



Informatica®
10.5.3

PowerCenter 및 Data Quality 설치

Informatica PowerCenter 및 Data Quality 설치

10.5.3

2022년 11월

© 저작권 Informatica LLC 1998, 2022

이 소프트웨어와 설명서는 사용 및 공개에 대한 제한 사항이 포함되어 있는 별도의 사용권 계약에 따라 제공됩니다. 본 문서의 어떤 부분도 Informatica LLC의 사전 통지 없이 어떠한 형태나 수단(전자적, 사진 복사, 녹음 등)으로 복제되거나 전송될 수 없습니다.

Informatica, Informatica 로고, PowerCenter 및 PowerExchange는 미국과 전 세계 여러 관할 국가에서 Informatica LLC의 상표 또는 등록 상표입니다. Informatica 상표의 현재 목록은 <https://www.informatica.com/trademarks.html> 웹에서 확인할 수 있습니다. 다른 회사 및 제품명은 해당 소유자의 상표 또는 등록 상표일 수 있습니다.

수신 거부 권한에 따라 소프트웨어는 소프트웨어가 배포된 컴퓨팅 및 네트워크 환경 그리고 배포의 데이터 사용 및 시스템 통계에 대한 정보를 미국 내 Informatica에 자동으로 전송합니다. 이 전송은 Informatica 개인 정보 보호 정책에 의거하여 서비스의 일부로 간주되며 Informatica는 <https://www.informatica.com/in/privacy-policy.html>에서 제공되는 Informatica 개인 정보 보호 정책에 따라 이 정보를 사용하고 처리합니다. Administrator 도구에서 사용자량 수집을 비활성화할 수 있습니다.

미국 정부 권한. 미국 정부 고객에게 제공되는 프로그램, 소프트웨어, 데이터베이스, 관련 문서 및 기술 데이터는 해당하는 연방 입수 규정 및 기관별 보안 규정에 따라 "상용 컴퓨터 소프트웨어" 또는 "상용 기술 데이터"입니다. 따라서 사용, 복제, 공개, 수정 및 조정은 해당하는 정부 계약에 규정된 제한 사항 및 라이선스 조건을 따르며, 정부 계약 조건에 의해 적용 가능한 한도 내에서, FAR 52.227-19, 상용 소프트웨어 라이선스에 규정된 추가 권한이 적용됩니다.

이 제품에는 Douglas C. Schmidt와 Washington University, University of California, Irvine, Vanderbilt University의 연구팀(저작권 ((c) 1993-2006, 모든 권리 보유.)이 저작권을 소유한 ACE(TM) 및 TAO(TM) 소프트웨어가 포함되어 있습니다.

이 제품에는 Curl 소프트웨어(저작권 1996-2013, Daniel Stenberg, <daniel@haxx.se>. 모든 권리 보유.)가 포함되어 있습니다. 이 소프트웨어와 관련된 사용 권한 및 제한 사항은 <http://curl.haxx.se/docs/copyright.html>에 명시된 조항에 따라 변경될 수 있습니다. 위와 같은 저작권 고지 및 이러한 허가 고지가 모든 제품에 표시되어 있는 경우 목적 및 사용료 유무에 관계없이 이 소프트웨어를 사용, 복사, 수정 및 배포할 수 있는 사용 권한이 부여됩니다.

이 제품에는 International Business Machines Corporation 등(저작권 International Business Machines Corporation and others. 모든 권리 보유.)이 저작권을 소유한 ICU 소프트웨어가 포함되어 있습니다. 이 소프트웨어와 관련된 사용 권한 및 제한은 <http://source.icu-project.org/repos/icu/icu/trunk/license.html>의 조항에 따라 변경될 수 있습니다.

이 제품에는 OSSP UUID 소프트웨어(저작권 (c) 2002 Ralf S. Engelschall, 저작권 (c) 2002 The OSSP Project 저작권 (c) 2002 Cable & Wireless Deutschland)가 포함되어 있습니다. 이 소프트웨어와 관련된 사용 권한 및 제한은 <http://www.opensource.org/licenses/mit-license.php>의 조항에 따라 변경될 수 있습니다.

이 소프트웨어 및 설명서의 정보는 Informatica LLC 소유이고 사용 및 공개 제한 사항을 포함한 라이선스 계약서에 따라 제공되며 저작권법의 보호를 받습니다. 소프트웨어의 리버스 엔지니어링은 금지되어 있습니다. 본 문서의 어떤 부분도 Informatica LLC의 사전 통지 없이 어떠한 형태나 수단(전자적, 사진 복사, 녹음 등)으로 복제되거나 전송될 수 없습니다. 이 소프트웨어는 미국 및/또는 국제 특허법의 보호를 받으며, 기타 특허 출원 중입니다.

<https://www.informatica.com/legal/patents.html>에서 특허를 참조하십시오.

이 설명서의 정보는 예고 없이 변경될 수 있습니다. 이 문서에서 문제가 발견되는 경우 infa_documentation@informatica.com으로 보고해 주십시오.

Informatica 제품은 제품이 제공될 당시의 계약 조건에 따라 보증됩니다. Informatica는 상품성과 특정 목적에의 적합성에 대한 보증 그리고 비침해에 대한 보증 또는 조건을 포함하여 어떠한 종류의 명시적이거나 묵시적인 보증 없이 이 문서의 정보를 "있는 그대로" 제공합니다.

이 소프트웨어 및/또는 설명서의 일부에는 타사의 저작권이 적용될 수 있습니다. 필요한 타사 고지 사항은 제품에 포함되어 있습니다.

발행 날짜: 2022-12-21

목차

서문	13
Informatica 리소스	13
Informatica Network	13
Informatica 기술 자료	13
Informatica 설명서	13
Informatica Product Availability Matrix	14
Informatica Velocity	14
Informatica Marketplace	14
Informatica 글로벌 고객 지원 센터	14
파트 I: 설치 시작	15
장 1: 설치 시작	16
시작을 위한 검사 목록	16
설치 개요	16
설치 프로세스	17
설치 옵션 계획	17
설치 구성 요소 계획	19
노드	19
서비스 관리자	20
응용 프로그램 서비스	20
데이터베이스	20
사용자 인증	21
보안 데이터 저장소	21
도메인 보안	21
Informatica 클라이언트 도구	22
파트 II: 서비스를 설치하기 전에	23
장 2: UNIX에 서비스를 설치하기 전에 (또는 Linux)	24
Before You Begin Checklist	24
릴리스 노트 읽기	25
시스템 요구 사항 확인	25
임시 디스크 공간 및 사용 권한 확인	25
UNIX 또는 Linux에서 패키지 요구 사항 검토	26
포트 요구 사항 확인	27
Verify Distribution Package Requirements (Linux and UNIX)	29
파일 설명자 제한 확인	29
응용 프로그램 서비스 하드웨어 요구 사항 확인	30
Data Transformation 파일 백업	31

POSIX 비동기 I/O 구성.	32
환경 변수 검토.	32
시스템 사용자 계정 작성.	33
키 저장소 파일 설정.	33
Download and Extract the Installer Files.	35
Verify Installer Code Signing.	35
Verify Installer Package Checksum on UNIX and Linux.	36
라이선스 키 확인.	36
장 3: Windows에 서비스를 설치하기 전에.	37
Windows에서 서비스를 설치하기 전에 개요.	37
릴리스 노트 읽기.	37
시스템 요구 사항 확인.	38
임시 디스크 공간 및 사용 권한 확인.	38
패치 요구 사항 검토.	38
포트 요구 사항 확인.	39
Verify Distribution Package Requirements (Windows).	40
응용 프로그램 서비스 하드웨어 요구 사항 확인.	40
Data Transformation 파일 백업.	42
환경 변수 검토.	42
시스템 사용자 계정 작성.	43
키 저장소 및 트러스트 저장소 파일 설정.	43
Download and Extract the Installer Files.	45
Verify Installer Code Signing.	45
Verify Installer Package Checksum on Windows.	46
라이선스 키 확인.	46
장 4: 응용 프로그램 서비스 및 데이터베이스 준비.	47
응용 프로그램 서비스 준비를 위한 검사 목록.	47
응용 프로그램 서비스 및 데이터베이스 준비 개요.	48
데이터베이스 사용자 계정 설정.	48
제품별 응용 프로그램 서비스 식별.	48
도메인 구성 리포지토리 데이터베이스 요구 사항.	49
IBM DB2 데이터베이스 요구 사항.	50
Microsoft SQL Server 데이터베이스 요구 사항.	51
Microsoft Azure SQL Database 요구 사항.	51
Oracle 데이터베이스 요구 사항.	51
PostgreSQL 데이터베이스 요구 사항.	52
Sybase 데이터베이스 요구 사항.	52
분석 서비스.	53
콘텐츠 관리 서비스.	54
참조 데이터 웨어하우스 요구 사항.	54

데이터 통합 서비스.	56
데이터 개체 캐시 데이터베이스 요구 사항.	57
프로파일링 웨어하우스 요구 사항.	58
워크플로우 데이터베이스 요구 사항.	59
Metadata Manager 서비스.	62
Metadata Manager 리포지토리 데이터베이스 요구 사항.	62
IBM DB2 데이터베이스 요구 사항.	63
Microsoft SQL Server 데이터베이스 요구 사항.	64
Oracle 데이터베이스 요구 사항.	65
Metadata Manager를 위한 분할 도메인.	66
모델 리포지토리 서비스.	67
모델 리포지토리 데이터베이스 요구 사항.	67
IBM DB2 데이터베이스 요구 사항.	68
Microsoft Azure SQL Database 요구 사항.	69
Microsoft SQL Server 데이터베이스 요구 사항.	69
Oracle 데이터베이스 요구 사항.	70
PostgreSQL 데이터베이스 요구 사항.	70
모니터링 모델 리포지토리 서비스.	71
PowerCenter 통합 서비스.	71
PowerCenter 리포지토리 서비스.	72
PowerCenter 리포지토리 데이터베이스 요구 사항.	72
IBM DB2 데이터베이스 요구 사항.	73
Microsoft SQL Server 데이터베이스 요구 사항.	73
Oracle 데이터베이스 요구 사항.	73
PostgreSQL Database Requirements	74
Sybase ASE 데이터베이스 요구 사항.	75
검색 서비스.	75
서비스 시스템에서 원시 연결 구성.	76
데이터베이스 클라이언트 소프트웨어 설치.	76
데이터베이스 클라이언트 환경 변수 구성.	77
장 5: Kerberos 인증 준비.	80
Kerberos 인증 준비를 위한 검사 목록.	80
Kerberos 인증 준비 개요.	80
Kerberos 구성 파일 설정.	81
서비스 사용자 및 키 탭 파일 이름 형식 생성.	82
노드 수준에서의 서비스 사용자 요구 사항.	82
프로세스 수준에서의 서비스 사용자 요구 사항.	83
SPN 형식 생성기 실행.	83
SPN 및 키 탭 형식 텍스트 파일 검토.	85
서비스 사용자 이름 및 키 탭 파일 생성.	86
서비스 사용자 이름 및 키 탭 파일 문제 해결.	87

장 6: 설치 프로그램 메시지에 필요한 정보 기록	89
설치 프로그램 메시지 기록을 위한 검사 목록	89
Record Information for Installer Prompts Overview	90
도메인	90
노드	91
Distribution Packages	91
응용 프로그램 서비스	91
데이터베이스	92
보안 데이터베이스에 대한 연결 문자열	94
보안 데이터 저장소	96
Kerberos	97
장 7: 서비스 설치 프로그램 소개	98
서비스 설치 프로그램 작업	98
보안 파일 및 디렉터리	98
설치 전 유틸리티	99
설치 전 시스템 검사 도구(i10Pi) 실행 (콘솔 모드)	99
설치 전 시스템 검사 도구(i10Pi) 실행(그래픽 모드)	102
자동 모드에서 설치 전 시스템 검사 도구(i10Pi) 실행	108
파트 III: 서비스 설치 프로그램 실행	109
장 8: Informatica 서비스 설치 (콘솔 모드)	110
Informatica 서비스 설치 개요	110
도메인 생성	110
설치 프로그램 실행	110
Informatica 설치 프로그램 시작	111
시작 - 약관 및 조건에 동의	111
구성 요소 선택	111
라이선스 및 설치 디렉터리	112
네트워크 보안 - 서비스 사용자 수준	112
네트워크 보안 - Kerberos 인증	113
도메인 선택	114
도메인 보안 - 보안 통신	117
Domain Configuration Repository	118
도메인 보안 - 암호화 키	123
도메인 및 노드 구성	123
Informatica 응용 프로그램 서비스 구성	126
모델 리포지토리 데이터베이스 구성	127
데이터 통합 서비스	131
모니터링 모델 리포지토리 데이터베이스 구성	132

콘텐츠 관리 서비스 매개 변수 및 데이터베이스.....	136
프로파일링 웨어하우스 데이터베이스.....	138
PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스.....	141
도메인에 가입.....	142
설치 프로그램 실행.....	142
시작 - 약관 및 조건에 동의.....	142
구성 요소 선택.....	143
설치 선행 조건.....	143
라이선스 및 설치 디렉터리.....	143
서비스 사용자 수준.....	144
도메인 선택.....	144
도메인 보안 - 보안 통신.....	145
도메인 구성.....	146
도메인 보안 - 암호화 키.....	147
도메인 가입 노드 구성.....	147
포트 구성.....	148
모델 리포지토리 데이터베이스 구성.....	149
데이터 통합 서비스.....	153
PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스.....	154

장 9: 그래픽 모드에서 Informatica 서비스 설치..... 155

그래픽 모드에서 Informatica 서비스 설치 개요.....	155
도메인 생성.....	155
설치 프로그램 실행.....	155
Informatica 설치 프로그램 시작.....	156
시작 - 약관 및 조건에 동의.....	157
License and Installation Directory.....	158
네트워크 보안 - 서비스 사용자 수준.....	161
네트워크 보안 - Kerberos 인증.....	162
도메인 선택.....	164
도메인 보안 - 보안 통신.....	170
도메인 구성 리포지토리.....	172
도메인 보안 - 암호화 키.....	175
도메인 및 노드 구성.....	176
포트 구성.....	179
Windows 서비스 구성.....	181
모델 리포지토리 서비스 데이터베이스 구성.....	182
모니터링 모델 리포지토리 서비스 데이터베이스 구성.....	186
데이터 통합 서비스.....	188
콘텐츠 관리 서비스 매개 변수 및 데이터베이스.....	190
프로파일링 웨어하우스 연결 데이터베이스.....	194
PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스.....	197

도메인에 가입.....	198
설치 프로그램 실행.....	198
Informatica 설치 프로그램 시작.....	199
시작 - 약관 및 조건에 동의.....	200
License and Installation Directory	201
네트워크 보안 - 서비스 사용자 수준.....	204
네트워크 보안 - Kerberos 인증.....	205
도메인 선택.....	207
도메인 보안 - 보안 연결.....	213
도메인 구성.....	215
도메인 보안 - 암호화 키.....	216
도메인 가입 노드 구성.....	217
포트 구성.....	218
Windows 서비스 구성.....	220
모델 리포지토리 서비스 데이터베이스 구성.....	221
데이터 통합 서비스.....	225
PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스.....	227
장 10: 자동 설치 프로그램 실행.....	229
자동 모드에서 설치.....	229
속성 파일 구성.....	229
설치 프로그램 실행.....	230
속성 파일의 암호 암호화.....	230
장 11: 문제 해결.....	232
설치 문제 해결 개요.....	232
실패한 설치 프로그램 프로세스 다시 시작.....	232
설치 프로그램을 다시 시작하기 전에.....	233
설치 프로그램 다시 시작.....	233
설치 로그 파일 문제 해결.....	233
디버그 로그 파일.....	234
파일 설치 로그 파일.....	234
서비스 관리자 로그 파일.....	234
도메인 및 노드 문제 해결.....	235
도메인 구성 리포지토리 작성.....	235
도메인 생성 또는 가입.....	235
Informatica 시작.....	236
도메인에 Ping 수행.....	236
라이선스 추가.....	236
Informatica Developer 문제 해결.....	237

파트 IV: 서비스를 설치한 후에	238
장 12: 도메인 구성 완료	239
도메인 구성 완료 검사 목록.....	239
도메인 구성 완료 개요.....	239
로컬 설정 및 코드 페이지 호환성 확인.....	240
로컬 환경 변수 구성.....	240
UNIX 또는 Linux에서 환경 변수 구성.....	241
Informatica 환경 변수 구성.....	241
라이브러리 경로 환경 변수 구성.....	242
Kerberos 환경 변수 구성.....	242
장 13: 응용 프로그램 서비스를 작성하기 위한 준비	244
응용 프로그램 서비스 생성 준비를 위한 검사 목록.....	244
분석 서비스용 디렉터리 작성.....	245
웹 응용 프로그램 서비스에 대한 보안 연결을 위한 키 저장소 작성.....	245
Informatica Administrator에 로그인.....	246
Informatica Administrator 로그인 문제 해결.....	246
연결 작성.....	247
IBM DB2 연결 속성.....	247
Microsoft Azure SQL Database 연결 속성.....	248
Microsoft SQL Server 연결 속성.....	249
Oracle 연결 속성.....	250
PostgreSQL 연결 속성.....	251
연결 작성.....	252
장 14: 응용 프로그램 서비스 생성 및 구성	253
응용 프로그램 생성 및 구성을 위한 검사 목록.....	253
응용 프로그램 서비스 생성 및 구성 개요.....	253
모델 리포지토리 서비스 작성 및 구성.....	254
모델 리포지토리 서비스 생성.....	254
모델 리포지토리 서비스를 생성한 후.....	257
데이터 통합 서비스 작성 및 구성.....	259
데이터 통합 서비스 작성.....	259
데이터 통합 서비스를 작성한 후.....	262
PowerCenter 리포지토리 서비스 작성 및 구성.....	262
PowerCenter 리포지토리 서비스 작성.....	262
PowerCenter 리포지토리 서비스를 작성한 후.....	264
PowerCenter 통합 서비스 작성 및 구성.....	266
PowerCenter 통합 서비스 작성.....	266
PowerCenter 통합 서비스를 작성한 후.....	268

Metadata Manager 서비스 작성 및 구성.	268
Metadata Manager 서비스 작성.	268
Metadata Manager 서비스를 작성한 후.	272
콘텐츠 관리 서비스 작성 및 구성.	272
콘텐츠 관리 서비스 작성.	272
분석 서비스 작성 및 구성.	274
분석 서비스 작성.	274
분석 서비스를 생성한 후.	276
검색 서비스 작성 및 구성.	276
검색 서비스 작성.	276

파트 V: Informatica 클라이언트 설치. 278

장 15: 클라이언트 설치. 279

클라이언트 설치 개요.	279
설치하기 전에.	280
Verify Installer Package Checksum.	280
시스템 요구 사항 확인.	280
Informatica Developer에 대한 타사 요구 사항 확인.	280
PowerCenter 클라이언트에 대한 타사 요구 사항 확인.	281
클라이언트 설치.	281
설치한 후에.	282
언어 설치.	282
보안 도메인을 위한 클라이언트 구성.	282
Developer tool 작업 공간 디렉터리 구성.	283
PowerCenter 클라이언트 시작.	284
Developer 도구 시작.	284

장 16: 자동 모드에서 설치. 286

자동 모드에서 설치 개요.	286
Configure the Properties File.	286
자동 설치 프로그램 실행.	287

파트 VI: 제거. 288

장 17: 제거. 289

Informatica 제거 개요.	289
제거 규칙 및 지침.	289
콘솔 모드에서 Informatica 서버 제거.	290
자동 모드에서 Informatica 서버 제거.	290
그래픽 모드에서 Informatica 서버 제거.	291
Informatica 클라이언트 제거.	291
그래픽 모드에서 Informatica 클라이언트 제거.	291

자동 모드에서 Informatica 클라이언트 제거.	292
---------------------------------------	-----

부록 A: Informatica 서비스 시작 및 중지. 294

Informatica 서비스 시작 및 중지 개요.	294
Informatica 서비스 시작 및 중지 (콘솔 사용).	294
Informatica Administrator에서 Informatica 중지.	295
제어판에서 Informatica 시작 또는 중지.	295
시작 메뉴에서 Informatica 시작 또는 중지.	295
명령 프롬프트에서 Informatica 시작 또는 중지.	295
Informatica 시작 또는 중지에 대한 규칙 및 지침.	296

부록 B: 배포 패키지 관리. 297

Managing Distribution Packages Overview.	297
Before You Begin.	297
Install or Remove Distribution Packages in Console Mode.	298
Install or Remove Distribution Packages in Silent Mode.	299
After You Install.	300

부록 C: UNIX 또는 Linux에서 데이터베이스에 연결. 301

UNIX 또는 Linux에서 데이터베이스에 연결 개요.	301
IBM DB2 범용 데이터베이스에 연결.	302
원시 연결 구성.	302
Informix 데이터베이스에 연결.	304
ODBC 연결 구성.	304
Microsoft SQL Server 데이터베이스에 연결.	305
ODBC를 통한 SSL 인증 구성.	305
Microsoft SQL Server의 사용자 지정 속성 구성.	305
Netezza 데이터베이스에 연결.	306
ODBC 연결 구성.	306
Oracle 데이터베이스에 연결.	308
원시 연결 구성.	308
PostgreSQL 데이터베이스에 연결.	310
Configuring Native Connectivity.	310
ODBC 연결 구성	312
Sybase ASE 데이터베이스에 연결.	314
원시 연결 구성.	314
Teradata 데이터베이스에 연결.	316
ODBC 연결 구성.	316
JDBC 데이터 소스에 연결.	318
ODBC 데이터 소스에 연결.	319
샘플 odbc.ini 파일.	321

부록 D: Windows에서 데이터베이스에 연결.....	328
Windows에서 데이터베이스에 연결 개요.....	328
Windows에서 IBM DB2 범용 데이터베이스에 연결.....	329
원시 연결 구성.....	329
Windows에서 Informix 데이터베이스에 연결.....	329
ODBC 연결 구성.....	330
Windows에서 Microsoft Access 및 Microsoft Excel에 연결.....	330
ODBC 연결 구성.....	330
Windows에서 Microsoft SQL Server 데이터베이스에 연결.....	330
원시 연결 구성.....	330
Microsoft SQL Server의 사용자 지정 속성 구성.....	331
Windows에서 Netezza 데이터베이스에 연결.....	332
ODBC 연결 구성.....	332
Windows에서 Oracle 데이터베이스에 연결.....	333
원시 연결 구성.....	333
PostgreSQL 데이터베이스에 연결.....	334
원시 연결 구성.....	334
ODBC 연결 구성.....	335
Windows에서 Sybase ASE 데이터베이스에 연결.....	335
원시 연결 구성.....	336
Windows에서 Teradata 데이터베이스에 연결.....	337
ODBC 연결 구성.....	337
부록 E: DB2 데이터베이스의 DynamicSections 매개 변수 업데이트.....	339
DynamicSections 매개 변수 개요.....	339
DynamicSections 매개 변수 설정.....	339
DDconnect JDBC 유틸리티 다운로드 및 설치.....	340
Test for JDBC 도구 실행.....	340
인덱스.....	341

서문

PowerCenter 및 *Data Quality* 설치의 지침에 따라 Informatica 서비스와 PowerCenter 및 Informatica Data Quality 제품을 설치하십시오. 하나 이상의 시스템에 Informatica 서비스 및 클라이언트를 설치할 수 있습니다. 이 가이드에는 Informatica 도메인에 대한 Informatica 서비스 및 클라이언트 설치를 위한 선행 및 후행 조건 태스크가 포함되어 있습니다. 선행 조건 태스크에는 환경 계획, 데이터베이스 설정 및 시스템 요구 사항 확인이 포함됩니다. 후행 조건 태스크에는 추가 응용 프로그램 서비스 및 환경 변수 구성이 포함됩니다.

Informatica 리소스

Informatica는 Informatica Network 및 기타 온라인 포털을 통해 다양한 범위의 제품 리소스를 제공합니다. 리소스를 통해 Informatica 제품 및 솔루션을 최대한 활용하고 다른 Informatica 사용자 및 주제별 전문가로부터 배울 수 있습니다.

Informatica Network

Informatica Network는 Informatica 기술 자료, Informatica 글로벌 고객 지원 센터 등 여러 리소스로 연결되는 관문입니다. Informatica Network를 시작하려면 <https://network.informatica.com>을 방문하십시오.

Informatica Network 멤버인 경우 다음 옵션이 가능합니다.

- 기술 자료에서 제품 리소스를 검색할 수 있습니다.
- 제품 사용 가능 여부에 대한 정보를 봅니다.
- 지원 사례를 생성하고 검토할 수 있습니다.
- 거주 지역의 Informatica 사용자 그룹 네트워크를 검색하고 동료와 협업 관계 유지

Informatica 기술 자료

Informatica 기술 자료를 사용하여 사용 방법 문서, 모범 사례, 비디오 자습서, 자주 묻는 질문에 대한 답변 등 제품 리소스를 확인할 수 있습니다.

기술 자료를 검색하려면 <https://search.informatica.com>을 방문하십시오. 기술 자료에 대한 질문, 의견 또는 아이디어가 있는 경우 KB_Feedback@informatica.com을 통해 Informatica 기술 자료 팀에 문의해 주시기 바랍니다.

Informatica 설명서

Informatica 설명서 포털에서 확장된 설명서 라이브러리를 탐색하여 현재 및 최근 제품 릴리스를 확인할 수 있습니다. 설명서 포털을 탐색하려면 <https://docs.informatica.com>을 방문하십시오.

제품 설명서에 대한 질문, 의견 또는 아이디어가 있는 경우 infa_documentation@informatica.com에서 Informatica 설명서 팀에 문의해 주시기 바랍니다.

Informatica Product Availability Matrix

PAM(Product Availability Matrix)은 제품 릴리스에서 지원하는 운영 체제 버전, 데이터베이스 및 데이터 소스 유형과 대상을 나타냅니다.

<https://network.informatica.com/community/informatica-network/product-availability-matrices>에서 Informatica PAM을 찾을 수 있습니다.

Informatica Velocity

Informatica Velocity는 수백 가지 데이터 관리 프로젝트의 실제 경험을 토대로 Informatica 전문 서비스업에서 개발한 팁과 모범 사례 모음입니다. Informatica Velocity는 전 세계의 조직과 협력하여 성공적인 데이터 관리 솔루션을 계획, 개발, 배포 및 유지 관리하는 Informatica 컨설턴트의 포괄적인 지식을 보여줍니다.

Informatica Velocity 리소스는 <http://velocity.informatica.com>에서 확인할 수 있습니다. Informatica Velocity에 대한 질문, 주석 또는 아이디어가 있으시면 Informatica 전문 서비스업(ips@informatica.com)에 문의하십시오.

Informatica Marketplace

Informatica Marketplace는 Informatica 구현을 확대 및 개선하기 위한 솔루션을 찾을 수 있는 포럼입니다.

Marketplace에서 Informatica 개발자와 파트너가 제공하는 수백 개의 솔루션을 활용하여 생산성을 향상시키고 프로젝트의 구현에 걸리는 시간을 줄일 수 있습니다. <https://marketplace.informatica.com>에서 Informatica Marketplace를 찾을 수 있습니다.

Informatica 글로벌 고객 지원 센터

전화 또는 Informatica 네트워크를 통해 글로벌 지원 센터에 문의할 수 있습니다.

해당 지역의 Informatica 글로벌 고객 지원 전화 번호는 Informatica 웹 사이트 (<https://www.informatica.com/services-and-training/customer-success-services/contact-us.html>)를 방문하여 찾을 수 있습니다.

Informatica 네트워크에 대한 온라인 지원 리소스를 찾으려면 <https://network.informatica.com>으로 이동하고 eSupport 옵션을 선택하십시오.

파트 I: 설치 시작

이 파트에 포함된 장:

- [설치 시작, 16](#)

제 1 장

설치 시작

이 장에 포함된 항목:

- [시작을 위한 검사 목록, 16](#)
- [설치 개요, 16](#)
- [설치 프로세스, 17](#)
- [설치 옵션 계획, 17](#)
- [설치 구성 요소 계획, 19](#)

시작을 위한 검사 목록

이 장에는 설치와 관련된 개요 수준의 개념 및 계획 정보가 포함되어 있습니다. 준비 태스크의 완료 여부를 추적하는 데 이 검사 목록을 사용하십시오.

- 개요 수준의 개념을 이해합니다.
 - 설치 프로그램 설명 및 프로세스
 - Informatica 도메인 용어 및 구성 요소
- 개요 수준의 계획을 시작합니다.
 - 설치 옵션. 설치 옵션을 검토하여 설치 제품 및 옵션을 이해합니다.
 - 설치 구성 요소. 설치 구성 요소 및 계획 참고 사항에 대한 설명을 검토합니다.

설치 개요

Informatica 설치 프로그램의 Informatica 도메인 서비스 및 클라이언트를 소개하겠습니다. Informatica 도메인 서비스는 도메인을 지원하는 핵심 서비스와 응용 프로그램 서비스로 구성됩니다. Informatica 클라이언트는 Thick 및 웹 클라이언트 응용 프로그램으로 구성됩니다.

Informatica 서비스를 설치하면 도메인을 생성하거나 도메인에 가입하라는 메시지가 표시됩니다. 도메인은 응용 프로그램 서비스가 실행되는 시스템을 나타내는 노드 컬렉션입니다. 설치 프로그램을 처음 실행할 경우에는 도메인을 반드시 생성해야 합니다. 단일 시스템에 설치하는 경우 해당 시스템에 Informatica 도메인 및 게이트웨이 노드를 생성합니다. 여러 시스템에 설치하는 경우 처음 설치할 때 Informatica 도메인 게이트웨이 노드를 생성합니다. 다른 시스템에 추가로 설치하는 동안 이 도메인에 가입시킬 게이트웨이 또는 작업자 노드를 생성합니다.

설치 프로그램을 실행하면 서비스 파일이 설치됩니다. 필요에 따라 설치 프로세스 중에 응용 프로그램 서비스를 생성하거나, 설치가 완료된 후 응용 프로그램 서비스를 수동으로 생성할 수 있습니다.

다른 Informatica 제품이 설치되어 있는 경우 설치된 버전이 설치 중인 제품 버전과 호환되는지 확인하십시오.

설치 프로세스

Informatica 도메인 서비스 및 Informatica 클라이언트의 설치는 여러 단계로 구성됩니다.

설치 프로세스는 설치하는 제품에 따라 다릅니다. 설치 프로세스의 기본적인 태스크는 다음과 같습니다.

설치 전 태스크를 수행합니다.

1. Informatica 설치를 계획합니다. 환경에서 실행하려는 제품을 결정합니다. 도메인을 생성하는 경우, 도메인의 노드 수, 각 노드에서 실행할 응용 프로그램 서비스, 시스템 요구 사항 및 도메인에서 사용할 사용자 인증 유형을 고려합니다.
2. 리포지토리, 웨어하우스 및 카탈로그에 필요한 데이터베이스를 준비합니다. 데이터베이스 요구 사항을 확인하고 데이터베이스를 설정합니다.
3. Informatica 서비스를 성공적으로 설치하고 실행할 수 있도록 시스템 요구 사항에 맞게 시스템을 설정합니다.
4. 도메인, 서비스 및 데이터베이스에 대한 보안 요구 사항을 결정합니다.

설치 프로그램을 실행합니다.

설치 프로그램을 실행할 때는 요구 사항에 따라 다른 옵션을 선택할 수 있습니다.

구성을 완료합니다.

1. 코드 페이지 호환성을 확인합니다.
2. 환경 변수를 구성합니다.
3. 도메인에서 사용하는 사용자 인증 유형에 필요한 태스크를 완료합니다.
4. 필요한 경우 도메인에 대해 보안 통신을 구성합니다.
5. 응용 프로그램 서비스를 생성 및 구성합니다.
6. 응용 프로그램 서비스에 필요한 연결을 구성합니다.
7. 응용 프로그램 서비스에 필요한 사용자 및 연결을 생성합니다.

Informatica 클라이언트 도구를 설치합니다.

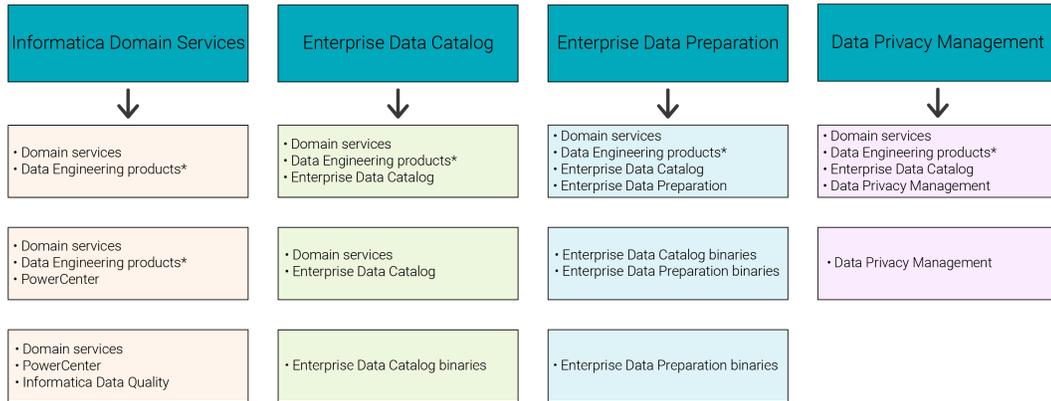
1. 클라이언트의 설치 및 타사 소프트웨어 요구 사항을 확인합니다.
2. 클라이언트 설치 프로그램을 사용하여 Windows 시스템에 설치합니다.
3. 필요한 환경 변수를 구성하고 필요한 경우 다른 언어를 설치합니다.

설치 옵션 계획

설치 계획 및 준비를 시작하기 전에, 실행할 설치 유형을 결정합니다.

설치 프로그램을 실행할 때 설치하려는 제품에 따라 시작 패널의 옵션에서 선택할 수 있습니다. 구성 요소 패널은 제품 선택에 따라 나타나므로 제품 구성 요소를 선택할 수 있습니다.

다음 이미지는 설치 옵션에 따라 설치 가능한 제품을 보여 줍니다.



*Data Engineering products include Data Engineering Integration, Data Engineering Quality, and Data Engineering Streaming.

설치 프로그램을 실행할 때 사용할 수 있는 다양한 옵션을 고려하십시오.

Informatica 도메인 서비스

Informatica 도메인 서비스를 설치하려면 구성 요소 패널에서 설치 옵션 1을 선택하여 Informatica 도메인 서비스를 설치하고 구성합니다.

Informatica 도메인 서비스를 설치할 때 다음 제품 옵션 중 하나에서 설치합니다.

- 통합, 품질 및 스트리밍에 대한 Data Engineering 제품만
- 기존 제품과 위에 언급된 Data Engineering 제품
- PowerCenter 및 Informatica Data Quality 같은 기존 제품만

Informatica 도메인 서비스를 설치할 때는 도메인을 생성할지 아니면 도메인에 가입할지 선택할 수 있습니다. Test Data Management가 기존 제품 및 Data Engineering 제품 둘 모두와 함께 설치되었습니다.

Enterprise Data Catalog

Enterprise Data Catalog를 설치하려면 구성 요소 패널에서 설치 옵션 2를 선택하여 Enterprise Data Catalog를 설치하고 구성합니다.

Enterprise Data Catalog를 설치할 때 다음 옵션 중 하나를 선택하십시오.

- 도메인 서비스, Data Engineering 제품 및 Enterprise Data Catalog.
- 도메인 서비스 및 Enterprise Data Catalog.
- 기존 도메인의 Enterprise Data Catalog 바이너리만. 바이너리를 설치한 후 설치 프로그램을 다시 실행하여 서비스를 구성할 수 있습니다.

Enterprise Data Preparation

Enterprise Data Preparation을 설치하려면 구성 요소 패널에서 설치 옵션 3을 선택하여 Enterprise Data Preparation을 설치하고 구성합니다.

Enterprise Data Preparation을 설치할 때 다음 옵션 중 하나를 선택하십시오.

- Data Engineering 제품, Enterprise Data Catalog 및 Enterprise Data Preparation
- 기존 도메인의 Enterprise Data Catalog 및 Enterprise Data Preparation 바이너리. 바이너리를 설치한 후 설치 프로그램을 다시 실행하여 서비스를 구성할 수 있습니다.
- 기존 도메인의 Enterprise Data Preparation 바이너리와 Enterprise Data Catalog만. 바이너리를 설치한 후 설치 프로그램을 다시 실행하여 서비스를 구성할 수 있습니다.

Data Privacy Management

Data Privacy Management를 설치하려면 구성 요소 패널에서 설치 옵션 4를 선택하여 Data Privacy Management를 설치하고 구성합니다.

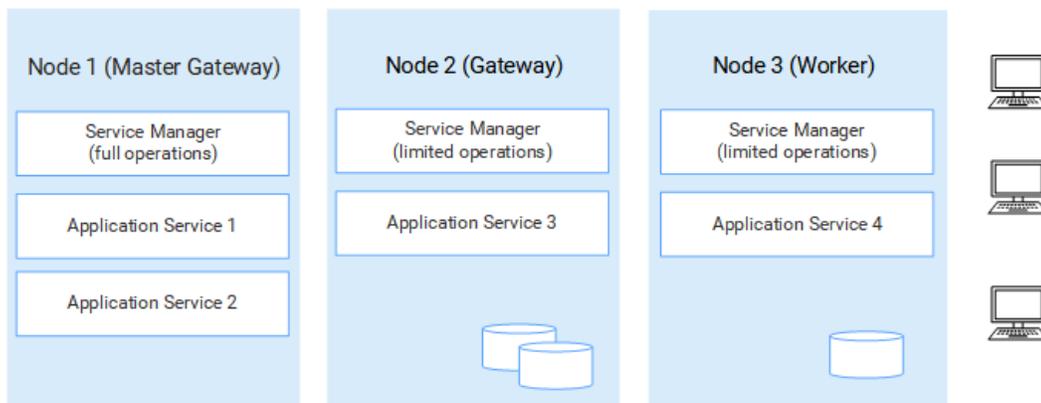
Data Privacy Management를 설치할 때 다음 옵션 중 하나를 선택하십시오.

- Data Engineering 제품, Enterprise Data Catalog 및 Data Privacy Management
- 기존 도메인의 Data Privacy Management와 Enterprise Data Catalog

설치 구성 요소 계획

Informatica 도메인은 노드 및 서비스의 컬렉션입니다. 노드는 도메인 시스템을 논리적으로 나타낸 것입니다. 서비스에는 모든 도메인 작업을 관리하는 서비스 관리자 및 서버 기반 기능을 나타내는 일련의 응용 프로그램 서비스가 포함됩니다. 도메인 및 일부 서비스에는 메타데이터와 런타임 결과를 쓰기 위한 데이터베이스가 필요합니다.

다음 그림은 여러 노드에 있는 도메인의 아키텍처를 간략하게 보여 줍니다.



노드

도메인 서비스를 처음으로 설치할 때 Informatica 도메인과 게이트웨이 노드를 생성합니다. 다른 시스템에 도메인 서비스를 설치하는 경우에는 도메인에 가입시킬 노드를 추가로 생성합니다.

도메인에는 다음과 같은 노드 유형이 있습니다.

- 게이트웨이 노드. 게이트웨이 노드는 도메인 게이트웨이로 사용되도록 구성하는 노드입니다. 게이트웨이 노드는 응용 프로그램 서비스를 실행할 수 있으며 마스터 게이트웨이 노드로 사용될 수 있습니다. 마스터 게이트웨이 노드는 도메인의 진입점입니다. 두 개 이상의 노드를 게이트웨이 노드로 구성할 수 있지만 어느 시점 이든 게이트웨이 노드 하나만 마스터 게이트웨이 노드로 작동합니다.
- 작업자 노드. 작업자 노드는 도메인의 게이트웨이로 노드로 구성하지 않은 모든 노드입니다. 작업자 노드는 응용 프로그램 서비스를 실행할 수 있지만 게이트웨이의 역할을 수행할 수는 없습니다.

설치 계획 시 참고 사항: 서비스 및 처리 요구 사항에 기반하여 필요한 노드의 유형과 개수를 계획해야 합니다. 고가용성을 구성한 경우에는 장애 조치 기능을 위해 게이트웨이 노드를 두 개 이상 생성하는 것이 좋습니다.

서비스 관리자

서비스 관리자는 모든 도메인 작업을 관리하는 서비스입니다. 서비스 관리자는 도메인의 각 노드에서 실행되며 인증, 로깅 및 응용 프로그램 서비스 관리 같은 도메인 기능을 수행합니다. 게이트웨이 노드의 서비스 관리자는 작업자 노드의 서비스 관리자보다 더 많은 태스크를 수행합니다.

설치 계획 시 참고 사항: 서비스 관리자 기능은 노드 유형과 관련됩니다.

응용 프로그램 서비스

응용 프로그램 서비스는 서버 기반 기능을 나타냅니다. 응용 프로그램 서비스는 필수 사항 또는 선택 사항일 수 있으며 데이터베이스에 액세스해야 할 수 있습니다.

설치 프로그램을 실행할 때 필요에 따라 일부 서비스를 생성할 수 있습니다. 설치를 완료한 후에는 조직에 대해 생성된 라이선스 키에 기반하여 다른 응용 프로그램 서비스를 생성합니다.

설치 계획 시 참고 사항: 응용 프로그램 서비스를 계획할 경우, 해당 응용 프로그램 서비스에 연결하는 연결된 서비스를 고려해야 합니다. 또한 응용 프로그램 서비스를 생성하는 데 필요한 관계형 데이터베이스도 계획해야 합니다.

데이터베이스

일부 응용 프로그램 서비스는 메타데이터를 저장하고 런타임 결과를 쓸 수 있는 데이터베이스를 필요로 합니다. 이러한 응용 프로그램 서비스가 사용할 데이터베이스를 도메인에 생성해야 합니다.

다음 데이터베이스를 생성할 수 있습니다.

도메인 구성 리포지토리 데이터베이스

도메인 구성 리포지토리에는 도메인의 구성 및 사용자 정보가 저장됩니다.

참조 데이터 웨어하우스 데이터베이스

참조 데이터 웨어하우스는 사용자가 모델 리포지토리에서 정의하는 참조 테이블 개체에 대한 데이터 값을 저장합니다. 참조 데이터 웨어하우스 및 모델 리포지토리를 식별하도록 콘텐츠 관리 서비스를 구성합니다.

데이터 개체 캐시 데이터베이스

데이터 개체 캐시에는 데이터 통합 서비스를 위해 캐싱된 논리적 데이터 개체 및 가상 테이블이 저장됩니다. 데이터 개체 캐싱을 통해 데이터 통합 서비스는 미리 작성된 논리적 데이터 개체 및 가상 테이블에 액세스할 수 있습니다.

프로파일링 웨어하우스 데이터베이스

프로파일링 웨어하우스에는 프로파일링 및 성과 기록표 결과가 저장됩니다. 프로파일링 및 데이터 검색을 수행하려면 프로파일링 웨어하우스가 필요합니다.

워크플로우 데이터베이스

워크플로우 데이터베이스에는 데이터 통합 서비스를 사용하는 워크플로우에 대한 런타임 메타데이터가 저장됩니다.

Metadata Manager 리포지토리 데이터베이스

Metadata Manager 리포지토리는 개별 메타데이터 소스의 메타데이터를 저장하는 관계형 데이터베이스의 중앙 위치입니다. 여기에는 Metadata Manager 웨어하우스 및 각 메타데이터 소스 유형에 대한 모델도 저장됩니다.

모델 리포지토리 데이터베이스

모델 리포지토리에는 Informatica 서비스 및 클라이언트의 데이터와 메타데이터가 저장됩니다. Analyst 도구 및 Developer tool과 같은 Informatica 클라이언트 도구는 데이터를 모델 리포지토리에 저장합니다.

모니터링 모델 리포지토리 데이터베이스

모니터링 모델 리포지토리에는 Informatica 클라이언트 및 응용 프로그램 서비스에서 생성된 임시 작업, 응용 프로그램, 논리적 데이터 개체, SQL Data Services, 웹 서비스 및 워크플로우에 대한 통계가 저장됩니다.

PowerCenter 리포지토리 데이터베이스

PowerCenter 리포지토리에는 PowerCenter 서비스 및 클라이언트의 데이터와 메타데이터가 저장됩니다. PowerCenter 리포지토리 서비스는 리포지토리를 관리하고 리포지토리 데이터베이스와 리포지토리 클라이언트 사이에서 모든 메타데이터 트랜잭션을 수행합니다.

설치 계획 시 참고 사항: 응용 프로그램 서비스가 사용할 데이터베이스 및 데이터베이스 사용자를 생성해야 합니다.

사용자 인증

설치 프로그램을 실행하면 도메인에 대해 사용할 인증을 선택할 수 있습니다.

도메인은 다음 인증 유형을 사용하여 Informatica 도메인의 사용자를 인증할 수 있습니다.

- 원시. 원시 사용자 계정은 도메인에 저장되며 해당 도메인 내에서만 사용될 수 있습니다. 기본값은 원시 인증입니다.
- LDAP. LDAP 사용자 계정은 LDAP 디렉터리 서비스에 저장되며 엔터프라이즈 내의 응용 프로그램 간에 공유됩니다. LDAP 인증은 설치 관리자를 실행한 이후에 구성할 수 있습니다.
- SAML. Administrator 도구, Analyst 도구 및 Monitoring 도구에 대해 SAML(Security Assertion Markup Language) 인증을 구성할 수 있습니다. SAML 인증은 설치 관리자를 실행한 이후에 구성할 수 있습니다.
- Kerberos. Kerberos 사용자 계정은 LDAP 디렉터리 서비스에 저장되며 엔터프라이즈 내의 응용 프로그램 간에 공유됩니다. 설치 중에 Kerberos 인증을 활성화하는 경우, Kerberos KDC(키 배포 센터)와 함께 작동하도록 Informatica 도메인을 구성해야 합니다.

설치 계획 시 참고 사항: 도메인에서 사용할 인증 유형을 계획해야 합니다. 설치 프로그램이 Kerberos 인증을 구성하도록 하려면 설치 전에 네트워크를 준비해야 합니다. 설치 후에 Kerberos를 구성할 수도 있습니다. SAML 인증과 Kerberos 인증을 모두 구성할 수는 없습니다.

보안 데이터 저장소

Informatica는 Informatica 리포지토리에 데이터를 저장하기 전에 중요 데이터를 암호화합니다.

