



Sun Java™ System

Identity Synchronization for Windows 1

설치 및 구성 설명서

2004Q3

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

부품 번호 : 817-7847

Copyright © 2004 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. 는 이 설명서에서 설명한 제품에 포함된 기술에 관련된 지적재산권을 보유합니다. 특히 이 지적재산권에는 <http://www.sun.com/patents> 의 목록에 나열된 미국 특허권을 하나 이상 포함하며 미국 및 기타 국가에서 하나 이상의 추가 특허 또는 특허 출원 신청을 포함합니다.

이 제품에는 Sun Microsystems, Inc. 의 비밀 정보 및 거래 비밀이 포함됩니다. Sun Microsystems, Inc. 의 사전 서면 허가 없이 사용, 공개 또는 재생산할 수 없습니다.

U.S. Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

이 배포에는 다른 업체가 개발한 자료가 포함될 수 있습니다.

이 제품의 일부는 University of California 에서 라이선스된 Berkeley BSD 시스템에서 유도되었습니다. UNIX 는 미국 및 기타 국가에서 등록된 등록상표이며 X/Open Company, Ltd 를 통하여 배타적으로 라이선스되었습니다.

Sun, Sun Microsystems, Sun 로고, Java, Solaris, JDK, Java Naming 및 Directory Interface, JavaMail, JavaHelp, J2SE, iPlanet, Duke 로고, Java Coffee Cup 로고, Solaris 로고, SunTone Certified 로고 및 Sun ONE 로고는 미국 및 기타 국가에서 Sun Microsystems, Inc. 의 상표 또는 등록상표입니다.

모든 SPARC 상표는 라이선스되었으며 미국 및 기타 국가에서 등록된 SPARC International, Inc. 의 상표 또는 등록상표입니다. SPARC 상표가 포함된 제품은 Sun Microsystems, Inc. 가 개발한 아키텍처에 기반합니다.

Legato 및 Legato 로고는 Legato Systems, Inc. 의 등록상표이며, Legato NetWorker 는 Legato Systems, Inc. 의 상표 또는 등록상표입니다. Netscape Communications Corp 로고는 Netscape Communications Corporation 의 상표 또는 등록상표입니다.

OPEN LOOK 및 Sun(TM) 그래픽 사용자 인터페이스는 Sun Microsystems, Inc. 에 의하여 해당 사용자 및 라이선스 보유자용으로 개발되었습니다. Sun 은 컴퓨터 업계를 위하여 시각적 또는 그래픽 사용자 인터페이스에 대한 연구 및 개발에 있어 Xerox 의 노력을 인지합니다. Sun 은 Xerox 로부터 Xerox 그래픽 사용자 인터페이스에 대한 비배타적인 라이선스를 보유하고 있으며, 이에 따라 Sun 의 OPEN LOOK GUI 에 대한 라이선스가 보장되며 기타 Sun 의 서면 라이선스 동의서를 준수합니다.

이 서비스 설명서에 포함된 제품 및 정보는 미국 수출법 및 기타 국가의 수출/입 관련 법률의 규제 대상입니다. 직접 또는 간접에 상관 없이 핵, 미사일, 생화학적 병기 또는 핵합성 등의 최종 사용 또는 최종 사용자는 엄격히 금지됩니다. 미국의 봉쇄 대상 국가 또는 거부 인물 또는 특별 지정 국가 목록을 포함하여 미국 수출 제의 목록에 기재된 국가에 대한 수출 또는 재수출은 엄격히 금지됩니다.

문서는 "수정 없이" 제공되며 상품성, 특정 용도에 대한 적합성 또는 암시 또는 비침해성에 대한 암시된 조건, 프레젠테이션 및 보장에 대하여 책임지지 않습니다. 단, 해당 면책 조항이 법적으로 불법인 경우는 제외합니다.

목차

그림 목록	9
표 목록	13
서문	15
활자체 규약	19
기호	19
대표키	20
기본 경로 및 파일 이름	20
이 설명서 세트의 구성	21
기타 설명서	21
온라인 Sun 리소스 사용	22
Sun 기술 지원 연락 방법	22
관련 다른 업체 웹 사이트 참조	23
귀사의 의견을 환영합니다	23
제 I 부 설치 및 구성	25
1 장 제품 이해	27
제품 기능	28
시스템 구성요소	29
WatchDog 프로세스	30
코어	30
구성 디렉토리	30
콘솔	31
명령줄 유틸리티	31
시스템 관리자	32
중앙 기록기	32
커벡터	33

커넥터 하위 구성요소	33
Directory Server 플러그인	34
Windows NT 커넥터 하위 구성요소	34
Message Queue	35
시스템 구성요소 배포	36
코어	36
Directory Server 커넥터 및 플러그인	36
Active Directory 커넥터	37
Windows NT 커넥터 및 하위 구성요소	38
Identity Synchronization for Windows 가 디렉토리 소스에서 변경을 검출하는 방법	39
Directory Server 커넥터가 변경을 검출하는 방법	39
Active Directory 커넥터가 변경을 검출하는 방법	40
Windows NT 커넥터가 변경을 검출하는 방법	41
비밀번호 업데이트 전달	42
비밀번호 필터 DLL 을 사용하여 일반 텍스트 비밀번호 가져오기	42
요청시 비밀번호 동기화를 사용하여 일반 텍스트 비밀번호 가져오기	42
신뢰할 수 있는 동기화	45
구현 예제 : 컴퓨터가 두 대인 구성	46
물리적 구현	48
구성요소 배포	49

2 장 설치 준비 51

설치 요구 사항	51
운영 체제 요구 사항	52
하드웨어 요구 사항	53
Sun Java System 소프트웨어 요구 사항	53
설치 자격 증명	54
설치 개요	55
코어 설치	57
제품 구성	58
Directory Server 준비	58
커넥터 및 Directory Server 플러그인 설치	58
기존 사용자 동기화	59
구성 개요	60
디렉토리	60
구성 디렉토리 및 전역 카탈로그	61
동기화 설정	61
Objectclass	61
속성 및 속성 매핑	62
속성 유형	62
매개변수화 속성 기본값	63
속성 매핑	63
Synchronization User Lists	64

버전 1 2004Q3 으로 이전	64
Active Directory 와 비밀번호 동기화	65
비밀번호 정책 실행	66
개요	67
중요 참고 내용	67
비밀번호 정책 예	71
오류 메시지	72
SSL 작업용으로 Windows 구성	73
설치 및 구성 결정	73
코어 설치	73
코어 구성	74
커넥터 및 Directory Server 플러그인 설치	75
명령줄 유틸리티 사용	76
설치 점검 목록	77

3 장 코어 설치	81
시작하기 전에	81
설치 프로그램 시작	82
Solaris SPARC	83
Solaris x86	83
Windows	84
코어 설치	85

4 장 코어 자원 구성	95
구성 개요	95
Identity Synchronization for Windows 콘솔 열기	96
디렉토리 소스 작성	101
Sun Java System 디렉토리 소스 작성	102
Directory Server 준비	109
Active Directory 소스 작성	113
Windows NT SAM 디렉토리 소스 작성	122
디렉토리 소스 삭제	124
사용자 속성 선택 및 매핑	125
속성 선택 및 매핑	125
매개변수화 속성 기본값 생성	127
스키마 소스 변경	128
시스템간 사용자 속성 전달	131
객체 작성 흐름 방법 지정	131
새 생성 속성 지정	134
기존 속성 편집	136
속성 제거	137
객체 수정 내용 흐름 방식 지정	137

방향 지정	138
객체 활성화 및 비활성화 구성 및 동기화	139
삭제 내용 흐름 방식 지정	147
Synchronization User Lists 작성	148
구성 저장	154

5 장 커넥터 및 Directory Server 플러그인 설치	157
시작하기 전에	157
설치 프로그램 실행	158
커넥터 설치	160
Directory Server 커넥터 설치	160
Active Directory 커넥터 설치	166
Windows NT 커넥터 설치	170
Directory Server 플러그인 설치	171

6 장 기존 사용자 동기화	175
idsync resync 사용	176
사용자 재동기화	177
사용자 연결	178
idsync resync 인수	179
중앙 로그에서 결과 확인	182
동기화 시작 및 정지	182
서비스 시작 및 정지	183

7 장 Identity Synchronization for Windows 1 2004Q3 으로 마이그레이션	185
개요	186
이전하기 전에	186
마이그레이션 준비	187
버전 1.0 구성 내보내기	188
export10cnf 유틸리티 사용	188
일반 텍스트 비밀번호 암호 삽입	189
예제 내보내기 구성 파일	190
전달되지 않은 메시지 확인	194
checktopics 유틸리티 사용	194
메시지 비우기	196
Windows NT 에서 비밀번호 강제 변경	196
시스템 이전	197
마이그레이션 준비	199
Identity Synchronization for Windows 제거	202
종속 제품 설치 또는 업그레이드	204
Identity Synchronization for Windows 1 2004Q3 설치	204
1.0 제거에 실패한 경우의 작업 방법	206

Solaris 에서 1.0 코어 및 인스턴스 직접 제거	207
Windows 2000 에서 1.0 코어 및 인스턴스 직접 제거	213
Windows NT 에서 1.0 인스턴스 직접 제거	218
기타 이전 시나리오	222
복수 마스터 복제 구현	223
Windows NT 를 포함하는 복수 호스트 구현	225
로그 확인	229

8 장 소프트웨어 제거 231

제거 계획	231
소프트웨어 제거	232
Directory Server 플러그인 제거	233
커넥터 제거	234
코어 제거	236
콘솔 수동 제거	238
Solaris 시스템	239
Windows 시스템	239

9 장 문제해결 241

문제해결 점검 목록	242
커넥터 문제 해결	245
디렉토리 소스를 관리하는 커넥터의 ID 를 확인하는 방법	246
중앙 로그 사용	246
idsync printstat 사용	246
커넥터의 현재 상태 확인 방법	247
커넥터의 상태가 UNINSTALLED 인 경우의 작업	248
커넥터 설치가 실패했으나 다시 설치할 수 없는 경우의 작업	248
커넥터의 상태가 INSTALLED 인 경우의 작업	248
커넥터의 상태가 READY 인 경우의 작업	248
커넥터의 상태가 SYNCING 인 경우의 작업	248
Active Directory 커넥터가 SSL 을 통하여 Active Directory 에 연결할 수 없는 경우의 작업	249
구성요소 문제해결	249
Solaris	249
Windows	251
WatchList.properties 검사	251
하위 구성요소 문제 해결	252
Message Queue 문제 해결	254
브로커 구성 디렉토리 통신 문제 해결	255
브로커 메모리 설정 문제 해결	256
SSL 문제 해결	257
코어 구성요소 사이의 SSL	258
커넥터와 Directory Server 또는 Active Directory 사이의 SSL	258

신뢰되지 않은 인증서	259
일치되지 않는 호스트이름	260
만료된 자격 증명	261
Directory Server 플러그인과 Active Directory 사이의 SSL	262
제어기 문제 해결	262
10 장 감사 및 오류 파일 이해	263
로그 이해	263
Log Types	265
중앙 로그	265
로컬 구성요소 로그	266
로컬 Windows NT 하위 구성요소 로그	266
Directory Server 플러그인 로그	267
로그 읽기	268
로그 파일 구성	269
디렉토리 소스 상태 보기	271
설치 및 구성 상태 보기	272
감사 및 오류 로그 보기	273
Windows NT 컴퓨터에서 감사 사용 설정	274
11 장 보안 구성	277
보안 개요	277
구성 비밀번호 지정	278
SSL 사용	279
신뢰된 SSL 인증서 필요	279
생성된 3DES 키	280
SSL 및 3DES 키 보호 요약	280
Message Queue 액세스 제어	281
디렉토리 자격 증명	282
영구 스토리지 보호 요약	282
보안 강화	283
구성 비밀번호	284
구성 디렉토리 자격 증명 생성	284
Message Queue 클라이언트 인증서 유효성 검사	285
Message Queue 자체 서명 SSL 인증서	285
Message Queue 브로커 액세스	285
제품의 구성 디렉토리 인증서 유효성 검사	286
구성 디렉토리에 대한 액세스 제한	286
복제된 구성 보안	286
idsync certinfo 사용	289
인수	289
사용법	290

Directory Server 에서 SSL 사용	290
디렉토리 서버 인증서 데이터베이스에서 CA 인증서 불러오기	293
Active Directory 커넥터에서 SSL 사용	293
Active Directory 인증서 불러오기	294
Windows certutil 사용	294
LDAP 사용	294
커넥터의 인증서 데이터베이스에 Active Directory 인증서 추가	295
Directory Server 로 Active Directory 인증서 추가	296
Directory Server 커넥터에 Directory Server 인증서 추가	297

제 II 부 부록 299

부록 A Identity Synchronization for Windows 명령줄 유틸리티 사용	301
공통 기능	302
공통 인수	302
비밀번호 입력	305
도움말 열기	305
idsync 명령 사용	306
certinfo 사용	307
changepw 사용	308
importcnf 사용	309
prepds 사용	310
printstat 사용	314
resetconn 사용	315
resync 사용	316
startsync 사용	318
stopsync 사용	319
forcepwchg 마이그레이션 유틸리티 사용	321
부록 B LinkUsers XML 문서 예제	323
예제 1: linkusers-simple.cfg	324
예제 2: linkusers.cfg	325
부록 C Solaris 에서 루트가 아닌 사용자로 서비스 실행	329
부록 D Synchronization User List 정의 및 구성	331
Synchronization User Lists 정의 이해	331
복수 Windows 도메인 구성	333

부록 E 복제 환경용 설치 노트	337
복제본 구성	338
SSL 을 통한 복제본 구성	340
MMR 환경에서 Identity Synchronization for Windows 구성	341
 용어	 343
 색인	 355

그림 목록

그림 1-1)	시스템 구성요소	29
그림 1-2)	Directory Server 및 Active Directory 구성요소 배포	37
그림 1-3)	Directory Server 및 NT 구성요소 배포	38
그림 1-4)	Directory Server 커넥터가 변경을 검출하는 방법	40
그림 1-5)	Active Directory 커넥터가 변경을 검출하는 방법	41
그림 1-6)	Windows NT 커넥터가 변경을 검출하는 방법	41
그림 1-7)	요청시 비밀번호 동기화 - 제 1 부	43
그림 1-8)	요청시 비밀번호 동기화 - 제 2 부	44
그림 1-9)	동기화 요구 사항	47
그림 1-10)	Directory Server 및 Active Directory 시나리오	48
그림 2-1)	단일 호스트 구현에서 설치	56
그림 2-2)	Identity Synchronization for Windows To Do 목록	57
그림 3-1)	구성 디렉토리 위치 지정	86
그림 3-2)	Administrator 의 자격 증명 지정	87
그림 3-3)	구성 비밀번호 지정	88
그림 3-4)	Java Home 디렉토리 지정	89
그림 3-5)	설치 디렉토리 지정	89
그림 3-6)	Message Queue 구성	90
그림 3-7)	Identity Synchronization for Windows To Do 목록	92
그림 3-8)	콘솔 시작	92
그림 3-9)	콘솔로 로그인	93
그림 4-1)	구현에 대하여 코어 자원 구성	96
그림 4-2)	Sun Java System 서버 콘솔	97
그림 4-3)	Server Group 확장	97

그림 4-4)	Identity Synchronization for Windows 정보 패널	98
그림 4-5)	Identity Synchronization for Windows 콘솔 : Tasks 탭	99
그림 4-6)	Identity Synchronization for Windows 콘솔 : Configuration 탭	100
그림 4-7)	Directory Sources 패널 사용	101
그림 4-8)	루트 접미어 선택	103
그림 4-9)	새 구성 디렉토리 선택	104
그림 4-10)	기본 서버 지정	106
그림 4-11)	보조 서버 지정	107
그림 4-12)	고급 보안 옵션 지정	108
그림 4-13)	디렉토리 관리자 자격 증명 입력	110
그림 4-14)	준비 구성 지정	111
그림 4-15)	Sun Directory Source 패널	112
그림 4-16)	Windows Global Catalog	114
그림 4-17)	Define an Active Directory Source 마법사	115
그림 4-18)	새 전역 카탈로그 지정	116
그림 4-19)	이 Active Directory 소스용 자격 증명 지정	117
그림 4-20)	도메인 제어기 지정	118
그림 4-21)	페일오버 제어기 지정	119
그림 4-22)	고급 보안 옵션 지정	120
그림 4-23)	Active Directory Source 패널	121
그림 4-24)	디렉토리 소스 패널	122
그림 4-25)	Windows NT SAM 도메인 이름 지정	122
그림 4-26)	기본 도메인 제어기의 이름 지정	123
그림 4-27)	Windows NT SAM Directory Source 패널	123
그림 4-28)	Synchronization User List 삭제	124
그림 4-29)	Attributes 탭	126
그림 4-30)	중요 속성 매핑 정의	126
그림 4-31)	속성 동기화 완료 표	127
그림 4-32)	스키마 소스 선택	128
그림 4-33)	구조적 및 보조 객체 클래스 선택	130
그림 4-34)	작성 선택 및 전달	132
그림 4-35)	생성 속성 매핑 및 값 : Directory Server 에서 Windows 로	133
그림 4-36)	생성 속성 매핑 및 값 : Windows 에서 Directory Server 로	133
그림 4-37)	생성 속성 매핑 및 값 정의	134
그림 4-38)	새 Active Directory 속성 선택	135
그림 4-39)	생성 속성에 복수 값 지정	135
그림 4-40)	Directory Server 속성 매핑	136

그림 4-41)	완료된 생성 속성 및 매핑 표	136
그림 4-42)	Attribute Modification 탭	138
그림 4-43)	객체 활성화 및 비활성화 동기화	139
그림 4-44)	활성화 및 비활성화를 위한 사용자 정의 방법 구성	143
그림 4-45)	상태 선택	145
그림 4-46)	예 : 완료된 대화 상자	147
그림 4-47)	사용자 항목 삭제 전달	148
그림 4-48)	새 Synchronization User List 작성	149
그림 4-49)	SUL 의 이름 지정	150
그림 4-50)	Windows Criteria 지정	150
그림 4-51)	기본 DN 선택	151
그림 4-52)	Directory Server 기준 지정	153
그림 4-53)	Synchronization List 패널	154
그림 4-54)	Configuration Validity Status 창	155
그림 4-55)	커넥터 설치 방법	156
그림 5-1)	Directory Server 커넥터 선택	161
그림 5-2)	Directory Server 커넥터 자격 증명 입력	162
그림 5-3)	커넥터 로컬 호스트 및 포트를 지정합니다.	163
그림 5-4)	Ready to Install 창	163
그림 5-5)	구성 경고 대화 상자	164
그림 5-6)	To Do 목록	165
그림 5-7)	커넥터 선택	166
그림 5-8)	Active Directory Connector 선택	167
그림 5-9)	Ready to Install 창	167
그림 5-10)	To Do 목록	169
그림 5-11)	Directory Server 플러그인 선택	172
그림 5-12)	Directory Server URL 및 자격 증명 지정	172
그림 5-13)	Directory Server 다시 시작 프롬프트	173
그림 6-1)	동기화 시작 및 중지	183
그림 7-1)	단일 호스트 구현 이전	198
그림 7-2)	MMR(Multi-Master Replication) 구현 이전	225
그림 7-3)	Windows NT 를 포함하는 복수 호스트 마이그레이션	228
그림 10-1)	Status 탭	264
그림 10-2)	로그 파일 구성	269
그림 10-3)	디렉토리 소스 상태	271
그림 10-4)	To Do 목록 보기	273
그림 10-5)	로그 보기	274

그림 11-1)	Identity Synchronization for Windows 보안 개요	281
그림 11-2)	복제된 구성	288

표 목록

표 1)	활자체 규약	19
표 2)	기호 규약	19
표 3)	기본 경로 및 파일 이름	20
표 4)	이 설명서 세트의 구성	21
표 2-1)	Solaris 요구 사항	52
표 2-2)	Windows 요구 사항	52
표 2-3)	레이블 이름 지정 형식	59
표 2-4)	비밀번호 정책이 동기화 작동에 영향을 미치는 방식	70
표 2-5)	비밀번호 정책이 재동기화 작동에 영향을 미치는 방식	71
표 2-6)	코어 설치 점검 목록	77
표 2-7)	코어 구성 점검 목록	77
표 2-8)	커넥터 및 Directory Server 플러그인 설치 점검 목록	78
표 2-9)	사용자 연결 점검 목록	78
표 2-10)	재동기화 점검 목록	79
표 4-1)	Directory Server 도구와 상호 운용	141
표 4-2)	Directory Server 의 nsAccountLock 속성 직접 수정	142
표 4-3)	활성화 및 비활성화된 상태 지정	144
표 4-4)	inetuserstatus 값을 사용하는 예제 결과	145
표 5-1)	디렉토리 소스 예제	161
표 6-1)	기존 사용자 입력 내용에 따른 설치 후 단계	176
표 6-2)	idsync resync 사용법	179
표 6-3)	idsync resync 가 Directory Server 에 있는 사용자의 비밀번호를 무효화합니까 ? ...	181
표 6-4)	idsync resync 사용법 예제	181
표 7-1)	제거할 Solaris 패키지	209

표 7-2)	MMR(Multi-Master Replication) 구현에서의 구성요소 배포	223
표 7-3)	복수 호스트 구현	227
표 9-1)	커넥터 상태 설명	247
표 9-2)	Identity Synchronization for Windows 프로세스	249
표 10-1)	Identity Synchronization for Windows 로그 종류	265
표 10-2)	로컬 로그	266
표 10-3)	로그 수준	268
표 11-1)	네트워크 보안을 사용하여 중요한 정보 보호	280
표 11-2)	영구 저장 장소 보호	282
표 11-3)	CA 인증서가 필요한 MMR 구성 구성요소	287
표 11-4)	certinfo 인수	289
표 A-1)	모든 하위 명령에 공통된 인수	303
표 A-2)	모든 하위 명령에 공통적인 SSL 관련 인수	304
표 A-3)	구성 디렉토리 인수	304
표 A-4)	idsync 하위 명령 빠른 참조	306
표 A-5)	idsync changepw 인수	308
표 A-6)	idsync importcnf <FILE>	310
표 A-7)	prepds 인수	312
표 A-8)	idsync resetconn <FILE>	316
표 A-9)	idsync resync 사용법	317
표 A-10)	idsync startsync <FILE>	319
표 A-11)	forcepwchg 인수	322
표 D-1)	SUL 정의 구성요소	332

서문

Sun Java™ System Identity Synchronization for Windows 1 2004Q3(이전 이름은 Sun™ ONE Identity Synchronization for Windows)에서는 비밀번호와 기타 지정된 사용자 속성을 Sun Java™ System Directory Server 와 기타 시스템 사이에서 교환할 수 있습니다.

이 설명서에서는 프로덕션 환경에서 Sun Java System Identity Synchronization for Windows 를 설치하고 구성하는 방법에 대하여 설명합니다.

이 릴리스 Identity Synchronization for Windows 의 새 기능과 개선 내용에 대한 최신 정보는 다음의 온라인 릴리스 노트를 참조하십시오.

<http://docs.sun.com/db/doc>

참고	이 설명서에서 묘사된 사용자 인터페이스는 제품의 이후 버전에서 변경될 수 있습니다.
-----------	--

이 서문의 내용 :

- " 대상 " 페이지 16
- " 이 책을 읽기 전에 " 페이지 16
- " 이 설명서의 구성 " 페이지 16
- " 이 설명서에서 사용된 표기 형식 " 페이지 18
- " 관련 설명서 " 페이지 20
- " 온라인 Sun 리소스 사용 " 페이지 22
- "Sun 기술 지원 연락 방법 " 페이지 22
- " 관련 다른 업체 웹 사이트 참조 " 페이지 23

- "귀사의 의견을 환영합니다." 페이지 23

대상

이 설치 및 구성 설명서의 대상은 Identity Synchronization for Windows 를 설치 및 구성하여 Sun Java™ System Directory Server 및 Windows Active Directory/NT 컴퓨터 사이에서 양방향으로 비밀번호 및 사용자 속성을 동기화하는 관리자, 시스템 엔지니어 및 전문가 서비스 엔지니어입니다.

다음의 내용을 숙지해야 합니다.

- Directory Server 및 Windows Active Directory/NT 구성 및 운영
- LDAP(Lightweight Directory Access Protocol)
- Java 기술
- XML(Extensible Markup Language)
- 공용키 암호화 및 SSL(Secure Sockets Layer) 프로토콜의 기본 개념
- 인트라넷, 엑스트라넷 및 인터넷 보안 및 엔터프라이즈 내에서의 전자 인증서의 역할에 대한 기본 개념

이 책을 읽기 전에

Sun Java System Identity Synchronization for Windows 1 2004Q3 릴리스 노트에는 이 설명서의 설명에 우선하는 내용을 포함하여 제품에 대한 최신 정보가 있습니다. 이 설명서의 절차를 사용하기 전에 릴리스 노트를 읽으십시오.

Identity Synchronization for Windows 구현에서 Sun Java System Directory Server 는 데이터 저장소의 역할을 하므로 해당 제품과 함께 제공되는 설명서를 읽어야 합니다. Directory Server 설명서는 http://docs.sun.com/coll/DirectoryServer_04q2 에서 온라인으로 확인할 수 있습니다.

이 설명서의 구성

*Sun Java System Identity Synchronization for Windows 1 2004Q3 설치 및 구성 설명서*의 내용은 다음의 장으로 구성되었습니다.

- 제 1 장, "제품 이해": 제품 기능, 시스템 구성요소, 명령줄 유틸리티, 시스템 구성요소 배포 및 구현 예제 등, Identity Synchronization for Windows 에 관련된 일부 기본 개념을 설명합니다.
- 제 2 장, "설치 준비": 설치 및 구성 과정을 설명하고 제품의 설치를 준비하는 데 도움이 될 정보를 제공합니다.
- 제 3 장, "코어 설치": Identity Synchronization for Windows 설치 프로그램을 사용하는 방법과 Identity Synchronization for Windows 코어 구성요소를 설치하는 방법에 대하여 설명합니다.
- 제 4 장, "코어 자원 구성": 콘솔을 사용하여 코어 리소스를 추가 및 구성하는 방법에 대하여 설명합니다.
- 제 5 장, "커넥터 및 Directory Server 플러그인 설치": Identity Synchronization for Windows 커넥터와 Directory Server 플러그인을 설치하는 방법에 대하여 설명합니다.
- 제 6 장, "기존 사용자 동기화": 신규 Identity Synchronization for Windows 설치에 대하여 기존 사용자를 링크하고 재동기화하는 방법에 대하여 설명합니다.
- 제 7 장, "Identity Synchronization for Windows 1 2004Q3 으로 마이그레이션": 시스템을 Sun Java System Identity Synchronization for Windows 버전 1.0 에서 버전 1 2004Q3 으로 이전하는 방법에 대하여 설명합니다.
- 제 8 장, "소프트웨어 제거": 제거 준비 방법 및 콘솔을 직접 제거하는 방법을 포함하여 Identity Synchronization for Windows 를 제거하는 방법에 대하여 설명합니다.
- 제 9 장, "문제해결": Identity Synchronization for Windows 설치에 대한 문제 해결에 사용할 수 있는 내용을 제공합니다.
- 제 10 장, "감사 및 오류 파일 이해": 로그 수준 설정 방법, 로그 파일과 디렉토리 소스 상태 보기 및 이해 등을 포함하여 감사 및 오류 로깅에 대한 내용이 제공됩니다.
- 제 11 장, "보안 구성": 보안 시스템 구성 방법에 대하여 설명합니다. 여기에는 보안 강화, 복제된 구성 보안, SSL 사용 설정 및 인증서 데이터베이스에 Active Directory CA 인증서 추가 등의 내용이 포함됩니다.
- 부록 A, "Identity Synchronization for Windows 명령줄 유틸리티 사용": Identity Synchronization for Windows 명령줄 유틸리티를 사용하여 다양한 작업을 하는 방법에 대하여 설명합니다.
- 부록 B, "LinkUsers XML 문서 예제": 환경을 사용자 정의하는 데 사용할 수 있는 예제 Linkers XML 문서 (linkusers-simple.cfg) 가 있습니다.

- [부록 C, "Solaris 에서 루트가 아닌 사용자로 서비스 실행 "](#): 루트가 아닌 사용자로 Identity Synchronization for Windows 서비스를 실행하는 방법에 대하여 설명합니다.
- [부록 D, "Synchronization User List 정의 및 구성 "](#): 동기화 사용자 목록 정의 및 복수 도메인 구성에 대한 내용이 제공됩니다.
- [부록 E, " 복제 환경용 설치 노트 "](#): MMR(Multimaster Replication) 구현을 구성하고 보안하는 데 필요한 단계를 간단히 살펴봅니다.

이 설명서에서 사용된 표기 형식

이절의 표에는 이 설명서에서 사용된 규약이 설명되어 있습니다.
규약 정보는 다음과 같은 내용으로 구성됩니다.

- [" 활자체 규약 " 페이지 19](#)
- [" 기호 " 페이지 19](#)
- [" 대표키 " 페이지 20](#)
- [" 기본 경로 및 파일 이름 " 페이지 20](#)

활자체 규약

이 설명서에서 사용한 활자체 규약은 다음 표의 설명과 같습니다.

표 1) 활자체 규약

활자체	의미	예
AaBbCc123 (고정 폭)	API 및 언어 요소 , HTML 태그 , 웹 사이트 URL , 명령 이름 , 파일 이름 , 디렉토리 경로 이름 , 화면 표시 컴퓨터 출력 , 예제 코드 .	.login 파일을 편집합니다 . 모든 파일의 목록을 표시하려면 ls -a 를 사용합니다 . % You have mail.
AaBbCc123 (고정 폭 굵은체)	사용자 입력 내용 . 화면에 표시되는 컴퓨터 출력과 대조되게 표시합니다 .	% su Password:
AaBbCc123 (기울임꼴)	책 제목 , 신규 항목 , 강조할 단어 . 실제 이름 또는 값으로 대체될 명령 또는 경로 이름의 자리 표시 .	User's Guide 의 제 6 장을 읽으십시오 . class 옵션이라고 합니다 . 파일을 저장하면 <i>안 됩니다</i> . 파일은 install-dir/bin 디렉토리에 있습니다 .

기호

이 설명서에서 사용한 기호 규약은 다음 표의 설명과 같습니다.

표 2) 기호 규약

기호	설명	예	의미
[]	선택 명령 옵션이 포함됩니다 .	ls [-l]	-l 옵션은 필수가 아닙니다 .
{ }	필요한 명령 옵션의 선택이 표시됩니다 .	-d {y n}	-d 옵션에는 사용자가 y 인수 또는 n 인수를 사용해야 합니다 .
-	동시에 누르는 복수 키 조합 .	Control-A	Control 키를 누른 채로 A 키를 누릅니다 .
+	연속으로 누르는 복수 키 조합 .	Ctrl+A+N	Control 키를 눌렀다 놓은 후 이어지는 키를 누릅니다 .
>	그래픽 사용자 인터페이스에서 메뉴 항목 선택을 표시합니다 .	File > New > Templates	File 메뉴에서 New 를 선택합니다 . New 하위 메뉴에서 Templates 를 선택합니다 .

대표키

Identity Synchronization for Windows 는 사용자 인터페이스 전체에서 **대표키**(밑줄이 있는 문자) 를 사용하여 사용자가 특정 작업을 더 빠르게 수행할 수 있도록 합니다 . 작업을 수행하려면 간단히 밑줄이 있는 문자를 누릅니다 . 대표키는 대소문자를 구분하지 않습니다 . 이 문자를 사용하려면 Alt 키를 함께 누릅니다 .

예를 들어 다음 대화 상자에서 대문자 "C" 또는 "Alt-c" 를 누르면 대화 상자가 최소화되며 대문자 "H" 또는 "Alt-h" 를 누르면 온라인 도움말 대화 상자가 표시됩니다 .

기본 경로 및 파일 이름

이 설명서에 사용하는 기본 경로와 파일 이름은 다음 표의 설명과 같습니다 .

표 3) 기본 경로 및 파일 이름

용어	설명
<serverroot>	Identity Synchronization for Windows 설치 위치의 상위 디렉토리를 나타냅니다 .
isw-<hostname>	Identity Synchronization for Windows 인스턴스 디렉토리를 표시합니다 .
<current-working-directory>/cert8.db	클라이언트 인증서 데이터베이스의 경로와 파일 이름을 나타냅니다 .
<installation_root>/isw-<machine_name>/logs/central/	Identity Synchronization for Windows 중앙 로그로의 기본 경로를 나타냅니다 .
<installation_root>/isw-<machine_name>/logs/	Identity Synchronization for Windows 로컬 로그 (시스템 관리자 , 각 커넥터 및 중앙 기록기용) 의 기본 경로를 나타냅니다 .
/usr/sfw/bin	Solaris 에서 certutil 은 기본으로 이 디렉토리 위치에 설치됩니다 .

관련 설명서

<http://docs.sun.com> 웹 사이트에서 Sun 기술 설명서를 온라인으로 사용할 수 있습니다 . 자료를 보거나 특정 제목 또는 주제로 검색할 수 있습니다 .

이 설명서 세트의 구성

Identity Synchronization for Windows 설명서 세트에 포함된 책은 다음 표에 요약된 것과 같습니다.

표 4) 이 설명서 세트의 구성

책 제목	설명
<i>Sun Java System Identity Synchronization for Windows 1 2004Q3 설치 및 구성 설명서</i> (http://docs.sun.com/doc/817-6199)	프로덕션 환경에서 Identity Synchronization for Windows 를 설치하고 구성하는 방법에 대하여 설명합니다.
<i>Sun Java System Identity Synchronization for Windows 1 2004Q3 Deployment Planning Guide</i> (http://docs.sun.com/doc/817-6200)	Identity Synchronization for Windows 를 계획하고 구현하는 일반 지침과 우수 사례를 제공합니다.
<i>Sun Java System Identity Synchronization for Windows 1 2004Q3 릴리스 노트</i> (http://docs.sun.com/doc/817-6202)	제품이 릴리스된 후 사용할 수 있습니다. 현재 릴리스의 새로운 기능에 대한 설명, 알려진 문제 및 제한, 설치 참고, 소프트웨어 또는 설명서에 대한 문제를 보고하는 방법 등을 포함하여 최신 내용이 포함됩니다.

기타 설명서

Directory Server 및 Sun Java™ System Message Queue 에서 작업하기 전에 이들 제품 설명서를 참고해야 할 경우가 있습니다. 설명서는 다음 위치에서 찾아볼 수 있습니다.

- Sun Java System Directory Server 설명서
http://docs.sun.com/coll/DirectoryServer_04q2
- Sun Java System Message Queue 설명서
<http://docs.sun.com/db/prod/2296#hic>

공용키 암호화, SSL(Secure Sockets Layer) 프로토콜, 인트라넷, 익스트라넷 및 인터넷 보안, 엔터프라이즈에서의 전자 인증서의 역할 등에 대한 기본 개념은 *Managing Servers with iPlanet Console 5.0* 설명서의 보안 관련 부록을 참조하십시오.

Windows 2003 Server 및 Windows 비밀번호 정책에 대한 내용은 다음의 Microsoft 출판물을 참조하십시오.

- *Using Secedit.exe to Force Group Policy to Be Applied Again - Windows 2000 Servers* Microsoft KB #227448
- *A Description of the Group Policy Update Utility - Windows 2003 Servers* Microsoft KB #298444

- *Microsoft Knowledge Base Article 232690*

온라인 Sun 리소스 사용

제품 다운로드, 전문가 서비스, 패치 및 지원, 추가 개발자 정보 등은 다음을 이용하십시오.

- 개발자 정보
<http://developers.sun.com/prodtech/index.html>
- 다운로드 센터
<http://www.sun.com/software/download/>
- 제품 데이터 시트
<http://www.sun.com/software/>
- 제품 설명서 온라인
<http://docs.sun.com>
- 제품 지원 및 상태
<http://www.sun.com/service/support/software/>
- 전문가 서비스
<http://www.sun.com/service/sunps/sunone/index.html>
- Sun 엔터프라이즈 서비스, Solaris 패치 및 지원
<http://sunsolve.sun.com>
- 지원 및 교육 -
<http://www.sun.com/supporttraining/>

Sun 기술 지원 연락 방법

본 제품의 제품 설명서에서 다루어지지 않고 있는 기술적 문제에 대한 의문 사항이 있을 경우 다음 사이트로 문의하시기 바랍니다.

<http://www.sun.com/service/contacting>

관련 다른 업체 웹 사이트 참조

이 책에서 참조된 다른 업체 웹 사이트는 다음과 같습니다.

- Windows 2003 용 비밀번호 정책에 대한 내용 :
http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dsscc_aut_xbby.asp
- Windows 2003 에서 비밀번호 및 그룹 정책을 적용 및 수정하는 방법 :
http://www.microsoft.com/resources/documentation/windowsserv/2003/standard/proddocs/en-us/password_grouppolicy.asp
- Microsoft Certificate Services Enterprise Root 인증 기관에 대한 내용 :
<http://support.microsoft.com/default.aspx?scid=kb;en-us;q247078>
- SSL 을 통한 LDAP 구성 방법 :
<http://support.microsoft.com/default.aspx?scid=kb;en-us;321051>

Sun 은 이 설명서에서 언급된 다른 회사 웹 사이트의 사용 가능성에 대하여 책임지지 않습니다. 해당 사이트 또는 자원을 통하여 사용 가능한 내용, 광고, 제품 또는 기타 자료에 대하여 보증하거나 책임지지 않습니다. Sun 은 해당 사이트 또는 자원을 통하여 사용 가능한 내용, 상품 또는 서비스의 사용 또는 신뢰에 관련하여 발생 또는 발생한 것으로 추정되는 실제 또는 추정 손실에 대하여 책임지지 않습니다.

귀사의 의견을 환영합니다.

Sun 은 설명서의 향상에 최선을 다하고 있으며 귀사의 의견 및 제안을 환영합니다.

의견을 공유하려면 <http://docs.sun.com> 을 방문하여 Send Comments 를 누르십시오. 온라인 양식에서 설명서 제목과 부품 번호를 입력합니다. 부품 번호는 설명서의 제목 페이지나 문서의 상단에 있으며 보통 7 자리 또는 9 자리 번호입니다.

예를 들어 이 책의 제목은 *Sun Java System Identity Synchronization for Windows 1 2004Q3 설치 및 구성 설명서*이며 부품 번호는 817-6199 입니다.

귀사의 의견을 환영합니다 .

설치 및 구성

제 1 장 , " 제품 이해 "

제 2 장 , " 설치 준비 "

제 3 장 , " 코어 설치 "

제 4 장 , " 코어 자원 구성 "

제 5 장 , " 커넥터 및 Directory Server 플러그인 설치 "

제 6 장 , " 기존 사용자 동기화 "

제 7 장 , "Identity Synchronization for Windows 1 2004Q3 으로 마이그레이션 "

제 8 장 , " 소프트웨어 제거 "

제 9 장 , " 문제해결 "

제 10 장 , " 감사 및 오류 파일 이해 "

제 11 장 , " 보안 구성 "

제품 이해

Identity Synchronization for Windows 는 Sun Java™ System Directory Server 5 2004Q2 와 다음간의 양방향 비밀번호 및 사용자 속성 동기화를 제공합니다.

- Windows 2000 또는 Windows 2003 Server Active Directory
- Windows NT SAM Registry

Identity Synchronization for Windows 동기화 이벤트 처리

- **보안** : Identity Synchronization for Windows 는 절대로 " 분명한 " 형태로 암호를 전송하지 않으며 시스템 액세스를 관리자에게로만 제한합니다 .
- **견고함** : Identity Synchronization for Windows 는 개별 구성요소가 일시적으로 사용할 수 없는 상태에서도 디렉토리를 동기화합니다 .
- **효율성** : Identity Synchronization for Windows 에서 사용하는 동기화 기법은 디렉토리 서버에 대한 부하를 최소화합니다 .

Sun Java System Identity Synchronization for Windows 버전 1 2004Q3 을 설치 (또는 마이그레이션) 하기 전에 이 장에서 설명한 개념을 숙지해야 합니다 . 이 장은 다음과 같은 절로 구성됩니다 .

- " 제품 기능 " 페이지 28
- " 시스템 구성요소 " 페이지 29
- " 시스템 구성요소 배포 " 페이지 36
- "Identity Synchronization for Windows 가 디렉토리 소스에서 변경을 검출하는 방법 " 페이지 39
- " 구현 예제 : 컴퓨터가 두 대인 구성 " 페이지 46

제품 기능

Identity Synchronization for Windows 는 다음의 기능을 제공합니다 .

- **양방향 비밀번호 동기화** : Sun Java System 디렉토리 소스와 Windows Active Directory 및 Windows NT 디렉토리 소스 사이에서 사용자 비밀번호를 동기화할 수 있습니다 .
비밀번호를 동기화하면 사용자가 로그인 인증에 이들 디렉토리 소스를 사용하는 응용 프로그램을 사용할 수 있으므로 비밀번호를 하나만 기억하면 됩니다 . 또한 주기적 비밀번호 업데이트를 적용해야 하는 경우 비밀번호를 하나의 환경에서만 업데이트하면 됩니다 .
- **양방향 사용자 속성 동기화** : 하나의 디렉토리 환경에서 선택한 속성을 생성 , 수정 및 삭제하고 해당 값을 자동으로 다른 디렉토리 환경으로 전달할 수 있습니다 .
- **양방향 사용자 계정 생성 동기화** : 하나의 디렉토리 환경에서 사용자 계정을 생성 또는 삭제하고 새 계정을 자동으로 다른 디렉토리 환경으로 전달할 수 있습니다 .
- **양방향 객체 삭제 , 활성화 및 비활성화** : Directory Server 및 Active Directory 디렉토리 소스 (Windows NT 에는 사용 불가능) 사이에서 객체 삭제 및 객체 활성화 / 비활성화의 흐름을 제어할 수 있습니다 .
- **복수 도메인 동기화** : 복수 Active Directory 및 Windows NT 도메인뿐 아니라 복수 Active Directory 포리스트에 대하여 동기화를 수행할 수 있습니다 .
- **중앙화된 시스템 감사** : 하나의 중앙화된 위치에서 설치 및 구성 상태 , 일상적인 시스템 작업 및 구현에 관련된 모든 오류 조건을 모니터링할 수 있습니다 .

Windows 디렉토리의 항목을 수정하거나 디렉토리를 사용하는 응용 프로그램을 변경할 필요가 없습니다 .

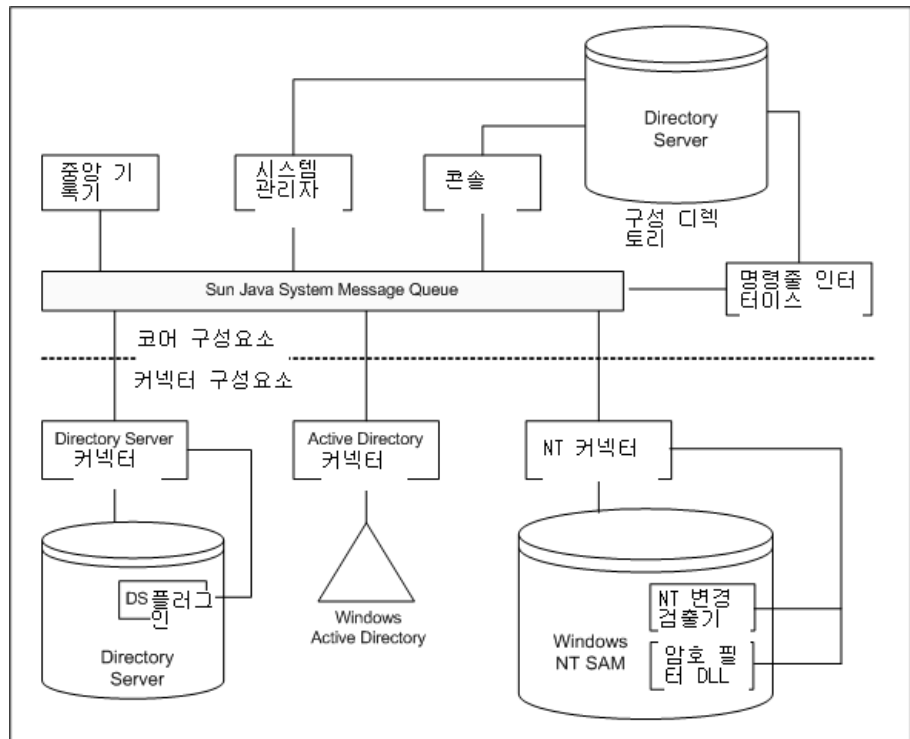
Identity Synchronization for Windows 를 사용하여 Directory Server 와 Active Directory 를 동기화하는 경우 Windows 운영 환경에 어떤 구성요소도 설치할 필요가 없습니다 .

Directory Server 와 Windows NT 를 동기화 하는 경우 반드시 제품의 NT 구성요소를 Windows NT 환경에 설치해야 합니다 .

시스템 구성요소

Identity Synchronization for Windows 는 일련의 코어 구성요소와 Sun Java System Directory Server 와 Windows 디렉토리 사이에서 비밀번호와 사용자 속성을 동기화할 수 있는 여러 개별 커넥터 및 커넥터 하위 구성요소로 구성되어 있습니다 (그림 1-1 참조).

그림 1-1) 시스템 구성요소



여기에서는 각 Identity Synchronization for Windows 구성요소를 정의 및 설명하며, 다음과 같이 구성됩니다.

- "WatchDog 프로세스" 페이지 30
- "코어" 페이지 30
- "커넥터" 페이지 33
- "커넥터 하위 구성요소" 페이지 33

WatchDog 프로세스

Watchdog 은 Identity Synchronization for Windows java 프로세스로 개별 배경 java 프로세스의 시작, 재시작 및 정지를 담당합니다. Watchdog 은 중앙 기록기, 시스템 관리자 및 커넥터를 시작하고 모니터링합니다 (그러나 하위 구성요소, Message Queue 또는 Identity Synchronization for Windows 콘솔을 모니터링하지는 않습니다).

Watchdog 은 코어를 설치하는 위치에 설치되며 Solaris 데몬 또는 Windows 서비스로 시작될 수 있습니다. (서비스의 시작 및 정지에 대한 내용은 "[서비스 시작 및 중지](#)" [페이지 183](#) 를 참조하십시오 .)

코어

Identity Synchronization for Windows 를 설치할 때 우선 코어를 설치하며, 그런 후 환경에 맞추어 구성합니다.

코어는 다음 구성요소로 구성되며, 이들 각각은 별도의 java 프로세스입니다. 각 구성요소에 대한 설명은 참조 페이지에 나와 있습니다.

- "[구성 디렉토리](#)" [페이지 30](#)
- "[콘솔](#)" [페이지 31](#)
- "[명령줄 유틸리티](#)" [페이지 31](#)
- "[시스템 관리자](#)" [페이지 32](#)
- "[중앙 기록기](#)" [페이지 32](#)

참고 Watchdog 은 코어를 설치할 때 설치되며 중앙 기록기와 시스템 관리자의 시작 및 모니터링을 담당합니다.

더 자세한 내용은 "[WatchDog 프로세스](#)" [페이지 30](#) 를 참조하십시오.

구성 디렉토리

Identity Synchronization for Windows 는 구성 데이터를 Directory Server 구성 디렉토리에 저장합니다. (프로그램이 구성 디렉토리를 설치하지는 않습니다 .)

콘솔, 시스템 관리자 및 설치 프로그램은 모두 다음을 포함하여 구성 디렉토리에서 제품의 구성 데이터를 읽고 씁니다.

- 각 구성요소 상태에 대한 설치 정보

- 모든 디렉토리, 도메인, 커넥터 및 Directory Server 플러그인의 구성 정보
- 커넥터 상태
- 사용자 생성, 사용자 삭제 및 속성 수정의 방향을 설명하는 동기화 설정
- 두 디렉토리 환경 (Active Directory 와 Directory Server 또는 Windows NT 와 Directory Server) 사이에서 동기화될 속성 및 속성 매핑
- 각 디렉토리 토폴로지의 Synchronization User List
- 로그 설정

콘솔

Identity Synchronization for Windows 는 제품의 구성요소 구성 및 관리 작업을 중앙화하는 콘솔을 제공합니다.

콘솔을 사용하여 다음 작업을 수행할 수 있습니다.

- 동기화될 디렉토리 소스 구성
- 비밀번호에 더하여 동기화될 사용자 항목 속성의 매핑 정의
- 디렉토리 또는 도메인 토폴로지에서 동기화될 (또는 동기화되지 않을) 사용자 및 속성을 지정
- 시스템 상태 모니터
- 동기화 시작 및 정지

명령줄 유틸리티

Identity Synchronization for Windows 는 또한 명령줄에서 직접 다음 작업을 수행할 수 있는 명령줄 유틸리티를 제공합니다.

- 구성 및 SSL 설정에 기반하여 인증서 정보 표시
- Identity Synchronization for Windows 구성 비밀번호 변경
- 내보내진 Identity Synchronization for Windows 버전 1.0 구성 XML 문서 가져오기
- Identity Synchronization for Windows 가 사용하도록 Sun Java System Directory Server 소스 준비
- 설치 / 구성 과정을 완료하기 위하여 반드시 수행해야 하는 단계를 표시하고 설치된 커넥터, 시스템 관리자 및 Message Queue 의 상태 표시
- 구성 디렉토리의 커넥터 상태를 *uninstalled* 로 재설정

- 설치 과정의 일부분으로 두 디렉토리의 기존 사용자를 동기화 및 링크하고 디렉토리를 미리 채움
- 동기화 시작
- 동기화 정지

제품의 명령줄 유틸리티에 대한 자세한 내용은 [부록 A, "Identity Synchronization for Windows 명령줄 유틸리티 사용."](#) 을 참조

시스템 관리자

Identity Synchronization for Windows 시스템 관리자는 다음의 작업을 하는 별도의 java 프로세스입니다.

- 제품의 백엔드 네트워크 장치를 활용하여 구성 업데이트를 동적으로 커넥터에 전달
- 각 커넥터와 모든 커넥터 하위 구성요소의 상태 유지
- 처음 두 디렉토리를 동기화하는 데 사용되는 `idsync resync` 작업 조정

중앙 기록기

커넥터가 지리적으로 분산되어 설치될 수 있으므로 모든 로깅 정보를 중앙 집중식으로 관리할 경우 관리에 있어 상당한 이점을 누릴 수 있습니다. 이렇게 함으로써 관리자는 단일 위치에서 동기화 작업을 모니터링하고 오류를 검출하며 전체 시스템의 상태를 평가할 수 있습니다.

관리자는 중앙 기록기로 다음의 작업을 할 수 있습니다.

- 시스템이 올바르게 실행되는지 확인
- 개별 구성요소 및 시스템 전체의 문제 검출 및 해결
- 개별 및 시스템 전체의 동기화 작업 감사
- 디렉토리 환경 사이의 사용자 비밀번호 동기화 추적

로그의 종류는 두 가지입니다.

- **감사 로그**에는 시스템의 일상 작동 내역에 대한 정보가 제공되며, 여기에는 디렉토리 사이에서 사용자의 비밀번호가 동기화되는 등의 중요한 이벤트가 포함됩니다. 로그 메시지에 제공되는 세부 내용을 증가 또는 감소시켜 감사 로그에 기록되는 정보의 수준을 제어할 수 있습니다.

참고

Identity Synchronization for Windows에서는 모든 오류 로그 메시지를 감사 로그에 기록하여 다른 이벤트와 쉽게 상호 관련시킬 수 있습니다.

- **오류 로그**에는 심각한 오류 또는 경고로 판단되는 정보가 제공됩니다. 모든 오류 로그는 주의해야 하므로 오류가 로그 되지 않도록 할 수는 없습니다. 오류 조건이 발생하는 경우 항상 오류 로그에 해당 내용이 기록됩니다.

커넥터

커넥터는 단일 데이터 소스 유형에서 동기화 프로세스를 관리하는 java 프로세스입니다. 커넥터는 데이터 소스에서의 사용자 변경 내용을 검출하고 이들 변경 내용을 Message Queue를 통하여 원격 커넥터에 게시합니다.

Identity Synchronization for Windows는 디렉토리에 국한된 커넥터가 디렉토리외 도메인 사이에서 양방향으로 사용자 속성과 비밀번호 업데이트를 동기화하는 다음의 디렉토리 특정 커넥터를 제공합니다.

- **Directory Server 커넥터** : Directory Server에서 단일 루트 접미어 (예 : suffix/database) 지원
- **Active Directory 커넥터** : Windows 2000 또는 Windows 2003 Server Active Directory 환경에서 단일 인스턴스를 지원합니다. 추가 도메인에 대하여 복수 커넥터를 사용할 수 있습니다.
- **Windows NT 커넥터** : Windows NT 환경에서 단일 도메인을 지원합니다.

참고

Watchdog은 커넥터를 설치한 위치에 설치되며 커넥터의 시작, 재시작 및 정지를 담당합니다. 더 자세한 내용은 "[WatchDog 프로세스](#)" [페이지 30](#)를 참조하십시오.

커넥터 하위 구성요소

하위 구성요소는 커넥터와 별도로 실행되는 경량 프로세스 또는 라이브러리입니다. 커넥터는 하위 구성요소를 사용하여 Directory Server 또는 Windows NT에 있는 암호를 캡처하는 등의 원격으로 액세스할 수 없는 원시 리소스에 액세스합니다.

다음 커넥터 하위 구성요소는 동기화되는 디렉토리와 함께 설치되며 암호화된 연결을 통하여 해당 커넥터와 통신합니다.

- ["Directory Server 플러그인 " 페이지 34](#)
- ["Windows NT 커넥터 하위 구성요소 " 페이지 34](#)

참고 Active Directory 커넥터에는 하위 구성요소가 필요 없습니다.

Directory Server 플러그인

Directory Server 플러그인은 Directory Server 커넥터의 하위 구성요소입니다. Directory Server 플러그인은 동기화되는 각 Directory Server 에 설치합니다.

이 플러그인의 용도

- Retro Changelog 에 암호화된 비밀번호를 저장하여 Directory Server 커넥터의 변경 검출 기능을 향상
- Active Directory 와 Directory Server 사이의 사용자 속성 및 비밀번호 동기화를 양방향으로 지원합니다.
(" 요청시 비밀번호 동기화를 사용하여 일반 텍스트 비밀번호 가져오기 " 페이지 42 참조)

참고 MMR(Multi-Master Replication) 환경에서 Directory Server 플러그인은 4 방향으로 작동합니다. (이전에 Identity Synchronization for Windows 는 양방향 MMR 만 지원했습니다.)

Windows NT 커넥터 하위 구성요소

설치에서 Windows NT SAM Registries 와 동기화해야 하는 경우 Identity Synchronization for Windows 설치 프로그램이 다음 기본 도메인 제어기 (PDC) 를 Windows NT 커넥터와 함께 설치합니다.

- **변경 검출기** : 보안 로그를 모니터링하여 사용자 항목과 비밀번호 변경 이벤트를 감지한 후, 변경 내용을 커넥터로 전달합니다.
- **비밀번호 필터** : NT 도메인 제어기에서 변경된 비밀번호를 캡처하고 이를 안전하게 NT 커넥터로 전달

Message Queue

Identity Synchronization for Windows 는 Message Queue(게시 / 가입 모델이 있는 일관적인 메시지 대기열 메커니즘) 를 사용하여 디렉토리 소스 사이에서 속성과 비밀번호 변경 내용을 전달하고 해당 디렉토리 소스에 대한 동기화를 관리하는 커넥터에 관리 및 구성 정보를 배포합니다 .

Message Queue 는 Java Message Service(JMS) 개방형 표준을 구현하는 엔터프라이즈 메시징 시스템입니다 . JMS 표준은 일련의 프로그래밍 인터페이스를 기술하여 java 응용 프로그램이 분산 환경에서 메시지를 작성 , 송신 , 수신 및 읽을 수 있는 공통 방법을 제공합니다 .

Message Queue 는 공통 메시지 서비스를 사용하여 메시지를 교환하는 메시지 게시자와 가입자로 구성됩니다 . 이 메시지 서비스는 하나 이상의 전용 메시지 브로커로 구성되며 , 브로커는 메시지 대기열에 대한 액세스 제어 , 사용 중인 게시자 및 가입자에 대한 정보 유지 , 메시지 전달 확인 등의 기능을 담당합니다 .

Message Queue 는 다음과 같은 이유로 인해 최상의 방법론이라고 할 수 있습니다 .

- 커넥터 사이에 신뢰 시스템 구축
- 모든 구성요소에 대한 보안 액세스 제어 단순화
- 비밀번호의 엔드 투 엔드 암호화 용이
- 모든 비밀번호 업데이트 메시지가 전달되는지 확인
- 커넥터 사이 통신 복잡성 및 보안 위험 감소
- 구성 정보를 배포하는 중앙 권한 사용 가능
- 모든 커넥터 로그를 중앙의 위치에서 집산 가능

시스템 구성요소 배포

효과적인 구현을 개발하기 전에 반드시 Identity Synchronization for Windows 구성요소가 구성되는 방법과 제품이 운영되는 방법을 이해해야 합니다. 이 부분은 다음과 같은 내용으로 구성됩니다.

- "코어" 페이지 36
- "Directory Server 커넥터 및 플러그인" 페이지 36
- "Active Directory 커넥터" 페이지 37
- "Windows NT 커넥터 및 하위 구성요소" 페이지 38

이 단원과 구현 시나리오 예제 ([페이지 46](#) 참조) 에서 설명하는 기본 개념을 이해하면 더욱 복잡한 고도의 시나리오 (복합 Active Directory 및 Windows NT 환경 또는 복수 서버 환경 등) 에 대한 구현 전략을 만들 수 있는 정보를 추론할 수 있을 것입니다.

코어

코어 구성요소는 임의의 지원되는 운영 체제 디렉토리 서버에 한 번만 설치합니다. Administration Server 는 반드시 코어와 동일한 컴퓨터에 있어야 합니다. 반드시 코어를 설치하기 전에 Message Queue 3.5 SP1 Enterprise Edition 을 설치해야 합니다.

Directory Server 커넥터 및 플러그인

Directory Server 커넥터는 임의의 지원되는 운영 체제에 설치할 수 있습니다 (목록은 " 운영 체제 요구 사항 " [페이지 52](#) 참조). Directory Server 커넥터를 동기화되는 Directory Server 가 실행되는 컴퓨터와 동일한 컴퓨터에 설치해야 하는 것은 아닙니다. 그러나 구성된 Directory Server 소스의 각각에 반드시 하나의 Directory Server 커넥터가 설치되어야 합니다.

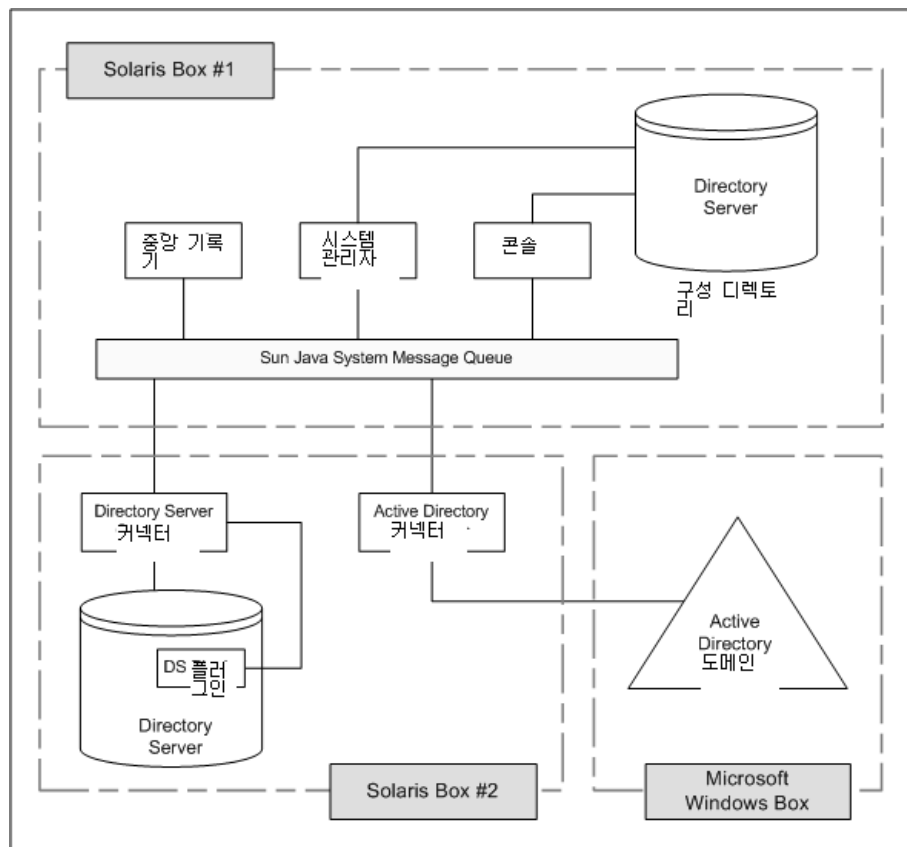
반드시 동기화되는 Directory Server 가 있는 모든 호스트에 Directory Server 플러그인을 설치해야 합니다.

참고 각 Directory Server 소스마다 하나의 Directory Server 커넥터가 설치됩니다. 그러나 Directory Server 플러그인은 동기화될 각 마스터, 허브 및 소비자 복제본에 설치되어야 합니다.

Active Directory 커넥터

Active Directory 커넥터는 임의의 지원되는 운영 체제에 설치할 수 있습니다 (그림 1-2 참조). Windows 환경의 경우 Active Directory 커넥터를 설치할 필요가 없으나, 각 Active Directory 도메인에 반드시 하나의 Active Directory 커넥터가 설치되어야 합니다.

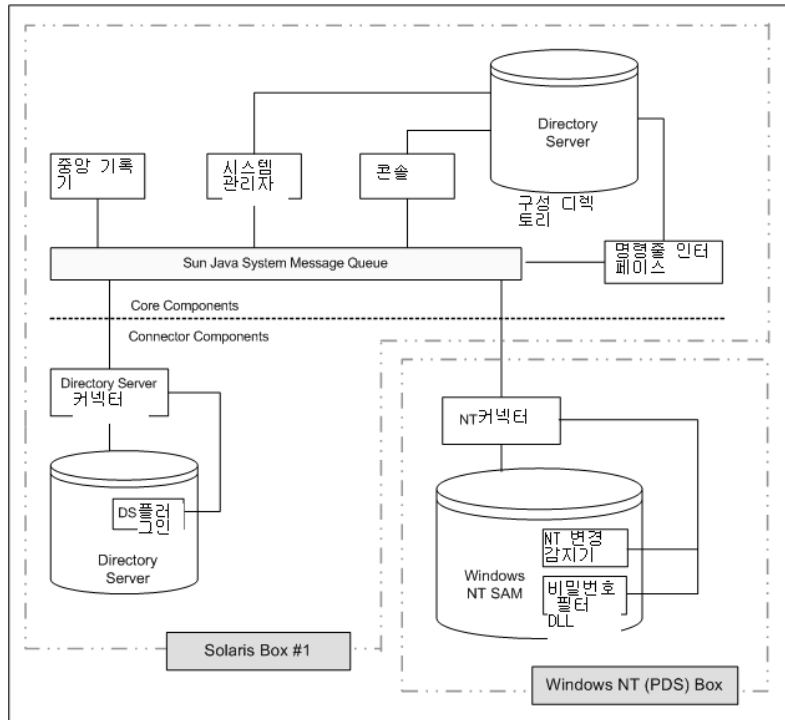
그림 1-2) Directory Server 및 Active Directory 구성요소 배포



Windows NT 커넥터 및 하위 구성요소

Windows NT SAM Registries 와 동기화하려면 (그림 1-3 참조) 반드시 Windows NT 커넥터를 PDC(Primary Domain Controller) 에 설치해야 합니다 . 또한 설치 프로그램은 NT 도메인의 PDC 에 커넥터와 함께 두 개의 NT 커넥터 구성요소 (변경 검출기 및 비밀번호 필터 DLL)를 설치합니다 . 단일 NT 커넥터는 단일 NT 도메인용 사용자 및 비밀번호를 동기화합니다 .

그림 1-3) Directory Server 및 NT 구성요소 배포



Identity Synchronization for Windows 가 디렉토리 소스에서 변경을 검출하는 방법

이 부분에서는

Sun Java System Directory Server(Directory Server), Windows Active Directory 및 Windows NT 커넥터가 사용자 항목 및 비밀번호 변경을 검출하는 방법에 대하여 설명합니다 .

다음과 같은 내용으로 구성됩니다 .

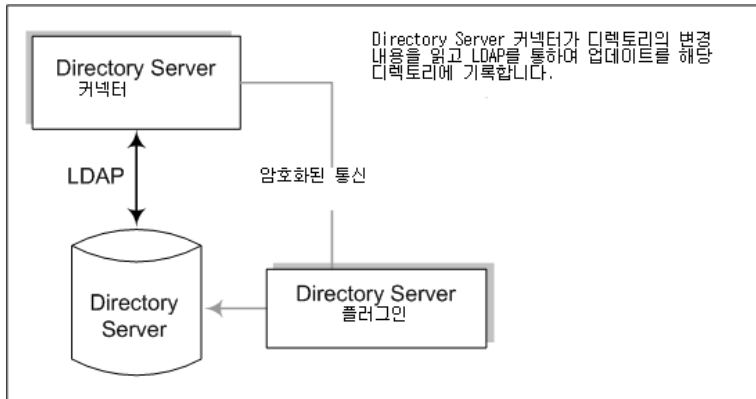
- ["Directory Server 커넥터가 변경을 검출하는 방법 " 페이지 39](#)
- ["Active Directory 커넥터가 변경을 검출하는 방법 " 페이지 40](#)
- ["Windows NT 커넥터가 변경을 검출하는 방법 " 페이지 41](#)
- [" 비밀번호 업데이트 전달 " 페이지 42](#)

Directory Server 커넥터가 변경을 검출하는 방법

Directory Server 커넥터는 LDAP 를 통하여 Directory Server Retro-Changelog 를 검사하여 사용자 항목 및 비밀번호 변경 이벤트를 검출합니다 . Directory Server 플러그인은 다음과 같은 방법으로 커넥터를 지원합니다 .

- 암호화를 사용하여 일반 텍스트 비밀번호를 캡처한 후 이를 Retro Changelog 에서 사용할 수 있도록 합니다 . 플러그인이 없는 경우 Retro Changelog 에 오직 해시된 비밀번호만 표시되며 해시된 비밀번호는 동기화할 수 없습니다 .
- Active Directory 로 요청시 비밀번호 동기화를 수행하면 Windows 환경에서 Identity Synchronization for Windows 구성요소를 설치할 필요가 없습니다 ("[요청시 비밀번호 동기화를 사용하여 일반 텍스트 비밀번호 가져오기 " 페이지 42 참조](#)).

그림 1-4) Directory Server 커넥터가 변경을 검출하는 방법



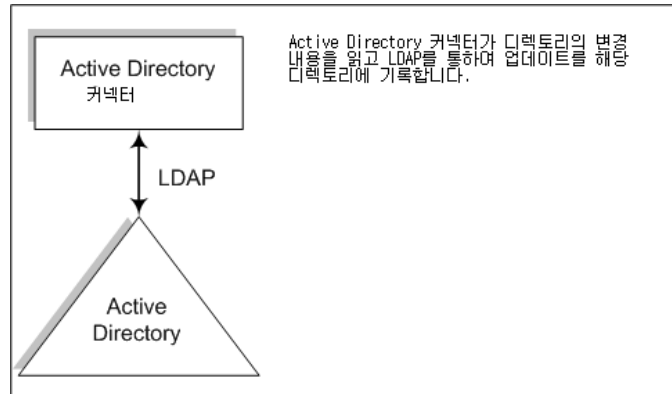
Active Directory 커넥터가 변경을 검출하는 방법

Windows 2000/2003 Server Active Directory 커넥터는 Active Directory USNChanged 및 PwdLastSet 속성 값을 검사하여 사용자 항목 및 비밀번호 변경을 검출합니다.

Directory Server 의 Retro Changelog 와 달리 항목의 속성을 변경하면 Active Directory 가 어느 속성이 변경되었는지 보고하지 않습니다. 대신 Active Directory 는 USNchanged 속성을 증분시켜 항목 변경을 확인합니다. Active Directory 및 Windows NT 커넥터는 개별 속성의 변경을 검출하기 위하여 객체 캐시라고 하는 처리 중인 데이터베이스를 사용합니다. 객체 캐시에는 각 Active Directory 항목의 해시된 사본이 저장되며, 따라서 커넥터가 정확히 항목의 어느 속성이 수정되었는지 판단할 수 있습니다.

Windows 환경에 Active Directory 커넥터를 설치할 필요는 없습니다. Active Directory 커넥터는 Solaris 시스템 등과 같은 다른 환경에서 실행될 수 있으며 LDAP 를 통하여 원격으로 검출 및 변경 작업을 수행할 수 있습니다.

그림 1-5) Active Directory 커넥터가 변경을 검출하는 방법

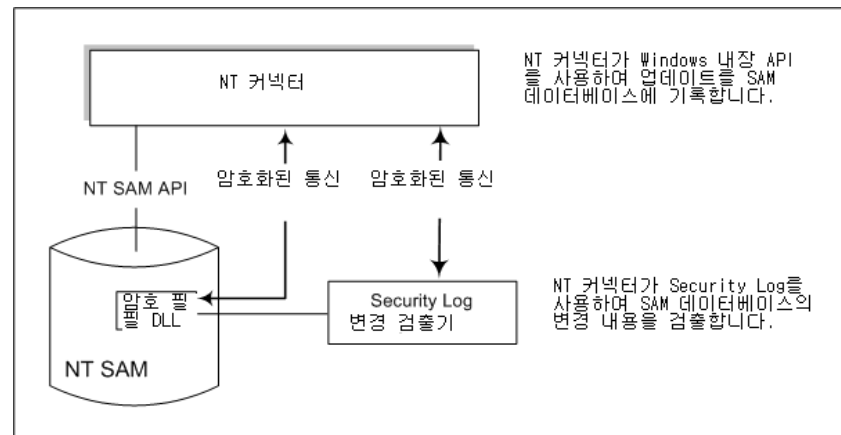


Windows NT 커넥터가 변경을 검출하는 방법

Windows NT 커넥터는 사용자 객체에 대한 감사 이벤트용 보안 로그를 검사하여 사용자 항목 및 비밀번호 변경을 검출합니다.

Windows NT SAM Registries 와 동기화하려면 (그림 1-6 참조) 반드시 Windows NT 커넥터를 PDC(Primary Domain Controller) 에 설치해야 합니다. 또한 설치 프로그램은 NT 도메인의 PDC 에 커넥터와 함께 두 개의 NT 커넥터 하위 구성요소 (변경 검출기 및 비밀번호 필터 DLL) 를 설치합니다. 단일 NT 커넥터는 단일 NT 도메인용 사용자 및 비밀번호를 동기화합니다.

그림 1-6) Windows NT 커넥터가 변경을 검출하는 방법



참고 구현에 Windows NT 컴퓨터가 있는 경우 감사를 반드시 사용 설정해야 하며, 그렇지 않은 경우 Identity Synchronization for Windows 가 해당 컴퓨터에서 메시지를 기록할 수 없습니다. Windows NT 컴퓨터에서 감사 로그를 사용하는지 확인하려면 "[Windows NT 컴퓨터에서 감사 사용 설정](#) " 페이지 274 를 참조하십시오 .

변경 검출기 및 비밀번호 필터 DLL 하위 구성요소에 대한 설명은 "[Windows NT 커넥터 하위 구성요소](#) " 페이지 34 를 참조하십시오 .

비밀번호 업데이트 전달

여기에서는 Windows 시스템과 Directory Server 시스템 사이에서 비밀번호 변경을 전달하기 위하여 일반 텍스트 비밀번호를 가져오는 방법에 대하여 설명합니다 .

- "[비밀번호 필터 DLL 을 사용하여 일반 텍스트 비밀번호 가져오기](#) " 페이지 42
- "[요청시 비밀번호 동기화를 사용하여 일반 텍스트 비밀번호 가져오기](#) " 페이지 42

비밀번호 필터 DLL 을 사용하여 일반 텍스트 비밀번호 가져오기

비밀번호 업데이트를 Sun Java System Directory Server 로 전달하려면 Windows NT 커넥터가 반드시 일반 텍스트 비밀번호를 가져와야 합니다 . 그러나 Windows 디렉토리에서는 일반 텍스트 비밀번호를 추출할 수 없는데, 비밀번호가 이 디렉토리에 저장되는 시점에서 이미 암호화되기 때문입니다 .

Windows NT 에는 비밀번호 필터 DLL 인터페이스가 제공되며, 이를 사용하여 구성요소가 일반 텍스트 비밀번호를 디렉토리에 영구적으로 저장되기 전에 캡처할 수 있습니다 .

요청시 비밀번호 동기화를 사용하여 일반 텍스트 비밀번호 가져오기

Active Directory 가 Windows NT 와 동일한 비밀번호 필터를 지원하지만, 반드시 기본 도메인 제어기 (PDC) 뿐 아니라 모든 도메인 제어기에 비밀번호 필터 DLL 을 설치해야 합니다 . 이렇게 하면 시스템에 상당한 부하가 발생하므로 Identity Synchronization for Windows 는 *요청시 비밀번호 동기화*라고 하는 다른 접근 방법을 사용하여 Active Directory 에서 Directory Server 로 비밀번호 변경을 동기화합니다 .

요청시 비밀번호 동기화는 Windows 2000 에서 사용자의 암호가 변경된 후 해당 사용자가 로그인하려 할 때 Directory Server 에서 새 비밀번호 값을 가져올 수 있는 방법을 제공합니다 .

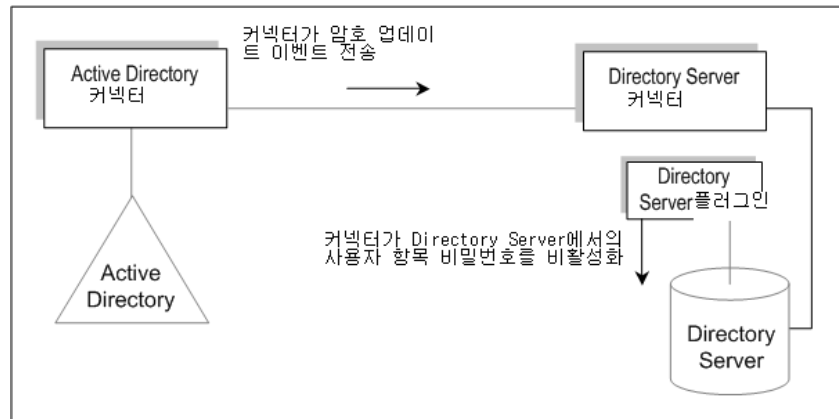
또한 요청시 비밀번호 동기화를 사용하면 비밀번호 필터 DLL 없이 Active Directory 에서 비밀번호를 동기화할 수 있습니다 .

요청시 비밀번호 동기화 프로세스는 다음과 같습니다 .

1. 사용자가 Windows 워크스테이션에서 Ctrl-Alt-Del 을 눌러 비밀번호를 변경합니다 . Active Directory 에 새 비밀번호가 저장됩니다 .
2. Active Directory 커넥터는 예약된 간격으로 시스템을 폴합니다 .

커넥터가 비밀번호 변경을 감지하면 (USNchanged(업데이트 시퀀스 번호) 및 PwdLastSet 속성에서 변경된 내용 기준) 커넥터는 Message Queue 에 해당 비밀번호 변경에 대한 메시지를 게시합니다 . 메시지는 SSL 암호화 채널로 전송됩니다 .

그림 1-7) 요청시 비밀번호 동기화 - 제 1 부



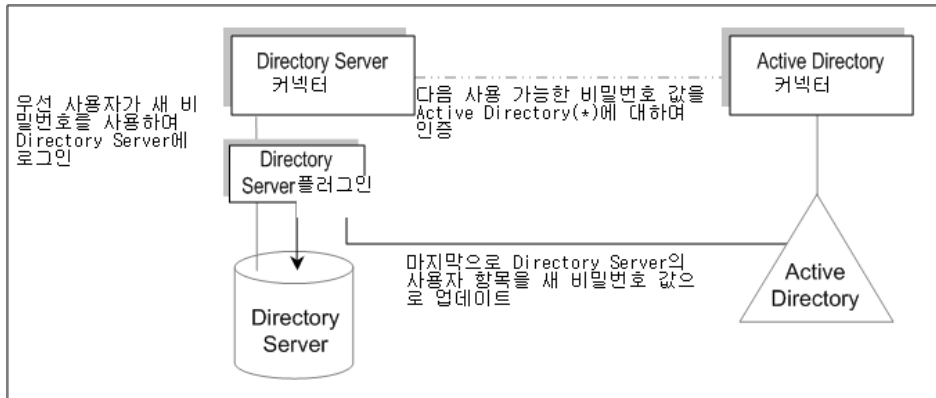
3. Directory Server 커넥터가 Message Queue 에서 비밀번호 변경 메시지를 수신합니다 (SSL 경유).
4. Directory Server 커넥터가 사용자 항목의 dspswvalidate 속성을 true 로 설정하면 이전 비밀번호는 무효화되고 Directory Server 플러그인에 비밀번호 변경을 경고합니다 .
5. 사용자가 LDAP 응용 프로그램(Portal Server 등)을 사용한 Directory Server에 대한 인증을 통하여 로그온을 시도하면 Sun Java System Directory Server 플러그인이 Directory Server 항목에 있는 비밀번호 값이 유효하지 않음을 검출합니다 .

6. Directory Server 플러그인이 Active Directory에서 해당 사용자를 검색합니다. 플러그인이 해당 사용자를 찾으면 사용자가 Directory Server 에 로그인할 때 입력한 비밀번호를 사용하여 Active Directory 로의 바인딩을 시도합니다.

참고 요청시 비밀번호 동기화에는 SASL Digest-MD5 등의 더 복잡한 인증 메커니즘을 사용하는 것이 아니라 Directory Server 에 대한 간단한 인증을 사용하는 응용 프로그램이 필요합니다.

7. Active Directory에 대한 바인딩이 성공하면 사용자가 새 Active Directory 비밀번호를 입력하고, Directory Server 플러그인은 해당 비밀번호를 설정하고 Directory Server 의 사용자 항목에서 무효화된 비밀번호 플래그를 제거합니다.

그림 1-8) 요청시 비밀번호 동기화 - 제 2 부



참고 사용자 인증이 실패하는 경우 사용자 항목 비밀번호는 Directory Server 에 유지되며, Directory Server 및 Active Directory 의 비밀번호는 사용자가 유효한 비밀번호 (Active Directory 로 인증할 때 사용하는 비밀번호) 로 로그인할 때까지 동기화되지 않습니다.

신뢰할 수 있는 동기화

Identity Synchronization for Windows 는 구성요소를 일시적으로 사용 불가능한 경우에도 사용자 변경 이벤트를 잃지 않도록 매우 신중하게 작업합니다. Identity Synchronization for Windows 의 신뢰도는 TCP 네트워크 프로토콜과 유사합니다. TCP 는 끊어지거나 중단되는 네트워크의 경우에도 결국 모든 데이터를 순서대로 전달합니다. 네트워크가 일시적으로 끊어진 동안 송신된 데이터는 네트워크가 중단된 동안 대기열에 놓여지며 연결이 복구되면 다시 전달됩니다. Identity Synchronization for Windows 는 다음 구성요소 중 한 가지를 일시적으로 사용할 수 없는 경우에도 사용자 변경 이벤트를 검출하고 적용합니다

- 커넥터
- Directory Server
- Message Queue
- Active Directory 도메인 제어기
- Windows NT 기본 도메인 제어기
- 시스템 관리자
- 구성 디렉토리

이들 구성요소 중 한 가지를 사용할 수 없는 경우 Identity Synchronization for Windows 는 변경 내용을 잃지 않고 (비밀번호 포함) 해당 구성요소를 다시 사용할 수 있을 때까지 동기화를 연기합니다. 이 버전의 Identity Synchronization for Windows 는 Sun Cluster 또는 기타 진정한 고가용도 솔루션은 지원하지 않습니다. Identity Synchronization for Windows 는 사용자가 직접 상호작용하지 않는 배경의 응용 프로그램이므로 보통 고가용성이 필요하지 않습니다.

중요한 오류가 발생하는 경우 Identity Synchronization for Windows 구성요소를 다시 설치하고 idsync resync 명령을 사용하여 모든 디렉토리 소스를 다시 동기화할 수 있습니다.

대부분의 경우 구성요소를 사용할 수 없으면 프로그램은 동기화 이벤트를 대기열에 넣고 구성요소를 사용할 수 있는 경우에만 이를 적용합니다. 이 프로세스에는 두 가지 예외가 있습니다.

- 복수 마스터 복제 (MMR) Directory Server 환경의 경우 Windows 사용자에게 대한 외부 변경 내용은 기본 또는 보조 Directory Server 로 동기화될 수 있습니다.

기본 Directory Server 를 사용할 수 없는 경우 Directory Server 커넥터는 보조 서버에 변경을 적용합니다 . Identity Synchronization for Windows 는 기본 마스터를 사용할 수 있을 때까지 Directory Server 마스터에 수행된 외부 변경 내용을 검출 및 전달하지 않습니다 .

- Active Directory Connector 가 단일 Active Directory 도메인 컨트롤러와만 통신할 수 있는 반면 , Directory Server 플러그인은 요청시 암호 동기화를 수행하는 동안 모든 Active Directory 도메인 컨트롤러 사이에서 실패할 수 있습니다 . 이 경우 페일오버가 가장 중요한 순간으로 Directory Server 플러그인이 Active Directory 도메인 컨트롤러와 연결하여 사용자의 새 비밀번호를 확인할 수 없는 경우 사용자는 Directory Server 로 로그인할 수 없습니다 .

구현 예제 : 컴퓨터가 두 대인 구성

여기에서는 Sun 과 Windows 디렉토리 사이에서 Identity Synchronization for Windows 를 사용하여 사용자 객체 생성과 양방향 비밀번호 수정을 동기화하는 구현 시나리오에 대하여 설명합니다 .

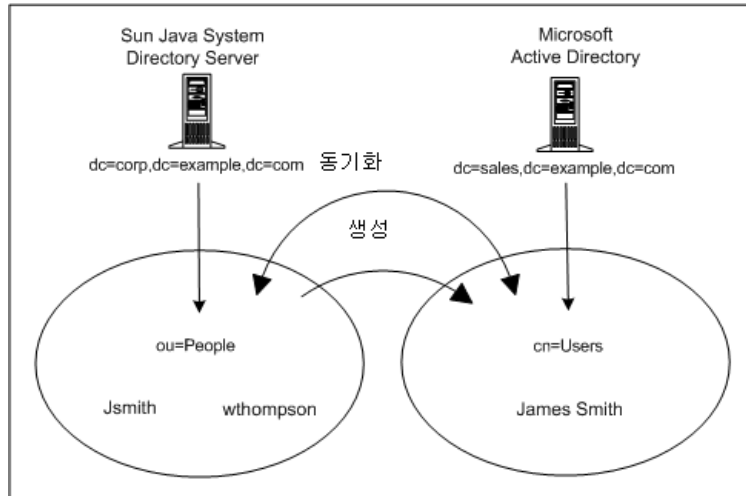
이 구현 시나리오에는 두 대의 시스템으로 구성됩니다 .

- Sun Java System 디렉토리 서버를 실행하는 시스템 (호스트 이름 : *corp.example.com*)
- Windows 2000 서버에서 Active Directory 를 실행하는 시스템 (호스트 이름 : *sales.example.com*)

참고 이 시나리오에서는 NT 를 사용하지 않지만 Identity Synchronization for Windows 는 NT 도메인과의 동기화 또한 지원한다는 것을 유의하십시오 .

이 구현 시나리오에서 동기화 요구 사항은 (노드 구조와 연결된 속성 값) 에 보이는 것과 같습니다 .

그림 1-9) 동기화 요구 사항



이 시나리오의 목적은 두 가지입니다.

- **사용자 하위 트리 (Directory Server의 *ou=people* 과 Active Directory의 *cn=users*)** 사이에서 사용자 비밀번호를 양방향으로 동기화. 따라서 하나의 디렉토리어서 사용자 비밀번호가 변경되면 비밀번호 변경 내용이 다른 디렉토리의 연결된 사용자에게 동기화됩니다.

예를 들어 Directory Server의 *ou=people* 컨테이너에서 *uid=JSmith*의 비밀번호를 변경하는 경우 새 비밀번호가 Active Directory 서버의 *cn=users* 컨테이너에 있는 *cn=Joe Smith*로 자동으로 동기화됩니다.

- Directory Server 사용자 하위 트리에서 Active Directory 사용자 하위 트리로만 사용자 객체 생성 작업을 동기화.

예를 들어 지정된 일련의 속성으로 새 사용자 (*ou=People* 컨테이너의 *uid=WThompson*)를 만드는 경우 Identity Synchronization for Windows는 Active Directory에 동일한 일련의 속성으로 *WThompson* (*cn=Users* 컨테이너의 *cn=William Thompson*)용 새 계정을 만들 수 있습니다.

참고

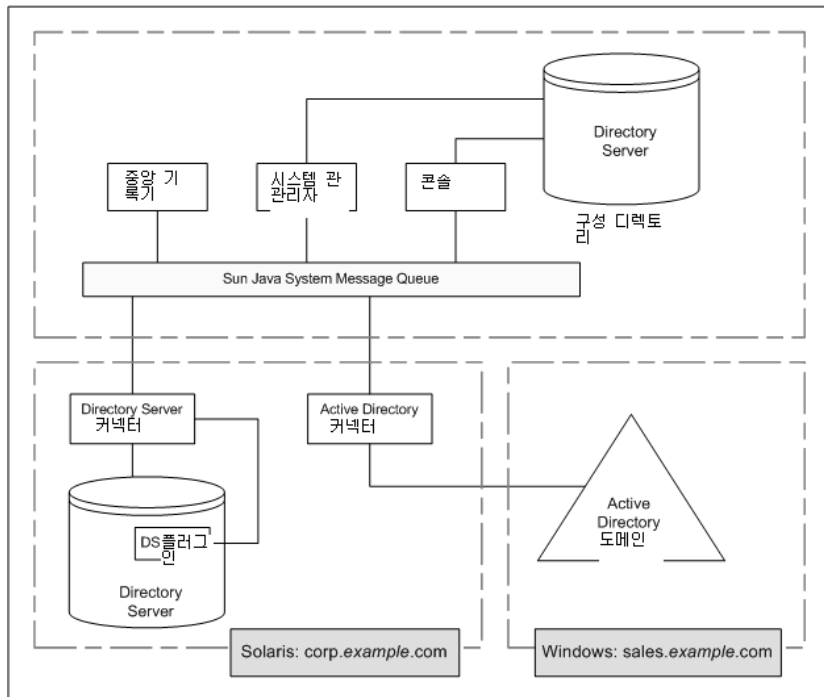
Identity Synchronization for Windows 는 동일한 유형의 복수 동기화를 지원합니다. (예를 들어 단일 구현에서 Directory Server 가 두 개 이상 있거나 복수 Active Directory 도메인이 가능합니다.)

생성, 수정 및 삭제 동기화 설정은 전체 디렉토리에 전역적이며 개별 디렉토리 소스에 지정될 수 없습니다. Sun 에서 Windows 로 사용자 생성 내용을 동기화하면 사용자 생성 내용은 설치에서 구성된 모든 Sun Directory Server 에서 모든 Active Directory 도메인 및 Windows NT 도메인으로 전달됩니다.

물리적 구현

그림 1-10 에서는 모든 제품의 구성요소가 단일 Solaris 박스에 물리적으로 구현된 반면 Active Directory 도메인은 별도의 구성요소가 설치되지 않은 Active Directory 도메인 컨트롤러에 상주합니다.

그림 1-10) Directory Server 및 Active Directory 시나리오



구성요소 배포

호스트 *corp.example.com* 은 Solaris 운영 체제에 설치된 Directory Server 입니다 . 동기화되는 Directory Server 용 루트 접미어는 *dc=corp,dc=example,dc=com* 입니다 .

