아래에 ou=XPS 를 생성합니다.

정책 저장소 스키마가 생성되었습니다.

정책 서버를 정책 저장소에 연결

정책 서버가 정책 저장소에 액세스할 수 있도록 정책 서버를 정책 저장소에 연결하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.

중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "데이터" 탭을 클릭합니다.
3. "데이터베이스" 목록에서 다음 값을 선택합니다.

정책 저장소

4. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

5. "LDAP 정책 저장소" 그룹 상자에서 다음 설정을 구성합니다.

- LDAP IP 주소
- 관리자 사용자 이름
- 암호
- 암호 확인
- 루트 DN

참고: "도움말"을 클릭하면 필드, 컨트롤 및 해당되는 요구 사항에 대한 설명을 볼 수 있습니다.

6. "적용"을 클릭합니다.
7. "LDAP 연결 테스트"를 클릭하여 정책 서버에서 정책 저장소에 액세스할 수 있는지 여부를 확인합니다.
8. "데이터베이스" 목록에서 다음 값을 선택합니다.

키 저장소

9. "저장소" 목록에서 다음 값을 선택합니다.

LDAP

10. 다음 옵션을 선택합니다.

정책 저장소 데이터베이스 사용

11. "확인"을 클릭합니다.

SiteMinder 슈퍼 사용자 암호 설정

기본 SiteMinder 관리자 계정의 이름은 다음으로 지정됩니다.

siteminder

이 계정에는 최대 권한이 있습니다.

일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다.
다음과 같은 경우에 기본 슈퍼 사용자를 사용합니다.

- 관리 UI 에 처음 액세스할 경우
- SiteMinder 유틸리티를 처음 관리할 경우
- 슈퍼 사용자 권한이 있는 다른 관리자를 생성할 경우

다음 단계를 수행하십시오.

1. smreg 유틸리티를 *siteminder_home*\bin 에 복사합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

참고: 이 유틸리티는 정책 서버 설치 키트의 최상위 수준에 있습니다.

2. 다음 명령을 실행합니다.

smreg -su *password*

password

기본 SiteMinder 관리자의 암호를 지정합니다.

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: Oracle 정책 저장소를 구성하는 경우 암호의 대/소문자를 구분합니다. 다른 모든 정책 저장소에서는 암호의 대/소문자를 구분하지 않습니다.

3. *siteminder_home\bin* 에서 **smreg** 를 삭제합니다. **smreg** 를 삭제하면 이전 암호를 모르는 다른 사람은 암호를 변경할 수 없게 됩니다.
기본 SiteMinder 관리자 계정의 암호가 설정되었습니다.

정책 저장소 데이터 정의 가져오기

정책 저장소 데이터 정의 가져오기를 사용하여 정책 저장소에서 생성하고 저장할 수 있는 개체의 유형을 정의합니다.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home\xps\dd* 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

```
XPDDInstall SmMaster.xdd
```

XPDDInstall

필수 데이터 정의를 가져옵니다.

기본 정책 저장소 개체 가져오기

기본 정책 저장소 개체 가져오기를 사용하여 관리 UI 및 정책 서버에서 사용할 정책 저장소를 구성합니다.

다음 사항을 고려하십시오.

- *siteminder_home\bin* 에 대한 쓰기 액세스 권한이 있는지 확인하십시오. 가져오기 유틸리티에서 정책 저장소 개체를 가져오려면 이 권한이 필요합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

- Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 `siteminder_home\db` 로 이동합니다.

2. 다음 파일 중 하나를 가져옵니다.

- `smpolicy.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy.xml -npass
```

- `smpolicy-secure.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy-secure.xml -npass
```

npass

암호를 사용할 필요가 없음을 지정합니다. 기본 정책 저장소 개체에 암호화된 데이터가 포함되지 않습니다.

두 파일 모두 기본 정책 저장소 개체를 포함합니다. 이러한 개체는 기본 ACO(에이전트 구성 개체) 템플릿의 기본 보안 설정을 포함합니다. `smpolicy-secure` 파일은 보다 제한적인 보안 설정을 제공합니다. 자세한 내용은 [기본 정책 저장소 개체 고려 사항](#) (페이지 98)을 참조하십시오.

- 옵션 팩 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport ampolicy.xml -npass
```

- 페더레이션 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

정책 저장소 개체를 가져왔습니다.

참고: `smpolicy.xml` 을 가져오면 SiteMinder 에서 별도로 라이선스가 제공되는 레거시 페더레이션 및 웹 서비스 변수 기능을 사용할 수 있게 됩니다. 웹 서비스 변수 기능을 사용하려면 CA 고객 담당자에게 라이선스 정보에 대해 문의하십시오.

고급 인증 서버를 사용하도록 설정

정책 서버를 구성하는 과정에서 고급 인증 서버를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 구성 마법사를 시작합니다.
2. 마법사의 첫 번째 화면에서 모든 확인란을 **선택 취소**한 상태로 둡니다.
3. "다음"을 클릭합니다.
4. 고급 인증 서버에 대한 마스터 암호화 키를 생성합니다.

참고: 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

5. 정책 서버 구성 마법사의 나머지 과정을 완료합니다.
고급 인증 서버가 사용되도록 설정되었습니다.

관리 UI 등록 준비

기본 SiteMinder 슈퍼 사용자 계정(siteminder)을 사용하여 관리 UI 에 최초로 로그인합니다. 최초 로그인 시 관리 UI 를 정책 서버에 등록하여 두 구성 요소 간에 트러스트 관계를 생성해야 합니다.

등록을 준비하려면 XPSRegClient 유틸리티를 사용하여 슈퍼 사용자 계정 이름과 암호를 제공합니다. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 트러스트 관계를 설정할 수 있는지 확인합니다.

다음 사항을 고려하십시오.

- 자격 증명을 제공한 때부터 **24 시간** 이내에 최초 관리 UI 로그인 이루어져야 합니다. 관리 UI 설치를 하루 안에 수행할 계획이 아니면 관리 UI 를 설치하기 전에 다음 단계를 완료하십시오.
- (UNIX) XPSRegClient 를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c  
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

기본 SiteMinder 슈퍼 사용자 계정(siteminder)의 암호를 지정합니다.

참고: 암호를 지정하지 않으면 XPSRegClient 에서 암호를 입력하고
확인하라는 메시지가 표시됩니다.

-adminui-setup

관리 UI 가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 관리 UI 를 설치할 때부터 정책 서버에 로그인하고 정책
서버와의 트러스트 관계를 생성할 때까지 할당된 시간을
지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록
요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 15

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI 를 등록할 때 허용되는 시도 실패 횟수를
지정합니다. 관리 UI 에 최초로 로그인할 때 올바르게 않은
SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수
있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을
삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error_path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: `stderr`

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

XPSRegClient 가 정책 서버에 관리자 자격 증명을 제공합니다. 정책 서버에서는 관리 UI 에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

별도의 키 저장소 구성

정책 저장소와 키 저장소가 함께 배치되어 있을 경우 별도의 키 저장소를 사용하도록 정책 서버를 구성할 수 있습니다.

별도의 키 저장소로 작동할 디렉터리 서버의 유형에 따라 저장소를 구성하는 방법이 결정됩니다.

- SiteMinder smldapsetup 유틸리티를 사용하여 정책 저장소를 구성할 수 있으면 키 저장소별 스키마를 사용하여 별도의 키 저장소를 구성할 수 있습니다. 다음 디렉터리 서버를 이러한 방식으로 구성할 수 있습니다.
 - Microsoft Active Directory
 - Microsoft AD LDS
 - Oracle Directory Server Enterprise Edition
 - Oracle Internet Directory Server
 - Red Hat Directory Server
- SiteMinder smldapsetup 유틸리티를 사용하여 정책 저장소를 구성할 수 없을 경우에는 다음을 수행해야 합니다.
 - a. 정책 저장소 스키마만 사용하여 별도의 디렉터리 서버 인스턴스를 구성합니다. 정책 저장소 스키마에 키 저장소 스키마가 포함됩니다. 다음을 수행할 필요는 없습니다.
 - SiteMinder 슈퍼 사용자 암호 설정
 - 기본 정책 저장소 개체 가져오기
 - 정책 저장소 데이터 정의 가져오기별도의 키 저장소에는 이러한 개체가 필요하지 않습니다.
 - b. 이 정책 저장소 인스턴스를 키 저장소 전용으로 사용하도록 정책 서버를 구성합니다.

참고: 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

Microsoft Active Directory 를 키 저장소로 구성

Microsoft Active Directory 를 별도의 키 저장소로 구성할 수 있습니다.

키 저장소를 구성하는 방법

키 저장소를 생성하려면 다음 태스크를 완료하십시오.

1. 키 저장소로 작동할 디렉터리 서버 인스턴스를 생성합니다. SiteMinder 키를 저장할 루트 개체와 루트 접미사를 생성해야 합니다.

참고: 자세한 내용은 공급업체별 설명서를 참조하십시오.

2. 스키마 생성 권한과 LDAP 트리에서 키 저장소 루트 개체 아래의 개체에 대한 읽기, 수정 및 삭제 권한이 있는 LDAP 사용자를 생성합니다.

참고: 자세한 내용은 공급업체별 설명서를 참조하십시오.

3. 키 저장소를 등록합니다.
4. 키 저장소 스키마를 생성합니다.
5. 키 저장소 스키마를 가져옵니다.
6. 정책 서버를 다시 시작합니다.

디렉터리 서버 정보 수집

별도의 키 저장소를 구성하기 위해서는 특정 정보가 필요합니다. 다음 정보를 수집하십시오.

호스트

디렉터리 서버 호스트 시스템의 정규화된 이름 또는 IP 주소입니다.

포트

디렉터리 서버 인스턴스가 수신 대기하는 포트입니다. 이 값은 디렉터리 서버 인스턴스가 비표준 포트에서 수신 대기하는 경우에만 필요합니다.

기본값: 636(SSL) 및 389(비 SSL)

관리 DN

다음 권한을 가진 사용자의 LDAP 사용자 이름을 지정합니다.

- 스키마 만들기

참고: 이 권한은 키 저장소 스키마를 가져올 때만 필요합니다. 키 저장소를 배포한 후에는 이 권한이 없는 사용자로 정책 서버를 구성할 수 있습니다.

- 읽기
- 쓰기

- 수정
- 삭제

관리 암호

관리 DN의 암호를 지정합니다.

키 저장소 루트 DN

LDAP 트리에서 키 저장소 개체를 가져와야 하는 노드의 고유 이름을 지정합니다.

SSL 클라이언트 인증서

SSL 클라이언트 인증서 데이터베이스 파일이 있는 디렉터리의 경로 이름을 지정합니다.

제한: SSL에만 해당

키 저장소 등록

키 저장소를 등록하여 키 저장소와 정책 서버 간의 연결을 구성합니다. 정책 서버는 사용자가 키 저장소를 관리하기 위해 제공하는 자격 증명을 사용합니다.

중요! 등록은 별도의 키 저장소를 사용하도록 정책 서버를 구성하지 않습니다. 이 설정은 정책 서버가 다시 시작될 때까지 적용되지 않습니다. 키 저장소가 구성되고 이를 배포할 준비가 될 때까지 정책 서버를 다시 시작하지 마십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 연결을 구성합니다.

```
smlldapsetup reg -hhost -pport -dadmin_user -wadmin_password -rroot -k1
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

참고: 이러한 모드와 인수에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

예:

```
smlldapsetup reg -host172.16.0.0 -p389 -d"cn=directory manager" -wpassword -r"dc=test" -k1
```

3. 정책 서버 관리 콘솔을 시작하고 "데이터" 탭을 엽니다.
4. 다음 절차 중 하나를 완료합니다.
 - 정책 서버가 데이터 관계형 데이터베이스를 사용하도록 구성된 경우:
 - a. "데이터베이스" 목록에서 "키 저장소"를 선택합니다.
 - b. "저장소" 목록에서 LDAP 을 선택하여 연결 설정과 관리 자격 증명을 표시합니다.
 - c. 연결 설정과 관리 사용자 설정이 나타나는지 확인합니다.
 - d. "LDAP 연결 테스트"를 클릭하여 정책 서버가 키 저장소 인스턴스와 통신할 수 있는지 확인합니다.
 - 정책 서버가 디렉터리 서버를 사용하도록 구성된 경우:
 - a. "데이터베이스" 목록에서 "키 저장소"를 선택합니다.
 - b. 연결 설정과 관리 사용자 설정이 나타나는지 확인합니다.
 - c. "LDAP 연결 테스트"를 클릭하여 정책 서버가 키 저장소 인스턴스와 통신할 수 있는지 확인합니다.

참고: "정책 저장소 데이터베이스 사용" 설정은 해제됩니다. 이 설정 해제는 예상되는 정상 동작입니다. 정책 서버는 정책 저장소와 함께 배치된 키 저장소를 계속 사용합니다.

5. 정책 서버 관리 콘솔을 종료합니다.
별도의 키 저장소가 정책 서버에 등록됩니다.

키 저장소 스키마 만들기

키 저장소 인스턴스를 사용하려면 SiteMinder 웹 에이전트 키를 저장하고 검색할 스키마가 필요합니다. `smlldapsetup` 유틸리티를 사용하여 키 저장소 스키마 파일을 생성할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 키 저장소 스키마 파일을 생성합니다.

```
smlldapsetup ldgen -ffile_name -k1
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

참고: 이러한 모드와 인수에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

예: `smlldapsetup ldgen -fkeystoreschema -k1`

키 저장소 스키마 파일이 생성되었습니다.

키 저장소 스키마 가져오기

키 저장소 인스턴스를 사용하려면 SiteMinder 웹 에이전트 키를 저장하고 검색할 스키마가 필요합니다. `smlldapsetup` 유틸리티를 사용하여 키 저장소 스키마 파일을 가져올 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 키 저장소 스키마를 가져옵니다.

```
smlldapsetup ldmod -ffile_name -k1
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

다음 사항을 고려하십시오.

- 이러한 모드 및 인수에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.
- 표준 출력을 통해 가져오는 모든 정책 저장소 스키마가 표시됩니다. 이 동작은 예상된 정상 동작입니다. 이 유틸리티는 키 저장소 관련 스키마만 가져옵니다.

예: `smlldapsetup ldmod -fkeystoreschema -k1`

키 저장소 관련 스키마를 가져왔습니다.

정책 서버를 다시 시작합니다.

정책 서버를 다시 시작할 때까지 정책 서버는 함께 배치된 키 저장소를 계속 사용합니다. 별도의 키 저장소를 사용하기 시작하려면 정책 서버를 다시 시작하십시오.

참고: 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

Microsoft AD LDS 를 키 저장소로 구성

Microsoft AD LDS 를 별도의 키 저장소로 구성할 수 있습니다.

키 저장소를 구성하는 방법

키 저장소를 생성하려면 다음 태스크를 완료하십시오.

1. 키 저장소로 작동할 디렉터리 서버 인스턴스를 생성합니다. SiteMinder 키를 저장할 루트 개체와 루트 접미사를 생성해야 합니다.

참고: 자세한 내용은 공급업체별 설명서를 참조하십시오.

2. 스키마 생성 권한과 LDAP 트리에서 키 저장소 루트 개체 아래의 개체에 대한 읽기, 수정 및 삭제 권한이 있는 LDAP 사용자를 생성합니다.

참고: 자세한 내용은 공급업체별 설명서를 참조하십시오.

3. 디렉터리 서버가 키 저장소 사전 요구 사항을 충족하는지 확인합니다.
4. 키 저장소를 등록합니다.
5. 키 저장소 스키마를 생성합니다.
6. 키 저장소 스키마를 가져옵니다.
7. 정책 서버를 다시 시작합니다.

키 저장소 사전 요구 사항

키 저장소를 구성하기 전에 다음 사전 요구 사항을 충족하는지 확인합니다.

1. 키 저장소 파티션을 생성합니다.
2. 구성 파티션에 사용자를 생성할 수 있는지 확인합니다. 구성 파티션의 관리 사용자만 키 저장소 스키마를 가져올 수 있습니다.

구성 파티션에서 사용자 생성 허용

구성 파티션의 관리 사용자만 키 저장소 스키마를 가져올 수 있습니다. 이 사용자는 구성 파티션은 물론 키 저장소 파티션을 비롯한 모든 응용 프로그램 파티션에 대한 관리 권한을 가져야 합니다.

다음 단계를 수행하십시오.

1. ADSI Edit 콘솔을 엽니다.
2. 구성 파티션의 다음 항목으로 이동합니다.
`cn=directory service, cn=windows nt, cn=services, cn=configuration, cn={guid}`
3. msDS-Other-Settings 특성을 찾습니다.

4. 다음 새 값을 msDS-Other-Settings 특성에 추가합니다.
ADAMAllowADAMSecurityPrincipalsInConfigPartition=1
 5. 구성 및 정책 저장소 응용 프로그램 파티션에서 다음을 수행합니다.
 - a. CN=Administrators, CN=Roles 로 이동합니다.
 - b. CN=Administrators 의 속성을 엽니다.
 - c. 구성원 특성을 편집합니다.
 - d. "DN 추가"를 클릭하고 구성 파티션에 생성한 사용자의 전체 DN 을 붙여 넣습니다.
 - e. 생성한 사용자의 속성으로 이동하고 다음 개체의 값을 확인합니다.
msDS-UserAccountDisabled
값이 false 로 설정되었는지 확인합니다.
- 이 관리 사용자는 구성 파티션은 물론 키 저장소 파티션을 비롯한 모든 응용 프로그램 파티션에 대한 권한을 가집니다.

디렉터리 서버 정보 수집

별도의 키 저장소를 구성하기 위해서는 특정 정보가 필요합니다. 다음 정보를 수집하십시오.

호스트

디렉터리 서버 호스트 시스템의 정규화된 이름 또는 IP 주소입니다.

포트

디렉터리 서버 인스턴스가 수신 대기하는 포트입니다. 이 값은 디렉터리 서버 인스턴스가 비표준 포트에서 수신 대기하는 경우에만 필요합니다.

기본값: 636(SSL) 및 389(비 SSL)

■ 관리자 DN

디렉터리 서버 관리자의 guid 값을 포함한 전체 도메인 이름입니다.

예: CN=user1,CN=People,CN=Configuration,CN,{guid}

이 사용자는 다음 권한이 있어야 합니다.

- 스키마 만들기

참고: 이 권한은 키 저장소 스키마를 가져올 때만 필요합니다. 키 저장소를 배포한 후에는 이 권한이 없는 사용자로 정책 서버를 구성할 수 있습니다.

- 읽기
- 쓰기
- 수정
- 삭제

관리자 암호

디렉터리 서버 관리자의 암호입니다.

응용 프로그램 파티션의 루트 DN

키 저장소 스키마를 가져와야 하는 응용 프로그램 파티션의 루트 DN 위치입니다.

(선택 사항) SSL 클라이언트 인증서

디렉터리 연결이 SSL 을 통해 이루어진 경우 SSL 클라이언트 인증서 데이터베이스가 있는 디렉터리의 경로입니다.

키 저장소 등록

키 저장소를 등록하여 키 저장소와 정책 서버 간의 연결을 구성합니다. 정책 서버는 사용자가 키 저장소를 관리하기 위해 제공하는 자격 증명을 사용합니다.

중요! 등록은 별도의 키 저장소를 사용하도록 정책 서버를 구성하지 않습니다. 이 설정은 정책 서버가 다시 시작될 때까지 적용되지 않습니다. 키 저장소가 구성되고 이를 배포할 준비가 될 때까지 정책 서버를 다시 시작하지 마십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 연결을 구성합니다.

```
smlldapsetup reg -hhost -pport -dadmin_user -wadmin_password -rroot -k1
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

참고: 이러한 모드와 인수에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

예:

```
smlldapsetup reg -host172.16.0.0 -p389 -d"cn=directory manager" -wpassword -r"dc=test" -k1
```

3. 정책 서버 관리 콘솔을 시작하고 "데이터" 탭을 엽니다.
4. 다음 절차 중 하나를 완료합니다.
 - 정책 서버가 데이터 관계형 데이터베이스를 사용하도록 구성된 경우:
 - a. "데이터베이스" 목록에서 "키 저장소"를 선택합니다.
 - b. "저장소" 목록에서 LDAP 을 선택하여 연결 설정과 관리 자격 증명을 표시합니다.
 - c. 연결 설정과 관리 사용자 설정이 나타나는지 확인합니다.
 - d. "LDAP 연결 테스트"를 클릭하여 정책 서버가 키 저장소 인스턴스와 통신할 수 있는지 확인합니다.
 - 정책 서버가 디렉터리 서버를 사용하도록 구성된 경우:
 - a. "데이터베이스" 목록에서 "키 저장소"를 선택합니다.
 - b. 연결 설정과 관리 사용자 설정이 나타나는지 확인합니다.
 - c. "LDAP 연결 테스트"를 클릭하여 정책 서버가 키 저장소 인스턴스와 통신할 수 있는지 확인합니다.

참고: "정책 저장소 데이터베이스 사용" 설정은 해제됩니다. 이 설정 해제는 예상되는 정상 동작입니다. 정책 서버는 정책 저장소와 함께 배치된 키 저장소를 계속 사용합니다.

5. 정책 서버 관리 콘솔을 종료합니다.
별도의 키 저장소가 정책 서버에 등록됩니다.

키 저장소 스키마 만들기

키 저장소 인스턴스를 사용하려면 SiteMinder 웹 에이전트 키를 저장하고 검색할 스키마가 필요합니다. `smlldapsetup` 유틸리티를 사용하여 키 저장소 스키마 파일을 생성할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 키 저장소 스키마 파일을 생성합니다.

```
smlldapsetup ldgen -ffile_name -k1
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

참고: 이러한 모드와 인수에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

예: `smlldapsetup ldgen -fkeystoreschema -k1`

키 저장소 스키마 파일이 생성되었습니다.

키 저장소 스키마 가져오기

키 저장소 인스턴스를 사용하려면 SiteMinder 웹 에이전트 키를 저장하고 검색할 스키마가 필요합니다. `smlldapsetup` 유틸리티를 사용하여 키 저장소 스키마 파일을 가져올 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 키 저장소 스키마를 가져옵니다.

```
smlldapsetup ldmod -ffile_name -k1
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

다음 사항을 고려하십시오.

- 이러한 모드 및 인수에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.
- 표준 출력을 통해 가져오는 모든 정책 저장소 스키마가 표시됩니다. 이 동작은 예상된 정상 동작입니다. 이 유틸리티는 키 저장소 관련 스키마만 가져옵니다.

예: `smlldapsetup ldmod -fkeystoreschema -k1`

키 저장소 관련 스키마를 가져왔습니다.

정책 서버를 다시 시작합니다.

정책 서버를 다시 시작할 때까지 정책 서버는 함께 배치된 키 저장소를 계속 사용합니다. 별도의 키 저장소를 사용하기 시작하려면 정책 서버를 다시 시작하십시오.

참고: 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

Oracle Directory Server Enterprise Edition 을 키 저장소로 구성

Oracle Directory Server Enterprise Edition 을 별도의 키 저장소로 구성할 수 있습니다.

키 저장소를 구성하는 방법

키 저장소를 생성하려면 다음 태스크를 완료하십시오.

1. 키 저장소로 작동할 디렉터리 서버 인스턴스를 생성합니다. SiteMinder 키를 저장할 루트 개체와 루트 접미사를 생성해야 합니다.

참고: 자세한 내용은 공급업체별 설명서를 참조하십시오.

2. 스키마 생성 권한과 LDAP 트리에서 키 저장소 루트 개체 아래의 개체에 대한 읽기, 수정 및 삭제 권한이 있는 LDAP 사용자를 생성합니다.

참고: 자세한 내용은 공급업체별 설명서를 참조하십시오.

3. 키 저장소 고려 사항을 검토합니다.
4. 디렉터리 서버 정보를 수집합니다.
5. 키 저장소를 등록합니다.
6. 키 저장소 스키마를 생성합니다.
7. 키 저장소 스키마를 가져옵니다.
8. 정책 서버를 다시 시작합니다.

키 저장소 고려 사항

smldapsetup 유틸리티는 ou=Netegrity, root 하위 접미사 및 PolicySvr4 데이터베이스를 생성합니다.

root

키 저장소를 등록할 때 지정하는 디렉터리 루트입니다. 이 변수는 기존의 루트 접미사 또는 하위 접미사여야 합니다.

예: 루트 접미사가 dc=netegrity,dc=com 일 경우 smldapsetup 을 실행하면 디렉터리 서버에 다음 항목이 생성됩니다.

- 루트 접미사, dc=netegrity,dc=com 과 해당 userRoot 데이터베이스
- 하위 접미사, ou=Netegrity,dc=netegrity,dc=com 과 해당 PolicySvr4 데이터베이스

키 저장소를 ou=apps,dc=netegrity,dc=com 아래에 배치하려는 경우 ou=apps,dc=netegrity,dc=com 이 루트 접미사이거나 루트 접미사 dc=netegrity,dc=com 의 하위 접미사여야 합니다.

하위 접미사일 경우 `smldapsetup` 을 실행하면 다음 항목이 생성됩니다.

- 루트 접미사, `dc=netegrity,dc=com` 과 해당 `userRoot` 데이터베이스
- 하위 접미사, `ou=apps,dc=netegrity,dc=com` 과 해당 `Apps` 데이터베이스
- 하위 접미사, `ou=Netegrity,ou=apps,dc=netegrity,dc=com` 과 해당 `PolicySvr4` 데이터베이스

참고: 루트 접미사 및 하위 접미사에 대한 자세한 내용은 공급업체별 설명서를 참조하십시오.

디렉터리 서버 정보 수집

별도의 키 저장소를 구성하기 위해서는 특정 정보가 필요합니다. 다음 정보를 수집하십시오.

호스트

디렉터리 서버 호스트 시스템의 정규화된 이름 또는 IP 주소입니다.

포트

디렉터리 서버 인스턴스가 수신 대기하는 포트입니다. 이 값은 디렉터리 서버 인스턴스가 비표준 포트에서 수신 대기하는 경우에만 필요합니다.

기본값: 636(SSL) 및 389(비 SSL)

관리 DN

다음 권한을 가진 사용자의 LDAP 사용자 이름을 지정합니다.

- 스키마 만들기

참고: 이 권한은 키 저장소 스키마를 가져올 때만 필요합니다. 키 저장소를 배포한 후에는 이 권한이 없는 사용자로 정책 서버를 구성할 수 있습니다.

- 읽기
- 쓰기
- 수정
- 삭제

관리 암호

관리 DN의 암호를 지정합니다.

키 저장소 루트 DN

LDAP 트리에서 키 저장소 개체를 가져와야 하는 노드의 고유 이름을 지정합니다.

SSL 클라이언트 인증서

SSL 클라이언트 인증서 데이터베이스 파일이 있는 디렉터리의 경로 이름을 지정합니다.

제한: SSL에만 해당

키 저장소 등록

키 저장소를 등록하여 키 저장소와 정책 서버 간의 연결을 구성합니다. 정책 서버는 사용자가 키 저장소를 관리하기 위해 제공하는 자격 증명을 사용합니다.

중요! 등록은 별도의 키 저장소를 사용하도록 정책 서버를 구성하지 않습니다. 이 설정은 정책 서버가 다시 시작될 때까지 적용되지 않습니다. 키 저장소가 구성되고 이를 배포할 준비가 될 때까지 정책 서버를 다시 시작하지 마십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 연결을 구성합니다.

```
smldapsetup reg -hhost -pport -dadmin_user -wadmin_password -rroot -k1
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

참고: 이러한 모드와 인수에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

예:

```
smldapsetup reg -host172.16.0.0 -p389 -d"cn=directory manager" -wpassword -r"dc=test" -k1
```

3. 정책 서버 관리 콘솔을 시작하고 "데이터" 탭을 엽니다.
 4. 다음 절차 중 하나를 완료합니다.
 - 정책 서버가 데이터 관계형 데이터베이스를 사용하도록 구성된 경우:
 - a. "데이터베이스" 목록에서 "키 저장소"를 선택합니다.
 - b. "저장소" 목록에서 LDAP 을 선택하여 연결 설정과 관리 자격 증명을 표시합니다.
 - c. 연결 설정과 관리 사용자 설정이 나타나는지 확인합니다.
 - d. "LDAP 연결 테스트"를 클릭하여 정책 서버가 키 저장소 인스턴스와 통신할 수 있는지 확인합니다.
 - 정책 서버가 디렉터리 서버를 사용하도록 구성된 경우:
 - a. "데이터베이스" 목록에서 "키 저장소"를 선택합니다.
 - b. 연결 설정과 관리 사용자 설정이 나타나는지 확인합니다.
 - c. "LDAP 연결 테스트"를 클릭하여 정책 서버가 키 저장소 인스턴스와 통신할 수 있는지 확인합니다.
- 참고:** "정책 저장소 데이터베이스 사용" 설정은 해제됩니다. 이 설정 해제는 예상되는 정상 동작입니다. 정책 서버는 정책 저장소와 함께 배치된 키 저장소를 계속 사용합니다.
5. 정책 서버 관리 콘솔을 종료합니다.
- 별도의 키 저장소가 정책 서버에 등록됩니다.

키 저장소 스키마 만들기

키 저장소 인스턴스를 사용하려면 SiteMinder 웹 에이전트 키를 저장하고 검색할 스키마가 필요합니다. `smldapsetup` 유틸리티를 사용하여 키 저장소 스키마 파일을 생성할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 키 저장소 스키마 파일을 생성합니다.

```
smldapsetup ldgen -ffile_name -k1
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

참고: 이러한 모드와 인수에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

예: `smldapsetup ldgen -fkeystoreschema -k1`

키 저장소 스키마 파일이 생성되었습니다.

키 저장소 스키마 가져오기

키 저장소 인스턴스를 사용하려면 SiteMinder 웹 에이전트 키를 저장하고 검색할 스키마가 필요합니다. `smldapsetup` 유틸리티를 사용하여 키 저장소 스키마 파일을 가져올 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 키 저장소 스키마를 가져옵니다.

```
smldapsetup ldmod -ffile_name -k1
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

다음 사항을 고려하십시오.

- 이러한 모드 및 인수에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.
- 표준 출력을 통해 가져오는 모든 정책 저장소 스키마가 표시됩니다. 이 동작은 예상된 정상 동작입니다. 이 유틸리티는 키 저장소 관련 스키마만 가져옵니다.

예: `smldapsetup ldmod -fkeystoreschema -k1`

키 저장소 관련 스키마를 가져왔습니다.

정책 서버를 다시 시작합니다.

정책 서버를 다시 시작할 때까지 정책 서버는 함께 배치된 키 저장소를 계속 사용합니다. 별도의 키 저장소를 사용하기 시작하려면 정책 서버를 다시 시작하십시오.

참고: 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

Oracle Directory Server 키 저장소 복제

SiteMinder 는 UserRoot 및 PolicySvr4 데이터베이스를 생성합니다. 접미사 매핑은 PolicySvr4 데이터베이스를 가리킵니다. 키 저장소를 복제하려면 PolicySvr4 데이터베이스 디렉터리에 대한 복제 계약을 설정해야 합니다.

다음 단계를 수행하십시오.

1. 공급업체별 설명서에 설명된 대로 복제 계약을 구성합니다.
2. 정책 서버 호스트 시스템에 로그인합니다.
3. 다음 명령을 실행하여 SiteMinder 인덱스를 생성합니다.

```
smldapsetup ldgen -x -findexes.ldif
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

4. 복제본 서버에서 인덱스를 설정합니다.

```
smldapsetup ldmod -x -findexes.ldif -hhost -preplicaport  
-dAdminDN -wAdminPW
```

host

복제본 호스트를 지정합니다.

replicaport

복제본 포트 번호를 지정합니다.

AdminDN

복제본 관리자 DN 을 지정합니다.

예: cn=directory manager

AdminPW

복제본 관리자 암호를 지정합니다.

SiteMinder 인덱스가 복제되었습니다.

Oracle Internet Directory Server 를 키 저장소로 구성

Oracle Internet Directory Server 를 별도의 키 저장소로 구성할 수 있습니다.

키 저장소를 구성하는 방법

키 저장소를 생성하려면 다음 태스크를 완료하십시오.

1. 키 저장소로 작동할 디렉터리 서버 인스턴스를 생성합니다. SiteMinder 키를 저장할 루트 개체와 루트 접미사를 생성해야 합니다.

참고: 자세한 내용은 공급업체별 설명서를 참조하십시오.

2. 스키마 생성 권한과 LDAP 트리에서 키 저장소 루트 개체 아래의 개체에 대한 읽기, 수정 및 삭제 권한이 있는 LDAP 사용자를 생성합니다.

참고: 자세한 내용은 공급업체별 설명서를 참조하십시오.

3. 키 저장소를 등록합니다.
4. 키 저장소 스키마를 생성합니다.
5. 키 저장소 스키마를 가져옵니다.
6. 정책 서버를 다시 시작합니다.

디렉터리 서버 정보 수집

별도의 키 저장소를 구성하기 위해서는 특정 정보가 필요합니다. 다음 정보를 수집하십시오.

호스트

디렉터리 서버 호스트 시스템의 정규화된 이름 또는 IP 주소입니다.

포트

디렉터리 서버 인스턴스가 수신 대기하는 포트입니다. 이 값은 디렉터리 서버 인스턴스가 비표준 포트에서 수신 대기하는 경우에만 필요합니다.

기본값: 636(SSL) 및 389(비 SSL)

관리 DN

다음 권한을 가진 사용자의 LDAP 사용자 이름을 지정합니다.

- 스키마 만들기

참고: 이 권한은 키 저장소 스키마를 가져올 때만 필요합니다. 키 저장소를 배포한 후에는 이 권한이 없는 사용자로 정책 서버를 구성할 수 있습니다.

- 읽기
- 쓰기
- 수정
- 삭제

관리 암호

관리 DN의 암호를 지정합니다.

키 저장소 루트 DN

LDAP 트리에서 키 저장소 개체를 가져와야 하는 노드의 고유 이름을 지정합니다.

SSL 클라이언트 인증서

SSL 클라이언트 인증서 데이터베이스 파일이 있는 디렉터리의 경로 이름을 지정합니다.

제한: SSL에만 해당

키 저장소 등록

키 저장소를 등록하여 키 저장소와 정책 서버 간의 연결을 구성합니다. 정책 서버는 사용자가 키 저장소를 관리하기 위해 제공하는 자격 증명을 사용합니다.

중요! 등록은 별도의 키 저장소를 사용하도록 정책 서버를 구성하지 않습니다. 이 설정은 정책 서버가 다시 시작될 때까지 적용되지 않습니다. 키 저장소가 구성되고 이를 배포할 준비가 될 때까지 정책 서버를 다시 시작하지 마십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 연결을 구성합니다.

```
smlldapsetup reg -hhost -pport -dadmin_user -wadmin_password -rroot -k1
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

참고: 이러한 모드와 인수에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

예:

```
smlldapsetup reg -host172.16.0.0 -p389 -d"cn=directory manager" -wpassword -r"dc=test" -k1
```

3. 정책 서버 관리 콘솔을 시작하고 "데이터" 탭을 엽니다.
4. 다음 절차 중 하나를 완료합니다.
 - 정책 서버가 데이터 관계형 데이터베이스를 사용하도록 구성된 경우:
 - a. "데이터베이스" 목록에서 "키 저장소"를 선택합니다.
 - b. "저장소" 목록에서 LDAP 을 선택하여 연결 설정과 관리 자격 증명을 표시합니다.
 - c. 연결 설정과 관리 사용자 설정이 나타나는지 확인합니다.
 - d. "LDAP 연결 테스트"를 클릭하여 정책 서버가 키 저장소 인스턴스와 통신할 수 있는지 확인합니다.

- 정책 서버가 디렉터리 서버를 사용하도록 구성된 경우:
 - a. "데이터베이스" 목록에서 "키 저장소"를 선택합니다.
 - b. 연결 설정과 관리 사용자 설정이 나타나는지 확인합니다.
 - c. "LDAP 연결 테스트"를 클릭하여 정책 서버가 키 저장소 인스턴스와 통신할 수 있는지 확인합니다.

참고: "정책 저장소 데이터베이스 사용" 설정은 해제됩니다. 이 설정 해제는 예상되는 정상 동작입니다. 정책 서버는 정책 저장소와 함께 배치된 키 저장소를 계속 사용합니다.

5. 정책 서버 관리 콘솔을 종료합니다.
별도의 키 저장소가 정책 서버에 등록됩니다.

키 저장소 스키마 만들기

키 저장소 인스턴스를 사용하려면 SiteMinder 웹 에이전트 키를 저장하고 검색할 스키마가 필요합니다. `smlldapsetup` 유틸리티를 사용하여 키 저장소 스키마 파일을 생성할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 키 저장소 스키마 파일을 생성합니다.

```
smlldapsetup ldgen -ffile_name -k1
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

참고: 이러한 모드와 인수에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

예: `smlldapsetup ldgen -fkeystoreschema -k1`

키 저장소 스키마 파일이 생성되었습니다.

키 저장소 스키마 가져오기

키 저장소 인스턴스를 사용하려면 SiteMinder 웹 에이전트 키를 저장하고 검색할 스키마가 필요합니다. `smlldapsetup` 유틸리티를 사용하여 키 저장소 스키마 파일을 가져올 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 키 저장소 스키마를 가져옵니다.

```
smlldapsetup ldmod -ffile_name -k1
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

다음 사항을 고려하십시오.

- 이러한 모드 및 인수에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.
- 표준 출력을 통해 가져오는 모든 정책 저장소 스키마가 표시됩니다. 이 동작은 예상된 정상 동작입니다. 이 유틸리티는 키 저장소 관련 스키마만 가져옵니다.

예: `smlldapsetup ldmod -fkeystoreschema -k1`

키 저장소 관련 스키마를 가져왔습니다.

정책 서버를 다시 시작합니다.

정책 서버를 다시 시작할 때까지 정책 서버는 함께 배치된 키 저장소를 계속 사용합니다. 별도의 키 저장소를 사용하기 시작하려면 정책 서버를 다시 시작하십시오.

참고: 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

Red Hat Directory Server 를 키 저장소로 구성

Red Hat Directory Server 를 별도의 키 저장소로 구성할 수 있습니다.

키 저장소를 구성하는 방법

키 저장소를 생성하려면 다음 태스크를 완료하십시오.

1. 키 저장소로 작동할 디렉터리 서버 인스턴스를 생성합니다. SiteMinder 키를 저장할 루트 개체와 루트 접미사를 생성해야 합니다.

참고: 자세한 내용은 공급업체별 설명서를 참조하십시오.

2. 스키마 생성 권한과 LDAP 트리에서 키 저장소 루트 개체 아래의 개체에 대한 읽기, 수정 및 삭제 권한이 있는 LDAP 사용자를 생성합니다.

참고: 자세한 내용은 공급업체별 설명서를 참조하십시오.

3. 키 저장소를 등록합니다.
4. 키 저장소 스키마를 생성합니다.
5. 키 저장소 스키마를 가져옵니다.
6. 정책 서버를 다시 시작합니다.

키 저장소 등록

키 저장소를 등록하여 키 저장소와 정책 서버 간의 연결을 구성합니다. 정책 서버는 사용자가 키 저장소를 관리하기 위해 제공하는 자격 증명을 사용합니다.

중요! 등록은 별도의 키 저장소를 사용하도록 정책 서버를 구성하지 않습니다. 이 설정은 정책 서버가 다시 시작될 때까지 적용되지 않습니다. 키 저장소가 구성되고 이를 배포할 준비가 될 때까지 정책 서버를 다시 시작하지 마십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 연결을 구성합니다.

```
smlldapsetup reg -hhost -pport -dadmin_user -wadmin_password -rroot -k1
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

참고: 이러한 모드와 인수에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

예:

```
smlldapsetup reg -host172.16.0.0 -p389 -d"cn=directory manager" -wpassword -r"dc=test" -k1
```

3. 정책 서버 관리 콘솔을 시작하고 "데이터" 탭을 엽니다.
4. 다음 절차 중 하나를 완료합니다.
 - 정책 서버가 데이터 관계형 데이터베이스를 사용하도록 구성된 경우:
 - a. "데이터베이스" 목록에서 "키 저장소"를 선택합니다.
 - b. "저장소" 목록에서 LDAP 을 선택하여 연결 설정과 관리 자격 증명을 표시합니다.
 - c. 연결 설정과 관리 사용자 설정이 나타나는지 확인합니다.
 - d. "LDAP 연결 테스트"를 클릭하여 정책 서버가 키 저장소 인스턴스와 통신할 수 있는지 확인합니다.
 - 정책 서버가 디렉터리 서버를 사용하도록 구성된 경우:
 - a. "데이터베이스" 목록에서 "키 저장소"를 선택합니다.
 - b. 연결 설정과 관리 사용자 설정이 나타나는지 확인합니다.
 - c. "LDAP 연결 테스트"를 클릭하여 정책 서버가 키 저장소 인스턴스와 통신할 수 있는지 확인합니다.

참고: "정책 저장소 데이터베이스 사용" 설정은 해제됩니다. 이 설정 해제는 예상되는 정상 동작입니다. 정책 서버는 정책 저장소와 함께 배치된 키 저장소를 계속 사용합니다.

5. 정책 서버 관리 콘솔을 종료합니다.
별도의 키 저장소가 정책 서버에 등록됩니다.

키 저장소 스키마 만들기

키 저장소 인스턴스를 사용하려면 SiteMinder 웹 에이전트 키를 저장하고 검색할 스키마가 필요합니다. `smlldapsetup` 유틸리티를 사용하여 키 저장소 스키마 파일을 생성할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 키 저장소 스키마 파일을 생성합니다.

```
smlldapsetup ldgen -ffile_name -k1
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

참고: 이러한 모드와 인수에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

예: `smlldapsetup ldgen -fkeystoreschema -k1`

키 저장소 스키마 파일이 생성되었습니다.

키 저장소 스키마 가져오기

키 저장소 인스턴스를 사용하려면 SiteMinder 웹 에이전트 키를 저장하고 검색할 스키마가 필요합니다. `smlldapsetup` 유틸리티를 사용하여 키 저장소 스키마 파일을 가져올 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 키 저장소 스키마를 가져옵니다.

```
smlldapsetup ldmod -ffile_name -k1
```

참고:

- 이러한 모드 및 인수에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.
- 표준 출력을 통해 가져오는 모든 정책 저장소 스키마가 표시됩니다. 이 동작은 예상된 정상 동작입니다. 이 유틸리티는 키 저장소 관련 스키마만 가져옵니다. 이 유틸리티는 키 저장소 관련 스키마만 가져옵니다.

예:

```
smldapsetup ldmod -fkeystoreschema -k1
```

키 저장소 관련 스키마를 가져왔습니다.

3. 다음 단계를 완료합니다.

- a. 디렉터리 서버를 다시 시작합니다. 키 저장소 스키마를 올바르게 저장하기 위해서는 디렉터리 서버를 다시 시작해야 합니다.
- b. 2 단계를 반복합니다. 디렉터리 서버를 다시 시작하면 키 저장소 루트가 제거됩니다. 키 저장소 루트를 생성하려면 키 저장소 스키마를 다시 가져와야 합니다.

키 저장소 관련 스키마를 가져왔습니다.

정책 서버를 다시 시작합니다.

정책 서버를 다시 시작할 때까지 정책 서버는 함께 배치된 키 저장소를 계속 사용합니다. 별도의 키 저장소를 사용하기 시작하려면 정책 서버를 다시 시작하십시오.

참고: 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

제 7 장: 관계형 데이터베이스에 SiteMinder 데이터 저장소 구성

이 섹션은 다음 항목을 포함하고 있습니다.

[관계형 데이터베이스를 정책 또는 키 저장소로 사용](#) (페이지 302)

[설치 로드맵](#) (페이지 302)

[중요 고려 사항](#) (페이지 304)

[기본 정책 저장소 개체 고려 사항](#) (페이지 304)

[관계형 데이터베이스의 스키마 파일](#) (페이지 305)

[MySQL 정책 저장소 구성](#) (페이지 310)

[SQL Server 정책 저장소 구성](#) (페이지 326)

[PostgreSQL 서버 정책 저장소를 구성하는 방법](#) (페이지 344)

[Oracle 정책 저장소 구성](#) (페이지 359)

[IBM DB2 정책 저장소 구성](#) (페이지 385)

[IBM DB2 에서 세션 정보를 저장하는 방법](#) (페이지 400)

[MySQL 에 세션 정보를 저장하는 방법](#) (페이지 402)

[Oracle 에서 세션 정보를 저장하는 방법](#) (페이지 405)

[SQL Server 에서 세션 정보를 저장하는 방법](#) (페이지 408)

[PostgreSQL 에 세션 정보를 저장하는 방법](#) (페이지 410)

[IBM DB2 에서 감사 로그를 저장하는 방법](#) (페이지 412)

[MySQL 에서 감사 로그를 저장하는 방법](#) (페이지 415)

[Oracle 에서 감사 로그를 저장하는 방법](#) (페이지 418)

[SQL Server 에서 감사 로그를 저장하는 방법](#) (페이지 421)

[PostgreSQL 에서 감사 로그를 저장하는 방법](#) (페이지 423)

[IBM DB2 에서 키 정보를 저장하는 방법](#) (페이지 426)

[MySQL 에서 키 정보를 저장하는 방법](#) (페이지 429)

[Oracle 에서 키 정보를 저장하는 방법](#) (페이지 431)

[SQL Server 에서 키 정보를 저장하는 방법](#) (페이지 434)

[PostgreSQL 에서 키 정보를 저장하는 방법](#) (페이지 436)

[샘플 사용자 디렉터리](#) (페이지 439)

관계형 데이터베이스를 정책 또는 키 저장소로 사용

SiteMinder 정책 저장소는 모든 정책 관련 정보를 저장하는 리포지토리입니다. SiteMinder 설치 환경의 모든 정책 서버는 정책 저장소 데이터를 직접적으로 또는 복제를 통해 공유해야 합니다. SiteMinder 는 관리자가 정책 저장소 데이터를 한 저장소에서 다른 저장소로 이동할 수 있는 도구와 함께 설치됩니다.

정책 서버를 설치할 때 다음 관계형 데이터베이스 중 하나를 정책 저장소로 자동 구성할 수 있습니다.

- Microsoft SQL Server
- Oracle RDBMS

또는, 정책 서버를 설치한 후에는 정책 저장소를 수동으로 구성할 수 있습니다. 정책 서버를 설치한 후에는 정책 서버 관리 콘솔을 사용하여 정책 서버를 기존 정책 저장소에 연결할 수도 있습니다.

참고: 지원되는 CA 및 타사 구성 요소의 목록에 대해서는 기술 지원 사이트의 **SiteMinder 12.52 SP1 Platform Support Matrix**(플랫폼 지원표)를 참조하십시오.

정책 저장소 지원 외에도 관계형 데이터베이스를 사용하여 SiteMinder 키, 감사 로그 및 세션 데이터를 저장할 수 있습니다.

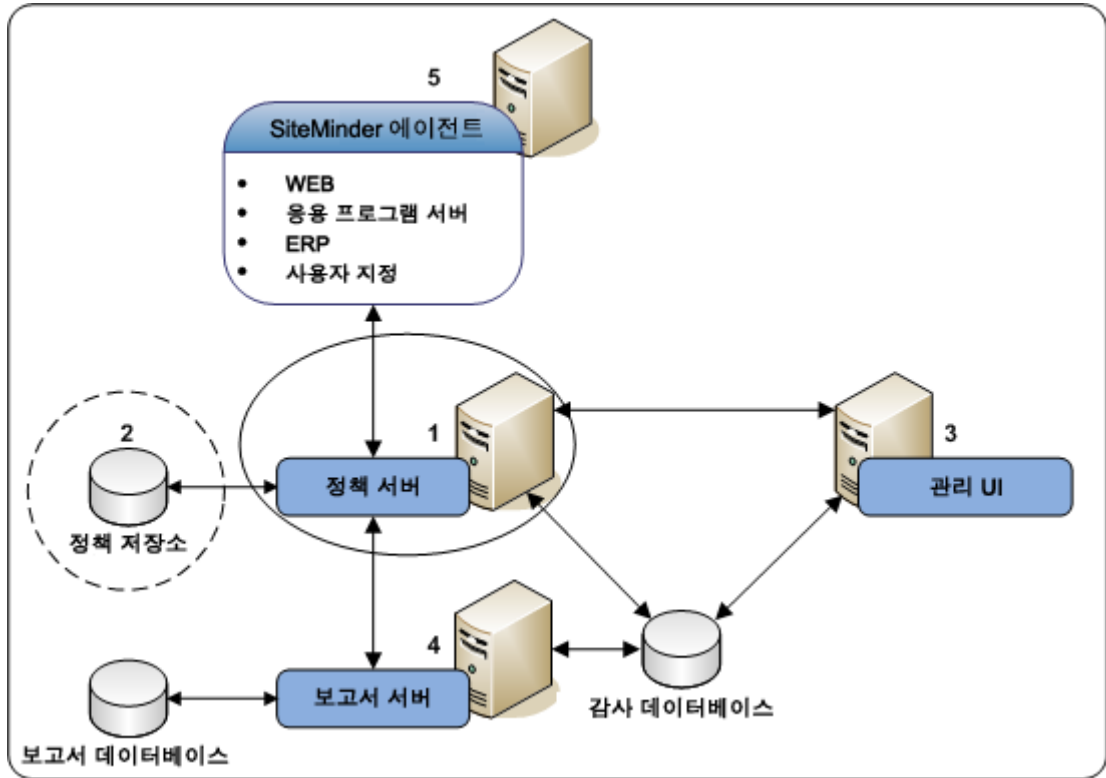
설치 로드맵

다음 다이어그램에서는 샘플 SiteMinder 설치를 보여 주고 각 구성 요소를 설치 및 구성하는 순서를 나열합니다.

- 실선으로 둘러싸인 부분은 정책 서버입니다. 이 정책 서버는 정책 저장소를 구성하기 전에 필요합니다. 정책 서버가 환경에 포함되어 있지 않은 경우 계속하기 전에 설치해야 합니다.
- 점선으로 둘러싸인 부분은 정책 저장소입니다. 지금 이 구성 요소를 구성합니다.

다음 그림은 단일 정책/키 저장소 인스턴스를 보여 줍니다. 그림에는 표시되지 않았지만 환경에서 각 정책 및 키 저장소에 별도의 인스턴스를 사용할 수 있습니다.

수식2: 설치 로드맵



중요 고려 사항

정책 저장소를 구성하기 전에 다음 문제를 고려하십시오.

- 가능한 정책 저장소 손상을 방지하십시오. 정책 저장소를 호스트할 데이터베이스 서버가 개체를 UTF-8 형식으로 저장하도록 구성되어 있는지 확인하십시오.
 - (Oracle) 데이터베이스가 개체를 UTF-8 형식으로 저장하도록 구성되어 있는지 확인하십시오. 대부분의 Oracle 문자 집합에서 유니코드가 지원됩니다.
 - (SQL Server) 데이터베이스가 기본 데이터 정렬(SQL_Latin1_General_CP1_CI_AS)을 사용하여 구성되어 있는지 확인하십시오. 대/소문자를 구분하는 데이터 정렬을 사용할 경우 예기치 않은 동작이 발생할 수 있습니다.
- IPv6 ODBC 데이터 원본을 사용할 때 IP 주소를 대괄호로 묶으면 연결에 실패하므로 대괄호를 사용하지 마십시오.
예: [fec0::9255:20c:29ff:fe47:8089] 대신 fec0::9255:20c:29ff:fe47:8089 를 사용하십시오.

기본 정책 저장소 개체 고려 사항

정책 저장소를 구성할 때 다음 기본 정책 저장소 개체 파일을 사용할 수 있습니다.

- smpolicy.xml
- smpolicy-secure.xml

두 파일 모두에 정책 저장소에 필요한 기본 개체가 포함되어 있습니다.

- 정책 서버 구성 마법사를 사용하여 정책 저장소를 자동으로 구성하는 경우 마법사는 smpolicy.xml 만 사용합니다.
- smpolicy-secure.xml 을 사용하려면 정책 저장소를 수동으로 구성해야 합니다.

두 파일 모두에서 기본 보안 설정을 제공합니다. 이러한 설정은 관리 UI 에서 제공하는 기본 ACO(에이전트 구성 개체) 템플릿에서 사용할 수 있습니다. smpolicy-secure 파일은 보다 제한적인 기본 보안 설정을 제공합니다. smpolicy.xml 을 선택해도 보다 제한적인 기본 보안 설정을 사용할 수 있습니다. 관리 UI 를 사용하면 기본 ACO 설정을 수정할 수 있습니다.

다음 표에는 두 파일의 보안 설정이 요약되어 있습니다.

매개 변수 이름	smpolicy 값	smpolicy-secure 값
BadCssChars	값이 없음	<, >, ', ;,), (, &, +, %00
BadQueryChars	값이 없음	<, >, ', ;,), (, &, +, %00
BadUrlChars	//, ./, /., /*, *, ~, \, %00-%1f, %7f-%ff, %25	smpolicy.smdif 값과 다음 값: <, >, ', ;,), (, &, +
EnableCookieProvider	예	아니요
IgnoreExt	.class, .gif, .jpg, .jpeg, .png, .fcc, .scc, .sfcc, .ccc, .ntc	모든 smpolicy 값
LimitCookieProvider	아니요	예
ValidTargetDomain	이 파일에는 이 매개 변수가 없습니다.	이 매개 변수에는 기본값이 없습니다. 올바른 리디렉션 도메인을 제공하십시오. 예: validtargetdomain=".example.com"

관계형 데이터베이스의 스키마 파일

SiteMinder 는 다음과 같은 SiteMinder 데이터 저장소를 구성하는 데 필요한 스키마 파일을 제공합니다.

- 정책 저장소
- 키 저장소
- 로깅 데이터베이스

- 세션 저장소
- 샘플 사용자 데이터베이스

참고: SiteMinder 스키마 파일은 정책 서버와 함께 설치됩니다. UNIX 시스템에서 *siteminder_home/db/SQL* 디렉터리의 스키마 파일을 데이터베이스가 있는 Windows 시스템의 임시 디렉터리(C:\temp)로 복사하십시오.

siteminder_home

정책 서버 설치 경로를 지정합니다.

IBM DB2 스키마 파일

다음 SQL Server 스키마 파일은 *siteminder_home\db\tier2\DB2* 디렉터리에서 제공됩니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

sm_db2_ps.sql

정책 저장소 및 키 저장소에 대한 스키마를 생성합니다.

참고: 여러 데이터베이스에 키를 저장하는 경우 이 스키마 파일은 키 저장소 데이터에 대한 스키마를 생성합니다.

sm_db2_logs.sql

감사 로그에 대한 스키마를 생성합니다. 감사 저장소를 만들려면 사용하기 전에 [이 스크립트를 편집](#) (페이지 413)하십시오.

sm_db2_ss.sql

세션 저장소에 대한 스키마를 생성합니다.

smsampleusers_db2.sql

샘플 사용자 데이터베이스에 대한 스키마를 생성하고 데이터베이스를 샘플 사용자로 채웁니다.

다음 IBM DB2 스키마 파일은 *siteminder_home\xps\db* 디렉터리에서 제공됩니다.

DB2.sql

정책 저장소에 대한 XPS 스키마를 생성합니다.

MySQL 스키마 파일

다음 SQL Server 스키마 파일은 *siteminder_home\db\tier2\MySQL* 디렉터리에서 제공됩니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

sm_mysql_ps.sql

정책 저장소 및 키 저장소에 대한 스키마를 생성합니다.

참고: 여러 데이터베이스에 키를 저장하는 경우 이 스키마 파일은 키 저장소 데이터에 대한 스키마를 생성합니다.

sm_mysql_logs.sql

감사 로그에 대한 스키마를 생성합니다.

sm_mysql_ss.sql

세션 저장소에 대한 스키마를 생성합니다.

smsampleusers_mysql.sql

샘플 사용자 데이터베이스에 대한 스키마를 생성하고 데이터베이스를 샘플 사용자로 채웁니다.

다음 MySQL 스키마 파일은 *siteminder_home\xps\db* 디렉터리에 있습니다.

MySQL.sql

정책 저장소에 대한 XPS 스키마를 생성합니다.

SQL Server 스키마 파일

다음 SQL Server 스키마 파일은 *siteminder_home*\db\SQL 디렉터리에서 제공됩니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

sm_mssql_ps.sql

정책 저장소 및 키 저장소에 대한 스키마를 생성합니다.

참고: 여러 데이터베이스에 키를 저장하는 경우 이 스키마 파일은 키 저장소 데이터에 대한 스키마를 생성합니다.

sm_mssql_logs.sql

감사 로그에 대한 스키마를 생성합니다.

sm_mssql_ss.sql

세션 저장소에 대한 스키마를 생성합니다.

참고: 유니코드 문자를 세션 저장소에 저장할 계획이 없다면 이 파일을 사용하지시오.

sm_mssql_ss.sql.unicode

SiteMinder 세션 저장소에 대한 스키마를 생성합니다.

참고: 유니코드 문자를 세션 저장소에 저장할 계획이라면 이 파일을 사용하지시오.

smsampleusers_sqlserver.sql

SiteMinder 샘플 사용자 데이터베이스에 대한 스키마를 생성하고 데이터베이스를 샘플 사용자로 채웁니다.

다음 SQL Server 스키마 파일은 *siteminder_home*\xps\db 에서 제공됩니다.

SQLServer.sql

정책 저장소에 대한 XPS 스키마를 생성합니다.

PostgreSQL Server 스키마 파일

다음 PostgreSQL 스키마 파일은 *siteminder_home\db*PostgreSQL 디렉터리에서 제공됩니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

sm_postgresql_ps.sql

정책 저장소 및 키 저장소에 대한 스키마를 생성합니다.

참고: 여러 데이터베이스에 키를 저장하는 경우 이 스키마 파일은 키 저장소 데이터에 대한 스키마를 생성합니다.

sm_postgresql_logs.sql

감사 로그에 대한 스키마를 생성합니다.

sm_postgresql_ss.sql

세션 저장소에 대한 스키마를 생성합니다.

참고: 유니코드 문자를 세션 저장소에 저장할 계획이 없다면 이 파일을 사용하지시오.

smsampleusers_postgresql.sql

SiteMinder 샘플 사용자 데이터베이스에 대한 스키마를 생성하고 데이터베이스를 샘플 사용자로 채웁니다.

다음 PostgreSQL 서버 스키마 파일은 *siteminder_home\xps\db* 에서 제공됩니다.

PostgreSQL.sql

정책 저장소에 대한 XPS 스키마를 생성합니다.

Oracle 스키마 파일

다음 Oracle 스키마 파일은 *siteminder_home\db\SQL* 디렉터리에 있습니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

sm_oracle_ps.sql

정책 저장소 및 키 저장소에 대한 스키마를 생성합니다.

참고: 여러 데이터베이스에 키를 저장하는 경우 이 스키마 파일은 키 저장소 데이터에 대한 스키마를 생성합니다.

sm_oracle_logs.sql

감사 로그에 대한 스키마를 생성합니다.

sm_oracle_ss.sql

세션 저장소에 대한 스키마를 생성합니다.

smsampleusers_oracle.sql

샘플 사용자 데이터베이스에 대한 스키마를 생성하고 데이터베이스를 샘플 사용자로 채웁니다.

다음 Oracle 스키마 파일은 *policy_server_home\xps\db* 디렉터리에서 제공됩니다.

Oracle.sql

정책 저장소에 대한 XPS 스키마를 생성합니다.

MySQL 정책 저장소 구성

MySQL 정책 저장소는 다음 기능도 수행할 수 있습니다.

- 키 저장소
- 감사 로깅 데이터베이스

참고: 세션 정보는 별도의 데이터베이스에 저장됩니다. 정책 저장소를 사용하여 세션 정보를 저장하지 마십시오.

단일 데이터베이스를 사용하면 관리 태스크를 간소화할 수 있습니다. 다음 단원에서는 단일 데이터베이스 서버를 구성하는 방법에 대한 지침을 제공합니다.

데이터베이스 정보 수집

정책 저장소나 다른 유형의 SiteMinder 데이터 저장소를 구성하기 전에 다음 정보를 수집하십시오.

- **데이터베이스 호스트** - 데이터베이스 호스트 시스템의 이름을 식별합니다.
- **데이터베이스 이름** - 정책 저장소 또는 데이터 저장소로 사용할 데이터베이스 인스턴스의 이름을 식별합니다.
- **데이터베이스 포트** - 데이터베이스가 수신 대기하는 포트를 식별합니다.
- **관리자 계정** - 데이터베이스의 개체에 대한 관리 권한이 있는 관리자 계정의 로그인 ID 를 식별합니다.
- **관리자 암호** - 관리자 계정의 암호를 식별합니다.

정책 저장소를 구성하는 방법

정책 서버 설정을 시작하기 전에 필수 데이터베이스 정보를 수집했는지 확인하십시오.

다음 단계를 수행하십시오.

1. MySQL 이 Latin1 또는 UTF8 문자 집합을 사용하는지 확인합니다.
유니코드 문자를 지원하려면 UTF8 문자 집합을 사용하십시오.
2. 정책 서버 호스트 시스템에서 정책 저장소 역할을 하는 MySQL 데이터베이스에 액세스할 수 있는지 확인합니다.
3. 공급업체별 사용자 인터페이스를 사용하여 데이터 저장소에 대한 데이터베이스 인스턴스를 생성합니다.
 - 유니코드 문자에 대한 데이터베이스 인스턴스를 생성하려면 UTF8 문자 집합 및 데이터 정렬을 사용합니다.
 - 유니코드를 지원하지 않는 문자에 대한 데이터베이스 인스턴스를 생성하려면 Latin1 문자 집합 및 데이터 정렬을 사용합니다.
4. SiteMinder 스키마를 생성합니다.
5. SiteMinder 에 대한 MySQL 데이터 원본을 구성합니다.
 - (Windows) MySQL 데이터 원본을 생성합니다.
 - (UNIX) UNIX 시스템에서 MySQL 데이터 원본을 생성합니다.
 - (UNIX) MySQL 유선 프로토콜 드라이버를 구성합니다.

6. 정책 서버를 데이터베이스에 연결합니다.
7. SiteMinder 슈퍼 사용자 암호를 설정합니다.
8. 정책 저장소 데이터 정의를 가져옵니다.
9. 기본 정책 저장소 개체를 가져옵니다.
10. 정책 서버를 다시 시작합니다.
11. 관리 UI 등록을 준비합니다.

SiteMinder 스키마 만들기

MySQL 데이터베이스에 정책, 키 및 감사 로깅 정보를 저장할 수 있도록 SiteMinder 스키마를 생성하십시오.

다음 단계를 수행하십시오.

1. 쿼리 브라우저를 시작하고 정책 서버 데이터베이스를 관리하는 사용자로 로그인합니다.
2. 데이터베이스 목록에서 데이터베이스 인스턴스를 선택합니다.
3. 다음 위치로 이동합니다.

siteminder_home\db\tier2\MySQL

siteminder_home

정책 서버 설치 경로를 지정합니다.

4. 텍스트 편집기에서 다음 파일 중 *하나*를 엽니다.
 - 정책 저장소에 유니코드 문자를 저장하려면 *sm_mysql_ps.sql.unicode* 를 엽니다.
 - 정책 저장소에 유니코드를 지원하지 않는 문자를 저장하려면 *sm_mysql_ps.sql* 을 엽니다.
5. *sm_mysql_ps* 파일에서 다음 줄을 찾습니다.

```
DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$  
CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
```
6. 'databaseName'의 각 인스턴스를 정책 저장소로 작동하는 데이터베이스의 이름으로 바꿉니다.
7. *databaseName* 인스턴스를 바꾼 후 전체 파일의 내용을 복사합니다.
8. 파일 내용을 쿼리에 붙여 넣고 쿼리를 실행합니다.
정책 및 키 저장소 스키마가 데이터베이스에 추가됩니다.

9. 다음 위치로 이동합니다.

`siteminder_home\mps\db\Tier2DirSupport\MySQL`

10. 텍스트 편집기에서 다음 파일 중 *하나*를 열고 전체 파일의 내용을 복사합니다.

- 정책 저장소에 유니코드 문자를 저장하려면 `MySQL.sql.unicode` 를 엽니다.
- 정책 저장소에 유니코드를 지원하지 않는 문자를 저장하려면 `MySQL.sql` 을 엽니다.

11. 해당 MySQL 파일의 스키마를 쿼리에 붙여 넣고 쿼리를 실행합니다.

정책 저장소 스키마가 확장됩니다.

12. 정책 저장소를 감사 로깅 데이터베이스로 사용하려면 다음 로깅 스키마 파일을 사용하여 3 단계와 4 단계를 반복합니다.

`sm_mysql_logs.sql`

데이터베이스에서 SiteMinder 데이터를 저장할 수 있습니다.

참고: 추가 SiteMinder 데이터를 저장하기 위해 정책 저장소를 구성할 필요는 없습니다. 각각의 데이터베이스를 별도의 감사 로그 데이터베이스, 키 저장소 및 세션 저장소로 작동하도록 구성할 수 있습니다.

SiteMinder 에 대한 MySQL 데이터 원본 구성

정책 서버가 SiteMinder 데이터 저장소와 통신할 수 있도록 하려면 데이터 원본을 구성해야 합니다.

참고: MySQL 5.1.x 를 사용하는 경우 DSN 을 생성하는 데 사용된 사용자 이름에 TRIGGER 권한을 할당하십시오.

Windows 에서 MySQL 데이터 원본 만들기

MySQL 유선 프로토콜 드라이버에 대한 MySQL 데이터 원본을 생성합니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 단계 중 하나를 수행합니다.
 - 지원되는 32 비트 Windows 운영 체제를 사용 중인 경우 "시작"을 클릭하고 "프로그램", "관리 도구", "ODBC 데이터 원본"을 차례로 선택합니다.
 - 지원되는 64 비트 Windows 운영 체제를 사용 중인 경우 다음을 수행합니다.
 - a. `install_home\Windows\SysWOW64` 로 이동합니다.
 - b. `odbcad32.exe` 를 두 번 클릭합니다."ODBC 데이터 원본 관리자"가 표시됩니다.
3. "시스템 DSN"을 클릭합니다.
4. "추가"를 클릭합니다.
5. 아래로 스크롤하여 "SiteMinder MySQL Wire Protocol"을 선택하고 "마침"을 클릭합니다.
6. "일반" 탭에서 다음 단계를 완료합니다.
 - a. "데이터 원본 이름" 필드에 데이터 원본 이름을 입력합니다.

예:

`SiteMinder MySQL 유선 데이터 원본`
 - b. "호스트 이름" 필드에 MySQL 데이터베이스 호스트 시스템의 이름을 입력합니다.
 - c. "포트 번호" 필드에 MySQL 데이터베이스가 수신 대기하는 포트를 입력합니다.
 - d. "데이터베이스 이름" 필드에 MySQL 데이터베이스의 이름을 입력합니다.

7. "연결 테스트"를 클릭합니다.

8. "확인"을 클릭합니다.

데이터 원본이 생성되고 "시스템 데이터 원본" 목록에 표시됩니다.

참고: 이제 정책 서버를 SiteMinder 데이터 저장소에 연결할 수 있습니다.

UNIX 시스템에서 MySQL 데이터 원본 만들기

SiteMinder ODBC 데이터 원본은 `system_odbc.ini` 파일을 사용하여 구성합니다. 이 파일은 `mysqlwire.ini` 를 `system_odbc.ini` 로 이름을 바꿔 생성할 수 있습니다. `mysqlwire.ini` 파일은 `siteminder_home/db` 에 있습니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

이 `system_odbc.ini` 파일에는 사용할 수 있는 ODBC 데이터 원본의 이름과 이러한 데이터 원본에 연결된 특성이 모두 들어 있습니다. 각 사이트에 맞게 이 파일을 사용자 지정해야 합니다. SiteMinder 에 대한 다른 ODBC 사용자 디렉터리를 정의하는 등 이 파일에 데이터 원본을 더 추가할 수도 있습니다.

`system_odbc.ini` 파일의 첫 번째 섹션인 [ODBC Data Sources]에는 현재 사용할 수 있는 모든 데이터 원본의 목록이 들어 있습니다. "=" 앞의 이름은 해당 파일에서 각 개별 데이터 원본을 설명하는 이후 섹션을 나타냅니다. "=" 뒷부분은 주석 필드입니다.

참고: 데이터 원본 항목의 첫 번째 줄의 값은 정책 저장소로 데이터베이스를 구성할 때 필요합니다.

`system_odbc.ini` 파일에는 각 데이터 원본의 특성을 설명하는 섹션이 있습니다. 첫 번째 특성은 SiteMinder 가 해당 데이터 원본을 사용할 때 로드되는 ODBC 드라이버입니다. 나머지 특성은 드라이버마다 다릅니다.

MySQL Server 데이터 원본의 추가는 다음을 포함합니다.

- 파일의 [ODBC Data Sources] 섹션에 새 데이터 원본 이름
- 데이터 원본과 동일한 이름을 사용하여 데이터 원본을 설명하는 섹션

새 서비스 이름을 만들 때 `system_odbc.ini` 파일을 업데이트하십시오. [SiteMinder Data Source] 아래에 MySQL 드라이버에 대한 항목이 있습니다.

또한 MySQL Server 데이터 원본을 구성하려면 `mysqlwire.ini` 를 `system_odbc.ini` 로 이름을 바꿔 `system_odbc.ini` 파일을 생성하십시오.

MySQL 유선 프로토콜 드라이버 만들기

유선 프로토콜 드라이버를 구성하여 SiteMinder 가 데이터베이스에 연결하는 데 사용할 설정을 지정할 수 있습니다.

참고: 이 절차는 정책 서버가 UNIX 시스템에 설치된 경우에만 적용됩니다. 아직 수행하지 않은 경우 아래의 파일 중 하나를 복사하고 이름을 `system_odbc.ini` 로 바꾸십시오. 이름을 바꾸는 파일은 SiteMinder 데이터 저장소로 구성하는 데이터베이스 공급업체에 따라 다릅니다.

- `sqlserverwire.ini`
- `oraclewire.ini`
- `mysqlwire.ini`
- `postgresqlwire.ini`

이러한 파일은 `siteminder_home/db` 에 있습니다.

`system_odbc.ini` 파일은 다음 섹션으로 구성되어 있습니다. 구성하는 데이터 원본에 따라 편집할 섹션이 결정됩니다.