도메인을 생성할 때 암호화 키 디렉터리를 지정해야 합니다. 설치 프로그램은 siteKey라는 암호화 키 파일을 생성하고, 기본 디렉터리 또는 사용자가 지정하는 지정된 디렉터리에 이 파일을 저장합니다. 도메인의 모든 노드는 동일한 암호화 키를 사용해야 합니다.

중요: 설치 프로그램은 고유한 사이트 키도 생성합니다. 사이트 키를 분실하는 경우 사이트 키를 다시 생성할 수 없습니다. 이 키의 사본을 반드시 저장하고 고유한 사이트 키를 다른 사람과 공유하지 마십시오.

도메인 보안

도메인을 생성할 때 옵션을 활성화하여 도메인의 보안을 구성할 수 있습니다.

다음 도메인 구성 요소에 대해 보안 통신을 구성할 수 있습니다.

- Administrator 도구. Administrator 도구에 대해 보안 HTTPS 연결을 구성합니다. 설치 중에 HTTPS 연결에 사용할 키 저장소 파일을 제공할 수 있습니다.
- 서비스 관리자. 서비스 관리자와 다른 도메인 서비스 사이에 보안 연결을 구성합니다. 설치 중에, 사용할 SSL 인증서가 포함된 키 저장소 및 트러스트 저장소 파일을 제공할 수 있습니다.

- 도메인 구성 리포지토리. SSL 프로토콜을 사용하여 도메인 구성 리포지토리를 보호할 수 있습니다. 사용할 SSL 인증서가 포함된 트러스트 저장소 파일을 설치 중에 제공할 수 있습니다.

설치 계획 시 참고 사항: 도메인 구성 요소에 구성할 보안 수준을 결정합니다. 도메인에 대해 보안을 구성할 경우 키 저장소 파일과 트러스트 저장소 파일의 위치 및 암호를 알고 있어야 합니다. Informatica 도메인에 대해 Kerberos 인증을 사용할 경우 Kerberos 관리자와 협력하여 도메인에 필요한 사용자 및 서비스 사용자를 설정해야 합니다.

Informatica 클라이언트 도구

도메인의 기본 Informatica 기능에 액세스하려면 Informatica 클라이언트를 사용합니다. 클라이언트는 서비스 관리자 및 응용 프로그램 서비스에 요청을 합니다.

Informatica 클라이언트는 도메인에서 서비스 및 리포지토리에 액세스하기 위해 사용하는 Thick 클라이언트 응용 프로그램과 Thin 또는 웹 클라이언트 응용 프로그램으로 구성됩니다.

다음 테이블에는 PowerCenter용 도구가 설명되어 있습니다.

Informatica 클라이언트	설명
Informatica Developer(Developer tool)	데이터 개체, 매핑, 프로필 및 워크플로우를 생성하고 실행하는 Thick 클라이언트 응용 프로그램입니다.
Informatica Administrator(Administrator 도구)	도메인 및 응용 프로그램 서비스를 관리하는 웹 응용 프로그램입니다.
Informatica Analyst(Analyst 도구)	엔터프라이즈에서 데이터 분석, 정리, 통합 및 표준화에 사용되는 웹 응용 프로그램입니다.
PowerCenter Client	매핑, 세션 및 워크플로우를 생성하고 실행하는 Thick 클라이언트 응용 프로그램입니다.

설치 계획 시 참고 사항: 설치할 PowerCenter 클라이언트 및 Developer tool 인스턴스 수를 결정합니다. 웹 클라이언트 응용 프로그램은 계획하지 않아도 됩니다.

파트 II: 서비스를 설치하기 전에

이 파트에 포함된 장:

- [UNIX에 서비스를 설치하기 전에 \(또는 Linux\), 24](#)
- [Windows에 서비스를 설치하기 전에, 37](#)
- [응용 프로그램 서비스 및 데이터베이스 준비, 47](#)
- [Kerberos 인증 준비, 80](#)
- [설치 프로그램 메시지에 필요한 정보 기록, 89](#)
- [서비스 설치 프로그램 소개, 98](#)

제 2 장

UNIX에 서비스를 설치하기 전에 (또는 Linux)

이 장에 포함된 항목:

- [Before You Begin Checklist , 24](#)
- [릴리스 노트 읽기, 25](#)
- [시스템 요구 사항 확인, 25](#)
- [Data Transformation 파일 백업, 31](#)
- [POSIX 비동기 I/O 구성, 32](#)
- [환경 변수 검토, 32](#)
- [시스템 사용자 계정 작성, 33](#)
- [키 저장소 파일 설정, 33](#)
- [Download and Extract the Installer Files, 35](#)
- [라이선스 키 확인, 36](#)

Before You Begin Checklist

This chapter contains preliminary tasks that you must complete. Use this checklist to track preliminary tasks before you prepare for services.

- Read the Informatica Release Notes for updates to the installation and upgrade process.
- Verify system requirements:
 - Verify sizing requirements based upon your processing and concurrency requirements.
 - Review the patch requirements to verify that the machine has the required operating system patches and libraries.
 - Verify that the port numbers to use for application service processes are available on the machines where you install the Informatica services.
 - Review the distribution requirements to integrate the Informatica domain with the Hadoop or Databricks environment.
 - Verify that the operating system meets the file descriptor limit.
- Back up the Data Transformation files that were created in a previous installation.

- Review system environment variables.
- Create a system user account to run the installer.
- Set up keystore and truststore files if you want to configure secure communication for the domain and set up a secure connection to web client applications.
- Extract the installer files:
 - Verify installer code signing.
 - Verify installer package integrity with checksum.
- Verify the license key.

릴리스 노트 읽기

릴리스 노트에서 설치 및 업그레이드 프로세스에 대한 업데이트를 확인하십시오. 또한 릴리스에 대해 알려지거나 수정된 문제에 대한 정보도 확인할 수 있습니다.

Informatica [documentation portal](#)에서 릴리스 정보를 확인하십시오.

시스템 요구 사항 확인

환경이 설치 프로세스, 임시 디스크 공간, 포트 가용성, 데이터베이스 및 응용 프로그램 서비스 하드웨어에 대한 최소 시스템 요구 사항을 충족하는지 확인하십시오.

제품 요구 사항 및 지원되는 플랫폼에 대한 자세한 내용은 [Product Availability Matrix](#)를 참조하십시오.

임시 디스크 공간 및 사용 권한 확인

환경이 임시 디스크 공간, 임시 파일 권한 및 Informatica 클라이언트 도구에 대한 최소 시스템요구 사항을 충족하는지 확인합니다.

임시 파일의 디스크 공간

설치 프로그램은 하드 디스크에 임시 파일을 씁니다. 설치를 지원할 1GB 디스크 공간이 시스템에 있는지 확인하십시오. 설치가 완료되면 설치 프로그램이 임시 파일을 삭제하고 디스크 공간을 해제합니다.

다음 테이블에는 PowerCenter 또는 Data Engineering 제품 설치에 대한 최소 디스크 공간 및 메모리 요구 사항이 설명되어 있습니다.

옵션	최소 요구 사항
설치 프로그램을 실행하는 데 필요한 임시 디스크 공간	1GB 디스크 공간
Data Engineering 제품에 대한 응용 프로그램 서비스 설치	50GB 디스크 공간, 8GB RAM 및 8개 코어. 50GB 중에서 25GB는 제품 설치 바이너리에 사용됩니다.
PowerCenter에 대한 응용 프로그램 서비스 설치	50GB 디스크 공간, 4GB RAM 및 6개 코어. 50GB 중에서 25GB는 제품 설치 바이너리에 사용됩니다.

임시 파일에 대한 사용 권한

/tmp 디렉터리에 대한 읽기, 쓰기 및 실행 권한이 있어야 합니다.

제품 요구 사항 및 지원되는 플랫폼에 대한 자세한 내용은 [Product Availability Matrix](#)를 참조하십시오.

UNIX 또는 Linux에서 패치 요구 사항 검토

Informatica 서비스를 설치하기 전에 필요한 운영 체제 패치 및 라이브러리가 시스템에 있는지 확인하십시오.

UNIX에 설치된 PowerCenter

The following table lists the patches and libraries that the Informatica services require for PowerCenter on UNIX:

Platform	Compiler Version	Operating System	Operating System Patch
AIX	16	7.1 TL5	OS level: 7100-05 bos.adt.debug Version 7.1.5.32
AIX	16	7.2 TL4	OS level: 7200-04 bos.adt.debug Version 7.2.4.0

Linux에 설치된 PowerCenter

The following table lists the patches and libraries that the Informatica services require for PowerCenter on Linux:

Platform	Operating System	Operating System Patch
AWS Linux	Linux 2 - 2.0.20220805.0	All of the following packages: - e2fsprogs-libs-1.42.9-19.amzn2.x86_64 - keyutils-libs-1.5.8-3.amzn2.0.2.x86_64 - libsepol-2.5-8.1.amzn2.0.2.x86_64 - libselinux-2.5-12.amzn2.0.2.x86_64
Ubuntu	20.04.1	All of the following packages: - e2fsprogs/focal,now 1.45.5-2ubuntu1 amd64 [installed] - libkeyutils1/focal,now 1.6-6ubuntu1 amd64 [installed,automatic] - libselinux1/focal,now 3.0-1build2 amd64 [installed,automatic] - libsepol1/focal,now 3.0-1 amd64 [installed,automatic]
Ubuntu	18.04	All of the following packages: - e2fsprogs/focal,now 1.45.5-2ubuntu1 amd64 [installed] - libkeyutils1/focal,now 1.5.9-9.2ubuntu2 amd64 [installed,automatic] - libselinux1/focal,now 2.7-2build2 amd64 [installed,automatic] - libsepol1/focal,now 2.7-1ubuntu0.1 amd64 [installed,automatic]
Linux-x64	Red Hat Enterprise Linux 7.3	All of the following packages, where <version> is any version of the package: - e2fsprogs-libs-<version>.el7 - keyutils-libs-<version>.el7 - libselinux-<version>.el7 - libsepol-<version>.el7
Linux-x64	Red Hat Enterprise Linux 8	All of the following packages, where <version> is any version of the package: - e2fsprogs-libs-<version>.el8 - keyutils-libs-<version>.el8 - libselinux-<version>.el8 - libsepol-<version>.el8
Linux-x64	SUSE Linux Enterprise Server 12	Service Pack 2
Linux-x64	SUSE Linux Enterprise Server 15	Service Pack 0 and Service Pack 1.

포트 요구 사항 확인

설치 프로그램에서 Informatica 도메인의 구성 요소에 대한 포트를 설정하고, 일부 응용 프로그램 서비스에 사용할 동적 포트 범위를 지정합니다.

구성 요소에 사용할 포트 번호와 응용 프로그램 서비스에 사용할 동적 포트 번호 범위를 지정할 수 있습니다. 또는 설치 프로그램에서 제공하는 기본 포트 번호를 사용할 수 있습니다. 설치 프로그램을 실행하는 시스템에서 포트 번호를 사용할 수 있는지 확인합니다.

참고: 포트가 충돌할 경우 서비스 및 노드를 시작하지 못할 수 있습니다.

다음 테이블에는 설치를 위한 포트 요구 사항이 설명되어 있습니다.

포트	설명
노드 포트	설치 중에 작성된 노드의 포트 번호입니다. 기본값은 6005입니다.
서비스 관리자 포트	노드에서 서비스 관리자가 사용하는 포트 번호입니다. 서비스 관리자가 이 포트에서 들어오는 연결 요청을 수신합니다. 클라이언트 응용 프로그램은 이 포트를 사용하여 도메인의 서비스와 통신합니다. Informatica 명령줄 프로그램은 이 포트를 사용하여 도메인과 통신합니다. 또한 SQL 데이터 서비스 JDBC/ODBC 드라이버용 포트입니다. 기본값은 6006입니다.
서비스 관리자 종료 포트	도메인 서비스 관리자에 대한 서버 종료를 제어하는 포트 번호입니다. 서비스 관리자는 이 포트에서 종료 명령을 수신합니다. 기본값은 6007입니다.
Informatica Administrator 포트	Informatica Administrator에서 사용하는 포트 번호입니다. 기본값은 6008입니다.
Informatica Administrator 종료 포트	Informatica Administrator에 대한 서버 종료를 제어하는 포트 번호입니다. Informatica Administrator가 이 포트에서 종료 명령을 수신합니다. 기본값은 6009입니다.
최소 포트 번호	이 노드에서 실행되는 응용 프로그램 서비스 프로세스에 할당할 수 있는 동적 포트 번호 범위에서 가장 낮은 포트 번호입니다. 기본값은 6014입니다.
최대 포트 번호	이 노드에서 실행되는 응용 프로그램 서비스 프로세스에 할당할 수 있는 동적 포트 번호 범위에서 가장 높은 포트 번호입니다. 기본값은 6114입니다.
응용 프로그램 서비스용 동적 포트 범위	응용 프로그램 서비스 프로세스가 시작될 때 동적으로 할당할 수 있는 포트 번호 범위입니다. 동적 포트를 사용하는 응용 프로그램 서비스를 시작할 경우 서비스 관리자가 이 범위에서 사용 가능한 첫 번째 포트를 서비스 프로세스에 동적으로 할당합니다. 범위의 포트 수는 노드에서 실행되는 응용 프로그램 서비스 프로세스 수의 두 배 이상이어야 합니다. 기본값은 6014 - 6114입니다. 서비스 관리자는 이 범위의 포트 번호를 모델 리포지토리 서비스에 동적으로 할당합니다.
응용 프로그램 서비스용 정적 포트	정적 포트에는 변경되지 않는 전용 포트 번호가 할당됩니다. 응용 프로그램 서비스를 작성할 경우 기본 포트 번호를 사용하거나 수동으로 포트 번호를 할당할 수 있습니다. 다음 서비스에서 정적 포트 번호를 사용합니다. - 콘텐츠 관리 서비스. HTTP의 경우 기본값은 8105입니다. - 데이터 통합 서비스. HTTP의 경우 기본값은 8095입니다.

포트 구성 지침

설치 프로그램은 도메인 포트 충돌을 방지하기 위해 사용자가 지정한 포트 번호에 대해 유효성 검사를 수행합니다.

다음 지침을 사용하여 포트 번호를 결정하십시오.

- 도메인과 해당 도메인에 있는 각 구성 요소에 대해 지정하는 포트 번호는 고유해야 합니다.
- 도메인과 도메인 구성 요소의 포트 번호는 응용 프로그램 서비스 프로세스에 대해 지정하는 포트 번호 범위 내에 있을 수 없습니다.
- 응용 프로그램 서비스 프로세스에 대해 지정하는 포트 번호 범위에서 가장 높은 번호는 가장 낮은 포트 번호보다 3 이상 커야 합니다. 예를 들어 범위의 최소 포트 번호가 6400이면 최대 포트 번호는 6403 이상이어야 합니다.
- 지정한 포트 번호가 1025보다 낮거나 65535보다 높을 수는 없습니다.

Verify Distribution Package Requirements (Linux and UNIX)

You can use third-party distribution packages to integrate the Informatica domain with the Hadoop or Databricks environment.

The Informatica domain and client require the distribution packages to process complex files within the Informatica domain or to connect to Hadoop or Databricks environment when you process within the Informatica domain.

If you need a distribution package, you can install it through the installer or through Integration Package Manager (the package manager) at any time.

You can use the Cloudera CDP Private Cloud distribution package to process complex files within the Informatica domain or to connect to the Hadoop or Databricks environment when you process within the Informatica domain. However, you can use a different distribution package according to your requirements.

The following adapters require distribution packages for processing within the Informatica domain:

- PowerExchange for Amazon S3
- PowerExchange for Google Cloud Storage
- PowerExchange for Google Cloud Storage for PowerCenter
- PowerExchange for Hadoop for PowerCenter
- PowerExchange for HBase
- PowerExchange for HDFS
- PowerExchange for Hive
- PowerExchange for JDBC V2
- PowerExchange for Kafka for PowerCenter
- PowerExchange for MapR-DB
- PowerExchange for Microsoft Azure Blob Storage
- PowerExchange for Microsoft Azure Data Lake Storage Gen1
- PowerExchange for Microsoft Azure Data Lake Storage Gen2

파일 설명자 제한 확인

운영 체제가 파일 설명자 요구 사항을 충족하는지 확인합니다.

Informatica 서비스 프로세스에서 많은 파일을 사용할 수 있습니다. 다수의 파일 및 프로세스로 인해 발생하는 오류를 방지하려면 C 셸을 사용하는 경우 **limit** 명령 또는 Bash 셸을 사용하는 경우 **ulimit** 명령을 사용하여 시스템 설정을 변경할 수 있습니다.

운영 체제 설정 목록 표시

파일 설명자 제한 설정을 포함한 운영 체제 설정 목록을 가져오려면 다음 명령을 실행합니다.

C 셸에서 **limit**을 실행합니다.

Bash 셸에서 **ulimit -a**를 실행합니다.

파일 설명자 제한 설정

Informatica 서비스 프로세스에서 많은 파일을 사용할 수 있습니다. 프로세스당 파일 설명자 제한을 16,000 이상으로 설정하십시오. 프로세스당 32,000개의 파일 설명자 제한을 권장합니다.

시스템 설정을 변경하려면 `limit` 또는 `ulimit` 명령을 적절한 플래그 및 값을 사용하여 실행합니다. 예를 들어 파일 설정자 제한을 설정하려면 다음 명령을 실행하십시오.

C 셸에서 `limit -h filesize <값>`을 실행합니다.

Bash 셸에서 `ulimit -n <값>`을 실행합니다.

최대 사용자 프로세스 설정

Informatica 서비스는 많은 수의 사용자 프로세스를 사용합니다. `ulimit -u` 명령을 사용하면 Blaze 엔진에 필요한 모든 프로세스에 적합한 높은 수준으로 최대 사용자 프로세스 수 설정을 조정할 수 있습니다.

최대 사용자 프로세스를 설정하려면 다음 명령을 실행합니다.

C 셸에서 `limit -u processes <값>`을 실행합니다.

Bash 셸에서 `ulimit -u <값>`을 실행합니다.

응용 프로그램 서비스 하드웨어 요구 사항 확인

도메인 노드에 해당 노드에서 실행되는 응용 프로그램 서비스 및 서비스 관리자를 위한 하드웨어가 충분히 있는지 확인합니다.

노드가 1개인 Informatica 도메인을 작성하고 모든 응용 프로그램 서비스를 해당 노드에서 실행할 수 있습니다. 노드가 여러 개인 Informatica 도메인을 작성하면 여러 개별 노드에서 응용 프로그램 서비스를 실행할 수 있습니다. 도메인의 응용 프로그램 서비스를 계획할 경우, 노드에서 실행하는 서비스를 기반으로 시스템 요구 사항을 고려하십시오.

참고: 작업 부하 및 동시 실행 요구 사항에 따라 노드에 코어 및 메모리를 추가하여 성능을 최적화해야 할 수도 있습니다.

다음 테이블에는 몇 가지 공통 구성 시나리오를 기반으로 노드에 필요한 최소 시스템 요구 사항이 나열되어 있습니다. 도메인을 다르게 구성하려면 이 정보를 지침으로 사용하십시오.

서비스	프로세서	메모리	디스크 공간
노드 1개에서 다음 서비스를 실행합니다. - 분석 서비스 - 콘텐츠 관리 서비스 - 데이터 통합 서비스 - Metadata Manager 서비스 - 모델 리포지토리 서비스 - PowerCenter 통합 서비스 - PowerCenter 리포지토리 서비스 - 검색 서비스 - 웹 서비스 협	여러 개의 코어를 포함하는 CPU 2개	12 GB	20 GB
노드 1개에서 다음 서비스를 실행합니다. - 분석 서비스 - 콘텐츠 관리 서비스 - 데이터 통합 서비스 - 모델 리포지토리 서비스 - 검색 서비스	여러 개의 코어를 포함하는 CPU 2개	12 GB	20 GB
노드 1개에서 다음 서비스를 실행합니다. - 분석 서비스	여러 개의 코어를 포함하는 CPU 1개	4GB	해당 없음
노드 1개에서 다음 서비스를 실행합니다. - 검색 서비스	여러 개의 코어를 포함하는 CPU 1개	4GB	10GB

서비스	프로세서	메모리	디스크 공간
노드 1개에서 다음 서비스를 실행합니다. - 분석 서비스 - 검색 서비스	여러 개의 코어를 포함하는 CPU 1개	4GB	10GB
노드 1개에서 다음 서비스를 실행합니다. - Metadata Manager 서비스 - PowerCenter 통합 서비스 - PowerCenter 리포지토리 서비스	여러 개의 코어를 포함하는 CPU 2개	8 GB	10GB
노드 1개에서 다음 서비스를 실행합니다. - Metadata Manager 서비스 - PowerCenter 통합 서비스 - PowerCenter 리포지토리 서비스	여러 개의 코어를 포함하는 CPU 2개	8 GB	10GB
노드 1개에서 다음 서비스를 실행합니다. - PowerCenter 통합 서비스 - PowerCenter 리포지토리 서비스	여러 개의 코어를 포함하는 CPU 1개	4GB	10GB
노드 1개에서 다음 서비스를 실행합니다. - 데이터 통합 서비스 - 모델 리포지토리 서비스	여러 개의 코어를 포함하는 CPU 1개	4GB	10GB
노드 1개에서 다음 서비스를 실행합니다. - 데이터 통합 서비스 - 콘텐츠 관리 서비스	여러 개의 코어를 포함하는 CPU 1개	4GB	10GB
노드 1개에서 다음 서비스를 실행합니다. - Metadata Manager 서비스	여러 개의 코어를 포함하는 CPU 1개	4GB	10GB
노드 1개에서 다음 서비스 구성 요소를 실행합니다. - Metadata Manager 에이전트	여러 개의 코어를 포함하는 CPU 1개	4GB	400 MB
노드 1개에서 다음 서비스를 실행합니다. - 웹 서비스 헵	여러 개의 코어를 포함하는 CPU 1개	4GB	5GB

Data Transformation 파일 백업

설치하기 전에 이전 버전에서 작성된 Data Transformation 파일을 백업해야 합니다. 설치를 완료한 후 파일을 새로운 설치 디렉터리에 복사하여 이전 버전에서와 동일한 리포지토리 및 사용자 지정 글로벌 구성 요소를 가져 오십시오.

다음 테이블에는 백업해야 하는 파일 또는 디렉터리가 나열되어 있습니다.

파일 또는 디렉터리	기본 위치
리포지토리	<Informatica 설치 디렉터리>\DataTransformation\ServiceDB
사용자 지정 글로벌 구성 요소 디렉터리(TGP 파일)	<Informatica 설치 디렉터리>\DataTransformation\autoInclude\user

파일 또는 디렉터리	기본 위치
사용자 지정 글로벌 구성 요소 디렉터리(DLL 및 JAR 파일)	<Informatica 설치 디렉터리>\DataTransformation\externLibs\user
구성 파일	<Informatica 설치 디렉터리>\DataTransformation\CMConfig.xml
라이선스 파일	<Informatica 설치 디렉터리>\DataTransformation\CDELICENSE.cfg

Data Transformation 라이브러리 파일을 복사하지 마십시오. 대신 Data Transformation 라이브러리를 다시 설치하십시오.

POSIX 비동기 I/O 구성

IBM AIX에 Informatica를 설치한 경우 PowerCenter 통합 서비스를 실행할 노드에서 POSIX 비동기 I/O를 사용 가능하게 하십시오. POSIX 비동기 I/O를 사용할 수 없는 경우 IBM AIX 시스템에서 실행되는 PowerCenter 통합 서비스가 시작되지 않을 수 있습니다.

환경 변수 검토

Informatica 설치를 위한 환경 변수를 구성합니다.

다음 테이블에는 검토해야 할 환경 변수가 설명되어 있습니다.

변수	설명
IATEMPDIR	<p>설치 중에 생성되는 임시 파일의 위치입니다. Informatica에서는 임시 파일을 위해 1GB 디스크 공간이 필요합니다.</p> <p>임시 파일을 /tmp 디렉터리에 생성하지 않으려는 경우 이 환경 변수를 구성하십시오.</p> <p>기본값인 /tmp 디렉터를 변경하려면 IATEMPDIR 및 _JAVA_OPTIONS 환경 변수를 새 디렉터리로 설정해야 합니다.</p> <p>예를 들어 IATEMPDIR=/home/user를 내보내도록 변수를 설정합니다.</p> <p>참고: 설치 후에는 IATEMPDIR 변수의 설정을 해제합니다.</p>
_JAVA_OPTIONS	<p>임시 디렉터를 변경하려면 이 환경 변수를 구성합니다.</p> <p>기본값인 /tmp 디렉터를 변경하려면 IATEMPDIR 및 _JAVA_OPTIONS 환경 변수를 새 디렉터리로 설정해야 합니다.</p> <p>예를 들어 _JAVA_OPTIONS=-Djava.io.tmpdir=/home/user를 내보내도록 변수를 설정합니다.</p> <p>참고: 설치 후에는 JAVA_OPTIONS 변수의 설정을 해제합니다.</p>
LANG 및 LC_ALL	<p>터미널 세션에 대해 적절한 문자 인코딩을 설정하려면 로깅을 변경합니다. 예를 들어 인코딩을 프랑스어의 경우 Latin1 또는 ISO-8859-1로 설정하고, 일본어의 경우 EUC-JP 또는 Shift JIS로 설정하고, 중국어 또는 한국어의 경우 UTF-8을 설정하십시오. 문자 인코딩은 UNIX 터미널에 표시되는 문자의 유형을 결정합니다.</p>

변수	설명
DISPLAY	설치 프로그램을 실행하기 전에 DISPLAY 환경을 설정 해제합니다. DISPLAY 환경 변수에 값이 있는 경우 설치가 실패할 수 있습니다.
SKIP_VENDOR_CHECK	Linux 또는 AIX의 설치 프로그램에서 sudo 프롬프트를 제거하도록 환경 변수를 구성합니다. Linux 또는 AIX의 Informatica 서버 설치에서 sudo 프롬프트를 제거하려면 환경 변수를 true로 설정합니다. 참고: sudo 권한이 없는 경우 설치 프로그램을 실행하기 전에 환경 변수를 true로 설정합니다. sudo 권한이 있으면 환경 변수를 설정할 필요가 없습니다.

참고: /tmp 디렉터리에 마운트된 파일 시스템에 NOEXEC 플래그가 설정되어 있지 않아야 합니다.

시스템 사용자 계정 작성

Informatica 서비스를 실행할 사용자 계정을 생성합니다.

Informatica를 설치하기 위해 사용하는 사용자 계정에 설치 디렉터리에 대한 쓰기 권한이 있는지 확인하십시오.

Informatica 서비스를 설치하는 사용자 계정에 Informatica 서비스를 설치할 시스템의 중요한 파일에 대한 액세스 권한 및 사용 권한이 있는지 확인하십시오.

키 저장소 파일 설정

Informatica 서비스를 설치할 때 도메인에 대해 보안 통신을 구성하고 Informatica Administrator(Administrator 도구)에 대한 보안 연결을 설정할 수 있습니다. 이러한 보안 옵션을 구성하는 경우 키 저장소 파일과 트러스트 저장소 파일을 설정해야 합니다.

Informatica 서비스를 설치하기 전에 Informatica 도메인 내에서의 보안 통신을 위한 파일이나 Administrator 도구에 대한 보안 연결을 위한 파일을 설정합니다. 필요한 파일을 생성하려면 다음 프로그램을 사용하면 됩니다.
keytool

keytool을 사용하면 SSL 인증서 또는 CSR(인증서 서명 요청)은 물론, JKS 형식의 키 저장소 및 트러스트 저장소를 생성할 수도 있습니다.

OpenSSL

OpenSSL을 사용하여 SSL 인증서 또는 CSR을 생성하거나 JKS 형식의 키 저장소를 PEM 형식으로 변환할 수 있습니다.

OpenSSL에 대한 자세한 내용은 다음 웹 사이트에서 설명서를 참조하십시오.

<https://www.openssl.org/docs/>

좀 더 높은 보안 수준이 필요한 경우에는 CSR을 CA(인증 기관)로 보내 서명된 인증서를 받습니다.

참조된 링크에서 다운로드할 수 있는 소프트웨어는 Informatica가 아니라 타사에 속합니다. 다운로드 링크에는 오류 또는 누락이 있거나 변경될 수 있습니다. Informatica는 해당 링크 및/또는 해당 소프트웨어에 대한 책임을 지지 않으며, 상품성, 특수 목적에 대한 적합성, 소유권 및 비침해성을 포함하되 이에 제한하지 않고 명시적 또는 묵시적인 모든 보증을 부인하며, 이와 관련된 모든 책임을 부인하는 바입니다.

Informatica 도메인 내에서의 보안 통신

Informatica 도메인 내에서 보안 통신을 활성화하기 전에 다음 요구 사항을 충족하는지 확인합니다.

CSR(인증서 서명 요청)과 개인 키를 작성했습니다.

keytool 또는 OpenSSL을 사용하여 CSR과 개인 키를 작성할 수 있습니다.

RSA 암호화를 사용하는 경우 512비트를 초과하여 사용해야 합니다.

서명된 SSL 인증서가 있습니다.

인증서는 자체 서명되었거나 CA에서 서명했을 수 있습니다. Informatica는 CA 서명 인증서를 권장합니다.

인증서를 키 저장소로 가져왔습니다.

이름이 `infa_keystore.pem`인 PEM 형식의 키 저장소와 이름이 `infa_keystore.jks`인 JKS 형식의 키 저장소가 있어야 합니다.

키 저장소 파일에는 루트 및 중간 SSL 인증서가 포함되어야 합니다.

참고: JKS 형식의 키 저장소에 대한 암호는 SSL 인증서를 생성하는 데 사용되는 개인 키 암호와 동일해야 합니다.

인증서를 트러스트 저장소로 가져왔습니다.

이름이 `infa_truststore.pem`인 PEM 형식의 트러스트 저장소와 이름이 `infa_truststore.jks`인 JKS 형식의 트러스트 저장소가 있어야 합니다.

트러스트 저장소 파일에는 루트, 중간 및 최종 사용자 SSL 인증서가 포함되어야 합니다.

키 저장소 및 트러스트 저장소가 올바른 디렉터리에 있습니다.

키 저장소 및 트러스트 저장소는 설치 프로그램에서 액세스할 수 있는 디렉터리에 있어야 합니다.

Administrator 도구에 사용되는 키 저장소 유형에 따라 콘텐츠 관리 서비스의 키 저장소 유형이 결정됩니다.

Administrator 도구에 기본 키 저장소 인증서를 사용한 경우 콘텐츠 관리 서비스에 대해 기본 또는 사용자 지정 키 저장소 인증서를 사용할 수 있습니다.

Administrator 도구에 사용자 지정 키 저장소 인증서를 사용한 경우 콘텐츠 관리 서비스에 대해 사용자 지정 키 저장소 인증서를 사용해야 합니다.

사용자 지정 키 저장소 및 트러스트 저장소를 생성하는 방법에 대한 자세한 내용은

[Informatica How-To Library article "How to Create Keystore and Truststore Files for Secure Communication in the Informatica Domain"](#) 문서를 참조하십시오.

Administrator 도구에 대한 보안 연결

Administrator 도구에 대한 연결의 보안을 유지하려면 먼저 다음 요구 사항을 충족하는지 확인합니다.

CSR(인증서 서명 요청)과 개인 키를 작성했습니다.

keytool 또는 OpenSSL을 사용하여 CSR과 개인 키를 작성할 수 있습니다.

RSA 암호화를 사용하는 경우 512비트를 초과하여 사용해야 합니다.

서명된 SSL 인증서가 있습니다.

인증서는 자체 서명되었거나 CA에서 서명했을 수 있습니다. Informatica는 CA 서명 인증서를 권장합니다.

인증서를 JKS 형식의 키 저장소로 가져왔습니다.

키 저장소에는 하나의 인증서만 포함되어 있어야 합니다. 각 웹 응용 프로그램 서비스에 대해 고유한 인증서를 사용하는 경우 각 인증서에 대해 별도의 키 저장소를 작성합니다. 또는 공유 인증서 및 키 저장소를 사용할 수 있습니다.

Administrator 도구에 대해 설치 프로그램에서 생성한 SSL 인증서를 사용하는 경우 인증서를 JKS 형식의 키 저장소로 가져올 필요가 없습니다.

키 저장소가 올바른 디렉터리에 있습니다.

키 저장소는 설치 프로그램에서 액세스할 수 있는 디렉터리에 있어야 합니다.

Download and Extract the Installer Files

The installer files are distributed as compressed files. You can get the Informatica installation file and distribution packages from the FTP link contained in your fulfillment email.

Download the Informatica installation tar file and the required distribution package ZIP files from the Informatica Electronic Software Download site. You can download them to a local directory or a shared network drive that is mapped on your machine.

Extract the Informatica installer files to a directory on your machine. The user that runs the installer must have read and write permissions on the installer files directory and execute permissions on the executable file.

참고: Ensure that you extract the installer files to a local directory as you can't run the installer from a mapped file.

Copy the ZIP files of the distribution packages to the following location: <Informatica installer files>/source

참고: The installer fails if the ZIP files for distribution packages aren't available in the source directory.

Verify Installer Code Signing

You can verify the signature of the Informatica software code.

Informatica uses a certificate based digital signature to sign the Informatica software code. The code signing helps to validate the authenticity of the code and ensures that there has been no changes or corruptions to the code after Informatica signs the code. You can determine whether to trust the software based on whether the code sign is present or not.

You can request a code signing certificate that contains information that fully identifies Informatica LLC and a Certificate Authority (CA) that issues the certificate. The digital certificate binds the identity of Informatica to a public key and to a private key.

Digital signing of software begins with the creation of a cryptographic hash, or a digest. The digest has a one to one correspondence with the original data. Use the digest as there are no hints on how to recreate the original data, and even a small change in the original data results in a change in the hash value. Informatica uses its private key to sign the digest, or generates a signature in the form of a string of bits. Good digital signature algorithms allow a user with the public key to verify the creator of the signature.

To Verify the Signed Code is Authentic

After Informatica signs the software bundle, you can contact Informatica Global Customer Support to access the code signing certificate. Informatica ships the installer along with the signature file that contains the hash of the installer binary encrypted with Informatica's private key. You can validate the integrity of digitally signed binaries using any available tools, such as OpenSSL.

For instance, if you have to verify the package authentication and confirm the code security, enter the following OpenSSL commands:

```
openssl base64 -d -in $signature -out /tmp/sign.sha256
openssl dgst -sha256 -verify <(openssl x509 -in <cert> -pubkey -noout) -signature /tmp/sign.sha256 <file>
```

Where <signature> is the file containing the signature in Base64, <cert> is the code signing certificate, and <file> is the file to verify.

Based on verification process, OpenSSL displays a success or error message to validate if the installer code is genuine or not. Note that the verification for the installer might take around two minutes.

Verify Installer Package Checksum on UNIX and Linux

Before you run the services installer, verify the install package integrity through the cksum command. The cksum command calculates the checksum value for the installers.

Verify the checksum for the specific installer files against the checksum of the installation files downloaded from the Informatica Electronic Software Download site.

The following table lists the checksum and file size for the Informatica services installer for UNIX and Linux:

파일	체크섬 값	파일 크기
informatica_1053_server_linux-x64.tar	2154528627	11639828480
informatica_1053_server_aix-ppc64.tar	561493064	10006200320

A checksum mismatch can occur when there are data errors during download due to network issues or when data corruption occurs in the file on disk. For more information about the checksum errors, see [HOW TO: Identify file errors after downloading Informatica installation files.](#)

라이선스 키 확인

소프트웨어를 설치하기 전에 사용 가능한 라이선스 키가 있는지 확인합니다.

Informatica ESD(Electronic Software Download) 사이트에서 설치 파일을 다운로드한 경우 라이선스 키는 Informatica에서 보낸 전자 메일 메시지에 있습니다. 제품을 설치하는 사용자 계정에서 액세스할 수 있는 디렉터리에 라이선스 키 파일을 복사합니다.

라이선스 키가 없는 경우 또는 증분 라이선스 키를 보유하고 있고 도메인을 생성하려는 경우 Informatica 글로벌 고객 지원 센터에 문의하십시오.

제 3 장

Windows에 서비스를 설치하기 전에

이 장에 포함된 항목:

- [Windows에서 서비스를 설치하기 전에 개요, 37](#)
- [릴리스 노트 읽기, 37](#)
- [시스템 요구 사항 확인, 38](#)
- [Data Transformation 파일 백업, 42](#)
- [환경 변수 검토, 42](#)
- [시스템 사용자 계정 작성, 43](#)
- [키 저장소 및 트러스트 저장소 파일 설정, 43](#)
- [Download and Extract the Installer Files, 45](#)
- [라이선스 키 확인, 46](#)

Windows에서 서비스를 설치하기 전에 개요

Informatica 서비스를 설치하기 전에 Informatica 플랫폼 설치 및 실행을 위한 요구 사항을 충족하도록 시스템을 설정하십시오. Informatica 서비스를 설치할 시스템이 올바로 구성되어 있지 않으면 설치에 실패할 수 있습니다.

릴리스 노트 읽기

릴리스 노트에서 설치 및 업그레이드 프로세스에 대한 업데이트를 확인하십시오. 또한 릴리스에 대해 알려지거나 수정된 문제에 대한 정보도 확인할 수 있습니다.

Informatica [documentation portal](#)에서 릴리스 정보를 확인하십시오.

시스템 요구 사항 확인

환경이 설치 프로세스, 임시 디스크 공간, 포트 가용성, 데이터베이스 및 응용 프로그램 서비스 하드웨어에 대한 최소 시스템 요구 사항을 충족하는지 확인하십시오.

제품 요구 사항 및 지원되는 플랫폼에 대한 자세한 내용은 [Product Availability Matrix](#)를 참조하십시오.

임시 디스크 공간 및 사용 권한 확인

환경이 임시 디스크 공간, 임시 파일 권한 및 Informatica 클라이언트 도구에 대한 최소 시스템요구 사항을 충족하는지 확인합니다.

임시 파일의 디스크 공간

설치 프로그램은 하드 디스크에 임시 파일을 씁니다. 설치를 지원할 1GB 디스크 공간이 시스템에 있는지 확인하십시오. 설치가 완료되면 설치 프로그램이 임시 파일을 삭제하고 디스크 공간을 해제합니다.

다음 테이블에는 PowerCenter 또는 Data Engineering 제품 설치에 대한 최소 디스크 공간 및 메모리 요구 사항이 설명되어 있습니다.

옵션	최소 요구 사항
설치 프로그램을 실행하는 데 필요한 임시 디스크 공간	1GB 디스크 공간
Data Engineering 제품에 대한 응용 프로그램 서비스 설치	50GB 디스크 공간, 8GB RAM 및 8개 코어. 50GB 중에서 25GB는 제품 설치 바이너리에 사용됩니다.
PowerCenter에 대한 응용 프로그램 서비스 설치	50GB 디스크 공간, 4GB RAM 및 6개 코어. 50GB 중에서 25GB는 제품 설치 바이너리에 사용됩니다.

임시 파일에 대한 사용 권한

/tmp 디렉터리에 대한 읽기, 쓰기 및 실행 권한이 있어야 합니다.

제품 요구 사항 및 지원되는 플랫폼에 대한 자세한 내용은 [Product Availability Matrix](#)를 참조하십시오.

패치 요구 사항 검토

Informatica 서비스를 설치하기 전에 필요한 운영 체제 패치 및 라이브러리가 시스템에 있는지 확인하십시오.

The following table lists the patches and libraries that the Informatica services require on a Windows platform:

Platform	Operating System	Operating System Patch
Windows x64	2016 64-bit	None required
Windows 2019	2019 64-bit	None required
Windows 2022	2022 64-bit	None required

포트 요구 사항 확인

설치 프로그램에서 Informatica 도메인의 구성 요소에 대한 포트를 설정하고, 일부 응용 프로그램 서비스에 사용할 동적 포트 범위를 지정합니다.

구성 요소에 사용할 포트 번호와 응용 프로그램 서비스에 사용할 동적 포트 번호 범위를 지정할 수 있습니다. 또는 설치 프로그램에서 제공하는 기본 포트 번호를 사용할 수 있습니다. 설치 프로그램을 실행하는 시스템에서 포트 번호를 사용할 수 있는지 확인합니다.

참고: 포트가 충돌할 경우 서비스 및 노드를 시작하지 못할 수 있습니다.

다음 테이블에는 설치를 위한 포트 요구 사항이 설명되어 있습니다.

포트	설명
노드 포트	설치 중에 작성된 노드의 포트 번호입니다. 기본값은 6005입니다.
서비스 관리자 포트	노드에서 서비스 관리자가 사용하는 포트 번호입니다. 서비스 관리자가 이 포트에서 들어오는 연결 요청을 수신합니다. 클라이언트 응용 프로그램은 이 포트를 사용하여 도메인의 서비스와 통신합니다. Informatica 명령줄 프로그램은 이 포트를 사용하여 도메인과 통신합니다. 또한 SQL 데이터 서비스 JDBC/ODBC 드라이버용 포트입니다. 기본값은 6006입니다.
서비스 관리자 종료 포트	도메인 서비스 관리자에 대한 서버 종료를 제어하는 포트 번호입니다. 서비스 관리자는 이 포트에서 종료 명령을 수신합니다. 기본값은 6007입니다.
Informatica Administrator 포트	Informatica Administrator에서 사용하는 포트 번호입니다. 기본값은 6008입니다.
Informatica Administrator 종료 포트	Informatica Administrator에 대한 서버 종료를 제어하는 포트 번호입니다. Informatica Administrator가 이 포트에서 종료 명령을 수신합니다. 기본값은 6009입니다.
최소 포트 번호	이 노드에서 실행되는 응용 프로그램 서비스 프로세스에 할당할 수 있는 동적 포트 번호 범위에서 가장 낮은 포트 번호입니다. 기본값은 6014입니다.
최대 포트 번호	이 노드에서 실행되는 응용 프로그램 서비스 프로세스에 할당할 수 있는 동적 포트 번호 범위에서 가장 높은 포트 번호입니다. 기본값은 6114입니다.
응용 프로그램 서비스용 동적 포트 범위	응용 프로그램 서비스 프로세스가 시작될 때 동적으로 할당할 수 있는 포트 번호 범위입니다. 동적 포트를 사용하는 응용 프로그램 서비스를 시작할 경우 서비스 관리자가 이 범위에서 사용 가능한 첫 번째 포트를 서비스 프로세스에 동적으로 할당합니다. 범위의 포트 수는 노드에서 실행되는 응용 프로그램 서비스 프로세스 수의 두 배 이상이어야 합니다. 기본값은 6014 - 6114입니다. 서비스 관리자는 이 범위의 포트 번호를 모델 리포지토리 서비스에 동적으로 할당합니다.
응용 프로그램 서비스용 정적 포트	정적 포트에는 변경되지 않는 전용 포트 번호가 할당됩니다. 응용 프로그램 서비스를 작성할 경우 기본 포트 번호를 사용하거나 수동으로 포트 번호를 할당할 수 있습니다. 다음 서비스에서 정적 포트 번호를 사용합니다. - 콘텐츠 관리 서비스. HTTP의 경우 기본값은 8105입니다. - 데이터 통합 서비스. HTTP의 경우 기본값은 8095입니다.

포트 구성 지침

설치 프로그램은 도메인 포트 충돌을 방지하기 위해 사용자가 지정한 포트 번호에 대해 유효성 검사를 수행합니다.

다음 지침을 사용하여 포트 번호를 결정하십시오.

- 도메인과 해당 도메인에 있는 각 구성 요소에 대해 지정하는 포트 번호는 고유해야 합니다.
- 도메인과 도메인 구성 요소의 포트 번호는 응용 프로그램 서비스 프로세스에 대해 지정하는 포트 번호 범위 내에 있을 수 없습니다.
- 응용 프로그램 서비스 프로세스에 대해 지정하는 포트 번호 범위에서 가장 높은 번호는 가장 낮은 포트 번호보다 3 이상 커야 합니다. 예를 들어 범위의 최소 포트 번호가 6400이면 최대 포트 번호는 6403 이상이어야 합니다.
- 지정된 포트 번호가 1025보다 낮거나 65535보다 높을 수는 없습니다.

Verify Distribution Package Requirements (Windows)

The Informatica domain and client require the distribution packages to process complex files within the domain or to connect to Hadoop or Databricks environment when you process within the domain.

If you need a distribution package, you can install it through the installer or through Integration Package Manager (the package manager) at any time.

You can use the Cloudera CDP Private Cloud distribution package to process complex files within the Informatica domain or to connect to the Hadoop or Databricks environment when you process within the Informatica domain. However, you can use a different distribution package according to your requirements.

The following adapters require distribution packages for processing within the Informatica domain:

- PowerExchange for Amazon S3
- PowerExchange for Google Cloud Storage
- PowerExchange for Google Cloud Storage for PowerCenter
- PowerExchange for Kafka for PowerCenter
- PowerExchange for Microsoft Azure Blob Storage
- PowerExchange for Microsoft Azure Data Lake Storage Gen1
- PowerExchange for Microsoft Azure Data Lake Storage Gen2

응용 프로그램 서비스 하드웨어 요구 사항 확인

도메인 노드에 해당 노드에서 실행되는 응용 프로그램 서비스 및 서비스 관리자를 위한 하드웨어가 충분히 있는지 확인합니다.

노드가 1개인 Informatica 도메인을 작성하고 모든 응용 프로그램 서비스를 해당 노드에서 실행할 수 있습니다. 노드가 여러 개인 Informatica 도메인을 작성하면 여러 개별 노드에서 응용 프로그램 서비스를 실행할 수 있습니다. 도메인의 응용 프로그램 서비스를 계획할 경우, 노드에서 실행하는 서비스를 기반으로 시스템 요구 사항을 고려하십시오.

참고: 작업 부하 및 동시 실행 요구 사항에 따라 노드에 코어 및 메모리를 추가하여 성능을 최적화해야 할 수도 있습니다.

다음 테이블에는 몇 가지 공통 구성 시나리오를 기반으로 노드에 필요한 최소 시스템 요구 사항이 나열되어 있습니다. 도메인을 다르게 구성하려면 이 정보를 지침으로 사용하십시오.