컴퓨터에 포함된 내용 :

- Identity Synchronization for Windows 코어 구성요소
- Identity Synchronization for Windows Directory Server 커넥터
- Identity Synchronization for WindowsDirectory Server 플러그인
- Identity Synchronization for Windows 구성 디렉토리 (동기화되는 Directory Server 인스턴스가 아닌 다른 인스턴스에 위치)

호스트 *sales.example.com* 은 동기화되는 Active Directory 도메인입니다 .

구현 예제 : 컴퓨터가 두 대인 구성

설치 준비

Identity Synchronization for Windows 1 2004Q3 을 설치하거나 버전 1.0 에서 버전 1 2004Q3 으로 이전하기 전에 설치 및 구성 프로세스를 숙지해야 합니다 .

이 장에서는 이 과정을 설명하고 제품의 설치를 준비하는 데 도움이 될 기타 정보를 제공합니다 . 이 정보는 다음과 같이 구성되었습니다 .

- " 설치 요구 사항 " 페이지 51
- " 설치 개요 " 페이지 55
- " 구성 개요 " 페이지 60
- " 버전 1 2004Q3 으로 이전 " 페이지 64
- " Active Directory 와 비밀번호 동기화 " 페이지 65
- " SSL 작업용으로 Windows 구성 " 페이지 73
- " 설치 및 구성 결정 " 페이지 73
- " 설치 점검 목록 " 페이지 77

설치 요구 사항

여기에서는 Identity Synchronization for Windows 의 설치 요구 사항에 대하여 설명하며 , 운영 체제 버전 , 패치 및 각 플랫폼용 유틸리티가 포함됩니다 .

- " 운영 체제 요구 사항 " 페이지 52
- " 하드웨어 요구 사항 " 페이지 53
- " Sun Java System 소프트웨어 요구 사항 " 페이지 53
- " 설치 자격 증명 " 페이지 54

운영 체제 요구 사항

아래 표에서는 금번 Identity Synchronization for Windows 릴리스에 필요한 운영 체제 요구 사항을 설명합니다.

표 2-1) Solaris 요구 사항

구성요소	Solaris 요구 사항
코어 구성요소	Solaris 8™ for UltraSPARC® (32 비트 및 64 비트) Solaris 9™ SPARC® Platform Edition (32 비트 및 64 비트) Solaris 9™ 운영 체제 (Pentium II 이상용 x86 Platform Edition) IA-32
Sun Java™ System Directory Server 및 Windows Active Directory 용 커넥터	Solaris 8 for UltraSPARC (32 비트 및 64 비트) Solaris 9 for SPARC Platforms (32 비트 및 64 비트) Solaris 9 운영 체제 (Pentium II 이상용 x86 Platform Edition) IA-32
Sun Java™ System Directory Server 용 플러그인	Solaris 8 for UltraSPARC (32 비트 및 64 비트) Solaris 9 for SPARC Platforms (32 비트 및 64 비트) Solaris 9 운영 체제 (Pentium II 이상용 x86 Platform Edition) IA-32

표 2-2) Windows 요구 사항

구성요소	Windows 요구 사항
코어	Windows 2000 Server SP4 Windows 2000 Advanced Server SP4 Windows 2003 Server Standard Edition (최신 보안업데이트 포함) Windows 2003 Server Enterprise Edition (최신 보안 업데이트 포함)
Sun Java™ System Directory Server 및 Windows Active Directory 용 커넥터	Windows 2000 Server SP4 Windows 2000 Advanced Server SP 4 Windows 2003 Server Standard Edition (최신 보안업데이트 포함) Windows 2003 Server Enterprise Edition (최신 보안 업데이트 포함)
Sun Java™ System Directory Server 용 플러그인	Windows 2000 Server SP4 Windows 2000 Advanced Server SP 4 Windows 2003 Server Standard Edition (최신 보안업데이트 포함) Windows 2003 Server Enterprise Edition (최신 보안 업데이트 포함)

표 2-2) Windows 요구 사항 (계속)

구성요소	Windows 요구 사항
NT 커넥터 및 하위 구성요소	Windows Primary Domain Controller NT 4.0 Server SP 6A (x86 전용)

하드웨어 요구 사항

Identity Synchronization for Windows 를 실행하려면 반드시 하드웨어 (모든 플랫폼) 에 다음의 최소 요구 사항이 갖추어져야 합니다 .

- Directory Server 에 설치하기 위한 최소 약 400MB 의 디스크 공간
- 서버가 임의의 Identity Synchronization for Windows 구성요소를 실행하는 경우 최소 512MB 의 RAM. (메모리는 클 수록 좋습니다 .)

Sun Java System 소프트웨어 요구 사항

Identity Synchronization for Windows 를 설치하려면 반드시 먼저 다음 Sun Java System 소프트웨어 구성요소를 설치해야 합니다 .

- Sun Java System Directory Server version 5 2004Q2 패치 117907-02(이상)
패치 교정을 적용하면 Directory Server 5 2004Q2 가 있는 Identity Synchronization for Windows 1 2004Q2 용 삭제 기능을 사용할 수 있습니다 .
 - **Solaris SPARC 패키지 형식** : 부품 번호 117907-02 이상
 - **Solaris SPARC 압축 아카이브 설치** : 패치 5077789
 - **Solaris x86 패키지 형식** : 부품 번호 117908-02 이상
 - **Solaris x86 압축 아카이브 설치** : 패치 5077789
 - **Windows 압축 아카이브 설치** : 패치 5077789

이들 패치와 패치를 Directory Server 환경에 적용하는 방법은 다음에 있는 Identity Synchronization for Windows 다운로드 디렉토리의 README.patch 파일을 참조하십시오 .

<download_root>/patches/directory/README.patch

Solaris 에 Directory Server 5 2004Q2 를 설치하는 데 필요한 최신 정보와 패치는 다음 웹사이트에 있는 *Sun Java System Directory Server 5 2004Q2 Installation and Tuning Guide* 및 *Sun Java System Directory Server 5 2004Q2 릴리스 노트*를 참조하십시오 .

http://docs.sun.com/db/coll/DirectoryServer_04q2

- Sun Java System Message Queue (이전 이름은 Sun ONE Message Queue) 버전 3.5 SP1 Enterprise Edition.

참고

Identity Synchronization for Windows 버전 1.0에서는 자동으로 Message Queue가 설치되지만 *버전 1 2004Q3에서는 설치되지 않습니다.*

이미 설치된 Sun Java System Message Queue에 Identity Synchronization for Windows 코어를 설치하려면 반드시 Message Queue 버전 3.5 SP1 Enterprise Edition을 사용해야 합니다. Message Queue의 버전이 부적절한 경우 코어를 설치하면 오류가 발생합니다.

Identity Synchronization for Windows 다운로드 번들에는 Message Queue가 포함됩니다. 소프트웨어는 다음과 같이 각 플랫폼의 /messagequeue 디렉토리에서 사용할 수 있습니다.

- **Solaris SPARC:** /messagequeue/imq3_5-ent-solsparc.zip
- **Solaris x86:** /messagequeue/imq3_5-ent-soli386.zip
- **Windows:** /messagequeue/imq3_5-ent-win.exe
- Java Runtime Environment
 - 이 제품에는 Java Runtime Environment(JRE)가 제공되지 않습니다.
 - Solaris 또는 Windows에서 Identity Synchronization for Windows 설치 프로그램을 실행하려면 반드시 J2SE (또는 JRE) 1.4.2_04 이상을 설치해야 합니다.
 - 반드시 Windows NT에 JRE 1.4.1_03(이상)을 설치해야 합니다.

설치 자격 증명

Identity Synchronization for Windows를 설치하려면 반드시 다음에 대한 자격 증명을 제공해야 합니다.

- 구성 디렉토리
- 동기화되는 Directory Server

- Active Directory(자세한 내용은 " [코어 설치](#) " 를 참조하십시오 .)

또한 Identity Synchronization for Windows 를 설치하려면 다음 권한이 있어야 합니다 .

- **Solaris 시스템** : 반드시 루트로 설치해야 합니다 .
- **Windows 시스템** : 반드시 *Administrator* 로 설치해야 합니다 .

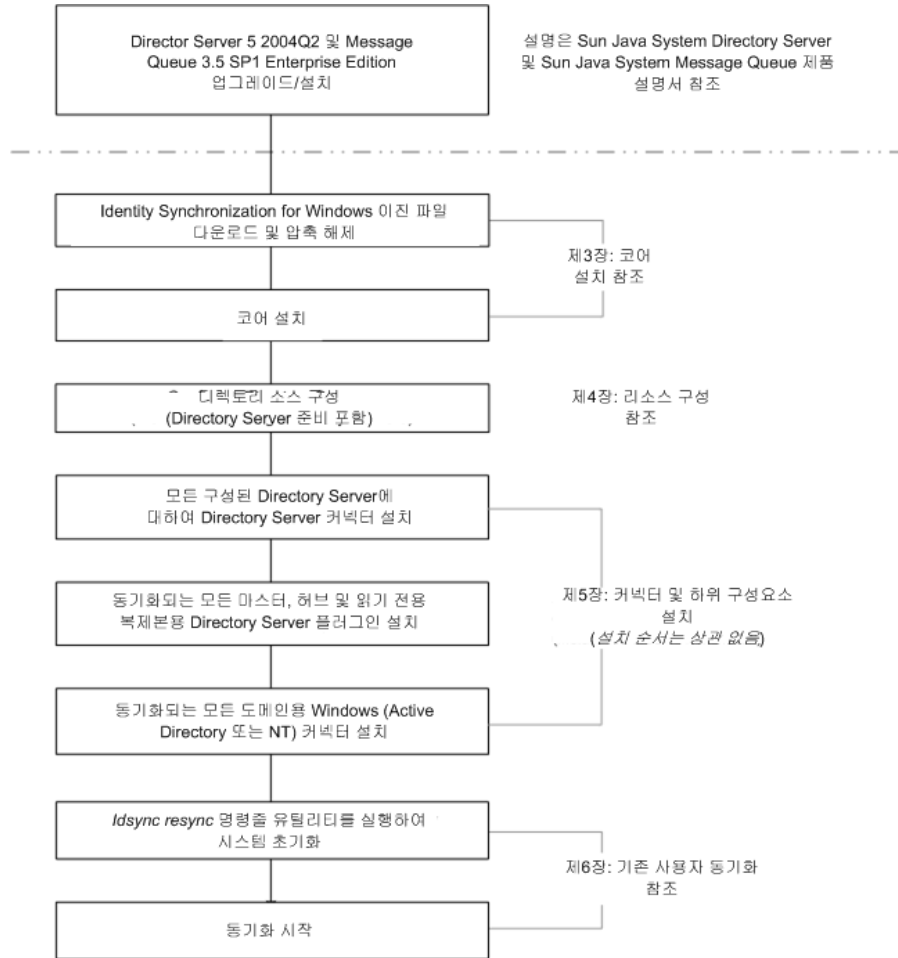
참고

텍스트 기반 설치 프로그램을 사용하여 비밀번호를 입력할 때 프로그램은 자동으로 비밀번호를 숨겨 비밀번호가 반향되어 표시되지 않도록 합니다 . 텍스트 기반 설치 프로그램은 Solaris 시스템에서만 지원됩니다 .

설치 개요

단일 호스트 구현용 제품 설치 과정은 에 보이는 것과 같습니다 .

그림 2-1) 단일 호스트 구현에서 설치



일부 구성요소는 반드시 순서에 따라 설치되어야 하므로 설치 방법을 모두 신중히 읽으십시오.

Identity Synchronization for Windows에는 "To Do" 목록이 제공되며, 이는 설치 및 구성의 모든 과정 동안 표시됩니다. 이 정보 패널에는 제품을 성공적으로 설치하고 구성하기 위하여 반드시 따라야 하는 모든 단계 목록이 있습니다.

그림 2-2) Identity Synchronization for Windows To Do 목록

설치 및 구성의 나머지 단계는 이 목록과 같습니다.:

- ✓ 1 : Identity Synchronization 코어 구성 요소를 설치합니다.
- 2 : 제품의 콘솔을 사용하거나 'idsync importentf'로 이전 설치에서 이전하여 초기 구성을 만듭니다.
- 3 : 콘솔을 사용하거나 'idsync prepds' 명령을 사용하여 이 구성에 있는 모든 Sun Directory Server를 준비합니다.
- 4 : 모든 구성된 디렉토리 소스의 커넥터를 설치합니다.
- 5 : 각 Sun Directory Server 커넥터를 설치한 후 모든 마스터와 모든 읽기 전용 복제본에서 설치 프로그램을 다시 실행하여 Sun Directory Server 플러그인을 설치합니다.
- 6 : 'idsync resync'를 실행하여 기존 Directory Server와 Windows 사용자 사이의 링크를 설정합니다.
- 7 : 콘솔 또는 'idsync startsync' 명령을 사용하여 동기화를 시작합니다.

설치 및 구성 프로세스를 진행하는 동안 목록에서 완료된 단계는 흐리게 표시됩니다 (그림 2-2 참조).

이 단원의 나머지에서는 다음과 같은 구성으로 설치 및 구성 과정에 대한 개요를 설명합니다 .

- " 코어 설치 " 페이지 57
- " 제품 구성 " 페이지 58
- "Directory Server 준비 " 페이지 58
- " 커넥터 및 Directory Server 플러그인 설치 " 페이지 58
- " 기존 사용자 동기화 " 페이지 59

참고 자세한 설치 및 구성 설명은 이 설명서의 뒤에서 제공합니다 .

코어 설치

코어를 설치하면 다음 구성요소가 설치됩니다 .

- **콘솔**: 제품의 모든 구성요소 구성과 관리 작업을 수행할 수 있는 중앙화된 도구입니다 .

- **중앙 기록기** : 모든 감사 및 오류 기록 정보를 중앙의 위치로 중앙화합니다.
- **시스템 관리자** : 구성 업데이트를 동적으로 커넥터에 전달하며 각 커넥터의 상태를 유지합니다.

참고 코어 설치 방법은 [제 3 장](#) , "[코어 설치](#) "에 있습니다.

제품 구성

코어를 설치한 후 콘솔을 사용하여 중앙의 위치에서 동기화될 디렉토리 소스 (또한 구현의 기타 특성) 를 모두 초기 구성합니다 .

참고 디렉토리 리소스를 구성하는 방법은 [제 4 장](#) , "[코어 자원 구성](#) "에 있습니다.

Directory Server 준비

Directory Server 커넥터는 Sun Java System Directory Server 5 2004Q2 를 지원합니다 .

Directory Server 커넥터를 설치하기 전에 반드시 동기화되는 모든 구성된 Directory Server 마스터 (기본 및 보조 마스터 모두) 용 Sun Java System Directory Server 소스를 준비해야 합니다 .

이 작업은 콘솔에서 수행하거나 `idsync prepds` 하위 명령을 사용하여 명령줄에서 수행할 수 있습니다 .

참고 Directory Server 를 준비하는 방법은 "[Directory Server 준비](#) " [페이지 109](#) 에 있습니다.

커넥터 및 Directory Server 플러그인 설치

시스템에 구성된 디렉토리의 수에 따라 설치하는 커넥터와 Directory Server 플러그인의 수가 달라집니다 .

참고 콘솔과 설치 프로그램은 모두 디렉토리의 *레이블*을 사용하여 커넥터를 동기화되는 디렉토리와 연결합니다. 예서는 Identity Synchronization for Windows 의 레이블 이름 지정 형식에 대하여 설명합니다.

표 2-3) 레이블 이름 지정 형식

커넥터 유형	디렉토리 소스 레이블	하위 구성요소
Directory Server 커넥터	루트 접미어 또는 접미어 / 데이터베이스	Directory Server 플러그인 동기화되는 루트 접미어에 대하여 각 Directory Server(마스터 또는 소비자)에 하나의 플러그인을 설치합니다.
AD 커넥터	도메인 이름	없음
NT 커넥터	도메인 이름	(Windows NT 커넥터와 자동으로 설치) 변경 검출기와 비밀번호 필터 DLL 하위 구성요소는 함께 동일한 설치로 설치됩니다. 반드시 그래픽 사용자 인터페이스 (GUI) 설치 프로그램을 사용하여 Windows NT 커넥터를 설치해야 합니다.

참고 커넥터 및 Directory Server 플러그인의 설치 및 구성 방법은 제 5 장, "커넥터 및 Directory Server 플러그인 설치"에 있습니다.

기존 사용자 동기화

커넥터, 플러그인 및 하위 구성요소를 설치한 후 반드시 `idsync resync` 명령줄 유틸리티를 구현을 기존 사용자와 부트스트랩해야 합니다. 이 명령은 다음에 대한 관리자가 지정한 일치 규칙을 사용합니다.

- 기존 항목 링크 (링크에 대한 정의는 "[사용자 연결](#)" 페이지 178 를 참조하십시오.)
- 원격 디렉토리의 내용으로 빈 디렉토리 입력
- Windows 및 Directory Server 디렉토리 모두의 항목이 고유하게 식별되며 서로 링크된 경우 두 기존 사용자 입력 사이에 속성 값 (비밀번호 포함)을 일괄 동기화합니다.

참고 구현에서 기존 사용자를 동기화하는 방법은 [제 6 장](#), "[기존 사용자 동기화](#)"에 있습니다.

구성 개요

제품을 설치한 후 반드시 다음을 포함하여 제품 구현을 구성해야 합니다.

- 동기화될 디렉토리 및 전역 카탈로그 구성
- 속성 수정 및 객체 활성화 / 비활성화에 동기화 설정 지정
- 구성된 디렉토리 사이의 사용자 항목 작성 및 삭제 내용 (선택)에 대한 동기화 설정 지정

여기에서는 다음 구성요소 개념에 대한 개요를 설명합니다.

- "[디렉토리](#)" [페이지 60](#)
- "[구성 디렉토리 및 전역 카탈로그](#)" [페이지 61](#)
- "[동기화 설정](#)" [페이지 61](#)
- "[Objectclass](#)" [페이지 61](#)
- "[속성 및 속성 매핑](#)" [페이지 62](#)
- "[Synchronization User Lists](#)" [페이지 64](#)

참고 자세한 구성 설명은 이 설명서의 뒤에서 제공합니다.

디렉토리

디렉토리가 표시하는 내용은 다음과 같습니다.

- 하나 이상의 Sun Java System Directory Server에 있는 단일 루트 접미어 (접미어 / 데이터베이스)
- Windows 2000 또는 Windows 2003 Server Active Directory 포리스트에 있는 단일 Active Directory 도메인
- 단일 Windows NT 도메인

각 디렉토리 유형을 원하는 만큼 구성할 수 있습니다.

구성 디렉토리 및 전역 카탈로그

Identity Synchronization for Windows 는 Sun Java System Directory Server 구성 디렉토리 및 Active Directory 전역 카탈로그를 저장소로 사용하여 여기에서 Directory Server 또는 Active Directory 디렉토리 토폴로지뿐 아니라 이들 디렉토리의 스키마 정보를 불러옵니다.

동기화 설정

동기화 설정을 사용하여 객체 작성, 객체 삭제, 비밀번호 및 기타 속성 수정이 Sun 과 Windows 디렉토리 사이에서 전달되는 방향을 제어할 수 있습니다. 동기화의 흐름 옵션은 다음과 같습니다.

- Sun 에서 Windows 로
- Windows 에서 Sun 으로
- 양방향으로

참고 Active Directory 및 Windows NT 가 포함되는 구성의 경우 Windows NT 및 Sun 사이와 Active Directory 및 Sun 사이의 생성 또는 수정에 대하여 서로 다른 동기화 설정을 지정하는 구성은 저장할 수 없습니다.

Objectclass

리소스를 구성할 때 해당 *objectclass* 에 따라 동기화할 항목을 지정합니다. 객체 클래스에 따라 Directory Server 및 Active Directory 모두에 대한 동기화에 사용 가능한 속성이 결정됩니다.

참고 Objectclass 는 Windows NT 에 적용할 수 없습니다.

Identity Synchronization for Windows 가 지원하는 objectclass 는 두 가지입니다.

- **구조적 objectclass**: 선택한 Directory Server 에서 만들어지거나 동기화된 모든 항목에는 반드시 구조적 objectclass 가 하나 이상 있어야 합니다. 드롭다운 목록에서 구조적 objectclass 를 선택합니다. (기본값은 Directory Server 의 경우 *inetorgperson* 이며 Active Directory 의 경우 *User* 입니다.)
- **보조 Objectclass**:
 - **Directory Server**에서는 Available Auxiliary Object Classes 목록창에서 하나 이상의 objectclass 를 선택하여 선택한 구조적 클래스를 사용할 수 있습니다. 이 경우 동기화용으로 추가 속성을 제공하게 됩니다.
 - **Active Directory**는 보조 objectclass에 대하여 더욱 제한적입니다. 선택한 구조적 objectclass 의 모든 유효한 보조 objectclass 에 대한 속성은 동기화용으로 사용할 수 있습니다.

참고 objectclass 및 속성을 구성하는 자세한 내용은 [제 4 장, "코어 자원 구성"](#) 을 참조하십시오.

속성 및 속성 매핑

속성에는 사용자 항목에 대한 설명적 정보가 유지됩니다. 각 속성에는 레이블과 하나 이상의 값이 있으며, 속성 값으로 저장되는 정보의 유형용 표준 구문을 따릅니다.

참고 콘솔에서 속성을 정의할 수 있습니다. 속성을 정의하는 방법은 [4 장](#) 을 참조하십시오.

속성 유형

Identity Synchronization for Windows 는 다음과 같이 **중요** 및 **작성** 사용자 속성을 동기화합니다.

- **중요 속성** : 지정된 수정 동기화 설정에 따라 속성이 수정되면 항상 Sun 과 Windows 디렉토리 사이에서 동기화됩니다.
- **생성 속성** : 지정된 객체 작성 동기화 설정에 따라 새 사용자가 만들어지면 항상 Sun 과 Windows 디렉토리 사이에서 동기화됩니다.

필수 생성 속성은 대상 디렉토리에서 작성 작업을 완료하기 위하여 " 필수적인 " 것으로 간주되는 속성입니다. 예를 들어 Active Directory 의 경우 생성시 cn 과 samaccountname 의 값이 유효해야 합니다. Sun 의 경우 user objectclass 의 inetorgperson 을 구성하면 Identity Synchronization for Windows 는 cn 과 sn 을 생성에 필수적인 속성으로 기대합니다.

생성 속성은 기본적으로 원래 디렉토리에서 전달되는 속성의 값이 없는 경우 오직 기본 값으로만 대상 디렉토리 생성 속성을 업데이트합니다. (생성 속성 기본 값은 다른 속성 값을 기반으로 할 수 있습니다. "매개변수화 속성 기본값" 페이지 63 를 참조하십시오.)

참고 중요 속성은 생성 속성으로 자동으로 동기화되지만 그 반대로는 동기화되지 않습니다. 생성 속성은 오직 사용자 작성시에만 동기화됩니다.

매개변수화 속성 기본값

Identity Synchronization for Windows 에서 다른 생성 또는 중요 속성을 사용하여 생성 속성에 대한 *매개변수화된* 기본값을 만들 수 있습니다.

매개변수화 기본 속성 값을 만들려면 퍼센트 기호 안에 표시되는 기존 생성 또는 중요 매개변수 이름 (%<attribute_name>%) 을 표현식 문자열에 포함해야 합니다. 예 :
 homedir=/home/%uid% or cn=%givenName%. %sn%.

이들 속성 기본 값을 만드는 경우 :

- 생성 표현식에 복수 속성을 사용할 수 있으나 (cn=%givenName% %sn%) %<attribute_name>% 의 속성에는 반드시 값이 한 개이어야 합니다.
- A=%B% 인 경우 B 에는 하나의 기본값만 있어야 합니다.
- 역슬래시 기호 (\) 를 인용에 사용할 수 있습니다 (예 :diskUsage=0\%).
- 순환적 대체 조건이 있는 표현식을 사용하면 안 됩니다. (예 :
 sn=%uid% 및 uid= %sn%).

속성 매핑

동기화할 속성을 정의한 후 , 반드시 Sun 과 Windows 시스템 사이에서 속성 이름을 매핑해야 합니다. 예를 들어 반드시 Sun inetorgperson 속성을 Active Directory user 속성으로 매핑해야 합니다.

참고 중요 및 생성 속성 모두의 속성 맵을 사용하며 , 반드시 각 디렉토리 유형에서 " 필수 생성 속성 " 용 속성 맵을 구성해야 합니다.

Synchronization User Lists

동기화 사용자 목록 (SUL) 을 만들어 Sun 과 Windows 디렉토리 모두에 있는 특정 사용자가 동기화되도록 정의합니다. 이들 정의에 의하여 평평한 디렉토리 정보 트리 (DIT) 를 계층적 디렉토리 트리로 동기화할 수 있습니다.

다음은 Synchronization User List 를 정의하는데 사용되는 개념입니다.

- **기본 DN**(Windows NT 에는 적용 안 됨): 다른 SUL 이 더욱 구체적이거나 필터에 의하여 제외되지 않는 한 해당 DN 의 모든 사용자를 포함합니다.
- **필터**: 사용자의 항목에 있는 속성을 사용하여 사용자를 동기화에서 제외하거나 기본 DN 이 동일한 사용자를 복수 SUL 로 나눕니다. 이 필터는 LDAP 필터 구문을 사용합니다.
- **생성 표현식** (Windows NT 에는 적용 안 됨): 새 사용자가 만들어지는 위치의 DN 을 만듭니다. 예: `cn=%cn%,ou=sales,dc=example,dc=com` 여기에서 `%cn%` 은 기존 사용자 항목의 `cn` 값으로 대체됩니다. 작성 표현식은 반드시 기본 DN 으로 끝나야 합니다.

SUL 에는 두 가지 정의가 포함되며, 여기에서 각 정의는 디렉토리 유형의 토폴로지의 면에서 동기화될 사용자 그룹을 식별합니다.

- 하나의 정의는 동기화할 Directory Server 사용자를 식별합니다.(예: `ou=people, dc=example, dc=com`)
- 다른 정의는 동기화할 Windows 사용자 식별 (예: `cn=users, dc=example, dc=com`)

SUL 을 만들 시기에 대하여는 아래의 질문을 고려하십시오.

- 어느 사용자를 동기화할 것인가?
- 어느 사용자를 동기화에서 제외할 것인가?
- 어디에 새 사용자를 만들 것인가?

참고 이들 유틸리티에 대한 자세한 내용은 [부록 D](#) 를 참조하십시오.

버전 1 2004Q3 으로 이전

Identity Synchronization for Windows 버전 1.0(또는 1.0 SP1) 에서 이전할 때 사용하는 절차는 처음 1 2004Q3 을 설치할 때 사용하는 절차와 비슷하지만 몇 가지 다른 점이 있습니다.

참고 이전 절차는 [7 장](#)에서 설명합니다 .

Identity Synchronization for Windows 1 2004Q3 으로 마이그레이션하기 전에 다음의 사항에 유의해야 합니다 .

- 커넥터를 설치한 후 반드시 Directory Server 커넥터 상태 파일과 Active Directory 및 NT 커넥터 객체 캐시 파일을 직접 복구해야 합니다 . 각 Active Directory 및 NT 커넥터 객체 캐시를 저장할 충분한 디스크 공간 (/isw-home/persist 디렉토리 및 하위 디렉토리의 크기를 기준) 이 충분한지 확인하십시오 .
- 반드시 모든 버전 1.0 및 1.0 SP1 구성요소를 제거해야 합니다 .
1 2004Q3 설치 프로그램이 1.0 시스템의 남아 있는 부분을 발견하면 Directory Server 에 설치된 Identity Synchronization for Windows 스키마와 컴퓨터에 설치된 실제 Identity Synchronization for Windows 이진에서 문제가 발생할 수 있습니다 .

참고 더 자세한 내용은 "[1.0 제거에 실패한 경우의 작업 방법](#) " 페이지 [206](#) 를 참조하십시오 .

- 반드시 1.0 용으로 설치되었던 동일한 플랫폼 및 하드웨어 구조에 Identity Synchronization for Windows 1 2004Q3 구성요소를 설치해야 합니다 .

Active Directory 와 비밀번호 동기화

Windows 2000 의 기본 비밀번호 정책은 Windows 2003 에서 변경되었으며 기본적으로 비밀번호를 더 엄격히 적용합니다 .

Identity Synchronization for Windows 서비스는 반드시 때때로 암호가 없는 항목을 만들어야 합니다 (예 : Directory Server 에서 Active Directory 로의 resync -c 실행 동안) . 따라서 Active Directory(Windows 2000 또는 2003 에서 실행) 나 Directory Server 에서 비밀번호 정책을 사용하는 경우 사용자 작성 오류가 발생할 수 있습니다 .

Active Directory 나 Directory Server 에서 비밀번호 정책을 사용 안 하도록 설정할 필요는 없으나 서로 다른 시스템에서 비밀번호 정책을 실행하는 데 관련된 문제를 이해해야 합니다 .

Windows 2003 Server Standard 또는 Enterprise Edition 에서 Active Directory 와 암호를 동기화하려는 경우 다음의 중요한 설치 정보를 숙지하십시오 .

- Windows 에서 설치하는 경우 Solaris 에 Active Directory 커넥터를 설치할 수 있습니다 .

참고	Active Directory 커넥터는 Windows 2000 및 Windows 2003 Server 모두에서 Active Directory 와 작동합니다 .
-----------	--

- Windows 2000 의 Active Directory 에서와 동일한 프로시저를 사용하여 Windows 2003 Server 용 디렉토리 소스 , 전역 카탈로그 및 동기화 사용자 목록을 만들 수 있습니다 .
- Windows 2003 Server 에서 기본 암호 정책은 엄격한 암호를 사용하며 , 이는 Windows 2000 의 기본 암호 정책과 다릅니다 .

이 단원의 나머지 내용은 다음과 같습니다 .

- " [비밀번호 정책 실행](#) " [페이지 66](#): Windows 또는 Directory Server 에서 비밀번호 정책을 반드시 실행해야 하는 경우 이 부분을 읽고 Active Directory 와 Directory Server 사이에서 비밀번호 정책이 동기화 결과에 어떤 영향을 미치는지 숙지하십시오 .
- " [비밀번호 정책 예](#) " [페이지 71](#): 여기에서는 다양한 시나리오에 대한 비밀번호 정책 예를 제공합니다 .

비밀번호 정책 실행

여기에서는 Windows 2003 Server, Windows 2000 및 Sun Java System Directory Server 5 2004Q2 의 Active Directory 용 비밀번호 정책이 동기화 결과에 영향을 미치는 방법에 대하여 설명합니다 .

다음과 같은 내용으로 구성됩니다 .

- " [개요](#) " [페이지 67](#)
- " [중요 참고 내용](#) " [페이지 67](#)
- " [비밀번호 정책 예](#) " [페이지 71](#)
- " [오류 메시지](#) " [페이지 72](#)

개요

Active Directory(또는 Directory Server) 에서 해당 시스템의 비밀번호 정책 요구 사항에 맞는 사용자를 만드는 경우 사용자가 만들어지고 두 시스템에서 적절히 동기화됩니다 . 두 시스템 모두에서 비밀번호 정책을 사용하는 경우 비밀번호는 반드시 두 시스템 모두의 정책을 만족해야 하며 , 그렇기 않은 경우 동기화된 사용자 생성이 실패하게 됩니다 .

- Active Directory 에서 비밀번호 정책 기능을 사용하는 경우 Directory Server 에서 또한 이와 일치하거나 유사하게 구성된 비밀번호 정책을 사용해야 합니다 .
- Active Directory 와 Directory Server 모두에서 일관적인 비밀번호 정책을 만들 수 없는 경우에는 비밀번호 및 사용자 작성용 권한 소스로 취급되는 측에 비밀번호 정책을 사용해야 합니다 . 그러나 일부 비밀번호 정책 구성으로 인하여 원하는 대로 사용자 작성 작업이 수행될 수 없는 경우도 있습니다 .

중요 참고 내용

다음에서는 비밀번호 정책에 대한 중요한 정보를 제공합니다 .

- ["Directory Server 비밀번호 정책 " 페이지 67](#)
- ["Active Directory 비밀번호 정책 " 페이지 67](#)
- [" 비밀번호 없이 계정 생성 " 페이지 68](#)

Directory Server 비밀번호 정책

Active Directory 에 Directory Server 비밀번호 정책을 위반하는 사용자를 만들 경우 , 해당 사용자가 생성되어 Directory Server 에 동기화되지만 비밀번호는 부여받지 못하게 됩니다 . 새 사용자가 Directory Server 로 로그인할 때까지 비밀번호가 설정되지 않으며 , 이 때 요청시 비밀번호 동기화가 설정됩니다 . 이 때 비밀번호가 Directory Server 비밀번호 정책을 위반하므로 로그인이 실패하게 됩니다 .

이러한 상황은 여러 가지 방법으로 복구할 수 있습니다 .

- 사용자가 이후 Active Directory 에 로그인할 때 암호를 변경하도록 합니다 .
- Active Directory 에서 사용자 비밀번호를 변경하고 새 비밀번호가 Directory Server 비밀번호 정책 요구사항에 맞는지 확인합니다 .

Active Directory 와 Directory Server 에 설정된 비밀번호 정책이 동등한지 (또는 가능한 한 유사한지) 확인해야 할 수 있습니다 .

Active Directory 비밀번호 정책

Active Directory 비밀번호 정책을 만족하지 않는 사용자를 Active Directory 에 만드는 경우 해당 사용자가 반드시 Directory Server 에 만들어집니다 .

- Active Directory 는 실제로 사용자를 "임시적으로" 만들며, 이 후 비밀번호가 비밀번호 정책 요구 사항을 만족하지 않으면 해당 항목을 삭제합니다. 결과적으로 Active Directory 커넥터는 이 임시 추가내용을 확인하고 Directory Server 측에 사용자를 만듭니다. 사용자는 Directory Server 에 비밀번호가 없게 되므로 누구도 사용자로 로그인할 수 없게 됩니다. 또한 이들 항목은 Active Directory 의 유효한 항목으로 연결되지 않습니다. Active Directory 에서 Directory Server 로 삭제가 동기화되는 경우 임시로 생성된 사용자는 자동으로 삭제됩니다.
- Directory Server 의 사용자가 비밀번호 없이 만들어집니다. 항목에 비밀번호가 없는 경우 Directory Server 는 사용자 작성에 대하여 비밀번호 정책을 실행하지 않습니다.

이러한 상황은 여러 가지 방법으로 해결할 수 있습니다. 많이 사용되는 방법은 Active Directory 에서 Directory Server 로 삭제를 동기화하는 방법입니다. 다른 방법으로 Directory Server 에서 해당 사용자를 제거하고 Active Directory 에서 Active Directory 비밀번호 정책에 맞는 비밀번호를 포함하여 사용자를 추가하는 방법입니다. 이 방법을 사용하면 Directory Server 에서 사용자를 만들고 적절히 연결할 수 있습니다. Directory Server 의 사용자가 처음으로 Active Directory 에 로그인하고 비밀번호를 변경하면 비밀번호가 무효화됩니다.

- Directory Server 에서 해당 사용자를 삭제하지 않고 새 비밀번호로 Active Directory 에서 해당 사용자를 다시 추가하려 하면 Directory Server 에 사용자가 이미 존재하므로 Directory Server 로의 ADD 가 실패합니다. 이들 항목은 서로 링크되지 않으며 idsync resync 명령을 실행하여 두 개의 별도 계정을 링크해야 합니다.
- idsync resync 명령을 사용하는 경우 반드시 Active Directory 에서 Directory Server 의 항목으로 연결된 계정의 비밀번호를 재설정해야 합니다. 비밀번호를 재설정하면 Directory Server 에서 해당 비밀번호가 무효화되며, 따라서 이 후 사용자가 새 Active Directory 비밀번호로 Directory Server 에 인증하면 요청시 동기화가 실행되어 Directory Server 비밀번호를 업데이트합니다.

비밀번호 없이 계정 생성

재동기화 등의 상황에 따라 이러한 Identity Synchronization for Windows 는 반드시 비밀번호 없이 계정을 만들어야 합니다.

Directory Server Identity Synchronization for Windows 가 비밀번호 없이 항목을 Directory Server 에 만드는 경우 userpassword 속성을 {PSWSYNC}*INVALID*PASSWORD* 으로 설정합니다. 사용자는 비밀번호를 재설정할 때까지 Directory Server 로 로그인할 수 없습니다. 이에 대한 예외는 resync 를 -i NEW_USERS 또는 NEW_LINKED_USERS 옵션과 함께 사용하는 경우입니다. 이 경우 resync 는 새 사용자의 비밀번호를 무효화하여 다음 사용자가 로그인 할 때 요청시 비밀번호 동기화가 시작되도록 합니다.

Active Directory Identity Synchronization for Windows 가 비밀번호 없이 Active Directory 에서 항목을 만드는 경우 사용자의 비밀번호를 Active Directory 비밀번호 정책 요구 사항에 맞는 강력한 무작위 비밀번호로 설정합니다 . 이 경우 경고 메시지가 기록되며 사용자는 비밀번호를 재설정할 때까지 Active Directory 에 로그인할 수 없습니다 .

다음 표는 Identity Synchronization for Windows 의 작업 동안 발생할 수 있는 몇 가지 서로 다른 시나리오에 대한 설명입니다 .

- 암호 정책이 동기화에 영향을 미치는 방식은 의 설명과 같습니다 .
- 비밀번호 정책이 재동기화에 영향을 미치는 방식은 의 설명과 같습니다 .

비밀번호가 동기화된 상태를 유지하는데 도움이 되도록 이 지침의 정보를 사용합니다 . (시스템마다 구성이 다를 수 있으므로 이 표에서 모든 가능한 구성 시나리오를 설명하지는 않습니다 .)

표 2-4) 비밀번호 정책이 동기화 작동에 영향을 미치는 방식

시나리오			결과		
사용자의 원래 생성 위치	사용자가 충족하는 비밀번호 정책 대상		사용자 생성 위치		설명
	Directory Server	Active Directory	Directory Server	Active Directory	
Active Directory	예	예	예	예	
	예	아니오	예 (설명 참조)	아니오	사용자가 Directory Server 에 생성됩니다 . 그러나 Active Directory 에서 Directory Server 로 삭제가 동기화되면 이 사용자는 즉시 삭제됩니다 . 더 자세한 내용은 "Active Directory 비밀번호 정책 " 페이지 67 을 참조하십시오 .
	아니오	예	예	예	더 자세한 내용은 " 중요 참고 내용 " 페이지 67 을 참조하십시오 .
	아니오	아니오	예 (설명 참조)	아니오	사용자가 Directory Server 에 생성되었습니다 . 그러나 Active Directory 에서 Directory Server 로 삭제가 동기화되면 이 사용자는 즉시 삭제됩니다 . 더 자세한 내용은 "Active Directory 비밀번호 정책 " 페이지 67 을 참조하십시오 .
Directory Server	예	예	예	예	
	예	아니오	예	아니오	
	아니오	예	아니오	아니오	
	아니오	아니오	아니오	아니오	

표 2-5) 비밀번호 정책이 재동기화 작동에 영향을 미치는 방식

시나리오			
Resync 명령	사용자가 충족하는 비밀번호 정책 대상		결과
	Directory Server	Active Directory	
resync -c -o Sun	해당 없음	예	사용자가 Active Directory 에 생성되지만 로그인 할 수 없습니다 . 더 자세한 내용은 " 비밀번호 없이 계정 생성 " 페이지 68 을 참조하십시오 .
	해당 없음	아니오	사용자가 Active Directory 에 생성되지만 로그인 할 수 없습니다 . 더 자세한 내용은 " 비밀번호 없이 계정 생성 " 페이지 68 을 참조하십시오 .
resync -c -i NEW_USERS NEW_LINKED_USERS	예	해당 없음	사용자가 Directory Server 에 만들어지면 해당 사용자가 처음 로그인할 때 비밀번호가 설정됩니다 . 더 자세한 내용은 " 비밀번호 없이 계정 생성 " 페이지 68 을 참조하십시오 .
	아니오	해당 없음	사용자가 Directory Server 에 생성되지만 비밀번호가 Directory Server 비밀번호 정책에 위반되므로 로그인할 수 없습니다 . 자세한 내용은 " 중요 참고 내용 " 페이지 67 및 " 비밀번호 없이 계정 생성 " 페이지 68 를 참조하십시오 .
resync -c	예	해당 없음	사용자가 Directory Server 에 생성되지만 Active Directory 또는 Directory Server 에 새 비밀번호 값을 설정할 때까지 로그인할 수 없습니다 . 더 자세한 내용은 " 비밀번호 없이 계정 생성 " 페이지 68 을 참조하십시오 .
	아니오	해당 없음	사용자가 Directory Server 에 생성되지만 Active Directory 또는 Directory Server 에 새 비밀번호 값을 설정할 때까지 로그인할 수 없습니다 . 더 자세한 내용은 " 비밀번호 없이 계정 생성 " 페이지 68 을 참조하십시오 .

비밀번호 정책 예

여기에서는 다음 내용의 Active Directory 와 Directory Server 비밀번호 정책을 사용하는 여러 가지 시나리오에 대하여 설명합니다 .

- **Active Directory:**

- 비밀번호 이력 실행 : 20 일
- 최대 비밀번호 지속 시간 : 30 일
- 최소 비밀번호 지속 시간 : 0 일
- 최소 비밀번호 길이 : 7 문자
- 비밀번호가 복잡성 요구 사항을 만족해야 함 : 사용
- **Directory Server:**
 - 재설정 후 사용자가 반드시 비밀번호를 변경해야 함
 - 사용자가 비밀번호를 변경할 수 있음
 - 이력에 보관할 비밀번호 20 개
 - 비밀번호 만료 기간 30 일
 - 비밀번호 만료 5 일 전에 경고 보냄
 - 비밀번호 구문 검사 : 비밀번호 최소 길이 7 문자

오류 메시지

코어 시스템에 있는 중앙 기록기 audit.log 파일에서 다음의 오류 메시지를 확인하십시오 .

요청시 동기화 동안 비밀번호 정책으로 인하여 DS 의 비밀번호를 업데이트할 수 없음 :

```
WARNING 125 CNN100 hostname "DS Plugin (SUBC100): unable to update password of entry 'cn=John Doe,ou=people,o=sun', reason: possible conflict with local password policy"
```

참고

Windows 2003 용 비밀번호 정책에 대한 자세한 내용은 http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dsscc_aut_xbby.asp 를 참조하십시오 .

Directory Server 5 2004Q2 용 비밀번호 정책에 대한 자세한 내용은 다음을 참조하십시오 .

http://docs.sun.com/db/coll/DirectoryServer_04q2

SSL 작업용으로 Windows 구성

Directory Server 에서 Windows Active Directory 서버로 비밀번호 변경 내용을 전달 하려는 경우 반드시 각 Active Directory 서버가 SSL 을 사용하도록 구성해야 하며 고급 암호화 팩을 설치해야 합니다 .

다음에서 설명하는 Microsoft Certificate Services Enterprise Root 인증 기관에서 자동으로 자격 증명을 받아 Active Directory 의 SSL 상의 LDAP 가 자동으로 사용 설정된 경우 , Identity Synchronization for Windows Active Directory 커넥터 설치 프로그램은 자동으로 Active Directory 커넥터에 SSL 을 설정합니다 .

<http://support.microsoft.com/default.aspx?scid=kb;en-us;q247078>

그러나 SSL 상의 LDAP 는 다음 MSDN 기술 노트에 설명한 대로 더 쉽게 구성할 수 있습니다 .

<http://support.microsoft.com/default.aspx?scid=kb;en-us;321051>

이 경우 SSL 통신용으로 신뢰된 인증서가 필요하도록 하면 반드시 "**Active Directory 커넥터에서 SSL 사용**" [페이지 293](#)의 설명과 같이 커넥터의 인증서 데이터베이스에 해당 인증서를 직접 설치해야 합니다 .

설치 및 구성 결정

여기에서는 Identity Synchronization for Windows 를 구현할 때의 설치 및 구성에 대하여 요약하고 선택할 수 있는 내용에 대하여 설명합니다 . 설치를 시작하기 전에 이러한 내용을 숙지하도록 하십시오 . 이 절에서 다루는 내용은 다음과 같습니다 .

- [코어 설치](#)
- [코어 구성](#)
- 커넥터 및 Directory Server 플러그인 설치
- 명령줄 유틸리티 사용

코어 설치

코어를 설치할 때 반드시 다음 정보를 입력해야 합니다 .

- **구성 디렉토리 호스트 및 포트** : Identity Synchronization for Windows 구성 정보가 저장될 Directory Server 인스턴스용 구성 디렉토리 호스트 및 포트를 지정합니다.

SSL 포트를 구성 디렉토리 포트에 구성할 수 있으며, 이렇게 하는 경우 반드시 설치 과정 동안 포트를 SSL 포트에 지정해야 합니다.

참고 Identity Synchronization for Windows 는 *localhost* 로 설치되는 구성 디렉토리는 지원하지 않습니다.

- **루트 접미어** : 구성 디렉토리의 루트 접미어를 지정합니다. 모든 구성 정보는 이 접미어 아래에 저장됩니다.
- **관리자의 이름 및 비밀번호** : 구성 Directory Server 용 자격 증명을 지정합니다.
- **구성 비밀번호** : 중요한 구성 정보를 보호할 보안 비밀번호를 지정합니다.
- **파일 시스템 디렉토리** : Identity Synchronization for Windows 를 설치할 위치를 지정합니다. 코어는 반드시 Directory Server Administration Server 와 동일한 디렉토리에 저장해야 합니다.
- **사용하지 않는 포트 번호** : 사용 가능한 Message Queue 인스턴스용 포트 번호를 지정합니다.

코어 구성

코어를 구성할 때 반드시 다음 정보를 입력해야 합니다.

- **Sun Java System 디렉토리 스키마 서버** : 구성 디렉토리에서 로드할 Directory Server 데이터를 지정합니다.
- **사용자 객체 클래스 (Directory Server 전용)** : 사용자 유형을 결정할 때 사용할 사용자 객체 클래스를 지정합니다. Identity Synchronization for Windows 는 이 객체 클래스에 기반하여 속성 목록 (비밀번호 속성 포함) 을 유도합니다. 이 목록은 스키마에서 채워집니다.
- **동기화된 속성** : Directory Server 와 Windows 환경 사이에서 동기화될 사용자 항목 속성을 지정합니다.
- **수정, 작성 및 삭제 흐름** : Sun 과 Windows 시스템 사이에서 수정, 작성 및 삭제가 전달되는 방법을 지정합니다. 옵션 :
 - Sun 에서 Windows 로
 - Windows 에서 Sun 으로

○ 양방향으로

Sun 및 Windows 시스템 사이에서 객체 활성화 및 비활성화 동기화를 전달할 것인지 지정하고 이들 객체의 동기화 방법을 지정합니다.

- **전역 카탈로그** : 전역 카탈로그 (Active Directory 토폴로지 및 스키마 정보용 저장소) 를 지정합니다.
- **Active Directory 스키마 제어기** : Windows 전역 카탈로그에서 불러 올 Active Directory 스키마 소스의 FQDN(Fully Qualified Domain Name) 을 지정합니다.
- **구성 디렉토리** : Identity Synchronization for Windows 구성을 저장할 Directory Server 를 지정합니다.
- **Active Directory 소스** : Active Directory 도메인을 동기화할 때 사용할 소스를 지정합니다.
- **Windows NT 기본 도메인 제어기** : 동기화될 Windows NT 도메인과 각 도메인의 기본 도메인 제어기 이름을 지정합니다.
- **SUL(Synchronization User Lists)**: LDAP DIT 및 필터 정보를 사용하여 Directory Server, Active Directory 및 NT 에서 동기화될 사용자를 지정합니다.
- **Sun Java System Directory Servers**: 동기화될 사용자를 저장하는 Directory Server 인스턴스를 지정합니다.

커넥터 및 Directory Server 플러그인 설치

커넥터와 Directory Server 플러그인을 설치할 때 반드시 다음 정보를 입력해야 합니다.

- **구성 디렉토리 호스트 및 포트** : Identity Synchronization for Windows 구성 정보가 저장될 Directory Server 인스턴스용 구성 디렉토리 호스트 및 포트를 지정합니다.
- **루트 접미어** : 구성 디렉토리의 루트 접미어를 지정합니다. 코어 설치 동안 지정된 루트 접미어를 사용하십시오.
- **관리자의 이름 및 비밀번호** : 구성 Directory Server 용 자격 증명을 지정합니다.
- **구성 비밀번호** : 중요한 구성 정보를 보호할 보안 비밀번호를 지정합니다.
- **파일 시스템 디렉토리** : Identity Synchronization for Windows 를 설치할 위치를 지정합니다. 동일한 컴퓨터에 설치된 모든 구성요소에는 반드시 동일한 설치 경로가 있어야 합니다.
- **디렉토리 소스** : 커넥터 또는 플러그인을 설치할 디렉토리 소스를 지정합니다.

Directory Server 및 Windows NT 커넥터를 설치하는 경우 반드시 사용하지 않는 포트를 지정해야 합니다.

Directory Server 커넥터 및 플러그인을 설치하는 경우 반드시 커넥터 및 플러그인에 해당하는 Directory Server 용 호스트, 포트 및 자격 증명을 지정해야 합니다.

명령줄 유틸리티 사용

Identity Synchronization for Windows에서는 다음 유틸리티를 사용하여 명령줄에서 다양한 작업을 수행할 수 있습니다.

- `idsync` 스크립트를 다음 하위 명령과 함께 사용하여 Identity Synchronization for Windows 명령줄 유틸리티를 실행합니다.
 - `certinfo`: 구성 및 SSL 설정에 기반하여 자격 증명 정보를 표시합니다.
 - `changepw`: Identity Synchronization for Windows 구성 비밀번호를 변경합니다.
 - `prepds`: Identity Synchronization for Windows가 사용하도록 Sun Java System Directory Server 소스를 준비합니다.
 - `printstat`: 설치된 커넥터, 시스템 관리자 및 Message Queue의 상태를 인쇄합니다.
또한 `printstat` 명령을 사용하여 설치 프로세스를 완료하기 위하여 수행해야 하는 나머지 설치 및 구성 단계 목록을 표시할 수 있습니다.
 - `resetconn`: 구성 디렉토리의 커넥터 상태를 *uninstalled*로 재설정(하드웨어 또는 제거 프로그램 오류의 경우만 해당)
 - `resync`: 설치 과정의 일부분으로 기존 사용자를 재동기화 및 링크하고 디렉토리를 미리 채움
 - `startsync`: 동기화를 시작합니다.
 - `stopsync`: 동기화를 중지합니다.

참고

이들 유틸리티에 대한 자세한 내용은 [부록 A](#)을 참조하십시오.

- 다음 유틸리티를 사용하여 Identity Synchronization for Windows 1.0 또는 1.0 SP1에서 Identity Synchronization for Windows 1 2004Q3으로 이전합니다.

- forcepwchg: Identity Synchronization for Windows 버전 1.0에서 1 2004Q3으로의 마이그레이션 과정에서 비밀번호를 변경한 사용자에게 비밀번호를 변경하도록 요구합니다.
- importcnf: 내보내진 버전 1.0 구성 XML 문서 가져옴

참고 이들 유틸리티에 대한 자세한 내용은 [7 장](#)을 참조하십시오.

설치 점검 목록

이 점검 목록은 설치 과정을 보조하기 위한 것입니다. 이 목록을 인쇄하고 Identity Synchronization for Windows 를 설치하기 전에 다음 정보를 기록하십시오.

표 2-6) 코어 설치 점검 목록

필요한 정보	항목
구성 디렉토리 호스트 및 포트	
구성 디렉토리용 루트 접미어 (예 : dc=example,dc=com)	
Identity Synchronization for Windows 를 설치할 파일 시스템 디렉토리	
구성 Directory Server 관리자의 이름 및 비밀번호	
중요한 구성 정보를 보호하는 보안 구성 비밀번호	
Message Queue 인스턴스용 포트 번호	

표 2-7) 코어 구성 점검 목록

필요한 정보	항목
Active Directory 전역 카탈로그 (적용되는 경우)	
Directory Server 스키마 서버	
Directory Server 사용자 구조 및 보조 객체 클래스	
동기화된 속성	
사용자 항목 작성 흐름	

표 2-7) 코어 구성 점검 목록 (계속)

필요한 정보	항목
사용자 항목 수정 흐름	
사용자 항목 활성화 및 비활성화 흐름	
사용자 항목 삭제 흐름	
Sun Java System Directory Server 디렉토리 소스	
Active Directory 디렉토리 소스	
SUL(Synchronization User List)	
Windows 소스 필터 작성 표현식	
Sun Java System 소스 필터 작성 표현식	

표 2-8) 커넥터 및 Directory Server 플러그인 설치 점검 목록

필요한 정보	항목
구성 디렉토리 호스트 및 포트	
구성 디렉토리용 루트 접미어	
커넥터를 설치할 파일 시스템 디렉토리	
구성 Directory Server 관리자의 이름 및 비밀번호	
중요한 구성 정보를 보호하는 보안 구성 비밀번호	
디렉토리 소스	
Directory Server 및 Windows NT 용 사용하지 않은 포트	
커넥터 및 플러그인에 해당하는 Directory Server 용 호스트, 포트 및 자격 증명	

표 2-9) 사용자 연결 점검 목록

필요한 정보	항목
연결될 SUL	
동등한 사용자를 일치할 때 사용하는 속성	
XML 구성 파일	

표 2-10) 재동기화 점검 목록

필요한 정보	항목
SUL 선택	
동기화 소스 .	
대상 디렉토리 소스에 해당 사용자가 없는 경우 자동으로 사용자 항목을 만들겠습니까 ?	
Directory Server 비밀번호를 무효화하겠습니까 ?	
지정한 LDAP 필터와 일치하고 선택한 SUL에 존재하는 사용자만 동기화하겠습니까 ?	

코어 설치

이 장에서는 Identity Synchronization for Windows 설치 프로그램을 사용하는 방법과 Identity Synchronization for Windows 코어 구성요소를 설치하는 방법에 대하여 설명합니다.

정보는 다음과 같이 구성되었습니다.

- " 시작하기 전에 " 페이지 81
- " 설치 프로그램 시작 " 페이지 82
- " 코어 설치 " 페이지 85

시작하기 전에

Identity Synchronization for Windows 설치 작업을 시작하기 전에 다음 작업을 수행하십시오.

- 제 2 장, " 설치 준비 " 를 읽으십시오. 이 장에서는 설치 전제조건, 점검 목록 및 관리자 권한 요구 사항 등 중요한 정보가 있습니다.
- 이 제품에는 Java Runtime Environment(JRE) 가 제공되지 않습니다. 필요한 경우 다음 위치에서 Java Development Kit 를 다운로드할 수 있습니다.

<http://java.sun.com> or <http://www.java.com>

Solaris 또는 Windows 2000/2003 시스템에서 Identity Synchronization for Windows 설치 프로그램을 실행하려면 반드시 JRE 1.4.2_04(이상) 를 설치해야 합니다.

- **Windows 시스템 전용** : 코어 설치를 시작하기 전에 열려있는 Service Control Panel 창을 모두 닫아야 합니다. 그렇지 않은 경우 설치가 실패하게 됩니다.

- 컴퓨터에 Identity Synchronization for Windows 버전 1.0(또는 1.0 SP1) 이 설치된 경우 제 7 장 , "[Identity Synchronization for Windows 1 2004Q3 으로 마이그레이션](#) " 을 읽으십시오 .

참고

SUNWjss 패키지가 다른 응용 프로그램이 사용할 수 있도록 (Identity Synchronization for Windows 1.0 제외) 등록되지 않은 경우 Identity Synchronization for Windows 1.0 설치 프로그램은 이 패키지를 제거합니다 . 특히 이러한 상황은 Directory Server 5.2.2 를 설치한 경우 Solaris 컴퓨터에서 발생할 수 있으며 , 이 경우 제거 프로그램이 /usr/share/lib/mps/secv1 에서 jss3.jar 파일을 제거합니다 .

Identity Synchronization for Windows 11 2004Q3 로 마이그레이션할 때 이러한 상황이 발생하면 설치 프로그램이 필요한 파일이 없음을 보고하고 파일 이름을 설치 로그에 기록합니다 . 이 경우가 발생하면 반드시 필요한 패치 ("[Sun Java System 소프트웨어 요구 사항](#) " [페이지 53](#) 참조) 를 다시 설치하고 설치 프로세스를 다시 시작해야 합니다 .

- Identity Synchronization for Windows 버전 1.0 에서는 자동으로 Message Queue 가 설치되지만 *버전 1 2004Q3* 에서는 *설치되지 않습니다* . Message Queue 3.5 SP1 Enterprise Edition 이 미리 설치되어 있어야 합니다 .

Solaris 시스템 : Message Queue 와 Identity Synchronization for Windows 를 동일한 디렉토리에 설치하면 안 됩니다 .

설치 프로그램 시작

여기에서는 다음 플랫폼에서 Identity Synchronization for Windows 설치 프로그램을 다운로드 , 압축 해제 (또는 unzip) 및 실행하는 방법에 대하여 설명합니다 .

- "[Solaris SPARC](#)" [페이지 83](#)
- "[Solaris x86](#)" [페이지 83](#)
- "[Windows](#)" [페이지 84](#)

Solaris SPARC

다음과 같이 Solaris SPARC 운영 체제에서 Identity Synchronization for Windows 설치 프로그램을 준비하고 실행합니다.

1. root 로 로그인합니다.
2. `# mkdir isw12004Q3`을 입력하여 새 디렉토리를 만들고 이 디렉토리로 변경(`cd`)합니다.
3. 아직 제품 바이너리 파일(`isw-12004Q3.sparc-sun-solaris.tar.gz`)을 다운로드 하지 않았으면 설치 디렉토리로 다운로드합니다.
4. 다음 명령을 사용하여 제품 바이너리 파일의 압축을 해제합니다.
`# gunzip -dc isw-12004Q3.sparc-sun-solaris.tar.gz | tar -xvof -`
5. `isw12004Q3` 디렉토리에서 `installer` 디렉토리로 변경한 후 `./runInstaller.sh`를 입력하여 설치 프로그램을 실행합니다.

참고

텍스트 기반 모드에서 설치 프로그램을 실행하려면

`./runInstaller.sh -nodisplay`를 입력합니다.

`runInstaller.sh` 프로그램을 실행하면 Identity Synchronization for Windows가 자동으로 암호를 마스킹하여 해당 암호가 해독된 상태에서 반향되지 않도록 합니다.

Solaris x86

다음과 같이 Solaris x86 운영 체제에서 Identity Synchronization for Windows 설치 프로그램을 준비하고 실행합니다.

1. root 로 로그인합니다.
2. `# mkdir isw12004Q3`을 입력하여 새 디렉토리를 만들고 이 디렉토리로 변경(`cd`)합니다.
3. 아직 제품 이진 파일(`isw-12004Q3.x86-sun-solaris.tar.gz`)을 다운로드 하지 않았으면 설치 디렉토리로 다운로드합니다.
4. 다음 명령을 사용하여 제품 바이너리 파일의 압축을 해제합니다.
`# gunzip -dc isw-12004Q3.x86-sun-solaris.tar.gz | tar -xvof -`

5. isw12004Q3 디렉토리에서 installer 디렉토리로 변경한 후 **./runInstaller.sh** 를 입력하여 설치 프로그램을 실행합니다.

참고

텍스트 기반 모드에서 설치 프로그램을 실행하려면

./runInstaller.sh -nodisplay 를 입력합니다.

runInstaller.sh 프로그램을 실행하면 Identity Synchronization for Windows 가 자동으로 암호를 마스킹하여 보이게 반향되지 않도록 합니다.

Windows

다음과 같이 Windows 운영 체제에서 Identity Synchronization for Windows 설치 프로그램을 준비하고 실행합니다.

1. Administrator 로 로그인합니다.
2. # **mkdir isw12004Q3** 를 입력하여 새 디렉토리를 만듭니다.
3. isw12004Q3 디렉토리로 변경 (**cd**) 합니다.
4. 아직 제품 이진 파일 (isw-12004Q3-windows.zip) 을 다운로드 하지 않았으면 설치 디렉토리로 다운로드합니다.
5. isw-12004Q3-windows.zip 파일을 빈 디렉토리로 압축 해제합니다.
6. isw12004Q3 디렉토리에서 installer 디렉토리로 변경(**cd**)한 후 **setup.exe**를 입력하여 설치 프로그램을 실행합니다.

Identity Synchronization for Windows 설치 마법사가 표시됩니다.

참고

코어를 Administrator Server 루트에 설치하므로 Identity Synchronization for Windows 마법사는 설치에 필요한 대부분의 정보 (디렉토리 경로 및 이름 등) 를 감지하며 마법사 패널의 일부 필드를 자동으로 입력합니다.

누락되거나 잘못된 정보가 있는 경우 필요한 정보를 직접 입력할 수 있습니다.

코어 설치 방법은 다음 부분으로 계속하십시오 .

코어 설치

여기에서는 Solaris 와 Windows 운영 체제 모두에서 Identity Synchronization for Windows 코어를 설치하는 과정에 대하여 설명합니다 .

코어를 설치하기 전에 다음의 요구 사항에 유의해야 합니다 .

- **Solaris 시스템** : Solaris 서비스를 설치하고 실행하려면 반드시 루트 권한이 있어야 합니다 .

참고

반드시 루트로 프로그램을 설치해야 하지만 설치 후에는 루트가 아닌 사용자로 소프트웨어를 구성하여 Solaris 서비스를 실행할 수 있습니다 . (부록 C, "[Solaris 에서 루트가 아닌 사용자로 서비스 실행](#) ." 참조)

- **Windows 2000/2003 시스템** : Identity Synchronization for Windows 를 설치하려면 반드시 Administrator 권한이 있어야 합니다 .
- 이미 Administrator Server(버전 5 2004Q2 이상) 가 관리하는 서버 루트가 있는 디렉토리에 코어를 설치해야 하며 , 그렇지 않은 경우 설치 프로그램이 실패합니다 . (Directory Server 5 2004Q2 설치 프로그램을 사용하여 Administrator Server 를 설치할 수 있습니다 .)

다음과 같이 설치 마법사를 사용하여 Identity Synchronization for Windows 코어 구성요소를 설치합니다 .

1. 시작 화면이 표시되면 제공된 정보를 읽고 다음을 눌러 사용권 계약 패널로 이동합니다 .
2. 사용권 계약을 읽은 후 다음과 같이 선택합니다 .
 - 라이선스 계약 조건에 동의하고 다음 패널로 계속하려면 **Yes(Accept License)** 를 선택합니다 .
 - 설치 과정을 중단하고 설치 프로그램을 종료하려면 **No** 를 선택합니다 .
3. 구성 디렉토리 위치를 지정할 수 있도록 Configuration Location 패널이 표시 (그림 3-1) 됩니다 .

그림 3-1) 구성 디렉토리 위치 지정

코어 설치: 구성 위치

Sun Java(TM) System Identity Synchronization for Windows가 저장될 예정이거나 이미 저장된 구성 디렉토리 및 루트 컨텍스트에 대한 정보를 지정합니다.

구성 디렉토리 호스트:

구성 디렉토리 포트: ☐ 보안 포트

구성 루트 접미사:

다음 정보를 입력합니다.

- **구성 디렉토리 호스트** : Identity Synchronization for Windows 구성 정보가 저장되는 Sun Java 시스템 Directory Server 인스턴스 (로컬 Administrator Server 와 연계) 의 정규화된 도메인 이름 (FQDN) 을 입력합니다.

로컬 컴퓨터의 인스턴스 또는 다른 컴퓨터에서 실행되는 인스턴스를 지정할 수 있습니다.

참고 잘못된 자격 증명 또는 호스트 이름에 대한 경고를 방지하려면 설치 프로그램이 실행되는 컴퓨터로 DNS 해석 가능한 호스트 이름을 입력해야 합니다.

- **구성 디렉토리 포트** : 구성 디렉토리를 설치할 포트를 지정합니다. (기본 포트는 389 입니다.)

보안 통신을 사용 설정하려면 Secure Port 옵션을 사용하도록 설정하고 SSL 포트를 지정합니다. (기본 SSL 포트는 636 입니다.)

프로그램이 구성 디렉토리에 SSL 을 사용한다는 것을 감지하면 모든 Identity Synchronization for Windows 구성요소가 SSL 을 사용하여 구성 디렉토리와 통신하게 됩니다.

참고

Identity Synchronization for Windows 는 중요한 구성 정보를 구성 Directory Server 로 보내기 전에 암호화합니다 .

그러나 콘솔과 구성 디렉토리 사이에 추가의 전송 암호화를 원하는 경우 Administrator Server 와 구성 Directory Server 모두에서 SSL 을 사용해야 합니다 . 그런 후 , Directory Server 콘솔을 인증하려는 Administrator Server 사이의 연결을 보안 구성해야 합니다 . (자세한 내용은 *Sun Java 시스템 Administrator Server 5 2004Q2 Administration Guide* 를 참조하십시오 .)

- 구성 루트 접미어 : 메뉴에서 Identity Synchronization for Windows 구성을 저장할 루트 접미어를 선택합니다 .

참고

프로그램이 루트 접미어를 찾을 수 없으며 정보를 직접 입력해야 하는 경우 (또는 기본값을 변경하는 경우) 반드시 Refresh 를 눌러 루트 접미어의 목록을 다시 만들어야 합니다 . (반드시 구성 Directory Server 에 있는 루트 접미어를 지정해야 합니다 .)

4. Next 를 눌러 디렉토리 자격 증명 구성 패널을 엽니다 .

그림 3-2) Administrator 의 자격 증명 지정

코어 설치: 구성 디렉토리 증명서

구성 디렉토리 서버에 액세스하기 위해 관리 증명서를 지정해야 합니다.

관리자 사용자 ID:

관리자 비밀번호:

5. 구성 디렉토리 Administrator 의 사용자 ID 및 비밀번호를 입력합니다 .
 - 사용자 ID 로 admin 을 지정하면 User ID 와 DN 을 지정할 필요가 없습니다 .

- 다른 사용자 ID를 사용하는 경우 반드시 ID와 전체 DN을 지정해야 합니다.
예 : `cn=Directory Manager`.

참고 구성 디렉토리와의 통신에 SSL 을 사용하지 않는 경우 ([단계 3, 페이지 86](#) 참조) 이들 자격 증명은 암호화 없이 전송됩니다 .

6. 작업을 완료했으면 Next 를 눌러 비밀번호 구성 패널을 엽니다 .

그림 3-3) 구성 비밀번호 지정

코어 설치: 구성 비밀번호

구성의 민감한 부분을 암호화하는 데 사용할 비밀번호를 제공하십시오. 콘솔을 사용하고 명령행 유틸리티를 사용하거나 다른 구성요소를 설치할 경우 제공해야 하므로 이 비밀번호를 기억하십시오.

구성 비밀번호:

비밀번호 확인:

7. 자격 증명 등 중요한 구성 정보를 암호화할 때 사용할 비밀번호를 입력하고 확인해야 합니다 . 작업을 완료했으면 Next 를 누릅니다 .

참고 이 비밀번호는 다음의 경우 필요하므로 기억해 두도록 하십시오 .

- Identity Synchronization for Windows 콘솔에 액세스할 시
- 구성을 작성하거나 편집할 시
- 구성요소 설치 시
- 명령줄 유틸리티를 실행 시

구성 비밀번호의 변경에 대한 내용은 "[changepw 사용](#)" [페이지 308](#) 을 참조하십시오 .

Select Java Home 패널이 표시됩니다 (그림 3-4 참조). 프로그램은 설치된 구성 요소가 사용할 Java Virtual Machine 디렉토리의 위치를 자동으로 삽입합니다 .

그림 3-4) Java Home 디렉토리 지정

8. Java Home 디렉토리를 확인합니다 (반드시 JDK/JRE 1.4.2_04 이상).

- 위치가 적절하면 Next를 눌러 Select Installation Directories 패널([페이지 89](#))로 계속합니다 .
- 위치가 잘못되었으면 찾아보기를 눌러 Java 가 설치된 디렉토리를 찾아 선택합니다 . 예 :
 - **Solaris:** /var/java
 - **Windows:** C:\Program Files\j2sdk1.4.2_04

그림 3-5) 설치 디렉토리 지정

9. 제공된 텍스트 입력란에 다음 정보를 입력하거나 찾아보기를 눌러 사용 가능한 디렉토리를 찾아 선택합니다 .
- **서비스 루트 디렉토리 :** Directory Server 설치 서버 루트의 경로와 디렉토리 이름을 지정합니다 . 콘솔은 이 위치에 설치됩니다 .

참고

Windows 운영 체제의 경우 사용 가능한 서버 루트 디렉토리는 오직 하나이며 , 모든 제품은 이 위치에 설치됩니다 .

- **설치 디렉토리** (*Solaris 에 코어를 설치하는 경우에만 사용 가능*): 설치 디렉토리의 경로와 디렉토리 이름을 지정합니다. 코어 바이너리, 라이브러리 및 실행 파일이 이 디렉토리에 설치됩니다.
- **인스턴스 디렉토리** (*Solaris 에 코어를 설치하는 경우에만 사용 가능*): 인스턴스 디렉토리의 경로와 디렉토리 이름을 지정합니다. 변경되는 구성 정보 (로그 파일 등) 가 이 디렉토리에 저장됩니다.

10. Next 를 눌러 Message Queue 구성 패널로 계속합니다.

참고

Identity Synchronization for Windows 설치를 시작하기 전에 Message Queue 3.5 SP1 Enterprise Edition 이 설치되어 있어야 합니다.

Solaris 시스템 : Message Queue 와 Identity Synchronization for Windows 를 동일한 디렉토리에 설치하면 안 됩니다.

Windows 시스템 : 계속하기 전에 열려있는 Service Control Panel 창을 모두 닫아야 합니다. 그렇지 않은 경우 코어 설치가 실패하게 됩니다.

그림 3-6) Message Queue 구성

코어 설치: Message Queue 구성

이 제품에서는 이전의 기존 Message Queue를 사용해야 합니다. 설치 위치와 새 브로커 인스턴스의 전체 호스트 이름 및 포트를 지정하십시오.

설치 디렉토리:

/usr

찾아보기...

구성 디렉토리:

/var/imq

찾아보기...

전체 로컬 호스트 이름:

alclab-014.sfbay.sun.com

브로커 포트 번호:

7676

11. 제공된 텍스트 입력란에 다음 정보를 입력하거나 찾아보기를 눌러 사용 가능한 디렉토리를 찾아 선택합니다.

- **설치 디렉토리** : Message Queue 설치 디렉토리를 지정합니다.

- **구성 디렉토리** : Message Queue 인스턴스 디렉토리의 경로와 디렉토리 이름을 지정합니다.
- **정규화된 로컬 호스트 이름** : 로컬 호스트 컴퓨터의 정규화된 도메인(FQDN) 이름을 지정합니다. (각 호스트마다 하나의 Message Queue 브로커 인스턴스만 존재할 수 있습니다.)
- **브로커 포트 번호** : Message Queue 브로커가 사용할 사용되지 않는 포트를 지정합니다. (기본 포트는 7676 입니다.)

12. Next 를 눌러 설치 준비 패널을 표시합니다.

이 패널에서는 코어가 설치될 디렉토리 및 코어를 설치하기 위하여 필요한 공간 등, 설치에 관련된 정보가 제공됩니다.

- 표시된 정보가 적절하면 **Install Now**를 눌러 코어 구성요소를 설치합니다(여기에서 설치 프로그램은 이진, 파일 및 패키지를 설치합니다).
- 정보가 잘못되었으면 **Back** 를 눌러 변경합니다.

"Installing" 메시지가 잠시 표시된 후, 설치 프로그램이 구성 데이터를 지정된 구성 Directory Server 로 추가하는 동안 Component Configuration 패널이 표시됩니다. 이 작업에는 다음 내용이 포함됩니다.

- Message Queue 브로커 인스턴스 작성
- 스키마를 구성 디렉토리로 업로드
- 구현 특정 구성 정보를 구성 디렉토리로 업로드

이 작업에는 다소 시간이 걸리며 때로 잠시 멈출 수 있으므로 과정이 10 분을 넘기지 않는 경우 걱정할 필요는 없습니다. (설치 프로그램의 상태는 진행표시줄에서 확인할 수 있습니다.)

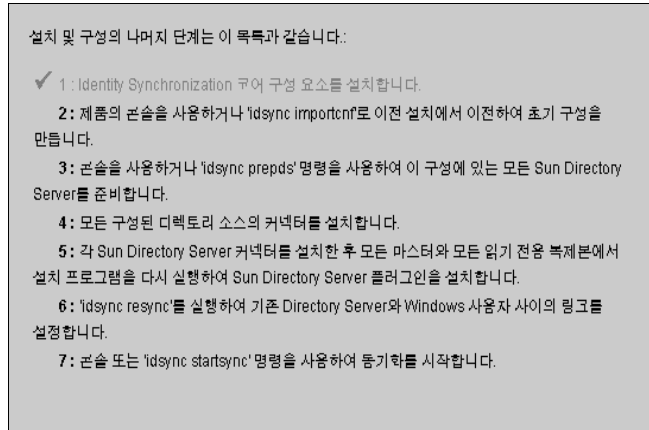
13. 구성요소 구성 작업이 완료되면 Installation Summary 패널이 표시되어 Identity Synchronization for Windows 가 성공적으로 설치되었음을 확인합니다.

설치된 파일과 파일의 위치 목록을 보려면 Details 버튼을 누릅니다.

14. Next 를 누르면 프로그램이 Identity Synchronization for Windows 를 성공적으로 설치 및 구성하는 데 반드시 수행해야 하는 나머지 단계를 결정합니다.

"Loading..." 메시지 다음 Remaining Installation 패널이 각각 짧게 표시된 후, 다음 패널 (그림 3-7) 이 표시됩니다. 이 패널에는 나머지 설치 및 구성 단계의 "To Do" 목록이 포함됩니다. (또한 콘솔의 Status 탭에서 이 패널에 액세스할 수 있습니다.)

그림 3-7) Identity Synchronization for Windows To Do 목록

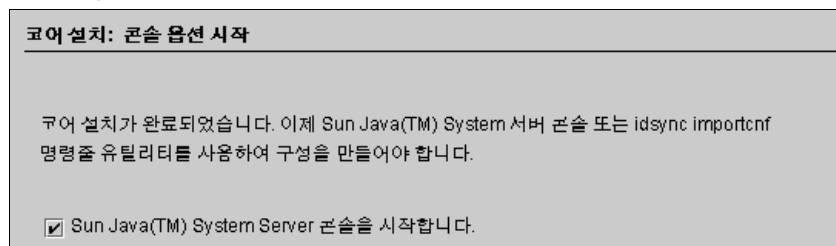


"To Do" 패널은 설치 및 구성 프로세스 전체에서 계속 표시됩니다 . 목록에서 완료된 단계는 흐리게 표시됩니다 .

이 시점에서 To Do 목록에는 일반적인 단계 목록이 포함됩니다 . 구성을 저장하면 프로그램에는 구현에 맞는 단계 목록이 제공됩니다 (예 : 반드시 설치해야 하는 커넥터).

15. 이 단계 목록을 확인한 후 Next 를 누르면 Start Console Option 패널이 표시되며 코어 설치가 완료되었음이 표시됩니다 .

그림 3-8) 콘솔 시작



16. 다음으로 반드시 코어 구성요소를 구성해야 하며, 이 작업은 Sun Java 시스템 콘솔에서 할 수 있습니다. (Start the Sun Java 시스템 Console 옵션은 기본으로 사용 설정되어 있습니다.)

Identity Synchronization for Windows 버전 1.0 또는 SP1 에서 Identity Synchronization for Windows 1 2004Q3 으로 마이그레이션하는 경우 idsync importcnf 명령줄 유틸리티를 사용하여 내보낸 1.0 또는 SP1 구성 XML 문서를 가져올 수 있습니다. (방법은 제 7 장, "Identity Synchronization for Windows 1 2004Q3 으로 마이그레이션 " 를 참조하십시오 .)

17. Finished 를 누릅니다 .
18. 콘솔을 사용하려는 경우 Sun Java 시스템 Console Login 대화 상자가 표시됩니다 (그림 3-9 참조).

그림 3-9) 콘솔로 로그인

사용자 ID:

암호:

관리 URL: ▼

확인(O) 취소(C) 도움말(H)

콘솔에 로그인하려면 반드시 다음 정보를 입력해야 합니다.

- **사용자 ID:** 컴퓨터에 Administrator Server를 설치할 때 지정한 Administrator의 사용자 ID를 입력합니다.
- **Password:** Administrator Server 설치 동안 지정한 Administrator의 비밀번호를 입력합니다.
- **Administration URL:** 다음 형식으로 Administrator Server의 현재 URL 위치를 입력합니다.

`http://<hostname.your_domain.domain:port_number>`

여기에서,

- `hostname.your_domain.domain` 은 Administrator Server를 설치할 때 선택한 컴퓨터 호스트 이름입니다.
- `port_number` 는 Administrator Server 용으로 지정한 포트입니다.

19. 자격 증명을 입력한 후 OK 를 눌러 대화 상자를 닫습니다.

20. 그런 후 구성 비밀번호를 묻는 메시지가 나타납니다 . 비밀번호를 입력하고 OK를 누릅니다 .

Sun Java 시스템 서버 콘솔 창이 표시되면 코어 구성을 시작할 수 있습니다 . 방법을 보려면 제 4 장 , " 코어 자원 구성 " 으로 계속하십시오 .

코어 자원 구성

Identity Synchronization for Windows 코어를 설치 (3 장 참조) 한 후 바로 코어 자원을 구성해야 합니다.

이 장에서는 콘솔을 사용하여 이들 자원을 추가 및 구성하는 방법을 설명하며, 다음의 내용으로 구성됩니다.

- "구성 개요" 페이지 95
- "Identity Synchronization for Windows 콘솔 열기" 페이지 96
- "디렉토리 소스 작성" 페이지 101
- "사용자 속성 선택 및 매핑" 페이지 125
- "시스템간 사용자 속성 전달" 페이지 131
- "Synchronization User Lists 작성" 페이지 148
- "구성 저장" 페이지 154

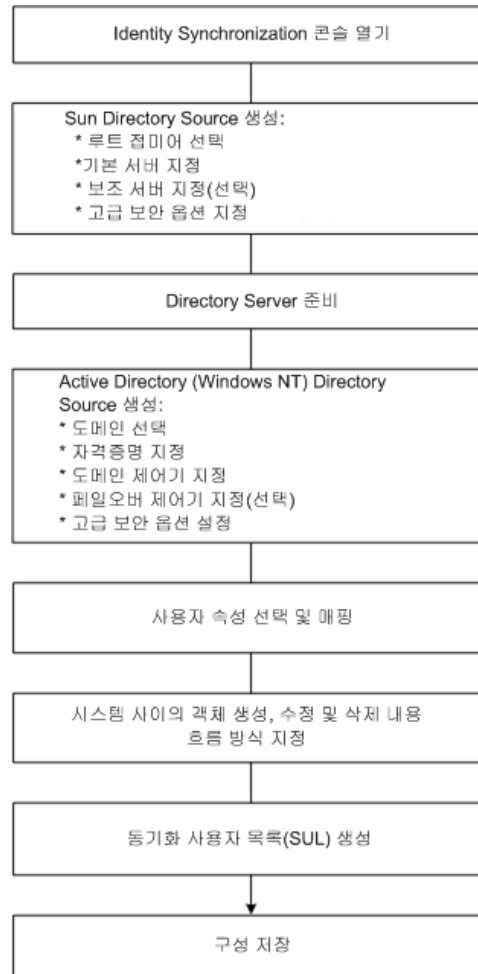
참고 코어 자원을 효과적으로 구성하려면 Directory Server 및 Active Directory 의 구성 및 운영에 대하여 알아야 합니다.

이들 자원을 (텍스트에 명시하지 않은 경우) 정해진 순서로 구성해야 하는 것은 아니지만 제품에 익숙해질 때까지 이 장에서 설명한 순서로 구성하면 시간을 절약하고 오류를 방지할 수 있습니다.

구성 개요

구현에 대하여 코어를 구성하는 단계는 에 보이는 것과 같습니다.

그림 4-1) 구현에 대하여 코어 자원 구성



Identity Synchronization for Windows 콘솔 열기

참고 아직 Sun Java System 서버 콘솔에 로그인하지 않았으면 [페이지 93](#)로 되돌아가 방법을 참조하십시오 .

Sun Java System 서버 콘솔 창 (그림 4-2) 에는 제어할 수 있는 모든 서버와 자원 목록이 표시되며 시스템에 대한 정보가 제공됩니다 .

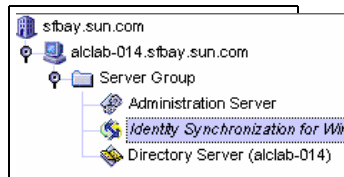
그림 4-2) Sun Java System 서버 콘솔



Identity Synchronization for Windows 콘솔을 열려면 다음과 같이 합니다 .

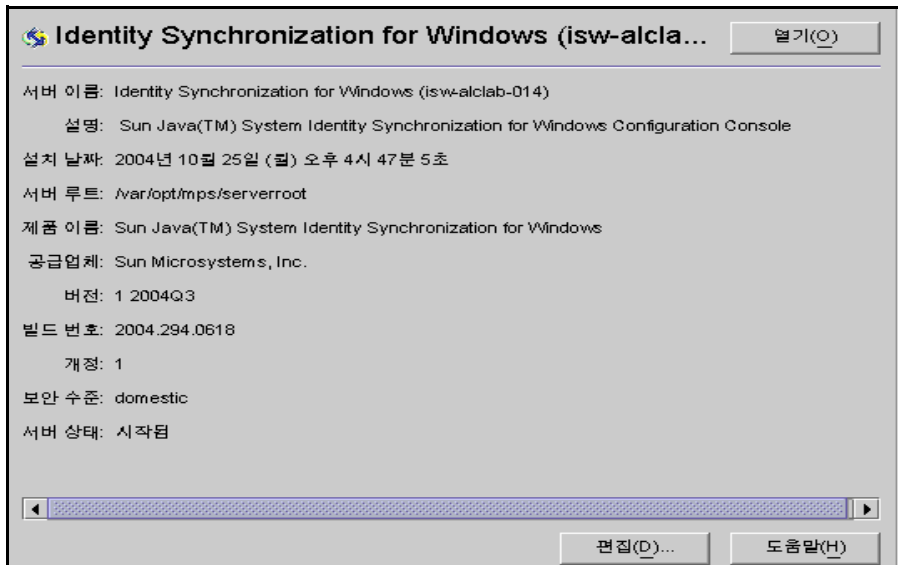
1. Servers and Applications 탭의 Identity Synchronization for Windows 인스턴스가 속한 서버 그룹이 있는 탐색 트리에서 hostname 노드를 선택합니다 .
2. Server Group 노드를 확장하고 Identity Synchronization for Windows 노드를 선택합니다 (그림 4-3 참조) .

그림 4-3) Server Group 확장



정보 패널이 변경되어 Identity Synchronization for Windows 와 시스템에 대한 정보가 제공됩니다 (예는 그림 4-4 참조) .

그림 4-4) Identity Synchronization for Windows 정보 패널



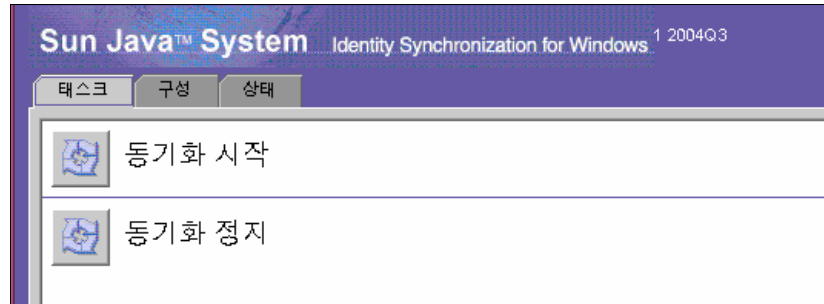
3. 열기 버튼 (패널의 오른쪽 상단에 위치) 을 누릅니다 .

참고	편집 버튼 (패널의 하단에 위치) 을 사용하면 서버 이름과 설명을 편집할 수 있습니다 .
-----------	---

4. 코어 설치(페이지 88 참조)에서 지정한 구성 비밀번호를 입력하라는 프롬프트가 표시됩니다 . 비밀번호를 입력하고 확인을 누릅니다 .

Identity Synchronization for Windows 콘솔에 다음과 같이 표시됩니다 .

그림 4-5) Identity Synchronization for Windows 콘솔 : 태스크 탭



이 창에는 세 개의 탭과 상태 표시줄이 있습니다.

- **태스크(기본값)**: 이 탭을 사용하여 Sun과 Windows 시스템 사이의 동기화를 시작 및 중지합니다. (서비스의 시작 및 중지에는 제 6 장, "기본 사용자 동기화"에 있습니다.)

참고

동기화 서비스의 시작 및 중지를 Windows 서비스의 시작 및 중지와 혼동하면 안 됩니다.

Windows 서비스를 시작 또는 중지하려면 시작 > 콘솔 > 관리 도구 > 컴퓨터 관리 > 서비스를 선택하고 Windows 콘솔에서 수행해야 합니다.

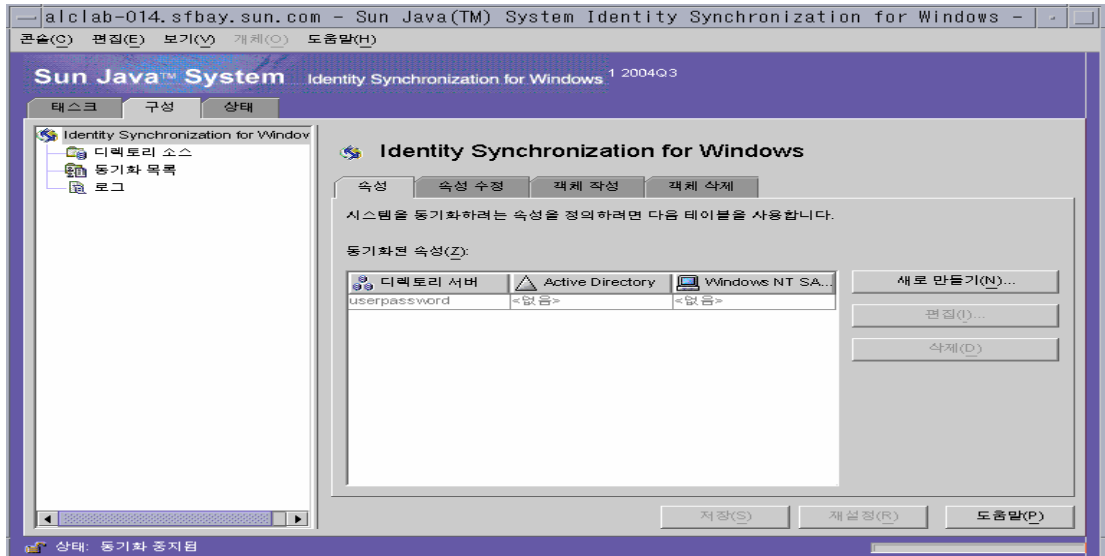
- **구성**: 시스템을 동기화용으로 구성하려면 이 탭을 사용합니다.
- **상태**: 이 탭을 사용하여 다음 작업을 수행합니다.
 - 시스템 구성요소 (커넥터 등) 상태를 모니터링합니다.
 - 구성 및 동기화 동안 Identity Synchronization for Windows 가 생성한 감사 및 오류 로그를 확인합니다.
 - 설치 및 구성 To Do 목록을 업데이트 및 확인합니다.
 - **Status Bar**: 여기에서 시스템 상태를 간단히 확인할 수 있습니다.

참고

상태 탭에 대한 더 자세한 내용은 10 장을 참조하십시오.

5. 구성 탭을 선택합니다 (그림 4-6 참조).

그림 4-6) Identity Synchronization for Windows 콘솔 : 구성 탭



Configuration 패널은 다음과 같은 탭으로 구성됩니다.