[SiteMinder Data Source]

SiteMinder 가 정책 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SiteMinder Logs Data Source]

SiteMinder 가 감사 로그 데이터베이스로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SiteMinder Keys Data Source]

SiteMinder 가 키 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SiteMinder Session Data Source]

SiteMinder 가 세션 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SmSampleUsers Data Source]

SiteMinder 가 샘플 사용자 데이터 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

다음 단계를 수행하십시오.

1. system_odbc.ini 파일을 엽니다.
2. [ODBC Data Sources] 아래에 다음 행을 입력합니다.

```
SiteMinder Data Source=DataDirect 7.1 MySQL Wire Protocol
```

3. 구성하려는 데이터 원본에 따라 다음 정보를 사용하여 하나 이상의 데이터 원본 섹션을 편집합니다.

```
Driver=nete_ps_root/odbc/lib/NSmysql27.so
Description=DataDirect 7.1 MySQL Wire Protocol
Database=database_name
HostName=host_name
LogonID=root_user
Password=root_user_password
PortNumber=mysql_port
```

참고: 데이터 원본 정보를 편집할 때 파운드 기호(#)는 사용하지 마십시오. 파운드 기호를 입력하면 정보가 주석으로 처리되어 값이 잘립니다. 값이 잘리면 ODBC 연결이 실패할 수 있습니다.

nete_ps_root

정책 서버 설치 경로를 지정합니다. 이 값은 환경 변수를 포함하지 않는 명시적 경로로 입력합니다.

예: /export/smuser/siteminder

database_name

SiteMinder 데이터 저장소로 사용할 MySQL 데이터베이스의 이름을 지정합니다.

host_name

MySQL 데이터베이스 호스트 시스템의 이름을 지정합니다.

root_user

MySQL 루트 사용자의 로그인 ID 를 지정합니다.

root_user_password

MySQL 루트 사용자의 암호를 지정합니다.

mysql_port

MySQL 데이터베이스가 수신 대기하는 포트를 지정합니다.

4. 파일을 저장합니다.

유선 프로토콜 드라이버가 구성되었습니다.

정책 서버를 데이터베이스에 연결

정책 서버가 정책 저장소의 **SiteMinder** 데이터에 액세스할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.
2. "저장소" 목록에서 다음 값을 선택합니다.
ODBC
3. "데이터베이스" 목록에서 다음 값을 선택합니다.
정책 저장소
4. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.
 - (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
 - (UNIX) 입력하는 이름은 `system_odbc.ini` 파일의 데이터 원본 항목 첫 줄과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 `[SiteMinder Data Sources]`입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.
5. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.
6. SiteMinder 에 할당되는 최대 데이터베이스 연결 수를 지정합니다.
참고: 최상의 성능을 위해서는 기본 연결 수인 25 를 유지하는 것이 좋습니다.
7. "적용"을 클릭하여 설정을 저장합니다.
8. "데이터베이스" 목록에서 다음 값을 선택합니다.
키 저장소
9. "저장소" 목록에서 다음 값을 선택합니다.
ODBC
10. 다음 옵션을 선택합니다.
정책 저장소 데이터베이스 사용
11. "데이터베이스" 목록에서 다음 값을 선택합니다.
감사 로그

12. "저장소" 목록에서 다음 값을 선택합니다.

ODBC

13. 다음 옵션을 선택합니다.

정책 저장소 데이터베이스 사용

14. "적용"을 클릭하여 설정을 저장합니다.

15. (선택 사항) "연결 테스트"를 클릭하여 정책 서버가 정책 저장소에 액세스할 수 있는지 확인합니다.

16. "확인"을 클릭합니다.

데이터베이스를 정책 저장소, 키 저장소 및 로깅 데이터베이스로 사용하도록 정책 서버가 구성되었습니다.

SiteMinder 슈퍼 사용자 암호 설정

기본 SiteMinder 관리자 계정의 이름은 다음으로 지정됩니다.

siteminder

이 계정에는 최대 권한이 있습니다.

일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 다음과 같은 경우에 기본 슈퍼 사용자를 사용합니다.

- 관리 UI에 처음 액세스할 경우
- SiteMinder 유틸리티를 처음 관리할 경우
- 슈퍼 사용자 권한이 있는 다른 관리자를 생성할 경우

다음 단계를 수행하십시오.

1. smreg 유틸리티를 *siteminder_home*\bin에 복사합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

참고: 이 유틸리티는 정책 서버 설치 키트의 최상위 수준에 있습니다.

2. 다음 명령을 실행합니다.

smreg -su *password*

password

기본 SiteMinder 관리자의 암호를 지정합니다.

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: Oracle 정책 저장소를 구성하는 경우 암호의 대/소문자를 구분합니다. 다른 모든 정책 저장소에서는 암호의 대/소문자를 구분하지 않습니다.

3. *siteminder_home*\bin 에서 *smreg* 를 삭제합니다. *smreg* 를 삭제하면 이전 암호를 모르는 다른 사람은 암호를 변경할 수 없게 됩니다.

기본 SiteMinder 관리자 계정의 암호가 설정되었습니다.

정책 저장소 데이터 정의 가져오기

정책 저장소 데이터 정의 가져오기를 사용하여 정책 저장소에서 생성하고 저장할 수 있는 개체의 유형을 정의합니다.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home*\xps\dd 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

`XPSPDDInstall SmMaster.xdd`

XPSPDDInstall

필수 데이터 정의를 가져옵니다.

기본 정책 저장소 개체 가져오기

기본 정책 저장소 개체 가져오기를 사용하여 관리 UI 및 정책 서버에서 사용할 정책 저장소를 구성합니다.

다음 사항을 고려하십시오.

- `siteminder_home\bin`에 대한 쓰기 액세스 권한이 있는지 확인하십시오. 가져오기 유틸리티에서 정책 저장소 개체를 가져오려면 이 권한이 필요합니다.

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

- Windows Server 2008에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 `siteminder_home\db` 로 이동합니다.

2. 다음 파일 중 하나를 가져옵니다.

- `smpolicy.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy.xml -npass
```

- `smpolicy-secure.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy-secure.xml -npass
```

npass

암호를 사용할 필요가 없음을 지정합니다. 기본 정책 저장소 개체에 암호화된 데이터가 포함되지 않습니다.

두 파일 모두 기본 정책 저장소 개체를 포함합니다. 이러한 개체는 기본 ACO(에이전트 구성 개체) 템플릿의 기본 보안 설정을 포함합니다. `smpolicy-secure` 파일은 보다 제한적인 보안 설정을 제공합니다. 자세한 내용은 [기본 정책 저장소 개체 고려 사항](#) (페이지 98)을 참조하십시오.

- 옵션 팩 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport ampolicy.xml -npass
```

- 페더레이션 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

정책 저장소 개체를 가져왔습니다.

참고: `smpolicy.xml` 을 가져오면 SiteMinder 에서 별도로 라이선스가 제공되는 레거시 페더레이션 및 웹 서비스 변수 기능을 사용할 수 있게 됩니다. 웹 서비스 변수 기능을 사용하려면 CA 고객 담당자에게 라이선스 정보에 대해 문의하십시오.

고급 인증 서버를 사용하도록 설정

정책 서버를 구성하는 과정에서 고급 인증 서버를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 구성 마법사를 시작합니다.
2. 마법사의 첫 번째 화면에서 모든 확인란을 **선택 취소**한 상태로 둡니다.
3. "다음"을 클릭합니다.
4. 고급 인증 서버에 대한 마스터 암호화 키를 생성합니다.

참고: 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

5. 정책 서버 구성 마법사의 나머지 과정을 완료합니다.
고급 인증 서버가 사용되도록 설정되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 **stop-all** 명령 다음에 **start-all** 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

관리 UI 등록 준비

기본 SiteMinder 슈퍼 사용자 계정(siteminder)을 사용하여 관리 UI에 최초로 로그인합니다. 최초 로그인 시 관리 UI를 정책 서버에 등록하여 두 구성 요소 간에 트러스트 관계를 생성해야 합니다.

등록을 준비하려면 XPSRegClient 유틸리티를 사용하여 슈퍼 사용자 계정 이름과 암호를 제공합니다. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 트러스트 관계를 설정할 수 있는지 확인합니다.

다음 사항을 고려하십시오.

- 자격 증명을 제공한 때부터 24 시간 이내에 최초 관리 UI 로그인이 이루어져야 합니다. 관리 UI 설치를 하루 안에 수행할 계획이 아니면 관리 UI를 설치하기 전에 다음 단계를 완료하십시오.
- (UNIX) XPSRegClient를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c  
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

기본 SiteMinder 슈퍼 사용자 계정(siteminder)의 암호를 지정합니다.

참고: 암호를 지정하지 않으면 XPSRegClient에서 암호를 입력하고 확인하라는 메시지가 표시됩니다.

-adminui-setup

관리 UI가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 관리 UI 를 설치할 때부터 정책 서버에 로그인하고 정책 서버와의 트러스트 관계를 생성할 때까지 할당된 시간을 지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록 요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 15

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI 를 등록할 때 허용되는 시도 실패 횟수를 지정합니다. 관리 UI 에 최초로 로그인할 때 올바르게 않은 SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수 있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을 삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error_path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: stderr

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

XPSRegClient 가 정책 서버에 관리자 자격 증명을 제공합니다. 정책 서버에서는 관리 UI에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

SQL Server 정책 저장소 구성

단일 SQL Server 데이터베이스가 다음 기능을 수행할 수 있습니다.

- 정책 저장소
- 키 저장소
- 로깅 데이터베이스

참고: SiteMinder 세션 정보를 별도의 데이터베이스에 저장하십시오. 정책 저장소를 사용하여 세션 정보를 저장하지 마십시오.

단일 데이터베이스를 사용하면 관리 태스크를 간소화할 수 있습니다. 다음 단원에서는 SiteMinder 데이터를 저장할 단일 데이터베이스 서버를 구성하는 방법에 대한 지침을 제공합니다.

다음 사항을 고려하십시오.

- SQL Server 정책 저장소를 수동으로 구성하거나, 정책 서버 설치 관리자를 사용하여 정책 저장소를 자동으로 구성할 수 있습니다.
- 데이터베이스는 Windows 시스템에 설치되어야 합니다. 또한 SiteMinder 스키마 파일은 정책 서버와 함께 설치됩니다. 정책 서버가 UNIX 시스템에 설치되어 있으면 *policy_server_home/db/SQL* 디렉터리에서 Windows 시스템의 임시 디렉터리로 스키마 파일을 복사합니다.

데이터베이스 정보 수집

정책 저장소나 다른 유형의 SiteMinder 데이터 저장소로 사용할 단일 SQL Server 데이터베이스를 구성하려면 특정 데이터베이스 정보가 필요합니다.

참고: 정보 앞에 (W)가 있으면 정책 서버가 Windows 시스템에 설치된 경우에만 해당 정보가 필요하다는 것을 나타내고, (U)가 있으면 정책 서버가 UNIX 시스템에 설치된 경우에만 해당 정보가 필요하다는 것을 나타냅니다. SQL Server 데이터 원본을 구성할 때는 다른 정보가 필요합니다.

정책 저장소나 다른 유형의 SiteMinder 데이터 저장소를 구성하기 전에 다음 정보를 수집하십시오. SQL Server 정보 워크시트를 사용하여 값을 기록할 수도 있습니다.

데이터베이스 인스턴스 이름

정책 저장소 또는 데이터 저장소로 기능하는 데이터베이스 인스턴스의 이름을 결정합니다.

관리 계정 이름 및 암호

데이터베이스의 개체에 대한 생성, 읽기, 수정 및 삭제 권한이 있는 계정의 사용자 이름 및 암호를 결정합니다.

(W) 데이터 원본 이름

데이터 원본을 식별하는 데 사용할 이름을 결정합니다.

예: SM SQL Server Wire DS

(W) SQL 서버 이름

정책 저장소로 기능하는 인스턴스가 포함된 SQL 서버 데이터베이스의 이름을 결정합니다.

(U) 정책 서버 루트

정책 서버가 설치된 명시적 경로를 결정합니다.

(U) IP 주소

SQL Server 데이터베이스의 IP 주소를 결정합니다.

정책 저장소를 구성하는 방법

SQL Server 데이터베이스를 정책 저장소로 구성하려면 다음 절차를 완료하십시오.

참고: 시작하기 전에 필수 데이터베이스 정보를 수집했는지 확인하십시오. 아래 단계 중 일부에서 이 정보가 필요합니다.

1. SiteMinder 데이터를 포함하는 SQL Server 데이터베이스 인스턴스를 정책 서버 시스템에서 액세스할 수 있는지 확인합니다.
2. SQL Server Enterprise Manager 를 사용하여 SiteMinder 데이터 저장소에 대한 데이터베이스 인스턴스를 생성합니다.

예:

smdatastore

3. SiteMinder 스키마를 생성합니다.
4. SiteMinder 에 대한 SQL Server 데이터 원본을 구성합니다.
 - (Windows) SQL Server 데이터 원본을 생성합니다.
 - (UNIX) UNIX 시스템에서 SQL Server 데이터 원본을 생성합니다.
 - (UNIX) SQL Server 유선 프로토콜 드라이버를 구성합니다.
5. 정책 서버를 데이터베이스에 연결합니다.
6. SiteMinder 슈퍼 사용자 암호를 설정합니다.
7. 정책 저장소 데이터 정의를 가져옵니다.
8. 기본 SiteMinder 개체를 가져옵니다.
9. 정책 서버를 다시 시작합니다.
10. 관리 UI 등록을 준비합니다.

SiteMinder 스키마 만들기

SQL Server 데이터베이스에서 정책, 키 및 감사 로깅 정보를 저장할 수 있도록 SiteMinder 스키마를 생성하십시오.

정책 저장소 및 감사 로깅 스키마 파일을 실행하면 다음 경고가 표시됩니다. 이러한 경고는 정책 저장소 구성에 영향을 주지 않습니다.

- Warning: The table 'smvariable5' has been created but its maximum row size (8746) exceeds the maximum number of bytes per row (8060). INSERT or UPDATE of a row in this table will fail if the resulting row length exceeds 8060 bytes.
- Warning: The table 'smodbcquery4' has been created but its maximum row size (64635) exceeds the maximum number of bytes per row (8060). INSERT or UPDATE of a row in this table will fail if the resulting row length exceeds 8060 bytes.
- Warning: The table 'smaccesslog4' has been created but its maximum row size (9668) exceeds the maximum number of bytes per row (8060). INSERT or UPDATE of a row in this table will fail if the resulting row length exceeds 8060 bytes.

다음 단계를 수행하십시오.

1. 쿼리 분석기를 시작하고 정책 서버 데이터베이스를 관리하는 사용자로 로그인합니다.
2. 데이터베이스 목록에서 데이터베이스 인스턴스를 선택합니다.
3. 텍스트 편집기에서 `sm_mssql_ps.sql` 을 열고 전체 파일의 내용을 복사합니다.
4. `sm_mssql_ps.sql` 에서 쿼리로 스키마를 붙여 넣고 쿼리를 실행합니다.
정책 및 키 저장소 스키마가 데이터베이스에 추가됩니다.
5. 텍스트 편집기에서 `SQLServer.sql` 을 열고 전체 파일의 내용을 복사합니다.
6. `SQLServer.sql` 의 스키마를 쿼리에 붙여 넣고 쿼리를 실행합니다.
정책 저장소 스키마가 확장됩니다.
7. 정책 저장소를 감사 로깅 데이터베이스로 사용하기 위해 3~4 단계를 반복합니다. 다음 스키마 파일을 사용합니다.

`sm_mssql_logs.sql`

참고: 추가 SiteMinder 데이터를 저장하기 위해 정책 저장소를 구성할 필요는 없습니다. 각각의 데이터베이스를 별도의 감사 로그 데이터베이스, 키 저장소 및 세션 저장소로 작동하도록 구성할 수 있습니다.

데이터베이스에서 SiteMinder 데이터를 저장할 수 있습니다.

SiteMinder 에 대한 SQL Server 데이터 원본 구성

ODBC 를 사용하는 경우 SiteMinder 가 SiteMinder 데이터 저장소와 통신할 수 있도록 데이터 원본을 구성해야 합니다.

추가 정보:

[SQL Server 인증 모드 고려 사항](#) (페이지 330)

SQL Server 인증 모드 고려 사항

SiteMinder 데이터 원본은 Windows 인증을 지원하지 않습니다.

데이터베이스에 저장된 사용자의 자격 증명을 사용하여 SiteMinder 데이터 원본을 구성하십시오.

참고: SQL Server 인증 모드에 대한 자세한 내용은 해당 공급업체의 설명서를 참조하십시오.

Windows 에서 SQL Server 데이터 원본 만들기

ODBC 를 사용하려면 SQL Server 유선 프로토콜에 대해 데이터 원본을 구성해야 합니다.

참고: 이 절차는 정책 서버가 Windows 시스템에 설치되어 있는 경우에만 적용됩니다.

다음 단계를 수행하십시오.

1. 다음 단계 중 하나를 완료하십시오.

- 지원되는 32 비트 Windows 운영 체제를 사용 중인 경우 "시작"을 클릭하고 "프로그램", "관리 도구", "ODBC 데이터 원본"을 차례로 선택합니다.

- 지원되는 64 비트 Windows 운영 체제를 사용 중인 경우 다음을 수행합니다.

a. C:\Windows\SysWOW64 로 이동합니다.

b. odbcad32.exe 를 두 번 클릭합니다.

"ODBC 데이터 원본 관리자"가 표시됩니다.

2. "시스템 DSN" 탭을 클릭합니다.

시스템 데이터 원본 설정이 표시됩니다.

3. "추가"를 클릭합니다.

"새 데이터 원본 만들기" 대화 상자가 표시됩니다.

4. "SiteMinder SQL Server Wire Protocol"을 선택하고 "마침"을 클릭합니다.

"ODBC SQL Server Wire Protocol Driver 설정" 대화 상자가 표시됩니다.

5. "데이터 원본 이름" 필드에 데이터 원본 이름을 입력합니다.

예: SiteMinder 데이터 원본

참고: 데이터 원본 이름을 적어 두십시오. 이 정보는 데이터베이스를 정책 저장소로 구성할 때 필요합니다.

6. "서버" 필드에 SQL Server 호스트 시스템의 이름을 입력합니다.

7. "데이터베이스 이름" 필드에 데이터베이스 이름을 입력합니다.

8. "테스트"를 클릭합니다.

연결 설정이 테스트되고 연결에 성공했음을 나타내는 메시지가 표시됩니다.

9. "확인"을 클릭합니다.

SQL Server 데이터 원본이 구성되어 "시스템 데이터 원본" 목록에 표시됩니다.

UNIX 시스템에서 SQL Server 데이터 원본 만들기

SiteMinder ODBC 데이터 원본은 `system_odbc.ini` 파일을 사용하여 구성합니다. 이 파일은 `policy_server_installation/db`에 있는 `sqlserverwire.ini`를 `system_odbc.ini`로 이름을 바꿔 생성할 수 있습니다. 이 `system_odbc.ini` 파일에는 사용할 수 있는 ODBC 데이터 원본의 이름뿐 아니라 이러한 데이터 원본과 연관된 특성도 모두 들어 있습니다. 각 사이트에 맞게 이 파일을 사용자 지정해야 합니다. SiteMinder에 대한 추가 ODBC 사용자 디렉터리를 정의하는 등 이 파일에 데이터 원본을 더 추가할 수도 있습니다.

`system_odbc.ini` 파일의 첫 번째 섹션인 [ODBC Data Sources]에는 현재 사용할 수 있는 모든 데이터 원본의 목록이 들어 있습니다. "=" 앞의 이름은 해당 파일에서 각 개별 데이터 원본을 설명하는 이후 섹션을 나타냅니다. "=" 뒷부분은 주석 필드입니다.

참고: 데이터 원본 항목의 첫 행인 [SiteMinder Data Source]를 수정할 경우 변경한 값을 적어 두십시오. 이 값은 ODBC 데이터베이스를 정책 저장소로 구성할 때 필요합니다.

`system_odbc.ini` 파일에는 각 데이터 원본의 특성을 설명하는 섹션이 있습니다. 첫 번째 특성은 해당 데이터 원본이 SiteMinder에서 사용될 때 로드되는 ODBC 드라이버입니다. 나머지 특성은 드라이버마다 다릅니다.

MS SQL Server 데이터 원본을 추가하려면 파일의 [ODBC Data Sources] 섹션에 새 데이터 원본 이름을 추가한 후 데이터 원본과 동일한 이름을 사용하여 데이터 원본을 설명하는 섹션을 추가해야 합니다. 새 서비스 이름을 생성하거나 다른 드라이버를 사용하려는 경우에는 `system_odbc.ini` 파일을 변경해야 합니다. Oracle 또는 SQL 드라이버에 대한 항목은 [SiteMinder Data Source] 아래에 추가해야 합니다.

또한 MS SQL Server 데이터 원본을 구성하려면 먼저 `policy_server_installation/db` 디렉터리에 `system_odbc.ini` 파일을 생성해야 합니다. 이를 위해서는 `policy_server_installation/db`에 있는 `sqlserverwire.ini`를 `system_odbc.ini`로 이름을 바꿔야 합니다.

SQL Server 유선 프로토콜 드라이버 구성

유선 프로토콜 드라이버를 구성하여 SiteMinder 가 데이터베이스에 연결하는 데 사용할 설정을 지정할 수 있습니다.

참고: 이 절차는 정책 서버가 UNIX 시스템에 설치된 경우에만 적용됩니다. 아직 수행하지 않은 경우 아래의 파일 중 하나를 복사하고 이름을 `system_odbc.ini` 로 바꾸십시오. 이름을 바꾸는 파일은 SiteMinder 데이터 저장소로 구성하는 데이터베이스 공급업체에 따라 다릅니다.

- `sqlserverwire.ini`
- `oraclewire.ini`
- `mysqlwire.ini`
- `postgresqlwire.ini`

이러한 파일은 `siteminder_home/db` 에 있습니다.

`system_odbc.ini` 파일은 다음 섹션으로 구성되어 있습니다. 구성하는 데이터 원본에 따라 편집할 섹션이 결정됩니다.

[SiteMinder Data Source]

SiteMinder 가 정책 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SiteMinder Logs Data Source]

SiteMinder 가 감사 로그 데이터베이스로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SiteMinder Keys Data Source]

SiteMinder 가 키 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SiteMinder Session Data Source]

SiteMinder 가 세션 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SmSampleUsers Data Source]

SiteMinder 가 샘플 사용자 데이터 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

다음 단계를 수행하십시오.

1. system_odbc.ini 파일을 엽니다.
2. [ODBC Data Sources] 아래에 다음을 입력합니다.

SiteMinder Data Source=DataDirect 7.1 SQL Server Wire Protocol

3. 구성하려는 데이터 원본에 따라 다음 정보를 사용하여 하나 이상의 데이터 원본 섹션을 편집합니다.

Driver=nete_ps_root/odbc/lib/NSsqls27.so

Description=DataDirect 7.1 SQL Server Wire Protocol

Database=SiteMinder Data

Address=myhost, 1433

QuotedId=No

AnsiNPW=No

참고: 데이터 원본 정보를 편집할 때 파운드 기호(#)는 사용하지 마십시오. 파운드 기호를 입력하면 정보가 주석으로 처리되어 값이 잘립니다. 값이 잘리면 ODBC 연결이 실패할 수 있습니다.

nete_ps_root

환경 변수를 사용한 경로가 아닌 정책 서버 설치의 명시적 경로를 지정합니다.

예: export/smuser/siteminder

SiteMinder Data

SQL Server 데이터베이스 인스턴스 이름을 지정합니다.

myhost

SQL Server 데이터베이스의 IP 주소를 지정합니다.

1433

SQL Server 의 기본 수신 대기 포트를 나타냅니다.

4. Microsoft SQL Server 2008 을 사용하여 SiteMinder 저장소로 작동하도록 하려면 다음과 같이 [ODBC] 섹션을 편집합니다.

TraceFile=nete_ps_root/db/odbctrace.out

TraceDll=nete_ps_root/odbc/lib/NStrc27.so

InstallDir=nete_ps_root/odbc

nete_ps_root

정책 서버 설치 디렉터리의 명시적 경로를 지정합니다. 이 경로에는 환경 변수를 포함할 수 없습니다.

5. 파일을 저장합니다.

유선 프로토콜 드라이버가 구성되었습니다.

정책 서버를 데이터베이스에 연결

정책 서버가 정책 저장소의 SiteMinder 데이터에 액세스할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.

2. "저장소" 목록에서 다음 값을 선택합니다.

ODBC

3. "데이터베이스" 목록에서 다음 값을 선택합니다.

정책 저장소

4. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.

- (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
- (UNIX) 입력하는 이름은 system_odbc.ini 파일의 데이터 원본 항목 첫 줄과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 [SiteMinder Data Sources]입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.

5. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.

6. SiteMinder에 할당되는 최대 데이터베이스 연결 수를 지정합니다.

참고: 최상의 성능을 위해서는 기본 연결 수인 25를 유지하는 것이 좋습니다.

7. "적용"을 클릭하여 설정을 저장합니다.

8. "데이터베이스" 목록에서 다음 값을 선택합니다.

키 저장소

9. "저장소" 목록에서 다음 값을 선택합니다.

ODBC

10. 다음 옵션을 선택합니다.

정책 저장소 데이터베이스 사용

11. "데이터베이스" 목록에서 다음 값을 선택합니다.
감사 로그
12. "저장소" 목록에서 다음 값을 선택합니다.
ODBC
13. 다음 옵션을 선택합니다.
정책 저장소 데이터베이스 사용
14. "적용"을 클릭하여 설정을 저장합니다.
15. (선택 사항) "연결 테스트"를 클릭하여 정책 서버가 정책 저장소에 액세스할 수 있는지 확인합니다.
16. "확인"을 클릭합니다.
데이터베이스를 정책 저장소, 키 저장소 및 로깅 데이터베이스로 사용하도록 정책 서버가 구성되었습니다.

SiteMinder 슈퍼 사용자 암호 설정

기본 SiteMinder 관리자 계정의 이름은 다음으로 지정됩니다.

siteminder

이 계정에는 최대 권한이 있습니다.

일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다.
다음과 같은 경우에 기본 슈퍼 사용자를 사용합니다.

- 관리 UI에 처음 액세스할 경우
- SiteMinder 유틸리티를 처음 관리할 경우
- 슈퍼 사용자 권한이 있는 다른 관리자를 생성할 경우

다음 단계를 수행하십시오.

1. smreg 유틸리티를 *siteminder_home*\bin에 복사합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

참고: 이 유틸리티는 정책 서버 설치 키트의 최상위 수준에 있습니다.

2. 다음 명령을 실행합니다.

```
smreg -su password
```

password

기본 SiteMinder 관리자의 암호를 지정합니다.

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: Oracle 정책 저장소를 구성하는 경우 암호의 대/소문자를 구분합니다. 다른 모든 정책 저장소에서는 암호의 대/소문자를 구분하지 않습니다.

3. *siteminder_home*\bin 에서 smreg 를 삭제합니다. smreg 를 삭제하면 이전 암호를 모르는 다른 사람은 암호를 변경할 수 없게 됩니다.

기본 SiteMinder 관리자 계정의 암호가 설정되었습니다.

정책 저장소 데이터 정의 가져오기

정책 저장소 데이터 정의 가져오기를 사용하여 정책 저장소에서 생성하고 저장할 수 있는 개체의 유형을 정의합니다.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home*\xps\dd 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

```
XPSDDInstall SmMaster.xdd
```

XPSDDInstall

필수 데이터 정의를 가져옵니다.

기본 정책 저장소 개체 가져오기

기본 정책 저장소 개체 가져오기를 사용하여 관리 UI 및 정책 서버에서 사용할 정책 저장소를 구성합니다.

다음 사항을 고려하십시오.

- *siteminder_home\bin*에 대한 쓰기 액세스 권한이 있는지 확인하십시오. 가져오기 유틸리티에서 정책 저장소 개체를 가져오려면 이 권한이 필요합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

- Windows Server 2008에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 `siteminder_home\db` 로 이동합니다.

2. 다음 파일 중 하나를 가져옵니다.

- `smpolicy.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy.xml -npass
```

- `smpolicy-secure.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy-secure.xml -npass
```

npass

암호를 사용할 필요가 없음을 지정합니다. 기본 정책 저장소 개체에 암호화된 데이터가 포함되지 않습니다.

두 파일 모두 기본 정책 저장소 개체를 포함합니다. 이러한 개체는 기본 ACO(에이전트 구성 개체) 템플릿의 기본 보안 설정을 포함합니다. `smpolicy-secure` 파일은 보다 제한적인 보안 설정을 제공합니다. 자세한 내용은 [기본 정책 저장소 개체 고려 사항](#) (페이지 98)을 참조하십시오.

- 옵션 팩 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport ampolicy.xml -npass
```

- 페더레이션 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

정책 저장소 개체를 가져왔습니다.

참고: `smpolicy.xml` 을 가져오면 SiteMinder 에서 별도로 라이선스가 제공되는 레거시 페더레이션 및 웹 서비스 변수 기능을 사용할 수 있게 됩니다. 웹 서비스 변수 기능을 사용하려면 CA 고객 담당자에게 라이선스 정보에 대해 문의하십시오.

고급 인증 서버를 사용하도록 설정

정책 서버를 구성하는 과정에서 고급 인증 서버를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 구성 마법사를 시작합니다.
2. 마법사의 첫 번째 화면에서 모든 확인란을 **선택 취소**한 상태로 둡니다.
3. "다음"을 클릭합니다.
4. 고급 인증 서버에 대한 마스터 암호화 키를 생성합니다.

참고: 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

5. 정책 서버 구성 마법사의 나머지 과정을 완료합니다.
고급 인증 서버가 사용되도록 설정되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 **stop-all** 명령 다음에 **start-all** 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

관리 UI 등록 준비

기본 SiteMinder 슈퍼 사용자 계정(siteminder)을 사용하여 관리 UI에 최초로 로그인합니다. 최초 로그인 시 관리 UI를 정책 서버에 등록하여 두 구성 요소 간에 트러스트 관계를 생성해야 합니다.

등록을 준비하려면 XPSRegClient 유틸리티를 사용하여 슈퍼 사용자 계정 이름과 암호를 제공합니다. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 트러스트 관계를 설정할 수 있는지 확인합니다.

다음 사항을 고려하십시오.

- 자격 증명을 제공한 때부터 24 시간 이내에 최초 관리 UI 로그인이 이루어져야 합니다. 관리 UI 설치를 하루 안에 수행할 계획이 아니면 관리 UI를 설치하기 전에 다음 단계를 완료하십시오.
- (UNIX) XPSRegClient를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

기본 SiteMinder 슈퍼 사용자 계정(siteminder)의 암호를 지정합니다.

참고: 암호를 지정하지 않으면 XPSRegClient에서 암호를 입력하고 확인하라는 메시지가 표시됩니다.

-adminui-setup

관리 UI가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 관리 UI 를 설치할 때부터 정책 서버에 로그인하고 정책 서버와의 트러스트 관계를 생성할 때까지 할당된 시간을 지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록 요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 15

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI 를 등록할 때 허용되는 시도 실패 횟수를 지정합니다. 관리 UI 에 최초로 로그인할 때 올바르게 않은 SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수 있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을 삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error_path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: stderr

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

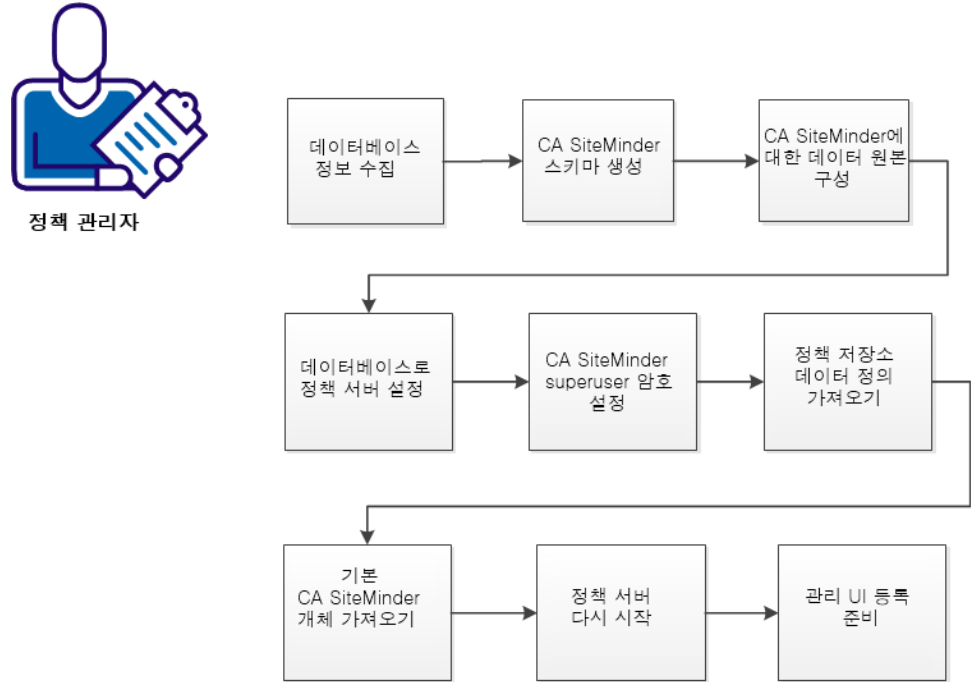
(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

XPSRegClient 가 정책 서버에 관리자 자격 증명을 제공합니다. 정책 서버에서는 관리 UI에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

PostgreSQL 서버 정책 저장소를 구성하는 방법

다음 다이어그램은 PostgreSQL 서버 데이터베이스를 정책 저장소로 구성하는 프로세스를 설명합니다.



사전 요구 사항

- SiteMinder 데이터를 포함하는 PostgreSQL 데이터베이스 인스턴스를 정책 서버 시스템에서 액세스할 수 있는지 확인하십시오.
- SiteMinder 데이터 저장소에 대한 데이터베이스 인스턴스를 만드십시오.

예:

smdatastore

다음 단계를 수행하십시오.

1. PostgreSQL 데이터베이스 정보를 수집합니다.
2. SiteMinder 스키마를 생성합니다.

3. SiteMinder 에 대한 PostgreSQL 데이터 원본을 구성합니다.
 - (Windows) PostgreSQL 데이터 원본을 생성합니다.
 - (UNIX) UNIX 시스템에서 PostgreSQL 데이터 원본을 생성합니다.
 - (UNIX) PostgreSQL 유선 프로토콜 드라이버를 구성합니다.
4. 정책 서버를 데이터베이스에 연결합니다.
5. SiteMinder 슈퍼 사용자 암호를 설정합니다.
6. 정책 저장소 데이터 정의를 가져옵니다.
7. 기본 SiteMinder 개체를 가져옵니다.
8. 정책 서버를 다시 시작합니다.
9. 관리 UI 등록을 준비합니다.

PostgreSQL 데이터베이스 정보 수집

정책 저장소나 다른 유형의 SiteMinder 데이터 저장소로 사용할 단일 PostgreSQL 서버 데이터베이스를 구성하려면 특정 데이터베이스 정보가 필요합니다.

정책 저장소나 다른 유형의 SiteMinder 데이터 저장소를 구성하기 전에 다음 정보를 수집하십시오.

데이터베이스 인스턴스 이름

정책 저장소 또는 데이터 저장소로 기능하는 데이터베이스 인스턴스의 이름을 결정합니다.

관리 계정 이름 및 암호

데이터베이스의 개체에 대한 생성, 읽기, 수정 및 삭제 권한이 있는 계정의 사용자 이름 및 암호를 결정합니다.

데이터 원본 이름

데이터 원본을 식별하는 데 사용할 이름을 결정합니다.

예: SM PostgreSQL Server Wire DS

PostgreSQL 서버 이름

정책 저장소로 기능하는 인스턴스가 포함된 PostgreSQL 서버 데이터베이스의 이름을 결정합니다.

정책 서버 루트

정책 서버가 설치된 명시적 경로를 결정합니다.

IP 주소

PostgreSQL 서버 데이터베이스의 IP 주소를 결정합니다.

PostgreSQL 용 SiteMinder 스키마 만들기

SQL Server 데이터베이스에서 정책, 키, 세션, 감사 로깅 정보를 저장할 수 있도록 SiteMinder 스키마를 생성하십시오.

다음 단계를 수행하십시오.

1. PostgreSQL 클라이언트를 시작하고 정책 서버 데이터베이스를 관리하는 사용자로 로그인합니다.
2. 데이터베이스 목록에서 데이터베이스 인스턴스를 선택합니다.
3. 텍스트 편집기에서 *policy_server_home/db/SQL/sm_postgresql_ps.sql* 을 열고 전체 파일의 내용을 복사합니다.
4. *sm_postgresql_ps.sql* 에서 쿼리로 스키마를 붙여 넣고 쿼리를 실행합니다.
정책 및 키 저장소 스키마가 데이터베이스에 추가됩니다.
5. 텍스트 편집기에서 *policy_server_home/xps/db/PostgreSQL.sql* 을 열고 전체 파일의 내용을 복사합니다.
6. *PostgreSQL.sql* 의 스키마를 쿼리에 붙여 넣고 쿼리를 실행합니다.
정책 저장소 스키마가 확장됩니다.
7. 정책 저장소를 감사 로깅 데이터베이스로 사용하기 위해 3~4 단계를 반복합니다. 다음 스키마 파일을 사용합니다.

sm_postgresql_logs.sql

참고: 추가 SiteMinder 데이터를 저장하기 위해 정책 저장소를 구성할 필요는 없습니다. 각각의 데이터베이스를 별도의 감사 로그 데이터베이스, 키 저장소 및 세션 저장소로 작동하도록 구성할 수 있습니다.

데이터베이스에서 SiteMinder 데이터를 저장할 수 있습니다.

Windows 에서 PostgreSQL 데이터 원본 만들기

ODBC 를 사용하려면 SQL Server 유선 프로토콜에 대해 데이터 원본을 구성해야 합니다.

다음 단계를 수행하십시오.

1. 다음 단계 중 하나를 완료하십시오.
 - 지원되는 32 비트 Windows 운영 체제를 사용 중인 경우 "시작"을 클릭하고 "프로그램", "관리 도구", "ODBC 데이터 원본"을 차례로 선택합니다.
 - 지원되는 64 비트 Windows 운영 체제를 사용 중인 경우 다음을 수행합니다.
 - a. C:\Windows\SysWOW64 로 이동합니다.
 - b. odbcad32.exe 를 두 번 클릭합니다.

"ODBC 데이터 원본 관리자"가 표시됩니다.
2. "시스템 DSN" 탭을 클릭합니다.
3. "추가"를 클릭합니다.
4. "SiteMinder PostgreSQL Server Wire Protocol"을 선택하고 "마침"을 클릭합니다.
5. "데이터 원본 이름" 필드에 데이터 원본 이름을 입력합니다.

예: SiteMinder 데이터 원본

참고: 데이터 원본 이름을 적어 두십시오. 이 정보는 데이터베이스를 정책 저장소로 구성할 때 필요합니다.
6. "서버" 필드에 PostgreSQL 호스트 시스템의 이름을 입력합니다.
7. "데이터베이스 이름" 필드에 데이터베이스 이름을 입력합니다.

8. "테스트"를 클릭합니다.

연결 설정이 테스트되고 연결에 성공했음을 나타내는 메시지가 표시됩니다.

9. "확인"을 클릭합니다.

PostgreSQL 데이터 원본이 구성되어 "시스템 데이터 원본" 목록에 표시됩니다.

UNIX 에서 PostgreSQL 데이터 원본 만들기

SiteMinder ODBC 데이터 원본은 `system_odbc.ini` 파일을 사용하여 구성합니다. 이 파일은 `policy_server_installation/db` 에 있는 `sqlserverwire.ini` 를 `system_odbc.ini` 로 이름을 바꿔 생성할 수 있습니다. 이 `system_odbc.ini` 파일에는 사용할 수 있는 ODBC 데이터 원본의 이름뿐 아니라 이러한 데이터 원본과 연관된 특성도 모두 들어 있습니다. 각 사이트에 맞게 이 파일을 사용자 지정해야 합니다. SiteMinder 에 대한 추가 ODBC 사용자 디렉터리를 정의하는 등 이 파일에 데이터 원본을 더 추가할 수도 있습니다.

`system_odbc.ini` 파일의 첫 번째 섹션인 [ODBC Data Sources]에는 현재 사용할 수 있는 모든 데이터 원본의 목록이 들어 있습니다. "=" 앞의 이름은 해당 파일에서 각 개별 데이터 원본을 설명하는 이후 섹션을 나타냅니다. "=" 뒷부분은 주식 필드입니다.

참고: 데이터 원본 항목의 첫 행인 [SiteMinder Data Source]를 수정할 경우 변경한 값을 적어 두십시오. 이 값은 ODBC 데이터베이스를 정책 저장소로 구성할 때 필요합니다.

`system_odbc.ini` 파일에는 각 데이터 원본의 특성을 설명하는 섹션이 있습니다. 첫 번째 특성은 해당 데이터 원본이 SiteMinder 에서 사용될 때 로드되는 ODBC 드라이버입니다. 나머지 특성은 드라이버마다 다릅니다.

PostgreSQL 서버 데이터 원본을 추가하려면 파일의 [ODBC Data Sources] 섹션에 새 데이터 원본 이름을 추가한 후 데이터 원본과 동일한 이름을 사용하여 데이터 원본을 설명하는 섹션을 추가해야 합니다. 새 서비스 이름을 생성하거나 다른 드라이버를 사용하려는 경우에는 `system_odbc.ini` 파일을 변경해야 합니다. Oracle 또는 SQL 드라이버에 대한 항목은 [SiteMinder Data Source] 아래에 있습니다.

PostgreSQL Server 유선 프로토콜 드라이버 구성

유선 프로토콜 드라이버를 구성하여 SiteMinder 가 데이터베이스에 연결하는 데 사용할 설정을 지정할 수 있습니다.

참고: 이 절차는 정책 서버가 UNIX 시스템에 설치된 경우에만 적용됩니다. 아직 수행하지 않은 경우 아래의 파일 중 하나를 복사하고 이름을 `system_odbc.ini` 로 바꾸십시오. 이름을 바꾸는 파일은 SiteMinder 데이터 저장소로 구성하는 데이터베이스 공급업체에 따라 다릅니다.

- `sqlserverwire.ini`
- `oraclewire.ini`
- `mysqlwire.ini`
- `postgresqlwire.ini`

이러한 파일은 `siteminder_home/db` 에 있습니다.

`system_odbc.ini` 파일은 다음 섹션으로 구성되어 있습니다. 구성하는 데이터 원본에 따라 편집할 섹션이 결정됩니다.

[SiteMinder Data Source]

SiteMinder 가 정책 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SiteMinder Logs Data Source]

SiteMinder 가 감사 로그 데이터베이스로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SiteMinder Keys Data Source]

SiteMinder 가 키 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SiteMinder Session Data Source]

SiteMinder 가 세션 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SmSampleUsers Data Source]

SiteMinder 가 샘플 사용자 데이터 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

다음 단계를 수행하십시오.

1. `system_odbc.ini` 파일을 엽니다.

2. [ODBC Data Sources] 아래에 다음을 입력합니다.

SiteMinder Data Source=DataDirect 7.1 PostgrSQL Server Wire Protocol

3. 구성하려는 데이터 원본에 따라 다음 정보를 사용하여 하나 이상의 데이터 원본 섹션을 편집합니다.

Driver=*nete_ps_root*/odbc/lib/NSpsql27.so

Description=DataDirect 7.1 PostgreSQL Server Wire Protocol

Database=*SiteMinder Data*

Address=*myhost*, 1433

QuotedId=No

AnsiNPW=No

참고: 데이터 원본 정보를 편집할 때 파운드 기호(#)는 사용하지 마십시오. 파운드 기호를 입력하면 정보가 주석으로 처리되어 값이 잘립니다. 값이 잘리면 ODBC 연결이 실패할 수 있습니다.

nete_ps_root

환경 변수를 사용한 경로가 아닌 정책 서버 설치의 명시적 경로를 지정합니다.

예: export/smuser/siteminder

SiteMinder Data

PostgreSQL Server 데이터베이스 인스턴스 이름을 지정합니다.

myhost

PostgreSQL Server 데이터베이스의 IP 주소를 지정합니다.

1433

PostgreSQL Server 의 기본 수신 대기 포트를 나타냅니다.

4. 다음과 같이 [ODBC] 섹션을 편집합니다.

TraceFile=*nete_ps_root*/db/odbctrace.out

TraceDll=*nete_ps_root*/odbc/lib/NStrc27.so

InstallDir=*nete_ps_root*/odbc

nete_ps_root

정책 서버 설치 디렉터리의 명시적 경로를 지정합니다. 이 경로에는 환경 변수를 포함할 수 없습니다.

5. 파일을 저장합니다.

유선 프로토콜 드라이버가 구성되었습니다.

정책 서버를 데이터베이스에 연결

정책 서버가 정책 저장소의 SiteMinder 데이터에 액세스할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.
2. "저장소" 목록에서 다음 값을 선택합니다.

ODBC

3. "데이터베이스" 목록에서 다음 값을 선택합니다.

정책 저장소

4. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.
 - (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
 - (UNIX) 입력하는 이름은 `system_odbc.ini` 파일의 데이터 원본 항목 첫 줄과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 [SiteMinder Data Sources]입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.
5. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.
6. SiteMinder에 할당되는 최대 데이터베이스 연결 수를 지정합니다.

참고: 최상의 성능을 위해서는 기본 연결 수인 25를 유지하는 것이 좋습니다.

7. "적용"을 클릭하여 설정을 저장합니다.
8. "데이터베이스" 목록에서 다음 값을 선택합니다.

키 저장소

9. "저장소" 목록에서 다음 값을 선택합니다.

ODBC

10. 다음 옵션을 선택합니다.

정책 저장소 데이터베이스 사용

11. "데이터베이스" 목록에서 다음 값을 선택합니다.

감사 로그

12. "저장소" 목록에서 다음 값을 선택합니다.

ODBC

13. 다음 옵션을 선택합니다.

정책 저장소 데이터베이스 사용

14. "적용"을 클릭하여 설정을 저장합니다.

15. (선택 사항) "연결 테스트"를 클릭하여 정책 서버가 정책 저장소에 액세스할 수 있는지 확인합니다.

16. "확인"을 클릭합니다.

데이터베이스를 정책 저장소, 키 저장소 및 로깅 데이터베이스로 사용하도록 정책 서버가 구성되었습니다.

SiteMinder 슈퍼 사용자 암호 설정

기본 SiteMinder 관리자 계정의 이름은 다음으로 지정됩니다.

siteminder

이 계정에는 최대 권한이 있습니다.

일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 다음과 같은 경우에 기본 슈퍼 사용자를 사용합니다.

- 관리 UI에 처음 액세스할 경우
- SiteMinder 유틸리티를 처음 관리할 경우
- 슈퍼 사용자 권한이 있는 다른 관리자를 생성할 경우

다음 단계를 수행하십시오.

1. smreg 유틸리티를 *siteminder_home*\bin에 복사합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

참고: 이 유틸리티는 정책 서버 설치 키트의 최상위 수준에 있습니다.

2. 다음 명령을 실행합니다.

smreg -su *password*

password

기본 SiteMinder 관리자의 암호를 지정합니다.

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: Oracle 정책 저장소를 구성하는 경우 암호의 대/소문자를 구분합니다. 다른 모든 정책 저장소에서는 암호의 대/소문자를 구분하지 않습니다.

3. *siteminder_home*\bin 에서 *smreg* 를 삭제합니다. *smreg* 를 삭제하면 이전 암호를 모르는 다른 사람은 암호를 변경할 수 없게 됩니다.

기본 SiteMinder 관리자 계정의 암호가 설정되었습니다.

정책 저장소 데이터 정의 가져오기

정책 저장소 데이터 정의 가져오기를 사용하여 정책 저장소에서 생성하고 저장할 수 있는 개체의 유형을 정의합니다.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home*\xps\dd 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

```
XPSDDInstall SmMaster.xdd
```

XPSDDInstall

필수 데이터 정의를 가져옵니다.

기본 정책 저장소 개체 가져오기

기본 정책 저장소 개체 가져오기를 사용하여 관리 UI 및 정책 서버에서 사용할 정책 저장소를 구성합니다.

다음 사항을 고려하십시오.

- `siteminder_home\bin`에 대한 쓰기 액세스 권한이 있는지 확인하십시오. 가져오기 유틸리티에서 정책 저장소 개체를 가져오려면 이 권한이 필요합니다.

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

- Windows Server 2008에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 `siteminder_home\db` 로 이동합니다.

2. 다음 파일 중 하나를 가져옵니다.

- `smpolicy.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy.xml -npass
```

- `smpolicy-secure.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy-secure.xml -npass
```

npass

암호를 사용할 필요가 없음을 지정합니다. 기본 정책 저장소 개체에 암호화된 데이터가 포함되지 않습니다.

두 파일 모두 기본 정책 저장소 개체를 포함합니다. 이러한 개체는 기본 ACO(에이전트 구성 개체) 템플릿의 기본 보안 설정을 포함합니다. `smpolicy-secure` 파일은 보다 제한적인 보안 설정을 제공합니다. 자세한 내용은 [기본 정책 저장소 개체 고려 사항](#) (페이지 98)을 참조하십시오.

- 옵션 팩 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport ampolicy.xml -npass
```

- 페더레이션 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

정책 저장소 개체를 가져왔습니다.

참고: `smpolicy.xml` 을 가져오면 SiteMinder 에서 별도로 라이선스가 제공되는 레거시 페더레이션 및 웹 서비스 변수 기능을 사용할 수 있게 됩니다. 웹 서비스 변수 기능을 사용하려면 CA 고객 담당자에게 라이선스 정보에 대해 문의하십시오.

고급 인증 서버를 사용하도록 설정

정책 서버를 구성하는 과정에서 고급 인증 서버를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 구성 마법사를 시작합니다.
2. 마법사의 첫 번째 화면에서 모든 확인란을 *선택 취소*한 상태로 둡니다.
3. "다음"을 클릭합니다.
4. 고급 인증 서버에 대한 마스터 암호화 키를 생성합니다.

참고: 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

5. 정책 서버 구성 마법사의 나머지 과정을 완료합니다.
고급 인증 서버가 사용되도록 설정되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 `stop-all` 명령 다음에 `start-all` 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

관리 UI 등록 준비

기본 SiteMinder 슈퍼 사용자 계정(siteminder)을 사용하여 관리 UI에 최초로 로그인합니다. 최초 로그인 시 관리 UI를 정책 서버에 등록하여 두 구성 요소 간에 트러스트 관계를 생성해야 합니다.

등록을 준비하려면 XPSRegClient 유틸리티를 사용하여 슈퍼 사용자 계정 이름과 암호를 제공합니다. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 트러스트 관계를 설정할 수 있는지 확인합니다.

다음 사항을 고려하십시오.

- 자격 증명을 제공한 때부터 24 시간 이내에 최초 관리 UI 로그인이 이루어져야 합니다. 관리 UI 설치를 하루 안에 수행할 계획이 아니면 관리 UI를 설치하기 전에 다음 단계를 완료하십시오.
- (UNIX) XPSRegClient를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

기본 SiteMinder 슈퍼 사용자 계정(siteminder)의 암호를 지정합니다.

참고: 암호를 지정하지 않으면 XPSRegClient에서 암호를 입력하고 확인하라는 메시지가 표시됩니다.

-adminui-setup

관리 UI가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 관리 UI 를 설치할 때부터 정책 서버에 로그인하고 정책 서버와의 트러스트 관계를 생성할 때까지 할당된 시간을 지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록 요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 15

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI 를 등록할 때 허용되는 시도 실패 횟수를 지정합니다. 관리 UI 에 최초로 로그인할 때 올바르게 않은 SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수 있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을 삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error_path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: stderr

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

XPSRegClient 가 정책 서버에 관리자 자격 증명을 제공합니다. 정책 서버에서는 관리 UI에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

Oracle 정책 저장소 구성

단일 Oracle 데이터베이스가 다음 기능을 수행할 수 있습니다.

- 정책 저장소
- 키 저장소
- 로깅 데이터베이스

단일 데이터베이스를 사용하면 관리 태스크를 간소화할 수 있습니다. 다음 단원에서는 SiteMinder 데이터를 저장할 단일 데이터베이스 서버를 구성하는 방법에 대한 지침을 제공합니다.

Oracle 정책 저장소는 수동으로 구성하거나 정책 서버 설치 관리자를 사용하여 자동으로 구성할 수 있습니다.

Oracle 10g 데이터베이스에 대한 사전 요구 사항

Oracle 10g 데이터베이스를 설치한 후 다음 사전 요구 사항을 완료하십시오.

- 정책 저장소의 테이블스페이스를 생성하십시오.
- 데이터베이스에서 이 테이블스페이스를 관리할 수 있는 적절한 권한이 있는 사용자를 생성하십시오.

정책 저장소의 Oracle 10g 테이블스페이스 만들기

정책 저장소의 테이블스페이스를 생성하는 작업은 Oracle 10g 데이터베이스에만 필요합니다.

다음 단계를 수행하십시오.

1. Oracle Enterprise Manager 10g Database Control 에서 Oracle 데이터베이스를 관리할 수 있는 적절한 권한이 있는 SYSDBA 사용자로 로그인합니다.
2. Oracle 전역 데이터베이스의 구성 화면에서 "Administration"(관리), "Tablespaces"(테이블스페이스)를 차례로 선택합니다.
3. "Tablespaces"(테이블스페이스) 화면에서 "Create"(만들기)를 클릭합니다.
4. "Create Tablespaces"(테이블스페이스 만들기) 화면에서 테이블스페이스 이름을 입력하고 "ADD"(추가)를 클릭합니다.

예: NETE_TB

5. "Create Tablespaces: Add Datafile"(테이블스페이스 만들기: 데이터 파일 추가) 화면에서 다음을 수행합니다.

- a. 파일 이름을 입력합니다.

예: NETE_TB

- b. 파일 크기를 지정합니다.

예: 100 MB

- c. 계속을 클릭합니다.

테이블스페이스가 생성되어 "Tablespaces"(테이블스페이스) 화면에 표시됩니다.

정책 저장소의 테이블스페이스를 관리할 사용자를 생성하여 사전 요구 사항을 완료합니다.

추가 정보:

[정책 저장소의 테이블스페이스를 관리할 Oracle 10g 사용자 생성](#) (페이지 361)

정책 저장소의 테이블스페이스를 관리할 Oracle 10g 사용자 생성

정책 저장소의 테이블스페이스를 관리할 사용자를 생성하는 작업은 Oracle 10g 데이터베이스에만 필요합니다.

다음 단계를 수행하십시오.

1. Oracle 전역 데이터베이스의 구성 화면에서 "Administration"(관리), "Users"(사용자)를 차례로 선택합니다.
2. "Create Tablespaces"(테이블스페이스 만들기) 화면에서 "Create"(만들기)를 클릭합니다.
3. "Create User"(사용자 만들기) 화면에서 다음을 입력합니다.
 - 사용자의 이름
예: NETE
 - 사용자의 암호
 - 생성한 기본 테이블스페이스
 - 임시 테이블스페이스
예: TEMP
4. "Roles"(역할)를 클릭합니다.
5. "Modify"(수정)를 선택합니다.
6. "Modify Roles"(역할 수정) 화면에서 다음을 수행합니다.
 - a. 이 사용자의 역할로 "CONNECT"(연결)와 "RESOURCE"(리소스)를 선택합니다.
 - b. "적용"을 클릭합니다.

7. 명령 창에서 다음을 입력하여 **sqlplus** 를 시작합니다.

- a. **sqlplus**
- b. **"Create User"**(사용자 만들기) 화면에서 생성한 정책 저장소
사용자의 자격 증명

Oracle 10g 데이터베이스에 대한 사전 요구 사항이 완료되었으며 이제 데이터베이스에 대한 **SiteMinder** 데이터 저장소를 구성할 수 있습니다.

Oracle 12c 데이터베이스에 대한 사전 요구 사항

Oracle 12c 데이터베이스를 설치한 후에 다음 단계를 수행하십시오.

- 1. 정책 저장소의 테이블스페이스를 생성하십시오.
- 2. 데이터베이스에서 테이블스페이스를 관리하기 위해 다음 권한이 있는
사용자를 만듭니다.
 - 연결
 - 리소스
 - 제한 없는 테이블스페이스

데이터베이스 정보 수집

정책 저장소나 다른 유형의 **SiteMinder** 데이터 저장소로 사용할 단일 **Oracle** 데이터베이스를 구성하려면 특정 데이터베이스 정보가 필요합니다.

정보 앞에 **(U)**가 있으면 정책 서버가 **UNIX** 시스템에 설치된 경우에만 해당 정보가 필요하다는 것을 나타냅니다. 이 정보는 **UNIX**에 대한 **Oracle** 데이터 원본을 구성할 때 필요합니다.

필요한 정보

지원되는 Oracle 데이터베이스 또는 Oracle RAC 데이터베이스를 정책 저장소나 다른 유형의 SiteMinder 데이터 저장소로 구성하기 전에 다음과 같은 필요한 정보를 수집하십시오.

- **(U) 정책 서버 설치 경로** - 정책 서버가 설치된 위치의 명시적 경로를 확인합니다.
- **데이터 원본** - Oracle 데이터 원본을 식별하는 데 사용할 이름을 결정합니다.
예: SM Oracle Server Wire DS
- **데이터베이스 관리 계정** - 데이터베이스의 개체에 대한 생성, 읽기, 수정 및 삭제 권한이 있는 계정의 사용자 이름을 확인합니다.
참고: 관리 계정에는 DB 역할이 없어야 합니다. 관리 계정에 DB 역할이 있으면 감사 기반 보고서에 올바른 결과가 반환되지 않습니다.
- **데이터베이스 관리 암호** - 관리 계정의 암호를 확인합니다.

Oracle 데이터베이스 정보

지원되는 Oracle 데이터베이스를 정책 저장소나 다른 유형의 SiteMinder 데이터 저장소로 구성하려는 경우에만 다음 정보를 수집하십시오.

- **Oracle 컴퓨터 이름** - Oracle 데이터베이스가 설치된 컴퓨터의 이름을 확인합니다.
- **Oracle 인스턴스 서비스 이름** - 연결할 데이터베이스 인스턴스의 서비스 이름을 확인합니다. tnsnames.ora 파일에 서비스 이름이 지정되어 있습니다.
- **Oracle 포트 번호** - Oracle 데이터베이스가 수신 대기하는 포트 번호를 확인합니다.

Oracle RAC 데이터베이스 정보(SCAN 사용 안 함)

지원되는 Oracle RAC 데이터베이스(SCAN 기능이 구성 안 됨)를 정책 저장소나 다른 SiteMinder 데이터 저장소로 구성하려는 경우에 다음 정보를 수집하십시오.

- **Oracle RAC 시스템 서비스 이름** - 전체 시스템의 서비스 이름을 확인합니다.

예: 다음 tnsnames.ora 파일에서 SMDB 는 전체 시스템의 서비스 이름입니다.

```
SMDB=
(Description =
  (ADDRESS = PROTOCOL = TCP)(HOST = nete_servername1)(PORT=1521
  (ADDRESS = PROTOCOL = TCP)(HOST = nete_servername2)(PORT=1521)
  (ADDRESS = PROTOCOL = TCP)(HOST = nete_servername3)(PORT=1521))
  (LOAD_BALANCE = yes)
  (CONNECT_DATA=
    (SERVER = DEDICATED)
    (SERVER_NAME = SMDB))
  )
```

- **Oracle RAC 노드 서비스 이름** - 시스템에 있는 각 노드의 서비스 이름을 확인합니다.
- **Oracle RAC 노드 IP 주소** - Oracle RAC 시스템에 있는 각 노드의 IP 주소를 확인합니다.

참고: Oracle RAC 10g 를 사용하는 경우 시스템에 있는 각 노드의 가상 IP 주소를 확인하십시오.

- **Oracle RAC 노드 포트 번호** - Oracle RAC 시스템에 있는 각 노드의 포트 번호를 확인합니다.

Oracle RAC 데이터베이스 정보(SCAN 사용)

Oracle RAC SCAN(Single Client Access Name) 기능은 클러스터에서 실행하는 모든 Oracle 데이터베이스에 액세스할 수 있도록 여러 클라이언트에 단일 이름을 제공합니다.

SCAN 기능이 있는 Oracle RAC 데이터베이스를 정책 저장소나 다른 SiteMinder 데이터 저장소로 구성하려는 경우에 다음 정보를 수집하십시오.

- **Oracle RAC 시스템 서비스 이름** - 전체 시스템의 서비스 이름을 확인합니다.

예: 다음 tnsnames.ora 파일에서 SMDB 는 전체 시스템의 서비스 이름입니다.

```
SMDB=
(DESCRIPTION =
  (ADDRESS = (PROTOCOL = TCP)(HOST = clus-scan.example.com)(PORT = 1521))
  (CONNECT_DATA =
    (SERVER = DEDICATED)
    (SERVICE_NAME = SMDB)
  )
)
```

- **Oracle RAC SCAN 주소** - Oracle RAC 시스템 SCAN 의 FQDN 을 확인합니다.
- **Oracle RAC SCAN 포트 번호** - Oracle RAC 시스템 SCAN 의 포트 번호를 확인합니다.

정책 저장소를 구성하는 방법

단일 Oracle 데이터베이스를 정책 저장소, 키 저장소 및 로깅 데이터베이스로 구성하려면 다음 절차를 완료하십시오.

참고: 시작하기 전에 필수 데이터베이스 정보를 수집했는지 확인하십시오. 아래 단계 중 일부에서 이 정보가 필요합니다.

1. SiteMinder 데이터를 포함하는 Oracle 데이터베이스 인스턴스를 정책 서버 시스템에서 액세스할 수 있는지 확인합니다. tnspring 또는 sqlplus 를 사용하여 통신을 테스트합니다.
2. SiteMinder 스키마를 생성합니다.
3. SiteMinder 에 대한 Oracle 데이터 원본을 구성합니다.
 - (Windows) Windows 시스템에서 Oracle 데이터 원본을 생성합니다.
 - (Windows) Windows 시스템에서 Oracle RAC 데이터 원본을 생성합니다.
 - (UNIX) UNIX 에서 Oracle 데이터 원본을 생성합니다.
 - (UNIX) 유선 프로토콜 드라이버를 구성합니다.

- (UNIX) Oracle 유선 프로토콜 드라이버를 구성합니다.
 - (UNIX) Oracle RAC 유선 프로토콜 드라이버를 구성합니다.
4. 정책 서버를 데이터베이스에 연결합니다.
 5. SiteMinder 슈퍼 사용자 암호를 설정합니다.
 6. 정책 저장소 데이터 정의를 가져옵니다.
 7. 기본 정책 저장소 개체를 가져옵니다.
 8. 정책 서버를 다시 시작합니다.
 9. 관리 UI 등록을 준비합니다.

SiteMinder 스키마 만들기

단일 Oracle 데이터베이스에서 정책, 키 및 감사 로깅 정보를 저장할 수 있도록 SiteMinder 스키마를 생성하십시오.

다음 단계를 수행하십시오.

1. sqlplus 또는 다른 Oracle 유틸리티를 사용하여 정책 서버 데이터베이스 정보를 관리하는 사용자로 Oracle 에 로그인합니다.

참고: SYS 또는 SYSTEM 사용자로 SiteMinder 스키마를 생성하지 않는 것이 좋습니다. 필요한 경우 SMOWNER 같은 Oracle 사용자를 생성한 후 해당 사용자로 스키마를 생성하십시오.

2. 다음 스크립트를 가져옵니다.

```
$NETE_PS_ROOT/db/sql/sm_oracle_ps.sql
```

참고: 환경 변수는 Oracle 의 SQL 유틸리티에서 작동하지 않을 수 있습니다. 이 유틸리티를 사용하여 스크립트를 가져오는 동안 문제가 발생하면 명시적 경로를 지정하십시오.

정책 저장소 및 키 저장소 스키마가 데이터베이스에 추가됩니다.

3. 다음 스크립트를 가져옵니다.

```
$NETE_PS_ROOT/xps/db/Oracle.sql
```

정책 저장소 스키마가 확장됩니다.

4. 정책 저장소를 감사 로깅 데이터베이스로 사용하도록 다음 스크립트를 가져옵니다.

`sm_oracle_logs.sql`

참고: 추가 SiteMinder 데이터를 저장하기 위해 정책 저장소를 구성할 필요는 없습니다. 각각의 데이터베이스를 별도의 감사 로그 데이터베이스, 키 저장소 및 세션 저장소로 작동하도록 구성할 수 있습니다.

데이터베이스에서 SiteMinder 데이터를 저장할 수 있습니다.

SiteMinder에 대한 Oracle 데이터 원본 구성

ODBC를 사용하는 경우 Oracle 유선 프로토콜 드라이버에 대한 데이터 원본을 구성해야 합니다.

Windows에서 Oracle 데이터 원본 만들기

Oracle 데이터베이스용 ODBC 데이터 원본을 만듭니다.

다음 단계를 수행하십시오.

1. 다음 작업 중 하나를 수행하십시오.
 - 지원되는 32 비트 Windows 운영 체제를 사용 중인 경우 "시작"을 클릭하고 "프로그램", "관리 도구", "ODBC 데이터 원본"을 차례로 선택합니다.
 - 지원되는 64 비트 Windows 운영 체제를 사용 중인 경우 다음을 수행합니다.
 - a. `install_home\Windows\SysWOW64`로 이동합니다.
 - b. `odbcad32.exe`를 두 번 클릭합니다.

"ODBC 데이터 원본 관리자"가 표시됩니다.
2. "시스템 DSN" 탭을 클릭하고 "추가"를 클릭합니다.
"새 데이터 원본 만들기" 대화 상자가 표시됩니다.
3. "SiteMinder Oracle Wire Protocol"을 선택하고 "마침"을 클릭합니다.
"ODBC Oracle Wire Protocol Driver 설정" 대화 상자가 표시됩니다. "일반" 탭이 선택되어 있습니다.

4. "데이터 원본 이름" 필드에 데이터 원본을 식별할 수 있는 이름을 입력합니다.

참고: 이 이름을 기록해 두십시오. 정책 서버를 데이터베이스에 연결할 때 이 데이터 원본 이름이 필요합니다.

5. "호스트 이름" 필드에 Oracle 데이터베이스가 설치된 컴퓨터의 컴퓨터 이름을 입력합니다.
6. "포트 번호" 필드에 Oracle 데이터베이스가 컴퓨터에서 수신 대기하는 포트 번호를 입력합니다.
7. "SID" 필드에 연결할 Oracle 인스턴스의 이름을 입력합니다.

참고: 서비스 이름은 `tnsnames.ora` 파일에 지정되어 있습니다. SID 는 데이터베이스 인스턴스의 시스템 식별자입니다. `tnsnames.ora` 파일에는 서비스 이름과 Oracle 이 Oracle 인스턴스를 식별하고 해당 인스턴스에 연결하는 데 사용하는 상세 정보가 들어 있습니다.

예: `tnsnames.ora` 파일에 Oracle 인스턴스에 대한 다음 항목이 들어 있으면 SID 필드에 `instance1` 을 입력합니다.

```
instance1 =
  (Description=
    (Address = (PROTOCOL = TCP)(Host = myhost)(Port=1521))
    (Connect_DATA_ = (SID = SIDofinstance1))
  )
```

8. "연결 테스트"를 클릭합니다.

연결 설정이 테스트되고 연결에 성공했음을 나타내는 메시지가 표시됩니다.

9. "확인"을 클릭합니다.

유선 프로토콜 드라이버에 대해 Oracle 데이터 원본이 구성됩니다.

Windows 에서 Oracle RAC 데이터 원본 만들기(SCAN 사용 안 함)

SCAN 기능을 사용하지 않는 Oracle RAC 데이터베이스에 대해 ODBC 데이터 원본을 만듭니다.

다음 단계를 수행하십시오.

1. 다음 작업 중 하나를 수행하십시오.
 - 지원되는 32 비트 Windows 운영 체제를 사용 중인 경우 "시작"을 클릭하고 "프로그램", "관리 도구", "ODBC 데이터 원본"을 차례로 선택합니다.

- 지원되는 64 비트 Windows 운영 체제를 사용 중인 경우 다음을 수행합니다.

- a. C:\Windows\SysWOW64 로 이동합니다.
- b. odbcad32.exe 를 두 번 클릭합니다.

"ODBC 데이터 원본 관리자"가 표시됩니다.

2. "시스템 DSN" 탭을 클릭하고 "추가"를 클릭합니다.

"새 데이터 원본 만들기" 대화 상자가 표시됩니다.

3. "SiteMinder Oracle Wire Protocol"을 선택하고 "마침"을 클릭합니다.

"ODBC Oracle Wire Protocol Driver 설정" 대화 상자가 표시됩니다. "일반" 탭이 선택되어 있습니다.

4. "데이터 원본 이름" 필드에 데이터 원본을 식별할 수 있는 이름을 입력합니다.

참고: 이 이름을 기록해 두십시오. 정책 서버를 데이터베이스에 연결할 때 이 데이터 원본 이름이 필요합니다.

5. "호스트" 필드에 Oracle RAC 시스템에서 첫 번째 노드의 IP 주소를 입력합니다.

Oracle RAC 10g: 가상 IP 주소를 입력합니다.

6. "서비스 이름" 필드에 전체 Oracle RAC 시스템의 서비스 이름을 입력합니다.

예: 다음 tnsnames.ora 파일에서 SMDB 값이 3 개의 노드로 구성된 전체 Oracle RAC 시스템의 서비스 이름입니다.