서비스	프로세서	메모리	디스크 공간
노드 1개에서 다음 서비스를 실행합니다. - 분석 서비스 - 콘텐츠 관리 서비스 - 데이터 통합 서비스 - Metadata Manager 서비스 - 모델 리포지토리 서비스 - PowerCenter 통합 서비스 - PowerCenter 리포지토리 서비스 - 검색 서비스 - 웹 서비스 협	여러 개의 코어를 포함하는 CPU 2개	12 GB	20 GB
노드 1개에서 다음 서비스를 실행합니다. - 분석 서비스 - 콘텐츠 관리 서비스 - 데이터 통합 서비스 - 모델 리포지토리 서비스 - 검색 서비스	여러 개의 코어를 포함하는 CPU 2개	12 GB	20 GB
노드 1개에서 다음 서비스를 실행합니다. - 분석 서비스	여러 개의 코어를 포함하는 CPU 1개	4GB	해당 없음
노드 1개에서 다음 서비스를 실행합니다. - 검색 서비스	여러 개의 코어를 포함하는 CPU 1개	4GB	10GB
노드 1개에서 다음 서비스를 실행합니다. - 분석 서비스 - 검색 서비스	여러 개의 코어를 포함하는 CPU 1개	4GB	10GB
노드 1개에서 다음 서비스를 실행합니다. - Metadata Manager 서비스 - PowerCenter 통합 서비스 - PowerCenter 리포지토리 서비스	여러 개의 코어를 포함하는 CPU 2개	8 GB	10GB
노드 1개에서 다음 서비스를 실행합니다. - Metadata Manager 서비스 - PowerCenter 통합 서비스 - PowerCenter 리포지토리 서비스	여러 개의 코어를 포함하는 CPU 2개	8 GB	10GB
노드 1개에서 다음 서비스를 실행합니다. - PowerCenter 통합 서비스 - PowerCenter 리포지토리 서비스	여러 개의 코어를 포함하는 CPU 1개	4GB	10GB
노드 1개에서 다음 서비스를 실행합니다. - 데이터 통합 서비스 - 모델 리포지토리 서비스	여러 개의 코어를 포함하는 CPU 1개	4GB	10GB
노드 1개에서 다음 서비스를 실행합니다. - 데이터 통합 서비스 - 콘텐츠 관리 서비스	여러 개의 코어를 포함하는 CPU 1개	4GB	10GB
노드 1개에서 다음 서비스를 실행합니다. - Metadata Manager 서비스	여러 개의 코어를 포함하는 CPU 1개	4GB	10GB

서비스	프로세서	메모리	디스크 공간
노드 1개에서 다음 서비스 구성 요소를 실행합니다. - Metadata Manager 에이전트	여러 개의 코어를 포함하는 CPU 1개	4GB	400 MB
노드 1개에서 다음 서비스를 실행합니다. - 웹 서비스 헵	여러 개의 코어를 포함하는 CPU 1개	4GB	5GB

Data Transformation 파일 백업

설치하기 전에 이전 버전에서 작성된 **Data Transformation** 파일을 백업해야 합니다. 설치를 완료한 후 파일을 새로운 설치 디렉터리에 복사하여 이전 버전에서와 동일한 리포지토리 및 사용자 지정 글로벌 구성 요소를 가져 오십시오.

다음 테이블에는 백업해야 하는 파일 또는 디렉터리가 나열되어 있습니다.

파일 또는 디렉터리	기본 위치
리포지토리	<Informatica 설치 디렉터리>\DataTransformation\ServiceDB
사용자 지정 글로벌 구성 요소 디렉터리(TGP 파일)	<Informatica 설치 디렉터리>\DataTransformation\autoInclude\user
사용자 지정 글로벌 구성 요소 디렉터리(DLL 및 JAR 파일)	<Informatica 설치 디렉터리>\DataTransformation\externLibs\user
구성 파일	<Informatica 설치 디렉터리>\DataTransformation\CMConfig.xml
라이선스 파일	<Informatica 설치 디렉터리>\DataTransformation\CDELICENSE.cfg

Data Transformation 라이브러리 파일을 복사하지 마십시오. 대신 **Data Transformation** 라이브러리를 다시 설치하십시오.

환경 변수 검토

Informatica 설치 작업을 위해 환경 변수를 구성하십시오.

다음 테이블에는 Windows에서 검토해야 할 환경 변수가 설명되어 있습니다.

변수	설명
%TEMP%	설치 중에 생성되는 임시 파일의 위치입니다. Informatica에서는 임시 파일을 위해 1GB 디스크 공간이 필요합니다. 임시 파일을 기본 드라이브에 생성하지 않으려면 이 환경 변수를 구성하십시오.
PATH	설치 프로그램이 Informatica에 필요한 파일 경로를 PATH 환경 변수에 추가합니다. PATH 환경 변수의 길이가 시스템 제한을 초과하지 않는지 확인하십시오.

시스템 사용자 계정 작성

설치를 수행하고 Informatica 서비스를 실행하려면 시스템 사용자 계정을 작성하십시오. Informatica 서비스를 설치하기 위해 사용하는 사용자 계정에 설치 디렉터리에 대한 쓰기 권한이 있는지 확인하십시오.

시스템에 로그인한 사용자 계정을 사용하여 Informatica를 설치할 수 있고, Informatica를 다른 사용자 계정에 설치할 수 있습니다. 로컬 계정 또는 도메인 계정을 작성하여 Informatica를 설치하거나 Informatica Windows 서비스를 실행할 수 있습니다.

참고: Windows 신뢰할 수 있는 연결을 사용하는 Microsoft SQL Server에서 리포지토리에 액세스하려면 도메인 계정을 작성합니다.

설치 프로그램을 실행하거나 Informatica Windows 서비스를 실행하려면 사용자 계정에 다음 사용 권한이 필요합니다.

- **로그인한 사용자 계정.** 사용자 계정이 관리자 그룹의 멤버여야 하고 *서비스로 로그인* 사용 권한이 있어야 합니다. Informatica를 설치하기 전에 이 사용자 계정으로 로그인하십시오.
- **다른 사용자 계정.** 사용자 계정이 관리자 그룹의 멤버여야 하고 '서비스로 로그인' 및 '운영 체제의 일부로 활동' 사용 권한이 있어야 합니다. Informatica를 설치하기 전에 이 사용자 계정으로 로그인할 필요가 없습니다. 설치 중에 Informatica Windows 서비스를 실행할 사용자 계정을 지정할 수 있습니다.

키 저장소 및 트러스트 저장소 파일 설정

Informatica 서비스를 설치할 때 도메인에 대해 보안 통신을 구성하고 Informatica Administrator(Administrator 도구)에 대한 보안 연결을 설정할 수 있습니다. 이러한 보안 옵션을 구성하는 경우 키 저장소 파일과 트러스트 저장소 파일을 설정해야 합니다.

Informatica 서비스를 설치하기 전에 Informatica 도메인 내에서의 보안 통신을 위한 파일이나 Administrator 도구에 대한 보안 연결을 위한 파일을 설정합니다. 필요한 파일을 작성하려면 다음 프로그램을 사용하면 됩니다. keytool

keytool을 사용하면 SSL 인증서 또는 CSR(인증서 서명 요청)은 물론, JKS 형식의 키 저장소 및 트러스트 저장소를 작성할 수도 있습니다.

keytool 사용에 대한 자세한 내용은 다음 웹 사이트의 설명서를 참조하십시오.

<http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html>

OpenSSL

OpenSSL을 사용하여 SSL 인증서 또는 CSR을 작성하거나 JKS 형식의 키 저장소를 PEM 형식으로 변환할 수 있습니다.

OpenSSL에 대한 자세한 내용은 다음 웹 사이트에서 설명서를 참조하십시오.

<https://www.openssl.org/docs/>

좀 더 높은 보안 수준이 필요한 경우에는 CSR을 CA(인증 기관)로 보내 서명된 인증서를 받습니다.

참조된 링크에서 다운로드할 수 있는 소프트웨어는 Informatica가 아니라 타사에 속합니다. 다운로드 링크에는 오류 또는 누락이 있거나 변경될 수 있습니다. Informatica는 해당 링크 및/또는 해당 소프트웨어에 대한 책임을 지지 않으며, 상품성, 특수 목적에 대한 적합성, 소유권 및 비침해성을 포함하되 이에 제한하지 않고 명시적 또는 묵시적인 모든 보증을 부인하며, 이와 관련된 모든 책임을 부인하는 바입니다.

Informatica 도메인 내에서의 보안 통신

Informatica 도메인 내에서 보안 통신을 활성화하기 전에 다음 요구 사항을 충족하는지 확인합니다.

CSR(인증서 서명 요청)과 개인 키를 작성했습니다.

keytool 또는 OpenSSL을 사용하여 CSR과 개인 키를 작성할 수 있습니다.

RSA 암호화를 사용하는 경우 512비트를 초과하여 사용해야 합니다.

서명된 SSL 인증서가 있습니다.

인증서는 자체 서명되었거나 CA에서 서명했을 수 있습니다. Informatica는 CA 서명 인증서를 권장합니다.

인증서를 키 저장소로 가져왔습니다.

이름이 `infa_keystore.pem`인 PEM 형식의 키 저장소와 이름이 `infa_keystore.jks`인 JKS 형식의 키 저장소가 있어야 합니다.

키 저장소 파일에는 루트 및 중간 SSL 인증서가 포함되어야 합니다.

참고: JKS 형식의 키 저장소에 대한 암호는 SSL 인증서를 생성하는 데 사용되는 개인 키 암호와 동일해야 합니다.

인증서를 트러스트 저장소로 가져왔습니다.

이름이 `infa_truststore.pem`인 PEM 형식의 트러스트 저장소와 이름이 `infa_truststore.jks`인 JKS 형식의 트러스트 저장소가 있어야 합니다.

트러스트 저장소 파일에는 루트, 중간 및 최종 사용자 SSL 인증서가 포함되어야 합니다.

키 저장소 및 트러스트 저장소가 올바른 디렉터리에 있습니다.

키 저장소 및 트러스트 저장소는 설치 프로그램에서 액세스할 수 있는 디렉터리에 있어야 합니다.

Administrator 도구에 대한 보안 연결

Administrator 도구에 대한 연결의 보안을 유지하려면 먼저 다음 요구 사항을 충족하는지 확인합니다.

CSR(인증서 서명 요청)과 개인 키를 작성했습니다.

keytool 또는 OpenSSL을 사용하여 CSR과 개인 키를 작성할 수 있습니다.

RSA 암호화를 사용하는 경우 512비트를 초과하여 사용해야 합니다.

서명된 SSL 인증서가 있습니다.

인증서는 자체 서명되었거나 CA에서 서명했을 수 있습니다. Informatica는 CA 서명 인증서를 권장합니다.

인증서를 JKS 형식의 키 저장소로 가져왔습니다.

키 저장소에는 하나의 인증서만 포함되어 있어야 합니다. 각 웹 응용 프로그램 서비스에 대해 고유한 인증서를 사용하는 경우 각 인증서에 대해 별도의 키 저장소를 작성합니다. 또는 공유 인증서 및 키 저장소를 사용할 수 있습니다.

Administrator 도구에 대해 설치 프로그램에서 생성한 SSL 인증서를 사용하는 경우 인증서를 JKS 형식의 키 저장소로 가져올 필요가 없습니다.

키 저장소가 올바른 디렉터리에 있습니다.

키 저장소는 설치 프로그램에서 액세스할 수 있는 디렉터리에 있어야 합니다.

Download and Extract the Installer Files

The installer files are distributed as compressed files. You can get the Informatica installation file and distribution packages from the FTP link contained in your fulfillment email.

Download the Informatica installation tar file and the required distribution package ZIP files from the Informatica Electronic Software Download site. You can download them to a local directory or a shared network drive that is mapped on your machine.

Extract the Informatica installer files to a directory on your machine. The user that runs the installer must have read and write permissions on the installer files directory and execute permissions on the executable file.

참고: Ensure that you extract the installer files to a local directory as you can't run the installer from a mapped file.

Copy the ZIP files of the distribution packages to the following location: <Informatica installer files>/source

참고: The installer fails if the ZIP files for distribution packages aren't available in the source directory.

Verify Installer Code Signing

You can verify the signature of the Informatica software code.

Informatica uses a certificate based digital signature to sign the Informatica software code. The code signing helps to validate the authenticity of the code and ensures that there has been no changes or corruptions to the code after Informatica signs the code. You can determine whether to trust the software based on whether the code sign is present or not.

You can request a code signing certificate that contains information that fully identifies Informatica LLC and a Certificate Authority (CA) that issues the certificate. The digital certificate binds the identity of Informatica to a public key and to a private key.

Digital signing of software begins with the creation of a cryptographic hash, or a digest. The digest has a one to one correspondence with the original data. Use the digest as there are no hints on how to recreate the original data, and even a small change in the original data results in a change in the hash value. Informatica uses its private key to sign the digest, or generates a signature in the form of a string of bits. Good digital signature algorithms allow a user with the public key to verify the creator of the signature.

To Verify the Signed Code is Authentic

After Informatica signs the software bundle, you can contact Informatica Global Customer Support to access the code signing certificate. Informatica ships the installer along with the signature file that contains the hash of the installer binary encrypted with Informatica's private key. You can validate the integrity of digitally signed binaries using any available tools, such as OpenSSL.

For instance, if you have to verify the package authentication and confirm the code security, enter the following OpenSSL commands:

```
openssl base64 -d -in $signature -out /tmp/sign.sha256
openssl dgst -sha256 -verify <(openssl x509 -in <cert> -pubkey -noout) -signature /tmp/sign.sha256 <file>
```

Where <signature> is the file containing the signature in Base64, <cert> is the code signing certificate, and <file> is the file to verify.

Based on verification process, OpenSSL displays a success or error message to validate if the installer code is genuine or not. Note that the verification for the installer might take around two minutes.

Verify Installer Package Checksum on Windows

Before you run the services installer, verify the install package integrity through the cksum command. The cksum command calculates the checksum value for the installer.

Verify the checksum for the specific installer files against the checksum of the installation files downloaded from the Informatica Electronic Software Download site.

다음 테이블에는 Windows의 Informatica 서비스에 대한 체크섬 및 파일 크기가 나와 있습니다.

파일	체크섬 값	파일 크기
informatica_1053_server_winem-64t.zip	3333101514	10112422360

A checksum mismatch can occur when there are data errors during download due to network issues or when data corruption occurs in the file on disk. For more information about the checksum errors, see [HOW TO: Identify file errors after downloading Informatica installation files.](#)

라이선스 키 확인

소프트웨어를 설치하기 전에 사용 가능한 라이선스 키가 있는지 확인합니다.

Informatica ESD(Electronic Software Download) 사이트에서 설치 파일을 다운로드한 경우 라이선스 키는 Informatica에서 보낸 전자 메일 메시지에 있습니다. 제품을 설치하는 사용자 계정에서 액세스할 수 있는 디렉터리에 라이선스 키 파일을 복사합니다.

라이선스 키가 없는 경우 또는 증분 라이선스 키를 보유하고 있고 도메인을 생성하려는 경우 Informatica 글로벌 고객 지원 센터에 문의하십시오.

제 4 장

응용 프로그램 서비스 및 데이터베이스 준비

이 장에 포함된 항목:

- [응용 프로그램 서비스 준비를 위한 검사 목록, 47](#)
- [응용 프로그램 서비스 및 데이터베이스 준비 개요, 48](#)
- [데이터베이스 사용자 계정 설정, 48](#)
- [제품별 응용 프로그램 서비스 식별, 48](#)
- [도메인 구성 리포지토리 데이터베이스 요구 사항, 49](#)
- [분석 서비스, 53](#)
- [콘텐츠 관리 서비스, 54](#)
- [데이터 통합 서비스, 56](#)
- [Metadata Manager 서비스, 62](#)
- [모델 리포지토리 서비스, 67](#)
- [모니터링 모델 리포지토리 서비스, 71](#)
- [PowerCenter 통합 서비스, 71](#)
- [PowerCenter 리포지토리 서비스, 72](#)
- [검색 서비스, 75](#)
- [서비스 시스템에서 원시 연결 구성, 76](#)

응용 프로그램 서비스 준비를 위한 검사 목록

이 장에는 Informatica 환경에 필요한 응용 프로그램 서비스 및 데이터베이스에 대한 정보가 포함되어 있습니다. 서비스 계획 및 데이터베이스 준비를 추적하는 데 이 검사 목록을 사용하십시오.

- 환경에 필요한 응용 프로그램 서비스를 식별합니다.
- 설치 프로그램을 통해 생성할 응용 프로그램 서비스를 식별합니다.
- 서비스에 필요한 데이터베이스를 준비합니다.
 - 데이터베이스를 생성합니다.
 - 데이터베이스 사용자를 생성합니다.

- 환경 변수를 생성합니다.
- 연결을 구성합니다.

응용 프로그램 서비스 및 데이터베이스 준비 개요

응용 프로그램 서비스를 계획할 경우, 해당 응용 프로그램 서비스에 연결하는 서비스를 고려해야 합니다. 또한 응용 프로그램 서비스에 필요한 관계형 데이터베이스도 계획해야 합니다.

설치 프로그램은 일부 서비스를 생성할 수 있는 메시지를 설치 중에 표시합니다. 일부 서비스 속성에는 데이터베이스 정보가 필요합니다. 설치 프로그램을 통해 데이터베이스가 필요한 서비스를 생성하려는 경우에는 설치 프로그램을 실행하기 전에 해당 데이터베이스를 준비해야 합니다. 데이터베이스를 준비하려면 데이터베이스 요구 사항을 확인하고, 데이터베이스를 설정하고 사용자 계정을 설정해야 합니다. 데이터베이스 요구 사항은 생성하려는 응용 프로그램 서비스에 따라 다릅니다.

설치 중에 서비스를 생성하지 않은 경우에는 설치 후에 수동으로 생성할 수 있습니다.

데이터베이스 사용자 계정 설정

리포지토리 데이터베이스에 대한 데이터베이스 및 사용자 계정을 설정합니다.

사용자 계정을 설정할 때 다음 규칙과 지침을 사용하십시오.

- 데이터베이스 사용자 계정에는 테이블, 인덱스 및 보기를 생성하고 삭제하는 사용 권한과 테이블에서 데이터를 선택, 삽입, 업데이트, 삭제하는 사용 권한이 있어야 합니다.
- 7비트 ASCII를 사용하여 계정의 암호를 생성합니다.
- 한 리포지토리의 데이터베이스 오류가 다른 리포지토리에 영향을 미치지 않게 하려면 다른 데이터베이스 사용자 계정으로 별도의 데이터베이스 스키마에서 각각의 리포지토리를 생성합니다. 도메인 구성 리포지토리 또는 도메인의 다른 리포지토리나 동일한 데이터베이스 스키마에서 리포지토리를 생성하지 마십시오.

제품별 응용 프로그램 서비스 식별

각 응용 프로그램 서비스는 Informatica 도메인 내에서 서로 다른 기능을 제공합니다. 조직에 대해 생성된 라이선스 키를 기반으로 응용 프로그램 서비스를 생성합니다.

다음 테이블에는 PowerCenter 및 Informatica Data Quality 제품에서 사용할 수 있는 응용 프로그램 서비스가 나열되어 있습니다.

제품	응용 프로그램 서비스
PowerCenter	<ul style="list-style-type: none"> - 분석 서비스 - 콘텐츠 관리 서비스 * - 데이터 통합 서비스 * - Metadata Manager 서비스 - 모델 리포지토리 서비스 * - 모니터링 모델 리포지토리 서비스 * - PowerCenter 통합 서비스 * - PowerCenter 리포지토리 서비스 * - 검색 서비스 - 웹 서비스 협 서비스
Informatica Data Quality	<ul style="list-style-type: none"> - 분석 서비스 - 콘텐츠 관리 서비스 * - 데이터 통합 서비스 * - Metadata Manager 서비스 - 모델 리포지토리 서비스 * - 모니터링 모델 리포지토리 서비스 * - PowerCenter 통합 서비스 * - PowerCenter 리포지토리 서비스 * - 검색 서비스
<p>* 이러한 서비스는 제품을 설치할 때 생성할 수 있습니다. 서비스는 사용하는 제품 버전에 따라 다를 수 있습니다.</p>	

도메인 구성 리포지토리 데이터베이스 요구 사항

Informatica 구성 요소는 관계형 데이터베이스 리포지토리에 메타데이터를 저장합니다. 도메인은 구성 및 사용자 정보를 도메인 구성 리포지토리에 저장합니다.

설치를 실행하기 전에 도메인 구성 리포지토리에 대해 데이터베이스 및 사용자 계정을 설정해야 합니다. 데이터베이스는 Informatica 도메인의 모든 게이트웨이 노드에서 액세스할 수 있어야 합니다.

Informatica를 설치할 때 도메인 구성 리포지토리의 데이터베이스 및 사용자 계정 정보를 제공하십시오. Informatica 설치 프로그램은 JDBC를 사용하여 도메인 구성 리포지토리와 통신합니다.

도메인 구성 리포지토리는 다음 데이터베이스 유형을 지원합니다.

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle
- PostgreSQL
- Sybase ASE

데이터베이스에 대해 200 MB 디스크 공간을 허용합니다.

IBM DB2 데이터베이스 요구 사항

IBM DB2에서 리포지토리를 설정할 때 다음 지침을 사용하십시오.

- 리포지토리가 IBM DB2 데이터베이스에 있는 경우 IBM DB2 버전 10.5가 설치되었는지 확인합니다.
- 데이터베이스를 작성할 IBM DB2 인스턴스에서 다음 매개 변수를 ON으로 설정합니다.
 - DB2_SKIPINSERTED
 - DB2_EVALUNCOMMITTED
 - DB2_SKIPDELETED
 - AUTO_RUNSTATS
- 데이터베이스에서 구성 매개 변수를 설정합니다.
다음 표에는 설정해야 하는 구성 매개 변수가 나열되어 있습니다.

매개 변수	값
logfilsiz	8000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

- 테이블스페이스 **pageSize** 매개 변수를 32768바이트로 설정합니다.
단일 파티션 데이터베이스에서 **pageSize** 요구 사항을 충족하는 테이블스페이스를 지정합니다. 테이블스페이스를 지정하지 않은 경우, 기본 테이블스페이스가 **pageSize** 요구 사항을 충족해야 합니다.
다중 파티션 데이터베이스에서 **pageSize** 요구 사항을 충족하는, 분할되지 않은 테이블스페이스를 지정합니다. 데이터베이스의 카탈로그 파티션에 테이블스페이스를 정의합니다.
- NPAGES 매개 변수를 5000 이상으로 설정합니다. NPAGES 매개 변수는 테이블스페이스의 페이지 수를 결정합니다.
- 데이터베이스 사용자에게 CREATETAB, CONNECT 및 BINDADD 권한이 있는지 확인합니다.
- Informatica는 리포지토리 테이블에 대해 IBM DB2 테이블 별칭을 지원하지 않습니다. 데이터베이스의 테이블에 대해 테이블 별칭이 작성되지 않았는지 확인합니다.
- DataDirect Connect for JDBC 유틸리티에서 DynamicSections 매개 변수를 3000으로 업데이트합니다.
DynamicSections의 기본값은 Informatica 리포지토리에 대해 너무 낮습니다. Informatica에서는 기본값보다 더 큰 DB2 패키지가 필요합니다. 도메인 구성 리포지토리 또는 모델 리포지토리에 대한 DB2 데이터베이스를 설정할 경우 DynamicSections 매개 변수를 3000 이상으로 설정해야 합니다. DynamicSections 매개 변수가 더 낮은 숫자로 설정되어 있으면 Informatica 서비스를 설치하거나 실행할 때 문제가 발생할 수 있습니다.

Microsoft SQL Server 데이터베이스 요구 사항

리포지토리를 설정할 때는 다음 지침을 사용하십시오.

- 잠금 경합을 최소화하려면 스냅숏 격리 허용 및 READ COMMITTED 분리 수준을 ALLOW_SNAPSHOT_ISOLATION 및 READ_COMMITTED_SNAPSHOT으로 설정하십시오. 데이터베이스에 대한 분리 수준을 설정하려면 다음 명령을 실행하십시오.

```
ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
```

데이터베이스에 대한 분리 수준이 올바른지 확인하려면 다음 명령을 실행하십시오.

```
SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
```

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
```
- 데이터베이스 사용자 계정에 CONNECT, CREATE TABLE 및 CREATE VIEW 권한이 있어야 합니다.

Microsoft Azure SQL Database 요구 사항

리포지토리를 설정할 때는 다음 지침을 사용하십시오.

- 잠금 경합을 최소화하려면 스냅숏 격리 허용 및 READ COMMITTED 분리 수준을 ALLOW_SNAPSHOT_ISOLATION 및 READ_COMMITTED_SNAPSHOT으로 설정하십시오. 데이터베이스에 대한 분리 수준을 설정하려면 다음 명령을 실행하십시오.

```
ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
```

데이터베이스에 대한 분리 수준이 올바른지 확인하려면 다음 명령을 실행하십시오.

```
SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
```

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
```
- 데이터베이스 사용자 계정에 CONNECT, CREATE TABLE 및 CREATE VIEW 권한이 있어야 합니다.

Oracle 데이터베이스 요구 사항

Oracle에서 리포지토리를 설정할 경우 다음 지침을 사용하십시오.

- open_cursors 매개 변수를 4000 이상으로 설정하십시오.
- \$parameter 보기에 대한 데이터베이스 사용자의 사용 권한을 설정하십시오.
- Oracle 데이터베이스에서 *show parameter open_cursors*를 실행할 수 있도록 데이터베이스 사용자의 권한을 설정하십시오.
설치 전 시스템 검사 도구(i10Pi)를 실행하는 경우 i10Pi는 데이터베이스에 대해 해당 명령을 실행하여 도메인 데이터베이스 사용자 자격 증명으로 OPEN_CURSORS 매개 변수를 식별합니다.
다음 쿼리를 실행하여 도메인 데이터베이스 사용자 계정에 대한 개방형 커서 설정을 확인할 수 있습니다.

```
SELECT VALUE OPEN_CURSORS FROM V$PARAMETER WHERE UPPER(NAME)=UPPER('OPEN_CURSORS')
```

- 데이터베이스 사용자에게 다음과 같은 권한이 있는지 확인합니다.

```
CREATE SEQUENCE  
CREATE SESSION  
CREATE SYNONYM  
CREATE TABLE  
CREATE VIEW
```

- Informatica에서 리포지토리 테이블에 대한 Oracle 공용 동의어를 지원하지 않습니다. 데이터베이스의 테이블에 대한 공용 동의어가 생성되지 않았는지 확인합니다.

PostgreSQL 데이터베이스 요구 사항

PostgreSQL에서 리포지토리를 설정할 때 다음 지침을 사용하십시오.

- 데이터베이스 사용자 계정에 CONNECT, CREATE TABLE 및 CREATE VIEW 권한이 있는지 확인하십시오.
- PostgreSQL을 데이터베이스로 사용하는 경우 데이터베이스 스키마 이름을 지정합니다.
- PostgreSQL에 데이터 파일에 사용할 충분한 디스크 공간이 있는지 확인하십시오. 기본적으로 데이터 파일은 다음 위치에 있습니다.

<PostgreSQL 설치 디렉터리>/data

- 데이터베이스에서 구성 매개 변수를 설정합니다.

다음 테이블에는 설정해야 하는 구성 매개 변수에 대한 최소 및 권장 값이 나와 있습니다.

매개 변수	최소값	권장 값
max_connections	200	4000
shared_buffers	2GB	16GB
max_locks_per_transaction	1024	1024
max_wal_size	1GB	8GB
checkpoint_timeout	5분	30분

Sybase 데이터베이스 요구 사항

Sybase ASE에서 리포지토리를 설정하는 경우 다음 지침을 사용하십시오.

- 데이터베이스 서버 페이지 크기를 16K 이상으로 설정하십시오. 페이지 크기 설정은 1회성 구성이며 나중에 변경할 수 없으므로 페이지 크기를 16K로 설정해야 합니다.
- 행 수준 잠금을 사용하도록 데이터베이스 잠금 구성을 설정하십시오.

다음 테이블에는 설정해야 하는 데이터베이스 잠금 구성이 설명되어 있습니다.

데이터베이스 구성	Sybase 시스템 프로시저	값
잠금 구성표	sp_configure "lock scheme"	0, datarows

- Sybase 데이터베이스 옵션 "ddl in tran"을 TRUE로 설정하십시오.
- "allow nulls by default"를 TRUE로 설정하십시오.
- Sybase 데이터베이스 옵션 select into/bulkcopy/pllsort를 설정하십시오.
- sysobjects 시스템 테이블에 대해 "select" 권한을 활성화하십시오.
- 다음 로그인 스크립트를 생성하여 기본 VARCHAR 잘라내기를 비활성화하십시오.

```
create procedure dbo.sp_string_rtrunc_proc as set string_rtruncation on
sp_modifylogin "user_name", "login script", sp_string_rtrunc_proc
```

로그인 스크립트는 사용자가 Sybase 인스턴스에 로그인할 때마다 실행됩니다. 이 저장 프로시저는 세션 수준에서 매개 변수를 설정합니다. `sp_modifylogin` 시스템 프로시저는 저장 프로시저를 "login script"로 지정하여 "user_name"을 업데이트합니다. 사용자에게는 저장 프로시저를 호출할 수 있는 사용 권한이 있어야 합니다.

- 데이터베이스 사용자에게 CREATE DEFAULT, CREATE PROCEDURE, CREATE RULE, CREATE TABLE 및 CREATE VIEW 권한이 있는지 확인하십시오.
- 데이터베이스 구성을 권장 기준값으로 설정하십시오.
다음 테이블에는 설정해야 하는 데이터베이스 메모리 구성 매개 변수가 나열되어 있습니다.

데이터베이스 구성	Sybase 시스템 프로시저	값
최대 총 실제 메모리	sp_configure "최대 메모리"	2097151
프로시저 캐시 크기	sp_configure "프로시저 캐시 크기"	500000
열린 개체 수	sp_configure "열린 개체 수"	5000
열린 인덱스 수	sp_configure "열린 인덱스 수"	5000
열린 파티션 수	sp_configure "열린 파티션 수"	5000
사용자당 힙 메모리	sp_configure "사용자당 힙 메모리"	49152
잠금 수	sp_configure "잠금 수"	100000

분석 서비스

분석 서비스는 Analyst 도구를 실행합니다. 이 서비스는 Analyst 도구에 액세스할 수 있는 사용자와 서비스 구성 요소 간의 연결을 관리합니다. 서비스를 생성할 때 서비스를 다른 응용 프로그램 서비스와 연결해야 합니다.

다음 테이블에는 분석 서비스와 관련된 몇 가지 종속성이 요약되어 있습니다.

종속성	요약
제품	<p>분석 서비스를 사용하는 제품은 다음과 같습니다.</p> <ul style="list-style-type: none"> - Data Engineering Integration - Data Engineering Quality - Data Engineering Streaming - Enterprise Data Catalog - Informatica Data Quality - PowerCenter - Test Data Management
서비스	<p>분석 서비스는 다음 서비스와 직접 연결되어야 합니다.</p> <ul style="list-style-type: none"> - 데이터 통합 서비스 - 모델 리포지토리 서비스
데이터베이스	분석 서비스에는 연결된 데이터베이스가 없습니다.
설치 프로그램	분석 서비스는 설치 중에 생성할 수 없습니다.

콘텐츠 관리 서비스

콘텐츠 관리 서비스는 참조 테이블을 사용하는 데이터 도메인을 위해 참조 데이터를 관리합니다. 이 서비스는 데이터 통합 서비스를 통해 매핑을 실행하여 참조 테이블과 외부 데이터 소스 간에 데이터를 전송합니다. 서비스를 생성할 때 서비스를 다른 응용 프로그램 서비스와 연결해야 합니다.

다음 테이블에는 콘텐츠 관리 서비스에 연결된 제품, 서비스 및 데이터베이스에 대한 종속성이 요약되어 있습니다.

종속성	요약
제품	콘텐츠 관리 서비스를 사용하는 제품은 다음과 같습니다. - Data Engineering Quality - Data Privacy Management - Enterprise Data Catalog - 엔터프라이즈 데이터 준비 - Informatica Data Quality - Test Data Management
서비스	콘텐츠 관리 서비스는 다음 서비스와 직접 연결되어야 합니다. - 모델 리포지토리 서비스 - 데이터 통합 서비스
데이터 베이스	콘텐츠 관리 서비스는 다음 데이터베이스를 사용합니다. - 참조 데이터 웨어하우스. 모델 리포지토리에 정의하는 참조 테이블 개체의 데이터 값을 저장합니다. 참조 테이블에 데이터를 추가하면 콘텐츠 관리 서비스가 참조 데이터 웨어하우스의 테이블에 데이터 값을 씁니다.
설치 프로그램	콘텐츠 관리 서비스는 설치 프로그램을 실행할 때 생성할 수 있습니다. 참고: 콘텐츠 관리 서비스는 데이터 관리 서비스와 같은 노드에 생성해야 합니다.

참조 데이터 웨어하우스 요구 사항

참조 데이터 웨어하우스는 사용자가 모델 리포지토리에서 정의하는 참조 테이블 개체에 대한 데이터 값을 저장합니다. 참조 데이터 웨어하우스 및 모델 리포지토리를 식별하도록 콘텐츠 관리 서비스를 구성합니다.

참조 데이터 웨어하우스를 단일 모델 리포지토리와 연결합니다. 콘텐츠 관리 서비스에서 공통 모델 리포지토리를 식별하는 경우 여러 콘텐츠 관리 서비스에 대해 공통 참조 데이터 웨어하우스를 선택할 수 있습니다. 참조 데이터 웨어하우스는 대/소문자가 혼합된 열 이름을 지원해야 합니다.

참조 데이터 웨어하우스는 다음 데이터베이스 유형을 지원합니다.

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle
- JDBC 드라이버를 사용하는 PostgreSQL

데이터베이스에 대해 200 MB 디스크 공간을 허용합니다.

참고: 콘텐츠 관리 서비스를 실행할 시스템에 데이터베이스 클라이언트를 설치해야 합니다.

IBM DB2 데이터베이스 요구 사항

IBM DB2에서 리포지토리를 설정할 때 다음 지침을 사용하십시오.

- 데이터베이스 사용자 계정에 `CREATETAB` 및 `CONNECT` 권한이 있는지 확인합니다.
- 데이터베이스 사용자에게 `SYSCAT.DBAUTH` 및 `SYSCAT.DBTAUTH` 테이블에 대한 `SELECT` 권한이 있는지 확인합니다.
- Informatica는 리포지토리 테이블에 대해 IBM DB2 테이블 별칭을 지원하지 않습니다. 데이터베이스의 테이블에 대해 테이블 별칭이 작성되지 않았는지 확인합니다.
- 테이블스페이스 `pageSize` 매개 변수를 32768바이트로 설정합니다.
- `NPAGES` 매개 변수를 5000 이상으로 설정합니다. `NPAGES` 매개 변수는 테이블스페이스의 페이지 수를 결정합니다.

Microsoft Azure SQL Database 요구 사항

리포지토리를 설정할 때는 다음 지침을 사용하십시오.

- 잠금 경합을 최소화하려면 스냅샷 격리 허용 및 `READ COMMITTED` 분리 수준을 `ALLOW_SNAPSHOT_ISOLATION` 및 `READ_COMMITTED_SNAPSHOT`으로 설정하십시오. 데이터베이스에 대한 분리 수준을 설정하려면 다음 명령을 실행하십시오.

```
ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
```

데이터베이스에 대한 분리 수준이 올바른지 확인하려면 다음 명령을 실행하십시오.

```
SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
```

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
```
- 데이터베이스 사용자 계정에 `CONNECT`, `CREATE TABLE` 및 `CREATE VIEW` 권한이 있어야 합니다.

Microsoft SQL Server 데이터베이스 요구 사항

리포지토리를 설정할 때는 다음 지침을 사용하십시오.

- 데이터베이스 사용자 계정에 `CONNECT` 및 `CREATE TABLE` 권한이 있는지 확인합니다.

Oracle 데이터베이스 요구 사항

Oracle에서 리포지토리를 설정할 경우 다음 지침을 사용하십시오.

- 데이터베이스 사용자에게 다음과 같은 권한이 있는지 확인합니다.

```
ALTER SEQUENCE
```

```
ALTER TABLE
```

```
CREATE SEQUENCE
```

```
CREATE SESSION
```

```
CREATE TABLE
```

```
CREATE VIEW
```

```
DROP SEQUENCE
```

```
DROP TABLE
```
- Informatica에서 리포지토리 테이블에 대한 Oracle 공용 동의어를 지원하지 않습니다. 데이터베이스의 테이블에 대한 공용 동의어가 생성되지 않았는지 확인합니다.

PostgreSQL 데이터베이스 요구 사항

PostgreSQL에서 리포지토리를 설정할 때 다음 지침을 사용하십시오.

- JDBC 연결을 사용하여 PostgreSQL 데이터베이스에 연결합니다.
그러면 데이터베이스에 연결하는 데 사용할 수 있는 PostgreSQL용 DataDirect JDBC 드라이버가 설치됩니다. clients/DeveloperClient/infacmd 설치 디렉터리에서 드라이버를 찾고, 이 드라이버를 clients/externaljdbcjars 디렉터리에 복사합니다.
- 데이터베이스 스키마 이름을 지정합니다. 스키마 이름을 공백으로 두지 마십시오.
데이터베이스가 기본 PostgreSQL 스키마 이름인 public을 사용하는 경우 스키마 이름으로 public을 지정할 수 있습니다.
- 데이터베이스 사용자에게 CONNECT 및 CREATE TABLE 권한이 있는지 확인합니다.

데이터 통합 서비스

데이터 통합 서비스는 Informatica 클라이언트 도구로부터 통합, 프로필 및 데이터 준비 작업에 대한 실행 요청을 받습니다. 이 서비스는 서로 다른 데이터베이스에 결과를 쓰고, 모델 리포지토리에 런타임 메타데이터를 씁니다. 서비스를 생성할 때 서비스에 다른 응용 프로그램 서비스를 연결해야 합니다.

다음 테이블에는 데이터 통합 서비스에 연결된 제품, 서비스 및 데이터베이스에 대한 종속성이 나열되어 있습니다.

종속성	요약
제품	<p>데이터 통합 서비스를 사용하는 제품은 다음과 같습니다.</p> <ul style="list-style-type: none"> - Data Engineering Integration - Data Engineering Quality - Data Engineering Streaming - Data Privacy Management - Enterprise Data Catalog - 엔터프라이즈 데이터 준비 - Informatica Data Quality - PowerCenter - Test Data Management
서비스	<p>데이터 통합 서비스는 다음 서비스와 직접 연결되어야 합니다.</p> <ul style="list-style-type: none"> - 모델 리포지토리 서비스
데이터베이스	<p>데이터 통합 서비스는 다음 데이터베이스를 사용합니다.</p> <ul style="list-style-type: none"> - 데이터 개체 캐시 캐시된 논리적 데이터 개체 및 가상 테이블을 저장합니다. - 프로파일링 웨어하우스. 프로필 결과 및 성과 기록표 결과와 같은 프로파일링 정보를 저장합니다. - 워크플로우 데이터베이스. 워크플로우의 런타임 메타데이터를 저장합니다.
설치 프로그램	<p>설치 프로그램을 실행할 때 데이터 통합 서비스를 생성할 수 있습니다.</p>

데이터 개체 캐시 데이터베이스 요구 사항

데이터 개체 캐시 데이터베이스는 데이터 통합 서비스를 위해 캐싱된 논리적 데이터 개체 및 가상 테이블을 저장합니다. 데이터 통합 서비스를 작성하는 경우 데이터 개체 캐시 데이터베이스 연결을 지정합니다.

데이터 개체 캐시 데이터베이스는 다음 데이터베이스 유형을 지원합니다.

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle

데이터베이스에 대해 200 MB 디스크 공간을 허용합니다.

참고: 데이터 통합 서비스를 실행할 시스템에 데이터베이스 클라이언트를 설치해야 합니다.

IBM DB2 데이터베이스 요구 사항

IBM DB2에서 리포지토리를 설정할 때 다음 지침을 사용하십시오.

- 데이터베이스 사용자 계정에 `CREATETAB` 및 `CONNECT` 권한이 있는지 확인합니다.
- **Informatica**는 리포지토리 테이블에 대해 IBM DB2 테이블 별칭을 지원하지 않습니다. 데이터베이스의 테이블에 대해 테이블 별칭이 작성되지 않았는지 확인합니다.
- 테이블스페이스 `pageSize` 매개 변수를 32768바이트로 설정합니다.
- `NPAGES` 매개 변수를 5000 이상으로 설정합니다. `NPAGES` 매개 변수는 테이블스페이스의 페이지 수를 결정합니다.

Microsoft SQL Server 데이터베이스 요구 사항

리포지토리를 설정할 때는 다음 지침을 사용하십시오.

- 데이터베이스 사용자 계정에 `CONNECT` 및 `CREATE TABLE` 권한이 있는지 확인합니다.

Microsoft Azure SQL Database 요구 사항

리포지토리를 설정할 때는 다음 지침을 사용하십시오.

- 데이터베이스 사용자 계정에 `CONNECT` 및 `CREATE TABLE` 권한이 있는지 확인합니다.

Oracle 데이터베이스 요구 사항

Oracle에서 리포지토리를 설정할 경우 다음 지침을 사용하십시오.

- 데이터베이스 사용자에게 다음과 같은 권한이 있는지 확인합니다.

```
CREATE INDEX
CREATE SESSION
CREATE SYNONYM
CREATE TABLE
CREATE VIEW
DROP TABLE
INSERT INTO TABLE
UPDATE TABLE
```

- Informatica에서 리포지토리 테이블에 대한 Oracle 공용 동의어를 지원하지 않습니다. 데이터베이스의 테이블에 대한 공용 동의어가 생성되지 않았는지 확인합니다.

프로파일링 웨어하우스 요구 사항

프로파일링 웨어하우스 데이터베이스는 프로파일링 및 성과 기록표 결과를 저장합니다. 데이터 통합 서비스를 생성하는 경우 프로파일링 웨어하우스 연결을 지정합니다.

프로파일링 웨어하우스는 다음 데이터베이스 유형을 지원합니다.

- IBM DB2 UDB
- Microsoft SQL Server
- Oracle

데이터베이스에 대해 10 GB 디스크 공간을 허용합니다.

참고: 데이터 통합 서비스를 실행할 시스템에 데이터베이스 클라이언트를 설치해야 합니다. JDBC 연결을 IBM DB2 UDB, Microsoft SQL Server 및 Oracle 데이터베이스 유형에 대한 프로파일링 웨어하우스 연결로 지정할 수 있습니다.

데이터베이스 구성에 대한 자세한 내용은 데이터베이스 시스템에 대한 설명서를 참조하십시오.

IBM DB2 데이터베이스 요구 사항

IBM DB2에서 리포지토리를 설정할 때 다음 지침을 사용하십시오.

- 데이터베이스 사용자 계정에 CREATETAB, CONNECT, CREATE VIEW 및 CREATE FUNCTION 권한이 있어야 합니다.
- Informatica는 리포지토리 테이블에 대해 IBM DB2 테이블 별칭을 지원하지 않습니다. 데이터베이스의 테이블에 대해 테이블 별칭이 작성되지 않았는지 확인합니다.
- 테이블스페이스 pageSize 매개 변수를 32768바이트로 설정합니다.
- NPAGES 매개 변수를 5000 이상으로 설정합니다. NPAGES 매개 변수는 테이블스페이스의 페이지 수를 결정합니다.

참고: 프로파일링 웨어하우스 연결로 JDBC 연결을 사용하는 경우 Informatica는 IBM DB2 데이터베이스에 대한 분할된 데이터베이스 환경을 지원하지 않습니다.

Microsoft SQL Server 데이터베이스 요구 사항

리포지토리를 설정할 때는 다음 지침을 사용하십시오.

- 데이터베이스 사용자 계정에 **CONNECT, CREATE TABLE, CREATE VIEW** 및 **CREATE FUNCTION** 권한이 있어야 합니다.

Oracle 데이터베이스 요구 사항

Oracle에서 리포지토리를 설정할 경우 다음 지침을 사용하십시오.

- 데이터베이스 사용자에게 다음과 같은 권한이 있는지 확인합니다.

ALTER TABLE
CREATE ANY INDEX
CREATE PROCEDURE
CREATE SESSION
CREATE TABLE
CREATE VIEW
DROP TABLE
UPDATE TABLE

- Informatica에서 리포지토리 테이블에 대한 Oracle 공용 동의어를 지원하지 않습니다. 데이터베이스의 테이블에 대한 공용 동의어가 생성되지 않았는지 확인합니다.
- 다음 매개 변수를 Informatica 권장 값으로 설정하십시오.

매개 변수	권장 값
open_cursors	4000
세션	1000
프로세스	1000

워크플로우 데이터베이스 요구 사항

데이터 통합 서비스는 워크플로우의 런타임 메타데이터를 워크플로우 데이터베이스에 저장합니다. 워크플로우 데이터베이스를 생성하기 전에 워크플로우에 데이터베이스에 대한 데이터베이스 및 데이터베이스 사용자 계정을 설정하십시오.

데이터 통합 서비스를 생성할 때 워크플로우 데이터베이스 연결을 지정합니다.

워크플로우 데이터베이스는 다음 데이터베이스 유형을 지원합니다.

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle
- PostgreSQL

데이터베이스에 대해 200 MB 디스크 공간을 허용합니다.

참고: 데이터 통합 서비스를 실행할 시스템에 데이터베이스 클라이언트를 설치해야 합니다.

IBM DB2 데이터베이스 요구 사항

IBM DB2에서 리포지토리를 설정할 때 다음 지침을 사용하십시오.

- 데이터베이스 사용자 계정에 **CREATETAB** 및 **CONNECT** 권한이 있는지 확인합니다.
- Informatica는 리포지토리 테이블에 대해 IBM DB2 테이블 별칭을 지원하지 않습니다. 데이터베이스의 테이블에 대해 테이블 별칭이 작성되지 않았는지 확인합니다.
- 테이블스페이스 **pageSize** 매개 변수를 32768바이트로 설정합니다.
- NPAGES 매개 변수를 5000 이상으로 설정합니다. NPAGES 매개 변수는 테이블스페이스의 페이지 수를 결정합니다.
- 연결 풀링 매개 변수를 설정합니다.

다음 표에는 설정해야 하는 연결 풀링 매개 변수가 나열되어 있습니다.

매개 변수	값
최대 연결 풀 크기	128
최소 연결 풀 크기	0
최대 유휴 시간	120초

Microsoft Azure SQL Database 요구 사항

리포지토리를 설정할 때는 다음 지침을 사용하십시오.

- 잠금 경합을 최소화하려면 스냅샷 격리 허용 및 **READ COMMITTED** 분리 수준을 **ALLOW_SNAPSHOT_ISOLATION** 및 **READ_COMMITTED_SNAPSHOT**으로 설정하십시오. 데이터베이스에 대한 분리 수준을 설정하려면 다음 명령을 실행하십시오.