- **속성** : 시스템 사이에서 동기화할 속성을 지정하려면 이 탭을 사용합니다.
- **속성 수정** : 이 탭을 사용하여 비밀번호, 속성 수정 및 객체 비활성화 등을 시스템 사이에서 전달하는 방법을 지정합니다.
- **객체 작성** : 이 탭을 사용하여 새로 만든 비밀번호와 속성이 시스템 사이에서 전달되는 방법을 지정하고 동기화 동안 Identity Synchronization for Windows 가 만든 객체의 초기 값을 지정합니다.
- **객체 삭제** : 이 탭을 사용하여 삭제된 비밀번호와 기타 속성을 시스템 사이에서 전달하는 방법을 지정합니다.

반드시 하나 이상의 Sun Java System Directory Server Directory Server 와 하나 이상의 Windows 서버 디렉토리 소스 (Active Directory 또는 Windows NT) 를 구성해야 합니다 . 방법은 다음 단원으로 계속하십시오 .

디렉토리 소스 작성

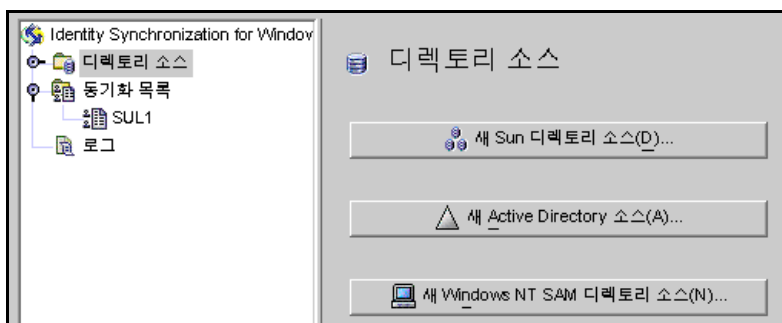
반드시 다음 순서대로 디렉토리 소스를 만들어야 합니다. (순서는 동기화하는 소스에 따라 다릅니다.)

1. "Sun Java System 디렉토리 소스 작성 " 페이지 102
2. "Directory Server 준비 " 페이지 109
3. "Active Directory 소스 작성 " 페이지 113
4. "Windows NT SAM 디렉토리 소스 작성 " 페이지 122

참고 최소한 반드시 하나 이상의 Sun Java System 디렉토리 소스와 하나 이상의 Windows 디렉토리 소스 (Active Directory 및 NT SAM) 을 구성해야 합니다.

탐색 트리에서 Directory Sources 노드를 선택하면 Directory Source 패널이 표시됩니다 (그림 4-7 참조).

그림 4-7) Directory Sources 패널 사용



Sun Java System 디렉토리 소스 작성

참고 각 Sun Java System 디렉토리 소스는 마스터가 최고 네 개인 복제 시나리오에서 구현될 수 있는 커넥터와 플러그인에 연결됩니다. 모든 Directory Server 플러그인이 Windows 디렉토리 소스에서 비밀번호 검증을 처리할 수 있으며 사용자는 원하는 마스터에서 비밀번호를 변경할 수 있습니다. 그러나 Directory Server 커넥터는 Windows 디렉토리 소스에서의 비밀번호를 최대 두 개의 마스터 (기본 및 보조)와 동기화할 수 있습니다. Directory Server 복제는 이들 두 마스터 중 하나에서 변경된 내용을 토폴로지의 다른 서버로 복제합니다.

새 Sun Java System 디렉토리 소스를 만들려면 다음과 같이 합니다.

1. 새 Sun 디렉토리 소스 버튼을 눌러 Define Sun Java System Directory Source 마법사를 시작합니다.

그림 4-8) 루트 접미어 선택

<p>단계</p> <ol style="list-style-type: none"> 1. 루트 접미사를 선택합니다. 2. 우선 서버를 지정합니다. 3. 보조 서버를 지정합니다. 4. 고급 보안 옵션을 지정합니다. 	<p>루트 접미사를 선택합니다.</p> <p>동기화된 사용자 데이터를 저장할 루트 접미어를 선택합니다.</p> <p>루트 접미어(X): <input type="text" value="구성 디렉토리(D)"/></p> <div style="border: 1px solid black; padding: 5px;"> <p>dc=example, dc=com</p> <p>dc=sfbay, dc=sun, dc=com</p> </div> <p>앞의 목록은 알려진 구성 디렉토리 세트를 쿼리하여 만들어진 것입니다. 이 목록을 관리하려면 구성 디렉토리를 선택합니다.</p>
--	---

프로그램은 일련의 알려진 구성 디렉토리 소스를 쿼리하고 기존 루트 접미어 (또한 이름 지정 컨텍스트라고 함) 를 목록 창에 표시합니다.

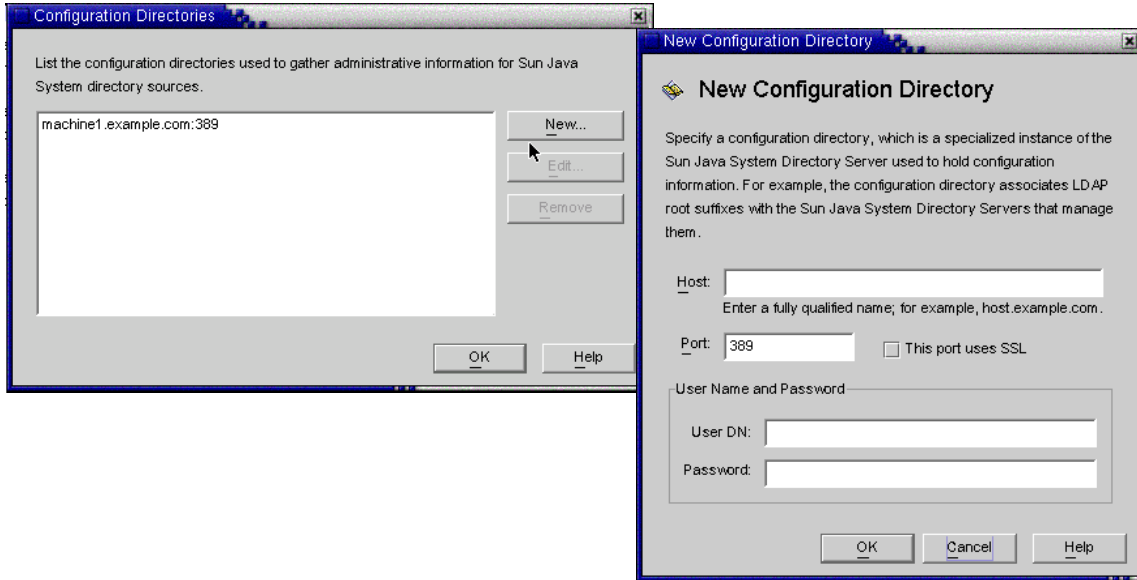
기본적으로 프로그램은 제품을 설치한 구성 디렉토리를 알고 있으며, 구성 디렉토리에 알려진 루트 접미어는 목록 창에 표시됩니다.

2. 목록창에서 사용자가 위치한 루트 접미어를 선택합니다. (목록의 루트 접미어가 여러 개인 경우 사용자가 위치한 접미어를 한 개 선택합니다.) 다음을 눌러 단계 3 로 계속합니다.

동기화하려는 루트 접미어가 Identity Synchronization for Windows 와 등록된 구성 디렉토리와 연결되지 않은 경우 반드시 다음과 같이 새 구성 디렉토리를 지정해야 합니다.

- a. 구성 디렉토리 버튼을 눌러 새 구성 디렉토리를 지정합니다.
- b. 구성 디렉토리 대화 상자가 표시되면 (그림 4-9) New 버튼을 눌러 New Configuration Directories 대화 상자를 표시합니다.

그림 4-9) 새 구성 디렉토리 선택



c. 다음 정보를 입력한 후, 확인을 눌러 변경 내용을 저장하고 대화 상자를 닫습니다.

- **Host:** 정규화된 호스트 이름을 입력합니다.

예 : **machine1.example.com**

- **Port:** 유효하며 사용되지 않은 LDAP 포트 번호를 입력합니다. (기본값은 389 입니다.)

Identity Synchronization for Windows 가 SSL(Secure Socket Layer) 포트를 사용하여 구성 디렉토리 와 통신하는 경우 This port uses SSL 선택란을 선택합니다.

- **User DN:** 관리자의 (바인드된) 고유 이름을 입력합니다.

예 :

uid=admin,ou=Administrators,ou=TopologyManagement,o=Netscape Root

- **Password:** 관리자의 비밀번호를 입력합니다.

마법사는 지정된 구성 디렉토리를 쿼리하여 모든 Directory Server 가 해당 디렉토리에 의하여 관리되는지 판단합니다.

참고	Identity Synchronization for Windows 는 오직 Sun Java System Directory Server 소스마다 하나의 루트 접미어만 지원합니다.
-----------	--

참고	<p>구성 디렉토리 편집 및 제거</p> <p>또한 구성 디렉토리 대화 상자를 사용하여 다음과 같이 구성 디렉토리 목록을 관리할 수 있습니다.</p> <ul style="list-style-type: none"> • 목록 창에서 구성 디렉토리를 선택한 후, 편집 버튼을 누릅니다. Edit Configuration Directories 대화 상자가 표시되면 Host, Port, Secure Port, User Name 및 Password 매개변수를 변경할 수 있습니다. • 목록 창에서 구성 디렉토리를 선택한 후, Remove 를 눌러 목록에서 해당 디렉토리를 삭제합니다.
-----------	--

- d. Configuration Directories 대화 상자를 닫으려면 OK 를 누릅니다. 새로 선택한 구성 디렉토리의 루트 접미어가 목록 창에 표시됩니다.

기본적으로 Directory Server 는 접두어가 컴퓨터의 DNS 도메인 항목의 구성요소에 해당하는 루트 접미어를 만듭니다. 다음 접미어를 사용합니다.

`dc=<your_machine's_DNS_domain_name>`

따라서 컴퓨터 도메인이 *example.com* 인 경우 서버에 대하여 접미어 `dc=example`, `dc=com` 를 구성해야 합니다. 선택한 접미어로 이름을 지정한 항목은 반드시 디렉토리에 미리 존재해야 합니다.

- e. 루트 접미어를 선택하고 Next 를 누릅니다.

Preferred Server 패널이 표시됩니다 (그림 4-10 참조).

그림 4-10) 기본 서버 지정

Identity Synchronization for Windows 는 기본 Directory Server 를 사용하여 Directory Server 에서 변경된 내용을 검출합니다 . 기본 서버는 또한 Windows 시스템에서 발생한 변경 내용을 Sun Java System 디렉토리 시스템에 적용하는 기본 위치의 역할을 합니다 .

기본 서버에 이상이 발생하면 기본 서버가 복구될 때까지 보조 서버가 이들 변경 내용을 저장할 수 있습니다 .

3. 기본 마스터를 선택하려면 다음 방법 중 한 가지를 사용합니다 .
 - Choose a known server 버튼을 사용 설정한 후 드롭다운 목록에서 서버 이름을 선택합니다 .

참고 Directory Server 는 반드시 목록에서 실행되는 것으로 표시되어야 합니다 .
서버가 일시적으로 정지한 경우 호스트 이름 및 포트를 입력하여 서버 지정 버튼을 사용 설정한 후 직접 서버 정보를 입력합니다 .

Directory Server 가 SSL 을 사용하여 통신하도록 하려면 보안 통신 용으로 SSL 사용 상자를 활성화합니다 . 그러나 이 기능을 사용 설정하면 설치 후 반드시 수행해야 하는 추가 설정 단계가 있습니다 . 더 자세한 내용은 ["Directory Server 에서 SSL 사용 " 페이지 290](#) 를 참조하십시오 .

- Specify a server by providing a fully qualified hostname and port 버튼을 사용 설정한 후 제공된 텍스트 입력란에 서버의 호스트 이름과 포트를 입력합니다.

지정한 포트가 SSL 을 사용하는 경우 This port uses SSL 를 사용하도록 설정합니다.

4. Next 를 누르면 보조 서버를 지정합니다 패널이 표시됩니다.

그림 4-11) 보조 서버 지정

- 보조 Directory Server 를 지정하려면 드롭다운 목록에서 이름을 선택하거나 직접 정보를 입력 (기본 서버를 지정할 때의 절차와 동일) 한 후 Next 를 누릅니다.

참고

Directory Server 가 반드시 실행되어야 하며 , 그렇지 않은 경우 서버 이름이 드롭다운 목록에 표시되지 *않습니다*. 서버가 일시적으로 정지된 경우 서버 정보를 직접 입력하십시오.

- 보조 서버를 사용하지 않으려면 그냥 Next 를 누릅니다.

참고

- Sun 디렉토리 소스에서 기본 및 보조 서버에 대하여 동일한 호스트 이름을 사용하면 안 됩니다.
- Secure Port 기능을 사용 설정하면 설치 후 반드시 수행해야 하는 추가 설정 단계가 있습니다. 더 자세한 내용은 ["Directory Server 에서 SSL 사용 " 페이지 290](#) 를 참조하십시오.

다음과 같이 고급 보안 옵션 지정 패널이 표시됩니다.

그림 4-12) 고급 보안 옵션 지정

단계	고급 보안 옵션을 지정합니다.
1. 루트 접미사를 선택합니다.	<input checked="" type="checkbox"/> 신뢰할 수 있는 SSL 인증서 필요(R)
2. 우선 서버를 지정합니다.	이 옵션은 디렉토리 서버 커넥터와 디렉토리 서버 사이의 SSL 통신에만 적용됩니다.
3. 보조 서버를 지정합니다.	<input type="checkbox"/> Active Directory 통신에 대한 플러그인으로 SSL 사용(U)
4. 고급 보안 옵션을 지정합니다.	경고: 이 설정을 활성화하기 전에 제품 설명서에 제공된 보안 정보를 읽고 이해하도록 하십시오. 또한 'idsync certinfo' 명령줄 유틸리티를 사용하여 시스템의 SSL을 구성하는 데 필요한 증명서의 특정한 정보를 얻을 수 있습니다.

설치 과정의 일부분으로 사용자가 바인드되거나 비밀번호가 변경되는 각 Directory Server(마스터 , 복제 또는 허브) 에 Directory Server 플러그인을 반드시 설치해야 합니다 .

Directory Server 플러그인이 Active Directory 로 비밀번호 및 속성을 동기화할 때 반드시 Active Directory 로 바인드되어 사용자와 해당 비밀번호를 검색해야 합니다 . 또한 플러그인은 중앙 로그와 Directory Server 의 로그에 메시지를 기록합니다 . 기본적으로 이 통신은 SSL 을 통하여 완료될 수 없습니다 .

5. 보안 SSL 통신을 사용하려면 *제공된 경고*를 읽고 다음 옵션 중 한 가지 또는 모두를 사용 설정합니다.
 - 채널 통신만 암호화하거나 채널 통신을 암호화하고 인증서를 사용하여 Directory Server 와 Directory Server 커넥터 사이에서 참가자의 ID 를 검증하려면 Require Certificates for SSL 선택란을 선택합니다.

인증서를 신뢰하지 않으려면 선택란의 선택을 취소합니다.

- Directory Server 플러그인과 Active Directory 사이의 SSL 통신을 보호하려면 Active Directory 통신에 대한 플러그인으로 SSL 사용 선택란을 선택합니다.

참고

- 이 기능을 사용 설정하면 설치 후 추가 설정을 해야 합니다. 더 자세한 내용은 제 11 장, "보안 구성" 을 참조하십시오.
- idsync certinfo 명령줄 유틸리티를 사용하여 각 Directory Server 플러그인 및 커넥터 인증서 데이터베이스에 반드시 추가해야 하는 인증서를 결정할 수 있습니다. 자세한 내용은 "certinfo 사용" 페이지 307 를 참조하십시오.
- 기본 및 보조 Directory Server 가 MMR(Multi-Master Replication) 구현의 일부분인 경우 더 자세한 설명은 부록 E, "복제 환경용 설치 노트" 을 참조하십시오.

6. 고급 보안 옵션 지정 패널의 작업이 완료되었으면 Finish 를 누릅니다.

이 프로그램은 디렉토리 소스 아래의 탐색 트리에 선택한 디렉토리 소스를 추가하며, Prepare Directory Server Now? 대화 상자가 표시됩니다.

Identity Synchronization for Windows 가 사용할 Directory Server 를 반드시 준비해야 합니다. 이 작업은 지금 수행하거나 나중에 수행할 수 있으나, 반드시 커넥터를 설치하기 전에 Directory Server 를 준비해야 합니다. (커넥터 설치 방법은 5 장에 있습니다.)

- 지금 Directory Server 를 준비하려면 Yes 를 눌러 마법사를 열고 다음 ("Directory Server 준비" 페이지 109) 으로 계속합니다.
- 이 작업을 나중에 수행하려면 No 를 누르고 "Active Directory 소스 작성" 페이지 113 으로 계속합니다.

Directory Server 준비

여기에서는 Identity Synchronization for Windows 가 사용할 Sun Java System Directory Server 소스를 준비하는 방법에 대하여 설명합니다.

디렉토리 서버 준비

- 기본 호스트에서 사용 가능한 Retro Changelog 데이터베이스와 액세스 컨트롤 인스턴스 작성
- 기본 호스트에서 사용 가능한 커넥터 사용자 및 사용자 액세스 컨트롤 인스턴스 작성
- 기본 및 보조 호스트에서 동일성 색인 작성

참고

- 콘솔을 사용하는 대신 `idsync prepds` 명령줄 유틸리티를 사용하여 Directory Server 를 준비할 수 있습니다. 더 자세한 내용은 "[prepds 사용](#)" 페이지 310 를 참조하십시오.
- `idsync prepds` 명령줄 유틸리티를 사용하는 Directory Server 를 준비하려면 반드시 사용할 호스트 및 접미어를 알아야 하며 디렉토리 관리자의 자격 증명이 있어야 합니다.

Prepare Directory Server 마법사 (그림 4-13) 를 사용하여 Directory Server 를 준비할 수 있습니다.

그림 4-13) 디렉토리 관리자 자격 증명 입력

단계	디렉토리 관리자 자격 증명을 지정합니다.
1. 디렉토리 관리자 자격 증명을 지정합니다.	<p>Sun Java System Identity Synchronization for Windows가 사용할 Sun Java 시스템 디렉토리 서버를 준비하려면 디렉토리 관리자 자격 증명을 제공해야 합니다.</p> <p>우선 호스트 : <code>alclab-014.sfbay.sun.com:389</code></p> <p>디렉토리 관리자 사용자 이름(U): <input type="text" value="cn=Directory Manager"/></p> <p>디렉토리 관리자 비밀번호(P): <input type="password"/></p> <p>보조 호스트 :</p> <p>디렉토리 관리자 사용자 이름(A): <input type="text" value="cn=Directory Manager"/></p> <p>디렉토리 관리자 비밀번호(W): <input type="password"/></p>
2. 준비 구성을 준비합니다.	
3. 준비 상태입니다.	

이 마법사를 사용하려면 다음 중 한 가지 방법을 사용합니다.

- Prepare Directory Server Now? 대화 상자가 표시되면 Yes 버튼을 누릅니다.

- Sun 디렉토리 소스 창이 표시되면 (구성 탭) Prepare Directory Server 버튼을 누릅니다 .

Directory Server 소스를 준비하려면 다음과 같이 합니다 .

1. 디렉토리 관리자 계정에 다음 자격 증명을 입력합니다 .

- 디렉토리 관리자 사용자 이름
- 디렉토리 관리자 비밀번호

보조 호스트 (MMR 구성) 를 사용하는 경우 Secondary Host 옵션이 활성화되며 반드시 이들 호스트용 자격 증명 또한 지정해야 합니다 .

2. 작업을 완료했으면 Next 를 누릅니다 . Specify Preparation Configuration 패널 (그림 4-14) 이 표시됩니다 .

그림 4-14) 준비 구성 지정

<p>Steps</p> <ol style="list-style-type: none"> 1. Specify Directory Manager Credentials. 2. Specify Preparation Configuration. 3. Preparation Status. 	<p>Specify Preparation Configuration.</p> <p>Warning. This operation puts the database into read-only mode while creating an index in Directory Server. The database is read-only for just a few seconds unless it contains many entries. If necessary, you can create the index later by running this wizard again or using the 'idsync prepds' command line utility.</p> <p><input checked="" type="checkbox"/> Create indexes for database dc=example,dc=com</p>
---	---

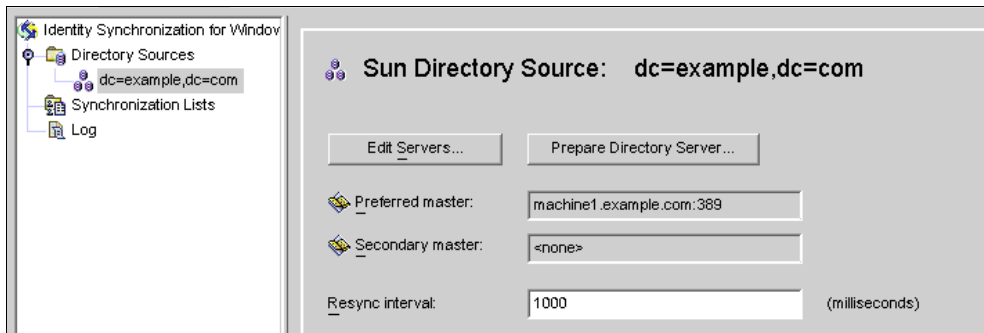
경고를 읽은 후 Directory Server 색인을 지금 만들 것인지 또는 나중에 만들 것인지 결정합니다 .

참고

- 이 작업은 데이터베이스의 크기에 따라 수 초에서 수 분까지 걸립니다 .
- 데이터베이스가 읽기 전용인 경우 데이터베이스의 정보 업데이트는 실패합니다 .
- 데이터베이스를 오프라인으로 하면 색인을 더욱 빨리 만들 수 있습니다 .

- 지금 색인을 만들려면 **Create indexes for database** 선택란을 선택하고 **Next**를 누릅니다.
- 나중에 (수동으로 또는 마법사를 다시 실행하여) 색인을 만들려면 **Create indexes for database** 선택란의 선택을 취소하고 **Next** 를 누릅니다.
- 3. **Preparation Status** 패널이 표시되어 **Directory Server** 준비 과정에 대한 정보가 제공됩니다.
 - 메시지 창 하단에 **SUCCESS** 메시지가 표시되면 **Finish** 를 누릅니다.
 - 오류 메시지가 표시되면 계속하기 전에 반드시 보고된 문제를 해결해야 합니다. 더 자세한 내용은 오류 로그 (상태 탭) 를 확인하십시오.
- 4. 콘솔의 **Configuration** 탭으로 되돌아갑니다. 탐색 트리에서 **Directory Sources** 노드를 선택하면 **Directory Source** 패널이 표시됩니다 (참조).

그림 4-15) Sun Directory Source 패널



이 패널에서 다음 작업을 수행할 수 있습니다.

- **Edit servers:** 이 버튼을 눌러 **Define Sun Java System Directory Source** 패널을 다시 열고 서버 구성 매개변수를 변경할 수 있습니다. 필요한 경우 "**Sun Java System 디렉토리 소스 작성**"의 설명을 참조하십시오.
- **Prepare Directory Server:** Directory Server를 준비하려면 이 버튼을 누르고 "**Directory Server 준비**" [페이지 109](#)의 설명을 따라 합니다.

처음 서버를 준비한 후 Directory Server에 변경 내용이 있는 경우 (예를 들어 색인이 삭제되거나 Retro-Changelog 데이터베이스가 손상된 경우) 서버를 다시 준비할 수 있습니다.

참고

기본 Sun 디렉토리 소스에 대하여 Retro-Changelog 데이터베이스를 다시 만드는 경우 기본 액세스 제어 설정으로 인하여 Directory Server 커넥터가 데이터베이스 내용을 읽을 수 없게 됩니다.

새 Retro-Changelog 데이터베이스용 액세스 제어 설정을 복구하려면 `idsync prepds` 를 실행하거나 콘솔에서 적절한 Sun 디렉토리 소스를 선택한 후 Prepare Directory Server 버튼을 누릅니다.

- **Resync interval:** Directory Server 커넥터가 변경 내용을 확인하는 주기를 지정합니다. (기본값은 1000 밀리초입니다.)
- 5. 동기화하려는 Sun Java System Directory Server 엔터프라이즈에 있는 각 사용자 입력 내용에 대한 Directory Server 디렉토리 소스를 추가합니다.

작업을 완료했으면 반드시 Windows 디렉토리 소스를 하나 이상 만들어야 합니다.

- Active Directory 디렉토리 소스를 만들려면 "[Active Directory 소스 작성](#)" [페이지 113](#) 으로 계속합니다.
- Windows NT 디렉토리 소스를 만들려면 "[Windows NT SAM 디렉토리 소스 작성](#)" [페이지 122](#) 으로 계속합니다.

Active Directory 소스 작성

동기화하려는 네트워크에 있는 각 Windows 도메인마다 Active Directory 디렉토리 소스를 추가해야 합니다.

각 Active Directory 구현에는 모든 Active Directory 도메인 전체에 있는 전역 정보가 있는 전역 카탈로그가 최소한 하나 이상 있습니다.

참고

각 Active Directory 서버가 전역 카탈로그가 되고 구현에 여러 개의 전역 카탈로그가 있을 수 있으나, 전역 카탈로그는 오직 하나만 지정하면 됩니다.

네트워크에 Windows Active Directory 서버가 있는 경우 다음과 같이 하십시오.

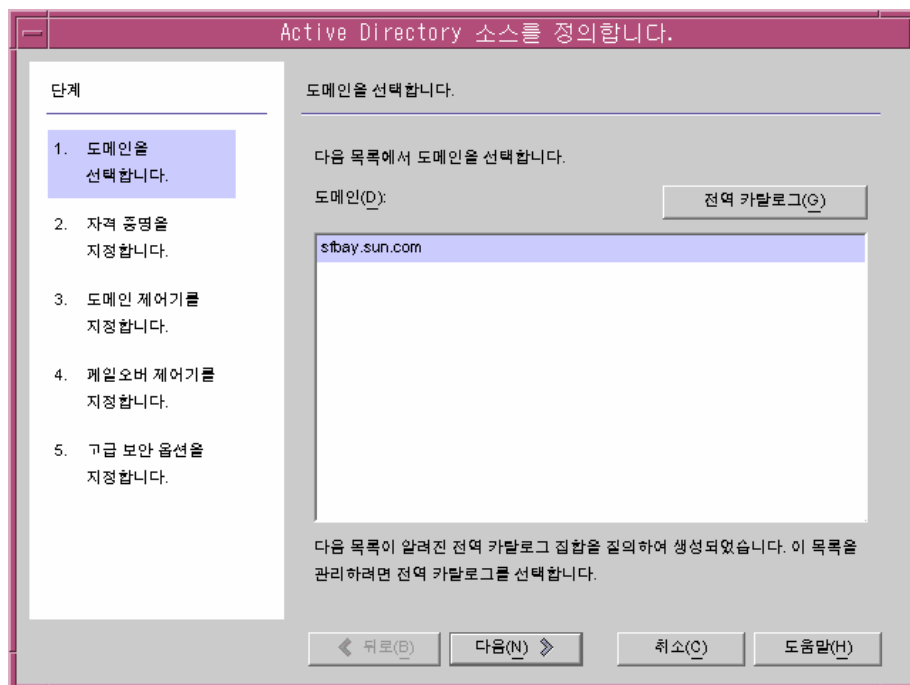
1. 탐색 트리에서 Directory Source 노드를 선택한 후 Directory Source 패널에서 New Active Directory Source 버튼을 누릅니다.

Windows 전역 카탈로그 대화 상자가 표시됩니다 (그림 4-16).

그림 4-16) Windows Global Catalog

2. 다음 정보를 입력하고 OK 를 누릅니다.
 - **Host:** Active Directory 포리스트용 전역 카탈로그가 있는 컴퓨터의 정규화된 호스트 이름을 입력합니다.
예 : **machine2.example.com**
 - **This port uses SSL:** Identity Synchronization for Windows 가 SSL 포트를 사용하여 전역 카탈로그와 통신하는 경우 이 옵션을 사용 설정합니다.
 - **User DN:** 정규화된 관리자의(바인드된) 고유 이름을 입력합니다. (시스템에서 스키마를 찾아 볼 수 있으며 사용 가능한 Active Directory 도메인을 결정할 수 있는 모든 자격 증명이면 충분합니다.)
예 : **cn=Administrator,cn=Users,dc=example,dc=com**
 - **Password:** 지정된 사용자의 비밀번호를 입력합니다.
3. 다음과 같이 Active Directory 소스 정의 마법사가 표시됩니다.

그림 4-17) Active Directory 소스 정의 마법사



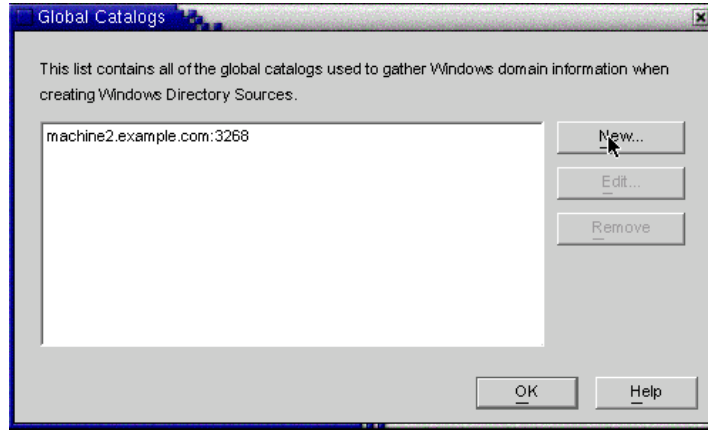
마법사는 Active Directory 전역 카탈로그를 쿼리하여 존재하는 다른 도메인을 확인하고 Domains 목록창에 해당 도메인을 표시합니다.

4. 목록 창에서 이름을 선택하여 Active Directory 도메인을 지정하고 OK를 누른 후, [단계 5 - 페이지 116](#)로 계속합니다.

목록에 사용하려는 도메인이 표시되지 않으면 다음과 같이 반드시 해당 도메인이 알려진 전역 카탈로그를 추가해야 합니다.

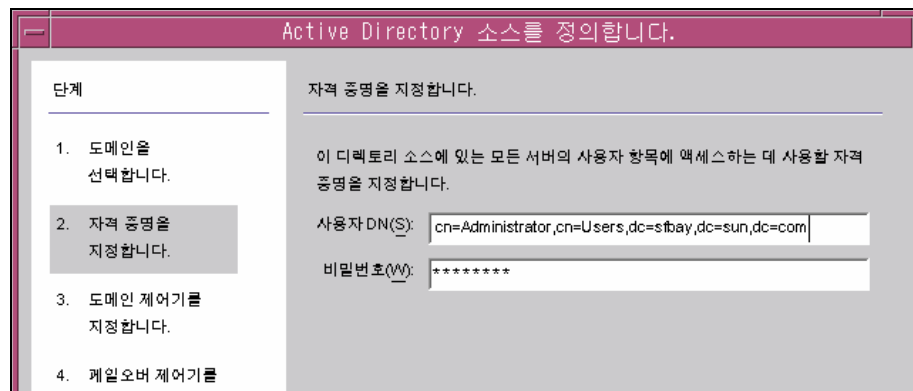
- a. 전역 카탈로그 버튼을 누르면 전역 카탈로그 마법사가 표시됩니다 (그림 4-18).

그림 4-18) 새 전역 카탈로그 지정



- b. New 버튼을 누릅니다.
 - c. Windows Global Catalog 대화 상자가 표시되면 전역 카탈로그의 호스트 이름과 디렉토리 소스 자격 증명을 입력한 후 ([페이지 114](#) 참조), OK 를 누릅니다.
 - d. 새 전역 카탈로그와 포트가 Global Catalogs 목록창에 표시됩니다. 카탈로그 이름을 선택하고 OK 를 누릅니다.
 - e. 시스템에 더 많은 전역 카탈로그(도메인)를 추가하려면 이 단계를 반복합니다.
 - f. 작업이 완료되었으면 Select a Domain 창에서 Next 버튼을 누릅니다.
5. Specify Credentials 창이 표시되면 User DN 필드의 값을 확인합니다.

그림 4-19) 이 Active Directory 소스용 자격 증명 지정



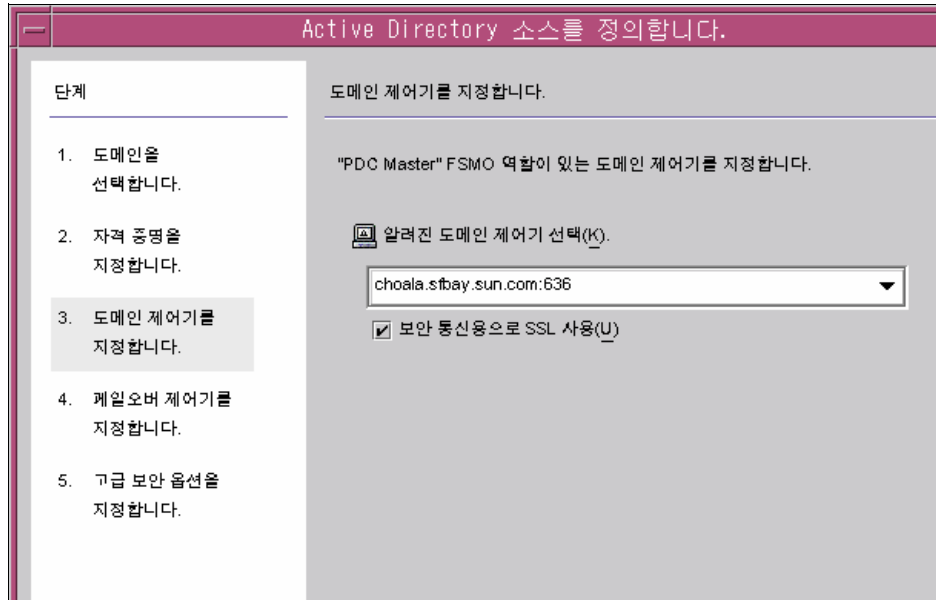
프로그램에서 User DN 필드에 사용자의 고유 이름이 자동으로 입력되지 않으면 (또는 관리자의 자격 증명을 사용하지 않으려면) 직접 User DN 과 비밀번호를 입력합니다.

Active Directory 소스를 구성할 때 반드시 Active Directory 커넥터가 Active Directory 로 연결할 때 사용할 사용자 이름과 비밀번호를 입력해야 합니다.

- 참고** 커넥터에는 특정 액세스 권한이 필요합니다. 최소 권한은 다음과 같이 동기화의 방향에 따라 다릅니다.
- Active Directory 에서 Directory Server 로만 동기화를 구성하는 경우 Active Directory 커넥터용으로 제공되는 사용자에게 특별한 권한은 필요하지 않습니다. 동기화될 도메인에서 " 모든 속성 읽기 " 의 특별 권한이 있는 정상 사용자면 충분합니다.
 - Directory Server 에서 Active Directory 로 동기화 흐름을 구성하는 경우, 동기화에 의하여 Active Directory 에서 사용자 항목이 변경되므로 커넥터 사용자에게 반드시 더 많은 권한이 있어야 합니다. 이 단계에서 커넥터 사용자에게 반드시 " 모든 권한 " 이 있거나 Administrator 그룹의 일원이어야 합니다.

6. Next 를 눌러 도메인 제어기 지정 패널을 엽니다.

그림 4-20) 도메인 제어기 지정



이 패널에서 지정된 도메인과 동기화할 제어기를 선택합니다. (개념에 있어 도메인 제어기는 Directory Server 의 기본 서버와 비슷합니다.)

선택된 Active Directory 도메인에 여러 개의 도메인 제어기가 있는 경우 동기화용으로 기본 도메인 제어기 FSMO 역할이 있는 도메인 제어기를 선택합니다. .

기본적으로 모든 도메인 제어기에서 비밀번호가 변경되면 즉시 기본 도메인 제어기 FSMO 역할 소유자에게 복제되며, 이 도메인 제어기를 선택하면 Identity Synchronization for Windows 가 이들 비밀번호 변경을 즉시 Directory Server 로 동기화합니다. .

일부 구현에서 PDC 로의 상당한 네트워크 "거리 "가 있으므로 Windows 레지스트리에 AvoidPdcOnWan 속성이 설정될 수 있는데, 이 경우 동기화가 상당히 지연될 수 있습니다. (자세한 내용은 *Microsoft 기술 자료 Article 232690* 을 참조하십시오.)

7. 드롭다운 목록에서 도메인 제어기를 선택합니다. .
8. Identity Synchronization for Windows 커넥터가 안전한 포트를 통하여 도메인 제어기와 통신하도록 하려면 Use a Secure Port 선택란을 선택합니다. .

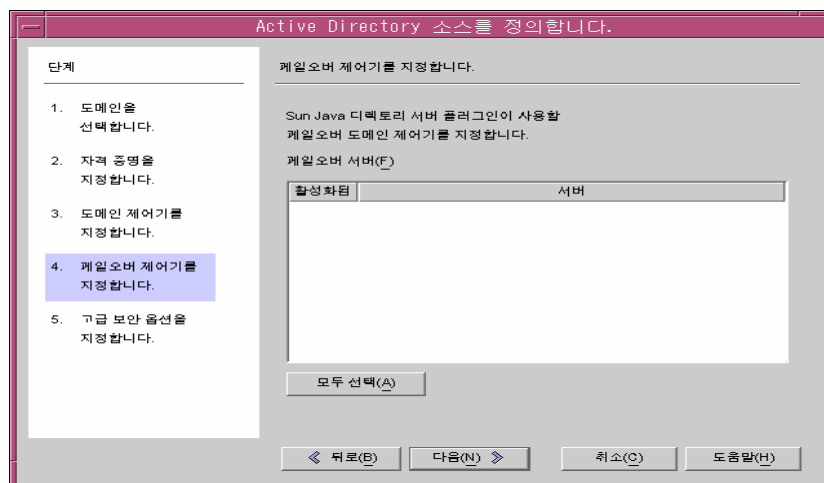
참고

Microsoft 인증 서버를 사용하는 경우 프로그램에서 자동으로 Active Directory 커넥터에 CA 인증서가 설치됩니다. 그렇지 않은 경우 반드시 Active Directory 커넥터에 직접 CA 인증서를 추가해야 합니다 ("Active Directory 커넥터에서 SSL 사용" 페이지 293 참조). 또한 처음 구성한 후 흐름 설정을 변경하는 경우에도 이 절차를 적용합니다.

9. 작업을 완료했으면 다음을 누릅니다.

페일오버 제어기 지정 패널이 표시됩니다 (그림 4-21 참조). 이 패널에서 장애 복구 도메인 제어기의 수를 지정할 수 있습니다.

그림 4-21) 페일오버 제어기 지정



Active Directory 커넥터는 오직 Active Directory 도메인 제어기와 통신하며, Identity Synchronization for Windows 는 해당 커넥터가 적용한 장애 복구 변경 내용을 지원하지 않습니다. 그러나 Directory Server 플러그인은 Directory Server 로 비밀번호 변경의 유효성을 검사할 때 수에 상관 없이 도메인 제어기와 통신합니다.

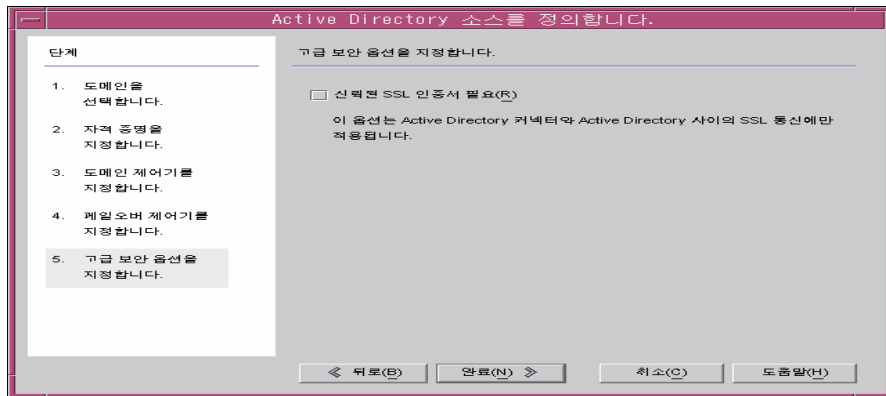
Directory Server 가 Active Directory 도메인 제어기와 연결하려 하지만 해당 도메인 제어기를 사용할 수 없는 경우, Directory Server 는 순서에 따라 지정된 장애 복구 도메인 제어기로 연결을 시도합니다.

10. Failover Servers 목록 창에서 서버 이름을 하나 이상 선택(또는 목록의 서버를 모두 지정하려면 모두 선택 버튼을 누름) 하고 다음을 누릅니다.

11. 다음과 같이 고급 보안 옵션 지정 패널 (그림 4-22) 이 표시됩니다.

도메인 제어기 지정 패널 (참조) 에서 보안 통신용으로 SSL 사용 선택란을 사용 설정한 경우에만 신뢰된 SSL 인증서 필요 옵션을 사용수 있게 (선택 가능) 됩니다.

그림 4-22) 고급 보안 옵션 지정



- 신뢰된 SSL 인증서 필요 선택란을 선택하지 않는 경우 (기본 설정) Active Directory 커넥터는 SSL 을 통하여 Active Directory 에 연결하며 Active Directory 가 전달한 인증서를 신뢰하는지 검증하지 않습니다.

이 옵션을 사용하지 않도록 설정하면 Active Directory 인증서 데이터베이스에 Active Directory 인증서를 넣을 필요가 없으므로 설정 과정이 간단해집니다.

- 신뢰된 SSL 인증서 필요 선택란을 선택하는 경우 Active Directory 커넥터가 SSL 을 통하여 Active Directory 에 연결하며 반드시 Active Directory 가 전달한 인증서를 신뢰하는지 검증해야 합니다.

참고

반드시 Active Directory 커넥터의 인증서 데이터베이스에 Active Directory 인증서를 추가해야 합니다 . 방법은 " 커넥터의 인증서 데이터베이스에 Active Directory 인증서 추가 " 페이지 295 를 참조하십시오 .

12. Advanced Security Options 패널의 작업이 완료되었으면 완료 버튼을 누릅니다.
프로그램에서 새로 지정된 Active Directory 디렉토리 소스가 디렉토리 소스 아래의 탐색 트리에 추가됩니다.
13. Active Directory 소스 패널을 보려면 Active Directory 소스 노드를 선택합니다 (그림 4-23).

그림 4-23) Active Directory 소스 패널

△ Active Directory 소스: sfbay.sun.com

컨트롤러 편집(I)...

도메인 제어기(D): choala.sfbay.sun.com:636

재동기화 간격(Y): 1000 (밀리초)

디렉토리 소스 자격 증명

사용자 DN(S): cn=Administrator,cn=Users,dc=sfbay,dc=sun,dc=com

비밀번호(W): *****

이 패널에서 다음 작업을 수행할 수 있습니다.

- **컨트롤러 편집**: 이 버튼을 눌러 도메인 제어기 지정 패널을 다시 열고 원하는 도메인 제어기 구성 매개변수를 변경할 수 있습니다. 필요한 경우 "[Active Directory 소스 작성](#)"의 설명을 참조하십시오.
- **재 동기화 간격**: Active Directory 커넥터가 변경 내용을 확인하는 주기를 지정합니다. (기본값은 1000 밀리초입니다.)
- **디렉토리 소스 자격 증명**: 지정된 User DN 및 비밀번호를 변경합니다.

Active Directory 디렉토리 소스를 만들었으면 다음과 같이 합니다.

- Windows NT 디렉토리 소스를 만들려면 "[Windows NT SAM 디렉토리 소스 작성](#)"으로 계속합니다.
- 동기화할 속성을 만들고 매핑하려면 "[사용자 속성 선택 및 매핑](#)" 페이지 125으로 계속합니다.

Windows NT SAM 디렉토리 소스 작성

Windows NT 플랫폼에서 Identity Synchronization for Windows 를 구현하려면 다음과 같이 NT SAM 디렉토리 소스를 지정해야 합니다 .

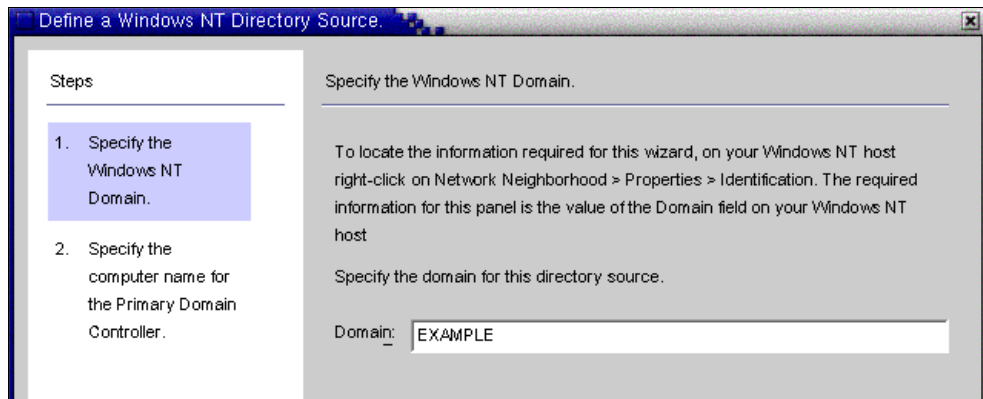
1. 탐색 트리에서 Directory Source 노드를 선택한 후 New Windows NT SAM Directory Source 버튼을 누릅니다 .

그림 4-24) 디렉토리 소스 패널



2. Define a Windows NT SAM Directory Source 패널이 표시되면 (그림 4-25 참조) Windows NT 도메인 이름을 찾는 설명을 따라하고 Domain 필드에 고유한 NT 디렉토리 소스 도메인 이름을 입력합니다 . 작업을 완료했으면 Next 를 누릅니다 .

그림 4-25) Windows NT SAM 도메인 이름 지정



3. Specify the Computer Name for the Primary Domain Controller 패널이 표시되면 (그림 4-26 참조) 기본 도메인 제어기 컴퓨터 이름을 찾는 설명을 따라하고 Computer Name 필드에 정보를 입력합니다 .

그림 4-26) 기본 도메인 제어기의 이름 지정

<p>Steps</p> <ol style="list-style-type: none"> 1. Specify the Windows NT Domain. 2. Specify the computer name for the Primary Domain Controller. 	<p>Specify the computer name for the Primary Domain Controller.</p> <p>To locate the information required for this wizard, on your Windows NT host right-click on Network Neighborhood > Properties > Identification. The required information for this panel is the value of the Computer Name field on your Windows NT host</p> <p>Specify the computer name for the Primary Domain Controller.</p> <p>Computer Name: MACHINE3</p>
---	--

4. Finish 를 누릅니다 .

프로그램에서 새로 지정된 Windows NT SAM 디렉토리 소스가 Directory Source 아래의 탐색 트리에 추가됩니다 . Windows NT SAM Source 패널을 보려면 새 디렉토리 소스 노드를 선택합니다 (그림 4-27 참조).

그림 4-27) Windows NT SAM Directory Source 패널

<p>Identify Synchronization for Win</p> <ul style="list-style-type: none"> Directory Sources <ul style="list-style-type: none"> dc=example,dc=com example.com EXAMPLE Synchronization Lists Log 	<p>Windows NT SAM Directory Source: EXAMPLE</p> <p>Domain: EXAMPLE Edit...</p> <p>Specify the domain name for this directory source.</p> <p>Computer Name: machine3</p> <p>Specify the computer name for the Primary Domain Controller.</p> <p>Resync interval: 1000 (milliseconds)</p>
---	---

이 패널에서 다음 작업을 수행할 수 있습니다 .

- 편집 : 이 버튼을 눌러 Specify a Domain Controller 패널을 다시 열고 원하는 도메인 제어기 구성 매개변수를 변경할 수 있습니다 . 필요한 경우 "Active Directory 소스 작성 "의 설명을 참조하십시오 .

- **재동기화 간격** : Identity Synchronization for Windows 가 Windows NT 에서 수정된 내용을 확인하는 주기를 지정합니다. (기본값은 1000 밀리초입니다 .)
5. 네트워크의 각 Windows NT 컴퓨터에 Windows NT 디렉토리 소스를 추가합니다 .

Windows NT SAM 디렉토리 소스를 작성하고 나면 동기화할 속성을 만들고 매핑할 수 있습니다 . 자세한 지침은 "[사용자 속성 선택 및 매핑](#)" 페이지 125 으로 계속합니다 .

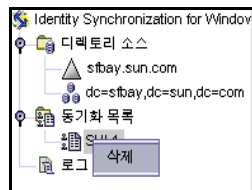
디렉토리 소스 삭제

참고 이미 디렉토리 소스와 연결된 커넥터가 설치되어 있는 경우 반드시 디렉토리 소스를 삭제하기 전에 해당 커넥터를 제거해야 합니다 .

디렉토리 소스를 반드시 삭제해야 하는 경우 다음과 같이 합니다 .

1. 디렉토리 소스를 삭제하기 전에 반드시 해당 소스와 연결된 모든 동기화 사용자 목록 (SUL) 을 우선 삭제해야 합니다 .
 - a. 탐색 트리의 Synchronization List 아래에 있는 해당 동기화 사용자 목록 노드를 마우스 오른쪽 버튼으로 누릅니다 .
 - b. 팝업 메뉴가 표시되면 Delete 를 선택하여 해당 SUL 을 제거합니다 .

그림 4-28) Synchronization User List 삭제



2. 탐색 트리의 Directory Sources 아래에 있는 목록에서 디렉토리 소스 노드를 마우스 오른쪽 버튼으로 누릅니다 .
3. 팝업 메뉴가 표시되면 Delete 를 선택하여 해당 디렉토리 소스를 제거합니다 .

사용자 속성 선택 및 매핑

Directory Server 와 Windows 디렉토리 소스를 만들고 구성한 후, 반드시 동기화할 사용자 속성을 결정하고 시스템 사이에서 해당 속성을 매핑해야 합니다.

이 부분의 내용은 다음과 같습니다.

- "속성 선택 및 매핑" 페이지 125
- "매개변수화 속성 기본값 생성" 페이지 127
- "스키마 소스 변경" 페이지 128

속성 선택 및 매핑

속성은 다음과 같은 두 가지 유형으로 구분됩니다.

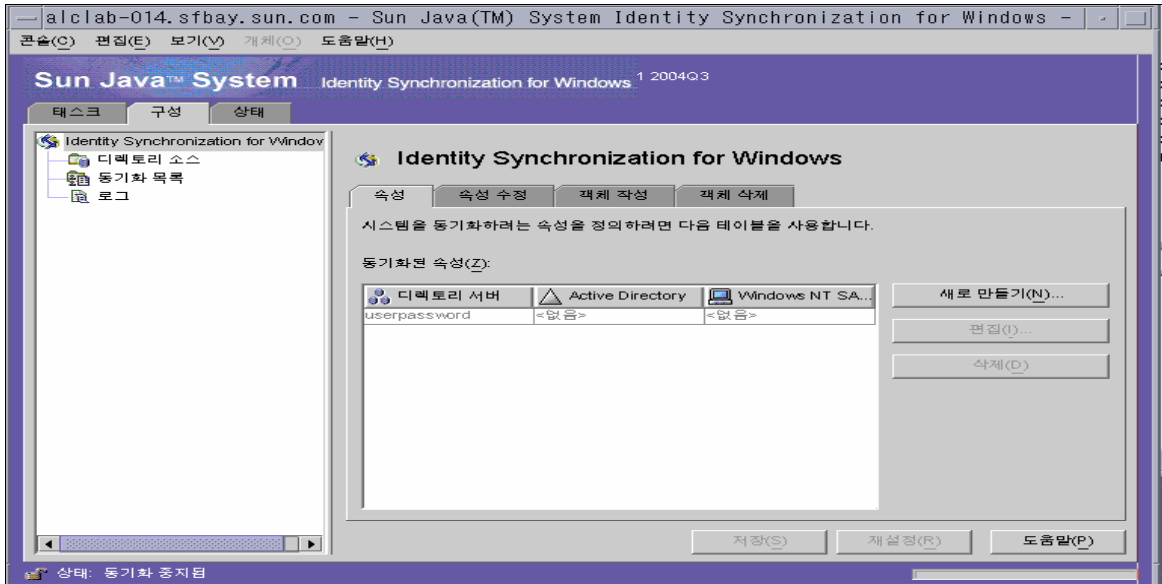
- **Significant:** 사용자 항목을 만들거나 수정할 때 시스템 사이에서 동기화되는 속성.
- **Creation:** 사용자 항목을 만들 때 시스템 사이에서만 동기화되는 속성.
 각 플랫폼에 사용되는 스키마에 따라 필수적인 생성 속성이 있습니다. 이러한 속성은 비밀번호 동기화에 필요하며 Active Directory 서버에서 사용자 객체 클래스 항목을 만들려면 반드시 Sun 속성으로 매핑되어야 합니다.

여기에서는 동기화용으로 사용자 속성을 선택하는 방법에 대하여 설명하며, Directory Server 용으로 속성을 지정할 때 Active Directory 및 Windows 환경에서 동등한 속성이 표시 (또는 그 반대로) 되도록 하고 부속 Windows 속성의 값이 동기화 되도록 해당 속성을 매핑하는 방법에 대하여 설명합니다.

동기화용 속성을 선택하고 매핑하려면 다음과 같이 합니다.

1. 탐색 트리 상단의 Identity Synchronization for Windows 노드를 선택합니다 (그림 4-29 참조).

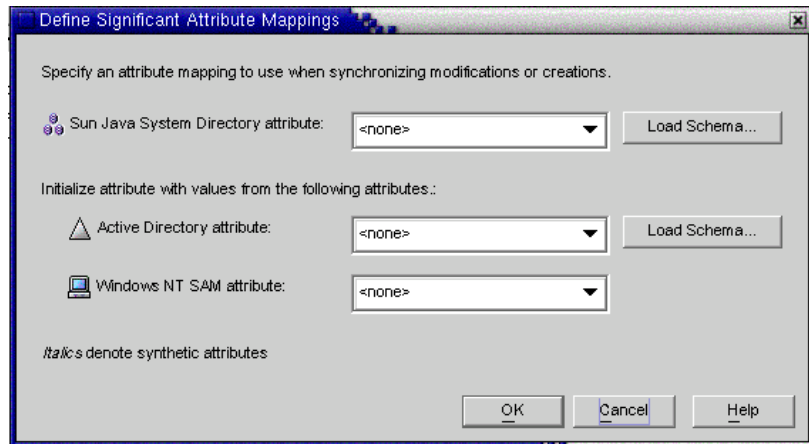
그림 4-29) Attributes 탭



2. 속성 탭을 선택한 후 New 버튼을 누릅니다.

Define Significant Attribute Mappings 대화 상자가 표시됩니다 (그림 4-30). 이 대화 상자를 사용하여 Directory Server 에서 Windows 시스템 (Active Directory 및 Windows NT) 으로 속성을 매핑합니다.

그림 4-30) 중요 속성 매핑 정의



참고 Directory Server(또는 Active Directory) 용으로 필수인 creation 속성은 Sun 측 (또는 Active Directory 측) 사용자 항목용으로 구성된 objectclass 에 따라 달라집니다 .

3. Sun Java System 속성 드롭다운 목록에서 속성을 선택하고
(예 : cn) Active Directory 속성 및 Windows NT SAM 속성 드롭다운 메뉴에서 동등한 속성을 선택합니다 .
4. 작업을 완료했으면 OK 를 누릅니다 .
5. 추가 속성을 지정하려면 [단계 2](#) 에서 [단계 4](#) 까지의 단계를 반복합니다 .

완료된 Synchronized Attributes 표는 다음 예에서 보이는 것과 유사합니다 . 여기에 userpassword, cn 및 telephonenumber Directory Server 속성은 unicodepwd, cn 및 telephonenumber Active Directory 속성과 매핑되어 있습니다 .

그림 4-31) 속성 동기화 완료 표

Directory Server	Active Directory	Windows NT SAM
userpassword	unicodepwd	user_password
cn	cn	<none>
telephonenumber	telephonenumber	<none>

참고 프로그램은 자동으로 *inetOrgPerson* 을 Sun Java System Directory Server 용 기본 objectclass 로 사용하며 , 사용자는 전역 카탈로그를 지정할 때 Active Directory 스키마를 로드합니다 . 따라서 기본 스키마를 변경하지 않는 한 Load Schema 버튼을 사용하지 않습니다 .

기본 스키마 소스를 변경하는 방법은 "[스키마 소스 변경](#) " [페이지 128](#) 을 참조하십시오 .

매개변수화 속성 기본값 생성

Identity Synchronization for Windows 에서 다른 생성 또는 중요 속성을 사용하여 속성에 대한 *매개변수화된* 기본값을 만들 수 있습니다 .

매개변수화 기본 속성 값을 만들려면 퍼센트 기호 안에 표시되는 기존 생성 또는 중요 매개변수 이름 (`<attribute_name>`) 을 표현식 문자열에 포함해야 합니다. 예 :
`homedir=/home/%uid% or cn=%givenName% %sn%.`

이들 속성 값을 만드는 경우 :

- 생성 표현식에 복수 속성을 사용할 수 있습니다 (`cn=%givenName% %sn%`).
- `A=%B%` 인 경우 B 에는 하나의 기본값만 있어야 합니다.
- 역슬래시 기호 (\) 를 인용에 사용할 수 있습니다 (예 :`diskUsage=0\%`).
- 순환적 대체 조건이 있는 표현식을 사용하면 안 됩니다.(예 :
`description=%uid%` 를 지정하는 경우 `uid=%description%` . 를 사용하면 안 됩니다.)

스키마 소스 변경

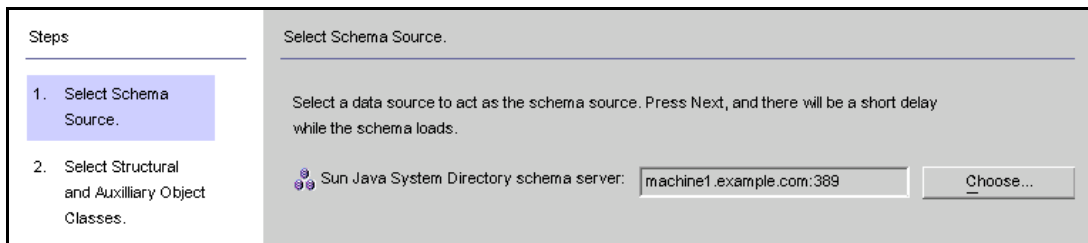
프로그램은 자동으로 기본 스키마 소스를 제공하지만 기본 스키마를 변경할 수 있습니다.

기본 스키마 소스를 변경하려면 다음과 같이 합니다.

1. Define Significant Attribute Mappings 대화 상자에서 Load Schema 버튼을 누릅니다.

Select Schema Sources 패널이 표시됩니다 (그림 4-32 참조).

그림 4-32) 스키마 소스 선택



이 패널을 사용하여 스키마를 읽을 Sun Java System Directory Server 스키마 서버를 지정합니다. 이 스키마에는 시스템에서 사용 가능한 객체 클래스와 시스템에서 사용자에게 사용 가능한 속성을 지정하는 객체 클래스가 있습니다.

프로그램에서 기본적으로 Sun Java System 디렉토리 스키마 서버 필드에 구성 디렉토리가 추가됩니다.

2. 다른 서버를 선택하려면 Choose 버튼을 누릅니다.

Select a Sun Schema Host 대화 상자가 표시됩니다. 이 대화 상자에는 디렉토리 소스에 대한 관리 정보를 수집하는 구성 디렉토리의 목록이 있습니다.

이 대화 상자에서 할 수 있는 작업은 다음과 같습니다.

- 새 구성 디렉토리를 만들고 이를 목록에 추가합니다.

New 를 누르고 New Configuration Directory 대화 상자가 표시되면 Host, Port, User DN 및 Password 를 지정합니다. 작업을 완료하려면 OK 를 누릅니다.

- 기존 디렉토리를 편집합니다.

Edit 를 누르고 Edit Configuration Directory 대화 상자가 표시되면 Host, Port, User DN 및 Password 를 변경합니다. 작업을 완료하려면 OK 를 누릅니다.

- 목록에서 디렉토리를 제거합니다.

목록 창에서 구성 디렉토리를 선택한 후, Remove 버튼을 누릅니다.

3. 목록에서 서버를 선택하고 선택을 완료했으면 OK 를 누릅니다. (일반적으로 스키마 소스로 Sun 동기화 호스트 중 하나를 선택하는 것이 좋습니다.)
4. Next 버튼을 누르면 Select Structural and Auxiliary Object Classes 패널이 표시됩니다 (그림 4-33).

그림 4-33) 구조적 및 보조 객체 클래스 선택

이 패널을 사용하여 다음과 같이 동기화할 객체 클래스를 지정합니다.

- **구조적 객체 클래스:** 선택한 Directory Server에서 만들어지거나 동기화된 모든 항목에는 반드시 구조적 객체 클래스가 하나 이상 있어야 합니다.
- **보조 객체 클래스:** 이 객체 클래스는 선택한 구조적 클래스를 사용하며 동기화에 대한 추가 속성을 제공합니다.

구조적 및 보조 객체 클래스를 지정하려면 다음과 같이 합니다.

- a. 드롭다운 목록에서 구조적 객체 클래스를 선택합니다. (기본값은 *inetorgperson* 입니다.)
- b. Available Auxiliary Object Classes 목록창에서 객체 클래스를 하나 이상 선택한 후 Add 를 눌러 선택한 내용을 Selected Auxiliary Object Classes 목록창으로 옮깁니다.

선택한 객체 클래스에 따라 중요 또는 생성 속성으로 선택할 수 있는 디렉토리 소스 속성이 결정됩니다.

또한 객체 클래스에 따라 필수 생성 속성이 달라집니다.

Selected Auxiliary Object Classes 목록에서 선택 항목을 삭제하려면 해당 객체 클래스 이름을 누르고 Remove 버튼을 누릅니다.

- c. 작업을 완료했으면 Finish를 누릅니다. 프로그램에 스키마와 선택한 객체 클래스가 로드됩니다.

시스템간 사용자 속성 전달

동기화하려는 사용자 속성을 만들고 매핑한 후, 반드시 Identity Synchronization for Windows가 속성 작성, 수정 및 삭제를 Sun과 Windows 시스템 사이에서 전달하는 방법을 지정해야 합니다.

기본적으로 Identity Synchronization for Windows는

- Windows에서 Sun Java System Directory Server로만 동기화합니다.
- 비밀번호 속성만 동기화합니다 (앞의 단원에서 significant 속성을 지정하지 않은 경우).
- 항목의 생성 또는 삭제를 동기화하지 않습니다.

여기에서는 시스템 사이의 속성 동기화를 구성하는 방법에 대하여 설명합니다. 다음과 같은 내용으로 구성됩니다.

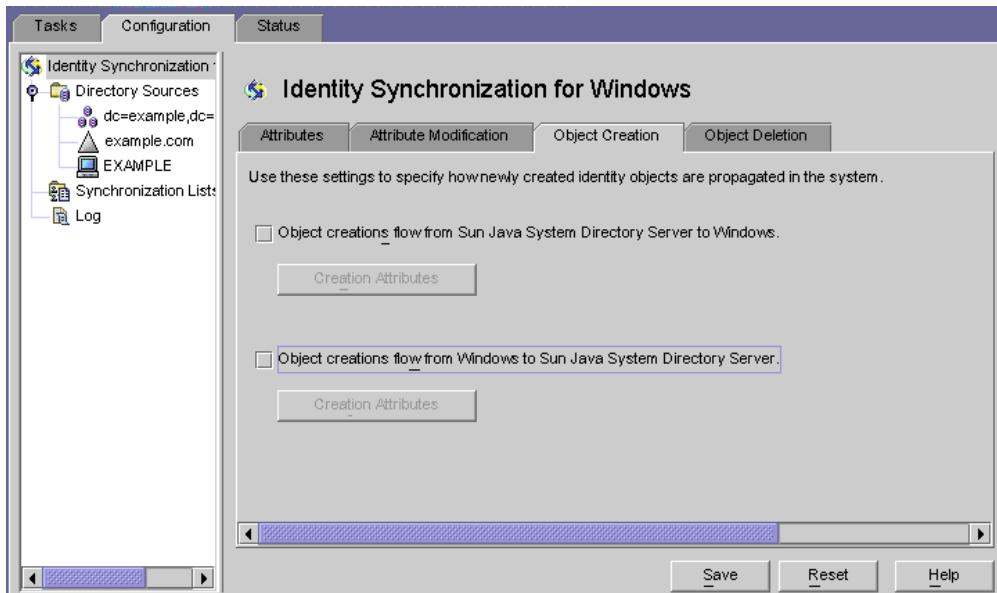
- "객체 작성 흐름 방법 지정" 페이지 131
- "객체 수정 내용 흐름 방식 지정" 페이지 137
- "삭제 내용 흐름 방식 지정" 페이지 147

객체 작성 흐름 방법 지정

Directory Server와 Active Directory 시스템에서 객체 생성이 흐르는 방법을 지정하려면 다음과 같이 합니다.

1. Object Creation 탭을 누릅니다.

그림 4-34) 작성 선택 및 전달



2. 다음과 같이 작성 흐름을 사용 또는 사용 불가로 설정할 수 있습니다.
 - Directory Server 환경에서 작성한 내용을 Windows 서버로 전달하려면 **Object creations flow from Sun Java System Directory Server to Windows** 를 사용 설정합니다.
 - Windows 환경에서 작성한 내용을 Directory Server 로 전달하려면 **Object creations flow from Windows to Sun Java System Directory Server** 를 사용 설정합니다.
 - 양방향 흐름의 경우 두 옵션을 모두 사용 설정합니다.
 - 한 시스템에서 다른 시스템으로 사용자 작성 내용이 전달되지 않도록 하려면 두 옵션을 모두 사용 불가로 설정합니다. (기본값)
3. 시스템 사이에서 동기화할 생성 속성을 추가, 편집 또는 삭제하려면 선택한 옵션의 아래에 있는 **Creation Attributes** 버튼을 누릅니다.

Creation Attribute Mappings and Values 대화 상자가 표시됩니다.
(그림 4-35 및 그림 4-36 참조)

그림 4-35) 생성 속성 매핑 및 값 : Directory Server 에서 Windows 로

Use Creation Attributes only when synchronizing an object creation to the Windows domain. An attribute can be populated from a Sun Java System Directory Server attribute and/or a default value.

Active Directory	Directory Server	Value
cn	cn	
samaccountname	<none>	

New... Edit... Delete

그림 4-36) 생성 속성 매핑 및 값 : Windows 에서 Directory Server 로

Use Creation Attributes only when synchronizing an object creation to the Sun Java System Directory Server. An attribute can be populated from a Windows user attribute and/or a default value. You must specify a Creation Attribute for each mandatory attribute in the synchronized object class that is not already defined as a Synchronization Attribute.

Directory Server	Active Directory	Windows NT SA...	Value
cn	cn	<none>	
sn	<none>	<none>	

New... Edit... Delete

두 대화 상자에서 다음 작업을 할 수 있습니다.

- 새 생성 속성 지정 ([페이지 134](#))

참고

사용자 객체 클래스용으로 필요한 속성에 대한 스키마 제한을 만족하려면 사용자 작성 동안 시스템을 통하여 전달되는 추가 속성을 지정해야 할 수 있습니다.

필요한 속성을 수정 속성으로 지정한 경우 ("[사용자 속성 선택 및 매핑](#)" [페이지 125](#)의 설명 참조) 추가 속성은 필요하지 않습니다.

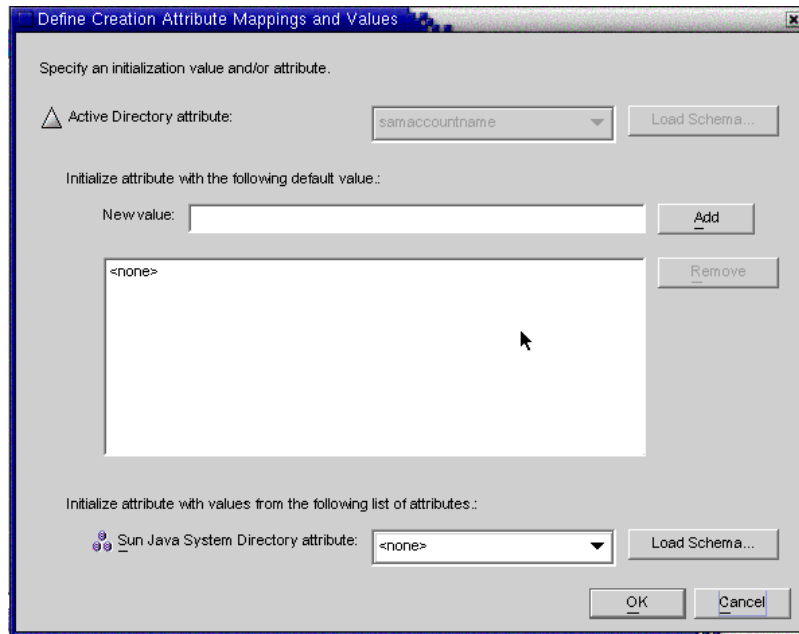
- 기존 속성 편집 ([페이지 134](#) 참조)
- 기존 속성 제거 ([페이지 134](#) 참조)

새 생성 속성 지정

Active Directory 에서 Directory Server 로 생성 속성을 추가하고 매핑하는 방법은 아래에 설명하는 것과 같습니다 . (Directory Server 에서 Windows 로 , 또한 Windows 에서 Directory Server 로 전달되는 생성 속성의 추가 및 매핑 방법도 이와 비슷합니다 .)

1. Creation Attribute Mappings and Values 대화 상자에서 New 버튼을 누릅니다 . Define Creation Attribute Mappings and Values 대화 상자가 표시됩니다 (그림 4-37).

그림 4-37) 생성 속성 매핑 및 값 정의



2. Active Directory 속성 드롭다운 목록에서 속성 값을 선택합니다 .

그림 4-38) 새 Active Directory 속성 선택

Identity Synchronization for Windows 를 사용하여 속성 자체가 복수 값을 허용하는 경우 이 속성을 복수 값으로 초기화할 수 있습니다.

예를 들어 회사에 세 개의 팩스 번호가 있는 경우 Sun Java System Directory Server 와 Active Directory 모두에 facsimiletelephonenumber 속성을 지정하고 세 개의 번호를 지정할 수 있습니다.

반드시 복수 값을 허용하는 속성이 어느 것인지 알아야 합니다. 복수 값을 허용하지 않는 속성에 복수 값을 추가하면 프로그램이 객체를 만들려고 시도하는 런타임에 오류가 발생합니다.

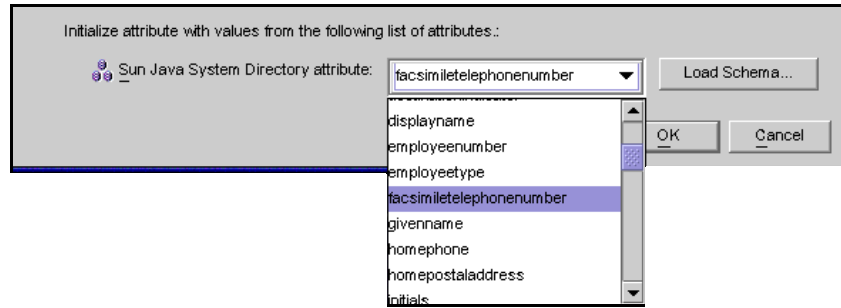
3. New value 필드에 값을 입력하고 Add 를 누릅니다.

프로그램에서 속성 값이 목록 창에 추가됩니다. 복수 속성 값을 모두 추가할 때까지 이 단계를 반복합니다.

그림 4-39) 생성 속성에 복수 값 지정

4. 속성을 Directory Server로 매핑하려면 Directory Server 속성 드롭다운 목록에서 속성 이름을 선택합니다.

그림 4-40) Directory Server 속성 매핑



- 작업을 완료했으면 OK 를 누릅니다 .
예제에서 완료된 생성 속성과 매핑 표는 다음 그림에 보이는 것과 유사합니다 .

그림 4-41) 완료된 생성 속성 및 매핑 표

Active Directory	디렉토리 서버	값
cn	cn	
samaccountname	<없음>	
facsimiletelephonenumber...	facsimiletelephonenumber...	222-222-222,555-555,...

- 추가 속성을 지정하려면 이들 단계를 반복합니다 .

기존 속성 편집

생성 속성 매핑 또는 값을 편집하려면 다음과 같이 합니다 .

- Object Creation 탭을 선택하고 선택한 작성 옵션의 아래에 있는 Creation Attributes 버튼을 누릅니다 .
- Creation Mappings and Values 대화 상자가 표시되면 표에서 속성을 선택하고 Edit 버튼을 누릅니다 .
Define Creation Attribute Mappings and Values 대화 상자가 표시됩니다 .
- 드롭다운 메뉴를 사용하여 Directory Server 와 Active Directory(또는 Windows NT) 사이의 기존 매핑을 변경합니다 .
예를 들어 Sun Java System Directory Server 의 homephone 속성이 Active Directory 의 othertelephone 속성으로 매핑될 수 있습니다 . Active Directory 속성 드롭다운 목록을 사용하여 이 매핑을 homephone 으로 변경할 수 있습니다 .
- 또한 속성 값을 추가하거나 제거할 수 있습니다 .
 - 값을 추가하려면 New Value 필드에 정보를 입력하고 Add 를 누릅니다 .

- 값을 제거하려면 목록 창에서 값을 선택하고 Remove 를 누릅니다 .
- 5. 작업을 완료했으면 OK 를 눌러 변경 내용을 적용하고 Define Creation Mappings and Values 대화 상자를 닫습니다 .
- 6. OK 를 다시 눌러 Creation Mappings and Attributes 대화 상자를 닫습니다 .

속성 제거

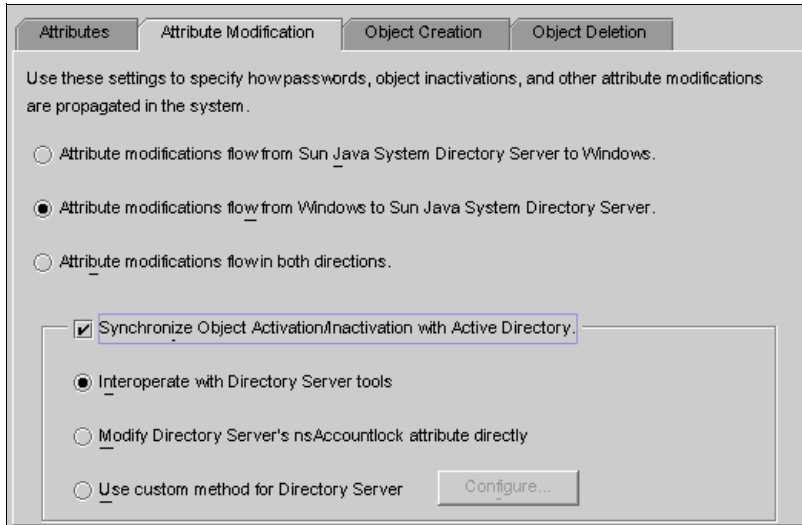
생성 속성 매핑 또는 값을 제거하려면 다음과 같이 합니다 .

1. Object Creation 탭을 선택하고 선택한 작성 옵션의 아래에 있는 Creation Attributes 버튼을 누릅니다 .
2. Creation Mappings and Values 대화 상자가 표시되면 표에서 속성을 선택하고 Delete 버튼을 누릅니다 .
즉시 테이블에서 속성이 제거됩니다 .
3. 작업을 완료했으면 OK 를 눌러 Creation Mappings and Attributes 대화 상자를 닫습니다 .

객체 수정 내용 흐름 방식 지정

Attribute Modification 탭 (그림 4 42) 을 사용하여 사용자 속성과 비밀번호의 변경 내용이 Sun 과 Windows 시스템 사이에서 전달되는 방식을 제어할 수 있습니다 .

그림 4-42) Attribute Modification 탭



이 탭을 사용하여 다음을 구성합니다.

- Directory Server 및 Windows 디렉토리 소스 사이에서 수정이 전달되는 방향을 지정합니다.
- Directory Server 와 Active Directory 디렉토리 소스 사이에서 객체 활성화 및 비활성화 (Active Directory 에서 사용 또는 사용 안 하도록 설정) 를 동기화할 것인지 제어하고 사용자 계정을 활성화 및 비활성화하는 방법을 지정합니다.

참고 Windows NT 디렉토리 소스와 계정 상태를 동기화할 수 없습니다.

방향 지정

다음 버튼 중 하나를 선택하여 Directory Server 와 Windows 환경에서 변경된 내용이 시스템 사이에서 전달되는 방식을 제어합니다.

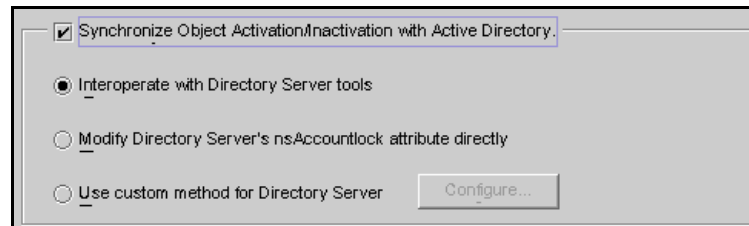
- 속성 변경 내용을 Sun Java System Directory Server 에서 Windows 로 전달 : Directory Server 환경의 변경 내용을 Windows 서버로 전달합니다.
- 속성 변경 내용을 Windows 에서 Sun Java System Directory Server 로 전달 (기본값): Windows 서버 환경의 변경 내용을 Directory Server 로 전달합니다.
- 속성 변경 내용을 양 방향으로 전달 : 변경 내용을 양방향 (한 시스템에서 다른 시스템) 으로 전달합니다.

객체 활성화 및 비활성화 구성 및 동기화

Synchronize Object Activations/Inactivations with Active Directory 선택란 (그림 4-43 참조) 을 선택하여 Directory Server 및 Active Directory 디렉토리 소스 사이에서 객체 활성화 및 비활성화 (Active Directory 에서 *사용* 및 *사용 안 함* 설정) 를 동기화할 수 있습니다 .

참고 Windows NT 디렉토리 소스와 활성화 및 비활성화를 동기화할 수 없습니다 .

그림 4-43) 객체 활성화 및 비활성화 동기화



객체 활성화 / 비활성화를 동기화하려면 다음과 같이 합니다 .

1. Synchronize Object Inactivations between Directory Server & Active Directory 선택란을 선택합니다 .
2. 다음 버튼 중 하나를 선택하여 Identity Synchronization for Windows가 객체 활성화 및 비활성화를 찾고 동기화하는 방식을 지정합니다 .
 - **Interoperate with Directory Server tools** ([페이지 140](#) 참조)
 - **Modify Directory Server's nsAccountLock attribute directly** ([페이지 141](#) 참조)
 - **Use custom method for Directory Server** ([페이지 142](#) 참조)

참고

이들 옵션은 동시에 사용할 수 없습니다.

- Interoperate with Directory Server Tools 옵션을 사용 설정하면 Identity Synchronization for Windows 가 nsAccountLock 속성을 직접 설정하거나 제거할 수 없습니다. 또한 프로그램은 cn=nsdisabledrole, <database suffix> 등의 다른 역할이나 cn=nsdisabledrole, <database suffix> 또는 cn=nsmanageddisabledrole, <database suffix> 등의 다른 역할에 중첩된 역할을 사용하여 활성화한 객체를 찾을 수 없습니다.
- Modify Directory Server's nsAccountLock attribute 옵션을 사용 설정하면 Identity Synchronization for Windows 는 Directory Server 콘솔 또는 명령줄 유틸리티를 사용하여 활성화 / 비활성화된 객체를 찾을 수 없습니다.
- Use custom method for Directory Server 옵션을 사용 설정하면 Identity Synchronization for Windows 는 Sun JavaTM System Access Manager(기존의 Sun JES Identity Server) 등의 외부 응용 프로그램으로 디렉토리에 대한 액세스를 제한하지 않는 한 객체를 디렉토리 밖으로 고정할 수 없습니다.

Directory Server 도구와 상호 운용

Directory Server 콘솔 또는 명령줄 도구를 사용하여 객체를 활성화 / 비활성화하는 경우 이 옵션을 선택합니다.

- Identity Synchronization for Windows 는 객체를 활성화하기 위하여 nsroledn 에서 cn=nsmanageddisabledrole, <database suffix> 값을 제거합니다.
- Identity Synchronization for Windows 는 객체를 활성화하기 위하여 nsroledn 에 cn=nsmanageddisabledrole, <database suffix> 값을 추가합니다.

참고

Interoperate with Directory Server Tools 옵션을 사용 설정하면 Identity Synchronization for Windows 가 nsAccountLock 속성을 직접 설정하거나 제거할 수 없습니다. 또한 다른 역할을 사용하여 비활성화된 객체를 찾을 수 없습니다.

예 : cn=nsdisabledrole, <database suffix> 또는
cn=nsdisabledrole, <database suffix> 또는
cn=nsmanageddisabledrole, <database suffix> 등의 다른 역할 내에
중첩된 역할

Interoperate with Directory Server Tools 옵션을 사용 설정하는 경우 Identity Synchronization for Windows 가 객체 활성화 / 비활성화를 찾고 동기화하는 방식은 의 설명과 같습니다.

표 4-1) Directory Server 도구와 상호 운용

활성화	비활성화
Identity Synchronization for Windows 는 객체에서 cn=nsmanageddisabledrole, <database suffix> 역할이 제거된 경우에만 활성화를 찾습니다.	Identity Synchronization for Windows 는 항목의 nsroledn 속성에 cn=nsmanageddisabledrole, <database suffix> 역할이 포함된 경우에만 비활성화를 찾습니다.
Active Directory 에서 객체 활성화를 동기화하는 경우 Identity Synchronization for Windows 는 해당 객체에서 cn=nsmanageddisabledrole, <database suffix> 역할을 제거하여 객체를 활성화합니다.	Active Directory 에서 객체 비활성화를 동기화하는 경우 Identity Synchronization for Windows 는 해당 객체에 cn=nsmanageddisabledrole, <database suffix> 역할을 추가하여 객체를 활성화합니다.

Directory Server 의 NsAccountLock 속성 직접 수정

Directory Server 활성화 및 비활성화가 Directory Server 의 운영 속성 nsAccountLock 에 기반하는 경우 이 방법을 사용합니다. 이 속성이 제어하는 객체 상태는 다음과 같습니다.

- nsAccountLock=true 의 경우 객체는 비활성화되며 사용자는 로그인할 수 없습니다.
- nsAccountLock=false 의 (또는 값이 없는) 경우 객체는 활성화됩니다.

Modify Directory Server's nsAccountLock Attribute Directly 옵션을 사용 설정하는 경우 Identity Synchronization for Windows 가 객체 활성화 / 비활성화를 찾고 동기화하는 방식은 의 설명과 같습니다.

표 4-2) Directory Server 의 nsAccountLock 속성 직접 수정

활성화	비활성화
Identity Synchronization for Windows 는 nsAccountLock 속성이 true 로 설정된 경우에만 비활성화된 객체를 찾습니다.	Identity Synchronization for Windows 는 nsAccountLock 속성이 false 로 설정된 경우에만 활성화된 객체를 찾습니다.

표 4-2) Directory Server 의 nsAccountLock 속성 직접 수정

Active Directory 에서 객체 비활성화를 동기화하는 경우 Identity Synchronization for Windows 는 nsAccountLock 속성을 제거합니다 .	Active Directory 에서 객체 활성화를 동기화하는 경우 Identity Synchronization for Windows 는 nsAccountLock 속성을 true 로 설정합니다 .
--	---

Directory Server 용 사용자 정의 방법 사용

Sun Java™ System Access Manager(기존의 Sun JES Identity Server) 등의 외부 응용 프로그램을 사용하여 Directory Server 의 활성화 및 비활성화를 전적으로 제어하는 경우 이 방법을 사용합니다 .

Directory Server 용 사용자 정의 방법을 구성하는 경우 반드시 다음을 지정합니다 .

- Identity Synchronization for Windows 가 Directory Server 에서 외부 응용 프로그램으로 객체를 활성화 또는 비활성화하는지 찾는 방식
- Active Directory 에서 Directory Server 로 동기화할 때 Identity Synchronization for Windows 가 객체를 활성화 또는 비활성화하는 방식

참고

Use custom method for Directory Server 옵션을 사용 설정하는 경우 Identity Synchronization for Windows 는 Access Manager 등의 외부 응용 프로그램으로 디렉토리에 대한 액세스를 제한하지 않는 한 객체를 디렉토리 밖으로 고정할 수 없습니다 .

활성화 및 비활성화를 위하여 사용자 정의 방법을 구성하려면 **Configure** 버튼을 클릭합니다 . **Configure Custom Method for Directory Server** 대화 상자가 표시됩니다 (그림 4-44 참조) .

그림 4-44) 활성화 및 비활성화를 위한 사용자 정의 방법 구성

Configure a custom method for activating and inactivating Directory Server objects.

Activation state attribute :

Values used by Identity Synchronization for Windows to **detect** an object's activation state.

Value	State
No Value	Activated
All Other Values	Inactivated

Values used by Identity Synchronization for Windows to **set** an object's activation state.

Activated value :

Inactivated value :

이 대화 상자에는 다음 기능이 있습니다.

- **활성화 상태 속성 드롭다운 목록** : 이 목록을 사용하여 Identity Synchronization for Windows 가 Directory Server 와 Active Directory 사이에서 활성화 및 비활성화를 동기화할 때 사용할 속성을 지정합니다.

목록에는 현재 선택된 Directory Server 구조 및 보조 objectclass 의 스키마에 있는 속성이 모두 포함됩니다.

- **Value 및 State 표** : 이 표를 사용하여 선택된 속성과 연결된 값이 동기화 또는 비동기화되는 시간을 지정합니다.

- **Value 열** : 이 열을 사용(New 및 Remove 버튼과 함께 사용)하여 활성화 또는 비활성 상태를 표시하는 데 사용할 속성 값을 지정합니다.

프로그램은 이 열에 자동으로 두 개의 값을 입력합니다.

- **No Value** : Activation 상태 속성에 값이 없는 경우

- **All Other Values** : Active 상태 속성에 값이 있으나 이 Value 및 State 표에 지정되지 않은 값인 경우.

- **State 열** : 이 열을 사용하여 Value 항목 (같은 열) 이 활성화 또는 비활성화되는 객체에 해당하는지 지정합니다.

표 4-3) 활성화 및 비활성화된 상태 지정

값	상태	결과
No Value	Activated	속성이 없거나 속성에 값이 없는 경우 Identity Synchronization for Windows 는 객체를 활성화된 것으로 검출합니다 .
	Inactivated	속성이 없거나 속성에 값이 없는 경우 Identity Synchronization for Windows 는 객체를 비활성화된 것으로 검출합니다 .
< 사용자 정의 > 값	Activated	속성에 < 사용자 정의 > 속성이 있는 경우 Identity Synchronization for Windows 는 객체가 활성화된 것으로 검출합니다 .
	Inactivated	속성에 사용자 정의 속성이 있는 경우 Identity Synchronization for Windows 는 객체가 비활성화된 것으로 검출합니다 .
All Other Values	Activated	속성에 값이 있으나 표에 지정된 값이 아닌 경우 Identity Synchronization for Windows 는 객체를 활성화된 것으로 검출합니다 .
	Inactivated	속성에 값이 있으나 표에 지정된 값이 아닌 경우 Identity Synchronization for Windows 는 객체를 비활성화된 것으로 검출합니다 .

- **New 버튼** : 이 버튼을 사용하여 Value 열에 새 항목을 추가합니다 .
- **Remove 버튼** : Value 열의 항목을 선택한 후 , 이 버튼을 눌러 해당 항목을 삭제합니다 .
- **활성화된 값 및 비활성화된 값 드롭다운 목록** : 이 두 목록을 사용하여 Identity Synchronization for Windows 가 객체의 상태를 설정할 때 사용하는 값을 지정합니다 .

동기화 및 비동기화 동기화 Directory Server 및 Active Directory 사이에서 객체 상태를 찾고 동기화하도록 Identity Synchronization for Windows를 구성하려면 다음과 같이 합니다 .