```
SMDB=
(Description =
  (ADDRESS = (Protocol = TCP)(HOST = nete_servername1)(PORT = 1521))
  (ADDRESS = (Protocol = TCP)(HOST = nete_servername2)(PORT = 1521))
  (ADDRESS = (Protocol = TCP)(HOST = nete_servername3)(PORT = 1521))
  (LOAD_BALANCE = yes)
  (CONNECT_DATA =
    (SERVER = DEDICATED)
    (SERVICE_NAME = SMDB)
  )
)
```

7. "장애 조치(failover)" 탭을 클릭합니다.

장애 조치 설정이 표시됩니다.

8. "대체 서버" 필드에 해당 환경의 나머지 Oracle RAC 노드에 대한 호스트 이름 또는 가상 IP 주소, 포트 번호 및 서비스 이름을 지정합니다.

참고: ServiceName 은 전체 Oracle RAC 시스템의 서비스 이름입니다.

9. 기본 서버에서 연결을 허용하지 않을 경우 다른 Oracle 노드에 대한 연결 장애 조치를 제공하는 대체 서버를 지정합니다. 다음과 같은 형식으로 입력해야 합니다.

(HostName=nete_servername2:PortNumber=1521:ServiceName=nete_servicename[,...])

10. "부하 분산"을 선택합니다.

11. "확인"을 클릭합니다.

Oracle RAC 데이터 원본이 유선 프로토콜 드라이버에 대해 구성됩니다.

Windows 에서 Oracle RAC SCAN 데이터 원본 만들기

SCAN 기능을 사용하는 Oracle RAC 데이터베이스에 대해 ODBC 데이터 원본을 만듭니다.

다음 단계를 수행하십시오.

1. 다음 작업 중 하나를 수행하십시오.

- 지원되는 32 비트 Windows 운영 체제를 사용 중인 경우 "시작"을 클릭하고 "프로그램", "관리 도구", "ODBC 데이터 원본"을 차례로 선택합니다.
- 지원되는 64 비트 Windows 운영 체제를 사용 중인 경우 다음을 수행합니다.

a. C:\Windows\SysWOW64 로 이동합니다.

b. odbcad32.exe 를 두 번 클릭합니다.

"ODBC 데이터 원본 관리자"가 표시됩니다.

2. "시스템 DSN" 탭을 클릭하고 "추가"를 클릭합니다.

"새 데이터 원본 만들기" 대화 상자가 표시됩니다.

3. "CA SiteMinder Oracle Wire Protocol"을 선택하고 "마침"을 클릭합니다.

"ODBC Oracle Wire Protocol Driver 설정" 대화 상자가 표시됩니다. "일반" 탭이 선택되어 있습니다.

4. "데이터 원본 이름" 필드에 데이터 원본을 식별할 수 있는 이름을 입력합니다.

참고: 이 이름을 기록해 두십시오. 정책 서버를 데이터베이스에 연결할 때 이 데이터 원본 이름이 필요합니다.

5. SCAN 의 FQDN 또는 IP 주소를 "호스트" 필드에 입력합니다.
6. SCAN 의 포트 번호를 "포트 번호" 필드에 입력합니다.
7. "서비스 이름" 필드에 전체 Oracle RAC 시스템의 서비스 이름을 입력합니다.

예: 다음 tnsnames.ora 파일에서 SMDB 값은 SCAN 기능이 포함된 전체 Oracle RAC 시스템의 서비스 이름입니다.

```
SMDB =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = clus-scan.rac.com)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = ORCL)
    )
  )
```

8. "확인"을 클릭합니다.

Oracle RAC 데이터 원본이 유선 프로토콜 드라이버에 대해 구성됩니다.

UNIX 시스템에서 Oracle 데이터 원본 만들기

사용할 수 있는 ODBC 데이터 원본의 이름과 이러한 데이터 원본에 연결된 특성을 system_odbc.ini 파일에 구성할 수 있습니다.

system_odbc.ini 파일을 만들려면

1. *policy_server_installation/db* 로 이동합니다.
2. oraclewire.ini 의 이름을 "system_odbc.ini"로 변경합니다.

각 사이트에 대해 system_odbc.ini 파일을 사용자 지정합니다. 또한 SiteMinder 에 대한 추가 ODBC 사용자 디렉터리를 정의하는 등 이 파일에 데이터 원본을 더 추가할 수도 있습니다.

system_odbc.ini 파일의 첫 번째 섹션인 [ODBC Data Sources]에는 현재 사용할 수 있는 모든 데이터 원본의 목록이 들어 있습니다. "=" 앞의 이름은 해당 파일에서 각 개별 데이터 원본을 설명하는 이후 섹션을 나타냅니다. "=" 뒷부분은 주석 필드입니다.

참고: 데이터 원본 항목의 첫 행([SiteMinder Data Source])을 수정할 경우 변경 내용을 적어 두십시오. 이 값은 ODBC 데이터베이스를 정책 저장소로 구성할 때 필요합니다.

system_odbc.ini 파일에는 각 데이터 원본의 특성을 설명하는 섹션이 있습니다. 첫 번째 특성은 SiteMinder 가 해당 데이터 원본을 사용할 때 로드되는 ODBC 드라이버입니다. 나머지 특성은 드라이버마다 다릅니다.

Oracle 데이터 원본을 추가하려면

1. 파일의 [ODBC Data Sources] 섹션에 새 데이터 원본 이름을 정의합니다.
2. 데이터 원본과 동일한 이름을 사용하여 데이터 원본을 설명하는 섹션을 추가합니다.

서비스 이름을 생성하거나 다른 드라이버를 사용하려는 경우에는 system_odbc.ini 파일을 편집합니다. SQL Server 또는 Oracle 드라이버에 대한 항목은 [SiteMinder Data Source] 아래에 위치합니다.

Oracle 유선 프로토콜 드라이버 구성

유선 프로토콜 드라이버를 구성하여 SiteMinder 가 데이터베이스에 연결하는 데 사용할 설정을 지정할 수 있습니다.

참고: 이 절차는 정책 서버가 UNIX 시스템에 설치된 경우에만 적용됩니다. 아직 수행하지 않은 경우 아래의 파일 중 하나를 복사하고 이름을 system_odbc.ini 로 바꾸십시오. 이름을 바꾸는 파일은 SiteMinder 데이터 저장소로 구성하는 데이터베이스 공급업체에 따라 다릅니다.

- sqlserverwire.ini
- oraclewire.ini
- mysqlwire.ini
- postgresqlwire.ini

이러한 파일은 *siteminder_home/db* 에 있습니다.

system_odbc.ini 파일은 다음 섹션으로 구성되어 있습니다. 구성하는 데이터 원본에 따라 편집할 섹션이 결정됩니다.

[SiteMinder Data Source]

SiteMinder 가 정책 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SiteMinder Logs Data Source]

SiteMinder 가 감사 로그 데이터베이스로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SiteMinder Keys Data Source]

SiteMinder 가 키 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SiteMinder Session Data Source]

SiteMinder 가 세션 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SmSampleUsers Data Source]

SiteMinder 가 샘플 사용자 데이터 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

다음 단계를 수행하십시오.

1. system_odbc.ini 파일을 엽니다.
2. 구성하려는 데이터 원본에 따라 다음 정보를 사용하여 해당 데이터 원본 섹션을 편집합니다.

```
Driver=nete_ps_root/odbc/lib/NSora27.so
Description=DataDirect 7.1 Oracle Wire Protocol
LoginID=uid
Password=pwd
HostName=nete_servername
PortNumber=1521
SID=nete_serverid
CatalogOptions=0
ProcedureResults=0
EnableDisableParam=0
EnableStaticCursorsForLongData=0
ApplicationUsingThreads=1
```

참고: 데이터 원본 정보를 편집할 때 파운드 기호(#)는 사용하지 마십시오. 파운드 기호를 입력하면 정보가 주석으로 처리되어 값이 잘립니다. 값이 잘리면 ODBC 연결이 실패할 수 있습니다.

nete_ps_root

정책 서버 설치의 명시적 경로를 지정합니다.

uid

데이터베이스에 대한 모든 액세스 권한을 가진 데이터베이스 계정의 사용자 이름을 지정합니다.

pwd

데이터베이스에 대한 모든 액세스 권한을 가진 데이터베이스 계정의 암호를 지정합니다.

nete_servername

Oracle 데이터베이스 호스트 시스템의 이름을 지정합니다.

nete_serverid

Oracle 인스턴스 서비스 이름(SID)을 지정합니다. SID 는 데이터베이스 인스턴스의 시스템 식별자입니다.

예: 다음 샘플 tnsnames.ora 파일에서 instance1 값이 SID 입니다.

```
instance1 =  
(Description =  
(ADDRESS = (Protocol = TCP)(Host = myhost)(Port = 1521)  
(CONNECT_DATA = (SID = instance1))  
)
```

3. 파일을 저장합니다.

Oracle 유선 프로토콜 드라이버가 구성됩니다.

SCAN 을 사용하지 않는 Oracle RAC 용 Oracle 유선 프로토콜 드라이버 구성

유선 프로토콜 드라이버를 구성하여 SiteMinder 가 데이터베이스에 연결하는 데 사용할 설정을 지정할 수 있습니다.

참고: 이 절차는 정책 서버가 UNIX 시스템에 설치된 경우에만 적용됩니다. 아직 수행하지 않은 경우 아래의 파일 중 하나를 복사하고 이름을 `system_odbc.ini` 로 바꾸십시오. 이름을 바꾸는 파일은 SiteMinder 데이터 저장소로 구성하는 데이터베이스 공급업체에 따라 다릅니다.

- `sqlserverwire.ini`
- `oraclewire.ini`
- `mysqlwire.ini`
- `postgresqlwire.ini`

이러한 파일은 `siteminder_home/db` 에 있습니다.

`system_odbc.ini` 파일은 다음 섹션으로 구성되어 있습니다. 구성하는 데이터 원본에 따라 편집할 섹션이 결정됩니다.

[SiteMinder Data Source]

SiteMinder 가 정책 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SiteMinder Logs Data Source]

SiteMinder 가 감사 로그 데이터베이스로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SiteMinder Keys Data Source]

SiteMinder 가 키 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SiteMinder Session Data Source]

SiteMinder 가 세션 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

[SmSampleUsers Data Source]

SiteMinder 가 샘플 사용자 데이터 저장소로 작동하는 데이터베이스에 연결하는 데 사용할 설정을 지정합니다.

다음 단계를 수행하십시오.

1. system_odbc.ini 파일을 엽니다.
2. 구성하려는 데이터 원본에 따라 다음 정보를 사용하여 해당 데이터 원본 섹션을 편집합니다.

- ServiceName=*nete_servicename* 추가
- AlternateServers= 추가
- Loadbalancing=1 추가
- SID=*nete_serverid* 제거 또는 주석 처리

데이터 원본의 수정된 내용은 다음과 같이 표시되어야 합니다.

```
Driver=nete_ps_root/odbc/lib/NSora27.so
Description=DataDirect 7.1 Oracle Wire Protocol
Logon=uid
Password=pwd
HostName=nete_servername1
PortNumber=1521
ServiceName=nete_servicename
CatalogOptions=0
ProcedureRetResults=0
EnableDescribeParam=0
EnableStaticCursorsForLongData=0
ApplicationUsingThreads=1
AlternateServers=
LoadBalancing=1
```

참고: 데이터 원본 정보를 편집할 때 파운드 기호(#)는 사용하지 마십시오. 파운드 기호를 입력하면 정보가 주석으로 처리되어 값이 잘립니다. 값이 잘리면 ODBC 연결이 실패할 수 있습니다.

nete_ps_root

정책 서버가 설치된 디렉터리의 명시적 경로를 지정합니다.

uid

데이터베이스에 대한 모든 액세스 권한을 가진 데이터베이스 계정의 사용자 이름을 지정합니다.

pwd

데이터베이스에 대한 모든 액세스 권한을 가진 데이터베이스 계정의 암호를 지정합니다.

nete_servername1

첫 번째 Oracle RAC 노드의 IP 주소를 지정합니다.

(Oracle 10g) 첫 번째 Oracle RAC 노드의 가상 IP 주소를 지정합니다.

nete_servicename

전체 RAC 시스템에 대한 Oracle RAC 시스템 서비스 이름을 지정합니다.

AlternateServers=

기본 서버에서 연결을 허용하지 않을 경우 다른 Oracle 노드에 대한 연결 장애 조치를 지정합니다.

예:

(HostName=nete_servername2:PortNumber=1521:ServiceName=nete_servicename[,...])

LoadBalancing=1

새로운 연결을 분산하여 RAC 노드에서 연결 요청 부하가 발생하지 않도록 하는 데 유용한 클라이언트 부하 분산을 설정합니다. 설정할 경우 액세스되는 기본 및 대체 데이터베이스 서버의 순서가 임의로 결정됩니다.

3. 파일을 저장합니다.

Oracle 유선 프로토콜 드라이버가 구성됩니다.

정책 서버를 데이터베이스에 연결

정책 서버가 정책 저장소의 SiteMinder 데이터에 액세스할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.
2. "저장소" 목록에서 다음 값을 선택합니다.

ODBC

3. "데이터베이스" 목록에서 다음 값을 선택합니다.

정책 저장소

4. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.
 - (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
 - (UNIX) 입력하는 이름은 `system_odbc.ini` 파일의 데이터 원본 항목 첫 줄과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 [SiteMinder Data Sources]입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.
5. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.
6. SiteMinder 에 할당되는 최대 데이터베이스 연결 수를 지정합니다.
참고: 최상의 성능을 위해서는 기본 연결 수인 25 를 유지하는 것이 좋습니다.
7. "적용"을 클릭하여 설정을 저장합니다.
8. "데이터베이스" 목록에서 다음 값을 선택합니다.
키 저장소
9. "저장소" 목록에서 다음 값을 선택합니다.
ODBC
10. 다음 옵션을 선택합니다.
정책 저장소 데이터베이스 사용
11. "데이터베이스" 목록에서 다음 값을 선택합니다.
감사 로그
12. "저장소" 목록에서 다음 값을 선택합니다.
ODBC
13. 다음 옵션을 선택합니다.
정책 저장소 데이터베이스 사용
14. "적용"을 클릭하여 설정을 저장합니다.
15. (선택 사항) "연결 테스트"를 클릭하여 정책 서버가 정책 저장소에 액세스할 수 있는지 확인합니다.
16. "확인"을 클릭합니다.
데이터베이스를 정책 저장소, 키 저장소 및 로깅 데이터베이스로 사용하도록 정책 서버가 구성되었습니다.

SiteMinder 슈퍼 사용자 암호 설정

기본 SiteMinder 관리자 계정의 이름은 다음으로 지정됩니다.

siteminder

이 계정에는 최대 권한이 있습니다.

일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다. 다음과 같은 경우에 기본 슈퍼 사용자를 사용합니다.

- 관리 UI에 처음 액세스할 경우
- SiteMinder 유틸리티를 처음 관리할 경우
- 슈퍼 사용자 권한이 있는 다른 관리자를 생성할 경우

다음 단계를 수행하십시오.

1. smreg 유틸리티를 *siteminder_home\bin*에 복사합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

참고: 이 유틸리티는 정책 서버 설치 키트의 최상위 수준에 있습니다.

2. 다음 명령을 실행합니다.

smreg -su password

password

기본 SiteMinder 관리자의 암호를 지정합니다.

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: Oracle 정책 저장소를 구성하는 경우 암호의 대/소문자를 구분합니다. 다른 모든 정책 저장소에서는 암호의 대/소문자를 구분하지 않습니다.

3. *siteminder_home\bin*에서 smreg를 삭제합니다. smreg를 삭제하면 이전 암호를 모르는 다른 사람은 암호를 변경할 수 없게 됩니다.

기본 SiteMinder 관리자 계정의 암호가 설정되었습니다.

정책 저장소 데이터 정의 가져오기

정책 저장소 데이터 정의 가져오기를 사용하여 정책 저장소에서 생성하고 저장할 수 있는 개체의 유형을 정의합니다.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home*\xps\dd 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

XPSDDInstall SmMaster.xdd

XPSDDInstall

필수 데이터 정의를 가져옵니다.

기본 정책 저장소 개체 가져오기

기본 정책 저장소 개체 가져오기를 사용하여 관리 UI 및 정책 서버에서 사용할 정책 저장소를 구성합니다.

다음 사항을 고려하십시오.

- *siteminder_home*\bin 에 대한 쓰기 액세스 권한이 있는지 확인하십시오. 가져오기 유틸리티에서 정책 저장소 개체를 가져오려면 이 권한이 필요합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

- Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 `siteminder_home\db` 로 이동합니다.

2. 다음 파일 중 하나를 가져옵니다.

- `smpolicy.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy.xml -npass
```

- `smpolicy-secure.xml` 을 가져오려면 다음 명령을 실행합니다.

```
XPSImport smpolicy-secure.xml -npass
```

npass

암호를 사용할 필요가 없음을 지정합니다. 기본 정책 저장소 개체에 암호화된 데이터가 포함되지 않습니다.

두 파일 모두 기본 정책 저장소 개체를 포함합니다. 이러한 개체는 기본 ACO(에이전트 구성 개체) 템플릿의 기본 보안 설정을 포함합니다. `smpolicy-secure` 파일은 보다 제한적인 보안 설정을 제공합니다. 자세한 내용은 [기본 정책 저장소 개체 고려 사항](#) (페이지 98)을 참조하십시오.

- 옵션 팩 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport ampolicy.xml -npass
```

- 페더레이션 기능을 가져오려면 다음 명령을 실행합니다.

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

정책 저장소 개체를 가져왔습니다.

참고: `smpolicy.xml` 을 가져오면 SiteMinder 에서 별도로 라이선스가 제공되는 레거시 페더레이션 및 웹 서비스 변수 기능을 사용할 수 있게 됩니다. 웹 서비스 변수 기능을 사용하려면 CA 고객 담당자에게 라이선스 정보에 대해 문의하십시오.

고급 인증 서버를 사용하도록 설정

정책 서버를 구성하는 과정에서 고급 인증 서버를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 구성 마법사를 시작합니다.
2. 마법사의 첫 번째 화면에서 모든 확인란을 **선택 취소**한 상태로 둡니다.
3. "다음"을 클릭합니다.
4. 고급 인증 서버에 대한 마스터 암호화 키를 생성합니다.

참고: 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

5. 정책 서버 구성 마법사의 나머지 과정을 완료합니다.
고급 인증 서버가 사용되도록 설정되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 **stop-all** 명령 다음에 **start-all** 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

관리 UI 등록 준비

기본 SiteMinder 슈퍼 사용자 계정(siteminder)을 사용하여 관리 UI에 최초로 로그인합니다. 최초 로그인 시 관리 UI를 정책 서버에 등록하여 두 구성 요소 간에 트러스트 관계를 생성해야 합니다.

등록을 준비하려면 XPSRegClient 유틸리티를 사용하여 슈퍼 사용자 계정 이름과 암호를 제공합니다. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 트러스트 관계를 설정할 수 있는지 확인합니다.

다음 사항을 고려하십시오.

- 자격 증명을 제공한 때부터 24 시간 이내에 최초 관리 UI 로그인이 이루어져야 합니다. 관리 UI 설치를 하루 안에 수행할 계획이 아니면 관리 UI를 설치하기 전에 다음 단계를 완료하십시오.
- (UNIX) XPSRegClient를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

기본 SiteMinder 슈퍼 사용자 계정(siteminder)의 암호를 지정합니다.

참고: 암호를 지정하지 않으면 XPSRegClient에서 암호를 입력하고 확인하라는 메시지가 표시됩니다.

-adminui-setup

관리 UI가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 관리 UI 를 설치할 때부터 정책 서버에 로그인하고 정책 서버와의 트러스트 관계를 생성할 때까지 할당된 시간을 지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록 요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 15

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI 를 등록할 때 허용되는 시도 실패 횟수를 지정합니다. 관리 UI 에 최초로 로그인할 때 올바르게 않은 SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수 있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을 삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error_path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: stderr

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

XPSRegClient 가 정책 서버에 관리자 자격 증명을 제공합니다. 정책 서버에서는 관리 UI에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

IBM DB2 정책 저장소 구성

단일 IBM DB2 데이터베이스가 다음 기능을 수행할 수 있습니다.

- 정책 저장소
- 키 저장소
- 로깅 데이터베이스

참고: SiteMinder 세션 정보를 별도의 데이터베이스에 저장하십시오. 정책 저장소를 사용하여 세션 정보를 저장하지 마십시오.

단일 데이터베이스를 사용하면 관리 태스크를 간소화할 수 있습니다. 다음 단원에서는 SiteMinder 데이터를 저장할 단일 데이터베이스 서버를 구성하는 방법에 대한 지침을 제공합니다.

데이터베이스 정보 수집

단일 IBM DB2 데이터베이스를 정책 저장소 또는 다른 유형의 SiteMinder 데이터 저장소로 작동하도록 구성하려면 특정 데이터베이스 정보가 필요합니다.

다음 사항을 고려하십시오.

- W 접두사가 붙은 정보는 Windows 요구 사항을 나타냅니다.
- U 접두사가 붙은 정보는 UNIX 요구 사항을 나타냅니다.

정책 저장소나 다른 유형의 SiteMinder 데이터 저장소를 구성하기 전에 다음 정보를 수집하십시오. IBM DB2 정보 워크시트를 사용하여 값을 기록할 수 있습니다.

- **데이터베이스 인스턴스 이름** - 정책 저장소 또는 데이터 저장소로 사용할 데이터베이스 인스턴스의 이름을 확인합니다.
- **관리 계정** - 데이터베이스의 개체에 대한 생성, 읽기, 수정 및 삭제 권한이 있는 계정의 사용자 이름을 확인합니다.
- **관리 암호** - 관리 계정의 암호를 확인합니다.
- **IP 주소** - 데이터베이스 호스트 시스템의 IP 주소를 확인합니다.
- **Tcp 포트** - 데이터베이스가 수신 대기하는 포트를 확인합니다.
- **(W) 데이터 원본 이름** - 데이터베이스 원본을 식별할 이름을 확인합니다.
- **(U) 정책 서버 루트** - 정책 서버가 설치된 위치의 명시적 경로를 확인합니다.
- **(U) 패키지** - 동적 SQL 을 처리할 패키지의 이름을 확인합니다.
- **(U) 패키지 소유자** - 패키지에 할당된 AuthID 를 확인합니다. AuthID 는 패키지의 모든 SQL 을 실행할 권한이 있어야 합니다.
- **(U) 권한 부여 AuthID** - 패키지에 대한 실행 권한을 제한하려면 패키지에 대한 실행 권한이 부여된 AuthID 를 확인합니다.

기본 유선 프로토콜 설정: 공용

- **(U) 격리 수준** - 시스템에서 잠금을 획득하고 해제하는 방법을 확인합니다.

기본 유선 프로토콜 설정: CURSOR_STABILITY

- (U) 동적 섹션 - 유선 프로토콜 드라이버 패키지에서 단일 사용자에게 대해 준비할 수 있는 섹션의 수를 확인합니다.

기본 유선 프로토콜 설정: 100

정책 저장소를 구성하는 방법

IBM DB2 데이터베이스를 정책 저장소, 키 저장소 및 로깅 데이터베이스로 구성하려면 다음 절차를 완료하십시오.

참고: 시작하기 전에 필수 데이터베이스 정보를 수집했는지 확인하십시오. 아래 단계 중 일부에서 이 정보가 필요합니다.

1. SiteMinder 데이터를 포함하는 IBM DB2 데이터베이스 인스턴스를 정책 서버 시스템에서 액세스할 수 있는지 확인합니다.
2. 다음의 데이터베이스 인스턴스 설정을 확인합니다.
 - 정책 저장소만 구성할 경우 테이블스페이스 페이지 크기(`page_size`) 및 버퍼 풀 페이지 크기 설정을 각각 16,000 이상으로 설정해야 합니다.
 SiteMinder 정책 저장소 스키마에는 각 설정의 기본 DB2 값이 충분하지 않습니다.
 - 정책 저장소 및 감사 저장소를 구성할 경우 테이블스페이스 페이지 크기(`page_size`) 및 버퍼 풀 페이지 크기 설정을 각각 32,000 이상으로 설정해야 합니다.
 SiteMinder 정책 저장소 및 감사 저장소 스키마에는 각 설정의 기본 DB2 값이 충분하지 않습니다.
3. SiteMinder 스키마를 생성합니다.
4. SiteMinder 에 대한 DB2 데이터 원본을 구성합니다.
5. 정책 서버를 데이터베이스에 연결합니다.
6. SiteMinder 슈퍼 사용자 암호를 설정합니다.
7. 정책 저장소 데이터 정의를 가져옵니다.
8. 기본 정책 저장소 개체를 가져옵니다.
9. 정책 서버를 다시 시작합니다.
10. 관리 UI 등록을 준비합니다.

SiteMinder 스키마 만들기

다음 단계를 수행하십시오.

1. `siteminder_home\db\tier2\DB2` 로 이동합니다.

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

2. 텍스트 편집기에서 다음 파일을 열고 전체 파일의 내용을 복사합니다.

`sm_db2_ps.sql`

DB2 데이터베이스의 정책 또는 키 저장소에 대한 스키마를 지정합니다.

3. 파일 내용을 쿼리에 붙여 넣고 쿼리를 실행합니다.

정책 및 키 저장소 스키마가 DB2 데이터베이스에 생성됩니다.

4. (선택 사항) 2~3 단계를 반복하여 DB2 데이터베이스에 감사 로그 또는 샘플 사용자 스키마를 생성합니다.

`sm_db2_logs.sql`

DB2 데이터베이스의 감사 로그 저장소에 대한 스키마를 지정합니다.
12.52 SP1 의 경우 감사 저장소를 만들기 전에 [이 스크립트를 편집](#)
(페이지 413)하십시오.

`smsampleusers_db2.sql`

DB2 데이터베이스의 샘플 사용자에 대한 스키마를 지정하고
데이터베이스를 샘플 사용자로 채웁니다.

해당 SiteMinder 스키마가 DB2 데이터베이스에 생성됩니다.

참고: 정책 저장소를 사용하여 키, 감사 및 샘플 사용자를 저장하는 것은 선택 사항입니다. 별도의 데이터베이스를 사용하여 이러한 유형의 SiteMinder 데이터 저장소로 각각 작동하도록 할 수 있습니다.

5. 다음 스키마 파일을 DB2 호스트 시스템에 복사합니다.

`siteminder_home\xps\db\DB2.sql`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

6. 명령 프롬프트를 열고 다음 명령을 실행합니다.

```
db2 -td@ [-v] -f path\DB2.sql
```

path

DB2 스키마 파일의 경로를 지정합니다.

정책 저장소 스키마가 생성되었습니다.

SiteMinder 에 대해 IBM DB2 데이터 원본 구성

ODBC 를 사용하는 경우 SiteMinder 가 SiteMinder 데이터 저장소와 통신할 수 있도록 데이터 원본을 구성합니다.

Windows 시스템에서 DB2 데이터 원본 만들기

ODBC 를 사용하는 경우 DB2 유선 프로토콜 드라이버에 대한 DB2 데이터 원본을 생성할 수 있습니다.

다음 단계를 수행하십시오.

1. 다음 단계 중 하나를 완료하십시오.

- 지원되는 32 비트 Windows 운영 체제를 사용 중인 경우 "시작"을 클릭하고 "프로그램", "관리 도구", "ODBC 데이터 원본"을 차례로 선택합니다.
- 지원되는 64 비트 Windows 운영 체제를 사용 중인 경우 다음을 수행합니다.
 - a. `install_home\Windows\SysWOW64` 로 이동합니다.
 - b. `odbcad32.exe` 를 두 번 클릭합니다.

"ODBC 데이터 원본 관리자"가 표시됩니다.

2. "시스템 DSN" 탭을 클릭하고 "추가"를 클릭합니다.
3. 아래로 스크롤하여 "SiteMinder DB2 Wire Protocol"을 선택하고 "마침"을 클릭합니다.

4. "ODBC DB2 Wire Protocol Driver 설정" 대화 상자의 "일반" 탭에서 다음 단계를 완료합니다.

- a. "데이터 원본 이름" 필드에 이름을 입력합니다.

예:

SiteMinder DB2 유선 데이터 원본

- b. (선택 사항) "설명" 필드에 DB2 유선 프로토콜 데이터 원본에 대한 설명을 입력합니다.
- c. "IP 주소" 필드에 DB2 데이터베이스가 설치된 IP 주소를 입력합니다.
- d. "TCP 포트" 필드에 DB2가 시스템에서 수신 대기하는 포트 번호를 입력합니다.
- e. "연결 테스트"를 클릭합니다.

연결이 테스트됩니다.

5. "확인"을 클릭합니다.

"ODBC DB2 Wire Protocol Driver 설정" 대화 상자가 닫히고, 선택 내용이 저장되고 DB2 데이터 원본이 Windows 시스템에 생성됩니다.

참고: 이제 생성한 데이터 원본을 사용하도록 SiteMinder를 구성할 수 있습니다.

UNIX 시스템에서 DB2 데이터 원본 만들기

SiteMinder ODBC 데이터 원본은 `system_odbc.ini` 파일을 사용하여 구성합니다. 이 파일은 `policy_server_home/db`에 있는 `db2wire.ini`를 `system_odbc.ini`로 이름을 바꿔 생성할 수 있습니다. 이 `system_odbc.ini` 파일에는 사용할 수 있는 ODBC 데이터 원본의 이름뿐 아니라 이러한 데이터 원본과 연관된 특성도 모두 들어 있습니다. 각 사이트에 맞게 이 파일을 사용자 지정해야 합니다. SiteMinder에 대한 추가 ODBC 사용자 디렉터리를 정의하는 등 이 파일에 데이터 원본을 더 추가할 수도 있습니다.

`system_odbc.ini` 파일의 첫 번째 섹션인 [ODBC Data Sources]에는 현재 사용할 수 있는 모든 데이터 원본의 목록이 들어 있습니다. "=" 앞의 이름은 해당 파일에서 각 개별 데이터 원본을 설명하는 이후 섹션을 나타냅니다. "=" 뒷부분은 주석 필드입니다.

`system_odbc.ini` 파일에는 각 데이터 원본의 특성을 설명하는 섹션이 있습니다. 첫 번째 특성은 해당 데이터 원본이 SiteMinder에서 사용될 때 로드되는 ODBC 드라이버입니다. 나머지 특성은 드라이버마다 다릅니다.

DB2 데이터 원본을 추가하려면 파일의 [ODBC Data Sources] 섹션에 새 데이터 원본 이름을 추가한 후 데이터 원본과 동일한 이름을 사용하여 데이터 원본을 설명하는 섹션을 추가해야 합니다. 새 서비스 이름을 생성하거나 다른 드라이버를 사용하려는 경우에는 `system_odbc.ini` 파일을 변경해야 합니다. [SiteMinder Data Source] 아래에 DB2 드라이버에 대한 항목을 추가해야 합니다.

또한 DB2 데이터 원본을 구성하려면 먼저 `policy_server_home/db` 디렉터리에 `system_odbc.ini` 파일을 생성해야 합니다. 이를 위해서는 `policy_server_home/db`에 있는 `db2wire.ini`를 `system_odbc.ini`로 이름을 바꿔야 합니다.

참고: `policy_server_home`은 정책 서버 설치 경로를 지정합니다.

DB2 유선 프로토콜 드라이버 구성

다음 표에서는 DB2 데이터 원본의 구성 매개 변수를 보여 줍니다. 이러한 매개 변수를 편집하여 데이터 원본에 대해 별도의 키, 감사 로그, 세션 및 샘플 사용자 데이터베이스를 구성할 수 있습니다.

매개 변수	설명	편집 방법
Data Source Name	데이터 원본의 이름입니다.	데이터 원본 이름을 대괄호로 묶어 입력합니다.
Driver	SiteMinder DB2 유선 프로토콜 드라이버의 전체 경로입니다.	"nete_ps_root"를 SiteMinder 설치 디렉터리로 바꿉니다.
설명	데이터 원본에 대한 설명입니다.	원하는 대로 설명을 입력합니다.
Database	DB2 UDB 데이터베이스의 이름입니다.	"nete_database"를 DB2 UDB 서버에 구성된 데이터베이스의 이름으로 바꿉니다.
LogonID	데이터베이스에 액세스하는 데 필요한 사용자 이름입니다.	"uid"를 DB2 UDB 관리자의 사용자 이름으로 바꿉니다.
Password	데이터베이스에 액세스하는 데 필요한 암호입니다.	"pwd"를 DB2 UDB 관리자의 암호로 바꿉니다.
IPAddress	DB2 UDB 서버의 IP 주소나 호스트 이름입니다.	"nete_server_ip"를 DB2 UDB 서버의 IP 주소나 호스트 이름으로 바꿉니다.

TcpPort	DB2 UDB 서버의 TCP 포트 번호입니다.	기본값 50000 을 DB2 UDB 서버의 실제 TCP 포트 번호로 바꿉니다.
Package	동적 SQL 을 처리할 패키지의 이름입니다.	"nete_package"를 생성하려는 패키지의 이름으로 바꿉니다.
PackageOwner	(선택 사항) 패키지에 할당된 AuthID 입니다.	기본적으로 비어 있습니다. 이 DB2 AuthID 에는 패키지의 모든 SQL 을 실행할 수 있는 권한이 있어야 합니다.
GrantAuthid	패키지에 대한 실행 권한이 부여된 AuthID 입니다.	기본적으로 "PUBLIC"입니다. 패키지에 대한 실행 권한을 제한하려는 경우 원하는 AuthID 를 지정합니다.
GrantExecute	GrantAuthid 에 나열된 AuthID 에 실행 권한을 부여할지 여부를 지정합니다.	1 또는 0 이 될 수 있습니다. 기본적으로 0 으로 설정됩니다.
IsolationLevel	시스템에서 잠금을 확보 및 해제하는 방법입니다.	기본값은 CURSOR_STABILITY 입니다.
DynamicSections	DB2 유선 프로토콜 드라이버 패키지가 단일 사용자에게 준비할 수 있는 문의 수입니다.	기본값은 100 입니다. 원하는 문 수를 입력합니다.

정책 서버를 데이터베이스에 연결

정책 서버가 정책 저장소의 SiteMinder 데이터에 액세스할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.
2. "저장소" 목록에서 다음 값을 선택합니다.
ODBC
3. "데이터베이스" 목록에서 다음 값을 선택합니다.
정책 저장소

4. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.
 - (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
 - (UNIX) 입력하는 이름은 `system_odbc.ini` 파일의 데이터 원본 항목 첫 줄과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 [SiteMinder Data Sources]입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.
5. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.
6. SiteMinder 에 할당되는 최대 데이터베이스 연결 수를 지정합니다.
참고: 최상의 성능을 위해서는 기본 연결 수인 25 를 유지하는 것이 좋습니다.
7. "적용"을 클릭하여 설정을 저장합니다.
8. "데이터베이스" 목록에서 다음 값을 선택합니다.
 키 저장소
9. "저장소" 목록에서 다음 값을 선택합니다.
 ODBC
10. 다음 옵션을 선택합니다.
 정책 저장소 데이터베이스 사용
11. "데이터베이스" 목록에서 다음 값을 선택합니다.
 감사 로그
12. "저장소" 목록에서 다음 값을 선택합니다.
 ODBC
13. 다음 옵션을 선택합니다.
 정책 저장소 데이터베이스 사용
14. "적용"을 클릭하여 설정을 저장합니다.
15. (선택 사항) "연결 테스트"를 클릭하여 정책 서버가 정책 저장소에 액세스할 수 있는지 확인합니다.
16. "확인"을 클릭합니다.
 데이터베이스를 정책 저장소, 키 저장소 및 로깅 데이터베이스로 사용하도록 정책 서버가 구성되었습니다.

SiteMinder 슈퍼 사용자 암호 설정

기본 SiteMinder 관리자 계정의 이름은 다음으로 지정됩니다.

`siteminder`

이 계정에는 최대 권한이 있습니다.

일상적인 작업에는 기본 슈퍼 사용자를 사용하지 않는 것이 좋습니다.
다음과 같은 경우에 기본 슈퍼 사용자를 사용합니다.

- 관리 UI에 처음 액세스할 경우
- SiteMinder 유틸리티를 처음 관리할 경우
- 슈퍼 사용자 권한이 있는 다른 관리자를 생성할 경우

다음 단계를 수행하십시오.

1. `smreg` 유틸리티를 `siteminder_home\bin`에 복사합니다.

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

참고: 이 유틸리티는 정책 서버 설치 키트의 최상위 수준에 있습니다.

2. 다음 명령을 실행합니다.

`smreg -su password`

`password`

기본 SiteMinder 관리자의 암호를 지정합니다.

제한:

- 암호는 적어도 6 자보다 길어야 하며 24 자를 넘을 수 없습니다.
- 암호에 앰퍼샌드(&)나 별표(*)를 사용할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

참고: Oracle 정책 저장소를 구성하는 경우 암호의 대/소문자를 구분합니다. 다른 모든 정책 저장소에서는 암호의 대/소문자를 구분하지 않습니다.

3. `siteminder_home\bin`에서 `smreg`를 삭제합니다. `smreg`를 삭제하면 이전 암호를 모르는 다른 사람은 암호를 변경할 수 없게 됩니다.

기본 SiteMinder 관리자 계정의 암호가 설정되었습니다.

정책 저장소 데이터 정의 가져오기

정책 저장소 데이터 정의 가져오기를 사용하여 정책 저장소에서 생성하고 저장할 수 있는 개체의 유형을 정의합니다.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home*\xps\dd 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

```
XPSDDInstall SmMaster.xdd
```

XPSDDInstall

필수 데이터 정의를 가져옵니다.

기본 정책 저장소 개체 가져오기

기본 정책 저장소 개체 가져오기를 사용하여 관리 UI 및 정책 서버에서 사용할 정책 저장소를 구성합니다.

다음 사항을 고려하십시오.

- *siteminder_home*\bin 에 대한 쓰기 액세스 권한이 있는지 확인하십시오. 가져오기 유틸리티에서 정책 저장소 개체를 가져오려면 이 권한이 필요합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

- Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 `siteminder_home\db` 로 이동합니다.
2. 다음 파일 중 하나를 가져옵니다.
 - `smpolicy.xml` 을 가져오려면 다음 명령을 실행합니다.
`XPSImport smpolicy.xml -npass`
 - `smpolicy-secure.xml` 을 가져오려면 다음 명령을 실행합니다.
`XPSImport smpolicy-secure.xml -npass`

npass

암호를 사용할 필요가 없음을 지정합니다. 기본 정책 저장소 개체에 암호화된 데이터가 포함되지 않습니다.

두 파일 모두 기본 정책 저장소 개체를 포함합니다. 이러한 개체는 기본 ACO(에이전트 구성 개체) 템플릿의 기본 보안 설정을 포함합니다. `smpolicy-secure` 파일은 보다 제한적인 보안 설정을 제공합니다. 자세한 내용은 [기본 정책 저장소 개체 고려 사항](#) (페이지 98)을 참조하십시오.

- 옵션 팩 기능을 가져오려면 다음 명령을 실행합니다.
`XPSImport ampolicy.xml -npass`
- 페더레이션 기능을 가져오려면 다음 명령을 실행합니다.
`XPSImport fedpolicy-12.52 SP1.xml -npass`

정책 저장소 개체를 가져왔습니다.

참고: `smpolicy.xml` 을 가져오면 SiteMinder 에서 별도로 라이선스가 제공되는 레거시 페더레이션 및 웹 서비스 변수 기능을 사용할 수 있게 됩니다. 웹 서비스 변수 기능을 사용하려면 CA 고객 담당자에게 라이선스 정보에 대해 문의하십시오.

고급 인증 서버를 사용하도록 설정

정책 서버를 구성하는 과정에서 고급 인증 서버를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 구성 마법사를 시작합니다.
2. 마법사의 첫 번째 화면에서 모든 확인란을 **선택 취소**한 상태로 둡니다.
3. "다음"을 클릭합니다.
4. 고급 인증 서버에 대한 마스터 암호화 키를 생성합니다.

참고: 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

5. 정책 서버 구성 마법사의 나머지 과정을 완료합니다.
고급 인증 서버가 사용되도록 설정되었습니다.

관리 UI 등록 준비

기본 SiteMinder 슈퍼 사용자 계정(siteminder)을 사용하여 관리 UI에 최초로 로그인합니다. 최초 로그인 시 관리 UI를 정책 서버에 등록하여 두 구성 요소 간에 트러스트 관계를 생성해야 합니다.

등록을 준비하려면 XPSRegClient 유틸리티를 사용하여 슈퍼 사용자 계정 이름과 암호를 제공합니다. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 트러스트 관계를 설정할 수 있는지 확인합니다.

다음 사항을 고려하십시오.

- 자격 증명을 제공한 때부터 **24 시간** 이내에 최초 관리 UI 로그인이 이루어져야 합니다. 관리 UI 설치를 하루 안에 수행할 계획이 아니면 관리 UI를 설치하기 전에 다음 단계를 완료하십시오.
- (UNIX) XPSRegClient를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c  
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

기본 SiteMinder 슈퍼 사용자 계정(siteminder)의 암호를 지정합니다.

참고: 암호를 지정하지 않으면 XPSRegClient 에서 암호를 입력하고
확인하라는 메시지가 표시됩니다.

-adminui-setup

관리 UI 가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 관리 UI 를 설치할 때부터 정책 서버에 로그인하고 정책
서버와의 트러스트 관계를 생성할 때까지 할당된 시간을
지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록
요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 15

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI 를 등록할 때 허용되는 시도 실패 횟수를
지정합니다. 관리 UI 에 최초로 로그인할 때 올바르게 않은
SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수
있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을
삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error_path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: `stderr`

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

XPSRegClient 가 정책 서버에 관리자 자격 증명을 제공합니다. 정책 서버에서는 관리 UI에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

IBM DB2 에서 세션 정보를 저장하는 방법

IBM DB2 데이터베이스를 세션 저장소로 구성하려면 다음 절차를 완료하십시오.

1. 필수 데이터베이스 정보를 수집했는지 확인합니다.
2. 세션 저장소 스키마를 생성합니다.
3. SiteMinder 에 대한 IBM DB2 데이터 원본을 구성합니다.
4. 정책 서버를 세션 저장소에 연결합니다.

추가 정보:

[데이터베이스 정보 수집](#) (페이지 386)

[SiteMinder 에 대해 IBM DB2 데이터 원본 구성](#) (페이지 389)

세션 저장소 스키마 만들기

IBM DB2 데이터베이스에서 세션 정보를 저장할 수 있도록 SiteMinder 스키마를 생성하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. `siteminder_home\db\tier2\DB2` 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

3. 다음 파일을 열고 내용을 텍스트 편집기에 복사합니다.

`sm_db2_ss.sql`

4. 내용을 쿼리에 붙여 넣고 쿼리를 실행합니다.

참고: 쿼리 실행에 대한 자세한 내용은 IBM 설명서를 참조하십시오.

세션 저장소 스키마가 데이터베이스에 추가됩니다.

정책 서버를 데이터베이스에 연결

정책 서버가 세션 정보를 읽고 저장할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

정책 서버를 데이터 저장소에 연결하려면

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.
데이터베이스 설정이 표시됩니다.
2. "데이터베이스" 목록에서 "세션 서버"를 선택합니다.
데이터 원본 설정이 활성화됩니다.
3. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.
 - (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
 - (UNIX) 입력하는 이름은 `system_odbc.ini` 파일의 데이터 원본 항목 첫 행과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 `[SiteMinder Data Sources]`입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.
4. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.
5. SiteMinder 에 할당되는 최대 데이터베이스 연결 수를 지정합니다.
참고: 최상의 성능을 위해서는 기본값을 유지하는 것이 좋습니다.
6. "적용"을 클릭합니다.
설정이 저장됩니다.
7. "연결 테스트"를 클릭합니다.
정책 서버가 데이터 저장소에 액세스할 수 있다는 확인 메시지가 표시됩니다.
8. "확인"을 클릭합니다.
정책 서버가 데이터베이스를 세션 저장소로 사용하도록 구성되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 `stop-all` 명령 다음에 `start-all` 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

MySQL 에 세션 정보를 저장하는 방법

MySQL 을 독립 실행형 세션 저장소로 구성하려면 다음 절차를 완료하십시오.

1. MySQL 이 기본 문자 집합(Latin1)을 사용하여 설치되어 있는지 확인합니다. MySQL 이 기본 문자 집합을 사용하여 설치되지 않은 경우 SiteMinder 데이터 저장소를 구성하기 전에 MySQL 을 다시 설치합니다.
2. 데이터베이스 정보를 수집합니다.
3. 세션 저장소 스키마를 생성합니다.
4. SiteMinder 에 대한 MySQL 데이터 원본을 구성합니다.
5. 정책 서버를 데이터베이스에 연결합니다.
6. 정책 서버를 다시 시작합니다.

추가 정보:

[데이터베이스 정보 수집](#) (페이지 311)

[SiteMinder 에 대한 MySQL 데이터 원본 구성](#) (페이지 313)

세션 저장소 스키마 만들기

MySQL 데이터베이스에서 세션 정보를 저장할 수 있도록 세션 저장소 스키마를 생성하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 위치로 이동합니다.

```
siteminder_home\db\tier2\MySQL
```

siteminder_home

정책 서버 설치 경로를 지정합니다.

3. 텍스트 편집기에서 다음 파일을 엽니다.

```
sm_mysql_ss.sql
```

4. 다음 행을 찾습니다.

```
DROP FUNCTION IF EXISTS `dbName`.`getdate` $$
CREATE FUNCTION `dbName`.`getdate` () RETURNS DATE
```

5. 'dbName'의 각 인스턴스를 세션 저장소로 작동하는 데이터베이스의 이름으로 바꿉니다.
6. 전체 파일의 내용을 복사합니다.
7. 파일 내용을 쿼리에 붙여 넣고 쿼리를 실행합니다.
세션 저장소 스키마가 생성됩니다.

정책 서버를 데이터베이스에 연결

정책 서버가 세션 정보를 읽고 저장할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

정책 서버를 데이터 저장소에 연결하려면

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.
데이터베이스 설정이 표시됩니다.
2. "데이터베이스" 목록에서 "세션 서버"를 선택합니다.
데이터 원본 설정이 활성화됩니다.

3. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.
 - (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
 - (UNIX) 입력하는 이름은 `system_odbc.ini` 파일의 데이터 원본 항목 첫 행과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 `[SiteMinder Data Sources]`입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.
4. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.
5. SiteMinder 에 할당되는 최대 데이터베이스 연결 수를 지정합니다.
참고: 최상의 성능을 위해서는 기본값을 유지하는 것이 좋습니다.
6. "적용"을 클릭합니다.
설정이 저장됩니다.
7. "연결 테스트"를 클릭합니다.
정책 서버가 데이터 저장소에 액세스할 수 있다는 확인 메시지가 표시됩니다.
8. "확인"을 클릭합니다.
정책 서버가 데이터베이스를 세션 저장소로 사용하도록 구성되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.
정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 `stop-all` 명령 다음에 `start-all` 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

Oracle 에서 세션 정보를 저장하는 방법

Oracle 데이터베이스를 세션 저장소로 구성하려면 다음 절차를 완료하십시오.

1. 데이터베이스 정보를 수집합니다.
2. 세션 저장소 스키마를 생성합니다.
3. SiteMinder 에 대한 Oracle 데이터 원본을 구성합니다.
4. 정책 서버를 데이터베이스에 연결합니다.
5. 정책 서버를 다시 시작합니다.

추가 정보:

[SiteMinder 에 대한 Oracle 데이터 원본 구성](#) (페이지 367)
[데이터베이스 정보 수집](#) (페이지 362)

세션 저장소 스키마 만들기

Oracle 데이터베이스에서 세션 정보를 저장할 수 있도록 세션 저장소 스키마를 생성하십시오.

다음 단계를 수행하십시오.

1. 데이터베이스 정보를 관리하는 사용자로 Oracle 에 로그인합니다.
sqlplus 와 같은 Oracle 유틸리티를 사용하여 로그인합니다.

참고: SYS 또는 SYSTEM 사용자로 스키마를 생성하지 않는 것이 좋습니다.
필요한 경우 SMOWNER 같은 Oracle 사용자를 생성한 후 해당 사용자로 스키마를 생성하십시오.

2. 유니코드 문자를 저장하려면 Oracle 데이터베이스의 문자 집합이 올바르게 설정되었는지 확인하십시오. 영어 문자만 사용하려면 이 단계를 건너뜁니다.

- a. 문자 집합을 찾으려면 다음 쿼리를 사용합니다.

```
SELECT value$ FROM sys.props$ WHERE name = 'NLS_CHARACTERSET' ;
```

- b. 스키마를 가져오기 전에 문자 집합이 AL32UTF8 또는 UTF8 인지 확인합니다.

3. 다음 스크립트를 가져옵니다.

```
$NETE_PS_ROOT/db/sql/sm_oracle_ss.sql
```

참고: 일부 Oracle SQL 유틸리티에는 환경 변수와 관련한 문제가 있습니다. 이 유틸리티를 사용하여 스크립트를 가져오는 동안 문제가 발생하면 명시적 경로를 지정하십시오.

4. 세션 저장소의 테이블스페이스를 생성하십시오.
5. 데이터베이스에서 테이블스페이스를 관리하기 위해 다음 권한이 있는 사용자를 만듭니다.

- 연결
- 리소스
- 제한 없는 테이블스페이스

정책 서버를 데이터베이스에 연결

정책 서버가 세션 정보를 읽고 저장할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

정책 서버를 데이터 저장소에 연결하려면

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.
데이터베이스 설정이 표시됩니다.
2. "데이터베이스" 목록에서 "세션 서버"를 선택합니다.
데이터 원본 설정이 활성화됩니다.

3. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.
 - (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
 - (UNIX) 입력하는 이름은 `system_odbc.ini` 파일의 데이터 원본 항목 첫 행과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 [SiteMinder Data Sources]입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.
4. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.
5. SiteMinder 에 할당되는 최대 데이터베이스 연결 수를 지정합니다.
참고: 최상의 성능을 위해서는 기본값을 유지하는 것이 좋습니다.
6. "적용"을 클릭합니다.
설정이 저장됩니다.
7. "연결 테스트"를 클릭합니다.
정책 서버가 데이터 저장소에 액세스할 수 있다는 확인 메시지가 표시됩니다.
8. "확인"을 클릭합니다.
정책 서버가 데이터베이스를 세션 저장소로 사용하도록 구성되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.
정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 `stop-all` 명령 다음에 `start-all` 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

SQL Server 에서 세션 정보를 저장하는 방법

SQL Server 데이터베이스를 독립 실행형 세션 저장소로 구성하려면 다음 절차를 완료하십시오.

1. 데이터베이스 정보를 수집합니다.
2. 세션 저장소 스키마를 생성합니다.
3. SiteMinder 에 대한 SQL Server 데이터 원본을 구성합니다.
4. 정책 서버를 데이터베이스에 연결합니다.
5. 정책 서버를 다시 시작합니다.

추가 정보:

[SiteMinder 에 대한 SQL Server 데이터 원본 구성](#) (페이지 330)
[데이터베이스 정보 수집](#) (페이지 327)

세션 저장소 스키마 만들기

SQL Server 데이터베이스에서 세션 정보를 저장하고 읽을 수 있도록 세션 저장소 스키마를 생성하십시오.

세션 저장소 스키마를 생성하려면

1. 다음 작업 중 하나를 수행하십시오.
 - 세션 저장소에 유니코드 문자를 저장하려는 경우 텍스트 편집기에서 `sm_mssql_ss.sql.unicode` 를 열고 전체 파일의 내용을 복사합니다.
 - 세션 저장소에 유니코드 문자를 저장하지 않으려는 경우 텍스트 편집기에서 `sm_mssql_ss.sql` 를 열고 전체 파일의 내용을 복사합니다.
2. 쿼리 분석기를 시작하고 정책 서버 데이터베이스 관리자로 로그인합니다.
3. 데이터베이스 목록에서 데이터베이스 인스턴스를 선택합니다.
4. 쿼리에 스키마를 붙여 넣습니다.
5. 쿼리를 실행합니다.
데이터베이스에 세션 저장소 스키마가 생성되었습니다.

정책 서버를 데이터베이스에 연결

정책 서버가 세션 정보를 읽고 저장할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

정책 서버를 데이터 저장소에 연결하려면

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.
데이터베이스 설정이 표시됩니다.
2. "데이터베이스" 목록에서 "세션 서버"를 선택합니다.
데이터 원본 설정이 활성화됩니다.
3. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.
 - (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
 - (UNIX) 입력하는 이름은 `system_odbc.ini` 파일의 데이터 원본 항목 첫 행과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 `[SiteMinder Data Sources]`입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.
4. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.
5. SiteMinder 에 할당되는 최대 데이터베이스 연결 수를 지정합니다.
참고: 최상의 성능을 위해서는 기본값을 유지하는 것이 좋습니다.
6. "적용"을 클릭합니다.
설정이 저장됩니다.
7. "연결 테스트"를 클릭합니다.
정책 서버가 데이터 저장소에 액세스할 수 있다는 확인 메시지가 표시됩니다.
8. "확인"을 클릭합니다.
정책 서버가 데이터베이스를 세션 저장소로 사용하도록 구성되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 `stop-all` 명령 다음에 `start-all` 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

PostgreSQL 에 세션 정보를 저장하는 방법

PostgreSQL Server 데이터베이스를 독립 실행형 세션 저장소로 구성하려면 다음 절차를 완료하십시오.

1. 데이터베이스 정보를 수집합니다.
2. 세션 저장소 스키마를 생성합니다.
3. SiteMinder 에 대한 PostgreSQL Server 데이터 원본을 구성합니다.
4. 정책 서버를 데이터베이스에 연결합니다.
5. 정책 서버를 다시 시작합니다.

세션 저장소 스키마 만들기

SQL Server 데이터베이스에서 세션 정보를 저장하고 읽을 수 있도록 세션 저장소 스키마를 생성하십시오.

세션 저장소 스키마를 생성하려면

1. 텍스트 편집기에서 `sm_postgresql_ss.sql` 을 열고 전체 파일의 내용을 복사합니다.

2. `psql` 과 같은 SQL 클라이언트를 사용하여 정책 서버 데이터베이스를 관리하는 사용자로 로그인합니다.
 3. 데이터베이스 목록에서 데이터베이스 인스턴스를 선택합니다.
 4. 쿼리에 스키마를 붙여 넣습니다.
 5. 쿼리를 실행합니다.
- 데이터베이스에 세션 저장소 스키마가 생성되었습니다.

정책 서버를 데이터베이스에 연결

정책 서버가 세션 정보를 읽고 저장할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

정책 서버를 데이터 저장소에 연결하려면

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.
데이터베이스 설정이 표시됩니다.
2. "데이터베이스" 목록에서 "세션 서버"를 선택합니다.
데이터 원본 설정이 활성화됩니다.
3. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.
 - (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
 - (UNIX) 입력하는 이름은 `system_odbc.ini` 파일의 데이터 원본 항목 첫 행과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 `[SiteMinder Data Sources]`입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.
4. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.
5. SiteMinder 에 할당되는 최대 데이터베이스 연결 수를 지정합니다.
참고: 최상의 성능을 위해서는 기본값을 유지하는 것이 좋습니다.
6. "적용"을 클릭합니다.
설정이 저장됩니다.

7. "연결 테스트"를 클릭합니다.

정책 서버가 데이터 저장소에 액세스할 수 있다는 확인 메시지가 표시됩니다.

8. "확인"을 클릭합니다.

정책 서버가 데이터베이스를 세션 저장소로 사용하도록 구성되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 **stop-all** 명령 다음에 **start-all** 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

IBM DB2 에서 감사 로그를 저장하는 방법

IBM DB2 데이터베이스를 감사 로그 저장소로 구성하려면 다음 절차를 완료하십시오.

1. 필수 데이터베이스 정보를 수집했는지 확인합니다.
2. 데이터베이스 인스턴스에 대한 테이블 공간 페이지 크기(**page_size**) 및 버퍼 풀 페이지 크기 설정을 각각 **16,000** 이상으로 설정해야 합니다.
SiteMinder 감사 로그 스키마에는 각 설정의 기본 DB2 값이 충분하지 않습니다.
3. 감사 저장소 스키마를 생성합니다.
4. SiteMinder 에 대한 IBM DB2 데이터 원본을 구성합니다.

5. 정책 서버를 감사 저장소에 연결합니다.
6. 정책 서버를 다시 시작합니다.

추가 정보:

[데이터베이스 정보 수집](#) (페이지 386)

[SiteMinder 에 대해 IBM DB2 데이터 원본 구성](#) (페이지 389)

감사 저장소 스키마 만들기

IBM DB2 데이터베이스에서 감사 로그를 저장할 수 있도록 SiteMinder 스키마를 생성하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. `siteminder_home\db\tier2\DB2` 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

3. 다음 파일을 열고 내용을 텍스트 편집기에 복사합니다.

`sm_db2_logs.sql`

4. 다음 줄에서 NULL 을 제거합니다.

```
sm_assertion_id          VARCHAR(255) NULL,
sm_assertion_issuerid    VARCHAR(255) NULL,
sm_assertion_destinationurl  VARCHAR(4096) NULL,
sm_assertion_statuscode  VARCHAR(255) NULL,
sm_assertion_NotOnBefore  TIMESTAMP,
sm_assertion_notonorafter  TIMESTAMP,
sm_assertion_sess_starttime  TIMESTAMP,
sm_assertion_sess_notonorafter  TIMESTAMP,
sm_assertion_authcontext  VARCHAR(255) NULL,
sm_assertion_versionid    VARCHAR(255) NULL,
sm_assertion_claims       VARCHAR(255) NULL,
sm_application_name       VARCHAR(255) NULL,
sm_tenant_name            VARCHAR(255) NULL,
sm_authentication_method  VARCHAR(255) NULL
```

5. 변경 내용을 파일에 저장합니다.
6. 내용을 쿼리에 붙여 넣고 쿼리를 실행합니다.

참고: 쿼리 실행에 대한 자세한 내용은 IBM 설명서를 참조하십시오.
감사 저장소 스키마가 데이터베이스에 추가됩니다.

정책 서버를 데이터베이스에 연결

정책 서버가 감사 로그를 읽고 저장할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

정책 서버를 데이터 저장소에 연결하려면

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.
데이터베이스 설정이 표시됩니다.
2. "저장소" 목록에서 "ODBC"를 선택합니다.
ODBC 설정이 표시됩니다.
3. "데이터베이스" 목록에서 "감사 로그"를 선택합니다.
4. "저장소" 목록에서 "ODBC"를 선택합니다.
데이터 원본 설정이 활성화됩니다.
5. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.
 - (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
 - (UNIX) 입력하는 이름은 `system_odbc.ini` 파일의 데이터 원본 항목 첫 행과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 [SiteMinder Data Sources]입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.
6. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.
7. SiteMinder 에 할당되는 최대 데이터베이스 연결 수를 지정합니다.
참고: 최상의 성능을 위해서는 기본값을 유지하는 것이 좋습니다.
8. "적용"을 클릭합니다.
설정이 저장됩니다.

9. "연결 테스트"를 클릭합니다.

정책 서버가 데이터 저장소에 액세스할 수 있다는 확인 메시지가 표시됩니다.

10. "확인"을 클릭합니다.

정책 서버가 데이터베이스를 감사 로깅 데이터베이스로 사용하도록 구성되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 **stop-all** 명령 다음에 **start-all** 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

MySQL 에서 감사 로그를 저장하는 방법

MySQL 을 독립 실행형 감사 로그 저장소로 구성하려면 다음 절차를 완료하십시오.

1. MySQL 이 기본 문자 집합(Latin1)을 사용하여 설치되어 있는지 확인합니다. MySQL 이 기본 문자 집합을 사용하여 설치되지 않은 경우 SiteMinder 데이터 저장소를 구성하기 전에 MySQL 을 다시 설치합니다.
2. 데이터베이스 정보를 수집합니다.
3. 감사 로그 스키마를 생성합니다.
4. SiteMinder 에 대한 MySQL 데이터 원본을 구성합니다.
5. 정책 서버를 데이터베이스에 연결합니다.
6. 정책 서버를 다시 시작합니다.

추가 정보:

[데이터베이스 정보 수집 \(페이지 311\)](#)

[SiteMinder에 대한 MySQL 데이터 원본 구성 \(페이지 313\)](#)

감사 로그 스키마 만들기

MySQL 데이터베이스에서 감사 로그를 저장할 수 있도록 감사 로그 스키마를 생성하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 위치로 이동합니다.

`siteminder_home\db\tier2\MySQL`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

3. 텍스트 편집기에서 다음 파일을 엽니다.

`sm_mysql_logs.sql`

4. 다음 행을 찾습니다.

```
DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$  
CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
```

5. 'databaseName'의 각 인스턴스를 감사 저장소로 작동하는 데이터베이스의 이름으로 바꿉니다.
6. 전체 파일의 내용을 복사합니다.
7. 파일 내용을 쿼리에 붙여 넣고 쿼리를 실행합니다.

감사 저장소 스키마가 생성됩니다.

정책 서버를 데이터베이스에 연결

정책 서버가 감사 로그를 읽고 저장할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

정책 서버를 데이터 저장소에 연결하려면

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.
데이터베이스 설정이 표시됩니다.
2. "저장소" 목록에서 "ODBC"를 선택합니다.
ODBC 설정이 표시됩니다.
3. "데이터베이스" 목록에서 "감사 로그"를 선택합니다.
4. "저장소" 목록에서 "ODBC"를 선택합니다.
데이터 원본 설정이 활성화됩니다.
5. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.
 - (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
 - (UNIX) 입력하는 이름은 `system_odbc.ini` 파일의 데이터 원본 항목 첫 행과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 [SiteMinder Data Sources]입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.
6. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.
7. SiteMinder 에 할당되는 최대 데이터베이스 연결 수를 지정합니다.
참고: 최상의 성능을 위해서는 기본값을 유지하는 것이 좋습니다.
8. "적용"을 클릭합니다.
설정이 저장됩니다.
9. "연결 테스트"를 클릭합니다.
정책 서버가 데이터 저장소에 액세스할 수 있다는 확인 메시지가 표시됩니다.
10. "확인"을 클릭합니다.
정책 서버가 데이터베이스를 감사 로깅 데이터베이스로 사용하도록 구성되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 `stop-all` 명령 다음에 `start-all` 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

Oracle 에서 감사 로그를 저장하는 방법

Oracle 데이터베이스를 감사 로그 저장소로 구성하려면 다음 절차를 완료하십시오.

1. 데이터베이스 정보를 수집합니다.
2. 감사 저장소 스키마를 생성합니다.
3. SiteMinder 에 대한 Oracle 데이터 원본을 구성합니다.
4. 정책 서버를 데이터베이스에 연결합니다.
5. 정책 서버를 다시 시작합니다.

추가 정보:

[SiteMinder 에 대한 Oracle 데이터 원본 구성](#) (페이지 367)
[데이터베이스 정보 수집](#) (페이지 362)

감사 로그 스키마 만들기

Oracle 데이터베이스에 감사 로그를 저장할 수 있도록 감사 로그 스키마를 생성하십시오.

다음 단계를 수행하십시오.

1. sqlplus 나 다른 Oracle 유틸리티를 사용하여 정책 서버 데이터베이스 정보를 관리하는 사용자로 Oracle 에 로그인합니다.

참고: SYS 또는 SYSTEM 사용자로 SiteMinder 스키마를 생성하지 않는 것이 좋습니다. 필요한 경우 SMOWNER 같은 Oracle 사용자를 생성한 후 해당 사용자로 스키마를 생성하십시오.

2. 다음 스크립트를 가져옵니다.

`$NETE_PS_ROOT/db/sql/sm_oracle_logs.sql`

참고: Oracle 의 SQL 유틸리티에서는 환경 변수가 작동하지 않을 수 있습니다. 이 유틸리티를 사용하여 스크립트를 가져오는 동안 문제가 발생하면 명시적 경로를 지정하십시오.

3. 감사 로그 스키마에 대한 테이블스페이스를 만듭니다.
4. 데이터베이스에서 테이블스페이스를 관리하기 위해 다음 권한이 있는 사용자를 만듭니다.
 - 연결
 - 리소스
 - 제한 없는 테이블스페이스

정책 서버를 데이터베이스에 연결

정책 서버가 감사 로그를 읽고 저장할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

정책 서버를 데이터 저장소에 연결하려면

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.
데이터베이스 설정이 표시됩니다.
2. "저장소" 목록에서 "ODBC"를 선택합니다.
ODBC 설정이 표시됩니다.

3. "데이터베이스" 목록에서 "감사 로그"를 선택합니다.
4. "저장소" 목록에서 "ODBC"를 선택합니다.
데이터 원본 설정이 활성화됩니다.
5. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.
 - (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
 - (UNIX) 입력하는 이름은 `system_odbc.ini` 파일의 데이터 원본 항목 첫 행과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 [SiteMinder Data Sources]입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.
6. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.
7. SiteMinder 에 할당되는 최대 데이터베이스 연결 수를 지정합니다.
참고: 최상의 성능을 위해서는 기본값을 유지하는 것이 좋습니다.
8. "적용"을 클릭합니다.
설정이 저장됩니다.
9. "연결 테스트"를 클릭합니다.
정책 서버가 데이터 저장소에 액세스할 수 있다는 확인 메시지가 표시됩니다.
10. "확인"을 클릭합니다.
정책 서버가 데이터베이스를 감사 로깅 데이터베이스로 사용하도록 구성되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 `stop-all` 명령 다음에 `start-all` 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

SQL Server 에서 감사 로그를 저장하는 방법

SQL Server 데이터베이스를 독립 실행형 감사 로그 데이터베이스로 구성하려면 다음 절차를 완료하십시오.

1. 데이터베이스 정보를 수집합니다.
2. 감사 저장소 스키마를 생성합니다.
3. SiteMinder 에 대한 SQL Server 데이터 원본을 구성합니다.
4. 정책 서버를 데이터베이스에 연결합니다.
5. 정책 서버를 다시 시작합니다.

추가 정보:

[SiteMinder 에 대한 SQL Server 데이터 원본 구성](#) (페이지 330)
[데이터베이스 정보 수집](#) (페이지 327)

감사 로그 스키마 만들기

SQL Server 데이터베이스에 감사 로그를 저장할 수 있도록 로깅 스키마를 생성하십시오.

감사 로그 스키마를 생성하려면

1. 텍스트 편집기에서 `sm_mssql_logs.sql` 을 열고 전체 파일의 내용을 복사합니다.
2. 쿼리 분석기를 시작하고 정책 서버 데이터베이스를 관리하는 사용자로 로그인합니다.
3. 데이터베이스 목록에서 데이터베이스 인스턴스를 선택합니다.
4. `sm_mssql_logs.sql` 의 스키마를 쿼리에 붙여 넣습니다.
5. 쿼리를 실행합니다.

데이터베이스에 SiteMinder 감사 로그 저장소 스키마가 생성되었습니다.

정책 서버를 데이터베이스에 연결

정책 서버가 감사 로그를 읽고 저장할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

정책 서버를 데이터 저장소에 연결하려면

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.
데이터베이스 설정이 표시됩니다.
2. "저장소" 목록에서 "ODBC"를 선택합니다.
ODBC 설정이 표시됩니다.
3. "데이터베이스" 목록에서 "감사 로그"를 선택합니다.
4. "저장소" 목록에서 "ODBC"를 선택합니다.
데이터 원본 설정이 활성화됩니다.
5. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.
 - (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
 - (UNIX) 입력하는 이름은 `system_odbc.ini` 파일의 데이터 원본 항목 첫 행과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 [SiteMinder Data Sources]입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.
6. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.

7. SiteMinder 에 할당되는 최대 데이터베이스 연결 수를 지정합니다.

참고: 최상의 성능을 위해서는 기본값을 유지하는 것이 좋습니다.

8. "적용"을 클릭합니다.

설정이 저장됩니다.

9. "연결 테스트"를 클릭합니다.

정책 서버가 데이터 저장소에 액세스할 수 있다는 확인 메시지가 표시됩니다.

10. "확인"을 클릭합니다.

정책 서버가 데이터베이스를 감사 로깅 데이터베이스로 사용하도록 구성되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 `stop-all` 명령 다음에 `start-all` 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

PostgreSQL 에서 감사 로그를 저장하는 방법

PostgreSQL 데이터베이스를 독립 실행형 감사 로그 데이터베이스로 구성하려면 다음 절차를 완료하십시오.

1. 데이터베이스 정보를 수집합니다.
2. 감사 저장소 스키마를 생성합니다.
3. SiteMinder 에 대한 PostgreSQL Server 데이터 원본을 구성합니다.

4. 정책 서버를 데이터베이스에 연결합니다.
5. 정책 서버를 다시 시작합니다.

감사 로그 스키마 만들기

PostgreSQL Server 데이터베이스에 감사 로그를 저장할 수 있도록 로깅 스키마를 생성하십시오.

감사 로그 스키마를 생성하려면

1. 텍스트 편집기에서 `sm_postgresql_logs.sql` 을 열고 전체 파일의 내용을 복사합니다.
2. `psql` 과 같은 SQL 클라이언트를 시작하고 정책 서버 데이터베이스를 관리하는 사용자로 로그인합니다.
3. 데이터베이스 목록에서 데이터베이스 인스턴스를 선택합니다.
4. `sm_postgresql_logs.sql` 의 스키마를 쿼리에 붙여 넣습니다.
5. 쿼리를 실행합니다.

데이터베이스에 감사 로그 저장소 스키마가 생성되었습니다.

정책 서버를 데이터베이스에 연결

정책 서버가 감사 로그를 읽고 저장할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

정책 서버를 데이터 저장소에 연결하려면

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.
데이터베이스 설정이 표시됩니다.
2. "저장소" 목록에서 "ODBC"를 선택합니다.
ODBC 설정이 표시됩니다.

3. "데이터베이스" 목록에서 "감사 로그"를 선택합니다.
4. "저장소" 목록에서 "ODBC"를 선택합니다.
데이터 원본 설정이 활성화됩니다.
5. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.
 - (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
 - (UNIX) 입력하는 이름은 `system_odbc.ini` 파일의 데이터 원본 항목 첫 행과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 [SiteMinder Data Sources]입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.
6. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.
7. SiteMinder 에 할당되는 최대 데이터베이스 연결 수를 지정합니다.
참고: 최상의 성능을 위해서는 기본값을 유지하는 것이 좋습니다.
8. "적용"을 클릭합니다.
설정이 저장됩니다.
9. "연결 테스트"를 클릭합니다.
정책 서버가 데이터 저장소에 액세스할 수 있다는 확인 메시지가 표시됩니다.
10. "확인"을 클릭합니다.
정책 서버가 데이터베이스를 감사 로깅 데이터베이스로 사용하도록 구성되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 `stop-all` 명령 다음에 `start-all` 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

IBM DB2 에서 키 정보를 저장하는 방법

IBM DB2 데이터베이스를 독립 실행형 키 저장소로 구성하려면 다음 절차를 완료하십시오.

1. 데이터베이스 정보를 수집합니다.
2. 키 저장소 스키마를 생성합니다.
3. SiteMinder 에 대한 IBM DB2 데이터 원본을 구성합니다.
4. 정책 서버를 키 저장소에 연결합니다.
5. 정책 서버를 다시 시작합니다.

추가 정보:

[데이터베이스 정보 수집](#) (페이지 386)

[SiteMinder 에 대해 IBM DB2 데이터 원본 구성](#) (페이지 389)

키 저장소 스키마 만들기

IBM DB2 데이터베이스에서 키 정보를 저장할 수 있도록 SiteMinder 스키마를 생성하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. `siteminder_home\db\tier2\DB2` 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

3. 다음 파일을 열고 내용을 텍스트 편집기에 복사합니다.

`sm_db2_ps.sql`

4. 내용을 쿼리에 붙여 넣고 쿼리를 실행합니다.

참고: 쿼리 실행에 대한 자세한 내용은 IBM 설명서를 참조하십시오.

키 저장소 스키마가 데이터베이스에 추가됩니다.

정책 서버를 데이터베이스에 연결

정책 서버가 키 정보를 읽고 저장할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

정책 서버를 데이터 저장소에 연결하려면

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.
데이터베이스 설정이 표시됩니다.
2. "저장소" 목록에서 "ODBC"를 선택합니다.
ODBC 설정이 표시됩니다.
3. "데이터베이스" 목록에서 "키 저장소"를 선택하고 "정책 저장소 데이터베이스 사용" 확인란의 선택을 취소합니다.
데이터 원본 설정이 활성화됩니다.

4. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.
 - (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
 - (UNIX) 입력하는 이름은 `system_odbc.ini` 파일의 데이터 원본 항목 첫 행과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 `[SiteMinder Data Sources]`입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.
5. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.
6. SiteMinder 에 할당되는 최대 데이터베이스 연결 수를 지정합니다.
참고: 최상의 성능을 위해서는 기본값을 유지하는 것이 좋습니다.
7. "적용"을 클릭합니다.
설정이 저장됩니다.
8. "연결 테스트"를 클릭합니다.
정책 서버가 데이터 저장소에 액세스할 수 있다는 확인 메시지가 표시됩니다.
9. "확인"을 클릭합니다.
정책 서버가 데이터베이스를 키 저장소로 사용하도록 구성되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.
정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 `stop-all` 명령 다음에 `start-all` 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

MySQL 에서 키 정보를 저장하는 방법

MySQL 을 독립 실행형 키 저장소로 구성하려면 다음 절차를 완료하십시오.

1. MySQL 이 기본 문자 집합(Latin1)을 사용하여 설치되어 있는지 확인합니다. MySQL 이 기본 문자 집합을 사용하여 설치되지 않은 경우 SiteMinder 데이터 저장소를 구성하기 전에 MySQL 을 다시 설치합니다.
2. 데이터베이스 정보를 수집합니다.
3. 키 저장소 스키마를 생성합니다.
4. SiteMinder 에 대한 MySQL 데이터 원본을 구성합니다.
5. 정책 서버를 데이터베이스에 연결합니다.
6. 정책 서버를 다시 시작합니다.

추가 정보:

[데이터베이스 정보 수집](#) (페이지 311)

[SiteMinder 에 대한 MySQL 데이터 원본 구성](#) (페이지 313)

키 저장소 스키마 만들기

MySQL 데이터베이스에서 키 정보를 저장할 수 있도록 키 저장소 스키마를 생성하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 위치로 이동합니다.