```
ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
```

데이터베이스에 대한 분리 수준이 올바른지 확인하려면 다음 명령을 실행하십시오.

```
SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
```

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
```

- 데이터베이스 사용자 계정에 **CONNECT**, **CREATE TABLE** 및 **CREATE VIEW** 권한이 있어야 합니다.

Microsoft SQL Server 데이터베이스 요구 사항

리포지토리를 설정할 때는 다음 지침을 사용하십시오.

- 데이터베이스 사용자 계정에 **CONNECT** 및 **CREATE TABLE** 권한이 있는지 확인합니다.
- 연결 풀링 매개 변수를 설정합니다.

다음 표에는 설정해야 하는 연결 풀링 매개 변수가 나열되어 있습니다.

매개 변수	값
최대 연결 풀 크기	128
최소 연결 풀 크기	0
최대 유휴 시간	120초

Oracle 데이터베이스 요구 사항

Oracle에서 리포지토리를 설정할 경우 다음 지침을 사용하십시오.

- 데이터베이스 사용자에게 다음과 같은 권한이 있는지 확인합니다.

```
ALTER TABLE
ALTER VIEW
CREATE SEQUENCE
CREATE SESSION
CREATE SYNONYM
CREATE TABLE
CREATE VIEW
DROP TABLE
DROP VIEW
```

- Informatica에서 리포지토리 테이블에 대한 Oracle 공용 동의어를 지원하지 않습니다. 데이터베이스의 테이블에 대한 공용 동의어가 생성되지 않았는지 확인합니다.
- 연결 풀링 매개 변수를 설정합니다.

다음 표에는 설정해야 하는 연결 풀링 매개 변수가 나열되어 있습니다.

매개 변수	값
최대 연결 풀 크기	128
최소 연결 풀 크기	0
최대 유휴 시간	120초

PostgreSQL 데이터베이스 요구 사항

PostgreSQL에서 리포지토리를 설정할 때 다음 지침을 사용하십시오.

- JDBC 연결을 사용하여 PostgreSQL 데이터베이스에 연결합니다.
- 데이터베이스 사용자 계정에 CONNECT, CREATE TABLE 및 CREATE VIEW 권한이 있는지 확인하십시오.
- PostgreSQL을 데이터베이스로 사용하는 경우 데이터베이스 스키마 이름을 지정합니다.
- PostgreSQL에 데이터 파일에 사용할 충분한 디스크 공간이 있는지 확인하십시오. 기본적으로 데이터 파일은 다음 위치에 있습니다.

<PostgreSQL 설치 디렉터리>/data

- 데이터베이스에서 구성 매개 변수를 설정합니다.

다음 테이블에는 설정해야 하는 구성 매개 변수에 대한 최소 및 권장 값이 나와 있습니다.

매개 변수	최소값	권장 값
max_connections	200	4000
shared_buffers	2GB	16GB
max_locks_per_transaction	1024	1024
max_wal_size	1GB	8GB
checkpoint_timeout	5분	30분

Metadata Manager 서비스

Metadata Manager 서비스는 Informatica 도메인에서 Metadata Manager 웹 클라이언트를 실행합니다.

Metadata Manager 서비스는 Metadata Manager에 액세스할 수 있는 사용자와 서비스 구성 요소 간의 연결을 관리합니다.

다음 테이블에는 Metadata Manager 서비스에 연결된 제품, 서비스 및 데이터베이스에 대한 종속성이 요약되어 있습니다.

종속성	요약
제품	Metadata Manager 서비스를 사용하는 제품은 다음과 같습니다. - Informatica Data Quality - PowerCenter
서비스	Metadata Manager 서비스는 다음 서비스에 직접 연결되어야 합니다. - PowerCenter 통합 서비스 - PowerCenter 리포지토리 서비스
데이터베이스	Metadata Manager 서비스는 다음 데이터베이스를 사용합니다. - Metadata Manager 리포지토리. Metadata Manager 웨어하우스 및 메타데이터 모델을 저장합니다.
설치 프로그램	Metadata Manager 서비스는 설치 프로그램을 실행할 때 생성할 수 없습니다. 이 서비스는 설치가 완료된 후에 생성해야 합니다.

Metadata Manager 리포지토리 데이터베이스 요구 사항

Metadata Manager 리포지토리는 개별 메타데이터 소스의 메타데이터를 저장하는 관계형 데이터베이스의 중앙 위치입니다. 여기에는 Metadata Manager 웨어하우스 및 각 메타데이터 소스 유형에 대한 모델도 저장됩니다. 모든 Metadata Manager 응용 프로그램은 하나의 Metadata Manager 리포지토리에서 실행되도록 구성되어 있습니다.

Metadata Manager 리포지토리는 다음 데이터베이스 유형을 지원합니다.

- IBM DB2 UDB

- Microsoft SQL Server
- Oracle

데이터베이스에 대해 1 GB 디스크 공간을 허용합니다.

IBM DB2 데이터베이스 요구 사항

IBM DB2에서 리포지토리를 설정할 때 다음 지침을 사용하십시오.

- 리포지토리를 작성하는 데이터베이스 사용자 계정은 다음 작업을 수행할 수 있는 권한이 있어야 합니다.

```
ALTER TABLE
CREATE FUNCTION
CREATE INDEX
CREATE PROCEDURE
CREATE TABLE
CREATE VIEW
DROP PROCEDURE
DROP TABLE
INSERT INTO
```

- 리포지토리를 작성하는 데이터베이스 사용자는 페이지 크기가 32KB인 테이블스페이스를 작성할 수 있어야 합니다.
- 기본 페이지 크기(4KB)보다 큰 시스템 임시 테이블스페이스를 설정하고 힙 크기를 업데이트하십시오. 4KB보다 큰 페이지 크기로 정의된 테이블스페이스의 테이블에 대해 실행 중인 쿼리에는 4KB보다 큰 페이지 크기를 가진 시스템 임시 테이블스페이스가 필요합니다. 더 큰 페이지 크기로 정의된 시스템 임시 테이블스페이스가 없는 경우 쿼리가 실패할 수 있습니다. 서버에서 다음 오류를 표시합니다.

```
SQL 1585N A system temporary table space with sufficient page size does not exist. SQLSTATE=54048
```

페이지 크기가 8KB, 16KB 및 32KB인 시스템 임시 테이블스페이스를 작성하십시오. 각 데이터베이스에서 다음 SQL 문을 실행하여 시스템 임시 테이블스페이스를 구성하고 힙 크기를 업데이트하십시오.

```
CREATE Bufferpool RBF IMMEDIATE SIZE 1000 PAGESIZE 32 K EXTENDED STORAGE ;
CREATE Bufferpool STBF IMMEDIATE SIZE 2000 PAGESIZE 32 K EXTENDED STORAGE ;
CREATE REGULAR TABLESPACE REGTS32 PAGESIZE 32 K MANAGED BY SYSTEM USING ('C:\DB2\NODE0000\reg32' )
EXTENTSIZE 16 OVERHEAD 10.5 PREFETCHSIZE 16 TRANSFERRATE 0.33 BUFFERPOOL RBF;
CREATE SYSTEM TEMPORARY TABLESPACE TEMP32 PAGESIZE 32 K MANAGED BY SYSTEM USING
('C:\DB2\NODE0000\temp32' ) EXTENTSIZE 16 OVERHEAD 10.5 PREFETCHSIZE 16 TRANSFERRATE 0.33 BUFFERPOOL
STBF;
GRANT USE OF TABLESPACE REGTS32 TO USER <USERNAME>;
UPDATE DB CFG FOR <DB NAME> USING APP_CTL_HEAP_SZ 16384
UPDATE DB CFG FOR <DB NAME> USING APPLHEAPSZ 16384
UPDATE DBM CFG USING QUERY_HEAP_SZ 8000
UPDATE DB CFG FOR <DB NAME> USING LOGPRIMARY 100
UPDATE DB CFG FOR <DB NAME> USING LOGFILSIZ 2000
UPDATE DB CFG FOR <DB NAME> USING LOCKLIST 1000
UPDATE DB CFG FOR <DB NAME> USING DBHEAP 2400
"FORCE APPLICATIONS ALL"
DB2STOP
DB2START
```

- IBM DB2에서 메타데이터를 Metadata Manager 리포지토리에 로드할 경우 교착 상태를 방지하려면 잠금 매개 변수를 설정하십시오.

다음 테이블에는 구성할 수 있는 잠금 매개 변수가 나열되어 있습니다.

매개 변수 이름	값	IBM DB2 설명
LOCKLIST	8192	잠금 목록의 최대 저장소(4KB)
MAXLOCKS	10	응용 프로그램별 잠금 목록 비율
LOCKTIMEOUT	300	잠금 제한 시간(초)
DLCHKTIME	10000	교착 상태를 확인하는 간격(ms)

IBM DB2 9.7 및 이전 버전의 경우, 읽기 정책을 반복 가능한 읽기에서 읽기 안정성으로 변경하려면 DB2_RR_TO_RS 매개 변수를 YES로 설정하십시오.

- Informatica는 리포지토리 테이블에 대해 IBM DB2 테이블 별칭을 지원하지 않습니다. 데이터베이스의 테이블에 대해 테이블 별칭이 작성되지 않았는지 확인합니다.

참고: IBM DB2를 메타데이터 소스로 사용할 경우 소스 데이터베이스의 구성 요구 사항이 동일합니다.

Microsoft SQL Server 데이터베이스 요구 사항

리포지토리를 설정할 때는 다음 지침을 사용하십시오.

- 리포지토리를 작성하는 데이터베이스 사용자 계정에는 다음 작업을 수행할 수 있는 권한이 있어야 합니다.

```
ALTER TABLE
CREATE CLUSTERED INDEX
CREATE INDEX
CREATE PROCEDURE
CREATE TABLE
CREATE VIEW
DROP PROCEDURE
DROP TABLE
INSERT INTO
```

- 리포지토리가 다중 바이트 언어로 메타데이터를 저장해야 하는 경우, Microsoft SQL Server를 설치할 때 데이터베이스 정렬을 해당 다중 바이트 언어로 설정합니다. 예를 들어 리포지토리가 일본어로 메타데이터를 저장해야 하는 경우 Microsoft SQL Server를 설치할 때 데이터베이스 정렬 옵션을 일본어 정렬로 설정합니다. 이는 1회성 구성이며 변경될 수 없습니다.

Oracle 데이터베이스 요구 사항

Oracle에서 리포지토리를 설정할 경우 다음 지침을 사용하십시오.

- 데이터베이스 사용자에게 다음과 같은 권한이 있는지 확인합니다.

ALTER TABLE
CREATE CLUSTER
CREATE INDEX
CREATE OR REPLACE FORCE VIEW
CREATE OR REPLACE PROCEDURE
CREATE OR REPLACE VIEW
CREATE SESSION
CREATE TABLE
DROP TABLE
INSERT INTO TABLE

- Oracle에서 테이블스페이스에 대해 다음 매개 변수를 설정하십시오.

<임시 테이블스페이스>

2GB 이상 크기로 조정하십시오.

CURSOR_SHARING

FORCE로 설정하십시오.

MEMORY_TARGET

4GB 이상으로 설정하십시오.

SELECT * FROM v\$memory_target_advice ORDER BY memory_size; 를 실행하여 최적의 MEMORY_SIZE를 확인하십시오.

MEMORY_MAX_TARGET

MEMORY_TARGET 크기 이상으로 설정하십시오.

MEMORY_MAX_TARGET이 지정되지 않은 경우 MEMORY_MAX_TARGET이 MEMORY_TARGET 설정으로 기본값 설정됩니다.

OPEN_CURSORS

3000 공유로 설정하십시오.

개방형 커서를 모니터링 및 조정하십시오. v\$sesstat를 쿼리하여 현재 개방된 커서 개수를 확인하십시오. 실행 중인 세션이 한계에 가까울 경우 OPEN_CURSORS 값을 늘리십시오.

UNDO_MANAGEMENT

AUTO로 설정하십시오.

- 리포지토리에서 다중 바이트 언어로 메타데이터를 저장해야 할 경우 데이터베이스 인스턴스에서 NLS_LENGTH_SEMANTICS 매개 변수를 CHAR로 설정하십시오. 기본값은 BYTE입니다.
- Informatica에서 리포지토리 테이블에 대한 Oracle 공용 동의어를 지원하지 않습니다. 데이터베이스의 테이블에 대한 공용 동의어가 생성되지 않았는지 확인합니다.

Metadata Manager를 위한 분할 도메인

제품 번들에 Metadata Manager가 포함되는 경우 한 도메인을 작성할지 분할 도메인을 작성할지를 결정해야 합니다. 분할 도메인에서는 제품 번들의 기본 구성 요소에 연결된 응용 프로그램 서비스가 한 도메인에서 실행되고 Metadata Manager에 연결된 응용 프로그램 서비스는 별개의 도메인에서 실행됩니다.

분할 도메인을 구성하는 경우 제품 번들의 기본 구성 요소를 업그레이드하지 않고 Metadata Manager를 업그레이드할 수 있습니다. Metadata Manager는 다른 구성 요소보다 최신인 제품 버전에서 실행될 수 있습니다.

예를 들어 제품 번들에 PowerCenter와 Metadata Manager가 포함되어 있습니다. 분할 도메인에서 PowerCenter에 연결된 응용 프로그램 서비스는 기본 도메인에서 실행되고 Metadata Manager에 연결된 응용 프로그램 서비스는 보조 도메인에서 실행됩니다. Metadata Manager를 업그레이드하려면 보조 도메인에서 제품 구성 요소를 업그레이드합니다. PowerCenter를 동시에 업그레이드할 필요 없이 Metadata Manager를 업그레이드할 수 있습니다.

각 도메인을 작성하려면 Informatica 서비스 설치 프로그램을 개별적으로 실행합니다. 개별 시스템에 각 도메인을 작성하거나 두 도메인을 하나의 시스템에 작성할 수 있습니다.

분할 도메인 고려 사항

분할 도메인 작성을 결정하기 전에 이점 및 가능한 문제를 고려하십시오.

분할 도메인의 주요 이점은 Metadata Manager의 잦은 업그레이드를 지원한다는 데 있습니다. 제품 번들의 다른 구성 요소를 동시에 업그레이드하지 않고 Metadata Manager를 업그레이드할 수 있습니다. 따라서 데이터 통합 작업과 같은 기본 도메인의 활동에 영향을 미치지 않고 Metadata Manager의 새 기능 및 버그 픽스를 사용할 수 있습니다. Metadata Manager를 업그레이드하는 동안 기본 도메인이 완벽히 작동하는 상태로 유지됩니다.

그러나 다음 문제도 고려해야 합니다.

분할 도메인 구성은 단일 도메인 구성보다 복잡합니다.

분할 도메인에서는 중복된 서비스, 리포지토리 및 사용자를 작성해야 합니다. 두 도메인을 동일한 시스템에 설치하는 경우 각 도메인의 구성 요소에 대한 포트가 충돌하지 않는지 확인해야 합니다. 각 도메인에서 서로 다른 Informatica 버전을 실행하는 경우 데이터베이스 버전이 충돌할 가능성도 고려해야 합니다. 예를 들어 다른 Informatica 제품 버전에 대한 PowerCenter 리포지토리를 동일한 Oracle 데이터베이스에 작성하는 경우 두 Informatica 제품 버전이 Oracle 데이터베이스 버전을 지원하는지 확인해야 합니다.

라이선스 영향이 발생할 수 있습니다.

Informatica 제품을 데이터 통합에 사용하는 경우 일반적으로 사용권 계약에 따라 하나의 도메인에서만 데이터 통합 활동을 수행할 수 있습니다. 사용권 계약에 따라 응용 프로그램 서비스를 작성할 수 있는 시스템의 수 또는 중복할 수 있는 서비스 유형이 제한될 수 있습니다. 또한 각 도메인에 대한 개별 라이선스 파일이 필요할 수 있습니다.

라이선스에 대한 질문은 Informatica 제품 담당자에게 문의하십시오.

추가 데이터베이스 스키마 및 사용자 계정이 필요합니다.

분할 도메인에서는 중복 리포지토리를 작성해야 합니다. 예를 들어 각 도메인에 도메인 구성 리포지토리를 작성합니다. PowerCenter 및 Metadata Manager를 개별 도메인에서 실행하는 경우 각 도메인에 PowerCenter 리포지토리도 작성해야 합니다.

각 리포지토리는 개별 스키마에 있어야 합니다. 또한 각 도메인 구성 리포지토리에 대한 개별 데이터베이스 사용자 계정이 필요합니다.

추가 RAM 및 디스크 공간이 필요합니다.

Informatica 서비스를 설치할 때 두 도메인에 필요한 RAM 및 디스크 공간의 양은 한 도메인에 필요한 양의 두 배입니다.

제품 버전과 관련된 제한이 있습니다.

분할 도메인에서 보조 도메인의 구성 요소는 기본 도메인의 구성 요소와 동일한 버전 또는 이후 버전의 Informatica 제품을 실행할 수 있습니다. 따라서 PowerCenter보다 이후 버전의 Metadata Manager를 실행할 수 있습니다. 그러나 Metadata Manager보다 이후 버전의 PowerCenter는 실행할 수 없습니다.

각 도메인에서 다른 버전의 PowerCenter 클라이언트를 실행해야 할 수 있습니다.

예를 들어 기본 도메인의 PowerCenter 클라이언트를 실행하여 데이터 통합 작업을 수행합니다. 보조 도메인에서 이후 버전의 Metadata Manager를 실행합니다. 이때 Metadata Manager 리소스 로드에서 세션 로그를 보려면 보조 도메인에서 이후 버전의 PowerCenter 클라이언트를 실행해야 합니다.

PowerCenter Designer에서 Metadata Manager 데이터 연계에 액세스할 수 없습니다.

분할 도메인에서 기본 도메인의 PowerCenter 서비스는 보조 도메인의 Metadata Manager 서비스와 통신하지 않습니다. 따라서 PowerCenter Designer에서 Metadata Manager 데이터 연계에 액세스할 수 없습니다.

모델 리포지토리 서비스

모델 리포지토리 서비스는 모델 리포지토리를 관리합니다. 이 서비스는 Informatica 클라이언트 및 응용 프로그램 서비스의 요청을 받아서 모델 리포지토리에서 메타데이터에 저장하거나 액세스합니다.

다음 테이블에는 모델 리포지토리 서비스에 연결된 제품, 서비스 및 데이터베이스에 대한 종속성이 요약되어 있습니다.

종속성	요약
제품	모델 리포지토리 서비스를 사용하는 제품은 다음과 같습니다. <ul style="list-style-type: none"> - Data Engineering Integration - Data Engineering Quality - Data Engineering Streaming - Data Privacy Management - Enterprise Data Catalog - 엔터프라이즈 데이터 준비 - Informatica Data Quality - PowerCenter - Test Data Management
서비스	모델 리포지토리 서비스는 다른 응용 프로그램 서비스와 연결할 필요가 없습니다.
데이터베이스	모델 리포지토리 서비스는 다음 데이터베이스를 사용합니다. <ul style="list-style-type: none"> - 모델 리포지토리. Informatica 클라이언트 및 응용 프로그램 서비스가 생성한 메타데이터를 저장합니다.
설치 프로그램	모델 리포지토리 서비스는 설치 프로그램을 실행할 때 생성할 수 있습니다.

모델 리포지토리 데이터베이스 요구 사항

Informatica 서비스 및 클라이언트는 데이터와 메타데이터를 모델 리포지토리에 저장합니다. 임시 작업, 응용 프로그램, 논리적 데이터 개체, SQL 데이터 서비스, 웹 서비스 및 워크플로우에 대한 통계를 모니터링 모델 리포지토리를 구성합니다. 모델 리포지토리 서비스를 생성하기 전에 모델 리포지토리에 대해 데이터베이스 및 데이

터베이스 사용자 계정을 설정하십시오. 모델 리포지토리와 모니터링 모델 리포지토리에 대해 서로 다른 데이터베이스 구성을 사용하는 것이 좋습니다.

모델 리포지토리는 다음 데이터베이스 유형을 지원합니다.

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle
- PostgreSQL

Microsoft SQL Server를 구성할 때 Microsoft Azure SQL 데이터베이스를 모델 리포지토리로 구성하도록 선택할 수 있습니다.

Microsoft SQL Server에서 모델 리포지토리 데이터베이스에 대한 Windows NT 자격 증명을 지정한 경우 또한 NTLM을 인증 방법으로 포함하도록 연결 문자열 구문을 지정해야 합니다.

DB2에 대해 3GB 디스크 공간을 허용합니다. 다른 모든 데이터베이스 유형에 대해 200MB 디스크 공간을 허용합니다.

데이터베이스 구성에 대한 자세한 내용은 데이터베이스 시스템에 대한 설명서를 참조하십시오.

IBM DB2 데이터베이스 요구 사항

IBM DB2에서 리포지토리를 설정할 때 다음 지침을 사용하십시오.

- IBM DB2를 모델 리포지토리 데이터베이스로 사용하는 경우 테이블스페이스 이름을 지정합니다.
- 리포지토리가 IBM DB2 데이터베이스에 있는 경우 IBM DB2 버전 10.5가 설치되었는지 확인합니다.
- 데이터베이스를 작성할 IBM DB2 인스턴스에서 다음 매개 변수를 ON으로 설정합니다.
 - DB2_SKIPINSERTED
 - DB2_EVALUNCOMMITTED
 - DB2_SKIPDELETED
 - AUTO_RUNSTATS
- 데이터베이스에서 구성 매개 변수를 설정합니다.

다음 표에는 설정해야 하는 구성 매개 변수가 나열되어 있습니다.

매개 변수	값
logfilsiz	8000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

- 테이블스페이스 **pageSize** 매개 변수를 32768바이트로 설정합니다.
단일 파티션 데이터베이스에서 **pageSize** 요구 사항을 충족하는 테이블스페이스를 지정합니다. 테이블스페이스를 지정하지 않은 경우, 기본 테이블스페이스가 **pageSize** 요구 사항을 충족해야 합니다.
다중 파티션 데이터베이스에서 **pageSize** 요구 사항을 충족하는, 분할되지 않은 테이블스페이스를 지정합니다. 데이터베이스의 카탈로그 파티션에 테이블스페이스를 정의합니다.

- NPAGES 매개 변수를 5000 이상으로 설정합니다. NPAGES 매개 변수는 테이블스페이스의 페이지 수를 결정합니다.
- 데이터베이스 사용자에게 CREATETAB, CONNECT 및 BINDADD 권한이 있는지 확인합니다.
- Informatica는 리포지토리 테이블에 대해 IBM DB2 테이블 별칭을 지원하지 않습니다. 데이터베이스의 테이블에 대해 테이블 별칭이 작성되지 않았는지 확인합니다.
- DataDirect Connect for JDBC 유틸리티에서 DynamicSections 매개 변수를 3000으로 업데이트합니다. DynamicSections의 기본값은 Informatica 리포지토리에 대해 너무 낮습니다. Informatica에서는 기본값보다 더 큰 DB2 패키지가 필요합니다. 도메인 구성 리포지토리 또는 모델 리포지토리에 대한 DB2 데이터베이스를 설정할 경우 DynamicSections 매개 변수를 3000 이상으로 설정해야 합니다. DynamicSections 매개 변수가 더 낮은 숫자로 설정되어 있으면 Informatica 서비스를 설치하거나 실행할 때 문제가 발생할 수 있습니다.

Microsoft Azure SQL Database 요구 사항

리포지토리를 설정할 때는 다음 지침을 사용하십시오.

- 잠금 경합을 최소화하려면 스냅샷 격리 허용 및 READ COMMITTED 분리 수준을 ALLOW_SNAPSHOT_ISOLATION 및 READ_COMMITTED_SNAPSHOT으로 설정하십시오. 데이터베이스에 대한 분리 수준을 설정하려면 다음 명령을 실행하십시오.

```
ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
```

데이터베이스에 대한 분리 수준이 올바른지 확인하려면 다음 명령을 실행하십시오.

```
SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
```

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
```
- 데이터베이스 사용자 계정에 CONNECT, CREATE TABLE 및 CREATE VIEW 권한이 있어야 합니다.

참고: Active Directory 인증을 사용하는 Azure SQL Database에 대한 리포지토리를 설정하는 지침은 동일합니다.

Microsoft SQL Server 데이터베이스 요구 사항

리포지토리를 설정할 때는 다음 지침을 사용하십시오.

- Microsoft SQL Server를 모델 리포지토리 데이터베이스로 사용하는 경우 데이터베이스 스키마 이름을 지정합니다.
- 잠금 경합을 최소화하려면 스냅샷 격리 허용 및 READ COMMITTED 분리 수준을 ALLOW_SNAPSHOT_ISOLATION 및 READ_COMMITTED_SNAPSHOT으로 설정하십시오. 데이터베이스에 대한 분리 수준을 설정하려면 다음 명령을 실행하십시오.

```
ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
```

데이터베이스에 대한 분리 수준이 올바른지 확인하려면 다음 명령을 실행하십시오.

```
SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
```

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
```
- 데이터베이스 사용자 계정에 CONNECT, CREATE TABLE 및 CREATE VIEW 권한이 있어야 합니다.

참고: Microsoft Azure SQL Database와 Active Directory 인증을 사용하는 Azure SQL Database에 대한 리포지토리를 설정하는 지침은 동일합니다.

Oracle 데이터베이스 요구 사항

Oracle에서 리포지토리를 설정할 경우 다음 지침을 사용하십시오.

- OPEN_CURSORS 매개 변수를 4000 이상으로 설정합니다.
데이터베이스 사용자에게 다음과 같은 권한이 있는지 확인합니다.

CREATE SEQUENCE

CREATE SESSION

CREATE SYNONYM

CREATE TABLE

CREATE VIEW

- Informatica에서 리포지토리 테이블에 대한 Oracle 공용 동의어를 지원하지 않습니다. 데이터베이스의 테이블에 대한 공용 동의어가 생성되지 않았는지 확인합니다.
- Informatica 도메인, 모델 리포지토리 서비스 또는 PowerCenter 리포지토리 서비스와 Oracle RAC 간의 연결을 구성할 수 있습니다. Oracle RAC(Real Application Cluster)는 데이터베이스 응용 프로그램의 고가용성을 활성화합니다. Informatica 도메인, 모델 리포지토리 서비스 및 PowerCenter 리포지토리 서비스는 모든 CRUD 작업에 대한 Oracle RAC 데이터베이스의 장애 조치에 대해 복원력을 가집니다. Informatica 도메인 및 모델 리포지토리 서비스에 대한 Oracle RAC 데이터베이스 장애 조치와 관련된 관리자 작업은 수행할 수 없습니다.

PostgreSQL 데이터베이스 요구 사항

PostgreSQL에서 리포지토리를 설정할 때 다음 지침을 사용하십시오.

- 데이터베이스 사용자 계정에 CONNECT, CREATE TABLE 및 CREATE VIEW 권한이 있는지 확인하십시오.
- PostgreSQL을 데이터베이스로 사용하는 경우 데이터베이스 스키마 이름을 지정합니다.
- PostgreSQL에 데이터 파일에 사용할 충분한 디스크 공간이 있는지 확인하십시오. 기본적으로 데이터 파일은 다음 위치에 있습니다.

<PostgreSQL 설치 디렉터리>/data

- 데이터베이스에서 구성 매개 변수를 설정합니다.

다음 테이블에는 설정해야 하는 구성 매개 변수에 대한 최소 및 권장 값이 나와 있습니다.

매개 변수	최소값	권장 값
max_connections	200	4000
shared_buffers	2GB	16GB
max_locks_per_transaction	1024	1024
max_wal_size	1GB	8GB
checkpoint_timeout	5분	30분

모니터링 모델 리포지토리 서비스

모니터링 모델 리포지토리 서비스는 데이터 통합 서비스 작업에 대한 통계를 모니터링하는 모델 리포지토리 서비스입니다. 모니터링 모델 리포지토리 서비스는 도메인 속성에 구성합니다.

참고: 모니터링 통계를 생성하려면 모니터링 용도로 사용할 전용 모델 리포지토리 서비스를 생성해야 합니다. 개체 메타데이터가 저장된 리포지토리에 런타임 모니터링 통계를 함께 저장할 수 없습니다.

다음 테이블에는 모니터링 모델 리포지토리 서비스에 연결된 제품, 서비스 및 데이터베이스에 대한 종속성이 요약되어 있습니다.

종속성	요약
제품	모니터링 모델 리포지토리 서비스를 사용하는 제품은 다음과 같습니다. <ul style="list-style-type: none"> - Data Engineering Integration - Data Engineering Quality - Data Engineering Streaming - Data Privacy Management - Enterprise Data Catalog - 엔터프라이즈 데이터 준비 - Informatica Data Quality - PowerCenter - Test Data Management
서비스	모니터링 모델 리포지토리 서비스는 다른 응용 프로그램 서비스에 연결하지 않아도 됩니다.
데이터베이스	모니터링 모델 리포지토리 서비스는 다음 데이터베이스를 사용 합니다. <ul style="list-style-type: none"> - 모델 리포지토리. Administrator 도구에서 볼 수 있는 런타임 모니터링 통계를 저장합니다.
설치 프로그램	모니터링 모델 리포지토리 서비스는 설치 프로그램을 실행할 때 생성할 수 있습니다.

PowerCenter 통합 서비스

PowerCenter 통합 서비스는 PowerCenter 클라이언트 도구에서 요청을 받아 데이터 통합 작업을 실행합니다. 이 서비스는 서로 다른 데이터베이스에 결과를 쓰고, PowerCenter 리포지토리에 런타임 메타데이터를 씁니다. 서비스를 생성할 때 서비스에 다른 응용 프로그램 서비스를 연결해야 합니다.

다음 테이블에는 PowerCenter 통합 서비스에 연결된 제품, 서비스 및 데이터베이스에 대한 종속성이 나열되어 있습니다.

종속성	요약
제품	PowerCenter 통합 서비스를 사용하는 제품은 다음과 같습니다. <ul style="list-style-type: none"> - PowerCenter - Informatica Data Quality - Test Data Management
서비스	PowerCenter 통합 서비스는 다음 서비스와 직접 연결되어야 합니다. <ul style="list-style-type: none"> - PowerCenter 리포지토리 서비스

종속성	요약
데이터베이스	PowerCenter 통합 서비스에는 연결된 데이터베이스가 없습니다.
설치 프로그램	설치 프로그램을 실행할 때 PowerCenter 통합 서비스를 생성할 수 있습니다.

PowerCenter 리포지토리 서비스

PowerCenter 리포지토리 서비스는 PowerCenter 리포지토리를 관리합니다. 이 서비스는 Informatica 클라이언트 및 응용 프로그램 서비스의 요청을 받아서 PowerCenter 리포지토리에서 메타데이터에 저장하거나 액세스합니다.

다음 테이블에는 PowerCenter 리포지토리 서비스에 연결된 제품, 서비스 및 데이터베이스에 대한 종속성이 요약되어 있습니다.

종속성	요약
제품	PowerCenter 리포지토리 서비스를 사용하는 제품은 다음과 같습니다. <ul style="list-style-type: none"> - PowerCenter - Informatica Data Quality - Test Data Management
서비스	PowerCenter 리포지토리 서비스는 다른 응용 프로그램 서비스와 연결할 필요가 없습니다.
데이터베이스	PowerCenter 리포지토리 서비스는 다음 데이터베이스를 사용합니다. <ul style="list-style-type: none"> - PowerCenter 리포지토리. Informatica 클라이언트 및 응용 프로그램 서비스가 생성한 메타데이터를 저장합니다.
설치 프로그램	PowerCenter 리포지토리 서비스는 설치 프로그램을 실행할 때 생성할 수 있습니다.

PowerCenter 리포지토리 데이터베이스 요구 사항

PowerCenter 리포지토리는 메타데이터를 포함하는 데이터베이스 테이블의 컬렉션입니다. PowerCenter 리포지토리 서비스는 리포지토리를 관리하고 리포지토리 데이터베이스와 리포지토리 클라이언트 사이에서 모든 메타데이터 트랜잭션을 수행합니다.

PowerCenter 리포지토리는 다음 데이터베이스 유형을 지원합니다.

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle
- PostgreSQL

참고: 10.5.3 설치 프로그램을 사용하여 PowerCenter 리포지토리 서비스를 생성하려면 Oracle, Microsoft SQL Server 또는 PostgreSQL 데이터베이스를 사용하면 됩니다. 다른 데이터베이스에 PowerCenter 리포지토리 서비스를 설치하려는 경우 설치 프로그램을 실행한 후 필요한 데이터베이스로 서비스를 생성하십시오.

데이터베이스에 대해 35 MB 디스크 공간을 허용합니다.

참고: PowerCenter 리포지토리 서비스를 실행할 시스템에 데이터베이스 클라이언트를 설치해야 합니다. 데이터베이스 구성에 대한 자세한 내용은 데이터베이스 시스템에 대한 설명서를 참조하십시오.

IBM DB2 데이터베이스 요구 사항

IBM DB2에서 리포지토리를 설정할 때 다음 지침을 사용하십시오.

- 리포지토리 성능을 최적화하려면 단일 노드에서 테이블스페이스가 있는 데이터베이스를 설정하십시오. 테이블스페이스가 하나의 노드에 있는 경우 PowerCenter 클라이언트 및 PowerCenter 통합 서비스는 리포지토리 테이블이 다른 데이터베이스 노드에 있는 것보다 더 빨리 리포지토리에 액세스합니다.
리포지토리를 작성, 복사 또는 복원할 경우 단일 노드 테이블스페이스 이름을 지정합니다. 테이블스페이스 이름을 지정하지 않은 경우 DB2에서 기본 테이블스페이스를 사용합니다.
- Informatica는 리포지토리 테이블에 대해 IBM DB2 테이블 별칭을 지원하지 않습니다. 데이터베이스의 테이블에 대해 테이블 별칭이 작성되지 않았는지 확인합니다.

Microsoft SQL Server 데이터베이스 요구 사항

리포지토리를 설정할 때는 다음 지침을 사용하십시오.

- 데이터베이스 서버 페이지 크기를 8K 이상으로 설정하십시오. 이는 1회성 구성이며 이후에 변경될 수 없습니다.
- 데이터베이스 사용자 계정에 CONNECT, CREATE TABLE 및 CREATE VIEW 권한이 있는지 확인하십시오.

Oracle 데이터베이스 요구 사항

Oracle에서 리포지토리를 설정할 경우 다음 지침을 사용하십시오.

- 리포지토리가 너무 많은 공간을 사용하지 않도록 방지하려면 테이블스페이스에 대한 저장소 크기를 작은 숫자로 설정합니다. 또한 리포지토리 테이블을 소유하는 사용자의 기본 테이블스페이스가 작은 크기로 설정되어 있는지 확인합니다.

다음 예제에서는 REPOSITORY라는 테이블스페이스에 대해 권장되는 저장소 매개 변수를 설정하는 방법을 보여 줍니다.

```
ALTER TABLESPACE "REPOSITORY" DEFAULT STORAGE ( INITIAL 10K NEXT 10K MAXEXTENTS UNLIMITED PCTINCREASE 50 );
```

리포지토리를 생성하기 전에 테이블스페이스에 대한 저장소 매개 변수를 확인하거나 변경합니다.

- 데이터베이스 사용자에게 다음과 같은 권한이 있는지 확인합니다.

```
CREATE SEQUENCE
```

```
CREATE SESSION
```

```
CREATE SYNONYM
```

```
CREATE TABLE
```

```
CREATE VIEW
```

- Informatica에서 리포지토리 테이블에 대한 Oracle 공용 동의어를 지원하지 않습니다. 데이터베이스의 테이블에 대한 공용 동의어가 생성되지 않았는지 확인합니다.
- Informatica 도메인, 모델 리포지토리 서비스 또는 PowerCenter 리포지토리 서비스와 Oracle RAC 간의 연결을 구성할 수 있습니다. Oracle RAC(Real Application Cluster)는 데이터베이스 응용 프로그램의 고가용성을 활성화합니다. Informatica 도메인, 모델 리포지토리 서비스 및 PowerCenter 리포지토리 서비스는 모든 CRUD 작업에 대한 Oracle RAC 데이터베이스의 장애 조치에 대해 복원력을 가집니다.

PowerCenter 리포지토리 서비스의 다음 작업은 Oracle RAC 설정의 데이터베이스 장애 조치에 대해 복원력을 가집니다.

- ExecuteQuery
- ObjectExport
- ObjectImport
- PurgeVersion
- RollbackDeployment

PostgreSQL Database Requirements

PostgreSQL에서 리포지토리를 설정할 때 다음 지침을 사용하십시오.

- 데이터베이스 사용자 계정에 CREATE TABLE 및 CREATE VIEW 권한이 있는지 확인하십시오.
- PostgreSQL에 데이터 파일에 사용할 충분한 디스크 공간이 있는지 확인하십시오. 기본적으로 데이터 파일은 다음 위치에 있습니다.

<PostgreSQL 설치 디렉터리>/data

- 데이터베이스에서 구성 매개 변수를 설정합니다.

다음 테이블에는 설정해야 하는 구성 매개 변수에 대한 최소 및 권장 값이 나와 있습니다.

매개 변수	최소값	권장 값
max_connections	200	4000
shared_buffers	2GB	16GB
max_locks_per_transaction	1024	4000
max_wal_size	1GB	8 GB
checkpoint_timeout	5분	30분

- To configure PostgreSQL database for the PowerCenter repository, set values for the PostgreSQL database host, port, and service name for the pg_service.conf file in the following format:

```
[PCRS_DB_SERVICE_NAME]
host=Database host IP
port=Database port
dbname=PowerCenter Repository Service database service name
```

Ensure that the entries for the [PCRS_DB_SERVICE_NAME] entry matches the information for the PowerCenter Repository Service. To securely connect to PostgreSQL for the PowerCenter repository, set the security property along with the remaining required database properties in the pg_service.conf file in the following format: sslmode=require

- Set the PGSERVICEFILE environment variable to the location of the pg_service.conf file. The pg_service.conf file contains the connection parameters for PostgreSQL database connection in the Informatica installation directory. For example, set the variable as follows:

Using a Bourne shell:

```
$ export PGSERVICEFILE; PGSERVICEFILE=<pg_service.conf file
directory>/pg_service.conf
```

Using a C shell:

```
$ setenv PGSERVICEFILE <pg_service.conf file
directory>/pg_service.conf
```

Sybase ASE 데이터베이스 요구 사항

Sybase ASE에서 리포지토리를 설정하는 경우 다음 지침을 사용하십시오.

- 데이터베이스 서버 페이지 크기를 8K 이상으로 설정하십시오. 이는 1회성 구성이며 이후에 변경될 수 없습니다.
- Sybase 데이터베이스 옵션 "ddl in tran"을 TRUE로 설정하십시오.
- "allow nulls by default"를 TRUE로 설정하십시오.
- 데이터베이스 사용자 계정에 CREATE TABLE 및 CREATE VIEW 권한이 있는지 확인합니다.
- 데이터베이스 메모리 구성 요구 사항을 설정합니다.
다음 테이블에는 메모리 구성 요구 사항 및 권장 기준값이 나와 있습니다.

데이터베이스 구성	Sybase 시스템 프로시저	값
열린 개체 수	sp_configure "열린 개체 수"	5000
열린 인덱스 수	sp_configure "열린 인덱스 수"	5000
열린 파티션 수	sp_configure "열린 파티션 수"	8000
잠금 수	sp_configure "잠금 수"	100000

검색 서비스

검색 서비스는 Analyst 도구에서 검색을 관리하고, 검색 결과를 모델 리포지토리에서 반환합니다. 서비스를 생성할 때 서비스에 다른 응용 프로그램 서비스를 연결해야 합니다.

다음 테이블에는 검색 서비스에 연결된 제품, 서비스 및 데이터베이스에 대한 종속성이 요약되어 있습니다.

종속성	요약
제품	검색 서비스를 사용하는 제품은 다음과 같습니다. - Data Engineering Integration - Data Engineering Quality - Data Engineering Streaming - Enterprise Data Catalog - Enterprise Data Preparation - Informatica Data Quality - PowerCenter
서비스	검색 서비스는 다음 서비스와 직접 연결되어야 합니다. - 모델 리포지토리 서비스
데이터베이스	검색 서비스에는 연결된 데이터베이스가 없습니다.
설치 프로그램	검색 서비스는 설치 프로그램을 실행할 때 생성할 수 없습니다.

서비스 시스템에서 원시 연결 구성

응용 프로그램 서비스와 데이터베이스 간에 원시 연결을 설정하려면 액세스하려는 데이터베이스에 대해 데이터베이스 클라이언트 소프트웨어를 설치하십시오.

원시 드라이버는 데이터베이스 서버 및 클라이언트 소프트웨어에 패키징되어 있습니다. 데이터베이스에 액세스해야 하는 시스템에서 연결을 구성해야 합니다. 응용 프로그램 서비스와 데이터베이스 간에 호환성을 보장하려면 데이터베이스 버전과 호환되는 클라이언트 소프트웨어를 설치하고 적절한 데이터베이스 클라이언트 라이브러리를 사용하십시오.

다음 서비스는 원시 연결을 사용하여 여러 데이터베이스에 연결합니다.

데이터 통합 서비스

데이터 통합 서비스는 원시 데이터베이스 드라이버를 사용하여 다음 데이터베이스에 연결합니다.

- 소스 데이터베이스 및 대상 데이터베이스. 소스 데이터베이스에서 데이터를 읽고 대상 데이터베이스에 데이터를 씁니다.
- 데이터 개체 캐시 데이터베이스. 데이터 개체 캐시를 저장합니다.
- 프로파일링 소스 데이터베이스. 관계형 소스 데이터베이스로부터 읽어서 소스에 대해 프로필을 실행합니다.
- 프로파일링 웨어하우스. 프로파일링 결과를 프로파일링 웨어하우스에 씁니다.
- 참조 테이블. 매핑을 실행하여 참조 테이블과 외부 데이터 소스 간에 데이터를 전송합니다.

데이터 통합 서비스가 단일 노드에서 실행되거나 기본 및 백업 노드에서 실행되는 경우에는 데이터베이스 클라이언트 소프트웨어를 설치하고, 데이터 통합 서비스가 실행되는 시스템에서 연결을 구성합니다.

데이터 통합 서비스가 그리드에서 실행되는 경우에는 데이터베이스 클라이언트 소프트웨어를 설치하고, 계산 역할이 있는 노드 또는 서비스 및 계산 역할 모두 있는 노드를 나타내는 각 시스템에서 연결을 구성합니다.

PowerCenter 리포지토리 서비스

PowerCenter 리포지토리 서비스는 원시 데이터베이스 드라이버를 사용하여 PowerCenter 리포지토리 데이터베이스에 연결합니다.

PowerCenter 리포지토리 서비스 및 PowerCenter 리포지토리 서비스 프로세스가 실행되는 시스템에서 데이터베이스 클라이언트 소프트웨어를 설치하고 연결을 구성하십시오.

PowerCenter 통합 서비스

PowerCenter 통합 서비스는 원시 데이터베이스 드라이버를 사용하여 다음 데이터베이스에 연결합니다.

- 소스 데이터베이스 및 대상 데이터베이스. 소스 데이터베이스에서 읽고 대상 데이터베이스에 씁니다.
- Metadata Manager 소스 데이터베이스. Metadata Manager에 있는 관계형 데이터 소스를 로드합니다.

PowerCenter 통합 서비스가 실행되는 시스템에서 관계형 데이터 소스 및 리포지토리 데이터베이스와 연결된 데이터베이스 클라이언트 소프트웨어를 설치하십시오.

데이터베이스 클라이언트 소프트웨어 설치

응용 프로그램 서비스가 액세스하는 데이터베이스 유형에 따라 필요한 시스템에 데이터베이스 클라이언트를 설치해야 합니다.

응용 프로그램 서비스와 데이터베이스 간의 호환성을 보장하려면 해당하는 데이터베이스 클라이언트 라이브러리를 사용하고 데이터베이스 버전과 호환 가능한 클라이언트 소프트웨어를 설치합니다.

응용 프로그램 서비스가 액세스하는 데이터베이스 유형을 기반으로 다음 데이터베이스 클라이언트 소프트웨어를 설치합니다.

IBM DB2 CAE(Client Application Enabler)

Informatica 서비스를 시작하는 사용자로 시스템에 로그인하여, 필요한 시스템에서 연결을 구성합니다.

Microsoft SQL Server 2014 Native Client

다음 Microsoft 웹 사이트에서 클라이언트를 다운로드합니다.

<http://www.microsoft.com/en-in/download/details.aspx?id=42295>.

Oracle 클라이언트

호환되는 버전의 Oracle 클라이언트 및 Oracle 데이터베이스 서버를 설치합니다. 동일한 버전의 Oracle 클라이언트가 필요한 모든 시스템에도 해당 클라이언트를 설치해야 합니다. 호환성을 확인하려면 Oracle에 문의하십시오.

Sybase Open Client(OCS)

Sybase ASE 데이터베이스 서버와 호환 가능한 Open Client 버전을 설치합니다. 또한 Sybase ASE 데이터베이스 및 Informatica를 호스트하는 시스템에 동일한 버전의 Open Client를 설치해야 합니다. 호환성을 확인하려면 Sybase에 문의하십시오.

PostgreSQL 클라이언트(psql)

PostgreSQL 대화형 터미널 프로그램인 psql을 설치하고 실행하면 SQL 명령을 대화형으로 입력, 편집 및 실행할 수 있습니다.

psql은 PostgreSQL에 대한 터미널 기반 프론트엔드입니다. 쿼리를 대화형으로 입력하고 PostgreSQL로 쿼리를 실행하고 쿼리 결과를 확인할 수 있습니다. 또는 파일 또는 명령줄 인수의 입력을 사용할 수 있습니다.

Linux 또는 Windows에서만 작동하는 PostgreSQL용 psql 클라이언트 응용 프로그램을 설치할 수 있습니다.