1. Activation 상태 속성 드롭다운 목록에서 속성을 선택합니다 .
2. 표의 Value 열에 속성 값을 추가하려면 New 버튼을 누릅니다 .
3. 각 Value 항목의 옆에 있는 State 열을 누르고 드롭다운 목록이 표시되면 Activated 또는 Inactivated 를 선택합니다 .

그림 4-45) 상태 선택

Value	State
No Value	Activated
active	Inactivated
All Other Values	Activated
	Inactivated

예를 들어 Access Manager 를 사용하는 경우 ,

1. Activation 상태 속성 드롭다운 목록에서 **inetuserstatus** 속성을 선택합니다 .
2. New 버튼을 누르고 표의 Value 열에 **active**, **inactive** 및 **deleted** 속성 값을 입력합니다 .
3. State 열을 누르고 다음과 같이 각 값에 대하여 Activated 또는 Inactivated 를 선택합니다 .
 - **No Value**: Activated
 - **active**: Activated
 - **inactive**: Inactivated
 - **deleted**: Inactivated
 - **All Other Values**: Inactivated

이 예제 이외에도 Use Custom Method for Directory Server 옵션을 사용 설정 (inetuserstatus 예제 사용) 하는 경우 Identity Synchronization for Windows 가 활성화 / 비활성화를 찾고 동기화하는 방법은 표 4-4 의 설명과 같습니다 .

표 4-4) inetuserstatus 값을 사용하는 예제 결과

값	상태	결과
No Value	Activated	inetuserstatus 속성이 없거나 속성에 값이 없는 경우 Identity Synchronization for Windows 는 객체를 활성화된 것으로 검출합니다 .
active	Activated	속성이 active 인 경우 Identity Synchronization for Windows 는 객체가 활성화된 것으로 검출합니다 .
inactive	Inactivated	속성 값이 inactive 인 경우 Identity Synchronization for Windows 는 객체가 비활성화된 것으로 검출합니다 .
deleted	Inactivated	속성 값이 deleted 인 경우 Identity Synchronization for Windows 는 객체가 비활성화된 것으로 검출합니다 .

표 4-4) inetuserstatus 값을 사용하는 예제 결과

All Other Values	Inactivated	속성에 값이 있으나 표에 지정된 값이 아닌 경우 Identity Synchronization for Windows 는 객체를 비활성화된 것으로 검출합니다.
------------------	-------------	--

동기화 및 비동기화 동기화 설정 Value 및 State 표에 항목을 입력하는 동안 Identity Synchronization for Windows 는 다음과 같이 자동으로 **Activated** 값 및 **Inactivated** 값 드롭다운 목록을 입력합니다.

- **Activated** 값 목록에는 상태가 **Activated** 인 모든 값 (예 : **No Value** 및 **active**) 이 포함됩니다.
- **Inactivated** 값 목록에는 상태가 **Inactivated** 인 모든 값 (예 : **inactive** 및 **deleted**) 이 포함됩니다.
- 두 목록 모두 All Other Values 값을 포함하지 않습니다.

Activated 값 또는 **Inactivated** 값 드롭다운 목록에서 값을 선택하여 Identity Synchronization for Windows 가 Active Directory 에서 동기화할 때 활성화 및 비활성화할 객체를 지정합니다.

- **Activated** 값 : 객체의 활성화 상태를 제어합니다.
 - **No Value**: 객체에 활성화 값이 있는 경우 Identity Synchronization for Windows 는 Directory Server 에서의 상태를 활성화로 설정합니다.
 - **active**: 객체에 활성화 값이 있는 경우 Identity Synchronization for Windows 는 Directory Server 에서의 상태를 활성화로 설정합니다.
- **Inactivated** 값 : 객체의 활성화 상태를 제어합니다.
 - **inactive** 또는 **deleted**: Identity Synchronization for Windows 는 Directory Server 에서 객체의 상태를 비활성화로 설정합니다.
 - **<none>**: 유효한 설정이 아닙니다. 반드시 값을 선택해야 합니다.

참고	반드시 Inactivated 값을 지정해야 하며 , 그렇지 않은 경우 구성이 무효화됩니다.
-----------	---

완료된 Configure Custom Method for Directory Server 대화 상자는 에 보이는 것과 같습니다.

그림 4-46) 예 : 완료된 대화 상자

Configure a custom method for activating and inactivating Directory Server objects.

Activation state attribute :

Values used by Identity Synchronization for Windows to **detect** an object's activation state.

Value	State
No Value	Activated
active	Activated
inactive	Inactivated
deleted	Inactivated
All Other Values	Inactivated

Values used by Identity Synchronization for Windows to **set** an object's activation state.

Activated value :

Inactivated value :

New

Remove

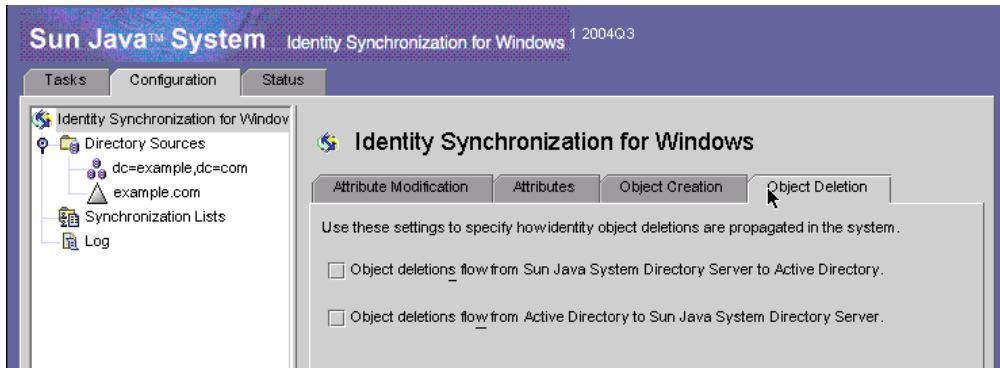
삭제 내용 흐름 방식 지정

Object Deletions 탭을 사용하여 Directory Server 와 Active Directory 시스템 사이에서 삭제된 사용자를 전달하는 방식을 지정합니다.

참고 Windows NT 용 객체 삭제 흐름은 지정할 수 없습니다.

1. 탐색 창의 상단에서 Identity Synchronization for Windows 노드를 선택하고 Object Deletion 탭을 누릅니다.

그림 4-47) 사용자 항목 삭제 전달



2. 다음과 같이 삭제의 흐름을 사용 또는 사용 불가로 설정합니다.
 - Directory Server 환경에서 삭제한 내용을 Active Directory 서버로 전달하려면 **Object deletions flow from Sun Java System Directory Server to Active Directory** 를 사용 설정합니다.
 - Active Directory 환경에서 삭제한 내용을 Directory Server 로 전달하려면 **Object deletions flow from Active Directory to Sun Java System Directory Server** 를 사용 설정합니다.
 - 양방향 흐름의 경우 두 옵션을 모두 사용 설정합니다.
 - 한 시스템에서 다른 시스템으로 사용자 삭제 내용이 전달되지 않도록 하려면 두 옵션을 모두 사용 불가로 설정합니다. (기본 설정)

Synchronization User Lists 작성

Synchronization User List 는 두 디렉토리 소스에서 동기화할 사용자를 지정합니다. SUL 에 있는 모든 항목은 커넥터를 통과하며 해당 SUL 용으로 구성된 제한을 확인합니다.

각 SUL 에는 두 개의 요소가 있으며 하나는 동기화할 디렉토리 사용자를 식별하며 다른 하나는 동기화할 Windows 사용자를 식별합니다.

참고

Directory Server 의 사용자를 복수 Active Directory 도메인과 동기화하려면 반드시 각 Active Directory 도메인마다 하나의 SUL 을 정의해야 합니다 .

SUL 의 정의와 구성 (정의의 구성요소 , 복수 SUL 정의 방법 , 복수 SUL 을 처리하는 방식 및 복수 Windows 도메인 지원을 구성하는 방법 등을 포함) 에 대한 자세한 내용은 [부록 D, "Synchronization User List 정의 및 구성" - 페이지 331](#) 를 참조하십시오 .

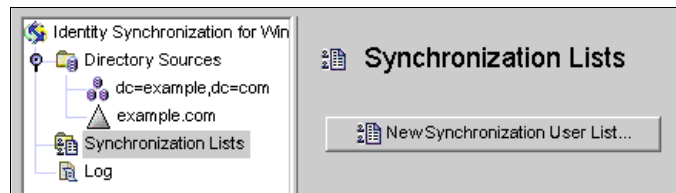
두 SUL 요소에는 모두 동기화할 사용자를 식별하는 세 개의 정의가 포함됩니다 .

- **기본 DN**: 동기화될 사용자의 위치 (NT 의 경우 적용되지 않음)
- **이름 지정 속성**: 새로 만든 사용자용으로 사용되는 속성 (생성 표현식)(NT 에는 적용되지 않음)
- **필터**: 지정한 사용자를 동기화에서 제외

서버 사이에서 사용자 유형을 식별하고 연결하려면 다음과 같이 합니다 .

1. 탐색 트리에서 Synchronization User Lists 노드를 선택하고 New Synchronization User List 버튼을 누릅니다 .

그림 4-48) 새 Synchronization User List 작성



다음과 같이 Define a Synchronization User List 마법사가 표시됩니다 .

그림 4-49) SUL 의 이름 지정

첫 번째 동기화 사용자 목록의 프로그램 기본값은 *SUL1* 입니다 .

- 기본 이름이 적절한 경우 **Next** 를 누릅니다 .
- 다른 이름을 사용하려면 **Name** 필드에 다른 이름을 입력하고 **Next** 를 누릅니다 .

참고

- SUL 이름에 공백이나 문장 부호를 사용하면 안 됩니다 .
- 반드시 시스템에서 고유한 이름을 지정해야 합니다 .

그림 4-50 에 보이는 것과 같이 **Windows Criteria** 패널이 표시됩니다 .

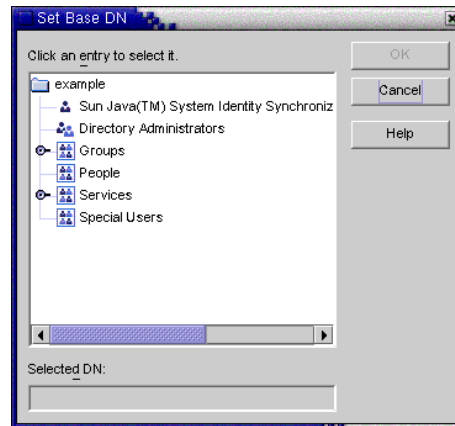
그림 4-50) Windows Criteria 지정

2. 드롭다운 목록에서 **Windows Directory Source** 를 선택합니다 .

참고 SUL 을 만든 후에는 이 디렉토리 소스를 편집할 수 없습니다.

3. *User Set Domain*은 동기화될 모든 사용자의 집합입니다. 다음 방법 중 한 가지를 사용하여 User Set Domain 의 기본 DN 을 입력합니다.
 - 입력란에 이름을 입력합니다 (예 : **DC=example,DC=com**).
 - 찾아보기 버튼을 눌러 검색할 수 있는 Set 기본 DN 대화 상자를 열고 기본 DN 을 선택합니다.

그림 4-51) 기본 DN 선택



필터를 사용하여 특별히 제외하지 않는 한, 지정한 기본 DN 에 속하는 모든 사용자는 이 SUL 에 포함됩니다.

참고 Windows NT 컴퓨터의 경우 기본 DN과 작성 표현식을 사용할 수 없습니다.

4. 동일성, 존재 또는 하위 문자열 필터를 입력하여 이 기본 DN에서 동기화될 사용자를 지정합니다. 예를 들어 여러 SUL에 동일한 기본 DN을 사용하는 경우 필터를 사용하여 이들 사이를 구분할 수 있습니다.

동일성 필터 구문은 동일성 하위 문자열에서는 *, &, |, =, ! 문자만을 사용할 수 있는 점을 제외하고 LDAP 쿼리 구문과 유사합니다. 예를 들어 다음 필터를 사용하여 SUL에서 Administrator를 제외할 수 있습니다.

(!(cn=Administrator))

프로그램에서 자동으로 Creation Expression 필드가 입력됩니다.

참고

작성 표현식은 새 항목이 Active Directory에서 Directory Server로 전달될 때 사용하는 상위 DN과 이름 지정 속성을 정의합니다.

사용자 속성 작성이 Active Directory에서 Directory Server로 전달되도록 구성하지 않는 한 Sun 디렉토리에서는 작성 표현식을 사용할 수 없습니다 ("객체 작성 흐름 방법 지정" 페이지 131 참조).

5. 작성 표현식이 없거나 기존 항목을 변경하려면 모든 Windows Active Directory SUL용 작성 표현식을 입력합니다. 예:

cn=%cn%,cl=users,dc=example,dc=com

작성 표현식을 변경하려는 경우 반드시 동기화할 속성을 선택해야 합니다. 필요한 경우 Object Creation 탭으로 되돌아가 Creation Attribute 버튼을 사용하여 이 속성을 추가 및 매핑합니다.

6. Next를 눌러 Sun Java System Directory Server 기준을 지정합니다.
7. Specify the Sun Java System Directory Server Criteria 패널이 표시되면 [단계 2](#)에서 [단계 5](#)까지 반복하여 Directory Server 기준을 입력합니다.

그림 4-52) Directory Server 기준 지정

단계

- 이름을 지정합니다.
- Windows 기준을 지정합니다.
- Sun Java 시스템 디렉토리 서버 기준을 지정합니다.**

Sun Java 시스템 디렉토리 서버 기준을 지정합니다.

디렉토리 소스(D):

사용자 설정 도메인

기본 DN(A):

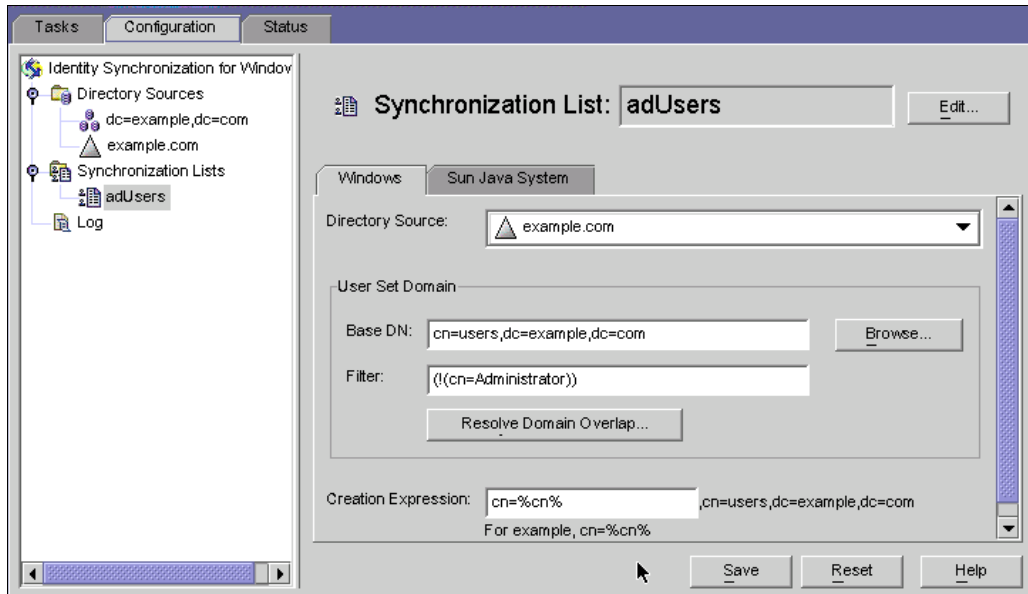
필터(F):

생성 표현식(X): 예: cn=%cn%

참고 Finish 버튼을 눌러 SUL 을 만든 후에는 이 SUL 에 포함된 Active Directory 또는 Directory Server 디렉토리 소스를 편집할 수 없습니다 .

- 작업을 완료했으면 Finish 를 누릅니다 .
- 프로그램이 새 SUL 노드를 탐색 트리에 추가하며 Configuration 탭에 Synchronization User List 패널이 표시됩니다 .

그림 4-53) Synchronization List 패널



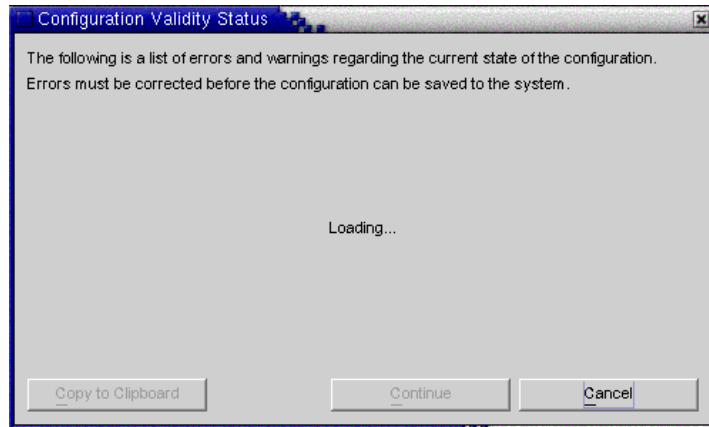
10. 사용자가 여러 개의 목록과 일치하는 경우 동기화 사용자 목록용 기본 설정을 정의하려면 **Resolve Domain Overlap** 버튼을 누릅니다. (더 자세한 내용은 ["Synchronization User Lists 정의 이해" 페이지 331](#) 를 참조하십시오.)
11. 네트워크에서 **Directory Server**를 제외한 모든 디렉토리 소스가 포함되는 동기화 사용자 목록을 만듭니다.

구성 저장

콘솔 패널에서 현재 구성을 저장하려면 다음과 같이 합니다.

1. Save 를 눌러 현재의 설정을 저장합니다 .
2. 프로그램이 구성 설정을 검사하는 동안 Configuration Validity Status 창이 표시됩니다 .

그림 4-54) Configuration Validity Status 창



프로그램은 정보를 구성 디렉토리에 다시 쓰고 시스템 관리자에게 알리므로 구성을 저장할 때 약간의 시간이 걸릴 수 있습니다.

시스템 관리자 (코어 구성요소) 는 구성 설정을 정보가 필요한 구성요소에 배포하는 임무를 수행합니다.

참고

구성 검증 오류는 빨간색이며 경고는 노란색입니다.

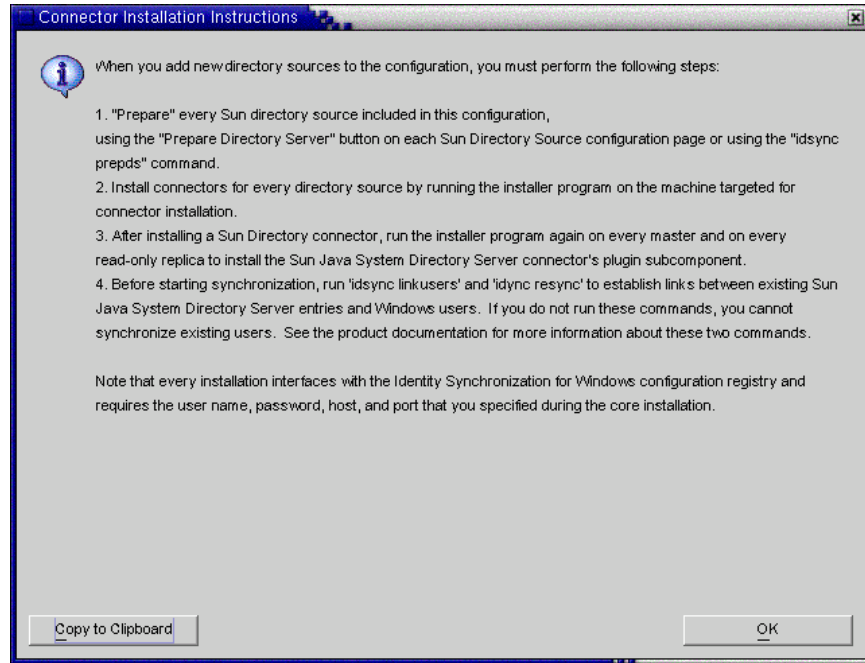
- 오류가 있는 구성은 저장할 수 없습니다.
 - 경고가 있는 구성은 저장할 수 있으나 우선 경고 내용을 수정하는 것이 좋습니다.
-

3. 구성이 유효하면 Continue 를 눌러 구성을 저장합니다.

Identity Synchronization for Windows 커넥터 및 하위 구성요소 설치 지침이 표시된 Connector Installation Instructions 대화 상자가 나타납니다 (그림 4-55 의 목록과 유사).

이 목록은 이제 구현에 맞게 사용자 정의된 To Do 목록으로 업데이트됩니다. (이 시점까지의 단계는 일반적인 단계입니다.) 또한 참고로 Identity Synchronization for Windows 콘솔의 Status 탭에서 To Do 목록을 액세스하고 업데이트할 수 있습니다.

그림 4-55) 커넥터 설치 방법



4. 내용을 신중히 읽고 OK 를 누릅니다 .

초기 코어 구성이 완료되면 Identity Synchronization for Windows 커넥터와 하위 구성요소를 설치할 수 있습니다 . 방법을 보려면 제 5 장 , " 커넥터 및 Directory Server 플러그인 설치 " 으로 계속하십시오 .

커넥터 및 Directory Server 플러그인 설치

이 장에서는 Identity Synchronization for Windows 커넥터와 Directory Server 플러그인을 설치하는 방법에 대하여 설명합니다. 다음과 같은 내용으로 구성됩니다.

- " 시작하기 전에 " 페이지 157
- " 설치 프로그램 실행 " 페이지 158
- " 커넥터 설치 " 페이지 160
- "Directory Server 플러그인 설치 " 페이지 171

Identity Synchronization for Windows는 커넥터를 사용하여 디렉토리 소스 사이에서 사용자 비밀번호를 동기화하며, 하위 구성요소를 사용하여 커넥터의 변경 감지 및 양방향 동기화 지원 기능을 더욱 강화합니다.

시작하기 전에

커넥터 /Directory Server 플러그인 설치 과정을 시작하기 전에 다음 사항에 유의해야 합니다.

- 설치 과정을 시작하기 전에 콘솔을 닫습니다. 커넥터 또는 플러그인을 설치할 때 콘솔이 열려 있으면 프로그램에 어느 구성요소가 구성 데이터를 추가하는지 혼동이 발생하며 오류 메시지가 생성됩니다.
- 반드시 구현에서 마스터, 복제본 및 허브를 포함하여 동기화될 사용자를 저장하는 모든 Directory Server 컴퓨터에 Directory Server 플러그인을 설치해야 합니다.
- Active Directory 커넥터에는 하위 구성요소가 없습니다.
- Windows NT 커넥터와 하위 구성요소는 동시에 설치됩니다.

- Directory Server 와 Active Directory 커넥터를 코어가 설치된 동일한 컴퓨터에 설치하거나 커넥터를 다른 컴퓨터에 설치할 수 있습니다. (Windows NT 커넥터는 반드시 동기화에 사용되는 도메인의 기본 도메인 제어기에 설치되어야 합니다.)
 - 커넥터를 코어와 동일한 컴퓨터에 설치하는 경우 자동으로 커넥터가 코어와 동일한 디렉토리에 설치됩니다.
 - 커넥터를 다른 컴퓨터에 설치하는 경우 다음을 지정하라는 프롬프트가 표시됩니다.
 - 코어 설치 동안 제공된 구성 디렉토리 정보
 - 설치 디렉토리
- 커넥터 또는 Directory Server 플러그인을 설치할 때마다 반드시 설치 프로그램을 실행해야 합니다.

예를 들어 Directory Server 커넥터, 단일 Directory Server 플러그인 및 Active Directory 커넥터를 설치하는 경우 코어가 설치된 후 설치 프로그램을 각각 세 번 실행해야 합니다.

설치 프로그램 실행

다음 절차를 사용하여 설치 프로그램을 재시작하고 실행합니다. 커넥터 또는 Directory Server 플러그인을 설치할 때마다 이 단계를 반복합니다.

1. 다음과 같이 커넥터를 설치할 컴퓨터에서 설치 프로그램을 다시 실행합니다.
 - **Solaris:** installer 디렉토리로 변경하고 **./runInstaller.sh** 를 입력하여 설치 프로그램을 실행합니다.

참고

텍스트 기반 모드에서 설치 프로그램을 실행하려면

./runInstaller.sh -nodisplay 를 입력합니다.

runInstaller.sh 프로그램을 실행하면 Identity Synchronization for Windows 가 자동으로 암호를 마스킹하여 보이게 반향되지 않도록 합니다.

- **Windows:** installer 디렉토리로 변경하고 **setup.exe** 를 입력하여 설치 프로그램을 실행합니다.
2. 인사말 화면이 표시되면 제공된 정보를 읽고 다음을 눌러 소프트웨어 사용권 계약 패널로 계속합니다.

3. 라이선스 계약을 읽은 후,
 - 라이선스 계약 조건에 동의하고 다음 패널로 계속하려면 **Yes(Accept License)**를 선택합니다.
 - 설치 과정을 중단하고 설치 프로그램을 종료하려면 **No**를 선택합니다.
4. Sun Java 시스템 Directory Server 패널이 표시됩니다. 다음과 같이 구성 디렉토리 위치를 지정합니다.
 - **구성 디렉토리 호스트**: Identity Synchronization for Windows 구성 정보가 저장되는 Sun Java 시스템 Directory Server 인스턴스 (Administration Server와 연계)의 정규화된 도메인 이름 (FQDN)을 입력합니다. 반드시 코어 설치 동안 지정한 동일한 인스턴스를 지정해야 합니다.
 - **구성 디렉토리 포트** (기본 포트 389): 구성 디렉토리용 포트를 지정합니다. 포트에 기본 값을 사용하거나 다른 사용 가능한 포트로 변경할 수 있습니다.
코어와 구성 디렉토리 사이에서 SSL(Secure Socket Layer)을 사용하려면 Secure Port 옵션을 사용 설정하고 SSL 포트 (기본 SSL 포트는 636)를 지정합니다. 이 옵션을 사용하면 중요한 정보가 네트워크에서 명확한 형태로 전달되는 것을 방지할 수 있습니다.
 - **구성 루트 접미어**: 메뉴에서 코어 설치 동안 지정한 루트 접미어를 선택합니다. Identity Synchronization for Windows 구성은 이 루트 접미어에 저장됩니다.

참고 프로그램에서 루트 접미어를 찾을 수 없으며 서버 정보를 직접 입력하는 경우 반드시 Refresh를 눌러 루트 접미어 목록을 다시 입력해야 합니다.

5. Next를 눌러 디렉토리 자격 증명 구성 패널을 엽니다.
6. 구성 디렉토리 Administrator의 사용자 ID 및 비밀번호를 입력합니다.
 - 사용자 ID로 admin을 지정하면 User ID와 DN을 지정할 필요가 없습니다.
 - 다른 사용자 ID를 사용하는 경우 반드시 ID와 전체 DN을 지정해야 합니다.
예 : *cn=Directory Manager*.

참고 단계 4에서 SSL을 활성화하지 않으면 자격 증명이 암호화되지 않은 상태에서 전송됩니다.

7. Next를 눌러 Configuration Password 패널을 열고, 여기에서 반드시 코어를 설치할 때 지정한 구성 비밀번호를 입력해야 합니다.

또한 이 컴퓨터에 코어가 설치되지 않은 경우 **Java Home** 디렉토리의 위치를 입력하라는 프롬프트가 표시됩니다 ([페이지 89](#) 참조).

8. 작업을 완료했으면 **Next** 를 누릅니다 .

참고 이 때 설치 과정은 설치하는 **Directory Server** 플러그인 또는 커넥터 유형으로 국한됩니다 .

- 커넥터를 설치하려면 "[커넥터 설치](#)" [페이지 160](#) 로 계속합니다 .
 - **Directory Server** 플러그인을 설치하려면 "[Directory Server 플러그인 설치](#)" [페이지 171](#) 로 계속합니다 .
-

커넥터 설치

여기에서는 다음과 같이 세 가지 유형의 **Identity Synchronization for Windows** 커넥터를 설치하는 방법에 대하여 설명합니다 .

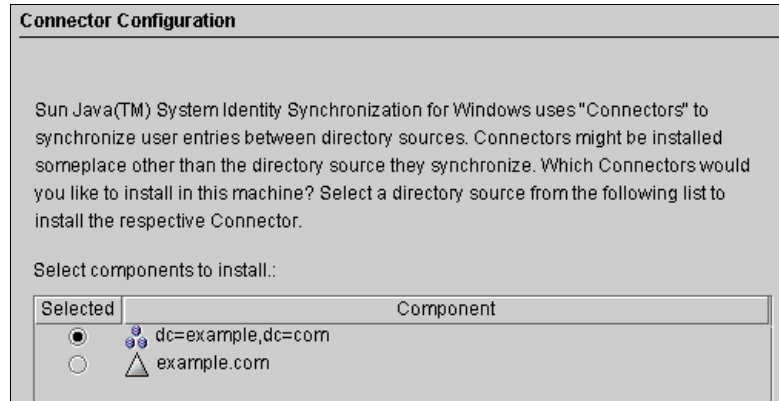
- "[Directory Server 커넥터 설치](#)" [페이지 160](#)
- "[Active Directory 커넥터 설치](#)" [페이지 166](#)
- "[Windows NT 커넥터 설치](#)" [페이지 170](#)

참고 커넥터는 순서에 상관 없이 설치할 수 있으나 여러 개의 커넥터를 동시에 설치하려 하면 안 됩니다 .

Directory Server 커넥터 설치

"[설치 프로그램 실행](#)" [페이지 158](#) 에 설명한 단계를 완료하면 **Connector Configuration** 패널이 표시됩니다 .

그림 5-1) Directory Server 커넥터 선택



Select components to install 목록에는 아직 설치되지 않은 커넥터 구성요소만 포함됩니다. 예를 들어 Directory Server 커넥터 (의 dc=example,dc=com) 를 설치하면 프로그램의 목록 창에서 해당 항목이 제거됩니다.

몇 가지 예제 디렉토리 소스 항목은 다음 표와 같습니다.

표 5-1) 디렉토리 소스 예제

디렉토리 소스	예제 항목
Sun Java 시스템 Directory Server	dc=example,dc=com
Windows Active Directory	example.com
Windows NT SAM	EXAMPLE

Directory Server 커넥터를 설치하려면 다음과 같이 합니다.

1. Directory Server Connector 구성요소 옆의 버튼을 선택하고 Next 를 누릅니다.
Directory Server Connector Credentials 패널이 표시됩니다 (그림 5-2).

그림 5-2) Directory Server 커넥터 자격 증명 입력

Directory Server Connector Credentials

Enter the directory manager credentials for the Sun Java(TM) System Directory Server(s) associated with the connector being installed.

Primary: ldap://machine1.example.com:389

Primary Directory Server User DN:

Primary Directory Server Password:

Secondary: none

Secondary Directory Server User DN:

Secondary Directory Server Password:

참고 프로그램이 자동으로 User DN 필드에 정규화된 Directory Manager 고유 이름을 입력하지만 필요한 경우 이 정보를 변경할 수 있습니다.

다음 정보를 입력합니다.

- 기본 **Directory Server** 사용자 DN: 필요한 경우 정규화된 Directory Manager 고유 이름을 입력하여 기본 사용자 DN 을 변경합니다.
- 기본 **Directory Server** 비밀번호: 디렉토리 관리자 비밀번호를 입력합니다.

보조 마스터를 사용하는 경우 Secondary Directory Server User Name 및 Password 필드가 활성화됩니다. 프로그램은 Primary Directory Server User DN 및 Password 필드에 입력된 동일한 항목을 Directory Manager DN 필드에 자동으로 입력합니다. 필요한 경우 이 정보를 변경할 수 있습니다.

프로그램은 해당 Directory Server 가 준비되었으며 데이터를 동기화할 수 있는지 검사합니다. Directory Server([페이지 109](#)) 가 준비되었으면 프로그램에서 커넥터가 Directory Server(예 :uid=PSWConnector,suffix) 로 연결할 때 사용할 계정이 만들어집니다.

2. Next 를 눌러 Connector Port Configuration 패널로 계속합니다.

그림 5-3) 커넥터 로컬 호스트 및 포트를 지정합니다.

커넥터 포트 구성	
<p>일부 Sun Java(TM) System Identity Synchronization for Windows 커넥터에는 TCP/IP 포트 번호가 필요합니다. 커넥터와 하위 구성요소 사이의 통신을 활성화하려면 TCP/IP 서버 포트 번호를 지정해야 합니다. 이 시스템의 다른 응용프로그램에서 사용될 수 없는 포트 번호를 지정해야 합니다.</p>	
전체 로컬 호스트 이름:	<input type="text" value="alclab-014.sfbay.sun.com"/>
커넥터 포트 번호:	<input type="text"/>

3. 도메인이 있는 정규화된 호스트 이름과 커넥터가 수신할 사용 가능한 포트 번호를 입력합니다. (이미 사용 중인 포트를 지정하면 오류 메시지가 발생합니다.)

Directory Server 플러그인은 콘솔에서 저장한 구성 정보를 사용할 수 있어야 합니다. 이 정보를 가져오려면 플러그인이 이 포트의 서버 소켓을 통하여 Directory Server 커넥터와 통신합니다. 또한 플러그인은 이 채널을 통한 메시지를 기록하여 해당 메시지가 중앙 로그로 기록될 수 있도록 합니다.

4. Next 를 눌러 Ready to Install 창을 엽니다. 여기에는 커넥터의 설치 위치에 대한 정보와 설치에 필요한 디스크 공간이 표시됩니다. 준비가 되었으면 Install Now 버튼을 누릅니다.

그림 5-4) Ready to Install 창

설치 준비가 되었습니다.
<p>제품: Identity Synchronization for Windows 위치: /opt/SUNWisw 필요한 공간: 5.75 MB ----- Sun Java(TM) System Identity Synchronization for Windows Connector</p>

참고 로컬 컴퓨터에 코어를 설치한 경우 Ready to Install 창에 커넥터를 설치하기 위하여 필요한 공간이 0 으로 표시됩니다. 이러한 상황은 코어 설치가 이미 커넥터 이진을 설치한 경우 발생합니다. 설치할 추가 이진이 없으므로 추가 공간이 필요하지 않습니다.

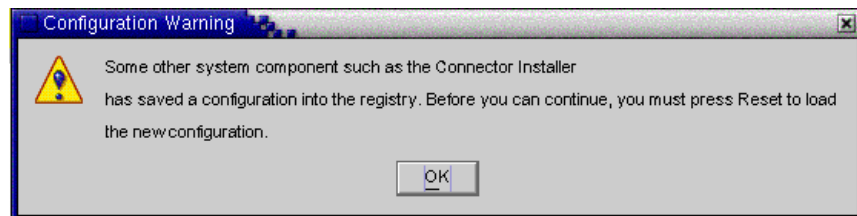
코어를 설치한 컴퓨터와 다른 컴퓨터에 커넥터를 설치하는 경우 Ready to Install 창에 로컬 컴퓨터에서 커넥터 설치를 완료하는 데 필요한 공간이 표시됩니다.

커넥터 설치의 두 단계로 완료됩니다.

- 프로그램에서 이진 설치가 진행되며 진행표시줄이 있는 Installing 창이 표시됩니다.
- 다음, Component Configuration 창이 표시됩니다. 이 단계가 완료되려면 다소 시간이 걸리므로 진행표시줄이 표시됩니다.

참고 설치를 시작하기 전에 콘솔을 닫지 않은 경우 다음 경고가 표시됩니다 (그림 5-5). 콘솔에서 Reset 을 눌러 커넥터의 구성 설정을 다시 로드합니다.

그림 5-5) 구성 경고 대화 상자



두 단계가 모두 완료되면 Installation Summary 창이 표시됩니다.

5. 설치 로그를 보려면 Details 버튼을 누릅니다.
 - **Solaris:** 설치 로그는 /var/sadm/install/logs/ 에 기록됩니다.
 - **Windows:** 설치 로그는 %TEMP% 디렉토리에 기록되며, 이 디렉토리는 다음 폴더 아래에 있는 Local Settings 폴더의 하위 디렉토리입니다.
C:\Documents and Settings\Administrator

참고

일부 Windows 시스템 (Windows 2000 Advanced Server 등) 의 경우 Local Settings 폴더가 숨겨져 있습니다 .

이 폴더와 Temp 하위 디렉토리를 보려면 Windows 탐색기를 열고 메뉴줄에서 도구 > 폴더 옵션을 선택합니다 . 폴더 옵션 대화 상자가 표시되면 보기 탭을 누르고 숨긴 파일 표시 옵션을 선택합니다 .

6. Next 를 누르면 성공적으로 완료된 단계와 남은 단계를 보여주는 "To Do list" 패널 (그림 5-6) 이 표시됩니다 .

그림 5-6) To Do 목록

설치 및 구성의 나머지 단계는 이 목록과 같습니다.:

- ✓ 1 : Identity Synchronization 코어 구성 요소를 설치합니다.
- ✓ 2 : 제품의 콘솔을 사용하거나 'idsync importcnf'로 이전 설치에서 이전하여 초기 구성을 만듭니다.
- ✓ 3 : 콘솔 또는 'idsync prepds' 명령을 사용하여 이 구성에 있는 모든 Sun Directory Server 마스터 [ldap://alclab-014.sfbay.sun.com:389]을(를) 준비합니다.
- ✓ 4 : 설치 프로그램을 다시 실행하여 임의의 Solaris 또는 Windows 2000 컴퓨터에 Sun Directory 소스dc=sfbay,dc=sun,dc=com용 커넥터를 설치합니다.
- 5 : 설치 프로그램을 다시 실행하여 임의의 Solaris 또는 Windows 2000 컴퓨터에 Active Directory 도메인 sfbay.sun.com용 커넥터를 설치합니다.
- 6 : 설치 프로그램을 다시 실행하여 마스터 ldap://alclab-014.sfbay.sun.com:389에 Sun Directory Server 플러그인을 설치합니다.
- 7 : 다른 모든 마스터와 dc=sfbay,dc=sun,dc=com 아래에서 사용자를 관리하는 읽기 전용 복제본에 Sun Directory Server 플러그인을 설치합니다.
- 8 : 'idsync resync'를 실행하여 기존 Directory Server와 Windows 사용자 사이의 링크를 설정합니다.
- 9 : 콘솔 또는 'idsync startsync' 명령을 사용하여 동기화를 시작합니다.

7. 패널에서의 작업을 완료했으면 Finish 를 누릅니다 .

Directory Server 커넥터를 설치한 후 자원을 구성할 때 구성한 기타 커넥터 및 Directory Server 플러그인을 설치할 수 있습니다 (4 장).

- 추가 Directory Server 커넥터 설치 : 설치 프로그램을 다시 시작 (" 설치 프로그램 실행 " 페이지 158 의 설명 참조) 하고 단계 1 에서 단계 7 까지의 단계를 반복합니다 .

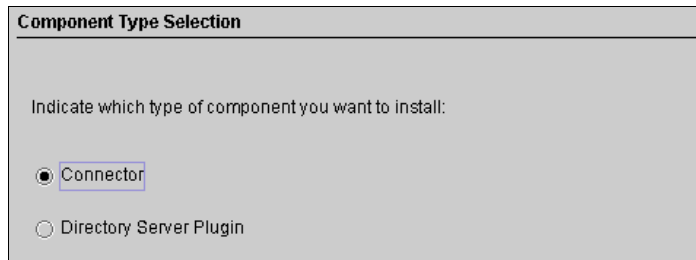
- Active Directory 커넥터 설치 : "[Active Directory 커넥터 설치](#) " 페이지 166 로 이동합니다 .
- Windows NT 커넥터 설치 : "[Windows NT 커넥터 설치](#) " 페이지 170 로 이동합니다 .
- Directory Server 플러그인 설치 : "[Directory Server 플러그인 설치](#) " 페이지 171 로 이동합니다 .

Active Directory 커넥터 설치

" [설치 프로그램 실행](#) " 페이지 158 에 설명한 단계를 완료하면 Component Type Selection 패널이 표시됩니다 .

참고 Directory Server 커넥터를 설치한 후 구성된 다른 커넥터를 설치해야 하는 경우 , Connector Configuration 창을 표시하기 전에 설치 프로그램에 커넥터 설치 또는 Directory Server 플러그인 설치용 옵션이 표시됩니다 (그림 5-7).

그림 5-7) 커넥터 선택

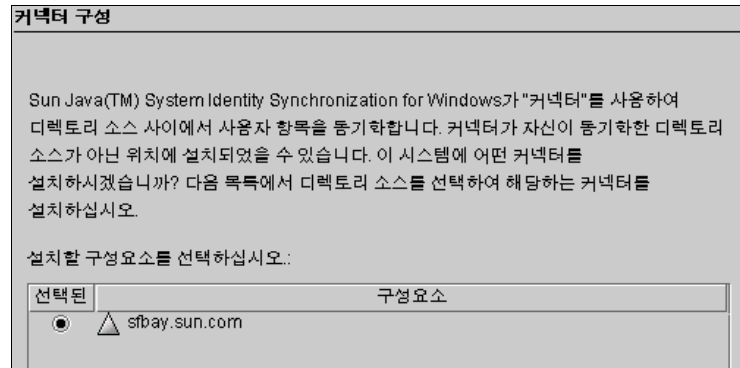


구성요소 목록에는 아직 설치하지 않은 커넥터 구성요소만 포함됩니다 . 예를 들어 이미 Directory Server 커넥터 (이 경우 dc=example,dc=com) 를 설치한 경우 이 커넥터는 표시되지 않습니다 .

Active Directory 커넥터를 설치하려면 다음과 같이 합니다 .

1. Connector 버튼을 사용 설정하고 Next 를 누릅니다 .
커넥터 구성 패널이 표시됩니다 (그림 5-8 참조).

그림 5-8) Active Directory Connector 선택

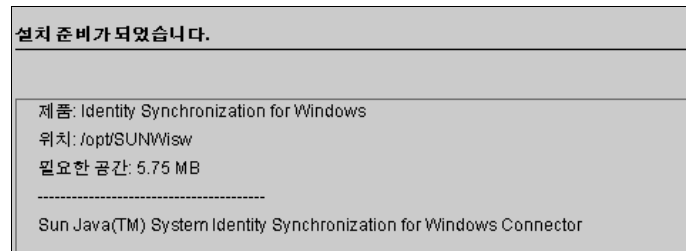


Select components to install 목록에는 아직 설치되지 않은 커넥터 구성요소만 포함됩니다. 예를 들어 Directory Server 커넥터 (dc=example,dc=com in this case) 를 설치하면 프로그램의 목록 창에서 해당 항목이 제거됩니다.

2. Active Directory component 옆의 버튼을 선택하고 Next 를 누릅니다.

Ready to Install 창이 열리며 (그림 5-9), 커넥터의 설치 위치에 대한 정보와 설치에 필요한 디스크 공간이 표시됩니다.

그림 5-9) Ready to Install 창



참고

로컬 컴퓨터에 코어를 설치한 경우 Ready to Install 창에 커넥터를 설치하기 위하여 필요한 공간이 0 으로 표시됩니다. 이러한 상황은 코어 설치가 이미 커넥터 이진을 설치한 경우 발생합니다. 설치할 추가 이진이 없으므로 추가 공간이 필요하지 않습니다.

코어를 설치한 컴퓨터와 다른 컴퓨터에 커넥터를 설치하는 경우 Ready to Install 창에 로컬 컴퓨터에서 커넥터 설치를 완료하는 데 필요한 공간이 표시됩니다.

3. 준비가 되었으면 **Install Now** 버튼을 누릅니다.

프로그램이 이진을 설치하는 동안 진행 표시줄이 있는 **Installing** 창이 표시되며, 설치가 완료되면 이를 확인하는 **Installation Summary** 창이 표시됩니다.

4. 설치 로그를 보려면 **Details** 버튼을 누릅니다.

- **Solaris:** 설치 로그는 `/var/sadm/install/logs/` 에 기록됩니다.
- **Windows:** 설치 로그는 `%TEMP%` 디렉토리에 기록되며, 이 디렉토리는 다음 폴더 아래에 있는 `Local Settings` 폴더의 하위 디렉토리입니다.
`C:\Documents and Settings\Administrator`

참고

일부 Windows 시스템 (Windows 2000 Advanced Server 등) 의 경우 `Local Settings` 폴더가 숨겨져 있습니다.

이 폴더와 `Temp` 하위 디렉토리를 보려면 Windows 탐색기를 열고 메뉴줄에서 도구 > 폴더 옵션을 선택합니다. 폴더 옵션 대화 상자가 표시되면 보기 탭을 누르고 숨긴 파일 표시 옵션을 선택합니다.

5. Next를 누르면 "To Do list" 창(그림 5-10)이 표시되어 성공적으로 완료된 단계와 나머지 단계가 표시됩니다.

그림 5-10) To Do 목록

설치 및 구성의 나머지 단계는 이 목록과 같습니다.:

- ✓ 1 : Identity Synchronization 쿼어 구성 요소를 설치합니다.
- ✓ 2 : 제품의 콘솔을 사용하거나 'idsync importcnf'로 이전 설치에서 이전하여 초기 구성을 만듭니다.
- ✓ 3 : 콘솔 또는 'idsync prepds' 명령을 사용하여 이 구성에 있는 모든 Sun Directory Server 마스터 [ldap://alclab-014.sfbay.sun.com:389]을(를) 준비합니다.
- ✓ 4 : 설치 프로그램을 다시 실행하여 임의의 Solaris 또는 Windows 2000 컴퓨터에 Active Directory 도메인 sfbay.sun.com용 커넥터를 설치합니다.
- ✓ 5 : 설치 프로그램을 다시 실행하여 임의의 Solaris 또는 Windows 2000 컴퓨터에 Sun Directory 소스 dc=sfbay,dc=sun,dc=com용 커넥터를 설치합니다.
- 6 : 설치 프로그램을 다시 실행하여 마스터 ldap://alclab-014.sfbay.sun.com:389에 Sun Directory Server 플러그인을 설치합니다.
- 7 : 다른 모든 마스터와 dc=sfbay,dc=sun,dc=com 아래에서 사용자를 관리하는 읽기 전용 복제본에 Sun Directory Server 플러그인을 설치합니다.
- 8 : 'idsync resync'를 실행하여 기존 Directory Server와 Windows 사용자 사이의 링크를 설정합니다.
- 9 : 콘솔 또는 'idsync startsync' 명령을 사용하여 동기화를 시작합니다.

6. 패널에서의 작업을 완료했으면 Finish 를 눌러 설치 프로그램을 종료합니다 .

Active Directory 커넥터를 설치한 후 자원을 구성할 때 구성한 기타 커넥터 및 Directory Server 플러그인을 설치할 수 있습니다 (4 장).

- 추가 Active Directory 커넥터를 설치하려면 다음과 같이 합니다 . 설치 프로그램을 다시 시작 (" 설치 프로그램 실행 " 페이지 158 참조) 하고 단계 1 에서 단계 6 까지의 단계를 반복합니다 .
- Windows NT 커넥터 설치 : "Windows NT 커넥터 설치 " 페이지 170 로 이동합니다 .
- 추가 Directory Server 커넥터 설치 : 설치 프로그램을 다시 시작 (" 설치 프로그램 실행 " 페이지 158 의 설명 참조) 하고 단계 1 에서 단계 7 까지의 단계를 반복합니다 .
- Directory Server 플러그인 설치 : "Directory Server 플러그인 설치 " 페이지 171 로 이동합니다 .

Windows NT 커넥터 설치

참고 반드시 Windows NT 커넥터를 구성한 도메인의 기본 도메인 제어기 (PDC) 에 설치해야 합니다.

"설치 프로그램 실행" 페이지 158 에 설명한 단계를 완료하면 Connector Configuration 패널이 표시됩니다.

Windows NT 커넥터와 NT 하위 구성요소를 설치하려면 다음과 같이 합니다.

1. Windows NT Connector 버튼을 사용 설정하고 Next 를 누릅니다.
2. Connector Port Configuration 창이 표시되면 도메인이 있는 정규화된 호스트 이름과 커넥터가 수신할 사용 가능한 포트 번호를 입력합니다. (이미 사용 중인 포트를 지정하면 오류 메시지가 발생합니다.)

Directory Server 플러그인은 콘솔에서 저장한 구성 정보를 사용할 수 있어야 합니다. 이 정보를 가져오려면 플러그인이 이 포트의 서버 소켓을 통하여 Windows NT 커넥터와 통신합니다. 또한 플러그인은 이 채널을 통한 메시지를 기록하여 해당 메시지가 중앙 로그로 기록될 수 있도록 합니다.

3. 작업을 완료했으면 Next 를 누릅니다.

Ready to Install 창이 열리며, 여기에는 커넥터의 설치 위치에 대한 정보와 필요한 디스크 공간이 표시됩니다.

4. 준비가 되었으면 Install Now 버튼을 누릅니다.

커넥터 설치는 두 단계로 완료됩니다.

- 프로그램에서 이진 설치가 진행되며 진행표시줄이 있는 Installing 창이 표시됩니다.
- 그런 다음 Component Configuration 창이 표시됩니다. 이 단계가 완료되려면 다소 시간이 걸리므로 진행표시줄이 표시됩니다.

참고 설치를 시작하기 전에 콘솔을 닫지 않은 경우 경고가 표시됩니다. 콘솔에서 Reset 을 눌러 커넥터의 구성 설정을 다시 로드합니다.

두 단계가 모두 완료되면 Installation Summary 창이 표시됩니다.

5. 설치 로그를 보려면 Details 버튼을 누릅니다.

설치 로그는 %TEMP% 디렉토리에 기록되며, 대부분의 Windows NT 시스템의 경우 C:\TEMP 입니다.

6. Close 를 눌러 설치 프로그램을 종료합니다.

Windows NT 커넥터를 설치한 후 자원을 구성할 때 구성한 기타 커넥터 및 Directory Server 플러그인을 설치할 수 있습니다 (4 장).

- 추가 Windows NT 커넥터를 설치하려면 다음과 같이 합니다. 설치 프로그램을 다시 시작 ("설치 프로그램 실행" 페이지 158 참조) 하고 단계 1 에서 단계 6 까지의 단계를 반복합니다.
- Directory Server 커넥터 설치 : "Directory Server 커넥터 설치" 페이지 160 로 이동합니다.
- Active Directory 커넥터 설치 : "Active Directory 커넥터 설치" 페이지 166 로 이동합니다.
- Directory Server 플러그인 설치 : "Directory Server 플러그인 설치" 페이지 171 로 이동합니다.

Directory Server 플러그인 설치

여기에서는 Identity Synchronization for Windows Directory Server 플러그인 설치 방법에 대하여 설명합니다.

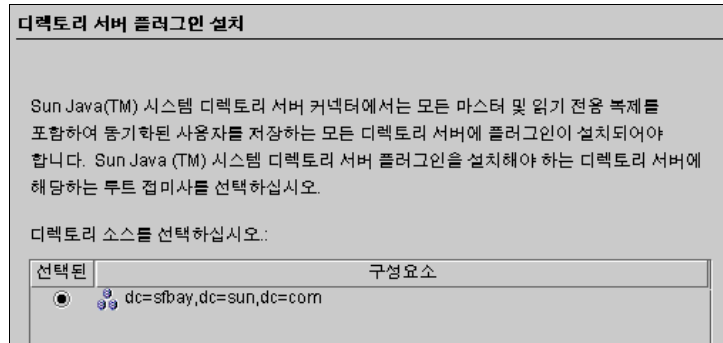
참고

반드시 Directory Server 를 설치한 동일한 컴퓨터에 Directory Server 플러그인을 설치해야 합니다.

코어 또는 임의의 커넥터와 동일한 시스템에 플러그인을 설치하는 경우 설치 프로그램은 코어 또는 커넥터가 시스템에 이미 설치되어 있는지 확인합니다. 추가 구성요소는 모두 설치 디렉토리에 설치됩니다.

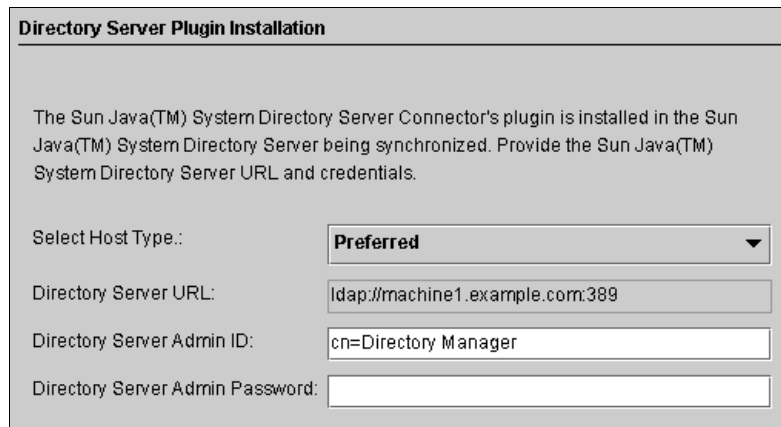
1. "설치 프로그램 실행" 페이지 158 에서 설명한 단계를 완료합니다.

그림 5-11) Directory Server 플러그인 선택



2. Connector Configuration 패널이 표시되면 Directory Server Plugin (dc=example,dc=com) 버튼을 선택하고 Next 를 누릅니다 .
3. 다른 Directory Server Plugin Installation 창이 표시됩니다 (그림 5-12).

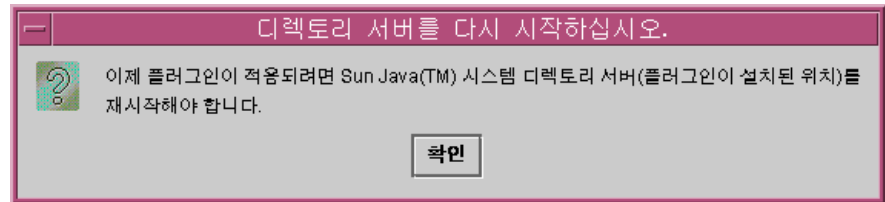
그림 5-12) Directory Server URL 및 자격 증명 지정



4. 드롭다운 목록에서 적절한 호스트 유형을 선택합니다 .
 - **Preferred:** 기본 서버에 플러그인을 설치하는 경우 이 옵션을 선택합니다 .
 - **Secondary:** 보조 서버에 플러그인을 설치하는 경우 이 옵션을 선택합니다 .
 - **Other:** 기본 또는 보조 서버가 아닌 다른 컴퓨터에 플러그인을 설치하는 경우 이 옵션을 선택합니다 .

5. 서버가 기본 또는 보조 호스트가 아닌 경우 해당 Directory Server 가 위치하는 URL 을 입력합니다.
6. Directory Server 관리자의 이름과 비밀번호를 입력한 후 Next 를 누릅니다.
Ready to Install 창이 열리며, 여기에는 플러그인의 설치 위치에 대한 정보와 설치에 필요한 디스크 공간이 표시됩니다.
7. 준비가 되었으면 Install Now 버튼을 누릅니다.
플러그인 설치하는 두 단계로 완료됩니다.
 - 프로그램에서 이진 설치가 진행되며 진행표시줄이 있는 Installing 창이 표시됩니다.
 - 다음, Component Configuration 창이 표시됩니다. 이 단계가 완료되려면 다소 시간이 걸리므로 진행표시줄이 표시됩니다.
8. 두 단계를 모두 완료했으면 다음 프롬프트가 표시됩니다. 정보를 읽은 후 OK 를 눌러 대화 상자를 닫습니다.

그림 5-13) Directory Server 다시 시작 프롬프트



9. 설치 로그를 보려면 Details 버튼을 누릅니다.
 - **Solaris:** 설치 로그는 /var/sadm/install/logs/ 에 기록됩니다.
 - **Windows:** 설치 로그는 %TEMP% 디렉토리에 기록되며, 이 디렉토리는 다음 폴더 아래에 있는 Local Settings 폴더의 하위 디렉토리입니다.
C:\Documents and Settings\Administrator

참고

일부 Windows 시스템 (Windows 2000 Advanced Server 등) 의 경우 Local Settings 폴더가 숨겨져 있습니다.

이 폴더와 Temp 하위 디렉토리를 보려면 Windows 탐색기를 열고 메뉴줄에서 도구 > 폴더 옵션을 선택합니다. 폴더 옵션 대화 상자가 표시되면 보기 탭을 누르고 숨긴 파일 표시 옵션을 선택합니다.

10. Close 를 눌러 설치 프로그램을 종료합니다 .

Directory Server 플러그인을 설치한 후 자원을 구성할 때 구성한 기타 커넥터 및 Directory Server 플러그인을 설치할 수 있습니다 (4 장).

- 추가 Directory Server 플러그인 설치 : 설치 프로그램을 다시 시작 (" [설치 프로그램 실행 " 페이지 158](#) 참조) 하고 [단계 2](#) 에서 [단계 9](#) 까지의 단계를 반복합니다 .

Identity Synchronization for Windows 에서 구현의 모든 Directory Server 에 플러그인을 설치해야 하므로 플러그인 설치 프로그램은 원하는 횟수만큼 제한 없이 실행할 수 있습니다 .

- Directory Server 커넥터 설치 : "[Directory Server 커넥터 설치](#)" [페이지 160](#)로 이동합니다 .
- Active Directory 커넥터 설치 : "[Active Directory 커넥터 설치](#)" [페이지 166](#)로 이동합니다 .
- Windows NT 커넥터 설치 : "[Windows NT 커넥터 설치](#) " [페이지 170](#) 로 이동합니다 .

11. Directory Server 를 다시 시작합니다 .

기존 사용자 동기화

Identity Synchronization for Windows 명령줄 유틸리티에는 기존 사용자를 부트스트랩하는 `idsync resync` 하위 명령이 제공됩니다. 이 명령은 관리자에 특정한 일치 규칙을 사용하여 기존 항목을 링크하고, 원격 디렉토리의 내용으로 빈 디렉토리를 채우며 두 개의 기존 사용자 사이에서 속성 값 (비밀번호 포함) 을 일괄적으로 동기화합니다.

이 장에서는 `idsync resync` 하위 명령을 사용하여 새 Identity Synchronization for Windows 설치에 대하여 기존 사용자를 링크하고 동기화하는 방법에 대하여 설명합니다. 또한 이 장에서는 동기화 및 서비스를 시작 / 정지하는 방법에 대하여 설명합니다. 다음과 같은 내용으로 구성됩니다.

- ["idsync resync 사용" 페이지 176](#)
- ["중앙 로그에서 결과 확인" 페이지 182](#)
- ["동기화 시작 및 정지" 페이지 182](#)
- ["서비스 시작 및 정지" 페이지 183](#)

참고

기존 사용자를 연결하고 동기화하기 전에 반드시 코어와 커넥터를 설치해야 합니다.

`idsync resync` 하위 명령에 대한 자세한 내용은 [부록 A, "Identity Synchronization for Windows 명령줄 유틸리티 사용."](#) 을 참조하십시오.

기존 사용자 입력 내용에 따른 설치 후 단계는 에서 간단히 설명합니다.

표 6-1) 기존 사용자 입력 내용에 따른 설치 후 단계

기존 사용자 위치		설치 후 단계	
Windows	Directory Server	기존 사용자 동기화	기존 사용자 동기화 안 함
아니오	아니오	없음	없음
아니오	예	idsync resync -o Sun -c 를 실행하여 Windows 에 기존 Directory Server 사용자를 만듭니다 .	없음
예	아니오	idsync resync -c 를 실행하여 Directory Server 에 기존 Windows 사용자를 만듭니다 .	idsync resync -u 를 실행하여 커넥터의 사용자 항목 로컬 캐시 입력 .
예	예	다음 방법 중 한 가지를 선택합니다 . <ul style="list-style-type: none">idsync resync -f <filename> 를 실행하여 Active Directory 와 Directory Server 에서 사용자를 링크하고 동기화합니다 .idsync resync -f <filename> -k 를 실행하여 사용자만 링크합니다 .idsync resync -f <filename> -k 를 실행하여 사용자만 링크한 후 idsync resync -o Sun 을 실행하여 Directory Server 에서 기존 사용자를 재동기화합니다 .	idsync resync -u 를 실행하여 커넥터의 사용자 항목 로컬 캐시 입력 .

idsync resync 사용

여기에서는 링크 및 동기화 과정을 설명하며 idsync resync 하위 명령을 사용하기 위한 적절한 구문을 설명하고 해당 프로세스가 성공적으로 완료되었는지 확인하는 방법에 대하여 설명합니다 . 다음과 같은 내용으로 구성됩니다 .

- " 사용자 연결 " 페이지 178
- " 사용자 재동기화 " 페이지 177
- "idsync resync 인수 " 페이지 179
- " 중앙 로그에서 결과 확인 " 페이지 182

사용자 재동기화

참고 구현에서 동기화를 시작하기 전에 서버 사이에서 기존 사용자가 동기화되었는지 확인해야 합니다.

idsync resync 명령을 사용하여 기존 항목을 링크하고, 사용자를 만들고, 두 디렉토리 소스에서 사용자 속성을 동기화할 수 있습니다. 특히 idsync resync 명령을 사용하여 다음 작업을 할 수 있습니다.

- 기존 Active Directory 또는 Windows NT SAM 도메인 사용자로 빈 Directory Server 입력
- 기존의 두 디렉토리 소스에서 모든 사용자를 링크하고 모든 사용자 항목 속성 값 (비밀번호 제외) 을 동기화

참고 Directory Server 및 Windows 에 사용자가 있는 경우 반드시 idsync resync -f <filename> 을 사용하여 해당 사용자를 링크하고 동기화해야 합니다.

기존 사용자를 Directory Server 로 동기화하지 않으려면 -u 인수를 사용하여 idsync resync 를 실행합니다. 이 경우 객체 캐시만 업데이트되며 Windows 의 항목을 Directory Server 로 동기화하지 않습니다.

기존 Windows 사용자가 있으며 idsync resync 를 실행하지 않는 경우 해당 사용자에 대한 변경 내용이 전달되지 않을 수 있으며, 흐름 설정에 따라 해당 항목이 Directory Server 에 자동으로 만들어지지 않을 수 있습니다. idsync resync 를 이미 실행한 경우에도 이 명령을 다시 실행해야 합니다.

- 두 디렉토리 소스가 동기화되지 않는 경우 사용자 항목 동기화
- Active Directory 및 Windows NT SAM 커넥터 객체 캐시 데이터베이스를 "준비" 하며, 이에 따라 Active Directory 또는 Windows NT SAM 사용자 항목의 세도우 사본을 유지합니다.

비밀번호의 동기화에는 idsync resync 명령을 사용할 수 없습니다 (Directory Server 비밀번호를 무효화하여 Active Directory 환경에서 요청시 비밀번호 동기화가 실행되도록 하는 경우 제외).

사용자 연결

Active Directory 및 Directory Server 에 사용자를 입력하고 Active Directory 및 Directory Server 를 설치한 후 (동기화를 시작하기 전), 반드시 idsync resync 명령을 사용하여 두 디렉토리 소스에서 모든 사용자가 링크되었는지 확인해야 합니다 .

링크 설명 Identity Synchronization for Windows 는 다음의 고유하며 변경 불가능한 식별자를 저장하여 Directory Server 와 Windows 에 있는 동일한 사용자를 상호 관련시킵니다 .

- 각 Directory Server 사용자 항목의 dspswuserlink 속성
- 각 Active Directory 사용자의 objectguid 속성
- 각 Windows NT SAM 사용자의 도메인 이름 및 RID 조합

변경 불가능한 식별자를 저장하면 Identity Synchronization for Windows가 uid 및 cn 등의 다른 주요 식별자를 동기화할 수 있습니다. dspswuserlink 속성은 다음의 경우 입력됩니다 .

- Identity Synchronization for Windows 가 Directory Server 에 새 사용자를 생성할 경우 (Windows 에서 새 사용자가 동기화된 후 또는 idsync resync -c 를 실행하여 새 사용자가 동기화된 후)
- Identity Synchronization for Windows 가 Windows 에 새 사용자를 만드는 때 (idsync resync -c -o Sun 을 실행하여 Directory Server 에서 새 사용자를 동기화한 후)
- 이 장에서 설명한 것과 같이 idsync resync -c -f 를 실행하여 이미 Directory Server 와 Windows 에 있는 항목을 링크합니다 .

기존 사용자를 링크하려면 반드시 두 디렉토리 사이에서 사용자를 일치시키는 규칙을 제공해야 합니다 . 예를 들어 두 디렉토리에서 사용자 항목을 링크하려면 두 디렉토리 항목에서 이름과 성이 반드시 일치해야 합니다 .

사용자 항목을 연결하고 데이터 충돌을 해결하는 것은 과학이라기보다 기법에 가깝습니다 . 상반되는 디렉토리 소스에서 두 사용자를 연결할 때 idsync resync 하위 명령이 실패하고 연결된 디렉토리의 데이터 일관성에 따라 크게 달라지는 이유는 여러 가지입니다 .

idsync resync 를 사용하는 한 가지 전략은 -n 인수를 사용하는 것으로, 이 경우 "안전 모드" 로 실행되므로 실제 변경 내용 없이 효과를 미리 확인할 수 있습니다. 안전 모드에서 실행하면 사용자 일치 기준이 최적화될 때까지 점진적으로 링크 기준을 조정할 수 있습니다.

그러나 연결 정확도와 연결 범위 사이에는 적당한 균형이 이루어져야 합니다.

예를 들어 두 디렉토리 소스에 직원 ID 또는 주민번호가 있는 경우 이 번호만 포함하는 연결 기준으로 시작할 수 있습니다. 또한 연결 정확도를 향상시키기 위하여 기준에 성을 포함시킬 수 있습니다. 그러나 데이터의 성 값이 일관적이지 않으므로 ID 만으로는 일치되지 않기 때문에 연결이 끊어질 수 있습니다. 링크에 실패하는 항목에 대하여 데이터 청소 프로세스를 실행해야 할 수 있습니다.

idsync resync 인수

idsync resync 명령에는 다음 인수를 사용할 수 있습니다.

표 6-2) idsync resync 사용법

인수	의미
-f <filename>	Identity Synchronization for Windows 가 제공한 지정된 XML 구성 파일 중 하나를 사용하여 링크되지 않은 사용자 항목 사이의 링크를 만듭니다. (부록 B, "LinkUsers XML 문서 예제" 참조)
-k	링크되지 않은 사용자 사이에만 링크를 만듭니다 (사용자를 만들거나 기존 사용자를 수정하지 않음). 반드시 이 인수를 -f 인수와 조합하여 사용해야 합니다.
-a <ldap-filter>	동기화할 항목을 제한하는 LDAP 필터를 지정합니다. 필터는 재동기화 작업의 소스에 적용됩니다. 예를 들어 idsync resync -o Sun -a "usid=*" 지정하면 uid 가 있는 모든 Directory Server 사용자가 Active Directory 로 동기화됩니다.
-l <sul-to-sync>	동기화할 개별 동기화 사용자 목록 (SUL) 을 지정합니다. 참고: 복수 SUL ID 를 지정하여 복수 SUL 을 재동기화하거나, SUL ID 를 지정하지 않는 경우 프로그램은 모든 SUL 을 재동기화합니다.
-o (Sun Windows)	재동기화 작업의 소스를 지정합니다. <ul style="list-style-type: none"> Sun: Windows 항목용 속성 값을 Sun Java 시스템 Directory Server 디렉토리 소스 항목에 있는 해당 속성 값으로 설정합니다. Windows: Sun Java 시스템 Directory Server 항목의 속성 값을 Windows 디렉토리 소스 항목에 있는 해당 속성 값으로 설정합니다. (기본값은 Windows 입니다.)

표 6-2) idsync resync 사용법 (계속)

인수	의미
-c	<p>대상에서 해당 사용자를 찾을 수 없는 경우 사용자 항목을 자동으로 만듭니다 .</p> <ul style="list-style-type: none"> Active Directory 또는 Windows NT 에서 만든 사용자에 대하여 무작위로 암호학적으로 안전한 비밀번호를 생성합니다 . Directory Server 에서 만든 사용자에 대하여 특수 비밀번호 값 ((PSWSYNC)*INVALID PASSWORD*) 을 자동으로 만듭니다 (-i 옵션을 지정하지 않은 경우) . <p>참고 : Identity Synchronization for Windows 는 해당 방향으로 생성을 구성하지 않은 경우에도 사용자를 만들려고 시도합니다 . 예를 들어 Identity Synchronization for Windows 가 Windows 에서 Sun 으로 (또는 그 반대로) 동기화하도록 구성하지 않았지만 -c 인수를 지정하는 경우 Identity Synchronization for Windows 는 검색되지 않은 사용자를 만들려고 시도합니다 .</p>
-i (ALL_USERS NEW_USERS NEW_LINKED_USERS)	<p>Sun 디렉토리 소스에서 동기화된 사용자 항목의 비밀번호를 재설정하고 이후 사용자 비밀번호가 필요할 때 해당 사용자에 대하여 현재 도메인 내의 비밀번호 동기화를 수행하도록 합니다 .</p> <ul style="list-style-type: none"> ALL_USERS: 모든 동기화된 사용자에 대하여 요청시 비밀번호 동기화를 수행하도록 합니다 . NEW_USERS: 새로 생성된 사용자에 대하여 요청시 비밀번호 동기화를 수행하도록 합니다 . NEW_LINKED_USERS: 모든 새로 생성 또는 링크된 사용자에 대하여 요청시 비밀번호 동기화를 수행하도록 합니다 . <p>이들 옵션이 비밀번호 검증에 영향을 미치는 방식에 대한 자세한 내용은 을 참조하십시오 .</p>
-u	<p>객체 캐시를 업데이트합니다 .</p> <p>이 인수는 Windows 디렉토리 소스용 사용자 항목의 로컬 캐시만 업데이트하며 , 따라서 이미 존재하는 Windows 사용자가 Directory Server 에서 생성되지 않도록 방지합니다 . 이 인수를 사용하는 경우 Windows 사용자 항목이 Directory Server 사용자 항목과 동기화되지 않습니다 . 이 인수는 resync 소스가 Windows 인 경우에만 유효합니다 .</p>
-x	<p>소스 항목과 일치하지 않는 모든 대상 사용자 항목을 삭제합니다 .</p>
-n	<p>실제 변경 없이 작업의 효과를 미리 볼 수 있도록 안전 모드에서 실행합니다 .</p>

표 6-3) idsync resync 가 Directory Server 에 있는 사용자의 비밀번호를 무효화합니까 ?

	사용자에게 Active Directory 와 링크된 Directory Server 에 항목이 있습니다 .	사용자에게 Active Directory 와 링크되지 않은 Directory Server 에 항목이 있습니다 .	사용자에게 Active Directory 에 항목이 있거나 Directory Server 에는 없습니다 .
-i ALL_USERS	예	예	예
-i NEW_LINKED_USERS	아니오	예	예
-i NEW_USERS	아니오	아니오	예
No -i value	아니오	아니오	아니오

는 서로 다른 인수를 조합하는 결과의 예입니다 . (-h, -p, -D, -w, - 및 -s 인수는 기본 값으로 간략히 하기 위하여 생략되었습니다 .)

표 6-4) idsync resync 사용법 예제

인수	결과
idsync resync	resync 사용법이 표시됩니다 .
idsync resync -i ALL_USERS	모든 사용자의 비밀번호를 무효화하여 요청시 비밀번호 동기화가 실행 되도록 합니다 (Active Directory 환경에서만 유효). 혼합된 환경 (Active Directory 및 NT 도메인 모두) 의 경우 반드시 Active Directory SUL 목록을 명시해야 합니다 .
idsync resync -c -i NEW_USERS	Directory Server 에서 검색되지 않은 사용자를 만들고 해당 비밀번호를 무효화하여 요청시 비밀번호 동기화가 실행되도록 합니다 . 이 명령을 사용하여 빈 Directory Server 인스턴스에 기존 Windows 사용자를 채웁니다 .
idsync resync -c -l SUL_sales -l SUL_finance	SUL_sales 및 SUL_finance SUL 의 기존 Active Directory 사용자만 Directory Server 에 만듭니다 . (그러나 요청시 동기화는 수행하지 않습니다 .)
idsync resync -n	실제 변경 없이 작업의 효과를 미리 볼 수 있도록 resync 작업을 안전 모드에서 실행합니다 .
idsync resync -o Sun -a "(sn=Smith)"	Windows 에서 성 (sn) 이 Smith 인 모든 Directory Server 사용자를 동기화합니다 .
idsync resync -u	Windows 커넥터용 객체 캐시만 업데이트하여 기존 사용자가 Directory Server 에서 만들어지지 않도록 합니다 . 실제로 동기화되는 사용자는 없습니다 .

표 6-4) idsync resync 사용법 예제 (계속)

인수	결과
idsync resync	resync 사용법이 표시됩니다 .
idsync resync -f link.cfg -k -i NEW_LINKED_USERS	link.cfg 파일에 지정된 링크 기준에 따라 링크가 해제된 사용자를 링 크합니다 . Identity Synchronization for Windows 는 사용자를 만들거 나 수정하지 않지만 새로 링크된 사용자의 Directory Server 비밀번호 는 Active Directory 사용자의 비밀번호로 설정됩니다 .

주의	idsync resync를 사용하여 사용자를 링크하는 경우 작업에 색인화된 속성을 사용해야 합니다 . 색인화되지 않은 속성은 성능에 영향을 미칠 수 있습니다 . UserMatchingCriteria 세트에 여러 개의 속성이 있으며 이 중 하나 이 상이 색인화 된 경우 성능이 만족스러울 것입니다 . 그러나 UserMatchingCriteria 에 색인화된 속성이 없는 경우 디렉토리가 크 면 성능이 만족스럽지 않을 것입니다 .
----	--

중앙 로그에서 결과 확인

모든 idsync resync 작업의 결과는 이름이 resync.log 인 특수 중앙 로그에 보고됩니다 . 이 로그에는 적절히 링크 및 동기화된 사용자 , 링크에 실패한 사용자 및 이전에 링크된 사용자의 목록이 표시됩니다 .

참고	이 로그에서 Administrator 및 Guest 등의 이미 존재하는 특수 Active Directory 사용자는 실패로 기록됩니다 .
----	--

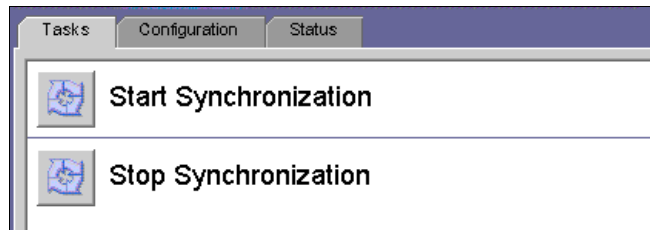
동기화 시작 및 정지

동기화를 시작 및 정지해도 개변 java 프로세스 , 데몬 및 서비스가 시작 또는 정지되지는 않습니다 . 동기화를 시작한 후 동기화를 정지하면 해당 작업만 일시 정지됩니다 . 동기화를 다시 시작하면 동기화가 정지된 곳에서 계속되므로 변경 내용을 잃지는 않습니다 .

동기화를 시작 또는 정지하려면 다음과 같이 합니다 .

1. Sun Java 시스템 서버 콘솔 탐색창에서 Identity Synchronization for Windows 인스턴스를 선택합니다.
2. Identity Synchronization for Windows 창이 표시되면 오른쪽 상단의 Open 버튼을 누릅니다.
3. 프롬프트가 표시되면 구성 비밀번호를 입력합니다.
4. Tasks 탭 (그림 6-1) 을 선택합니다.

그림 6-1) 동기화 시작 및 정지



- 동기화를 시작하려면 Start Synchronization 을 누릅니다.
- 동기화를 정지하려면 Stop Synchronization 을 누릅니다.

참고

또한 `idsync startsync` 및 `idsync stopsync` 명령줄 유틸리티를 사용하여 동기화를 시작 및 정지할 수 있습니다. 자세한 내용은 ["startsync 사용" 페이지 318](#) 및 ["stopsync 사용" 페이지 319](#) 를 참조하십시오.

서비스 시작 및 정지

Identity Synchronization for Windows 및 Message Queue 는 Solaris 의 경우 *데몬*으로 설치되며 Windows 의 경우 *서비스*로 설치됩니다. 이들 프로세스는 시스템이 부트 될 때 자동으로 시작되나, 또한 다음과 같이 직접 시작 및 정지할 수 있습니다.

- **Solaris:** 명령줄에서,
 - `/etc/init.d/isw start` 를 입력하여 모든 Identity Synchronization for Windows 프로세스를 시작합니다.
 - `/etc/init.d/isw stop` 을 입력하여 모든 Identity Synchronization for Windows 프로세스를 정지합니다.

- `/etc/init.d/imq start` 를 입력하여 Message Queue 브로커를 시작합니다.
- `/etc/init.d/imq stop` 을 입력하여 Message Queue 브로커를 정지합니다.
- **Windows:**
 - Windows 시작 메뉴에서 다음과 같이 합니다.
 - I. 시작 > 설정 > 제어판 > 관리 서비스를 선택합니다.
 - II. 관리 서비스 대화 상자가 표시되면 서비스 아이콘을 두 번 눌러 서비스 대화 상자를 엽니다.
 - III. Identity Synchronization for Windows 를 선택한 후 메뉴 표시줄에서 Action > Start(또는 Stop) 를 선택합니다. iMQ Broker 의 경우도 같은 방법을 반복합니다.
 - 명령줄에서 `net` 명령을 입력하여 서비스를 제어합니다.

참고	Identity Synchronization for Windows 데몬 / 서비스를 정지하고 다시 시작하기 전에 30 초의 여유를 두십시오. 커넥터가 완전히 종료되려면 몇 초의 시간이 걸릴 수 있습니다.
-----------	---

Identity Synchronization for Windows 1 2004Q3 으로 마이그레이 션

이 장에서는 시스템을 Sun Java System Identity Synchronization for Windows 버전 1.0 에서 버전 1 2004Q3 으로 이전하는 방법에 대하여 설명합니다 .

참고

Identity Synchronization for Windows 버전 1.0 에서는 자동으로 Message Queue 가 설치되지만 *Identity Synchronization for Windows 1 2004Q3* 에서는 설치되지 않습니다.

설치 방법은 Sun Java System Message Queue 제품 설명서를 참조하십시오 .

정보는 다음과 같이 구성되었습니다 .

- " 개요 " 페이지 186
- " 이전하기 전에 " 페이지 186
- " 마이그레이션 준비 " 페이지 187
- " 시스템 이전 " 페이지 197
- " 1.0 제거에 실패한 경우의 작업 방법 " 페이지 206
- " 기타 이전 시나리오 " 페이지 222
- " 로그 확인 " 페이지 229

개요

Identity Synchronization for Windows 버전 1.0(또는 버전 1.0 SP1) 에서 1 2004Q3 으로의 마이그레이션은 여러 가지 주요 단계를 거쳐 완료됩니다 .

1. Identity Synchronization for Windows 버전 1.0(또는 1.0 SP1) 설치를 마이그레이션용으로 준비 .
2. Identity Synchronization for Windows 버전 1.0(또는 1.0 SP1) 제거 .
3. 종속된 제품 설치 및 업그레이드 .
4. 백업한 구성 및 커넥터 상태를 사용하여 Identity Synchronization for Windows 1 2004Q3 설치 .

참고	Identity Synchronization for Windows 1 2004Q3 을 Identity Synchronization for Windows 버전 1.0(또는 1.0 SP1) 을 설치한 동일한 플랫폼 및 아키텍처에 설치합니다 .
-----------	--

이전하기 전에

이전 과정을 시작하기 전에 다음 내용에 유의하십시오 .

- Sun Java System Identity Synchronization for Windows 버전 1 2004Q3 에 제공된 새 기능과 기능성을 숙지해야 합니다 .
- [제 2 장 , " 설치 준비 "](#) 에서 이전 과정을 계획하는 데 사용할 수 있는 설치 및 구성 정보를 읽습니다 .
- 버전 1.0 구현 및 구성을 기록합니다 .
구성에서 사용자 정의한 내용을 반드시 기록해야 합니다 .
- 마이그레이션 일정을 계획합니다 .
마이그레이션 프로세스에는 최소한 네 시간이 필요하므로 정상 근무시간 이후로 마이그레이션을 계획하는 것이 좋습니다 .

시스템을 버전 1.0 에서 1 2004Q3 으로 이전하는 동안 사용자가 비밀번호를 입력하거나 속성을 변경하는 경우 Identity Synchronization for Windows 는 이러한 변경 내용을 다음과 같이 처리합니다 .

- **Active Directory:** 마이그레이션 과정 동안 Active Directory 에서 변경된 비밀번호는 마이그레이션 과정이 완료된 후 Directory Server 플러그인에 의하여 요청시 동기화됩니다 .

- **Directory Server:** 이전하는 과정에서 Directory Server 에서 변경된 모든 비밀번호는 동기화되지 않습니다 . 그러나 이전이 완료된 후 Identity Synchronization for Windows 1 2004Q3 로그에서 영향을 받는 사용자를 확인할 수 있습니다 (" 로그 확인 " 페이지 229 참조).
- **Windows NT:** 이전 과정 동안 NT 에서 변경된 비밀번호는 동기화되지 않습니다 .

그러나 forcepwchg 유틸리티를 사용하면 영향을 받는 사용자를 확인하고 이들이 비밀번호를 다시 변경하도록 할 수 있습니다 . (자세한 내용은 "Windows NT 에서 비밀번호 강제 변경 " 페이지 196 및 " 로그 확인 " 페이지 229 을 참조하십시오 .)
- 마이그레이션 동안 변경된 모든 기타 속성 (임의의 디렉토리 소스)은 마이그레이션 과정을 완료한 후 동기화됩니다 .

마이그레이션 준비

다음 유틸리티를 사용하여 버전 1.0 에서 버전 1 2004Q3 으로 이전합니다 .

- **export10cnf:** 독립형 유틸리티로 Identity Synchronization for Windows 1.0 구성에서 구성 파일을 내보낼 수 있습니다 . (자세한 내용은 " 버전 1.0 구성 내보내기 " 페이지 188 를 참조하십시오 .)

내보내기 한 XML 문서에는 디렉토리 구현의 토폴로지와 Identity Synchronization for Windows 버전 1 2004Q3 설치를 구성하는 데 충분한 정보가 있습니다 .
- **checktopics:** 1.0 설치에서 Message Queue 동기화 문제를 확인하고 대기열에 전달되지 않은 메시지가 있는지 판단하는 유틸리티입니다 .

1.0 동기화를 중지한 이후에도 Message Queue 에 업데이트가 남아 있을 수 있습니다 . 마이그레이션을 계속하기 전에 반드시 Message Queue 에 업데이트가 없는지 확인해야 합니다 . (자세한 내용은 " 전달되지 않은 메시지 확인 " 페이지 194 를 참조하십시오 .)
- **forcepwchg:** Windows NT 도구로의 마이그레이션 과정 동안 비밀번호를 변경한 사용자를 확인하고 버전 1 2004Q3 이 준비된 후 이들이 비밀번호를 다시 변경하도록 합니다 . (Windows NT 에서 변경된 비밀번호는 이전 과정 동안 포착되지 않습니다 .) (자세한 내용은 "Windows NT 에서 비밀번호 강제 변경 " 페이지 196 를 참조하십시오 .)

참고 이 유틸리티는 Identity Synchronization for Windows 버전 1.0 에서 1 2004Q3 으로의 이전을 간편하게 합니다 . 이전은 Identity Synchronization for Windows 1.0 이 구현된 동일한 환경에서 수행됩니다 . 따라서 이들 유틸리티는 Solaris/SPARC 및 Windows 패키지에 서만 사용할 수 있습니다 .

이전 유틸리티는 installation migration 디렉토리에 있으며 추가의 설치 단계는 필요하지 않습니다 .

버전 1.0 구성 내보내기

export10cnf 유틸리티를 사용하여 기존의 버전 1.0 구성 파일을 XML 파일로 내보내고 커넥터를 설치하기 전에 idsync importcnf 명령을 사용하여 빠르고 정확하게 파일을 1 2004Q3 시스템으로 가져올 수 있습니다 .

팁 Identity Synchronization for Windows 콘솔을 사용하여 직접 1.0 구성을 다시 입력할 수는 있으나, export10cnf 유틸리티를 사용하는 것이 가장 좋습니다 . export10cnf 를 사용하지 않으려는 경우 커넥터의 상태를 보존할 수 없게 됩니다 .

버전 1.0 의 구성을 내보내기 하면 다음과 같은 장점이 있습니다 .

- 관리 콘솔에서 수행해야 하는 대부분의 초기 구성 과정을 생략할 수 있습니다 .
- 버전 1 2004Q3 에서 지정한 커넥터 ID 가 버전 1.0 에서 사용한 커넥터 ID 와 일치할 것이므로 버전 1 2004Q3 구현에서 바로 사용할 수 있는 기존 커넥터 상태를 보존하는 작업을 간단히 할 수 있습니다 .

(보통 persist 및 etc 디렉토리를 백업하고 이하의 디렉토리 구조에 대한 걱정 없이 나중에 이를 복구할 수 있습니다 .)

export10cnf 유틸리티는 설치 마이그레이션 디렉토리에 있으며 추가의 설치 단계는 필요하지 않습니다 .

export10cnf 유틸리티 사용

Identity Synchronization for Windows 구성을 XML 파일로 내보내려면 다음과 같이 migration 디렉토리에서 export10cnf 를 실행합니다 .

- 터미널 창을 열고 다음을 입력합니다.

```
java -jar export10cnf.jar -h <hostname> -p <port> -D <bind DN>
-w <bind password> -s <rootsuffix> -q <configuration password> -Z
-P <cert-db-path> -m <secmod-db-path> -f <filename>
```

예 :

```
java -jar export10cnf.jar -D "cn=dirmanager" -w - -q - -s "dc=example,dc=com" -f
exported-configuration
```

export10cnf 유틸리티는 Identity Synchronization for Windows 명령줄 유틸리티와 동일한 공통 인수를 공유합니다 ("공통 인수" 페이지 302 참조). export10cnf 에 국한된 유일한 옵션은 -f <filename> 입니다. 작업이 성공하는 경우 유틸리티는 현재 구성을 -f 옵션의 인수에서 지정한 파일로 내보냅니다.

일반 텍스트 비밀번호 삽입

export10cnf 유틸리티는 버전 1.0 구성에 있는 일반 텍스트 비밀번호를(보안상의 이유로) 내보내지 않습니다. 대신 적절한 경우 빈 문자열을 cleartextPassword 필드에 삽입합니다. 예 :

<자격 증명

```
userName="cn=iswservice,cn=users,dc=example,dc=com"
```

```
cleartextPassword="" />
```

```
<!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD
```

```
-->
```

파일을 Identity Synchronization for Windows 1 2004Q3 로 가져오기 전에 내보내진 구성 파일의 cleartextPassword 필드 마다 인용 부호 사이에 직접 비밀번호를 입력해야 합니다. (importcnf 유효성 검사에 의하여 빈 비밀번호 값이 있는 구성 파일은 가져올 수 없습니다.)

예 :

<자격 증명

```
userName="cn=iswservice,cn=users,dc=example,dc=com"
```

```
cleartextPassword="mySecretPassword" />
```

```
<!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE
```

```
FIELD -->
```

예제 내보내기 구성 파일

페이지 190 에는 내보내기 한 구성 파일의 예제가 있습니다 .

이 파일에서 ,

- ad-host.example.com 은 Active Directory 도메인 제어를 나타냅니다 .
- ds-host.example.com 은 Sun Java System Directory Server 에서 실행되는 호스트를 나타냅니다 .