```
siteminder_home\db\tier2\MySQL
```

siteminder_home

정책 서버 설치 경로를 지정합니다.

3. 텍스트 편집기에서 다음 파일을 엽니다.

```
sm_mysql_ps.sql
```

4. 다음 행을 찾습니다.

```
DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$
CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
```

5. 'databaseName'의 각 인스턴스를 키 저장소로 작동하는 데이터베이스의 이름으로 바꿉니다.
6. 전체 파일의 내용을 복사합니다.
7. 파일 내용을 쿼리에 붙여 넣고 쿼리를 실행합니다.
키 저장소 스키마가 생성되었습니다.

정책 서버를 데이터베이스에 연결

정책 서버가 키 정보를 읽고 저장할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

정책 서버를 데이터 저장소에 연결하려면

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.
데이터베이스 설정이 표시됩니다.
2. "저장소" 목록에서 "ODBC"를 선택합니다.
ODBC 설정이 표시됩니다.
3. "데이터베이스" 목록에서 "키 저장소"를 선택하고 "정책 저장소 데이터베이스 사용" 확인란의 선택을 취소합니다.
데이터 원본 설정이 활성화됩니다.
4. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.
 - (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
 - (UNIX) 입력하는 이름은 `system_odbc.ini` 파일의 데이터 원본 항목 첫 행과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 [SiteMinder Data Sources]입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.
5. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.
6. SiteMinder에 할당되는 최대 데이터베이스 연결 수를 지정합니다.
참고: 최상의 성능을 위해서는 기본값을 유지하는 것이 좋습니다.
7. "적용"을 클릭합니다.
설정이 저장됩니다.

8. "연결 테스트"를 클릭합니다.
정책 서버가 데이터 저장소에 액세스할 수 있다는 확인 메시지가 표시됩니다.
9. "확인"을 클릭합니다.
정책 서버가 데이터베이스를 키 저장소로 사용하도록 구성되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.
정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 `stop-all` 명령 다음에 `start-all` 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

Oracle 에서 키 정보를 저장하는 방법

Oracle 데이터베이스를 키 저장소로 구성하려면 다음 절차를 완료하십시오.

1. 데이터베이스 정보를 수집합니다.
2. 키 저장소 스키마를 생성합니다.
3. SiteMinder 에 대한 Oracle 데이터 원본을 구성합니다.
4. 정책 서버를 데이터베이스에 연결합니다.
5. 정책 서버를 다시 시작합니다.

추가 정보:

[SiteMinder 에 대한 Oracle 데이터 원본 구성](#) (페이지 367)
[데이터베이스 정보 수집](#) (페이지 362)

키 저장소 스키마 만들기

Oracle 데이터베이스에 키 정보를 저장할 수 있도록 키 저장소 스키마를 생성하십시오.

다음 단계를 수행하십시오.

1. sqlplus 나 다른 Oracle 유틸리티를 사용하여 정책 서버 데이터베이스 정보를 관리하는 사용자로 Oracle 에 로그인합니다.

참고: SYS 또는 SYSTEM 사용자로 SiteMinder 스키마를 생성하지 않는 것이 좋습니다. 필요한 경우 SMOWNER 같은 Oracle 사용자를 생성한 후 해당 사용자로 스키마를 생성하십시오.

2. 다음 스크립트를 가져옵니다.

```
$NETE_PS_ROOT/db/sql/sm_oracle_ps.sql
```

참고: Oracle 의 SQL 유틸리티에서는 환경 변수가 작동하지 않을 수 있습니다. 이 유틸리티를 사용하여 스크립트를 가져오는 동안 문제가 발생하면 명시적 경로를 지정하십시오.

3. 키 저장소의 테이블스페이스를 생성하십시오.
4. 데이터베이스에서 테이블스페이스를 관리하기 위해 다음 권한이 있는 사용자를 만듭니다.
 - 연결
 - 리소스
 - 제한 없는 테이블스페이스

정책 서버를 데이터베이스에 연결

정책 서버가 키 정보를 읽고 저장할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

정책 서버를 데이터 저장소에 연결하려면

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.
데이터베이스 설정이 표시됩니다.
2. "저장소" 목록에서 "ODBC"를 선택합니다.
ODBC 설정이 표시됩니다.

3. "데이터베이스" 목록에서 "키 저장소"를 선택하고 "정책 저장소 데이터베이스 사용" 확인란의 선택을 취소합니다.
데이터 원본 설정이 활성화됩니다.
4. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.
 - (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
 - (UNIX) 입력하는 이름은 `system_odbc.ini` 파일의 데이터 원본 항목 첫 행과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 [SiteMinder Data Sources]입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.
5. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.
6. SiteMinder 에 할당되는 최대 데이터베이스 연결 수를 지정합니다.
참고: 최상의 성능을 위해서는 기본값을 유지하는 것이 좋습니다.
7. "적용"을 클릭합니다.
설정이 저장됩니다.
8. "연결 테스트"를 클릭합니다.
정책 서버가 데이터 저장소에 액세스할 수 있다는 확인 메시지가 표시됩니다.
9. "확인"을 클릭합니다.
정책 서버가 데이터베이스를 키 저장소로 사용하도록 구성되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 `stop-all` 명령 다음에 `start-all` 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

SQL Server 에서 키 정보를 저장하는 방법

SQL Server 데이터베이스를 독립 실행형 키 저장소로 구성하려면 다음 절차를 완료하십시오.

1. 데이터베이스 정보를 수집합니다.
2. 키 저장소 스키마를 생성합니다.
3. SiteMinder 에 대한 SQL Server 데이터 원본을 구성합니다.
4. 정책 서버를 데이터베이스에 연결합니다.
5. 정책 서버를 다시 시작합니다.

추가 정보:

[SiteMinder 에 대한 SQL Server 데이터 원본 구성](#) (페이지 330)
[데이터베이스 정보 수집](#) (페이지 327)

키 저장소 스키마 만들기

SQL Server 데이터베이스에 키 정보를 저장할 수 있도록 키 저장소 스키마를 생성하십시오.

키 저장소 스키마를 생성하려면

1. 텍스트 편집기에서 `sm_mssql_ps.sql` 을 열고 전체 파일의 내용을 복사합니다.
 2. 쿼리 분석기를 시작하고 정책 서버 데이터베이스 관리자로 로그인합니다.
 3. 데이터베이스 목록에서 데이터베이스 인스턴스를 선택합니다.
 4. `sm_mssql_ps.sql` 의 스키마를 쿼리에 붙여 넣습니다.
 5. 쿼리를 실행합니다.
- 데이터베이스에 SiteMinder 키 저장소 스키마가 생성되었습니다.

정책 서버를 데이터베이스에 연결

정책 서버가 키 정보를 읽고 저장할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

정책 서버를 데이터 저장소에 연결하려면

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.
데이터베이스 설정이 표시됩니다.
2. "저장소" 목록에서 "ODBC"를 선택합니다.
ODBC 설정이 표시됩니다.
3. "데이터베이스" 목록에서 "키 저장소"를 선택하고 "정책 저장소 데이터베이스 사용" 확인란의 선택을 취소합니다.
데이터 원본 설정이 활성화됩니다.
4. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.
 - (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
 - (UNIX) 입력하는 이름은 `system_odbc.ini` 파일의 데이터 원본 항목 첫 행과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 [SiteMinder Data Sources]입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.
5. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.

6. SiteMinder 에 할당되는 최대 데이터베이스 연결 수를 지정합니다.

참고: 최상의 성능을 위해서는 기본값을 유지하는 것이 좋습니다.

7. "적용"을 클릭합니다.

설정이 저장됩니다.

8. "연결 테스트"를 클릭합니다.

정책 서버가 데이터 저장소에 액세스할 수 있다는 확인 메시지가 표시됩니다.

9. "확인"을 클릭합니다.

정책 서버가 데이터베이스를 키 저장소로 사용하도록 구성되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.

2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.

정책 서버가 중지되고 빨강 표시등이 표시됩니다.

3. "시작"을 클릭합니다.

정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 `stop-all` 명령 다음에 `start-all` 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

PostgreSQL 에서 키 정보를 저장하는 방법

PostgreSQL Server 데이터베이스를 독립 실행형 키 저장소로 구성하려면 다음 절차를 완료하십시오.

1. 데이터베이스 정보를 수집합니다.
2. 키 저장소 스키마를 생성합니다.
3. SiteMinder 에 대한 PostgreSQL Server 데이터 원본을 구성합니다.

4. 정책 서버를 데이터베이스에 연결합니다.
5. 정책 서버를 다시 시작합니다.

키 저장소 스키마 만들기

SQL Server 데이터베이스에 키 정보를 저장할 수 있도록 키 저장소 스키마를 생성하십시오.

키 저장소 스키마를 생성하려면

1. 텍스트 편집기에서 `sm_postgresql_ps.sql` 을 열고 전체 파일의 내용을 복사합니다.
2. `psql` 과 같은 SQL 클라이언트를 열고 정책 서버 데이터베이스를 관리하는 사용자로 로그인합니다.
3. 데이터베이스 목록에서 데이터베이스 인스턴스를 선택합니다.
4. `sm_postgresql_ps.sql` 의 스키마를 쿼리에 붙여 넣습니다.
5. 쿼리를 실행합니다.

데이터베이스에 SiteMinder 키 저장소 스키마가 생성되었습니다.

정책 서버를 데이터베이스에 연결

정책 서버가 키 정보를 읽고 저장할 수 있도록 정책 서버를 데이터베이스에 연결하십시오.

정책 서버를 데이터 저장소에 연결하려면

1. 정책 서버 관리 콘솔을 열고 "데이터" 탭을 클릭합니다.
데이터베이스 설정이 표시됩니다.
2. "저장소" 목록에서 "ODBC"를 선택합니다.
ODBC 설정이 표시됩니다.
3. "데이터베이스" 목록에서 "키 저장소"를 선택하고 "정책 저장소 데이터베이스 사용" 확인란의 선택을 취소합니다.
데이터 원본 설정이 활성화됩니다.

4. "데이터 원본 정보" 필드에 데이터 원본 이름을 입력합니다.
 - (Windows) 입력하는 이름은 데이터 원본을 생성할 때 "데이터 원본 이름" 필드에 입력한 이름과 일치해야 합니다.
 - (UNIX) 입력하는 이름은 `system_odbc.ini` 파일의 데이터 원본 항목 첫 행과 일치해야 합니다. 기본적으로 이 파일의 첫 행은 `[SiteMinder Data Sources]`입니다. 첫 번째 항목을 수정한 경우 올바른 값을 입력해야 합니다.
5. 데이터베이스 인스턴스에 대한 모든 권한이 있는 데이터베이스 계정의 사용자 이름 및 암호를 해당 필드에 입력하고 확인합니다.
6. SiteMinder 에 할당되는 최대 데이터베이스 연결 수를 지정합니다.
참고: 최상의 성능을 위해서는 기본값을 유지하는 것이 좋습니다.
7. "적용"을 클릭합니다.
설정이 저장됩니다.
8. "연결 테스트"를 클릭합니다.
정책 서버가 데이터 저장소에 액세스할 수 있다는 확인 메시지가 표시됩니다.
9. "확인"을 클릭합니다.
정책 서버가 데이터베이스를 키 저장소로 사용하도록 구성되었습니다.

정책 서버를 다시 시작합니다.

특정 설정을 적용하려면 정책 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 엽니다.
2. "상태" 탭을 클릭하고 "정책 서버" 그룹 상자에서 "중지"를 클릭합니다.
정책 서버가 중지되고 빨강 표시등이 표시됩니다.
3. "시작"을 클릭합니다.
정책 서버가 시작되고 녹색 표시등이 표시됩니다.

참고: UNIX 또는 Linux 운영 체제의 경우 `stop-all` 명령 다음에 `start-all` 명령을 실행하여 정책 서버를 다시 시작할 수도 있습니다. 이러한 명령은 정책 서버 관리 콘솔 대신 사용할 수 있습니다.

샘플 사용자 디렉터리

SiteMinder에서는 전용 사용자 저장소를 사용할 필요가 없습니다. 하지만 SiteMinder는 관계형 데이터베이스를 샘플 사용자로 채우는 스키마 파일을 제공합니다.

IBM DB2 샘플 사용자 디렉터리 구성

샘플 사용자 디렉터를 구성하여 데이터베이스에 샘플 사용자를 채우십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. `siteminder_home\db\tier2\DB2`로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

3. 다음 파일을 열고 내용을 텍스트 편집기에 복사합니다.

`smampleusers_db2.sql`

4. 내용을 쿼리에 붙여 넣고 쿼리를 실행합니다.

참고: 쿼리 실행에 대한 자세한 내용은 IBM 설명서를 참조하십시오.

사용자 디렉터리가 샘플 사용자로 채워집니다.

5. 정책 서버에 대한 사용자 디렉터리 연결을 구성합니다.

참고: 사용자 디렉터리 연결 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

MySQL 샘플 사용자 디렉터리 구성

샘플 사용자 디렉터를 구성하여 데이터베이스에 샘플 사용자를 채우십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 위치로 이동합니다.

```
siteminder_home\db\tier2\MySQL
```

siteminder_home

정책 서버 설치 경로를 지정합니다.

3. 텍스트 편집기에서 다음 파일을 엽니다.

```
smampleusers_mysql.sql
```

4. 다음 행을 찾습니다.

```
DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$  
CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
```

5. 'databaseName'의 각 인스턴스를 샘플 사용자 저장소로 작동하는 데이터베이스의 이름으로 바꿉니다.
6. 전체 파일의 내용을 복사합니다.
7. 파일 내용을 쿼리에 붙여 넣고 쿼리를 실행합니다.

참고: 쿼리 실행에 대한 자세한 내용은 MySQL 설명서를 참조하십시오.

사용자 저장소가 샘플 사용자로 채워집니다.

8. 정책 서버에 대한 사용자 디렉터리 연결을 구성합니다.

참고: 사용자 디렉터리 연결 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

Oracle 샘플 사용자 디렉터리 구성

샘플 사용자 디렉터를 구성하여 데이터베이스에 샘플 사용자를 채우십시오.

다음 단계를 수행하십시오.

1. sqlplus 나 다른 Oracle 유틸리티를 사용하여 정책 서버 데이터베이스 정보를 관리하는 사용자로 Oracle 에 로그인합니다.

참고: SYS 또는 SYSTEM 사용자로 SiteMinder 스키마를 생성하지 않는 것이 좋습니다. 필요한 경우 SMOWNER 같은 Oracle 사용자를 생성한 후 해당 사용자로 스키마를 생성하십시오.

2. 다음 스크립트를 가져옵니다.

```
$NETE_PS_ROOT/db/sql/smsampleusers_oracle.sql
```

참고: Oracle 의 SQL 유틸리티에서는 환경 변수가 작동하지 않을 수 있습니다. 이 유틸리티를 사용하여 스크립트를 가져오는 동안 문제가 발생하면 명시적 경로를 지정하십시오.

사용자 디렉터리가 샘플 사용자로 채워집니다.

3. 사용자 디렉터리에 대한 테이블스페이스를 만듭니다.
4. 데이터베이스에서 테이블스페이스를 관리하기 위해 다음 권한이 있는 사용자를 만듭니다.
 - 연결
 - 리소스
 - 제한 없는 테이블스페이스
5. 정책 서버에 대한 사용자 디렉터리 연결을 구성합니다.

참고: 사용자 디렉터리 연결 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

SQL Server 샘플 사용자 디렉터리 구성

샘플 사용자 디렉터를 구성하여 데이터베이스에 샘플 사용자를 채우십시오.

샘플 사용자 디렉터를 구성하려면

1. 텍스트 편집기에서 smsampleusers_sqlserver.sql 을 열고 전체 파일의 내용을 복사합니다.
2. 쿼리 분석기를 시작하고 정책 서버 데이터베이스를 관리하는 사용자로 로그인합니다.
3. 데이터베이스 목록에서 데이터베이스 인스턴스를 선택합니다.

4. smsampleusers_sqlserver.sql 의 스키마를 쿼리에 붙여 넣습니다.

5. 쿼리를 실행합니다.

사용자 디렉터리가 샘플 사용자로 채워집니다.

6. 정책 서버에 대한 사용자 디렉터리 연결을 구성합니다.

참고: 사용자 디렉터리 연결 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

제 8 장: 관리 UI 설치

UI 와 정책 서버 사이의 트러스트 관계

기본 슈퍼 사용자 계정(siteminder)과 암호를 사용하여 관리 UI 에 처음 로그인할 때 관리 UI 와 정책 서버 사이에 트러스트 관계를 구성합니다. 이 관계는 환경을 관리하기 위해 필요합니다.

슈퍼 사용자 계정 자격 증명은 정책 저장소에 저장됩니다. 정책 서버 설치 중에 기본 정책 저장소 중 하나를 구성하는 경우 설치 관리자는 이러한 자격 증명을 자동으로 제출합니다. 정책 저장소 설치와 독립적으로 정책 저장소를 구성하는 경우 XPSRegClient 유틸리티를 사용하여 자격 증명을 정책 서버로 제출하십시오. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 관계를 생성할 수 있는지 확인합니다.

중요! 슈퍼 사용자 계정 자격 증명에 정책 저장소에 제출된 후 24 시간 이내에 관리자가 관리 UI 에 로그인해야 합니다. 24 시간이 경과할 때까지 관리 UI 에 최초 로그인하지 않은 경우 XPSRegClient 유틸리티를 사용하여 자격 증명을 재설정하십시오.

관리 UI 설치 검사 목록 완료

설치 프로그램은 필요한 응용 프로그램 서버 인프라를 만듭니다. 이 인프라는 포함된 응용 프로그램 서버(JBoss) 및 필요한 JDK 를 포함합니다. 설치를 시작하기 전에 관리 UI 호스트 시스템이 최소 시스템 요구 사항을 충족하는지 확인하십시오.

관리 UI 를 설치하기 전에 다음 단계를 완료하십시오.

- ☐ 지원되는 운영 체제를 사용하고 있는지 여부를 확인합니다.
- ☐ 관리 UI 호스트 시스템이 최소 시스템 요구 사항을 충족하는지 여부를 확인합니다.
- ☐ (Linux) 필요한 Linux 라이브러리가 관리 UI 호스트 시스템에 설치되었는지 확인합니다.

- 정책 저장소가 구성된 시기를 확인합니다.

정책 저장소가 구성된 지 24 시간 이상 되었을 경우 관리 UI 를 설치하기 전에 XPSRegClient 유틸리티를 사용하여 기본 SiteMinder 슈퍼 사용자 계정 자격 증명을 정책 서버에 제출할 수 있습니다. 정책 서버에서는 관리 UI 와 트러스트 관계를 생성하기 위해 이러한 자격 증명이 필요합니다.

참고: 지원되는 CA 및 타사 구성 요소의 목록에 대해서는 기술 지원 사이트의 SiteMinder 12.52 SP1 Platform Support Matrix(플랫폼 지원표)를 참조하십시오.

관리 UI 설치 방법

다음 단계를 완료하여 관리 UI 를 설치하십시오.

1. 관리 UI 설치 검사 목록을 검토했는지 확인합니다.
2. (Linux) 필요한 Linux 라이브러리 요구 사항을 검토합니다.
3. 설치 관리자에 필요한 정보를 수집합니다.
4. (선택 사항) 등록 창을 재설정합니다.
5. 관리 UI 설치
6. 관리 UI 를 등록합니다.

다음 사항을 고려하십시오.

- Windows 설치에 성공한 후에는 SiteMinder 관리 UI 로그인 화면이 표시되고 응용 프로그램 서버가 자동으로 시작되므로 관리 UI 를 정책 서버에 등록할 수 있습니다.
- UNIX 설치에 성공한 후에는 수동으로 응용 프로그램 서버를 시작하고 관리 UI 에 로그인하여 등록을 완료해야 합니다. 자세한 내용은 "관리 UI 등록 방법"을 참조하십시오.

설치 관리자에 필요한 정보 수집

관리 UI 를 설치하고 등록하기 전에 다음 정보를 수집하십시오.

- **설치 위치** - 관리 UI 설치 경로를 결정합니다.
- **관리 UI 시스템 이름** - 관리 UI 호스트 시스템의 정규화된 이름을 식별합니다.
- **서버 포트** - JBoss 가 HTTP 요청을 수신 대기해야 하는 포트를 식별합니다.
- **SiteMinder 슈퍼 사용자 계정 암호** - 기본 사용자 계정(siteminder)의 암호를 식별합니다.
- **정책 서버 시스템 이름** - 다음을 식별합니다.
 - 관리 UI 를 등록할 정책 서버
 - 정책 서버 호스트 시스템의 정규화된 이름
- **정책 서버 인증 포트** - 정책 서버를 설치한 후 기본 설정을 변경한 경우 정책 서버 인증 포트를 식별합니다. 정책 서버 관리 콘솔의 "설정" 탭에 액세스 제어 포트가 표시됩니다.

관리 UI 등록 창 재설정

다음 작업 중 하나를 수행한 후 24 시간 이상 경과한 경우 이 단계를 수행해야 합니다.

- 정책 서버 설치 마법사를 사용하여 정책 저장소를 자동으로 구성
- XPSRegClient 유틸리티를 사용하여 SiteMinder 슈퍼 사용자 자격 증명을 정책 서버에 제출

참고: (UNIX) XPSRegClient 를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder_administrator[:passphrase] -adminui-setup -t timeout -r
retries -c comment -cp -l log_path -e error_path -VT -VI -VW -VE -VF
```

siteminder_administrator

SiteMinder 관리자를 지정합니다. 관리 UI 설치 시 다음 사항을 고려하십시오.

- 새로운 12.52 SP1 환경의 일부로 설치할 경우 다음 기본 계정을 지정합니다.

siteminder

- 업그레이드의 일부로 설치할 경우 정책 저장소에서 슈퍼 사용자 권한을 갖는 SiteMinder 관리자 계정을 지정합니다. 정책 저장소에 슈퍼 사용자 계정이 없으면 smreg 유틸리티를 사용하여 기본 계정을 생성하십시오.

passphrase

SiteMinder 관리자 계정의 암호를 지정합니다.

-adminui-setup

관리 UI가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 등록을 완료하기 위해 관리 UI 설치 후 로그인하기까지 허용되는 제한 시간을 지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록 요청을 거부합니다.

측정 단위: 분

기본값: 1440(24 시간)

최소 제한: 1

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI를 등록할 때 허용되는 시도 실패 횟수를 지정합니다. 관리 UI에 최초로 로그인할 때 올바르지 않은 SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수 있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을 삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: `stderr`

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

정책 서버에 관리자 자격 증명이 제공됩니다. 정책 서버에서는 관리 UI에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

관리 UI 설치 방법

다음 단원에서는 독립 실행형 설치 옵션의 일부로 필수 구성 요소 설치 관리자를 사용하여 관리 UI를 설치하는 방법을 설명합니다.

사전 요구 사항 정보 검토

관리 UI를 설치하기 전에 다음 사항을 고려하십시오.

- 기술 지원 사이트의 설치 미디어를 사용하여 관리 UI를 설치합니다.
참고: 설치 미디어 이름의 목록에 대해서는 *정책 서버 릴리스 정보*를 참조하십시오.
- 독립 실행형 옵션을 사용하여 설치하는 경우 다음 절차가 적용됩니다. 기존 응용 프로그램 서버 인프라에 설치하는 경우 "기존 응용 프로그램 서버에 관리 UI 설치"를 참조하십시오.
- (Windows) 관리 UI 호스트 시스템에서 설치 관리자를 실행합니다. 설치 관리자를 매핑된 네트워크 공유 또는 UNC 경로에서 실행하지 마십시오.
- 설치 zip 파일에는 필수 구성 요소 설치 관리자와 관리 UI 설치 관리자가 포함되어 있습니다.
 - Windows에서 필수 구성 요소 설치 관리자를 실행하는 경우에는 두 실행 파일이 동일한 위치에 있어야 합니다. 필수 구성 요소 설치 관리자가 관리 UI 설치 관리자를 자동으로 시작하여 설치를 완료합니다.
 - UNIX에서 필수 구성 요소 설치 관리자를 실행하는 경우에는 두 실행 파일이 동일한 위치에 있어야 합니다. 하지만 관리 UI 설치 관리자를 수동으로 시작하여 설치를 완료해야 합니다. 필수 구성 요소 설치 관리자가 관리 UI 설치 관리자를 자동으로 시작하지 않습니다.
- 설치 zip 파일에는 설치 미디어와 같은 수준에서 `layout.properties` 파일이 포함되어 있습니다. 설치 zip 파일의 압축을 풀 후 설치 미디어를 이동한 경우 속성 파일을 동일한 위치로 이동해야 합니다. 그렇지 않으면 설치가 실패합니다.
- (Red Hat Linux) Red Hat 6 운영 체제는 성능을 위해 엔트로피를 사용합니다. 구성 요소를 설치하기 전에 엔트로피를 늘리십시오. 엔트로피가 충분하지 않으면 설치를 완료하는 데 시간이 매우 오래 걸릴 수 있습니다. 기호화된 링크를 설정하려면 다음 명령을 사용하십시오.

```
mv /dev/random /dev/random.org  
ln -s /dev/urandom /dev/random
```

- (UNIX) 권한에 따라 다음 명령을 실행하여 설치 미디어가 있는 디렉터리에 대한 실행 권한을 추가합니다.

```
chmod -R+x directory
```

directory

설치 미디어가 들어 있는 디렉터리를 지정합니다.

- (UNIX) 여러 서버넷에서 관리 UI 설치 관리자를 실행하면 설치 관리자가 충돌할 수 있습니다. 호스트 시스템에서 직접 관리 UI 를 설치하십시오.

추가 정보:

[관리 UI 설치](#) (페이지 549)

관리 UI 설치 및 등록(Windows)

필수 설치 관리자를 실행한 후 관리 UI 설치 관리자를 실행하십시오.

다음 단계를 수행하십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. 설치 미디어를 탐색합니다.
3. *prerequisite_installation_media* 를 두 번 클릭합니다.

prerequisite_installation_media

관리 UI 필수 구성 요소 설치 관리자 실행 파일을 지정합니다.

설치 관리자가 시작됩니다.

4. "Install"(설치)을 클릭합니다.
필요한 구성 요소가 설치됩니다.
5. "Done"(완료)을 클릭합니다.
관리 UI 설치 관리자가 시작됩니다.
6. 지시를 따르고 "Install"(설치)을 클릭합니다.
관리 UI 가 설치됩니다. SiteMinder 관리 UI 로그인 화면이 표시됩니다.
7. "사용자 이름" 필드에 *siteminder* 를 입력합니다.

8. "암호" 필드에 siteminder 계정 암호를 입력합니다.

참고: 슈퍼 사용자 계정 암호에 달러 -기호(\$) 문자가 있으면 달러 기호 문자의 각 인스턴스를 \$DOLLAR\$로 바꾸십시오. 예를 들어 SiteMinder 슈퍼 사용자 계정 암호가 \$password 이면 "암호" 필드에 \$DOLLAR\$password 를 입력하십시오.

9. "서버" 필드에 정책 서버의 정규화된 호스트 이름을 입력합니다.

다음 사항을 고려하십시오.

- 유효한 IPv4 주소 또는 IPv6 주소를 입력할 수 있습니다.
- 포트를 지정하지 않으면 등록에서 정책 서버의 기본 인증 포트인 44442 로 기본 지정됩니다.

관리 UI 가 열리고 정책 서버에 등록됩니다.

관리 UI 설치(UNIX 시스템)

관리를 위한 콘솔을 제공하려면 관리 UI 및 필수 구성 요소를 설치하십시오. 이 절차는 UNIX 시스템에 관리 UI 를 설치하는 방법을 설명합니다.

여기에 나오는 지침은 GUI 및 콘솔 모드 설치에 사용됩니다. 두 모드의 단계는 동일하지만 콘솔 모드에는 다음의 예외가 있습니다.

- 콘솔 모드 지침은 명령 **-i console** 을 포함합니다.
- 해당 번호를 입력하여 옵션을 선택합니다.
- 각 단계가 끝나면 Enter 키를 눌러 계속 진행합니다.
- 이전 단계로 가려면 BACK 을 입력하십시오.

다음 단계를 수행하십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. 셸을 열고 설치 미디어를 탐색합니다.
3. 다음 명령 중 하나를 입력합니다.

GUI 모드

```
./prerequisite_installation_media
```

콘솔 모드

```
./prerequisite_installation_media -i console  
prerequisite_installation_media
```

관리 UI 필수 구성 요소 설치 관리자 실행 파일을 지정합니다.

설치 관리자가 시작됩니다.

4. "Install"(설치)을 클릭합니다.

필요한 구성 요소가 설치됩니다. 관리 UI 설치 관리자를 실행하라는 메시지가 표시됩니다.

5. 다음 명령 중 하나를 입력합니다.

GUI 모드

```
./installation_media
```

콘솔 모드

```
./installation_media -i console  
installation_media
```

관리 UI 설치 관리자 실행 파일을 지정합니다.

관리 UI 설치 관리자가 시작됩니다.

6. 지시를 따르고 "Install"(설치)을 클릭합니다.

관리 UI 가 설치됩니다.

참고: 정책 서버에 등록하기 전까지는 관리 UI 를 사용할 수 없습니다.

UNIX 설치에 성공한 후에는 수동으로 응용 프로그램 서버를 시작하고 관리 UI 에 로그인하여 등록을 완료해야 합니다. 자세한 내용은 관리 UI 등록 방법을 참조하십시오.

관리 UI 설치 문제 해결

다음 파일을 사용하여 관리 UI 설치 문제를 해결하십시오.

- **Administrative_UI_Prerequisite_Installer_InstallLog.log**

독립 실행형 설치 옵션을 사용한 경우 이 로그에는 필수 구성 요소 설치 중 발생한 성공, 경고, 심각하지 않은 오류 및 오류의 수가 표시됩니다. 개별 설치 작업이 해당 상태와 함께 표시됩니다.

위치: *administrative_ui_home*\CA\SiteMinder\adminui\install_config_info
administrative_ui_home

관리 UI 설치 경로를 지정합니다.

- **CA_SiteMinder_Administrative_UI_InstallLog.log**

이 로그에는 관리 UI 설치 중 발생한 성공, 경고, 심각하지 않은 오류 및 오류의 수가 표시됩니다. 개별 설치 작업이 해당 상태와 함께 표시됩니다.

위치: *administrative_ui_home*\CA\SiteMinder\adminui\install_config_info
administrative_ui_home

관리 UI 설치 경로를 지정합니다.

관리 UI 등록 방법

관리 UI 를 사용하여 SiteMinder 개체를 관리하려면 먼저 관리 UI 를 등록해야 합니다. 관리 UI 를 등록하면 관리 UI 와 정책 서버 간에 신뢰할 수 있는 연결이 생성됩니다. 다음 사항을 고려하십시오.

- (UNIX) 등록을 완료하려면 수동으로 응용 프로그램 서버를 시작하고 관리 UI 에 로그인해야 합니다.
- (Windows) SiteMinder 관리 UI 를 Windows 에 설치한 후 관리 UI 로그인 화면이 표시되고 응용 프로그램 서버가 자동으로 시작됩니다. 이러한 작업을 통해 관리 UI 를 즉시 등록할 수 있습니다. 관리 UI 를 설치한 후 즉시 등록하지 않은 경우 다음 프로세스를 완료하십시오.

다음 단계를 수행하십시오.

1. r12.52 SP1 보다 이전 버전의 경우 [FIPS 환경 변수를 만듭니다.](#) (페이지 453)
2. [응용 프로그램 서버를 시작합니다](#) (페이지 454).
3. 관리 UI 를 등록합니다.

추가 정보:

[관리 UI 등록 방법](#) (페이지 553)

FIPS 환경 변수 만들기

사용자 환경이 다음 두 조건을 모두 충족할 경우 처음으로 관리 UI 를 등록할 때 FIPS 환경 변수를 생성해야 합니다.

- 등록하려는 정책 서버가 FIPS 전용 모드에서 작동 중입니다.
- 관리 UI 가 정책 서버 호스트 시스템에 설치되어 있지 않습니다.

다음 단계를 수행하십시오.

1. 다음 단계 중 하나를 완료하십시오.
 - (Windows) 관리 사용자로 관리 UI 호스트 시스템에 로그인합니다.
 - (UNIX) 관리 UI 를 설치한 사용자로 관리 UI 호스트 시스템에 로그인합니다.

2. 다음 환경 변수를 설정합니다.

CA_SM_PS_FIPS140=ONLY

참고: 환경 변수 설정에 대한 자세한 내용은 해당 OS 설명서를 참조하십시오.

3. 관리 UI 를 실행하는 Windows 또는 UNIX 셸이 CA_SM_PS_FIPS140 변수를 올바르게 인식하는지 확인합니다.

응용 프로그램 서버 시작

독립 실행형 옵션을 사용하여 관리 UI 를 설치한 경우 다음 절차가 적용됩니다. 관리 UI 를 기존 응용 프로그램 서버가 있는 시스템에 설치한 경우 기존 응용 프로그램 서버에 관리 UI 를 설치하는 지침을 참조하십시오.

응용 프로그램 서버를 시작하려면

1. 관리 UI 호스트 시스템에서 다음 작업 중 하나를 수행하십시오.

- **Windows** - Microsoft 서비스 콘솔을 엽니다.

Windows 에 관리 UI 가 설치된 후 응용 프로그램 서버가 자동으로 시작되므로 설치 후 응용 프로그램 서버를 수동으로 시작할 필요가 없습니다.

- **UNIX** - `install_home/CA/siteminder/adminui/bin` 으로 이동합니다.

`install_home`

관리 UI 설치 경로를 지정합니다.

2. 다음 작업 중 하나를 수행하십시오.

- **Windows** - SiteMinder 관리 UI 서비스를 시작합니다.

- **UNIX** - `run.sh` 를 입력하고 Enter 키를 누릅니다.

응용 프로그램 서버가 시작됩니다.

추가 정보:

[기존 응용 프로그램 서버에 관리 UI 설치](#) (페이지 539)

[응용 프로그램 서버 시작](#) (페이지 558)

관리 UI 등록

환경 관리를 시작하려면 관리 UI 를 정책 서버에 등록하십시오.

다음 단계를 수행하십시오.

1. 다음 단계 중 하나를 완료하십시오.

■ Windows:

- (권장) 관리 UI 바로 가기를 사용하여 관리 UI 를 엽니다. 바로 가기를 사용하면 관리 UI 가 SSL 을 통해 등록됩니다. 바로 가기에 대한 액세스 권한이 없을 경우 웹 브라우저를 열고 다음 위치로 이동하십시오.

`https://host:8443/iam/siteminder/adminui`

참고: 10 년 동안 유효한 자체 서명 인증서가 생성되고 연결에 사용됩니다. 인증서는 RSA 2048 키 강도를 사용하여 생성됩니다.

- 웹 브라우저를 열고 다음 위치로 이동합니다.

`http://host:8080/iam/siteminder/adminui`

■ UNIX:

- (권장) 웹 브라우저를 열고 다음 위치로 이동하여 SSL 을 통해 관리 UI 를 등록합니다.

`https://host:8443/iam/siteminder/adminui`

- 브라우저를 열고 다음 위치로 이동합니다.

`http://host:8080/iam/siteminder/adminui`

참고: 호스트 시스템에 웹 브라우저가 없을 경우 원격으로 로그인 화면에 액세스할 수 있습니다.

host

정규화된 관리 UI 호스트 시스템 이름을 지정합니다.

SiteMinder 관리 UI 로그인 화면이 표시됩니다.

2. "사용자 이름" 필드에 다음 값을 입력합니다.

siteminder

3. "암호" 필드에 SiteMinder 슈퍼 사용자 계정 암호를 입력합니다.

참고: 슈퍼 사용자 계정 암호에 달러 -기호(\$) 문자가 있으면 달러 기호 문자의 각 인스턴스를 \$DOLLAR\$로 바꾸십시오. 예를 들어 SiteMinder 슈퍼 사용자 계정 암호가 \$password 이면 "암호" 필드에 \$DOLLAR\$password 를 입력하십시오.

4. "서버" 필드에 정책 서버의 정규화된 호스트 이름을 입력합니다.

다음 사항을 고려하십시오.

- 유효한 IPv4 주소 또는 IPv6 주소를 입력할 수 있습니다.
- 포트를 지정하지 않으면 등록에서 정책 서버의 기본 인증 포트인 44442 로 기본 지정됩니다.

관리 UI 가 열리고 정책 서버에 등록됩니다.

추가 정보:

[파일에 등록 기록이 없다는 오류가 나타남](#) (페이지 581)

[HTTPS 를 사용한 관리 UI 등록](#) (페이지 456)

HTTPS 를 사용한 관리 UI 등록

HTTPS 를 사용하여 관리 UI 를 등록하는 경우 응용 프로그램 서버의 context.xml 파일을 수정하여 보안 쿠키를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 응용 프로그램 서버를 종료합니다.

2. 다음 위치로 이동합니다.

user_console.war\WEB-INF

3. context.xml 파일을 엽니다.

4. SessionCookie 태그에 다음 매개 변수를 추가합니다.

secure="true"

5. 파일을 저장한 후 닫습니다.

6. 응용 프로그램 서버를 다시 시작합니다.

context.xml 파일이 업데이트되고 보안 쿠키가 사용되도록 설정됩니다.

추가 정보:

[응용 프로그램 서버 시작](#) (페이지 454)

[응용 프로그램 서버 중지](#) (페이지 457)

응용 프로그램 서버 중지

독립 실행형 옵션을 사용하여 관리 UI 를 설치한 경우 다음 절차가 적용됩니다. 관리 UI 를 기존 응용 프로그램 서버가 있는 시스템에 설치한 경우 기존 응용 프로그램 서버에 관리 UI 를 설치하는 지침을 참조하십시오.

응용 프로그램 서버를 중지하려면

1. 관리 UI 호스트에서 다음 작업 중 하나를 수행하십시오.
 - **Windows** - Microsoft 서비스 콘솔을 엽니다.
 - **UNIX** - `install_home/CA/siteminder/adminui/bin` 으로 이동합니다.

`administrative_ui_install`

관리 UI 설치 경로를 지정합니다.

2. 다음 작업 중 하나를 수행하십시오.
 - **Windows** - SiteMinder 관리 UI 서비스를 중지합니다.
 - **UNIX** - `shutdown.sh` 를 입력하고 Enter 키를 누릅니다.

응용 프로그램 서버가 중지됩니다.

추가 정보:

[기존 응용 프로그램 서버에 관리 UI 설치](#) (페이지 539)

[응용 프로그램 서버 중지](#) (페이지 561)

관리자 자격 증명

기본적으로 관리 UI 는 정책 저장소를 SiteMinder 관리자 자격 증명의 원본으로 사용합니다. 관리 UI 가 회사 디렉터리 같은 외부 저장소를 사용하도록 구성할 수 있습니다.

참고: 외부 관리자 사용자 저장소 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

(선택 사항) 고가용성을 위해 추가 관리 UI 설치 및 구성

예기치 않은 중단으로 인해 SiteMinder 개체를 관리하지 못하게 되는 문제가 발생하지 않도록 관리 UI 를 두 개 이상 설치하십시오. 다른 관리 UI 를 설치하기 전에 다음 사항을 고려하십시오.

- 아직 특정 관리 UI 와 트러스트 연결을 공유하지 않는 정책 서버에 해당 관리 UI 를 등록합니다. 다른 정책 서버에 등록하면 특정 단일 정책 서버가 중지되어 두 GUI 가 모두 비활성화되는 문제를 예방할 수 있습니다.
- 관리 UI 는 여러 정책 서버로 장애 조치될 수 없습니다. 하지만 여러 정책 서버를 관리하도록 관리 UI 를 구성할 수 있습니다.
- 기존 관리 UI 가 외부 SiteMinder 관리자 인증에 대해 구성된 경우:
 - 새 관리 UI 를 동일한 외부 저장소를 사용하여 구성합니다. 새 관리 UI 를 동일한 외부 저장소를 사용하여 구성하면 모든 SiteMinder 관리자가 모든 GUI 를 사용할 수 있습니다.
 - 동일한 외부 저장소에 대한 이후의 관리 UI 연결은 동일한 네트워크 식별자를 사용하여 구성해야 합니다. 동일한 외부 저장소에 대한 여러 관리 UI 연결에는 네트워크 식별자를 혼합해서 사용할 수 없습니다.

예: 첫 번째 연결을 172.16.0.0 을 사용하여 구성한 경우 이후의 연결도 172.16.0.0 을 사용하여 생성합니다. 마찬가지로 첫 번째 연결을 comp001@example.com 을 사용하여 구성한 경우 이후의 연결도 comp001@example.com 을 사용하여 생성합니다.

관리 UI에 대한 추가 정책 서버 연결

기본적으로 관리 UI는 하나의 정책 서버를 사용하여 구성됩니다. 추가 정책 서버 연결을 구성하고 관리 UI에서 이러한 서버를 관리할 수 있습니다. 예를 들어 개발 및 스테이징 환경에서 정책 서버를 관리하기 위한 연결을 생성할 수 있습니다.

관리 UI가 여러 정책 서버에 연결하도록 하려면 외부 관리자 저장소를 사용하십시오. 외부 사용자 저장소는 외부 정책 서버 연결을 위해 필요합니다. 저장소에서 관리자 아이덴티티에 대한 관리자 계정을 만드십시오. 이 계정은 관리 UI가 외부 저장소에서 관리자 기록을 찾을 수 있도록 해 줍니다.

관리자 및 외부 관리자 저장소에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

다음 단계를 수행하십시오.

1. 외부 관리자 사용자 저장소에 대한 연결을 구성합니다.

참고: 관리 UI가 정책 저장소를 관리자 아이덴티티의 원본으로 사용하는 경우에는 추가 정책 서버 연결을 구성할 수 없습니다.

2. 등록 도구를 실행합니다.
3. 정책 서버에 대한 연결을 구성합니다.

관리 UI 등록 도구 실행

관리 UI 등록 도구를 실행하여 클라이언트 이름 및 암호를 생성하십시오. 클라이언트 이름 및 암호 쌍은 등록할 관리 UI를 정책 서버에서 식별하는 데 사용되는 값입니다. 관리 UI에서 클라이언트 및 암호 값을 제출하여 등록 프로세스를 완료하십시오.

등록 도구를 실행하려면

1. 정책 서버 호스트 시스템에서 명령 프롬프트를 엽니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient client_name[:passphrase] -adminui -t timeout -r retries -c comment
-cp -l log_path -e error_path
-vT -vI -vW -vE -vF
```

참고: *client_name* 과 *[:passphrase]* 사이에 공백을 삽입하면 오류가 발생합니다.

client_name

등록할 관리 UI를 식별합니다.

제한: 이 값은 고유해야 합니다. 예를 들어 이전에 smui1을 사용하여 관리 UI를 등록했으면 smui2를 입력합니다.

참고: 이 값을 기록해 두십시오. 이 값은 관리 UI에서 등록 프로세스를 완료하는 데 필요합니다.

passphrase

관리 UI 등록을 완료하는 데 필요한 암호를 지정합니다.

제한:

- 암호에 6자 이상을 포함해야 합니다.
- 암호에 앰퍼샌드(&)나 별표(*)는 포함할 수 없습니다.
- 암호에 공백이 포함되어 있는 경우 암호를 따옴표로 묶어야 합니다.
- 업그레이드의 일부로 관리 UI를 등록하는 경우 이전 암호를 다시 사용할 수 있습니다.

참고: 이 단계에서 암호를 지정하지 않으면 XPSRegClient에서 암호를 입력하고 확인하라는 메시지가 표시됩니다.

중요! 나중에 참조할 수 있도록 암호를 기록해 두십시오.

-adminui

관리 UI를 등록하도록 지정합니다.

-t timeout

(선택 사항) 관리 UI에서 등록 프로세스를 완료해야 하는 시간을 지정합니다. 이 시간 만료 값에 도달할 경우 정책 서버에서는 등록 요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 1

최대 제한: 1440(1 일)

-r retries

(선택 사항) 관리 UI에서 등록 프로세스를 완료할 때 허용되는 시도 실패 횟수를 지정합니다. 등록 프로세스 중 정책 서버에 제출한 클라이언트 이름이나 암호가 올바르지 않으면 등록 시도가 실패할 수 있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을 삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 등록 도구에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log_path

(선택 사항) 등록 로그 파일을 내보낼 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error_path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: `stderr`

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

등록 로그 파일의 이름이 표시되고 암호를 묻는 메시지가 표시됩니다.

3. Enter 키를 누릅니다.

클라이언트 이름 및 암호 쌍이 생성됩니다.

이제 관리 UI를 정책 서버에 등록할 수 있습니다. 관리 UI에서 등록 프로세스를 완료하십시오.

등록 정보 수집

관리 UI는 사용자가 정책 서버에서 등록할 수 있도록 등록 프로세스로부터 특정 정보가 필요합니다.

관리 UI에 로그인하기 전에 다음 정보를 수집하십시오.

- **클라이언트 이름** - XPSRegClient 도구를 사용하여 지정한 클라이언트 이름입니다.
- **암호** - XPSRegClient 도구를 사용하여 지정한 암호입니다.
- **정책 서버 호스트** - 정책 서버 호스트 시스템의 IP 주소 또는 이름입니다.
- **정책 서버 인증 포트** - 정책 서버가 인증 요청을 수신 대기하는 포트입니다.

기본값: 44442

정책 서버에 대한 연결 구성

관리 UI를 사용하여 SiteMinder 개체를 관리할 수 있도록 연결을 구성하십시오.

정책 서버 연결을 구성하려면

1. 슈퍼 사용자 권한이 있는 계정으로 관리 UI에 로그인합니다.
2. "관리", "관리 UI"를 차례로 클릭합니다.
3. "정책 서버 연결", "정책 서버 연결 등록"을 차례로 클릭합니다.

4. "이름" 필드에 연결 이름을 입력합니다.
5. "정책 서버 호스트" 필드에 정책 서버의 호스트 이름이나 IP 주소를 입력합니다.
6. "정책 서버 포트" 필드에 정책 서버 인증 포트를 입력합니다.

참고: 이 값은 정책 서버 관리 콘솔의 "설정" 탭에 있는 "인증 포트(TCP)" 필드 값과 일치해야 합니다. 기본 인증 포트는 44442 입니다. 포트 번호를 확인하려면 정책 서버 관리 콘솔에서 "설정" 탭을 엽니다.

7. 등록 도구를 사용하여 생성한 클라이언트 이름과 암호를 해당 필드에 입력합니다.
8. FIPS 모드를 선택합니다
 - FIPS 호환성 모드로 정책 서버를 설치한 경우 "호환성" 모드를 선택합니다.
 - FIPS 전용 모드로 정책 서버를 설치한 경우 FIPS 전용 모드를 선택합니다.
9. 제출을 클릭합니다.

관리 UI 와 정책 서버 간에 연결이 구성됩니다.

관리 UI 로그인 화면에는 관리 UI 가 등록된 정책 서버 목록이 표시됩니다. 기본적으로 가장 먼저 등록된 정책 서버가 기본 연결이 됩니다.

기본 정책 서버 연결 수정

관리 UI 로그인 화면에는 관리 UI 가 등록된 정책 서버 목록이 표시됩니다. 기본적으로 가장 먼저 등록된 정책 서버가 기본 연결로 나타납니다. 이 목록을 수정하여 다른 정책 서버 연결을 기본 연결로 표시할 수 있습니다.

다음 단계를 수행하십시오.

1. "관리", "관리 UI"를 차례로 클릭합니다.
2. "정책 서버 연결", "정책 서버 연결 수정"을 차례로 클릭합니다.
3. 검색 조건을 지정하고 "검색"을 클릭합니다.
조건과 일치하는 관리 UI 연결이 표시됩니다.
4. 원하는 연결을 선택하고 "선택"을 클릭합니다.

5. "고급" 그룹 상자에서 화살표 아이콘을 클릭합니다.
6. "기본 연결" 확인란을 선택하고 "제출"을 클릭합니다.
정책 서버 연결이 기본 연결로 구성됩니다.

정책 서버 연결 삭제

관리 UI 로그인 화면에는 관리 UI가 등록된 정책 서버 목록이 표시됩니다. 더 이상 필요하지 않은 정책 서버 연결은 삭제하여 목록에서 제거하십시오.

다음 단계를 수행하십시오.

1. "관리", "관리 UI"를 차례로 클릭합니다.
2. "정책 서버 연결", "정책 서버 연결 삭제"를 차례로 클릭합니다.
3. 검색 조건을 지정하고 "검색"을 클릭합니다.
조건과 일치하는 관리 UI 연결이 표시됩니다.
4. 원하는 연결을 선택하고 "선택"을 클릭합니다.
연결을 삭제해도 되는지 확인하라는 메시지가 표시됩니다.
5. "예"를 클릭합니다.
정책 서버에 대한 연결이 삭제됩니다.

(선택 사항) 관리 UI 제거

시스템에서 더 이상 필요하지 않을 경우 관리 UI를 제거하십시오.

참고: 독립 실행형 옵션을 사용하여 관리 UI를 설치한 경우 다음 절차가 적용됩니다. 관리 UI를 기존 응용 프로그램 서버가 있는 시스템에 설치한 경우 기존 응용 프로그램 서버에 관리 UI를 설치하는 지침을 참조하십시오.

다음 단계를 수행하십시오.

1. 응용 프로그램 서버를 중지합니다.
2. Windows 제어판을 열고 프로그램 목록으로 이동합니다.
3. CA SiteMinder 관리 UI를 마우스 오른쪽 단추로 클릭합니다.
4. "제거/변경"을 클릭합니다.

5. 마법사의 지시를 따릅니다.

참고: 공유 파일을 제거할지 묻는 메시지가 표시되면 "No to All"(모두 아니요)을 클릭합니다.

6. 필요한 경우 시스템을 재부팅합니다.

7. Windows 제어판을 열고 프로그램 목록으로 이동합니다.

8. "관리 UI Prerequisite Installer"(관리 UI 필수 구성 요소 설치 관리자)를 마우스 오른쪽 단추로 클릭합니다.

9. 마법사의 지시를 따릅니다.

참고: 공유 파일을 제거할지 묻는 메시지가 표시되면 "No to All"(모두 아니요)을 클릭합니다.

10. 필요한 경우 시스템을 재부팅합니다.

관리 UI 및 필수 타사 구성 요소가 제거되었습니다.

추가 정보:

[기존 응용 프로그램 서버에 관리 UI 설치](#) (페이지 539)

[Windows 에서 관리 UI 제거](#) (페이지 563)

UNIX 에서 관리 UI 제거

시스템에서 더 이상 필요하지 않을 경우 관리 UI 를 제거하십시오.

다음 사항을 고려하십시오.

- 이 구성 요소를 제거하기 위해 설치 디렉터리를 수동으로 제거하지 마십시오. 제거용 셸 스크립트를 실행해야 합니다. 설치 디렉터리만 제거한 경우 관련 레지스트리가 남아 있게 됩니다. 이 호스트 시스템에 이 구성 요소를 다시 설치하려고 하면 이러한 항목으로 인해 설치가 실패할 수 있습니다.
- 독립 실행형 옵션을 사용하여 관리 UI 를 설치한 경우 다음 절차가 적용됩니다. 관리 UI 를 기존 응용 프로그램 서버가 있는 시스템에 설치한 경우 기존 응용 프로그램 서버에 관리 UI 를 설치하는 지침을 참조하십시오.

다음 단계를 수행하십시오.

1. 응용 프로그램 서버를 중지합니다.
2. 셸을 열고 다음으로 이동합니다.

```
administrative_ui_home/CA/SiteMinder/adminui/install_config_info
```

administrative_ui_home

관리 UI 설치 경로를 지정합니다.

3. 다음 명령을 실행합니다.

```
./sm-wamui-uninstall.sh
```

관리 UI 제거 프로세스가 시작됩니다.

4. 지시에 따라 관리 UI 를 제거합니다.
관리 UI 가 제거되면 메시지가 표시됩니다.

5. 명령 창을 열고 다음으로 이동합니다.

```
administrative_ui_home/CA/SiteMinder/webadmin/install_config_info
```

administrative_ui_home

관리 UI 설치 경로를 지정합니다.

6. 다음 명령을 실행합니다.