GCC 컴파일러 패키지, readline 및 readline-devel 패키지와 zlib-devel 압축 라이브러리 패키지 등 PostgreSQL 구축에 필요한 소프트웨어 종속성 패키지를 설치하고 실행하십시오. GNU Readline 라이브러리에서 패키지를 설치하면 입력한 각 명령이 psql에 기억되며 화살표 키를 사용하여 이전 명령을 회수하고 편집할 수 있습니다.

또한 yum install 명령을 사용하여 필요한 라이브러리 파일을 실행할 수 있습니다.

Windows의 PostgreSQL

Windows의 경우 다음 링크에서 psql 클라이언트를 다운로드합니다.

<https://www.enterprisedb.com/downloads/postgres-postgresql-downloads>

PostgreSQL 라이브러리가 Windows의 다음 디렉터리에 있는지 확인해야 합니다.

- 설치 디렉터리: C:\Program Files\PostgreSQL\10
- 명령줄 도구 설치 디렉터리: C:\Program Files\PostgreSQL\10
- pgAdmin4 설치 디렉터리: C:\Program Files\PostgreSQL\10\pgAdmin 4

Linux의 PostgreSQL

Linux에서도 필요한 postgresql 라이브러라인 postgresql10-10.10-1PGDG.rhel7.x86_64 및 postgresql10-libs-10.10-1PGDG.rhel7.x86_64를 설치해야 합니다.

psql에 대한 자세한 내용은 다음 링크의 psql 클라이언트 설명서를 참조하십시오.

<https://www.postgresql.org/docs/10/app-psql.html>

데이터베이스 클라이언트 환경 변수 구성

데이터 통합 서비스, PowerCenter 통합 서비스 및 PowerCenter 리포지토리 서비스 프로세스를 실행하는 시스템에서 데이터베이스 클라이언트 환경 변수를 구성합니다.

데이터베이스 환경 변수를 구성한 후에 데이터베이스 클라이언트에서 데이터베이스에 대한 연결을 테스트할 수 있습니다.

Oracle 데이터베이스

다음 테이블에는 Oracle 데이터베이스에 대해 sqlplus를 데이터베이스 유틸리티로 설정해야 하는 데이터베이스 환경 변수가 나와 있습니다.

환경 변수	값
ORACLE_HOME	<Client InstallDatabasePath>
PATH	<DatabasePath>/bin 및 USER_INSTALL_DIR/server/bin:\$PATH
LD_LIBRARY_PATH	\$ORACLE_HOME/lib 및 USER_INSTALL_DIR/server/bin:\$LD_LIBRARY_PATH
TNS_ADMIN	tnsnames.ora 파일의 위치로 설정: \$ORACLE_HOME/network/admin
INFA_TRUSTSTORE	기본 SSL 도메인의 경우 다음에 추가: USER_INSTALL_DIR/services/shared/security 사용자 지정 SSL 도메인의 경우 INFA_TRUSTSTORE 및 INFA_TRUSTSTORE_PASSWORD 설정

IBM DB2 데이터베이스

다음 테이블에는 IBM DB2 데이터베이스에 대해 db2connect를 데이터베이스 유틸리티로 설정해야 하는 데이터베이스 환경 변수가 나와 있습니다.

환경 변수	값
DB2DIR	<데이터베이스 경로>
DB2INSTANCE	<DB2InstanceName>
PATH	<데이터베이스 경로>/bin

Sybase ASE 데이터베이스

다음 테이블에는 Sybase ASE 데이터베이스에 대해 isql을 데이터베이스 유틸리티로 설정해야 하는 데이터베이스 환경 변수가 나와 있습니다.

환경 변수	값
SYBASE15	<<데이터베이스 경로>/sybase<버전>>
SYBASE_ASE	\${SYBASE15}/ASE-<버전>
SYBASE_OCS	\${SYBASE15}/OCS-<version>
PATH	\${SYBASE_ASE}/bin:\${SYBASE_OCS}/bin:\$PATH

PostgreSQL 데이터베이스

다음 테이블에는 PostgreSQL 데이터베이스에 대해 설정해야 하는 데이터베이스 환경 변수가 나와 있습니다.

환경 변수	값
PGSERVICEFILE	pg_service.conf 파일의 위치로 설정: <pg_service.conf 파일 디렉터리>/pg_service.conf
PGHOME	/usr/pgsql-10
PATH	\$PGHOME:\${PATH}
LD_LIBRARY_PATH	\$PGHOME/lib:\${LD_LIBRARY_PATH}
INFA_TRUSTSTORE	기본 SSL 도메인의 경우 다음에 추가: <InstallationDirectory>/services/shared/security 사용자 지정 SSL 도메인의 경우 INFA_TRUSTSTORE 및 INFA_TRUSTSTORE_PASSWORD 설정
POSTGRES_ODBC	PostgreSQL ODBC 연결의 경우 값을 1로 설정합니다. 도메인의 모든 리포지토리 또는 ODBC 연결을 사용하는 모든 PostgreSQL 리포지토리에 대해 설정할 수 있습니다.

Microsoft SQL Server 데이터베이스

다음 테이블에는 Microsoft SQL Server 데이터베이스에 대해 설정해야 하는 데이터베이스 환경 변수가 나와 있습니다.

환경 변수	값
ODBCHOME	USER_INSTALL_DIR/ODBC7.1
ODBCINI	\$ODBCHOME/odbc.ini
ODBCINST	\$ODBCHOME/odbcinst.ini
PATH	/opt/mssql-tools/bin:\$PATH\$USER_INSTALL_DIR/ ODBC7.1:\$PATH\$USER_INSTALL_DIR/server/bin:\$PATH
LD_LIBRARY_PATH	\$ODBCHOME/lib
INFA_TRUSTSTORE	USER_INSTALL_DIR/server/bin:\$LD_LIBRARY_PATH 기본 SSL 도메인의 경우 다음에 추가: USER_INSTALL_DIR/services/shared/security 사용자 지정 SSL 도메인의 경우 INFA_TRUSTSTORE 및 INFA_TRUSTSTORE_PASSWORD 설정

제 5 장

Kerberos 인증 준비

이 장에 포함된 항목:

- [Kerberos 인증 준비를 위한 검사 목록, 80](#)
- [Kerberos 인증 준비 개요, 80](#)
- [Kerberos 구성 파일 설정, 81](#)
- [서비스 사용자 및 키 탭 파일 이름 형식 생성, 82](#)
- [SPN 및 키 탭 형식 텍스트 파일 검토, 85](#)
- [서비스 사용자 이름 및 키 탭 파일 생성, 86](#)

Kerberos 인증 준비를 위한 검사 목록

이 장에는 설치 중 설치 프로그램을 통해 Kerberos를 활성화하려는 경우에 수행해야 하는 태스크가 포함되어 있습니다. Kerberos 인증을 준비하는 데 필요한 태스크를 추적하는 데 이 검사 목록을 사용하십시오.

- Kerberos 구성 파일을 설정합니다.
- 서비스 사용자 및 키 탭 이름 파일 형식을 생성합니다.
- SPN 및 키 탭 형식 텍스트 파일을 검토합니다.
- SPN 및 키 탭 파일을 생성합니다.

Kerberos 인증 준비 개요

사용자, 서비스 및 노드 인증을 위해 Kerberos 네트워크 인증을 사용하도록 Informatica 도메인을 구성할 수 있습니다.

Kerberos는 네트워크의 서비스 및 노드에 대한 액세스를 인증하기 위해 티켓을 사용하는 네트워크 인증 프로토콜입니다. Kerberos는 KDC(키 배포 센터)를 사용하여 사용자 및 서비스의 ID 유효성을 검사하고 인증된 사용자 및 서비스 계정에 티켓을 부여합니다. Kerberos 프로토콜에서는 사용자(user) 및 서비스를 사용자(principal)라고 합니다. KDC에는 사용자 및 ID 증명으로 사용되는 연결 암호 키가 포함된 데이터베이스가 있습니다.

Kerberos는 LDAP 디렉터리 서비스를 사용자 데이터베이스로 사용할 수 있습니다.

Kerberos 인증을 사용하려면 Kerberos 네트워크 인증을 사용하는 네트워크에서 Informatica 도메인을 설치하고 실행해야 합니다. Informatica는 Kerberos 인증을 사용하는 네트워크에서 Microsoft Active Directory 서비스를 사용자 데이터베이스로 사용하여 실행될 수 있습니다.

네트워크를 통해 암호를 전송하지 않으면서 도메인의 노드 및 서비스를 인증하려면 Informatica 도메인에 키 탭 파일이 필요합니다. 키 탭 파일에는 SPN(서비스 사용자 이름) 및 연결된 암호화 키가 포함됩니다. Informatica 도메인에서 노드 및 서비스를 작성하기 전에 키 탭 파일을 작성하십시오.

참고: Enterprise Data Catalog 또는 Enterprise Data Preparation은 Kerberos 인증을 위해 활성화된 Informatica 도메인을 지원하지 않습니다.

Kerberos 구성 파일 설정

Kerberos는 구성 정보를 *krb5.conf*라는 파일에 저장합니다. Informatica의 경우 Kerberos 구성 파일의 특정 속성을 설정해야 Informatica 도메인에서 Kerberos 인증을 올바르게 사용할 수 있습니다. *krb5.conf* 구성 파일에서 해당 속성을 설정해야 합니다.

구성 파일에는 Kerberos 영역 및 KDC 주소 등 Kerberos 서버에 대한 정보가 포함됩니다. Kerberos 관리자에게 구성 파일의 속성을 설정하여 파일의 사본을 보내줄 것을 요청할 수 있습니다.

1. *krb5.conf* 파일을 백업한 다음 변경합니다.
2. *krb5.conf* 파일을 편집합니다.
3. *libdefaults* 섹션에서 Informatica에 필요한 속성을 설정하거나 추가합니다.

다음 테이블에는 *libdefaults* 섹션에서 설정해야 하는 속성의 값이 나열되어 있습니다.

매개 변수	값
default_realm	Informatica 도메인에 대한 서비스 영역의 이름입니다. 비원시 환경과 도메인을 통합하는 경우 default_realm 속성을 클러스터의 default_realm 속성과 동일하게 설정합니다.
forwardable	서비스에서 클라이언트 사용자 자격 증명을 다른 서비스에 위임할 수 있습니다. 이 매개 변수를 True로 설정합니다. Informatica 도메인에서 응용 프로그램 서비스는 다른 서비스를 통해 클라이언트 사용자 자격 증명을 인증해야 합니다.
default_tkt_enctypes	TGT(티켓 부여 티켓)에서 세션 키의 암호화 유형입니다. 이 매개 변수는 세션 키에 특정 암호화 유형을 사용해야 하는 경우에만 설정합니다.
udp_preference_limit	Kerberos에서 KDC에 메시지를 전송할 때 사용할 프로토콜을 결정합니다. 항상 TCP를 사용하도록 udp_preference_limit = 1로 설정합니다. Informatica 도메인은 TCP 프로토콜만 지원합니다. udp_preference_limit을 1 이외의 다른 값으로 설정하면 Informatica 도메인이 예기치 않게 종료될 수 있습니다.

4. *realms* 섹션의 KDC 주소 안에 포트 번호를 콜론으로 구분하여 포함합니다.

예를 들어 KDC 주소가 *kerberos.example.com*이고 포트 번호가 88일 경우 *kdc* 매개 변수를 다음으로 설정합니다.

```
kdc = kerberos.example.com:88
```

5. *krb5.conf* 파일을 저장합니다.
6. Informatica 서비스를 설치하려는 시스템에 액세스할 수 있는 디렉터리에 *krb5.conf* 파일을 저장합니다.

다음 예제에서는 필수 속성이 포함된 *krb5.conf*의 콘텐츠를 보여 줍니다.

```
[libdefaults]
default_realm = AFNIKRB.AFNIDEV.COM
forwardable = true
udp_preference_limit = 1
```

```
[realms]
AFNIKRB.AFNIDEV.COM = {
  admin_server = SMPLKERDC01.AFNIKRB.AFNIDEV.COM
  kdc = SMPLKERDC01.AFNIKRB.AFNIDEV.COM:88
}
```

```
[domain_realm]
afnikrb.afnidev.com = AFNIKRB.AFNIDEV.COM
.afnikrb.afnidev.com = AFNIKRB.AFNIDEV.COM
```

Kerberos 구성 파일에 대한 자세한 내용은 Kerberos 네트워크 인증 설명서를 참조하십시오.

서비스 사용자 및 키 탭 파일 이름 형식 생성

Kerberos 인증이 포함된 Informatica 도메인을 실행하는 경우 Kerberos SPN(서비스 사용자 이름) 및 키 탭 파일을 Informatica 도메인의 노드 및 프로세스와 연결해야 합니다. Informatica에서는 암호를 요구하지 않고 서비스를 인증하기 위해 키 탭 파일이 필요합니다.

도메인의 보안 요구 사항에 따라 서비스 사용자 수준을 다음 수준 중 하나로 설정할 수 있습니다.

노드 수준

도메인이 테스트 또는 개발용으로 사용되며 도메인에 높은 보안 수준이 요구되지 않는 경우 서비스 사용자를 노드 수준에서 설정할 수 있습니다. 노드 및 노드의 모든 서비스 프로세스에 대해 하나의 SPN 및 키 탭 파일을 사용할 수 있습니다. 노드의 HTTP 프로세스에 대해서도 별도의 SPN 및 키 탭 파일을 설정해야 합니다.

프로세스 수준

도메인이 프로덕션용으로 사용되며 도메인에 높은 보안 수준이 요구되는 경우 서비스 사용자를 프로세스 수준에서 설정할 수 있습니다. 각 노드 및 노드의 각 프로세스에 대해 고유한 SPN 및 키 탭 파일을 작성합니다. 노드의 HTTP 프로세스에 대해서도 별도의 SPN 및 키 탭 파일을 설정해야 합니다.

Informatica 도메인의 경우 서비스 사용자 및 키 탭 파일 이름이 특정 형식을 따라야 합니다. 서비스 사용자 및 키 탭 파일 이름이 올바른 형식을 따르도록 Informatica Kerberos SPN 형식 생성기를 사용하여 Informatica 도메인에 필요한 형식으로 서비스 사용자 및 키 탭 파일 이름 목록을 생성하십시오.

Informatica Kerberos SPN 형식 생성기는 Informatica 서비스 설치 프로그램과 함께 제공됩니다.

노드 수준에서의 서비스 사용자 요구 사항

Informatica 도메인에 높은 수준의 보안이 필요하지 않는 경우 노드와 서비스 프로세스가 동일한 SPN 및 키 탭 파일을 공유할 수 있습니다. 따라서 도메인 노드의 각 서비스 프로세스에 대해 별도의 SPN이 필요하지 않습니다.

Informatica 도메인은 노드 수준에서 다음 구성 요소에 대한 SPN 및 키 탭 파일을 필요로 합니다.

LDAP 디렉터리 서비스의 사용자 DN(고유 이름)

LDAP 디렉터리 서비스 검색에 사용되는 바인딩 사용자 DN의 사용자 이름입니다. 키 탭 파일의 이름은 `infa_ldapuser.keytab`이어야 합니다.

노드 프로세스

인증 호출을 개시하거나 수락하는 Informatica 노드의 사용자 이름입니다. 동일한 사용자 이름이 노드의 서비스를 인증하는 데 사용됩니다. 도메인의 각 게이트웨이 노드에는 별도의 사용자 이름이 필요합니다.

도메인의 HTTP 프로세스

Informatica Administrator를 포함하여 Informatica 도메인에 있는 모든 웹 응용 프로그램 서비스의 사용자 이름입니다. 브라우저는 이 사용자 이름을 사용하여 도메인의 모든 HTTP 프로세스에 대해 인증됩니다. 키 탭 파일의 이름은 `webapp_http.keytab`이어야 합니다.

프로세스 수준에서의 서비스 사용자 요구 사항

Informatica 도메인에 높은 수준의 보안이 필요한 경우 각 노드 및 해당 노드의 각 서비스에 대해 별도의 SPN 및 키 탭 파일을 작성하십시오.

Informatica 도메인은 프로세스 수준에서 다음 구성 요소에 대해 SPN 및 키 탭 파일을 필요로 합니다.

LDAP 디렉터리 서비스의 사용자 DN(고유 이름)

LDAP 디렉터리 서비스 검색에 사용되는 바인딩 사용자 DN의 사용자 이름입니다. 키 탭 파일의 이름은 `infa_ldapuser.keytab`이어야 합니다.

노드 프로세스

인증 호출을 개시하거나 수락하는 Informatica 노드의 사용자 이름입니다.

Informatica Administrator 서비스

Informatica 도메인의 다른 서비스와 함께 Informatica Administrator 서비스를 인증하는 Informatica Administrator 서비스의 사용자 이름입니다. 키 탭 파일의 이름은 `_AdminConsole.keytab`이어야 합니다.

도메인의 HTTP 프로세스

Informatica Administrator를 포함하여 Informatica 도메인에 있는 모든 웹 응용 프로그램 서비스의 사용자 이름입니다. 브라우저는 이 사용자 이름을 사용하여 도메인의 모든 HTTP 프로세스에 대해 인증됩니다. 키 탭 파일의 이름은 `webapp_http.keytab`이어야 합니다.

서비스 프로세스

Informatica 도메인의 노드에서 실행되는 서비스의 사용자 이름입니다. 각 서비스는 고유한 서비스 사용자 및 키 탭 파일 이름을 필요로 합니다.

설치 프로그램을 실행하기 전에 서비스에 대해 SPN 및 키 탭 파일을 작성하지 않아도 됩니다. 도메인에서 서비스를 작성할 때 해당 서비스에 대해 SPN 및 키 탭 파일을 작성할 수 있습니다. 서비스를 활성화할 때 해당 서비스의 SPN 및 키 탭 파일을 사용할 수 있어야 합니다.

SPN 형식 생성기 실행

Informatica Kerberos SPN 형식 생성기를 실행하여 Informatica 도메인에 필요한 올바른 형식의 SPN 및 키 탭 파일 이름을 갖춘 파일을 생성할 수 있습니다.

SPN 형식 생성기는 명령줄 또는 Informatica 설치 프로그램에서 실행할 수 있습니다. SPN 형식 생성기는 사용자가 제공한 매개 변수에 따라 서비스 사용자 및 키 탭 파일의 이름을 포함하는 파일을 생성합니다.

참고: 제공한 정보가 올바른지 확인하십시오. SPN 형식 생성기는 입력한 값의 유효성을 검사하지 않습니다.

1. 설치 파일을 압축 해제한 시스템에서 다음 디렉터리로 이동합니다. `<Informatica 설치 파일 디렉터리>/Server/Kerberos`
2. 셸 명령줄에서 `SPNFormatGenerator` 파일을 실행합니다.
3. **Enter** 키를 눌러 계속 진행합니다.
4. **서비스 사용자 수준** 섹션에서 도메인에 대해 Kerberos 서비스 사용자를 어떤 수준에 설정할지 선택합니다.

다음 테이블에는 선택 가능한 수준이 설명되어 있습니다.

수준	설명
프로세스 수준	<p>각 노드 및 노드의 각 응용 프로그램 서비스에 대해 고유한 SPN(서비스 사용자 이름) 및 키 탭 파일을 사용하도록 도메인을 구성합니다.</p> <p>각 노드에 필요한 SPN 및 키 탭 파일의 수는 노드에서 실행되는 응용 프로그램 서비스 프로세스의 수에 따라 달라집니다. 운영 도메인 같이 높은 보안 수준이 필요한 도메인에 대해 프로세스 수준 옵션을 사용하십시오.</p>
노드 수준	<p>노드에서 SPN 및 키 탭 파일을 공유하도록 도메인을 구성합니다.</p> <p>이 옵션에는 노드에 대한 하나의 SPN과 키 탭 파일 및 노드에서 실행되는 모든 응용 프로그램 서비스가 필요합니다. 또한 노드의 모든 HTTP 프로세스에 대해 별도의 SPN 및 키 탭 파일이 필요합니다.</p> <p>테스트 및 개발 도메인 같이 높은 보안 수준이 필요하지 않은 도메인에 대해 노드 수준 옵션을 사용하십시오.</p>

5. SPN 형식을 생성하는 데 필요한 도메인 및 노드 매개 변수를 입력합니다.

다음 테이블에는 지정해야 하는 매개 변수가 설명되어 있습니다.

프롬프트	설명
도메인 이름	도메인의 이름입니다. 이름은 128자를 초과하지 않아야 하고 7비트 ASCII여야만 합니다. 이름에는 공백이나 ` % * + ; " ? , < > \ /` 문자를 사용할 수 없습니다.
노드 이름	Informatica 노드의 이름입니다.
노드 호스트 이름	<p>노드를 작성할 시스템의 정규화된 호스트 이름 또는 IP 주소입니다. 노드 호스트 이름에는 밑줄(_) 문자를 사용할 수 없습니다.</p> <p>참고: <i>localhost</i>는 사용하지 마십시오. 호스트 이름은 명시적으로 시스템을 식별해야 합니다.</p>
서비스 영역 이름	Informatica 도메인 서비스의 Kerberos 영역 이름입니다. 해당 영역 이름은 대문자여야 합니다.

노드 수준에서 서비스 사용자를 설정하면 프롬프트에 **노드 추가?**가 표시됩니다. 프로세스 수준에서 서비스 사용자를 설정하면 프롬프트에 **서비스 추가?**가 표시됩니다.

6. **노드 추가?** 프롬프트에서 1을 입력하여 추가적인 노드에 대해 SPN 형식을 생성합니다. 그런 다음, 노드 이름 및 노드 호스트 이름을 입력합니다.

여러 노드에 대해 SPN 형식을 생성하려면 각 **노드 추가?** 프롬프트에 1을 입력하고 노드 이름 및 노드 호스트 이름을 입력합니다.

7. **서비스 추가?** 프롬프트에서 1을 입력하여 바로 위의 노드에서 실행될 서비스에 대해 SPN 형식을 생성합니다. 그런 다음, 서비스 이름을 입력합니다.

여러 서비스에 대해 SPN 형식을 생성하려면 각 **서비스 추가?** 프롬프트에 1을 입력하고 서비스 이름을 입력합니다.

8. 2를 입력하여 **서비스 추가?** 또는 **노드 추가?** 프롬프트를 종료합니다.

SPN 형식 생성기가 서비스 사용자 및 키 탭 파일 이름의 목록을 포함하는 파일의 경로 및 파일 이름을 표시합니다.

9. Enter 키를 눌러 SPN 형식 생성기를 종료합니다.

SPN 형식 생성기는 SPN 및 키 탭 파일 이름을 포함하는 텍스트 파일을 Informatica 도메인에 필요한 형식으로 생성합니다.

SPN 및 키 탭 형식 텍스트 파일 검토

Kerberos SPN 형식 생성기는 Informatica 도메인에 필요한 서비스 사용자 및 키 탭 파일 이름의 형식을 나열하는 SPNKeytabFormat.txt라는 텍스트 파일을 생성합니다. 이 파일에는 사용자가 선택한 서비스 사용자 수준을 기반으로 하는 SPN 및 키 탭 파일 이름이 포함됩니다.

텍스트 파일을 검토하고 오류 메시지가 없는지 확인하십시오.

텍스트 파일에는 다음 정보가 포함됩니다.

항목 이름

프로세스에 연결된 노드 또는 서비스를 식별합니다.

SPN

Kerberos 사용자 데이터베이스의 SPN에 대한 형식입니다. SPN은 대/소문자를 구분합니다. SPN은 유형에 따라 형식이 다릅니다.

SPN의 형식은 다음 중 하나일 수 있습니다.

키 탭 유형	SPN 형식
NODE_SPN	isp/<NodeName>/<DomainName>@<REALMNAME>
NODE_AC_SPN	_AdminConsole/<NodeName>/<DomainName>@<REALMNAME>
NODE_HTTP_SPN	HTTP/<NodeHostName>@<REALMNAME> 참고: Kerberos SPN 형식 생성기는 노드 호스트 이름의 유효성을 검사합니다. 노드 호스트 이름이 올바르지 않을 경우 이 유틸리티가 SPN을 생성하지 않습니다. 대신에 "호스트 이름을 확인할 수 없습니다."라는 메시지가 표시됩니다.
SERVICE_PROCESS_SPN	<ServiceName>/<NodeName>/<DomainName>@<REALMNAME>

키 탭 파일 이름

Kerberos 사용자 데이터베이스의 연결된 SPN에 대해 작성할 키 탭 파일 이름의 형식입니다. 키 탭 파일 이름은 대/소문자를 구분합니다.

키 탭 파일 이름은 다음 형식을 사용합니다.

키 탭 유형	키 탭 파일 이름
NODE_SPN	<NodeName>.keytab
NODE_AC_SPN	_AdminConsole.keytab
NODE_HTTP_SPN	webapp_http.keytab
SERVICE_PROCESS_SPN	<ServiceName>.keytab

키 탭 유형

키 탭의 유형입니다. 키 탭 유형은 다음 중 하나일 수 있습니다.

- NODE_SPN. 노드 프로세스에 대한 키 탭 파일입니다.
- NODE_AC_SPN. Informatica Administrator 서비스 프로세스에 대한 키 탭 파일입니다.
- NODE_HTTP_SPN. 노드의 HTTP 프로세스에 대한 키 탭 파일입니다.
- SERVICE_PROCESS_SPN. 서비스 프로세스에 대한 키 탭 파일입니다.

노드 수준의 서비스 사용자

다음 예제에서는 노드 수준의 서비스 사용자에 대해 생성된 SPNKeytabFormat.txt 파일의 콘텐츠를 보여 줍니다.

ENTITY_NAME	SPN	KEY_TAB_NAME	KEY_TAB_TYPE
Node01	isp/Node01/InfaDomain@MY.SVCREALM.COM	Node01.keytab	NODE_SPN
Node01	HTTP/NodeHost01.enterprise.com@MY.SVCREALM.COM	webapp_http.keytab	NODE_HTTP_SPN
Node02	isp/Node02/InfaDomain@MY.SVCREALM.COM	Node02.keytab	NODE_SPN
Node02	HTTP/NodeHost02.enterprise.com@MY.SVCREALM.COM	webapp_http.keytab	NODE_HTTP_SPN
Node03	isp/Node03/InfaDomain@MY.SVCREALM.COM	Node03.keytab	NODE_SPN
Node03	HTTP/NodeHost03.enterprise.com@MY.SVCREALM.COM	webapp_http.keytab	NODE_HTTP_SPN

프로세스 수준의 서비스 사용자

다음 예제에서는 프로세스 수준의 서비스 사용자에 대해 생성된 SPNKeytabFormat.txt 파일의 콘텐츠를 보여 줍니다.

ENTITY_NAME	SPN	KEY_TAB_NAME	KEY_TAB_TYPE
Node01	isp/Node01/InfaDomain@MY.SVCREALM.COM	Node01.keytab	NODE_SPN
Node01	_AdminConsole/Node01/InfaDomain@MY.SVCREALM.COM	_AdminConsole.keytab	NODE_AC_SPN
Node01	HTTP/NodeHost01.enterprise.com@MY.SVCREALM.COM	webapp_http.keytab	NODE_HTTP_SPN
Node02	isp/Node02/InfaDomain@MY.SVCREALM.COM	Node02.keytab	NODE_SPN
Node02	_AdminConsole/Node02/InfaDomain@MY.SVCREALM.COM	_AdminConsole.keytab	NODE_AC_SPN
Node02	HTTP/NodeHost02.enterprise.com@MY.SVCREALM.COM	webapp_http.keytab	NODE_HTTP_SPN
Service10:Node01	Service10/Node01/InfaDomain@MY.SVCREALM.COM	Service10.keytab	
SERVICE_PROCESS_SPN			
Service100:Node02	Service100/Node02/InfaDomain@MY.SVCREALM.COM	Service100.keytab	
SERVICE_PROCESS_SPN			
Service200:Node02	Service200/Node02/InfaDomain@MY.SVCREALM.COM	Service200.keytab	
SERVICE_PROCESS_SPN			

서비스 사용자 이름 및 키 탭 파일 생성

Informatica 형식의 SPN 및 키 탭 파일 목록을 생성한 후에 Kerberos 관리자에게 요청을 보내어 SPN을 Kerberos 사용자 데이터베이스에 추가하고 키 탭 파일을 생성하도록 하십시오.

SPN 및 키 탭 파일을 작성할 경우 다음 지침을 사용하십시오.

UPN(사용자 이름)은 SPN과 동일해야 합니다.

서비스 사용자의 사용자 계정을 작성할 경우 SPN과 이름이 동일한 UPN을 설정해야 합니다. Informatica 도메인의 응용 프로그램 서비스는 운영 방식에 따라 서비스 또는 클라이언트로 작동할 수 있습니다. 동일한 UPN 및 SPN으로 식별 가능하도록 서비스 사용자를 구성해야 합니다.

사용자 계정은 하나의 SPN에만 연결되어야 합니다. 사용자 계정 하나에 대해 여러 개의 SPN을 설정하지 마십시오.

Microsoft Active Directory에서 위임을 활성화합니다.

Informatica 도메인에서 사용되는 서비스 사용자로 모든 사용자 계정에 대해 위임을 활성화해야 합니다. Microsoft Active Directory 서비스에서 SPN을 설정한 각 사용자 계정에 대해 **모든 서비스에 대한 위임용으로 이 사용자 트러스트(Kerberos만)** 옵션을 설정하십시오.

사용자가 특정 서비스에 인증되고 해당 서비스가 인증된 사용자의 자격 증명을 사용하여 다른 서비스에 연결할 경우 위임된 인증이 발생합니다. Informatica 도메인의 서비스는 작업을 완료하기 위해 다른 서비스에 연결해야 하기 때문에 Informatica 도메인을 위해 Microsoft Active Directory에서 위임 옵션이 활성화되어야 합니다.

ktpass 유틸리티를 사용하여 서비스 사용자 키 탭 파일을 작성합니다.

Microsoft Active Directory는 키 탭 파일을 작성할 수 있는 ktpass 유틸리티를 제공합니다. Informatica는 Microsoft Active Directory에서만 Kerberos 인증을 지원하며, ktpass를 통해 작성된 키 탭 파일만 인증해 왔습니다.

노드의 키 탭 파일은 해당 노드를 호스트하는 시스템에서 사용 가능해야 합니다. 기본적으로 키 탭 파일은 다음 디렉터리에 저장됩니다. <Informatica 설치 디렉터리>/isp/config/keys 설치 중에 키 탭 파일을 저장할 노드의 디렉터리를 지정할 수 있습니다.

Kerberos 관리자로부터 키 탭 파일을 받으면 Informatica 서비스를 설치하려는 시스템에서 액세스할 수 있는 디렉터리에 키 탭 파일을 복사하십시오. Informatica 설치 프로그램을 실행할 때 키 탭 파일의 위치를 지정하십시오. Informatica 설치 프로그램은 Informatica 노드의 키 탭 파일 디렉터리로 키 탭 파일을 복사합니다.

서비스 사용자 이름 및 키 탭 파일 문제 해결

Kerberos 유틸리티를 사용하여 Kerberos 관리자가 작성한 서비스 사용자 및 키 탭 파일 이름이 사용자가 요청한 서비스 사용자 및 키 탭 파일 이름과 일치하는지 확인할 수 있습니다. 또한 이 유틸리티를 사용하여 Kerberos KDC(키 배포 센터)의 상태를 확인할 수도 있습니다.

setspn, *kinit* 및 *klist* 같은 Kerberos 유틸리티를 사용하여 SPN 및 키 탭 파일을 보고 확인할 수 있습니다. 이 유틸리티를 사용하려면 KRB5_CONFIG 환경 변수에 Kerberos 구성 파일의 경로 및 파일 이름이 포함되어 있는지 확인하십시오.

참고: 다음 예제에서는 Kerberos 유틸리티를 사용하여 SPN 및 키 탭 파일이 유효한지 확인하는 방법을 보여 줍니다. Kerberos 관리자가 유틸리티를 사용하여 Informatica 도메인에 필요한 SPN 및 키 탭 파일을 작성하는 방법과 예제가 다를 수 있습니다. Kerberos 유틸리티 실행에 대한 자세한 내용은 Kerberos 설명서를 참조하십시오.

다음 유틸리티를 사용하여 SPN 및 키 탭 파일을 확인합니다.

klist

*klist*를 사용하여 키 탭 파일의 Kerberos 사용자 및 키를 나열할 수 있습니다. 키 탭 파일의 키와 키 탭 항목의 타임스탬프를 나열하려면 다음 명령을 실행합니다.

```
klist -k -t <keytab_file>
```

다음 출력 예제에서는 키 탭 파일의 사용자를 표시합니다.

```
Keytab name: FILE:int_srvc01.keytab
KVNO Timestamp          Principal
-----
3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
```

kinit

*kinit*를 사용하여 사용자 계정에 대한 티켓 부여 티켓을 요청하여 KDC가 실행 중이고 티켓을 부여할 수 있는지 확인할 수 있습니다. 사용자 계정에 대한 티켓 부여 티켓을 요청하려면 다음 명령을 실행합니다.

```
kinit <user_account>
```

또한 *kinit*를 사용하여 티켓 부여 티켓을 요청하고, 키 탭 파일을 사용하여 Kerberos 연결을 설정할 수 있는지 확인할 수 있습니다. SPN에 대한 티켓 부여 티켓을 요청하려면 다음 명령을 실행합니다.

```
kinit -V -k -t <keytab_file> <SPN>
```

다음 출력 예제에서는 지정된 키 탭 파일 및 SPN에 대한 기본 캐시에 작성된 티켓 부여 티켓을 보여 줍니다.

```
Using default cache: /tmp/krb5cc_10000073
Using principal: int_srvc01/node01_vMPE/Domn96_vMPE@REALM
Using keytab: int_srvc01.keytab
Authenticated to Kerberos v5
```

setspn

*setspn*을 사용하여 Active Directory 서비스 계정의 SPN을 보거나, 수정 또는 삭제할 수 있습니다. Active Directory 서비스를 호스트하는 시스템에서 명령줄 창을 열고 명령을 실행합니다.

사용자 계정과 연관된 SPN을 보려면 다음 명령을 실행합니다.

```
setspn -L <user_account>
```

다음 출력 예제에서 사용자 계정 is96svc와 연관된 SPN을 보여 줍니다.

```
Registered ServicePrincipalNames for CN=is96svc,OU=AllSvcAccts,OU=People,
DC=ds,DC=intrac0rp,DC=zec0rp:
int_srvc01/node02_vMPE/Domn96_vMPE
```

SPN과 연관된 사용자 계정을 보려면 다음 명령을 실행합니다.

```
setspn -Q <SPN>
```

다음 출력 예제에서는 SPN int_srvc01/node02_vMPE/Domn96_vMPE와 연관된 사용자 계정을 보여 줍니다.

```
Checking domain DC=ds,DC=intrac0rp,DC=zec0rp
CN=is96svc,OU=AllSvcAccts,OU=People,DC=ds,DC=intrac0rp,DC=zec0rp
int_srvc01/node02_vMPE/Domn96_vMPE
```

```
Existing SPN found!
```

중복 SPN을 검색하려면 다음 명령을 실행합니다.

```
setspn -X
```

다음 출력 예제에서는 하나의 SPN과 연관된 여러 사용자 계정을 보여 줍니다.

```
Checking domain DC=ds,DC=intrac0rp,DC=zec0rp
Processing entry 1125
HOST/mtb01.REALM is registered on these accounts:
CN=Team1svc,OU=AllSvcAccts,OU=People,DC=ds,DC=intrac0rp,DC=zec0rp
CN=MTB1svc,OU=IIS,OU=WPC960K3,OU=WINServers,DC=ds,DC=intrac0rp,DC=zec0rp
```

참고: 중복되는 SPN을 검색하는 데 시간이 많이 걸리고 많은 메모리 양이 사용될 수 있습니다.

kdestroy

*kdestroy*를 사용하여 활성 Kerberos 권한 부여 티켓 및 이를 포함하는 사용자 자격 증명 캐시를 삭제할 수 있습니다. 매개 변수 없이 *kdestroy*를 실행할 경우 기본 자격 증명 캐시를 삭제합니다.

제 6 장

설치 프로그램 메시지에 필요한 정보 기록

이 장에 포함된 항목:

- [설치 프로그램 메시지 기록을 위한 검사 목록, 89](#)
- [Record Information for Installer Prompts Overview, 90](#)
- [도메인, 90](#)
- [노드, 91](#)
- [Distribution Packages, 91](#)
- [응용 프로그램 서비스, 91](#)
- [데이터베이스, 92](#)
- [보안 데이터베이스에 대한 연결 문자열, 94](#)
- [보안 데이터 저장소, 96](#)
- [Kerberos, 97](#)

설치 프로그램 메시지 기록을 위한 검사 목록

이 장에는 설치 프로그램을 실행할 때 입력해야 하는 정보가 포함되어 있습니다. 설치 프로그램을 실행하기 전에 수행해야 하는 기록 태스크를 추적하는 데 이 검사 목록을 사용하십시오.

- 생성할 노드의 이름 및 각 노드에 생성할 서비스의 이름을 기록합니다.
- 생성하려는 서비스에 연결된 각 데이터베이스에 대한 기본적인 데이터베이스 정보를 기록합니다.
- 도메인 구성 및 모델 리포지토리 데이터베이스에 보안이 구성된 경우, JDBC 연결 문자열과 필요한 보안 매개 변수를 기록합니다.
- 설치 프로그램의 사이트 키를 기록합니다.
- 설치 프로그램을 실행할 때 Kerberos 인증을 활성화하려면 도메인에 있는 각 노드의 Kerberos 정보를 기록합니다.

Record Information for Installer Prompts Overview

When you install the Informatica services, you need to know information about the domain, nodes, application services, databases, and distribution packages for the environment.

This section lists information that you need to provide when you run the installer. Informatica recommends recording installer prompts before you start the installation process. For example, you might want to create a text file of information so you can copy into the installer.

Domain Object Naming Conventions

You cannot change domain, node, and application service names. Use names that continue to work if you migrate a node to another machine or if you add additional nodes and services to the domain. In addition, use names that convey how the domain object is used. Naming conventions are provided in applicable topics.

도메인

도메인을 생성할 때는 도메인 이름과 게이트웨이 노드 이름을 입력해야 합니다.

다음 테이블에는 설치 프로세스 중에 입력해야 하는 도메인 정보가 설명되어 있습니다.

도메인 정보	설명
도메인 이름	작성하려고 계획한 도메인의 이름입니다. 이름은 128자를 초과하지 않아야 하고 7비트 ASCII여야만 합니다. 이름에는 공백이나 ` % * + ; " ? , < > \ /` 문자를 사용할 수 없습니다. DMN, DOM, DOMAIN, _<ORG>_<ENV> 같은 이름 지정 규칙 중 하나를 사용할 수 있습니다.
마스터 게이트웨이 노드 호스트 이름	마스터 게이트웨이 노드를 작성할 시스템의 정규화된 호스트 이름입니다. 시스템이 단일 네트워크 이름을 갖는 경우 기본 호스트 이름을 사용하십시오. 노드 호스트 이름에는 밑줄(_) 문자를 사용할 수 없습니다. 시스템이 여러 네트워크 이름을 갖는 경우 대체 네트워크 이름을 사용하도록 기본 호스트 이름을 수정할 수 있습니다. 시스템이 단일 네트워크 이름을 갖는 경우 기본 호스트 이름을 사용하십시오. 참고: localhost는 사용하지 마십시오. 호스트 이름은 명시적으로 시스템을 식별해야 합니다.
마스터 게이트웨이 노드 이름	이 시스템에 작성하려고 계획한 마스터 게이트웨이 노드의 이름입니다. 노드 이름은 시스템의 호스트 이름이 아닙니다. Node<node##>_<ORG>_<선택적 구분자>_<ENV> 이름 지정 규칙을 사용할 수 있습니다.

노드

Informatica 서비스를 설치할 때 설치 시스템을 도메인에 노드로 추가합니다. 여러 노드를 도메인에 추가할 수 있습니다.

다음 테이블에는 도메인에 가입할 때 입력해야 하는 노드 정보가 설명되어 있습니다.

노드 정보	설명
노드 호스트 이름	<p>노드가 생성될 시스템의 정규화된 호스트 이름입니다. 시스템이 단일 네트워크 이름을 갖는 경우 기본 호스트 이름을 사용하십시오. 노드 호스트 이름에는 밑줄(_) 문자를 사용할 수 없습니다.</p> <p>시스템이 여러 네트워크 이름을 갖는 경우 대체 네트워크 이름을 사용하도록 기본 호스트 이름을 수정할 수 있습니다. 시스템이 단일 네트워크 이름을 갖는 경우 기본 호스트 이름을 사용하십시오.</p> <p>참고: localhost는 사용하지 마십시오. 호스트 이름은 명시적으로 시스템을 식별해야 합니다.</p>
노드 이름	<p>이 시스템에 생성하려고 계획한 노드의 이름입니다. 노드 이름은 시스템의 호스트 이름이 아닙니다.</p> <p>Node<node###>_<ORG>_<선택적 구분자>_<ENV> 이름 지정 규칙을 사용할 수 있습니다.</p>

Distribution Packages

If you are going to install a distribution package through the installer, record the distribution package that you downloaded.

응용 프로그램 서비스

응용 프로그램 서비스 이름과 해당 응용 프로그램 서비스를 생성할 노드를 기록하십시오.

다음 테이블에는 설치 프로그램을 실행할 때 생성할 수 있는 응용 프로그램 서비스가 나열되어 있습니다.

응용 프로그램 서비스	이름 지정 규칙
카탈로그 서비스	CS_<ORG>_<ENV>
콘텐츠 관리	CMS_<ORG>_<ENV>
데이터 통합 서비스	DIS_<ORG>_<ENV>
Data Privacy Management Service	DPM_<ORG>_<ENV>
대화형 데이터 준비 서비스	DPS_<ORG>_<ENV>
엔터프라이즈 데이터 준비 서비스	EDLS_<ORG>_<ENV>

응용 프로그램 서비스	이름 지정 규칙
메타데이터 액세스 서비스	MAS_<ORG>_<ENV>
Informatica 클러스터 서비스	ICS_<ORG>_<ENV>
모델 리포지토리 서비스	MRS_<ORG>_<ENV>
모니터링 모델 리포지토리 서비스	mMRS_<ORG>_<ENV>
PowerCenter 리포지토리 서비스	PCRS, RS_<ORG>_<ENV>
PowerCenter 통합 서비스	PCIS, IS_<ORG>_<ENV>

모든 서비스 이름 지정 규칙에 대한 자세한 내용은 Informatica 네트워크를 통해 제공되는 다음 Informatica Velocity Best Practice 문서를 참조하십시오. [Velocity Naming Conventions](#)

중요: Kerberos 인증을 사용할 계획이면 키 탭 파일을 작성하기 전에 응용 프로그램 서비스 및 노드 이름을 알고 있어야 합니다.

데이터베이스

설치를 계획하는 경우 필요한 관계형 데이터베이스도 계획해야 합니다. 도메인에는 구성 정보, 사용자 계정 권한 및 사용 권한을 저장하기 위한 데이터베이스가 필요합니다. 일부 응용 프로그램 서비스는 해당 응용 프로그램 서비스에 의해 처리되는 정보를 저장하기 위해 데이터베이스를 필요로 합니다.

도메인

다음 테이블에는 설치 프로세스 중에 입력해야 하는 정보가 설명되어 있습니다.

데이터베이스 정보	설명
도메인 구성 데이터베이스 유형	도메인 구성 리포지토리에 대한 데이터베이스 유형입니다. 도메인 구성 리포지토리는 IBM DB2 UDB, Microsoft SQL Server, Oracle, PostgreSQL 또는 Sybase ASE를 지원합니다.
도메인 구성 데이터베이스 호스트 이름	데이터베이스를 호스트하는 시스템의 이름입니다.

콘텐츠 관리 서비스

다음 테이블에는 설치 프로세스 중에 입력해야 하는 정보가 설명되어 있습니다.

데이터베이스 정보	설명
참조 데이터 웨어하우스 데이터베이스 유형	참조 데이터 웨어하우스의 데이터베이스 유형입니다. 참조 데이터 웨어하우스는 IBM DB2 UDB, Microsoft Azure SQL Database, Microsoft SQL Server, Oracle 또는 PostgreSQL을 지원합니다.
참조 데이터 웨어하우스 데이터베이스 호스트 이름	데이터베이스를 호스트하는 시스템의 이름입니다.

데이터 통합 서비스

다음 테이블에는 설치 프로세스 중에 입력해야 하는 정보가 설명되어 있습니다.

데이터베이스 정보	설명
데이터 개체 캐시 데이터베이스 유형	데이터 개체 캐시 데이터베이스의 데이터베이스 유형입니다. 데이터 개체 캐시 데이터베이스는 IBM DB2 UDB, Microsoft SQL Server 또는 Oracle을 지원합니다.
데이터 개체 캐시 데이터베이스 호스트 이름	데이터베이스를 호스트하는 시스템의 이름입니다.
프로파일링 웨어하우스 데이터베이스 유형	프로파일링 웨어하우스의 데이터베이스 유형입니다. 프로파일링 웨어하우스는 IBM DB2 UDB, Microsoft SQL Server 또는 Oracle을 지원합니다.
프로파일링 웨어하우스 데이터베이스 호스트 이름	데이터베이스를 호스트하는 시스템의 이름입니다.
워크플로우 데이터베이스 유형	워크플로우 데이터베이스의 데이터베이스 유형입니다. 워크플로우 데이터베이스는 IBM DB2 UDB, Microsoft Azure SQL Database, Microsoft SQL Server, Oracle 또는 PostgreSQL을 지원합니다.
워크플로우 데이터베이스 호스트 이름	데이터베이스를 호스트하는 시스템의 이름입니다.

모델 리포지토리 서비스

다음 테이블에는 설치 프로세스 중에 입력해야 하는 정보가 설명되어 있습니다.

데이터베이스 정보	설명
모델 리포지토리 데이터베이스 유형	모델 리포지토리의 데이터베이스 유형입니다. 모델 리포지토리는 IBM DB2 UDB, Microsoft SQL Server, PostgreSQL 또는 Oracle을 지원합니다.
모델 리포지토리 데이터베이스 호스트 이름	데이터베이스를 호스트하는 시스템의 이름입니다.

PowerCenter 리포지토리 서비스

다음 테이블에는 설치 프로세스 중에 입력해야 하는 정보가 설명되어 있습니다.