코드 예제 7-1) 예제 내보내기 구성 파일

```
<?xml version="1.0" encoding="UTF-8"?>

<ActiveConfiguration>
  <SunDirectorySource
    parent.attr="DirectorySource"
    onDemandSSLOption="true"
    maxConnections="5"
    displayName="dc=example,dc=com"
    resyncInterval="1000">
    <SynchronizationHost
      hostOrderOfSignificance="1"
      hostname="ds-host.example.com"
      port="389"
      portSSLOption="true"
      securePort="636">
      </>
      userName="uid=PSWConnector,dc=example,dc=com" />
    </SynchronizationHost>
  <SyncScopeDefinitionSet
    index="0"
    location="ou=people,dc=example,dc=com"
    filter=""
    creationExpression="cn=%cn%,ou=people,dc=example,dc=com"
    sulid="SUL" />
  </SunDirectorySource>
  <ActiveDirectorySource
    parent.attr="DirectorySource"
    displayName="example.com"
    resyncInterval="1000">
```



```
<SyncScopeDefinitionSet
  index="0"
  location="cn=users,dc=example,dc=com"
  filter=""
  creationExpression="cn=%cn%,cn=users,dc=example,dc=com"
  sulid="SUL"/>
</ActiveDirectorySource>
<ActiveDirectoryGlobals
  flowInboundCreates="true"
  flowInboundModifies="true"
  flowOutboundCreates="true"
  flowOutboundModifies="true">
  <AttributeDescription
    parent.attr="CreationAttribute"
    name="samaccountname"
    syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
  <AttributeMap>
    <AttributeDescription
      parent.attr="WindowsAttribute"
      name="samaccountname"
      syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
    <AttributeDescription
      parent.attr="SunAttribute"
      name="uid"
      syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
  </AttributeMap>
  <AttributeDescription
    parent.attr="SignificantAttribute"
    name="description"
    syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
  <AttributeMap>
    <AttributeDescription
      parent.attr="SunAttribute"
      name="sn"
      syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
  <AttributeDescription
    parent.attr="WindowsAttribute"
    name="sn"
    syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
  </AttributeMap>
```

```

<SynchronizationHost
  hostOrderOfSignificance="1"
  hostname="ad-host.example.com"
  port="389"
  portSSLOption="true"
  securePort="636">
  </x>
  <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
  </SynchronizationHost>
<AttributeDescription
  parent.attr="CreationAttribute"
  name="cn"
  syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
<TopologyHost
  parent.attr="SchemaLocation"
  hostname="ad-host.example.com"
  port="3268"
  portSSLOption="true"
  securePort="3269">
  <자격 증명
    parent.attr="Credentials"
    userName="cn=iswservice,cn=users,dc=example,dc=com"
    cleartextPassword=""/>
    <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
  </TopologyHost>
  <TopologyHost
    parent.attr="HostsTopologyConfiguration"
    hostname="ad-host.example.com"
    port="3268"
    portSSLOption="true"
    securePort="3269">
    <자격 증명
      parent.attr="Credentials"
      userName="cn=iswservice,cn=users,dc=example,dc=com"
      cleartextPassword=""/>
      <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
    </TopologyHost>
  <AttributeMap>
    <AttributeDescription
      parent.attr="SunAttribute"
      name="cn"
      syntax="1.3.6.1.4.1.1466.115.121.1.15"/>

```

```

<AttributeDescription
  parent.attr="WindowsAttribute"
  name="cn"
  syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
</AttributeMap>
<AttributeMap>
  <AttributeDescription
    parent.attr="SunAttribute"
    name="description"
    syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
<AttributeDescription
  parent.attr="WindowsAttribute"
name="description"
  syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
</AttributeMap>
</ActiveDirectoryGlobals>
<SunDirectoryGlobals
  userObjectClass="inetorgperson"
  flowInboundCreates="true"
  flowInboundModifies="true"
  flowOutboundCreates="true"
  flowOutboundModifies="true">
<TopologyHost
  parent.attr="SchemaLocation"
  hostname="ds-host.example.com"
  port="389"
  portSSLOption="false"
  securePort="636">
  < 자격 증명
    parent.attr="Credentials"
    userName="cn=directory manager"
    cleartextPassword=""/>
    <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
  </TopologyHost>
<TopologyHost
  parent.attr="HostsTopologyConfiguration"
  hostname="ds-host.example.com"
  port="389"
  portSSLOption="false"
  securePort="636"><Credentials
    parent.attr="Credentials"
    userName="cn=directory manager"
    cleartextPassword=""/>
    <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
  </TopologyHost>

```

```
<AttributeDescription
  parent.attr="SignificantAttribute"
  name="description"
  syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
<AttributeDescription
  parent.attr="CreationAttribute"
  name="sn"
  syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
<AttributeDescription
  parent.attr="CreationAttribute"
  name="cn"
  syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
</SunDirectoryGlobals>
</ActiveConfiguration>
```

구성을 내보내면 export10cnf 에 작업 결과가 보고됩니다. 작업이 실패하는 경우 적절한 오류 메시지가 해당 오류 ID 와 함께 표시됩니다.

전달되지 않은 메시지 확인

Identity Synchronization for Windows 1.0 에서 1 2004Q3 으로 마이그레이션 하는 동안 기존 구현의 커넥터 상태를 보존함으로써 시스템 중단 시간을 최소화합니다. 그러나 이러한 상태는 Message Queue 가 마지막으로 수신하고 인식한 변경 내용만을 반영하므로 메시지가 실제로 대상 커넥터에 전달되고 적용되었는지 알 수 없습니다.

이 경우 Message Queue 의 상태가 변하지 않으면 문제를 일으키지 않지만 이전 과정 동안 (Message Queue 3.5 SP1 을 설치할 때) Message Queue 에 있는 모든 메시지를 잃게 됩니다.

이전을 진행하기 전에 반드시 기존 Message Queue 의 동기화 항목에서 전달되지 않은 메시지가 있는지 확인해야 합니다. Identity Synchronization for Windows checktopics 유틸리티를 사용하여 모든 동기화 항목이 비었는지 (또한 시스템이 정지 상태인지) 검사할 수 있습니다.

checktopics 유틸리티 사용

checktopics 유틸리티는 Solaris/SPARC 및 Windows Identity Synchronization for Windows 1 2004Q3 패키지의 migration 디렉토리에 제공됩니다.

참고 checktopics를 실행할 때 유일하게 필요한 것은 Java Virtual Machine (1.4.2_04 버전 이상) 입니다.

checktopics 유틸리티를 실행하면 이 유틸리티는 구성 디렉토리로 연결하며, 이 디렉토리에 Message Queue 에서 사용하는 동기화 사용자 목록 (SUL) 과 현재 동기화 항목 이름이 있습니다. 또한 checktopics 를 실행하는 경우 이 유틸리티는 Message Queue 를 쿼리하여 각 사용 중인 동기화 항목에 남아 있는 보류중 메시지의 수를 확인한 후 이 정보를 표시합니다.

checktopics 명령줄 유틸리티를 실행하려면 다음과 같이 합니다.

- a. 터미널 창을 열고 **cd** 명령으로 migration 디렉토리로 이동합니다.
- b. 명령 프롬프트에서 다음과 같이 하위 명령을 입력합니다.

```
java -jar checktopics.jar -h <hostname> -p <port> -D <bind_DN> -w <bind_password> -s <root_suffix> -q <configuration_password> -z
```

예 :

```
java -jar checktopics.jar -D "cn=directory manager" -w - -s "dc=example,dc=com" -q -
```

-
- 참고**
- checktopics 인수에 대한 자세한 내용은 "[공통 인수](#)" [페이지 302](#) 를 참조하십시오.
 - checktopics 사용에 대한 더 자세한 내용은 "[전달되지 않은 메시지 확인](#)" [페이지 194](#) 를 참조하십시오.
-

checktopics 를 실행한 후 터미널에서 메시지를 확인합니다.

- 작업이 성공한 경우 로그에 보류중인 메시지가 없다는 내용의 메시지가 터미널에 표시됩니다.
- 작업이 실패하는 경우 적절한 오류 메시지가 해당 오류 ID 와 함께 표시됩니다.

메시지 비우기

사용중인 동기화 항목에 보류중인 메시지가 있는 경우 다음과 같이 메시지를 비울 수 있습니다.

1. 동기화를 재시작합니다.
2. 메시지가 대상 커넥터에 적용될 때까지 기다립니다.
3. 동기화를 정지합니다.
4. `checktopics` 를 다시 실행합니다.

Windows NT 에서 비밀번호 강제 변경

Windows NT 에서 마이그레이션 과정 동안 비밀번호 변경은 모니터링되지 않으며 새 비밀번호 값은 캡처되지 않습니다. 따라서 이전이 완료된 후 새 비밀번호 값이 있는지 알 수 없게 됩니다.

1 2004Q3 로의 이전이 완료된 후 모든 사용자에게 비밀번호를 변경하지 않고 `forcepwchg` 명령줄 유틸리티를 사용하여 이전 과정 동안 비밀번호를 변경한 사용자만 모두 비밀번호를 변경하도록 할 수 있습니다.

참고 `forcepwchg` 유틸리티는 Windows 패키지에서만 사용할 수 있습니다.

`forcepwchg` 유틸리티는 Windows migration 디렉토리에 있습니다. 이 디렉토리에 서 바로 `forcepwchg` 유틸리티를 실행하며 추가의 설치 단계는 필요하지 않습니다.

`forcepwchg` 는 반드시 NT 구성요소 (커넥터, 변경 검출기 DLL, 비밀번호 필터 DLL) 가 설치된 기본 도메인 제어기 (PDC) 에서 실행해야 하며 `forcepwchg` 를 원격으로 실행할 수는 없습니다.

`forcepwchg` 유틸리티는 또한 이전하려는 계정 이름을 인쇄 (한 줄에 하나씩) 합니다. 이전 과정 동안 오류가 발생하면 이전 동안 오류가 발생한 사용자 계정이 마지막으로 인쇄됩니다.

시스템 이전

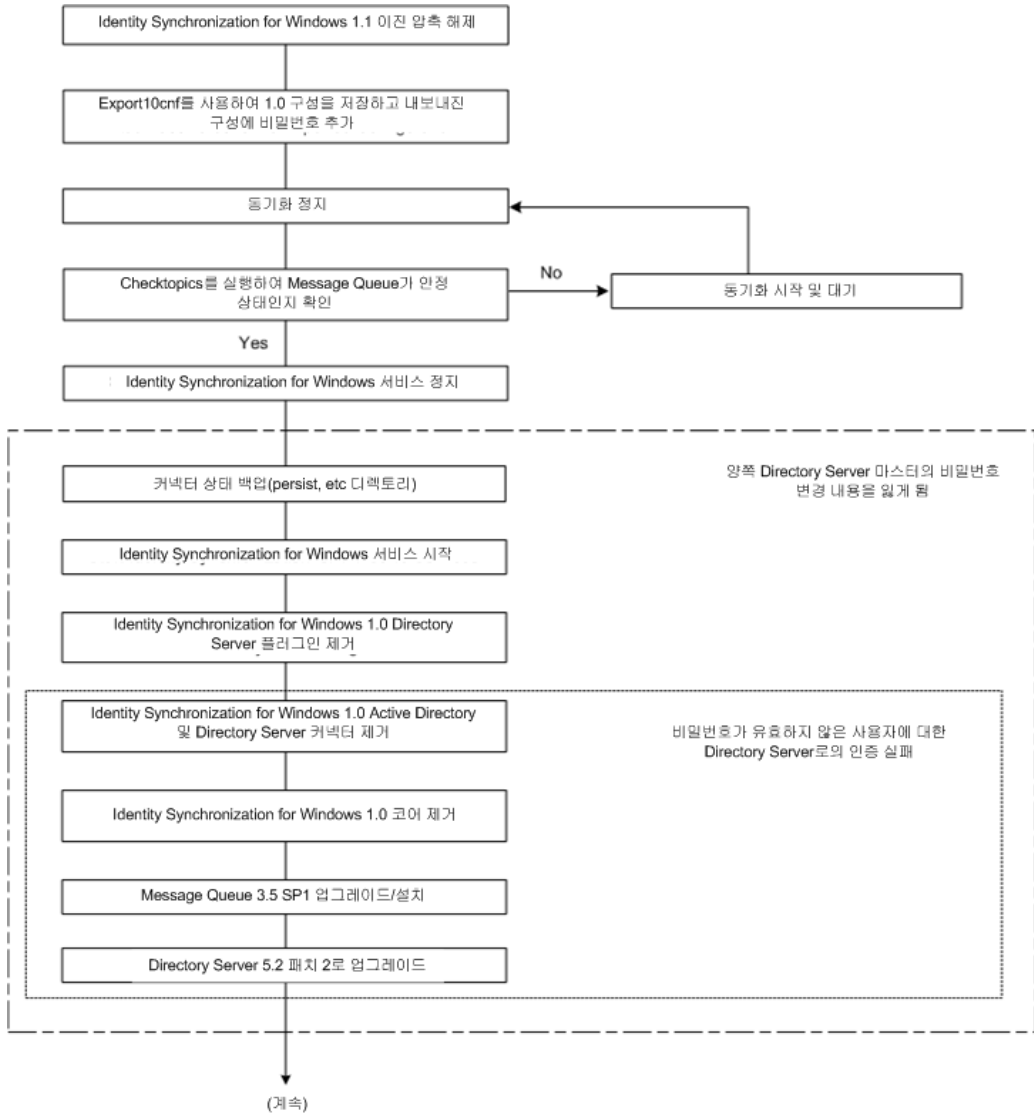
여기에서는 단일 호스트 구현을 버전 1 2004Q3 으로 이전하는 방법에 대하여 설명합니다. 단일 호스트 구현에서 모든 Identity Synchronization for Windows 구성요소는 다음과 같이 하나의 호스트 (Windows 2000 Server, Solaris 버전 8 또는 9, SPARC 등)에 설치됩니다.

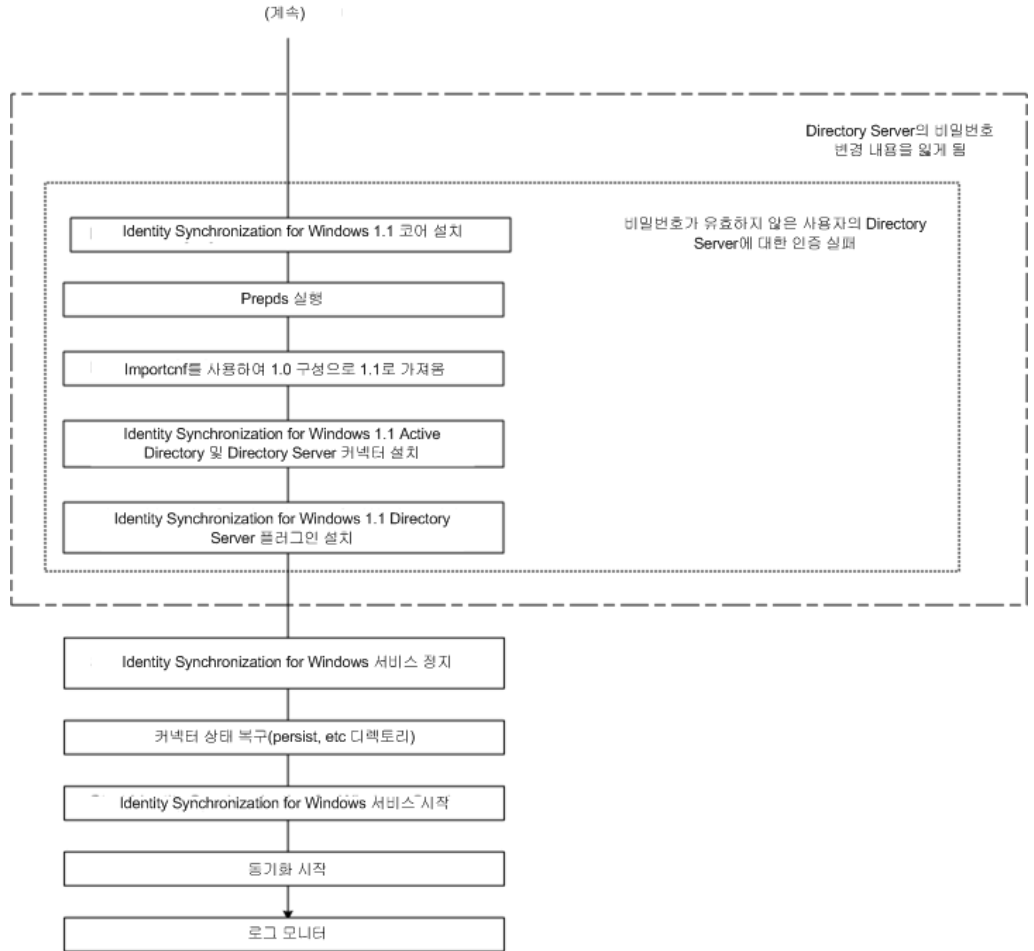
- Directory Server(인스턴스 1 개)
- 코어 (Message Queue, 중앙 기록기 , 시스템 관리자 및 콘솔)
- Active Directory 커넥터
- Directory Server 커넥터
- Directory Server 플러그인

참고	Solaris 를 설치 호스트로 사용하는 경우 Active Directory 가 있는 Windows 2000 은 동기화의 용도로만 필요합니다 . (Windows 2000 컴퓨터에 설치되는 구성요소는 없습니다 .)
-----------	--

이전 과정은 다음 그림에 보이는 것과 같으며 그 뒤의 이전 설명을 보완하는 점검 목록으로 사용할 수 있습니다.

그림 7-1) 단일 호스트 구현 이전





마이그레이션 준비

다음과 같이 Identity Synchronization for Windows 버전 1.0 에서 버전 1 2004Q3 으로의 마이그레이션을 준비합니다 .

1. 명령 프롬프트에서 다음과 같이 합니다 .

- Solaris 또는 SPARC: `uncompress -c <filename> | tar xf -` 를 입력합니다

- **Windows:** %JAVA_HOME%\bin\jar -xf <filename>

을 입력합니다. (또는 WinZip® 등의 Windows 용 압축 해제 프로그램을 사용 합니다.)

이전의 압축이 해제된 후 다음과 같은 하위 디렉토리에 마이그레이션에 필요한 도구가 포함됩니다.

- installer/
- lib/
- migration/

Solaris	Windows
export10cnf.jar	export10cnf.jar
—	forcepwchg.exe
checktopics.jar	checktopics.jar

2. 버전 1.0 구성 설정을 XML 파일로 내보냅니다.
migration 디렉토리에서 ["export10cnf 유틸리티 사용" 페이지 188](#)의 설명과 같이 export10cnf를 실행합니다. 예 :

```
java -jar export10cnf.jar -D "cn=directory manager" -w - -s
"dc=example,dc=com" -q - -f export.cfg
```

3. 내보낸 XML 파일에 비밀번호를 추가합니다.

내보낸 구성 파일의 각 cleartextPassword 필드의 인용부호 사이에 비밀번호를 입력합니다 (["일반 텍스트 비밀번호 삽입" 페이지 189](#) 참조)

4. ["동기화 시작 및 정지" 페이지 182](#)에 설명한 것과 같이 동기화를 정지합니다.
5. 시스템이 안정 상태인지 확인하십시오. migration 디렉토리에서 ["checktopics 유틸리티 사용" 페이지 194](#)의 설명과 같이 checktopics를 실행합니다.

예 :

```
java -jar checktopics.jar -D "cn=directory manager" -w - -s
"dc=example,dc=com" -q -
```

6. ["서비스 시작 및 정지" 페이지 183](#)에 설명한 것과 같이 Identity Synchronization for Windows 서비스 (데몬)를 정지합니다.

참고

이 때 Sun ONE Message Queue 서비스를 정지하면 안 됩니다.

7. *Windows NT 시스템만 적용* - Sun One NT ChangeDetector 서비스를 정지합니다. 명령줄에서 다음을 입력하여 서비스를 정지할 수 있습니다.

```
net stop "Sun One NT ChangeDetector Service"
```

8. *Windows NT 시스템만 적용* - 다음과 같이 NT ChangeDetector 서비스 카운터를 저장합니다.

- a. regedt32.exe 를 실행하여 레지스트리 편집기를 엽니다.
- b. HKEY_LOCAL_MACHINE 창을 선택합니다.
- c. SOFTWARE\Sun Microsystems\PSW\1.0 노드로 이동합니다.
- d. 다음 레지스트리 값을 저장합니다.
 - HighestChangeNumber
 - LastProcessedSecLogRecordNumber
 - LastProcessedSecLogTimeStamp
 - QueueSize

9. 기존 1.0 설치 트리에서 persist 및 etc 디렉토리를 백업하여 커넥터 상태를 저장합니다.

- **Solaris:** `cd <serverroot>/isw-<hostname>`
`tar cf /var/tmp/connector-state.tar persist etc` 를 입력
- **Windows:** `cd <serverroot>\isw-<hostname>`
`zip -r C:\WINNT\Temp\connector-state.zip persist etc` 를 입력
`%JAVA_HOME%\bin\jar -cfm %TEMP%\connector-state.jar persist etc`
 (또는 WinZip 등의 Windows 용 압축 해제 프로그램 사용)

10. Identity Synchronization for Windows 서비스를 시작합니다 ([페이지 183](#) 참조).

참고

Sun ONE Message Queue 서비스를 정지하지 않았으므로 다시 시작할 필요는 없습니다.

Identity Synchronization for Windows 제거

참고

SUNWjss 패키지가 다른 응용 프로그램이 사용할 수 있도록 (Identity Synchronization for Windows 1.0 제외) 등록되지 않은 경우 Identity Synchronization for Windows 1.0 설치 프로그램은 이 패키지를 제거합니다. 특히 이러한 상황은 Directory Server 5.2.2 를 설치한 경우 Solaris 컴퓨터에서 발생할 수 있으며, 이 경우 제거 프로그램이 /usr/share/lib/mps/secv1 에서 jss3.jar 파일을 제거합니다.

Identity Synchronization for Windows 11 2004Q3 로 마이그레이션할 때 이러한 상황이 발생하면 설치 프로그램이 필요한 파일이 없음을 보고하고 파일 이름을 설치 로그에 기록합니다. 이 경우가 발생하면 반드시 필요한 패치 ("[Sun Java System 소프트웨어 요구 사항](#)" [페이지 53](#) 참조) 를 다시 설치하고 설치 프로세스를 다시 시작해야 합니다.

준비 단계를 완료하면 다음과 같이 Identity Synchronization for Windows 버전 1.0(또는 1.0 SP1) 의 제거를 시작할 수 있습니다.

1. Directory Server 플러그인을 직접 제거하고 플러그인이 설치된 위치의 각 Directory Server 를 다시 시작합니다.
2. 플러그인이 설치된 위치의 각 Directory Server 에서 다음 단계를 실행합니다.
 - a. Directory Server 에서 다음 항목을 제거합니다.


```
cn=config,cn=pswsync,cn=plugins,cn=config
cn=pswsync,cn=plugins,cn=config
```

 예 :


```
ldapdelete -D "cn=directory manager" -w - -p <port> -c
cn=config, cn=pswsync,cn=plugins,cn=config
cn=pswsync,cn=plugins,cn=config
```
 - b. Directory Server 를 다시 시작합니다.
 - **Solaris:** <serverroot>/slapd-<hostname>/restart-slapd 입력
 - **Windows:** <serverroot>\slapd-<hostname>\restart-slapd.bat 입력
 - c. 시스템에서 플러그인 이진을 제거합니다.

- **Solaris:** `rm <serverroot>/lib/psw-plugin.so`
`rm <serverroot>/lib/64/psw-plugin.so` 입력
 - **Windows:** `del <serverroot>\lib\psw-plugin.dll` 입력
3. `<server_root>\isw-<hostname>` 디렉토리로 변경 (`cd`) 한 후 Identity Synchronization for Windows 1.0 제거 프로그램을 사용하여 버전 1.0/1.0 SP1 커넥터 및 코어 구성요소를 제거합니다.

참고

반드시 항상 코어 구성요소를 제거하기 전에 커넥터를 제거해야 합니다.

- **Solaris 또는 SPARC:** `./runUninstaller.sh` 입력
 - **Windows:** `\runUninstaller.bat` 입력
4. 다음 단계와 같이 제품 레지스트리 파일에서 Identity Synchronization for Windows에 관련된 항목을 제거합니다.
- a. 파일의 사본 백업 (위치):
 - **Solaris:** `/var/sadm/install/productregistry`
 - **Windows:** `C:\WINNT\System32\productregistry`
 - b. 제품 레지스트리 파일에서 Identity Synchronization for Windows 관련 항목을 제거하려면 "Solaris에서 1.0 코어 및 인스턴스 직접 제거"의 단계 6에서 제공한 설명을 따라 하십시오.
5. *Windows에만 적용* -- 코어를 제거한 후 컴퓨터를 다시 시작합니다.

참고

어떤 이유든지 제거가 실패하는 경우 Identity Synchronization for Windows 구성요소를 직접 제거해야 합니다. 방법은 "1.0 제거에 실패한 경우의 작업 방법" 페이지 206에 있습니다.

6. *Windows에만 적용* -- Identity Synchronization for Windows가 실행되지 않도록 확인합니다. 필요한 경우 명령줄에서 다음을 입력하여 서비스를 정지할 수 있습니다.

```
net stop "Sun ONE Identity Synchronization for Windows"
```

제거가 완료된 후 서비스가 계속 실행되는 경우 공유 위반이 발생하며, 따라서 인스턴스를 직접 제거할 수 없게 됩니다.

7. Identity Synchronization for Windows 인스턴스 디렉토리 (isw-<hostname>) 를 제거합니다 .

종속 제품 설치 또는 업그레이드

다음과 같이 Java Runtime Environment 업그레이드 , Message Queue 설치 및 Directory Server 업그레이드를 수행합니다 .

1. Identity Synchronization for Windows 구성요소가 설치된 위치의 각 호스트 (Windows NT 제외) 에서 Java 2 Runtime Environment 를 업그레이드합니다 . (최소 요구 버전은 1.4.2_04 입니다 .)
 - **Java 2 SDK:** <http://java.sun.com/j2se/1.4.2/install.html>
 - **Java 2 Runtime Environment:**
<http://java.sun.com/j2se/1.4.2/jre/install.html>
2. *Sun Java System Message Queue 3.5 SP1 Installation Guide* 에 제공된 설명대로 Message Queue 3.5 SP1 을 설치합니다 .
3. *Sun Java System Directory Server 5 2004Q2 Installation and Migration Guide* 에 제공된 설명대로 Directory Server 를 버전 5.2 SP2 로 업그레이드합니다 . 이 설명서는 다음 위치에 있습니다 .

http://docs.sun.com/db/coll/DirectoryServer_04q2

Directory Server 를 업그레이드하면 현재 Directory Server 구성 및 데이터베이스가 보존됩니다 .

Identity Synchronization for Windows 1 2004Q3 설치

다음과 같이 Identity Synchronization for Windows 1 2004Q3 구성요소를 설치합니다 .

1. Identity Synchronization for Windows 1 2004Q3 코어를 설치합니다 . (" 코어 설치 " 페이지 85 참조)
2. 다음과 같이 Directory Server 에 idsync prepds 를 실행하여 스키마를 업데이트 합니다 .
 - **Solaris:** `cd /opt/SUNWisw/bin` 입력
그런 후 `idsync prepds <arguments>` 입력

- **Windows:** `cd \<serverroot>\isw-<hostname>\bin` 입력
그런 후 `idsync prepds <arguments>` 입력

idsync prepds 를 사용하는 자세한 방법은 [부록 A, "Identity Synchronization for Windows 명령줄 유틸리티 사용."](#) 참조

3. 다음을 입력하여 버전 1.0 구성 XML 파일을 가져옵니다.

```
idsync importcnf <인수>
```

참고

프로그램이 입력 구성 파일에서 오류를 발견하면 오류가 발생합니다. Identity Synchronization for Windows 는 importcnf 프로세스를 중단하고 실수를 수정하는 데 필요한 정보를 제공합니다.

idsync importcnf 를 사용하는 자세한 방법은 [부록 A](#)의 "importcnf 사용" 을 참조하십시오.

4. Identity Synchronization for Windows 1 2004Q3 커넥터를 설치합니다 ("커넥터 설치" [페이지 160](#) 참조).
5. Identity Synchronization for Windows 1 2004Q3 Directory Server 플러그인을 설치합니다 ("Directory Server 플러그인 설치" [페이지 171](#)).
6. "서비스 시작 및 정지" [페이지 183](#)에 설명한 것과 같이 Identity Synchronization for Windows 서비스 (데몬) 를 정지합니다.
7. *Windows NT 시스템만 적용* -- Sun Java™ System NT Change Detector 서비스를 정지합니다. 명령줄에서 다음을 입력하여 서비스를 정지할 수 있습니다.
net stop "Sun Java(TM) System NT Change Detector"
8. *Windows NT 시스템만 적용* -- NT ChangeDetector Service 카운터를 복구합니다.
 - a. regedt32.exe 를 실행하여 레지스트리 편집기를 엽니다.
 - b. HKEY_LOCAL_MACHINE 창을 선택합니다.
 - c. SOFTWARE\Sun Microsystems\Sun Java(TM) System Identity Synchronization for Windows\1.1 노드로 이동합니다.
 - d. 다음의 각 항목을 두 번 눌러 해당 값(버전 1.0을 제거하기 전에 저장한 값)을 복구합니다.
 - HighestChangeNumber
 - LastProcessedSecLogRecordNumber
 - LastProcessedSecLogTimeStamp

- QueueSize

9. *Windows NT 시스템만 적용* -- Sun Java™ System NT Change Detector 서비스를 시작합니다. 명령줄에서 다음을 입력하여 서비스를 시작할 수 있습니다.

```
net start "Sun Java(TM) System NT Change Detector"
```

10. 인스턴스 디렉토리에서 1 2004Q3 persist 및 etc 디렉토리 (또한 디렉토리의 모든 내용) 를 제거하고 "마이그레이션 준비" [페이지 199](#) 에서 백업한 버전 1.0(또는 1.0 SP1) persist 및 etc 디렉토리를 복구합니다.

- Solaris: 입력

```
cd /var/opt/SUNWisw
rm -rf etc persist
tar xf /var/tmp/connector-state.tar
```

- Windows: 입력

```
cd <serverroot>\isw-<hostname>
rd /s etc persist
%JAVA_HOME%\bin\jar -xf %TEMP%\connector-state.jar
( 또는 WinZip 등의 Windows 용 압축 해체 프로그램 사용 )
```

11. Identity Synchronization for Windows 서비스를 시작합니다 ([페이지 183](#) 참조).
12. " 동기화 시작 및 중지 " [페이지 182](#) 에 설명한 것과 같이 동기화를 시작합니다 .
13. 중앙 감사 로그에서 경고 메시지가 없는지 확인합니다 .

참고 버전 1.0 로그 설정을 사용자 정의한 경우 반드시 버전 1 2004Q3 설치에 해당 사용자 정의를 수동으로 적용해야 합니다 .
Identity Synchronization for Windows 콘솔을 사용하여 1 2004Q3 로그 설정을 구성합니다 .

1.0 제거에 실패한 경우의 작업 방법

1 2004Q3 설치 프로그램이 버전 1.0 시스템의 흔적을 발견하는 경우 1 2004Q3 설치가 실패합니다 . 따라서 버전 1 2004Q3 을 설치하기 전에 시스템에서 1.0 구성요소가 완전히 제거되었는지 확인해야 합니다 .

제거 프로그램이 버전 1.0/1.0 SP1 구성요소를 모두 제거할 수 없는 경우 반드시 Identity Synchronization for Windows 제품 레지스트리와 Solaris 패키지를 직접 제거해야 합니다 .

Identity Synchronization for Windows 버전 1.0 을 직접 제거하는 자세한 방법은 아래의 세 단원에서 설명합니다.

- ["Solaris 에서 1.0 코어 및 인스턴스 직접 제거 " 페이지 207](#)
- ["Windows 2000 에서 1.0 코어 및 인스턴스 직접 제거 " 페이지 213](#)
- ["Windows NT 에서 1.0 인스턴스 직접 제거 " 페이지 218](#)

참고

여기에서 제공된 방법은 Identity Synchronization for Windows *버전 1.0*에만 적용되는 방법입니다.

Identity Synchronization for Windows 제거 프로그램이 실패하지 않는 경우 다음에서 제공하는 직접 제거 방법을 사용하면 *안 됩니다*.

Solaris 에서 1.0 코어 및 인스턴스 직접 제거

여기에 제공된 방법을 사용하여 Solaris 컴퓨터에서 코어를 직접 제거합니다.

참고

여기에서 Identity Synchronization for Windows 위치는 다음과 같은 방식으로 설명합니다.

```
<serverroot>/isw-<hostname>
```

여기에서 <serverroot> 는 Identity Synchronization for Windows 설치 위치의 상위 디렉토리입니다.

예를 들어 Identity Synchronization for Windows 를
/var/Sun/mps/isw-<example> 에 설치한 경우 <serverroot> 는
/var/Sun/mps 입니다.

1. 터미널 창에서 `/etc/init.d/isw stop` 을 입력하여 모든 Identity Synchronization for Windows Java 프로세스를 정지합니다.

앞의 명령으로 모든 Java 프로세스가 정지되지 않으면 다음을 입력합니다.

```
/usr/ucb/ps -gauxwww | grep java
```

```
kill -s SIGTERM <이전 명령의 프로세스 ID>
```

2. 다음과 같이 Message Queue 를 정지합니다.

- a. 프롬프트에서 다음 명령을 입력하여 Message Queue 브로커를 정지합니다.

```
/etc/init.d/imq stop
```

- b. 나머지 imq 프로세스를 정지하려면 다음을 입력합니다.

```
* ps -ef | grep imqbroker
```

```
* kill -s SIGTERM < 이전 명령의 프로세스 ID>
```

- c. 다음 방법 중 한 가지를 사용하여 브로커 패키지과 디렉토리를 제거합니다.

- Message Queue 브로커 제거 스크립트 (코어를 설치한 호스트의 Identity Synchronization for Windows instance 디렉토리) 를 사용하여 브로커를 제거합니다. 다음을 입력합니다.

```
/<serverroot>/isw-<hostname>/imq_uninstall
```

- 다음과 같이 패키지과 디렉토리를 직접 제거합니다.

pkgrm: 명령을 사용하여 다음 패키지를 제거합니다.

SUNWaclg	SUNWiqum	SUNWiqjx
SUNWiqlen	SUNWxsrt	SUNWiqu
SUNWjaf	SUNWiqfs	SUNWjhrt
SUNWiqdoc	SUNWiquc	SUNWiqsup
SUNWiqr	SUNWjmail	

rm -rf 명령을 사용하여 다음 디렉토리를 제거합니다.

```
rm -rf /etc/imq
```

```
rm -rf /var/imq
```

```
rm -rf /usr/bin/imq*
```

3. Identity Synchronization for Windows 1.0 Solaris 패키지를 제거하려면
의 각 패키지에 대하여 pkgrm <packageName> 을 실행합니다.
(예 : pkgrm SUNWidscm SUNWidscn SUNWidscr SUNWidsct SUNWidsoc)

표 7-1) 제거할 Solaris 패키지

패키지 이름	설명
SUNWidscm	코어 구성요소와 커넥터용 Sun ONE Directory Server Identity Synchronization 패키지 .
SUNWidscn	콘솔 도움말 파일용 Sun ONE Directory Server Identity Synchronization 패키지 .
SUNWidscr	코어 구성요소용 Sun ONE Directory Server Identity Synchronization 패키지 .
SUNWidset	커넥터용 Sun ONE Directory Server Identity Synchronization 패키지 .
SUNWidsoc	객체 캐시용 Sun ONE Directory Server Identity Synchronization 패키지 .

패키지가 모두 제거되었는지 확인하려면 다음을 입력합니다 .

```
pkginfo | grep -i "Identity Synchronization"
```

참고	종속성으로 인하여 아직 남아 있는 패키지가 있으면 <code>pkgrm <packageName></code> 명령을 다시 실행합니다 .
-----------	---

4. 다음과 같이 Directory Server 플러그인을 제거합니다 .
 - a. Directory Server 콘솔을 열고 구성 탭을 선택합니다 .
 - b. 왼쪽 창에서 Plugins 노드를 확장하고 pswsync 노드를 선택합니다 .
 - c. 오른쪽 창에서 Enable plug-in 선택란의 선택을 해제합니다 .
 - d. 저장을 눌러 변경 내용을 저장합니다 .
 - e. Directory Server 콘솔에서 다음 항목을 Configuration 디렉토리로부터 찾아 제거합니다 .


```
cn=pswsync,cn=plugins,cn=config
```
 - f. Directory Server 를 정지합니다 .
 - g. 플러그인 바이너리를 제거하려면 다음을 입력합니다 .


```
rm -f /<serverroot>/lib/psw-plugin.so
```
 - h. Directory Server 를 다시 시작합니다 .

5. /var/sadm/install/productregistry 에 있는 현재 productregistry 파일을 백업 (복사하여 이름 변경) 합니다 .
6. /var/sadm/install/ 에 있는 productregistry 파일을 직접 편집하여 다음 항목을 (있는 경우) 제거합니다 .

참고

- XML 편집기를 사용하면 가장 좋습니다 . 또는 표준 텍스트 편집기를 사용할 수도 있습니다 .
 - 다음 구성요소 중 일부는 파일에 포함되지 않을 수 있습니다 .
 - 시작 태그 (<compid>), 종료 태그 (</compid>) 및 이 두 태그 사이의 모든 내용을 삭제해야 합니다 . 다음 목록에서 타원은 이 태그의 일부분으로 포함된 추가 텍스트 및 태그를 표시합니다 . ([페이지 211](#) 의 예를 참조하십시오 .)
-

```

○ <compid>Identity Synchronization for Windows . . . </compid>
○ <compid>Core . . . </compid>
○ <compid>unistaller . . . </compid>
○ <compid>wpsyncwatchdog . . . </compid>
○ <compid>setenv . . . </compid>
○ <compid>Create DIT . . . </compid>
○ <compid>Extend Schema . . . </compid>
○ <compid>resources . . . </compid>
○ <compid>CoreComponents . . . </compid>
○ <compid>Connector . . . </compid>
○ <compid>DSConnector . . . </compid>
○ <compid>Directory Server Plugin . . . </compid>
○ <compid>DSSubcomponents . . . </compid>
○ <compid>ObjectCache . . . </compid>
○ <compid>ObjectCacheDLLs . . . </compid>
○ <compid>SUNWidscr . . . </compid>
○ <compid>SUNWidscm . . . </compid>

```

- `<compid>SUNWidsct . . . </compid>`
- `<compid>SUNWidscn . . . </compid>`
- `<compid>SUNWidsoc . . . </compid>`
- `<compid>ADConnector . . . </compid>`

다음은 `<compid>` 태그의 예입니다. `<compid>`, `</compid>` 및 이 사이의 모든 텍스트를 제거합니다.

```
<compid>Identity Synchronization for Windows
  <compversion>1.0
    <uniquename>Identity Synchronization for Windows</uniquename>
    <compinstance>1
      <children>
        <compref>ADConnector
          <instance>1
            <version>1.0</version>
          </instance>
        </compref>
        <compref>DSSubcomponents
          . . .
        </compref>
      </children>
    </compinstance>
  </compversion>
</compid>
```

7. 다음의 Identity Synchronization for Windows 디렉토리 및 파일을 제거합니다.

- a. 설치 위치에서 다음을 입력합니다.

```
rm -rf /<serverroot>/isw-<hostname>
```

- b. 다음을 입력하여 bootstrap 파일을 제거합니다.

```
rm -rf /etc/init.d/isw
```

8. 다음과 같이 구성 디렉토리를 비웁니다.

- a. Identity Synchronization for Windows 코어가 설치된 구성 디렉토리에 대하여 다음 `ldapsearch` 명령을 수행하여 Identity Synchronization for Windows 콘솔 하위 트리를 찾습니다.

```
ldapsearch -D "cn=directory manager" -w <my_password> -b
o=netscaperoot "(nsnickname=isw)" dn
```

참고 ldapsearch 는 Directory Server 의
 <serverroot>/shared/bin/ldapsearch 에 있습니다.
 예 : /var/Sun/mps/shared/bin/ldapsearch

결과 항목은 다음과 비슷할 것입니다. (참고로 항목은 항상
o=NetscapeRoot 로 끝납니다.)

```
"cn=Sun ONE Identity Synchronization for Windows,cn=server
group, cn=myhost.mydomain.com,ou=mydomain.com,o=NetscapeRoot"
```

- b. Directory Server 콘솔을 사용하여 Identity Synchronization for Windows 콘
솔 하위 트리 및 그 아래의 모든 하위 트리를 제거합니다.

- 9. 다음과 같이 Identity Synchronization for Windows 구성 레지스트리를 비웁니다.

- a. 다음 ldapsearch 명령을 사용하여 Directory Server 에서 Identity
Synchronization for Windows 구성 레지스트리를 찾습니다.

```
ldapsearch -D "cn=directory manager" -w <my_password> -b
"dc=my,dc=domain"
"(&(objectclass=iplanetservice)(ou=IdentitySynchronization))" dn
```

결과와 항목은 다음과 비슷합니다.

```
"ou=IdentitySynchronization,ou=Services,dc=my,dc=domain"
```

- b. Directory Server 콘솔을 사용하여 Identity Synchronization for Windows 구
성 레지스트리 및 그 아래의 모든 하위 트리를 제거합니다.

- 10. 다음과 같이 모든 콘솔 관련 파일을 제거합니다.

- a. 다음을 입력하여 모든 콘솔 jar 파일을 제거합니다.

```
rm -rf <serverroot>/java/jars/isw*
```

예 : /var/Sun/mps/java/jars/isw*

- b. 다음을 입력하여 모든 콘솔 서버릿 jar 파일을 제거합니다.

```
rm -rf <serverroot>/bin/isw/
```

예 : /var/Sun/mps/bin/isw/

Windows 2000 에서 1.0 코어 및 인스턴스 직접 제거

여기에 제공된 방법을 사용하여 Windows 2000 컴퓨터에서 코어를 직접 제거합니다.

참고

여기에서 Identity Synchronization for Windows 위치는 다음과 같은 방식으로 설명합니다.

`<serverroot>\isw-<hostname>`

여기에서 `<serverroot>` 는 Identity Synchronization for Windows 설치 위치의 상위 디렉토리입니다.

예를 들어 Identity Synchronization for Windows 를 C:\Program Files\Sun\mps\isw-example 에 설치한 경우 `<serverroot>` 는 C:\Program Files\Sun\mps 입니다.

1. 다음 방법 중 한가지를 사용하여 모든 Identity Synchronization for Windows java 프로세스를 중지합니다.

- 시작 > 설정 > 제어판 > 관리 도구 > 서비스를 선택하여 서비스 창을 엽니다. 오른쪽 창에서 Identity Synchronization for Windows 를 마우스 오른쪽 버튼으로 누르고 정지를 선택합니다.

- 명령 프롬프트 창을 열고 다음 명령을 입력합니다.

```
net stop "Sun ONE Identity Synchronization for Windows"
```

- 앞의 방법으로 정지하지 않는 경우 다음과 같이 Java 프로세스를 직접 정지해야 합니다.

I. 서비스 창을 열고 Identity Synchronization for Windows 를 마우스 오른쪽 버튼으로 누른 후 등록 정보를 선택합니다.

II. 등록 정보 창의 일반 탭으로 이동한 후 시작 유형 드롭다운 목록에서 수동을 선택합니다.

참고

Windows 작업 관리자에서 Java 프로세스 (pswatchdog.exe 등) 를 볼 수는 있으나 Identity Synchronization for Windows 에 관련된 프로세스를 확인할 수는 없습니다. 그러므로 Windows 작업 관리자에서 프로세스를 정지하면 안 됩니다.

2. 다음 방법 중 한 가지를 사용하여 Message Queue 를 정지합니다 (코어 제거에만 적용).
 - 서비스 창에서 오른쪽 창의 iMQ Broker 를 마우스 오른쪽 버튼으로 누른 후 정지를 선택합니다.
 - 명령 프롬프트 창을 열고 다음 명령을 입력합니다.


```
net stop "iMQ Broker"
```
 - 앞의 방법으로 정지하지 않는 경우 다음과 같이 Message Queue 를 직접 정지해야 합니다.
 - I. 서비스 창을 열고 iMQ Broker 를 마우스 오른쪽 버튼으로 누른 후 등록 정보를 선택합니다.
 - II. 등록 정보 창의 일반 탭으로 이동한 후 시작 유형 드롭다운 목록에서 수동을 선택합니다.
3. 다음과 같이 Directory Server 플러그인을 제거합니다.
 - a. Directory Server 콘솔을 열고 구성 탭을 선택합니다.
 - b. 왼쪽 창에서 Plugins 노드를 확장하고 psync 노드를 선택합니다.
 - c. 오른쪽 창에서 Enable plug-in 선택란의 선택을 해제합니다.
 - d. 저장을 눌러 변경 내용을 저장합니다.
 - e. 콘솔에서 다음 항목을 Configuration 디렉토리로부터 찾아 제거합니다.


```
cn=psync,cn=plugins,cn=config
```
 - f. 다음 방법 중 한가지를 사용하여 모든 Directory Server 를 정지합니다.
 - 서비스 창에서 오른쪽 창의 Sun ONE Directory Server 5.2 를 마우스 오른쪽 버튼으로 누른 후 정지를 선택합니다.
 - 명령 프롬프트 창을 열고 다음 명령을 입력합니다.


```
net stop slapd-<myhostname>
```
 - g. Windows 탐색기를 열고 플러그인 이진을 찾아 제거합니다.


```
<serverroot>\lib\psw-plugin.so
```
 - h. Directory Server 를 다시 시작합니다.
4. 명령 프롬프트 창을 열고 **regedit** 를 입력하여 레지스트리 편집기 창을 엽니다.

중요 -- 단계 5 로 계속하기 전에 현재 레지스트리 파일을 백업하십시오.

- a. 레지스트리 편집기의 왼쪽 창에서 최상단 노드 (My Computer) 를 선택합니다.
 - b. 메뉴줄에서 레지스트리 > 레지스트리 파일 내보내기를 선택합니다.
 - c. 레지스트리 파일 내보내기 대화 상자가 표시되면 파일의 이름을 지정하고 백업 레지스트리를 저장할 위치를 선택합니다.
5. 레지스트리 편집기의 메뉴줄에서 편집 > 삭제를 선택하여 다음 Identity Synchronization for Windows 키를 Windows 레지스트리에서 제거합니다.
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Identity Synchronization for Windows 아래의 모든 항목
 - HKEY_LOCAL_MACHINE\SYSTEM* 아래의 모든 CurrentControlSet 및 ControlSet (ControlSet001, ControlSet002 등) 항목. 여기에는 다음 항목이 (있는 경우) 포함됩니다.
 - ...\Control\Session Manager\Environment\<isw-installation directory>
 - ...\Services\Eventlog\Application\Sun ONE Identity Synchronization for Windows
 - ...\Services\Sun ONE Identity Synchronization for Windows
 - ...\Services\iMQBroker
6. C:\WINNT\system32에 있는 현재 productregistry 파일을 백업 (복사하여 이름 변경) 합니다.
7. C:\WINNT\system32\productregistry 파일을 편집하여 다음 태그를 제거합니다.

참고

- XML 편집기를 사용하면 가장 좋습니다. 또는 표준 텍스트 편집기를 사용할 수도 있습니다.
 - 다음 구성요소 중 일부는 파일에 포함되지 않을 수 있습니다.
 - 시작 태그 (<compid>), 종료 태그 (</compid>) 및 이 두 태그 사이의 모든 내용을 삭제해야 합니다. 다음 목록에서 타원은 이 태그의 일부분으로 포함된 추가 텍스트 및 태그를 표시합니다. (페이지 216의 예를 참조하십시오.)
-

- <compid>Identity Synchronization for Windows . . . </compid>

- <compid>Core . . . </compid>
- <compid>unistaller . . . </compid>
- <compid>wpsyncwatchdog . . . </compid>
- <compid>setenv . . . </compid>
- <compid>Create DIT . . . </compid>
- <compid>Extend Schema . . . </compid>
- <compid>resources . . . </compid>
- <compid>CoreComponents . . . </compid>
- <compid>Connector . . . </compid>
- <compid>DSConnector . . . </compid>
- <compid>Directory Server Plugin . . . </compid>
- <compid>DSSubcomponents . . . </compid>
- <compid>ObjectCache . . . </compid>
- <compid>ObjectCacheDLLs . . . </compid>
- <compid>ADConnector . . . </compid>

다음은 <compid> 태그의 예입니다. <compid>, </compid> 및 이 사이의 모든 텍스트를 제거합니다.

```
<compid>Identity Synchronization for Windows
  <compversion>1.0
    <uniquename>Identity Synchronization for Windows</uniquename>
    <compinstance>1
      <children>
        <compref>ADConnector
          <instance>1
            <version>1.0</version>
          </instance>
        </compref>
        <compref>DSSubcomponents
          . . .
        </compref>
      </children>
    </compinstance>
  </compversion>
</compid>
```

8. <serverroot>\isw-<hostname> 에 위치 한 Identity Synchronization for Windows 설치 폴더를 제거합니다 .

예 : C:\Program Files\Sun\mps\isw-example

9. 다음과 같이 구성 디렉토리를 비웁니다 .
- 명령 프롬프트 창에서 Identity Synchronization for Windows 코어가 설치된 구성 디렉토리에 대하여 ldapsearch 명령을 수행하여 Identity Synchronization for Windows 콘솔 하위 트리를 찾습니다 .

참고 ldapsearch는 <serverroot>\shared\bin\ldapsearch에 있습니다 .

예 :

C:\Program Files\Sun\mps\shared\bin\ldapsearch

```
ldapsearch -D "cn=directory manager" -w <my_password> -b
o=netscaperoot "(nsnickname=isw)" dn
```

결과 항목은 다음과 비슷할 것입니다 . (참고로 항목은 항상 o=NetscapeRoot 로 끝납니다 .)

```
"cn=Sun ONE Identity Synchronization for Windows,cn=server
group, cn=myhost.mydomain.com,ou=mydomain.com,o=NetscapeRoot"
```

- Directory Server 콘솔을 사용하여 찾은 Identity Synchronization for Windows 콘솔 하위 트리 및 그 아래의 모든 하위 트리를 제거합니다 .
10. 다음과 같이 Identity Synchronization for Windows 구성 디렉토리(다른 이름으로 구성 레지스트리)를 제거합니다 .
- 명령 프롬프트 창에서 다음 ldapsearch 명령을 사용하여 Directory Server에 있는 Identity Synchronization for Windows 구성 디렉토리를 찾습니다 .
- ```
ldapsearch -D "cn=directory manager" -w <my_password> -b
"dc=my,dc=domain"
"(&(objectclass=iplanetservice)(ou=IdentitySynchronization))" dn
```
- 결과와 항목은 다음과 비슷합니다 .
- ```
"ou=IdentitySynchronization,ou=Services,dc=my,dc=domain"
```
- Directory Server 콘솔을 사용하여 찾은 구성 디렉토리 하위 트리 및 그 아래의 모든 하위 트리를 제거합니다 .
11. 다음과 같이 모든 콘솔 관련 파일을 제거합니다 .

- a. `<serverroot>\java\jars\isw*` 에 있는 모든 콘솔 jar 파일 제거합니다.
예 : `C:\Program Files\Sun\mps\java\jars\isw*`
- b. `\<directory_server_install_root>\bin\isw\` 에 있는 모든 콘솔 서브릿 jar 파일을 제거합니다.
예 : `C:\SunOne\Servers\bin\isw\`

12. 컴퓨터를 다시 시작하여 모든 변경 내용이 적용되도록 합니다.

Windows NT 에서 1.0 인스턴스 직접 제거

여기에 제공된 방법을 사용하여 Windows NT 컴퓨터에서 인스턴스를 직접 제거합니다.

참고 여기에서 Identity Synchronization for Windows 위치는 다음과 같은 방식으로 설명합니다.

`<serverroot>\isw-<hostname>`

여기에서 `<serverroot>` 는 Identity Synchronization for Windows 설치 위치의 상위 디렉토리입니다. 예를 들어 Identity Synchronization for Windows 를

`C:\Program Files\Sun\mps\isw-example` 에 설치한 경우

`<serverroot>` 는 `C:\Program Files\Sun\mps` 입니다.

1. 다음 방법 중 한가지를 사용하여 모든 Identity Synchronization for Windows Java 프로세스 (코어 및 인스턴스 설치) 를 정지합니다.
 - 시작 > 설정 > 제어판 > 관리 도구 > 서비스를 선택하여 서비스 창을 엽니다. 오른쪽 창에서 Identity Synchronization for Windows 를 마우스 오른쪽 버튼으로 누르고 정지를 선택합니다.
 - 명령 프롬프트 창을 열고 다음 명령을 입력합니다.
net stop "Sun ONE Identity Synchronization for Windows"
 - 앞의 방법으로 정지하지 않는 경우 다음과 같이 Java 프로세스를 직접 정지할 수 있습니다.
 - I. 서비스 창을 열고 Identity Synchronization for Windows 를 마우스 오른쪽 버튼으로 누른 후 등록 정보를 선택합니다.
 - II. 등록 정보 창의 일반 탭으로 이동한 후 시작 유형 드롭다운 목록에서 수동을 선택합니다.

참고 Windows 작업 관리자에서 Java 프로세스 (pswatchdog.exe 등)를 볼 수는 있으나 Identity Synchronization for Windows에 관련된 프로세스를 확인할 수는 없습니다. 그러므로 Windows 작업 관리자에서 프로세스를 정지하면 안 됩니다.

2. 다음 중 한 가지 방법으로 변경 검출기를 정지합니다.
 - 서비스 창에서 오른쪽 창의 Sun ONE NT 변경 검출기 Service를 마우스 오른쪽 버튼으로 누른 후 정지를 선택합니다.
 - 명령 프롬프트 창을 열고 다음 명령을 입력합니다.
net stop Sun ONE NT Change Detector Service
 - 앞의 방법으로 정지하지 않는 경우 다음과 같이 변경 검출기 Service를 직접 정지할 수 있습니다.
 - I. 서비스 창을 열고 변경 검출기 Service를 마우스 오른쪽 버튼으로 누른 후 등록 정보를 선택합니다.
 - II. 등록 정보 창의 일반 탭으로 이동한 후 시작 유형 드롭다운 목록에서 수동을 선택합니다.
3. Windows NT 컴퓨터를 다시 시작합니다.
4. 반드시 Identity Synchronization for Windows 레지스트리 키를 제거해야 합니다. 명령 프롬프트 창을 열고 **regedt32**를 입력하여 레지스트리 편집기 창을 엽니다.

주의 regedit에서는 복수 값 문자열을 편집할 수 없으므로 이 프로그램을 사용하면 **안 됩니다**.

단계 5로 진행하기 전에 반드시 현재 Windows 레지스트리 파일을 백업해야 합니다.

- a. 레지스트리 편집기의 왼쪽 창에서 최상단 노드 (My Computer)를 선택합니다.
 - b. 메뉴줄에서 레지스트리 > 레지스트리 파일 내보내기를 선택합니다.
 - c. 레지스트리 파일 내보내기 대화 상자가 표시되면 파일의 이름을 지정하고 백업 레지스트리를 저장할 위치를 선택합니다.
5. 레지스트리 편집기의 메뉴줄에서 편집 > 삭제를 선택하여 다음 Identity Synchronization for Windows 키를 레지스트리에서 제거합니다.

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Identity Synchronization for Windows 아래의 모든 항목
 - HKEY_LOCAL_MACHINE\SYSTEM* 아래의 모든 CurrentControlSet 및 ControlSet (ControlSet001, ControlSet002 등) 항목. 여기에는 다음 항목이 (있는 경우) 포함됩니다.
 - ...\Control\Session Manager\Environment\<isw-installation directory>
 - ...\Services\Eventlog\Application\Sun ONE Identity Synchronization for Windows
 - ...\Services\Sun ONE Identity Synchronization for Windows
 - ...\Services\iMQBroker
 - HKEY_LOCAL_MACHINE\SOFTWARE\Sun Microsystems\PSW
6. **regedt32**를 사용하여 다음 레지스트리 키를 수정 (**삭제** **아님**) 합니다. (regedit를 사용하면 **안 됩니다**.)
- a. 왼쪽 창에서 레지스트리 키를 선택합니다.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\CONTROL\LSA
레지스트리 값 유형은 반드시 REG_MULTI_SZ 이어야 합니다.
 - b. 오른쪽 창에서 Notification Packages 값을 마우스 오른쪽 버튼으로 누르고 수정을 선택합니다.
 - c. PASSFLT 값을 FPNWCLNT로 변경합니다.
7. C:\WINNT\system32에 있는 현재 productregistry 파일을 백업 (복사하여 이름 변경) 합니다.
8. C:\WINNT\system32 productregistry 파일을 편집하여 다음 태그를 제거합니다.

참고

- XML 편집기를 사용하면 가장 좋습니다. 또는 표준 텍스트 편집기를 사용할 수도 있습니다.
- 다음 구성요소 중 일부는 파일에 포함되지 않을 수 있습니다.
- 시작 태그 (<compid>), 종료 태그 (<\compid>) 및 이 두 태그 사이의 모든 내용을 삭제해야 합니다. 다음 목록에서 타원은 이 태그의 일부분으로 포함된 추가 텍스트 및 태그를 표시합니다. ([페이지 216](#)의 예를 참조하십시오.)

- <compid>Identity Synchronization for Windows . . . </compid>
- <compid>Core . . . </compid>
- <compid>uninstaller . . . </compid>
- <compid>wpsyncwatchdog . . . </compid>
- <compid>setenv . . . </compid>
- <compid>Create DIT . . . </compid>
- <compid>Extend Schema . . . </compid>
- <compid>resources . . . </compid>
- <compid>CoreComponents . . . </compid>
- <compid>Connector . . . </compid>
- <compid>DSConnector . . . </compid>
- <compid>Directory Server Plugin . . . </compid>
- <compid>DSSubcomponents . . . </compid>
- <compid>ObjectCache . . . </compid>
- <compid>ObjectCacheDLLs . . . </compid>
- <compid>ADConnector . . . </compid>

다음은 <compid> 태그의 예입니다. <compid>, </compid> 및 이 사이의 모든 텍스트를 제거합니다.

```
<compid>Identity Synchronization for Windows
  <compversion>1.0
    <uniquename>Identity Synchronization for Windows</uniquename>
      <compinstance>1
        <children>
          <compref>ADConnector
            <instance>1
              <version>1.0</version>
            </instance>
          </compref>
          <compref>DSSubcomponents
            . . .
          </compref>
        </children>
      </compinstance>
    </compversion>
  </compid>
```

9. `<serverroot>\isw-<hostname>` 에 위치한 Identity Synchronization for Windows 설치 폴더를 제거합니다.

예 : `C:\Program Files\Sun\mps\isw-example`

참고 단계 10 으로 계속하기 전에 반드시 단계 8 에서 설명한 것과 같이 Windows 레지스트리를 편집해야 합니다.

10. 비밀번호 필터 DLL 을 제거합니다.

`C:\winnt\system32` 폴더에서 `passflt.dll` 파일을 찾아 파일의 이름을 **`passflt.dll.old`** 로 변경합니다.

11. 컴퓨터를 다시 시작하여 모든 변경 내용이 적용되도록 합니다.

기타 이전 시나리오

다른 구현 토폴로지가 가능하므로 실제 마이그레이션 과정은 단일 호스트 구현용으로 설명한 과정과 일부 다를 수 있습니다.

여기에서는 두 가지 대안 구현 시나리오에 대하여 설명하고 각 경우의 이전 방법에 대하여 설명합니다. 예제 구현 시나리오는 다음과 같습니다.

- "복수 마스터 복제 구현"
- "Windows NT 를 포함하는 복수 호스트 구현" 페이지 225

복수 마스터 복제 구현

MMR(Multi-Master Replication) 구현의 경우 서로 다른 호스트에 두 개의 Directory Server 인스턴스가 설치됩니다. 서로 다른 운영 체제에서 호스트를 실행할 수 있으나 이 시나리오에서 두 호스트는 모두 동일한 운영 체제에서 실행됩니다.

두 호스트 사이에서 Identity Synchronization for Windows 구성요소가 배포되는 방식은 에 보이는 것과 같습니다.

표 7-2) MMR(Multi-Master Replication) 구현에서의 구성요소 배포

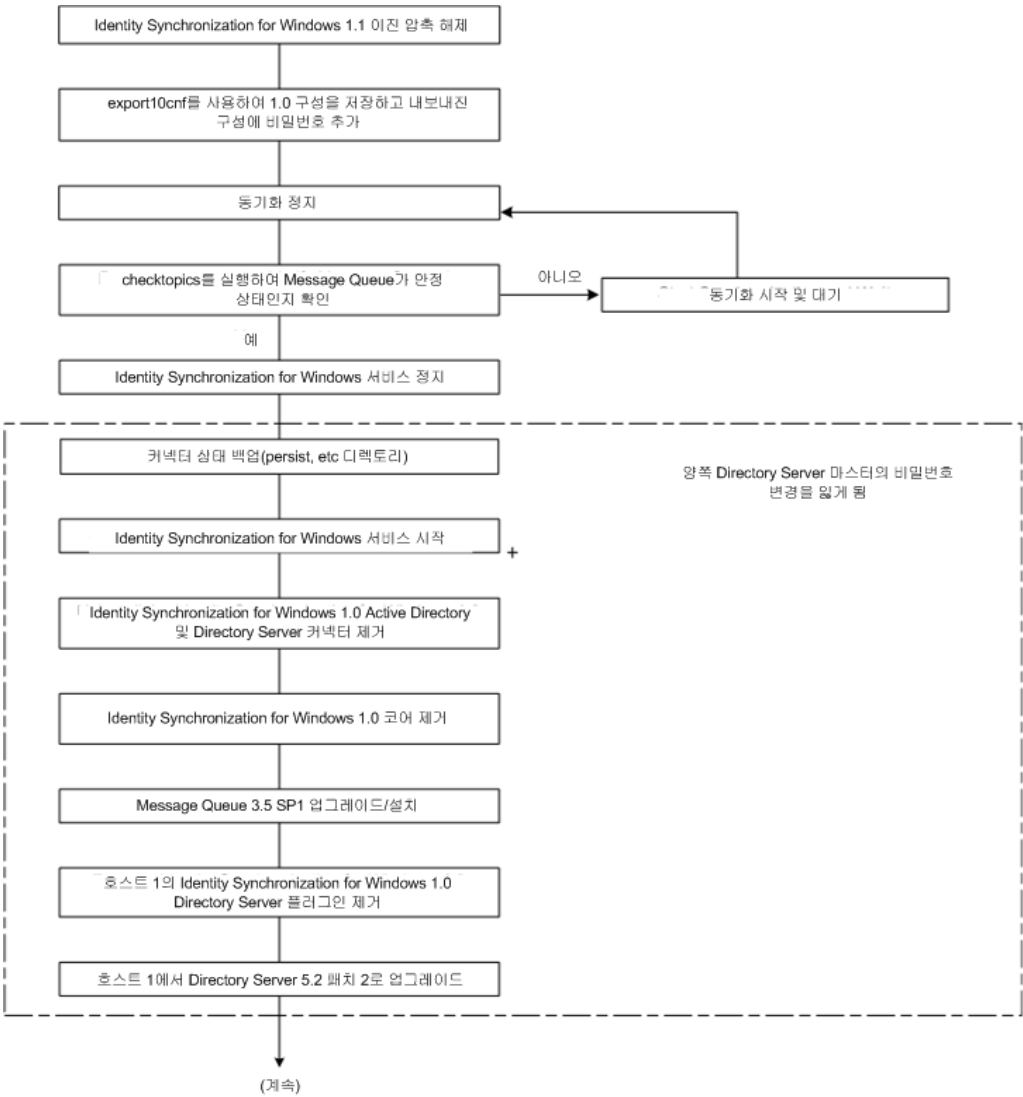
호스트 1	호스트 2
동기화된 사용자용 보조 마스터로서의 Directory Server(인스턴스 1 개)	동기화된 사용자용 기본 마스터로서의 Directory Server(인스턴스 1 개)
코어 (Message Queue, 중앙 기록기, 시스템 관리자 및 콘솔)	Directory Server 플러그인
Active Directory 커넥터	
Directory Server 커넥터	
Directory Server 플러그인	

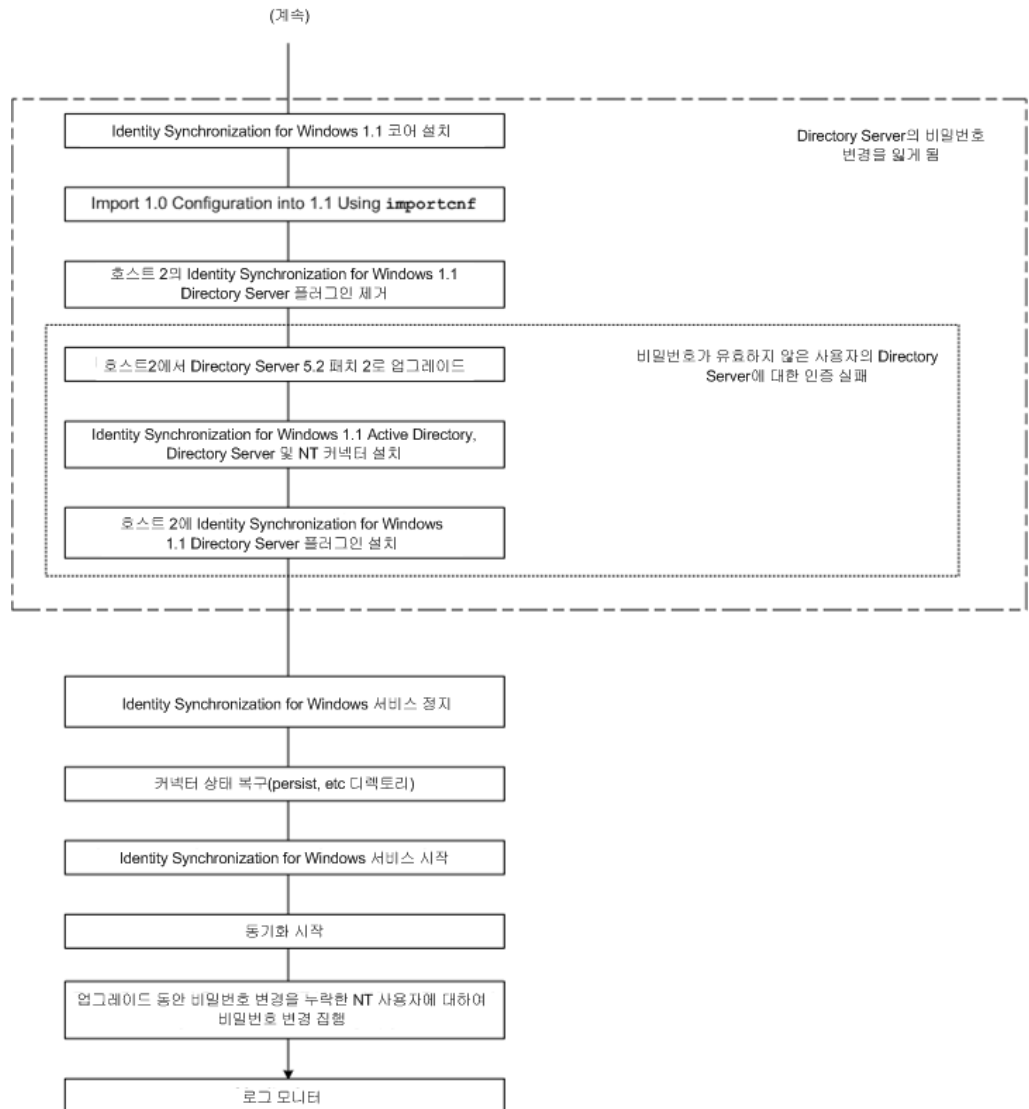
이전 프로세스는 기본 마스터 또는 보조 마스터에서 요청시 비밀번호 동기화가 계속 실행되도록 유지합니다.

참고	두 호스트가 모두 Solaris 운영 체제에서 실행되는 경우 Active Directory 가 있는 Windows 2000 에서 실행되는 세 번째 호스트는 동기화의 용도로만 필요합니다. (세 번째 호스트에 설치되는 구성요소는 없습니다.)
-----------	--

MMR 구현에서 Identity Synchronization for Windows 를 이전하는 프로세스는 다음 그림에 보이는 것과 같습니다.

그림 7-2) MMR(Multi-Master Replication) 구현 이전





Windows NT 를 포함하는 복수 호스트 구현

이 구현 시나리오에는 세 개의 호스트가 사용됩니다.

- Windows NT 시스템

- 동기화된 사용자가 있는 Directory Server 와 Directory Server 커넥터용 호스트
- 기타 모든 구성요소용 호스트

세 호스트 사이에서 Identity Synchronization for Windows 구성요소가 배포되는 방식은 에 보이는 것과 같습니다 .

표 7-3) 복수 호스트 구현

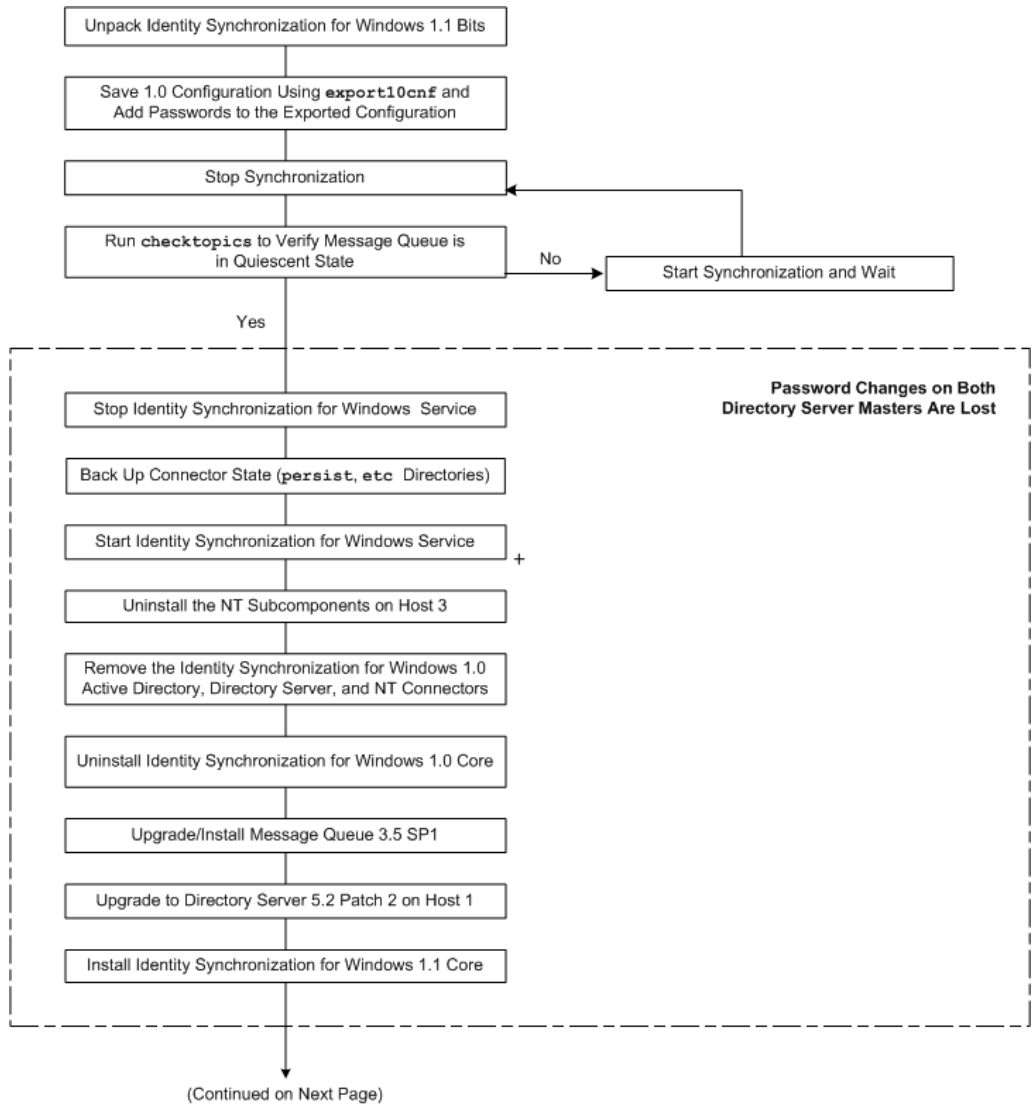
호스트 1	호스트 2	호스트 3
구성 저장고가 있는 Directory Server	동기화된 사용자용 Directory Server	Windows NT 커넥터
코어 (Message Queue, 중앙 기록기 , 시스템 관리자 및 콘솔)	Directory Server 커넥터	Windows NT 하위 구성요소 (비밀번호 필터 DLL 및 변경 검출기 서비스)
Active Directory 커넥터	Directory Server 플러그인	

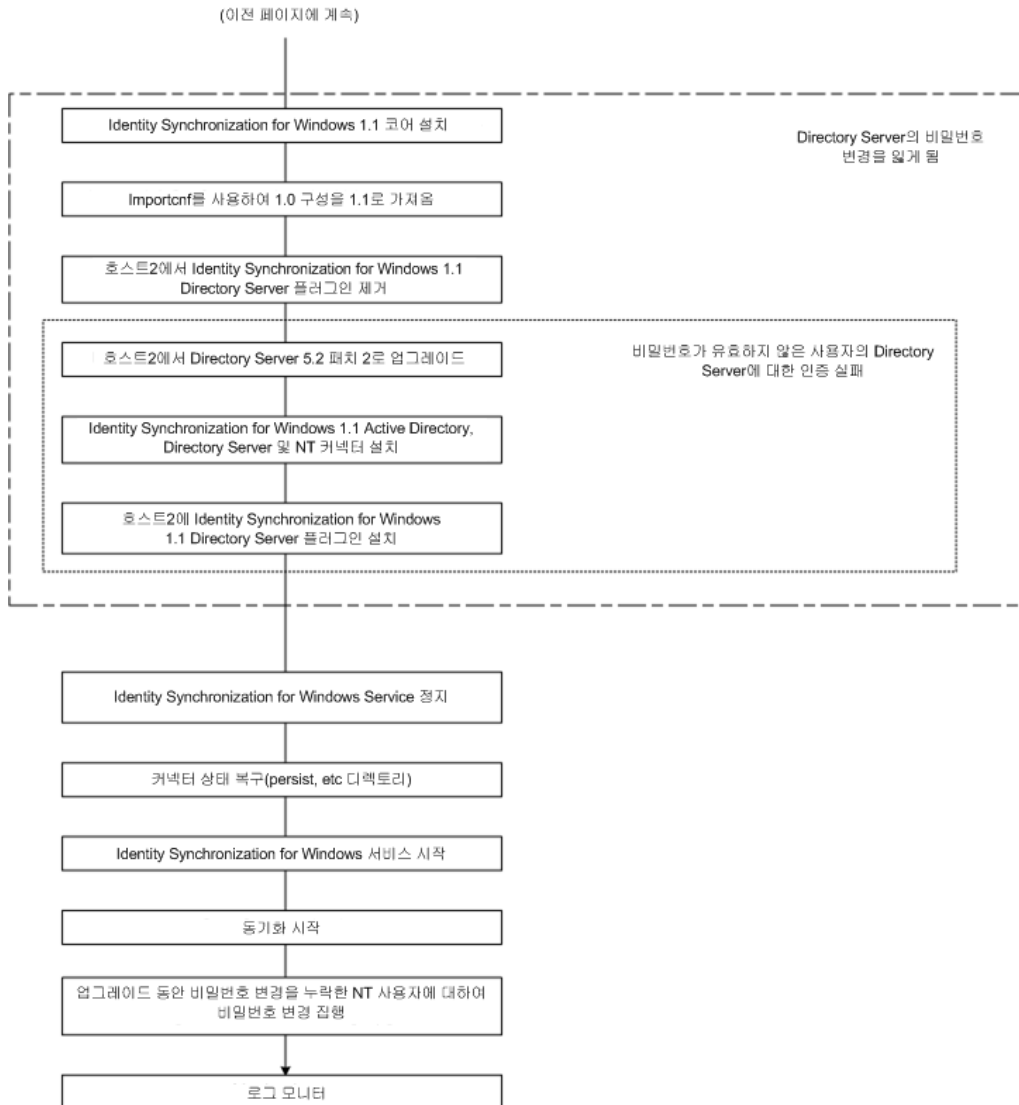
이전 시나리오와 같이 호스트 1 과 2 는 동일한 운영 체제에서 실행됩니다 .

참고	두 호스트가 모두 Solaris 운영 체제에서 실행되는 경우 Active Directory 가 있는 Windows 2000 에서 실행되는 네 번째 호스트는 동기화의 용도로만 필요합니다 . (네 번째 호스트에 설치되는 구성요소는 없습니다 .)
-----------	--

복수 호스트 구현용 Identity Synchronization for Windows 이전 프로세스는 에 보이는 것과 같습니다 .

그림 7-3) Windows NT 를 포함하는 복수 호스트 마이그레이션





로그 확인

버전 1 2004Q3 으로 이전한 후 중앙 감사 로그에서 문제가 있는지 확인합니다. 특히 비밀번호가 변경된 **Directory Server** 사용자는 이전 과정 동안 누락될 수 있으며 따라서 다음과 같은 메시지가 표시됩니다.

```
[16/Apr/2004:14:23:41.029 -0500] WARNING    14  CNN101
```

```
ds-connector-host.example.com "Unable to obtain password of user  
cn=JohnSmith,ou=people,dc=example,dc=com, because the password was encoded  
by a previous installation of Identity Synchronization for Windows  
Directory Server Plugin. The password of this user cannot be synchronized at  
this time. Update the password of this user again in the Directory Server."
```

이 로그 메시지는 Identity Synchronization for Windows 1 2004Q3 에서 동기화를 시작할 때까지 확인할 수 없으므로 로그를 확인하는 작업은 이전 절차의 마지막 단계에서 수행합니다.

로그 확인

소프트웨어 제거

여기에서는 Identity Synchronization for Windows 를 제거하는 절차가 있으며 , 다음 단원으로 구성됩니다 .

- " 제거 계획 " 페이지 231
- " 소프트웨어 제거 " 페이지 232
- " 콘솔 수동 제거 " 페이지 238

제거 계획

소프트웨어를 제거하기 전에 다음 사항에 유의해야 합니다 .

참고	반드시 제품 구성요소와 하위 구성요소를 제거하는 방법을 <i>정확히</i> 따라야 하며 모든 구성요소를 성공적으로 제거했는지 확인해야 합니다 .
-----------	--

- 반드시 관련 커넥터를 제거하기 전에 하위 구성요소와 Directory Server 플러그인을 제거해야 하며 코어를 제거하기 전에 모든 커넥터를 제거해야 합니다 . (Active Directory 커넥터에는 제거할 하위 구성요소가 없습니다 .)
이들 구성요소 중 하나라도 순서에 맞추어 제거하지 않는 경우 다른 구성요소를 선택하고 제거할 수 없게 됩니다 . 예를 들어 커넥터를 먼저 제거하지 않으면 코어를 선택하여 제거할 수 없습니다 .
- 코어를 제거하기 전에 반드시 Directory Server 플러그인을 제거해야 합니다 .
cn=pswsync,cn=plugins,cn=config 를 직접 제거하지 않는 한 , 코어를 먼저 제거하면 Directory Server 에 등록된 플러그인 비트를 해제하지 않은 채 삭제하게 되므로 Directory Server 가 시작할 수 없게 됩니다 .

- 복제본 (기본 및 보조 서버에 추가) 이 있는 복제 환경에서 반드시 Directory Server 플러그인을 제거한 후 서버를 다시 시작해야 합니다 .
- 커넥터를 제거하는 순서는 상관 없습니다 .
- Sun Java 시스템 Directory Server 또는 Windows NT 커넥터를 제거한 후, 반드시 커넥터를 다른 컴퓨터에 다시 설치하는 추가 단계를 수행하거나 다른 서버 포트를 사용해야 합니다 .

이 경우 반드시 해당 하위 구성요소를 제거한 후 다시 설치해야 하며 , 또한 코어가 설치된 위치의 Identity Synchronization for Windows 데몬 / 서비스를 다시 시작해야 합니다 (" 서비스 시작 및 정지 " 페이지 183 참조) .

- 절대로 모든 시스템에서 커넥터와 하위 구성요소를 모두 제거하지 않은 상태에서 코어를 제거하면 안 됩니다 .
- Windows 2000 및 NT 플랫폼에서 반드시 `uninstall.cmd` 스크립트 (`isw-<hostname>` 디렉토리에 위치) 를 실행해야 합니다 . (이 배치 파일은 Administrator 로 실행해야 합니다 .)
- Solaris 운영 체제에서 반드시 `Uninstall.sh` 스크립트 (설치 디렉토리 `/opt/SUNWisw`에 위치) 를 실행해야 합니다 . (이 스크립트는 루트로 실행해야 합니다 .)

소프트웨어 제거

시스템에 다음 Identity Synchronization for Windows 구성요소의 전체 또는 일부분이 있을 수 있습니다 .

- Active Directory 커넥터
- Directory Server 커넥터 및 플러그인
- 코어

Windows NT 시스템에 Windows NT 커넥터 및 하위 구성요소가 포함되었을 수 있습니다 .

`runUninstaller.sh`(Solaris) 또는 `uninstall.cmd`(Windows) 를 사용하여 커넥터와 하위 구성요소를 모두 제거한 뒤 코어 (설치된 경우) 를 제거하십시오 .

여기에서는 다음에 대하여 설명합니다 .

- [Directory Server 플러그인 제거](#)
- [커넥터 제거](#)

- [코어 제거](#)

Directory Server 플러그인 제거

참고

- 제거 프로그램은 Identity Synchronization for Windows Directory Server 플러그인만 제거합니다. 이 제거 프로그램을 사용하여 다른 Directory Server 플러그인을 제거할 수 없습니다.

(따로 명시하지 않는 한) 이 설명서에서 *Directory Server 플러그인*이란 Identity Synchronization for Windows Directory Server 플러그인을 의미합니다.

- 텍스트 기반 모드에서 제거 프로그램을 실행하려면 (Solaris에만 적용) 다음을 입력합니다.

```
./runUninstaller.sh -nodisplay
```

이 프로그램을 실행하면 Identity Synchronization for Windows가 자동으로 암호를 마스킹하여 해당 암호가 해독된 상태에서 반환되지 않도록 합니다.

다음과 같이 Identity Synchronization for Windows Directory Server 플러그인을 설치합니다.

1. 제거 프로그램 (Solaris의 경우 runUninstaller.sh 또는 Windows의 경우 uninstall.cmd)을 시작합니다.
제거 프로그램은 설치 디렉토리 (기본 디렉토리는 /opt/SUNWisdw)에 있습니다.
2. 시작 화면에서 다음을 누릅니다.
3. 구성 디렉토리 호스트 이름과 포트 번호를 입력합니다.
 - 구성 디렉토리의 루트 접미어를 선택합니다. (필요한 경우 새로 고침을 눌러 접미어 목록을 확인합니다.)
 - 제거 프로그램과 구성 Directory Server 사이의 안전한 통신을 위하여 보안 포트 선택란을 선택하고 Directory Server의 SSL 포트 번호를 지정합니다.
4. 구성 디렉토리의 관리자 이름과 비밀번호를 입력합니다.
5. Directory Server 플러그인 제거 옵션을 선택합니다.
6. Directory Server 호스트 이름, 포트 및 관리자의 자격증명 (이름 및 비밀번호)를 입력합니다.

7. 다음을 눌러 제거 관련 작업을 계속합니다.
8. 프롬프트가 표시되면 플러그인이 설치된 위치의 Directory Server를 다시 시작합니다.
9. 요약 창이 표시됩니다. 이 창에 표시된 설명을 따라 하십시오.
 - **Solaris 시스템**: 제거 로그는 /var/sadm/install/logs/에 기록됩니다.
 - **Windows 시스템**: 제거 로그는 %TEMP% 디렉토리에 기록되며, 이 디렉토리는 다음 폴더 아래에 있는 Local Settings 폴더의 하위 디렉토리입니다.

C:\Documents and Settings\Administrator

참고

일부 Windows 시스템 (Windows 2000 Advanced Server 등)의 경우 Local Settings 폴더가 숨겨져 있습니다.

이 폴더와 Temp 하위 디렉토리를 보려면 다음과 같이 합니다.

Windows 탐색기를 열고 메뉴 줄에서 도구 > 폴더 옵션을 선택합니다. 폴더 옵션 대화 상자가 표시되면 보기 탭을 누르고 숨긴 파일 표시 옵션을 선택합니다.

단기를 눌러 프로그램을 종료합니다.

10. Directory Server 플러그인이 대상 호스트에 설치된 *유일한* Identity Synchronization for Windows 구성요소인 경우 isw-hostname 폴더를 삭제할 수 있습니다.
11. 네트워크의 Windows 2000에 설치된 각 Directory Server 플러그인에 대하여 [단계 1](#)에서 [단계 9](#)까지의 단계를 반복합니다.

커넥터 제거

커넥터를 제거하려면 다음과 같이 합니다.

1. 제거 프로그램 (Solaris의 경우 runUninstaller.sh 또는 Windows의 경우 uninstall.cmd)을 시작합니다.
이 프로그램은 설치 디렉토리 (기본 디렉토리는 /opt/SUNWisw)에 있습니다.
2. 시작 화면에서 다음을 누릅니다.
3. 구성 디렉토리 호스트 이름과 포트 번호를 입력합니다.

- 구성 디렉토리의 루트 접미어를 선택합니다. (필요한 경우 새로 고침을 눌러 접미어 목록을 확인합니다.)
 - 제거 프로그램과 구성 Directory Server 사이의 안전한 통신을 위하여 보안 포트 선택란을 선택하고 Directory Server의 SSL 포트 번호를 지정합니다.
4. 구성 디렉토리용 관리자 이름과 비밀번호를 입력합니다.
 5. 제거할 커넥터를 선택합니다.

참고

선택한 커넥터는 반드시 대상 호스트에 존재해야 합니다.

6. 다음을 눌러 제거 관련 작업을 계속합니다.
7. 요약 창이 표시됩니다. 이 창에 표시된 설명을 따라 하십시오.
 - **Solaris 시스템**: 제거 로그는 /var/sadm/install/logs/에 기록됩니다.
 - **Windows 시스템**: 제거 로그는 %TEMP% 디렉토리에 기록되며, 이 디렉토리는 다음 폴더 아래에 있는 Local Settings 폴더의 하위 디렉토리입니다.

C:\Documents and Settings\Administrator

참고

일부 Windows 시스템 (Windows 2000 Advanced Server 등)의 경우 Local Settings 폴더가 숨겨져 있습니다. 이 폴더와 Temp 하위 디렉토리를 보려면 다음과 같이 합니다.

Windows 탐색기를 열고 메뉴 줄에서 도구 > 폴더 옵션을 선택합니다. 폴더 옵션 대화 상자가 표시되면 보기 탭을 누르고 숨긴 파일 표시 옵션을 선택합니다.

8. 단기를 눌러 프로그램을 종료합니다.
9. 대상 호스트에 다른 커넥터가 설치되지 않은 경우 안전하게 isw-*<hostname>* 폴더를 제거할 수 있습니다.
10. 커넥터가 설치된 모든 호스트에 대하여 단계 1에서 단계 7까지의 단계를 반복합니다.

코어 제거

참고 코어를 제거하기 전에 반드시 Directory Server 플러그인을 제거해야 합니다.

cn=pswsync,cn=plugins,cn=config를 직접 제거하지 않는 한 플러그인보다 코어를 먼저 제거하면 Directory Server에 등록된 플러그인 비트를 해제하지 않은 채 삭제하게 되므로 Directory Server가 시작할 수 없게 됩니다.

다음과 같이 코어를 제거합니다.

1. 제거 프로그램을 시작합니다.
 - **Windows** 컴퓨터 :
 - I. 시작을 누른 후 설정 > 제어판을 선택합니다.
 - II. 프로그램 추가/제거를 두 번 누릅니다.
 - III. 프로그램 추가/제거 창에서 Identity Synchronization for Windows를 선택한 후 제거를 누릅니다.
 - **Solaris 또는 Windows** 컴퓨터에서, Solaris의 경우 runUninstaller.sh 또는 Windows의 경우 uninstall.cmd를 실행합니다.