```
./prerequisite-uninstall.sh
```

7. 지시에 따라 관리 UI 필수 구성 요소를 제거합니다.
타사 구성 요소가 제거되면 메시지가 표시됩니다.
관리 UI 및 필수 타사 구성 요소가 제거되었습니다.

추가 정보:

[기존 응용 프로그램 서버에 관리 UI 설치](#) (페이지 539)

웹 에이전트 설치를 위한 정책 서버 준비

웹 에이전트를 설치하기 전에 다음 작업을 완료해야 합니다.

- 정책 서버를 설치합니다.
- 정책/키 저장소가 정책 서버와 통신하도록 구성합니다.

- 관리 UI 를 설치하고 등록합니다.
- 정책 서버가 웹 에이전트를 설치할 시스템과 통신할 수 있는지 확인합니다.

웹 에이전트 사이트에 트러스트된 호스트를 등록하려면 먼저 관리 UI 에서 다음 개체를 구성해야 합니다.

참고: 다음에 나오는 각 개체의 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

중앙에서 에이전트를 관리하려면 관리 UI 를 사용하여 다음을 구성하십시오.

- **트러스트된 호스트를 등록할 수 있는 권한이 있는 SiteMinder 관리자** - 트러스트된 호스트는 SiteMinder 웹 에이전트가 하나 이상 설치된 클라이언트 컴퓨터입니다. 트러스트된 호스트라는 용어는 물리적 시스템을 나타냅니다. 트러스트된 호스트를 등록할 수 있는 권한이 있는 관리자가 있어야 합니다. 기본 SiteMinder 관리자에게는 이 권한이 있습니다.
- **에이전트 아이덴티티** - 에이전트 아이덴티티는 웹 에이전트를 호스트하는 웹 서버 인스턴스의 이름과 IP 주소 간에 매핑을 설정합니다. 관리 UI 의 "에이전트" 개체에서 에이전트 아이덴티티를 정의합니다. 에이전트 아이덴티티에 이름을 할당하고 에이전트 유형을 웹 에이전트로 지정하십시오.

참고: 에이전트에 할당하는 이름은 에이전트 구성 개체에 대해 DefaultAgentName 매개 변수로 지정하는 이름과 동일해야 합니다.

- **호스트 구성 개체** - 호스트 구성 개체는 트러스트된 호스트와 정책 서버 간의 최초 연결이 설정된 후 둘 간의 통신을 정의합니다.
호스트 구성 개체와 트러스트된 호스트 구성 파일(SmHost.conf)을 혼동하지 마십시오. 트러스트된 호스트 구성 파일은 호스트가 등록된 후 트러스트된 호스트에 설치됩니다. 최초 연결에 한해 호스트는 SmHost.conf 파일의 설정을 사용하여 정책 서버에 연결할 수 있습니다. 이후 연결은 호스트 구성 개체가 제어합니다.
- **에이전트 구성 개체** - 에이전트 구성 개체는 웹 에이전트 구성을 정의하는 매개 변수를 포함합니다. 아래에 설명된 기본 작업에 대해 몇 가지 필수 매개 변수를 설정해야 합니다.

참고: 에이전트 매개 변수에 대한 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

- **모든 에이전트에 대해 설정** - 에이전트 구성 개체에 `DefaultAgentName` 값을 포함해야 합니다. `DefaultAgentName` 은 "에이전트" 개체에 지정한 에이전트 아이덴티티 이름과 일치해야 합니다. `DefaultAgentName` 은 에이전트 아이덴티티가 할당되지 않은 웹 서버에서 웹 에이전트가 IP 주소를 검색할 때 사용하는 에이전트 아이덴티티를 식별합니다.
- **Domino 웹 에이전트에 대해 설정** - 에이전트 구성 개체에 다음 매개 변수에 대한 값을 포함해야 합니다.
 - **DominoDefaultUser** - 사용자가 Domino Directory 에 있지 않고 SiteMinder 에 의해 다른 사용자 디렉터리에 대해 인증된 경우, Domino 웹 에이전트가 Domino 서버에 대해 사용자를 식별하는데 사용하는 이름입니다. `DominoDefaultUser` 값은 암호화될 수 있습니다.
 - **DominoSuperUser** - SiteMinder 에 로그인된 모든 사용자가 Domino 에 DominoSuperUser 로 로그인되도록 합니다. `DominoSuperUser` 값은 암호화될 수 있습니다.
- **IIS 웹 에이전트에 대해 설정** - 에이전트 구성 개체에 `DefaultUserName` 및 `DefaultPassword` 매개 변수 값을 포함해야 합니다. `DefaultUserName` 및 `DefaultPassword` 는 SiteMinder 에서 보호되는 IIS 웹 서버의 리소스에 액세스할 수 있는 권한이 있는 기존 Windows 계정을 식별합니다. 사용자가 SiteMinder 에서 보호되는 IIS 웹 서버의 리소스에 액세스해야 할 때 필요한 서버 액세스 권한을 가지고 있지 않을 수 있습니다. 웹 에이전트는 SiteMinder 에 의해 액세스 권한이 부여된 사용자에게 대해 관리자가 이전에 할당한 Windows 계정을 프록시 사용자 계정으로 사용해야 합니다.

참고: NTLM 인증 체계를 사용하려고 하거나 Windows 사용자 보안 컨텍스트 기능이 사용되도록 설정하려는 경우에는 이러한 IIS 웹 에이전트 매개 변수의 값을 지정하지 마십시오.

제 9 장: 보고서 설치

이 섹션은 다음 항목을 포함하고 있습니다.

- [설치 로드맵](#) (페이지 469)
- [보고서 설치 검사 목록](#) (페이지 470)
- [보고 고려 사항](#) (페이지 477)
- [보고서 설치 작동 방식](#) (페이지 478)
- [보고서 서버 설치 방법](#) (페이지 479)
- [보고서 템플릿 설치 방법](#) (페이지 493)
- [보고서 서버 등록 방법](#) (페이지 499)
- [감사 데이터베이스 구성 방법](#) (페이지 507)
- [보고서 서버 시작](#) (페이지 510)
- [보고서 서버 중지](#) (페이지 512)
- [보고서 제거 방법](#) (페이지 513)
- [보고서 서버와 관리 UI의 연결 삭제](#) (페이지 518)
- [보고서 서버 다시 설치](#) (페이지 518)

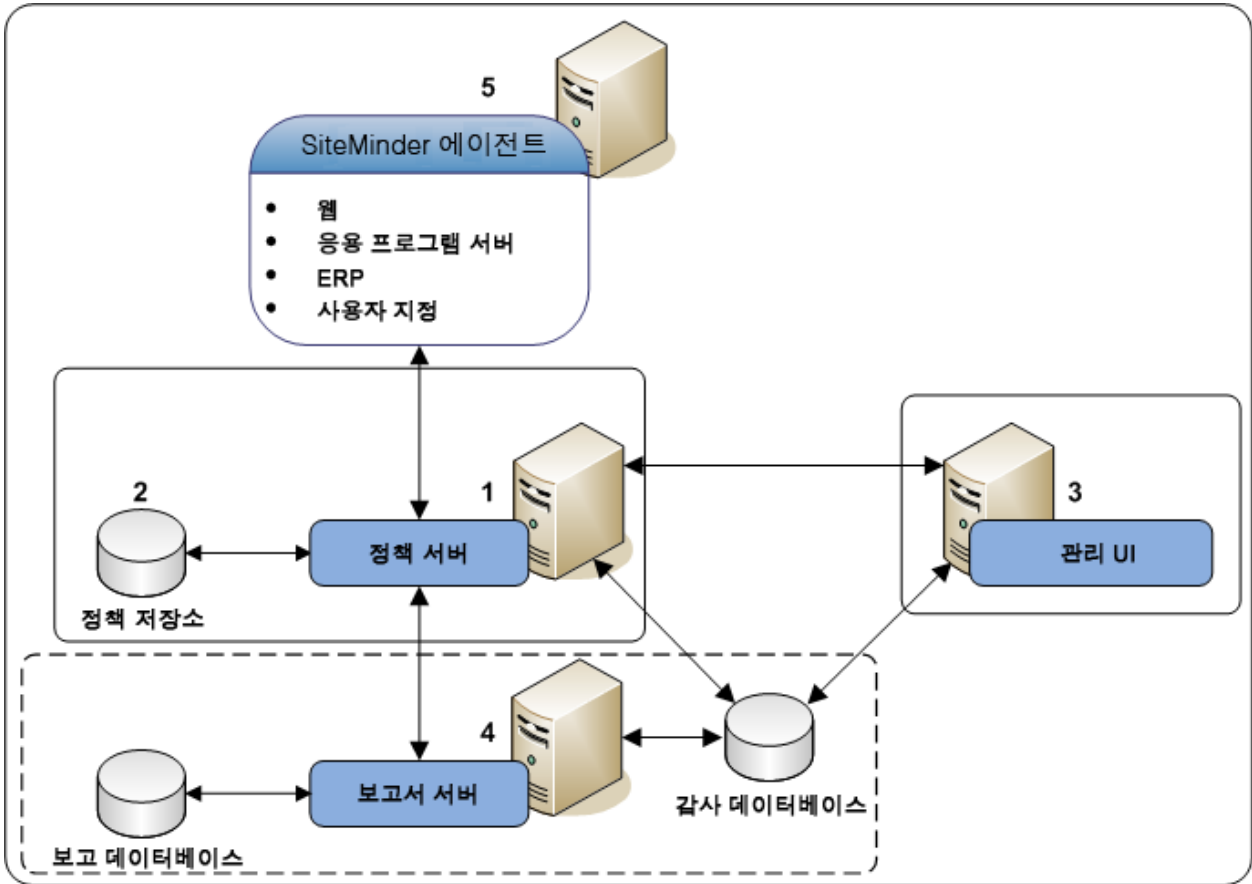
설치 로드맵

다음 그림은 샘플 SiteMinder 설치를 보여 주고 각 구성 요소를 설치 및 구성하는 순서를 나열합니다.

- 실선으로 둘러싸인 부분은 보고서를 설치 및 구성하기 전에 필요한 구성 요소로, 다음이 포함됩니다.
 - 정책 서버
 - 정책 저장소
 - 정책 서버에 등록된 관리 UI
- 점선으로 둘러싸인 부분은 지금 설치 및 구성해야 할 구성 요소로, 다음이 포함됩니다.
 - 보고서 서버
 - 보고서 데이터베이스

- SiteMinder 감사 데이터베이스

그림 3: 보고서 서버 설치 로드맵



보고서 설치 검사 목록

보고서 서버 및 보고서 데이터베이스 검사 목록을 검토하여 다음 사항을 확인하십시오.

- 사용 환경이 최소 운영 체제 및 데이터베이스 요구 사항을 충족합니다.
- 필요한 필수 구성 요소가 구성되었습니다.

보고서 서버

- 보고서 서버 호스트 시스템이 다음과 같은 최소 운영 체제 요구 사항을 충족하는지 확인하십시오.
 - [Windows](#) (페이지 27)
 - UNIX
- (Solaris) 보고서 서버 호스트 시스템에 필수 운영 체제 패치를 설치하십시오.
참고: 자세한 내용은 *정책 서버 릴리스 정보*를 참조하십시오.
- 보고서 서버 호스트가 [연결 요구 사항](#) (페이지 29)을 충족하는지 확인하십시오.
- 보고서 서버 호스트 이름에 다음과 같은 문자가 포함되어 있지 않은지 확인하십시오.
 - 밑줄(_)
 - 마침표(.)
 - 슬래시(/)\
- 보고서 서버를 다시 설치하려면 현재 인스턴스를 제거하십시오. 기존 인스턴스 위에 설치하려고 하면 설치가 실패합니다.
- Windows 설치:
 - 로컬 관리자 그룹의 구성원인 사용자 계정에 대한 액세스 권한이 있는지 확인하십시오. 설치 관리자를 실행하는 사용자 계정은 로컬 관리자 그룹의 구성원이어야 합니다.
중요! 로컬 관리자 그룹에 대한 기본 Windows 보안 설정이 수정된 시스템에 설치하는 것은 지원되지 않습니다.
 - 설치할 대상 시스템이 도메인 컨트롤러가 아닌지 확인하십시오. 도메인 컨트롤러에 설치하는 것은 지원되지 않습니다.
- UNIX 설치:
 - IP 확인에 문제가 없도록 `/etc/hosts` 파일에 보고서 서버 호스트 IP 가 올바르게 구성되어 있는지 확인하십시오.

- 루트 사용자 계정 및 루트 아닌 사용자 계정에 대한 액세스 권한이 있는지 확인하십시오. 설치를 시작하려면 루트 사용자 계정이 필요하고, 설치를 완료하려면 루트 아닌 사용자 계정이 필요합니다. 루트 아닌 사용자 계정이 다음을 충족하는지 확인하십시오.
 - 유효한 홈 디렉터리의 소유자입니다.
 - 홈 디렉터리에 대한 쓰기 권한이 있습니다.
- 다음과 같은 명령 및 유틸리티가 운영 체제에 설치되어 있으며 루트 사용자 계정의 **PATH** 환경 변수에서 사용할 수 있는지 확인하십시오.
 - `/bin/sh`
 - `uname`
 - `awk`
 - `tar`
 - `stty`
 - `pwd`
 - `expr`
 - `chown`
 - `id`
 - `ulimt`
 - 읽기
 - `hostname`
 - `grep`
 - `dirname`
 - `which`
 - `touch`
 - `sed`
 - `tail`
 - `gzip`
- 루트 사용자 계정의 **PATH** 환경 변수에 핵심 시스템 명령줄 도구를 대체하는 **GNU** 또는 타사 도구나 개별적으로 다운로드하여 컴파일한 도구 버전이 포함되어 있지 않은지 확인하십시오.

- 다음 변수 중 적어도 하나를 유효한 utf8/UTF-8 로캘로 설정하십시오.
 - LC_ALL
예: export LC_ALL=en_US.UTF-8
 - LANG
예: export LANG=en_US.UTF-8
 - LC_CTYPE
예: export LC_CTYPE=en_US.UTF-8

보고서 데이터베이스 및 감사 데이터베이스

- 포함된 MySQL 버전을 사용하지 않는 경우:
 - 데이터베이스 서버 호스트 시스템의 호스트 이름이 고정되어 있는지 확인하십시오.
 - [보고서 데이터베이스](#) (페이지 29) 기능을 수행하는 지원되는 데이터베이스를 사용하는 중인지 확인하십시오.
 - 비어 있는 새 데이터베이스를 사용할 수 있는지 확인하십시오.
 - 데이터베이스 클라이언트 및 서버가 UTF8 문자 인코딩을 사용하도록 구성되어 있는지 확인하십시오. 유니코드 구성에 필요한 설정에 대한 자세한 내용은 공급업체의 설명서를 참조하십시오.
- (SQL Server) SQL Server 를 보고서 데이터베이스나 감사 데이터베이스 또는 둘 모두로 사용하는 경우 보고서 서버 호스트 시스템에서 다음을 수행하십시오.
 - SiteMinder 지원 SQL Server 드라이버가 보고서 서버 호스트 시스템에 설치되어 있는지 확인하십시오.
 - 각 데이터베이스를 식별하는 DSN(데이터 원본 이름)을 만드십시오. 보고서 서버는 이 DSN 을 사용하여 각 데이터베이스와 통신합니다.

- (Oracle) Oracle 을 보고서 데이터베이스나 감사 데이터베이스 또는 둘 모두로 사용하는 경우:

- 보고서 서버 호스트 시스템에서 다음을 수행하십시오.

- 지원되는 Oracle Net Client 가 설치되어 있는지 확인하십시오.
- Oracle Net 서비스 이름을 사용하여 tnsnames.ora 파일에서 각 데이터베이스를 식별하십시오. 보고서 서버는 이 서비스 이름을 사용하여 각 데이터베이스와 통신합니다.
- NLS_LANG 변수를 다음 UTF-8 설정 중 하나로 설정하십시오.
 - AMERICAN_AMERICA.WE8MSWIN1252
 - AMERICAN_AMERICA.AL32UTF8
- ORACLE_HOME 변수를 *Oracle_Net_client* 로 설정하십시오.

Oracle_Net_client

Oracle Net client 설치 경로를 지정하십시오.

Windows 예: C:\oracle\product\10.2.0\client

UNIX 예: export

ORACLE_HOME=/opt/oracle/product/10.2.0/client1

- (Windows) ORACLE_HOME 변수를 시스템 환경 변수에 추가하십시오.

예: %Oracle_Home%\bin

- (UNIX) LD_LIBRARY_PATH 변수를 \$ORACLE_HOME/lib32:\$ORACLE_HOME/lib 로 설정하십시오.

예:

LD_LIBRARY_PATH=\$ORACLE_HOME/lib32:\$ORACLE_HOME/lib:\$LD_LIBRARY_PATH

- (UNIX) PATH 변수를 \$ORACLE_HOME/bin:\$PATH 로 설정하십시오.

예: export PATH=\$ORACLE_HOME/bin:\$PATH

- 데이터베이스 서버 호스트 시스템에서 NLS_LANG 변수를 다음 UTF-8 설정 중 하나로 설정하십시오.

- AMERICAN_AMERICA.WE8MSWIN1252
- AMERICAN_AMERICA.AL32UTF8

보고서 데이터베이스 및 감사 데이터베이스

- 포함된 MySQL 버전을 사용하지 않는 경우:
 - 데이터베이스 서버 호스트 시스템의 호스트 이름이 고정되어 있는지 확인하십시오.
 - [보고서 데이터베이스](#) (페이지 29) 기능을 수행하는 지원되는 데이터베이스를 사용하는 중인지 확인하십시오.
 - 비어 있는 새 데이터베이스를 사용할 수 있는지 확인하십시오.
 - 데이터베이스 클라이언트 및 서버가 UTF-8 문자 인코딩을 사용하도록 구성되어 있는지 확인하십시오. 유니코드 구성에 필요한 설정에 대한 자세한 내용은 공급업체의 설명서를 참조하십시오.
- (SQL Server) SQL Server 를 보고서 데이터베이스나 감사 데이터베이스 또는 둘 모두로 사용하는 경우 보고서 서버 호스트 시스템에서 다음을 수행하십시오.
 - SiteMinder 지원 SQL Server 드라이버가 보고서 서버 호스트 시스템에 설치되어 있는지 확인하십시오.
 - 각 데이터베이스를 식별하는 DSN(데이터 원본 이름)을 만드십시오. 보고서 서버는 이 DSN 을 사용하여 각 데이터베이스와 통신합니다.
 - 데이터베이스가 UTF-8 문자 인코딩을 사용하는지 확인하십시오. 유니코드 구성에 필요한 설정에 대한 자세한 내용은 SQL 서버 설명서를 참조하십시오.

- (Oracle) Oracle 을 보고서 데이터베이스나 감사 데이터베이스 또는 둘 모두로 사용하는 경우:

- 보고서 서버 호스트 시스템에서 다음을 수행하십시오.

- 지원되는 Oracle Net Client 가 설치되어 있는지 확인하십시오.
- 데이터베이스 클라이언트 및 서버가 UTF-8 문자 인코딩을 사용하도록 구성되어 있는지 확인하십시오. 유니코드 구성에 필요한 설정에 대한 자세한 내용은 공급업체의 설명서를 참조하십시오.
- Oracle Net 서비스 이름을 사용하여 tnsnames.ora 파일에서 각 데이터베이스를 식별하십시오. 보고서 서버는 이 서비스 이름을 사용하여 각 데이터베이스와 통신합니다.
- NLS_LANG 변수를 다음 UTF-8 설정 중 하나로 설정하십시오.
 - AMERICAN_AMERICA.WE8MSWIN1252
 - AMERICAN_AMERICA.AL32UTF8
- ORACLE_HOME 변수를 *Oracle_Net_client* 로 설정하십시오.

Oracle_Net_client

Oracle Net client 설치 경로를 지정하십시오.

Windows 예: C:\oracle\product\10.2.0\client

UNIX 예: export

ORACLE_HOME=/opt/oracle/product/10.2.0/client1

- (Windows) ORACLE_HOME 변수를 시스템 환경 변수에 추가하십시오.

예: %Oracle_Home%\bin

- (UNIX) LD_LIBRARY_PATH 변수를 \$ORACLE_HOME/lib32:\$ORACLE_HOME/lib 로 설정하십시오.

예:

LD_LIBRARY_PATH=\$ORACLE_HOME/lib32:\$ORACLE_HOME/lib:\$LD_LIBRARY_PATH

- (UNIX) PATH 변수를 \$ORACLE_HOME/bin:\$PATH 로 설정하십시오.

예: export PATH=\$ORACLE_HOME/bin:\$PATH

- 데이터베이스 서버 호스트 시스템에서 `NLS_LANG` 변수를 다음 UTF-8 설정 중 하나로 설정하십시오.
 - `AMERICAN_AMERICA.WE8MSWIN1252`
 - `AMERICAN_AMERICA.AL32UTF8`

보고 고려 사항

보고서 서버를 설치하기 전에 다음 항목을 확인하십시오.

- 다른 SiteMinder 구성 요소가 있는 호스트 시스템에 보고서 서버를 설치하는 것은 지원되지 않습니다. 별도의 호스트 시스템에 보고서 서버를 설치해야 합니다.
- UNIX 설치에는 수 시간이 걸릴 수 있습니다. 설치하기 전에 페이지 크기를 4 GB 이상이나 RAM 크기까지 늘리십시오. 설치에 네 시간 이상이 걸리는 경우 설치를 중지하고 페이지 크기를 늘리십시오.
- 보고서 서버 호스트 시스템에 JBoss 가 설치되어 있으면 포트 충돌이 발생할 수 있습니다. 보고서 서버를 설치한 후 포트 충돌이 발생하는 경우 다음 파일에서 JBoss 포트 정보를 찾을 수 있습니다.
 - `jboss-service.xml`
 기본 위치: `jboss_home\server\server_configuration\conf`
 - `server.xml`
 기본 위치:
`jboss_home\server\server_configuration\deploy\jbossweb-tomcat55.sar`
`jboss_home`
 JBoss 설치 경로를 지정합니다.
`server_configuration`
 서버 구성의 이름을 지정합니다.
 기본값: `default`

참고: 이러한 파일을 변경한 경우 JBoss 를 다시 시작하십시오.
 자세한 내용은 Red Hat 설명서를 참조하십시오.
- `service-bindings.xml`
 독립 실행형 옵션을 사용하여 보고서 서버 호스트 시스템에 관리 UI 를 설치한 경우에만 이 파일이 존재합니다.

기본 위치: `administrative_ui_install\webadmin\conf`
`administrative_ui_installation`

관리 UI 설치 경로를 지정합니다.

참고: 이 파일을 변경한 경우 관리 UI 응용 프로그램 서버를 다시 시작하십시오.

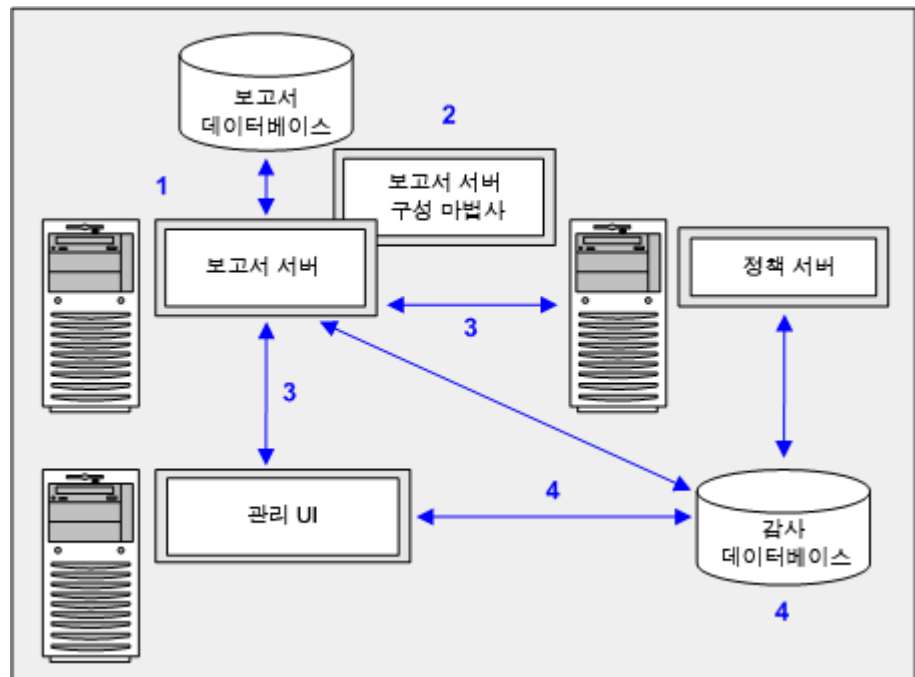
추가 정보:

[응용 프로그램 서버 시작](#) (페이지 454)

[응용 프로그램 서버 중지](#) (페이지 457)

보고서 설치 작동 방식

SiteMinder 보고 기능으로 SiteMinder 정책 분석 및 감사 기반 보고서를 관리하려면 보고서 서버, 보고서 데이터베이스 및 SiteMinder 감사 데이터베이스를 설치하고 구성해야 합니다. 다음 다이어그램에서는 샘플 SiteMinder 환경과 각 구성 요소의 설치 또는 구성 순서를 보여 줍니다.



다음은 위 다이어그램에 나온 각 단계에 대한 설명입니다.

1. **보고서 서버 설치** - 프로세스의 첫 번째 단계에서는 보고서 서버를 설치합니다. 또한 설치 중에 보고서 데이터베이스를 구성합니다.
2. **SiteMinder 보고서 템플릿 설치** - 프로세스의 두 번째 단계에서는 SiteMinder 보고서 템플릿을 설치합니다. SiteMinder 보고서 서버 구성 마법사는 보고서 서버가 SiteMinder 정책 분석 및 감사 보고서 템플릿 집합을 사용하도록 구성합니다.
3. **보고서 서버 등록** - 프로세스의 세 번째 단계에서는 보고서 서버를 등록합니다. 등록하려면 다음 요소 간의 연결을 구성해야 합니다.
 - 보고서 서버와 정책 서버
 - 보고서 서버와 관리 UI
4. **SiteMinder 감사 데이터베이스 구성** - 프로세스의 네 번째 단계에서는 SiteMinder 감사 데이터베이스를 구성합니다. 감사 기반 보고서를 실행하려면 관리 UI에 등록된 별도의 SiteMinder 감사 데이터베이스가 있어야 합니다.

보고서 서버 설치 방법

보고서 서버를 설치하려면 다음 절차를 완료하십시오.

1. 설치 검사 목록을 검토합니다.
2. 설치 관리자에 필요한 정보를 수집합니다.
3. 보고서 서버를 설치합니다.

설치 관리자에 필요한 정보 수집

다음 단원을 검토하여 보고서 서버 설치 관리자에 필요한 정보를 확인하십시오.

설치 자격 증명

설치를 수행하는 운영 체제에 따라서는 설치 관리자에 하나 이상의 자격 증명 집합이 필요합니다.

■ (Windows 및 UNIX) BusinessObjects 관리자 암호

설치 관리자가 기본 SAP BusinessObjects Enterprise 관리자 계정(administrator)을 만듭니다. 이 계정을 사용하여 SiteMinder 보고서 템플릿을 가져오고 BusinessObjects 콘텐츠 관리 콘솔에 액세스할 수 있습니다. 이 계정의 암호를 결정하십시오.

암호는 다음과 같은 구성 조건을 충족해야 합니다.

- 암호는 6 자 이상이어야 합니다.
- 암호에 "administrator"라는 단어가 어떤 형태로도 포함될 수 없습니다.
- 암호에 다음과 같은 문자 유형이 두 개 이상 포함되어야 합니다.
 - 대문자
 - 소문자
 - 숫자
 - 문장 부호

■ (UNIX) 루트 아닌 사용자 계정 - 설치를 시작하려면 루트 사용자 계정이 필요하고, 설치를 완료하려면 루트 아닌 사용자 계정이 필요합니다. 루트 아닌 사용자 계정을 확인하십시오.

- 사용자 이름
- 그룹 이름

MySQL 보고서 데이터베이스

포함된 MySQL 버전을 사용하여 보고서 데이터베이스 기능을 수행하는 경우 설치 관리자에 관련 정보가 필요합니다. 설치를 시작하기 전에 보고서 데이터베이스 설치 워크시트를 사용하여 다음과 같은 정보를 수집하십시오.

■ MySQL 루트 암호

MySQL 루트 사용자 계정의 암호입니다.

참고: 루트 사용자 계정의 이름을 변경할 수 없습니다. 설치 관리자는 기본적으로 root 라는 이름을 사용합니다.

- 사용자

보고서 데이터베이스 관리자 계정의 이름입니다.

설치 관리자 기본값: sa

- 암호

보고서 데이터베이스 관리자 계정의 암호입니다.

SQLAnywhere 보고서 데이터베이스

포함된 SQLAnywhere 버전을 사용하여 보고서 데이터베이스 기능을 수행하려면 설치 관리자에 관련 정보가 필요합니다. 설치를 시작하기 전에 보고서 데이터베이스 설치 워크시트를 사용하여 다음과 같은 정보를 수집하십시오.

- SQLAnywhere 루트 암호

SQLAnywhere 루트 사용자 계정의 암호입니다.

참고: 루트 사용자 계정의 이름을 변경할 수 없습니다. 설치 관리자는 기본적으로 root 라는 이름을 사용합니다.

- 사용자

보고서 데이터베이스 관리자 계정의 이름입니다.

설치 관리자 기본값: sa

- 암호

보고서 데이터베이스 관리자 계정의 암호입니다.

Microsoft SQL Server 보고서 데이터베이스

Microsoft SQL Server 를 사용하여 보고서 데이터베이스 기능을 수행하는 경우 설치 관리자에 관련 정보가 필요합니다. 설치를 시작하기 전에 보고서 데이터베이스 설치 워크시트를 사용하여 다음과 같은 정보를 수집하십시오.

- DSN(데이터 원본 이름)

보고서 서버가 보고서 데이터베이스와 통신하기 위해 사용하는 DSN 입니다.

참고: 보고서 서버는 32 비트 네이티브 바이너리로 컴파일되며 32 비트 데이터 원본 미들웨어 연결을 사용하도록 설계되어 있습니다. Windows 64 비트 운영 체제에 설치하는 경우 `odbcad32.exe` 를 사용하여 DSN 을 만들어야 합니다. 이 실행 파일은 다음 위치에 있습니다.

`install_home\Windows\SysWOW64.`

`install_home`

Windows 운영 체제의 설치 경로를 지정합니다.

■ **로그인 ID**

보고서 데이터베이스 관리자 계정의 이름입니다. 이 계정에는 기본(DBO) 계정 권한이 있어야 합니다.

■ **암호**

보고서 데이터베이스 관리자 계정의 암호입니다.

Oracle 보고서 데이터베이스

Oracle 을 사용하여 보고서 데이터베이스 기능을 수행하는 경우 설치 관리자에 관련 정보가 필요합니다. 설치를 시작하기 전에 보고서 데이터베이스 설치 워크시트를 사용하여 다음과 같은 정보를 수집하십시오.

■ **Oracle Net Client 서비스 이름**

보고서 서버가 보고서 데이터베이스와 통신하기 위해 사용하는 서비스 이름입니다.

- (Windows) 설치 관리자에서 Oracle Net Client 서비스 이름이 "Server"(서버)로 나타납니다.
- (UNIX) 설치 관리자에서 Oracle Net Client 서비스 이름이 TNSNAME 으로 나타납니다.

■ **사용자 이름**

보고서 데이터베이스 관리자 계정의 이름입니다. 이 계정에는 다음 권한이 있어야 합니다.

- 세션 만들기
- 테이블 만들기

- 프로시저 만들기

참고: CONNECT 및 RESOURCE 역할이 사용되도록 설정된 관리자 계정을 사용할 수도 있습니다. 두 역할 모두에서 "Admin Option"(관리 옵션) 설정이 사용되지 않도록 설정해야 합니다.

- 암호

보고서 데이터베이스 관리자 계정의 암호입니다.

Apache Tomcat 설치

SiteMinder 에서는 보고서 서버 설치에 포함되어 있는 Apache Tomcat 버전만 지원합니다. 설치를 시작하기 전에 웹 응용 프로그램 설치 워크시트를 사용하여 다음과 같은 정보를 수집하십시오.

- 연결 포트

Apache Tomcat 이 연결하고 요청을 대기하는 포트입니다.

설치 관리자 기본값: 8080

- 리디렉션 포트

Apache Tomcat 이 요청을 리디렉션해야 하는 포트를 지정합니다.

설치 관리자 기본값: 8443

- 종료 포트

Apache Tomcat SHUTDOWN 명령이 실행되는 포트입니다.

설치 관리자 기본값: 8005

보고서 서버 설치

다음 단원에서는 Windows 및 UNIX 에 보고서 서버를 설치하는 방법에 대해 자세히 설명합니다.

설치하기 전에

보고서 서버를 설치하기 전에 다음 항목을 확인하십시오.

- 다른 SiteMinder 구성 요소가 있는 호스트 시스템에 보고서 서버를 설치하는 것은 지원되지 않습니다. 별도의 호스트 시스템에 보고서 서버를 설치해야 합니다.
- 기술 지원 사이트의 설치 미디어를 사용하여 보고서 서버를 설치하십시오.

참고: 설치 미디어 이름의 목록에 대해서는 *정책 서버 릴리스 정보*를 참조하십시오.

- 보고서 서버는 32 비트 네이티브 바이너리로 컴파일되며 32 비트 데이터 원본 미들웨어 연결을 사용하도록 설계되어 있습니다. Windows 64 비트 운영 체제에 설치하는 경우 `odbcad32.exe` 를 사용하여 DSN 을 만들어야 합니다. 이 실행 파일은 다음 위치에 있습니다.

`install_home\Windows\SysWOW64.`

install_home

Windows 운영 체제의 설치 경로를 지정합니다.

- UNIX 콘솔 설치 는 지원되지 않습니다.
- 보고서 서버 설치에는 프로세스로 실행되는 다음과 같은 구성 요소가 포함됩니다.
 - 콘텐츠 관리 서버
 - Server Intelligence Agent

이러한 구성 요소에는 통신에 사용할 TCP/IP 포트가 필요합니다. 보고서 서버 호스트 시스템의 포트 충돌을 방지하기 위해 설치 관리자에서 기본 설정을 수정할 수 있습니다.

- **중요!** 설치 zip에는 여러 폴더가 포함되어 있습니다. 설치 관리자 실행 파일에는 이 폴더 구조가 필요합니다. zip 파일의 압축을 풀 후 보고서 서버 설치 관리자를 이동한 경우에는 전체 폴더 구조를 동일한 위치로 복사하십시오. 이 폴더 구조에서 설치 미디어를 실행하십시오.

- **중요!** (UNIX) 보고서 서버를 설치하는 사용자 계정에는 설치 미디어가 들어 있는 디렉터리에 대한 실행 권한이 있어야 합니다. 사용자 계정에 이러한 권한이 없는 경우 다음 명령을 실행하십시오.

```
chmod -R+x directory
```

directory

설치 미디어가 들어 있는 디렉터를 지정합니다.

- (UNIX) 서로 다른 서브넷 전체에 걸쳐 보고서 서버 설치 관리자를 실행하면 충돌이 발생합니다. 호스트 시스템에서 직접 보고서 서버를 설치하십시오.
- (UNIX) RHEL 6 컴퓨터에 보고서 서버를 설치하기 전에 RHEL 6 컴퓨터에서 다음 태스크를 완료해야 합니다.
 - 다음 RPM 을 설치합니다.
 - ncurses-libs.i686
 - Compat-libstdc++-33.3.3-69.el6.i686
 - libXext-1.1-3.el6.i686
 - libXext-devel-1.1-3.el6.i686
 - ncurses-base
 - ncurses-libs 5.9-7.20121017
 - xorg-x11-libX11-7.6-23.1.2.i586
 - xorg-x11-libXau-7.6_1.0.6-9.1.1.i586
 - xorg-x11-libxcb-7.6_1.7-8.1.i586
 - LD_LIBRARY_PATH 환경 변수를 32 비트 libncurses.so.5 라이브러리의 위치로 설정합니다.

Windows

다음 단계를 수행하십시오.

1. [설치 검사 목록](#) (페이지 470)을 검토했는지 확인합니다.
2. [설치 관리자에 필요한 정보](#) (페이지 479)를 수집했는지 확인합니다.
3. 실행 중인 응용 프로그램을 모두 종료합니다.

4. *installation_media* 를 두 번 클릭합니다.

installation_media

보고서 서버 설치 실행 파일을 지정합니다.

CA Business Intelligence 설치 마법사가 나타나고 로컬을 묻는 메시지가 표시됩니다.

참고: 설치 미디어 이름의 목록에 대해서는 정책 서버 릴리스 정보를 참조하십시오.

5. "English"(영어)를 선택하고 "OK"(확인)를 클릭합니다.

설치 관리자 소개가 나타납니다.

6. "다음"을 클릭합니다.

CA 사용권 계약이 나타납니다.

7. 사용권 계약에 동의하고 "Next"(다음)를 클릭합니다.

CA 샘플 템플릿을 설치할지 묻는 메시지가 표시됩니다.

8. "아니요"를 선택하고 "Next"(다음)를 클릭합니다.

참고: CA 샘플 템플릿은 SiteMinder 보고 템플릿과 관련이 없습니다.

SiteMinder 보고서 서버 구성 마법사가 필요한 보고 템플릿을 설치합니다. 보고서 서버를 설치한 후 이 마법사를 실행하십시오.

자동 설치용 응답 파일을 저장할 것인지 묻는 메시지가 표시됩니다.

9. "Yes"(예)를 선택하고 "Next"(다음)를 클릭합니다.

설치 요약이 나타납니다.

10. 요약 정보를 검토한 다음 "Install"(설치)을 클릭합니다.

구성 요소가 설치됩니다. CA Business Intelligence 설치 마법사가 나타납니다.

11. "다음"을 클릭합니다.

설치 관리자 소개가 나타납니다.

12. "다음"을 클릭합니다.

SAP BusinessObjects Enterprise 사용권 계약이 나타납니다.

13. 사용권 계약에 동의하고 "Next"(다음)를 클릭합니다.

언어 팩을 선택하라는 메시지가 표시됩니다. 기본적으로 영어가 선택되어 있습니다.

14. 기본값인 영어 설정을 그대로 두고 "Next"(다음)를 클릭합니다.
설치 유형에 대한 메시지가 표시됩니다.
15. "New"(새로 만들기)를 선택하고 다음 단계 중 하나를 수행하여 보고서(CMS) 데이터베이스를 구성합니다.
 - (권장) 포함된 MySQL 버전을 설치하려면 "Install MySQL Database Server"(MySQL 데이터베이스 서버 설치)를 선택하고 "Next"(다음)를 클릭합니다.
 - 기존 Microsoft SQL Server 또는 Oracle 데이터베이스를 구성하려면 "Use an existing database server"(기존 데이터베이스 서버 사용)를 선택하고 "Next"(다음)를 클릭합니다.

콘텐츠 관리 서버 포트와 SAP BusinessObjects Enterprise 관리자 계정의 암호를 묻는 메시지가 표시됩니다.
16. 다음 단계를 완료합니다.
 - a. 콘텐츠 관리 서버가 수신 대기하는 포트를 지정합니다.
 - b. 기본 SAP BusinessObjects Enterprise 관리자의 암호를 지정합니다.
중요! "Configure the SAP BusinessObjects Enterprise Administrator password at a later time"(나중에 SAP BusinessObjects Enterprise 관리자 암호 구성)을 선택하지 마십시오.
 - c. "다음"을 클릭합니다.
Server Intelligence Agent 노드 이름 및 포트를 묻는 메시지가 표시됩니다.
17. 노드 이름 및 포트를 지정합니다. "다음"을 클릭합니다.
보고서(CMS) 데이터베이스를 구성하라는 메시지가 표시됩니다.
중요! 보고서 서버는 CA 제품 간에 공유할 수 있는 CA 공용 구성 요소입니다. 따라서 SiteMinder 가 아닌 다른 제품이 지원하는 데이터베이스 유형 및 버전으로 보고서 데이터베이스를 구성할 수 있습니다. 지원되는 데이터베이스 유형 및 버전 목록에 대해서는 "SiteMinder 12.52 SP1 Platform Support Matrix"(SiteMinder 12.52 SP1 플랫폼 지원표)를 참조하십시오.
18. 다음 단계 중 하나를 수행합니다.
 - (권장) MySQL 을 구성하는 경우 루트 사용자 계정에 대한 암호와 보고서 데이터베이스 관리자 자격 증명을 입력합니다.

- Microsoft SQL Server 를 구성하는 경우:
 - a. "SQL Server (ODBC)"를 선택하고 "Browse"(찾아보기)를 클릭하여 "SQL Server Logon"(SQL Server 로그인) 화면을 엽니다.
 - b. DSN 을 선택하고 관리자 자격 증명을 입력합니다.

참고: 64 비트 버전의 Windows 를 설치하는 경우 "Consume DSN created under WOW64"(WOW64 아래에서 생성된 DSN 사용)를 선택하십시오. 이 옵션을 선택하면 32 비트 DSN 을 사용할 수 있습니다.

- c. "확인"을 클릭합니다.
- Oracle 을 구성하는 경우 서비스 이름 및 관리자 자격 증명에 필요한 값을 입력합니다.

참고: 감사 데이터베이스를 구성하지 마십시오. 이 구성 요소는 SiteMinder 감사 기반 보고서와 관련이 없습니다. 콘텐츠 관리 서버 감사 데이터베이스는 보고서 서버와 관련된 감사 활동에 사용되며 SiteMinder 에는 사용되지 않습니다. 감사 기반 보고서를 실행하려면 SiteMinder 감사 데이터베이스가 필요합니다.

19. "다음"을 클릭합니다.

웹 응용 프로그램 서버를 선택하라는 메시지가 표시됩니다.

20. 다음 단계를 완료합니다.

- a. "Install Tomcat application server and deploy to it"(Tomcat 응용 프로그램 서버 설치 후 해당 서버에 배포)을 선택합니다.

참고: SiteMinder 는 포함된 Apache Tomcat 버전만 지원합니다.

- b. "IIS Web Application Server"(IIS 웹 응용 프로그램 서버) 옵션을 해제합니다.
- c. "다음"을 클릭합니다.

Apache Tomcat 정보를 묻는 메시지가 표시됩니다.

21. Apache Tomcat 포트를 입력하고 "Next"(다음)를 클릭합니다.

설치를 시작할지 묻는 메시지가 표시됩니다.

22. "Next"(다음)를 클릭하여 설치를 시작합니다.

설치가 완료되면 메시지가 표시됩니다.

23. "Launch SAP BusinessObjects Administration Console"(SAP BusinessObjects 관리 콘솔 시작) 옵션을 해제하고 "Finish"(마침)를 클릭합니다.
보고서 서버가 설치되었습니다.

UNIX

다음 단계를 수행하십시오.

1. [설치 검사 목록](#) (페이지 470)을 검토했는지 확인합니다.
2. [설치 관리자에 필요한 정보](#) (페이지 479)를 수집했는지 확인합니다.
3. 루트 사용자 계정을 사용하여 설치를 시작하고 있는지 확인합니다.
4. 실행 중인 응용 프로그램을 모두 종료합니다.
5. Bourne 셸을 열고 설치 미디어 위치로 이동합니다.
6. 다음 명령을 입력합니다.

```
./installation_media -i console
```

installation_media

보고서 서버 설치 실행 파일을 지정합니다.

CA Business Intelligence 설치 관리자가 시작되고 로깅을 묻는 메시지가 표시됩니다.

참고: 설치 미디어 이름의 목록에 대해서는 정책 서버 릴리스 정보를 참조하십시오.

7. 영어에 해당하는 값을 입력하고 Enter 키를 누릅니다.
설치 관리자 소개가 나타납니다.
8. Enter 키를 누릅니다.
CA 사용권 계약이 나타납니다.
9. 다음 단계를 완료합니다.
 - a. Enter 키를 눌러 사용권 계약의 다음 단계로 이동합니다.
 - b. y 를 입력하여 사용권 계약에 동의합니다.
 - c. Enter 키를 누릅니다.
 루트 아닌 사용자의 자격 증명을 묻는 메시지가 표시됩니다.

10. 사용자 이름 및 그룹 이름을 입력하고 **Enter** 키를 누릅니다.
CA 공유 구성 요소 디렉터리의 경로를 지정하라는 메시지가 표시됩니다.
11. 기본값을 그대로 두고 **Enter** 키를 누릅니다.
CA 샘플 템플릿을 설치할지 묻는 메시지가 표시됩니다.
12. **N** 을 입력하고 **Enter** 키를 누릅니다.
참고: CA 샘플 템플릿은 SiteMinder 보고 템플릿과 관련이 없습니다.
SiteMinder 보고서 서버 구성 마법사가 필요한 보고 템플릿을 설치합니다. 보고서 서버를 설치한 후 이 마법사를 실행하십시오.
자동 설치용 응답 파일을 저장할 것인지 묻는 메시지가 표시됩니다.
13. **Y** 를 입력하고 **Enter** 키를 누릅니다.
설치 요약이 나타납니다.
14. 요약 내용을 검토하고 **Enter** 키를 누릅니다.
구성 요소가 설치됩니다. SAP BusinessObjects Enterprise 설치 관리자에서 설치 언어를 선택하라는 메시지가 표시됩니다.
15. "English"(영어)를 선택하고 **Enter** 키를 누릅니다.
SAP BusinessObjects Enterprise 사용권 계약이 나타납니다.
16. **y** 를 눌러 사용권 계약에 동의합니다.
보고서 서버 설치 디렉터리를 입력하라는 메시지가 표시됩니다.
17. **Tab** 키를 눌러 기본 설정을 자동 완성하고 **Enter** 키를 누릅니다.
언어 팩을 선택하라는 메시지가 표시됩니다. 기본적으로 영어가 선택되어 있습니다.
18. 기본값을 그대로 두고 **Enter** 키를 누릅니다.
설치 유형에 대한 메시지가 표시됩니다.
19. "User - Regular SAP BusinessObjects Enterprise installation"(사용자 - 일반 SAP BusinessObjects Enterprise 설치)을 선택하고 **Enter** 키를 누릅니다.
설치 유형에 대한 메시지가 표시됩니다.

20. "New"(새로 만들기)를 선택하고 Enter 키를 누릅니다.

참고: "Enable servers after installation"(설치 후 서버 활성화) 옵션을 해제하지 마십시오.

콘텐츠 관리 서버 포트와 SAP BusinessObjects Enterprise 관리자 계정의 암호를 묻는 메시지가 표시됩니다.

21. 다음 단계를 완료합니다.

- a. 콘텐츠 관리 서버가 연결하고 요청을 수신 대기해야 하는 포트를 지정합니다.
- b. 기본 SAP BusinessObjects Enterprise 관리자의 암호를 지정합니다.
- c. Enter 키를 누릅니다.

보고서(CMS) 데이터베이스 기능을 수행할 데이터베이스 유형을 선택하라는 메시지가 표시됩니다.

22. 다음 단계 중 하나를 완료하십시오.

- (권장) 포함된 MySQL 버전을 설치하려면 "Install MySQL"(MySQL 설치)을 선택하고 Enter 키를 누릅니다.
- 기존 Oracle 데이터베이스를 구성하려면 "Use an existing database server"(기존 데이터베이스 서버 사용)를 선택하고 Enter 키를 누릅니다.
- (RHEL 6) SQLAnywhere 를 설치하려면 "Install SQLAnywhere"(SQLAnywhere 설치)를 선택하고 Enter 키를 누릅니다.

중요! 보고서 서버는 CA 제품 간에 공유할 수 있는 CA 공용 구성 요소입니다. 따라서 SiteMinder 가 아닌 다른 제품이 지원하는 데이터베이스 유형 및 버전으로 보고서 데이터베이스를 구성할 수 있습니다. 지원되는 데이터베이스 유형 및 버전 목록에 대해서는 "SiteMinder 12.52 SP1 Platform Support Matrix"(SiteMinder 12.52 SP1 플랫폼 지원표)를 참조하십시오.

추가적인 보고서 데이터베이스 정보를 묻는 메시지가 표시됩니다.

23. 다음 단계 중 하나를 완료하십시오.

- (MySQL/SQLAnywhere) 루트 사용자 계정에 필요한 값과 보고서 데이터베이스 관리자 자격 증명을 입력합니다.

- (Oracle) 다음 단계를 완료합니다.
 - a. "Oracle"을 선택하고 Enter 키를 누릅니다.
데이터베이스 정보를 묻는 메시지가 표시됩니다.
 - b. 서비스 이름 및 관리자 자격 증명을 입력합니다.

24. Enter 키를 누릅니다.

- 포함된 MySQL 버전을 설치하는 경우 감사 데이터베이스 정보를 묻는 메시지가 표시됩니다.
- Oracle 을 구성하는 경우 감사 데이터베이스를 설치할지 묻는 메시지가 표시됩니다.

감사 데이터베이스는 SiteMinder 감사 기반 보고서와 관련이 없습니다. 콘텐츠 관리 서버 감사 데이터베이스는 보고서 서버와 관련된 감사 활동에 사용되며 SiteMinder 에는 사용되지 않습니다. 감사 기반 보고서를 실행하려면 SiteMinder 감사 데이터베이스가 필요합니다.

25. 다음 단계 중 하나를 완료합니다.

- (MySQL/SQLAnywhere) 기본값을 적용하고 Enter 키를 누릅니다.
- (Oracle) 다음 단계를 완료합니다.
 - a. "Do not install Auditing Database"(감사 데이터베이스 설치 안 함) 옵션을 선택합니다.
 - b. Enter 키를 누릅니다.
데이터베이스를 다시 초기화할지 묻는 메시지가 표시됩니다.
 - c. "Yes"(예)를 선택하고 Enter 키를 누릅니다.

서비스 인텔리전스 에이전트 노드 이름 및 포트를 묻는 메시지가 표시됩니다.

26. 노드 이름과 포트를 입력하고 Enter 키를 누릅니다.

웹 응용 프로그램 서버를 선택하라는 메시지가 표시됩니다.

27. Install Tomcat deploy web applications"(Tomcat 배포 웹 응용 프로그램 설치) 옵션을 선택합니다.

참고: SiteMinder 는 포함된 Apache Tomcat 버전만 지원합니다.

Apache Tomcat 포트를 묻는 메시지가 표시됩니다.

28. 필요한 Apache Tomcat 포트 정보를 입력하고 Enter 키를 누릅니다.

설치 디렉터리 경로가 표시됩니다.

29. Enter 키를 눌러 설치를 시작합니다.

설치 진행률이 표시되고 설치가 완료되면 확인 메시지가 표시됩니다.

30. Enter 키를 눌러 설치 관리자를 종료합니다.

보고서 서버 설치 문제 해결

다음 파일을 사용하여 보고서 서버 설치 문제를 해결할 수 있습니다.

- CA_Business_Intelligence_InstallLog.log

먼저 이 로그를 열고 보고된 오류를 확인하는 것이 좋습니다.

- ca-install.log

이 파일의 맨 아래로 스크롤하여 보고된 오류를 확인하는 것이 좋습니다.

"BIEK_GetExitCode"를 검색하여 "BIEK_GetExitCode" 함수의 반환 값을 확인하십시오. 반환된 값이 0 이 아니면 설치 오류가 있는 것입니다.

다음 키워드를 검색하여 오류 원인을 확인하십시오.

- Error
- Warning
- CMS
- InfoStore

로그 파일은 설치 중 임시 위치에 저장됩니다. 임시 위치는 시스템의 TEMP 환경 속성에 따라 결정됩니다. 설치가 제대로 이루어지지 않은 경우, 로그 파일을 여기에 임시적으로 저장할 수 있습니다. 설치에 성공한 경우 로그 파일은 보고서 서버 설치 디렉터리의 최상위 수준에 저장됩니다.

보고서 템플릿 설치 방법

다음 절차에 따라 보고서 템플릿을 설치하십시오.

1. 설치 관리자에 필요한 정보를 수집합니다.
2. 보고서 템플릿을 설치합니다.
3. 보고서 서버를 다시 시작합니다.
4. 작업 서버 서비스 시간 만료 값을 늘립니다.

설치 관리자에 필요한 정보 수집

보고서 서버 구성 마법사를 실행하려면 다음 정보가 필요합니다.

- **BusinessObjects 관리자 암호** - 기본 BusinessObjects 관리자 계정의 암호를 식별합니다. 보고서 서버 설치 관리자는 설치 중에 기본 관리 계정을 생성합니다. 설치를 완료하려면 이 계정의 암호가 필요합니다. 보고서 서버 구성 마법사가 기본 관리 계정을 사용하여 보고서 템플릿을 설치하려면 암호가 필요합니다.
- **SiteMinder 감사 데이터베이스 유형** - SiteMinder 감사 데이터베이스로 사용할 데이터베이스의 유형을 식별합니다. 감사 기반 보고서를 실행하려면 별도의 SiteMinder 감사 데이터베이스가 필요합니다. 보고서 서버 구성 마법사에서 보고서 서버가 감사 데이터베이스 유형을 기반으로 한 보고서 템플릿 집합을 사용하도록 구성하려면 데이터베이스 유형이 필요합니다.

참고: 보고서 서버 구성 마법사를 실행하기 전에 SiteMinder 감사 데이터베이스를 구성할 필요는 없습니다.

보고서 템플릿을 설치하기 전에 필요한 정보를 수집 및 기록하는 데 유용하도록 워크시트가 제공됩니다.

보고서 템플릿 설치

보고서 서버 구성 마법사를 사용하여 SiteMinder 보고서 템플릿을 설치하십시오. 다음 단원에서는 Windows 및 UNIX 에서 보고서 서버 구성 마법사를 실행하는 방법에 대해 자세히 설명합니다.

설치하기 전에

보고서 템플릿을 설치하기 전에 다음 항목을 확인하십시오.

- 기술 지원 사이트의 설치 미디어를 사용하여 보고서 서버 구성 마법사를 실행하십시오.

참고: 설치 미디어 이름의 목록에 대해서는 *정책 서버 릴리스 정보*를 참조하십시오.

중요! (UNIX) 설치 미디어를 사용하려면 실행 권한이 있어야 합니다. 권한을 추가하려면 다음 명령을 실행하십시오.

```
chmod +x installation_media
```

installation_media

보고서 서버 구성 마법사 설치 실행 파일의 이름을 지정합니다.

- (UNIX) 서로 다른 서브넷 전체에 걸쳐 보고서 서버 구성 마법사를 실행하면 충돌이 발생합니다. 보고서 서버 호스트 시스템에서 직접 보고서 템플릿을 설치하십시오.

Windows

Windows 에 보고서 템플릿을 설치하려면

1. [설치 관리자에 필요한 정보](#) (페이지 494)를 수집했는지 확인합니다.
2. 실행 중인 응용 프로그램을 모두 종료합니다.
3. *installation_media* 를 두 번 클릭합니다.

installation_media

보고서 서버 구성 마법사 설치 실행 파일의 이름을 지정합니다.

설치 관리자가 시작됩니다.

참고: 설치 미디어 이름의 목록에 대해서는 *정책 서버 릴리스 정보*를 참조하십시오.

4. 값이 요구될 때마다 완성된 보고서 서버 구성 워크시트를 사용하여 필요한 값을 입력합니다.
5. 설치 설정을 검토하고 "설치"를 클릭합니다.
보고서 템플릿이 설치됩니다.
6. 보고서 서버를 다시 시작합니다.

보고서 서버가 SiteMinder 보고서 템플릿을 사용하도록 구성됩니다.

UNIX GUI

UNIX GUI 를 사용하여 보고서 템플릿을 설치하려면

1. [설치 관리자에 필요한 정보](#) (페이지 494)를 수집했는지 확인합니다.
2. 실행 중인 응용 프로그램을 모두 종료합니다.
3. 셸을 열고 설치 미디어를 탐색합니다.
4. 다음 명령을 입력합니다.

```
./installation_media  
installation_media
```

보고서 서버 구성 마법사 설치 실행 파일의 이름을 지정합니다.
설치 관리자가 시작됩니다.

참고: 설치 미디어 이름의 목록에 대해서는 *정책 서버 릴리스 정보*를 참조하십시오.

5. 값이 요구될 때마다 완성된 보고서 서버 구성 워크시트를 사용하여 필요한 값을 입력합니다.

참고: Solaris 보고서 서버에 지원되는 감사 데이터베이스는 Oracle 뿐입니다. 따라서 Solaris 에 보고서 서버를 설치한 경우에는 감사 데이터베이스 유형을 묻는 메시지가 표시되지 않습니다. 보고서 서버 구성 마법사는 Oracle 관련 보고서 템플릿을 자동으로 설치합니다.

6. 설치 설정을 검토하고 "설치"를 클릭합니다.

보고서 템플릿이 설치됩니다.

7. 보고서 서버를 다시 시작합니다.

보고서 서버가 SiteMinder 보고서 템플릿을 사용하도록 구성됩니다.

UNIX 콘솔

UNIX 콘솔을 사용하여 보고서 템플릿을 설치하려면

1. [설치 관리자에 필요한 정보](#) (페이지 494)를 수집했는지 확인합니다.
2. 실행 중인 응용 프로그램을 모두 종료합니다.
3. 셸을 열고 설치 미디어를 탐색합니다.

4. 다음 명령을 입력합니다.

```
./installation_media -i console
```

installation_media

보고서 서버 구성 마법사 설치 실행 파일의 이름을 지정합니다.

-i console

UNIX 콘솔에서 설치를 시작하도록 지정합니다.

설치 관리자가 시작됩니다.

참고: 설치 미디어 이름의 목록에 대해서는 *정책 서버 릴리스 정보*를 참조하십시오.

5. 값이 요구될 때마다 완성된 보고서 서버 구성 워크시트를 사용하여 필요한 값을 입력합니다.

참고: Solaris 보고서 서버에 지원되는 감사 데이터베이스는 Oracle 뿐입니다. 따라서 Solaris 에 보고서 서버를 설치한 경우에는 감사 데이터베이스 유형을 묻는 메시지가 표시되지 않습니다. 보고서 서버 구성 마법사는 Oracle 관련 보고서 템플릿을 자동으로 설치합니다.

6. 설치 설정을 검토하고 Enter 키를 누릅니다.

보고서 템플릿이 설치됩니다.

7. 보고서 서버를 다시 시작합니다.

보고서 서버가 SiteMinder 보고서 템플릿을 사용하도록 구성됩니다.

작업 서버 서비스 시간 만료 값 늘리기

일부 보고서 서버 서비스는 기본 시간 만료 값이 10 분입니다. 보고서 서버에서 대용량 분석 보고서를 생성할 경우에는 10 분 이상이 걸릴 수 있습니다.

대용량 분석 보고서가 제대로 생성되도록 Crystal Reports 작업 서버 서비스의 시간 만료 값을 늘리십시오.

Windows 에서 시간 만료 값 늘리기

다음 단계를 수행하십시오.

1. "시작", "프로그램", "BusinessObjects XI Release 3.1", "BusinessObjects Enterprise", "Central Configuration Manager"를 차례로 클릭합니다.

Central Configuration Manager 콘솔이 나타납니다.

2. Crystal Reports 작업 서버를 마우스 오른쪽 단추로 클릭한 다음 "Stop"(중지)을 선택합니다.

Crystal Reports 작업 서버 서비스가 중지됩니다.

3. Crystal Reports 작업 서버를 마우스 오른쪽 단추로 클릭한 다음 "Properties"(속성)를 선택합니다.

Crystal Reports 작업 서버 속성 대화 상자가 나타납니다.

4. "Properties"(속성) 탭에서 "Command"(명령) 필드의 끝에 다음 항목을 추가합니다.

`-requesttimeout 6000000`

참고: 시간 만료 값의 측정 단위는 밀리초입니다. 6000000 을 지정하여 시간 만료 값을 1 시간 늘립니다.

5. "확인"을 클릭합니다.

Central Configuration Manager 가 나타납니다.

6. Crystal Reports 작업 서버를 마우스 오른쪽 단추로 클릭한 다음 "Start"(시작)를 선택합니다.

Crystal Reports 작업 서버 서비스가 시작됩니다.

7. Central Configuration Manager 를 종료합니다.

Crystal Reports 작업 서버 서비스의 시간 만료 값이 1 시간으로 설정됩니다.

UNIX 에서 시간 만료 값 늘리기

다음 단계를 수행하십시오.

1. `report_server_home/CommonReporting3/bobje` 로 이동합니다.

`report_server_home`

보고서 서버 설치 경로를 지정합니다.

2. `ccm.config` 파일을 열고 `reportjobserverLAUNCH` 키의 값 끝에 다음 항목을 추가합니다.

```
-requesttimeout 6000000
```

참고: 시간 만료 값의 측정 단위는 밀리초입니다. `6000000` 을 지정하여 시간 만료 값을 1 시간 늘립니다.

3. `ccm.config` 파일을 저장하고 닫습니다.

Crystal Reports 작업 서버 서비스의 시간 만료 값이 1 시간으로 설정됩니다.

보고서 서버 등록 방법

보고서 서버를 등록하려면 정책 서버 호스트 시스템, 보고서 서버 호스트 시스템 및 관리 UI 호스트 시스템에 액세스해야 합니다. 등록 프로세스는 다음과 같습니다.

- 보고서 서버와 정책 서버 간에 트러스트 관계를 설정합니다.
- 보고서 서버와 관리 UI 간에 트러스트 관계를 설정합니다.

보고서 서버를 등록하려면 다음 단계를 완료하십시오.

1. 클라이언트 이름 및 암호를 생성합니다.
2. 등록 정보를 수집합니다.
3. 보고서 서버를 정책 서버에 등록합니다.
4. 보고서 서버를 다시 시작합니다.
5. 관리 UI 에 대한 연결을 구성합니다.

클라이언트 이름 및 암호 만들기

XPSRegClient 유틸리티를 실행하여 클라이언트 이름 및 암호를 생성하십시오. 클라이언트 이름 및 암호의 용도는 다음과 같습니다.

- 등록할 보고서 서버를 정책 서버에서 식별하는 데 사용됩니다.
- XPSRegClient 도구로 보고서 서버를 정책 서버에 등록하는 데 사용됩니다.

등록 도구를 실행하려면

1. 정책 서버 호스트 시스템에서 명령줄 창을 엽니다.
2. *siteminder_home/bin* 으로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

3. 다음 명령을 실행합니다.

```
XPSRegClient client_name[:passphrase] -report -t timeout -r retries  
-c comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

client_name

등록할 보고서 서버의 이름을 식별합니다.

제한: 이 값은 고유해야 합니다. 예를 들어 이전에 reportserver1 을 사용했으면 reportserver2 를 입력합니다.

참고: 이 값을 기록해 두십시오. 이 값은 보고서 서버 호스트 시스템에서 등록 프로세스를 완료하는 데 필요합니다.

passphrase

보고서 서버 등록을 완료하는 데 필요한 암호를 지정합니다.

제한: 암호는 다음 조건을 충족해야 합니다.

- 6 자 이상을 포함해야 합니다.
- 암호에 앰퍼샌드(&)나 별표(*)는 포함할 수 없습니다.
- 암호에 공백이 포함되어 있는 경우 암호를 따옴표로 묶어야 합니다.

이 단계에서 암호를 지정하지 않으면 XPSRegClient 에서 암호를 입력하고 확인하라는 메시지가 표시됩니다.

참고: 이 값을 기록해 두십시오. 이 값은 보고서 서버 호스트 시스템에서 등록 프로세스를 완료하는 데 필요합니다.

-report

보고서 서버를 등록하도록 지정합니다.

-t timeout

(선택 사항) 보고서 서버 호스트 시스템에서 등록 프로세스를 완료해야 하는 시간을 지정합니다. 이 시간 만료 값에 도달할 경우 정책 서버에서는 등록 요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 1

최대 제한: 1440(1 일)

-r retries

(선택 사항) 보고서 서버 호스트 시스템에서 등록 프로세스를 완료할 때 허용되는 시도 실패 횟수를 지정합니다. 등록 중 정책 서버에 제출한 암호가 올바르지 않으면 등록 시도가 실패할 수 있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을 삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 등록 도구에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: siteminder_home\log. 여기서 siteminder_home 은 정책 서버가 설치된 위치입니다.

-e error path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: stderr

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

등록 로그 파일의 이름이 표시됩니다. 암호를 제공하지 않은 경우 암호를 묻는 메시지가 표시됩니다.

4. Enter 키를 누릅니다.

클라이언트 이름 및 암호가 생성됩니다.

이제 보고서 서버를 정책 서버에 등록할 수 있습니다. 보고서 서버 호스트 시스템에서 등록 프로세스를 완료합니다.

등록 정보 수집

보고서 서버와 정책 서버 간의 등록 프로세스를 완료하려면 특정 정보가 필요합니다. 보고서 서버 호스트 시스템에서 XPSRegClient 유틸리티를 실행하기 전에 다음 정보를 수집하십시오.

- **클라이언트 이름** - XPSRegClient 도구를 사용하여 지정한 클라이언트 이름입니다.
- **암호** - XPSRegClient 도구를 사용하여 지정한 암호입니다.
- **정책 서버 호스트** - 정책 서버 호스트 시스템의 IP 주소 또는 이름입니다.

정책 서버에 보고서 서버 등록

정책 서버에 보고서 서버를 등록하여 두 구성 요소 간에 트러스트 관계를 생성하십시오. 보고서 서버 등록 도구를 사용하여 보고서 서버 호스트 시스템에서 연결을 구성하십시오.

다음 단계를 수행하십시오.

1. 보고서 서버 호스트 시스템에서 명령줄 창을 열고 `report_server_home\external\scripts` 로 이동합니다.

`report_server_home`

보고서 서버 설치 위치를 지정합니다.

기본값: (Windows) C:\Program Files\CA\SC\CommonReporting3

기본값: (UNIX) /opt/CA/SharedComponents/CommonReporting3

2. 다음 명령 중 하나를 실행합니다.

■ (Windows)

```
regreportserver.bat -pshost host_name -client client_name -passphrase
passphrase -psport portnum -fipsmode 0|1
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

■ (UNIX)

```
regreportserver.sh -pshost host_name -client client_name -passphrase
passphrase -psport portnum -fipsmode 0|1
```

`-pshost host name`

보고서 서버를 등록하는 정책 서버 호스트 시스템의 IP 주소 또는 이름을 지정합니다.

`-client client name`

클라이언트 이름을 지정합니다. 클라이언트 이름은 등록하려는 보고서 서버 인스턴스를 식별합니다.

참고: 이 값은 정책 서버 호스트 시스템에서 보고서 서버를 등록할 때 XPSRegClient 유틸리티를 사용하여 지정한 클라이언트 이름과 일치해야 합니다.

예: XPSRegClient 유틸리티를 사용할 때 "reportserver1"을 지정한 경우 "reportserver1"을 입력합니다.

-passphrase *passphrase*

클라이언트 이름과 쌍을 이루는 암호를 지정합니다. 클라이언트 이름은 등록하려는 보고서 서버 인스턴스를 식별합니다.

참고: 이 값은 정책 서버 호스트 시스템에서 보고서 서버를 등록할 때 XPSRegClient 유틸리티를 사용하여 지정한 암호와 일치해야 합니다.

예: XPSRegClient 유틸리티를 사용할 때 SiteMinder 를 지정한 경우 SiteMinder 를 입력합니다.

-psport *portnum*

(선택 사항) 정책 서버가 등록 요청을 수신 대기하는 포트를 지정합니다.

fipsmode

(선택 사항) 보고서 서버와 정책 서버 간의 통신이 암호화되는 방식을 지정합니다.

기본값: 0

- 0 은 FIPS 호환성 모드를 지정합니다.
- 1 은 FIPS 전용 모드를 지정합니다.

3. Enter 키를 누릅니다.

등록했음을 알리는 메시지가 표시됩니다.

보고서 서버 다시 시작

(Windows) 다음 단계를 수행하십시오.

1. "시작", "프로그램", "BusinessObjects XI 3.1", "BusinessObjects Enterprise", "Central Configuration Manager"를 차례로 클릭합니다.

Central Configuration Manager 콘솔이 나타납니다.

2. Apache Tomcat 서비스와 Server Intelligence Agent 서비스를 중지합니다.
보고서 서버가 중지됩니다.
3. Apache Tomcat 서비스와 Server Intelligence Agent 서비스를 시작합니다.
보고서 서버가 다시 시작됩니다.

(UNIX) 다음 단계를 수행하십시오.

1. 보고서 서버를 설치한 시스템에 루트 아닌 사용자로 로그인합니다.
2. 다음 환경 변수 중 적어도 하나가 유효한 utf8/UTF-8 로캘로 설정되어 있는지 확인합니다.

- LC_ALL
- LANG
- LC_CTYPE

3. *report_server_home/CommonReporting3/external/scripts* 로 이동하여 다음 명령을 실행합니다.

```
../setupenv.sh
```

report_server_home

보고서 서버 설치 경로를 지정합니다.

4. 다음을 확인합니다.

- IAM_RPTSRV_HOME 변수가 *report_server_home/CommonReporting3* 으로 설정되어 있어야 합니다.

report_server_home

보고서 서버 설치 경로를 지정합니다.

- (Oracle 보고서 데이터베이스만 해당) LD_LIBRARY_PATH 변수는 다음과 같이 설정되어 있습니다.

```
$ORACLE_HOME/lib32:$ORACLE_HOME/lib:$LD_LIBRARY_PATH
```

예:

```
export
LD_LIBRARY_PATH=$ORACLE_HOME/lib32:$ORACLE_HOME/lib:$LD_LIBRARY_PATH
```

5. *report_server_home/CommonReporting3/bobje* 로 이동하여 다음 명령을 실행합니다.

```
./stopservers
```

report_server_home

보고서 서버 설치 경로를 지정합니다.

6. 다음 명령을 실행합니다.

```
./tomcatshutdown.sh
```

보고서 서버가 중지됩니다.

7. 다음 명령을 실행합니다.

```
./startservers
```

8. 다음 명령을 실행합니다.

```
./tomcatstartup.sh
```

보고서 서버가 다시 시작됩니다.

관리 UI 에 대한 연결 구성

보고서 서버와 관리 UI 간의 연결을 구성하여 두 구성 요소 간의 트러스트 관계를 구성하십시오. 관리 UI 에서 연결을 구성합니다.

참고: 관리 UI 는 하나 이상의 정책 서버와 트러스트 관계에 있을 수 있습니다. 하지만 각 트러스트 관계에서 보고서 서버 연결은 하나만 허용됩니다. 새 보고서 서버에 연결해야 할 경우 현재 보고서 서버 연결을 삭제하거나 다른 정책 서버에 연결하여 연결을 구성하십시오.

관리 UI 에 대한 연결을 구성하려면

1. 관리 UI 에 로그인합니다.
2. "관리", "관리 UI"를 차례로 클릭합니다.
3. "보고서 연결", "보고서 서버 연결 만들기"를 차례로 클릭합니다.

"보고서 서버 연결 만들기" 창이 표시됩니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

4. "연결 이름" 필드에 연결 이름을 입력합니다.
5. "보고서 서버 호스트" 필드에 보고서 서버 호스트의 시스템 이름이나 IP 주소를 입력합니다.
6. "Tomcat 포트" 필드에 Apache Tomcat 연결 포트를 입력합니다.

참고: 이 값은 보고서 서버를 설치할 때 입력한 웹 서버 포트입니다.

7. 해당 필드에 관리자 암호를 입력합니다.

참고: 이 값은 보고서 서버를 설치할 때 기본 BusinessObjects 관리자 계정에 대해 입력한 암호입니다.

8. "제출"을 클릭합니다.

보고서 서버와 관리 UI 간의 연결이 구성됩니다.

보고서 서버 설치 및 등록을 완료했습니다. 이제 정책 분석 보고서를 실행할 수 있습니다.

참고: 감사 보고서를 생성하고 관리하려면 별도의 감사 데이터베이스가 필요합니다.

감사 데이터베이스 구성 방법

SiteMinder 감사 기반 보고서를 실행하려면 SiteMinder 감사 데이터베이스가 필요합니다.

참고: 감사 정보를 텍스트 파일에 기록할 수도 있지만 감사 기반 보고서를 생성하고 관리하려면 지원되는 ODBC 데이터베이스에 감사 정보를 저장해야 합니다. 지원되는 버전 목록은 "SiteMinder 12.52 SP1 Platform Support Matrix"(SiteMinder 12.52 SP1 플랫폼 지원표)를 참조하십시오.

감사 데이터베이스를 구성하려면 다음 단계를 완료하십시오.

1. (선택 사항) 아직 SiteMinder 감사 데이터베이스를 구성하지 않은 경우 구성합니다.

중요! Oracle 에서 감사 데이터베이스를 구성하는 경우 DB 역할이 없는 사용자 계정을 제공해야 합니다. 사용자 계정에 DB 역할이 있으면 감사 기반 보고서에 올바른 결과가 반환되지 않습니다.

2. 감사 데이터베이스를 관리 UI 에 등록합니다.
3. 감사 데이터베이스와 보고서 서버 간의 연결을 구성합니다.

관리 UI 에 감사 데이터베이스 등록

관리 UI 에 감사 데이터베이스를 등록하여 구성 요소 간의 트러스트된 연결을 생성하십시오. 관리 UI 에 감사 데이터베이스를 등록하면 SiteMinder 관리자가 감사 기반 보고서를 생성하고 관리할 수 있습니다.

참고: 관리 UI 는 하나 이상의 정책 서버와 트러스트 관계에 있을 수 있습니다. 하지만 각 트러스트 관계에서 감사 데이터베이스 연결은 하나만 허용됩니다. 새 감사 데이터베이스에 연결해야 할 경우 현재 연결을 삭제하거나 다른 정책 서버에 연결하여 연결을 구성하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "관리", "관리 UI"를 차례로 클릭합니다.
3. "보고서 연결", "감사 보고서 연결 만들기"를 차례로 클릭합니다.

"감사 보고서 연결 만들기" 창이 표시됩니다.

참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.

4. "데이터베이스 공급업체" 드롭다운 목록에서 데이터베이스 공급업체를 선택합니다.

공급업체 관련 필드가 표시됩니다.

5. "연결 이름" 필드에 연결 이름을 입력합니다.
6. "데이터베이스 서버 호스트" 필드에 감사 데이터베이스 호스트의 시스템 이름이나 IP 주소를 입력합니다.

7. "DSN" 필드에 감사 데이터베이스 데이터 원본 정보를 입력합니다.
 - **Oracle** - 감사 데이터베이스 DSN 을 생성할 때 지정한 Oracle Net Service 이름을 입력합니다.
참고: 서비스 이름은 감사 데이터베이스와 정책 서버의 연결을 구성할 때 정책 서버 관리 콘솔의 "데이터" 탭에서 입력한 DSN 과 연결되어 있어야 합니다. 서비스 이름은 보고서 서버에서 생성하는 DSN 과 일치해야 합니다.
 - **SQL Server** - DSN 을 입력합니다.
참고: DSN 이름은 감사 데이터베이스와 정책 서버의 연결을 구성할 때 정책 서버 관리 콘솔의 "데이터" 탭에서 지정한 DSN 과 일치해야 합니다. DSN 이름은 보고서 서버에서 생성하는 DSN 과도 일치해야 합니다.
8. "데이터베이스 서버 포트" 필드에 감사 데이터베이스 서버가 수신 대기하는 포트를 입력합니다.
9. 다음 단계 중 *하나*를 완료하십시오.
 - **Oracle** - "서비스 이름" 필드에 Oracle Net Service 이름을 다시 입력합니다.
 - **SQL Server** - "데이터베이스 이름" 필드에 감사 데이터베이스 이름을 입력합니다.
10. 해당 필드에 감사 데이터베이스 관리자의 자격 증명을 입력합니다.
참고: 관리자 자격 증명은 감사 데이터베이스와 정책 서버의 연결을 구성할 때 정책 서버 관리 콘솔의 "데이터" 탭에서 지정한 자격 증명과 일치해야 합니다.
11. 제출을 클릭합니다.
 감사 데이터베이스가 관리 UI 에 등록됩니다.

감사 데이터베이스와 보고서 서버의 연결

보고서 서버는 감사 기반 보고서를 생성하기 위해 SiteMinder 감사 데이터베이스에 연결합니다. 관리 UI 에서 감사 기반 보고서를 예약하면 관리 UI 는 다음 정보를 보고서 서버에 전달합니다.

- (Oracle) 감사 데이터베이스를 식별하는 Oracle Net Service 이름
- (Microsoft SQL Server) 다음 항목의 이름
 - 감사 데이터베이스
 - 감사 데이터베이스에 연결하는 데 사용되는 데이터 원본
- 감사 데이터베이스에 액세스하는 데 필요한 사용자 계정 자격 증명

감사 데이터베이스와 보고서 서버 간의 연결을 구성하려면 다음 작업 중 하나를 수행하십시오.

- (Oracle) 다음 사항을 확인합니다.
 - Oracle Net 클라이언트가 보고서 서버 호스트 시스템에 설치되어 있어야 합니다.
 - 감사 데이터베이스를 식별하는 Oracle Net Service 이름이 보고서 서버 호스트 시스템의 tnsnames.ora 파일에 있어야 합니다.
- (Microsoft SQL Server) 감사 데이터베이스에 연결하는 데 사용되는 데이터 원본이 보고서 서버 호스트 시스템에 있습니다.

참고: 지원되는 데이터베이스 드라이버에 대한 자세한 내용은 "12.52 SP1 SiteMinder Platform Support Matrix"(12.52 SP1 SiteMinder 플랫폼 지원표)를 참조하십시오.

보고서 서버 시작

(Windows) 다음 단계를 수행하십시오.

1. "시작", "프로그램", "BusinessObjects XI 3.1", "BusinessObjects Enterprise", "Central Configuration Manager"를 차례로 클릭합니다.
Central Configuration Manager 콘솔이 나타납니다.
2. Apache Tomcat 서비스와 Server Intelligence Agent 서비스를 시작합니다.
보고서 서버가 시작됩니다.

(UNIX) 다음 단계를 수행하십시오.

1. 보고서 서버를 설치한 시스템에 루트 아닌 사용자로 로그인합니다.
2. 다음 환경 변수 중 적어도 하나가 유효한 utf8/UTF-8 로캘로 설정되어 있는지 확인합니다.

- LC_ALL
- LANG
- LC_CTYPE

3. *report_server_home/CommonReporting3/external/scripts* 로 이동하여 다음 명령을 실행합니다.

```
../setupenv.sh
```

report_server_home

보고서 서버 설치 경로를 지정합니다.

4. 다음을 확인합니다.

- IAM_RPTSRV_HOME 변수가 *report_server_home/CommonReporting3* 으로 설정되어 있어야 합니다.

report_server_home

보고서 서버 설치 경로를 지정합니다.

- (Oracle 보고서 데이터베이스에만 해당) LD_LIBRARY_PATH 변수가 \$ORACLE_HOME/lib32:\$ORACLE_HOME/lib:\$ETPKIHOME/lib:\$LD_LIBRARY_PATH 로 설정되어 있어야 합니다.

예: export

```
LD_LIBRARY_PATH=$ORACLE_HOME/lib32:$ORACLE_HOME/lib:$ETPKIHOME/lib:$LD_LIBRARY_PATH
```

- ETPKIHOME 변수가 *report_server_home/CommonReporting3* 으로 설정되어 있어야 합니다.

report_server_home

보고서 서버 설치 경로를 지정합니다.

5. *report_server_home/CommonReporting3/bobje* 로 이동합니다.

report_server_home

보고서 서버 설치 경로를 지정합니다.

6. 다음 명령을 실행합니다.

```
./startservers
```

7. 다음 명령을 실행합니다.

```
./tomcatstartup.sh
```

보고서 서버가 시작됩니다.

보고서 서버 중지

(Windows) 다음 단계를 수행하십시오.

1. "시작", "프로그램", "BusinessObjects XI 3.1", "BusinessObjects Enterprise", "Central Configuration Manager"를 차례로 클릭합니다.

Central Configuration Manager 콘솔이 나타납니다.

2. Apache Tomcat 서비스와 Server Intelligence Agent 서비스를 중지합니다.

보고서 서버가 중지됩니다.

(UNIX) 다음 단계를 수행하십시오.

1. 보고서 서버를 설치한 시스템에 루트 아닌 사용자로 로그인합니다.
2. 다음 환경 변수 중 적어도 하나가 유효한 utf8/UTF-8 로캘로 설정되어 있는지 확인합니다.

- LC_ALL
- LANG
- LC_CTYPE

3. *report_server_home*/CommonReporting3/external/scripts 로 이동하여 다음 명령을 실행합니다.