데이터베이스 정보	설명
PowerCenter 리포지토리 데이터베이스 유형	PowerCenter 리포지토리의 데이터베이스 유형입니다. PowerCenter 리포지토리는 IBM DB2 UDB, Microsoft SQL Server, Oracle 또는 PostgreSQL을 지원합니다.
PowerCenter 리포지토리 데이터베이스 호스트 이름	데이터베이스를 호스트하는 시스템의 이름입니다.

보안 데이터베이스에 대한 연결 문자열

보안 데이터베이스에 리포지토리를 작성하는 경우 데이터베이스에 대한 트러스트 저장소 정보와 데이터베이스의 보안 매개 변수를 포함하는 JDBC 연결 문자열을 제공해야 합니다.

설치 중에 보안 데이터베이스에서 도메인 구성 리포지토리를 작성할 수 있습니다. 보안 데이터베이스에서 모델 리포지토리 및 PowerCenter 리포지토리도 작성할 수 있습니다.

다음 데이터베이스에 대한 보안 연결을 구성할 수 있습니다.

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- PostgreSQL
- Azure PostgreSQL
- Oracle

참고: Sybase 데이터베이스에 대한 보안 연결은 구성할 수 없습니다.

보안 데이터베이스에 대한 연결을 구성할 때 JDBC 연결 문자열에 연결 정보를 지정해야 합니다. 연결 문자열에는 데이터베이스 서버의 호스트 이름과 포트 번호에 더해 보안 매개 변수가 포함되어야 합니다.

The following table describes the security parameters that you must include in the JDBC connection string:

Parameter	Description
EncryptionMethod	Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to SSL .
ValidateServerCertificate	Optional. Indicates whether Informatica validates the certificate that is sent by the database server. If this parameter is set to True, Informatica validates the certificate that is sent by the database server. If you specify the HostNameInCertificate parameter, Informatica also validates the host name in the certificate. If this parameter is set to false, Informatica doesn't validate the certificate that is sent by the database server. Informatica ignores any truststore information that you specify.
HostNameInCertificate	Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the SSL certificate. If SSL encryption and validation is enabled and this property is not specified, the driver uses the server name specified in the connection URL or data source of the connection to validate the certificate.
cryptoProtocolVersion	Required. Specifies the cryptographic protocol to use to connect to a secure database. You can set the parameter to cryptoProtocolVersion=TLSv1.1 or cryptoProtocolVersion=TLSv1.2 based on the cryptographic protocol used by the database server.

You can use the following syntax in the JDBC connection string to connect to a secure database:
IBM DB2

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
```

Oracle

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=<service name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS server name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
```

Microsoft SQL Server with Windows NT credentials

If you specified the Windows NT credentials for the Model repository database on Microsoft SQL Server, specify the connection string syntax to include the authentication method as NTLM.

Microsoft SQL Server that uses the default instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<호스트 이름>:<포트 번호>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server that uses a named instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<호스트 이름>\<명명된 인스턴스 이름>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

참고: The installer doesn't validate the connection string. Verify that the connection string contains all the connection parameters and security parameters required by your database.

보안 데이터 저장소

Informatica 서비스를 설치할 때 설치 프로그램이 생성하는 사이트 키를 백업하고 사이트 키를 저장해야 합니다. 사이트 키를 분실하는 경우 사이트 키를 다시 생성할 수 없습니다.

다음 테이블을 사용하여 보안 데이터 저장소를 구성하는 데 필요한 정보를 기록하십시오.

Property	Description
Encryption key directory	Directory in which to store the encryption key for the domain. By default, the encryption key is created in the following directory: <Informatica installation directory>/isp/config/keys .
Specify if you want to back up the site key that the installer generates or not:	Specify if you want to back up the site key that the installer generates or not: <ul style="list-style-type: none"> - Select 1 for No. If you choose No, the installer exits. - Select 2 for Yes. If you choose Yes, you agree to back up the file manually. A unique site key is generated. If you lose the site key, you cannot generate the site key again. Make sure that you save a copy of this key and do not share the unique site key with others.

Kerberos

Informatica 응용 프로그램 서비스를 설치할 때 Informatica 도메인의 옵션을 활성화하여 도메인, 서비스 및 데이터베이스에 대한 보안을 구성할 수 있습니다.

Kerberos 인증을 활성화한 경우에 기본 파일을 사용하지 않으려면 키 저장소 및 트러스트 저장소 디렉터리 같은 정보를 제공해야 합니다. 각 노드에는 해당 노드의 모든 서비스가 사용하는 키 저장소와 트러스트 저장소가 포함되어 있어야 합니다.

다음 테이블에는 설치 중 제공해야 하는 보안 정보가 설명되어 있습니다.

보안 정보	설명
서비스 영역 이름	Informatica 도메인 서비스가 속하는 Kerberos 영역의 이름입니다. 해당 영역 이름은 대문자여야 합니다. 서비스 영역 이름과 사용자 영역 이름은 동일해야 합니다.
사용자 영역 이름	Informatica 도메인 사용자가 속하는 Kerberos 영역의 이름입니다. 해당 영역 이름은 대문자여야 합니다. 서비스 영역 이름과 사용자 영역 이름은 동일해야 합니다.
Kerberos 구성 파일의 위치	<i>krb5.conf</i> 라는 Kerberos 구성 파일이 저장되는 디렉터리입니다. 이 구성 파일에 특정 속성이 설정되어 있어야 합니다. Kerberos 구성 파일을 복사하거나 업데이트할 수 있는 사용 권한이 없으면 Kerberos 관리자에게 파일 업데이트를 요청해야 할 수 있습니다.
키 저장소 파일 디렉터리	키 저장소 파일이 포함된 디렉터리입니다. 이 디렉터리에는 <i>infa_keystore.jks</i> 및 <i>infa_keystore.pem</i> 이라는 파일이 포함되어야 합니다.
키 저장소 암호	키 저장소 <i>infa_keystore.jks</i> 의 일반 텍스트 암호입니다.
트러스트 저장소 파일 디렉터리	트러스트 저장소 파일이 포함된 디렉터리입니다. 이 디렉터리에는 <i>infa_truststore.jks</i> 및 <i>infa_truststore.pem</i> 이라는 파일이 포함되어야 합니다.
트러스트 저장소 암호	<i>infa_truststore.jks</i> 파일의 암호입니다.

제 7 장

서비스 설치 프로그램 소개

이 장에 포함된 항목:

- [서비스 설치 프로그램 작업, 98](#)
- [보안 파일 및 디렉터리, 98](#)
- [설치 전 유틸리티, 99](#)
- [설치 전 시스템 검사 도구\(i10Pi\) 실행 \(콘솔 모드\), 99](#)
- [설치 전 시스템 검사 도구\(i10Pi\) 실행\(그래픽 모드\), 102](#)
- [자동 모드에서 설치 전 시스템 검사 도구\(i10Pi\) 실행, 108](#)

서비스 설치 프로그램 작업

설치 프로그램은 설치할 제품에 따라 설치 태스크를 수행합니다.

설치 프로그램은 다음 태스크를 수행할 수 있습니다.

1. 설치 전 유효성 검사 및 시스템 검사를 수행합니다.
2. 도메인을 생성하거나, 기존 도메인에 노드를 조인합니다.
3. 서비스 지원을 위한 바이너리를 설치합니다.
4. 응용 프로그램 서비스를 생성합니다.
5. 도메인과 서비스 간의 보안을 구성합니다.
6. 생성한 도메인 및 응용 프로그램 서비스를 시작합니다.
7. 로그 파일에 메시지를 씁니다.

보안 파일 및 디렉터리

Informatica를 설치하거나 업그레이드할 경우, 설치 프로그램은 제한적인 액세스를 필요로 하는 도메인 암호화 키 파일 및 **nodemeta.xml** 등의 **Informatica** 파일을 저장할 디렉터리를 작성합니다. 설치 프로그램은 디렉터리 및 해당 디렉터리의 파일별로 서로 다른 사용 권한을 할당합니다.

기본적으로 설치 프로그램은 **Informatica** 설치 디렉터리 내에 다음 디렉터리를 작성합니다.

<Informatica **설치 디렉터리**>/isp/config

nodemeta.xml 파일을 포함합니다. 암호화 키 파일이 저장되는 /keys 디렉터리 또한 포함합니다. Kerberos 인증을 사용하도록 도메인을 구성하는 경우, /keys 디렉터리에는 Kerberos 키 탭 파일도 포함됩니다. 이 파일을 저장할 다른 디렉터리를 지정할 수 있습니다. 설치 프로그램은 기본 디렉터리와 동일한 사용 권한을 지정된 디렉터리에 할당합니다.

<Informatica **설치 디렉터리**>/services/shared/security

도메인에 대해 보안 통신을 활성화하는 경우, /security 디렉터리에 기본 SSL 인증서의 키 저장소 및 트러스트 저장소 파일이 포함됩니다.

디렉터리 및 파일의 보안을 유지하기 위해 설치 프로그램이 디렉터리 및 디렉터리의 파일에 대한 액세스를 제한합니다. 설치 프로그램은 디렉터리 및 파일을 소유한 그룹 및 사용자 계정에 특정 사용 권한을 할당합니다.

디렉터리 및 파일에 할당되는 사용 권한에 대한 자세한 내용은 Informatica 보안 가이드를 참조하십시오.

설치 전 유틸리티

Informatica는 Informatica 서비스 설치 프로세스를 용이하게 하기 위한 유틸리티를 제공합니다. Informatica 설치 프로그램을 사용하여 이 유틸리티를 실행할 수 있습니다.

Informatica 서비스를 설치하기 전에 다음 유틸리티를 실행하십시오.

설치 전 시스템 검사 도구(i10Pi)

설치 전 시스템 검사 도구(i10Pi)에서는 컴퓨터가 Informatica 설치를 수행하기 위한 시스템 요구 사항을 충족하는지 여부를 확인합니다. 설치를 시작하기 전에 최소 시스템 요구 사항을 확인하는 것이 좋습니다. 설치를 수행하기 전에 시스템 검사 도구를 실행하면 설치 프로그램에서 시스템 검사 중에 사용자가 입력한 정보에 따라 데이터베이스 연결 및 도메인 포트 번호 등의 특정 필드에 대해 값을 설정합니다.

Informatica Kerberos SPN 형식 생성기

Informatica Kerberos SPN 형식 생성기는 Kerberos SPN(서비스 사용자 이름) 및 키 탭 파일 이름의 목록을 Informatica에서 필요한 형식에 따라 생성합니다. Kerberos 인증을 사용하는 네트워크에 Informatica를 설치하는 경우, 이 유틸리티를 실행하여 서비스 사용자 및 키 탭 파일 이름을 informatica 형식으로 생성하십시오. 그런 다음, 설치를 시작하기 전에 Kerberos 관리자에게 요청하여 SPN을 Kerberos 사용자 데이터베이스에 추가하고 키 탭 파일을 작성하도록 하십시오.

설치 전 시스템 검사 도구(i10Pi) 실행 (콘솔 모드)

설치 전 시스템 검사 도구(i10Pi)를 실행하여 시스템이 설치 또는 업그레이드에 대한 시스템 요구 사항을 충족하는지 여부를 확인합니다.

시스템 요구 사항을 확인했고 도메인 구성 리포지토리 데이터베이스를 준비했는지 확인하십시오.

1. 시스템 사용자 계정으로 시스템에 로그인합니다.
2. 기타 모든 응용 프로그램을 닫습니다.
3. 셸 명령줄에서 설치 파일을 실행합니다.

설치 프로그램에 로컬 환경 변수가 설정되었는지 확인하라는 메시지가 표시됩니다.

4. 환경 변수가 설정되지 않은 경우 **n**을 눌러 설치 프로그램을 종료하고 필요에 따라 환경 변수를 설정합니다.
환경 변수가 설정된 경우 **y**를 눌러 계속 진행합니다.
5. **1**를 눌러 **Informatica**를 설치하거나 업그레이드합니다.
6. **1**을 눌러 시스템이 설치 또는 업그레이드에 대한 시스템 요구 사항을 충족하는지 여부를 확인하는 설치 전 시스템 검사 도구(i10Pi)를 실행합니다.
7. **Informatica** 설치 전 시스템 검사 도구(i10Pi) **시작** 섹션에서 **Enter** 키를 누릅니다.
시스템 정보 섹션이 나타납니다.
8. 설치 디렉터리의 절대 경로를 입력합니다.
경로의 디렉터리 이름에 공백이나 @|* \$ # !와 같은 특수 문자가 있어서는 안 됩니다. % () { } [] , ; '

참고: Informatica는 설치 디렉터리 경로에 영숫자 문자를 사용할 것을 권장합니다. á 또는 €와 같은 특수 문자를 사용할 경우 런타임에 예기치 않은 결과가 발생할 수 있습니다.
9. **Enter** 키를 누릅니다.
10. 시스템에서 생성하거나 업그레이드할 노드에 대한 시작 포트 번호를 입력합니다. 노드의 기본 포트 번호는 6005입니다.
11. **Enter** 키를 누릅니다.
데이터베이스 및 연결 정보 섹션이 나타납니다.
12. 사용자 지정 JDBC 연결 문자열을 사용하여 JDBC 연결 정보를 입력하려면 **1**를 누릅니다. JDBC URL 정보를 사용하여 JDBC 연결 정보를 입력하려면 **2**를 누릅니다.
보안 데이터베이스에 연결하려면 사용자 지정 JDBC 연결 문자열을 사용하여 JDBC 연결을 입력해야 합니다.
13. JDBC 연결 정보를 입력합니다.
 - 사용자 지정 JDBC 연결 문자열을 사용하여 연결 정보를 입력하려면 연결 문자열을 입력하고 연결 매개 변수를 지정합니다.
Use the following syntax in the JDBC connection string:
IBM DB2


```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

 Oracle


```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

 Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:


```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

 Microsoft SQL Server


```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

 Microsoft SQL Server with Windows NT credentials

If you specified the Windows NT credentials for the Model repository database on Microsoft SQL Server, specify the connection string syntax to include the authentication method as NTLM.

 Microsoft SQL Server that uses the default instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<호스트 이름>:<포트 번호>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server that uses a named instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<호스트 이름>\<명명된 인스턴스 이름>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

Azure SQL Database with Active Directory authentication

```
jdbc:informatica: sqlserver://
<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>
```

PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

Sybase

```
jdbc:Informatica:sybase://<host name>:<port number>;DatabaseName=
```

Verify that the connection string contains all the connection parameters required by your database system.

- JDBC URL 정보를 사용하여 연결 정보를 입력하려면 JDBC URL 속성을 지정합니다. 다음 테이블에는 연결 정보가 설명되어 있습니다.

프롬프트	설명
데이터베이스 유형	도메인 구성 리포지토리의 데이터베이스 유형입니다. 다음 데이터베이스 유형에서 선택하십시오. - 1 - Oracle - 2 - Microsoft SQL Server - 3 - IBM DB2 - 4 - Sybase ASE - 5 - PostgreSQL
데이터베이스 사용자 ID	도메인 구성 리포지토리에 대한 데이터베이스 사용자 계정의 사용자 ID입니다.
데이터베이스 사용자 암호	데이터베이스 사용자 계정의 암호입니다.
데이터베이스 호스트 이름	데이터베이스 서버의 호스트 이름입니다.

프롬프트	설명
데이터베이스 포트 번호	데이터베이스의 포트 번호입니다.
데이터베이스 서비스 이름	Oracle 및 IBM DB2 데이터베이스의 서비스 이름이거나 PostgreSQL, Microsoft SQL Server 및 Sybase ASE의 데이터베이스 이름입니다.

- 보안 데이터베이스에 연결하려면 **1**을 선택하여 사용자 지정 문자열로 연결 문자열을 입력하십시오. 보안 매개 변수를 연결 매개 변수와 함께 포함해야 합니다. 보안 데이터베이스의 JDBC 연결에 포함해야 하는 보안 매개 변수에 대한 자세한 내용은 [“보안 데이터베이스에 대한 연결 문자열” 페이지 94](#)을 참조하십시오.

이 도구는 하드 드라이브의 설정, 포트의 가용성 및 데이터베이스의 구성을 검사합니다. 시스템 검사가 완료된 후 **시스템 검사 요약** 섹션에 시스템 검사 결과가 표시됩니다.

14. 시스템 검사 결과를 분석합니다.

Each requirement is listed, along with one of the following check statuses:

- [Pass] - The requirement meets the criteria for the Informatica installation or upgrade.
- [Fail] - The requirement doesn't meet the criteria for the Informatica installation or upgrade. Resolve the issue before you proceed with the installation or upgrade.
- [Information] - Verify the information and perform any additional tasks as outlined in the details.

The results of the system check are saved to the following file: ...<Informatica installation directory>/Server/I10PI/I10PI/en/I10PI_summary.txt

15. **Enter** 키를 눌러 설치 전 시스템 검사 도구(i10Pi)를 닫습니다.

Informatica 서비스 설치나 업그레이드를 바로 계속하거나, 시스템 검사를 끝내고 나중에 설치나 업그레이드를 계속할 수 있습니다. 설치나 업그레이드를 바로 계속하는 경우, 설치 프로그램을 다시 시작할 필요가 없습니다.

16. Informatica 서비스 설치나 업그레이드를 바로 계속하려면 **y**를 누릅니다.

시스템 검사를 끝내고 나중에 설치나 업그레이드를 계속하려면 **n**을 누릅니다.

If the Pre-Installation (i10Pi) System Check Tool finishes with failed requirements, resolve the failed requirements and run the Pre-Installation (i10Pi) System Check Tool again.

참고: If the Informatica Pre-Installation (i10Pi) System Check Tool check finishes with failed requirements, you can still perform the Informatica installation or upgrade. However, Informatica highly recommends that you resolve the failed requirements before you proceed.

설치 전 시스템 검사 도구(i10Pi) 실행(그래픽 모드)

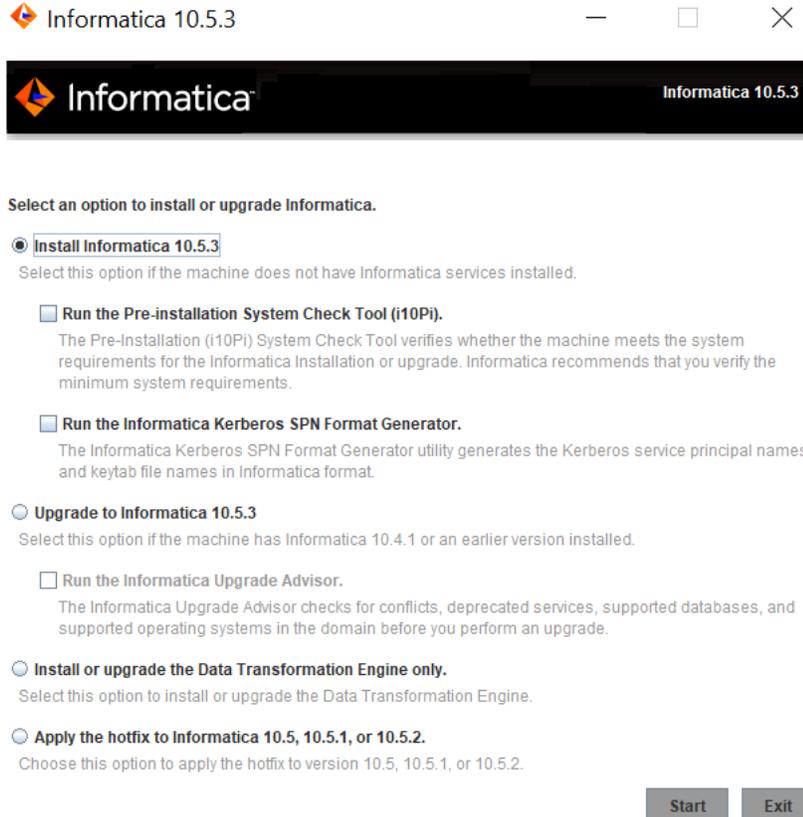
설치 전 시스템 검사 도구(i10Pi)를 실행하여 시스템이 설치 또는 업그레이드에 대한 시스템 요구 사항을 충족하는지 여부를 확인합니다.

시스템 요구 사항을 확인했고 도메인 구성 리포지토리 데이터베이스를 준비했는지 확인하십시오.

1. 시스템 사용자 계정으로 시스템에 로그인합니다.
2. 기타 모든 응용 프로그램을 닫습니다.
3. 설치 파일이 포함된 디렉터리 루트로 이동하고 관리자 권한으로 **install.bat**를 실행합니다.

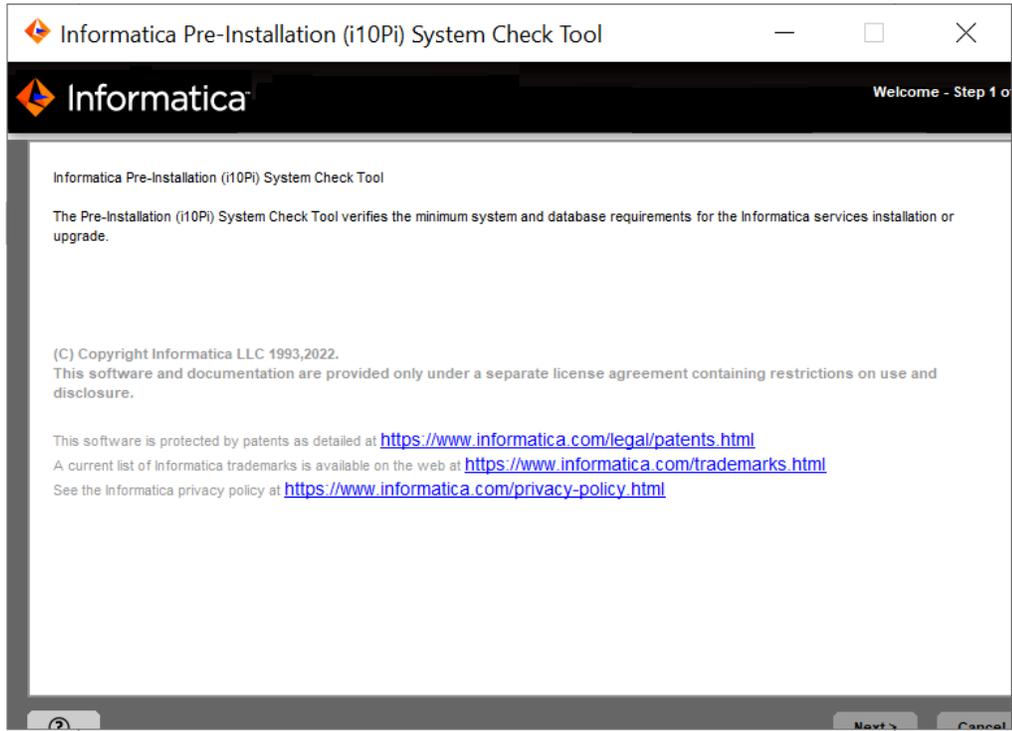
4. **Informatica 10.5.3** 설치를 선택합니다.

5. **설치 전 시스템 검사 도구(i10Pi) 실행**을 선택하여 시스템이 설치 또는 업그레이드에 대한 시스템 요구 사항을 충족하는지 여부를 확인합니다.

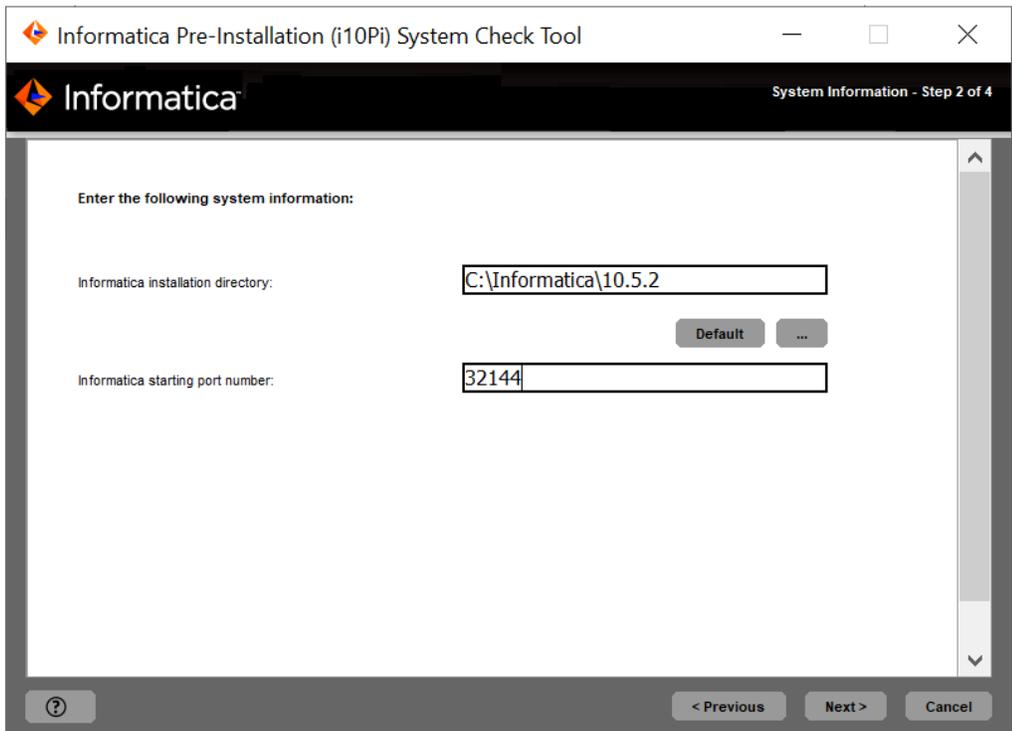


6. **시작**을 클릭합니다.

Informatica 설치 전 시스템 검사 도구(i10Pi) 시작 페이지가 나타납니다.



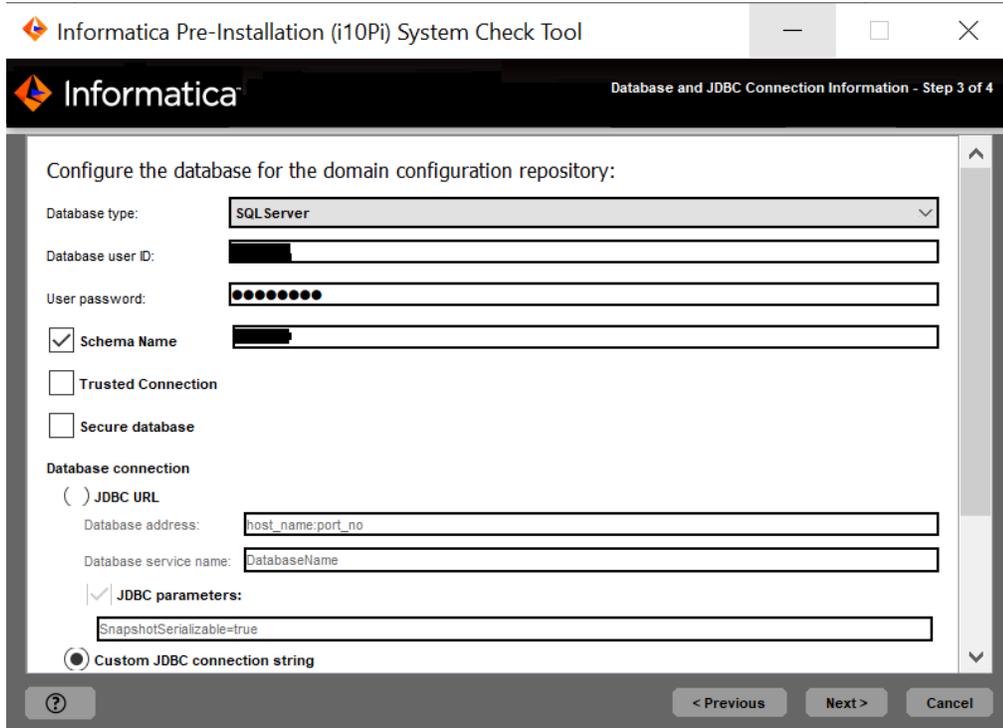
7. 다음을 클릭합니다.
시스템 정보 페이지가 나타납니다.



8. 설치 디렉터리의 절대 경로를 입력합니다.

경로의 디렉터리 이름에 공백이나 다음과 같은 특수 문자가 있어서는 안 됩니다. @ | * \$ # ! % () { } [] , ; '
참고: Informatica는 설치 디렉터리 경로에 영숫자 문자를 사용할 것을 권장합니다. á 또는 €와 같은 특수 문자를 사용할 경우 런타임에 예기치 않은 결과가 발생할 수 있습니다.

9. 시스템에서 생성하거나 업그레이드할 노드에 대한 시작 포트 번호를 입력합니다. 노드의 기본 포트 번호는 6005입니다.
10. 다음을 클릭합니다.
데이터베이스 및 JDBC 연결 정보 페이지가 나타납니다.



11. 도메인 구성 리포지토리 데이터베이스에 대한 정보를 입력합니다.

The following table describes the properties that you specify for the database and user account:

Property	Description
Database type	Database for the repository. Select one of the following databases: - Oracle - IBM DB2 - Microsoft SQL Server - PostgreSQL - Sybase ASE
Database user ID	User account for the repository database.
User password	Password for the database user account.

도메인 구성 리포지토리는 도메인의 모든 게이트웨이 노드에 액세스할 수 있어야 합니다.

12. 도메인 구성 리포지토리에 보안 데이터베이스를 사용하려는 경우 **보안 데이터베이스** 옵션을 선택합니다.

13. 데이터베이스 연결 정보를 입력합니다.

- JDBC URL 정보를 사용하여 연결 정보를 입력하려면 **JDBC URL**을 선택하고 JDBC URL 속성을 지정합니다.

The following table describes the JDBC URL properties that you specify:

Property	Description
Database address	Host name and port number for the database in the format host_name:port .
Database service name	Service or database name: - Oracle: Enter the service name. - Microsoft SQL Server: Enter the database name. - IBM DB2: Enter the service name. - Sybase ASE: Enter the database name. - PostgreSQL: Enter the database name.
JDBC parameters	Optional parameters to include in the database connection string. Use the parameters to optimize database operations for the database. Verify that the parameter string is valid. The installer does not validate the parameter string before it adds the string to the JDBC URL. If not selected, the installer creates the JDBC URL string without additional parameters.

- 사용자 지정 JDBC 연결 문자열을 사용하여 연결 정보를 입력하려면 **사용자 지정 JDBC 연결 문자열**을 선택하고 연결 문자열을 입력합니다.

Use the following syntax in the JDBC connection string:

IBM DB2

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

Microsoft SQL Server with Windows NT credentials

If you specified the Windows NT credentials for the Model repository database on Microsoft SQL Server, specify the connection string syntax to include the authentication method as NTLM.

Microsoft SQL Server that uses the default instance with Windows NT credentials:

```
"jjdbc:informatica:sqlserver://<호스트 이름>:<포트 번호>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server that uses a named instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<호스트 이름>\<명명된 인스턴스 이름>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

Azure SQL Database with Active Directory authentication

```
jdbc:informatica:sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>
```

PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

Sybase

```
jdbc:Informatica:sybase://<host name>:<port number>;DatabaseName=
```

Verify that the connection string contains all the connection parameters required by your database system.

- **보안 데이터베이스** 옵션을 선택하는 경우 **사용자 지정 JDBC 연결 문자열**을 선택하고 연결 문자열을 입력합니다.
보안 매개 변수를 연결 매개 변수와 함께 포함해야 합니다. 보안 데이터베이스의 JDBC 연결에 포함해야 하는 보안 매개 변수에 대한 자세한 내용은 [“보안 데이터베이스에 대한 연결 문자열” 페이지 94](#)을 참조하십시오.

14. **연결 테스트**를 클릭하여 데이터베이스에 연결할 수 있는지 확인한 다음 **확인**을 클릭하여 계속 진행합니다.
15. **다음**을 클릭하여 시스템 검사를 시작합니다.
이 도구는 하드 드라이브의 설정, 포트의 가용성 및 데이터베이스의 구성을 검사합니다. 시스템 검사가 완료된 후 **시스템 검사 요약** 페이지가 나타나고 시스템 검사 결과가 표시됩니다.
16. 시스템 검사 결과를 분석합니다.

Each requirement is listed, along with one of the following check statuses:

- [Pass] - The requirement meets the criteria for the Informatica installation or upgrade.
- [Fail] - The requirement doesn't meet the criteria for the Informatica installation or upgrade. Resolve the issue before you proceed with the installation or upgrade.
- [Information] - Verify the information and perform any additional tasks as outlined in the details.

The results of the system check are saved to the following file: ...<Informatica installation directory>/Server/I10PI/I10PI/en/I10PI_summary.txt

17. **완료**를 클릭하여 설치 전 시스템 검사 도구(i10Pi)를 닫습니다.

If the Pre-Installation (i10Pi) System Check Tool finishes with failed requirements, resolve the failed requirements and run the Pre-Installation (i10Pi) System Check Tool again.

참고: If the Informatica Pre-Installation (i10Pi) System Check Tool check finishes with failed requirements, you can still perform the Informatica installation or upgrade. However, Informatica highly recommends that you resolve the failed requirements before you proceed.

자동 모드에서 설치 전 시스템 검사 도구(i10Pi) 실행

자동 모드에서 설치 전 시스템 검사 도구(i10pi)를 실행하여 사용자 개입 없는 설치를 위한 시스템 요구 사항을 확인합니다.

1. Informatica 서비스 설치 프로그램 파일을 추출합니다.
2. 다음 위치로 이동합니다.
<Informatica 설치 디렉터리>/Server/I10PI
3. 자동 모드에서 I10PI 시스템 검사 도구의 속성을 지정하려면 I10PI 폴더에 있는 SilentInput.properties 파일을 업데이트합니다.
4. 자동 모드에서 i10Pi를 실행하려면 I10PI 폴더에 있는 silentInstall 파일을 실행합니다.

다음 위치의 I10PI_summary.txt 파일에서 자동 모드로 실행한 i10Pi 시스템 검사 도구의 결과를 볼 수 있습니다.
<Informatica 설치 디렉터리>/Server/I10PI/I10PI/en

If the Pre-Installation (i10Pi) System Check Tool finishes with failed requirements, resolve the failed requirements and run the Pre-Installation (i10Pi) System Check Tool again.

참고: If the Informatica Pre-Installation (i10Pi) System Check Tool check finishes with failed requirements, you can still perform the Informatica installation or upgrade. However, Informatica highly recommends that you resolve the failed requirements before you proceed.

파트 III: 서비스 설치 프로그램 실행

이 파트에 포함된 장:

- [Informatica 서비스 설치 \(콘솔 모드\), 110](#)
- [그래픽 모드에서 Informatica 서비스 설치, 155](#)
- [자동 설치 프로그램 실행, 229](#)
- [문제 해결, 232](#)

제 8 장

Informatica 서비스 설치 (콘솔 모드)

이 장에 포함된 항목:

- [Informatica 서비스 설치 개요, 110](#)
- [도메인 생성, 110](#)
- [도메인에 가입, 142](#)

Informatica 서비스 설치 개요

여러 시스템에 Informatica 서비스를 설치할 수 있습니다. 설치 중에는 데몬으로 실행되는 Informatica라는 서비스가 생성됩니다.

설치 프로그램을 처음 실행하는 경우에는 도메인을 생성합니다. 도메인이 생성되어 있고 여러 시스템에 설치하는 경우에는 도메인에 가입할 수 있습니다.

도메인을 생성하면 설치한 시스템 내의 노드가 도메인의 게이트웨이 노드가 됩니다. 도메인 내의 서비스 간에 보안 통신을 설정할지 선택할 수 있습니다. 또한 설치 프로세스 중에 일부 응용 프로그램 서비스를 생성하도록 선택할 수 있습니다.

도메인에 가입할 경우에는 생성한 노드를 게이트웨이 노드로 구성할 수 있습니다. 게이트웨이 노드를 생성할 때 Informatica Administrator에 대한 보안 HTTPS 연결 활성화를 선택할 수 있습니다.

참고: 콘솔 모드로 설치 프로그램을 실행하는 경우 Quit, Help 및 Back이라는 단어는 예약어입니다. 입력 텍스트로 이러한 단어를 사용하지 마십시오.

도메인 생성

처음으로 설치하는 경우 또는 별도 도메인의 노드를 관리하려는 경우 도메인을 생성합니다.

설치 프로그램 실행

설치 프로그램을 실행하려면 다음 단계를 수행하십시오.

1. 시스템 사용자 계정으로 시스템에 로그인하십시오.

2. 다음 명령을 실행하여 시스템에서 **DISPLAY** 변수를 지웁니다. `unset DISPLAY`
3. 기타 모든 응용 프로그램을 닫으십시오.
4. 셸 명령줄에서 `install.sh` 파일을 실행합니다.
설치 프로그램에 로컬 환경 변수가 설정되었는지 확인하라는 메시지가 표시됩니다.
5. 환경 변수가 설정되지 않은 경우 **n**을 눌러 설치 프로그램을 종료하고 필요에 따라 환경 변수를 설정합니다.
환경 변수가 설정된 경우 **y**를 눌러 계속 진행합니다.

Informatica 설치 프로그램 시작

- ▶ **1**을 눌러 설치 프로그램을 실행합니다.

제품을 설치하는 플랫폼에 따라 설치 프로그램에 표시되는 옵션이 다릅니다.
다음과 같은 옵션이 나타납니다.

- a. **1**을 눌러 설치 전 시스템 검사 도구를 실행합니다.

설치 전 시스템 검사 도구(i10Pi) 실행에 대한 자세한 내용은 [“설치 전 시스템 검사 도구\(i10Pi\) 실행 \(콘솔 모드\)” 페이지 99](#) 항목을 참조하십시오.

- b. **2**를 눌러 Informatica Kerberos SPN 형식 생성기를 실행합니다.

Informatica Kerberos SPN 형식 생성기 실행에 대한 자세한 내용은 [“SPN 형식 생성기 실행 ” 페이지 83](#) 항목을 참조하십시오.

- c. **3**을 눌러 설치 프로그램을 실행합니다.

시작 섹션이 나타납니다.

시작 - 약관 및 조건에 동의

- ▶ Informatica 설치 및 제품 사용 툴킷의 약관을 읽고 **약관을 읽고 동의함**을 선택합니다.

- a. 약관에 동의하지 않으려는 경우 **1**을 누릅니다.
- b. 약관에 동의하려는 경우 **2**를 누릅니다.

구성 요소 선택 섹션이 나타납니다.

구성 요소 선택

약관 및 조건에 동의하면 Informatica 도메인 서비스를 설치할 수 있습니다.

1. **1**을 눌러 Informatica 도메인 서비스를 설치합니다.

이 옵션은 버전 10.5.3 도메인 서비스와 응용 프로그램 서비스 바이너리를 설치합니다.

2. Kerberos 인증을 사용하는 네트워크에서 설치 프로그램을 실행할지 여부를 선택 합니다.

- a. **1**을 눌러 Kerberos 인증을 사용하지 않는 네트워크에서 Informatica 도메인이 실행되도록 구성합니다.

- b. **2**를 눌러 Kerberos 인증이 포함된 네트워크에서 Informatica 도메인이 실행되도록 구성합니다.

3. Choose whether you want to install distribution packages through the Informatica installer.

- Press **1** if you don't need distribution packages or if you want to install them later.
- Press **2** if you want to install distribution packages through the installer.

Default is 1.

4. If you choose to install distribution packages, select one or more packages from the list that you want to install. Separate multiple packages with a comma.

Default is 1.

설치 선행 조건 섹션에 설치 요구 사항이 표시됩니다. 설치를 계속하기 전에 모든 요구 사항이 충족되었는지 확인합니다.

라이선스 및 설치 디렉터리

설치 선행 조건을 확인한 후에는 설치 디렉터리를 지정할 수 있습니다.

1. 설치 디렉터리의 절대 경로를 입력합니다.

경로의 디렉터리 이름에 공백이나 다음과 같은 특수 문자가 있어서는 안 됩니다. @|* \$#!% (){}[] , ; ' "

기본값은 Informatica 설치를 실행하는 사용자의 사용자 홈 디렉터리입니다.

참고: Informatica는 설치 디렉터리 경로에 영숫자 문자를 사용할 것을 권장합니다. á 또는 €와 같은 특수 문자를 사용할 경우 런타임에 예기치 않은 결과가 발생할 수 있습니다.

2. Informatica 라이선스 키의 경로 및 파일 이름을 입력하고 **Enter** 키를 누릅니다.

3. Informatica 서비스 설치와 연결된 환경 유형을 지정하십시오.

- 최소한의 사용자가 포함된 개념 증명에 사용되는 기본 환경의 경우 **1**을 눌러 샌드박스 환경을 설정하십시오.
- 디자인 환경의 경우 **2**를 눌러 개발 환경을 설정하십시오.
- 프로덕션 환경과 유사하게 처리 볼륨이 많은 경우 **3**을 눌러 테스트 환경을 설정하십시오.
- 최종 사용자를 위한 높은 수준의 동시성으로 처리 볼륨이 많은 경우 **4**를 눌러 프로덕션 환경을 설정하십시오. 고급 프로덕션 환경은 일반적으로 다중 노드 설정입니다.

기본값은 샌드박스의 경우 **1**입니다.

Kerberos 네트워크 인증을 활성화한 경우, **서비스 사용자 수준** 섹션이 나타납니다.

Kerberos 네트워크 인증을 활성화하지 않은 경우, **설치 전 요약** 섹션이 나타납니다. 설치 정보를 검토하고 **Enter** 키를 눌러 계속 진행합니다. [“도메인 선택” 페이지 114](#) 단계로 건너뛩니다.

네트워크 보안 - 서비스 사용자 수준

설치 디렉터리를 지정한 후에는 보안 수준을 구성할 수 있습니다.

- ▶ **서비스 사용자 수준** 섹션에서 도메인에 대해 Kerberos 서비스 사용자를 설정할 수준을 선택합니다.

참고: 도메인의 모든 노드가 동일한 서비스 사용자 수준을 사용해야 합니다. 도메인에 노드를 가입시키는 경우 도메인의 게이트웨이 노드에서 사용하는 것과 동일한 서비스 사용자 수준을 선택하십시오.

다음 테이블에는 선택할 수 있는 수준이 설명되어 있습니다.

수준	설명
프로세스 수준	<p>각 노드 및 노드의 각 응용 프로그램 서비스에 대해 고유한 SPN(서비스 사용자 이름) 및 키 탭 파일을 사용하도록 도메인을 구성합니다.</p> <p>각 노드에 필요한 SPN 및 키 탭 파일의 수는 노드에서 실행되는 응용 프로그램 서비스 프로세스의 수에 따라 달라집니다. 운영 도메인 같이 높은 보안 수준이 필요한 도메인에 대해 프로세스 수준 옵션을 사용하십시오.</p>
노드 수준	<p>노드에서 SPN 및 키 탭 파일을 공유하도록 도메인을 구성합니다.</p> <p>이 옵션에는 노드에 대한 하나의 SPN과 키 탭 파일 및 노드에서 실행되는 모든 응용 프로그램 서비스가 필요합니다. 또한 노드의 모든 HTTP 프로세스에 대해 별도의 SPN 및 키 탭 파일이 필요합니다.</p> <p>테스트 및 개발 도메인 같이 높은 보안 수준이 필요하지 않은 도메인에 대해 노드 수준 옵션을 사용하십시오.</p>

네트워크 보안 - Kerberos 인증 섹션이 나타납니다.

네트워크 보안 - Kerberos 인증

보안 수준을 구성한 후에는 Kerberos 인증을 구성할 수 있습니다.

- ▶ **네트워크 보안 - Kerberos 인증** 섹션에서 Kerberos 인증에 필요한 매개 변수를 입력합니다.

다음 테이블에는 설정해야 하는 Kerberos 인증 매개 변수가 설명되어 있습니다.

속성	설명
도메인 이름	<p>도메인의 이름입니다. 이름은 128자를 초과하지 않아야 하고 7비트 ASCII여야만 합니다. 이름에는 공백이나 다음과 같은 문자를 사용할 수 없습니다. ` % * + ; " ? , < > \ /`</p>
노드 이름	<p>Informatica 노드의 이름입니다.</p>
노드 호스트 이름	<p>노드를 생성할 시스템의 정규화된 호스트 이름 또는 IP 주소입니다. 노드 호스트 이름에는 밑줄(_) 문자를 사용할 수 없습니다.</p> <p>참고: <i>localhost</i>는 사용하지 마십시오. 호스트 이름은 명시적으로 시스템을 식별해야 합니다.</p>
서비스 영역 이름	<p>Informatica 도메인 서비스가 속하는 Kerberos 영역의 이름입니다. 해당 영역 이름은 대문자여야 합니다.</p> <p>서비스 영역 이름과 사용자 영역 이름은 동일해야 합니다.</p>
사용자 영역 이름	<p>Informatica 도메인 사용자가 속하는 Kerberos 영역의 이름입니다. 해당 영역 이름은 대문자여야 합니다.</p> <p>서비스 영역 이름과 사용자 영역 이름은 동일해야 합니다.</p>

속성	설명
키 탭 디렉터리	Informatica 도메인의 모든 키 탭 파일이 저장된 디렉터리입니다. Informatica 도메인의 키 탭 파일 이름은 Informatica에서 설정한 형식을 따라야 합니다.
Kerberos 구성 파일의 정규화된 경로	Kerberos 구성 파일의 경로 및 파일 이름입니다. Informatica에는 다음과 같은 Kerberos 구성 파일 이름이 필요합니다. <i>krb5.conf</i>

중요: Kerberos 인증으로 실행되도록 도메인을 구성하는 경우, 도메인과 노드 이름 및 노드 호스트 이름이 사용자가 Informatica Kerberos SPN 형식 생성기를 실행하여 SPN 및 키 탭 파일 이름을 생성했을 때 지정한 이름과 일치해야 합니다. 다른 도메인, 노드 또는 호스트 이름을 사용하는 경우, SPN 및 키 탭 파일 이름을 다시 생성하고 Kerberos 관리자에게 새로운 SPN을 Kerberos 사용자 데이터베이스에 추가하고 키 탭 파일을 생성하도록 요청하십시오.

사전 설치 요약 섹션이 나타납니다. 설치 정보를 검토합니다.

도메인 선택

설치 전 요약을 검토한 후에는 도메인 정보를 입력할 수 있습니다.

1. **1**을 눌러 도메인을 생성합니다.

도메인을 생성하면, 생성하는 노드가 도메인의 게이트웨이 노드가 됩니다. 게이트웨이 노드에는 모든 도메인 작업을 관리하는 서비스 관리자가 포함됩니다.

2. 도메인에서 서비스에 대해 보안 통신을 활성화할지 여부를 선택합니다.

a. **1**을 눌러 도메인에 대해 보안 통신을 비활성화합니다.

b. **2**를 눌러 도메인에 대해 보안 통신을 활성화합니다.

기본적으로, 도메인에 대한 보안 통신을 활성화하는 경우 설치 프로그램이 Informatica Administrator에 대한 HTTPS 연결을 설정합니다. 또한 보안 데이터베이스에서 도메인 구성 리포지토리를 생성할 수 있습니다.

3. Informatica Administrator의 연결 세부 정보를 지정합니다.

a. 도메인에 대한 보안 통신을 활성화하지 않은 경우, Informatica Administrator에 대해 보안 HTTPS 연결을 설정할지 여부를 지정할 수 있습니다.

다음 테이블에는 Informatica Administrator에 대한 보안 연결을 활성화하거나 비활성화하는 데 사용 가능한 옵션이 설명되어 있습니다.

옵션	설명
Informatica Administrator에 HTTPS 사용	Informatica Administrator에 대한 보안 연결을 설정합니다.
HTTPS 비활성화	Informatica Administrator에 대한 보안 연결을 설정하지 마십시오.

- b. 도메인에 대한 보안 통신을 활성화하거나 Informatica Administrator에 대해 HTTPS 연결을 활성화하는 경우, Informatica Administrator에 대한 HTTPS 연결의 키 저장소 파일 및 포트 번호를 입력합니다.

다음 테이블에는 HTTPS를 활성화하는 경우 입력해야 하는 연결 정보가 설명되어 있습니다.

옵션	설명
포트	HTTPS 연결의 포트 번호입니다.
키 저장소 파일	설치 프로그램에 의해 생성된 키 저장소 파일 또는 사용자가 생성하는 키 저장소 파일을 사용할지 여부를 선택합니다. 자체 서명된 인증서 또는 인증 기관에 의해 서명된 인증서와 함께 키 저장소 파일을 사용할 수 있습니다. 1 - 설치 프로그램에 의해 생성된 키 저장소 사용 2 - 키 저장소 파일 및 암호 지정 설치 프로그램에 의해 생성된 키 저장소 파일을 사용하도록 선택하는 경우 설치 프로그램은 다음 위치에 Default.keystore라는 자체 서명된 키 저장소 파일을 생성합니다. <Informatica 설치 디렉터리>/tomcat/conf/

- c. 키 저장소를 지정하는 경우 키 저장소 파일의 암호와 위치를 입력합니다.
- d. 도메인에 대해 보안 통신을 활성화한 경우, **도메인 보안 - 보안 통신** 섹션이 나타납니다.
- e. 도메인에 대해 보안 통신을 활성화하지 않은 경우, **도메인 구성 리포지토리** 섹션이 나타납니다. [“Domain Configuration Repository” 페이지 118](#) 단계로 건너뛩니다.

4. Informatica 도메인에서 웹 기반 Informatica 응용 프로그램에 대해 SAML(Security Assertion Markup Language) SSO(Single Sign-on) 지원을 구성하려면 SAML 인증을 활성화할지 여부를 선택합니다. SAML 인증을 비활성화하려면 **1**을 누르고 [“도메인 보안 - 보안 통신” 페이지 117](#)으로 건너뛩니다. SAML 인증을 활성화하고 구성하려면 **2**를 누릅니다.
5. 도메인의 ID 공급자 URL을 입력합니다.
6. ID 공급자에 정의된 도메인의 신뢰 당사자 트러스트 이름 또는 서비스 공급자 식별자를 지정하십시오. 아니요를 선택하는 경우 서비스 공급자 식별자가 "Informatica"로 설정됩니다.
7. IdP에서 SAML 어설션을 서명할지 여부를 지정합니다.
8. ID 공급자 어설션 서명 인증서 별칭 이름을 입력합니다.
9. 도메인에서 SAML 인증을 활성화하는 데 기본 Informatica SSL 인증서를 사용할지 또는 사용자의 SSL 인증서를 사용할지 선택합니다.

다음 테이블에는 SAML 인증에 대한 SSL 인증서 옵션이 설명되어 있습니다.

옵션	설명
기본 Informatica SSL 인증서 파일을 사용합니다.	SAML 인증에 기본 Informatica 트러스트 저장소 파일을 사용하려면 선택합니다.
SSL 인증서 파일의 위치를 입력하십시오.	SAML 인증을 위한 사용자 지정 트러스트 저장소 파일을 사용하려면 선택합니다. 도메인 내의 게이트웨이 노드에 대한 사용자 지정 트러스트 저장소 파일이 포함된 디렉터리를 지정하십시오. 파일에 대한 전체 경로가 아닌 디렉터리만 지정하십시오.

10. 사용자가 보안 인증서를 제공하는 경우 키 저장소 및 트러스트 저장소 파일의 위치와 암호를 지정합니다.

다음 테이블에는 트러스트 저장소 및 키 저장소 파일의 위치와 암호가 설명되어 있습니다.

속성	설명
트러스트 저장소 디렉터리	도메인 내의 게이트웨이 노드에 대한 사용자 지정 트러스트 저장소 파일이 포함된 디렉터리를 지정하십시오. 파일에 대한 전체 경로가 아닌 디렉터리만 지정하십시오.
트러스트 저장소 암호	사용자 지정 트러스트 저장소 파일에 대한 암호입니다.
키 저장소 디렉터리	사용자 지정 키 저장소 파일이 포함된 디렉터리를 지정합니다.
키 저장소 암호	사용자 지정 키 저장소 파일에 대한 암호입니다.

11. 인증 컨텍스트 비교를 지정하려면 IdP 서버와 사용자가 사용하는 인증 메커니즘의 비교 강도를 지정합니다. 지원되는 값은 MINIMUM, MAXIMUM, BETTER 또는 EXACT 옵션입니다. 기본값은 MINIMUM입니다.
12. 인증 컨텍스트 클래스를 설정하려면 IdP 서버를 사용하는 사용자에게 예상되는 최초 인증 메커니즘을 지정합니다.
지원되는 값은 PASSWORD 또는 PASSWORDPROTECTEDTRANSPORT입니다. 기본값은 PASSWORD입니다.
13. 웹 응용 프로그램이 SAML 인증 요청에 서명하도록 활성화할지 여부를 지정하시겠습니까?
기본값은 비활성화됨입니다.
14. SAML 요청에 서명하는 데 사용하는 노드 SAML 키 저장소로 가져온 개인 키의 별칭 이름을 지정하십시오.
15. SAML 요청 서명에 사용된 개인 키 액세스를 위한 암호를 지정합니다.
16. 웹 응용 프로그램이 SAML 요청을 서명하는 데 사용하는 알고리즘을 지정하십시오.
지원되는 값은 RSA_SHA256, DSA_SHA1, DSA_SHA256, RSA_SHA1, RSA_SHA224, RSA_SHA384, RSA_SHA512, ECDSA_SHA1, ECDSA_SHA224, ECDSA_SHA256, ECDSA_SHA384, ECDSA_SHA512, RIPEMD160 또는 RSA_MD5입니다.
17. IdP가 SAML 응답에 서명하도록 할지 여부를 지정하시겠습니까?
웹 응용 프로그램을 활성화하여 서명된 SAML 응답을 수신할지 여부를 선택하십시오. 기본값은 비활성화됨입니다.
18. IdP에서 SAML 어설션을 암호화할지 여부를 지정하십시오.
웹 응용 프로그램을 활성화하여 암호화된 SAML 어설션을 수신할지 여부를 선택하십시오. 기본값은 활성화됨입니다.
19. Informatica가 SAML 어설션을 암호 해독하는 데 사용하는 게이트웨이 노드 SAML 트러스트 저장소에 있는 개인 키의 별칭 이름을 지정하십시오.
20. 어설션 암호화 키를 암호 해독할 때 사용하는 개인 키 액세스를 위한 암호를 제공하십시오.
21. 다음을 클릭합니다.
도메인 보안 - 보안 연결 섹션이 나타납니다.

도메인 보안 - 보안 통신

도메인을 구성한 후에는 도메인 보안을 구성할 수 있습니다.

- ▶ 도메인 보안 - 보안 통신 섹션에서 기본 Informatica SSL 인증서를 사용하거나 사용자의 SSL 인증서를 사용하여 도메인 통신을 보호할지 여부를 지정합니다.

- 사용할 SSL 인증서의 유형을 선택합니다.

다음 테이블에는 Informatica 도메인을 보호하는 데 사용할 수 있는 SSL 인증서에 대한 옵션이 설명되어 있습니다.

옵션	설명
기본 Informatica SSL 인증서 사용	기본 키 저장소 및 트러스트 저장소에 포함된 기본 SSL 인증서를 사용합니다. 참고: SSL 인증서를 제공하지 않을 경우 Informatica에서는 모든 Informatica 설치에 동일한 기본 개인 키를 사용합니다. 기본 Informatica 키 저장소 및 트러스트 저장소 파일을 사용하는 경우 도메인의 보안이 침해될 수 있습니다. 도메인의 보안 수준을 높이려면 SSL 인증서 파일의 위치를 지정하는 옵션을 선택하십시오.
사용자 지정 SSL 인증서 사용	SSL 인증서가 포함된 키 저장소와 트러스트 저장소 파일의 경로를 지정합니다. 키 저장소 및 트러스트 저장소의 암호도 지정해야 합니다. 자체 서명된 인증서 또는 CA(인증 기관)에서 발급한 인증서를 제공할 수 있습니다. SSL 인증서를 PEM 형식 및 JKS(Java 키 저장소) 파일로 제공해야 합니다. Informatica 도메인에 대한 SSL 인증서 파일 관련 이름이 필요합니다. 도메인의 모든 노드에 대해 동일한 SSL 인증서를 사용해야 합니다. 도메인의 모든 노드에 액세스 가능한 디렉터리에서 트러스트 저장소 및 키 저장소 파일을 저장하고 동일한 도메인의 모든 노드에 대해 동일한 키 저장소 파일 디렉터리 및 트러스트 저장소 파일 디렉터를 지정합니다.

- 사용자가 SSL 인증서를 제공하는 경우 키 저장소 및 트러스트 저장소 파일의 위치와 암호를 지정합니다.

다음 테이블에는 SSL 인증서 파일에 대해 입력해야 하는 매개 변수가 설명되어 있습니다.

속성	설명
키 저장소 파일 디렉터리	키 저장소 파일이 포함된 디렉터리입니다. 디렉터리에 이름이 <code>infa_keystore.jks</code> 인 파일이 포함되어 있어야 합니다.
키 저장소 암호	키 저장소 <code>infa_keystore.jks</code> 의 암호입니다.
트러스트 저장소 파일 디렉터리	트러스트 저장소 파일이 포함된 디렉터리입니다. 이 디렉터리에는 <code>infa_truststore.jks</code> 및 <code>infa_truststore.pem</code> 이라는 파일이 포함되어야 합니다.
트러스트 저장소 암호	<code>infa_truststore.jks</code> 파일의 암호입니다.

도메인 구성 리포지토리 섹션이 나타납니다.

Domain Configuration Repository

After you configure domain security, you can configure domain repository details.

1. Select the database to use for the domain configuration repository details.

The following table lists the databases you can use for the domain configuration repository:

Prompt	Description
Database type	Type of database for the domain configuration repository. Select from the following options: 1 - Oracle 2 - Microsoft SQL Server 3 - IBM DB2 4 - Sybase ASE 5 - PostgreSQL

The Informatica domain configuration repository stores metadata for domain operations and user authentication. The domain configuration repository must be accessible to all gateway nodes in the domain.

2. Enter the properties for the database user account.

The following table lists the properties for the database user account:

Property	Description
Database user ID	Name for the domain configuration database user account.
User password	Password for the domain configuration database user account.

3. Select whether to create a secure domain configuration repository.

You can create a domain configuration repository in a database secured with the SSL protocol. To create a domain configuration repository in a secure database, press 1 and skip to step to create a domain configuration repository.

To create a domain configuration repository in an unsecure database, press 2.

4. If you do not create a secure domain configuration repository, enter the parameters for the database.

- a. If you select IBM DB2, select whether to configure a tablespace and enter the tablespace name.

The following table describes the properties that you must configure for the IBM DB2 database:

Property	Description
Configure tablespace	In a single-partition database, if you select No, the installer creates the tables in the default tablespace. In a multi-partition database, you must select Yes. Select whether to specify a tablespace: 1 - No 2 - Yes
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single-partition database, enter the name of the tablespace in which to create the tables. In a multipartition database, specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

- b. If you select Microsoft SQL Server or PostgreSQL, enter the schema name for the database.

The following table describes the properties that you must configure for the database:

Property	Description
Schema name	Name of the schema that will contain domain configuration tables. If this parameter is blank, the installer creates the tables in the default schema.

- c. To enter the JDBC connection information using the JDBC URL information, press **1**. To enter the JDBC connection information using a custom JDBC connection string, press **2**.

- d. Enter the JDBC connection information.

- To enter the connection information using the JDBC URL information, specify the JDBC URL properties.

The following table describes the database connection information:

Prompt	Description
Database host name	Host name for the database.
Database port number	Port number for the database.

Prompt	Description
Database service name	Service or database name: - Oracle: Enter the service name. - Microsoft SQL Server: Enter the database name. - IBM DB2: Enter the service name. - Sybase ASE: Enter the database name. - PostgreSQL: Enter the database name.
Configure JDBC Parameters	Select whether to add additional JDBC parameters to the connection string: 1 - Yes 2 - No If you select Yes, enter the parameters or press Enter to accept the default. If you select No, the installer creates the JDBC connection string without parameters.

- To enter the connection information using a custom JDBC connection string, type the connection string.

Use the following syntax in the JDBC connection string:

IBM DB2

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

Microsoft SQL Server with Windows NT credentials

If you specified the Windows NT credentials for the Model repository database on Microsoft SQL Server, specify the connection string syntax to include the authentication method as NTLM.

Microsoft SQL Server that uses the default instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<호스트 이름>:<포트 번호>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server that uses a named instance with Windows NT credentials:

```
"jdbc:informatica:sqlserver://<호스트 이름>\<명명된 인스턴스 이름>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database
```

```
name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

Azure SQL Database with Active Directory authentication

```
jdbc:informatica:sqlserver://  
<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>
```

PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLsv1.2;
```

Sybase

```
jdbc:Informatica:sybase://<host name>:<port number>;DatabaseName=
```

Verify that the connection string contains all the connection parameters required by your database system.

5. If you create a secure domain configuration repository, enter the parameters for the secure database.

If you create the domain configuration repository on a secure database, you must provide the truststore information for the database.

The following table describes the options available to create a secure domain configuration repository database:

Property	Description
Database truststore file	Path and file name of the truststore file for the secure database.
Database truststore password	Password for the truststore file.
Custom JDBC Connection String	JDBC connection string to connect to the secure database, including the host name and port number and the security parameters for the database.

In addition to the host name and port number for the database server, you must include the following secure database parameters:

EncryptionMethod

Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to SSL.

ValidateServerCertificate

Optional. Indicates whether Informatica validates the certificate that the database server sends.

If this parameter is set to True, Informatica validates the certificate that the database server sends. If you specify the HostNameInCertificate parameter, Informatica also validates the host name in the certificate.

If this parameter is set to False, Informatica does not validate the certificate that the database server sends. Informatica ignores any truststore information that you specify

Default is True.

HostNameInCertificate

Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the SSL certificate.

cryptoProtocolVersion

Required. Specifies the cryptographic protocol to use to connect to a secure database. You can set the parameter to cryptoProtocolVersion=TLSv1.1 or cryptoProtocolVersion=TLSv1.2 based on the cryptographic protocol used by the database server.

You must also provide a JDBC connection string that includes the security parameters for the database. You can use the following syntax for the connection strings:

- Oracle: jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=<service name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
- IBM DB2: jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
- Microsoft SQL Server: jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
- Microsoft SQL Server with Windows NT credentials:
If you have previously specified the Windows NT credentials for the Model repository database on Microsoft SQL Server, specify the connection string syntax to include the authentication method as NTLM.
 - Microsoft SQL Server that uses the default instance with Windows NT credentials:
"jjdbc:informatica:sqlserver://<호스트 이름>:<포트 번호>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;authenticationMethod=NTLM"
 - Microsoft SQL Server that uses a named instance with Windows NT credentials:
"jjdbc:informatica:sqlserver://<호스트 이름>\<명명된 인스턴스 이름>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;authenticationMethod=NTLM"
- Microsoft Azure SQL: jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
- PostgreSQL: jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
- Azure PostgreSQL: jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;

참고: The installer does not validate the connection string. Verify that the connection string contains all the connection parameters and security parameters required by your database.

6. If the database contains a domain configuration repository for a previous domain, select to overwrite the data or set up another database.
 - a. Press 1 for OK to enter the connection information for a new database.
 - b. Press 2 for Continue for the installer to overwrite the data in the database with new domain configuration.

The **Domain Security - Encryption Key** section appears.

도메인 보안 - 암호화 키

도메인 리포지토리를 구성한 후에는 암호화 키를 구성할 수 있습니다.

- ▶ **도메인 보안 - 암호화 키** 섹션에서 Informatica 도메인에 대한 암호화 키의 디렉터리를 입력합니다. 다음 테이블에는 도메인을 생성할 때 지정해야 하는 암호화 키 매개 변수가 설명되어 있습니다.

속성	설명
암호화 키 디렉터리	도메인에 대한 암호화 키가 저장되는 디렉터리입니다. 기본적으로 암호화 키는 다음 디렉터리에 생성됩니다. <Informatica 설치 디렉터리>/isp/config/keys.
설치 프로그램에서 생성되는 사이트 키를 백업할지 여부를 지정하십시오.	<p>고유한 사이트 키가 생성됩니다. 사이트 키를 분실하는 경우 사이트 키를 다시 생성할 수 없습니다. 이 키의 사본을 반드시 저장하고 고유한 사이트 키를 다른 사람과 공유하지 마십시오.</p> <p>설치 프로그램에서 생성되는 사이트 키를 백업할지 여부를 지정하십시오.</p> <ul style="list-style-type: none"> - 아니요인 경우 1을 선택합니다. 아니요를 선택하는 경우 설치 프로그램에 오류가 생성됩니다. Enter 키를 눌러 계속 진행합니다. - 예인 경우 2를 선택합니다. 예를 선택하는 경우 파일을 수동으로 백업하는 데 동의하는 것입니다.

설치 프로그램이 디렉터리 및 해당 디렉터리의 파일에 대해 서로 다른 사용 권한을 설정합니다. 암호화 키 파일 및 디렉터리의 사용 권한에 대한 자세한 내용은 [“보안 파일 및 디렉터리” 페이지 98](#)를 참조하십시오.

도메인 및 노드 구성 섹션이 나타납니다.

도메인 및 노드 구성

암호화 키를 구성한 후에는 도메인 및 노드를 구성할 수 있습니다.

1. 생성할 도메인 및 노드에 대한 정보를 입력합니다.

다음 테이블에는 사용자가 도메인 및 게이트웨이 노드에 대해 설정하는 속성이 설명되어 있습니다.

속성	설명
도메인 이름	<p>생성할 Informatica 도메인의 이름입니다. 기본 도메인 이름은 Domain_<MachineName>입니다.</p> <p>이름은 128자를 초과하지 않아야 하고 7비트 ASCII여야만 합니다. 이름에는 공백이나 다음과 같은 문자를 사용할 수 없습니다. ` % * + ; " ? , < > \ /</p>
노드 이름	<p>생성할 노드의 이름입니다.</p>
노드 호스트 이름	<p>노드를 생성할 시스템의 호스트 이름 또는 IP 주소입니다.</p> <p>시스템이 단일 네트워크 이름을 갖는 경우 기본 호스트 이름을 사용하십시오. 시스템이 여러 네트워크 이름을 갖는 경우 대체 네트워크 이름을 사용하도록 기본 호스트 이름을 수정할 수 있습니다.</p> <p>참고: 노드 호스트 이름에는 밑줄(_) 문자를 사용할 수 없습니다. localhost는 사용하지 마십시오. 호스트 이름은 명시적으로 시스템을 식별해야 합니다.</p>
노드 포트 번호	<p>노드의 포트 번호입니다. 노드의 기본 포트 번호는 6005입니다. 시스템에서 해당 포트 번호를 사용할 수 없는 경우 사용 가능한 다음 포트 번호가 설치 프로그램에 표시됩니다.</p>
도메인 사용자 이름	<p>도메인 관리자의 사용자 이름입니다. 처음에 Informatica Administrator에 로그인할 때 이 사용자 이름을 사용할 수 있습니다. 다음 지침을 사용하십시오.</p> <ul style="list-style-type: none"> - 이름은 대/소문자를 구분하지 않으며 128자를 초과할 수 없습니다. - 이름에는 탭, 줄 바꿈 문자 또는 다음과 같은 특수 문자를 사용할 수 없습니다. % * + / ? ; < > - 첫 번째 문자와 마지막 문자를 제외하고 이름에는 ASCII 공백 문자를 사용할 수 있습니다. 다른 공백 문자는 사용할 수 없습니다.

2. 도메인에 있는 중요 데이터를 보호하기 위해 암호 복잡성을 활성화할지 선택합니다.

The following table describes the password complexity:

Property	Description
Password complexity	<p>Select whether you want to enable password complexity.</p> <p>1 - Yes 2 - No</p> <p>If you select Yes, the password must meet the following requirements: It must be at least eight characters long and contain at least one alphabetic character, one numeric character, and one special character.</p>
Configure password policy	<p>Select whether you want to configure a password policy.</p> <p>1 - Yes 2 - No</p> <p>If you select Yes, you can configure password complexity rules. If you select No, the default Informatica password policy rules apply.</p>

Property	Description
Number of special characters	The minimum number of special characters required in a password. You can use the following special characters: [! " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { } ~] You can enter a value between 0 and 255. Default is 1.
Number of alphabetic characters	The minimum number of alphabetic characters required in a password. You can enter a value between 0 and 255. Default is 1.
Number of numeric characters	The minimum number of numeric characters required in a password. You can enter a value between 0 and 255. Default is 1.
Minimum password length	The minimum number of characters required in a password. You can enter a value between 8 and 255. Default is 8.
Number of previous passwords to store	The number of consecutive previous passwords that can't be reused. You can enter a value between 0 and 12. Default is 0.
Password expiration in days	The duration of the validity of a password. If you don't want passwords to expire, set the value to 0. Default is 0.
Domain password	Password for the domain administrator. - If you don't enable password complexity, the password must be between 2 and 16 characters. - If you enable password complexity, the password must be at least eight characters long and contain at least one alphabetic character, one numeric character, and one special character. - If you configure a password policy, the password must meet the complexity rules that you set. Not available if you configure the Informatica domain to run on a network with Kerberos authentication.
Confirm password	Enter the password again to confirm. Not available if you configure the Informatica domain to run on a network with Kerberos authentication.

3. 설치 프로그램에 의해 할당된 도메인 및 노드 구성 요소에 대한 기본 포트를 표시할지 여부를 선택합니다. 다음 표에는 고급 포트 구성 페이지가 설명되어 있습니다.

프롬프트	설명
고급 포트 구성 페이지 표시	설치 프로그램에 의해 할당된 도메인 및 노드 구성 요소에 대한 포트 번호를 표시할지 여부를 선택합니다. 1 - 아니요 2 - 예 예를 선택하면 설치 프로그램에 도메인 구성 요소에 할당된 기본 포트 번호가 표시됩니다. 도메인 및 노드 구성 요소에 사용할 포트 번호를 지정할 수 있습니다. 노드에서 실행될 서비스 프로세스에 사용할 포트 번호의 범위도 지정할 수 있습니다. 기본 포트 번호를 사용하거나 새 포트 번호를 지정할 수 있습니다. 입력하는 포트 번호가 다른 응용 프로그램에서 사용되지 않는지 확인합니다.

4. 포트 구성 페이지를 표시하는 경우, 프롬프트에 새 포트 번호를 입력하거나 **Enter** 키를 눌러 기본 포트 번호를 사용합니다.

다음 테이블에는 사용자가 설정할 수 있는 포트가 설명되어 있습니다.

Port	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.

5. 서비스와 연결을 구성할지 선택합니다.

예를 선택하면 모델 리포지토리 서비스, 데이터 통합 서비스, 콘텐츠 관리 서비스, **PowerCenter** 리포지토리 서비스, **PowerCenter** 통합 서비스 그리고 프로파일링 웨어하우스 연결 및 클러스터 구성과 관련된 연결을 구성할 수 있습니다.

아니오를 선택하면 **Administrator** 도구에서 응용 프로그램 서비스를 구성할 수 있습니다.

서비스와 연결을 구성하도록 선택한 경우 **Informatica 응용 프로그램 서비스 구성** 섹션이 나타납니다. 서비스와 연결을 구성하지 않도록 선택하면 **설치 후 요약** 섹션에 설치가 완료되었는지 여부가 나타납니다. 또한 설치된 구성 요소 및 해당 구성의 상태도 요약에 표시됩니다.

Informatica 응용 프로그램 서비스 구성

1. 모델 리포지토리 서비스 및 데이터 통합 서비스를 구성할지 선택합니다.
2. 모니터링 모델 리포지토리 서비스를 구성할지 선택합니다.
3. 콘텐츠 관리 서비스를 구성할지 선택합니다.
4. 프로파일링 웨어하우스 연결을 구성할지 선택합니다.
5. 메타데이터 액세스 서비스를 생성할지 선택합니다. 도메인에서 **Kerberos** 인증을 사용하는 경우 메타데이터 액세스 서비스를 생성하도록 선택하지 마십시오.

6. PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스를 생성할지 여부를 선택합니다.

모델 리포지토리 데이터베이스 구성

도메인과 노드를 구성한 후에는 모델 리포지토리 데이터베이스 속성을 구성할 수 있습니다.

1. 모델 리포지토리 서비스 이름을 입력합니다.

서비스 이름을 입력합니다. 이름은 대/소문자를 구분하지 않으며 도메인 내에서 고유해야 합니다. 이름은 128자를 초과하거나 @로 시작할 수 없습니다. 또한 공백이나 다음과 같은 특수 문자를 포함할 수도 없습니다.

` ~ ^ * + = { } \ ; : ' " / ? . , < > | ! () []

서비스를 생성한 후에는 서비스 이름을 변경할 수 없습니다.

프로세스 수준 SPN을 선택한 경우 모델 리포지토리 서비스 키 탭 파일을 지정합니다. 모델 리포지토리 서비스 프로세스에 대한 키 탭 파일입니다. 키 탭 파일은 다음과 같은 이름을 가져야 합니다. **.keytab**

2. 모델 리포지토리를 구성할 데이터베이스를 선택합니다.

다음 테이블에는 모델 리포지토리를 구성할 수 있는 데이터베이스가 나열되어 있습니다.

프롬프트	설명
데이터베이스 유형	모델 리포지토리의 데이터베이스 유형입니다. 다음 옵션 중에서 선택하십시오. 1 - Oracle 2 - Microsoft SQL Server 3 - IBM DB2 4 - PostgreSQL

3. 데이터베이스 사용자 계정의 속성을 입력합니다.

다음 테이블에는 데이터베이스 사용자 계정의 속성이 나와 있습니다.

속성	설명
데이터베이스 사용자 ID	모델 리포지토리 데이터베이스 사용자 계정의 이름입니다. Microsoft SQL Server에서 신뢰할 수 있는 연결을 위해 Windows NT 사용자 이름을 입력할 수 있습니다.
사용자 암호	모델 리포지토리 사용자 계정의 암호입니다. Microsoft SQL Server에서 신뢰할 수 있는 연결을 위해 Windows NT 암호를 입력할 수 있습니다.

4. 보안 모델 리포지토리 데이터베이스를 생성할지 여부를 선택합니다.

SSL 프로토콜로 보호되는 데이터베이스에 모델 리포지토리 서비스를 생성할 수 있습니다. 보안 데이터베이스에 모델 리포지토리 서비스를 생성하려면 **1**을 누르고 JDBC 정보를 입력하는 단계로 건너뜁니다.

비보안 데이터베이스에 모델 리포지토리 서비스를 생성하려면 **2**를 누릅니다.

5. 보안 모델 리포지토리를 생성하지 않도록 선택한 경우 데이터베이스에 대한 매개 변수를 입력합니다.

- a. IBM DB2를 선택하는 경우 테이블스페이스를 구성할지 여부를 선택하고 테이블스페이스 이름을 입력합니다.

다음 테이블에는 IBM DB2 데이터베이스에 대해 구성해야 하는 속성이 설명되어 있습니다.

Property	Description
Configure tablespace	In a single-partition database, if you select No, the installer creates the tables in the default tablespace. In a multi-partition database, you must select Yes. Select whether to specify a tablespace: 1 - No 2 - Yes
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single-partition database, enter the name of the tablespace in which to create the tables. In a multipartition database, specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

- b. Microsoft SQL Server 또는 PostgreSQL을 선택하는 경우 데이터베이스의 스키마 이름을 입력합니다.
다음 테이블에는 데이터베이스에 대해 구성해야 하는 속성이 설명되어 있습니다.

Property	Description
Schema name	Name of the schema that will contain domain configuration tables. If this parameter is blank, the installer creates the tables in the default schema.

- c. JDBC URL 정보를 사용하여 JDBC 연결 정보를 입력하려면 **1**을 누릅니다. 사용자 지정 JDBC 연결 문자열을 사용하여 JDBC 연결 정보를 입력하려면 **2**를 누릅니다.
- d. JDBC 연결 정보를 입력합니다.
- JDBC URL 정보를 사용하여 연결 정보를 입력하려면 JDBC URL 속성을 지정합니다.
다음 테이블에는 데이터베이스 연결 정보가 설명되어 있습니다.

프롬프트	설명
데이터베이스 호스트 이름	데이터베이스의 호스트 이름입니다.
데이터베이스 포트 번호	데이터베이스의 포트 번호입니다.

프롬프트	설명
데이터베이스 서비스 이름	<p>서비스 또는 데이터베이스 이름:</p> <ul style="list-style-type: none"> - Oracle: 서비스 이름을 입력합니다. - Microsoft SQL Server: 데이터베이스 이름을 입력합니다. - IBM DB2: 서비스 이름을 입력합니다. - PostgreSQL: 데이터베이스 이름을 입력합니다.
JDBC 매개 변수 구성	<p>추가 JDBC 매개 변수를 연결 문자열에 추가할지 여부를 선택합니다.</p> <p>1 - 예 2 - 아니요</p> <p>예를 선택하는 경우 매개 변수를 입력하거나 Enter 키를 눌러 기본값을 수락합니다.</p> <p>아니요를 선택하는 경우 설치 프로그램이 매개 변수 없이 JDBC 연결 문자열을 생성합니다.</p>

- 사용자 지정 JDBC 연결 문자열을 사용하여 연결 정보를 입력하려면 연결 문자열을 입력합니다. JDBC 연결 문자열에 다음 구문을 사용합니다.

IBM DB2

```
jdbc:Informatica:db2://<호스트 이름>:<포트 번호>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<호스트 이름>:<포트 번호>;ServiceName=
```

Oracle Connection Manager를 통해 Oracle 데이터베이스에 연결하려면 다음 연결 문자열을 사용합니다.

```
jdbc:Informatica:oracle:TNSNamesFile=<tnsnames.ora 파일에 대한 정규화된 경로>;TNSServerName=<TNS 이름>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<호스트 이름>:<포트 번호>;SelectMethod=cursor;DatabaseName=
```

Windows NT 자격 증명이 있는 Microsoft SQL Server

Microsoft SQL Server에서 모델 리포지토리 데이터베이스에 대한 Windows NT 자격 증명을 지정한 경우 NTLM을 인증 방법으로 포함하도록 연결 문자열 구문을 지정합니다.

Windows NT 자격 증명이 있는 기본 인스턴스를 사용하는 Microsoft SQL Server:

```
"jdbc:informatica:sqlserver://<호스트 이름>:<포트 번호>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Windows NT 자격 증명이 있는 명명된 인스턴스를 사용하는 Microsoft SQL Server:

```
"jdbc:informatica:sqlserver://<호스트 이름>\<명명된 인스턴스 이름>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft Azure SQL Database

```
jdbc:Informatica:sqlserver://<호스트 이름>:<포트 번호>;SelectMethod=cursor;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

Active Directory 인증을 사용하는 Azure SQL Database

```
"jdbc:informatica: sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>"
```

PostgreSQL

```
jdbc:Informatica:postgresql://<호스트 이름>:<포트 번호>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<호스트 이름>:<포트 번호>;DatabaseName=<데이터베이스 이름>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

데이터베이스 시스템에 필요한 모든 연결 매개 변수가 연결 문자열에 포함되어 있는지 확인합니다.

서비스 매개 변수 섹션이 나타납니다.

데이터 통합 서비스

모델 리포지토리 데이터베이스를 구성한 후에는 응용 프로그램 서비스에 대한 서비스 매개 변수를 구성할 수 있습니다.

1. 다음 서비스 매개 변수 정보를 입력합니다.

포트	설명
데이터 통합 서비스 이름	Informatica 도메인에 생성할 데이터 통합 서비스의 이름입니다.
HTTP 프로토콜 유형	데이터 통합 서비스에 대한 연결 유형입니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> - HTTP. 서비스를 요청할 때 HTTP 연결을 사용합니다. - HTTPS. 서비스를 요청할 때 보안 HTTP 연결을 사용합니다. - HTTP&HTTPS. 서비스를 요청할 때 HTTP 또는 HTTPS 연결을 사용할 수 있습니다.
HTTP 포트	데이터 통합 서비스에 사용할 포트 번호입니다. 기본값은 9085입니다.
HTTPS 포트	데이터 통합 서비스에 사용할 포트 번호입니다. 기본값은 9085입니다.

2. 데이터 통합 서비스를 보호하는 데 사용할 SSL 인증서를 선택합니다.

옵션	설명
기본 Informatica SSL 인증서 파일을 사용합니다.	기본 키 저장소 및 트러스트 저장소에 포함된 기본 Informatica SSL 인증서를 사용합니다. 참고: SSL 인증서를 제공하지 않을 경우 Informatica에서는 모든 Informatica 설치에 동일한 기본 개인 키를 사용합니다. 기본 Informatica 키 저장소 및 트러스트 저장소 파일을 사용하는 경우 도메인의 보안이 침해될 수 있습니다. 도메인의 보안 수준을 높이려면 SSL 인증서 파일의 위치를 지정하는 옵션을 선택하십시오.
사용자 지정 SSL 인증서 사용	사용자 지정 SSL 인증서를 사용합니다. 키 저장소 및 트러스트 저장소 파일의 위치를 지정해야 합니다. 자체 서명된 인증서 또는 CA(인증 기관)에서 발급한 인증서를 제공할 수 있습니다. SSL 인증서를 PEM 형식 및 JKS(Java 키 저장소) 파일로 제공해야 합니다. Informatica 도메인에 대한 SSL 인증서 파일 관련 이름이 필요합니다. 도메인의 모든 노드에 대해 동일한 SSL 인증서를 사용해야 합니다. 도메인의 모든 노드에 액세스 가능한 디렉터리에서 트러스트 저장소 및 키 저장소 파일을 저장하고 동일한 도메인의 모든 노드에 대해 동일한 키 저장소 파일 디렉터리 및 트러스트 저장소 파일 디렉터를 지정합니다.

사용자 지정 SSL 인증서를 사용하도록 선택한 경우 다음 정보를 입력합니다.

속성	설명
키 저장소 파일 디렉터리	키 저장소 파일이 포함된 디렉터리입니다. 이 디렉터리에는 infa_keystore.jks 및 infa_keystore.pem이라는 파일이 포함되어야 합니다.
키 저장소 암호	키 저장소 infa_keystore.jks의 암호입니다.

속성	설명
트러스트 저장소 파일 디렉터리	트러스트 저장소 파일이 포함된 디렉터리입니다. 이 디렉터리에는 infa_truststore.jks 및 infa_truststore.pem이라는 파일이 포함되어야 합니다.
트러스트 저장소 암호	infa_truststore.jks 파일의 암호입니다.

모니터링 모델 리포지토리 데이터베이스 구성

모델 리포지토리 데이터베이스를 구성한 후에는 모니터링 모델 리포지토리 데이터베이스 속성을 구성할 수 있습니다.

1. 모니터링 모델 리포지토리 서비스 이름을 입력합니다.

서비스 이름을 입력합니다. 이름은 대/소문자를 구분하지 않으며 도메인 내에서 고유해야 합니다. 이름은 128자를 초과하거나 @로 시작할 수 없습니다. 또한 공백이나 다음과 같은 특수 문자를 포함할 수도 없습니다.

```
` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( ) ] [
```

서비스를 생성한 후에는 서비스 이름을 변경할 수 없습니다.

프로세스 수준 SPN을 선택한 경우 모니터링 모델 리포지토리 서비스 키 탭 파일을 지정합니다. 모델 리포지토리 서비스 프로세스 모니터링에 대한 키 탭 파일입니다. 키 탭 파일은 다음과 같은 이름을 가져야 합니다. **.keytab**

2. 모니터링 모델 리포지토리의 데이터베이스 유형을 선택합니다.

다음 테이블에는 모니터링 모델 리포지토리의 데이터베이스가 나열되어 있습니다.

프롬프트	설명
데이터베이스 유형	모니터링 모델 리포지토리의 데이터베이스 유형입니다. 다음 옵션 중에서 선택하십시오. 1 - Oracle 2 - Microsoft SQL Server 3 - IBM DB2 4 - PostgreSQL

3. 데이터베이스 사용자 계정의 속성을 입력합니다.

다음 테이블에는 데이터베이스 사용자 계정의 속성이 나와 있습니다.

속성	설명
데이터베이스 사용자 ID	모니터링 모델 리포지토리 데이터베이스 사용자 계정의 이름입니다. Microsoft SQL Server에서 신뢰할 수 있는 연결을 위해 Windows NT 사용자 이름을 입력할 수 있습니다.
사용자 암호	모니터링 모델 리포지토리 사용자 계정의 암호입니다. Microsoft SQL Server에서 신뢰할 수 있는 연결을 위해 Windows NT 암호를 입력할 수 있습니다.

4. 보안 모니터링 모델 리포지토리 데이터베이스를 생성할지 여부를 선택합니다.

SSL 프로토콜로 보호되는 데이터베이스에 모니터링 모델 리포지토리를 생성할 수 있습니다. 보안 데이터베이스에 모니터링 모델 리포지토리를 생성하려면 **1**을 누르고 JDBC 정보를 입력하는 단계로 건너뛩니다.

비보안 데이터베이스에 모니터링 모델 리포지토리를 생성하려면 **2**를 누릅니다.

5. 보안 모니터링 모델 리포지토리를 생성하지 않을 경우 데이터베이스에 대한 매개 변수를 입력합니다.

a. IBM DB2를 선택하는 경우 테이블스페이스를 구성할지 여부를 선택하고 테이블스페이스 이름을 입력합니다.

다음 테이블에는 IBM DB2 데이터베이스에 대해 구성해야 하는 속성이 설명되어 있습니다.

Property	Description
Configure tablespace	In a single-partition database, if you select No, the installer creates the tables in the default tablespace. In a multi-partition database, you must select Yes. Select whether to specify a tablespace: 1 - No 2 - Yes
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single-partition database, enter the name of the tablespace in which to create the tables. In a multipartition database, specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

b. Microsoft SQL Server 또는 PostgreSQL을 선택하는 경우 데이터베이스의 스키마 이름을 입력합니다.

다음 테이블에는 데이터베이스에 대해 구성해야 하는 속성이 설명되어 있습니다.

Property	Description
Schema name	Name of the schema that will contain domain configuration tables. If this parameter is blank, the installer creates the tables in the default schema.

c. JDBC URL 정보를 사용하여 JDBC 연결 정보를 입력하려면 **1**을 누릅니다. 사용자 지정 JDBC 연결 문자열을 사용하여 JDBC 연결 정보를 입력하려면 **2**를 누릅니다.

d. JDBC 연결 정보를 입력합니다.

- JDBC URL 정보를 사용하여 연결 정보를 입력하려면 JDBC URL 속성을 지정합니다.

다음 테이블에는 데이터베이스 연결 정보가 설명되어 있습니다.

프롬프트	설명
데이터베이스 호스트 이름	데이터베이스의 호스트 이름입니다.
데이터베이스 포트 번호	데이터베이스의 포트 번호입니다.
데이터베이스 서비스 이름	서비스 또는 데이터베이스 이름: - Oracle: 서비스 이름을 입력합니다. - Microsoft SQL Server: 데이터베이스 이름을 입력합니다. - IBM DB2: 서비스 이름을 입력합니다. - PostgreSQL: 데이터베이스 이름을 입력합니다.
JDBC 매개 변수 구성	추가 JDBC 매개 변수를 연결 문자열에 추가할지 여부를 선택합니다. 1 - 예 2 - 아니요 예를 선택하는 경우 매개 변수를 입력하거나 Enter 키를 눌러 기본값을 수락합니다. 아니요를 선택하는 경우 설치 프로그램이 매개 변수 없이 JDBC 연결 문자열을 생성합니다.

- 사용자 지정 JDBC 연결 문자열을 사용하여 연결 정보를 입력하려면 연결 문자열을 입력합니다. JDBC 연결 문자열에 다음 구문을 사용합니다.

IBM DB2

```
jdbc:Informatica:db2://<호스트 이름>:<포트 번호>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<호스트 이름>:<포트 번호>;ServiceName=
```

Oracle Connection Manager를 통해 Oracle 데이터베이스에 연결하려면 다음 연결 문자열을 사용합니다.

```
jdbc:Informatica:oracle:TNSNamesFile=<tnsnames.ora 파일에 대한 정규화된 경로>;TNSServerName=<TNS 이름>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<호스트 이름>:<포트 번호>;SelectMethod=cursor;DatabaseName=
```

Windows NT 자격 증명이 있는 Microsoft SQL Server

Microsoft SQL Server에서 모델 리포지토리 데이터베이스에 대한 Windows NT 자격 증명을 지정한 경우 NTLM을 인증 방법으로 포함하도록 연결 문자열 구문을 지정합니다.

Windows NT 자격 증명이 있는 기본 인스턴스를 사용하는 Microsoft SQL Server:

```
"jdbc:informatica:sqlserver://<호스트 이름>:<포트 번호>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Windows NT 자격 증명이 있는 명명된 인스턴스를 사용하는 Microsoft SQL Server:

```
"jdbc:informatica:sqlserver://<호스트 이름>\<명명된 인스턴스 이름>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft Azure SQL Database

```
jdbc:Informatica:sqlserver://<호스트 이름>:<포트 번호>;SelectMethod=cursor;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

Active Directory 인증을 사용하는 Azure SQL Database

```
"jdbc:informatica: sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>"
```

PostgreSQL

```
jdbc:Informatica:postgresql://<호스트 이름>:<포트 번호>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<호스트 이름>:<포트 번호>;DatabaseName=<데이터베이스 이름>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLsv1.2;
```

데이터베이스 시스템에 필요한 모든 연결 매개 변수가 연결 문자열에 포함되어 있는지 확인합니다.

서비스 매개 변수 섹션이 나타납니다.

콘텐츠 관리 서비스 매개 변수 및 데이터베이스

데이터 통합 서비스를 구성한 후에는 콘텐츠 관리 서비스에 대한 매개 변수를 구성할 수 있습니다.

1. 다음 서비스 매개 변수 정보를 입력합니다.

매개 변수	설명
콘텐츠 관리 서비스 이름	Informatica 도메인에 생성할 콘텐츠 관리 서비스의 이름입니다.
HTTP 프로토콜 유형	콘텐츠 관리 서비스에 대한 연결 유형입니다. 다음 옵션 중 하나를 선택합니다. - HTTP. 서비스를 요청할 때 HTTP 연결을 사용합니다. - HTTPS. 서비스를 요청할 때 보안 HTTP 연결을 사용합니다.
HTTP 포트	콘텐츠 관리 서비스에 사용할 포트 번호입니다. 기본값은 8105입니다.

2. 콘텐츠 관리 서비스에 대한 키 저장소를 선택한 경우 콘텐츠 관리 서비스를 HTTPS로 연결하기 위한 키 저장소 파일 및 포트 번호를 입력합니다.

설치 프로그램에 의해 생성된 키 저장소 파일 또는 사용자가 생성하는 키 저장소 파일을 사용할지 여부를 선택합니다. 자체 서명된 인증서 또는 인증 기관에 의해 서명된 인증서와 함께 키 저장소 파일을 사용할 수 있습니다.

- 설치 프로그램이 생성한 기본 키 저장소를 사용합니다.
- 사용자 지정 키 저장소 파일의 위치와 암호를 지정하십시오.

설치 프로그램에 의해 생성된 키 저장소 파일을 사용하도록 선택하는 경우 설치 프로그램은 다음 위치에 **Default.keystore**라는 자체 서명된 키 저장소 파일을 생성합니다. <Informatica 설치 디렉터리>/tomcat/conf/ 콘텐츠 관리 서비스의 키 저장소 인증서 유형은 **Administrator** 도구에 사용되는 인증서 유형에 따라 달라집니다.

- **Administrator** 도구에 기본 키 저장소 인증서를 사용한 경우 콘텐츠 관리 서비스에 대해 기본 또는 사용자 지정 키 저장소 인증서를 사용할 수 있습니다.
- **Administrator** 도구에 사용자 지정 키 저장소 인증서를 사용한 경우 콘텐츠 관리 서비스에 대해 사용자 지정 키 저장소 인증서를 사용해야 합니다.

3. 추천 데이터 웨어하우스의 데이터베이스 유형을 선택합니다.

다음 테이블에는 참조 데이터 웨어하우스에 대한 데이터베이스가 나열되어 있습니다.

프롬프트	설명
데이터베이스 유형	참조 데이터 웨어하우스의 데이터베이스 유형입니다. 다음 옵션 중에서 선택하십시오. - IBM DB2 - Microsoft Azure SQL Database - Microsoft SQL Server - Oracle - JDBC를 사용하는 PostgreSQL

4. 데이터베이스 사용자 계정의 속성을 입력합니다.

다음 테이블에는 데이터베이스 사용자 계정의 속성이 나와 있습니다.