이 프로그램은 설치 디렉토리 (기본 디렉토리는 /opt/SUNWiwsw)에 있습니다.
2. 시작 화면에서 다음을 누릅니다.
3. 구성 디렉토리 호스트 이름과 포트 번호를 입력합니다.
 - 구성 디렉토리의 루트 접미어를 선택합니다. (필요한 경우 새로 고침을 눌러 접미어 목록을 확인합니다.)
 - 제거 프로그램과 구성 Directory Server 사이의 안전한 통신을 위하여 보안 포트 선택란을 선택하고 Directory Server의 SSL 포트 번호를 지정합니다.
4. 구성 디렉토리용 관리자 이름과 비밀번호를 입력합니다.
5. 제거할 코어를 선택하고 다음을 누릅니다.
6. 구성 디렉토리 URL을 입력하고 Refresh를 누른 후, 드롭다운 목록에서 해당 루트 접미어를 선택합니다.
7. 다음을 눌러 제거 관련 작업을 계속합니다.

8. 요약 창이 표시됩니다. 이 창에 표시된 설명을 따라 하십시오.
- **Solaris 시스템**: 제거 로그는 /var/sadm/install/logs/ 에 기록됩니다.
 - **Windows 시스템**: 제거 로그는 %TEMP% 디렉토리에 기록되며, 이 디렉토리는 다음 폴더 아래에 있는 Local Settings 폴더의 하위 디렉토리입니다.

C:\Documents and Settings\Administrator

참고

일부 Windows 시스템 (Windows 2000 Advanced Server 등) 의 경우 Local Settings 폴더가 숨겨져 있습니다.

이 폴더와 Temp 하위 디렉토리를 보려면 다음과 같이 합니다.

Windows 탐색기를 열고 메뉴 줄에서 도구 > 폴더 옵션을 선택합니다. 폴더 옵션 대화 상자가 표시되면 보기 탭을 누르고 숨긴 파일 표시 옵션을 선택합니다.

9. 단기를 눌러 프로그램을 종료합니다.

참고

어떤 이유이든 해당 커넥터용 커넥터 제거 프로그램을 실행할 수 없는 경우 (하드 드라이브 이상시 커넥터 파일이 손실되는 등) `idsync resetconn` 하위 명령을 실행합니다 ("[resetconn 사용](#)" [페이지 315](#) 참조).

이 명령을 사용하면 구성 디렉토리의 커넥터 상태를 *uninstalled* 로 재설정하므로 다른 위치에서 해당 커넥터를 다시 설치할 수 있습니다. `resetconn` 하위 명령은 구성 디렉토리에 액세스하는 다른 명령과 유사하며, 두 가지 옵션이 제공됩니다.

- **-e <dir-source>**: 재설정할 디렉토리 소스의 이름을 지정합니다. (설치 프로그램에서 커넥터는 디렉토리 소스 이름으로 구분됩니다.)
- **-n** (안전모드): 수행하는 작업 없이 명령에 지정된 인수가 올바른지 표시합니다.

명령 예제:

```
idsync resetconn -D "cn=Directory Manager" -w [-h CR-hostname]
[-p 389] [-s dc=example,dc=sun,dc=com] -q [-Z] [-P "cert8.db"]
[-m "secmod.db"] -e "dc=central,dc=example,dc=com" [-n]
```

`resetconn` Output:

참고: This program will reset the installation state to UNINSTALLED for the Connector associated with the specified DirectorySource "dc=central,dc=example,dc=com".

Changing the Connector to an UNINSTALLED state is a last resort. This is NOT meant to be used for uninstalling connectors. It is typically used if you lost a machine with the connector on it and can not run the uninstaller. Additionally, this program will rewrite the existing configuration. This can be a lengthy process. Before proceeding, you should stop the Console, any running installers, and all other system processes. You may want to export the ou=Services tree in the configuration directory to ldif as a backup.

Do you want to reset the installer settings for the connector (y/n)?

콘솔 수동 제거

기타 Identity Synchronization for Windows 구성요소를 모두 제거한 후 콘솔을 수동으로 제거해야 합니다.

Solaris 시스템

Solaris 시스템에서 콘솔을 제거하려면 다음과 같이 합니다.

1. 구성 디렉토리에서 다음 하위 트리를 삭제합니다.

```
cn=Sun Java (TM) System Identity Synchronization for  
Windows,cn=<server_group>,cn=<hostname>, ou=<domain_name>, o=netscaperoot
```

2. 모든 콘솔 설치에 대하여 다음 디렉토리에서 접두어가 *isw* 인 모든 .jar 파일을 제거합니다.

```
<serverroot></server>/java/jars
```

Windows 시스템

Windows Active Directory 또는 NT 시스템에서 콘솔을 제거하려면 다음과 같이 합니다.

1. 구성 디렉토리에서 다음 하위 트리를 삭제합니다.

```
cn=Sun Java (TM) System Identity Synchronization for  
Windows,cn=<server_group>,cn=<hostname>, ou=<domain_name>, o=netscaperoot
```

2. 모든 콘솔 설치에 대하여 다음 디렉토리에서 접두어가 *isw* 인 모든 .jar 파일을 제거합니다.

```
<serverroot></server>/java/jars
```


문제해결

이 장에서는 Identity Synchronization for Windows 를 사용하는 동안 발생할 수 있는 문제를 해결하는 데 도움이 되는 내용을 제공합니다. 다음과 같은 내용으로 구성됩니다.

- " 문제해결 점검 목록 " 페이지 242
- " 커넥터 문제 해결 " 페이지 245
- " 구성요소 문제해결 " 페이지 249
- " 하위 구성요소 문제 해결 " 페이지 252
- "Message Queue 문제 해결 " 페이지 254
- "SSL 문제 해결 " 페이지 257
- " 제어기 문제 해결 " 페이지 262

문제해결 점검 목록

참고 관리자 : 문제를 디버깅할 때 로깅 수준 ("[로그 파일 구성](#)" [페이지 269](#)에서 설명)을 조정하여 로그에 문제의 원인이 될 수 있는 모든 이벤트가 반영되도록 합니다.

로그 수준을 FINE 이상으로 조정하지 않으면 일부 이벤트 (사용자가 SUL에 포함되지 않아 사용자 변경 내용을 동기화 할 수 없는 등)는 로그 파일에 포함되지 않습니다. 모든 idsync resync 작업 동안 로그 수준은 INFO로 유지되어야 합니다.

Identity Synchronization for Windows를 설치 및 구성하는 동안 idsync printstat 명령을 유용한 도구로 사용할 수 있습니다. printstat("[printstat 사용](#)" [페이지 314](#) 참조)를 실행하면 설치 및 구성 과정을 완료하기 위하여 수행해야 하는 나머지 단계 목록이 표시됩니다.

1. 중앙 error.log에 보고된 문제가 있습니까?

```
isw-<hostname>/logs/central/error.log
```

중앙 오류 로그 파일에 거의 모든 오류가 보고됩니다. 또한 오류에 대한 추가 정보는 보통 audit.log 파일에 있습니다. 관련 로그 항목의 상호 관계를 쉽게 하기 위하여 audit.log 파일에 또한 오류 로그의 모든 항목이 포함됩니다.

2. 릴리스 노트에 많은 알려진 문제가 있습니다. 여기에 문제가 설명되어 있습니까?

3. 설치가 초기화된 컴퓨터에 수행되었습니까? 이전 구성의 제거가 완료되지 않은 상태에서 제품을 다시 설치할 때 문제가 발생할 수 있습니다. 이전 설치를 완전히 제거하는 방법은 [제 8 장](#), "[소프트웨어 제거](#)"를 참조하십시오.

4. 코어가 적절히 설치되었습니까? 코어 설치가 성공적으로 완료되면 isw-<hostname>/logs/central/ 디렉토리에 로그 파일이 만들어집니다.

5. 자원 구성 동안 Directory Server가 실행되었습니까?

6. Message Queue와 시스템 관리자를 포함하여 코어가 현재 실행 중입니까? Windows의 경우 적절한 서비스 이름을 확인합니다. Solaris의 경우 적절한 데몬 이름을 확인합니다. idsync printstat 명령을 사용하여 Message Queue와 시스템 관리자가 작동 중인지 확인합니다.

7. 구성이 성공적으로 저장되었습니까? idsync printstat 명령에서 커넥터 목록이 만들어지면 구성이 성공적으로 저장된 것입니다.

8. 커넥터가 모두 설치되었습니까? 동기화되는 각 디렉토리 소스마다 하나의 커넥터가 반드시 설치되어야 합니다.
9. 하위 구성요소가 모두 설치되었습니까? 커넥터가 설치된 후 Directory Server 와 Windows NT 커넥터에 하위 구성요소가 설치되어야 합니다. Directory Server 플러그인은 반드시 각 Directory Server 복제본에 설치되어야 합니다.
10. 설치 후 절차를 수행했습니까? Directory Server 플러그인을 설치한 후 반드시 Directory Server 를 다시 시작해야 합니다. Windows NT 하위 구성요소를 설치한 후 반드시 Windows 기본 도메인 제어를 다시 시작해야 합니다.
11. 콘솔이나 명령줄에서 동기화가 시작되었습니까?
12. 모든 커넥터가 현재 실행 중입니까?
13. 콘솔 또는 `idsync printstat` 를 사용하여 모든 커넥터의 상태가 SYNCING 인지 확인합니다.
14. 동기화되는 디렉토리 소스가 현재 실행 중입니까?
15. 콘솔을 사용하여 수정 및 작성 내용이 예측한 방향으로 동기화되는지 확인합니다.
16. 오직 하나의 디렉토리 소스에만 존재하는 사용자를 동기화하는 경우 `idsync resync` 명령을 사용하여 다른 디렉토리 소스에서 해당 사용자가 만들어졌습니까?

참고

기존 사용자가 있는 경우 반드시 항상 `idsync resync` 를 실행해야 합니다. 기존 사용자를 재동기화하지 않는 경우 재동기화 작동은 정의되지 않은 채 유지됩니다.

17. 두 디렉토리 소스 모두에 있는 사용자를 동기화하는 경우 `idsync resync` 명령을 사용하여 해당 사용자를 연결했습니까?
18. Active Directory 또는 Windows NT 에서 Sun Java System Directory Server 로 사용자를 만들 수 없는 경우 Directory Server objectclass 의 모든 필수 속성이 생성 속성으로 지정되었으며 원래 사용자 항목에 해당 속성의 값이 있는지 확인하십시오.
19. 동기화가 Directory Server 에서 Windows NT 로 작성하며 사용자가 만들어졌으나 계정을 사용할 수 없는 경우, 사용자 이름이 Windows NT 요구 사항을 위반하지 않는지 확인하십시오.

예를 들어 Windows NT 에서 허용하는 최대 길이보다 긴 사용자 이름을 지정하는 경우 NT 에 사용자가 만들어지지만 이름을 변경 (사용자 > 이름 변경) 할 때까지 이 사용자를 사용하거나 편집할 수 없습니다.

20. Windows NT SAM 변경 감지기 하위 구성요소를 사용하려면 반드시 NT 감사 로그를 작동해야 합니다. 시작 > 프로그램 > 관리 도구 > 사용자 관리자를 선택한 후 정책 > 감사 정책을 선택합니다.
이 이벤트 감사를 선택하고 사용자 및 그룹 관리용 성공 및 실패 선택란을 모두 선택합니다.

이벤트 뷰어 > Event Log Wrapping 에서 Event Log Settings 를 선택한 후 Overwrite Events as Needed 를 선택합니다.
21. 동기화에 실패한 사용자가 Synchronization User List 에 있습니까? 예를 들어 동기화 사용자 목록의 기본 DN 과 필터가 일치합니까? Active Directory 가 포함된 구현에서 Sun Java System Directory Server 항목이 사용자 동기화 목록에 없으면 요청시 비밀번호 동기화가 아무런 표시 없이 실패합니다. 이는 대부분 Synchronization User List 가 잘못되었기 때문에 발생합니다.
22. 동기화 설정이 변경되었습니까? 동기화 설정이 Active Directory 에서 Sun Java System 디렉토리 서버로 사용자를 동기화시키는 것에서 디렉토리 서버에서 Active Directory 로 사용자를 동기화시키는 것으로만 변경된 경우 Active Directory SSL CA 인증서가 반드시 커넥터의 데이터베이스에 추가되어야 합니다. idsync certinfo 명령은 현재 SSL 설정에 따라 설치되어야 하는 SSL 인증서를 보고합니다.
23. 모든 호스트 이름이 적절히 지정되었으며 DNS에서 변환할 수 있습니까? Active Directory 도메인 제어기는 Active Directory 커넥터가 실행되는 컴퓨터와 Sun Java System Directory Server 플러그인이 실행되는 컴퓨터에서 DNS 변환할 수 있어야 합니다.
24. Active Directory 도메인 제어기의 IP 주소가 커넥터가 이 제어기에 연결하는 데 사용하는 동일한 이름으로 변환됩니까?
25. 소스 커넥터가 사용자에 대한 변경 내용을 찾습니까? 중앙 audit.log 를 사용하여 사용자가 추가 또는 수정되는 디렉토리 소스용 커넥터가 수정 내용을 찾는지 확인합니다.
26. 대상 커넥터가 이 수정 내용을 처리합니까?
27. 복수 Synchronization User List 가 구성되었습니까? 구성된 경우 충돌이 있습니까? 더욱 구체적인 Synchronization User List 가 덜 구체적인 Synchronization User List 보다 먼저 콘솔을 사용하도록 순서를 정해야 합니다.
28. 흐름이 양방향 또는 Sun 에서 Windows 로 설정되었으며 구현에 Active Directory 데이터 소스가 있는 경우 커넥터가 SSL 통신을 사용하도록 구성되었습니까?

29. Solaris 환경에서 메모리 문제가 의심되는 경우 프로세스를 확인합니다. 다른 프로세스로 실행되는 구성요소를 보려면 다음을 입력합니다.

```
/usr/ucb/ps -gauxwww | grep com.sun.directory.wps
```

출력에 커넥터의 ID, 시스템 관리자 및 중앙 기록기를 포함하여 자세한 내용이 모두 제공됩니다. 이는 과도한 메모리를 소모하는 프로세스가 있는 경우 유용합니다.

30. Sun Java System 디렉토리 소스를 만들거나 편집하고 Directory Server에 Choose a known server 드롭다운 목록이 표시되지 않는 경우 Directory Server 가 실행되는지 확인하십시오. Directory Server 가 사용 가능한 호스트의 드롭다운 목록에 표시되려면 반드시 실행 중이어야 합니다.

문제의 서버가 일시적으로 정지된 경우 Specify a server 의 호스트 이름과 포트 필드에 호스트와 포트를 입력합니다.

참고

Identity Synchronization for Windows 는 기본적으로 짧은 호스트 이름을 사용하지만 구성에 따라 기본 호스트 이름을 사용하지 못할 수 있습니다. 호스트 이름을 입력해야 하는 경우 항상 정규화된 이름을 사용하는 것이 좋습니다.

31. 제거 프로그램을 실행할 때 다음 오류가 표시됩니까?

```
./runInstaller.sh
IOException while making /tmp/SolarisNativeToolkit_5.5.1_1 executable:java.io.IOException:
Not enough space
java.io.IOException: Not enough space
```

/tmp 에 있는 스왑 파일의 크기를 늘립니다.

커넥터 문제 해결

이 부분의 내용을 사용하여 커넥터 문제를 해결하십시오. 다음과 같은 내용으로 구성됩니다.

- "디렉토리 소스를 관리하는 커넥터의 ID 를 확인하는 방법" 페이지 246
- "커넥터의 현재 상태 확인 방법" 페이지 247

디렉토리 소스를 관리하는 커넥터의 ID 를 확인하는 방법

다음 방법 중 한 가지를 사용하여 커넥터 ID 를 확인합니다 .

- " 중앙 로그 사용 "
- "idsync printstat 사용 "

중앙 로그 사용

중앙 audit.log 에서 동기화되는 디렉토리 소스의 커넥터 ID 를 확인합니다 . 시작 시에 중앙 기록기는 각 커넥터의 ID 와 커넥터가 관리하는 디렉토리 소스를 기록합니다 . 가장 최근 정보는 시작 배너의 마지막 인스턴스를 확인합니다 .

예를 들어 다음 로그 메시지에는 두 개의 커넥터가 있습니다 .

- **CNN101** is a Sun Directory Connector that manages dc=airius,dc=com
- **CNN100** is an Active Directory Connector that manages the airius.com domain

```
[2003/03/19 00:00:00.722 -0600] INFO 16 "System Component Information: SysMgr_100 is the system manager (CORE); console is the Product Console User Interface; CNN101 is the connector that manages [dc=airius,dc=com (ldap://host1.airius.com:389)]; CNN100 is the connector that manages [airius.com (ldaps://host2.airius.com:636)];"
```

idsync printstat 사용

idsync printstat 명령에서 또한 커넥터 ID 와 상태를 알 수 있습니다 ("[printstat 사용](#)" [페이지 314](#) 참조).

이 명령의 출력 예는 다음과 같습니다 .

```
Connector ID: CNN100
Type: Active Directory
Manages: airius.com (ldaps://host2.airius.com:636)
State: READY
```



```
Connector ID: CNN101
Type: Sun Java System Directory
Manages: dc=airius,dc=com (ldap://host1.airius.com:389)
State: READY
```

Sun Java System Message Queue Status: Started

Sun Java System Message Queue 를 통하여 System Manager 확인 .

System Manager Status: Started

SUCCESS

커넥터의 현재 상태 확인 방법

콘솔의 Status 창 , idsync printstat 명령 (앞의 설명 참조) 또는 중앙 audit.log 를 사용하여 동기화에 연관된 커넥터의 현재 상태를 확인할 수 있습니다 .

audit.log 의 마지막 메시지에서 커넥터 상태에 대한 보고를 찾습니다 .
예를 들어 다음 로그 메시지에서 커넥터 CNN101 의 상태는 READY 입니다 .

```
[2003/03/19 10:20:16.889 -0600] INFO 13 SysMgr_100 host1 "Connector [CNN101] is now in
state "READY"."
```

에서는 다양한 커넥터 상태를 설명합니다 .

표 9-1) 커넥터 상태 설명

상태	의미
UNINSTALLED	커넥터가 설치되지 않았습니다 .
INSTALLED	커넥터가 설치되었으나 구성을 수신하지 않았습니다 .
READY	커넥터가 설치되었으며 구성을 수신했으나 동기화를 시작하지 않았습니다 .
SYNCING	커넥터가 설치되고 구성을 수신했으며 동기화를 시작하려 합니다 .

커넥터의 상태가 UNINSTALLED 인 경우의 작업

커넥터를 설치합니다.

커넥터 설치가 실패했으나 다시 설치할 수 없는 경우의 작업

커넥터 상태가 실패했으나 Identity Synchronization for Windows 설치 프로그램은 커넥터가 설치된 것으로 간주하는 경우 설치 프로그램으로 해당 커넥터를 다시 설치할 수 없습니다.

idsync resetconn을 실행하여 ("[resetconn 사용](#)" [페이지 315](#)에서 설명) 커넥터의 상태를 UNINSTALLED 로 재설정한 후 커넥터를 다시 설치합니다.

커넥터의 상태가 INSTALLED 인 경우의 작업

오랫동안 커넥터의 상태가 설치된 상태로 유지되는 경우 대부분 실행되지 않거나 Message Queue 와 통신할 수 없게 됩니다.

커넥터가 설치된 컴퓨터에서 커넥터의 로그 (audit.log 및 error.log) 에서 잠재적 오류를 확인합니다. 커넥터가 Message Queue 에 연결되지 않는 경우 여기에 오류가 보고됩니다. 이 경우 가능한 원인은 "[Message Queue 문제 해결](#)" [페이지 254](#) 을 참조하십시오.

감사 로그의 가장 최신 메시지가 오래된 경우 커넥터가 실행되지 않을 수 있습니다. "[구성요소 문제해결](#)" [페이지 249](#) 참조.

커넥터의 상태가 READY 인 경우의 작업

동기화가 시작되고 해당 하위 구성요소가 설치되었으며 커넥터로 연결될 때까지 커넥터의 상태는 READY 로 유지됩니다. 동기화가 시작되지 않았으면 콘솔이나 명령줄 유틸리티를 사용하여 시작합니다.

동기화가 시작되었으나 커넥터의 상태가 SYNCING 로 변경되지 않는 경우 하위 구성요소에 문제가 있을 가능성이 높습니다. "[하위 구성요소 문제 해결](#)" [페이지 252](#) 참조.

커넥터의 상태가 SYNCING 인 경우의 작업

커넥터의 상태가 SYNCING 이지만 수정 내용이 동기화되지 않는 경우 동기화 설정이 올바른지 확인합니다.

- 콘솔을 사용하여 수정 내용 및 작성 내용이 원하는 방향으로 (즉, Windows 에서 Sun Java System Directory Server 로) 동기화되는지 확인합니다.

- 콘솔을 사용하여 수정되는 속성이 동기화된 속성인지 확인합니다. (참고 : 비밀 번호는 항상 동기화됩니다.) 작성된 사용자 항목이 동기화되지 않는 경우 콘솔에서 사용자 작성 흐름을 사용하는지 확인합니다.
- 소스 커넥터가 사용자에게 대한 변경 내용을 찾습니까? 중앙 audit.log 를 사용하여 사용자가 추가 또는 수정되는 디렉토리 소스용 커넥터가 수정 내용을 찾는지 확인합니다. 대상 커넥터가 이 수정 내용을 처리합니까?

Active Directory 커넥터가 SSL 을 통하여 Active Directory 에 연결할 수 없는 경우의 작업

Active Directory 커넥터가 SSL 을 통하여 Active Directory 에 연결할 수 없으며 다음 오류 메시지가 표시되는 경우 AD 도메인 제어를 다시 시작합니다.

Failed to open connection to ldaps://server.example.com:636, error(91): Cannot connect to the LDAP server, reason: SSL_ForceHandshake failed: (-5938) Encountered end of file.

구성요소 문제해결

이 부분의 내용을 사용하여 구성요소 문제를 해결합니다. 다음과 같은 내용으로 구성됩니다.

- ["Solaris" 페이지 249](#)
- ["Windows" 페이지 251](#)
- ["WatchList.properties 검사" 페이지 251](#)

Solaris

/usr/ucb/ps -auxww | grep com.sun.directory.wps 명령을 사용하여 실행되는 Identity Synchronization for Windows 프로세스를 모두 목록으로 만듭니다. 이 표에 실행되어야 하는 프로세스가 표시됩니다.

표 9-2) Identity Synchronization for Windows 프로세스

Java 프로세스 클래스 이름	구성요소	있는 경우
com.sun.directory.wps.watchdog.server.WatchDog	시스템 워치독	항상

표 9-2) Identity Synchronization for Windows 프로세스

com.sun.directory.wps.centrallogger.CentralLoggerManager	중앙 기록기	코어가 설치된 위치만
com.sun.directory.wps.manager.SystemManager	시스템 관리자	코어가 설치된 위치만
com.sun.directory.wps.controller.AgentHarness	커넥터	설치된 커넥터마다 한 개

기대한 수의 프로세스가 실행되지 않는 경우 다음 명령으로 모든 Identity Synchronization for Windows 프로세스를 다시 시작합니다 .

```
# /etc/init.d/isw stop
# /etc/init.d/isw start
```

위치독 프로세스가 실행되지만 기대한 수의 java.exe 프로세스가 실행되지 않는 경우 "WatchList.properties 검사" 부분에서 모든 구성요소가 적절히 설치되었는지 확인합니다 .

다른 시스템 구성요소와 마찬가지로 Sun Java System Directory Server 플러그인은 중앙 기록기가 관리하는 버스를 통하여 로그 기록을 송신하여 사용자가 볼 수 있도록 합니다 . 그러나 플러그인에는 버스를 통하여 표시되지 않는 일부 메시지가 기록됩니다 .(예 : 하위 구성요소가 커넥터에 연결하지 못한 인스턴스) 이 경우 로그 메시지는 파일 시스템에 있는 플러그인의 logs 디렉토리만 표시되며 , 다음과 유사합니다 .

```
<serverroot>/isw-<hostname>/logs/SUBC<id>.
```

플러그인은 Directory Server 프로세스와 함께 실행되므로 플러그인이 자체의 logs 디렉토리에 기록하는 기능에 문제가 있을 수 있습니다 . 이는 Directory Server 가 logs 디렉토리의 소유자가 아닌 다른 사용자로 실행되는 경우 발생합니다 . 이 경우 디렉토리 권한을 변경하거나 원래 운영 체제 명령을 사용하는 사용자로 변경하여 명시적으로 플러그인 권한을 부여해야 할 수 있습니다 .

Windows

서비스 제어판을 사용하여 "Sun Java System Identity Synchronization for Windows" 서비스가 시작되었는지 확인합니다. 시작되지 않았으면 Identity Synchronization for Windows가 컴퓨터에서 실행되지 않는 것이므로 시작해야 합니다. 서비스가 시작되면 작업 관리자를 사용하여 pswatchdog.exe(Watchdog 프로세스)가 실행되지 확인하고 예상된 숫자의 java.exe 프로세스가 실행되는지 확인합니다.

- 코어가 설치된 경우에만 Message Queue 브로커마다 한 개
- 코어가 설치된 경우에만 시스템 관리자 브로커마다 한 개
- 코어가 설치된 경우에만 중앙 기록기 브로커마다 한 개
- 해당 컴퓨터에 설치된 커넥터마다 한 개

참고

Directory Server 콘솔 등 다른 java 프로세스가 사용 중일 수 있습니다. pswatchdog.exe가 실행되지 않는 경우 "Sun Java System Identity Synchronization for Windows" 서비스를 다시 시작합니다. pswatchdog.exe가 실행되지만 기대한 수의 java.exe 프로세스가 실행되지 않는 경우 "[WatchList.properties 검사](#)" [페이지 251](#)에서 모든 구성요소가 적절히 설치되었는지 확인합니다.

WatchList.properties 검사

Identity Synchronization for Windows 구성요소가 설치된 각 컴퓨터에서 isw-<machine_name>/resources/WatchList.properties 파일이 해당 컴퓨터에서 실행되어야 하는 구성요소를 열거합니다. process.name[n] 기본 설정이 실행되어야 하는 구성요소의 이름을 지정합니다.

코어가 설치된 컴퓨터에서 WatchList.properties에 중앙 기록기 및 시스템 관리자용 항목이 포함됩니다.

```
process.name[1]=Central Logger
...
process.name[2]=System Manager
...
```

커넥터가 설치된 컴퓨터에서 `WatchList.properties`에 각 커넥터의 항목이 별도로 포함됩니다. `process.name` 등록 정보는 다음 커넥터 ID입니다.

```
process.name[3]=CNN100
...
process.name[4]=CNN100
...
```

`WatchList.properties`의 항목과 실제로 실행되는 프로세스 사이에 불일치가 있는 경우 Identity Synchronization for Windows 데몬 또는 서비스를 다시 시작합니다.

`WatchList.properties`의 항목이 기대한 수 보다 적은 경우(즉, 커넥터가 둘 설치되었으나 하나만 있는 경우) 설치 로그에서 설치 이상이 없는지 확인합니다.

- **Solaris 시스템**: 설치 로그는 `/var/sadm/install/logs/`에 기록됩니다.
- **Windows 시스템**: 설치 로그는 `%TEMP%` 디렉토리에 기록되며, 이 디렉토리는 다음 폴더 아래에 있는 Local Settings 폴더의 하위 디렉토리입니다.

`C:\Documents and Settings\Administrator`

참고

일부 Windows 시스템 (Windows 2000 Advanced Server 등)의 경우 Local Settings 폴더가 숨겨져 있습니다.

이 폴더와 Temp 하위 디렉토리를 보려면 다음과 같이 합니다.

1. Windows 탐색기를 열고 메뉴 줄에서 도구 > 폴더 옵션을 선택합니다.
2. 폴더 옵션 대화 상자가 표시되면 보기 탭을 누르고 숨긴 파일 표시 옵션을 선택합니다.

하위 구성요소 문제 해결

다음 점검 목록을 사용하여 구현의 하위 구성요소에 대한 문제를 해결합니다.

1. 모든 하위 구성요소가 설치되었습니까?

커넥터가 설치된 후 반드시 하위 구성요소 설치가 완료되어야 합니다.

- Active Directory 커넥터의 경우 설치되는 하위 구성요소가 없습니다.

- Sun Java System Directory Server 커넥터의 경우 동기화되는 Sun Java System Directory Server 에 Directory Server 플러그인을 설치해야 합니다 .
- Windows NT 커넥터의 경우 동기화되는 각 Windows NT 도메인용 기본 도메인 제어기에 Windows 변화 감지기와 비밀번호 필터 플러그인이 반드시 설치되어야 합니다 . 이 두 하위 구성요소는 Windows NT 커넥터가 설치된 후 함께 설치됩니다 .

참고

Windows NT SAM 변경 감지기 하위 구성요소를 사용하려면 반드시 NT 감사 로그를 작동해야 합니다 . 시작 > 프로그램 > 관리 도구 > 사용자 관리자를 선택한 후 정책 > 감사 정책을 선택합니다 . 이 이벤트 감사를 선택하고 사용자 및 그룹 관리용 성공 및 실패 선택란을 모두 선택합니다 .

이벤트 뷰어 > Event Log Wrapping 에서 Event Log Settings 를 선택한 후 Overwrite Events as Needed 를 선택합니다 .

2. 하위 구성요소 설치 후 단계를 수행했습니까 ?

Directory Server 에 Directory Server 플러그인을 설치한 후 서버를 반드시 다시 시작해야 합니다 . 기본 도메인 제어기에 NT Change Detector 와 Password Filter 가 설치된 후 반드시 서버를 다시 시작해야 합니다 .

3. 하위 구성요소가 실행됩니까 ?

플러그인이 설치된 위치의 Directory Server 가 실행 중입니까 ? 변경 감지기와 비밀번호 필터가 설치된 위치의 기본 도메인 제어기가 실행 중입니까 ?

4. 하위 구성요소에 커넥터로의 네트워크 연결이 설정되었습니까 ?

커넥터가 실행되는 컴퓨터에서 netstat -n -a 를 실행하여 커넥터가 하위 구성요소의 연결을 수신하는지 확인합니다 . 다음 예는 세 가지 서로 다른 시나리오에서 이 명령을 실행한 결과입니다 . (커넥터는 포트 9999 를 수신하도록 구성되었습니다 .)

a. 커넥터가 입중계 연결을 수신하며 하위 구성요소가 연결 (예상된 결과):

```
netstat -n -a | grep 9999
*.9999      *.  0  0 65536  0 LISTEN
12.13.1.2.44397 12.13.1.2.9999 73620 0 73620  0 ESTABLISHED
12.13.1.2.9999 12.13.1.2.44397 73620 0 73620  0 ESTABLISHED
```

- b. 커넥터가 입중계 연결을 수신하지만 하위 구성요소가 연결되지 않은 경우

```
# netstat -n -a | grep 9999
*.9999      *.  0  0 65536  0 LISTEN
```

하위 구성요소가 실행되는지 확인한 후 하위 구성요소의 로컬 로그에서 잠재적인 문제가 없는지 확인합니다.

- c. 커넥터가 입중계 연결을 수신하지 않는 경우:

```
# netstat -n -a | grep 9999
<no output>
```

올바른 포트 번호를 지정했는지 확인합니다. 커넥터가 실행 중이며 READY 상태인지 확인합니다. 커넥터의 로컬 로그에서 잠재적인 문제가 없는지 확인합니다.

Message Queue 문제 해결

Sun Java System Message Queue 브로커가 실행 중인지 확인합니다. Message Queue 브로커가 실행되는 컴퓨터와 포트에 telnet 명령을 실행하면 사용 중인 Message Queue 서비스 목록이 반환됩니다.

```
# telnet localhost 7676
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^J'.
101 psw-broker 3.0.1
cluster tcp CLUSTER 32914
admin tcp ADMIN 32912
portmapper tcp PORTMAPPER 7676
ssljms tis NORMAL 32913
jms tcp NORMAL 32911
.
Connection closed by foreign host.
```


- 출력 목록에 "ssljms tcp NORMAL" 서비스가 없는 경우 Message Queue 로그에서 잠재적 문제를 확인합니다. 코어가 Solaris 에 설치된 경우 Message Queue 브로커의 로그는 다음과 같습니다.

```
/var/imq/instances/psw-broker/log/log.txt
```

- 코어가 Windows 에 설치된 경우 브로커의 로그는 다음과 같습니다.

```
<installation_root>\isw-<machine_name>\imq\var\instances\isw-broker\log\log.txt
```

telnet 명령이 실패하는 경우 브로커가 실행되지 않거나 잘못된 포트가 지정된 것입니다. 브로커의 로그에서 포트 번호를 확인합니다. 브로커의 포트는 다음 줄에 지정됩니다.

```
[13/Mar/2003:18:17:09 CST] [B1004]: "Starting the portmapper service using tcp [ 7676, 50 ] with min threads 1 and max threads of 1"
```

브로커가 실행되지 않는 경우 Solaris 의 경우 /etc/init.d/imq start 를 실행하거나 Windows 의 경우 iMQ Broker Windows 서비스를 시작하여 브로커를 시작할 수 있습니다.

Message Queue 를 Solaris 8 에 설치하며 mqinstall 를 실행하여 패키지를 모두 설치하는 경우 반드시 mqinstall 를 실행하기 전에 IMQ_JAVAHOME 을 설정하여 소프트웨어가 올바른 버전의 Java 를 선택하도록 해야 합니다.

아직 코어를 설치하지 않았으면 Identity Synchronization for Windows 설치 프로그램이 Message Queue 브로커가 사용할 JVM 을 지정하므로 IMQ_JAVAHOME 을 설정하지 않아도 됩니다.

브로커 구성 디렉토리 통신 문제 해결

Message Queue 브로커는 Identity Synchronization for Windows 구성이 저장된 Directory Server 에 대하여 클라이언트를 인증합니다. 브로커가 이 Directory Server 에 연결할 수 없는 경우 모든 클라이언트가 Message Queue 에 연결할 수 없으며, 브로커 로그에 "javax.naming.CommunicationException" 또는 "javax.naming.NameNotFoundException" 등의 javax.naming 예외가 기록됩니다. javax.naming 예외가 발생하는 경우 다음과 같이 합니다.

- `/var/imq/instances/isw-broker/props/config.properties` 의 모든 `imq.user_repository.ldap` properties 에 올바른 값이 있는지 확인합니다. 잘못된 내용이 있으며 Message Queue 브로커를 정지하고 파일을 수정하여 저장한 후, 브로커를 다시 시작합니다. Directory Server 호스트 이름은 브로커의 컴퓨터에서 변환될 수 있어야 합니다.
- `/etc/imq/passfile` 의 `imq.user_repository.ldap.password` 등록정보가 올바른지 확인합니다.
- 일부 루트 접미어에 공백이 있는 경우 브로커가 항목을 검색하지 못할 수 있습니다.

브로커 메모리 설정 문제 해결

정상적인 운영 동안 Message Queue 브로커는 적절한 정도의 메모리를 사용합니다. 그러나 `idsync resync` 작업 동안 브로커의 메모리 요구 사항이 증가합니다. 브로커의 메모리 한계가 초과하면 전달되지 않은 메시지가 쌓이게 되고, `idsync resync` 작업이 매우 느려지거나 완전히 정지합니다. 또한 이 후 Identity Synchronization for Windows 시스템이 응답하지 않게 됩니다.

브로커가 메모리 부족 상태가 되면 로그에 다음 메시지가 표시됩니다.

```
[03/Nov/2003:14:07:51 CST] [B1089]: In low memory condition, Broker is attempting to free up resources
```

```
[03/Nov/2003:14:07:51 CST] [B1088]: Entering Memory State [B0024]: RED from previous state [B0023]: ORANGE - current memory is 1829876K, 90% of total memory
```

이러한 상황을 피하려면 다음과 같이 합니다.

- *Sun Java System 1 2004Q3 Identity Synchronization for Windows 릴리스 노트*에서 설명한 것과 같이 브로커의 메모리 한계를 1 또는 2GB 로 증가시킵니다.
- `idsync resync` 작업 동안 로그 수준을 INFO 설정으로 유지합니다. 로그 수준을 FINE 이상으로 올리면 브로커의 부하가 로그 메시지가 중앙 기록기로 전달되는 만큼 증가합니다.
- 한 번에 동기화 사용자 목록 하나에 대하여만 `idsync resync` 를 실행합니다.

브로커의 메모리가 부족해지는 경우 다음과 같이 복구합니다.

1. 적절한 디렉토리의 브로커의 영구 메시지 저장에서 전달되지 않은 메시지가 대기중인지 확인합니다.
 - **Solaris:** /var/imq/instances/psw-broker/filestore/message/
 - **Windows:** <installation_root>\isw-<machine_name>\imq\var\instances\isw-broker\filestore\message\
2. 이 디렉토리의 각 파일에는 하나의 전달되지 않은 메시지가 있습니다. 이 디렉토리의 파일 수가 10000 을 초과하는 경우 브로커가 메시지를 지연하고 있는 것입니다. ! 그렇지 않은 경우 브로커에 다른 문제가 있습니다.
3. 메시지 지연은 idsync resync 작업에 관련된 유일한 로그 파일일 것이므로 안전하게 제거할 수 있습니다.
4. "서비스 시작 및 정지" 페이지 183에 설명한 것과 같이 Message Queue 브로커를 정지합니다.
5. 영구 메시지 저장에서 모든 파일을 제거합니다. 이들 파일을 제거하는 가장 쉬운 방법은 message/ 디렉토리를 반복적으로 제거하고 이를 다시 만드는 방법입니다.
6. Message Queue 브로커를 다시 시작합니다.

여기의 단계를 통하여 브로커의 메모리가 다시 부족해지지 않도록 합니다.

SSL 문제 해결

SSL 의 문제를 진단할 때 제 11 장, "보안 구성," 에 설명한 Identity Synchronization for Windows 의 구성요소 사이에서 SSL 을 설정하는 방법 또한 참조하십시오. 이 부분의 내용 :

- 코어 구성요소 사이의 SSL
- 커넥터와 Directory Server 또는 Active Directory 사이의 SSL
- Directory Server 플러그인과 Active Directory 사이의 SSL

1. 모든 메시지가 전달된 경우라도 파일 작성 및 삭제로 인한 성능 저하를 피하기 위하여 브로커는 최대 10000 개의 메시지 파일을 유지할 수 있습니다.

코어 구성요소 사이의 SSL

Identity Synchronization for Windows 프로그램은 코어 설치 동안 제공된 SSL 포트가 올바른지 확인할 수 없습니다. 코어 설치 동안 SSL 포트를 잘못 입력한 경우 코어 구성요소가 적절히 통신할 수 없습니다. 구성을 처음 저장할 때까지 문제를 알 수 없을 것입니다. 콘솔에 다음 경고가 표시됩니다.

The configuration was successfully saved, however, the System Manager could not be notified of the new configuration.

시스템 관리자 로그에는 다음 항목이 표시됩니다.

[10/Nov/2003:10:24:35.137 -0600] WARNING 14 example "Failed to connect to the configuration directory because "Unable to connect: (-5981) Connection refused by peer.". Will retry shortly."

이 경우 코어를 제거하고 올바른 SSL 포트 번호로 다시 설치합니다.

커넥터와 Directory Server 또는 Active Directory 사이의 SSL

커넥터가 SSL 을 통하여 Directory Server 또는 Active Directory 로 연결할 수 없는 경우 중앙 오류 로그에 다음 메시지가 표시됩니다.

[06/Oct/2003:14:02:48.911 -0600] WARNING 14 CNN100 host1 "failed to open connection to ldaps://host2.airius.com:636."

콘솔을 열고 Specifying Advanced Security Options 패널을 선택합니다 ([페이지 120](#) 참조).

신뢰되지 않은 인증서

더 자세한 내용은 중앙 감사 로그에 있습니다. 예를 들어 LDAP 서버의 SSL 인증서가 신뢰되지 않는 경우 이 메시지가 기록됩니다.

```
[06/Oct/2003:14:02:48.951 -0600] INFO 14 CNN100 host1 "failed to open connection to
ldaps://host2.airius.com:636, error(91): Cannot connect to the LDAP server, reason:
SSL_ForceHandshake failed: (-8179) Peer's Certificate issuer is not recognized."
```

대부분의 경우 커넥터의 인증서 데이터베이스에 CA 인증서가 추가되지 않은 것입니다. 이는 Directory Server 와 함께 제공되는 certutil 프로그램을 실행하여 확인할 수 있습니다.¹

참고

certutil 등의 자격 증명 관리 유틸리티는 SUNWt1su 패키지와 함께 제공되며 Directory Server 에 포함되지는 않습니다. (이 패키지는 Sun Microsystems 에서 무료로 다운로드할 수 있습니다.

패키지를 다운로드한 후 다음에서 certutil 를 찾습니다.

```
/usr/sfw/bin/certutil
```

이 예에서 인증서 데이터베이스에 포함된 인증서가 없습니다.²

```
# /usr/sunone/servers/shared/bin/certutil -L -d /usr/sunone/servers/ isw-host1/etc/CNN100
인증서 이름                신뢰 속성
p   유효한 피어
P   신뢰된 피어 (p 포함)
c   유효한 CA
T   클라이언트 인증서 발행을 위한 신뢰된 CA (c 포함)
C   인증서에 대한 신뢰된 CA (SSL 용 서버 인증서 전용) (c 포함)
u   사용자 인증서
w   경고 보냄
```

1. Solaris 에서 이 명령을 실행하기 전에 반드시 LD_LIBRARY_PATH 환경 변수에 <installation_root>/lib 디렉토리를 추가해야 합니다.
2. Sun Java System Directory Server 와 Windows NT 커넥터용 기본 인증서 데이터베이스에는 saint-cert100 및 saintRootCA 의 두 개의 인증서가 있습니다. 이 릴리스에서는 이들 인증서를 사용하지 않습니다.

다음 예에서 인증서 데이터베이스에 오직 Active Directory CA 인증서만 있습니다 .

```
# /usr/sunone/servers/shared/bin/certutil -L -d /usr/sunone/servers/ isw-host1/etc/CNN100
인증서 이름                신뢰 속성
airius.com CA              C,c,
p   유효한 피어
P   신뢰된 피어 (p 포함 )
c   유효한 CA
T   클라이언트 인증서 발행을 위한 신뢰된 CA (c 포함 )
C   인증서에 대한 신뢰된 CA (SSL 용 서버 인증서 전용 ) (c 포함 )
u   사용자 인증서
w   경고 보냄
```

여기에 보이는 것과 같이 CA 인증서의 신뢰 플래그는 반드시 "c,," 이어야 합니다 . 인증서가 있으며 신뢰 플래그가 적절히 설정되었으나 커넥터가 여전히 연결할 수 없는 경우 우선 인증서를 추가한 후 커넥터가 다시 시작되었는지 확인한 후 , Sun Java System 디렉토리과 함께 제공되는 ldapsearch 명령을 사용하여 문제 진단을 보조합니다 . ldapsearch 에서 인증서가 허용되지 않는 경우 커넥터에서도 허용되지 않습니다 . 예를 들어 ldapsearch 는 신뢰되지 않은 인증서를 거부할 수 있습니다 .

```
# /usr/sunone/servers/shared/bin/ldapsearch -Z -P /usr/sunone/ servers/isw-host1/etc/CNN100 -h
host2 -b "" -s base "(objectclass=*)"
ldap_search: Can't contact LDAP server
SSL error -8179 (Peer's Certificate issuer is not recognized.)
```

-P 옵션을 사용하면 ldapsearch 가 커넥터 CNN100 의 인증서 데이터베이스를 SSL 인증서 유효성 검사에 사용합니다 . 커넥터의 인증서 데이터베이스에 올바른 인증서가 추가된 후 ldapsearch 가 해당 인증서를 허용하는지 확인한 후 커넥터를 다시 시작합니다 .

일치되지 않는 호스트이름

Identity Synchronization for Windows 가 SSL 연결 설정을 시도할 때 (모든 인증서 신뢰 설정 사용 안 함) Identity Synchronization for Windows 의 커넥터는 서버의 호스트 이름이 SSL 협상 단계 동안 서버가 제시한 인증서에 있는 호스트 이름과 일치하는지 확인합니다 . 호스트 이름이 일치하지 않으면 커넥터가 연결 설정을 거부합니다 .

Identity Synchronization for Windows 구성의 디렉토리 소스 호스트 이름은 반드시 항상 해당 디렉토리 소스가 사용하는 인증서에 포함된 호스트 이름과 일치해야 합니다.

다음과 같이 `ldapsearch` 를 사용하여 호스트 이름이 일치하는지 확인할 수 있습니다.

```
/var/mps/serverroot/shared/bin/ldapsearch.exe -Z -P /var/opt/SUNWsw/etc/CNN100 -3
-h host2.example.com -p 636 -s base -b "" "(objectclass=*)"
```

명령줄의 호스트 이름 (`host2.example.com`) 과 인증서에 포함된 호스트 이름이 일치하지 않는 경우 다음의 오류 메시지가 표시됩니다.

```
ldap_search: Can't contact LDAP server
SSL error -12276 (Unable to communicate securely with peer: requested do main name does not
match the server's certificate.)
```

호스트 이름이 일치하면 `ldapsearch` 명령이 성공하며 루트 DSE 의 내용이 표시됩니다.

만료된 자격 증명

서버의 인증서가 만료된 경우 이 메시지가 기록됩니다.

```
[06/Oct/2003:14:06:470.130 -0600] INFO 20 CNN100 host1 "failed to open connection to
ldaps://host2.airius.com:636, error(91): Cannot connect to the LDAP server, reason:
SSL_ForceHandshake failed: (-8181) Peer's Certificate has expired."
```

이 경우 서버는 반드시 새 인증서를 발행해야 합니다.

Directory Server 플러그인과 Active Directory 사이의 SSL

기본적으로 요청시 비밀번호 동기화를 수행할 때 Directory Server 는 SSL 을 통하여 Active Directory 와 통신하지 않습니다 . 기본값을 변경하여 이 통신을 SSL 로 보호 하도록 하면 제 11 장 , " 보안 구성 " 에 설명한 것과 같이 각 마스터 복제본의 디렉토리 서버 인증서 데이터베이스에 반드시 Active Directory CA 인증서가 추가되어야 합니다 . 이 인증서가 추가되지 않으면 사용자가 디렉토리 서버로 바인드할 수 없으며 "DSA is unwilling to perform" 오류가 발생합니다 . 또한 플러그인의 로그 (예를 들어 isw-<hostname>/logs/SUBC100/pluginwps_log_0.txt) 가 다음을 보고합니다 .

```
[06/Nov/2003:15:56:16.310 -0600] INFO  td=0x0376DD74 logCode=81
ADRepository.cpp:310  "unable to open connection to Active Directory server at
ldaps://host2.airius.com:636, reason: "
```

이 경우 반드시 Active Directory CA 인증서를 Directory Server 의 인증서 데이터베이스에 추가하고 Directory Server 를 다시 시작합니다 .

제어기 문제 해결

백업 파일에서 Active Directory 도메인 제어기를 복구할 때 일부 카운터는 재설정되지 않습니다 .

모든 카운터가 적절히 재설정되도록 하려면 Active Directory 도메인 제어기를 복구한 후 모든 사용자를 재동기화해야 합니다 .

감사 및 오류 파일 이해

Identity Synchronization for Windows에는 설치 및 구성 상태, 일상적인 시스템 운영 및 구현에 관련된 모든 오류 조건 등에 대한 정보가 제공됩니다.

이 장에서는 다음 절을 통해 이러한 정보를 액세스하고 이해하는 방법에 대해 설명합니다.

- "로그 이해" 페이지 263
- "로그 파일 구성" 페이지 269
- "디렉토리 소스 상태 보기" 페이지 271
- "설치 및 구성 상태 보기" 페이지 272
- "감사 및 오류 로그 보기" 페이지 273
- "Windows NT 컴퓨터에서 감사 사용 설정" 페이지 274

로그 이해

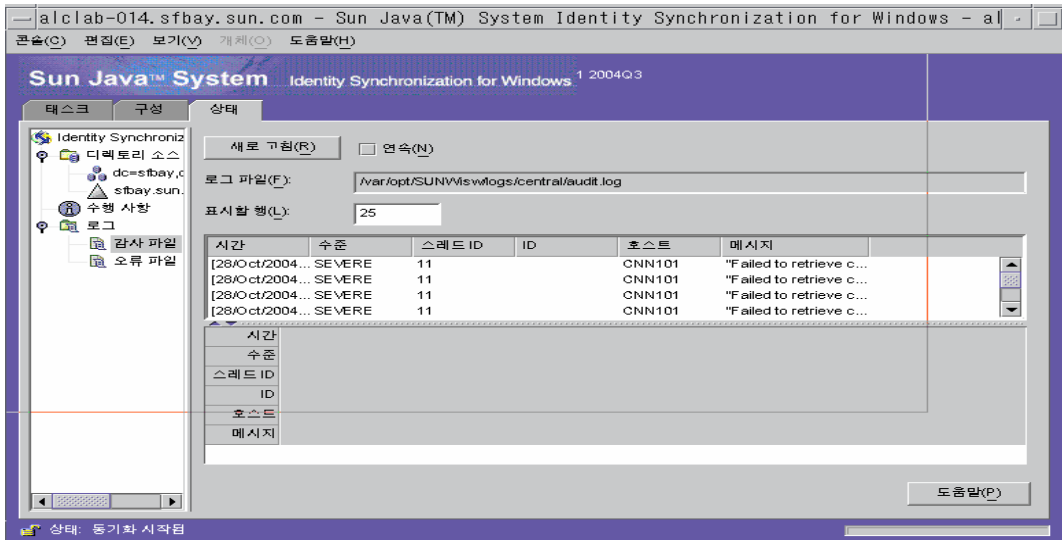
Identity Synchronization for Windows 콘솔의 Status 탭에 다양한 종류의 정보가 표시됩니다.

탐색 트리 창 (왼쪽)에서 다음 노드 중 하나를 선택하면 Status 탭의 내용이 해당 항목에 대한 정보를 표시하도록 변경됩니다.

- **Directory Source:** 해당 디렉토리 소스에 대한 상태 정보를 보려면 디렉토리 소스 노드 (dc=example,dc=com 등)를 선택합니다.
- **To Do:** Identity Synchronization for Windows를 성공적으로 설치 및 구성하기 위하여 반드시 완료해야 하는 단계 목록을 보려면 이 노드를 선택합니다 (완료된 단계는 흐리게 표시).

- **Audit File:** 일상적인 시스템 운영에 대한 정보 (오류 조건 포함) 를 보려면 이 노드를 선택합니다 .
- **Error File:** 시스템의 오류 조건에 대한 정보를 보려면 이 노드를 선택합니다 . (오류 로그는 오직 오류 항목만 표시하는 필터의 역할을 합니다 .)

그림 10-1) Status 탭



Log Types

여기에서는 Identity Synchronization for Windows 에서 사용할 수 있는 다양한 종류의 로그에 대하여 설명합니다 .

- " 중앙 로그 " 페이지 265
- " 로컬 구성요소 로그 " 페이지 266
- " 로컬 Windows NT 하위 구성요소 로그 " 페이지 266
- "Directory Server 플러그인 로그 " 페이지 267

중앙 로그

Identity Synchronization for Windows 구성요소가 Message Queue 에 액세스할 수 있는 한 모든 오류 및 감사 메시지가 Identity Synchronization for Windows 중앙 기록기에 기록됩니다 . 따라서 이 중앙 로그 (모든 구성요소의 메시지 포함) 가 주로 모니터링해야 하는 로그입니다 .

중앙화된 로그는 코어가 설치된 컴퓨터의 다음 디렉토리에 위치합니다 .

- **Solaris:** /var/opt/SUNWisw/logs
- **Windows:** <installation_root>/isw-<machine_name>/logs/central/

각 구체적인 로그는 의 설명과 같습니다 .

표 10-1) Identity Synchronization for Windows 로그 종류

로그 이름	설명
error.log	여기에 경고와 중요한 메시지가 보고됩니다 .
audit.log	각 동기화 이벤트에 대한 메시지를 포함하는 error.log 의 상위 집합입니다 .
resync.log	여기에 resync 명령이 생성한 메시지가 보고됩니다 .

각 중앙 로그에는 또한 각 구성요소 ID 에 대한 정보가 포함됩니다 . 예 :

```
[2003/03/14 14:48:23.296 -0600] INFO 13 "System Component Information:
SysMgr_100 is the system manager (CORE); console is the Product Console
User Interface; CNN100 is the connector that manages [airius.com (ldaps://
server1.airius.com:636)]; CNN101 is the connector that manages
[dc=airius,dc=com (ldap:// server2.airius.com:389)];"
```

중앙 로그에 더하여 각 구성요소에는 자체의 로컬 로그가 있습니다. 중앙 기록기로 기록할 수 없는 문제의 경우 이들 로컬 로그를 사용하여 커넥터의 문제를 진단할 수 있습니다.

로컬 구성요소 로그

각 커넥터, 시스템 관리자 및 중앙 기록기에는 다음의 로컬 로그가 있습니다.

표 10-2) 로컬 로그

로그 이름	설명
audit.log	각 동기화 이벤트에 대한 메시지를 포함하는 error.log 의 상위 집합입니다. 이들 메시지는 또한 중앙의 audit.log 에도 기록됩니다.
error.log	여기에 경고와 중요한 메시지가 보고됩니다. 이들 메시지는 또한 중앙의 error.log 에도 기록됩니다.

이들 로컬 로그는 다음 하위 디렉토리에 위치합니다.

- **Solaris:** /var/opt/SUNWisw/logs
- **Windows:** <installation_root>/isw-<machine_name>/logs/central/

sysmgr 및 clogger100(중앙 기록기) 디렉토리는 코어가 설치된 컴퓨터에 있습니다.

Identity Synchronization for Windows 에서 이들 로그는 다음과 같이 매일 현재 로그를 날짜가 포함된 로그 파일로 이동하여 교체됩니다.

audit_2004_08_06.log

참고	기본적으로 Identity Synchronization for Windows 는 10 일 후 커넥터 로그를 삭제합니다. 이 기간은 Log.properties 파일의 com.sun.directory.wps.logging.maxmiumDaysToKeepOldLogs 값을 편집하고 서버 데몬을 다시 시작하여 연장할 수 있습니다.
-----------	---

로컬 Windows NT 하위 구성요소 로그

또한 다음의 Windows NT 하위 구성요소에도 로컬 로그가 있습니다.

- Windows NT 변경 검출기 DLL
- 비밀번호 필터 DLL

이들 하위 구성요소 로그는 다음 디렉토리의 SUBC1XX (SUBC100 등) 하위 디렉토리에 있습니다.

<installation_root>/isw-<machine_name>/logs/

Identity Synchronization for Windows 에서 이들 파일의 크기는 1MB 로 제한되며 10 개의 로그만 유지합니다 .

Directory Server 플러그인 로그

Directory Server 플러그인은 Directory Server 를 통하여 중앙 로그로 정보를 기록하며 Directory Server 로그 프로그램을 통하여 기록합니다 . 따라서 로컬 Directory Server 플러그인 로그 메시지는 또한 Directory Server 오류 로그에도 저장됩니다 .

Directory Server 는 다른 Directory Server 플러그인 및 구성요소의 정보를 오류 로그에 저장합니다 . Identity Synchronization for Windows Directory Server 플러그인에서 메시지를 확인하려면 isw 문자열이 포함된 줄을 필터합니다 .

기본적으로 오류 로그에는 최소한의 플러그인 로그 메시지만 표시됩니다 .

예 :

```
[14/Jun/2004:17:08:36 -0500] - ERROR<38747> - isw - conn=-1 op=-1 msgId=-1
- Plugins unable to establish connection to DS Connector at attila:1388,
will retry later
```

Directory Server Management 콘솔에서 다음과 같이 Directory Server 오류 로그의 기본 표시 수준을 변경할 수 있습니다 .

1. Directory Server 콘솔을 엽니다 .
2. Configuration 탭을 선택합니다 .
3. 탐색 창에서 Logs 노드를 누릅니다 .
4. Errors 탭을 선택합니다 .
5. Log Level 버튼을 누릅니다 .
6. Plugins 선택란을 선택합니다 . 더 세밀히 표시하려면 Vervose Mode 를 사용 설정합니다 .
7. OK 를 누른 다음 Save 를 누릅니다 .

Directory Server 로깅에 대한 자세한 내용은 *Sun Java System Directory 5 2004Q2 Server Administrator's Guide*(http://docs.sun.com/db/coll/DirectoryServer_04q2)를 참조하십시오 .

로그 읽기

각 로그 메시지에는 다음 정보가 포함됩니다.

- **Time:** 로그 항목이 생성된 때 (시간 및 날짜) 를 표시합니다 . 예 :
[13/Aug/2004:06:14:36:753 -0500]
- **Level:** 로그 메시지의 중요도와 표시 수준을 표시합니다 .
Identity Synchronization for Windows 는 다음 로그 수준을 사용합니다 .

표 10-3) 로그 수준

로그 수준	설명
INFO	이들 메시지는 각 작업에 대한 최소 정보를 제공하므로 시스템이 올바르게 실행되는지 확인할 수 있습니다 . 예를 들어 변경이 검출된 때와 동기화가 발생한 때를 알 수 있습니다 . 이들 메시지는 항상 감사 로그에 기록됩니다 .
FINE	이들 메시지에는 동작이 시스템 사이에서 전달되면서 발생하는 자세한 정보가 포함됩니다 .
FINER	이들 메시지에는 동작이 시스템 사이에서 전달되면서 발생하는 정보가 더욱 자세히 포함됩니다 . 모든 구성요소에 대한 로그 수준을 FINER 로 설정하면 성능이 저하될 수 있습니다 .
FINEST	이들 메시지에는 동작이 시스템 사이에서 전달되면서 발생하는 가장 자세한 정보가 포함됩니다 . 모든 구성요소에 대한 로그 수준을 FINEST 로 설정하면 성능이 상당히 저하될 수 있습니다 .

- **Thread ID:** 이벤트를 생성한 기능의 Java 스레드 ID 를 표시합니다 .
- **ID:** 이벤트를 유발한 구성요소 (콘솔 , 시스템 관리자 등) 를 확인합니다 .
- **Host:** 이벤트를 유발한 호스트의 이름을 표시합니다 .
- **Message:** 이벤트와 관련된 감사 또는 오류 정보를 표시합니다 .
몇 가지 예는 다음과 같습니다 .

"Resetting Central Logger configuration ..."

"System manager is shutting down."

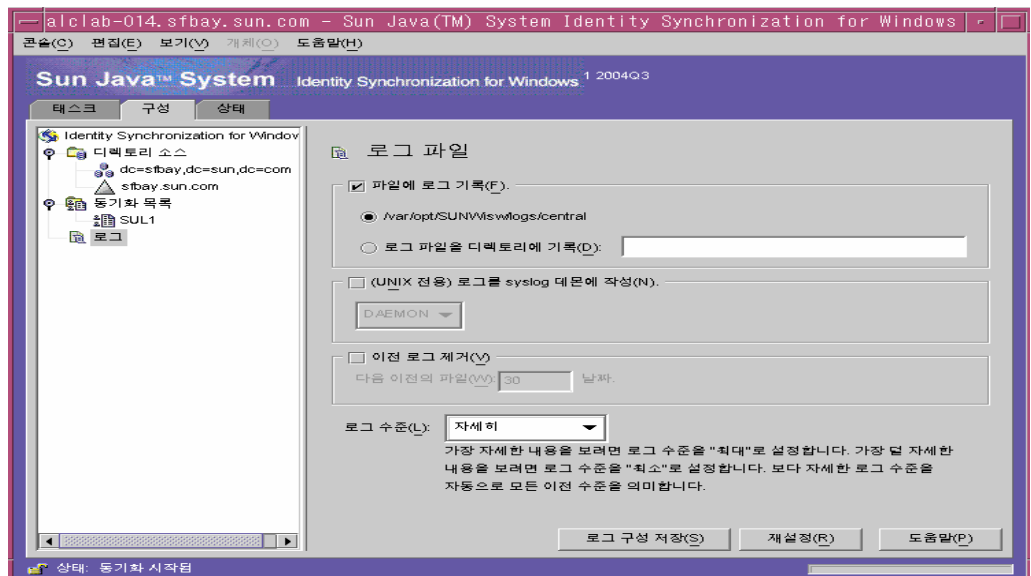
"Processing request (ID=<ID_number> from the console to stop synchronization."

로그 파일 구성

Identity Synchronization for Windows 콘솔을 사용하여 다음과 같이 구현에 대한 로깅을 구성할 수 있습니다.

1. 콘솔을 열고 Configuration 탭을 선택합니다.
2. 탐색 트리 창에서 Logs 노드가 보일 때까지 노드를 확장합니다.
3. Logs 노드를 선택하면 Configuration 탭에 Log Files 패널이 표시됩니다 (참조).

그림 10-2) 로그 파일 구성



4. 로그 파일 창에서 다음과 같이 로그 파일을 구성합니다.
 - **파일에 로그 기록.** 로그를 코어 호스트에 있는 파일에 기록하려면 이 옵션을 사용합니다.

이 옵션을 선택한 후 다음 작업을 할 수 있습니다.

 - 기본 로그 디렉토리 및 파일(예: /var/opt/SUNWlsw/logs/central)을 사용 설정합니다.
 - Write log files to directory 옵션을 사용 설정하고 로그 파일의 경로와 파일 이름을 지정합니다.

참고 콘솔은 지정한 로그 파일 위치가 실제로 존재하는지 확인하지 않습니다. 중앙 기록기는 로그 디렉토리가 없는 경우 이를 만듭니다. 따라서 로그를 확인할 때까지 존재하지 않는 로그 위치를 지정하고 정했다는 것을 알 수 없습니다. 몇 번의 로그 확인 시도 후에 콘솔이 지정한 위치에서 로그를 찾을 수 없다는 보고 메시지가 표시됩니다.

- *Solaris*에만 적용 -- **Write logs to syslog daemon:** Identity Synchronization for Windows가 Solaris 플랫폼에 있는 경우 이 옵션을 사용합니다. 드롭다운 목록을 사용하여 로그를 기록할 기준을 선택합니다. (기본값은 *DAEMON*입니다.)

참고 이 옵션을 선택하면 Identity Synchronization for Windows가 syslog에 모든 것을 기록하지만, syslog은 기본적으로 WARNING 및 SEVERE 메시지만 기록하도록 구성되었습니다.

syslog이 INFO 메시지를 기록하도록 하려면 `/etc/syslog.conf`를 편집하고 다음 줄을 변경합니다.

```
*.err;kern.debug;daemon.notice;mail.crit
/var/adm/messages
```

변경 후:

```
*.err;kern.debug;daemon.notice;daemon.info;mail.crit
/var/adm/messages
```

이렇게 변경한 후, 반드시 다음과 같이 syslog 데몬을 다시 시작해야 합니다.

```
/etc/init.d/syslog stop ; /etc/init.d/syslog start
```

FINE, FINER 및 FINEST 로깅을 사용하려면 세미 콜론 (;)으로 분리된 목록에 `daemon.debug`를 포함합니다.

- **Remove Old Logs:** 로그 파일의 수는 제한 없이 늘어납니다(하루에 하나씩). 디스크 공간이 부족해지는 경우를 피하려면 이 옵션을 사용 설정하고 프로그램이 중앙 로그 파일에서 이전 로그를 삭제하는 때를 지정하십시오.

예를 들어 30 일을 지정하면 Identity Synchronization for Windows 가 31 일 이 경과한 모든 파일을 삭제합니다 .

- **로그 수준** . 드롭 다운 목록을 사용하여 시스템 로그에서 표시할 세부 수준을 선택합니다 . (" 로그 수준 " 페이지 268 참조)
- 5. 이들 옵션을 기준으로 하는 로그 파일을 만들려면 Save Log Configuration 버튼을 누릅니다 .

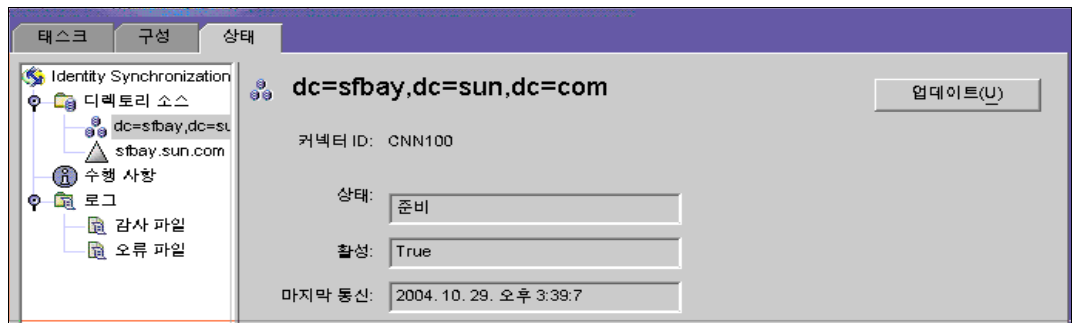
디렉토리 소스 상태 보기

디렉토리 소스의 상태를 보려면 다음과 같이 합니다 .

1. Identity Synchronization for Windows 콘솔에서 Status 탭을 누릅니다 .
2. 탐색 트리 창에서 Directory Source 노드를 확장한 후 , 해당 디렉토리 소스 노드 (dc=example,dc=com 등) 를 선택합니다 .

Status 탭 내용이 변경되어 선택한 디렉토리 소스에 관련된 정보가 표시됩니다 (예는 참조) .

그림 10-3) 디렉토리 소스 상태



참고 디렉토리 소스 상태를 표시할 때 실제로는 해당 디렉토리 소스에 연결된 커넥터의 상태가 표시되는 것입니다 .

Status 탭에 제공되는 정보는 다음과 같습니다 .

- **Update:** 이 탭의 정보를 새로 고치려면 Update 를 누릅니다 .

- **State:** 디렉토리 소스의 현재 상태가 표시됩니다. 유효한 상태는 다음과 같습니다.
 - **Uninstalled:** 커넥터가 설치되지 않았습니다.
 - **Installed:** 커넥터가 설치되었으나 아직 런타임 구성을 수신하지 않았으므로 동기화의 준비가 되지 않았습니다. 커넥터가 1 분 이상 이 상태를 유지하는 경우 잘못된 것이 있을 것입니다.
 - **Ready:** 커넥터가 동기화의 준비가 되었으나 현재 동기화하는 객체가 없습니다. 동기화가 아직 시작되지 않았거나 동기화가 시작되었으나 하위 구성요소 중 커넥터와의 연결이 설정되지 않은 것이 있는 경우 커넥터의 상태가 Ready 로 유지됩니다.
 - **Syncing:** 커넥터가 객체를 동기화하는 중입니다. 여전히 오류가 있을 수 있으므로 동기화되지 않은 변경 내용이 있는 경우 오류 로그를 확인하십시오.
- **Active:** 디렉토리 소스를 사용 중인지 또는 정지되었는지 표시합니다.
- **Last Communication:** 디렉토리 소스의 커넥터가 마지막으로 응답한 시간을 표시합니다.

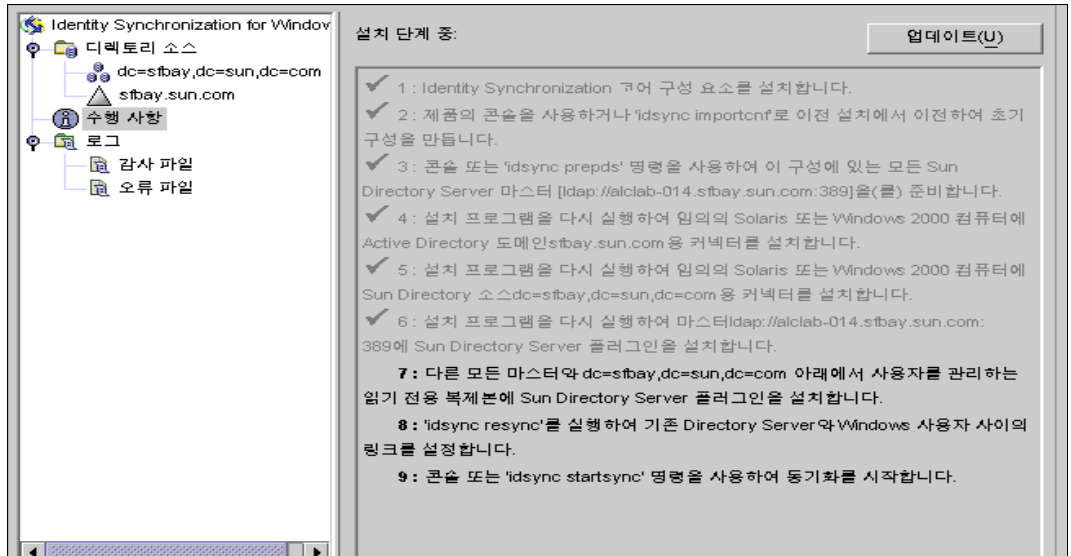
설치 및 구성 상태 보기

Identity Synchronization for Windows 설치 및 구성 프로세스에서 남아 있는 필수 완료 단계를 보려면 다음과 같이 합니다.

1. Identity Synchronization for Windows 콘솔에서 Status 탭을 누릅니다.
2. 탐색 트리 창에서 To Do 노드를 확장합니다.

Status 탭 내용이 변경되어 설치 및 구성 단계의 점검 목록이 표시됩니다 (예는 참조).

그림 10-4) To Do 목록 보기



3. Update 버튼 (오른쪽 상단) 을 눌러 목록을 새로 고칩니다 .

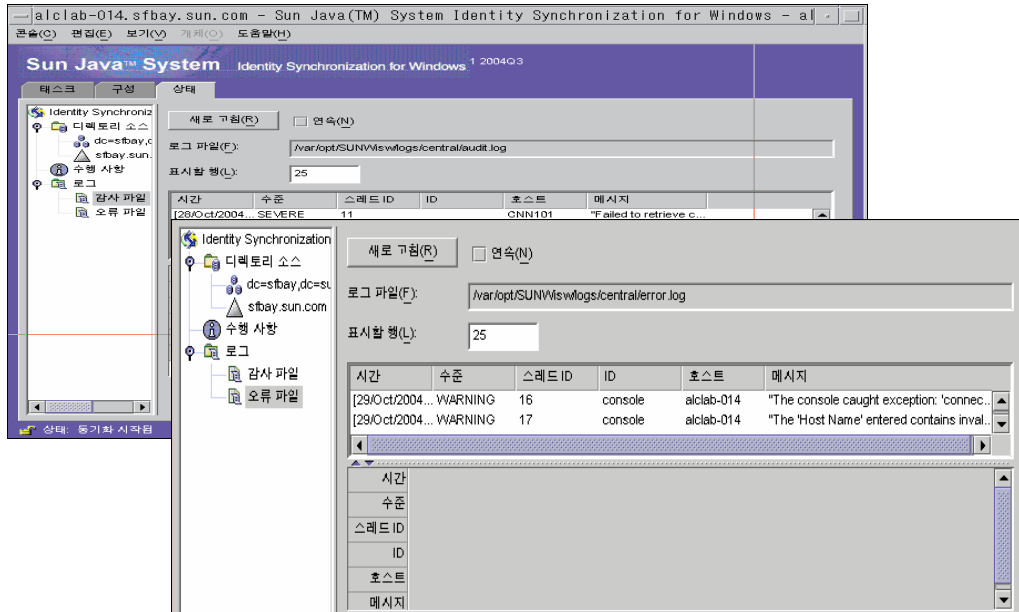
완료된 단계는 선택 표시되며 흐리게 표시됩니다 . 설치 및 구성 과정을 성공적으로 완료하려면 나머지 단계를 반드시 완료해야 합니다 .

감사 및 오류 로그 보기

오류 로그를 보려면 다음과 같이 합니다 .

1. Identity Synchronization for Windows 콘솔에서 Status 탭을 누릅니다 .
2. 탐색 트리 창에서 Audit File 또는 Error File 노드를 확장합니다 .
Status 탭 내용이 변경되어 현재 로그 () 를 표시합니다 .

그림 10-5) 로그 보기



Status 탭에 제공되는 정보는 다음과 같습니다.

- **Refresh:** 최신 감사 또는 오류 정보를 로드합니다.
- **Continuous:** 최근 감사 또는 오류 정보를 지속적으로 업데이트 및 표시합니다.
- **Log File:** 표시되는 감사 또는 오류 로그의 전체 경로 이름을 표시합니다. 예:
C:\Program Files\Sun\MPS\isw-<hostname>\logs\central\audit.log
- **Lines to show:** 표시할 감사 또는 오류 항목의 수를 지정합니다. (기본값은 25입니다.)

Windows NT 컴퓨터에서 감사 사용 설정

사용자의 구현 환경에 Windows NT 시스템이 있을 경우, 감사 기능의 활성화 여부를 확인하십시오. 감사 기능이 활성화 되어 있지 않으면 Identity Synchronization for Windows 가 해당 시스템의 메시지를 기록할 수 없습니다.

다음과 같은 방법으로 Windows NT 컴퓨터에서 감사 로깅을 사용 설정합니다.

1. Windows NT 시작 메뉴에서 프로그램 > 관리 도구 > 도메인 사용자 관리자를 선택합니다.
2. 사용자 관리자 대화 상자가 표시되면 메뉴 표시줄에서 정책 > 감사를 선택합니다.
감사 정책 대화 상자가 표시됩니다.
3. 이 이벤트 감사 버튼을 선택한 후 성공 및 실패 선택란을 선택합니다.
4. 확인을 눌러 대화 상자를 닫습니다.

이 설정은 이를 다시 변경할 때까지 유효합니다.

보안 구성

이 장에서는 구현에 대하여 보안을 구성하는 방법에 대하여 설명합니다. 다음과 같은 내용으로 구성됩니다.

- " 보안 개요 " 페이지 277
- " 보안 강화 " 페이지 283
- " 복제된 구성 보안 " 페이지 286
- "idsync certinfo 사용 " 페이지 289
- "Directory Server 에서 SSL 사용 " 페이지 290
- "Active Directory 커넥터에서 SSL 사용 " 페이지 293
- "Directory Server 로 Active Directory 인증서 추가 " 페이지 296
- "Directory Server 커넥터에 Directory Server 인증서 추가 " 페이지 297

참고

이 장에서는 공용키 암호화 및 SSL(Secure Sockets Layer)의 기본 개념에 익숙하며 엔터프라이즈에서의 인트라넷, 익스트라넷, 인터넷 보안 및 전자 서명의 역할에 대한 개념을 이해하는 것으로 가정합니다. 이들 개념에 익숙하지 않은 경우 설명서의 보안 관련 부록 *Managing Servers with iPlanet Console 5.0* 설명서를 참조하십시오.

보안 개요

비밀번호는 중요한 정보이므로 Identity Synchronization for Windows 는 안전을 위하여 동기화되는 디렉토리에 액세스할 때 사용하는 사용자 및 관리 비밀번호 자격 증명에 침해되지 않도록 보호합니다.

여기에서는 다음의 보안 방법론에 대해 설명합니다 .

- " 구성 비밀번호 지정 " 페이지 278
- "SSL 사용 " 페이지 279
- " 생성된 3DES 키 " 페이지 280
- "SSL 및 3DES 키 보호 요약 " 페이지 280
- "Message Queue 액세스 제어 " 페이지 281
- " 디렉토리 자격 증명 " 페이지 282
- " 영구 스토리지 보호 요약 " 페이지 282

이 보안 접근방법의 목적은 다음의 상황이 발생하지 않도록 예방하는 것입니다 .

- 네트워크의 일반 텍스트 비밀번호를 가로채는 경우
- 공격자가 커넥터를 조작하여 사용자의 비밀번호를 원하는 값으로 변경하는 경우 . 이는 사용자의 일반 텍스트 비밀번호를 포착하는 것과 같습니다 .
- 공격자가 Identity Synchronization for Windows 의 권한이 제한된 구성요소로 액세스하는 경우
- 권한이 없는 사용자가 디스크에 저장된 파일에서 파일을 구하는 경우 .
- 침입자가 시스템의 구성요소 중 하나에서 제거된 하드 디스크에서 비밀번호를 구하는 경우 . 동기화되는 비밀번호일 수 있으며 또는 디렉토리에 액세스하는 데 사용하는 시스템 비밀번호일 수 있습니다 .

구성 비밀번호 지정

중요한 정보가 제품의 구성 디렉토리에 있는 동안 , 또한 네트워크를 통하여 전송되는 동안 이 정보를 보호하기 위하여 Identity Synchronization for Windows 는 *구성 비밀번호를 사용합니다* . 관리자는 코어를 설치할 때 구성 비밀번호를 지정하며 반드시 콘솔을 열거나 Identity Synchronization for Windows 설치 프로그램을 실행할 때 반드시 이 비밀번호를 입력해야 합니다 .

참고

시스템 관리자는 반드시 구성 비밀번호에 액세스한 후 이를 커넥터에 전달하므로 비밀번호를 초기화 파일에 저장합니다.

파일 시스템 액세스 제어가 권한 없는 사용자가 시스템 관리자의 초기화 파일에 액세스할 수 없도록 방지합니다. Identity Synchronization for Windows 설치 프로그램은 이 비밀번호에 대하여 비밀번호 정책을 집행하지 않습니다.

구성 비밀번호를 선택할 때 보안을 강화하려면 ["보안 강화" 페이지 283](#) 를 참조하십시오.

SSL 사용

구성요소가 LDAP 를 사용하는 모든 위치에서 Identity Synchronization for Windows 가 SSL 을 통하여 LDAP 를 사용하도록 구성할 수 있습니다. Message Queue 에 대한 모든 액세스는 SSL 로 보호됩니다.

Directory Server 에서 Active Directory 로 동기화할 때 반드시 Active Directory 커넥터와 Active Directory 사이에 SSL 을 사용해야 합니다.

신뢰된 SSL 인증서 필요

기본적으로 SSL 을 사용하도록 구성된 커넥터는 서버 (Directory Server 또는 Active Directory) 가 반환한 SSL 인증서를 허용하며, 여기에는 신뢰, 만료 및 무효화 인증서가 포함됩니다. 커넥터와 서버 사이의 모든 트래픽은 암호화되지만 커넥터가 진정한 Active Directory 또는 Directory Server 를 모방하는 서버를 검출할 수는 없습니다.

커넥터가 신뢰된 인증서만 허용하도록 하려면 콘솔을 사용하여 Directory Source Configuration 마법사 ([페이지 120](#) 참조) 에 있는 Specify Advanced Security Options 패널의 Require trusted SSL 인증서 옵션을 사용 설정합니다. 이 옵션을 사용 설정한 후 반드시 idsync certinfo 가 보고한 것과 같이 커넥터의 인증서 데이터베이스에 적절한 CA 인증서를 추가해야 합니다.

생성된 3DES 키

구성 비밀번호에서 생성된 3DES 키는 제품의 구성 디렉토리에 있는 모든 중요한 정보를 보안하기 위하여 사용됩니다. 로그 메시지를 제외하고 Message Queue 로 전달되는 모든 메시지는 항목당 3DES 키로 암호화됩니다. 커넥터와 하위 구성요소 사이에 전송된 메시지는 세션당 3DES 키로 암호화됩니다. Directory Server 플러그인은 모든 사용자 비밀번호 변경을 3DES 키로 암호화합니다.

SSL 및 3DES 키 보호 요약

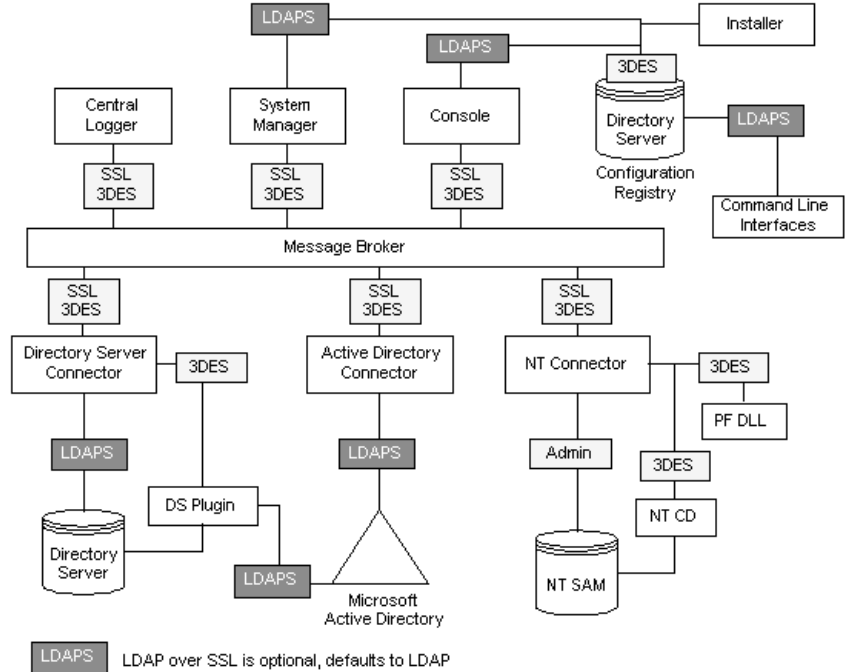
Identity Synchronization for Windows 가 네트워크에서 전송되는 중요한 정보를 보호하는 방법은 에서 간단히 설명합니다.

표 11-1) 네트워크 보안을 사용하여 중요한 정보 보호

다음 정보 유형 사이에서	이 보호 방법 사용 :
SSL 을 통한 LDAP (선택)	<ul style="list-style-type: none"> Directory Server 커넥터와 Directory Server, Active Directory 커넥터 및 Active Directory Directory Server 플러그인과 Active Directory 명령줄 인터페이스와 제품의 구성 디렉토리 콘솔과 제품의 구성 디렉토리 콘솔과 Active Directory 전역 카탈로그 콘솔과 동기화되는 Active Directory 도메인 또는 Directory Server Message Queue 브로커와 제품의 구성 디렉토리 커넥터, 시스템 관리자, 중앙 기록기, 명령줄 인터페이스 및 콘솔은 LDAPS 를 통하여 Message Queue 를 인증할 수 있습니다. 설치 프로그램과 구성 디렉토리 서버 설치 프로그램과 Active Directory 설치 프로그램과 동기화되는 Directory Server
3DES 키로 암호화 (기본값)	<ul style="list-style-type: none"> Directory Server 커넥터와 Directory Server 플러그인 (모든 데이터) Windows NT 커넥터, Windows NT 비밀번호 필터 DLL 및 Windows NT 변경 검출기 (모든 데이터) 제품의 구성 디렉토리에 있는 모든 중요한 정보 커넥터와 하위 구성요소 사이에 전송된 모든 메시지 (세션당 3DES 키로 암호화) Message Queue 를 통하여 전송된 모든 (로그가 아닌) 메시지

여기에서 논의된 보안 기능의 개요는 에 보이는 것과 같습니다.

그림 11-1) Identity Synchronization for Windows 보안 개요



Message Queue 액세스 제어

Identity Synchronization for Windows 는 Message Queue 의 액세스 제어를 사용하여 메시지 등록과 게시에 대한 무단 액세스를 방지하고 각 커넥터가 수신하는 메시지를 신뢰하도록 합니다.

Message Queue 브로커에 액세스하는 경우 오직 Message Queue 와 커넥터에만 알려진 고유한 사용자 이름과 비밀번호가 제공됩니다. Message Queue 를 통하여 전송되는 각 메시지는 항목당 3DEs 키로 암호화되며, 따라서 메시지 콘텐츠를 보호하고 항목키를 모르는 외부인이 의미 있는 메시지를 전송할 수 없도록 방지합니다. 이 방법을 사용하면 (a) 공격자가 조작된 비밀번호 동기화 메시지를 커넥터로 전송하거나 (b) 공격자가 커넥터를 모방하여 실제 비밀번호 업데이트를 수신할 수 없도록 방지합니다.

참고 기본적으로 커넥터와 시스템 관리자 등 , Message Queue 의 클라이언트는 Message Queue 브로커가 반환하는 모든 SSL 인증서를 허용합니다 . Message Queue 인증서 유효성 검사 강화와 기타 Message Queue 관련 보안 문제에 대한 자세한 내용은 " [보안 강화](#) " [페이지 283](#) 를 참조하십시오 .

디렉토리 자격 증명

커넥터가 동기화되는 Active Directory 와 Directory Server 에서 비밀번호를 변경하려면 특별한 자격 증명이 필요합니다 . 이 특별한 자격 증명은 제품의 구성 디렉토리에 저장되기 전에 암호화됩니다 .

영구 스토리지 보호 요약

Identity Synchronization for Windows 가 디스크에 저장된 중요한 정보를 보호하는 방법은 에 요약된 것과 같습니다 .

표 11-2) 영구 저장 장소 보호

영구 스토리지	자격 증명 정보	보호
Configuration Directory Server 에 저장된 제품의 구성	디렉토리 액세스용 자격 증명과 Message Queue 항목당 3DES 키가 제품의 구성 디렉토리에 저장됩니다 .	제품의 구성 디렉토리에 저장된 모든 중요한 정보는 구성 비밀번호에서 생성되는 3DES 키로 암호화됩니다 . 제품의 구성 디렉토리를 추가로 보호하는 권장 사항은 " 보안 강화 " 를 참조하십시오 .
Directory Server Retro Changelog	Directory Server 플러그인은 비밀번호 변경을 캡처하고 이를 Directory Server Retro Changelog 에 기록 g 하기 전에 암호화합니다 .	Directory Server 플러그인은 모든 사용자 비밀번호 변경을 각 구현에 고유한 3DES 키를 사용하여 암호화합니다 .
Message Queue 브로커 영구 스토리지	Message Queue 브로커는 커넥터 사이에서 전송되는 비밀번호 동기화 메시지를 저장합니다 .	로그 메시지를 제외하고 모든 지속적인 메시지는 항목당 3DES 키로 암호화됩니다 .
Message Queue 브로커 디렉토리 자격 증명	Message Queue 브로커는 제품의 구성 디렉토리에 대하여 사용자를 인증합니다 . 브로커는 코어 설치 동안 제공된 디렉토리 관리 사용자 이름과 비밀번호를 사용하여 구성 디렉토리에 연결합니다 .	디렉토리 비밀번호는 passfile 에 저장되며 , 이 파일은 파일 시스템 액세스 제어로 보호합니다 .

표 11-2) 영구 저장 장소 보호 (계속)

영구 스토리지	자격 증명 정보	보호
시스템 관리자 부트 파일	시스템 관리자의 부트 파일에는 구성에 액세스할 정보가 포함됩니다 . 여기에는 구성 비밀번호와 코어 설치 동안 제공된 디렉토리 관리 사용자 이름 및 비밀번호가 포함됩니다 .	이 파일은 파일 시스템 액세스 제어로 보호됩니다 .
커넥터 및 중앙 기록기 부트 파일	중앙 기록기뿐 아니라 각 커넥터에는 Message Queue 에 액세스하기 위한 자격 증명이 포함된 초기 구성 파일이 있습니다 .	이들 파일은 파일 시스템 액세스 제어로 보호됩니다 .
Directory Server 플러그인 부트 구성	플러그인의 구성은 cn=config 에 저장되며 커넥터에 연결하기 위한 자격 증명이 포함됩니다 .	cn=config 하위 트리는 ACI 와 dse.ldif 파일로 보호되며 , 이는 이 트리를 미러하는 것으로 파일 시스템 액세스 제어로 보호됩니다 .
NT 비밀번호 필터 DLL 및 NT 변경 검출기 부트 구성	NT 하위 구성요소의 구성은 Windows 레지스트리에 저장되며 커넥터로 연결하기 위한 자격 증명이 포함됩니다 .	PDC 레지스트리로의 액세스가 안전하지 않은 경우 이들 레지스트리 키를 액세스 제어로 보호할 수 있습니다 .
Windows 커넥터의 객체 캐시	Windows 커넥터는 해시된 사용자 비밀번호를 커넥터의 객체 캐시에 저장합니다 .	비밀번호는 일반 문자로 저장되는 것이 아니라 MD5 해시로 암호화됩니다 . 이들 데이터베이스 파일은 파일 시스템 액세스 제어로 보호됩니다 (" 보안 강화 " 참조) .

보안 강화

여기에서는 제품의 현재 릴리스에 존재하는 잠재적 보안 취약점에 대하여 설명하고 제품의 기본 구성 외에 보안을 확장 및 강화하는 방법에 대하여 설명합니다 . 다음의 내용으로 구성됩니다 .