```
../setupenv.sh
```

report_server_home

보고서 서버 설치 경로를 지정합니다.

4. 다음을 확인합니다.

- IAM_RPTSRV_HOME 변수가 *report_server_home/CommonReporting3* 으로 설정되어 있어야 합니다.

report_server_home

보고서 서버 설치 경로를 지정합니다.

- (Oracle 보고서 데이터베이스에만 해당) LD_LIBRARY_PATH 변수가 \$ORACLE_HOME/lib32:\$ORACLE_HOME/lib:\$ETPKIHOME/lib:\$LD_LIBRARY_PATH 로 설정되어 있어야 합니다.

예: export

LD_LIBRARY_PATH=\$ORACLE_HOME/lib32:\$ORACLE_HOME/lib:\$ETPKIHOME/lib:\$LD_LIBRARY_PATH

- ETPKIHOME 변수가 *report_server_home/CommonReporting3* 으로 설정되어 있어야 합니다.

report_server_home

보고서 서버 설치 경로를 지정합니다.

5. *report_server_home/CommonReporting3/bobje* 로 이동합니다.

report_server_home

보고서 서버 설치 경로를 지정합니다.

6. 다음 명령을 실행합니다.

./stopservers

7. 다음 명령을 실행합니다.

./tomcatshutdown.sh

보고서 서버가 중지됩니다.

보고서 제거 방법

다음 절차에 따라 SiteMinder 보고서를 제거하십시오.

1. SiteMinder 보고서 서버 구성 마법사를 제거합니다.
2. 보고서 서버를 제거합니다.
3. 남은 항목을 제거합니다.
4. 보고서 데이터베이스 테이블을 제거합니다.

Windows 에서 보고서 서버 구성 마법사 제거

다음 단계를 수행하십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. `report_server_home\CommonReporting3\Uninstall_CASiteMinder_ConfigurationWizard` 로 이동합니다.

report_server_home

보고서 서버 설치 경로를 지정합니다.

중요! 이 마법사를 Windows Server 2008 에서 실행하는 경우 관리자 권한을 사용하여 실행 파일을 실행하십시오. 관리자로 시스템에 로그인한 경우에도 이 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

3. `uninstall.exe` 를 두 번 클릭합니다.

마법사가 시작됩니다.

4. 지시에 따릅니다.

참고: 공유 파일을 제거할 것인지 묻는 메시지가 나타나면 "No to All"(모두 아니요)을 클릭합니다.

5. 필요한 경우 시스템을 다시 시작합니다.

보고서 서버 구성 마법사가 제거되었습니다.

UNIX 에서 보고서 서버 구성 마법사 제거

다음 단계를 수행하십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. `report_server_home/CommonReporting3/Uninstall_CASiteMinder_ConfigurationWizard` 로 이동합니다.

report_server_home

보고서 서버 설치 경로를 지정합니다.

3. 다음 명령을 실행합니다.
`./uninstall`
 프로세스가 시작됩니다.
4. 지시에 따릅니다.
 보고서 서버 구성 마법사가 제거되었습니다.

Windows 에서 보고서 서버 제거

다음 단계를 수행하십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. `report_server_home\CommonReporting3\Uninstall CA Business Intelligence 3.2` 로 이동합니다.

report_server_home

보고서 서버 설치 경로를 지정합니다.

3. `Uninstall CA Business Intelligence 3.2.exe` 를 두 번 클릭합니다.

중요! 이 마법사를 **Windows Server 2008** 에서 실행하는 경우 관리자 권한을 사용하여 실행 파일을 실행하십시오. 관리자로 시스템에 로그인한 경우에도 이 권한을 사용하십시오. 자세한 내용은 **SiteMinder** 구성 요소의 릴리스 정보를 참조하십시오.

제거 프로그램이 시작됩니다.

참고: 자동 설치를 사용하여 보고서 서버를 설치한 경우 제거 프로그램이 자동 모드로 시작됩니다. 마법사를 사용하여 제거하려는 경우:

- a. 명령 프롬프트를 엽니다.

중요! **Windows Server 2008** 에서 **SiteMinder** 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

- b. `report_server_home\CommonReporting3\Uninstall CA Business Intelligence 3.2` 로 이동합니다.
- c. 다음 명령을 입력합니다.

`Uninstall CA Business Intelligence 3.2.exe -i swing`

4. 지시에 따릅니다.

다음 사항을 고려하십시오.

- 공유 파일을 제거할 것인지 묻는 메시지가 나타나면 "No to All"(모두 아니요)을 클릭합니다.
- Java Platform SE 바이너리 및 BOE120MySQL 을 닫을 것인지 묻는 메시지가 나타나는 경우 "응용 프로그램을 닫지 않습니다"를 선택하고 "확인"을 클릭합니다.

5. 필요한 경우 시스템을 재부팅합니다.

보고서 서버가 제거되었습니다.

참고: 보고서 서버를 제거해도 보고서 데이터베이스에 있는 테이블은 제거되지 않습니다. 수동으로 테이블을 제거해야 합니다.

UNIX 에서 보고서 서버 제거

이 구성 요소를 제거하기 위해 설치 디렉터리를 수동으로 제거하지 마십시오. 제거용 셸 스크립트를 실행해야 합니다. 설치 디렉터리만 제거한 경우 관련 레지스트리가 남아 있게 됩니다. 이 호스트 시스템에 이 구성 요소를 다시 설치하려고 하면 이러한 항목으로 인해 설치가 실패할 수 있습니다.

다음 단계를 수행하십시오.

1. Bourne 셸을 열고 *report_server_home/CommonReporting3/Uninstall* 로 이동합니다.

report_server_home

보고서 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

```
./UninstallCABusinessIntelligence 3.2
```

프로세스가 시작됩니다.

3. 지시에 따릅니다.

보고서 서버가 제거되었습니다.

참고: 보고서 서버를 제거해도 보고서 데이터베이스에 있는 테이블은 제거되지 않습니다. 수동으로 테이블을 제거해야 합니다.

Windows 항목 제거

시스템을 최대한 깨끗하게 정리하려면 남은 항목을 수동으로 제거해야 합니다. 동일한 시스템에 보고서 서버를 다시 설치하려는 경우 남은 항목을 제거해야 보고서 서버 설치가 실패하지 않습니다.

다음 단계를 수행하십시오.

1. `report_server_home` 으로 이동합니다.

`report_server_home`

보고서 서버 설치 경로를 지정합니다.

2. 다음 디렉터리를 삭제합니다.

`CommonReporting3`

남은 항목을 제거했습니다.

UNIX 항목 제거

시스템을 최대한 깨끗하게 정리하려면 남은 항목을 수동으로 제거해야 합니다. 동일한 시스템에 보고서 서버를 다시 설치하려는 경우 남은 항목을 제거해야 보고서 서버 설치가 실패하지 않습니다.

중요! 다른 CA 제품이 `SharedComponents` 디렉터리를 공유할 수 있습니다. 이 위치에 대한 환경 변수는 `profile.CA` 파일에 설정되어 있습니다. 이 파일을 제거하기 전에 `SharedComponents` 디렉터리를 공유 중인 다른 CA 제품이 없는지 확인하십시오.

다음 단계를 수행하십시오.

1. `report_server_home` 으로 이동합니다.

`report_server_home`

보고서 서버 설치 경로를 지정합니다.

2. 다음 폴더를 삭제합니다.

`CommonReporting`

3. `/etc` 로 이동합니다.

4. 다음 파일을 제거합니다.

`profile.CA`

남은 항목을 제거했습니다.

보고서 데이터베이스 테이블 제거

보고서 서버를 제거해도 보고서 데이터베이스에 있는 테이블은 제거되지 않습니다. 보고서 데이터베이스로 사용되는 데이터베이스에 액세스하여 모든 테이블을 수동으로 제거하십시오.

보고서 서버와 관리 UI의 연결 삭제

보고서 서버 연결이 더 이상 필요 없게 되면 연결을 삭제하십시오.

다음 단계를 수행하십시오.

1. "관리", "관리 UI"를 차례로 클릭합니다.
2. "보고서 연결", "보고서 서버 연결 삭제"를 차례로 클릭합니다.
3. 검색 조건을 지정하고 "검색"을 클릭합니다.
4. 연결을 선택하고 "선택"을 클릭합니다.
연결을 삭제해도 되는지 확인하라는 메시지가 표시됩니다.
5. "예"를 클릭합니다.

보고서 서버 연결이 삭제됩니다.

보고서 서버 다시 설치

보고서 서버를 다시 설치하려면 먼저 기존 인스턴스를 제거하고 다시 설치하십시오. 기존 인스턴스 위에 다시 설치하면 설치가 실패합니다.

추가 정보:

[보고서 제거 방법](#) (페이지 513)

제 10 장: OneView 모니터 구성

이 섹션은 다음 항목을 포함하고 있습니다.

[OneView 모니터 개요](#) (페이지 519)

[OneView 모니터에 대한 시스템 요구사항](#) (페이지 520)

[OneView 모니터 구성](#) (페이지 520)

[OneView 모니터 GUI 와 IIS 웹 에이전트를 동일한 컴퓨터에 구성할 경우의 제한 사항](#) (페이지 521)

[Windows/IIS 에 OneView 모니터 GUI 를 구성하는 방법](#) (페이지 521)

[UNIX/Sun Java System 에 OneView 모니터 GUI 를 구성하는 방법](#) (페이지 523)

[OneView 모니터 서비스 시작](#) (페이지 526)

[OneView 모니터 GUI 액세스](#) (페이지 526)

[정책 서버 클러스터 모니터링](#) (페이지 527)

OneView 모니터 개요

OneView 모니터링 인프라는 SiteMinder 구성 요소를 모니터링할 수 있도록 해 주는 여러 모듈로 구성되어 있습니다. 이 중 하나가 JRE(Java Runtime Environment)의 컨텍스트에서 실행되는 모니터 프로세스입니다. 모니터 GUI 의 HTML 페이지는 정책 서버와 동일한 컴퓨터에서 실행되는 ServletExec 서블릿 엔진에서 호스트되는 서블릿 및 JSP(Java Server Page)에 의해 생성됩니다.

OneView 모니터 유틸리티는 다음 SiteMinder 구성 요소를 모니터링합니다.

- 정책 서버
- 웹 에이전트

참고: OneView 모니터 사용에 대한 자세한 내용은 *정책 서버 관리 안내서*에서 확인하십시오.

OneView 모니터에 대한 시스템 요구 사항

OneView 모니터 GUI 를 구성하려는 시스템은 최소한 다음 시스템 요구 사항을 충족해야 합니다.

- **JDK** - 필요한 버전의 Java SDK 가 시스템에 설치되어 있어야 합니다.
- **서블릿 엔진** - 필요한 버전의 ServletExec 가 시스템에 설치되어 있어야 합니다.

참고: 정책 서버 설치 키트에는 다음 위치에 ServletExec/AS 에 대한 설치 실행 파일이 포함되어 있습니다.

thirdparty-tools\servlet-engine-6.0

- **웹 서버** - 시스템에 지원되는 웹 서버가 설치되어 있어야 합니다.

참고: 지원되는 CA 및 타사 구성 요소의 목록에 대해서는 기술 지원 사이트의 SiteMinder 12.52 SP1 Platform Support Matrix(플랫폼 지원표)를 참조하십시오.

OneView 모니터 구성

정책 서버를 설치할 때 OneView 모니터 GUI 를 구성하지 않은 경우 정책 서버 구성 마법사를 사용하여 구성할 수 있습니다.

siteminder_home\siteminder\install_config_info(Windows) 및 siteminder_home/siteminder/install_config_info(UNIX)에서 다음 정책 서버 구성 마법사 실행 파일을 찾을 수 있습니다.

- ca-ps-config.exe

중요! 이 마법사를 Windows Server 2008 에서 실행하는 경우 관리자 권한을 사용하여 실행 파일을 실행하십시오. 관리자로 시스템에 로그인한 경우에도 이 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

- ca-ps-config.bin

siteminder_home

정책 서버가 설치된 경로를 지정합니다.

OneView 모니터 GUI 와 IIS 웹 에이전트를 동일한 컴퓨터에 구성할 경우의 제한 사항

에이전트의 등록 서비스가 활성화된 경우 IIS 기반 OneView 모니터 GUI 와 IIS 웹 에이전트를 동일한 컴퓨터에 구성할 수 없습니다. 이렇게 구성할 경우 동일한 ServletExec 인스턴스와의 충돌이 발생합니다.

Windows/IIS 에 OneView 모니터 GUI 를 구성하는 방법

Windows/IIS 에 OneView 모니터 GUI 를 구성하려면 다음 절차를 완료하십시오.

1. Windows 에 ServletExec 를 설치하기 위한 사전 요구 사항을 읽어 봅니다.
2. Windows/IIS 에 ServletExec/ISAPI 를 설치합니다.
참고: 모니터 GUI 의 HTML 페이지는 정책 서버와 동일한 컴퓨터에서 실행되는 ServletExec 서블릿 엔진에서 호스트되는 서블릿 및 JSP(Java Server Page)에 의해 생성됩니다.
3. 인터넷 게스트 계정에 `policy_server_home\monitor\settings` 폴더에 대한 수정 권한을 할당합니다.
4. IIS 사용자에게 권한을 설정합니다.
5. 정책 서버 설치 프로그램이 OneView 모니터 GUI 를 자동으로 구성하도록 하지 않은 경우 정책 서버 구성 마법사를 실행하여 OneView 모니터 GUI 를 구성합니다.
6. OneView 모니터 서비스를 시작합니다.
7. OneView 모니터 GUI 에 액세스합니다.

Windows 에 ServletExec 를 설치하기 위한 사전 요구 사항

ServletExec 를 설치하기 전에 다음 사전 요구 사항을 고려하십시오.

- ServletExec 는 타사 제품입니다. ServletExec 를 설치하기 전에 ServletExec 설명서를 읽어 보는 것이 좋습니다.

참고: 자세한 내용은 New Atlanta [웹 사이트](#)를 참조하십시오.

- 정책 서버를 지원되는 64 비트 Windows 운영 체제에 설치하는 경우 32 비트 JDK 가 필요합니다. ServletExec/AS 6.0 을 64 비트 Windows 운영 체제에 설치하려는 경우 ServletExec 에는 64 비트 JVM 이 필요합니다. 필요한 경우 ServletExec 를 설치하기 전에 64 비트 JVM 을 설치합니다.

Windows IIS 에 ServletExec 설치

다음 단계를 수행하십시오.

1. 이전 버전의 ServletExec 가 있을 경우 백업합니다.
2. ServletExec 설치 실행 파일을 실행합니다.

참고: 정책 서버 설치 키트에는 다음 위치에 ServletExec/AS 6.0 에 대한 설치 실행 파일이 포함되어 있습니다.

thirdparty-tools\servlet-engine-6.0

참고: ServletExec 업그레이드 및 설치에 대한 자세한 내용은 New Atlanta [설명서](#)를 참조하십시오.

3. ServletExec/AS 사전 요구 사항으로 64 비트 JVM 을 설치했을 경우 다음 단계를 완료합니다.
 - a. 서비스 제어판을 사용하여 ServletExec 서비스를 중지합니다.
 - b. (선택 사항) 64 비트 JVM 을 제거합니다.
 - c. 32 비트 JVM 을 가리키도록 StartServletExec.bat 및 StopServletExec.bat 파일을 편집합니다.
 - d. 서비스 제어판을 사용하여 ServletExec 서비스를 시작합니다.
4. IIS 관리 웹 서비스와 IIS 웹 서버를 중지한 후 다시 시작합니다.

ServletExec 설치 후 IIS 사용자에게 대한 권한 설정

ServletExec/AS 는 IIS 프로세스의 일부로 실행되므로 다양한 시간에 다양한 사용자로 실행됩니다. 따라서 ServletExec 설치 디렉터리 및 하위 디렉터리에 대해 다음 권한을 설정해야 합니다.

ServletExec 를 설치한 후 IIS 사용자에게 대한 권한을 설정하려면 IIS(예: 네트워크 서비스)를 실행하는 사용자에게 C:\Program Files\New Atlanta 아래의 전체 디렉터리 트리에 대한 읽기 및 쓰기 권한이 있는지 확인하십시오.

UNIX/Sun Java System 에 OneView 모니터 GUI 를 구성하는 방법

UNIX/Sun Java System 에 OneView 모니터 GUI 를 구성하려면 다음 절차를 완료하십시오.

1. ServletExec 를 설치하기 위한 사전 요구 사항을 읽어 봅니다.
2. Sun Java System(Sun One/iPlanet) 6.0 에서 서블릿이 사용되지 않도록 설정합니다.
3. UNIX/Sun Java System 에 ServletExec/AS 를 설치합니다.
4. 정책 서버 설치 프로그램이 OneView 모니터 GUI 를 자동으로 구성하도록 하지 않은 경우 정책 서버 구성 마법사를 실행하여 OneView 모니터 GUI 를 구성합니다.
5. OneView 모니터 서비스를 시작합니다.
6. OneView 모니터 GUI 에 액세스합니다.

ServletExec 설치를 위한 사전 요구 사항

ServletExec 를 설치하기 전에 ServletExec 설명서를 읽어 보는 것이 좋습니다. OneView 모니터 GUI 는 ServletExec 의 서블릿 엔진에 의존하므로 ServletExec 가 제대로 실행되지 않으면 OneView 모니터 GUI 가 작동하지 않습니다.

ServletExec 설명서를 보려면 [New Atlanta 웹 사이트](#)를 참조하십시오.

Sun Java System 6.0 에서 서블릿이 사용되지 않도록 설정

ServletExec 를 설치하기 전에 이 단원의 단계를 따르십시오.

Sun Java System 6.0 에서 서블릿이 사용되지 않도록 설정하려면

1. 브라우저에 `http://<yourserver.com>:<portnumber>`를 입력하여 Sun Java System Enterprise Administration Server 홈 페이지를 엽니다.

yourserver.com

Enterprise Administration Server 의 도메인 이름을 지정합니다.

port

포트 번호를 지정합니다.

2. "Select a Server"(서버 선택) 드롭다운 메뉴에서 대상 서버를 선택하고 "Manage"(관리)를 클릭합니다.
3. "Java" 탭을 선택합니다.
4. "Enable Java for class defaultclass"(defaultclass 클래스에 Java 사용) 및 "Enable Java Globally"(전역으로 Java 사용)의 선택을 취소하고 "OK"(확인)를 클릭합니다.
5. 웹 서버를 중지했다가 다시 시작하여 설정을 적용합니다.

UNIX/Sun Java System 에 ServletExec/AS 설치

모니터 GUI 의 HTML 페이지는 정책 서버와 동일한 컴퓨터에서 실행되는 ServletExec 서블릿 엔진에서 호스트되는 서블릿 및 JSP(Java Server Page)에 의해 생성됩니다.

ServletExec 를 설치하려면

1. 정책 서버를 설치하는 데 사용할 UNIX 계정에 로그인합니다.

참고: Sun Java System Web Server 를 설치한 사용자와 동일한 사용자로 로그인해야 합니다.

2. ServletExec AS 설치 관리자를 실행합니다.

참고: ServletExec AS 설치 관리자 실행에 대한 자세한 내용은 New Atlanta Communications 의 ServletExec 설명서를 참조하십시오. ServletExec 를 설치하기 전에 다음 사항을 고려하십시오.

- /tmp 에 새 파일을 생성할 수 있는 권한이 있는지 확인합니다. New Atlanta 에서는 /usr/local/NewAtlanta 에 ServletExec 를 설치할 것을 권장합니다. /usr/local/NewAtlanta 에 ServletExec 를 설치하면 obj.conf 파일과 Sun Java System 시작 스크립트에 대한 권한이 변경될 수 있습니다. 설치 후 obj.conf 와 시작 스크립트의 소유자가 웹 서버를 소유하는 사용자와 동일한지 확인합니다.
- 해당 메시지가 나타나면 웹 서버 어댑터와 ServletExec 인스턴스를 설치합니다.
- 해당 메시지가 나타나면 설치 관리자가 웹 서버의 구성 파일을 수정하지 않도록 합니다. 설치 관리자가 웹 서버의 obj.conf 및 magnus.conf 구성 파일을 수정하도록 하면 웹 서버 인스턴스에 OneView 모니터 GUI 를 구성한 후에 웹 서버 인스턴스가 실행되지 않습니다.

3. 설치 프로그램이 완료되면 웹 서버를 다시 시작합니다.

추가 정보:

[OneView 모니터 서비스 시작](#) (페이지 526)

OneView 모니터 서비스 시작

다음 단계를 수행하십시오.

1. IPC 포트 번호를 사용할 수 있는지 확인합니다.

OneView 모니터는 다음 포트 번호를 사용하여 정책 서버 프로세스와 통신합니다.

- 모니터링 에이전트: 44449

- 모니터: 44450

사용할 수 없는 포트 번호를 확인하려면 명령 창을 열고 다음을 입력합니다.

```
netstat -an
```

참고: 포트 번호 변경에 대한 자세한 내용은 정책 서버 관리 안내서를 참조하십시오.

2. 정책 서버 관리 콘솔의 "상태" 탭을 사용하여 모니터 서비스를 시작합니다.

OneView 모니터 GUI 액세스

다음 단계를 수행하십시오.

브라우저에 다음 URL 을 입력합니다.

`http://server:<portnumber>/sitemindermonitor`

server

웹 서버의 IP 주소를 지정합니다.

portnumber

포트 번호를 지정합니다.

정책 서버 클러스터 모니터링

한 정책 서버를 클러스터에 있는 다른 정책 서버의 중앙 모니터로 설정한 경우 **OneView** 모니터가 정책 서버 클러스터를 모니터링하도록 구성할 수 있습니다.

참고: **OneView** 모니터 사용에 대한 자세한 내용은 *정책 서버 관리 안내서*에서 확인하십시오.

제 11 장: SNMP 지원

이 섹션은 다음 항목을 포함하고 있습니다.

[SNMP 지원 개요](#) (페이지 529)

[Windows 및 UNIX 시스템에 대한 SNMP 사전 요구 사항](#) (페이지 531)

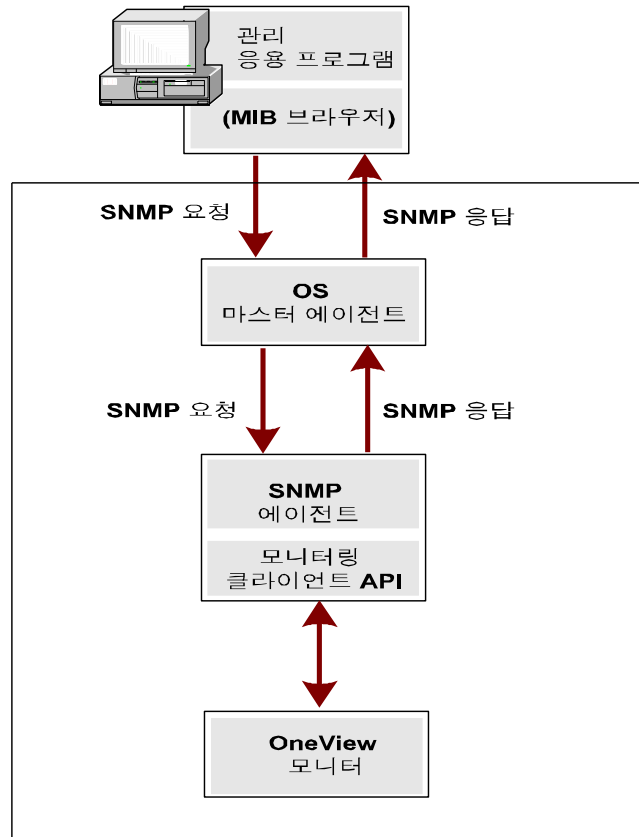
[Windows에 SNMP 에이전트 구성](#) (페이지 532)

[UNIX 시스템에 SNMP 에이전트 구성](#) (페이지 535)

SNMP 지원 개요

SNMP 지원에는 MIB(관리 정보 베이스), SNMP 에이전트 및 이벤트 SNMP 트랩 라이브러리가 포함됩니다. SNMP 에이전트와 이벤트 SNMP 트랩 라이브러리를 독립적으로 구성하여 하나는 사용하도록 설정하고 다른 하나는 사용하지 않도록 설정할 수 있습니다. SNMP 에이전트는 모니터링 응용 프로그램이 OneView 모니터에서 작업 데이터를 검색할 수 있도록 합니다. SNMP 에이전트는 데이터를 SNMP 관리자로 보내고 SNMP 요청 처리를 지원합니다.

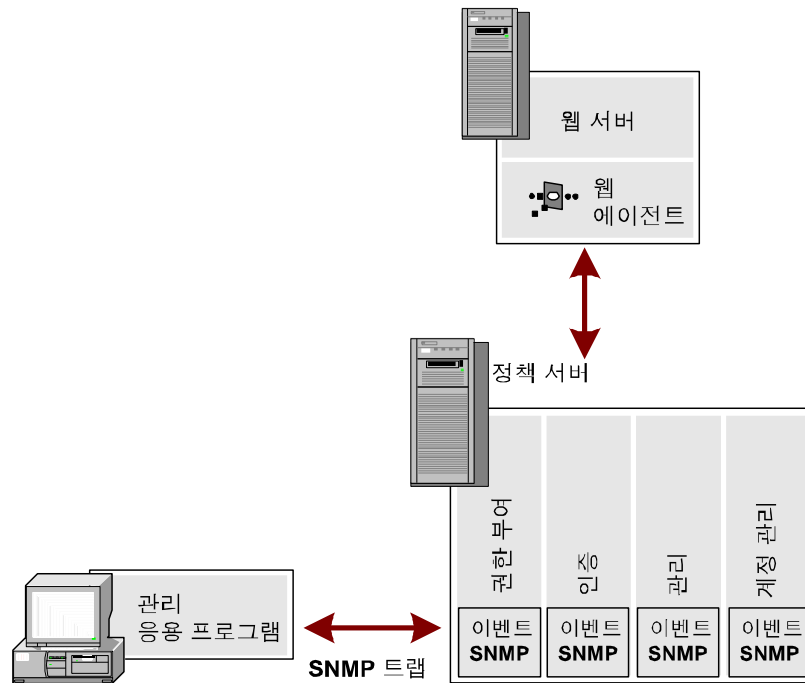
다음 그림에서는 관리 응용 프로그램, OS 마스터 에이전트, SNMP 에이전트 및 OneView 모니터 간의 아키텍처를 보여 줍니다.



네이티브 Solaris Sun Solstice Master Agent 같은 OS 마스터 에이전트는 마스터 에이전트가 다시 시작되면 SNMP 에이전트를 호출합니다. OS 마스터 에이전트는 관리 응용 프로그램으로부터 SNMP 요청을 받으면 SNMP 에이전트로 SNMP 요청을 전달합니다. SNMP 에이전트는 OneView 모니터에 연결하고, 모니터링 클라이언트 API를 사용하여 요청된 정보를 검색한 후, 마스터 에이전트로 응답을 보냅니다. 그러면 마스터 에이전트는 응답을 관리 응용 프로그램으로 전달합니다.

정책 서버 설치 중에 SNMP 에이전트를 구성하지 않더라도 나중에 에이전트를 사용할 경우에 대비하여 모든 SNMP 파일이 설치됩니다. 하지만 에이전트를 실행하려면 Windows 나 UNIX 시스템에 SNMP 에이전트를 구성하여 에이전트를 수동으로 시작해야 합니다.

다음 그림에 나온 것처럼 이벤트 SNMP 트랩 라이브러리는 일부 SiteMinder 이벤트를 SNMP 트랩으로 변환한 후 관리 응용 프로그램으로 보냅니다. 트랩 라이브러리는 정책 서버가 보낸 이벤트를 캡처하고, 해당 이벤트에서 SNMP 트랩을 생성할지 여부를 결정하고, 트랩을 생성합니다.



참고: SNMP 에이전트 및 OneView 모니터에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

Windows 및 UNIX 시스템에 대한 SNMP 사전 요구 사항

SNMP 에이전트를 설치하거나 사용하려면 운영 체제와 함께 마스터 에이전트를 설치해야 합니다.

Windows 사전 요구 사항

Windows 에서 SiteMinder SNMP 를 지원하려면 SNMP 서비스가 필요합니다. SNMP 서비스 설치에 대한 자세한 내용은 Windows 온라인 도움말 시스템을 참조하십시오.

UNIX 시스템 사전 요구 사항

다음 단원에서는 **SNMP** 지원을 위한 **UNIX** 사전 요구 사항에 대해 자세히 설명합니다.

Solaris

운영 체제와 함께 제공되는 네이티브 Solaris Sun Solstice Master Agent 가 필요합니다.

Linux

Red Hat Advanced Server 3.0 에서 지원되는 마스터 에이전트의 경우 net-snmp 패키지를 net-snmp-5.1-2.1 이상으로 업그레이드합니다.

net-snmp 패키지를 net-snmp-5.1-2.1 이상으로 업그레이드하려면 snmpd.conf 파일에서 net-snmpd 명령에 대해 다음 설정을 사용하십시오.
proxy -c public -v 1 localhost:8001 .1.3.6.1.4.1.2552

참고: net-snmp 패키지를 업그레이드한 후에는 snmpd.conf 파일에 프록시 지원을 추가하십시오.

SiteMinder 관련 snmpd.conf 파일은 다음 위치에서 찾을 수 있습니다.
호스트에는 대개 snmpd.conf 파일이 여러 개 있습니다.
/opt/siteminder/etc/snmp/conf/snmpd.conf

Windows 에 SNMP 에이전트 구성

다음 단계를 수행하십시오.

1. NETE_PS_ROOT 환경 변수가 SiteMinder 설치 디렉터리로 설정되었는지 확인합니다. 이 작업은 정책 서버 설치 프로그램에서 이미 수행했어야 합니다.
2. siteminder_home\config\snmp.conf 파일을 열고 마지막 행에 siteminder_home\log\snmp.log 의 전체 경로가 포함되도록 편집합니다.

참고: 이 작업은 정책 서버 설치 프로그램이 **SNMP** 를 자동으로 구성하도록 지정하지 않은 경우에만 수행하면 됩니다.

올바른 예: LOG_FILE=C:\Program
Files\Netegrity\siteminder\log\snmp.LOG

잘못된 예: LOG_FILE=\$NETE_PS_ROOT\log\snmp.log

3. *windows_dir/java_service.ini* 파일을 편집합니다.

참고: 이 작업은 정책 서버 설치 시 SNMP 가 자동으로 구성되도록 지정하지 않은 경우에만 수행하면 됩니다.

- a. SERVICE_BINARY_NAME 을 JavaService.exe 의 전체 경로 이름으로 설정합니다.

예: SERVICE_BINARY_NAME=c:\winnt\JavaService.exe

- b. WORKING_DIR 를 *siteminder_home\bin* 디렉터리의 전체 경로로 설정합니다.

예: WORKING_DIR=C:\Program files\Netegrity\siteminder\bin

- c. JRE_PATH 를 javaw.exe 의 전체 경로로 설정합니다.

4. *siteminder_home\bin\thirdparty\proxyreg.exe* 를 실행하여 *apadll.dll* 및 *snmp.conf* 의 레지스트리 키를 변경합니다.

proxyreg.exe full_path_for_apadll.dll full_path_for_snmp.conf

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

예: proxyreg.exe "c:\program files\netegrity\siteminder\ bin\ thirdparty\apadll.dll" "c:\programfiles\netegrity\ siteminder\ config\ snmp.conf"

5. -install 옵션으로 *WINNT dir/JavaService.exe* 를 실행하여 Netegrity SNMP 에이전트를 WINNT 서비스로 등록합니다.
6. "Windows 서비스" 대화 상자를 사용하여 Netegrity SNMP 에이전트를 시작합니다.
7. SNMP 서비스를 다시 시작합니다.

Windows 에서 SNMP 이벤트 트래핑을 구성하는 방법

Windows 에서 SNMP 이벤트 트래핑을 구성하려면 다음 작업을 수행해야 합니다.

1. SNMP 이벤트 트래핑이 사용되도록 설정합니다.
2. [snmptrap.config](#) 를 구성합니다 (페이지 534).

SNMP 이벤트 트래핑이 사용되도록 설정

SNMP 이벤트 트래핑이 사용되도록 설정하려면 XPSConfig 유틸리티를 사용하여 이벤트 처리기 라이브러리(eventsnmp.dll)를 XPSAudit 목록으로 설정하십시오. eventsnmp.dll 의 기본 위치는 *policy_server_home*\bin 입니다.

policy_server_home

정책 서버 설치 위치를 지정합니다.

참고: XPSConfig 유틸리티를 사용하여 이벤트 처리기 라이브러리를 설정하는 방법에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

SNMP 이벤트 트래핑이 사용되도록 설정했으면 snmptrap.conf 파일을 구성하십시오.

snmptrap.conf 구성

SNMP 구성 파일을 구성하려면

1. snmptrap.conf 를 편집합니다.

참고: snmptrap.conf 는 *policy_server_home*\config 에 있습니다.

policy_server_home

정책 서버 설치 위치를 지정합니다.

2. 수신하려는 특정 트랩에 해당하는 행을 찾아 주석 처리를 제거합니다.
3. 트랩이 전송되도록 할 위치의 IP 주소, 포트 번호 및 커뮤니티를 지정합니다.
4. 새로운 변경 내용과 함께 snmptrap.config 파일을 저장합니다.
5. 정책 서버를 다시 시작합니다.

추가 정보:

[정책 서버 중지 및 다시 시작](#) (페이지 536)

UNIX 시스템에 SNMP 에이전트 구성

다음 단계를 수행하십시오.

1. NETE_PS_ROOT 환경 변수가 SiteMinder 설치 디렉터리로 설정되었는지 확인합니다. 이 작업은 정책 서버 설치 프로그램에서 이미 수행했어야 합니다.

예: /home/smuser/siteminder

2. /etc/snmp/conf/RunSubagent.sh 파일을 편집합니다.

- a. JAVA_HOME=\$INSTALL_HOME/bin/jdk/<required_version>/jre 와 같이 올바른 JRE 경로를 설정합니다.

- b. 올바른 SiteMinder 경로를 설정합니다.

예: INSTALL_HOME=/home/smuser/siteminder

참고: INSTALL_HOME 변수에는 SiteMinder 설치 디렉터리의 전체 경로를 포함해야 합니다.

3. Solaris 에서 SNMP 데몬 다시 시작

- a. 루트로 전환합니다.

- b. /etc/rc3.d 로 이동합니다.

- c. 다음과 같이 S76snmpdx 스크립트를 두 번 실행합니다.

sh S76snmpdx stop 을 실행하여 Solaris 마스터 에이전트의 실행을 중지합니다.

sh S76snmpdx start 를 실행하여 Solaris 마스터 에이전트와 Netegrity 하위 에이전트를 시작합니다.

UNIX 시스템에서 SNMP 이벤트 트래핑을 구성하는 방법

UNIX 시스템에서 SNMP 이벤트 트래핑을 구성하려면 다음 작업을 수행해야 합니다.

1. SNMP 이벤트 트래핑이 사용되도록 설정합니다.
2. [snmptrap.config](#) 를 구성합니다 (페이지 536).

SNMP 이벤트 트래핑이 사용되도록 설정

SNMP 이벤트 트래핑이 사용되도록 설정하려면 XPSConfig 유틸리티를 사용하여 이벤트 처리기 라이브러리(libeventsnmp.so)를 XPSAudit 목록으로 설정하십시오. libeventsnmp.so 의 기본 위치는 *policy_server_home/lib* 입니다.

policy_server_home

정책 서버 설치 위치를 지정합니다.

참고: XPSConfig 유틸리티를 사용하여 이벤트 처리기 라이브러리를 설정하는 방법에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

SNMP 이벤트 트래핑이 사용되도록 설정했으면 *snmptrap.config* 파일을 구성하십시오.

snmptrap.config 구성

snmptrap.config 를 구성하려면

1. */home/smuser/siteminder/config* 에 있는 *snmptrap.config* 를 편집합니다.
2. 수신하려는 특정 트랩에 해당하는 행을 찾아 주석 처리를 제거합니다.
3. 트랩이 전송되도록 할 위치의 IP 주소, 포트 번호 및 커뮤니티를 지정합니다.
4. 새로운 변경 내용과 함께 *snmptrap.config* 파일을 저장합니다.
5. 정책 서버를 다시 시작합니다.

추가 정보:

[정책 서버 중지 및 다시 시작](#) (페이지 536)

정책 서버 중지 및 다시 시작

SNMP 구성 변경 내용을 적용하려면 정책 서버 관리 콘솔의 "상태" 탭을 사용하여 정책 서버를 중지했다가 다시 시작해야 합니다.

Red Hat Enterprise Linux Advanced Server 에 대해 SNMP Gets 테스트

SNMP 를 구성한 후에는 SNMP Gets 를 테스트해야 합니다.

SNMP Gets 를 테스트하려면

1. 네이티브 SNMP 마스터 에이전트를 시작합니다. Red Hat AS 에서는 시스템 시작 시 마스터 에이전트가 자동으로 시작되지 않으며 이는 Solaris 와 HP-UX 에서도 마찬가지입니다. 마스터 에이전트를 시작하려면 /etc/rc1.d 디렉터리로 이동하여 다음 명령을 실행합니다(루트로 실행).

```
K50snmpd start
```

2. 다음 명령을 사용하여(루트로 실행) Netegrity 하위 에이전트를 시작합니다.

```
sh /etc/init.d/NetegrityAgent
```

3. Red Hat AS 에서 Netegrity 하위 에이전트를 중지하려면 루트로 다음 명령을 실행합니다.

```
sh $NETE_PS_ROOT/etc/snmp/conf/StopSubagent.sh
```


제 12 장: 기존 응용 프로그램 서버에 관리 UI 설치

관리 UI 설치 요구 사항

기존 응용 프로그램 서버에 관리 UI 를 설치할 수 있습니다. 관리 UI 설치 관리자가 응용 프로그램 서버 관련 정보와 필요한 JDK 의 위치를 요구합니다. 설치를 시작하기 전에 관리 UI 호스트 시스템이 모든 시스템 및 타사 구성 요소 요구 사항을 충족하는지 확인하십시오.

다음 단원에서는 기존 응용 프로그램 서버 인프라에 관리 UI 를 설치하기 위한 최소 시스템 및 응용 프로그램 서버 요구 사항에 대해 자세히 설명합니다.

관리 UI 시스템 요구 사항

관리 UI 호스트는 다음과 같은 최소 시스템 요구 사항을 충족해야 합니다.

참고: 지원되는 CA 및 타사 구성 요소의 목록에 대해서는 기술 지원 사이트의 [SiteMinder 12.52 SP1 Platform Support Matrix](#)(플랫폼 지원표)를 참조하십시오.

Windows 시스템 요구 사항 확인

기존 응용 프로그램 서버에 관리 UI 를 설치하는 경우 Windows 시스템이 다음 최소 시스템 요구 사항을 충족하는지 여부를 확인합니다.

- **CPU** - x86 또는 x64, 1.2 GHz 이상
- **메모리** - 1 GB 시스템 RAM. 권장 크기는 2 GB 입니다.

참고: WebSphere 를 실행하는 경우에는 2 GB 의 시스템 RAM 이 필요합니다.

- **사용 가능한 디스크 공간**-540 MB

참고: WebSphere 를 실행하는 경우에는 2 GB 의 사용 가능한 디스크 공간이 필요합니다.

- **임시 디렉터리 공간-3 GB**
- **JDK-관리 UI** 를 설치하는 시스템에 필수 **JDK 버전**이 설치되어 있어야 합니다.
- **화면 해상도-관리 UI** 를 올바르게 표시하려면 **256 색** 이상을 지원하는 **1024 x 768** 이상의 해상도가 필요합니다.

UNIX 시스템 요구 사항 확인

기존 응용 프로그램 서버에 관리 UI 를 설치하려면 **UNIX** 시스템이 다음과 같은 최소 시스템 요구 사항을 충족해야 합니다.

- **CPU**

- Solaris - UltraSparc, 440 MHz 이상
- Red Hat Linux - x86 또는 x64, 700 MHz 이상

참고: Red Hat 6 운영 체제는 성능을 위해 엔트로피를 사용합니다. 구성 요소를 설치하기 전에 엔트로피를 늘리십시오. 엔트로피가 충분하지 않으면 설치를 완료하는 데 시간이 매우 오래 걸릴 수 있습니다. 기호화된 링크를 설정하려면 다음 명령을 사용하십시오.

```
mv /dev/random /dev/random.org  
ln -s /dev/urandom /dev/random
```

- **메모리 - 1 GB** 시스템 RAM. 권장 크기는 **2 GB** 입니다.

참고: WebSphere 를 실행하는 경우에는 **2 GB** 의 시스템 RAM 이 필요합니다.

- **사용 가능한 디스크 공간-540 MB**

참고: WebSphere 를 실행하는 경우에는 **2 GB** 의 사용 가능한 디스크 공간이 필요합니다.

- **임시 디렉터리 공간-3 GB**

- **JDK-관리 UI** 를 설치하는 시스템에 필수 **JDK 버전**이 설치되어 있어야 합니다.

참고: 응용 프로그램 서버가 Red Hat Linux 운영 체제에서 실행되는 경우 관리 UI 를 설치할 때 IBM JDK 에 대해 무제한 암호화 jar 파일을 설치하십시오.

- **화면 해상도-관리 UI** 를 올바르게 표시하려면 **256 색** 이상을 지원하는 **1024 x 768** 이상의 해상도가 필요합니다.

응용 프로그램 서버 요구 사항

관리 UI 는 J2EE 응용 프로그램으로, 지원되는 응용 프로그램 서버가 있어야 실행할 수 있습니다. 다음을 확인하십시오.

- 관리 UI 를 호스트할 시스템에 지원되는 버전의 JBoss, WebLogic 또는 WebSphere 가 설치되어 있어야 합니다.
- 관리 UI 가 응용 프로그램 서버에 배포된 유일한 응용 프로그램이어야 합니다.

참고: 지원되는 CA 및 타사 구성 요소의 목록에 대해서는 기술 지원 사이트의 SiteMinder 12.52 SP1 Platform Support Matrix(플랫폼 지원표)를 참조하십시오.

JBoss

관리 UI 설치를 위해 JBoss 를 준비하려면 HDScanner 서비스를 비활성화하십시오.

다음 단계를 수행하십시오.

1. `jboss_home/server/server_profile/deploy` 로 이동합니다.

jboss_home

JBoss 설치 경로를 지정합니다.

server_profile

응용 프로그램 서버에 배포된 서버 프로필의 이름을 지정합니다.

예: 기본값

2. 다음 파일을 제거하여 서비스를 비활성화합니다.

`hdscanner-jboss-beans.xml`

WebLogic 응용 프로그램 서버

다음 단원에서는 WebLogic 을 SiteMinder 응용 프로그램 서버로 사용하기 위한 기본 지침을 제공합니다.

WebLogic 설치

SiteMinder 에서 지원되는 버전의 WebLogic 서버를 설치하십시오.

참고: WebLogic 서버 설치에 대한 자세한 내용은 [BEA 의 WebLogic 서버 설명서](#)를 참조하십시오.

WebLogic 응용 프로그램 서버 인스턴스 만들기

관리 UI 를 설치하기 전에 WebLogic 설치의 일부로 제공되는 구성 마법사를 사용하여 WebLogic 도메인을 생성하고 다음을 수행하십시오.

- 도메인의 이름을 적어 둡니다. 도메인 이름은 관리 UI 를 설치할 때 필요합니다.
- "Basic WebLogic Server Domain"(기본 WebLogic Server 도메인) 템플릿을 선택합니다.
- setDomainEnv.cmd/ .sh 파일에서 JAVA_HOME 변수가 필요한 Java 환경의 경로로 설정되었는지 확인합니다. 이 파일은 `web_logic_home\user_projects\domains\weblogic_domain\bin` 에 있습니다.

web_logic_home

WebLogic 서버 설치 경로를 지정합니다.

weblogic_domain

생성한 WebLogic 도메인의 이름을 지정합니다.

WebLogic 도메인 확인

다음을 확인하십시오.

- WebLogic 서버가 실행되고 있어야 합니다.
- `http://server.domain.port/console` 에서 WebLogic 콘솔에 액세스할 수 있습니다.
예: `http://myserver.mycompany.com:7001/console`
- WebLogic 콘솔의 "Domain Configurations"(도메인 구성)에서 도메인 링크를 선택하고 생성한 WebLogic 도메인이 기존 도메인 목록에 표시되는지 확인합니다.

참고: 확인을 마친 후에는 응용 프로그램 서버를 종료하여 관리 UI 설치를 준비하십시오.

WebSphere 응용 프로그램 서버

다음 단원에서는 WebSphere 를 SiteMinder 응용 프로그램 서버로 사용하기 위한 기본 지침을 제공합니다.

WebSphere 설치

IBM 설명서를 참조하여 WebSphere 를 설치합니다.

WebSphere 를 설치할 때 다음 사항을 고려하십시오.

- "Server and Client"(서버 및 클라이언트) 옵션을 선택합니다.
- "Administrative Security"(관리 보안) 옵션을 사용하지 않도록 설정합니다.
- (Solaris) Embedded Messaging 서비스 설치 전 고려 사항:
 - 다음 그룹을 구성합니다.
 - mqm
 - mqbrkrs
 - 다음 사용자를 구성합니다.
 - mqm
 - root

참고: 자세한 내용은 IBM 설명서를 참조하십시오.

WebSphere 가 작동하는지 확인

관리 UI 를 설치하기 전에 IBM 에서 제공한 snoop 유틸리티를 사용하여 WebSphere 가 올바르게 설치되었는지 확인하십시오.

WebSphere 가 작동하는지 확인하려면

1. `http://<fqdn:port>/snoop` 를 입력하여 WebSphere 가 올바르게 설치되었는지 확인합니다.

예: `http:MyServer.MyCompany.com:9080/snoop`

WebSphere 가 올바르게 설치되었으면 브라우저에 "Snoop Servlet - Client Information"(Snoop 서블릿 - 클라이언트 정보) 페이지가 표시됩니다.

2. `http://<fqdn>/snoop` 를 입력하여 WebSphere 응용 프로그램 서버 플러그인이 올바르게 설치되었는지 확인합니다.

예: `http://MyServer.MyCompany.com/snoop`

WebSphere 가 올바르게 설치되었으면 브라우저에 위와 동일한 "Snoop Servlet - Client Information"(Snoop 서블릿 - 클라이언트 정보) 페이지가 표시됩니다.

WebSphere 가 제대로 작동하고 있는지 확인했습니다.

참고: WebSphere 에 관한 추가 지원을 받으려면 IBM 기술 지원부에 문의하십시오.

UI 와 정책 서버 사이의 트러스트 관계

기본 슈퍼 사용자 계정(siteminder)과 암호를 사용하여 관리 UI 에 처음 로그인할 때 관리 UI 와 정책 서버 사이에 트러스트 관계를 구성합니다. 이 관계는 환경을 관리하기 위해 필요합니다.

슈퍼 사용자 계정 자격 증명은 정책 저장소에 저장됩니다. 정책 서버 설치 중에 기본 정책 저장소 중 하나를 구성하는 경우 설치 관리자는 이러한 자격 증명을 자동으로 제출합니다. 정책 저장소 설치와 독립적으로 정책 저장소를 구성하는 경우 **XPSRegClient** 유틸리티를 사용하여 자격 증명을 정책 서버로 제출하십시오. 정책 서버는 이러한 자격 증명을 사용하여 등록 요청이 유효하며 관계를 생성할 수 있는지 확인합니다.

중요! 슈퍼 사용자 계정 자격 증명에 정책 저장소에 제출된 후 **24 시간** 이내에 관리자가 관리 UI에 로그인해야 합니다. **24 시간**이 경과할 때까지 관리 UI에 최초 로그인하지 않은 경우 **XPSRegClient** 유틸리티를 사용하여 자격 증명을 재설정하십시오.

관리 UI 설치 검사 목록

관리 UI를 설치하기 전에 다음을 완료하십시오.

- ☐ 지원되는 운영 체제를 사용하고 있는지 확인합니다.
- ☐ 관리 UI 호스트 시스템이 최소 시스템 요구 사항을 충족하는지 확인합니다.
- ☐ (Linux) 필요한 Linux 라이브러리가 관리 UI 호스트 시스템에 설치되었는지 확인합니다.
- ☐ 지원되는 응용 프로그램 서버가 관리 UI 호스트 시스템에 설치되었는지 확인합니다.
- ☐ 필요한 JDK가 관리 UI 호스트 시스템에 설치되었는지 확인합니다.
- ☐ 정책 저장소가 구성된 시기를 확인합니다.

정책 저장소가 구성된 지 **24 시간** 이상 되었을 경우 관리 UI를 설치하기 전에 **XPSRegClient** 유틸리티를 사용하여 기본 **SiteMinder** 슈퍼 사용자 계정 자격 증명을 정책 서버에 제출할 수 있습니다. 정책 서버에서는 관리 UI와 트러스트 관계를 생성하기 위해 이러한 자격 증명에 필요합니다.

참고: 지원되는 CA 및 타사 구성 요소의 목록에 대해서는 기술 지원 사이트의 **SiteMinder 12.52 SP1 Platform Support Matrix(플랫폼 지원표)**를 참조하십시오.

추가 정보:

[응용 프로그램 서버 요구 사항](#) (페이지 541)

[관리 UI 시스템 요구 사항](#) (페이지 539)

관리 UI 설치 방법

관리 UI 를 설치하려면 다음 절차를 완료하십시오.

1. 설치 검사 목록을 검토했는지 확인합니다.
2. (Linux) 필요한 Linux 라이브러리 요구 사항을 검토합니다.
3. 관리 UI 설치 관리자에 필요한 응용 프로그램 서버 정보를 수집합니다.
4. 관리 UI 설치
5. 응용 프로그램 서버를 시작합니다.

필요한 Linux 라이브러리

Linux 운영 환경에서 작동하는 구성 요소의 경우 특정 라이브러리 파일이 필요합니다. 올바른 라이브러리를 설치하지 못하면 다음과 같은 오류가 발생할 수 있습니다.

```
java.lang.UnsatisfiedLinkError
```

이 구성 요소의 Linux 버전을 설치, 구성 또는 업그레이드하는 경우 호스트 시스템에 다음 라이브러리가 필요합니다.

Red Hat 5.x

```
compat-gcc-34-c++-3.4.6-patch_version.l386
```

Red Hat 6.x(32 비트)

```
libstdc++-4.4.6-3.el6.i686.rpm
```

운영 환경에 적절한 32 비트 C 런타임 라이브러리가 포함되게 하려면 위의 rpm 을 설치하십시오.

Red Hat 6.x(64 비트)

libXau-1.0.5-1.el6.i686.rpm

libxcb-1.5-1.el6.i686.rpm

libstdc++-4.4.6-4.el6.i686.rpm

compat-db42-4.2.52-15.el6.i686.rpm

compat-db43-4.3.29-15.el6.i686.rpm

libX11-1.3-2.el6.i686.rpm

libXrender-0.9.5-1.el6.i686.rpm

libexpat.so.1(expat-2.0.1-11.el6_2.i686.rpm 에서 제공)

libfreetype.so.6(freetype-2.3.11-6.el6_2.9.i686.rpm 에서 제공)

libfontconfig.so.1(fontconfig-2.8.0-3.el6.i686.rpm 에서 제공)

libICE-1.0.6-1.el6.i686.rpm

libuuid-2.17.2-12.7.el6.i686.rpm

libSM-1.1.0-7.1.el6.i686.rpm

libXext-1.1-3.el6.i686.rpm

compat-libstdc++-33-3.2.3-69.el6.i686.rpm

compat-db-4.6.21-15.el6.i686.rpm

libXi-1.3-3.el6.i686.rpm

libXtst-1.0.99.2-3.el6.i686.rpm

libXft-2.1.13-4.1.el6.i686.rpm

libXt-1.0.7-1.el6.i686.rpm

libXp-1.0.0-15.1.el6.i686.rpm

응용 프로그램 서버 정보 수집

관리 UI 설치 관리자를 실행하려면 관리 UI 호스트 시스템에 설치된 응용 프로그램 서버에 대한 특정 정보가 필요합니다.

다음 단원에서는 응용 프로그램 서버 유형별로 필요한 정보에 대해 자세히 설명합니다.

참고: 관리 UI 를 설치하기 전에 필요한 정보를 수집 및 기록하는 데 유용한 워크시트가 제공됩니다.

JBoss Information(JBoss 정보)

관리 UI 를 설치 및 등록하기 전에 JBoss 에 대한 다음 정보를 수집하십시오.

JBoss 설치 폴더

JBoss 가 설치된 폴더의 경로입니다.

JBoss URL

JBoss 호스트 시스템의 정규화된 URL 입니다.

JDK

필요한 JDK 의 설치 위치입니다.

WebLogic Information(WebLogic 정보)

관리 UI 를 설치하고 등록하기 전에 다음 정보를 수집하십시오.

WebLogic 바이너리 폴더

WebLogic 설치 디렉터리의 경로입니다.

WebLogic 도메인 폴더

관리 UI 에 대해 생성한 WebLogic 도메인의 경로입니다.

WebLogic 서버 이름

WebLogic 도메인이 구성된 WebLogic 서버의 이름입니다.

응용 프로그램 서버 URL 및 포트

WebLogic 호스트 시스템의 정규화된 URL 입니다.

JDK

필요한 JDK 의 설치 위치입니다.

WebSphere Information(WebSphere 정보)

관리 UI 를 설치 및 등록하기 전에 WebSphere 에 대한 다음 정보를 수집하십시오.

WebSphere 설치 폴더

WebSphere 가 설치된 폴더의 전체 경로입니다.

WebSphere URL

WebSphere 호스트 시스템의 정규화된 URL 입니다.

서버 이름

응용 프로그램 서버의 이름입니다.

프로필 이름

관리 UI 에 대해 사용되는 프로필의 이름입니다.

셀 이름

서버가 위치한 셀의 이름입니다.

노드 이름

서버가 위치한 노드의 이름입니다.

JDK

필요한 JDK 의 설치 위치입니다.

관리 UI 설치

다음 단원에서는 기존 응용 프로그램 서버 인프라에 관리 UI 를 설치하는 방법에 대해 자세히 설명합니다.

설치하기 전에

관리 UI 를 설치하기 전에 다음 사항을 고려하십시오.

- 기술 지원 사이트의 설치 미디어를 사용하여 관리 UI 를 설치합니다.

참고: 설치 미디어 이름의 목록에 대해서는 *정책 서버 릴리스 정보*를 참조하십시오.

- 기존 응용 프로그램 서버 인프라에 설치하는 경우 다음 절차가 적용됩니다. 독립 실행형 옵션을 사용하여 설치하는 경우 "관리 UI 설치"를 참조하십시오.
- (Windows) 관리 UI 호스트 시스템에서 설치 관리자를 실행합니다. 설치 관리자를 매핑된 네트워크 공유 또는 UNC 경로에서 실행하지 마십시오.
- 설치 zip 파일에는 설치 미디어와 같은 수준에서 `layout.properties` 파일이 포함되어 있습니다. 설치 zip 파일의 압축을 풀 후 설치 미디어를 이동한 경우 속성 파일을 동일한 위치로 이동해야 합니다. 그렇지 않으면 설치가 실패합니다.
- (Red Hat Linux) Red Hat 6 운영 체제는 성능을 위해 엔트로피를 사용합니다. 구성 요소를 설치하기 전에 엔트로피를 늘리십시오. 엔트로피가 충분하지 않으면 설치를 완료하는 데 시간이 매우 오래 걸릴 수 있습니다. 기호화된 링크를 설정하려면 다음 명령을 사용하십시오.

```
mv /dev/random /dev/random.org  
ln -s /dev/urandom /dev/random
```
- (UNIX) 권한에 따라 다음 명령을 실행하여 설치 미디어가 있는 디렉터리에 대한 실행 권한을 추가합니다.

```
chmod -R+x directory
```

directory

설치 미디어가 들어 있는 디렉터리를 지정합니다.
- (UNIX) 관리 UI 를 설치하는 사용자는 응용 프로그램 서버가 설치된 디렉터리에 대한 읽기/쓰기 권한이 있어야 합니다.
- (UNIX) 여러 서브넷에서 관리 UI 설치 관리자를 실행하면 설치 관리자가 충돌할 수 있습니다. 호스트 시스템에서 직접 관리 UI 를 설치하십시오.

추가 정보:

[관리 UI 설치](#) (페이지 443)

[관리 UI 설치 방법](#) (페이지 448)

Windows 에서 관리 UI 설치

관리 UI 를 기존 응용 프로그램 서버에 설치하여 액세스 제어, 보고 및 정책과 관련된 모든 태스크를 수행할 수 있는 관리 콘솔을 제공하십시오.

다음 단계를 수행하십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. 설치 미디어를 탐색합니다.
3. *installation_media* 를 두 번 클릭합니다.

installation_media

관리 UI 설치 실행 파일을 지정합니다.

설치 관리자가 시작됩니다.

참고: 설치 미디어 이름의 목록에 대해서는 정책 서버 릴리스 정보를 참조하십시오.

4. 수집한 정보를 기초로 설치를 위해 필요한 값을 입력하십시오.
5. 설치 설정을 검토하고 "설치"를 클릭합니다.

관리 UI 가 설치됩니다.

참고: 관리 UI 를 정책 서버에 등록하기 전까지는 관리 UI 를 사용하여 환경을 관리할 수 없습니다.

GUI 를 사용하여 관리 UI 설치

관리 UI 를 기존 응용 프로그램 서버에 설치하여 액세스 제어, 보고 및 정책 분석과 관련된 모든 태스크를 수행할 수 있는 관리 콘솔을 제공하십시오.

다음 단계를 수행하십시오.

1. 포그라운드에서 실행 중인 응용 프로그램을 모두 종료합니다.
2. 셸을 열고 설치 미디어를 탐색합니다.

3. 다음 명령을 입력합니다.

```
./installation_media gui
```

installation_media

관리 UI 설치 실행 파일을 지정합니다.

설치 관리자가 시작됩니다.

참고: 설치 미디어 이름의 목록에 대해서는 *정책 서버 릴리스 정보*를 참조하십시오.

4. 완성된 설치 워크시트를 사용하여 필요한 값을 입력합니다.

5. 설치 설정을 검토하고 "설치"를 클릭합니다.

관리 UI 가 설치됩니다.

6. "Done"(완료)을 클릭하고 시스템을 재부팅합니다.

관리 UI 가 설치됩니다.

참고: 관리 UI 를 정책 서버에 등록하기 전까지는 관리 UI 를 사용하여 환경을 관리할 수 없습니다.

추가 정보:

[관리 UI 등록 방법](#) (페이지 553)

UNIX 콘솔을 사용하여 관리 UI 설치

관리 UI 를 기존 응용 프로그램 서버에 설치하여 액세스 제어, 보고 및 정책 분석과 관련된 모든 태스크를 수행할 수 있는 관리 콘솔을 제공하십시오.

다음 단계를 수행하십시오.

1. 포그라운드에서 실행 중인 응용 프로그램을 모두 종료합니다.

2. 셸을 열고 설치 미디어를 탐색합니다.
3. 다음 명령을 입력합니다.

```
./installation_media -i console
```

installation_media

관리 UI 설치 실행 파일을 지정합니다.

설치 관리자가 시작됩니다.

참고: 설치 미디어 이름의 목록에 대해서는 *정책 서버 릴리스 정보*를 참조하십시오.

4. 완성된 설치 워크시트를 사용하여 필요한 값을 입력합니다.
5. 설치 설정을 검토하고 Enter 키를 누릅니다.
관리 UI 가 설치됩니다.

6. Enter 키를 누릅니다.
설치 관리자가 닫힙니다.

7. 시스템을 재부팅합니다.
관리 UI 가 설치됩니다.

참고: 관리 UI 를 정책 서버에 등록하기 전까지는 관리 UI 를 사용하여 환경을 관리할 수 없습니다.

추가 정보:

[관리 UI 등록 방법](#) (페이지 553)

관리 UI 등록 방법

관리 UI 를 사용하여 환경을 관리하려면 먼저 등록해야 합니다. 관리 UI 를 등록하면 관리 UI 와 정책 서버 간에 신뢰할 수 있는 연결이 생성됩니다.

이 프로세스에서는 기존 응용 프로그램 서버 인프라에 설치한 관리 UI 를 등록하는 방법을 설명합니다. 독립 실행형 옵션을 사용하여 설치한 관리 UI 를 등록하려면 "관리 UI 설치"를 참조하십시오.

다음 단계를 수행하십시오.

1. [등록 창을 재설정합니다](#) (페이지 445).
2. 필요한 경우 [FIPS 환경 변수를 만듭니다](#) (페이지 453).
3. [응용 프로그램 서버를 시작합니다](#) (페이지 558).
4. [관리 UI 를 등록합니다](#) (페이지 559).

추가 정보:

[관리 UI 설치](#) (페이지 443)

[관리 UI 등록 방법](#) (페이지 453)

관리 UI 등록 창 재설정

다음 작업 중 하나를 수행한 후 24 시간 이상 경과한 경우 이 단계를 수행해야 합니다.

- 정책 서버 설치 마법사를 사용하여 정책 저장소를 자동으로 구성
- XPSRegClient 유틸리티를 사용하여 SiteMinder 슈퍼 사용자 자격 증명을 정책 서버에 제출

참고: (UNIX) XPSRegClient 를 사용하기 전에 SiteMinder 환경 변수가 설정되어야 합니다. 환경 변수가 설정되지 않은 경우 [수동으로 설정하십시오](#) (페이지 568).

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder_administrator[:passphrase] -adminui-setup -t timeout -r  
retries -c comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

siteminder_administrator

SiteMinder 관리자를 지정합니다. 관리 UI 설치 시 다음 사항을 고려하십시오.

- 새로운 12.52 SP1 환경의 일부로 설치할 경우 다음 기본 계정을 지정합니다.

siteminder

- 업그레이드의 일부로 설치할 경우 정책 저장소에서 슈퍼 사용자 권한을 갖는 SiteMinder 관리자 계정을 지정합니다. 정책 저장소에 슈퍼 사용자 계정이 없으면 smreg 유틸리티를 사용하여 기본 계정을 생성하십시오.

passphrase

SiteMinder 관리자 계정의 암호를 지정합니다.

-adminui-setup

관리 UI가 정책 서버에 최초로 등록됨을 지정합니다.

-t timeout

(선택 사항) 등록을 완료하기 위해 관리 UI 설치 후 로그인하기까지 허용되는 제한 시간을 지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록 요청을 거부합니다.

측정 단위: 분

기본값: 1440(24 시간)

최소 제한: 1

최대 제한: 1440(24 시간)

-r retries

(선택 사항) 관리 UI를 등록할 때 허용되는 시도 실패 횟수를 지정합니다. 관리 UI에 최초로 로그인할 때 올바르지 않은 SiteMinder 관리자 자격 증명을 제출하면 등록 시도가 실패할 수 있습니다.

기본값: 1

최대 제한: 5

-c comment

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을 삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 유틸리티에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l log path

(선택 사항) 등록 로그 파일을 내보내야 하는 위치를 지정합니다.

기본값: `siteminder_home\log`

`siteminder_home`

정책 서버 설치 경로를 지정합니다.

-e error path

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: `stderr`

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

3. Enter 키를 누릅니다.

정책 서버에 관리자 자격 증명이 제공됩니다. 정책 서버에서는 관리 UI에 최초로 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

FIPS 환경 변수 만들기

사용자 환경이 다음 두 조건을 모두 충족할 경우 처음으로 관리 UI 를 등록할 때 FIPS 환경 변수를 생성해야 합니다.

- 등록하려는 정책 서버가 FIPS 전용 모드에서 작동 중입니다.
- 관리 UI 가 정책 서버 호스트 시스템에 설치되어 있지 않습니다.

다음 단계를 수행하십시오.

1. 다음 단계 중 하나를 완료하십시오.

- (Windows) 관리 사용자로 관리 UI 호스트 시스템에 로그인합니다.
- (UNIX) 관리 UI 를 설치한 사용자로 관리 UI 호스트 시스템에 로그인합니다.

2. 다음 환경 변수를 설정합니다.

`CA_SM_PS_FIPS140=ONLY`

참고: 환경 변수 설정에 대한 자세한 내용은 해당 OS 설명서를 참조하십시오.

3. 관리 UI 를 실행하는 Windows 또는 UNIX 셸이 `CA_SM_PS_FIPS140` 변수를 올바르게 인식하는지 확인합니다.

응용 프로그램 서버 시작

기존 응용 프로그램 서버 인프라에 관리 UI 를 설치한 경우 다음 절차가 적용됩니다. 독립 실행형 옵션을 사용하여 관리 UI 를 설치한 경우 "관리 UI 설치"를 참조하십시오.

다음 단계를 수행하십시오.

1. 다음 단계 중 하나를 완료하십시오.

- **JBoss** - 명령 프롬프트에서 *jboss_home\bin* 으로 이동합니다.

jboss_home

JBoss 설치 경로를 지정합니다.

- **WebLogic** - 명령 프롬프트에서 *domains\bin* 으로 이동합니다.

domains

관리 UI 에 대해 생성한 WebLogic 도메인의 경로를 지정합니다.

예: C:\bea\user_projects\domains\mydomain

- **WebSphere** - 명령 프롬프트에서 *profile\bin* 으로 이동합니다.

profile

관리 UI 에 대해 생성한 WebSphere 프로파일 이름의 경로를 지정합니다.

예: C:\Program

Files\IBM\WebSphere\AppServer\profiles\AppSvr01\bin

2. 다음 단계 중 하나를 완료하십시오.

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

- **JBoss**

- Windows: 다음 명령을 입력하고 Enter 키를 누릅니다.

run.bat

- UNIX: 다음 명령을 입력하고 Enter 키를 누릅니다.

run.sh

■ WebLogic

- Windows: 다음 명령을 입력하고 Enter 키를 누릅니다.
`startWebLogic.cmd`
- UNIX: 다음 명령을 입력하고 Enter 키를 누릅니다.
`startWebLogic.sh`

■ WebSphere

- Windows: 다음 명령을 입력하고 Enter 키를 누릅니다.
`startServer.bat identifier`
- UNIX: 다음 명령을 입력하고 Enter 키를 누릅니다.
`startServer.sh identifier`
`identifier`

WebSphere 설치 식별자를 지정합니다.

예: `startServer.bat Server1`

응용 프로그램 서버가 시작됩니다.

추가 정보:

[관리 UI 설치](#) (페이지 443)

[응용 프로그램 서버 시작](#) (페이지 454)

관리 UI 등록

환경 관리를 시작하려면 관리 UI 를 정책 서버에 등록하십시오.

다음 단계를 수행하십시오.

1. 다음 단계 중 하나를 완료하십시오.

- (Windows) 관리 UI 바로 가기를 사용하여 관리 UI 를 엽니다.
- (UNIX) 웹 브라우저를 열고 다음 위치로 이동합니다.

`host:port/iam/siteminder/adminui`

참고: 호스트 시스템에 웹 브라우저가 없을 경우 원격으로 로그인 화면에 액세스할 수 있습니다.

host

정규화된 관리 UI 호스트 시스템 이름을 지정합니다.

port

JBoss 가 HTTP 요청에 대해 수신 대기하는 포트를 지정합니다.

SiteMinder 관리 UI 로그인 화면이 표시됩니다.

2. "사용자 이름" 필드에 다음 값을 입력합니다.

siteminder

3. "암호" 필드에 SiteMinder 슈퍼 사용자 계정 암호를 입력합니다.

참고: 슈퍼 사용자 계정 암호에 달러 -기호(\$) 문자가 있으면 달러 기호 문자의 각 인스턴스를 \$DOLLAR\$로 바꾸십시오. 예를 들어 SiteMinder 슈퍼 사용자 계정 암호가 \$password 이면 "암호" 필드에 \$DOLLAR\$password 를 입력하십시오.

4. "서버" 필드에 정책 서버의 정규화된 호스트 이름을 입력합니다.

다음 사항을 고려하십시오.

- 유효한 IPv4 주소 또는 IPv6 주소를 입력할 수 있습니다.
- 포트를 지정하지 않으면 등록에서 정책 서버의 기본 인증 포트인 44442 로 기본 지정됩니다.

관리 UI 가 열리고 정책 서버에 등록됩니다.

추가 정보:

[파일에 등록 기록이 없다는 오류가 나타남](#) (페이지 581)

응용 프로그램 서버 중지

기존 응용 프로그램 서버 인프라에 관리 UI 를 설치한 경우 다음 절차가 적용됩니다. 독립 실행형 옵션을 사용하여 관리 UI 를 설치한 경우 "관리 UI 설치"를 참조하십시오.

응용 프로그램 서버를 중지하려면

1. 다음 작업 중 하나를 수행하십시오.

- **JBoss** - 관리 UI 호스트 시스템에서 "Start Task Engine"(태스크 엔진 시작) 명령 프롬프트를 엽니다.
- **WebLogic** - 관리 UI 호스트 시스템에서 "Start Task Engine"(태스크 엔진 시작) 명령 프롬프트를 엽니다.
- **WebSphere** - 명령 프롬프트에서 *profile\bin* 으로 이동합니다.

profile

관리 UI 에 대해 생성한 WebSphere 프로파일 이름의 경로를 지정합니다.

예: C:\Program

Files\IBM\WebSphere\AppServer\profiles\AppSvr01\bin

2. 다음 작업 중 하나를 수행하십시오.

- **JBoss** - 다음 키 조합을 입력합니다.
Ctrl+C
- **WebLogic** - 다음 키 조합을 입력합니다.
Ctrl+C

■ WebSphere

- Windows: stopServer.bat 식별자를 입력하고 Enter 키를 누릅니다.

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

- UNIX: stopServer.sh 식별자를 입력하고 Enter 키를 누릅니다.
identifier

WebSphere 설치 식별자를 지정합니다.

예: stopServer.bat Server1

응용 프로그램 서버가 중지됩니다.

추가 정보:

[관리 UI 설치](#) (페이지 443)

[응용 프로그램 서버 중지](#) (페이지 457)

관리자 자격 증명

기본적으로 관리 UI 는 정책 저장소를 SiteMinder 관리자 자격 증명의 원본으로 사용합니다. 관리 UI 가 회사 디렉터리 같은 외부 저장소를 사용하도록 구성할 수 있습니다.

참고: 외부 관리자 사용자 저장소 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

관리 UI 고가용성

예기치 않은 중단으로 인해 SiteMinder 개체를 관리하지 못하게 되는 문제가 발생하지 않도록 관리 UI 를 두 개 이상 설치하십시오. 다른 관리 UI 를 설치하기 전에 다음 사항을 고려하십시오.

- 아직 특정 관리 UI 와 트러스트 연결을 공유하지 않는 정책 서버에 해당 관리 UI 를 등록합니다. 다른 정책 서버에 등록하면 특정 단일 정책 서버가 중지되어 두 GUI 가 모두 비활성화되는 문제를 예방할 수 있습니다.
- 관리 UI 는 여러 정책 서버로 장애 조치될 수 없습니다. 하지만 여러 정책 서버를 관리하도록 관리 UI 를 구성할 수 있습니다.
- 기존 관리 UI 가 외부 SiteMinder 관리자 인증에 대해 구성된 경우:
 - 새 관리 UI 를 동일한 외부 저장소를 사용하여 구성합니다. 새 관리 UI 를 동일한 외부 저장소를 사용하여 구성하면 모든 SiteMinder 관리자가 모든 GUI 를 사용할 수 있습니다.
 - 동일한 외부 저장소에 대한 이후의 관리 UI 연결은 동일한 네트워크 식별자를 사용하여 구성해야 합니다. 동일한 외부 저장소에 대한 여러 관리 UI 연결에는 네트워크 식별자를 혼합해서 사용할 수 없습니다.

예: 첫 번째 연결을 172.16.0.0 을 사용하여 구성한 경우 이후의 연결도 172.16.0.0 을 사용하여 생성합니다. 마찬가지로 첫 번째 연결을 comp001@example.com 을 사용하여 구성한 경우 이후의 연결도 comp001@example.com 을 사용하여 생성합니다.

추가 정보:

[관리 UI 설치 방법](#) (페이지 546)

Windows 에서 관리 UI 제거

시스템에서 더 이상 필요하지 않을 경우 기존 응용 프로그램 서버에서 관리 UI 를 제거하십시오.

다음 단계를 수행하십시오.

1. 응용 프로그램 서버를 중지합니다.
2. Windows 제어판을 열고 프로그램 목록으로 이동합니다.
3. CA SiteMinder 관리 UI 를 마우스 오른쪽 단추로 클릭합니다.
4. "제거/변경"을 클릭합니다.
5. 마법사의 지시를 따릅니다.

참고: 공유 파일을 제거할지 묻는 메시지가 표시되면 "No to All"(모두 아니요)을 클릭합니다.

6. 필요한 경우 시스템을 재부팅합니다.
관리 UI 가 제거되었습니다.

추가 정보:

[\(선택 사항\) 관리 UI 제거](#) (페이지 464)

UNIX 에서 관리 UI 제거

시스템에서 더 이상 필요하지 않을 경우 기존 응용 프로그램 서버에서 관리 UI 를 제거하십시오.

참고: 이 구성 요소를 제거하기 위해 설치 디렉터리를 수동으로 제거하지 마십시오. 제거용 셸 스크립트를 실행해야 합니다. 설치 디렉터리만 제거한 경우 관련 레지스트리가 남아 있게 됩니다. 이 호스트 시스템에 이 구성 요소를 다시 설치하려고 하면 이러한 항목으로 인해 설치가 실패할 수 있습니다.

다음 단계를 수행하십시오.

1. 응용 프로그램 서버를 중지합니다.
2. 셸을 열고 다음 디렉터리로 이동합니다.

`administrative_ui_home/CA/adminui/install_config_info`

`administrative_ui_home`

관리 UI 설치 경로를 지정합니다.

3. 다음 명령을 실행합니다.

```
./smwam-ui-uninstall.sh
```

관리 UI 제거 프로세스가 시작됩니다.

4. 지시에 따라 관리 UI 를 제거합니다.

관리 UI 가 제거되면 메시지가 표시됩니다.

관리 UI 가 제거되었습니다.

추가 정보:

[관리 UI 설치](#) (페이지 443)

[UNIX 에서 관리 UI 제거](#) (페이지 465)

제 13 장: 문제 해결

이 섹션은 다음 항목을 포함하고 있습니다.

[정책 서버 문제 해결](#) (페이지 567)

[정책 저장소 문제 해결](#) (페이지 574)

[OneView 모니터 문제 해결](#) (페이지 577)

[관리 UI 문제 해결](#) (페이지 579)

[보고서 서버 문제 해결](#) (페이지 588)

정책 서버 문제 해결

다음 단원에서는 설치 중 정책 서버와 관련하여 발생하는 일반적인 문제와 권장 해결책에 대해 자세히 설명합니다.

Solaris 의 NETE_PS_ALT_CONF_FILE 환경 변수

Solaris 에 정책 서버를 설치하면 `nete_ps_env.ksh` 스크립트에 다음 항목이 포함될 수 있습니다.

```
export NETE_PS_ALT_CONF_FILE=/export/siteminder/config/.siteminder.conf
```

NETE_PS_ALT_CONF_FILE 환경 변수는 정책 서버의 서비스를 중지하고 시작하는 `stop-all` 및 `start-all` 스크립트에서 사용됩니다. `.siteminder.conf` 파일은 이러한 스크립트에 의해 생성되는 임시 런타임 파일로, SiteMinder 구성에는 영향을 주지 않습니다.

NETE_PS_ALT_CONF_FILE 환경 변수는 수정하지 마십시오.

설치 후 정책 서버가 시작되지 않음

Windows 및 UNIX 시스템에 해당

증상:

정책 서버를 설치했는데 정책 서버가 시작되지 않습니다.

해결책:

잘못된 JRE 버전을 설치했을 수 있습니다. JRE 버전이 올바른지 확인하십시오.

참고: 지원되는 CA 및 타사 구성 요소의 목록에 대해서는 기술 지원 사이트의 SiteMinder 12.52 SP1 Platform Support Matrix(플랫폼 지원표)를 참조하십시오.

프로필 파일에 SiteMinder 환경 변수가 설정되지 않음

UNIX 에 해당

증상

정책 서버가 설치되었는데 .profile 파일에 SiteMinder 환경 변수(smprofile.ksh)가 추가되지 않았습니다. SiteMinder 환경 변수를 수동으로 설정해야 합니다.

해결 방법

SiteMinder 환경 변수를 추가하려면

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 셸을 열고 *siteminder_home* 으로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

3. 다음 명령을 실행합니다.