- " 구성 비밀번호 " 페이지 284
- " 구성 디렉토리 자격 증명 생성 " 페이지 284
- "Message Queue 클라이언트 인증서 유효성 검사 " 페이지 285
- "Message Queue 자체 서명 SSL 인증서 " 페이지 285
- "Message Queue 브로커 액세스 " 페이지 285
- " 제품의 구성 디렉토리 인증서 유효성 검사 " 페이지 286
- " 구성 디렉토리에 대한 액세스 제한 " 페이지 286

구성 비밀번호

구성 비밀번호는 중요한 구성 정보를 보호하기 위하여 사용하지만 설치 프로그램은 이 비밀번호에 대한 비밀번호 정책을 실행하지 않습니다. 이 비밀번호가 엄격한 지침을 따르도록 하고 쉽게 추측할 수 없는 복잡한 비밀번호를 선택하십시오. 또한 안전한 비밀번호를 위한 표준 정책 지침을 준수하십시오.

예를 들어 비밀번호의 길이는 최소 여덟 문자이어야 하며 대문자, 소문자 및 영문자가 아닌 문자를 포함해야 합니다. 사용자의 이름, 약자 및 날짜를 포함하면 안 됩니다.

구성 디렉토리 자격 증명 생성

제품의 구성 디렉토리가 있는 Directory Server 에 액세스하려면 구성 관리자 그룹에 반드시 자격 증명이 있어야 합니다. 그러나 어떤 이유이든 *admin* 이 아닌 다른 자격 증명을 만들어야 하는 경우 다음 사항을 고려하십시오.

설치 프로그램에는 콘솔 *administrative* 하위 트리에 저장된 사용자용 자격 증명을 입력해야 합니다. 그러나 코어 설치 프로그램은 *admin* 이 아닌 사용자를 "uid=admin,ou=Administrators, ou=TopologyManagement, o=NetscapeRoot" 로 확장하지 않습니다. 따라서 코어 설치 동안 반드시 전체 DN 을 지정해야 합니다.

admin 이 아닌 새 사용자를 만들려면 다음과 같이 합니다.

1. 다음에 사용자를 만듭니다.
ou=Administrators, ou=TopologyManagement, o=NetscapeRoot
2. 구성 관리자 그룹에 새 자격 증명을 추가합니다.
3. 구성 관리 그룹의 이 사용자 또는 모든 사용자가 제품 구성 디렉토리가 저장된 Directory Server 로 액세스할 수 있도록 ACI 를 설정합니다.
4. 코어 설치 동안 전체 DN 을 지정합니다.

Directory Server 에서의 액세스 제어 관리에 대한 자세한 내용은 *Sun Java System Directory Server 5 2004Q2 Administrator's Guide*, 제 6 장 : "Managing Access Control" 을 참조하십시오.

Message Queue 클라이언트 인증서 유효성 검사

기본적으로 커넥터와 시스템 관리자 등, Message Queue 의 클라이언트는 Message Queue 브로커가 반환하는 모든 SSL 인증서를 허용합니다.

1. 이 설정을 무시하려면 Message Queue 클라이언트가 Message Queue 브로커의 인증서에 대한 유효성을 검사해야 합니다. 다음을 편집합니다.

```
<installation_root>/resources/WatchList.properties
```

2. Watchlist.properties 에 있는 각 프로세스의 JVM 에 다음을 추가합니다.

```
-Djavax.net.ssl.trustStore=<keystore_path> -DimqSSLIsHostTrusted=false
```

3. Identity Synchronization for Windows 서비스 또는 데몬을 다시 시작합니다.

javax.net.ssl.trustStore 등록 정보는 브로커 인증서를 신뢰하는 JSEE 키스토어를 가리켜야 합니다. 예를 들어 /etc/imq/keystore 는 브로커가 사용하는 동일한 키스토어이므로 코어가 설치된 컴퓨터에서 사용할 수 있습니다.

Message Queue 자체 서명 SSL 인증서

기본적으로 Message Queue 브로커는 자체 서명한 SSL 인증서를 사용합니다. 다른 인증서를 설치하려면 Java 와 함께 제공되는 keytool 유틸리티를 사용하여 브로커의 키스토어 (Solaris 의 경우 /var/imq/instances/isw-broker/etc/keystore, Windows 2000 의 경우

<mq_installation_root>/var/instances/isw-broker/etc/keystore) 를 수정합니다. 인증서의 별칭은 반드시 imq 이어야 합니다.

Message Queue 브로커 액세스

기본적으로 Message Queue 는 자신의 포트 매핑을 제외한 모든 서비스용 동적 포트를 사용합니다. 방화벽 또는 브로커로 연결할 수 있는 제한된 일련의 호스트에서 브로커에 액세스하려면 브로커가 모든 서비스에 대하여 고정된 포트를 사용해야 합니다.

이렇게 하려면 imq.<service_name>.<protocol_type>.port 브로커 구성 기본 설정을 설정합니다. 자세한 내용은 *Sun Java System Message Queue Administrator's Guide* 를 참조하십시오.

제품의 구성 디렉토리 인증서 유효성 검사

시스템 관리자가 SSL 을 통하여 제품의 구성 디렉토리에 연결할 때 모든 인증서를 허용하며, Message Queue 브로커 또한 SSL 을 통하여 제품의 구성 디렉토리로 연결할 때 모든 인증서를 허용합니다. 현재 시스템 관리자나 Message Queue 브로커가 제품의 구성 디렉토리 SSL 인증서에 대한 유효성을 검사할 방법이 없습니다.

구성 디렉토리에 대한 액세스 제한

코어가 설치되면 제품의 구성 디렉토리가 설치된 Directory Server 에 정보를 추가하는 과정에 액세스 제어 정보를 추가하는 과정이 없습니다. 오직 구성 관리자에게만 액세스를 허용하려면 다음의 ACI 를 사용해야 합니다.

```
(targetattr = "*") (target =
"ldap:///ou=IdentitySynchronization,ou=Services,dc=example,dc=com")
(version 3.0;acl "Test";deny (all)(groupdn != "ldap:///cn=Configuration
Administrators, ou=Groups, ou=TopologyManagement, o=NetscapeRoot");)
```

Directory Server 에서의 액세스 제어 관리에 대한 자세한 내용은 *Sun Java System Directory Server 5 2004Q2 Administrator's Guide*, 제 6 장 : "Managing Access Control" 을 참조하십시오.

복제된 구성 보안

복제본을 사용하여 Directory Server 에 연결하는 구현 또한 [보안 개요](#)에 정의된 동일한 규칙을 준수합니다. 여기에서는 복제된 구성의 예를 제공하고 이 구성에서 SSL 을 사용하는 방법에 대하여 설명합니다.

참고 복제된 구성의 계획, 구현 및 보안에 대한 개요는 [부록 E, "복제 환경 용 설치 노트."](#) 를 참조하십시오.

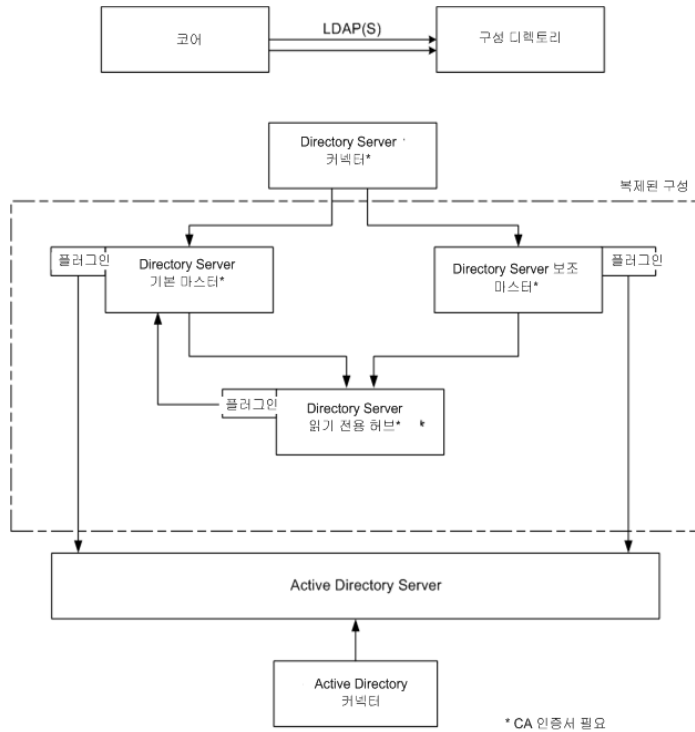
CA 인증서를 필요로 하는 구성 구성요소와 각 인증서가 필요한 위치는 에 보이는 것과 같습니다.

표 11-3) CA 인증서가 필요한 MMR 구성 구성요소

구성요소	CA 인증서 필요
기본 Directory Server 복제본 마스터	Active Directory 시스템
보조 Directory Server 복제본 마스터	Active Directory 시스템
읽기 전용 Directory Server 허브	기본 Directory Server 복제본 마스터 보조 Directory Server 복제본 마스터
Directory Server 커넥터	기본 Directory Server 복제본 마스터 보조 Directory Server 복제본 마스터
Active Directory 커넥터	Active Directory 시스템

는 Identity Synchronization for Windows 가 MMR 구성을 설치한 것이며 , 두 개의 복제된 Directory Server 마스터에 복수 Directory Server 읽기 전용 허브 또는 소비자가 있습니다 . 각 Directory Server 에는 플러그인이 있으며 Directory Server 커넥터 한 개 , Active Directory 시스템 한 개 및 Active Directory 커넥터 한 개만 있습니다 .

그림 11-2) 복제된 구성



참고

Directory Server가 SSL 용으로 구성되는 경우 반드시 복제본 Directory Server가 기본 및 보조 Directory Server 인증서를 모두 신뢰하는지 확인해야 합니다. 이는 또한 Directory Server 허브 또는 읽기 전용 복제본이 있는 시스템에 설치하는 other 유형의 모든 Directory Server 플러그인에도 마찬가지입니다.

디렉토리 서버 플러그인은 CA 인증서가 디렉토리 서버에 연결되면 동일한 인증서로 액세스할 수 있습니다.

idsync certinfo 사용

현재 Identity Synchronization for Windows SSL 설정에서 필요한 인증서를 판단하려면 idsync certinfo 유틸리티를 사용합니다. idsync certinfo 를 실행하여 각 인증서 데이터베이스에 어느 인증서가 필요한지의 정보를 불러옵니다.

참고

디렉토리 서버 소스를 SSL 용으로 구성하는 경우 모든 디렉토리 하위 구성요소 또는 플러그인에 대하여 복제본 디렉토리 서버가 기본 및 보조 디렉토리 서버 소스 인증서를 모두 신뢰해야 합니다.

Identity Synchronization for Windows 가 SSL 연결 (모든 인증서 신뢰 설정 사용) 을 시도하고 서버의 호스트 이름이 SSL 협상 단계 동안 서버가 제시한 인증서에 있는 호스트 이름과 일치하지 않는 경우

Identity Synchronization for Windows 커넥터는 연결의 설정을 거부합니다.

Identity Synchronization for Windows 구성의 디렉토리 소스 호스트 이름은 반드시 항상 해당 디렉토리 소스가 사용하는 인증서에 포함된 호스트 이름과 일치해야 합니다.

인수

idsync certinfo 하위 명령과 함께 사용할 수 있는 인수는 와 같습니다.

표 11-4) certinfo 인수

인수	설명
-h <CR-hostname>	구성 디렉토리 호스트 이름을 지정합니다. 이 인수는 코어 설치 동안 지정한 값을 기본값으로 사용합니다.
-p <CR-port-no>	구성 디렉토리 LDAP 포트 번호를 지정합니다. ((기본값은 389 입니다.))
-D <bind-DN>	구성 디렉토리 바인드 고유 이름 (DN) 을 지정합니다. 이 인수는 코어 설치 동안 지정한 값을 기본값으로 사용합니다.
-w <bind-password ->	구성 디렉토리 바인드 비밀번호를 지정합니다. 값이 - 이면 표준 입력 (STDIN) 에서 비밀번호를 읽습니다.
-s <rootsuffix>	구성 디렉토리 rootsuffix 를 지정합니다. 여기에서 rootsuffix 는 dc=example,dc=com 등의 고유한 이름입니다. 이 인수는 코어 설치 동안 지정한 값을 기본값으로 사용합니다.

표 11-4) certinfo 인수 (계속)

인수	설명
-q <configuration_password>	구성 비밀번호를 지정합니다. 값이 - 이면 표준 입력 (STDIN) 에서 비밀번호를 읽습니다.

사용법

다음 예제에서는 idsync certinfo 를 사용하여 SSL 통신에서 실행하도록 지정된 시스템 구성요소를 검색합니다. 이 예의 결과로 두 개의 커넥터 (CNN101 및 CNN100) 가 확인되었으며 적절한 CA 인증서를 가져올 위치에 대한 설명이 제공됩니다.

```
:\Program Files\Sun\MPS\isw-hostname\bin> idsync certinfo -h CR-hostname
-p 389 -D "cn=Directory Manager" -w dirmanager -s dc=example,dc=com
-q <password>
Connector: CNN101
Certificate Database Location: C:\Program Files\Sun\MPS\isw-hostname\etc\CNN101
Get &#xD5;Active Directory CA&#xD5; certificate from Active Directory and import into Active
Directory Connector certificate db for server ldaps://hostname.example.com:636
Connector: CNN100
Certificate Database Location: C:\Program Files\Sun\MPS\isw-hostname\etc\CNN100
Export &#xD5;Directory Server CA&#xD5; certificate from Directory Server certificate db and import
into Directory Server Connector certificate db ldaps://hostname.example.com:636
Export &#xD5;Active Directory CA&#xD5; certificate from Active Directory Server
hostname.example.sun.com:389 and import into Directory Server Server certificate db for server
ldaps://hostname.example.com:638
SUCCESS
```

Directory Server 에서 SSL 사용

자체 서명을 사용하는 Directory Server 에서 SSL 을 사용하도록 설정하려면 다음과 같이 합니다.

참고	이 설명은 편의를 위하여 간단히 축약되었습니다. 자세한 내용은 <i>Directory Server 5 2004Q2 Administrator's Guide</i> 를 참조하십시오.
-----------	---

참고

- Windows 의 경우 Directory Server 5 2004Q2 이상과 함께 제공된 certutil 을 사용합니다.
5 2004Q2 이전 버전의 Directory Server 와 함께 제공되는 certutil 을 사용하면 *안 됩니다*. 이전 버전의 certutil 는 Identity Synchronization for Windows 과 호환되지 않습니다.
- Solaris 의 경우 /usr/sfw/bin 에 기본으로 설치된 certutil 을 사용합니다.

1. 다음을 입력하여 디렉토리 서버용 키 인증서 데이터베이스를 새로 만듭니다.

```
C:\Program Files\Sun\WPS\shared\bin\certutil.exe -d . -P slapd-hostname-
```

데이터베이스 생성을 완료하려면
반드시 이 키와 이후의 키를 암호화할
때 사용할 비밀번호를 입력해야 합니다.
비밀번호는 8 문자 이상이어야 하며
반드시 영문자가 아닌 문자를 하나 이상 포함해야 합니다.
새 비밀번호 입력:
비밀번호 재입력:

참고

이 예는 서버 루트 바로 아래에 있는 alias 디렉토리에서 실행하는 경우입니다. 그렇지 않은 경우 디렉토리 서버가 인증서 데이터베이스를 찾을 수 없습니다.

2. 자체 서명한 인증서를 생성합니다. 이 인증서는 디렉토리가 사용하는 서버 인증서가 됩니다. 반드시 Directory Server 가 실행되는 위치의 서버 호스트 이름에 따라 대상 DN 을 선택해야 합니다.

참고

기본적으로 자체 서명된 인증서는 3 개월 동안 유효합니다. 이 기간을 변경하려면 -v <months-valid> 옵션을 사용합니다. 예를 들어 기간을 24 개월로 늘리려면 -v 21 을 입력하고 기간을 1 개월로 줄이려면 -v -2 를 입력합니다.

```
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -d . -P slapd-hostname- -S -n server-cert -s
"cn=hostname.example.com,c=us" -x -t CTu,,
A random seed must be generated that will be used in the
creation of your key. One of the easiest ways to create a
random seed is to use the timing of keystrokes on a keyboard.
To begin, type keys on the keyboard until this progress meter
is full. DO NOT USE THE AUTOREPEAT FUNCTION ON YOUR KEYBOARD!
Continue typing until the progress meter is full:
|*****|
Finished. Press enter to continue:
Enter Password or Pin for "NSS Certificate DB":
Generating key. This may take a few moments...
```

3. 검사 용도의 인증서가 표시됩니다 .

```
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -L -d . -P slapd-hostname-
인증서 이름      신뢰 속성
server-cert      CTu,,
p  유효한 피어
P  신뢰된 피어 (p 포함 )
c  유효한 CA
T  클라이언트 인증서 발행을 위한 신뢰된 CA (c 포함 )
C  인증서에 대한 신뢰된 CA (SSL 용 서버 인증서 전용 ) (c 포함 )
u  사용자 인증서
w  경고 보냄
```

4. Directory Server를 재시작할 때마다 인증서 데이터베이스 암호를 다시 입력하지 않도록 PIN 파일을 만듭니다 .

```
C:\Program Files\Sun\MPS\alias > echo Internal (Software) Token:<secret12>
slapd-hostname-pin.txt
```

5. 다음과 같이 Directory Server 에서 SSL 을 사용 설정합니다 .

- a. 콘솔을 엽니다 .
- b. Configuration 탭을 선택합니다 .
- c. Encryption 탭 (오른쪽 창) 을 선택합니다 .
- d. 이 서버에 SSL 사용을 선택합니다 .

- e. Use this cipher family: RSA 를 선택합니다 .
- f. Save 를 누르고 OK 를 두 번 누릅니다 .
- g. Network 탭을 선택합니다 .
- h. Secure Port 필드를 업데이트합니다 . Active Directory 와 동일한 컴퓨터에서 실행되는 경우 포트를 반드시 636 에서 사용하지 않는 포트로 변경해야 하며 , 변경하지 않으면 Directory Server 가 시작되지 않습니다 .
- i. Save 를 누른 후 OK 를 누릅니다 .
- j. Tasks 탭 (상단) 을 선택합니다 .
- k. Restart Directory Server 를 누른 후 Yes 를 누릅니다 .

디렉토리 서버 인증서 데이터베이스에서 CA 인증서 불러오기

Directory Server 에서 SSL 을 사용하는지 확인하십시오 . 디렉토리 서버 인증서를 임시 파일로 내보내어 이를 다시 디렉토리 서버 커넥터의 인증서 데이터베이스로 가져오도록 하려면 다음 명령을 사용합니다 .

```
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -L -d . -P slapd-hostname-  
-n server-cert -a > C:\s-cert.txt
```

이 예는 서버 루트 바로 아래에 있는 alias 디렉토리에서 실행하는 경우입니다 . 그렇지 않은 경우 디렉토리 서버가 인증서 데이터베이스를 찾을 수 없습니다 .

Active Directory 커넥터에서 SSL 사용

Identity Synchronization for Windows SSL 을 통한 Active Directory SSL 인증서를 자동으로 불러 오며 이를 커넥터용으로 제공한 동일한 인증서를 사용하는 커넥터의 인증서 데이터베이스로 가져옵니다 .

그러나 오류가 발생하는 경우 (예 : 잘못된 인증서 또는 SSL 인증서를 찾은 경우) Active Directory CA 인증서를 불러와 이를 커넥터 인증서 데이터베이스에 추가할 수 있습니다 . 방법은 다음 부분을 참조하십시오 .

- ["Active Directory 인증서 불러오기 " 페이지 294](#)
- [" 커넥터의 인증서 데이터베이스에 Active Directory 인증서 추가 " 페이지 295](#)

Active Directory 인증서 불러오기

오류가 발생하는 경우 certutil(Windows 2000/2003 과 함께 제공되는 프로그램) 또는 LDAP 를 사용하여 다음의 설명과 같이 Active Directory 인증서를 불러올 수 있습니다.

참고 여기에서 설명하는 certutil 는 이전 설명서에서 설명한 Directory Server 와 함께 제공되는 certutil 명령과 *다릅니다*.

Windows certutil 사용

certutil 프로그램을 사용하여 Active Directory 인증서를 불러오려면 다음과 같이 합니다.

1. Active Directory 컴퓨터에서 다음 명령을 사용하여 인증서를 내보냅니다.
`C:\>certutil -ca.cert cacert.bin`
2. 그런 다음 cacert.bin 파일을 인증서 데이터베이스로 가져올 수 있습니다.

LDAP 사용

LDAP 를 사용하여 Active Directory 인증서를 불러오려면 다음과 같이 합니다.

1. Active Directory 에 대하여 다음 검색을 수행합니다.

```
ldapsearch -h <CR-hostname> -D <administrator_DN> -w <administrator_password> -b "cn=configuration,dc=put,dc=your,dc=domain,dc=here" "cacertificate=*"

```

여기에서 <administrator_DN> 은 다음과 같을 것입니다.

```
cn=administrator,cn=users,dc=put,dc=your,dc=domain,dc=here

```

이 예에서 도메인 이름은 다음과 같습니다. <put.your.domain.name.here>.
서버 항목은 검색 필터와 일치합니다. 해당 DN 에 cn=Certification Authorities, cn=Public Key Services 를 사용하는 항목이 필요합니다.
2. 텍스트 편집기를 열고 첫 번째 CA 인증서 속성(BASE-64 암호화 텍스트 블록)의 첫 번째 값을 잘라냅니다. 이 값(텍스트 블록)을 텍스트 편집기로 (값만) 붙여 넣습니다. 공백으로 시작하는 줄이 없도록 내용을 편집합니다.
3. 첫 줄 앞에 -----BEGIN CERTIFICATE----- 를 추가하고 마지막 줄 뒤에 -----END CERTIFICATE----- 를 추가합니다. 다음 예를 참조하십시오.

-----BEGIN CERTIFICATE-----

```

MIIDvjCCA2igAwIBAgIQDgoyk+Tu14NGoQnxhmNHLjANBgkqhkiG9w0BAQUFA
DCBjijEeMBwGCSqGSIb3DQEJARYPYmVydG9sZEBzdW4uY29tMQswCQYDVQ
UzELMAkGA1UECBMCFVgxZDZANBgNVBACTBK1c3RpbjEzMBCGA1UEChMQU3
Y3Jvc3lzdGVtczEQMA4GA1UECXMHaVBsYW5ldDEUMBGA1UEAxMLUmVzdGF
1cmFudHMwHhcNMDIwMTExMDA1NDA5W5hcnMTIwMTExMDA1OTQ2WjCBjijEeMBwGCSqGSIb3
DQEJARYPYmVydG9sZEBzdW4uY29tMQswCQYDVQQUJVEUJELMAkGA1UECBMCFV
gxZDZANBgNVBACTBK1c3RpbjEzMBCGA1UEChMQU3VulE1pY3Jvc3lzdGVtczEQMA4GA
1UECXMHaVBsYW5ldDEUMBGA1UEAxMLUmVzdGF1cmFudHMwXDANBgkqhkiG9w0BA
QEFAANLADBIaEAYekZa8gwwhw3rLK3eV/12St1DVUsg31LOu3CnB8cMHQZXlgiUgtQ0h
m2kpZ4nEhwCAHhFLD3ilhIP4BGWQFjcwIDAQABo4IBnjCCAZowEwYJKwYBBAGCNxQC
BAYeBABDAEEwCwYDVR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFJ5Bgt6Oypq7T8Oykw4LH6ws2d/IMIbMgYDVR0fBIIBKTCASUwgdOggdCggc2Gg
cpsZGFwOi8vL0NOPVJlc3RhdXJhbnRzLENOPWRvd2l0Y2hlcixDTj1DRFAsQ049UHVibGlj
TlwsS2V5JTlwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1yZXN0
YXVyYW50cyxEQz1jZW50cmFsLERDPXN1bixEQz1jb20/Y2VydGlmZWVhdGV5S2V5Y2F0
aW9uTGldD9iYXNIP29iamVjdGNSYXNzPWNSTERpc3RyaWJ1dGlvbIbvaW50ME2gS6BJ
hkdotHRwOi8vZG93aXRjaGVyLnJlc3RhdXJhbnRzLmNlbnRyYVwuc3VulmNvbS9DZXJ0R
W5yb2xsL1Jlc3RhdXJhbnRzLmNybDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BA
QUFAANBAL5R9R+ONDDVHWu/5Sd9Tn9dpxN8oegjS88ztv1HD6XSTDzGTuaaVebSZV3I
+ghSInsgQbH0gW4fGRwal BvePI4=

```

-----END CERTIFICATE-----

4. 인증서를 파일 (ad-cert.txt 등)에 저장합니다.
5. 그런 다음 이 파일(ad-cert.txt 등)을 인증서 데이터베이스로 가져옵니다. 방법은 다음 단원 "[커넥터의 인증서 데이터베이스에 Active Directory 인증서 추가](#)"로 계속하십시오.

커넥터의 인증서 데이터베이스에 Active Directory 인증서 추가

이 방법은 커넥터를 설치한 후 Active Directory 커넥터에 대하여 SSL을 사용하도록 설정하였거나 설치 동안 잘못된 자격 증명을 입력한 경우에만 사용됩니다.

1. Active Directory 커넥터가 설치된 컴퓨터에서 Identity Synchronization for Windows 서비스 / 데몬을 정지시킵니다.

2. 다음 방법 중 한 가지를 사용하여 Active Directory CA 인증서를 불러옵니다.
 - "Windows certutil 사용 " 페이지 294
 - "LDAP 사용 " 페이지 294
3. Active Directory 커넥터에 커넥터 ID CNN101 (커넥터 ID 와 이 커넥터가 관리하는 디렉토리 소스로의 매핑은 logs/central/error.log 참조)이 있는 경우 커넥터가 설치된 컴퓨터의 해당 인증서 데이터베이스 디렉토리로 이동하여 인증서 파일을 가져옵니다.
 - certutil 을 사용하여 인증서를 불러온 경우 다음을 입력합니다.


```
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -A -d . -n ad-ca-cert -t C,, -i \cacert.bin
```
 - LDAP 를 사용하여 인증서를 불러온 경우 다음을 입력합니다.


```
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -A -d . -n ad-ca-cert -t C,, -a -i \ad-cert.txt
```
4. Identity Synchronization for Windows 서비스 / 데몬을 다시 시작합니다.

참고

Directory Server certutil.exe 는 Directory Server 5 2004Q2 를 설치할 때 자동으로 설치되므로 Directory Server 가 없는 컴퓨터에 설치된 커넥터로는 CA 인증서를 추가할 수 없습니다.

최소한 Active Directory 커넥터가 설치된 서버에 반드시 Directory Server 5 2004Q2 패키지의 Sun Java System 서버 기본 라이브러리와 Sun Java System 서버 시스템 라이브러리를 설치해야 합니다. (Administration Server 또는 Directory Server 구성요소는 설치할 필요 없습니다.)

또한 콘솔에서 JRE 하위 구성요소를 선택해야 합니다 (제거 기능용).

Directory Server 로 Active Directory 인증서 추가

다음과 같이 Directory Server 인증서 데이터베이스에 Active Directory CA 인증서를 추가합니다.

참고

Directory Server 에서 SSL 을 사용하는지 확인하십시오 .

1. 다음 방법 중 한 가지를 사용하여 Active Directory CA 인증서를 불러옵니다.
 - "Windows certutil 사용 " 페이지 294
 - "LDAP 사용 " 페이지 294
2. Directory Server 를 정지합니다.
3. 디렉토리 서버가 설치된 컴퓨터에서 다음과 같이 Active Directory CA 인증서를 가져옵니다.
 - certutil 을 사용하여 인증서를 불러온 경우 다음을 입력합니다.


```
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -A -d . -P slapd-hostname- -n ad-ca-cert -t C,, -i \cacert.bin
```
 - LDAP 를 사용하여 인증서를 불러온 경우 다음을 입력합니다.


```
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -A -d . -P slapd-hostname- -n ad-ca-cert -t C,, -a -i \ad-cert.txt
```
4. Directory Server 를 시작합니다.

Directory Server 커넥터에 Directory Server 인증서 추가

Directory Server 플러그인과 Active Directory 사이에 SSL 통신을 사용하도록 설정한 경우 반드시 Active Directory CA 인증서를 각 Directory Server 마스터의 인증서 데이터베이스에 추가해야 합니다. 다음과 같이 합니다.

1. Directory Server 커넥터가 설치된 컴퓨터에서 Identity Synchronization for Windows 서비스 / 도메인을 정지합니다.
2. 디렉토리 서버 CA 인증서를 불러옵니다.
3. 디렉토리 서버 커넥터에 커넥터 ID CNN100(커넥터 ID와 이 커넥터가 관리하는 디렉토리 소스로의 매핑은 logs/example/error.log 참조) 이 있는 경우 커넥터가 설치된 컴퓨터의 인증서 데이터베이스 디렉토리로 이동하여 cacert.bin 파일을 가져옵니다.

```
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -A -d . -n ds-cert -t C,, -i C:\s-cert.txt
```

참고	인증서가 ASCII 형식으로 구해지는 경우 certutil 명령줄에 "-a" 인수를 추가하여 해당 인증서가 이진 형식이 아닌 ASCII 형식임을 표시합니다.
-----------	---

4. Identity Synchronization for Windows 서비스 / 데몬을 다시 시작합니다.

부록 A, "Identity Synchronization for Windows 명령줄 유틸리티
사용 "

부록 B, "LinkUsers XML 문서 예제 "

부록 C, "Solaris 에서 루트가 아닌 사용자로 서비스 실행 "

부록 D, "Synchronization User List 정의 및 구성 "

부록 E, " 복제 환경용 설치 노트 "

Identity Synchronization for Windows 명령줄 유틸리티 사용

Identity Synchronization for Windows에서는 명령줄을 사용하여 다양한 작업을 수행할 수 있습니다. 이 부록에서는 Identity Synchronization for Windows 명령줄 유틸리티를 실행하여 다양한 작업을 수행하는 방법에 대하여 설명합니다. 정보는 다음과 같이 구성되었습니다.

- " 공통 기능 " 페이지 302
- "idsync 명령 사용 " 페이지 306
- "forcepwchg 마이그레이션 유틸리티 사용 " 페이지 321

공통 기능

Identity Synchronization for Windows 명령줄에는 다음 기능이 공통으로 포함됩니다.

- " 공통 인수 " 페이지 302
- " 비밀번호 입력 " 페이지 305
- " 도움말 열기 " 페이지 305

공통 인수

여기에서는 대부분의 명령줄 유틸리티에 공통적인 인수 (옵션) 에 대하여 설명합니다. 내용은 다음의 표와 같이 구성되었습니다.

- [표 A-1\) 모든 하위 명령에 공통된 인수](#): 다음 인수를 설명하며 이는 idsync 하위 명령 (*prepds 제외*) 및 마이그레이션 도구에 공통입니다.

```
-D <bind-DN> -w <bind-password> | -> [-h <Configuration Directory-hostname>]  
[-p <Configuration Directory-port-no>] [-s <rootsuffix>] [-Z] [-P <cert-db-path>]  
[-m <secmod-db-path>]
```

참고

대괄호 ([]) 는 선택 사항 인수를 나타냅니다 .

Identity Synchronization for Windows 설치 프로그램은 설치 동안 입력한 정보를 기준으로 -h, -p, -D 및 -s 인수의 값을 자동으로 입력합니다 . 그러나 명령줄에서 다른 값을 지정하여 기본 값을 대체할 수 있습니다 .

복수 바이트 문자를 지원하려면 Identity Synchronization for Windows base64 가 명령줄 인터페이스 (CLI) 환경 파일의 -s <rootsuffix> 및 -D <bind-DN> 의 기본 값을 암호화해야 합니다 . rootsuffix 기본값은 변경되면 안 됩니다 . 바인드 DN 기본값은 명령줄에서 대체하거나 CLI 환경 파일에서 적절한 base64 암호화 값으로 업데이트할 수 있습니다 .

- [표 A-2\) 모든 하위 명령에 공통적인 SSL 관련 인수](#) : SSL(Secure Socket Layer)을 사용하여 안전하게 구성 Directory Server 로 액세스하는 정보를 제공하는 선택 옵션입니다 . 이들 인수는 또한 모든 idsync 하위 명령과 이전 도구에 공통적인 인수입니다 .
- [표 A-3\) 구성 디렉토리 인수](#) : 구성 디렉토리에 관련된 인수입니다 . 이들 인수는 둘 이상의 idsync 하위 명령 및 이전 도구에 공통인 인수입니다 .

참고	특정 하위 명령에 고유한 인수는 관련 하위 명령 부분에서 설명합니다 .
----	---

표 A-1) 모든 하위 명령에 공통된 인수

인수	설명
-h <Configuration Directory-hostname>	구성 디렉토리 호스트 이름을 지정합니다 . 이 인수는 코어 설치 동안 지정한 값을 기본값으로 사용합니다 .
-p <Configuration Directory-port-no>	구성 디렉토리 LDAP 포트 번호를 지정합니다 .
-D <bind-DN>	구성 디렉토리 바인드 고유 이름 (DN) 을 지정합니다 . 이 인수는 코어 설치 동안 지정한 값을 기본값으로 사용합니다 .
-w <bind-password ->	구성 디렉토리 바인드 비밀번호를 지정합니다 . 값이 - 이면 표준 입력 (STDIN) 에서 비밀번호를 읽습니다 .
-s <rootsuffix>	구성 디렉토리 rootsuffix 를 지정합니다 . 여기에서 rootsuffix 는 dc=example , dc=com 등의 고유한 이름입니다 . 이 인수는 코어 설치 동안 지정한 값을 기본값으로 사용합니다 .
-q <configuration_password ->	구성 비밀번호를 지정합니다 . 값이 - 이면 표준 입력 (STDIN) 에서 비밀번호를 읽습니다 . 이 인수는 prepds 를 제외한 모든 하위 명령에 대하여 «b°»입니다 .

표 A-2) 모든 하위 명령에 공통적인 SSL 관련 인수

인수	설명
-Z	SSL 을 사용하여 보안 통신을 제공하도록 지정합니다 . 명령줄 인터페이스 또는 기본 / 보조 Directory Server 에 액세스하는 구성 디렉토리로 연결하는 경우 인증서 기반 클라이언트 인증을 제공합니다 .
-P <cert-db-path>	클라이언트 인증서 데이터베이스의 경로와 파일 이름을 지정합니다 . 이 인증서 데이터베이스에는 반드시 Directory Server 의 인증서 데이터베이스에 서명하는 데 사용하는 CA 인증서가 있어야 합니다 . -Z 는 지정하고 -P 는 사용하지 않는 경우 , <cert-db-path> 의 기본값으로 <current-working-directory>/cert8.db 이 사용됩니다 . 참고 : Identity Synchronization for Windows 가 지정한 디렉토리에서 인증서 데이터베이스를 찾을 수 없는 경우 프로그램을 해당 디렉토리에 " 빈 " 디렉토리를 만들면 , 이는 cert8.db, key3.db 및 secmod.db 의 세 가지 파일로 구성됩니다 .
-m <secmod-db-path>	보안 모듈 데이터베이스의 경로를 지정합니다 . 예 : /var/Sun/MPS/slapd-<serverID>/secmod.db 보안 모듈 디렉토리가 인증서 데이터베이스 자체와 다른 디렉토리에 있는 경우에만 이 옵션을 지정합니다 .

표 A-3) 구성 디렉토리 인수

인수	설명
-a <ldap_filter> forcepwchg 및 resync 하위 명령과 함께 사용합니다 .	소스 SUL 에서 사용자를 불러올 때 사용하는 LDAP 필터를 지정하고 사용자가 지정한 SUL 에 해당하는지 판단하기 전에 지목된 일부 해당 사용자를 디렉토리에서 불러올 수 있습니다 .
-f <filename> export10cnf, importcnf, 및 resync 하위 명령과 함께 사용합니다 .	구성 XML 문서 파일의 이름을 지정합니다 .
-n forcepwchg, importcnf 및 resetconn 하위 명령과 함께 사용합니다 .	실제 변경 없이 작업의 효과를 미리 볼 수 있도록 안전 모드에서 실행합니다 .

비밀번호 입력

비밀번호 인수 (-w <bind-password> 또는 -q <configuration_password> 등)가 필요한 경우 해당 비밀번호에 "-" 인수를 사용하여 STDIN에서 비밀번호를 읽을 수 있습니다.

복수 비밀번호 옵션에 "-" 값을 사용하면 idsync에 인수의 순서를 기준으로 하여 비밀번호를 입력하라는 프롬프트가 표시됩니다.

이 경우 프로그램은 우선 <bind-password>를 찾은 후, <configuration-password>를 찾습니다.

도움말 열기

다음 명령 중 한 가지를 사용하여 명령 콘솔에서 idsync 또는 해당 하위 명령에 대한 사용 방법을 표시할 수 있습니다.

- -help
- --help
- -?

사용 정보

- idsync 정보 (유효한 하위 명령 목록 포함)를 보려면 명령 프롬프트에서 앞의 도움말 옵션 중 한 가지를 입력하고 Return을 누릅니다.
- 하위 명령 정보는 명령 프롬프트에서 해당 하위 옵션과 도움말 옵션을 입력하고 Return을 누릅니다.

idsync 명령 사용

idsync 명령을 다음 하위 명령과 함께 사용하여 Identity Synchronization for Windows 명령줄 유틸리티를 실행할 수 있습니다.

참고

idsync 명령을 사용하면 인수를 Directory Server 로 전송하기 전에 모든 DN 값 인수 (바인드 DN 또는 접미어 이름 등) 가 해당 창에 대하여 지정된 문자 세트에서 UTF-8 로 변환됩니다.

접미어 이름에서는 이스케이프 문자로 백슬래시를 사용하면 안 됩니다.

Solaris 에서 UTF-8 문자를 지정하려면 터미널 창의 로케일이 반드시 UTF-8 을 기반으로 해야 합니다. 환경 변수의 LC_CTYPE 및 LANG. 가 올바르게 설정되었는지 확인하십시오.

별도로 명시하지 않는 한 다음 방법 중 한 가지를 사용하여 하위 명령이 있는 idsync 명령을 실행할 수 있습니다.

- Solaris:**
 - a. 터미널 창을 열고 **cd** 명령으로 /opt/SUNWisw/bin 디렉토리로 이동합니다.
 - b. 다음과 같이 idsync 명령을 하나의 하위 명령과 함께 입력합니다.
idsync < 하위 명령 >
- Windows:**
 - a. 명령 창을 열고 **cd** 명령으로 <install_path>\isw-<hostname>\bin 디렉토리로 이동합니다.
 - b. 다음과 같이 idsync 명령을 하나의 하위 명령과 함께 입력합니다.
idsync < 하위 명령 >

idsync 유틸리티 하위 명령과 용도는 의 목록과 같습니다.

표 A-4) idsync 하위 명령 빠른 참조

하위 명령	용도
certinfo	구성 및 SSL 설정에 기반하여 인증서 정보를 표시합니다. ("certinfo 사용 " 페이지 307 참조)

표 A-4) idsync 하위 명령 빠른 참조

하위 명령	용도
changepw	Identity Synchronization for Windows 구성 비밀번호를 변경합니다. ("changepw 사용" 페이지 308 참조)
importcnf	내보내진 Identity Synchronization for Windows 버전 1.0 구성 XML 문서를 가져옵니다 ("importcnf 사용" 페이지 309 참조)
prepsds	Identity Synchronization for Windows 가 사용하도록 Sun Java 시스템 Directory Server 소스를 준비합니다 ("prepsds 사용" 페이지 310 참조)
printstat	설치 / 구성 과정을 완료하기 위하여 반드시 수행해야 하는 단계 목록을 표시합니다. 또한 설치된 커넥터, 시스템 관리자 및 Message Queue 의 상태를 제공합니다 ("printstat 사용" 페이지 314 참조).
resetconn	구성 디렉토리의 커넥터 상태를 <i>uninstalled</i> 로 재설정합니다. ("resetconn 사용" 페이지 315 참조)
resync	설치 과정의 일부분으로 기존 사용자를 링크 및 재동기화하고 디렉토리를 미리 채웁니다 ("resync 사용" 페이지 316 참조).
startsync	동기화를 시작합니다 ("startsync 사용" 페이지 318 참조).
stopsync	동기화를 시작합니다 ("stopsync 사용" 페이지 319 참조).

certinfo 사용

certinfo 하위 명령을 사용하여 구성 및 SSL 설정에 따른 인증서 정보를 표시할 수 있습니다. 이 정보는 각 커넥터 및 Directory Server 플러그인 인증서 데이터베이스에 반드시 추가되어야 하는 인증서를 결정하는 데 도움이 됩니다.

인증서 정보를 표시하려면 터미널 창 (또는 명령 창) 을 열고 다음과 같이 **idsync certinfo** 를 입력합니다.

```
idsync certinfo [<bind-DN>] -w <bind-password | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q
<configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
```

참고

certinfo 하위 명령은 커넥터 및 Directory Server 의 인증서 데이터베이스에 액세스할 수 없으므로 목록의 일부 필수 단계가 이미 수행되었을 수 있습니다.

예 :

```
idsync certinfo -w <admin-password> -q <configuration-password>
```

참고	certinfo 인수에 대한 자세한 내용은 " 공통 인수 " 페이지 302 를 참조 하십시오 .
----	---

changepw 사용

changepw 하위 명령을 사용하여 Identity Synchronization for Windows 구성 비밀번호 호를 변경할 수 있습니다 .

Identity Synchronization for Windows 의 구성 비밀번호를 변경하려면 다음과 같이 합니다 .

- 1. 모든 Identity Synchronization for Windows 프로세스를 정지합니다 . (예 : 시스템 관리자 , 중앙 기록기 , 커넥터 , 콘솔 , 설치 / 제거 프로그램)
- 2. 모든 프로세스를 정지한 후 구성 디렉토리를 ldif 로 내보내어 ou=Services 트리 를 백업합니다 .
- 3. 다음과 같이 **idsync changepw** 명령을 입력합니다 .

```
idsync changepw [-D <bind-DN>] -w <bind-password> | -> [-h <Configuration Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>]
-q <configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
-b <new password> | - > [-y]
```

예 :

```
idsync changepw -w <admin password> -q <old config password> -b -q <new config password>
```

다음 인수는 changepw 에 고유 한 인수입니다 .

표 A-5) idsync changepw 인수

인수	설명
-b <password>	새 구성 비밀번호를 지정합니다 . 값이 - 이면 표준 입력 (STDIN) 에서 비밀번호를 읽습니다 .
[-y]	명령 확인용 프롬프트를 표시하지 않습니다 .

참고

기타 changepw 인수에 대한 자세한 내용은 "공통 인수" 페이지 302 를 참조하십시오 .

4. 터미널 창에 표시된 메시지에 대한 응답을 입력합니다 .
예 :

```
Are you sure that want to change the configuration password (y/n)? yes
시스템을 다시 시작하기 전에 반드시 $PSWHOME/resources/SystemManagerBootParams.cfg
파일을 편집하고 "deploymentPassword" 를 새 값으로 변경해야 합니다 .

SUCCESS
```

5. 시스템을 다시 시작하기 전에 반드시 SystemManagerBootParams.cfg 파일을 수정해야 합니다 .

\$PSWHOME/resources(여기에서 \$PSWHOME 은 <isw- 설치 디렉토리>) 의 SystemManagerBootParams.cfg 에는 시스템 관리자가 구성 디렉토리에 연결할 때 사용하는 구성 비밀번호가 있습니다 .

예를 들어 다음과 같이 비밀번호 값을 변경할 수 있습니다 .

변경 전 : <Parameter name="manager.configReg.deploymentPassword" value="oldpassword" />

변경 후 : <Parameter name="manager.configReg.deploymentPassword" value="newpassword" />

6. 프로그램에 오류가 보고되면 단계 2에서 ldif를 사용하여 구성 디렉토리를 복구하고 다시 하십시오 . 오류의 가장 큰 원인은 비밀번호 변경 도중 구성 디렉토리를 호스팅하는 Directory Server 가 사용 할 수 없게 되기 때문입니다 .

importcnf 사용

주의

Identity Synchronization for Windows 1.0 또는 1.0 SP1 에서 버전 1 2004Q3 으로 이전하는 경우에만 idsync importcnf 를 사용합니다 .

코어 (제 3 장 , " 코어 설치 ") 를 설치한 후 , idsync importcnf 하위 명령을 사용하여 내보낸 Identity Synchronization for Windows 버전 1.0(SP1) 구성 XML 파일을 가져옵니다 . 여기에는 코어 구성 정보가 있습니다 .

버전 1.0 구성 XML 문서를 가져오려면 터미널 창 (또는 명령 창) 을 열고 다음과 같이 **idsync importcnf** 명령을 입력합니다 .

```
idsync importcnf [-D <bind-DN>] -w <bind-password | -> [-h <Configuration Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q <configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>] -f <filename> [-n]
```

예 :

```
idsync importcnf -w <admin_password> -q <configuration_password> -f "MyConfig.cfg"
```

다음 인수는 importcnf 에 고유한 인수입니다 .

표 A-6) idsync importcnf 인수

인수	설명
-f <filename>	구성 XML 문서 파일의 이름을 지정합니다 .
-n	실제 변경 없이 작업의 효과를 미리 볼 수 있도록 안전 모드에서 실행합니다 .

참고	기타 importcnf 인수에 대한 자세한 내용은 " 공통 인수 " 페이지 302 를 참조하십시오 .
-----------	--

버전 1.0 구성 XML 문서를 가져온 후 반드시 동기화용으로 구성된 모든 Directory Server 소스에서 prepds 를 실행합니다 ("prepds 사용 " 페이지 310 참조) . 그런 후 Identity Synchronization for Windows 커넥터와 하위 구성요소를 설치할 수 있습니다 .

prepds 사용

prepds 하위 명령을 사용하여 Identity Synchronization for Windows 가 사용할 Sun Java 시스템 Directory Server 소스를 준비합니다 . Directory Server 커넥터를 설치하기 전에 반드시 prepds 를 실행해야 합니다 .

idsync prepds 하위 명령을 실행하면 적절한 ACI 를 `cn=changelog` 항목에 적용하며 , 이 항목은 Retro-Changelog 데이터베이스의 루트 노드입니다 .

- Identity Synchronization for Windows 가 사용하도록 *preferred* 마스터 Directory Server 를 준비하는 경우 반드시 *디렉토리 관리자* 자격 증명을 입력해야 합니다 .

디렉토리 관리자 사용자는 Directory Server 의 특수 사용자로 Directory Server 인스턴스의 모든 위치에서 전체 권한을 가집니다 . (ACI 는 디렉토리 관리자 사용자에게 적용되지 않습니다 .)

예를 들어 오직 디렉토리 관리자만이 Retro-Changelog 데이터베이스의 액세스 제어를 설정할 수 있으며 , 이는 Identity Synchronization for Windows 에 기본 마스터 서버용 디렉토리 관리자 자격 증명에 필요한 이유 중 하나입니다 .

참고

어떤 이유이든 기본 Sun 디렉토리 소스에 대하여 Retro-Changelog 데이터베이스를 다시 만드는 경우 기본 액세스 제어 설정으로 인하여 Directory Server 커넥터가 데이터베이스 내용을 읽을 수 없게 됩니다 .

Retro-Changelog 데이터베이스용 액세스 제어 설정을 복구하려면 idsync prepds 를 실행하거나 콘솔에서 적절한 Sun 디렉토리 소스를 선택한 후 Prepare Directory Server 버튼을 누릅니다 .

참고

지정된 시간이 경과하면 Change-log 항목을 자동으로 제거 (또는 *자르기*) 하도록 시스템을 구성할 수 있습니다 . 명령줄에서 `cn=RetroChangelog Plugin`, `cn=plugins`, `cn=config` 의 `nsslapd-changelogmaxage` 구성 속성을 수정합니다 .

`nsslapd-changelogmaxage: IntegerTimeunit`

여기에서 ,

- ***integer*** 는 숫자입니다 .
- ***Timeunit*** 에서 s 는 초 , m 은 분 , h 는 시 , d 는 일 및 w 는 주입니다 . (Integer 와 Timeunit 변수 사이에 공백이 있으면 안 됩니다 .)

예 : `nsslapd-changelogmaxage: 2d`

자세한 내용은 Sun Java TM 시스템 Directory Server 5 2004Q2 Administration Guide 의 "Managing Replication" 장을 참조하십시오 .

- *관리* 자격 증명을 사용하여 보조 서버를 준비할 수 있습니다 .

참고 사용할 호스트와 접미어를 반드시 알아야 하므로 idsync prepds 를 실행하기 전 Identity Synchronization for Windows 구성을 계획해야 합니다.

Directory Server 커넥터와 플러그인이 이미 설치된 위치의 Directory Server 접미어에서 idsync prepds 를 실행하면 Directory Server 커넥터를 설치하라는 메시지가 표시됩니다. 이 메시지는 무시하십시오.

Sun Java System 디렉토리 소스를 준비하려면 터미널 창 (또는 명령 창) 을 열고 다음과 같이 **idsync prepds** 명령을 입력합니다.

```
idsync prepds [-D <bind-DN>] -w <bind-password | -> [-h <preferred host>]
[-p <preferred-port>] [-s <database-suffix>] [-Z] [-P <cert-db-path>]
[-m <secmod-db-path>] [-j <secondary host>] [-r <secondary-port>] [-E <admin DN of
secondary host>] [-u <password for secondary host | ->] [-x]
```

예 :

```
idsync prepds -D "cn=Directory Manager" -w <preferred master password> -h
<preferred-host> -p 389 -s dc=example,dc=com -j "secondary host" -r 389 -E
"cn=Administrator" -u <secondary master password> -s dc=example,dc=com
```

참고 -h, -p, -D, -w 및 -s 인수는 prepds 하위 명령에 대하여만 재정의 (다음의 표에서 설명) 되었습니다. 또한 -q 인수는 적용되지 않습니다.

idsync prepds 에 고유한 인수는 과 같습니다.

표 A-7) prepds 인수

인수	설명
-h <name>	기본 호스트의 역할을 하는 Directory Server 인스턴스의 DNS 이름을 지정합니다.
-p <port>	기본 호스트의 역할을 하는 Directory Server 인스턴스의 포트 번호를 지정합니다. (기본값은 389 입니다.)
-j <name> (선택)	보조 호스트의 역할을 하는 Directory Server 인스턴스의 DNS 이름을 지정합니다 (Sun Java 시스템 Directory Server 5 2004Q2 복수 마스터 복제 (MMR) 환경에서 적용).

표 A-7) prepds 인수 (계속)

인수	설명
-r <port> (선택)	보조 호스트의 역할은 하는 Directory Server 의 포트를 지정합니다 (Sun Java 시스템 Directory Server 5 2004Q2 복수 마스터 복제 (MMR) 환경에서 적용). ((기본값은 389 입니다.)
-D <dn>	기본 호스트의 Directory Manager 사용자에게 대한 고유한 이름을 지정합니다 .
-w <password>	기본 호스트의 Directory Manager 사용자에게 대한 비밀번호를 지정합니다 . 값이 - 이면 표준 입력 (STDIN) 에서 비밀번호를 읽습니다 .
-E <admin-DN>	보조 호스트의 Directory Manager 사용자에게 대한 고유한 이름을 지정합니다 .
-u <password>	보조 호스트의 Directory Manager 사용자에게 대한 비밀번호를 지정합니다 . 값이 - 이면 표준 입력 (STDIN) 에서 비밀번호를 읽습니다 .
-s <rootsuffix>	색인을 추가할 때 사용할 루트 접미어를 지정합니다 (사용자를 동기화하는 위치의 루트 접미어). 참고 : 기본 및 보조 호스트의 데이터베이스 이름은 변할 수 있으나 접미어는 변할 수 없습니다 . 따라서 프로그램이 각 호스트의 데이터베이스 이름을 찾고 이를 사용하여 색인을 추가할 수 있습니다 .
-x	dspswuserlink 속성의 동일성 및 존재 색인을 데이터베이스에 추가하지 않습니다 .

복제된 환경 (예를 들어 기본 마스터 , 보조 마스터 및 두 개의 소비자가 있는 환경) 에서 idsync prepds 를 실행하는 경우 오직 기본 및 보조 마스터에 대하여 한 번만 idsync prepds 를 실행합니다 .

idsync prepds 를 실행하려면 다음과 같이 합니다 .

1. Directory Server 복제본이 실행 중인지 확인합니다 (적용되는 경우).
2. 콘솔 또는 명령 줄에서 idsync prepds 를 실행합니다 . 예 :

```
idsync prepds -h M1.example.com -p 389 -j M2.example.com -r 389 . . .
```

idsync prepds 명령을 실행한 결과는 다음과 같습니다

- M1:
 - RCL 이 더욱 많은 속성 (dspswuserlink 등) 을 캡처할 수 있도록 기능이 강화됩니다 .
RCL 은 M1 에서만 필요합니다 .
 - 스키마를 확장합니다 .
 - ACI 가 있는 uid=pswconnector , < 접미어 > 사용자를 추가합니다 .

- `dspswuserlink` 속성에 색인을 추가합니다. 이 속성은 색인화가 완료될 때까지 일시적으로 Directory Server 를 읽기 전용으로 전환합니다.
- 서비스 중단 시간을 피하기 위하여 나중에 색인을 추가할 수 있으나, 반드시 Directory Server 커넥터를 설치하기 전에 색인을 추가해야 합니다.
- M2 에 색인을 추가합니다.

참고

- 복제를 사용하면 Identity Synchronization for Windows 가 스키마 정보와 `uid=pswconnector` 를 기본 마스터에서 보조 마스터와 두 소비자에 복사합니다.
 - 반드시 Directory Server 커넥터를 한 번만 설치해야 합니다. 반드시 모든 디렉토리에 Directory Server 플러그인을 설치해야 합니다.
 - 색인화는 기본 및 보조 마스터에만 필요합니다. (복제가 색인 구성을 기본 마스터에서 보조 마스터로 보내지는 않습니다.)
-

printstat 사용

다음에 `printstat` 하위 명령을 사용할 수 있습니다.

- 설치 및 구성 과정을 완료하기 위하여 수행해야 하는 나머지 단계 목록을 표시합니다.
 - 설치된 커넥터, 시스템 관리자 및 Message Queue 의 상태를 인쇄합니다.
- 가능한 상태 설정은 다음과 같습니다.
- **Uninstalled.** 커넥터가 설치되지 않았습니다.
 - **Installed.** 커넥터가 설치되었으나 아직 런타임 구성을 수신하지 않았으므로 동기화의 준비가 되지 않았습니다.
 - **Ready.** 커넥터가 동기화의 준비가 되었으나 아직 동기화하는 객체가 없습니다.
 - **Syncing.** 커넥터가 객체를 동기화하는 중입니다.

설치된 커넥터, 시스템 관리자 및 Message Queue 의 상태를 인쇄하려면 터미널 창 (또는 명령 창) 을 열고 다음과 같이 `idsync printstat` 명령을 입력합니다.

```
idsync printstat [-D <bind-DN>] -w <bind-password> | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>]
-q <configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
```

예 :

```
idsync printstat -w <admin password> -q <configuration password>
```

참고

printstat 인수에 대한 자세한 내용은 "[공통 인수](#)" 페이지 302를 참조하십시오.

resetconn 사용

resetconn 하위 명령을 사용하여 구성 디렉토리에 있는 커넥터 상태를 *uninstalled*로 재설정합니다. 예를 들어 하드웨어 이상으로 인하여 커넥터를 제거할 수 없는 경우 해당 커넥터를 다시 설치할 수 있도록 resetconn 을 사용하여 커넥터의 상태를 *uninstalled* 로 변경합니다.

주의

resetconn 명령은 하드웨어 또는 제거 프로그램 오류의 경우에만 사용됩니다.

명령줄에서 커넥터의 상태를 재설정하려면 터미널 창 (또는 명령 창) 을 열고 다음과 같이 **idsync resetconn** 명령을 입력합니다.

```
idsync resetconn [-D <bind-DN>] -w <bind-password> | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q
<configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>] -e
<directory-source-name> [-n]
```

예 :

```
idsync resetconn -w <admin password> -q <configuration_password> -e
"dc=example,dc=com"
```

resetconn 에 고유한 인수는 과 같습니다 .

표 A-8) idsync resetconn 인수

인수	설명
-e <dir-source>	재설정할 디렉토리 소스의 이름을 지정합니다 .
-n	실제 변경 없이 작업의 효과를 미리 볼 수 있도록 안전 모드에서 실행합니다 .

참고	idsync printstat는 디렉토리 소스 이름을 찾을 때 사용할 수 있습니다 . 기타 resetconn 인수에 대한 자세한 내용은 " 공통 인수 " 페이지 302 를 참조하십시오 .
-----------	---

resync 사용

resync 하위 명령을 사용하여 기존 사용자를 부팅시 구현에 연결할 수 있습니다 . 이 명령은 다음에 대한 관리자가 지정한 일치 규칙을 사용합니다 .

- 기존 항목 링크
- 원격 디렉토리의 내용으로 빈 디렉토리 입력
- 두 개의 기존 사용자 입력 사이의 속성 값 일괄 동기화

참고	사용자 링크 및 동기화에 대한 자세한 내용은 " 기존 사용자 동기화 " 페이지 175 를 참조하십시오 .
-----------	--

기존 사용자를 재동기화하고 디렉토리를 미리 채우려면 터미널 창 (또는 명령 창) 을 열고 다음과 같이 **idsync resync** 명령을 입력합니다 .

```
idsync resync [-D <bind-DN>] -w <bind-password> | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q
<configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>] [-n] [-f <xml
filename for linking>] [-k] [-a <ldap-filter>] [-l <sul-to-sync>] [-o Sun | Windows]
[-c] [-x] [-u] [-i ALL_USERS | NEW_USERS | NEW_LINKED_USERS]
```

예 :

```
idsync resync -w <admin password> -q <configuration_password>
```

resync 에 고유한 인수는 와 같습니다 .

표 A-9) idsync resync 사용법

인수	의미
-f <filename>	Identity Synchronization for Windows 가 제공한 지정된 XML 구성 파일 중 하나를 사용하여 링크되지 않은 사용자 항목 사이의 링크를 만듭니다 . (부록 B, "LinkUsers XML 문서 예제 " 참조)
-k	링크되지 않은 사용자 사이에만 링크를 만듭니다 (사용자를 만들거나 기존 사용자를 수정하지 않음).
-a <ldap-filter>	동기화할 항목을 제한하는 LDAP 필터를 지정합니다 . 필터는 재동기화 작업의 소스에 적용됩니다 . 예를 들어 idsync resync -o Sun -a "uid="* 를 지정하면 uid 속성이 있는 모든 Directory Server 사용자가 Active Directory 로 동기화됩니다 .
-l <sul-to-sync>	동기화할 개별 동기화 사용자 목록 (SUL) 을 지정합니다 . 참고 : 복수 SUL ID 를 지정하여 복수 SUL 을 재동기화하거나 , SUL ID 를 지정하지 않는 경우 프로그램은 모든 SUL 을 재동기화합니다 .
-o (Sun Windows)	재동기화 작업의 소스를 지정합니다 . <ul style="list-style-type: none"> Sun: Windows 항목용 속성 값을 Sun Java 시스템 Directory Server 디렉토리 소스 항목에 있는 해당 속성 값으로 설정합니다 . Windows: Sun Java 시스템 Directory Server 항목의 속성 값을 Windows 디렉토리 소스 항목에 있는 해당 속성 값으로 설정합니다 . (기본값은 Windows 입니다.)
-c	대상에서 해당 사용자를 찾을 수 없는 경우 사용자 항목을 자동으로 만듭니다 . <ul style="list-style-type: none"> Active Directory 또는 Windows NT 에서 만든 사용자에 대하여 무작위로 비밀번호를 생성합니다 . Directory Server 에서 만든 사용자에 대하여 특수 비밀번호 값 ((PSWSYNC)*INVALID PASSWORD*) 을 자동으로 만듭니다 (-i 옵션을 지정하지 않은 경우) .

표 A-9) idsync resync 사용법 (계속)

인수	의미
-i (ALL_USERS NEW_USERS NEW_LINKED_USERS)	<p>Sun 디렉토리 소스에서 동기화된 사용자 항목의 비밀번호를 재설정하고 이후 사용자 비밀번호가 필요할 때 해당 사용자에 대하여 현재 도메인 내의 비밀번호 동기화를 수행하도록 합니다 .</p> <ul style="list-style-type: none">• ALL_USERS: 모든 동기화된 사용자에게 대하여 요청시 비밀번호 동기화를 수행하도록 합니다 .• NEW_USERS: 새로 생성된 사용자에게 대하여 요청시 비밀번호 동기화를 수행하도록 합니다 .• NEW_LINKED_USERS: 모든 새로 생성된 사용자 및 새로 링크된 사용자에게 대하여 요청시 비밀번호 동기화를 수행하도록 합니다 .
-u	<p>객체 캐시를 업데이트만 합니다 . 수정되는 항목은 없습니다 .</p> <p>이 인수는 Windows 디렉토리 소스용 사용자 항목의 로컬 캐시만 업데이트하며 , 따라서 이미 존재하는 Windows 사용자가 Directory Server 에서 생성되지 않도록 방지합니다 . 이 인수를 사용하는 경우 Windows 사용자 항목이 Directory Server 사용자 항목과 동기화되지 않습니다 . 이 인수는 resync 소스가 Windows 인 경우에만 유효합니다 .</p>
-x	<p>소스 항목과 일치하지 않는 모든 대상 사용자 항목을 삭제합니다 .</p>
-n	<p>실제 변경 없이 작업의 효과를 미리 볼 수 있도록 안전 모드에서 실행합니다 .</p>

참고	<ul style="list-style-type: none">• 사용 상태를 보려면 인수 없이 idsync resync 를 실행합니다 .• resync 인수에 대한 자세한 내용은 " 공통 인수 " 페이지 302 를 참조하십시오 .• 기존 사용자의 재동기화에 대한 자세한 내용은 " 기존 사용자 동기화 " 페이지 175 를 참조하십시오 .
----	--

resync를 실행한 후 중앙 감사 로그에 있는 resync.log를 확인합니다. 오류가 있는 경우 제 9 장, " 문제해결 " 을 참조하십시오 .

startsync 사용

startsync 하위 명령을 사용하여 명령줄에서 동기화를 시작합니다 .

동기화를 시작하려면 터미널 창 (또는 명령 창) 을 열고 다음과 같이 **idsync startsync** 명령을 입력합니다 .


```
idsync startsync [-D <bind-DN>] -w <bind-password> | -> [-h <Configuration Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q <configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
```

예 :

```
idsync startsync -w <admin password> -q <configuration_password>
```

startsync 에 고유한 인수는 과 같습니다 .

표 A-10) idsync startsync 인수

인수	설명
[-y]	명령 확인용 프롬프트를 표시하지 않습니다 .

참고 기타 startsync 인수에 대한 자세한 내용은 "[공통 인수](#)" 페이지 302 를 참조하십시오 .

stopsync 사용

stopsync 하위 명령을 사용하여 명령줄에서 동기화를 중지합니다 .

동기화를 중지하려면 터미널 창 (또는 명령 창) 을 열고 다음과 같이 **idsync stopsync** 명령을 입력합니다 .

```
idsync stopsync [-D <bind-DN>] -w <bind-password> | -> [-h <Configuration Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q <configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
```

예 :

```
idsync stopsync -w <admin password> -q <configuration_password>
```

참고

stopsync 인수에 대한 자세한 내용은 "[공통 인수](#)" [페이지 302](#)를 참조하십시오 .

forcepwhg 마이그레이션 유틸리티 사용

마이그레이션 작업이 진행되는 동안 비밀번호를 변경하는 사용자는 Windows NT와 Directory Server 에 각기 다른 비밀번호를 갖게 됩니다. forcepwhg 유틸리티를 사용하여 Identity Synchronization for Windows 버전 1.0 에서 버전 1 2004Q3 으로의 마이그레이션 과정 동안 비밀번호를 변경한 사용자가 비밀번호를 변경하도록 합니다.

참고

forcepwhg 유틸리티는 Windows 패키지에만 함께 제공됩니다.

forcepwhg 를 사용하기 전에 반드시 다음을 확인해야 합니다.

- userpassword 속성용 7 비트 값을 강화하기 위하여 Directory Server 에 7 비트 검사 플러그인을 구성하지 않도록 해야 합니다. Directory Server 콘솔을 사용하여 수행합니다.
- 인증용으로 사용하는 클라이언트가 현재 로케일에서 UTF-8 로 정확히 변환되는지 확인합니다. (예를 들어 Directory Server 와 함께 제공되는 ldapsearch 의 -i 옵션)

forcepwhg 명령줄 유틸리티를 실행하려면 다음과 같이 합니다.

1. 명령 프롬프트 창을 열고 cd 를 사용하여 이전을 수행하는 위치의 호스트에서 Windows migration 로 이동합니다. (Identity Synchronization for Windows 1.0 NT 구성요소 (커넥터 , 변경 검출기 DLL, 비밀번호 필터 DLL) 는 반드시 PDC 호스트에 설치되어야 합니다.)
2. migration 디렉토리에서 다음을 입력합니다.

```
java -jar forcepwhg.jar [-n] [-a] [-t <time_specification>]
```

예 :

```
forcepwhg.jar -n -a
forcepwhg.jar -t 33m
```

forcepwhg 에 고유한 인수는 과 같습니다.

표 A-11) forcepwchg 인수

옵션	설명
-n	<p><i>미리 보기</i> 모드를 지정합니다 .</p> <p>미리 보기 모드에서 유틸리티가 다음을 제외한 모든 정상적인 사용자의 이름을 인쇄합니다 .</p> <ul style="list-style-type: none">• -a 인수를 지정하는 경우 내장 계정 (Administrator 및 Guest).• -t 인수를 사용하여 지정한 시간 동안 비밀번호를 변경한 사용자 . <p>미리 보기에서는 모든 사용자가 <code>forcepwchg</code> 를 실행할 수 있습니다 .</p> <p>미리 보기 모드가 아닌 경우 오직 Administrator 만 <code>forcepwchg</code> 를 실행할 수 있습니다 .</p>
-a	<p>모든 사용자 (Administrator 및 Guest 제외) 가 비밀번호를 변경하도록 합니다 .</p> <p>-t 인수를 사용하는 경우 이 인수는 사용할 수 없습니다 .</p>
-t <time_specification>	<p>이전 <time_specification> 동안 비밀번호를 변경한 모든 사용자가 비밀번호를 변경하도록 합니다 . 여기에서 <time_specification> 의 형식은 다음과 같습니다 .</p> <ul style="list-style-type: none">• <숫자>: 초 단위 시간 (예 , -t 30)• <숫자>m: 분 단위 시간 (예 , -t 25m)• <숫자>h: 시 단위 시간 (예 , -t 6h) <p>예를 들어 <code>forcepwchg -t 6h</code> 를 지정하는 경우 지난 여섯 시간 동안 비밀번호를 변경한 모든 사용자는 다시 자신의 비밀번호를 변경해야 합니다 .</p>
-?	<p>사용 정보를 인쇄합니다 .</p>
참고	<p>forcepwchg 에 대한 더 자세한 내용은 "Windows NT 에서 비밀번호 강제 변경 " 페이지 196 를 참조하십시오 .</p>

LinkUsers XML 문서 예제

이 부록에서는 `idsync resync` 하위 명령을 사용하여 구현의 기존 사용자를 링크하는데 사용할 수 있는 두 가지 예제 XML 구성 문서를 제공합니다.

두 파일 모두는 코어를 설치한 위치의 `samples1` 하위 디렉토리에 있습니다.

- "예제 1: `linkusers-simple.cfg`" [페이지 324](#) (공통 및 단순 구성 예)
- "예제 2: `linkusers.cfg`" [페이지 325](#) (링크 기준 지정의 완전한 기능을 보여주는 더욱 복잡한 구성 예)

예제를 자신의 환경에 맞게 수정할 수 있습니다. 두 예제에는 복수 SUL의 사용자를 링크하는 방법을 포함하여 예제를 수정하여 사용자를 링크하는 방법이 주석으로 포함되어 있습니다.

예제 1: linkusers-simple.cfg

<!--

Copyright 2004 Sun Microsystems, Inc. All rights reserved

사용은 라이선스 조건에 따릅니다 .

-->

<!--

이 xml 파일은 명령줄에서 Windows 와 Sun Directory Server 사용자를 링크하는 데
사용합니다 . 이는 -f 옵션으로 "idsync resync" 스크립트로 전달됩니다 .

이는 동일한 로그인 이름이 있는 SUL 동기화 사용자 목록의 사용자를 링크하며 ,
따라서 Directory Server uid 속성이
Active Directory samaccountname 속성과 일치합니다 .

보다 복잡한 일치 규칙을 보려면 linkusers.cfg 예제를 참조하십시오 .

-->

<UserLinkingOperationList>

<UserLinkingOperation parent.attr="UserLinkingOperation" sulid="SUL1">

<UserMatchingCriteria parent.attr="UserMatchingCriteria">

<AttributeMap parent.attr="AttributeMap">

<AttributeDescription parent.attr="SunAttribute" name="uid"/>

<AttributeDescription parent.attr="WindowsAttribute"
name="samaccountname"/>

</AttributeMap>

</UserMatchingCriteria>

</UserLinkingOperation>

</UserLinkingOperationList>

예제 2: linkusers.cfg

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
    Copyright 2004 Sun Microsystems, Inc. All rights reserved
    사용은 라이선스 조건에 따릅니다 .
-->
<!--
    이 xml 파일은 명령줄에서 Windows 와 Sun Directory Server 사용자를 링크하는 데
    사용됩니다 . 이는 -f 옵션으로 'idsync resync' 스크립트로 전달됩니다 .
-->
<!--
    다음 매개변수로 LinkingOutOfScope 이 가능합니다 . TRUE 인 경우 Windows 사용자가
    사용자의 동기화 사용자 목록 밖에 있는 Sun Directory Server 사용자로 링크될
    수 있습니다 . 기본값은 FALSE 입니다 .
-->
<UserLinkingOperationList allowLinkingOutOfScope="false">
<!--
    UserLinkingOperation 는 링크할 단일 SUL 의 구성을 캡슐화합니다 .
    여기에는 일치할 SUL ID 와 속성 목록이 포함됩니다 .
    링크되는 각 SUL 에 대하여 반드시 별도의 UserLinkingOperation 를 지정해야 합니다 .
-->
<UserLinkingOperation parent.attr="UserLinkingOperation" sulid="SUL1">
<!--
    UserMatchingCriteria 는 링크될 사용자용으로 반드시 일치되어야 하는 속성
    목록을 캡슐화합니다 . -->
<!--
    이 UserMatchingCriteria 를 사용하여 두 사용자를 일치하는 경우 반드시
    givenName 및 sn 이 동일해야 합니다 . -->
<UserMatchingCriteria parent.attr="UserMatchingCriteria">
  <AttributeMap parent.attr="AttributeMap">
    <AttributeDescription parent.attr="SunAttribute" name="sn"/>
    <AttributeDescription parent.attr="WindowsAttribute" name="sn"/>
  </AttributeMap>
  <AttributeMap parent.attr="AttributeMap">
    <AttributeDescription parent.attr="SunAttribute" name="givenName"/>
  </AttributeMap>
</UserMatchingCriteria>
</UserLinkingOperation>
</UserLinkingOperationList>
```

```

    <AttributeDescription parent.attr="WindowsAttribute"
      name="givenName"/>
  </AttributeMap>
</UserMatchingCriteria>

```

```

<!--

```

단일 SUL 에 복수 UserMatchingCriteria 를 지정할 수 있습니다 . 이는 논리적 OR 로 처리됩니다 . 이 예에서 링크된 사용자에게 대하여 (givenName 과 sn 이 반드시 일치 (위 참조)) OR (employee(Number|ID) 가 반드시 일치) 참고로 지정된 속성 employeeNumber 는 DS 속성의 이름입니다 . -->

```

<!--

```

employeeNumber 가 DS 의 속성으로 색인화되지 않았으므로 UserMatchingCriteria 가 주석 처리됩니다 . UserMatchingCriteria 의 모든 속성은 반드시 색인화되어야 합니다 .

```

  <UserMatchingCriteria parent.attr="UserMatchingCriteria">
    <AttributeMap parent.attr="AttributeMap">
      <AttributeDescription parent.attr="SunAttribute" name="employeeNumber"/>
      <AttributeDescription parent.attr="WindowsAttribute" name="employeeID"/>
    </AttributeMap>
  </UserMatchingCriteria>

```

```

-->

```

```

</UserLinkingOperation>

```

```

<!--

```

복수 SUL 이 링크되면 각각에 대하여 별도의 UserLinkingOperation 이 지정됩니다 . 여기에 보이는 것과 같이 각 UserLinkingOperation 은 서로 다른 UserMatchingCriteria 를 사용할 수 있습니다 . 이 예에서 SUL2 의 사용자는 오직 sn 과 employeeNumber 이 일치되는 경우에만 링크됩니다 .

참고 : 예제 구성에는 오직 단인 SUL 만 있으므로 이 UserLinkingOperation 은 현재 주석 처리됩니다 .

```

<UserLinkingOperation parent.attr="UserLinkingOperation" sulid="SUL2">
  <UserMatchingCriteria parent.attr="UserMatchingCriteria">
    <AttributeMap parent.attr="AttributeMap">
      <AttributeDescription parent.attr="SunAttribute" name="sn"/>
      <AttributeDescription parent.attr="WindowsAttribute" name="sn"/>
    </AttributeMap>
    <AttributeMap parent.attr="AttributeMap">
      <AttributeDescription parent.attr="SunAttribute" name="employeeNumber"/>
      <AttributeDescription parent.attr="WindowsAttribute" name="employeeID"/>
    </AttributeMap>
  </UserMatchingCriteria>
</UserLinkingOperation>
-->

```


</UserLinkingOperationList>

예제 2: linkusers.cfg

Solaris 에서 루트가 아닌 사용자로 서비스 실행

Identity Synchronization for Windows 서비스를 설치하고 실행하려면 반드시 루트 권한이 있어야 합니다. 그러나 제품을 설치한 후 루트가 아닌 사용자로 프로그램 서비스를 실행할 수 있도록 소프트웨어를 구성할 수 있습니다.

참고 루트가 아닌 사용자로 서비스를 실행하려는 경우 반드시 Identity Synchronization for Windows 인스턴스 디렉토리 아래의 모든 디렉토리용 권한을 변경해야 합니다. (기본 디렉토리는 /var/opt/SUNWisiw 입니다.)

Solaris 에서 루트가 아닌 사용자로 서비스를 실행하려면 다음과 같이 합니다.

1. UNIX useradd 명령을 사용하여 Identity Synchronization for Windows용 사용자 계정을 만듭니다 (선택 단계).
또한 nobody 사용자를 사용하여 서비스를 실행할 수 있습니다.
이 절차의 나머지 예에서는 iswuser 라는 이름으로 사용자를 만든 것으로 가정합니다.
2. Solaris 에 Sun Java System Directory Server 커넥터를 설치하려면 반드시 설치 동안 커넥터용으로 권한이 지정되지 않은 포트를 선택해야 합니다.
(예를 들어 1024 보다 큰 포트를 사용할 수 있습니다.)

참고 반드시 나머지 단계의 모든 명령은 루트로 실행해야 합니다.

3. 모든 구성요소를 설치한 후 다음 명령을 사용하여 Identity Synchronization for Windows 를 정지합니다.

```
/etc/init.d/isw stop
```

4. 반드시 인스턴스 디렉토리의 소유권을 업데이트해야 합니다.
예를 들어 제품을 /var/opt/SUNWisw 에 설치할 수 있습니다.

```
chown -R iswuser /var/opt/SUNWisw  
chown -R iswuser /opt/SUNWisw
```

5. 텍스트 편집기에서 /etc/init.d/isw 파일을 열고 다음 줄을 변경합니다.

```
"$EXEC_START_WATCHDOG" "$JAVA_PATH" "$INSTALL_DIR" "CONFIG_DIR"
```

변경 후 :

```
su iswuser -c "$EXEC_START_WATCHDOG '$JAVA_PATH' '$INSTALL_DIR'  
'CONFIG_DIR'"
```

6. 다음 명령을 실행하여 서비스를 다시 시작합니다.

```
/etc/init.d/isw start
```

7. 다음 명령을 실행하여 해당 구성요소가 지정된 사용자의 userid로 실행되는지 확인합니다.

```
ps -ef | grep iswuser
```

Synchronization User List 정의 및 구성

이 부록에서는 동기화 사용자 목록 (SUL) 정의에 대한 보완 설명을 제공하고 복수 도메인을 구성하는 방법에 대하여 설명합니다. 다음과 같은 내용으로 구성됩니다.

- ["Synchronization User Lists 정의 이해" 페이지 331](#)
- ["복수 Windows 도메인 구성" 페이지 333](#)

Synchronization User Lists 정의 이해

모든 동기화 사용자 목록 (SUL)에는 두 가지 정의가 있으며, 한 가지는 동기화할 Directory Server 사용자를 식별하며 다른 한 가지는 동기화할 Windows 사용자를 식별합니다.

각 정의는 디렉토리에서 동기화할 사용자를 확인하고 동기화에서 제외할 사용자를 구분하며 새 사용자를 만들 위치를 확인합니다.

참고

Identity Synchronization for Windows 콘솔을 사용하여 선택하는 objectclass 또한 동기화할 사용자를 결정합니다. 프로그램은 오직 선택한 objectclass 가 있는 사용자만 동기화하며, 또한 선택한 objectclass 의 하위 클래스가 있는 사용자가 포함됩니다.

예를 들어 organizationalPerson objectclass 를 선택하는 경우 inetorgperson 이 organizationalPerson 의 하위 클래스이므로 Identity Synchronization for Windows 는 이 objectclass 가 있는 사용자를 동기화합니다.

SUL 정의의 구성요소는 에서 설명합니다 .

표 D-1) SUL 정의의 구성요소

구성요소	정의	적용 범위		
		Sun	AD	NT
기본 DN	동기화될 모든 사용자의 상위 LDAP 노드를 정의합니다 . 동기화 사용자 목록 기본 DN 에는 동기화 사용자 목록 필터에 의하여 사용자 가 제외되지 않고 사용자의 DN 이 더욱 구체적인 동기화 사용자 목록과 일치 하지 않는 한 모든 사용자가 포함됩니다 . 예 : ou=sales,dc=example,dc=com.	예	예	아니 오
필터	동기화 사용자 목록에서 사용자를 포함 또는 제외하는 데 사용하는 LDAP 형 식의 필터를 정의합니다 . 필터에는 &, , !, = 및 * 연산자가 포함될 수 있습니 다 . >= 및 <= 연산자는 지원하지 않습니다 . 모든 비교는 대소문자를 구분하 는 문자열 비교로 수행됩니다 . 예 : (& (employeeType=manager) (st=CA)) 는 California 에 있는 관리자만 포 함합니다 .	예	예	예
생성 표현식	새로 만든 사용자의 상위 DN 과 이름 지정 속성을 정의합니다 (생성을 사용 설정한 경우에만 적용). 생성 표현식에는 반드시 동기화 사용자 목록의 기본 DN 이 포함되어야 합니 다 . 예 : cn=%cn%,ou=sales,dc=example,dc=com. (여기에서 %cn% 토큰은 생 성되는 사용자 항목의 값으로 대체됩니다 .)	예	예	아니 오

참고	Sun Java System Directory Server 의 사용자를 복수 Active Directory 도메인과 동기화하려면 반드시 각 Active Directory 도메인마다 하나 이상의 SUL 을 정의해야 합니다 .
----	--

복수 SUL 을 정의하는 경우 Identity Synchronization for Windows 는 각 SUL 정의를 반복적으로 일치시켜 SUL 에서의 구성원을 확인합니다 . 프로그램은 SUL 정의를 우선 더욱 구체적인 기본 DN 을 사용하여 검사합니다 .
예를 들어 프로그램은 dc=example,dc=com 을 검사하기 전에 ou=sales,dc=example,dc=com 에 대하여 일치를 검사합니다 .

SUL 정의 두 개의 기본 DN 은 동일하며 필터는 서로 다른 경우 Identity Synchronization for Windows 가 어느 필터를 먼저 검사할 것인지 자동으로 결정할 수 없으므로 반드시 도메인 중복 해결을 사용하여 두 SUL 정의의 순서를 정해야 합니다. 사용자가 SUL 정의 기본 DN 과 일치하지만 해당 기본 DN 의 필터와 일치하지 않는 경우 해당 사용자가 이보다 덜 구체적인 기본 DN 의 필터와 일치하는 경우라도 프로그램이 이 사용자를 동기화에서 제외합니다.

복수 Windows 도메인 구성

복수 Windows 도메인을 동일한 Directory Server 컨테이너 (ou=people,dc=example,dc=com 등) 에 동기화할 수 있도록 Identity Synchronization for Windows 는 도메인 정보가 포함된 " 복합 " Windows 속성을 사용합니다.

- Active Directory 도메인의 경우 Identity Synchronization for Windows 는 항목을 Directory Server 로 동기화하기 전에 Active Directory 도메인 이름 (예 : east.example.com) 에 activedirectorydomainname 속성을 설정합니다.
- Windows NT 도메인의 경우 Identity Synchronization for Windows 는 항목을 Directory Server 에 동기화하기 전에 Windows NT 도메인 이름 (NTEXTAMPLE 등) 에 user_nt_domain_name 속성을 설정합니다.

이들 속성이 Windows 사용자 항목에 실제로 표시되지는 않으나 Identity Synchronization for Windows 콘솔에서 동기화할 수 있으며 Directory Server 사용자 속성으로 매핑될 수 있습니다. 일단 Identity Synchronization for Windows 가 도메인 속성을 매핑하면 동기화 동안 Directory Server 항목 안에 설정되며 SUL 필터에서 사용될 수 있습니다.

Identity Synchronization for Windows 가 이들 속성을 사용하는 방법은 다음 예에 보이는 것과 같습니다. 이 예에서는 세 개의 Windows 도메인 (Active Directory 도메인 두 개 및 Windows NT 도메인 한 개) 가 단일 Directory Server 인스턴스와 동기화되는 것으로 가정합니다.

1. Active Directory 도메인 east.example.com 에 있는 사용자는 ou=people,dc=example,dc=com 의 Directory Server 로 동기화됩니다.
2. Active Directory 도메인 west.example.com 에 있는 사용자는 ou=people,dc=example,dc=com 의 Directory Server 로 동기화됩니다.
3. Windows NT NTEXTAMPLE 도메인에 있는 사용자는 ou=people,dc=example,dc=com 의 Directory Server 로 동기화됩니다.

Directory Server 사용자를 만들거나 수정하면 프로그램은 SUL 필터를 사용하여 동기화될 사용자의 Windows 도메인을 결정합니다.(각 Directory Server SUL 에 동일한 기본 DN ou=people,dc=example,dc=com 이 있기 때문)
activedirectorydomainname 과 user_nt_domain_name 속성을 사용하여 이 필터를 쉽게 구성할 수 있습니다.

콘솔의 Attributes 탭에서 필터를 구성하려면 다음과 같이 합니다.

1. Directory Server destinationindicator 속성을 Active Directory activedirectorydomainname 속성과 Windows NT user_nt_domain_name 속성으로 매핑합니다.
2. 다음과 같이 각 Windows 도메인에 대하여 하나의 SUL 을 구성합니다.


```

EAST_SUL
  Sun Java System Directory Server definition
    Base DN:  ou=people,dc=example,dc=com
    Filter:   destinationindicator=east.example.com
    Creation Expression:  cn=%cn%,ou=people,dc=example,dc=com
Active Directory definition (east.example.com)
  Base DN:  cn=users,dc=east,dc=example,dc=com
  Filter:   <none>
  Creation Expression:  cn=%cn%,cn=users,dc=east,dc=example,dc=com
WEST_SUL
  Sun Java System Directory Server definition
    Base DN:  ou=people,dc=example,dc=com
    Filter:   destinationindicator=west.example.com
    Creation Expression:  cn=%cn%,ou=people,dc=example,dc=com
Active Directory definition (west.example.com)
  Base DN:  cn=users,dc=west,dc=example,dc=com
  Filter:   <none>
  Creation Expression:  cn=%cn%,cn=users,dc=west,dc=example,dc=com
NT_SUL
  Sun Java System Directory Server definition
    Base DN:  ou=people,dc=example,dc=com
    Filter:   destinationindicator=NTEXAMPLE
    Creation Expression:  cn=%cn%,ou=people,dc=example,dc=com
Windows NT definition (NTEXAMPLE)
  Base DN:  NA
  Filter:   <none>
  Creation Expression:  NA

```

참고로 각 Directory Server SUL 정의에는 동일한 기본 DN 과 생성 표현식이 있으나 필터는 해당 Windows 사용자 항목의 도메인을 표시합니다.

이들 설정으로 Directory Server 사용자 항목이 별도의 Windows 도메인과 동기화하도록 하는 방식에 대한 추가 내용은 다음의 시험 예를 참조하십시오.

1. Active Directory east.example.com domain 에 cn=Jane Test,cn=users,dc=east,dc=example,dc=com 을 만듭니다.
2. Identity Synchronization for Windows 는 destinationindicator=east.example.com 이 있는 Directory Server 에 사용자 항목 cn=Jane Test,ou=people,dc=example,dc=com 을 만듭니다.

3. Directory Server 의 `cn=Jane Test,ou=people,dc=example,dc=com` 항목을 수정합니다.
4. Jane Test 의 `destinationindicator` 속성이 `east.example.com` 이므로 그의 항목은 `EAST_SUL` 동기화 사용자 목록 필터와 일치하며, 수정 내용은 `east.example.com` Active Directory 도메인으로 동기화됩니다.

이 예에서는 Identity Synchronization for Windows 가 Windows 에서 Directory Server 로 사용자 생성을 동기화하는 것으로 가정합니다. 이렇게 동기화되지 않는 경우 `idsync resync` 명령을 사용하여 `destinationindicator` 속성을 설정할 수 있습니다.

참고 복수 SUL 이 있는 구현에서 `idsync resync -f` 를 사용하는 경우 링크 구성 파일의 `allowLinkingOutOfScope` 옵션을 `true` 로 설정해야 합니다. 더 자세한 내용은 [부록 B, "LinkUsers XML 문서 예제"](#) 을 참조하십시오.

이 예에서는 `inetorgperson`, `destinationIndicator` 에 있는 기존 속성을 사용하며, 이들 속성은 다른 용도로 사용할 수 있습니다. 이 속성이 이미 사용 중이거나 다른 `objectclass` 를 선택한 경우 반드시 사용자의 Directory Server 항목에 있는 일부 속성을 `user_nt_domain_name` 및 `activedirectorydomainname` 속성으로 매핑해야 합니다. 이 값을 유지하기 위하여 선택하는 Directory Server 속성은 반드시 나머지 속성 매핑 구성에 사용하는 `objectclass` 에 있어야 합니다.

이 도메인 정보를 유지할 사용하지 않은 속성이 없는 경우 반드시 새 `objectclass` 를 만들어 Identity Synchronization for Windows 와 사용할 새 도메인 속성과 모든 기타 속성을 포함하도록 해야 합니다.

복제 환경용 설치 노트

Identity Synchronization for Windows 1 2004Q3 는 단일 복제 접미어에 있는 사용자 동기화를 지원합니다 .

참고

이 부록에서는 MMR(Multimaster replication) 구현을 구성하고 보안하는 방법을 간단히 설명합니다 . 이 내용은 *Sun Java System Directory Server 5 2004Q2 Administrator's Guide* 에서 직접 발췌한 것이며 Identity Synchronization for Windows 에 국한된 것은 아닙니다 .

MMR 구현을 디자인하고 구현하는 것은 복잡한 과정입니다 . 구현 계획에 대한 내용은 *Sun Java System Directory Server 5 2004Q2 Deployment Guide* 를 참조하고 구현에 대한 내용은 *Sun Java System Directory Server 5 2004Q2 Administrator's Guide* 을 참조하십시오 .

이 부록은 다음과 같이 구성되었습니다 .

- " 복제본 구성 " 페이지 338
- "SSL 을 통한 복제본 구성 " 페이지 340

복제본 구성

참고 MMR(Multi-Master Replication) 환경의 경우 Identity Synchronization for Windows 에서 임의의 Sun 디렉토리 소스에 대하여 기본 및 보조 마스터 서버를 지정할 수 있습니다 .

Directory Server 버전 5 2004Q2 는 이제 4 방향 MMR 을 지원하며 , 이 경우 네 개의 마스터 중 임의의 마스터에서 복제된 데이터베이스를 변경할 수 있습니다 . 제 3 및 제 4 마스터에 플러그인을 설치할 때 반드시 플러그인 설치 동안 *기타* 호스트 유형을 선택하고 직접 Directory Server 인스턴스의 매개변수를 입력해야 합니다 .

다음 단계는 단일 접미어를 복제하는 것으로 가정합니다 . 둘 이상의 접미어를 복제하는 경우 각 서버에서 이들을 동시에 구성할 수 있습니다 . 달리 말하면 각 단계를 반복하여 복수 접미어에 대한 복제본을 구성할 수 있습니다 .

복제 토폴로지를 구성하려면 다음과 같은 순서로 진행해야 합니다 .

1. 단일 마스터를 제외한 모든 서버에서 복제 관리자를 정의합니다 (또는 모든 서버에 대하여 기본 복제 관리자를 사용) .
2. 지정된 소비자 복제본이 있는 모든 서버에서 다음과 같이 합니다 .
 - a. 소비자 복제본용 빈 접미어를 만듭니다 .
 - b. 복제 마법사를 사용하여 접미어에서 소비자 복제본을 사용하도록 설정합니다 .
 - c. 원하는 경우 고급 복제본 설정을 구성합니다 .
3. 적용되는 경우 허브 복제본이 있는 모든 서버에 대하여 다음과 같이 합니다 .
 - a. 허브 복제본용 빈 접미어를 만듭니다 .
 - b. 복제 마법사를 사용하여 접미어에서 허브 복제본을 사용하도록 설정합니다 .
 - c. 원하는 경우 고급 복제본 설정을 구성합니다 .
4. 마스터 복제본이 있는 모든 서버에서 다음과 같이 합니다 .
 - a. 마스터 중 마스터 복제본이 되는 마스터의 접미어를 선택하거나 또는 만듭니다 .
 - b. 복제 마법사를 사용하여 접미어에서 마스터 복제본을 사용하도록 설정합니다 .

- c. 원하는 경우 고급 복제본 설정을 구성합니다.
5. 다음과 같은 순서로 모든 공급자 복제본에 복제 동의서를 구성합니다.
- a. 복수 마스터 세트 내의 마스터 사이.
 - b. 마스터와 해당 지정 소비자 사이.
 - c. 마스터와 허브 복제본 사이.
- 원하는 경우 이 단계에서 부분적인 복제본을 구성할 수 있습니다.
6. 허브 복제본과 해당 소비자 사이의 복제본 동의서를 구성합니다.
7. MMR 의 경우 데이터의 원본 사본이 있는 동일한 마스터 복제본에서 모든 마스터를 초기화합니다. 허브와 소비자 복제본을 초기화합니다.

SSL 을 통한 복제본 구성

참고 이 절차에서 모든 참조 내용은 *Sun Java System Directory Server 5 2004Q2 Administration Guide* 의 각 장에 있습니다.

복제본에 관여된 Directory Server 를 구성하여 모든 복제본 작업이 SSL 연결을 통하여 수행되도록 하려면 다음 단계를 완료합니다.

1. 공급자 및 소비자 서버가 모두 SSL 을 사용하도록 구성합니다.
자세한 내용은 제 11 장 "인증 및 암호화 관리" 를 참조하십시오.

참고

- 공급자 서버 인증서가 SSL 서버 전용 인증서로 SSL 핸드셰이크 동안 클라이언트의 역할을 할 수 없는 경우 SSL 을 통한 복제는 실패합니다.
- 자체 서명 인증서의 경우 현재 SSL 을 통한 복제는 지원되지 않습니다.

2. 복제본이 소비자 서버의 접미어용으로 구성되지 않은 경우 제 8 장 "소비자 복제본 사용 설정" 의 설명과 같이 사용 설정합니다.
3. 제 8 장 "고급 소비자 구성" 의 절차에 따라 소비자에 있는 인증서 항목의 DN 을 다른 복제본 관리자로 정의합니다.
4. 복제본이 공급자 서버의 접미어용으로 구성되지 않은 경우 제 8 장 "허브 복제본 사용 설정" 또는 "마스터 복제본 사용 설정" 의 설명과 같이 사용 설정합니다.
5. 공급자 서버에서 업데이트를 SSL 포트를 통하여 소비자에게 전송할 새 복제 동의서를 만듭니다. 자세한 설명은 제 8 장 "복제본 동의서 작성" 의 설명을 참조하십시오. 소비자 서버에서 보안 포트를 지정하고 비밀번호 또는 인증서를 사용하여 SSL 옵션을 선택합니다. 복제 마스터 또는 인증서 등의 선택한 SSL 옵션에 대한 DN 을 입력합니다.

복제 동의서의 구성을 완료한 후, 공급자는 SSL 을 통하여, 또는 해당 옵션을 선택한 경우 인증서를 사용하여 모든 복제 업데이트 메시지를 소비자에게 전송합니다. 고객 초기화 또한 SSL 용 동의서 구성을 사용하여 콘솔에서 수행하는 경우 보안 연결을 사용합니다.

MMR 환경에서 Identity Synchronization for Windows 구성

MMR 환경에서 Identity Synchronization for Windows 를 구성하는 간단한 단계는 다음과 같으며, 자세한 설명은 이 책의 다른 부분에서 제공합니다.

1. Identity Synchronization for Windows 콘솔에서 동기화될 접미어용 기본 및 보조 Directory Server 마스터를 지정합니다.
(["Sun Java System 디렉토리 소스 작성 " 페이지 102](#) 참조)
토폴로지에 있는 다른 Directory Server 에 대한 정보를 제공할 필요는 없습니다.
2. 콘솔 또는 idsync prepds 명령줄 유틸리티를 사용하여 기본 및 보조 서버를 준비합니다. (["Directory Server 준비 " 페이지 109](#) 또는 ["prepds 사용 " 페이지 310](#) 참조)
명령줄 유틸리티를 사용하는 경우 기본 및 보조 서버의 인수를 지정하여 한번의 실행으로 두 서버 모두를 준비해야 합니다.
3. 이들 디렉토리 사이에서 복제된 접미어용 Directory Server 커넥터를 설치합니다.
(["Directory Server 커넥터 설치 " 페이지 160](#) 참조)
4. 기본 마스터, 보조 마스터 및 복제된 접미어에서 사용자를 관리하는 모든 기타 Directory Server 인스턴스에 Directory Server 플러그인을 설치합니다.
(["Directory Server 플러그인 설치 " 페이지 171](#) 참조)

용어

Identity Synchronization for Windows 제품과 이 설명서에서 사용된 용어는 다음과 같습니다.

액세서 LDAP 등의 프로토콜을 통하여 디렉토리와 직접 인터페이스하는 커넥터 레이어. Identity Synchronization for Windows 에는 Directory Server, Active Directory 및 Windows NT 에 대하여 별도의 액세서가 구현되어 있습니다. 액세서는 때로 작업에 대한 로그 메시지를 의미하기도 합니다.

긍정 응답 다른 구성요소에서 메시지를 수신했음을 응답하는 특화된 메시지. Identity Synchronization for Windows 는 커넥터와 Message Queue 및 커넥터 구성요소 (에이전트, 제어기 및 액세서) 사이에서 긍정 응답을 사용하여 모든 변경 내용이 제대로 동기화되었는지 확인합니다.

작업 하나의 동기화 이벤트에 대한 캡슐화. Identity Synchronization for Windows 커넥터는 작업을 사용하여 사용자 변경 이벤트를 통신합니다. 각 작업에는 유형 (CREATE, MODIFY, DELETE 등) 과 사용자 항목의 충분한 속성이 포함되어 대상 커넥터가 변경 내용을 동기화할 수 있도록 합니다. 모든 작업은 단위별로 처리됩니다.

에이전트 Message Queue 와 인터페이스하고 해당 Directory Server 이름과 Windows 이름 사이에서 속성을 변환하는 커넥터 구성요소. 에이전트는 때로 작업에 대한 로그 메시지를 의미하기도 합니다.

속성 항목에 대한 기술적 정보를 포함합니다. 속성에는 레이블과 값이 있습니다. 또한 각 속성은 속성 값으로 저장될 수 있는 정보 유형의 표준 구문을 따릅니다.

속성 목록 해당 항목 유형 또는 객체 클래스용 필수 및 선택 속성 목록.

감사 로그 동기화되는 사용자의 비밀번호 등 일상적인 이벤트에 대한 항목이 포함된 중앙 로그 파일. 관리자는 Identity Synchronization for Windows 콘솔을 사용하여 이 로그에 표시될 항목의 수와 세부 수준을 제어할 수 있습니다.

각 커넥터는 이 커넥터가 처리하는 사용자에 대한 감사 로그를 만들며, 구현에 있는 모든 커넥터가 만든 감사 로그를 집계하는 중앙의 감사 로그가 있습니다.

인증 클라이언트 사용자의 신분을 Directory Server 로 제공하는 프로세스. 디렉토리로의 액세스가 허용되려면 사용자는 반드시 바인드 DN 과 해당 비밀번호를 제공해야 합니다. Directory Server 는 디렉토리 관리자가 해당 사용자에게 허용한 권한에 따라 기능을 수행하고 파일 및 디렉토리에 액세스하도록 허용합니다.

인증용 인증서 다른 업체가 발행한 전자 파일로 이전 또는 변조할 수 없습니다. 인증서는 서버에서 클라이언트로 또는 클라이언트에서 서버로 송신되어 다른 업체를 확인 및 인증합니다.

보조 객체 클래스 선택된 구조적 클래스를 사용할 수 있게 하는 objectclass 로 동기화에 대한 추가 속성을 제공합니다. [구조적 객체 클래스](#)를 참조하십시오.

기본 DN Base distinguished name. 디렉토리 트리에서 기본 DN, 항목의 DN 및 그 이하의 모든 항목에 대한 검색 작업이 수행됩니다. Active Directory 와 Directory Server 의 경우 동기화 사용자 목록은 특정 기본 DN 을 루트로 합니다. 이 기본 DN 아래의 모든 사용자는 필터로 명시하여 제외하지 않는 한 모두 동기화됩니다.

base distinguished name [기본 DN](#) 을 참조하십시오.

바인드 DN 작업을 수행할 때 LDAP 디렉토리 (Active Directory 또는 Directory Server 등)에 대한 인증에 사용되는 고유한 이름.

bind distinguished name [바인드 DN](#) 을 참조하십시오.

브로커 [Sun Java System Message Queue 브로커](#) 참조.

CA [인증기관](#)을 참조하십시오.

중첩 복제 중첩 복제 시나리오에서 하나의 서버 (때로 *허브* 공급자라고 함)가 소비자 및 특정 복제본의 공급자의 역할 모두 합니다. 이 서버는 읽기 전용 복제본을 유지하고 변경 로그를 관리합니다. 데이터의 마스터 사본이 있는 공급자 서버에서 업데이트를 수신하며, 다시 해당 업데이트를 소비자에게 공급합니다.

중앙 기록기 중앙 로그를 모두 관리하는 코어 구성요소로 모든 커넥터의 감사 및 오류 로그를 집계한 것입니다. 관리자는 이 로그를 모니터링하여 Identity Synchronization for Windows 설치 전체의 상태를 모니터링할 수 있습니다. 중앙 로그는 직접 보거나 Identity Synchronization for Windows 콘솔에서 볼 수 있습니다. 기본적으로 중앙 로그는 코어가 설치된 컴퓨터의 <install-root>/logs/central/ 하위 디렉토리에서 사용할 수 있습니다.

인증서 네트워크 ID 가 있는 공용 키에 연결된 데이터의 컬렉션 . 전자 메시지를 수신하는 개체는 이 정보를 사용하여 메시지와 메시지 송신자의 신분을 확인합니다 . Identity Synchronization for Windows 커넥터가 SSL 통신을 사용하도록 구성하는 경우 반드시 신뢰된 SSL 통신을 수행하기 전에 커넥터의 인증서 데이터베이스에 인증서를 추가해야 합니다 . 또한 [인증기관](#)을 참조하십시오 .

인증기관 인증서를 판매 및 발행하는 회사 또는 조직 . 신뢰하는 인증 기관 (다른 이름은 *CA*) 에서 인증용 인증서를 구매할 수 있습니다 . 루트 인증 기관 인증서는 다른 인증서를 서명하는 데 사용됩니다 . Identity Synchronization for Windows 커넥터가 SSL 을 사용하도록 구성하는 경우 반드시 적절한 루트 인증 기관 인증서를 커넥터의 인증서 데이터베이스에 추가해야 합니다 .

인증서 데이터베이스 인증서용 안전한 저장 장소로 cert8.db, key3.db 및 secmod.db의 세 가지 파일이 포함됩니다 . Identity Synchronization for Windows에서 각 커넥터에는 자체의 인증서 디렉토리 (예 : <install-root>/etc/CNN100) 가 있습니다 . 또한 [인증서](#)을 참조하십시오 .

문자 유형 영문자를 숫자 문자 (또는 기타 문자) 와 구분하며 대문자에서 소문자로의 매핑을 구분합니다 .

CLI 자세한 내용은 [명령줄 인터페이스](#)를 참조하십시오 .

클라이언트 [LDAP 클라이언트](#)를 참조하십시오 .

명령줄 인터페이스 전적으로 텍스트 입력 및 출력을 기반으로 한 프로그램과 사용자 사이의 통신 수단 . 명령은 키보드 또는 이와 유사한 장치로 입력하며 프로그램에 의하여 해석 및 실행됩니다 . Identity Synchronization for Windows 명령줄 인터페이스의 이름은 idsync 이며 코어를 설치한 위치의 bin/ 디렉토리에서 사용할 수 있습니다 .

구성 디렉토리 구성 및 상태 정보용 저장소의 역할을 하도록 특별히 설치된 Directory Server . Identity Synchronization for Windows 는 모든 구성을 코어 설치 동안 선택한 구성 디렉토리 인스턴스 내에 저장합니다 .

구성 비밀번호 구성 디렉토리에 있는 모든 중요한 Identity Synchronization for Windows 정보를 보호하기 위하여 코어 설치 동안 선택한 비밀번호 . 설치 프로그램 , 콘솔 또는 명령줄 인터페이스를 사용할 때 반드시 구성 비밀번호를 제공해야 합니다 .

구성 레지스트리 Identity Synchronization for Windows 가 구성 디렉토리를 의미할 때 사용하는 또 다른 용어 .

커넥터 단일 데이터 소스 (Directory Server, Active Directory 도메인 또는 Windows NT 도메인) 가 있는 Identity Synchronization for Windows 의 상호 작용을 관리하는 Java 프로세스 . 커넥터는 데이터 소스에서의 사용자 변경 내용을 검출하고 해당 변경 내용을 Message Queue 를 통하여 원격 커넥터에 게시함으로써 사용자 변경 내용을 수신하고 해당 수신 내용으로 데이터 소스를 업데이트하는 작업을 담당합니다 .

콘솔 서버 응용 프로그램을 구성 및 모니터하는 용도로 사용하는 그래픽 사용자 인터페이스 . Sun Java System Directory Server 와 Identity Synchronization for Windows 에는 별도의 콘솔이 있습니다 .

제어기 에이전트 및 액세서 구성요소와 인터페이스하는 커넥터 구성요소 . 제어기는 동기화 사용자 목록에서 사용자의 구성원 여부 확인 , 동등한 사용자 항목 검색 및 링크 , 현재 사용자 항목과 객체 캐시에 저장된 이전 버전을 비교하여 사용자에게 대한 변경 내용 검출 등 , 주요 동기화 관련 작업을 수행합니다 . 제어기는 때로 작업에 대한 로그 메시지를 의미하기도 합니다 .

코어 첫 번째로 설치되는 Identity Synchronization for Windows 구성요소 . 코어에는 구성 디렉토리에 저장된 초기 구성 , 시스템 관리자 , 중앙 기록기 , 콘솔 및 명령줄 인터페이스가 포함됩니다 .

생성 속성 객체가 만들어질 때에만 동기화되는 속성 . 모든 중요한 속성은 객체가 만들어질 때 자동으로 동기화됩니다 . 기본 값을 구성하여 원격 디렉토리에 있는 속성 값과 다른 생성 속성을 만들 수 있습니다 .

데몬 특정 시스템 작업을 담당하는 UNIX 컴퓨터의 배경 프로세스 . 데몬 프로세스는 인간의 관여 없이 기능합니다 . 커넥터 , 시스템 관리자 및 중앙 기록기는 Identity Synchronization for Windows Watchdog 이 실행하고 모니터하는 데몬 프로세스로 실행됩니다 .

디렉토리 정보 트리 대부분의 파일 시스템에서 사용하는 트리 모델을 사용하여 디렉토리에 저장된 정보를 논리적으로 제시하는 방법으로 트리의 루트가 계층의 상단에 표시됩니다 .

디렉토리 관리자 권한이 있는 Directory Server 관리자로 UNIX 의 루트 사용자와 같습니다 . Identity Synchronization for Windows 가 특정 구성 작업을 수행하려면 Directory Manager 자격 증명이 필요하나 , 커넥터가 동기화하는 경우에는 Directory Manager 가 필요하지 않습니다 .

디렉토리 소스 Sun Java 시스템 Directory Server, Windows Active Directory 도메인 또는 Windows NT 도메인 . 디렉토리 소스에는 동기화할 사용자가 포함됩니다 .

고유 이름 LDAP 디렉토리에서 항목의 이름과 위치를 나타내는 문자열 .

DIT 디렉토리 정보 트리를 참조하십시오 .

DM 디렉토리 관리자를 참조하십시오 .

도메인 (1)(n.) 도메인 이름을 소유한 회사 또는 단체를 식별하는 정규화된 도메인 이름의 마지막 부분 (예 : example.com, host.example.com).

(2) (n.) 단일 컴퓨터 시스템이 제어하는 리소스 .

도메인 제어기 계정 정보를 저장하고, 사용자를 인증하며 Windows 도메인용 보안 정책을 집행하는 Windows 서버 . Identity Synchronization for Windows 커넥터는 도메인 제어기와 직접 통신하여 사용자 계정에 대한 변경 내용을 검출하고 Directory Server 사용자 항목의 변경 내용을 동기화합니다 .

DNS 도메인 이름 시스템 . 네트워크의 컴퓨터가 표준 IP 주소 (198.93.93.10 등) 를 호스트 이름 (www.example.com 등) 과 연결하는데 사용하는 체계 . 컴퓨터는 보통 DNS 서버에서 호스트 이름의 IP 주소를 받거나 자체 시스템에 보관된 테이블에서 이 정보를 검색합니다 .

파일 확장자 파일 이름에서 마침표 (.) 뒤에 이어지는 부분으로 보통 파일의 유형을 정의 (예 : .GIF 및 .HTML). 예를 들어 , index.html 이라는 파일 이름의 경우 파일 확장자는 html 입니다 .

파일 유형 파일의 형식 . 예를 들어 그래픽 파일은 때로 GIF 형식으로 저장되며 텍스트 파일은 주로 ASCII 텍스트 형식으로 저장됩니다 . 파일 유형은 주로 **파일 확장자** (.GIF 또는 .HTML 등) 에 의하여 구분됩니다 .

FSMO 역할 유연한 단일 마스터 작업 역할 . Active Directory 가 복수 마스터 구현에서 업데이트 충돌을 방지하기 위하여 사용하는 메커니즘입니다 . 복수 마스터 구현인 경우에도 일부 객체는 단일 마스터 모드에서 업데이트되며 이는 Windows NT 도메인의 기본 도메인 제어기 (PDC) 의 이전 개념과 매우 유사합니다 . Active Directory 구현에는 다섯 가지의 FSMO 역할이 있으나 오직 PDC 에뮬레이터 역할만 Identity Synchronization for Windows 에 영향을 미칩니다 . 비밀번호 업데이트는 오직 PDC 에뮬레이터 역할이 있는 Active Directory 도메인에서만 즉시 복제되므로 Identity Synchronization for Windows 는 이 도메인 제어기를 동기화에 사용합니다 . 그렇지 않은 경우 Sun Java System Directory Server 와의 동기화가 수 분 정도 지연될 수 있습니다 .

전역 카탈로그 Active Directory 디렉토리 토폴로지와 Active Directory 디렉토리용 스키마 정보를 저장하는 Windows 저장 장소 .

호스트이름 machine.domain.com 의 형식으로 표시되는 컴퓨터의 이름으로 이는 IP 주소로 변환됩니다 . 예를 들어 www.example.com 은 com 도메인의 example 하위 도메인에 있는 www 컴퓨터를 나타냅니다 .

Identity Synchronization for Windows 콘솔 Identity Synchronization for Windows 를 구성 및 모니터링하는 용도로 사용하는 그래픽 사용자 인터페이스 .

인바운드 커넥터에서 디렉토리 소스에서 Message Queue 로 향하는 작업의 방향 . 커넥터가 검출한 변경은 시스템에 대하여 인바운드로 흐릅니다 . 작업에 대한 로그 메시지는 때로 커넥터의 인바운드 측에서 발생한 이벤트를 의미합니다 .

IP 주소 인터넷 프로토콜 주소 . 마침표로 분리된 일련의 번호로 인터넷에 있는 컴퓨터의 실제 위치를 지정합니다 . (예 : 192.168.2.1)

ISO 국제 표준화 기구 .

Java Message Service Java 2 Platform Enterprise Edition(J2EE) 를 기반으로 한 응용 프로그램 구성요소가 메시지를 생성 , 전송 , 수신 및 읽을 수 있도록 하는 메시징 표준 API . 결합이 느슨하며 믿을 수 있고 비동기화된 통신을 배포할 수 있습니다 .

JMS [Java Message Service](#) 참조 .

LDAP 경량 디렉토리 액세스 프로토콜 TCP/IP 를 통하여 복수 플랫폼 전체에서 실행되도록 고안된 디렉토리 서비스 프로토콜입니다 . Identity Synchronization for Windows 는 LDAP 를 사용하여 Active Directory 도메인 컨트롤러 및 Sun Java System Directory Server 와 통신합니다 .

LDAP 클라이언트 LDAP Directory Server 에서 LDAP 항목을 요청하고 확인할 때 사용하는 소프트웨어 . Identity Synchronization for Windows 커넥터는 LDAP 서버에 연결할 때 LDAP 클라이언트의 역할을 합니다 .

LDAP URL DNS 를 사용하는 Directory Server 를 찾은 후 LDAP 를 통하여 쿼리를 완료하는 수단을 제공합니다 . 예제 LDAP URL 은 ldap://ldap.example.com 입니다 .

경량 디렉토리 액세스 프로토콜 [LDAP](#) 를 참조하십시오 .

로케일 특정 지역 , 문화 및 관습의 사용자의 데이터를 표현할 때 사용하는 조합 순서 , 문자 유형 , 통화 형식 및 시간 / 날짜 형식을 구분합니다 . 여기에는 지정된 언어의 데이터가 해석 , 저장 및 조합되는 방식이 포함됩니다 . 로케일은 또한 지정된 언어를 표시할 때 어느 코드 페이지를 사용할 것인지 나타냅니다 .

기본 객체 클래스 [구조적 객체 클래스](#) 참조 .

Message Queue 자세한 내용은 [Sun Java System Message Queue](#) 를 참조하십시오 .

MMR 복수 마스터 복제 참조 .

MQ Sun Java System Message Queue 참조 .

복수 마스터 복제 쓰기 또는 업데이트를 수행하기 전에 다른 마스터 복제본과 통신하지 않고 임의의 여러 마스터 복제본에서 항목을 쓰고 업데이트하는 디렉토리 서버 복제 모델 . 서버에서 수정된 내용은 자동으로 다른 서버로 복제됩니다 . Identity Synchronization for Windows 는 복수 디렉토리 서버 마스터가 있는 구현에 설치할 수 있습니다 . 그러나 변경 내용을 Windows 로 동기화하는 경우 반드시 기본 디렉토리 서버를 사용할 수 있어야 하며 Windows 에서 변경 내용을 동기화하는 경우 기본 또는 보조 디렉토리 서버를 반드시 사용할 수 있어야 합니다 .

이름 지정 컨텍스트 (또한 루트 접미어라 함) 고유한 이름 (DN) 으로 구분되는 디렉토리 정보 트리 (DIT) 의 특정 접미어 . 예 : dc=example,dc=com. Identity Synchronization for Windows 에서 Sun Java 시스템 Directory Server 용 디렉토리 소스는 동기화될 데이터에 포함된 접미어에 의하여 정의됩니다 .

객체 캐시 Windows 커넥터가 사용자 항목의 변경 내용을 검출하는 용도로 사용하는 프로세스 내 데이터베이스 . 객체 캐시는 각 사용자 항목의 해시된 요약이 저장되며 , 따라서 Windows 커넥터가 사용자 항목에서 변경된 특정 속성을 확인할 수 있습니다 .

객체 클래스 항목이 기술하는 객체의 종류와 항목에 포함된 일련의 유효한 필수 속성을 지정하는 템플릿 . 예를 들어 Directory Server 는 inetorgperson 객체 클래스를 지정하며 , 여기에는 cn 및 userpassword 등의 속성이 포함됩니다 . 요청시 비밀번호 동기화 : Directory 서버의 사용자 비밀번호를 사용자가 Directory Server 에 대한 인증을 시도할 때까지 업데이트되지 않는 메커니즘 . 사용자의 비밀번호는 입력한 비밀번호가 Active Directory 에 저장된 비밀번호와 일치되는 경우에만 동기화됩니다 . 이를 사용하면 Active Directory 환경에서의 비밀번호 동기화가 단순화됩니다 .

아웃바운드 커넥터에서 Message Queue 에서 디렉토리 소스로 향하는 작업의 방향 . 커넥터가 적용한 변경의 흐름이 아웃바운드로 디렉토리 소스를 동기화합니다 . 작업에 대한 로그 메시지는 때로 커넥터의 아웃바운드 측에서 발생한 이벤트를 의미합니다 .

비밀번호 파일 UNIX 컴퓨터에 있는 파일로 UNIX 사용자 로그인 이름 , 비밀번호 및 사용자 ID 번호를 저장합니다 . 또한 위치에 따라 /etc/passwd 라고도 합니다 .

비밀번호 정책 지정된 디렉토리에서 비밀번호의 사용 방식을 결정하는 일련의 규칙 .

권한 액세스 컨트롤이라는 면에서 권한에 따라 디렉토리 정보에 대한 액세스가 허용 또는 거부되며 , 허용 또는 거부된 액세스의 수준이 결정됩니다 .

플러그인 전체 시스템의 일부로 로드되고 사용되는 보조 프로그램 .

예를 들어 Identity Synchronization for Windows 는 Directory Server 플러그인을 사용하여 Directory Server 커넥터 변경 검출 기능을 강화하며 Active Directory 및 Directory Server 사이에서 비밀번호 동기화를 양방향으로 지원합니다 .

기본 디렉토리 서버 Identity Synchronization for Windows 가 사용자 항목에 대한 변경을 검출하고 적용하는 용도로 사용하는 디렉토리 서버 마스터 인스턴스 . 이 서버를 사용할 수 있는 경우 Identity Synchronization for Windows 는 다른 디렉토리 서버 마스터와 통신하지 않습니다 .

프로토콜 네트워크에 있는 장치가 정보를 교환하는 방법을 기술한 일련의 규칙 .

RCL retro changelog 를 참조하십시오 .

resync 간격 디렉토리 소스에서 변경을 확인하는 간격 . 이 주기적 확인은 효과적이며 마지막 확인 후 변경된 사용자의 항목만 읽으면 됩니다 . 콘솔에서는 이 값을 1/1000 초 단위로 표시하며 기본 값은 1000(1 초) 입니다 .

retro changelog Directory Server 에 대한 변경 내용의 기록을 모두 저장하는 Directory Server 데이터베이스 (cn=changelog). Identity Synchronization for Windows 는 retro changelog 를 사용하여 Directory Server 에서 변경된 내용을 검출합니다 . MMR 환경의 경우 반드시 Preferred Directory Server 에서 retro changelog 를 사용하도록 설정해야 합니다 .

루트 UNIX 컴퓨터에서 가장 권한이 많은 사용자 (슈퍼유저라고도 함). 루트 사용자는 컴퓨터의 모든 파일에 액세스할 수 있는 완전한 권한을 가집니다 . Solaris 시스템에서 Identity Synchronization for Windows 는 반드시 루트로 설치해야 합니다 .

루트 접미어 하나 이상의 LDAP 하위 접미어에 대한 상위 접미어 . 디렉토리 트리에는 하나 이상의 루트 접미어가 있습니다 .

스키마 디렉토리에서 항목으로 저장할 정보의 유형을 기술하는 정의 . 스키마와 일치하지 않는 정보가 디렉토리에 저장되는 경우 해당 디렉토리에 액세스하려는 클라이언트가 적절한 결과를 표시할 수 없게 됩니다 .

스키마 검사 디렉토리에서 추가 또는 수정된 항목이 정의된 스키마를 준수하는지 확인합니다 . 기본적으로 스키마 검사는 사용 설정되며 스키마를 준수하지 않는 항목을 저장하는 경우 오류가 수신됩니다 .

보조 디렉토리 서버 기본 디렉토리 서버를 사용할 수 없는 경우 Identity Synchronization for Windows 가 사용할 수 있는 MMR 환경의 디렉토리 서버 마스터 인스턴스 . 기본 디렉토리 서버를 사용할 수 없는 동안 Identity Synchronization for Windows 는 Active Directory 또는 Windows NT 에서 변경된 내용을 보조 디렉토리 서버와 동기화할 수 있습니다 . 그러나 보조 서버 또는 다른 디렉토리 서버 마스터에서 수정된 내용은 기본 디렉토리 서버를 사용할 수 있을 때까지 동기화되지 않습니다 .

Secure Sockets Layer SSL 을 참조하십시오 .

서버 콘솔 GUI 에서 Directory Server 의 관리를 수행할 수 있도록 하는 Java 기반 응용 프로그램 .

서버 루트 서버 프로그램 구성 , 유지 보수 및 정보 파일 전용으로 할당된 서버 컴퓨터 내의 디렉토리 .

서비스 특정 시스템 작업을 담당하는 Windows 컴퓨터의 배경 프로세스 . 서비스 프로세스는 인간의 관여 없이 기능합니다 . Windows 에서 커넥터 , 시스템 관리자 및 중앙 기록기는 Identity Synchronization for Windows Watchdog 서비스가 실행하고 모니터링하는 프로세스로 실행됩니다 .

중요 속성 항목을 만들거나 수정할 때 동기화되는 속성 .

SSL Secure Sockets Layer. 두 당사자 (클라이언트와 서버) 사이에서 안전한 연결을 설정하기 위하여 사용하는 소프트웨어 라이브러리 . HTTPS, HTTP 의 보안 버전 및 LFAP 의 보안 버전인 LDAPS 를 구현하는 용도로 사용됩니다 .

구조적 객체 클래스 Identity Synchronization for Windows 가 동기화하는 일련의 유효한 필수 속성을 정의하는 항목의 기본 객체 클래스 . 예를 들어 기본 Active Directory 객체 클래스는 user 이며 기본 Directory Server 객체 클래스는 inetorgperson 입니다 . **보조 객체 클래스**를 참조하십시오 .

하위 구성요소 커넥터와 별도로 실행되는 경량 프로세스 또는 라이브러리 . 하위 구성요소는 커넥터가 관리하는 디렉토리 소스에 가까이 실행되며 원격 컴퓨터 또는 별도의 프로세스에서 수행할 수 없는 기능을 커넥터에서 사용할 수 있습니다 . 하위 구성요소는 사용자 정의 암호화 채널을 통하여 커넥터와 통신하여 구성 정보를 수신하고 , 변경 이벤트를 보고하며 중앙 기록기로 로그합니다 . Identity Synchronization for Windows 에는 Directory Server 플러그인 , Windows NT 비밀번호 필터 DLL 및 Windows NT 변경 검출기 등의 세 가지 하위 구성요소가 있습니다 .

접미어 디렉토리 상단의 항목 이름으로 이 아래에 데이터가 저장됩니다 . 동일한 디렉토리에 여러 개의 접미어가 있을 수 있습니다 . 각 데이터베이스에는 오직 하나의 접미어만 있습니다 .

SUL [Synchronization User List](#) 참조.

Sun Java System Message Queue Java Message Service(JMS) 개방형 표준을 구현하는 엔터프라이즈 메시징 시스템. Message Queue 의 기본 아키텍처는 공통 서비스를 통하여 메시지를 교환하는 게시자와 가입자로 구성됩니다. Sun Java System Message Queue 는 전용 메시지 브로커가 관리하며 Message Queue 에 대한 액세스 제어, 사용 중인 게시자 및 가입자에 대한 정보 유지 및 메시지 전달 확인 등을 담당합니다. Identity Synchronization for Windows 는 Message Queue 를 사용하여 사용자 변경 이벤트를 안전하게 동기화하고 구성 정보를 배포하며 원격 구성요소의 상태를 모니터링합니다.

Sun Java System Message Queue 브로커 Sun Java System Message Queue에 대한 클라이언트 액세스를 제공하는 독립형 Java 서버. Solaris 에서 브로커는 /etc/init.d/imq 스크립트를 통하여 제어하며 Windows 의 경우 "iMQ Broker" 서비스를 통하여 제어합니다. Identity Synchronization for Windows 는 코어 설치 동안 브로커를 구성 및 시작합니다.

수퍼유저 [루트](#) 참조.

동기화 호스트 Synchronization User List(SUL) 에 정의된 규칙에 따라 동기화된 데이터를 저장하는 서버.

Synchronization User List 동기화될 Sun 및 Windows 디렉토리의 사용자를 정의. 동기화 사용자 목록으로 LDAP 기반 DN 또는 필터를 기준으로 동기화될 사용자의 범위를 제한할 수 있습니다.

동기화된 속성 [중요 속성](#) 참조.

시스템 관리자 코어가 설치된 위치의 Watchdog 데몬 / 서비스가 시작하는 독립형 Java 프로세스. 시스템 관리자는 구성 정보를 콘솔과 중앙 기록기에 배포하며, 시스템의 상태를 모니터링하고 idsync resync 작업을 조절합니다.

토폴로지 실제 서버에서 디렉토리 트리가 분할되는 방식과 해당 서버가 서로 연결되는 방식입니다.

uid UNIX 시스템의 각 사용자에게 연결된 고유 번호.

URL Uniform Resource Locator. 서버와 클라이언트가 문서를 요청할 때 사용하는 주소 지정 체계. URL 은 또한 위치라고도 합니다. URL 의 형식은 [protocol]://[machine:port]/[document] 입니다. 포트 번호는 선택한 서버에만 필요하며, 때로 사용자가 URL 에 명시할 필요가 없도록 서버가 지정합니다.

Watchdog 코어 또는 커넥터가 설치된 모든 컴퓨터에 설치되는 독립형 Java 프로세스. Watchdog 은 시스템 관리자, 중앙 기록기 및 커넥터를 포함하여 모든 Identity Synchronization for Windows Java 프로세스를 시작합니다. 이들 구성요소에 오류가 발생하는 경우 Watchdog 이 이를 다시 시작합니다. Solaris 에서 Watchdog 은 /etc/init.d/isw 데몬 스크립트를 통하여 제어하며 Windows 의 경우 "Sun Java™ 시스템 Identity Synchronization for Windows" 서비스를 통하여 제어합니다.

숫자

3DES 키 280

A

ACI 286, 311

Active Directory

MMR 구현 223

objectclasses 61

Resync 간격 121

SSL 구성 73, 109

SSL 사용 114, 120, 244, 258, 262, 279, 280, 293–297

SSL, 사용 114, 120, 244, 258, 262, 279, 280, 293–297

SUL 생성 149

객체 삭제 흐름 148

객체 작성 흐름 131, 132

객체 캐시 데이터베이스 177

객체 캐시 파일 65

고급 보안 옵션 120, 279

구성요소 배포 예 49

구현 113

기본 도메인 제어기 FSMO 역할 소유자 118

도메인 113, 115, 332, 333

도메인 제어기 46, 48, 118, 119, 121, 244, 262

도메인 제어기 구성 매개변수 편집 121

동기화 설정 48, 61, 244

디렉토리 60

디렉토리 소스 113, 161

디렉토리 소스 생성 113

마이그레이션 도중 197

마이그레이션 중 비밀번호 동기화 186

물리적 구현 48

미리 존재하는 사용자 182

변경 검색 40

보안 옵션 120

보안 통신 사용 109

복수 도메인 332, 333

복수 도메인 제어기 사용 118

복수 호스트 구현 226

비밀번호 동기화 46, 65, 108, 186

비밀번호 전달 73

비밀번호 정책 65, 67

사용자 DN 114

사용자 동기화 176, 179

사용자 연결 178, 179

사용자 인증 실패 44

삭제 동기화 147

샘플 구현 예 46

생성 내용 흐름, 지정 131

생성 속성, 지정 134

소스

만들기 101, 113

속성 61, 125, 136

속성 동기화 108, 125

속성 매핑 125, 134

속성 선택 125

속성 편집 136

스키마 제어기 75
 신뢰되지 않은 인증서 259
 신뢰된 인증서 120, 259, 279, 287
 양방향 동기화 28
 요청시 비밀번호 동기화 42, 46, 177, 186, 244, 258, 262
 인증서 119, 120, 244, 259, 262, 279, 287, 293–297
 인증서 데이터베이스 120
 인증서 가져오기 293–297
 작성 표현식 152
 전역 카탈로그 61, 75, 113, 114
 지원되는 버전 27
 커넥터 배포 157
 커넥터 설명 33
 커넥터 설치 37, 166
 커넥터 요구 사항 52
 커넥터, 문제 해결 246
 커넥터, 설치 166
 커넥터 - 도메인 제어기 통신 46
 코어 구성 75
 콘솔 제거 239
 특수 사용자 182
 파일오버 서버 120
 호스트 114, 116, 223, 226, 244
 활성화 / 비활성화 동기화 139

Administration Server
 SSL 통신 사용 설정 87
 URL 위치 93
 설치 85
 코어 설치 36, 84

audit.log 72
 결과 연결 및 재동기화 318
 문제 확인 242
 설명 32, 265
 용도 265
 위치 265, 274
 작동 244, 253
 커넥터 문제 해결 244, 246, 247

AvoidPdcOnWan 속성 118

B

base64 암호화 294, 302

C

CA 인증서
 SSL 사용 293
 가져오기 290
 구성요소 요구 사항 286
 문제 해결 244, 259
 불러오기 293, 296, 297
 예 260
 자동 설치 119
 추가 262, 279, 296, 297

certinfo 하위 명령
 구문 307
 사용 289
 설명 76, 306
 예 307
 인수 289
 인증서 정보 표시 76, 306
 인증서 추가 307

certutil
 SUNWtlsu 패키지 259
 기본 위치 20, 259, 291
 실행 259, 294
 인증서 불러오기 294

changeppw 하위 명령
 구문 308
 비밀번호 변경 308
 설명 76, 307, 308
 예 308
 인수 308

checktopics 유틸리티
checktopics.jar 200
 구문 195
 기본 위치 194
 메시지 비우기 195
 사용 194

설명 187, 194
 전제 조건 195
 checktopics.jar 195, 200
 Configuration 탭 99
 설명 99
 connector-state.jar 201, 206

D

Directory Server

Directory Server 도구와 상호 운용 140
 Identity Synchronization for Windows 소스 준비 109
 idsync prepds 사용 76, 307
 objectclasses 61
 SSL 을 통한 액세스 303
 디렉토리 소스 준비 58, 310
 변경 검출 39
 비밀번호 동기화 46
 비밀번호 전달 73, 74
 비밀번호 정책 67
 사용자 정의 방법 사용 140, 142
 설치 53
 설치 프로그램 158
 속성 동기화 125
 속성 수정 내용 흐름 138
 액세스 권한 117
 양방향 동기화 28
 업그레이드 204
 자격 증명 / 권한 282
 재시작 202
 준비 58, 76, 109, 110, 307, 312
 지정 106
 최소 디스크 공간 53
 커넥터 설치 36, 160
 커넥터, 설명 33
 커넥터, 설치 160
 콘솔 140, 251
 플러그인 설치 36
 필수 패치 53

Directory Server 도구와 상호 운용 140

Directory Server 플러그인

MMR 환경에서 설치 338
 SSL 사용 109, 297
 로그 267
 문제 해결 243, 244, 250, 253, 262
 변경 검출 39
 보안 통신 사용 109, 297
 비밀번호 변경 동기화 186
 비밀번호 암호화 280
 설명 34, 108
 설치 36, 108, 157-174
 양방향 동기화 34
 인증서 추가 307
 제거 202, 209, 214, 231, 233
 커넥터와 통신 163, 170

DLLs

NT 변경 검출기 266
 Windows NT 34, 38
 비밀번호 필터 42

DN 114

DNS

도메인 항목 105
 정의 347
 호스트 이름 244

dspswuserlink 속성 178, 313

dspswvalidate 속성 43

E

error.log

문제 해결 242
 설명 32, 265
 위치 242, 265, 274
 커넥터 ID 를 디렉토리 소스로 매핑 296, 297
 커넥터 문제 해결 248

etc 디렉토리

백업 188, 201
 복구 206
 제거 206

export10cnf 유틸리티 188
 export10cnf.jar 200
 설명 187
 일반 텍스트 비밀번호 삽입 189
 export10cnf.jar 189, 200

F

forcepwchg 유틸리티
 마이그레이션 준비 200
 비밀번호 변경 집행 196, 321
 비밀번호 변경 필요 196
 설명 77, 187, 321
 위치 196
 인수 321
 forcepwchg.jar 321
 FSMO 118

I

Identity Synchronization for Windows

Directory Server 디렉토리 소스 준비 58, 310
 Directory Server 소스 준비 109
 구성 187
 다운로드 54
 문제 해결 251
 서비스 확인 251
 설치 51, 204
 설치 요구 사항 51-55
 설치 프로그램 17, 81
 신뢰도 45
 자격 증명 / 권한 설치 54
 제거 17, 82, 202, 231-??, 231-239, ??-239
 코어 구성요소 설치 85
 콘솔 271, 272, 273

idsync certinfo 289

구문 308
 설명 307
 예 307

인수 307
 인증서 추가 307

idsync changepw

구문 307
 비밀번호 변경 308
 설명 308
 예 308
 인수 307

idsync importcnf

구문 310
 구성 파일 가져오기 188, 205, 310
 설명 77, 307, 310
 예 189
 인수 205, 304, 310

idsync prepds

Directory Server 준비 58, 307
 구문 312
 설명 76, 307
 자격 증명 311

idsync printstat

구문 314
 상태 인쇄 314
 설명 314
 설치 / 구성 단계 목록 314
 인수 314

idsync resetconn

구문 315
 설명 315
 인수 315

idsync resync 59

구문 316
 기존 사용자 동기화 316
 두 디렉토리 소스 재동기화 177
 로그 기록 182
 명령 243
 사용 177
 사용시 주의사항 182
 사용예 181
 사용자 동기화 문제 해결 243
 색인화된 속성 182
 설명 316
 스크립트 178

예제 linkusers XML 구성 문서 323
 인수 316
 인수 예제 181
 idsync script, 실행 76, 306
 idsync startsync
 구문 318
 설명 318
 인수 318
 idsync stopsync
 구문 319
 설명 319
 인수 319
 importcnf 하위 명령
 구성 파일 가져오기 188, 205
 설명 77, 307, 310
 예 189
 인수 205, 304, 310
 iMQ Broker 서비스 255
 imq start 명령 184
 imq stop 명령 184
 inetorgperson 속성 63
 isw start 명령 183
 isw stop 명령 183
 isw-12004Q3 디렉토리 83
 isw12004Q3 디렉토리 84
 isw-hostname 디렉토리 20, 204, 205, 207, 213, 232, 235

J

J2SE 요구 사항 54
 jar 파일
 checktopics 195, 200
 connector-state 201, 206
 export10cnf 200
 exportcnf 189
 forcepwchg 321
 jss3.jar 82, 202
 마이그레이션 도구 200

Java 2 SDK, 업그레이드 204
 Java Development Kits, 다운로드 81
 Java Home, 지정 89
 Java Runtime Environment. *JRE* 를 참조
 java 프로세스
 Watchdog 30
 구성 디렉토리 30
 명령줄 유틸리티 31
 시스템 관리자 32
 재시작 30
 정지 213
 중앙 기록기 32, 250
 커넥터 33
 콘솔 31
 클래스 이름 250
 java.exe 251
 JRE
 Java Home 디렉토리 확인 89
 다운로드 81
 업그레이드 204
 요구 사항 54
 jss3.jar 파일, 제거 82, 202

K

keytool 유틸리티 285

L

LDAP
 DIT 75
 ldapsearch 211, 321
 기본 포트 104
 예제 URL 348
 인증서 불러오기 294
 쿼리 구문 152
 필터 64, 79, 304, 317
 ldapsearch, 사용 211, 212, 321

LinkUsers XML 문서 323
linkusers.cfg 323, 325
linkusers-simple.cfg 324
localhost 이름, 지정 91

M

Message Queue 214
 localhost 이름 지정 90
 구성 90
 기본 브로커 포트 91
 문제 해결 254
 브로커 35
 설명 35
 설치 54
 설치용으로 필요 54
 액세스 제어 281
 업그레이드 204
 영구 메시지 저장 257
 인증서 승인 286
 인증서 유효성 검사 285
 자체 서명 인증서 285
 전달되지 않은 메시지 확인 257
 클라이언트 인증서 유효성 검사 285
 포트 번호 지정 90
Microsoft
 인증서 서버 119
 지식 베이스 자료 22, 118
 출판물 21

MMR

4 방향 지원 338
Directory Server 플러그인 설치 338
구성 337, 338, 341
구성 구성요소 287
구현 223
마이크레이션 시나리오 223
실행할 수 있는 동기화 45

Multimaster Replication. *MMR* 참조

N

netstat -n -a commands 253
nsAccountLock 속성 140, 141
NT Registry 디렉토리 소스 101
NT SAM
 도메인 사용자 177
 동기화 38
 디렉토리 소스 122
 디렉토리 소스 구성 122
 레지스트리 34, 41
 연결용 식별자 178
NT 변경 검출기 DLL 266

O

objectclasses
 Active Directory 61
 Directory Server 61
 구성 62
 구조적 61
 보조 61, 344
 사용자 74
 선택 130
 속성 61, 130
objectguid 속성 178

P

PDC
 forcepwhchg 유틸리티 실행 196
 FSMO 역할 소유자 118
 커넥터 및 하위 구성요소 설치 38
 컴퓨터 이름 위치 검색 123
PDC 컴퓨터 이름 위치 검색 123
persist 디렉토리 65
 백업 188, 201
 복구 206

제거 206

PIN 파일, 생성 292

prepdns 하위 명령

- Directory Server 준비 58, 76, 307
- 구문 312
- 설명 76, 307
- 예 312
- 인수 312
- 자격 증명 311

printstat 하위 명령

- 구문 314
- 설명 314
- 설치 / 구성 단계 표시 76, 307
- 인수 314
- 커넥터 상태 인쇄 76, 307

psswatchdog.exe. Watchdog 프로세스 참조

PwdLastSet 속성 43

R

RAM 요구사항 53

regedt32.exe 201, 205, 219, 220

resetconn 하위 명령 315

- 구문 315
- 설명 315
- 인수 315
- 커넥터 상태 재설정 76, 307

Resync 간격

- Active Directory 커넥터용 설정 121
- default 113
- Directory Server 커넥터용 설정 113
- NT 용 설정 124
- 설명 350

resync 하위 명령 179, 181, 317, 318, 323

- 구문 316
- 기존 사용자 동기화 316
- 부트스트랩 구현 59
- 사용자 링크 및 동기화 177
- 사용자 링크 / 동기화 76, 307

설명 316

인수 316

resync.log

- 결과 연결 및 재동기화 182, 318
- 설명 265
- 위치 265

Retro-Changelog 데이터베이스

- 만들기 110
- 변경 검색 39
- 재생성 113

S

samples1 디렉토리 323

SASL Digest-MD5 44

Secure Sockets Layer (SSL) 16, 21, 277

security

- Active Directory 120
- 강화 283
- 구성 277-298
- 구성 복제 286

setup.exe 84, 158

Solaris

- Identity Synchronization for Windows 제거 239
- SPARC 83
- x86 83
- 구성요소 문제해결 249
- 데몬 시작 / 정지 183
- 설치 프로그램 실행 83
- 요구 사항 52
- 패키지 제거 208
- 필수 패치 53

SSL

- Active Directory 구성 73, 114, 120
- Active Directory 에서 사용 258, 262, 279, 280
- Directory Server 액세스 303
- Windows 용 구성 73
- 기본 포트 86
- 문제 해결 257
- 복제본 구성 340

사용 109, 279, 290, 292, 297
 신뢰된 인증서 필요 120
 인증서 120, 279, 286
 코어용으로 사용 설정 159
 통신 사용 설정 107, 109, 290
 포트 선택 159
 startsync 하위 명령
 구문 318
 동기화 시작 76, 307
 설명 318
 인수 318
 status
 Configuration Validity Status 154
 보기 247, 264, 271, 272
 커넥터 247, 314
 커넥터 상태 인쇄 314
 Status 탭 99
 STDIN, 비밀번호 읽기 305
 stopsync 하위 명령
 구문 319
 동기화 정지 76, 307
 인수 319
 SUL
 관리자 필터링 152
 만들기 64, 66
 삭제 124
 설명 64, 149, 352
 저장 154
 정의 64
 정의 구성요소 149, 332
 SULs
 만들기 148–154
 정의 331–336
 Sun Java 시스템
 디렉토리 소스 생성 101, 102
 디렉토리 스키마 서버 74
 콘솔 97
 Sun Java^a System Directory Server. *Directory Server*
 참조

Sun Java^a System Identity Synchronization for
 Windows *Identity Synchronization for Windows* 를
 참조하십시오 .
 Sun Java^a System Message Queue. *Message Queue*
 참조
 Sun 온라인 리소스 22
 SUNWidscm 패키지 209
 SUNWidscn 패키지 209
 SUNWidscr 패키지 209
 SUNWidsct 패키지 209
 SUNWidsoc 패키지 209
 SUNWjss 패키지 , 제거 82, 202
 SUNWtlsu 패키지 259
 SystemManagerBootParams.cfg 파일 309

T

Tasks 탭 99
 telnet 명령 254
 TEMP 디렉토리 164, 234, 252
 To Do 노트 263, 272
 To Do 목록 56, 91, 155, 165, 168

U

uid 속성 179
 uninstall.cmd 스크립트 232
 UNIX 명령
 Directory Server 다시 시작 202
 Java Home 확인 89
 데몬 시작 / 정지 183
 디렉토리 제거 206
 이진 제거 203
 이진 파일 압축 해제 83
 제거 프로그램 203
 제품 이진 파일 압축 해제 199
 커넥터 상태 백업 201

UNIX 설치 권한 55

URL

Administration Server 93

구성 디렉토리 86, 159

useradd 명령 329

USNchanged 속성 40, 43

UTF-8 306, 321

W

Watchdog 프로세스 30, 250, 251

WatchList.properties 251, 252, 285

Windows

Identity Synchronization for Windows 제거 239

SSL 구성 73

구성요소 문제해결 251

디렉토리 소스 생성 113

디렉토리 소스 선택 150

서비스 시작 / 정지 99, 183

설치 권한 55

설치 프로그램 실행 84

요구 사항 52

Windows Active Directory. *Active Directory* 참조

Windows NT

Registry 46

감사 사용 42, 274

객체 캐시 파일 65

기본 도메인 제어기 75

도메인 이름 지정 122

동기화 설정 61

디렉토리 소스 생성 122

레지스트리 41

문제 해결 244, 253

변경 검출 41

커넥터 및 하위 구성요소 설치 38

커넥터 설명 33

커넥터 설치 170

하위 구성요소 244, 253

X

XML 구성 문서

export10cnf 187, 188

linkusers.cfg 325

linkusers-simple.cfg 324

구성 내보내기 188

내보낸 1.0 구성 가져오기 93

만들기 187

사용자 연결 78, 179, 317

예제 190, 323

오류 205

Z

가져오기

CA 인증서 290

구성 정보 310

감사, Windows NT 에서 사용 42, 274

감사 / 오류 로그 보기 273

객체 131

변경 내용 흐름 지정 137-146

삭제 148

삭제 흐름 지정 147

활성화 / 비활성화 구성 139

객체 캐시

데이터베이스 40, 177

초기화 177

파일 65

객체 캐시 초기화 177

검출

변경 33, 34, 39-42, 45, 106, 244, 249

오류 32, 205

활성화 / 비활성화 139-146

경고, 구성 155

경량 프로세스 33

계정

내장 322

만들기 68, 162, 329

문제 해결 243

고 가용도 설명 45

고급 보안 옵션, 지정 108, 120

고유한 이름

관리자 117

정의 346

지정 114, 117

관련 설명서 21

관리자

(바인드된) 고유 이름 입력 104, 114

Directory Server 준비 110, 312

SUL에서 필터링 152

uninstall.cmd 스크립트 실행 232

디렉토리 소스 재동기화 177

사용자 고유 이름 114

사용자 연결 178

액세스 제한 286

자격 증명 / 권한 74, 75, 87, 284

제품 설치 55

구문

changepw 하위 명령 308

checktopics 명령 195

checktopics 유틸리티 195

export10cnf 명령 189

forcepwchg 명령 321

idsync 306

idsync certinfo 명령 308

idsync changepw 명령 308

idsync importcnf 205, 310

idsync prepds 명령 312

idsync printstat 명령 315

idsync resetconn 명령 315

idsync resync 명령 317

idsync startsync 명령 319

idsync stopsync 명령 319

LDAP 쿼리 152

LDAP 필터 64

구성

Identity Synchronization for Windows 187

Message Queue 90

MMR 338

MMR 환경 341

security 277-298

SSL 73

SSL을 통한 복제 340

To Do 목록 56

내보내기 188

로그 파일 269, 271

배포 결정 73

복수 도메인 331-336

복수 접미어 338

상태 보기 272

속성 동기화 131

유효성 검사 155

저장 154

접미어 105

커넥터 253

코어 17, 74, 77, 95-156

필터 334

활성화 / 비활성화 139

구성 디렉토리

URL 74, 86, 159

관리자 이름 / 비밀번호 87, 159

구성 정보 암호화 88

기본 포트 86

기술 / 설명 91

설명 30

액세스 제한 286

연결 304

용도 74, 75

인증서 유효성 검사 286

읽기 / 쓰기 30

자격 증명 284

자격 증명 지정 87

쿼리 103

호스트 이름 / 포트 번호 179, 317

호스트 / 포트 지정 86

구성 비밀번호

idsync changepw 사용 308

변경 76, 307, 308

보호 284

지정 278

찾기 309

구성 요소

ID 265

- Sun Java System 소프트웨어 요구 사항 53
- 구성 디렉토리 30
- 로그 수준 268
- 로컬 로그 266
- 메시지 265
- 문제 해결 249
- 물리적 구현 예 48
- 배포 36-38, 49
- 배포 예 49
- 설명 29
- 설치 85
- 코어 30, 57, 344, 352, 353
- 콘솔 31
- 구성 저장 154
- 구조적 objectclass
 - 구성 62
 - 기본값 62
- 구현
 - Active Directory 113
 - idsync resync 실행 59
 - MMR 223, 337
 - NT 플랫폼 122
 - 구성 요소 배포 36
 - 단일 호스트 55
 - 동기화 요구 사항 46
 - 두 대의 컴퓨터가 있는 시나리오 46-49
 - 복수 호스트 225, 226
 - 부트스트랩 59
 - 설치 / 구성 결정 73
 - 예 48
 - 위상을 XML 문서로 내보내기 187
- 구현, 단일 호스트 197
- 권장 내용 16, 21
- 권한 / 자격 증명 74, 87
 - Directory Server 구성 75
 - idsync prepds 에 필요 311
 - 구성 디렉토리 284
 - 설치용으로 필요 54
 - 연결용으로 필요 282
 - 자격 증명 생성 284
 - 코어 설치 85
- 기능 28
- 기본 DN
 - 복수 SUL 용 사용 152
 - 사용자 설정 도메인 기본 DN 지정 151
 - 사용자 설정 도메인 지정 151
 - 설명 64, 149
- 기본 도메인 제어기 .PDC 참조
- 기본값
 - 3DES 키로 암호화 280
 - base64 암호화 값 302
 - certutil 위치 291
 - LDAP 포트 104
 - Require trusted SSL certificate 설정 120
 - Resync 간격 113
 - Solaris 용 설치 디렉토리 232
 - SSL 포트 86
 - SUL 이름 150
 - syslog 메시지 270
 - 경로 및 파일 이름 20
 - 구성 디렉토리 포트 86
 - 동기화 흐름 131
 - 로그 기록 270
 - 로그 디렉토리 269
 - 로그 유지 266
 - 로그 표시 수준 267
 - 루트 접미어 105, 302
 - 매개변수화 값 생성 63, 128
 - 명령줄 유틸리티 인수 181
 - 브로커 포트 91
 - 비밀번호 정책 65
 - 인스턴스 디렉토리 329
 - 인증서 데이터베이스 경로 20
 - 자체 서명 인증서 291
 - 재동기화 소스 179
 - 표시할 감사 / 오류 메시지 줄 수 274
- 기술 지원 22
- 기호 규약 19
- 내보내기
 - 1.0 구성 188
 - Directory Server 인증서 293
 - 버전 1.0 구성 파일 188

내장 계정 322
 다른 업체 웹사이트 23
 다운로드
 Identity Synchronization for Windows 번들 54
 Sun 제품 22
 설치 프로그램 82
 제품 바이너리 83, 84
 패치 53
 단일 호스트
 구현 197
 단일 호스트 구현 55
 대표키, 사용 20
 데몬
 로그 기록 270
 설명 346
 시작 / 정지 183
 재시작 252
 데이터베이스
 Retro-Changelog 110, 113
 객체 캐시 40
 색인 생성 112
 인증서 20, 109, 279, 291, 292, 293, 295, 296, 307, 345
 도메인
 Active Directory 113, 115, 332, 333
 NT 용으로 지정 122
 접침 해결 154
 복수 333
 복수 구성 331-336
 사용자 설정 151
 도메인 접침 해결 154
 도메인 제어기
 Active Directory 118, 119, 244
 매개변수 편집 121
 복구 262
 복수 사용 118
 장애 조치 119
 지정 117
 편집 121, 123
 도움말
 도움말 파일 제거 209
 사용 정보 305

동기화
 Active Directory 65
 Directory Server 플러그인으로 변경 186
 idsync resync 사용 76, 307
 idsync startsync 사용 76, 307
 idsync stopsync 사용 76, 307
 NT SAM 38
 구성 131
 구성요소를 사용할 수 없는 경우 45
 기본값 131
 기존 사용자 59
 문제 해결 243
 복수 도메인 154
 비밀번호 46, 65, 65-72, 108
 사용자 175-182
 사용자 목록 필터링 154
 사용자 생성 내용 47
 사용자 항목 속성 74, 125
 삭제 147
 설정 48, 61, 244
 속성 108, 125
 시작 318
 시작 / 정지 76, 182, 183, 307
 양방향 33
 요구 사항 46
 이벤트 메시지 266
 재시작 182, 196
 정지 319
 활성화 / 비활성화 139, 139-146
 동기화 사용자 목록 .SUL 참조
 동일성
 색인 110, 313
 필터 152
 디렉토리
 Active Directory 60
 certutil 기본 20
 clogger 100 (중앙 기록기) 266
 etc 206
 installer 83
 instance 20, 329
 isw-12004Q3 83
 isw12004Q3 84
 isw-hostname 20, 204, 205, 207, 213, 232, 235

- persist 65, 206
- samples1 323
- server_root 20
- TEMP 164, 234, 252
- 구성 30, 74, 75, 91
- 기본 경로 및 파일 이름 20
- 기본 인스턴스 329
- 기술 / 설명 60
- 레이블 사용 59
- 로그 242, 250, 269
- 로컬 로그 20
- 메시지 257
- 별칭 291, 293
- 사전 입력 316
- 상위 20
- 새로 만들기 83, 84
- 설치 84, 90, 158
- 설치 지정 89
- 소스 재동기화 177
- 영구 메시지 저장 257
- 이름 지정 제한 74
- 이전 . 188, 194, 196, 321
- 인증서 데이터베이스 296, 297
- 중앙 로그 265
- 중앙 로그 기본 20
- 중앙화된 로그 포함 265
- 커넥터와 연결 59
- 쿼리 103
- 디렉토리 사전 입력 316
- 디렉토리 소스
 - Active Directory 161
 - 만들기 66, 101–124
 - 사용자 연결 178
 - 삭제 124
 - 상태 272
 - 상태 보기 271
 - 예제 항목 161
 - 추가 101, 113, 124
- 디스크 공간 요구 사항 53
- 레이블 이름 지정 형식 59
- 레지스트리
 - NT SAM 41
- 편집 215
- 로그
 - audit.log 244, 246, 253, 265
 - Directory Server 플러그인 267
 - error.log 242
 - resync 265
 - resync.log 182
 - 감사 32, 265
 - 구성 269
 - 기본 경로 및 파일 이름 20
 - 로컬 266
 - 로컬 구성요소 로그 266
 - 로컬 하위 구성요소 로그 266
 - 보기 164, 168, 170, 173, 263, 273
 - 브로커 255
 - 사용 244, 253
 - 오류 32, 265, 274
 - 위치 265, 274
 - 읽기 268
 - 포맷 268
- 로그 디렉토리 242, 250, 265, 269
- 로그 읽기 268
- 로그인 83, 84, 93
- 로깅
 - audit.log 사용 244
 - Message Queue 브로커 문제 해결 255
 - resync.log 확인 182
 - 감사 로그 사용 244, 253
 - 감사 / 오류 파일 263–275
 - 구성 269
 - 기본 로그 디렉토리 / 파일 지정 269
 - 로그 보기 164, 168, 170, 173
 - 로그 수준 지정 268
 - 로그 종류 265
 - 오류 242, 264
 - 일상 작업 264
 - 적절히 연결된 사용자 182
 - 중앙 로그 265
 - 커넥터 상태 247
- 로컬 로그 266
 - 구성요소 266
 - 로컬 디렉토리 20

- 중앙 기록기 266
- 루트 접미어
 - default 105
 - 디렉토리 소스 레이블 59
 - 설명 74
 - 지정 87
- 마이크레이션
 - 버전 1.0 에서 1 2004Q3 으로 185-229
- 만들기
 - Active Directory 디렉토리 소스 113
 - Active Directory 소스 101, 113
 - NT Registry 디렉토리 소스 101
 - NT SAM 디렉토리 소스 122
 - PIN 파일 292
 - Retro-Changelog 데이터베이스 110
 - SUL 64, 66, 148-154
 - Sun Java System 디렉토리 소스 101, 102
 - Windows 2003 Server 디렉토리 소스 66
 - Windows 2003 Server 전역 카탈로그 66
 - Windows NT 디렉토리 소스 122
 - XML 구성 문서 187
 - 계정 68, 162, 329
 - 디렉토리 소스 101-124
 - 매개변수화 기본 속성 값 63
 - 새 디렉토리 83
 - 인증서 데이터베이스 291
- 매핑
 - 생성 속성 135
 - 속성 63, 125, 134, 136
 - 커넥터 ID 를 디렉토리 소스로 296, 297
- 메시지
 - audit.log 265, 266
 - debug.log 265
 - error.log 265, 266
 - resync.log 265
 - 구성요소용 265
 - 동기화 이벤트 266
 - 예 246, 247
 - 중앙 기록기에 제공 265
 - 커넥터 상태 보고 247
- 메시지 디렉토리 257
- 명령
 - idsync resync 243
 - imq start 184
 - imq stop 184
 - isw start 183
 - isw stop 183
 - Message Queue 브로커 확인 254
 - netstat -n -a 253
 - telnet 254
 - useradd 329
 - 목록 프로세스 249
 - 새 디렉토리 만들기 83, 84
 - 설명 76
 - 수신 커넥터 확인 253
 - 제품 바이너리 압축 해제 83, 84
 - 프로세스 재시작 250
- 명령줄 유틸리티
 - idsync resync 177
 - 공통 기능 302
 - 공통 인수 302
 - 비밀번호 입력 305
 - 사용 76, 301-322
 - 설명 31, 76, 301-322
- 목록
 - 사용중 서비스 254
 - 활성 Message Queue 서비스 254
- 문제 해결
 - Directory Server 플러그인 243, 244, 250, 253, 262
 - error.log 248
 - Identity Synchronization for Windows 241-262
 - Message Queue 254
 - Solaris 구성요소 249
 - SSL 257
 - WatchList.properties 252
 - Windows NT 하위 구성요소 253
 - Windows 구성요소 251
 - 계정 243
 - 구성 요소 249
 - 브로커 254, 256
 - 점검 목록 242, 252
 - 제어기 262
 - 중앙 기록기 266
 - 커넥터 245, 246, 247, 248
 - 코어 242, 258

- 통신 문제 248
- 하위 구성요소 252
- 버전 요구 사항 51
- 변경
 - 구성 비밀번호 76, 307
 - 기본 스키마 소스 128
- 변경 검출 33, 34, 39–42, 45, 106, 244, 249
- 변경 검출기 하위 구성요소 34, 38, 41, 59, 205, 206, 219, 226, 253, 321
- 변경 내용, 흐름 지정 137–146
- 별칭 디렉토리 291, 293
- 별칭, 인증서 285
- 보안 강화 283
- 보안 통신 109
- 보조 objectclass
 - 구성 62
 - 선택 129, 130
 - 설명 344
 - 제거 130
- 보호
 - 비밀번호 284
 - 전역 카탈로그 280
 - 중요한 정보 280
- 복구
 - 도메인 제어기 262
 - 디렉토리 206
- 복수 도메인 331–336
- 복수 도메인 제어기 118
- 복수 호스트 구현 225, 226
- 복제
 - SSL 경유 340
 - 구성 286, 338
 - 단일 접미어 337
 - 사용자 동기화 337
- 브로커
 - Message Queue 35
 - 로그 255
 - 문제 해결 254, 256
 - 설명 352
 - 시작 184
 - 엑세스 285
- 재시작 256, 257
- 정지 184
- 포트 지정 91
- 비밀번호
 - Directory Server 플러그인으로 변경 내용 동기화 186
 - 계정 생성 68
 - 구성 278
 - 구성 변경 308
 - 동기화 65–72
 - 만들기 131, 136, 137
 - 명령줄 유틸리티용으로 입력 305
 - 변경 내용 전달 42–44, 73
 - 변경 집행 196
 - 변경 필요 321
 - 보호 284
 - 암호화 39
 - 요청시 비밀번호 동기화 42, 46, 177, 244, 258, 262
 - 인수 305
 - 일반 텍스트, 삽입 189
 - 찾기 309
 - 해시 39
- 비밀번호 동기화, 요청시 39, 43, 44, 177, 186, 244, 258, 262
- 비밀번호 변경 집행 196
- 비밀번호 변경 필요 321
- 비밀번호 정책
 - Active Directory 67
 - Directory Server 67
 - 구성 비밀번호용 284
 - 기본 Windows 65
 - 동기화에 미치는 영향 69
 - 예 71
 - 집행 66
- 비밀번호 정책 집행 66
- 비밀번호 필터 하위 구성요소 34, 38, 41, 42, 59, 226, 253, 321
- 비활성화 138–146
- 사용
 - checktopics 유틸리티 194
 - Directory Server 용 사용자 정의 방법 140, 142
 - SSL 279, 290, 297

- SSL 통신 87, 107, 109, 159, 290, 292
- 작성 흐름 249
- 사용 정보, idsync 305
- 사용자
 - Active Directory 로 추가 68
 - Active Directory 에 특수 182
 - NT SAM 도메인 177
 - SUL 생성 64
 - 고유한 이름 114
 - 도메인 기본 DN, 지정 151
 - 링크 / 동기화 47, 59, 74, 76, 78, 125, 149, 175-182, 307
 - 삭제 147
 - 속성 63
 - 인증 실패 44
 - 재동기화 177, 316
 - 정의 64
 - 필터 152, 332
 - 하위 트리 47
- 사용자 DN
 - 예 104, 114
 - 지정 104, 114
- 사용자 objectclass 74
- 사용자 설정 도메인 151
- 사용자 연결 149, 175-182
 - idsync resync 사용 76, 307
 - XML 구성 문서 사용 317
- 사용자 유형 식별 149
- 사용자 정의 방법 140, 142
- 삭제
 - SUL 124
 - 객체 148
 - 동기화 147
 - 디렉토리 소스 124
 - 생성 속성 137
 - 속성 값 137
 - 흐름 지정 147
- 상위 디렉토리 20
- 상태
 - 디렉토리 소스 272
 - 커넥터 247
- 상태 표시줄 99
- 상호 운영
 - Directory Server 도구 140
- 색인
 - 동일성 생성 110
 - 만들기 112
 - 추가 313, 314
- 색인 생성 112
- 색인화된 속성 182
- 생성 내용 흐름 지정 131
- 생성 속성
 - 만들기 132
 - 매개변수화 기본값 63
 - 매핑 135
 - 삭제 132, 137
 - 설명 62
 - 지정 134
 - 편집 132, 136
 - 필수 125, 127
- 서버
 - 관리 36, 84, 85, 87, 93
 - 사용자 유형 식별 149
 - 사용자 유형 연결 149
 - 찾기 97
 - 최소 RAM 53
 - 페일오버 120
 - 호스트이름 97
- 서버 루트 디렉토리 20
- 서버 콘솔 351
- 서비스
 - Identity Synchronization for Windows 251
 - iMQ Broker 255
 - Message Queue 254
 - 동기화 183
 - 사용중 목록 254
 - 시작 / 정지 99, 183, 252
 - 재시작 330
 - 중앙 기록기 251
- 설명서
 - 개요 20
 - 권장 내용 21

설치

Active Directory 커넥터 37, 166
 Directory Server 53
 Directory Server 커넥터 36
 Directory Server 플러그인 36, 157-174
 Identity Synchronization for Windows 89, 204
 Message Queue 54
 To Do 목록 56, 91
 Windows NT 커넥터 및 하위 구성요소 38

결정 73

권한 55

디렉토리 83, 84, 158

디렉토리 지정 89, 90

디렉토리, 기본 232

디렉토리, 설명 90

로그 보기 164, 168, 170, 173

상태 보기 272

인증서 285

재시작 158

점검 목록 77, 79

준비 51-79

커넥터 155, 157-174

코어 36, 73, 85-94

코어 구성 요소 85

프로그램 다운로드 82

필수 유틸리티 51

필수 패치 51

필요한 운영 체제 버전 51

필요한 자격 증명 / 권한 54, 55

하위 구성요소 155

설치 계획 27, 55

설치 프로그램

Directory Server 158

Identity Synchronization for Windows 17, 81

위치 확인 158

소스

Active Directory 생성 113

NT SAM 디렉토리 생성 122

Sun Java System 디렉토리 생성 102

소프트웨어 요구 사항 53

속성

AvoidPdcOnWan 118

dspswuserlink 178, 313

dspswvalidate 43

inetorgperson 63

nsAccountLock 140, 141

objectguid 178

PwdLastSet 43

uid 179

USNchanged 40, 43

매개변수화 기본값 생성 63

매핑 63, 125, 134

사용자 63

사용자 항목 동기화 74, 125

색인화 182

생성 62

선택 61, 125, 130

설명 62

유형 62

이름 지정 149

재동기화 177

중요 62

편집 136

필수 생성 62, 127

확인 243, 249

속성 수정 내용 흐름 138

스크립트

idsync 76, 306

idsync resync 178

스키마

기본 소스 변경 128

서버 74

업데이트 204

제어기 75

시스템

감사 28

비밀번호 작성 흐름 131, 136, 137

안정 상태 확인 194

요구 사항 51

패치 51

시스템 관리자

java.exe 프로세스 250, 251

WatchList 기본 설정 항목 251

설명 32

인증서 승인 286

시스템 구성요소

배포 36-38

설명 29

시스템 구성요소 배포 36-38

시작

Message Queue 브로커 184

net start 206

데몬 183

동기화 76, 182, 318

서비스 99, 183, 206

콘솔 92, 93, 97

신뢰도 45

신뢰된 인증서 120, 279

실패

제거 206

제거 프로그램 76, 307

하드웨어 76, 307

실행

certutil 259, 294

idsync resync 스크립트 178

java.exe 프로세스 250

Watchdog 프로세스 250

디스크 공간 부족 270

실행 파일

java.exe 251

pswatchdog 251

setup.exe 84, 158

안전 모드 179

암호화

3DES 키 280

Message Queue 메시지 280, 281

구성 정보 87, 88

네트워크 트래픽 279

일반 텍스트 비밀번호 39

채널 통신 108

액세스 권한 117, 281, 286, 311

액세스 제한 286

양방향 동기화 28, 33

업데이트

스키마 204

창 271

업데이트, 검출 39-42

역할 소유자, 기본 도메인 제어기 FSMO 118

영구 메시지 저장 257

영구 저장 장소 보호 282

예

checktopics 명령 195

export10cnf 명령 189

forcepwchg 명령 321

idsync certinfo 명령 308

idsync changepw 명령 308

idsync importcnf 189, 205

idsync importcnf 명령 310

idsync prepds 명령 312

idsync printstat 명령 315

idsync resetconn 명령 315

idsync resync 명령 317

idsync startsync 명령 319

idsync stopsync 명령 319

prepds 하위 명령 312

resync 인수 181

감사 로그 경로 274

디렉토리 소스 항목 161

로그 메시지 246, 268

비밀번호 정책 71

사용자 설정 도메인 기본 DN 151

중앙 로그 265

예제

LDAP URL 348

linkusers.cfg 325

linkusers-simple.cfg 324

XML 구성 문서 323

오류

XML 구성 파일 205

검출 205

유효성 검사 155

오류 검출 32

온라인 리소스 22

온라인 지원 22

요구 사항

RAM 53

Solaris 52

Windows 52

- 동기화 46
- 소프트웨어 53
- 운영 체제 51, 52
- 운영 체제 버전 51
- 코어 52
- 하드웨어 53
- 요청시 비밀번호 동기화 39, 42, 43, 44, 46, 177, 244, 258, 262
- 인증 메커니즘 44
- 용어집 343
- 운영 체제 요구 사항 51, 52
- 웹사이트
 - Directory Server 출판물 16, 21, 72, 204
 - Identity Synchronization for Windows 출판물 21
 - Java Development Kit 다운로드 81
 - Message Queue 출판물 21
 - Microsoft 인증 기관 23, 73
 - Microsoft 제품 설명서 23, 72, 73
 - Sun 리소스 22
 - Sun 제품 설명서 15, 53
 - 다른 업체 23
 - 의견 및 제안 23
 - 지원 22
- 유틸리티
 - checktopics 187, 194
 - checktopics 사용 194
 - export10cnf 187, 188
 - forcepwchg 187, 321
 - keytool 285
 - 명령줄 31
 - 필요한 운영 체제 51
- 유효성 검사
 - 구성 155
 - 유효성 검사 오류 155
 - 인증서 285, 286
- 의견 및 제안 23
- 이름 지정 속성
 - 설명 149
- 이전 .
 - 1.0 구성 내보내기 188
 - checktopics 사용 194
 - directory 188, 194, 196, 321
 - forcepwchg 사용 321
 - 도구 200
 - 메시지 비우기 196
 - 버전 1.0 에서 1 2004Q3 으로 65
 - 비밀번호 변경 집행 196
 - 시나리오 222, 223
 - 전달되지 않은 메시지 확인 194
 - 준비 199
- 이진 파일
 - 다운로드 83, 84
 - 압축해제 83, 84, 200
 - 제거 209
- 인수
 - certinfo 289
 - changepw 하위 명령 308
 - checktopics 195
 - forcepwchg 321
 - importcnf 205, 304
 - prepds 312
 - printstat 314
 - resetconn 316
 - resync 179, 181, 317, 318
 - stopsync 319
 - 명령줄 유틸리티 302
 - 비밀번호 305
- 인스턴스 디렉토리, 기본 20, 329
- 인스턴스, 1.0 제거 218
- 인증
 - 구성 디렉토리로 연결 304
 - 설명 344
 - 실패 44
 - 요청시 비밀번호 동기화 44
 - 인증서 344
 - 클라이언트 321
- 인증서
 - Active Directory 119, 244, 259, 262, 293–297
 - CA 279, 286
 - certinfo 하위 명령 307
 - certinfo 하위 명령 사용 76, 306
 - certutil 사용 294
 - Directory Server 293
 - idsync certinfo 사용 289
 - PIN 파일 생성 292

- SSL 120, 279, 286
- 가져오기 296
- 내보내기 293
- 별칭 285
- 불러오기 293, 294
- 설치 285
- 승인 286
- 요구 120, 279, 289
- 유효성 검사 285, 286
- 인증 344
- 자체 서명 285, 290, 291
- 정보 가져오기 76, 306
- 정보 보기 307
- 추가 295, 296, 297
- 인증서 데이터베이스
 - 기본 경로 20
 - 디렉토리 296, 297
 - 만들기 291
 - 위치 지정 304
 - 인증서 불러오기 293
 - 인증서 추가 295, 297
 - 필요한 인증서 289
- 인증서 불러오기
 - certutil 사용 294
 - LDAP 사용 294
- 일반 텍스트 비밀번호
 - 가져오기 42
 - 비밀번호 필터 DLL 사용 42
 - 삽입 189
 - 전달 42
 - 캡처 39
- 자격 증명 / 권한 87
 - Directory Server 282
 - Directory Server 구성 75
 - idsync prepsd에 필요 311
 - 관리자 74
 - 구성 디렉토리 284
 - 구성 디렉토리용으로 지정 87
 - 설치용으로 필요 54
 - 연결용으로 필요 282
 - 자격 증명 생성 284
 - 지정 116
 - 코어 설치 85
- 자원
 - 온라인 22
 - 찾기 97
- 자체 서명 인증서 285, 290, 291
- 작성
 - syslog 데몬에 기록 270
 - 파일로 기록 269
- 작성 표현식 64, 152
- 작성 흐름
 - 구성 계획 74
 - 사용 46
 - 지정 131, 136, 137
 - 확인 249
- 재동기화
 - 디렉토리 소스 177
 - 사용자 76, 307, 316
 - 속성 177
- 재설정
 - 카운터 262
 - 커넥터 상태 76, 307, 315
- 재시작
 - Directory Server 202
 - java 프로세스 30
 - 데몬 252
 - 동기화 182, 196
 - 브로커 256, 257
 - 서비스 252, 330
 - 설치 프로그램 158
 - 커넥터 33
- 저장
 - SUL 154
 - 구성 정보 75, 159
- 전달
 - 비밀번호 변경 42-44, 73, 138
 - 사용자 삭제 147
 - 새 비밀번호 132
- 전역 동기화 설정 48
- 전역 카탈로그 61, 75
 - Active Directory 113
 - 만들기 66
 - 보호 280

- 복수 113
- 설명 61, 347
- 용도 75
- 지정 114, 115
- 전제 조건
 - checktopics 유틸리티 195
 - 권장 내용 16
- 점검 목록 91
 - 문제 해결 242, 252
 - 설치 77, 79
- 접두어 105
- 접미어
 - 구성 105
 - 복제 337
- 접미어 / 데이터베이스 59, 60
- 정보 패널 56, 91, 99, 165, 272, 273
- 정의
 - SUL 331-336
 - 복수 도메인 331-336
 - 사용자 64
- 정지
 - java 프로세스 213
 - Message Queue 214
 - Message Queue 브로커 184
 - net stop 205
 - 데몬 183
 - 동기화 76, 182, 319
 - 서비스 99, 183, 205
- 제거
 - 1.0 인스턴스 218
 - Directory Server 플러그인 202, 209, 214, 231, 233
 - Identity Synchronization for Windows 202, 231
 - Solaris 패키지 208
 - 도움말 파일 209
 - 디렉토리 소스 124
 - 보조 objectclass 130
 - 생성 속성 137
 - 소프트웨어 82, 231
 - 속성 값 137
 - 이진 파일 209
 - 커넥터 203, 234
 - 코어 203, 207, 213, 231, 236
 - 콘솔 238, 239
 - 콘솔 jar 파일 212, 217
 - 패키지 209
 - 제거 오류 76, 206, 307
 - 제안 및 의견 23
 - 제어기
 - 문제 해결 262
 - 제품 다운로드 22
 - 제품 이진 파일
 - 다운로드 83, 84
 - 압축해제 83, 84
 - 제품 이진 파일 압축 해제 83, 84, 200
 - 제품 지원 22
 - 존재
 - 색인 313
 - 필터 152
 - 중속 제품 업그레이드 204
 - 준비
 - Directory Server 58, 109, 310
 - 마이그레이션 199
 - 설치 51-79
 - 중앙 기록기
 - clogger 100 디렉토리 266
 - Identity Synchronization for Windows 확인 251
 - Java 프로세스 클래스 이름 250
 - WatchList.properties 251
 - 로컬 로그 266
 - 메시지 265
 - 문제 해결 266
 - 설명 32
 - 용도 246
 - 중앙 로그 디렉토리 20, 265
 - 중앙화
 - 로그 265, 344
 - 시스템 감사 28
 - 중요 속성
 - 매개변수화 기본값 생성 63
 - 설명 62
 - 중요한 정보 보호 282
 - 지원, 제품 22
 - 지정

- Active Directory 도메인 115
- Directory Server 106
- Java Home 89
- Resync 간격 121
- Windows NT 도메인 이름 122
- 객체 삭제 흐름 147
- 객체 수정 내용 흐름 137-146
- 객체 작성 흐름 131
- 구성 디렉토리 자격 증명 87
- 구성 디렉토리 호스트 / 포트 86
- 구성 비밀번호 278
- 도메인 제어기 117
- 동기화 설정 244
- 루트 접미어 87
- 사용자 DN 104, 114
- 사용자 설정 도메인 기본 DN 151
- 설치 디렉토리 89
- 속성 61, 130
- 자격 증명 116
- 작성 흐름 131, 136, 137
- 전역 카탈로그 114, 115
- 페일오버 서버 120
- 페일오버 제어기 119
- 포트 번호 91
- 호스트 114
- 채널 통신, 암호화 108
- 추가
 - SUL 149
 - XML 파일을 내보내기 위한 비밀번호 200
 - 관리자 그룹에 자격 증명 284
 - 구성 데이터를 Directory Server 로 91
 - 디렉토리 소스 101, 113, 124
 - 사용자를 Active Directory 로 68
 - 색인 313, 314
 - 속성 값 136
 - 인증서 295, 296, 297, 307
- 출판물
 - Microsoft 21
 - 관련 21
- 카운터, 재설정 262
- 카탈로그, 전역
 - 보호 280
 - 복수 113
 - 설명 61, 347
 - 용도 75
 - 지정 114, 115
- 커넥터
 - Active Directory 157
 - Directory Server 160
 - idsync printstat 사용 76, 307
 - Watchdog 프로세스 30
 - Windows NT 170
 - 구성 253
 - 디렉토리 연결 59
 - 문제 해결 245, 246, 266
 - 배포 157
 - 변경 검출 39, 40, 41
 - 상태 76, 247, 307, 315
 - 상태 인쇄 76, 307, 314
 - 설명 33
 - 설치 36, 37, 38, 155, 157-174
 - 시작 / 모니터 30
 - 양방향 동기화 33
 - 재시작 33
 - 제거 203, 234
- 커넥터 모니터 30
- 커넥터 상태 인쇄 314
- 커넥터 시작 30
- 커넥터 연결 59
- 코어
 - SSL 사용 159
 - Watchdog 30
 - 구성 17, 74, 77, 95-156
 - 구성 요소 29, 57, 344, 352, 353
 - 문제 해결 242, 258
 - 설명 30, 346
 - 설치 36, 73, 77, 85-94
 - 설치 권한 85
 - 요구 사항 52
 - 점검 목록 77
 - 제거 203, 207, 213, 231, 236
- 콘솔
 - Directory Server 140, 251

- Identity Synchronization for Windows 31, 98, 271, 272, 273
- jar 파일 제거 212, 217
- MMR 구성 223
- Sun Java System 콘솔 97
- 구성 디렉토리로 읽기 / 쓰기 30
- 도움말 파일 209
- 동기화 시작 / 정지 183, 248
- 동기화 확인 248
- 로그 보기 263
- 로그인 93
- 복수 호스트 구현 226
- 비밀번호 88
- 사용자 유형 식별 / 연결 149
- 상태 표시줄 99
- 서버 콘솔 351
- 설명 31, 57, 99
- 설치 89
- 시작 92, 93, 97
- 제거 238
- 코어 구성 95-156
- 쿼리
 - LDAP 사용 348
 - 구성 디렉토리 103, 105
- 클라이언트, 인증 321
- 탭
 - Configuration 99
 - Tasks 99
 - 상태 99
- 통신
 - SSL 사용 107, 109
 - 마지막 통신 272
 - 문제 해결 248
- 패치
 - 설치용으로 필요 53
 - 정보 22
 - 필수 51
- 패키지
 - SUNWidsem 209
 - SUNWidsen 209
 - SUNWidscr 209
 - SUNWidsct 209
 - SUNWidsoc 209
 - SUNWjss 82, 202
 - SUNWtlsu 259
- 제거 209
- 파일오버 제어기, 지정 119
- 편집
 - 도메인 제어기 121, 123
 - 도메인 제어기 구성 매개변수 121
 - 매핑된 속성 136
 - 생성 속성 136
 - 제품 레지스트리 파일 215
- 포트 번호
 - Message Queue 지정 90, 91
 - 구성 디렉토리 179, 317
 - 기본값 86, 91
 - 확인 255
- 표기 형식
 - 기본 경로 및 파일 이름 20
 - 기호 19
 - 대표키 20
 - 레이블 이름 지정 59
 - 활자체 19
- 프로그램
 - setup 158
 - 제거 82
- 프로세스
 - Watchdog 30, 251
 - 경량 33
 - 구성 디렉토리 30
 - 명령줄 유틸리티 31
 - 시스템 관리자 32
 - 정지 213
 - 중앙 기록기 32
 - 커넥터 33
 - 콘솔 31
- 플랫폼
 - Identity Synchronization for Windows 구현 122
 - 요구 사항 51
- 필수 생성 속성 62, 125, 127
- 필터
 - LDAP 64, 79, 304, 317
 - SUL 64, 75, 149
 - synchronization user lists 154

- 검색 294
- 구문 152, 332
- 구성 334
- 동일성 152
- 문제 해결 244
- 사용자 목록 152, 332
- 설명 64, 149
- 존재 152
- 하위 문자열 152
- 하드웨어 오류 76, 307
- 하드웨어 요구 사항 53
- 하위 구성요소
 - Windows NT 34, 244, 253
 - Windows NT SAM 변경 감지기 253
 - 문제 해결 252
 - 변경 감지기 253
 - 비밀번호 필터 253
 - 설명 33
 - 설치 155
- 하위 명령
 - certinfo 289, 307
 - changepw 사용 308
 - idsync 301–322
 - importcnf 77, 188, 189, 205, 304, 307, 310
 - importcnf 사용 310
 - printstat 314
 - resetconn 315
 - resync 316, 318, 323
 - startsync 318
 - stopsync 319
 - 설명 76, 306
- 하위 문자열 필터 152
- 하위 트리, 사용자 47
- 해시된 비밀번호 39
- 호스트
 - Active Directory 114, 116, 223, 226, 244
 - 구현 시나리오 225
 - 지정 114
- 호스트이름
 - Localhost 91
 - 구성 디렉토리 179, 317
 - 서버 그룹 97
- 확인
 - 빈 동기화 주제 194
 - 속성 243, 249
 - 시스템 안정 상태 194
 - 작성 흐름 249
 - 포트 번호 255
- 활성화 138–146
- 활자체 규약 19
- 흐름
 - 기본값 131
 - 삭제 지정 147
 - 생성용으로 지정 131
 - 수정 내용 지정 137–146