```
smprofile.ksh
```

SiteMinder 환경 변수가 설정됩니다.

Winsock 오류 10054 메시지

Windows 에 해당

증상:

정책 서버에 로그인하려고 하면 "Unable to proceed, winsock error 10054"(계속할 수 없습니다. winsock 오류 10054) 메시지가 표시됩니다.

해결책:

다음 중 하나가 문제의 원인일 수 있습니다.

- 정책 저장소에 적절한 SiteMinder 스키마가 없습니다. 올바른 SiteMinder 스키마를 가져왔는지 확인하십시오.
- 정책 서버가 실행되고 있지 않습니다. 정책 서버를 시작하려면 정책 서버 관리 콘솔의 "상태" 탭을 사용하십시오.

중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

- 정책 서버가 정책 저장소에 제대로 연결되지 않았습니다. 정책 서버 관리 콘솔의 "데이터" 탭에서 "연결 테스트"를 클릭하여 정책 저장소에 연결되는지 확인하십시오. 정책 저장소에 연결되지 않을 경우 "데이터" 탭에서 정책 서버를 정책 저장소에 연결하여 데이터 원본 정보 값을 다시 입력하십시오.

SiteMinder 라이선스 작업

증상

- 현재 정책 서버 평가판 라이선스를 사용 중이며 정품 라이선스를 구해서 추가하려고 합니다.
- SiteMinder 라이선스가 있지만 찾을 수 없습니다.
- SiteMinder 라이선스가 있지만 새 제품 키로 업데이트하는 방법을 모릅니다.

해결 방법

SiteMinder 라이선스를 요청하려면

1. [기술 지원 사이트](#)로 이동합니다.
2. "CA Licensing Inquires"(CA 라이선스 조회)를 클릭합니다. 이 링크는 "Address Licensing Needs"(라이선스 요구 해결) 아래에 있습니다.
"CA Customer Care"(CA 고객 서비스) 사이트가 새 창에서 열립니다.
3. "Licensing Issue Request"(라이선스 발급 요청)를 클릭합니다. 이 링크는 "Contact Us"(문의) 아래에 있습니다.
온라인 요청 양식이 새 창에서 열립니다.
4. 필요한 정보를 입력한 다음 "Submit"(제출)을 클릭합니다.

정품 SiteMinder 라이선스를 정책 서버에 추가하려면

1. SiteMinder 라이선스를 요청합니다.
2. 정책 서버 호스트 시스템에 액세스합니다.
3. 다음 작업 중 하나를 수행하십시오.
 - (Windows) *siteminder_home*\license 로 이동합니다.
 - (UNIX) *siteminder_home*/license 로 이동합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

4. license.dat 파일을 라이선스 디렉터리에 복사합니다.
5. 정책 서버를 다시 시작합니다.

기존 SiteMinder 라이선스를 찾으려면

1. [기술 지원 사이트](#)에 로그인합니다.
2. "Licensing"(라이선스)을 클릭합니다. "Licensing"(라이선스)은 "Support"(지원) 아래의 왼쪽에 있습니다.
"CA Licensing"(CA 라이선스) 화면이 표시됩니다.
3. "View Licenses"(라이선스 보기)를 클릭합니다. "View Licenses"(라이선스 보기)는 "SiteMinder and Identity Manager Licenses"(SiteMinder 및 Identity Manager 라이선스) 아래에 있습니다.
해당 키와 함께 모든 라이선스에 대한 상세 정보가 표시됩니다.

라이선스 파일에 SiteMinder 라이선스 키를 적용하려면

1. 정책 서버 호스트 시스템에 액세스합니다.
2. 다음 작업 중 하나를 수행하십시오.
 - (Windows) *siteminder_home*\license 로 이동합니다.
 - (UNIX) *siteminder_home*/license 로 이동합니다.
- siteminder_home***
- 정책 서버 설치 경로를 지정합니다.
3. license.dat 파일을 엽니다.
4. CA Support 사이트에서 받은 라이선스 키를 복사하여 라이선스 파일에 붙여 넣습니다.
5. 라이선스 파일을 저장합니다.
6. 정책 서버를 다시 시작합니다.

영어가 아닌 입력 문자에 정크 문자가 포함됨**UNIX/Linux 에 해당****증상**

영어가 아닌 일부 입력 문자가 콘솔 창에 올바르게 표시되지 않습니다.

해결 방법

콘솔 창의 터미널 설정을 확인하십시오. 콘솔이 입력 문자의 높은(8) 비트를 삭제하지 않는지 확인하십시오. 다음 명령을 실행합니다.

```
stty -istrip
```

설치 제거 시 Java 오류 메시지

증상:

정책 서버, 웹 에이전트, SDK 또는 설명서를 제거하려고 하면 제거 프로그램이 중지되고 다음 오류 메시지 중 하나가 나타납니다.

- "Could not find a valid Java virtual machine to load. You need to reinstall a supported Java virtual machine." (로드할 유효한 Java Virtual Machine 을 찾을 수 없습니다. 지원되는 Java Virtual Machine 을 다시 설치해야 합니다.)
- "No Java virtual machine could be found from your PATH environment variable. You must install a VM prior to running this program." (PATH 환경 변수에서 Java Virtual Machine 을 찾을 수 없습니다. 이 프로그램을 실행하기 전에 VM 을 설치해야 합니다.)

해결책:

PATH 변수에 JRE 가 있는지 확인하십시오.

Windows 에서 PATH 변수에 JRE 설정

PATH 변수에 JRE 를 설정하려면

1. 제어판으로 이동합니다.
2. "시스템"을 두 번 클릭합니다.
3. "환경 변수" 대화 상자에서 Path 시스템 변수에 JRE 의 위치를 추가합니다.

Solaris 에서 PATH 변수에 JRE 설정

PATH 변수에 JRE 를 설정하려면

다음 명령을 실행합니다.

1. PATH=\$PATH:<JRE>/bin

JRE

JRE 의 위치를 지정합니다.

2. export PATH

Adobe Acrobat Reader 가 설치되지 않음

Windows 에 해당

증상:

Adobe Acrobat 을 설치할 때 설치 프로그램이 중단됩니다.

해결책:

정책 서버 서비스가 실행 중인 경우 Acrobat Reader 설치 프로그램이 중단되면 정책 서버 관리 콘솔의 "상태" 탭을 사용하여 정책 서버 서비스를 중지하십시오. 서비스를 중지하면 설치 프로그램이 시작됩니다.

중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로서 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

Active Directory 를 사용자 저장소로 사용할 경우의 문제

증상:

Active Directory 를 사용자 저장소로 사용할 때 정책 서버에서 이 저장소에 연결할 수 없다는 오류 메시지가 표시됩니다.

해결책:

Active Directory 기반 사용자 저장소를 생성할 때 관리 UI 에서 정규화된 호스트 이름(예: host.domain.com)을 지정해야 하며 컴퓨터의 IP 주소를 사용하면 안 됩니다. 또한 Active Directory 는 정규화된 호스트 이름으로 식별된 정책 서버로 조회를 보내므로 정책 서버가 설치된 컴퓨터에서 host.domain.com 과 domain.com 을 ping 할 수 있는지 확인하십시오. 정규화된 호스트 이름이 잘못되어 연결이 불가능하면 정책 서버에서 오류 메시지가 표시됩니다.

"AE failed to load library 'smjavaapi'." (AE 에서 'smjavaapi' 라이브러리를 로드하지 못했습니다.) 시스템 오류

Windows 및 UNIX 시스템에 해당

증상:

권한 부여 중 "AE failed to load library 'smjavaapi'. System error: The specified module could not be found." (AE 에서 'smjavaapi' 라이브러리를 로드하지 못했습니다. 시스템 오류: 지정된 모듈을 찾을 수 없습니다.)라는 오류 메시지가 표시됩니다.

해결책:

Windows 의 경우 PATH 변수를

<SiteMinder_installation>\config\JVMOptions.txt 로 설정하고, UNIX 시스템의 경우 LD_LIBRARY_PATH 를 <SiteMinder_installation>/config/JVMOptions.txt 로 설정하십시오.

정책 저장소 문제 해결

다음 단원에서는 설치 중 정책 저장소와 관련하여 발생하는 일반적인 문제와 권장 해결책에 대해 자세히 설명합니다.

많은 수의 개체가 포함된 정책 저장소

Windows 및 UNIX 시스템에 해당

증상:

정책 저장소에서 관리 UI 에 java.lang.IndexOutOfBoundsException 예외가 반환되었습니다.

해결책:

정책 저장소에 많은 수의 개체가 포함된 경우 관리 UI 에 java.lang.IndexOutOfBoundsException 예외가 반환될 수 있습니다.

레지스트리 키

\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\ObjectStore\MaxObjects 를 100 보다 작은 값(예: 50)으로 정의하십시오.

SSL initialization failed: error -8174 (security library: bad database.)

Windows 및 UNIX 시스템에 해당

증상:

Oracle Directory Server 정책 저장소를 사용하여 환경이 구성되었고, SSL 을 통해 통신하도록 정책 저장소가 구성되었습니다.

다음과 같은 오류 메시지가 표시되었습니다.

SSL initialization failed: error -8174 (security library: bad database.)

이 메시지는 다음 명령을 실행한 후 표시됩니다.

```
smldapsetup ldmod -fpstore -ssl1 -c/app/siteminder/ssl/cert8.db
```

해결책:

1. key3.db 파일이 cert8.db 파일과 동일한 디렉터리에 있는지 확인합니다.
2. smldapsetup 명령을 다시 실행합니다. -c 옵션을 사용하여 SSL 클라이언트 인증서 데이터베이스 파일이 있는 디렉터리의 경로를 지정합니다.

예:

```
-c/app/siteminder/ssl/cert8.db
```

ODBC 정책 저장소를 가져올 때 UserDirectory 오류가 발생하고 가져오기가 실패함

증상

정책 저장소 데이터를 ODBC 정책 저장소로 가져올 때 개체 유형 "UserDirectory"를 정책 저장소에 "저장"하는 데 실패했다는 오류 메시지가 표시됩니다.

해결 방법

ODBC 저장소의 userDirectory 개체에 있는 서버 이름이 512 자보다 길 수 있습니다. 이 길이는 SiteMinder 와 함께 제공되는 MS SQL Server 및 Oracle 정책 저장소 스키마 스크립트에서 기본적으로 허용되는 제한을 초과합니다.

다음 작업 중 하나를 수행하십시오.

정책 데이터를 지원되는 버전의 MS SQL Server 정책 저장소로 가져오려면 다음을 수행하십시오.

1. sm_mssql_ps.sql 을 엽니다.
참고: 이 스키마 스크립트는 *policy_server_home\db\SQL* 에 있습니다.
2. 다음 텍스트를 검색합니다.
CREATE TABLE smuserdirectory5
3. "server smstringreq512N"을 필요에 따라 다음 중 하나로 수정합니다.
 - server smstringreq1024,N
 - server smstringreq4000,N
4. 정책 저장소 스키마를 정책 저장소로 다시 가져옵니다.
5. 정책 저장소 데이터를 가져옵니다.

정책 데이터를 지원되는 버전의 Oracle 정책 저장소로 가져오려면 다음을 수행하십시오.

1. sm_oracle_ps.sql 을 엽니다.
참고: 이 스키마 스크립트는 *policy_server_home\db\SQL* 에 있습니다.
2. 다음 텍스트를 검색합니다.
CREATE TABLE smuserdirectory5

3. "server VARCHAR2(512) NOT NULL,"을 필요에 따라 다음 중 하나로 수정합니다.
 - server VARCHAR2(1024) NOT NULL,
 - server VARCHAR2(4000) NOT NULL,
4. 정책 저장소 스키마를 정책 저장소로 다시 가져옵니다.
5. 정책 저장소 데이터를 가져옵니다.

OneView 모니터 문제 해결

다음 단원에서는 설치 중 OneView 모니터와 관련하여 발생하는 일반적인 문제와 권장 해결책에 대해 자세히 설명합니다.

수정된 UNIX/Sun Java System 웹 서버 구성 파일의 문제 수정

ServletExec 설치에서 Oracle iPlanet 웹 서버 구성 파일을 수정한 경우 OneView 모니터 UI 를 구성하면 웹 서버 인스턴스가 작동하지 않습니다. ServletExec 설치 관리자가 이러한 파일에 정책 서버의 항목과 충돌하는 항목을 추가했기 때문입니다.

다음 단계를 수행하십시오.

1. `/sunjavasystem_home/servers/https-web_server_instance_name.domain.com/config/magnus.conf` 구성 파일을 엽니다.
2. 첫 번째 행을 제거합니다.

```
Init fn="ServletExecInit"
ServExec_instance_name.instances="IP_address:port_number"
```

ServExec_instance_name

ServletExec 인스턴스의 이름을 지정합니다.

IP_address

ServletExec 가 설치된 시스템의 IP 주소를 지정합니다.

port_number

ServletExec 인스턴스에 대한 포트 번호를 지정합니다.

참고: 정책 서버 구성 마법사가 파일의 끝에 올바른 항목을 추가했습니다.

3. `/sunjavasystem_home/servers/https-web_server_instance_name.domain.com/config/obj.conf` 구성 파일을 엽니다.

4. 다음 단계를 완료합니다.

- a. 파일의 위에서 4 번째 줄과 5 번째 행을 제거합니다.

```
NameTrans fn="assign-name" from="/servlet/*"  
name="<ServExec_instance_name>"  
NameTrans fn="assign-name" from="*.jsp*"   
name="<ServExec_instance_name>"
```

중요! 2 번째 줄과 3 번째 줄에서 다음 항목을 제거하지 마십시오. 정책 서버 구성 마법사가 추가한 항목입니다.

```
name=se-ServExec_instance_name
```

- b. 파일의 끝에서 마지막 두 번째 섹션을 제거합니다.

```
<Object name="ServExec_instance_name"  
Service fn="ServletExecService" group="ServExec_instance_name"  
</Object>
```

중요! 다음 항목을 제거하지 마십시오. 정책 서버 구성 마법사가 추가한 항목입니다.

```
<Object name="se-ServExec_instance_name">
```

5. 구성 파일을 저장하고 웹 서버 인스턴스를 시작합니다.

/sitemindermonitor 에 대한 Windows/IIS 가상 경로가 없음

Windows 에 해당

증상:

IIS Microsoft Management Console 의 "기본 웹 사이트" 아래에 /sitemindermonitor 에 대한 가상 경로가 없습니다.

해결책:

가상 경로를 생성하십시오.

가상 경로를 생성하려면

1. "시작" 메뉴에서 "프로그램", "관리 도구", "인터넷 서비스 관리자"로 이동합니다.
2. "기본 웹 사이트"를 선택합니다.

3. "동작" 메뉴에서 "새로 만들기", "가상 디렉터리"를 차례로 선택합니다.
"가상 디렉터리 마법사"가 열립니다.
4. 가상 디렉터리의 이름(별칭)을 지정합니다. 예를 들면 다음과 같습니다.
`sitemindermonitor`
참고: `sitemindermonitor` 는 예일 뿐이며, 어떤 이름이든 별칭으로 사용할 수 있습니다.
5. "다음"을 클릭합니다.
6. `<siteminder_installation>\monitor\`의 경로를 지정합니다.
7. "다음"을 클릭합니다.
8. 다음 권한을 선택합니다.
실행
9. "마침"을 클릭합니다.

관리 UI 문제 해결

다음 단원에서는 설치 중 관리 UI 등록과 관련하여 발생하는 일반적인 문제와 권장 해결책에 대해 자세히 설명합니다.

관리 UI 가 중단되어 응답하지 않음

증상

관리 UI 가 등록된 정책 서버를 다시 시작했습니다. 관리 UI 에서 태스크를 시작하려고 시도하면 중단되어 응답하지 않습니다.

해결 방법

관리 UI 를 다시 시작하십시오.

처리되지 않은 예외가 발생하고 WebSphere 가 중단됨

증상

관리 UI 를 기존 WebSphere 인프라에 설치했습니다. WebSphere 가 중단되고 `native_stderr` 로그에서 IBM Java 가비지 수집기의 처리되지 않은 예외를 보고합니다.

해결 방법

WebSphere 에서 포함된 Java SDK 를 패치합니다.

참고: 자세한 내용은 [IBM 솔루션](#)을 참조하십시오.

정책 서버 연결을 등록할 수 없음

증상

관리 UI 가 사용할 수 없는 정책 서버에 등록되어 있어 다른 정책 서버 연결을 등록하려고 하는데, 슈퍼 사용자 권한이 있는 관리자로 관리 UI 에 로그인해도 "정책 서버 연결 등록" 태스크가 나타나지 않습니다.

해결 방법

외부 관리자 저장소에 대한 연결을 구성할 때 단일 사용자에게 슈퍼 사용자 권한을 위임했습니다. 이 슈퍼 사용자 계정을 사용하여 관리 UI 에 로그인하십시오. 정책 서버 연결을 사용할 수 없게 될 경우 이 슈퍼 사용자만 정책 서버 연결을 등록할 수 있습니다.

API 오류가 나타남

증상

관리 UI 등록 시 에이전트 Agent API 오류 메시지가 나타나고 등록이 실패합니다.

해결 방법

정책 서버가 시작되지 않았습니다. 정책 서버 관리 콘솔을 사용하여 정책 서버를 시작합니다.

파일에 등록 기록이 없다는 오류가 나타남

증상

정책 서버에 관리 UI 를 등록할 때 파일에 등록 레코드가 없다는 오류 메시지가 나타나고 등록이 실패합니다.

이 메시지는 다음과 같은 경우에 나타날 수 있습니다.

- 관리 UI 를 설치한 후 정책 서버에 관리 UI 를 처음으로 등록하려고 할 경우
- 관리 UI 를 등록한 후 추가 정책 서버 연결을 등록하려고 할 경우

해결 방법

다음 작업 중 하나를 수행하십시오.

관리 UI 를 처음으로 등록하려는 경우

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient siteminder_administrator[:passphrase] -adminui-setup
```

siteminder_administrator

SiteMinder 관리자를 지정합니다. 관리 UI 설치 시 다음 사항을 고려하십시오.

- 새로운 12.52 SP1 환경의 일부로 설치할 경우 기본 SiteMinder 관리자 계정(siteminder)을 지정합니다.
- 업그레이드의 일부로 설치할 경우 정책 저장소에서 슈퍼 사용자 권한을 갖는 SiteMinder 관리자 계정을 지정합니다.

참고: r12.0 SP1 에서 업그레이드하려는 경우 슈퍼 사용자 계정이 없으면 smreg 유틸리티를 사용하여 기본 SiteMinder 관리자(siteminder)를 생성하십시오. smreg 유틸리티 사용에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

passphrase

SiteMinder 관리자 계정의 암호를 지정합니다.

제한:

- 암호에 6 자 이상을 포함해야 합니다.
- 암호에 앰퍼샌드(&)나 별표(*)는 포함할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

3. 기본 SiteMinder 관리자 계정으로 관리 UI 에 로그인하여 등록을 완료합니다.

추가 정책 서버 연결을 등록하려는 경우

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient client_name[:passphrase] -adminui
```

client_name

등록할 관리 UI 를 식별합니다.

제한: 이 값은 고유해야 합니다. 예를 들어 이전에 smui1 을 사용하여 관리 UI 를 등록했으면 smui2 를 입력합니다.

passphrase

관리 UI 등록을 완료하는 데 필요한 암호를 지정합니다.

제한:

- 암호에 6 자 이상을 포함해야 합니다.
- 암호에 앰퍼샌드(&)나 별표(*)는 포함할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

3. 관리 UI 에 로그인하여 정책 서버 연결을 등록합니다.

등록 파일이 잘못되었다는 오류가 나타남

증상

추가 정책 서버 연결을 등록하려고 하면 등록 파일이 잘못되었다는 오류 메시지가 나타나고 등록이 실패합니다.

해결 방법

입력한 암호가 XPSRegClient 를 사용하여 생성한 암호와 동일한지 확인하십시오. 생성한 값과 관리 UI 를 사용하여 입력하는 값이 일치해야 합니다.

암호가 없으면 다음 작업을 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

```
XPSRegClient client_name[:passphrase] -adminui
```

client_name

등록할 관리 UI 를 식별합니다.

제한: 이 값은 고유해야 합니다. 예를 들어 이전에 smui1 을 사용하여 관리 UI 를 등록했으면 smui2 를 입력합니다.

passphrase

관리 UI 등록을 완료하는 데 필요한 암호를 지정합니다.

제한:

- 암호에 6 자 이상을 포함해야 합니다.
- 암호에 앰퍼샌드(&)나 별표(*)는 포함할 수 없습니다.
- 암호에 공백이 있는 경우 암호를 따옴표로 묶으십시오.

3. 관리 UI 에 로그인하여 정책 서버 연결을 등록합니다.

시간 만료 없이 등록이 실패함

증상

관리 UI 등록이 시간 만료 없이 실패합니다.

해결 방법

다음 작업을 수행하십시오.

- 정책 서버를 호스트하는 컴퓨터를 ping 하여 컴퓨터가 사용 가능한지 확인합니다.
- `policy_server_home\bin` 에서 다음 등록 파일을 찾습니다.

`name.XPSReg`

`policy_server_home`

정책 서버 설치 경로를 지정합니다.

이름

관리 UI 등록 도구(XPSRegClient)를 사용하여 클라이언트 이름 및 암호를 생성할 때 지정한 클라이언트 이름을 식별합니다.

등록 파일이 없으면 XPSRegClient 를 실행하여 클라이언트 이름 및 암호를 생성하십시오.

- 정책 서버 로그 파일(smgs.log)을 열고 등록 시점 전후에 발생한 오류를 검토합니다.

관리 UI 등록 로그를 찾을 수 없음

증상

관리 UI 등록 문제를 해결하려고 하는데 로그 파일을 찾을 수 없습니다.

해결 방법

XPSRegClient 는 로그 파일을 생성하여 *policy_server_home\log* 에 저장합니다. 이 파일의 이름은 *XPSRegClient.date* 입니다.

policy_server_home

정책 서버 설치 경로를 지정합니다.

date

XPSRegClient 가 해당 파일을 생성한 날짜를 지정합니다.

예: XPSRegClient.2007-12-1.154002

참고: 마지막 여섯 자리는 같은 날짜에 생성된 파일이 여러 개일 경우 사용할 수 있는 고유 식별자입니다.

시간 만료 오류가 발생하고 검색이 실패함

증상

정책 개체 검색을 완료할 수 없습니다. 관리 UI 에서 검색 결과 대신 연결 시간 만료 오류가 표시됩니다.

해결 방법

관리 UI 를 사용하여 많은 정책 개체를 검색하는 경우 다음 결과가 하나 또는 둘 다 발생할 수 있습니다.

- 관리 UI 와 정책 서버 간의 연결이 시간 만료될 수 있습니다.
- 정책 서버 터널 버퍼가 손상될 수 있습니다.

후자의 경우 연결 시간 만료 오류가 표시됩니다. 관리 UI 정책 서버 연결 시간 만료를 조정하고 정책 서버 터널 버퍼 크기에 대한 레지스트리 키를 생성하면 문제가 해결됩니다.

정책 서버 연결 시간 만료를 조정하려면

1. 관리 UI에 로그인합니다.
2. "관리", "관리 UI", "정책 서버 연결", "정책 서버 연결 수정", "검색"을 차례로 클릭하여 정책 서버 연결 개체를 엽니다.
3. 적절한 정책 서버를 선택하고 "제출"을 클릭합니다.
4. "고급" 섹션의 "시간 만료" 필드를 2,000 초와 같은 큰 값으로 설정합니다.

이제 정책 서버 연결 만료 시간이 늘어났습니다.

터널 버퍼 크기에 대한 레지스트리 키를 생성하려면

1. 다음 정책 서버 레지스트리 키를 생성합니다.
`HKLM\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\PolicyServer\
Max AdmComm Buffer Size`
2. 이 레지스트리 키를 2,097,000 KB(0x1FFF68) 등의 큰 값으로 설정합니다.
3. 변경 내용을 저장하고 레지스트리를 종료합니다.

참고: 연결 시간 만료 및 버퍼 크기를 변경한 후에도 문제가 계속되면 관리 UI를 다시 시작하십시오.

기본 로깅 파일을 찾을 수 없음

증상

배포된 관리 UI 인스턴스의 문제를 해결하려고 하는데 기본 응용 프로그램 서버 로그 파일을 찾을 수 없습니다.

해결 방법

독립 실행형 설치 옵션을 사용한 경우 기본 로그 파일의 이름은 `server.log` 입니다. 이 로그 파일은 `administrative_ui_home\CA\SiteMinder\adminui\server\default\log` 에 있습니다.

administrative_ui_home

관리 UI 설치 경로를 지정합니다.

참고: 관리 UI 를 JBoss, WebSphere 또는 WebLogic 의 기존 인스턴스에 설치한 경우 기본 로깅에 대한 자세한 내용은 해당 공급업체의 설명서를 참조하십시오.

기본 로그 파일에 충분한 정보가 없음

증상

배포된 관리 UI 인스턴스의 문제를 해결하려고 하는데 기본 응용 프로그램 서버 로그 파일에 충분한 정보가 없습니다.

해결 방법

SiteMinderLog4j 속성 파일을 사용하여 SiteMinder 관련 로깅 설정을 구성하십시오. 이 파일에는 로깅 설정 구성에 대한 설명이 포함되어 있습니다. 파일 위치는 관리 UI 를 설치하는 데 사용한 설치 옵션에 따라 달라집니다.

■ 독립 실행형 설치

독립 실행형 설치 옵션을 사용한 경우 이 속성 파일은 `administrative_ui_home\CA\SiteMinder\adminui\server\default\deploy\iam_siteminder.ear\user_console.war\META-INF` 에 있습니다.

administrative_ui_home

관리 UI 설치 경로를 지정합니다.

- 기존 응용 프로그램 서버 인프라

관리 UI 를 기존 응용 프로그램 서버 인프라에 설치한 경우 이 속성 파일은 `deploy\iam_siteminder.ear\user_console.war\META-INF` 에 있습니다.

deploy

응용 프로그램 서버가 응용 프로그램을 배포하는 위치를 지정합니다.

참고: 관리 UI 를 12.52 SP1 로 업그레이드한 경우 이 속성 파일은 `deploy/IdentityMinder.ear/user_console.war/META-INF` 에 있습니다.

보고서 서버 문제 해결

다음 단원에서는 설치 중 보고서 서버 사용과 관련하여 발생하는 일반적인 문제와 권장 해결책에 대해 자세히 설명합니다.

보고서 서버 설치 시 문자와 관련된 오류가 발생하고 설치가 실패함

증상

설치 시 설치 경로에 사용한 문자와 관련된 오류가 발생하고 설치가 실패합니다.

해결 방법

보고서 서버를 설치할 때 설치 경로에는 다음 문자 유형만 사용할 수 있습니다.

- 영숫자
- 공백
- 대시
- 밑줄

이러한 문자 유형만 포함하도록 설치 경로를 수정하십시오.

보고서 서버 설치 관리자에서 파일 누락 오류가 표시됨

Windows 에 해당

증상

설치하는 동안 `vcredist.msi` 파일이 없다는 메시지가 나타나고, 해당 파일이 위치한 디렉터리로 매핑하라는 메시지가 표시됩니다.

해결 방법

다음 해결 방법 중 하나를 시도합니다.

- Microsoft Visual C++ 2005 재배포 가능 요소를 제거하십시오.
- "취소"를 클릭하여 설치를 계속하십시오.

설치가 성공적으로 완료됩니다. Xcelsius 응용 프로그램과 관련된 문제가 발생한 경우 Microsoft 웹 사이트에서 `vcredist.msi` 를 다운로드하여 설치하십시오.

설치 제거에서 응용 프로그램을 닫으라는 메시지가 표시됨

Windows 2008 R2 에 해당

증상

보고서 서버를 제거할 때 계속하려면 다음과 같은 응용 프로그램을 닫으라는 메시지가 표시됩니다.

- Java Platform SE 바이너리
- BOE120MySQL

해결 방법

"Do not close the applications"(응용 프로그램을 닫지 않습니다) 옵션을 선택하고 "OK"(확인)를 클릭하십시오.

설치 관리자가 자동으로 응용 프로그램을 닫도록 두면 프로세스가 실패합니다.

감사 기반 보고서에 결과가 반환되지 않음

Oracle 기반 감사 저장소에 해당

증상

감사 기반 보고서에 결과가 반환되지 않습니다.

해결 방법

감사 데이터베이스를 구성할 때 사용된 사용자 계정에 DB 역할이 있는지 확인하십시오. 사용자 계정에 DB 역할이 있으면 제거하십시오. DB 역할이 있으면 감사 기반 보고서에서 올바른 감사 테이블을 쿼리하지 못합니다.

정책 분석 보고서를 실행할 수 없음

Solaris 에 해당

증상

정책 분석 보고서를 실행하면 보고서가 실패하고 다음과 같은 메시지가 표시됩니다.

Failed to retrieve data from the database(데이터베이스에서 데이터를 검색하지 못했습니다.)

해결 방법

이 오류는 다음 문제 중 하나와 관련이 있습니다.

CRConfig.xml 파일에서 **Java** 클래스가 누락되었습니다.

1. `report_server_home/CommonReporting3/bobje/java` 로 이동합니다.

report_server_home

보고서 서버 설치 경로를 지정합니다.

2. 파일의 **Classpath** 섹션에 다음 클래스가 있는지 확인합니다.

- `smjavaagentapi.jar`
- `smanalyzer.jar`

3. **JavaBeans** 섹션에 다음 클래스가 있는지 확인합니다.

`webadmin-report-ds.jar`

보고서 서버와 정책 서버 간의 연결이 끊어졌습니다.

보고서 서버를 다시 등록하십시오.

보고서 서버가 올바르게 시작되지 않았습니다.

보고서 서버를 다시 시작합니다.

추가 정보:

[보고서 서버 등록 방법](#) (페이지 499)

관리 UI에서 파일 누락 오류가 표시됨

증상

보고서 서버를 설치하고 구성했는데 관리 UI에서 보고서 매개 변수 정의 파일이 없다는 내용의 메시지가 표시됩니다.

해결 방법

보고서 템플릿을 다시 설치하십시오.

추가 정보:

[보고서 템플릿 설치 방법](#) (페이지 493)

제 14 장: 무인 설치

무인 설치 소개

SiteMinder 구성 요소를 설치한 후 무인 설치를 사용하여 해당 구성 요소를 다시 설치할 수 있습니다. 무인 설치를 사용하면 사용자 개입 없이 설치를 완료할 수 있습니다. 무인 설치를 사용하여 다음과 같은 구성 요소를 설치할 수 있습니다.

- 정책 서버
- 관리 UI
- 보고서 서버 하나

무인 설치 지침

각 SiteMinder 구성 요소에는 고유한 속성 파일이 연결되어 있습니다. 다음 지침은 모든 속성 파일에 적용됩니다. 무인 설치를 시작하기 전에 이러한 지침을 검토하십시오.

- 기본 속성 파일을 수정하기 전에 먼저 해당 기본 속성 파일을 백업하십시오.
- 매개 변수 이름, 등호(=) 및 매개 변수 값 사이에 불필요한 공백을 추가하지 마십시오.
- 파일을 변경했으면 저장하십시오.
- 암호화된 암호를 수동으로 편집하지 마십시오. 이러한 암호는 보안상의 이유로 암호화되며 일반 텍스트 형식으로 편집할 수 없습니다. 일반 텍스트 암호를 추가하려면 암호화된 암호 매개 변수를 주석 처리하고 일반 텍스트 참조의 주석 처리를 제거하십시오.

기본 속성 파일

텍스트 편집기를 사용하여 기본 속성 파일의 매개 변수를 수정할 수 있습니다. 기본 매개 변수는 초기 설치 중에 입력된 정보를 반영합니다.

정책 서버 속성 파일

정책 서버 속성 파일의 기본 이름 및 위치는 다음과 같습니다.

이름

`ca-ps-installer.properties`

위치

`policy_server_home\siteminder\install_config_info`

`policy_server_home`

정책 서버 설치 경로를 지정합니다.

관리 UI 속성 파일

관리 UI 를 자동으로 설치하는 데는 속성 파일이 하나만 필요합니다. 필요한 파일은 선택한 설치 옵션에 따라 다릅니다. 사용 가능한 속성 파일의 기본 이름 및 위치는 다음과 같습니다.

- `smwamui-installer.properties`

기존 응용 프로그램 서버 인프라에 설치하려는 경우 이 파일을 사용합니다.

위치

`admin_ui_home\siteminder\adminui\install_config_info`

`admin_ui_home`

관리 UI 설치 경로를 지정합니다.

- `prerequisite-installer.properties`

독립 실행형 설치 옵션을 사용하여 설치하려는 경우 이 파일을 사용합니다.

참고: 이 파일은 이전에 독립 실행형 설치 옵션을 사용하여 관리 UI 를 설치한 경우에만 사용할 수 있습니다.

위치

`admin_ui_home\siteminder\adminui\install_config_info`

`admin_ui_home`

관리 UI 설치 경로를 지정합니다.

보고 기능 속성 파일

SiteMinder 보고 기능을 자동 모드로 설치하려면 보고서 서버에 대한 응답 파일과 SiteMinder 보고서 서버 구성 마법사에 대한 응답 파일이 필요합니다. 이러한 파일의 이름과 기본 위치는 다음과 같습니다.

- cabiresponse.ini

이 파일을 사용하여 보고서 서버를 설치하십시오.

기본 위치: *report_server_home*\CA\SC\CommonReporting3

report_server_home

보고서 서버 설치 경로를 지정합니다.

- reportserver_config_installer.properties

이 파일을 사용하여 SiteMinder 보고 템플릿을 설치하십시오.

기본 위치: *report_server_home*\CommonReporting3\install_config_info

report_server_home

보고서 서버 설치 경로를 지정합니다.

정책 서버 무인 설치 실행 방법

정책 서버 무인 설치를 실행하려면 다음 단계를 수행하십시오.

1. 무인 설치 지침을 검토합니다.
 2. 정책 서버 호스트 시스템에서 정책 서버 속성 파일을 복사합니다.
 3. 다음 단계 중 하나를 완료합니다.
 - 정책 서버를 다시 설치하는 경우 파일을 임시 위치에 복사합니다.
 - 새 시스템에 정책 서버를 설치하는 경우 파일을 해당 시스템의 임시 위치에 복사합니다.
- 참고:** (UNIX) UNIX 사용자에게 이 디렉터리에서 설치할 수 있는 적절한 권한이 있는지 확인하십시오.
4. 정책 서버 설치 미디어를 속성 파일과 동일한 위치에 복사합니다.
 5. 정책 서버 설치 관리자 속성 파일을 수정합니다.
 6. 정책 서버 설치 관리자를 실행합니다.
 7. 정책 서버 설치를 확인합니다.

추가 정보:

[무인 설치 지침](#) (페이지 593)

정책 서버 설치 관리자 속성 파일 수정

정책 서버 설치 관리자 속성 파일을 수정하여 설치 변수를 정의하십시오. 이 파일의 기본 매개 변수, 암호 및 경로는 정책 서버의 초기 설치 중에 입력한 정보를 반영합니다.

중요! 속성 템플릿에는 정책 서버의 **FIPS** 작동 모드를 지정하는 변수인 **CA_SM_PS_FIPS140** 이 포함되어 있습니다. 정책 서버를 다시 설치하는 경우 변수의 값을 수정하지 마십시오. 필요하면 정책 서버를 다시 설치한 후에 **FIPS** 작동 모드를 변경하십시오. 정책 서버의 **FIPS** 작동 모드를 변경하는 방법에 대한 자세한 내용은 *업그레이드 안내서*를 참조하십시오.

일반 정책 서버 정보

"General Information"(일반 정보) 섹션에서는 다음을 설정할 수 있습니다.

DEFAULT_INSTALL_DIR

정책 서버 설치 위치를 지정합니다.

DEFAULT_SHORTCUTS_DIR

SiteMinder 프로그램 아이콘의 위치를 지정합니다.

예: C:\\Documents and Settings\\All Users\\Start 또는 /SiteMinder

참고: 아이콘 기능은 Windows 에서만 작동합니다.

DEFAULT_JRE_ROOT

JRE 설치 위치를 지정합니다.

DEFAULT_BROWSER

(UNIX 만 해당) 브라우저의 설치 위치를 지정합니다.

예: /usr/dt/appconfig/netscape/netscape

DEFAULT_SMPROFILE_CHOICE

(UNIX 만 해당) .profile 파일에 smprofile.ksh 를 추가할지 여부를 지정합니다. 추가하려면 **true** 를 지정하고, 추가하지 않으려면 **false** 를 지정합니다.

DEFAULT_ENCRYPTKEY

정책 서버와 정책 저장소 간에 전송되는 데이터를 보호하기 위한 ClearText 암호화 키를 입력할 수 있습니다.

참고: ENCRYPTED_ENCRYPTKEY 매개 변수를 주석 처리하고 DEFAULT_ENCRYPTKEY의 주석 처리를 제거하면 무인 설치 관리자는 DEFAULT_ENCRYPTKEY의 ClearText 암호화 키 값을 사용합니다. 정책 서버의 초기 설치 후 DEFAULT_ENCRYPTKEY 매개 변수는 기본적으로 주석 처리되어 있습니다.

ENCRYPTED_ENCRYPTKEY

정책 서버와 정책 저장소 간에 전송되는 데이터를 보호하기 위한 암호화된 암호화 키를 보여 줍니다. 이 키는 정책 서버의 초기 설치 중에 입력한 것으로, 변경할 수 없습니다.

중요! 이 암호화된 값을 변경하면 무인 설치를 실행할 때 정책 서버와 정책 저장소가 통신할 수 없게 되므로 값을 수정하지 마십시오.

DEFAULT_ENCRYPTKEY 매개 변수를 주석 처리하고 ENCRYPTED_ENCRYPTKEY의 주석 처리를 제거하면 무인 설치 관리자는 ENCRYPTED_ENCRYPTKEY의 암호화된 암호화 키 값을 사용합니다.

CA_SM_PS_FIPS140

정책 서버의 FIPS 작동 모드를 지정합니다.

값: COMPAT, MIGRATE 또는 ONLY

중요! 정책 서버를 다시 설치하려는 경우에는 이 값을 수정하지 마십시오.

정책 서버 기능

"Feature Selection"(기능 선택) 섹션에서는 다음 매개 변수를 설정할 수 있습니다.

DEFAULT_OVMGUI_CHOICE

정책 서버 설치 관리자가 선택된 웹 서버에서 OneView 모니터 GUI 를 구성하는지 여부를 결정합니다.

유효한 값: true 및 false

true

설치 관리자가 OneView 모니터 GUI 를 구성합니다.

이 값을 true 로 설정하려면 OneView 모니터 GUI 및 "웹 서버" 아래에서 추가 설정을 구성해야 합니다.

false

설치 관리자가 OneView 모니터 GUI 를 구성하지 않습니다.

DEFAULT_WEBSERVERS_CHOICE

정책 서버 설치 관리자가 지정된 웹 서버에서 FSS(Federation Security Services) UI 를 구성하는지 여부를 결정합니다.

유효한 값: true 및 false

true

설치 관리자가 지정된 웹 서버에서 구성 요소를 구성합니다.

이 값을 true 로 설정하려면 "웹 서버" 아래에서 추가 설정을 구성해야 합니다.

false

설치 관리자가 웹 서버에서 구성 요소를 구성하지 않습니다.

DEFAULT_SNMP_CHOICE

정책 서버 설치 관리자가 정책 서버에서 SiteMinder SNMP 지원을 구성할지 여부를 결정합니다.

유효한 값: true 및 false

true

설치 관리자가 SiteMinder SNMP 지원을 구성합니다.

이 값을 true 로 설정하려면 SNMP 아래에서 추가 설정을 구성해야 합니다.

false

설치 관리자가 SiteMinder SNMP 지원을 구성하지 않습니다.

DEFAULT_POLICYSTORE_CHOICE

정책 서버 설치 관리자가 정책 저장소를 자동으로 구성할지 여부를 결정합니다.

유효한 값: true 및 false

true

설치 관리자가 정책 저장소를 구성합니다.

이 값을 true 로 설정하려면 "정책 저장소" 아래에서 추가 설정을 구성해야 합니다.

false

설치 관리자가 정책 저장소를 구성하지 않습니다.

OneView 모니터 GUI

DEFAULT_OVMGUI_CHOICE 매개 변수를 true 로 설정한 경우 다음을 설정하십시오.

DEFAULT_JDK_ROOT

JDK 설치 위치를 지정합니다.

DEFAULT_SERVLETEXEC_INSTANCE_NAME

(UNIX 만 해당) ServletExec 인스턴스의 이름을 지정합니다.

예: se-testmachine-60psGUI

DEFAULT_SERVLETEXEC_ROOT

ServletExec 설치 위치를 지정합니다.

예: C:\\Program Files\\New Atlanta\\ServletExec ISAPI 또는
/export/NewAtlanta/ServletExecAS

DEFAULT_SERVLETEXEC_PORT

(UNIX 만 해당) ServletExec 인스턴스의 포트 번호를 지정합니다.

예: 7676

SNMP

SNMP 암호를 수정하려면 다음 작업을 수행하십시오.

DEFAULT_ROOT_PW

UNIX 시스템의 루트 사용자에게 ClearText SNMP 암호를 입력할 수 있습니다. ENCRYPTED_ROOT_PW 매개 변수를 주석 처리하고 DEFAULT_ROOT_PW 의 주석 처리를 제거하면 무인 설치 관리자는 DEFAULT_ROOT_PW 의 일반 텍스트 SNMP 암호를 사용합니다.

기본값: 정책 서버의 초기 설치 후 DEFAULT_ROOT_PW 매개 변수는 주석 처리되어 있습니다.

ENCRYPTED_ROOT_PW

UNIX 시스템의 루트 사용자에게 암호화된 SNMP 암호를 보여 줍니다. 이 암호는 UNIX 정책 서버의 초기 설치 중에 입력한 것으로, 변경할 수 없습니다.

중요! 이 암호화된 암호를 변경하면 정책 서버와 정책 저장소가 통신할 수 없게 되므로 값을 수정하지 마십시오. DEFAULT_ROOT_PW 매개 변수를 주석 처리하고 ENCRYPTED_ROOT_PW 의 주석 처리를 제거하면 무인 설치 관리자는 ENCRYPTED_ROOT_PW 의 암호화된 암호를 사용합니다.

정책 저장소

DEFAULT_POLICystore_CHOICE 매개 변수를 true 로 설정한 경우에는 다음 매개 변수를 설정하십시오.

DEFAULT_POLICystore_TYPE

정책 저장소의 역할을 할 저장소의 유형을 지정합니다.

유효한 값: LDAP 및 RDB

LDAP

LDAP 정책 저장소를 지정합니다.

RDB

ODBC 정책 저장소를 지정합니다.

DEFAULT_POLICystore_IP

(LDAP) LDAP 디렉터리 서버 호스트 시스템의 IP 주소 또는 이름을 지정합니다.

예: 172.16.0.0

DEFAULT_POLICystore_PORT

(LDAP) LDAP 디렉터리 서버가 수신하는 포트를 지정합니다.

예: 1356.

DEFAULT_POLICystore_ADMINDN

(LDAP) 다음 권한을 가진 관리자의 LDAP 사용자 이름을 지정합니다.

- 스키마 만들기
- 정책 저장소 루트 개체 아래의 LDAP 트리에서 개체 생성, 읽기, 수정 및 삭제

예: cn=Directory Manager.

DEFAULT_POLICystore_ADMINPW

(LDAP) LDAP 디렉터리 서버의 관리자에 대한 ClearText 암호를 입력할 수 있게 합니다.

ENCRYPTED_POLICystore_ADMINPW 를 주석 처리하고
DEFAULT_POLICystore_ADMINPW 의 주석 처리를 제거하면 자동 설치
관리자가 DEFAULT_POLICystore_ADMINPW 의 ClearText 암호를
사용합니다.

기본값: DEFAULT_POLICystore_ADMINPW 매개 변수는 정책 서버를
처음 설치한 후에 주석 처리됩니다.

ENCRYPTED_POLICystore_ADMINPW

(LDAP) LDAP 디렉터리 서버의 관리자에 대한 암호화된 암호를
나타냅니다. 이 암호는 정책 서버 설치 관리자가 마지막으로 정책
저장소를 관리할 때 입력한 암호입니다. 기존의 암호화된 값을 사용하여
새 정책 저장소에 대한 LDAP 관리자 암호를 제공할 수 있습니다. 이
암호는 변경할 수 없습니다.

중요! 이 암호를 수정하지 마십시오. 이 암호는 암호화되어 있습니다.

DEFAULT_POLICystore_ADMINPW 를 주석 처리하고
ENCRYPTED_POLICystore_ADMINPW 의 주석 처리를 제거하면 설치
관리자가 ENCRYPTED_POLICystore_ADMINPW 의 암호화된 암호를
사용합니다.

DEFAULT_POLICystore_ROOTDN

(LDAP) LDAP 디렉터리 서버의 루트 DN 을 사용합니다.

예: o=example.com.

DEFAULT_POLICystore_USER_CHOICE

(LDAP) DEFAULT_POLICystore_ADMINDN 매개 변수를 사용하려면 스키마를 생성하는 권한을 가진 LDAP 관리자 사용자 이름이 필요합니다. 기본적으로 정책 서버는 이 계정을 사용하여 정책 저장소를 관리합니다. 정책 저장소를 구성한 후에는 대체 LDAP 사용자 계정이 데이터 저장소의 SiteMinder 데이터를 관리할 수 있습니다. 대체 계정에는 개체를 생성하고, 읽고, 수정하고, 삭제할 수 있는 권한이 있어야 합니다.

유효한 값: true 및 false

true

정책 저장소가 구성된 후에 대체 LDAP 사용자 계정이 정책 저장소를 관리하도록 지정합니다.

false

정책 저장소가 구성된 후에 DEFAULT_POLICystore_ADMINDN 매개 변수로 지정된 LDAP 관리자 사용자 계정이 정책 저장소를 관리하도록 지정합니다.

DEFAULT_POLICystore_USERDN

(LDAP) 대체 LDAP 사용자 계정의 DN 을 지정합니다.

예:

uid=SMAdmin,ou=people,o=security.com.

DEFAULT_POLICystore_USERPW

(LDAP) 대체 LDAP 사용자의 ClearText 암호를 입력할 수 있게 합니다. ENCRYPTED_POLICystore_USERPW 를 주식 처리하고 DEFAULT_POLICystore_USERPW 의 주식 처리를 제거하면 자동 설치 관리자가 DEFAULT_POLICystore_USERPW 의 ClearText 암호를 사용합니다.

기본값: DEFAULT_POLICystore_USERPW 매개 변수는 정책 서버를 처음 설치한 후에 주식 처리됩니다.

ENCRYPTED_POLICYSTORE_USERPW

(LDAP) 대체 LDAP 사용자의 암호화된 암호를 나타냅니다. 이 암호는 정책 서버 설치 관리자가 마지막으로 정책 저장소를 관리할 때 입력한 암호입니다. 기존의 암호화된 값을 사용하여 새 정책 저장소에 대한 대체 관리자 암호를 설정할 수 있습니다. 이 암호는 변경할 수 없습니다.

중요! 이 암호를 수정하지 마십시오. 이 암호는 암호화되어 있습니다.

DEFAULT_POLICYSTORE_USERPW 를 주석 처리하고 ENCRYPTED_POLICYSTORE_USERPW 의 주석 처리를 제거하면 설치 관리자가 ENCRYPTED_POLICYSTORE_USERPW 의 암호화된 암호를 사용합니다.

DEFAULT_INIT_POLICYSTORE_CHOICE

(LDAP/RDB) 정책 서버 설치 관리자가 정책 저장소를 초기화해야 하는지 여부를 지정합니다.

유효한 값: true 및 false

true

설치 관리자가 정책 저장소를 초기화합니다.

false

설치 관리자가 정책 저장소를 초기화하지 않습니다.

DEFAULT_SM_ADMINPW

(LDAP/RDB) SiteMinder 슈퍼 사용자 계정의 ClearText 암호를 입력할 수 있게 합니다.

ENCRYPTED_SM_ADMINPW 를 주석 처리하고 DEFAULT_SM_ADMINPW 의 주석 처리를 제거하면 설치 관리자가 DEFAULT_SM_ADMINPW 의 ClearText 암호를 사용합니다.

기본값: DEFAULT_SM_ADMINPW 매개 변수는 정책 서버를 처음 설치한 후에 주석 처리됩니다.

ENCRYPTED_SM_ADMINPW

(LDAP/RDB) SiteMinder 슈퍼 사용자 계정의 암호화된 암호를 나타냅니다. 이 암호는 정책 서버 설치 관리자가 마지막으로 정책 저장소를 관리할 때 입력한 암호입니다. 기존의 암호화된 값을 사용하여 새 정책 저장소에 대한 SiteMinder 슈퍼 사용자 암호를 설정할 수 있습니다. 이 암호는 변경할 수 없습니다.

중요! 이 암호를 수정하지 마십시오. 이 암호는 암호화되어 있습니다.

DEFAULT_SM_ADMINPW 를 주석 처리하고 ENCRYPTED_SM_ADMINPW 의 주석 처리를 제거하면 설치 관리자가 ENCRYPTED_SM_ADMINPW 의 암호화된 암호를 사용합니다.

DEFAULT_RDB_DSN

(RDB) 정책 서버 설치 관리자가 생성하는 DSN 의 이름을 지정합니다.

DEFAULT_RDB_DBSERVER

(RDB) 데이터베이스 호스트 시스템의 IP 주소 또는 이름을 지정합니다.

DEFAULT_RDB_DBNAME

(RDB) 다음 값 중 하나를 지정합니다.

- (SQL Server) 정책 저장소의 역할을 할 명명된 인스턴스 또는 데이터베이스 이름
- (PostgreSQL) 정책 저장소의 역할을 할 PostgreSQL 명명된 인스턴스 또는 데이터베이스 이름
- (Oracle) 정책 저장소의 역할을 할 Oracle 데이터베이스의 서비스 이름

DEFAULT_RDB_PORT

(RDB) 데이터베이스가 수신하는 포트를 지정합니다.

DEFAULT_RDB_USER_NAME

(RDB) 다음 권한을 가진 데이터베이스 관리자 계정의 이름을 지정합니다.

- 스키마 만들기
- 개체 생성, 읽기, 수정 및 삭제

DEFAULT_RDB_DBTYPE

정책 저장소의 역할을 할 데이터베이스의 유형을 지정합니다.

유효한 값: DB_MSSQL, DB_ORACLE, and DB_POSTGRE.

DB_MSSQL

SQL Server 정책 저장소를 지정합니다.

DB_ORACLE

Oracle 정책 저장소를 지정합니다.

DB_POSTGRE

PostgreSQL 정책 저장소를 지정합니다.

DEFAULT_RDB_PASSWORD

(RDB) 데이터베이스 관리자의 ClearText 암호를 입력할 수 있게 합니다.

기본값: 이 매개 변수는 정책 서버를 처음 설치한 후에 주석 처리됩니다.

ENCRYPTED_RDB_PASSWORD 를 주석 처리하고

DEFAULT_RDB_PASSWORD 의 주석 처리를 제거하면 설치 관리자가

DEFAULT_RDB_PASSWORD 의 ClearText 암호를 사용합니다.

ENCRYPTED_RDB_PASSWORD

(RDB) 설치 관리자가 정책 저장소를 마지막으로 구성할 때 입력된 데이터베이스 관리자 암호의 암호화된 값을 나타냅니다.

기본값: 이 매개 변수의 주석 처리가 제거됩니다. 이 매개 변수를 주석 처리하고 DEFAULT_RDB_PASSWORD 의 주석 처리를 제거한 경우 외에는 설치 관리자가 이 값을 사용합니다.

DEFAULT_KEYSTORE_CONFIG

설치 관리자가 SiteMinder 키 저장소를 정책 저장소와 같은 곳에 배치해야 하는지 여부를 지정합니다.

유효한 값: true 및 false

true

설치 관리자가 키 저장소를 정책 저장소와 같은 곳에 배치합니다.

false

설치 관리자가 키 저장소를 구성하지 않습니다. 사용자가 정책 저장소를 구성한 후 독립 실행형 키 저장소를 구성합니다.

DEFAULT_SMKEYDB_IMPORT_CHOICE

기본 CA 인증서를 인증서 데이터 저장소로 가져와야 하는지 여부를 지정합니다.

유효한 값: true 및 false

true

기본 CA 인증서를 가져옵니다.

false

기본 CA 인증서를 가져오지 않습니다.

DeviceDNA™를 사용한 고급 세션 보증 설정

다음 항목은 DeviceDNA™를 사용한 고급 세션 보증에 적용됩니다.

MASTER_KEY=

CA SiteMinder for Secure Proxy Server 에서 실행되는 고급 인증 서버에 대한 마스터 암호화 키를 지정합니다. 마스터 암호화 키를 일반 텍스트 형식으로 저장합니다.

ENCRYPTED_MASTER_KEY=

CA SiteMinder for Secure Proxy Server 에서 실행되는 고급 인증 서버에 대한 마스터 암호화 키를 지정합니다. 마스터 암호화 키를 암호화된 형식으로 저장합니다.

IS_SA_ENABLED=true

DeviceDNA™를 사용한 고급 세션 보증이 사용되도록 설정되었는지 여부를 나타냅니다. 이 항목을 편집하지 *마십시오*.

정책 서버 설치 관리자 실행

무인 설치를 실행하여 사용자 개입 없이 정책 서버를 설치할 수 있습니다.

설치하기 전에

기술 지원 사이트의 설치 미디어를 사용하여 정책 서버를 설치하십시오.

참고: 설치 미디어 이름의 목록에 대해서는 *정책 서버 릴리스 정보*를 참조하십시오.

Windows

정책 서버 무인 설치를 실행하려면 정책 서버 설치 실행 파일 및 속성 파일을 복사한 디렉터리에서 다음 명령을 실행하십시오.

```
installation_media -f ca-ps-installer.properties -i silent
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

installation_media

정책 서버 설치 실행 파일을 지정합니다.

참고: 속성 파일이 설치 미디어와 동일한 디렉터리에 있지 않은 경우 해당 위치를 지정하십시오. 인수에 공백이 포함된 경우 큰따옴표로 묶으십시오.

-i silent

설치 관리자가 자동 모드로 실행되도록 지정합니다.

예:

```
installation_media -f "C:\Program  
Files\CA\siteminder\install_config_info\ca-ps-installer.properties  
" -i silent
```

설치가 시작됩니다. 설치 관리자는 사용자가 속성 파일에 지정한 매개 변수를 사용하여 정책 서버를 설치합니다.

UNIX

다음 단계를 수행하십시오.

1. 셸을 엽니다.
2. 정책 서버 설치 실행 파일 및 정책 서버 설치 속성 파일을 복사한 디렉터리에서 다음 명령을 실행합니다.

```
./installation_media -f ca-ps-installer.properties -i silent
```

installation_media

정책 서버 설치 실행 파일을 지정합니다.

-i silent

설치 관리자가 자동 모드로 실행되도록 지정합니다.

설치가 시작됩니다. 설치 관리자는 사용자가 속성 파일에 지정한 매개 변수를 사용하여 정책 서버를 설치합니다.

정책 서버 설치 문제 해결

다음 파일을 사용하여 정책 서버 설치 문제를 해결하십시오.

- CA_SiteMinder_Policy_Server_release_InstallLog.log

이 설치 로그에는 설치 중에 발생한 오류, 심각하지 않은 오류, 경고, 성공의 수를 보여 주는 요약 섹션이 포함됩니다. 개별 설치 작업이 해당 상태와 함께 표시됩니다.

release

정책 서버 릴리스를 지정합니다.

위치: *siteminder_home*\siteminder\install_config_info

- ca-ps-details.log

정책 저장소 로그는 정책 저장소 상태 정보를 제공합니다.

위치: *siteminder_home*\siteminder\install_config_info

- smps.log

정책 서버를 시작하면 *smps.log* 가 생성됩니다. 정책 서버가 성공적으로 설치되었을 경우 이 로그에는 다음과 같은 줄이 포함됩니다.

[Info] Journaling thread started, will delete commands older than 60 minutes.

위치: *siteminder_home*\siteminder\log

siteminder_home

정책 서버 설치 경로를 지정합니다.

무인 정책 서버 설치 중지

정책 서버가 지정한 Windows 시스템에서 설치되지 않도록 하려면 무인 정책 서버 설치를 중지하십시오.

설치를 중지하려면

- **Windows**

Windows 작업 관리자를 사용하여 다음 프로세스를 중지하십시오.

ca-ps-12.5-win32.exe
ps_install.exe

- **UNIX**

Ctrl+C 를 누르십시오.

관리 UI 무인 설치 실행 방법

관리 UI 무인 설치를 실행하려면 다음 단계를 수행하십시오.

1. 다음을 수행합니다.

- 필수 구성 요소 설치 관리자를 사용하는 경우 [설치 검사 목록](#) (페이지 443)을 검토합니다.
- 기존 응용 프로그램 서버 인프라에 설치하는 경우 [설치 검사 목록](#) (페이지 545)을 검토합니다.

2. 자동 설치에 대한 지침을 검토합니다.

3. 사용할 속성 파일을 결정합니다.

참고: 관리 UI 설치 옵션에 따라 사용할 속성 파일이 결정됩니다.

4. 관리 UI 호스트 시스템에서 다음 단계를 수행하십시오.
 - a. 속성 파일을 복사합니다. 다음을 수행합니다.
 - 관리 UI 를 다시 설치하는 경우 이 파일을 임시 위치에 복사합니다.
 - 새 시스템에 관리 UI 를 설치하는 경우 이 파일을 해당 시스템의 임시 위치에 복사합니다.
 - b. 필수 구성 요소 설치 관리자를 사용하는 경우
`admin_ui_home\SiteMinder\adminui` 로 이동하여 JBoss 사용권 계약(JBoss-ORG-ULA.txt)을 검토합니다. 필수 구성 요소 설치 관리자 속성 파일에는 LGPL(Lesser General Public License) 매개 변수가 포함되어 있습니다. 이 매개 변수를 업데이트하여 JBoss 사용권 계약을 검토하고 이에 동의했음을 확인합니다.
5. 설치 미디어를 속성 파일을 복사한 위치와 동일한 위치에 복사합니다.
참고: 관리 UI 설치 옵션에 따라 사용할 실행 파일이 결정됩니다.
6. 속성 파일을 수정합니다.
7. 관리 UI 설치 관리자를 실행합니다.
8. 정책 서버에 관리 UI 를 등록합니다.

필수 구성 요소 설치 관리자 속성 파일 수정

독립 실행형 옵션을 사용하여 관리 UI 를 설치하려면 필수 구성 요소 설치 관리자 속성 파일을 수정하여 설치 변수를 정의하십시오. 기본값은 관리 UI 의 최근 설치 중에 입력된 정보를 반영합니다.

General Information(일반 정보)

이 섹션에서는 관리 UI 설치 루트 폴더를 지정할 수 있습니다.

DEFAULT_INSTALL_FOLDER

루트 폴더를 지정합니다. 설치 중 모든 하위 폴더가 이 폴더 아래에 생성됩니다.

Server Information(서버 정보)

이 섹션에서는 JBoss 와 관리 UI 호스트 시스템에 대한 정보를 지정할 수 있습니다. 이 섹션에는 다음 매개 변수가 포함되어 있습니다.

DEFAULT_APP_SERVER_PORT

JBoss 가 HTTP 요청을 수신 대기해야 하는 포트를 지정합니다.

DEFAULT_APP_SERVER_HOST

관리 UI 호스트 시스템의 정규화된 이름을 지정합니다.

End User Licensing Agreement(최종 사용자 사용권 계약)

필수 구성 요소 설치 관리자는 JBoss 를 설치하며, 이때 LGPL(Lesser General Public License)에 동의해야 합니다. 이 섹션에서는 사용권 계약을 검토했으며 이에 동의하는 것으로 지정할 수 있습니다.

사용권 계약에 동의하려면

1. 먼저 JBoss 사용권 계약(JBossORG-EULA.txt)을 검토합니다.

사용권 계약 파일은 관리 UI 호스트 시스템의 다음 위치에 있습니다.

`admin_ui_home\iteminder\adminui`

`admin_ui_home`

관리 UI 설치 경로를 지정합니다.

2. 사용권 계약에 동의하면 ACCEPT_LGPL_EULA 의 값을 다음으로 변경합니다.

YES

사용권 계약을 검토했으며 이에 동의함을 지정합니다.

관리 UI 설치 관리자 속성 파일 수정

관리 UI 를 기존 응용 프로그램 서버 인프라에 설치하려면 관리 UI 설치 관리자 속성 파일을 수정하여 설치 변수를 정의하십시오. 이 파일의 기본값은 관리 UI 의 최근 설치 중에 입력된 정보를 반영합니다.

General Information(일반 정보)

이 섹션에서는 관리 UI 설치 루트 폴더를 지정할 수 있습니다.

DEFAULT_INSTALL_FOLDER

루트 폴더를 지정합니다. 설치 중 모든 하위 폴더가 이 폴더 아래에 생성됩니다.

Application Server Information(응용 프로그램 서버 정보)

이 섹션에서는 관리 UI 를 배포할 대상 응용 프로그램 서버에 대한 정보를 지정할 수 있습니다. 이 섹션에는 다음 매개 변수가 포함되어 있습니다.

DEFAULT_APP_SERVER

응용 프로그램 서버 유형을 지정합니다. 이 매개 변수에는 다음 설정이 사용됩니다.

JBoss

응용 프로그램 서버 유형을 JBoss 로 지정합니다.

WebLogic9

응용 프로그램 서버 유형을 WebLogic 로 지정합니다.

WebSphere6

응용 프로그램 서버 유형을 WebSphere 로 지정합니다.

DEFAULT_NETE_JAVA_HOME

응용 프로그램 서버에 필요한 JDK 또는 JRE 의 경로를 지정합니다. 이 값은 응용 프로그램 서버의 유형에 따라 달라집니다.

JBoss

필요한 최소 JDK 버전의 경로를 지정합니다.

WebLogic

필요한 최소 JDK 또는 JRE 버전의 경로를 지정합니다.

WebSphere

필요한 최소 JDK 또는 JRE 버전의 경로를 지정합니다.

DEFAULT_APP_SERVER_URL

응용 프로그램 서버가 설치된 시스템의 정규화된 URL 을 지정합니다.

JBoss Information(JBoss 정보)

이 섹션에서는 JBoss 에 대한 추가 정보를 지정할 수 있습니다.

참고: DEFAULT_APP_SERVER 의 값으로 JBoss 를 입력하지 않은 경우에는 이 섹션에서 값을 입력할 필요가 없습니다.

이 섹션에는 다음 매개 변수가 있습니다.

DEFAULT_JBOSS_FOLDER

JBoss 설치 디렉터리의 경로를 지정합니다.

참고: 경로에 공백을 포함하면 안 됩니다.

WebLogic Information(WebLogic 정보)

이 섹션에서는 WebLogic 에 대한 추가 정보를 지정할 수 있습니다.

참고: DEFAULT_APP_SERVER 의 값으로 WebLogic9 을 입력하지 않은 경우에는 이 섹션에서 값을 입력할 필요가 없습니다.

이 섹션에는 다음 매개 변수가 있습니다.

DEFAULT_BINARY_FOLDER

WebLogic 설치 디렉터리의 경로를 지정합니다.

DEFAULT_DOMAIN_FOLDER

관리 UI 에 대해 생성한 WebLogic 도메인의 경로를 지정합니다.

DEFAULT_SERVER_NAME

WebLogic 도메인이 구성된 WebLogic 서버의 이름을 지정합니다.

WebSphere Information(WebSphere 정보)

이 섹션에서는 WebSphere 에 대한 추가 정보를 지정할 수 있습니다.

참고: DEFAULT_APP_SERVER 의 값으로 WebSphere6 을 입력하지 않은 경우에는 이 섹션에서 값을 입력할 필요가 없습니다.

이 섹션에는 다음 매개 변수가 있습니다.

DEFAULT_WEBSphere_FOLDER

WebSphere 설치 디렉터리의 경로를 지정합니다.

DEFAULT_WAS_NODE

응용 프로그램 서버가 있는 노드의 이름을 지정합니다.

DEFAULT_WAS_SERVER

응용 프로그램 서버의 이름을 지정합니다.

DEFAULT_WAS_CELL

응용 프로그램 서버가 있는 셀의 이름을 지정합니다.

WAS_PROFILE

관리 UI 에 사용되는 프로파일의 이름을 지정합니다.

관리 UI 설치 관리자 실행

무인 설치를 실행하여 사용자 개입 없이 관리 UI 를 설치할 수 있습니다.

설치하기 전에

관리 UI 를 설치하기 전에 다음 사항을 고려하십시오.

- 기술 지원 사이트의 설치 미디어를 사용하여 관리 UI 를 설치합니다.
참고: 설치 미디어 이름의 목록에 대해서는 *정책 서버 릴리스* 정보를 참조하십시오.
- **중요!** 설치 zip 파일에는 설치 미디어와 같은 수준에서 layout.properties 파일과 Framework 폴더가 포함되어 있습니다. 설치 zip 파일의 압축을 풀 후 설치 미디어를 이동한 경우 다음을 동일한 위치로 이동해야 합니다. 그렇지 않으면 설치가 실패합니다.
 - layout.properties 파일
 - Framework 폴더

- 설치 zip 파일에는 필수 구성 요소 설치 관리자와 관리 UI 설치 관리자가 포함되어 있습니다.
필수 구성 요소 설치 관리자를 사용하여 관리 UI 를 설치하는 경우 두 실행 파일을 모두 동일한 위치에 넣습니다. 필수 구성 요소 설치 관리자가 관리 UI 설치 관리자를 자동으로 호출하여 설치를 완료합니다.

Windows

관리 UI 무인 설치를 실행하려면 관리 UI 설치 미디어 및 속성 파일을 복사한 디렉터리에서 다음 명령을 실행하십시오.

```
installation_media -f properties_file -i silent
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

installation_media

관리 UI 설치 실행 파일의 이름을 지정합니다. 관리 UI 설치 옵션에 따라 사용할 실행 파일이 결정됩니다.

-f properties_file

속성 파일의 경로를 지정합니다. 경로에 속성 파일 이름이 포함되어야 합니다. 관리 UI 설치 옵션에 따라 사용할 속성 파일이 결정됩니다.

참고: 인수에 공백이 포함된 경우 큰따옴표로 묶으십시오.

-i silent

설치 관리자가 자동 모드로 실행되도록 지정합니다.

예:

```
installation_media -f "C:\Program  
Files\CA\SiteMinder\adminui\install_config_info\properties_file" -i silent
```

설치 관리자는 속성 파일의 매개 변수를 사용하여 관리 UI 를 설치합니다.

정책 서버에 관리 UI 를 등록하여 설치를 완료하십시오.

- 독립 실행형 옵션을 사용하여 관리 UI 를 설치한 경우 [관리 UI 등록 방법](#) (페이지 453)을 참조하십시오.
- 기존 응용 프로그램 서버 인프라에 관리 UI 를 설치한 경우 [관리 UI 등록 방법](#) (페이지 553)을 참조하십시오.

UNIX

다음 단계를 수행하십시오.

1. 셸을 엽니다.
2. 관리 UI 설치 미디어 및 속성 파일을 복사한 디렉터리에서 다음 명령을 실행합니다.

```
./installation_media -f properties_file -i silent
```

installation_media

관리 UI 설치 실행 파일의 이름을 지정합니다. 관리 UI 설치 옵션에 따라 사용할 실행 파일이 결정됩니다.

-f properties_file

속성 파일의 경로를 지정합니다. 경로에 속성 파일 이름이 포함되어야 합니다. 관리 UI 설치 옵션에 따라 사용할 속성 파일이 결정됩니다.

-i silent

설치 관리자가 자동 모드로 실행되도록 지정합니다.

설치 관리자는 속성 파일의 매개 변수를 사용하여 관리 UI 를 설치합니다.

3. 정책 서버에 관리 UI 를 등록하여 설치를 완료합니다.
 - 독립 실행형 옵션을 사용하여 관리 UI 를 설치한 경우 [관리 UI 등록 방법](#) (페이지 453)을 참조하십시오.
 - 기존 응용 프로그램 서버 인프라에 관리 UI 를 설치한 경우 [관리 UI 등록 방법](#) (페이지 553)을 참조하십시오.

보고서 서버 무인 설치 실행 방법

관리 UI 무인 설치를 실행하려면 다음 단계를 수행하십시오.

1. [설치 검사 목록](#) (페이지 470)을 검토합니다.
2. 설치 관리자에 필요한 정보를 수집합니다.
3. 자동 설치에 대한 지침을 검토합니다.
4. 보고서 서버 응답 파일과 SiteMinder 보고서 서버 구성 마법사 속성 파일을 찾습니다.

5. 응답 파일과 속성 파일을 보고서 서버 호스트 시스템의 임시 위치에 복사합니다.
6. 보고서 서버 및 SiteMinder 보고서 서버 구성 마법사 설치 미디어를 보고서 서버 호스트 시스템의 임시 위치에 복사합니다.
참고: 기술 지원 사이트에서 설치 미디어를 다운로드할 수 있습니다.
7. 보고서 서버 응답 파일을 수정합니다.
8. SiteMinder 보고서 서버 구성 마법사 속성 파일을 수정합니다.
9. 보고서 서버 설치 관리자를 실행합니다.
10. SiteMinder 보고서 서버 구성 마법사를 실행합니다.
11. 보고서 서버를 등록합니다.

Windows 의 보고서 서버 응답 파일 수정

설치 관리자 응답 파일을 수정하여 설치 변수를 정의합니다. 기본값은 보고서 서버를 설치하고 응답 파일을 저장할 때 입력한 정보를 반영합니다.

중요! 파일을 수정하기 전에 다음 사항을 확인하십시오.

- 일부 매개 변수는 보고서(cms) 데이터베이스 기능을 수행할 데이터베이스 유형을 식별합니다. 설치 관리자가 구성하게 될 데이터베이스의 유형을 속성 파일을 사용해서 변경하지 마십시오. 보고서 데이터베이스 유형을 변경하려면 설치 관리자를 사용하여 또 다른 속성 파일을 만드십시오.
- 명령줄에서 매개 변수를 전달하면 응답 파일의 해당 설정이 재정의됩니다.
- 설치 관리자는 일부 매개 변수를 자동으로 생성합니다. 다음 매개 변수를 수정하지 마십시오.
 - DATABASECONNECT
 - DATACONNECTION
 - DATABASE_AUDIT_CONNSVR
 - INSTALLDBTYPE
 - INSTALL_DB_TYPE
 - INSTALLLEVEL
 - INSTALLSWITCH

- NEWCMSPASSWORD
- PRIVILEGED
- SINGLESERVER
- SKIP_DEPLOYMENT
- WCADOTNETINSTALL
- WCAJAVAINSTALL
- WCATOMCATINSTALL
- WDEPLOY_LANGUAGES
- WDEPLOY_LATER
- WEBSITE_METABASE_NUMBER
- WEBSITE_PORT
- ADDSOURCE
- ADVERTISE

Install

이 단원에서는 응답 파일의 **Install** 섹션에 있는 매개 변수에 대해 자세히 설명합니다.

AS_ADMIN_IS_SECURE

웹 응용 프로그램 서버에 액세스하려면 관리자 자격 증명을 전달해야 하도록 지정합니다.

SiteMinder 설정: 값을 빈 상태로 둡니다. 이 매개 변수는 SiteMinder 가 지원하지 않는 웹 응용 프로그램 서버에 적용됩니다.

AS_ADMIN_PASSWORD

웹 응용 프로그램 서버에 액세스하는 관리자 계정의 암호를 지정합니다. 포함된 Apache Tomcat 버전을 설치한 경우 이 매개 변수 값이 비어 있습니다. SiteMinder 는 포함된 Apache Tomcat 버전만 지원합니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

AS_ADMIN_PORT

웹 응용 프로그램 서버가 수신 대기하는 포트를 지정합니다. 포함된 Apache Tomcat 버전을 설치한 경우 기본값은 8080 입니다. SiteMinder 는 포함된 Apache Tomcat 버전만 지원합니다.

SiteMinder 설정: 8080

이 값이 TOMCAT_CONNECTION_PORT 의 값과 일치하는지 확인하십시오.

AS_ADMIN_USERNAME

웹 응용 프로그램 서버에 액세스하는 데 사용되는 관리자 계정의 계정 이름을 지정합니다. 포함된 Apache Tomcat 버전을 설치한 경우 기본값은 다음과 같은 값입니다.

admin

SiteMinder 는 포함된 Apache Tomcat 버전만 지원합니다.

SiteMinder 설정: admin

AS_DIR

포함된 Apache Tomcat 버전이 설치되어 있는 경로를 지정합니다. 이 경로는 설치 디렉터리를 사용하여 자동으로 설정됩니다.

참고: 백슬래시 문자를 사용하여 경로에서 백슬래시를 이스케이프 처리했는지 확인하십시오.

예: "C:\\Program Files\\CA\\SC\\CommonReporting3\\Tomcat55"

AS_INSTANCE

웹 응용 프로그램 서버 인스턴스의 이름을 지정합니다. 포함된 Apache Tomcat 버전을 설치한 경우 기본값은 localhost 입니다. SiteMinder 는 포함된 Apache Tomcat 버전만 지원합니다.

SiteMinder 설정: localhost

AS_SERVER

배포할 Java 웹 응용 프로그램 서버의 유형을 지정합니다. 포함된 Apache Tomcat 버전을 설치한 경우 기본값은 tomcat55 입니다. SiteMinder 는 포함된 Apache Tomcat 버전만 지원합니다.

SiteMinder 설정: tomcat55

AS_SERVICE_NAME

웹 응용 프로그램 서버를 Windows 의 서비스로 설치한 경우 서비스 이름을 지정합니다. 포함된 Apache Tomcat 버전을 설치한 경우 기본값은 다음과 같은 값입니다.

BOE120Tomcat

SiteMinder 는 포함된 Apache Tomcat 버전만 지원합니다.

SiteMinder 설정: BOE120Tomcat

AS_VIRTUAL_HOST

가상 환경에 보고서 서버를 배포하는 경우 응용 프로그램이 바인딩되어야 하는 가상 호스트를 지정합니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

AUDITINGALLOWED

Microsoft SQL Server 또는 Oracle 보고서 데이터베이스를 구성하는 경우 콘텐츠 관리 서버 감사 데이터베이스 구성 요소를 구성할 수 있는지 여부를 지정합니다.

0

감사가 허용됨을 나타냅니다.

1

감사가 허용되지 않음을 나타냅니다.

SiteMinder 설정: 0

AUDITINGENABLED

Microsoft SQL Server 또는 Oracle 보고서 데이터베이스를 구성하는 경우 콘텐츠 관리 서버 감사 데이터베이스가 사용되도록 설정할지 여부를 지정합니다. 이 매개 변수는 SiteMinder 감사 기반 보고서와 관련이 없습니다.

콘텐츠 관리 서버 감사 데이터베이스는 보고서 서버와 관련된 감사 활동에 사용되며 **SiteMinder**에는 사용되지 않습니다. 감사 기반 보고서를 실행하려면 **SiteMinder** 감사 데이터베이스가 필요합니다.

0

감사가 사용됨을 나타냅니다.

1

감사가 사용되지 않음을 나타냅니다.

SiteMinder 설정: 1

CANODE

SIA(Service Intelligence Agent) 노드의 이름을 지정합니다.

참고: 영숫자가 아닌 문자나 공백을 사용하지 마십시오.

CADPORT

SIA가 연결하고 요청을 수신 대기해야 하는 포트를 지정합니다.

기본값: 6410

CLIENTAUDITINGREPORT

콘텐츠 관리 서버 감사 데이터베이스 구성 요소가 사용되도록 설정한 경우 감사 서비스가 수신 대기해야 하는 포트를 지정합니다. 이 매개 변수는 **SiteMinder** 감사 기반 보고서와 관련이 없습니다. 콘텐츠 관리 서버 감사 데이터베이스는 보고서 서버와 관련된 감사 활동에 사용되며 **SiteMinder**에는 사용되지 않습니다.

감사 기반 보고서를 실행하려면 **SiteMinder** 감사 데이터베이스가 필요합니다.

SiteMinder 설정: 기본값(6420)을 그대로 둡니다.

CLIENTLANGUAGE

설치할 언어 팩을 지정합니다.

SiteMinder 설정: EN

CLUSTERCMS

서버를 기존 콘텐츠 관리 서버에 추가할지 여부를 지정합니다. 이 값을 변경해야 할 경우 설치 관리자를 사용하여 다른 응답 파일을 만드는 것이 좋습니다.

SiteMinder 설정: False

CMSPASSWORD

기존 SAP BusinessObjects Enterprise 관리자 계정의 암호를 지정합니다.
이 매개 변수는 사용자 지정 설치 또는 웹 계층 설치에만 적용됩니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

DATABASEAUDITDRIVER

콘텐츠 관리 서버 감사 데이터베이스에 사용할 드라이버를 지정합니다.
이 매개 변수는 SiteMinder 감사 기반 보고서와 관련이 없습니다. 콘텐츠 관리 서버 감사 데이터베이스는 보고서 서버와 관련된 감사 활동에 사용되며 SiteMinder에는 사용되지 않습니다.

감사 기반 보고서를 실행하려면 SiteMinder 감사 데이터베이스가 필요합니다.

SiteMinder 설정:

- 포함된 MySQL 버전을 설치하는 경우
기본값(MySQLDatabaseSubSystem)을 그대로 둡니다.
- Microsoft SQL Server 또는 Oracle 보고서 데이터베이스를 구성하는 경우 값을 빈 상태로 둡니다.

DATABASEAUTHENTICATION

Microsoft SQL Server 또는 Oracle 보고서 데이터베이스를 구성하는 경우 이 매개 변수가 자동으로 생성됩니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

DATABASEAUTHENTICATION_AUDIT

Microsoft SQL Server 또는 Oracle 보고서 데이터베이스를 구성하는 경우 이 매개 변수가 자동으로 생성됩니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

DATABASECONNECT

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

DATABASECONNECT_AUDIT

Microsoft SQL Server 또는 Oracle 보고서 데이터베이스를 구성하는 경우 이 매개 변수가 자동으로 생성됩니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

DATABASEDB

보고서 데이터베이스의 이름을 지정합니다.

SiteMinder 설정:

- 포함된 MySQL 버전을 설치하는 경우 기본값(BOE120)을 그대로 둡니다.
- Microsoft SQL Server 보고서 데이터베이스를 구성하는 경우 기본값(RSDB)을 그대로 둡니다.
- Oracle 보고서 데이터베이스를 구성하는 경우 값을 빈 상태로 둡니다.

DATABASEDB_AUDIT

콘텐츠 관리 서버의 감사 데이터베이스 이름을 지정합니다. 이 매개 변수는 SiteMinder 감사 기반 보고서와 관련이 없습니다. 콘텐츠 관리 서버 감사 데이터베이스는 보고서 서버와 관련된 감사 활동에 사용되며 SiteMinder에는 사용되지 않습니다.

감사 기반 보고서를 실행하려면 SiteMinder 감사 데이터베이스가 필요합니다.

SiteMinder 설정:

- 포함된 MySQL 버전을 설치하는 경우 기본값(BOE120_AUDIT)을 그대로 둡니다.
- Microsoft SQL Server 또는 Oracle 보고서 데이터베이스를 구성하는 경우 값을 빈 상태로 둡니다.

DATABASEDRIVER

보고서 데이터베이스에 사용할 드라이버를 지정합니다.

SiteMinder 설정: 기본값을 그대로 둡니다. 이 값을 변경해야 할 경우 설치 관리자를 사용하여 다른 응답 파일을 만드십시오.

DATABASEDSN

보고서 데이터베이스의 ODBC 연결 이름을 지정합니다.

SiteMinder 설정:

- 포함된 MySQL 버전을 설치하는 경우 기본값(Business Objects CMS)을 그대로 둡니다.
- 기존 Microsoft SQL Server 인스턴스를 사용하는 경우 DSN 을 입력합니다.
- 기존 Oracle 인스턴스를 사용하는 경우 값을 빈 상태로 둡니다.

DATABASESDSN_AUDIT

콘텐츠 관리 서버 감사 데이터베이스의 ODBC 연결 이름을 지정합니다. 이 매개 변수는 SiteMinder 감사 기반 보고서와 관련이 없습니다. 콘텐츠 관리 서버 감사 데이터베이스는 보고서 서버와 관련된 감사 활동에 사용되며 SiteMinder 에는 사용되지 않습니다.

감사 기반 보고서를 실행하려면 SiteMinder 감사 데이터베이스가 필요합니다.

SiteMinder 설정: 기본값(Business Objects Audit Server)을 그대로 둡니다.

DATABASENWLAYER_AUDIT

콘텐츠 관리 서버 감사 데이터베이스 유형을 지정합니다. 이 매개 변수는 SiteMinder 감사 기반 보고서와 관련이 없습니다. 콘텐츠 관리 서버 감사 데이터베이스는 보고서 서버와 관련된 감사 활동에 사용되며 SiteMinder 에는 사용되지 않습니다.

감사 기반 보고서를 실행하려면 SiteMinder 감사 데이터베이스가 필요합니다.

SiteMinder 설정: 기본값(ODBC)을 그대로 둡니다.

DATABASEPORT

보고서 데이터베이스가 수신 대기해야 하는 포트를 지정합니다.

SiteMinder 설정:

- 포함된 MySQL 버전을 설치하는 경우 포트를 입력합니다.

기본값: 3306

- Microsoft SQL Server 또는 Oracle 보고서 데이터베이스를 구성하는 경우 값을 빈 상태로 둡니다.

DATABASEPORT_AUDIT

콘텐츠 관리 서버 감사 데이터베이스가 수신 대기하는 포트를 지정합니다. 이 매개 변수는 SiteMinder 감사 기반 보고서와 관련이 없습니다. 콘텐츠 관리 서버 감사 데이터베이스는 보고서 서버와 관련된 감사 활동에 사용되며 SiteMinder 에는 사용되지 않습니다.

감사 기반 보고서를 실행하려면 SiteMinder 감사 데이터베이스가 필요합니다.

SiteMinder 설정: 이 매개 변수에 대한 값이 필요하지 않습니다.

- 포함된 MySQL 버전을 설치하는 경우 포트를 입력합니다.

기본값: 3306

- Microsoft SQL Server 또는 Oracle 보고서 데이터베이스를 구성하는 경우 매개 변수를 빈 상태로 둡니다. SiteMinder에서는 콘텐츠 관리 서버를 감사할 필요가 없습니다.

DATABASEPWD

보고서 데이터베이스에 액세스할 수 있는 관리자 계정의 암호를 지정합니다.

DATABASEPWD_AUDIT

콘텐츠 관리 서버 감사 데이터베이스에 액세스할 수 있는 관리자 계정의 암호를 지정합니다. 이 매개 변수는 SiteMinder 감사 기반 보고서와 관련이 없습니다. 콘텐츠 관리 서버 감사 데이터베이스는 보고서 서버와 관련된 감사 활동에 사용되며 SiteMinder에는 사용되지 않습니다.

감사 기반 보고서를 실행하려면 SiteMinder 감사 데이터베이스가 필요합니다.

SiteMinder 설정:

- 포함된 MySQL 버전을 설치하는 경우 이 값과 DATABASEPWD 매개 변수를 일치시킵니다.
- Microsoft SQL Server 또는 Oracle 보고서 데이터베이스를 구성하는 경우 매개 변수를 빈 상태로 둡니다.

DATABASEPWD_MYSQLROOT

포함된 MySQL 버전을 설치하는 경우 보고서 데이터베이스에 액세스할 수 있는 MySQL 루트 사용자 계정의 암호를 지정합니다.

DATABASERDMS_AUDIT

콘텐츠 관리 서버 감사 데이터베이스 유형을 지정합니다. 이 매개 변수는 SiteMinder 감사 기반 보고서와 관련이 없습니다. 콘텐츠 관리 서버 감사 데이터베이스는 보고서 서버와 관련된 감사 활동에 사용되며 SiteMinder에는 사용되지 않습니다.

감사 기반 보고서를 실행하려면 SiteMinder 감사 데이터베이스가 필요합니다.

SiteMinder 설정: 이 매개 변수의 기본값을 그대로 둡니다.

DATABASESERVER

Oracle 보고서 데이터베이스를 구성하는 경우 Oracle 데이터베이스 서비스의 이름을 지정합니다.

참고: 이 매개 변수는 Microsoft SQL Server 보고서 데이터베이스를 구성하는 응답 파일에 나타납니다. 이 값을 비워 두십시오.

DATABASESERVER_AUDIT

콘텐츠 관리 서버 감사 데이터베이스 서버 호스트 시스템의 이름을 지정합니다. 이 매개 변수는 SiteMinder 감사 기반 보고서와 관련이 없습니다. 콘텐츠 관리 서버 감사 데이터베이스는 보고서 서버와 관련된 감사 활동에 사용되며 SiteMinder 에는 사용되지 않습니다.

감사 기반 보고서를 실행하려면 SiteMinder 감사 데이터베이스가 필요합니다.

SiteMinder 설정:

- 포함된 MySQL 버전을 설치하는 경우 기본값(localhost)을 그대로 둡니다.
- Microsoft SQL Server 또는 Oracle 보고서 데이터베이스를 구성하는 경우 매개 변수를 빈 상태로 둡니다.

DATABASEDRIVER

보고서 데이터베이스에 사용할 드라이버를 지정합니다.

SiteMinder 설정: 기본값을 그대로 둡니다. 이 값을 변경해야 할 경우 설치 관리자를 사용하여 다른 응답 파일을 만드십시오.

DATABASEUID

보고서 데이터베이스에 액세스할 수 있는 관리자 계정의 이름을 지정합니다.

SiteMinder 설정:

- 포함된 MySQL 버전을 설치하는 경우 계정 이름을 입력합니다. 설치 관리자가 필요한 권한이 있는 관리자 계정을 생성합니다.
- Microsoft SQL Server 를 구성하는 경우 데이터베이스 소유자(DBO) 권한이 있는 계정 이름을 입력합니다.

- Oracle 을 구성하는 경우 세션 만들기, 테이블 만들기 및 프로시저 만들기 권한을 사용할 수 있는 계정 이름을 입력합니다.

CONNECT 및 RESOURCE 역할을 사용할 수 있는 계정 이름을 입력할 수도 있습니다. 두 역할 모두에서 "Admin Option"(관리 옵션) 설정이 사용되지 않도록 설정해야 합니다.

DATABASE_UID_AUDIT

콘텐츠 관리 서버 감사 데이터베이스에 액세스할 수 있는 관리자 계정의 이름을 지정합니다. 이 매개 변수는 SiteMinder 감사 기반 보고서와 관련이 없습니다. 콘텐츠 관리 서버 감사 데이터베이스는 보고서 서버와 관련된 감사 활동에 사용되며 SiteMinder 에는 사용되지 않습니다. 감사 기반 보고서를 실행하려면 SiteMinder 감사 데이터베이스가 필요합니다.

SiteMinder 설정:

- 포함된 MySQL 버전을 설치하는 경우 이 값과 DATABASEUID 매개 변수를 일치시킵니다.
- Microsoft SQL Server 또는 Oracle 보고서 데이터베이스를 구성하는 경우 값을 빈 상태로 둡니다.

DATABASEUSER

Microsoft SQL Server 또는 Oracle 보고서 데이터베이스를 구성하는 경우 DATABASEUID 값과 일치하도록 이 매개 변수가 자동으로 생성됩니다.

SiteMinder 설정: 이 값이 DATABASEUID 값과 일치하는지 확인하십시오.

DATABASEUSER_AUDIT

Microsoft SQL Server 또는 Oracle 보고서 데이터베이스를 구성하는 경우 이 매개 변수가 빈 값으로 자동으로 생성됩니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

DATABASE_AUDIT_CONNSVR

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다.

SiteMinder 설정: connsvr

ENABLELOGFILE

설치 관리자가 설치 로그 파일을 생성할지 여부를 지정합니다.

0

로그 파일을 생성하지 않습니다.

1

로그 파일을 생성합니다.

ENABLESERVERS

설치가 완료된 후 서버가 사용되도록 설정할지 여부를 지정합니다.

0

서버가 사용되도록 설정하지 않습니다.

1

서버가 사용되도록 설정합니다.

SiteMinder 설정: 1

EXPANDCMS

Microsoft SQL Server 또는 Oracle 보고서 데이터베이스를 구성하는 경우 이 매개 변수가 자동으로 생성됩니다. 이 매개 변수를 수정하지 마십시오.

SiteMinder 설정: 1

INSTALL.LP.EN.SELECTED

설치 관리자에서 영어 언어 팩을 설치하도록 지정합니다.

SiteMinder 설정: 1

INSTALLDBTYPE

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다.

INSTALLDIR

보고서 서버가 설치되는 디렉터리를 지정합니다.

참고: 백슬래시 문자를 사용하여 경로에서 백슬래시를 이스케이프 처리했는지 확인하십시오.

예: C:\\Program Files\\CA\\SC\\CommonReporting3\\

INSTALLLEVEL

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다.

INSTALLMODE

설치 방법을 지정합니다.

New

필요한 모든 서버 및 클라이언트 구성 요소를 설치합니다.

Custom

설치할 특정 서버 및 클라이언트 구성 요소를 선택합니다.

Web Tier

필수 웹 응용 프로그램 서버 구성 요소만 설치합니다.

SiteMinder 설정: New

INSTALL_DB_TYPE

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다.

MYSQLPORT

포함된 MySQL 버전을 사용하는 경우 MySQL 이 연결하여 요청을 수신 대기해야 하는 포트를 지정합니다.

기본값: 3306.

참고: 이 매개 변수는 Microsoft SQL Server 를 보고서 데이터베이스로 구성하는 속성 파일에 나타납니다. 기본값을 그대로 두십시오.

MYSQLSERVER

Microsoft SQL Server 또는 Oracle 보고서 데이터베이스를 구성하는 경우 이 매개 변수가 자동으로 생성됩니다. 이 매개 변수를 수정하지 마십시오.

SiteMinder 설정: 값을 빈 상태로 둡니다.

MYSQLSERVER_AUDIT

Microsoft SQL Server 또는 Oracle 보고서 데이터베이스를 구성하는 경우 이 매개 변수가 자동으로 생성됩니다. 이 매개 변수를 수정하지 마십시오.

SiteMinder 설정: 값을 빈 상태로 둡니다.

NEWCMSPASSWORD

기본 SAP BusinessObjects Enterprise 관리자 계정의 암호를 지정합니다.
이 매개 변수는 자동으로 생성됩니다.

SiteMinder 설정: 이 매개 변수를 수정하지 마십시오. 이 값을 변경해야 할 경우 설치 관리자를 사용하여 다른 응답 파일을 만드십시오.

MYSQL_REMOTE_ACCESS

보고서 데이터베이스 기능을 수행하기 위해 포함된 MySQL 버전을 사용하는 경우 원격 액세스가 사용되도록 설정할지 여부를 지정합니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

참고: 이 매개 변수는 Microsoft SQL Server 를 보고서 데이터베이스로 구성하는 속성 파일에 나타납니다. 이 값을 비워 두십시오.

NAMESERVER

보고서 서버 호스트 시스템의 이름을 지정합니다.

NEWCMSPASSWORD

기본 SAP BusinessObjects Enterprise 관리자 계정의 암호를 지정합니다.

SiteMinder 설정: 이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다. 이 값을 변경해야 할 경우 설치 관리자를 사용하여 다른 응답 파일을 만드십시오.

NSPORT

콘텐츠 관리 서버가 수신 대기하는 포트를 지정합니다.

기본값: 6400.

REINITIALIZE_CMS_DB

Microsoft SQL Server 또는 Oracle 보고서 데이터베이스를 구성하는 경우 데이터베이스를 다시 초기화하도록 지정합니다.

SiteMinder 설정: 1

SINGLESERVER

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다. 이 매개 변수를 수정하지 마십시오.

SiteMinder 설정: 값을 빈 상태로 둡니다.

SKIP_DEPLOYMENT

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다. 이 매개 변수를 수정하지 마십시오.

SiteMinder 설정: 값을 빈 상태로 둡니다.

SelectODBCDSN

Microsoft SQL Server 또는 Oracle 보고서 데이터베이스를 구성하는 경우 이 매개 변수가 자동으로 생성됩니다. 이 매개 변수를 수정하지 마십시오.

SiteMinder 설정: 값을 빈 상태로 둡니다.

TOMCAT_CONNECTION_PORT

포함된 Apache Tomcat 버전이 연결하고 요청을 수신 대기해야 하는 포트를 지정합니다.

기본값: 8080.

TOMCAT_REDIRECT_PORT

포함된 Apache Tomcat 버전이 요청을 리디렉션해야 하는 포트를 지정합니다.

기본값: 8443

TOMCAT_SHUTDOWN_PORT

포함된 Apache Tomcat 버전에 대한 SHUTDOWN 명령이 실행되는 포트를 지정합니다.

기본값: 8005

WCADOTNETINSTALL

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다.

SiteMinder 설정: False

WCAEXISTINGINSTALL

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다.

SiteMinder 설정: False

WCAJAVAINSTALL

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다.

SiteMinder 설정: False

WCATOMCATINSTALL

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다.

SiteMinder 설정: True

WDEPLOY_LANGUAGES

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다.

SiteMinder 설정: en

WDEPLOY_LATER

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다.

SiteMinder 설정: 이 값을 비워 두십시오.

WEBSITE_METABASE_NUMBER

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다.

SiteMinder 설정: 1

WEBSITE_NAME

IIS 웹 응용 프로그램 서버를 배포하는 경우 SAP BusinessObjects Enterprise 응용 프로그램이 배포되는 IIS 웹 사이트의 이름을 지정합니다.

SiteMinder 는 포함된 Apache Tomcat 버전만 지원합니다.

SiteMinder 설정: Default Web Site

WEBSITE_PORT

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다.

SiteMinder 설정: 80

기능

이 단원에서는 응답 파일의 **Features** 섹션에 있는 매개 변수에 대해 자세히 설명합니다.

REMOVE

설치하지 않을 클라이언트, 서버, 웹 계층 및 기타 SAP BusinessObjects Enterprise 구성 요소를 지정합니다.

SiteMinder 설정: 이 매개 변수 값을 변경하지 마십시오. 이 값을 변경하려면 설치 관리자를 사용하여 다른 응답 파일을 만드십시오.

ADDLOCAL

설치할 클라이언트, 서버, 웹 계층 및 기타 SAP BusinessObjects Enterprise 구성 요소를 지정합니다.

SiteMinder 설정: 이 매개 변수 값을 변경하지 마십시오. 이 값을 변경하려면 설치 관리자를 사용하여 다른 응답 파일을 만드십시오.

ADDSOURCE

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

ADVERTISE

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

BIEK

이 단원에서는 응답 파일의 BIEK 섹션에 있는 매개 변수에 대해 자세히 설명합니다.

BIEK_INSTALL_SAMPLES

설치 관리자가 CA 템플릿을 설치할지 여부를 지정합니다. 이 매개 변수는 SiteMinder 보고 템플릿과 관련이 없습니다. SiteMinder 보고서 서버 구성 마법사가 필요한 보고 템플릿을 설치합니다. 보고서 서버를 설치한 후 이 마법사를 실행하십시오.

0

샘플 템플릿을 설치하지 않습니다.

1

샘플 템플릿을 설치합니다.

SiteMinder 설정: 0

SUPPRESS_REBOOT

설치에 성공한 후 설치 관리자가 컴퓨터를 재부팅할지 여부를 지정합니다.

0

설치에 성공한 후 설치 관리자가 시스템을 다시 시작하도록 합니다.

1

설치에 성공한 후 설치 관리자가 시스템을 다시 시작하지 않도록 합니다. 설치를 완료하려면 시스템을 수동으로 다시 시작하십시오.

SiteMinder 설정: 1

UNIX 의 보고서 서버 응답 파일 수정

설치 관리자 응답 파일을 수정하여 설치 변수를 정의합니다. 기본값은 보고서 서버를 설치하고 응답 파일을 저장할 때 입력한 정보를 반영합니다.

중요! 파일을 수정하기 전에 다음 사항을 확인하십시오.

- 일부 매개 변수는 보고서 데이터베이스 기능을 수행할 데이터베이스 유형을 식별합니다. 설치 관리자가 구성하게 될 데이터베이스의 유형을 속성 파일을 사용해서 변경하지 마십시오. 보고서 데이터베이스 유형을 변경하려면 설치 관리자를 사용하여 또 다른 속성 파일을 만드십시오.
- 명령줄에서 매개 변수를 전달하면 응답 파일의 해당 설정이 재정의됩니다.

보고서 서버 설치 관리자는 일부 매개 변수를 자동으로 생성합니다. 다음 매개 변수를 수정하지 마십시오.

- PRODUCTID_NAME
- BOBJVERSION
- DATACONNECTION
- PRODUCTID_VER
- FUNCTION
- LANGUAGES_TO_INSTALL
- EXPANDSERVERS

Manual Settings

이 단원에서는 응답 파일의 **Manual Settings** 섹션에 있는 매개 변수에 대해 자세히 설명합니다.

MACHINENAME

보고서 서버 호스트의 이름을 지정합니다. 이 값이 로컬 서버 이름보다 우선합니다. 값을 제공하지 않으면 기본적으로 로컬 호스트 시스템 이름이 사용됩니다.

Paths

이 단원에서는 응답 파일의 **Paths** 섹션에 있는 매개 변수에 대해 자세히 설명합니다.

BOBJEDIR

bobje 디렉터리의 경로를 지정합니다. bobje 디렉터리는 공용 보고 디렉터리에 자동으로 생성됩니다.

예: /opt/CA/SharedComponents/CommonReporting3/bobje/

CDDIR

보고서 서버 설치 키트에서 **Disk1** 디렉터리의 경로를 지정합니다.

LICENSEDIR

제품 라이선스가 들어 있는 디렉터리의 경로를 지정합니다.

참고: 보고서 서버를 설치할 때 제품 라이선스를 제공할 필요가 없습니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

Product Information

이 단원에서는 응답 파일의 **Product Information** 섹션에 있는 매개 변수에 대해 자세히 설명합니다.

BOBJELANG

설치에서 사용하는 언어 설정을 지정합니다.

SiteMinder 설정: en

PRODUCTID_NAME

설치하려는 제품의 이름을 지정합니다.

SiteMinder 설정: BusinessObjects

BOBJEVERSION

SAP BusinessObjects Enterprise 버전을 지정합니다.

SiteMinder 설정: 12.0

PRODUCTID_VER

설치하려는 제품의 버전을 지정합니다.

SiteMinder 설정: 12.3

BOBJLICENSEKEY

제품 설치에 필요한 라이선스 키를 지정합니다. 이 값은 암호화되어 나타납니다.

SiteMinder 설정: 이 값을 수정하지 마십시오.

PIDKEY

제품 ID 키를 지정합니다. 이 값은 암호화되어 나타납니다.

SiteMinder 설정: 이 값을 수정하지 마십시오.

Installation Information

이 단원에서는 응답 파일의 **Installation Information** 섹션에 있는 매개 변수에 대해 자세히 설명합니다.

FUNCTION

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다.

SiteMinder 설정: install

INSTALLTYPE

설치 방법을 지정합니다.

new

필요한 모든 서버 및 클라이언트 구성 요소를 설치합니다.

custom

설치할 특정 서버 및 클라이언트 구성 요소를 선택합니다.

webtier

필수 웹 응용 프로그램 서버 구성 요소만 설치합니다.

SiteMinder 설정: new

INSTALLMODE

보고서 서버 설치 작동 모드를 쉼표로 구분된 목록으로 지정합니다. 이 매개 변수는 다음과 같은 옵션을 지원합니다.

- install
- 수정

- remove
- interactive

SiteMinder 설정: install

LOCALNAMESERVER

보고서 서버 호스트 시스템의 이름을 지정합니다.

BOBJEINSTALLLOCAL

사용자 설치를 실행할지, 아니면 시스템 설치를 실행할지를 지정합니다.

SiteMinder 설정: user

LANGPACKS_TO_INSTALL

설치할 언어 팩을 지정합니다. **SiteMinder** 는 영어 언어 팩만 지원합니다. 설치 관리자에서는 기본적으로 영어 언어 팩을 설치합니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

LANGUAGES_TO_INSTALL

SAP BusinessObjects Enterprise 에 포함된 모든 언어를 지정합니다. 이러한 값은 설치할 언어 팩이 아니라 사용 가능한 언어를 나타냅니다.

SiteMinder 설정: 쉼표로 구분된 값 목록을 그대로 두십시오.

BOBJEUSERNAME

루트 아닌 사용자 계정의 이름을 지정합니다.

SiteMinder 설정: 이 값과 응답 파일의 BIEK 섹션에 있는 BIEK_INSTALL_USER 값이 일치하는지 확인하십시오.

EXPANDSERVERS

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

Tomcat

이 단원에서는 응답 파일의 Tomcat 섹션에 있는 매개 변수에 대해 자세히 설명합니다.

INSTALLTOMCAT

포함된 Apache Tomcat 버전을 설치해야 하는지 여부를 지정합니다.

SiteMinder 설정: yes

참고: 설치 관리자는 웹 응용 프로그램 서버의 기존 인스턴스를 구성하도록 허용하지만 SiteMinder 는 포함된 Apache Tomcat 버전만 지원합니다.

CONNECTORPORT

포함된 Apache Tomcat 버전이 연결하고 요청을 수신 대기해야 하는 포트를 지정합니다.

기본값: 8080.

REDIRECTPORT

포함된 Apache Tomcat 버전이 요청을 리디렉션해야 하는 포트를 지정합니다.

기본값: 8443

SHUTDOWNPORT

포함된 Apache Tomcat 버전에 대한 SHUTDOWN 명령이 실행되는 포트를 지정합니다.

기본값: 8005

Application Server

이 단원에서는 응답 파일의 Application Server 섹션에 있는 매개 변수에 대해 자세히 설명합니다.

AS_DIR

포함된 Apache Tomcat 버전이 설치되어 있는 경로를 지정합니다. 이 경로는 설치 디렉터리를 사용하여 자동으로 설정됩니다.

예: /opt/CA/SharedComponents/CommonReporting3//bobje/tomcat/

AS_SERVER

배포할 Java 웹 응용 프로그램 서버의 유형을 지정합니다. 포함된 Apache Tomcat 버전을 설치한 경우 기본값은 tomcat55 입니다. SiteMinder 는 포함된 Apache Tomcat 버전만 지원합니다.

SiteMinder 설정: tomcat55

AS_INSTANCE

웹 응용 프로그램 서버 인스턴스의 이름을 지정합니다. 포함된 Apache Tomcat 버전을 설치한 경우 기본값은 localhost 입니다. SiteMinder 는 포함된 Apache Tomcat 버전만 지원합니다.

SiteMinder 설정: localhost

AS_VIRTUAL_HOST

가상 환경에 보고서 서버를 배포하는 경우 응용 프로그램이 바인딩되어야 하는 가상 호스트를 지정합니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

AS_ADMIN_PORT

웹 응용 프로그램 서버가 수신 대기하는 포트를 지정합니다. 포함된 Apache Tomcat 버전을 설치한 경우 이 값이 비어 있습니다. SiteMinder 는 포함된 Apache Tomcat 버전만 지원합니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

AS_ADMIN_USERNAME

웹 응용 프로그램 서버에 액세스하는 데 사용되는 관리자 계정의 계정 이름을 지정합니다. 포함된 Apache Tomcat 버전을 설치한 경우 이 값이 비어 있습니다. SiteMinder 는 포함된 Apache Tomcat 버전만 지원합니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

AS_ADMIN_PASSWORD

웹 응용 프로그램 서버에 액세스할 수 있는 관리자 계정의 암호를 지정합니다. 포함된 Apache Tomcat 버전을 설치한 경우 이 값이 비어 있습니다. SiteMinder 는 포함된 Apache Tomcat 버전만 지원합니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

AS_ADMIN_SECURE

웹 응용 프로그램 서버에 액세스하려면 관리자 자격 증명을 전달해야 하도록 지정합니다. 이 매개 변수는 SiteMinder 가 지원하지 않는 웹 응용 프로그램 서버에 적용됩니다.

SiteMinder 설정: false

AS_APPSERVER_ID

응용 프로그램 서버의 이름을 지정합니다. 이 매개 변수는 SiteMinder 가 지원하지 않는 웹 응용 프로그램 서버에 적용됩니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

AS_GROUP_ID

응용 프로그램 서버의 그룹 ID 를 지정합니다. 이 매개 변수는 SiteMinder 가 지원하지 않는 웹 응용 프로그램 서버에 적용됩니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

WEBDEPLOYACTION

웹 응용 프로그램 서버에서 수행할 작업을 지정합니다.

SiteMinder 설정: deploy

REDEPLOYWEBAPPS

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다.

SiteMinder 설정: true

CMS Cluster

이 단원에서는 응답 파일의 CMS Cluster 섹션에 있는 매개 변수에 대해 자세히 설명합니다.

CMSCLUSTER

서버를 기존 콘텐츠 관리 서버에 추가할지 여부를 지정합니다.

SiteMinder 설정: no

CLUSTER_NAMESERVER

서버를 콘텐츠 관리 서버로 클러스터링하는 경우 콘텐츠 관리 서버의 이름을 지정합니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

CLUSTERPORTNUMBER

서버를 콘텐츠 관리 서버로 클러스터링하는 경우 콘텐츠 관리 서버가 수신 대기하는 포트를 지정합니다. 이 값의 기본값은 CMSPORTNUMBER 매개 변수 값입니다. 이 매개 변수는 응답 파일의 CMS 섹션에 있습니다.

SiteMinder 설정: 이 값이 CMSPORTNUMBER 값과 일치하는지 확인하십시오.

CMS

이 단원에서는 응답 파일의 CMS 섹션에 있는 매개 변수에 대해 자세히 설명합니다.

DBTYPE

보고서 데이터베이스 기능을 수행할 데이터베이스 유형을 지정합니다.

SiteMinder 설정:

■ MySQL

중요! SiteMinder 는 포함된 MySQL 버전만 지원합니다.

■ Oracle

중요! 보고서 서버는 CA 제품 간에 공유할 수 있는 CA 공용 구성 요소입니다. 따라서 SiteMinder 가 아닌 다른 제품이 지원하는 데이터베이스 유형 및 버전으로 보고서 데이터베이스를 구성할 수 있습니다. 지원되는 데이터베이스 유형 및 버전 목록에 대해서는 "SiteMinder 12.52 SP1 Platform Support Matrix"(SiteMinder 12.52 SP1 플랫폼 지원표)를 참조하십시오.

SERVICENAME

보고서 데이터베이스 기능을 수행할 Oracle 데이터베이스의 서비스 이름을 지정합니다.

참고: MySQL 을 구성하는 경우 기본값은 BOE120 입니다. 기본값을 그대로 두십시오.

DATABASEUID

보고서 데이터베이스에 액세스하는 데 사용되는 관리자 계정의 이름을 지정합니다.

SiteMinder 설정:

- 포함된 MySQL 버전을 설치하는 경우 계정 이름을 입력합니다. 설치 관리자가 필요한 권한이 있는 관리자 계정을 생성합니다.

- Oracle 을 구성하는 경우 세션 만들기, 테이블 만들기 및 프로시저 만들기 권한을 사용할 수 있는 계정 이름을 입력합니다.

CONNECT 및 RESOURCE 역할을 사용할 수 있는 계정 이름을 입력할 수도 있습니다. 두 역할 모두에서 "Admin Option"(관리 옵션) 설정이 사용되지 않도록 설정해야 합니다.

DATABASEPASSWORD

보고서 데이터베이스에 액세스하는 데 사용되는 관리자 계정의 암호를 지정합니다.

CMSNAMESERVER

보고서 서버 호스트 시스템의 이름을 지정합니다.

SiteMinder 설정: 이 값과 응답 파일의 Installation Information 섹션에 있는 LOCALNAMESERVER 값이 일치하는지 확인하십시오.

CMSPORTNUMBER

콘텐츠 관리 서버가 연결하고 요청을 대기해야 하는 포트를 지정합니다.

기본값: 6400

CMSPASSWORD

중앙 관리 서버에 액세스하는 관리자 계정의 암호를 지정합니다. 이 암호는 SAP BusinessObjects Enterprise 시스템 관리자 계정의 암호입니다.

SIANODENAME

SIA(Service Intelligence Agent) 노드의 이름을 지정합니다.

참고: 영숫자가 아닌 문자나 공백을 사용하지 마십시오.

SIAPORTNUMBER

SIA 가 연결하고 요청을 대기해야 하는 포트를 지정합니다.

기본값: 6410

REINIT

보고서 데이터베이스를 다시 초기화해야 하는지 여부를 지정합니다. 이 매개 변수를 수정하지 마십시오. 이 매개 변수는 자동으로 생성됩니다.

SiteMinder 설정: yes

MySQL

이 단원에서는 응답 파일의 **MySQL** 섹션에 있는 매개 변수에 대해 자세히 설명합니다.

INSTALLMYSQL

포함된 MySQL 버전을 설치해야 하는지 여부를 지정합니다.

SiteMinder 설정:

- 포함된 MySQL 버전을 설치하는 경우 **yes** 를 입력합니다.
- Oracle 보고서 데이터베이스를 구성하는 경우 값을 빈 상태로 둡니다.

SERVICEPORT

포함된 MySQL 버전을 설치하는 경우 **MySQL** 이 연결하여 요청을 수신 대기해야 하는 포트를 지정합니다.

기본값: 3306

참고: Oracle 보고서 데이터베이스를 구성하는 경우 기본값을 그대로 둡니다.

MYSQLHOSTNAME

포함된 MySQL 버전을 설치하는 경우 **MySQL** 호스트 시스템의 IP 주소를 지정합니다. **MySQL** 호스트 시스템은 보고서 서버 호스트 시스템과 동일합니다.

MYSQLROOTPASSWORD

포함된 MySQL 버전을 설치하는 경우 **MySQL** 루트 사용자 계정의 암호를 지정합니다.

Audit

이 단원에서는 응답 파일의 **Audit** 섹션에 있는 매개 변수에 대해 자세히 설명합니다.

이러한 매개 변수는 **SiteMinder** 감사 기반 보고서와 관련이 없습니다. 콘텐츠 관리 서버 감사 데이터베이스는 보고서 서버와 관련된 감사 활동에 사용되며 **SiteMinder** 에는 사용되지 않습니다.

감사 기반 보고서를 실행하려면 **SiteMinder** 감사 데이터베이스가 필요합니다.

AUDITINGENABLED

콘텐츠 관리 서버 감사 데이터베이스가 사용되도록 설정할지 여부를 지정합니다.

- 포함된 MySQL 버전을 설치하는 경우 자동으로 감사 데이터베이스가 사용되도록 설정됩니다.

SiteMinder 설정: yes

- Oracle 보고서 데이터베이스를 구성하는 경우 콘텐츠 관리 서버를 감사할 필요가 없습니다.

SiteMinder 설정: no

SERVICENAME_AUDIT

콘텐츠 관리 서버가 사용하는 감사 서비스의 이름을 지정합니다. 이 값의 기본값은 BOE120_AUDIT 입니다. 이것은 감사 데이터베이스를 사용하지 않는 경우에도 마찬가지입니다.

SiteMinder 설정: 기본값을 그대로 둡니다.

SERVICEPORT_AUDIT

콘텐츠 관리 서버 감사 데이터베이스가 연결하고 요청을 수신 대기해야 하는 포트 번호를 지정합니다. 기본값은 3306 입니다.

SiteMinder 설정:

- 포함된 MySQL 버전을 설치하는 경우 이 값과 응답 파일의 MySQL 섹션에 있는 SERVICEPORT 매개 변수를 일치시킵니다.
- Oracle 보고서 데이터베이스를 구성하는 경우 기본값을 그대로 둡니다.

MYSQLHOSTNAME_AUDIT

콘텐츠 관리 서버 감사 데이터베이스 호스트 시스템의 IP 주소를 지정합니다.

SiteMinder 설정:

- 포함된 MySQL 버전을 설치하는 경우 이 값과 응답 파일의 MySQL 섹션에 있는 MYSQLHOSTNAME 매개 변수를 일치시킵니다.
- Oracle 보고서 데이터베이스를 구성하는 경우 값을 빈 상태로 둡니다.

DATABASEUID_AUDIT

콘텐츠 관리 서버 감사 데이터베이스에 액세스하는 데 사용되는 관리자 계정의 이름을 지정합니다.

SiteMinder 설정:

- 포함된 MySQL 버전을 설치하는 경우 이 값과 응답 파일의 MySQL 섹션에 있는 DATABASEUID 매개 변수를 일치시킵니다.
- Oracle 보고서 데이터베이스를 구성하는 경우 값을 빈 상태로 둡니다.

DATABASEPWD_AUDIT

콘텐츠 관리 서버 감사 데이터베이스에 액세스하는 데 사용되는 관리자 계정의 암호를 지정합니다.

SiteMinder 설정:

- 포함된 MySQL 버전을 설치하는 경우 이 값과 응답 파일의 MySQL 섹션에 있는 MYSQLROOTPWD 매개 변수를 일치시킵니다.
- Oracle 보고서 데이터베이스를 구성하는 경우 값을 빈 상태로 둡니다.

Marketing Products

이 단원에서는 응답 파일의 Marketing Products 섹션에 있는 매개 변수에 대해 자세히 설명합니다.

ENABLEMP

사용되도록 수동으로 설정할 클라이언트, 서버, 웹 계층 및 기타 SAP BusinessObjects Enterprise 구성 요소를 지정합니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

DISABLEMP

사용되지 않도록 수동으로 설정할 클라이언트, 서버, 웹 계층 및 기타 SAP BusinessObjects Enterprise 구성 요소를 지정합니다.

SiteMinder 설정: 이 매개 변수 값을 빈 상태로 두십시오.

BIEK

이 단원에서는 응답 파일의 BIEK 섹션에 있는 매개 변수에 대해 자세히 설명합니다.

BIEK_INSTALL_USER

설치 관리자가 사용해야 하는 루트 아닌 사용자 계정을 지정합니다.

BIEK_INSTALL_GROUP

루트 아닌 사용자가 속한 그룹을 지정합니다.

BIEK_CASHCOMP

CA 공유 구성 요소 환경 변수(CASHComp)에 설정해야 할 전체 경로를 지정합니다. CASHComp 가 이미 설정되어 있는 경우 이 값이 무시됩니다.

BIEK_INSTALL_SAMPLES

설치 관리자가 CA 템플릿을 설치할지 여부를 지정합니다. 이 매개 변수는 SiteMinder 보고 템플릿과 관련이 없습니다. SiteMinder 보고서 서버 구성 마법사가 필요한 보고 템플릿을 설치합니다. 보고서 서버를 설치한 후 이 마법사를 실행하십시오.

0

샘플 템플릿을 설치하지 않습니다.

1

샘플 템플릿을 설치합니다.

SiteMinder 설정: 0

BIEK_MIGRATE_CMS_DATA

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 업그레이드를 위해서만 사용됩니다.

SiteMinder 설정: 0

BIEK_SOURCE_CMS_PASSWORD

이 매개 변수를 수정하지 마십시오. 이 매개 변수는 업그레이드를 위해서만 사용됩니다.

SiteMinder 설정: 값을 빈 상태로 둡니다.

SiteMinder 보고서 서버 구성 마법사 속성 파일 수정

보고서 서버 구성 마법사 속성 파일을 수정하여 구성 변수를 정의하십시오. 이 파일의 기본 매개 변수, 암호 및 경로는 최근에 마법사를 실행할 때 입력한 정보를 반영합니다.

이 속성 파일에는 다음 매개 변수가 있습니다.

DEFAULT_BOXI_INSTALL_PATH

보고서 서버 설치 경로를 지정합니다.

DEFAULT_BOXI_PASSWORD

기본 BusinessObjects 관리자 계정의 암호를 지정합니다.

참고: ENCRYPTED_BOXI_PASSWORD 에서 암호화된 값을 사용할 경우 이 매개 변수에는 값을 입력할 필요가 없습니다.

ENCRYPTED_BOXI_PASSWORD

기본 BusinessObjects 관리자 계정의 암호화된 암호를 지정합니다.

중요! 암호화된 값을 변경하지 마십시오. 다른 암호를 입력하려면 암호화된 암호를 주석 처리하고 DEFAULT_BOXI_PASSWORD 에 값을 지정하십시오.

DEFAULT_AUDIT_DATABASE_TYPE

SiteMinder 감사 저장소로 사용할 데이터베이스의 유형을 지정합니다.

참고: 보고서 서버 구성 마법사를 실행하기 전에 SiteMinder 감사 데이터베이스를 구성할 필요는 없습니다.

값: 1 또는 2

1

Microsoft SQL Server 를 지정합니다.

2

Oracle 을 지정합니다.

보고서 서버 설치 관리자 실행

무인 설치를 실행하여 사용자 개입 없이 보고서 서버를 설치할 수 있습니다.

설치하기 전에

보고서 서버를 설치하기 전에 다음 항목을 확인하십시오.

- 기술 지원 사이트의 설치 미디어를 사용하여 보고서 서버를 설치하십시오.

참고: 설치 미디어 이름의 목록에 대해서는 *정책 서버 릴리스 정보*를 참조하십시오.

- 보고서 서버는 32 비트 네이티브 바이너리로 컴파일되며 32 비트 데이터 원본 미들웨어 연결을 사용하도록 설계되어 있습니다. Windows 64 비트 운영 체제에 설치하는 경우 `odbcad32.exe` 를 사용하여 DSN 을 만들어야 합니다. 이 실행 파일은 다음 위치에 있습니다.

`install_home\Windows\SysWOW64.`

install_home

Windows 운영 체제의 설치 경로를 지정합니다.

- 보고서 서버 설치에는 프로세스로 실행되는 다음과 같은 구성 요소가 포함됩니다.

- 콘텐츠 관리 서버
- Server Intelligence Agent

이러한 구성 요소에는 통신에 사용할 TCP/IP 포트가 필요합니다. 보고서 서버 호스트 시스템의 포트 충돌을 방지하기 위해 설치 관리자에서 기본 설정을 수정할 수 있습니다.

- **중요!** 설치 zip 에는 여러 폴더가 포함되어 있습니다. 보고서 서버 설치 관리자에는 이 폴더 구조가 필요합니다. zip 파일의 압축을 풀 후 보고서 서버 설치 관리자를 이동한 경우에는 전체 폴더 구조를 동일한 위치로 복사합니다. 이 폴더 구조에서 설치 미디어를 실행해야 합니다.

Windows

다음 단계를 수행하십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. 명령 프롬프트를 엽니다.
3. 디렉터리를 `temporary_location` 으로 변경합니다.

temporary_location

설치 미디어를 복사한 위치를 지정합니다.

4. 다음 명령을 입력합니다.

```
installation_media silent path_to_response_file
```

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

installation_media

보고서 서버 설치 실행 파일의 이름을 지정합니다.

참고: 설치 미디어 이름의 목록에 대해서는 *정책 서버 릴리스* 정보를 참조하십시오.

path_to_response_file

파일의 경로를 지정합니다. 경로에 응답 파일 이름이 포함되어야 합니다.

참고: 응답 파일이 설치 실행 파일과 같은 디렉터리에 있을 필요는 없습니다.

자동 설치가 시작됩니다.

UNIX

다음 단계를 수행하십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. 루트 사용자 권한이 있는 계정을 사용해야 합니다.
3. Bourne 셸을 열고 *temporary_location* 으로 이동합니다.

temporary_location

설치 미디어를 복사한 위치를 지정합니다.

4. 다음 명령을 입력합니다.

```
./installation_media silent path_to_response_file
```

installation_media

보고서 서버 실행 파일의 이름을 지정합니다.

참고: 설치 미디어 이름의 목록에 대해서는 *정책 서버 릴리스* 정보를 참조하십시오.

path_to_response_file

응답 파일의 경로를 지정합니다. 경로에 응답 파일 이름이 포함되어야 합니다.

참고: 응답 파일이 설치 실행 파일과 같은 디렉터리에 있을 필요는 없습니다.

자동 설치가 시작됩니다.

보고서 템플릿 설치

무인 설치를 실행하여 사용자 개입 없이 SiteMinder 보고서 템플릿을 설치할 수 있습니다.

설치하기 전에

기술 지원 사이트의 설치 미디어를 사용하여 SiteMinder 보고서 템플릿을 설치하십시오.

참고: 설치 미디어 이름의 목록에 대해서는 *정책 서버 릴리스 정보*를 참조하십시오.

부록 A: 다국어 환경의 정책 서버 구성

이 섹션은 다음 항목을 포함하고 있습니다.

[다국어 환경의 정책 서버](#) (페이지 653)

[정책 서버 설치 전 계획 고려 사항](#) (페이지 653)

[다국어 문자를 지원하는 SiteMinder 데이터 저장소 구성](#) (페이지 658)

다국어 환경의 정책 서버

다국어 환경에서 정책 서버는 Oracle 또는 SQL Server 데이터베이스와 LDAP 서버에 있는 SiteMinder 데이터 저장소를 지원합니다.

정책 서버 설치 전 계획 고려 사항

정책 서버를 설치하기 전에 다음 사항을 고려하십시오.

- 지원되는 운영 체제 및 타사 소프트웨어를 사용합니다.
- 지원되는 데이터베이스를 생성합니다.
 - 정책 또는 세션 데이터를 저장할 데이터베이스를 생성하기 전에 데이터베이스가 UTF-8 인코딩으로 형식이 지정되었는지 여부를 확인합니다.
 - 사용자 저장소 데이터베이스는 UTF-8 인코딩 제한을 받지 않습니다. 로컬 문자 집합 인코딩으로 사용자 데이터베이스를 생성할 수 있습니다.

참고: Active Directory 네임스페이스는 멀티바이트 문자를 지원하지 않습니다. 사용하는 코드 페이지에 관계없이 SiteMinder 는 문자를 유니코드로 정의된 문자로 취급합니다. 코드 페이지에서 특수 문자를 단일 바이트로 참조할 수 있지만 SiteMinder 는 유니코드에서 이 문자를 멀티바이트 문자로 정의하는 경우 해당 문자를 멀티바이트 문자로 취급합니다.

- 모든 관리 UI 필드는 멀티바이트 문자를 지원합니다.

- 일부 정책 서버 구성 요소는 다국어 환경에서 멀티바이트 문자와 ASCII 문자를 지원합니다.
- SiteMinder 는 MBCS(멀티바이트 문자) URL 을 지원합니다.

참고: 지원되는 CA 및 타사 구성 요소의 목록에 대해서는 기술 지원 사이트의 SiteMinder 12.52 SP1 Platform Support Matrix(플랫폼 지원표)를 참조하십시오.

멀티바이트 문자를 지원하는 정책 서버 구성 요소

다음 정책 서버 구성 요소는 다국어 환경에서 멀티바이트 문자와 ASCII 문자를 지원합니다.

- 관리 UI
- 정책 서버 관리 콘솔
- 인증 체계
 - HTML 양식
 - X.509 클라이언트 인증서
 - X.509 클라이언트 인증서 및 HTML 양식
 - X.509 클라이언트 인증서 또는 HTML 양식
 - RADIUS CHAP/PAP
 - SecurID 인증
 - 익명 인증
 - 사용자 지정 인증
 - 가장 인증

- 암호 서비스

참고: 암호 서비스는 ASCII 문자 제한을 받지만 리디렉션 URL 로 멀티바이트 문자 URL 을 지원할 수 있습니다.

- 응답
- POST 보존
- SiteMinder 테스트 도구
- 텍스트 파일에 대한 감사 로깅

- ODBC 데이터베이스에 대한 감사 로깅
- smobjimport
- XPSEExport 및 XPSImport
- Java Agent API

멀티바이트 문자 URL 지원

SiteMinder 는 멀티바이트 문자(MBCS)가 포함된 URL 을 지원합니다. MBCS URL 지원에는 다음에 대한 지원이 포함됩니다.

- **다국어 도메인 이름** - IDN(*다국어 도메인 이름*)은 분음 부호가 있는 문자를 비롯한 비 ASCII 문자와 아랍어 및 중국어 같은 비 라틴어 스크립트의 문자가 포함될 수 있는 인터넷 도메인 이름입니다.
- **다국어 리소스 식별자** - IRI(*다국어 리소스 식별자*)는 국제적으로 사용되는 URI(Uniform Resource Identifier)에 해당합니다. URI 에는 일부 ASCII 문자만 포함될 수 있는 반면, IRI 에는 ASCII 문자와 MBCS 집합의 문자가 포함될 수 있습니다.

MBCS URL 이 지원되므로 다음과 같은 이점이 있습니다.

- SiteMinder 에서 MBCS URL 을 통해 액세스되는 리소스를 보호할 수 있습니다.
- 특정 인증 체계를 IDN 과 IRI 를 사용하여 구성할 수 있습니다.

MBCS URL 지원이 사용되도록 설정하는 방법

SiteMinder 환경에서 MBCS URL 을 지원하려면 다음 조건을 충족해야 합니다.

- 보호되는 리소스에 액세스하는 데 사용되는 웹 브라우저가 특정 요구 사항을 충족해야 합니다.
- 사용 환경에 구현된 웹 서버가 특정 요구 사항을 충족해야 합니다.
- 웹 에이전트 구성 개체에서 잘못된 기본 문자를 제거해야 합니다.

MBCS URL 지원이 사용되도록 설정하려면

1. 웹 브라우저가 MBCS URL 에 대한 요구 사항을 충족하는지 확인합니다.
2. 웹 서버가 MBCS URL 에 대한 요구 사항을 충족하는지 확인합니다.
3. 웹 에이전트 구성 개체를 구성합니다.

MBCS URL 에 대한 웹 브라우저 요구 사항

웹 브라우저에서 UTF-8 형식으로 리소스를 제공하며 도메인 이름에 비 ASCII 문자가 포함된 웹 서버로 요청을 보낼 수 있어야 합니다.

보호되는 리소스에 액세스하는 데 사용되는 웹 브라우저가 다음 요구 사항을 충족해야 합니다.

- IDN(다국어 도메인 이름)을 지원할 수 있어야 합니다.
- IRI(다국어 리소스 식별자)를 지원할 수 있어야 합니다.
- UTF-8 형식으로 요청을 보낼 수 있어야 합니다.

MBCS URL 에 대한 웹 서버 요구 사항

다음 요구 사항 중 하나 이상을 충족하는 웹 서버에서는 MBCS URL 을 지원할 수 있습니다.

- UTF-8 요청을 사용하는 언어의 문자 집합 인코딩으로 변환할 수 있습니다.
또는
- 파일을 UTF-8 형식으로 저장할 수 있습니다. 그러면 웹 서버가 웹 브라우저로부터 UTF-8 형식의 IRI 요청을 받을 때 해당 형식의 파일을 제공할 수 있습니다.

멀티바이트 문자 지원이 사용되도록 설정

MBCS 를 지원하려면 웹 에이전트 구성 개체에서 특정 상위 비트 ASCII 문자 값을 제거해야 합니다.

참고: 상위 비트 ASCII 문자를 제거하면 웹 에이전트가 특정 문자를 차단할 수 없게 됩니다.

MBCS 지원이 사용되도록 설정하려면

1. 관리 UI 를 엽니다.
2. "인프라", "에이전트"를 차례로 클릭합니다.
3. "에이전트 구성", "에이전트 구성 수정"을 차례로 클릭합니다.
"에이전트 구성 수정" 창이 나타납니다.
4. 검색 조건을 입력하고 "검색"을 클릭합니다.
검색 조건과 일치하는 에이전트 구성 개체가 표시됩니다.

5. 원하는 에이전트 구성 개체를 선택하고 "선택"을 클릭합니다.
"매개 변수" 그룹 상자에 에이전트 구성 매개 변수의 목록이 표시됩니다.
6. "BadURLChars"의 "편집" 아이콘을 클릭합니다.
"매개 변수 편집" 창이 나타납니다.
7. "값" 필드에서 다음 값을 제거합니다.
 - %00-%1f
 - %7f-%ff
8. "확인"을 클릭합니다.
"BadURLChars" 필드에 편집한 값이 나타납니다.
9. "제출"을 클릭합니다.
웹 에이전트 구성 개체가 **MBCS URL** 을 지원하도록 구성됩니다.

MBCS URL 로 리소스 보호

MBCS URL 이 지원되면 SiteMinder 에서는 비 ASCII 문자가 포함된 URL 을 통해 액세스되는 리소스를 보호할 수 있습니다.

영역 및 관련된 리소스 보호 규칙을 생성할 때 "리소스" 필드에 **MBCS URL** 을 입력할 수 있습니다. 사용자는 IDN 과 IRI 를 지원하는 브라우저를 사용하여 보호되는 리소스에 액세스할 수 있습니다.

참고: 영역 및 규칙 생성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

MBCS URL 을 지원하는 인증 체계

다음 인증 체계는 "서버 이름" 필드에 IDN 을 사용하고 "대상" 필드에 IRI 를 사용하여 구성할 수 있습니다.

- SSL 을 통한 기본 인증
- HTML 양식 템플릿
- SSL 을 통한 HTML 양식 템플릿
- X509 클라이언트 인증서
- X509 클라이언트 인증서 및 양식

참고: Netscape 와 Firefox 에서는 IDN 이 포함된 URL 로의 리디렉션이 허용되지 않습니다. 양식 관련 인증 체계의 경우 Punycode <http://en.wikipedia.org/wiki/Punycode> 가 사용되지 않을 때 IDN 을 입력하면 오류가 발생합니다. 인증 체계 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

다국어 문자를 지원하는 SiteMinder 데이터 저장소 구성

SQL Server 또는 Oracle 데이터베이스에 SiteMinder 데이터 저장소를 구성할 수 있습니다. 이러한 데이터 저장소를 구성할 경우 정책 서버가 UTF-8 인코딩만 지원하는지, 즉 이 인코딩 유형을 지원하는 데이터베이스를 사용해야 하는지 확인해야 합니다.

참고: 이 단원의 내용은 관계형 데이터베이스에 SiteMinder 데이터 저장소를 구성할 경우에만 적용됩니다. LDAP 서버에 데이터 저장소를 구성하는 방법에 대한 자세한 내용은 "LDAP 디렉터리 서버를 정책 또는 키 저장소로 구성"을 참조하십시오.

SQL Server 에 다국어 SiteMinder 데이터 저장소 구성

정책, 키, 세션 또는 키 저장소를 생성하려면 SQL Server 데이터베이스에 SiteMinder 데이터 저장소를 구성하십시오.

참고: SQL Server 는 기본적으로 UTF-8 문자 인코딩을 지원합니다.

Oracle 에 다국어 SiteMinder 데이터 저장소 구성

Oracle 에 다국어 SiteMinder 데이터 저장소를 구성하려면

1. Oracle 이 설치된 컴퓨터에서 UTF-8 문자 인코딩을 지원하는 사용자 지정 Oracle 데이터베이스를 생성합니다.

참고: 자세한 내용과 지침은 Oracle 설명서를 참조하십시오.

기존 Oracle 데이터베이스가 UTF-8 문자 인코딩을 지원하는지 확인하려면 다음 쿼리를 실행합니다.

```
Select * from nls_database_parameters where parameter =  
'NLS_CHARACTERSET'
```

2. Oracle 데이터베이스에 SiteMinder 데이터 저장소를 구성하여 정책 서버에서 사용할 정책, 키, 세션 또는 키 저장소를 생성하십시오.

Oracle 데이터베이스에 UTF-8 문자를 로깅하는 Solaris/LINUX Red Hat 정책 서버

Solaris/LINUX Red Hat 정책 서버에서 Oracle 감사 로그 데이터베이스에 UTF-8 문자를 로깅할 수 있습니다. 이 구성을 사용하려면 다음 환경 변수를 설정해야 합니다.

중국어 간체 운영 체제의 경우

- LANG=zh_CN.utf8

일본어 운영 체제의 경우

- LANG=jp_JP.UTF-8

LANG 변수는 시스템 수준에서 설정하거나 정책 서버 프로세스에 대해서만 설정할 수 있습니다.

참고: 다른 응용 프로그램에 영향을 주지 않으려면 정책 서버 프로세스에 대해서만 이 변수를 설정해야 합니다.

데이터베이스 드라이버 변수

- IANAAppCodePage=utf-8

<policy_server_installation>/db 에 설치된 system_odbc.ini 파일의 적절한 데이터 원본 정의 섹션에서 이 변수를 설정합니다.

Oracle 클라이언트 설정

정책 서버는 Oracle 유선 프로토콜 드라이버를 사용하므로 Oracle 클라이언트가 필요하지 않습니다. 그러나 사용 환경에서 감사 로그 데이터베이스의 데이터를 읽기 위해 Oracle SQLPLUS 클라이언트가 필요한 경우에는 다음 환경 변수 중 하나 또는 둘 모두를 설정하여 멀티바이트 문자를 올바르게 표시해야 합니다.

중국어 간체 운영 체제의 경우

- LANG=zh_CN.utf8

일본어 운영 체제의 경우

- LANG=jp_JP.UTF-8

Oracle SQLPlus 클라이언트의 경우

- NLS_LANG(예: NLS_LANG=Japanese_Japan.UTF8)

참고: 자세한 내용은 운영 체제 및 데이터베이스 클라이언트의 구성 매뉴얼을 참조하십시오.

SQL Server 에서 유니코드를 지원하는 사용자 저장소 구성

정책 서버와 함께 설치된 smsampleusers_sqlserver.sql 파일을 사용하여 SQL Server 데이터베이스에 사용자 저장소를 구성할 수 있습니다. 이 파일은 *siteminder_installation\db\SQL 디렉터리*에 설치되어 있습니다.

참고: 사용자 저장소는 UTF-8 형식으로 제한되지 않습니다. 따라서 사용하는 언어의 문자 집합 인코딩으로 사용자 저장소를 생성할 수 있습니다.

다음 단계를 수행하십시오.

1. 다음을 수행하여 smsampleusers_sqlserver.sql 파일을 편집합니다.
 - a. 모든 varchar 를 **nvarchar** 로 바꿉니다.
 - b. 다국어 문자열이 있는 모든 insert 문 앞에 **N** 을 추가합니다.

일본어 예:

```
insert into SmUser ( UserID , Name, Password,
                    LastName, FirstName, ...)
values (12, N'やまもと',
        'siteminder','guest','guest','guest@mycompany.com...')
```

1. smsampleusers_sqlserver.sql 파일을 가져옵니다.

참고: smsampleusers_sqlserver.sql 파일 가져오기에 대한 자세한 내용은 "샘플 사용자 디렉터리"를 참조하십시오.

2. 정책 서버 사용자 인터페이스의 "SiteMinder ODBC 쿼리 체계" 대화 상자를 열고 **=%s** 문에 있는 모든 **%s** 참조 앞에 **N** 을 추가하여 정책 저장소의 SQL 쿼리 체계를 수정합니다.

예:

다음과 같은 샘플 쿼리 체계 문이 있을 경우

```
select Name, 'User' from SmUser where Name = '%s' Union select Name,
'Group' from SmGroup where Name = '%s'
```

다음과 같이 수정합니다.

```
select Name, 'User' from SmUser where Name = N'%s' Union select Name,
'Group' from SmGroup where Name = N'%s'
```


1. 정책 서버를 중지했다가 다시 시작합니다.

사용자 저장소 구성이 완료되었으므로 이제 멀티바이트 문자가 지원됩니다.

Oracle 에 일본어 사용자 저장소 구성

정책 서버와 함께 설치된 `smsampleusers_oracle.sql` 파일을 사용하여 Oracle 데이터베이스에 사용자 저장소를 구성할 수 있습니다. 이 파일은 `<siteminder_installation>\db\SQL` 디렉터리에 설치되어 있습니다.

참고: 사용자 저장소는 UTF-8 형식으로 제한되지 않습니다. 따라서 사용하는 언어의 문자 집합 인코딩으로 사용자 저장소를 생성할 수 있습니다.

Oracle 에 일본어 사용자 저장소를 구성하려면

1. Oracle 의 UTF-8 NLS_CHARACTERSET 인코딩을 지원하는 사용자 데이터용 데이터베이스를 생성합니다.
2. Oracle 의 SQL-Plus 를 사용하여 `smsampleusers_oracle.sql` 파일을 가져옵니다.

참고: `smsampleusers_oracle.sql` 파일 가져오기에 대한 자세한 내용은 "샘플 사용자 디렉터리"를 참조하십시오. 일본어 문자를 삽입하려는 경우 일본어 운영 체제에서 파일을 가져와야 합니다.

사용자 저장소 구성이 완료되었습니다.

부록 B: 수정된 환경 변수

이 섹션은 다음 항목을 포함하고 있습니다.

[수정된 Windows 환경 변수](#) (페이지 663)

[수정된 UNIX 환경 변수](#) (페이지 664)

수정된 Windows 환경 변수

정책 서버

Windows 환경에 정책 서버를 설치하면 다음 환경 변수가 추가 및 수정됩니다.

- NETE_PS_ROOT = \$INSTALL_PATH\$
- NETE_PS_PATH = \$INSTALL_PATH\$/\$bin;
\$INSTALL_PATH\$/\$bin/\$thirdparty;\$INSTALL_PATH\$/\$lib
- NETEGRITY_LICENSE_FILE = %NETE_PS_ROOT%/\$license/\$license.dat
- NETE_JVM_OPTION_FILE = %NETE_PS_ROOT%/\$config/\$JVMOptions.txt
- NETE_DOC_ROOT=\$INSTALL_PATH\$/\$netegrity_documents
- NETE_PS_OPACK="INSTALLED"
- NETE_JRE_ROOT = HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Runtime Environment\1.7 (JAVAHOME 값)
- NETE_JAVA_PATH=%NETE_JRE_ROOT%/\$bin;%NETE_JRE_ROOT%/\$bin/\$server
- NETE_JDK_ROOT = HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Development Kit\1.7 (JAVAHOME 값)
- NETE_SHORTCUTS = C:\Documents and Settings\All Users\Start Menu\Programs\SiteMinder

참고: 이것이 기본 위치입니다.

관리 UI

관리 UI 를 설치할 때는 Windows 환경에 환경 변수가 추가되지 않습니다.

보고서 서버

Windows 환경에 보고서 서버를 설치하면 다음 환경 변수가 추가 및 수정됩니다.

- IAM_RPTSRV_HOME=\$REPORT_SERVER_LOC\$
- BOE_SSL_JVMOPTIONS="-Dcom.ca.rptsrv.home=%IAM_RPTSRV_HOME%
-Djava.library.path=%IAM_RPTSRV_HOME%/external/bin"

수정된 UNIX 환경 변수

정책 서버

UNIX 환경에 정책 서버를 설치하면 다음 환경 변수가 추가 및 수정됩니다.

- NETE_PS_ROOT = \$INSTALL_PATH\$
- NETE_PS_PATH = \$INSTALL_PATH\$\$/bin;
\$INSTALL_PATH\$\$/bin\$/thirdparty;\$INSTALL_PATH\$\$/lib
- NETEGRITY_LICENSE_FILE = %NETE_PS_ROOT%\$/license\$/license.dat
- NETE_JVM_OPTION_FILE = %NETE_PS_ROOT%\$/config\$/JVMOptions.txt
- NETE_DOC_ROOT=\$INSTALL_PATH\$\$/netegrity_documents
- NETE_PS_OPACK="INSTALLED"
- NETE_JDK_ROOT = \$JDK_PATH\$
- NETE_JRE_ROOT = \$JRE_PATH\$
- NETE_JAVA_PATH=%NETE_JRE_ROOT%\$/bin;%NETE_JRE_ROOT%\$/bin\$/
\$server

관리 UI

관리 UI 를 설치할 때는 UNIX 환경에 환경 변수가 추가되지 않습니다.

보고서 서버

UNIX 환경에 보고서 서버를 설치하면 다음 환경 변수가 추가 및 수정됩니다.

- IAM_RPTSRV_HOME=\$REPORT_SERVER_LOC\$
- BOE_SSL_JVMOPTIONS="-Dcom.ca.rptsrv.home=\$IAM_RPTSRV_HOME
-Djava.library.path=\$IAM_RPTSRV_HOME%/external/bin"