속성	설명
데이터베이스 사용자 ID	참조 데이터 웨어하우스 사용자 계정의 이름입니다.
데이터베이스 사용자 암호	참조 데이터 웨어하우스 사용자 계정의 암호입니다.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

5. 스키마 이름을 지정하려면 **1**을 누릅니다. 스키마 이름을 지정하지 않으려면 **2**를 누릅니다. 기본값은 **2**입니다. Microsoft SQL Server를 선택하는 경우 리포지토리 테이블의 스키마 및 데이터베이스 연결을 지정합니다. 스키마 이름을 지정하지 않으면 설치 프로그램이 기본 스키마에 테이블을 생성합니다.
6. JDBC URL 정보를 사용하여 JDBC 연결 정보를 입력하려면 **1**을 누릅니다. 사용자 지정 JDBC 연결 문자열을 사용하여 JDBC 연결 정보를 입력하려면 **2**를 누릅니다.
 - a. JDBC 연결 정보를 입력합니다.
 - JDBC URL 정보를 사용하여 연결 정보를 입력하려면 JDBC URL 속성을 지정합니다. 다음 테이블에는 데이터베이스 연결 정보가 설명되어 있습니다.

프롬프트	설명
데이터베이스 호스트 이름	데이터베이스의 호스트 이름입니다.
데이터베이스 포트 번호	데이터베이스의 포트 번호입니다.

프롬프트	설명
데이터베이스 서비스 이름	서비스 또는 데이터베이스 이름: - Oracle: 서비스 이름을 입력합니다. - Microsoft SQL Server: 데이터베이스 이름을 입력합니다. - IBM DB2: 서비스 이름을 입력합니다.
JDBC 매개 변수 구성	추가적인 JDBC 매개 변수를 연결 문자열에 추가할지 여부를 선택합니다. 1 - 예 2 - 아니요 예를 선택하는 경우 매개 변수를 입력하거나 Enter 키를 눌러 기본값을 수락합니다. 아니요를 선택하는 경우 설치 프로그램이 매개 변수 없이 JDBC 연결 문자열을 생성합니다.

- 사용자 지정 JDBC 연결 문자열을 사용하여 연결 정보를 입력하려면 연결 문자열을 입력합니다. JDBC 연결 문자열에 다음 구문을 사용합니다.

IBM DB2

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLsv1.2;
```

데이터베이스 시스템에 필요한 모든 연결 매개 변수가 연결 문자열에 포함되어 있는지 확인합니다.

7. 데이터 액세스 연결 문자열을 입력합니다.

프로파일링 웨어하우스 데이터베이스

콘텐츠 관리 서비스를 구성한 후에는 데이터 프로파일링 웨어하우스 데이터베이스를 구성할 수 있습니다.

1. 데이터 프로파일링 웨어하우스의 데이터베이스 유형을 선택합니다.

다음 테이블에는 데이터 프로파일링 웨어하우스의 데이터베이스가 나열되어 있습니다.

프롬프트	설명
데이터베이스 유형	데이터 프로파일링 웨어하우스의 데이터베이스 유형입니다. 다음 옵션 중에서 선택하십시오. - Oracle - Microsoft SQL Server - IBM DB2

- 데이터베이스 사용자 계정의 속성을 입력합니다.

다음 테이블에는 데이터베이스 사용자 계정의 속성이 나와 있습니다.

속성	설명
데이터베이스 사용자 ID	데이터 프로파일링 웨어하우스 사용자 계정의 이름입니다.
데이터베이스 사용자 암호	데이터 프로파일링 웨어하우스 사용자 계정의 암호입니다.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

- 스키마 이름을 지정하려면 **1**을 누릅니다. 스키마 이름을 지정하지 않으려면 **2**를 누릅니다. 기본값은 **2**입니다. **Microsoft SQL Server**를 선택하는 경우 리포지토리 테이블의 스키마 및 데이터베이스 연결을 지정합니다. 스키마 이름을 지정하지 않으면 설치 프로그램이 기본 스키마에 테이블을 생성합니다.
- JDBC URL** 정보를 사용하여 **JDBC** 연결 정보를 입력하려면 **1**을 누릅니다. 사용자 지정 **JDBC** 연결 문자열을 사용하여 **JDBC** 연결 정보를 입력하려면 **2**를 누릅니다.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

a. JDBC 연결 정보를 입력합니다.

- JDBC URL 정보를 사용하여 연결 정보를 입력하려면 JDBC URL 속성을 지정합니다.
다음 테이블에는 데이터베이스 연결 정보가 설명되어 있습니다.

프롬프트	설명
데이터베이스 호스트 이름	데이터베이스의 호스트 이름입니다.
데이터베이스 포트 번호	데이터베이스의 포트 번호입니다.
데이터베이스 서비스 이름	서비스 또는 데이터베이스 이름: - Oracle: 서비스 이름을 입력합니다. - Microsoft SQL Server: 데이터베이스 이름을 입력합니다. - IBM DB2: 서비스 이름을 입력합니다.
JDBC 매개 변수 구성	추가적인 JDBC 매개 변수를 연결 문자열에 추가할지 여부를 선택합니다. 1 - 예 2 - 아니요 예를 선택하는 경우 매개 변수를 입력하거나 Enter 키를 눌러 기본값을 수락합니다. 아니요를 선택하는 경우 설치 프로그램이 매개 변수 없이 JDBC 연결 문자열을 생성합니다.

- 사용자 지정 JDBC 연결 문자열을 사용하여 연결 정보를 입력하려면 연결 문자열을 입력합니다. JDBC 연결 문자열에 다음 구문을 사용합니다.

IBM DB2

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

데이터베이스 시스템에 필요한 모든 연결 매개 변수가 연결 문자열에 포함되어 있는지 확인합니다.

5. 데이터 액세스 연결 문자열을 입력합니다.

PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스

PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스를 구성할 수 있습니다.

1. PowerCenter 리포지토리에 사용하도록 구성할 데이터베이스를 선택합니다. 다음 데이터베이스 중 하나를 사용하여 PowerCenter 리포지토리를 구성할 수 있습니다.
 - 1 - Oracle
 - 2 - Microsoft SQL Server
 - 3 - PostgreSQL
2. 데이터베이스 사용자 계정의 속성을 입력합니다.

다음 테이블에는 데이터베이스 사용자 계정의 속성이 나와 있습니다.

속성	설명
데이터베이스 사용자 ID	PowerCenter 리포지토리 데이터베이스 사용자 계정의 이름입니다.
사용자 암호	PowerCenter 구성 데이터베이스 사용자 계정의 암호입니다.
데이터베이스 서비스 이름	PowerCenter의 서비스 또는 데이터베이스 이름입니다. - Oracle: 서비스 이름을 입력합니다. - Microsoft SQL Server: 데이터베이스 이름을 입력합니다. - PostgreSQL: 데이터베이스 이름을 입력합니다.
데이터베이스 호스트 이름	PowerCenter 데이터베이스 호스트 이름을 입력합니다. .

3. 생성할 PowerCenter 리포지토리 서비스의 이름을 입력합니다.
4. 생성할 PowerCenter 통합 서비스의 이름을 입력합니다.
5. PowerCenter 리포지토리 서비스 코드 페이지를 선택합니다. 기본값은 7비트 ASCII입니다.
6. PowerCenter 통합 서비스 코드 페이지를 선택합니다. 기본값은 7비트 ASCII입니다.

설치 후 요약 섹션에 설치가 완료되었는지 여부가 나타납니다. 또한 설치된 구성 요소 및 해당 구성의 상태도 요약에 표시됩니다.

도메인에 가입

여러 시스템에서 설치하는 중이며 다른 시스템에 도메인을 이미 생성한 경우 도메인에 가입할 수 있습니다.

설치 프로그램 실행

설치 프로그램을 실행하려면 다음 단계를 수행하십시오.

1. 시스템 사용자 계정으로 시스템에 로그인하십시오.
2. 다음 명령을 실행하여 시스템에서 **DISPLAY** 변수를 지웁니다. **unset DISPLAY**
3. 기타 모든 응용 프로그램을 닫으십시오.
4. 셸 명령줄에서 **install.sh** 파일을 실행합니다.
 설치 프로그램에 로컬 환경 변수가 설정되었는지 확인하라는 메시지가 표시됩니다.
5. 환경 변수가 설정되지 않은 경우 **n**을 눌러 설치 프로그램을 종료하고 필요에 따라 환경 변수를 설정합니다.
 환경 변수가 설정된 경우 **y**를 눌러 계속 진행합니다.

시작 - 약관 및 조건에 동의

- ▶ Informatica 설치 및 제품 사용 툴킷의 약관을 읽고 **약관을 읽고 동의함**을 선택합니다.

Informatica DiscoveryIQ는 데이터 사용에 대한 루틴 보고서와 시스템 통계를 Informatica로 전송하는 제품 사용 도구입니다. Informatica DiscoveryIQ에서는 사용자가 Informatica 도메인을 설치 및 구성한 후

2. Informatica 라이선스 키의 경로 및 파일 이름을 입력하고 **Enter** 키를 누릅니다.
3. Informatica 서비스 설치와 연결된 환경 유형을 지정하십시오.
 - 최소한의 사용자가 포함된 개념 증명에 사용되는 기본 환경의 경우 **1**을 눌러 샌드박스 환경을 설정하십시오.
 - 디자인 환경의 경우 **2**를 눌러 개발 환경을 설정하십시오.
 - 프로덕션 환경과 유사하게 처리 볼륨이 많은 경우 **3**을 눌러 테스트 환경을 설정하십시오.
 - 최종 사용자를 위한 높은 수준의 동시성으로 처리 볼륨이 많은 경우 **4**를 눌러 프로덕션 환경을 설정하십시오. 고급 프로덕션 환경은 일반적으로 다중 노드 설정입니다.
 기본값은 샌드박스의 경우 **1**입니다.

Kerberos 네트워크 인증을 활성화한 경우, **서비스 사용자 수준** 섹션이 나타납니다.

Kerberos 네트워크 인증을 활성화하지 않은 경우, **설치 전 요약** 섹션이 나타납니다. 설치 정보를 검토하고 **Enter** 키를 눌러 계속 진행합니다. [“도메인 선택” 페이지 144](#) 단계로 건너뛩니다.

서비스 사용자 수준

설치 디렉터리를 지정한 후에는 보안 수준을 구성할 수 있습니다.

- ▶ 도메인에 대해 Kerberos 서비스 사용자를 어떤 수준으로 설정할지 선택합니다.

참고: 도메인의 모든 노드가 동일한 서비스 사용자 수준을 사용해야 합니다. 도메인에 노드를 가입시키는 경우 도메인의 게이트웨이 노드에서 사용하는 것과 동일한 서비스 사용자 수준을 선택하십시오.

다음 테이블에는 선택할 수 있는 수준이 설명되어 있습니다.

수준	설명
프로세스 수준	<p>각 노드 및 노드의 각 응용 프로그램 서비스에 대해 고유한 SPN(서비스 사용자 이름) 및 키 탭 파일을 사용하도록 도메인을 구성합니다.</p> <p>각 노드에 필요한 SPN 및 키 탭 파일의 수는 노드에서 실행되는 응용 프로그램 서비스 프로세스의 수에 따라 달라집니다. 운영 도메인 같이 높은 보안 수준이 필요한 도메인에 대해 프로세스 수준 옵션을 사용하십시오.</p>
노드 수준	<p>노드에서 SPN 및 키 탭 파일을 공유하도록 도메인을 구성합니다.</p> <p>이 옵션에는 노드에 대한 하나의 SPN과 키 탭 파일 및 노드에서 실행되는 모든 응용 프로그램 서비스가 필요합니다. 또한 노드의 모든 HTTP 프로세스에 대해 별도의 SPN 및 키 탭 파일이 필요합니다.</p> <p>테스트 및 개발 도메인 같이 높은 보안 수준이 필요하지 않은 도메인에 대해 노드 수준 옵션을 사용하십시오.</p>

사전 **설치 요약** 섹션이 나타납니다. **Enter** 키를 눌러 계속 진행합니다.

도메인 선택

설치 전 요약을 검토한 후에는 도메인 정보를 입력할 수 있습니다.

1. **2**를 눌러 도메인에 가입합니다.
 - 사용자가 설치한 시스템의 노드에 설치 프로그램이 가입합니다.
2. 가입하려는 도메인에서 보안 통신 옵션이 활성화되었는지 여부를 지정합니다.
 - 1**을 눌러 비보안 도메인에 가입하거나 **2**를 눌러 보안 도메인에 가입합니다.
3. 생성할 노드 유형을 선택합니다.

1을 눌러 게이트웨이 노드를 구성하거나 **2**를 눌러 작업자 노드를 구성합니다.

노드를 게이트웨이로 구성한 경우, Informatica Administrator에 대한 보안 HTTPS 연결을 활성화할 수 있습니다.

4. Informatica Administrator에 HTTPS 연결을 사용하는 경우 이 연결을 보호하는 데 사용할 HTTPS 포트 번호를 입력하십시오.
5. 도메인에서 SAML 인증을 활성화하는 데 기본 Informatica SSL 인증서를 사용할지 또는 사용자의 SSL 인증서를 사용할지 선택합니다.

다음 테이블에는 SAML 인증에 대한 SSL 인증서 옵션이 설명되어 있습니다.

옵션	설명
기본 Informatica SSL 인증서 파일을 사용합니다.	SAML 인증에 기본 Informatica 트러스트 저장소 파일을 사용하려면 선택합니다.
SSL 인증서 파일의 위치를 입력하십시오.	SAML 인증을 위한 사용자 지정 트러스트 저장소 파일을 사용하려면 선택합니다. 도메인 내의 게이트웨이 노드에 대한 사용자 지정 트러스트 저장소 파일이 포함된 디렉토리를 지정하십시오. 파일에 대한 전체 경로가 아닌 디렉터리만 지정하십시오.

6. Informatica 도메인에서 웹 기반 Informatica 응용 프로그램에 SAML(Security Assertion Markup Language) 기반 SSO(Single Sign-On) 지원을 구성하려면 SAML 인증을 활성화할지 여부를 선택합니다. 도메인에서 SAML 인증을 사용하는지 선택합니다.
 - a. 아니요의 경우 **1**을 눌러 SAML 인증을 비활성화합니다.
 - 아니요를 선택한 경우, [“도메인 보안 - 보안 통신” 페이지 145](#) 항목으로 건너뛸니다.
 - b. 예의 경우 **2**를 눌러 SAML 인증을 활성화합니다.
 - 예를 선택한 경우, SAML 인증을 구성합니다.

도메인 보안 - 보안 통신이 표시됩니다.

도메인 보안 - 보안 통신

도메인을 선택한 후에는 도메인 보안을 구성할 수 있습니다.

- ▶ 도메인 통신을 보호하는 데 기본 Informatica SSL 인증서를 사용할지 아니면 사용자의 SSL 인증서를 사용할지 지정합니다.
 - a. 사용할 SSL 인증서의 유형을 선택합니다.

다음 테이블에는 Informatica 도메인을 보호하는 데 사용할 수 있는 SSL 인증서에 대한 옵션이 설명되어 있습니다.

옵션	설명
기본 Informatica SSL 인증서 사용	기본 키 저장소 및 트러스트 저장소에 포함된 기본 SSL 인증서를 사용합니다. 참고: SSL 인증서를 제공하지 않을 경우 Informatica에서는 모든 Informatica 설치에 동일한 기본 개인 키를 사용합니다. 기본 Informatica 키 저장소 및 트러스트 저장소 파일을 사용하는 경우 도메인의 보안이 침해될 수 있습니다. 도메인의 보안 수준을 높이려면 SSL 인증서 파일의 위치를 지정하는 옵션을 선택하십시오.
사용자 지정 SSL 인증서 사용	SSL 인증서가 포함된 키 저장소와 트러스트 저장소 파일의 경로를 지정합니다. 키 저장소 및 트러스트 저장소의 암호도 지정해야 합니다. 자체 서명된 인증서 또는 CA(인증 기관)에서 발급한 인증서를 제공할 수 있습니다. SSL 인증서를 PEM 형식 및 JKS(Java 키 저장소) 파일로 제공해야 합니다. Informatica 도메인에 대한 SSL 인증서 파일 관련 이름이 필요합니다. 도메인의 모든 노드에 대해 동일한 SSL 인증서를 사용해야 합니다. 도메인의 모든 노드에 액세스 가능한 디렉터리에서 트러스트 저장소 및 키 저장소 파일을 저장하고 동일한 도메인의 모든 노드에 대해 동일한 키 저장소 파일 디렉터리 및 트러스트 저장소 파일 디렉터를 지정합니다.

- b. 사용자가 SSL 인증서를 제공하는 경우 키 저장소 및 트러스트 저장소 파일의 위치와 암호를 지정합니다.

다음 테이블에는 SSL 인증서 파일에 대해 입력해야 하는 매개 변수가 설명되어 있습니다.

속성	설명
키 저장소 파일 디렉터리	키 저장소 파일이 포함된 디렉터리입니다. 디렉터리에 이름이 infa_keystore.jks인 파일이 포함되어 있어야 합니다.
키 저장소 암호	키 저장소 infa_keystore.jks의 암호입니다.
트러스트 저장소 파일 디렉터리	트러스트 저장소 파일이 포함된 디렉터리입니다. 이 디렉터리에는 infa_truststore.jks 및 infa_truststore.pem이라는 파일이 포함되어야 합니다.
트러스트 저장소 암호	infa_truststore.jks 파일의 암호입니다.

도메인 구성 섹션이 나타납니다.

도메인 구성

도메인 보안을 구성한 후에는 도메인 리포지토리 연결 세부 정보를 구성할 수 있습니다.

- ▶ 가입할 도메인에 대한 정보를 입력합니다.

다음 테이블에는 사용자가 도메인에 대해 지정하는 속성이 설명되어 있습니다.

속성	설명
도메인 이름	가입할 도메인의 이름입니다.
게이트웨이 노드 호스트	도메인의 게이트웨이 노드를 호스팅하는 시스템의 호스트 이름입니다.
게이트웨이 노드 포트	게이트웨이 노드의 포트 번호입니다.
도메인 사용자 이름	가입할 도메인에 대한 관리자의 사용자 이름입니다.
도메인 암호	도메인 관리자의 암호입니다.
보안 도메인 이름	보안 도메인의 이름입니다.

도메인 보안 - 암호화 키 섹션이 나타납니다.

도메인 보안 - 암호화 키

도메인 리포지토리를 구성한 후에는 암호화 키를 구성할 수 있습니다.

- ▶ Informatica 도메인의 암호화 키에 대한 디렉터리를 입력합니다.

다음 테이블에는 도메인에 가입할 때 지정해야 하는 암호화 키 매개 변수가 설명되어 있습니다.

프롬프트	설명
암호화 키 선택	가입할 Informatica 도메인에 대한 암호화 키의 경로 및 파일 이름입니다. Informatica 도메인의 모든 노드는 동일한 암호화 키를 사용합니다. 가입할 도메인에 대한 게이트웨이 노드에서 생성된 암호화 키 파일을 지정해야 합니다. 암호화 키 파일을 임시 디렉터리에 복사하여 도메인의 노드에서 액세스할 수 있게 만든 경우 임시 디렉터리에 있는 암호화 키 파일의 경로 및 파일 이름을 지정하십시오.
암호화 키 디렉터리	이 설치 과정에서 생성되는 노드에서 암호화 키가 저장되는 디렉터리입니다. 설치 프로그램은 도메인의 암호화 키 파일을 새로운 노드의 암호화 키 디렉터리에 복사합니다.

설치 프로그램이 디렉터리 및 해당 디렉터리의 파일에 대해 서로 다른 사용 권한을 설정합니다. 암호화 키 파일 및 디렉터리의 사용 권한에 대한 자세한 내용은 [“보안 파일 및 디렉터리” 페이지 98](#)를 참조하십시오.

도메인 가입 노드 구성 섹션이 표시됩니다.

도메인 가입 노드 구성

암호화 키를 구성한 후에는 가입 도메인 및 노드를 구성할 수 있습니다.

1. 가입할 도메인 및 노드에 대한 정보를 입력합니다.

다음 테이블에는 현재 노드에 대해 설정해야 하는 속성이 설명되어 있습니다.

속성	설명
노드 호스트 이름	가입할 노드가 있는 시스템의 호스트 이름 또는 IP 주소입니다. 시스템이 단일 네트워크 이름을 갖는 경우 기본 호스트 이름을 사용하십시오. 시스템이 여러 네트워크 이름을 갖는 경우 대체 네트워크 이름을 사용하도록 기본 호스트 이름을 수정할 수 있습니다. 참고: 노드 호스트 이름에는 밑줄(_) 문자를 사용할 수 없습니다. localhost는 사용하지 마십시오. 호스트 이름은 명시적으로 시스템을 식별해야 합니다.
노드 이름	가입할 노드의 이름입니다.
노드 포트 번호	노드의 포트 번호입니다. 노드의 기본 포트 번호는 6005입니다. 시스템에서 해당 포트 번호를 사용할 수 없는 경우 사용 가능한 다음 포트 번호가 설치 프로그램에 표시됩니다.

- 설치 프로그램에 의해 할당된 도메인 및 노드 구성 요소에 대한 고급 포트 구성을 표시할지 여부를 선택합니다.
1을 선택하면 설치 프로그램이 포트 구성을 표시하지 않습니다. 포트를 생성하기 위해 **2**를 선택하면 **포트 구성** 섹션이 나타납니다. 도메인 구성 요소에 할당된 기본 포트 번호가 표시됩니다. 도메인 및 노드 구성 요소에 사용할 포트 번호를 지정할 수 있습니다. 노드에서 실행될 서비스 프로세스에 사용할 포트 번호의 범위도 지정할 수 있습니다. 기본 포트 번호를 사용하거나 새 포트 번호를 지정할 수 있습니다. 입력하는 포트 번호가 다른 응용 프로그램에서 사용되지 않는지 확인합니다.
- 설치 중에 모델 리포지토리 서비스와 데이터 통합 서비스를 생성하려면 **1**을 선택합니다. 나중에 생성하려면 **2**를 선택합니다.
- 설치 중에 PowerCenter 리포지토리 서비스와 PowerCenter 통합 서비스를 생성하려면 **1**을 선택합니다. 나중에 생성하려면 **2**를 선택합니다.

설치 후 요약 섹션에 설치가 완료되었는지 여부가 나타납니다. 또한 설치된 구성 요소 및 해당 구성의 상태도 요약에 표시됩니다.

포트 구성

고급 포트 구성 페이지를 표시하도록 선택한 경우 도메인 구성 요소에 대한 포트를 설정할 수 있습니다.

- ▶ 프롬프트에 새 포트 번호를 입력하거나 **Enter** 키를 눌러 기본 포트 번호를 사용합니다.

다음 테이블에는 사용자가 설정할 수 있는 포트가 설명되어 있습니다.

Port	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.

설치 후 요약 섹션이 나타납니다. **설치 후 요약** 섹션에 설치가 완료되었는지 여부가 나타납니다. 또한 설치된 구성 요소 및 해당 구성의 상태도 요약에 표시됩니다.

모델 리포지토리 데이터베이스 구성

도메인과 노드를 구성한 후에는 모델 리포지토리 데이터베이스 속성을 구성할 수 있습니다.

1. 모델 리포지토리 서비스 이름을 입력합니다.

서비스 이름을 입력합니다. 이름은 대/소문자를 구분하지 않으며 도메인 내에서 고유해야 합니다. 이름은 128자를 초과하거나 @로 시작할 수 없습니다. 또한 공백이나 다음과 같은 특수 문자를 포함할 수도 없습니다.

`` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! () [`

서비스를 생성한 후에는 서비스 이름을 변경할 수 없습니다.

프로세스 수준 SPN을 선택한 경우 모델 리포지토리 서비스 키 탭 파일을 지정합니다. 모델 리포지토리 서비스 프로세스에 대한 키 탭 파일입니다. 키 탭 파일은 다음과 같은 이름을 가져야 합니다. **.keytab**

2. 모델 리포지토리를 구성할 데이터베이스를 선택합니다.

다음 테이블에는 모델 리포지토리를 구성할 수 있는 데이터베이스가 나열되어 있습니다.

프롬프트	설명
데이터베이스 유형	<p>모델 리포지토리의 데이터베이스 유형입니다. 다음 옵션 중에서 선택하십시오.</p> <p>1 - Oracle 2 - Microsoft SQL Server 3 - IBM DB2 4 - PostgreSQL</p>

3. 데이터베이스 사용자 계정의 속성을 입력합니다.

다음 테이블에는 데이터베이스 사용자 계정의 속성이 나와 있습니다.

속성	설명
데이터베이스 사용자 ID	<p>모델 리포지토리 데이터베이스 사용자 계정의 이름입니다. Microsoft SQL Server에서 신뢰할 수 있는 연결을 위해 Windows NT 사용자 이름을 입력할 수 있습니다.</p>
사용자 암호	<p>모델 리포지토리 사용자 계정의 암호입니다. Microsoft SQL Server에서 신뢰할 수 있는 연결을 위해 Windows NT 암호를 입력할 수 있습니다.</p>

4. 보안 모델 리포지토리 데이터베이스를 생성할지 여부를 선택합니다.

SSL 프로토콜로 보호되는 데이터베이스에 모델 리포지토리 서비스를 생성할 수 있습니다. 보안 데이터베이스에 모델 리포지토리 서비스를 생성하려면 **1**을 누르고 **JDBC** 정보를 입력하는 단계로 건너뛩니다.

비보안 데이터베이스에 모델 리포지토리 서비스를 생성하려면 **2**를 누릅니다.

5. 보안 모델 리포지토리를 생성하지 않도록 선택한 경우 데이터베이스에 대한 매개 변수를 입력합니다.

- a. IBM DB2를 선택하는 경우 테이블스페이스를 구성할지 여부를 선택하고 테이블스페이스 이름을 입력합니다.

다음 테이블에는 IBM DB2 데이터베이스에 대해 구성해야 하는 속성이 설명되어 있습니다.

Property	Description
Configure tablespace	<p>In a single-partition database, if you select No, the installer creates the tables in the default tablespace. In a multi-partition database, you must select Yes.</p> <p>Select whether to specify a tablespace:</p> <p>1 - No 2 - Yes</p>
Tablespace	<p>Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes.</p> <p>In a single-partition database, enter the name of the tablespace in which to create the tables.</p> <p>In a multipartition database, specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.</p>

- b. Microsoft SQL Server 또는 PostgreSQL을 선택하는 경우 데이터베이스의 스키마 이름을 입력합니다. 다음 테이블에는 데이터베이스에 대해 구성해야 하는 속성이 설명되어 있습니다.

Property	Description
Schema name	Name of the schema that will contain domain configuration tables. If this parameter is blank, the installer creates the tables in the default schema.

- c. JDBC URL 정보를 사용하여 JDBC 연결 정보를 입력하려면 **1**을 누릅니다. 사용자 지정 JDBC 연결 문자열을 사용하여 JDBC 연결 정보를 입력하려면 **2**를 누릅니다.
- d. JDBC 연결 정보를 입력합니다.
- JDBC URL 정보를 사용하여 연결 정보를 입력하려면 JDBC URL 속성을 지정합니다. 다음 테이블에는 데이터베이스 연결 정보가 설명되어 있습니다.

프롬프트	설명
데이터베이스 호스트 이름	데이터베이스의 호스트 이름입니다.
데이터베이스 포트 번호	데이터베이스의 포트 번호입니다.
데이터베이스 서비스 이름	서비스 또는 데이터베이스 이름: - Oracle: 서비스 이름을 입력합니다. - Microsoft SQL Server: 데이터베이스 이름을 입력합니다. - IBM DB2: 서비스 이름을 입력합니다. - PostgreSQL: 데이터베이스 이름을 입력합니다.
JDBC 매개 변수 구성	추가 JDBC 매개 변수를 연결 문자열에 추가할지 여부를 선택합니다. 1 - 예 2 - 아니요 예를 선택하는 경우 매개 변수를 입력하거나 Enter 키를 눌러 기본값을 수락합니다. 아니요를 선택하는 경우 설치 프로그램이 매개 변수 없이 JDBC 연결 문자열을 생성합니다.

- 사용자 지정 JDBC 연결 문자열을 사용하여 연결 정보를 입력하려면 연결 문자열을 입력합니다. JDBC 연결 문자열에 다음 구문을 사용합니다.

IBM DB2

```
jdbc:Informatica:db2://<호스트 이름>:<포트 번호>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<호스트 이름>:<포트 번호>;ServiceName=
```

Oracle Connection Manager를 통해 Oracle 데이터베이스에 연결하려면 다음 연결 문자열을 사용합니다.

```
jdbc:Informatica:oracle:TNSNamesFile=<tnsnames.ora 파일에 대한 정규화된 경로>;TNSServerName=<TNS 이름>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<호스트 이름>:<포트 번호>;SelectMethod=cursor;DatabaseName=
```

Windows NT 자격 증명이 있는 Microsoft SQL Server

Microsoft SQL Server에서 모델 리포지토리 데이터베이스에 대한 Windows NT 자격 증명을 지정한 경우 NTLM을 인증 방법으로 포함하도록 연결 문자열 구문을 지정합니다.

Windows NT 자격 증명이 있는 기본 인스턴스를 사용하는 Microsoft SQL Server:

```
"jdbc:informatica:sqlserver://<호스트 이름>:<포트 번호>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Windows NT 자격 증명이 있는 명명된 인스턴스를 사용하는 Microsoft SQL Server:

```
"jdbc:informatica:sqlserver://<호스트 이름>\<명명된 인스턴스 이름>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft Azure SQL Database

```
jdbc:Informatica:sqlserver://<호스트 이름>:<포트 번호>;SelectMethod=cursor;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

Active Directory 인증을 사용하는 Azure SQL Database

```
"jdbc:informatica: sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>"
```

PostgreSQL

```
jdbc:Informatica:postgresql://<호스트 이름>:<포트 번호>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<호스트 이름>:<포트 번호>;DatabaseName=<데이터베이스 이름>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

데이터베이스 시스템에 필요한 모든 연결 매개 변수가 연결 문자열에 포함되어 있는지 확인합니다.

서비스 매개 변수 섹션이 나타납니다.

데이터 통합 서비스

모델 리포지토리 데이터베이스를 구성한 후에는 응용 프로그램 서비스에 대한 서비스 매개 변수를 구성할 수 있습니다.

1. 다음 서비스 매개 변수 정보를 입력합니다.

포트	설명
데이터 통합 서비스 이름	Informatica 도메인에 생성할 데이터 통합 서비스의 이름입니다.
HTTP 프로토콜 유형	데이터 통합 서비스에 대한 연결 유형입니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> - HTTP. 서비스를 요청할 때 HTTP 연결을 사용합니다. - HTTPS. 서비스를 요청할 때 보안 HTTP 연결을 사용합니다. - HTTP&HTTPS. 서비스를 요청할 때 HTTP 또는 HTTPS 연결을 사용할 수 있습니다.
HTTP 포트	데이터 통합 서비스에 사용할 포트 번호입니다. 기본값은 9085입니다.
HTTPS 포트	데이터 통합 서비스에 사용할 포트 번호입니다. 기본값은 9085입니다.

2. 데이터 통합 서비스를 보호하는 데 사용할 SSL 인증서를 선택합니다.

옵션	설명
기본 Informatica SSL 인증서 파일을 사용합니다.	기본 키 저장소 및 트러스트 저장소에 포함된 기본 Informatica SSL 인증서를 사용합니다. 참고: SSL 인증서를 제공하지 않을 경우 Informatica에서는 모든 Informatica 설치에 동일한 기본 개인 키를 사용합니다. 기본 Informatica 키 저장소 및 트러스트 저장소 파일을 사용하는 경우 도메인의 보안이 침해될 수 있습니다. 도메인의 보안 수준을 높이려면 SSL 인증서 파일의 위치를 지정하는 옵션을 선택하십시오.
사용자 지정 SSL 인증서 사용	사용자 지정 SSL 인증서를 사용합니다. 키 저장소 및 트러스트 저장소 파일의 위치를 지정해야 합니다. 자체 서명된 인증서 또는 CA(인증 기관)에서 발급한 인증서를 제공할 수 있습니다. SSL 인증서를 PEM 형식 및 JKS(Java 키 저장소) 파일로 제공해야 합니다. Informatica 도메인에 대한 SSL 인증서 파일 관련 이름이 필요합니다. 도메인의 모든 노드에 대해 동일한 SSL 인증서를 사용해야 합니다. 도메인의 모든 노드에 액세스 가능한 디렉터리에서 트러스트 저장소 및 키 저장소 파일을 저장하고 동일한 도메인의 모든 노드에 대해 동일한 키 저장소 파일 디렉터리 및 트러스트 저장소 파일 디렉터를 지정합니다.

사용자 지정 SSL 인증서를 사용하도록 선택한 경우 다음 정보를 입력합니다.

속성	설명
키 저장소 파일 디렉터리	키 저장소 파일이 포함된 디렉터리입니다. 이 디렉터리에는 infa_keystore.jks 및 infa_keystore.pem이라는 파일이 포함되어야 합니다.
키 저장소 암호	키 저장소 infa_keystore.jks의 암호입니다.

속성	설명
트러스트 저장소 파일 디렉터리	트러스트 저장소 파일이 포함된 디렉터리입니다. 이 디렉터리에는 infa_truststore.jks 및 infa_truststore.pem이라는 파일이 포함되어야 합니다.
트러스트 저장소 암호	infa_truststore.jks 파일의 암호입니다.

PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스

PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스를 구성할 수 있습니다.

- PowerCenter 리포지토리에 사용하도록 구성할 데이터베이스를 선택합니다.
다음 데이터베이스 중 하나를 사용하여 PowerCenter 리포지토리를 구성할 수 있습니다.
 - Oracle
 - Microsoft SQL Server
 - PostgreSQL
- 데이터베이스 사용자 계정의 속성을 입력합니다.
다음 테이블에는 데이터베이스 사용자 계정의 속성이 나와 있습니다.

속성	설명
데이터베이스 사용자 ID	PowerCenter 리포지토리 데이터베이스 사용자 계정의 이름입니다.
사용자 암호	PowerCenter 구성 데이터베이스 사용자 계정의 암호입니다.
데이터베이스 서비스 이름	PowerCenter의 서비스 또는 데이터베이스 이름입니다. - Oracle: 서비스 이름을 입력합니다. - Microsoft SQL Server: 데이터베이스 이름을 입력합니다. - PostgreSQL: 데이터베이스 이름을 입력합니다.
데이터베이스 호스트 이름	PowerCenter 데이터베이스 호스트 이름을 입력합니다. .

- 생성할 PowerCenter 리포지토리 서비스의 이름을 입력합니다.
 - 생성할 PowerCenter 통합 서비스의 이름을 입력합니다.
 - PowerCenter 리포지토리 서비스 코드 페이지를 선택합니다. 기본값은 7비트 ASCII입니다.
 - PowerCenter 통합 서비스 코드 페이지를 선택합니다. 기본값은 7비트 ASCII입니다.
- 설치 후 요약** 섹션에 설치가 완료되었는지 여부가 나타납니다. 또한 설치된 구성 요소 및 해당 구성의 상태도 요약에 표시됩니다.

제 9 장

그래픽 모드에서 Informatica 서비스 설치

이 장에 포함된 항목:

- [그래픽 모드에서 Informatica 서비스 설치 개요, 155](#)
- [도메인 생성, 155](#)
- [도메인에 가입, 198](#)

그래픽 모드에서 Informatica 서비스 설치 개요

Windows에서 Informatica 서비스를 그래픽 모드로 설치할 수 있습니다.

설치를 수행하기 전에 설치 전 시스템 검사 도구(i10Pi)를 실행하면 설치 프로그램에서 시스템 검사 중에 사용자가 입력한 정보에 따라 데이터베이스 연결 및 도메인 포트 번호 등의 특정 필드에 대해 값을 설정합니다.

Windows에서 루트 디렉터리의 `install.bat` 파일을 실행할 때 문제가 발생하는 경우 다음 파일을 실행하십시오.
<설치 프로그램 파일 디렉터리>\server\install.exe.

도메인 생성

처음으로 설치하는 경우 또는 별도 도메인의 노드를 관리하려는 경우 도메인을 생성합니다.

설치 프로그램 실행

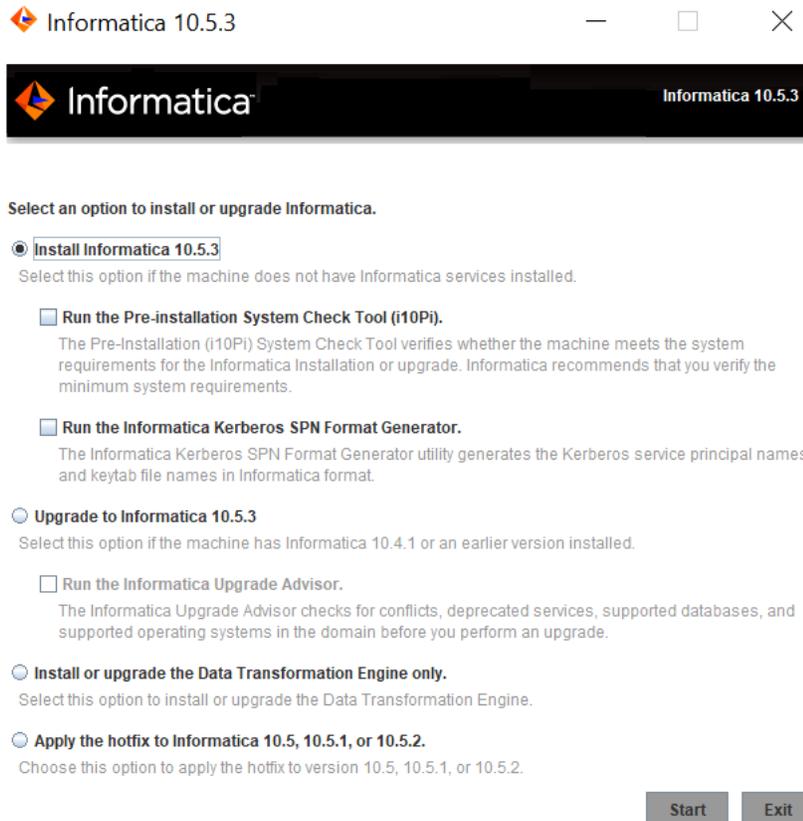
설치 프로그램을 실행하려면 다음 단계를 수행하십시오.

1. 시스템 사용자 계정으로 시스템에 로그인합니다.
2. 기타 모든 응용 프로그램을 닫습니다.

- 설치 파일의 디렉터리 루트로 이동하고 관리자 권한으로 `install.bat`를 실행합니다.
관리자로 이 파일을 실행하려면 `install.bat` 파일을 마우스 오른쪽 단추로 클릭하고 **관리자 권한으로 실행**을 선택합니다.
참고: 관리자 권한으로 설치 프로그램을 실행하지 않는 경우 Windows 시스템 관리자가 Informatica 설치 디렉터리의 파일을 액세스할 때 문제가 발생할 수 있습니다.
Informatica 10.5.3 페이지가 나타납니다.

Informatica 설치 프로그램 시작

- Informatica 10.5.3 설치를 선택합니다.



Informatica는 Informatica 서비스 설치 프로세스를 용이하게 하기 위한 유틸리티를 제공합니다. Informatica 서비스를 설치하기 전에 다음 유틸리티를 실행하십시오.

- 설치 전 시스템 검사 도구(i10Pi). Informatica 서비스를 설치할 시스템이 설치를 위한 시스템 요구 사항을 충족하는지 확인합니다.
설치 전 시스템 검사 도구(i10Pi) 실행에 대한 자세한 내용은 [“설치 전 시스템 검사 도구\(i10Pi\) 실행\(그래픽 모드\)” 페이지 102](#)을 참조하십시오.
- Informatica Kerberos SPN 형식 생성기. Kerberos 인증이 포함된 네트워크에서 Informatica 서비스를 실행하는 데 필요한 Kerberos 서비스 사용자 이름과 키 탭 파일 이름 목록을 생성합니다.

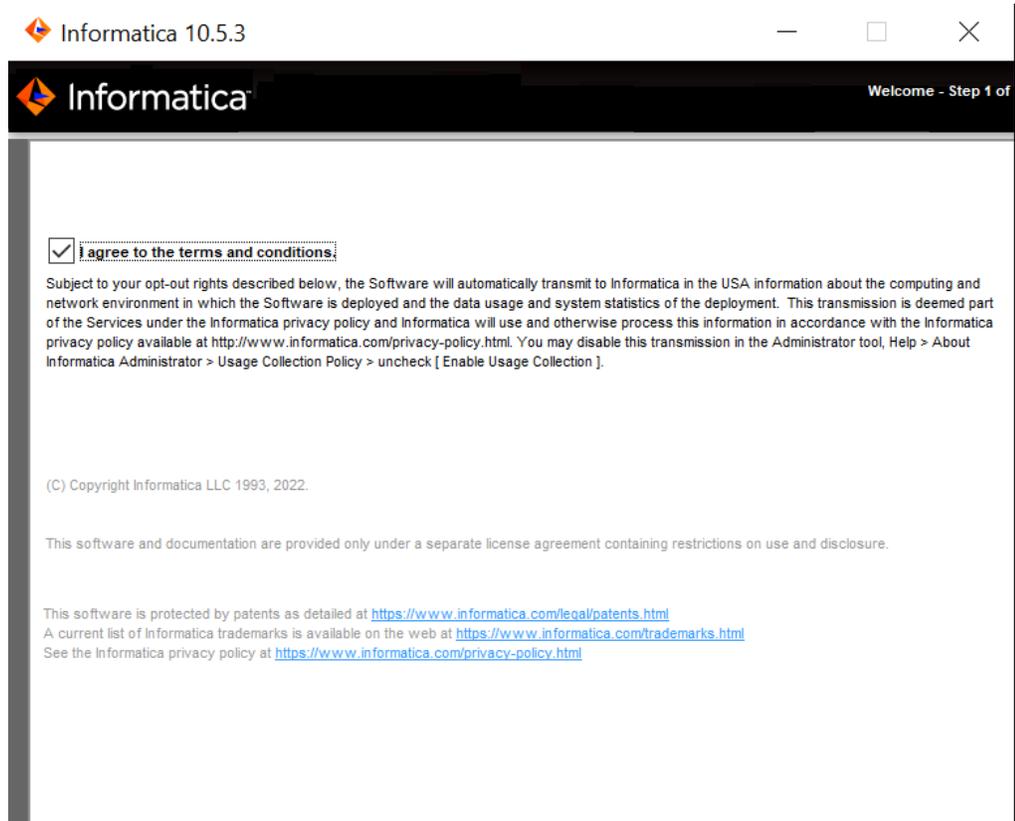
Informatica 서비스를 설치하기 전에 설치 프로그램을 사용하여 유틸리티를 실행할 수 있습니다. 유틸리티 실행을 마친 후 설치 프로그램을 다시 시작하여 다음 유틸리티를 실행하거나 Informatica 서비스를 설치합니다.

- 시작을 클릭합니다.

시작 섹션이 나타납니다.

시작 - 약관 및 조건에 동의

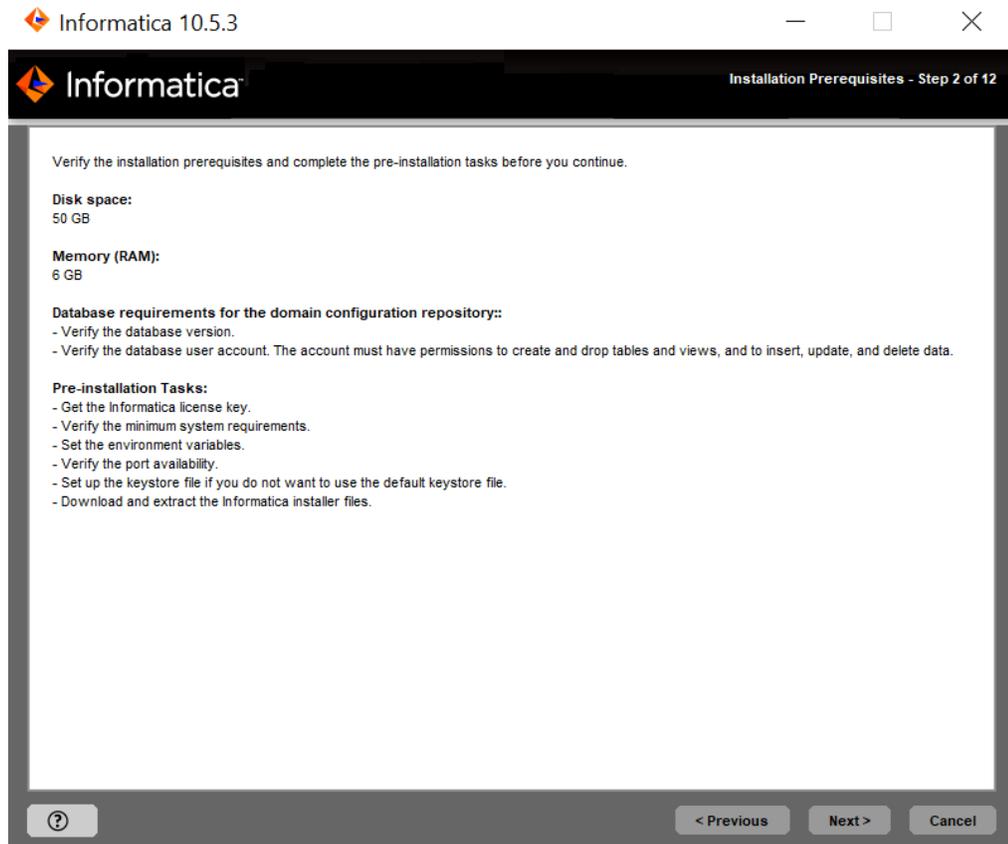
1. Informatica 설치 및 제품 사용 툴킷의 약관을 읽고 **약관을 읽고 동의함**을 선택합니다.



Informatica DiscoveryIQ는 데이터 사용에 대한 루틴 보고서와 시스템 통계를 Informatica로 전송하는 제품 사용 도구입니다. Informatica DiscoveryIQ에서는 사용자가 Informatica 도메인을 설치 및 구성한 후 15분이 지나면 데이터를 Informatica로 업로드합니다. 이후부터는 도메인에서 30일마다 데이터를 전송합니다. Administrator 도구에서 사용 통계를 비활성화하도록 선택할 수 있습니다.

2. 다음을 클릭합니다.

설치 선행 조건 페이지에 설치 요구 사항이 표시됩니다. 설치를 계속하기 전에 모든 요구 사항이 충족되었는지 확인합니다.



3. 다음을 클릭합니다.

라이선스 및 설치 디렉터리 섹션이 나타납니다.

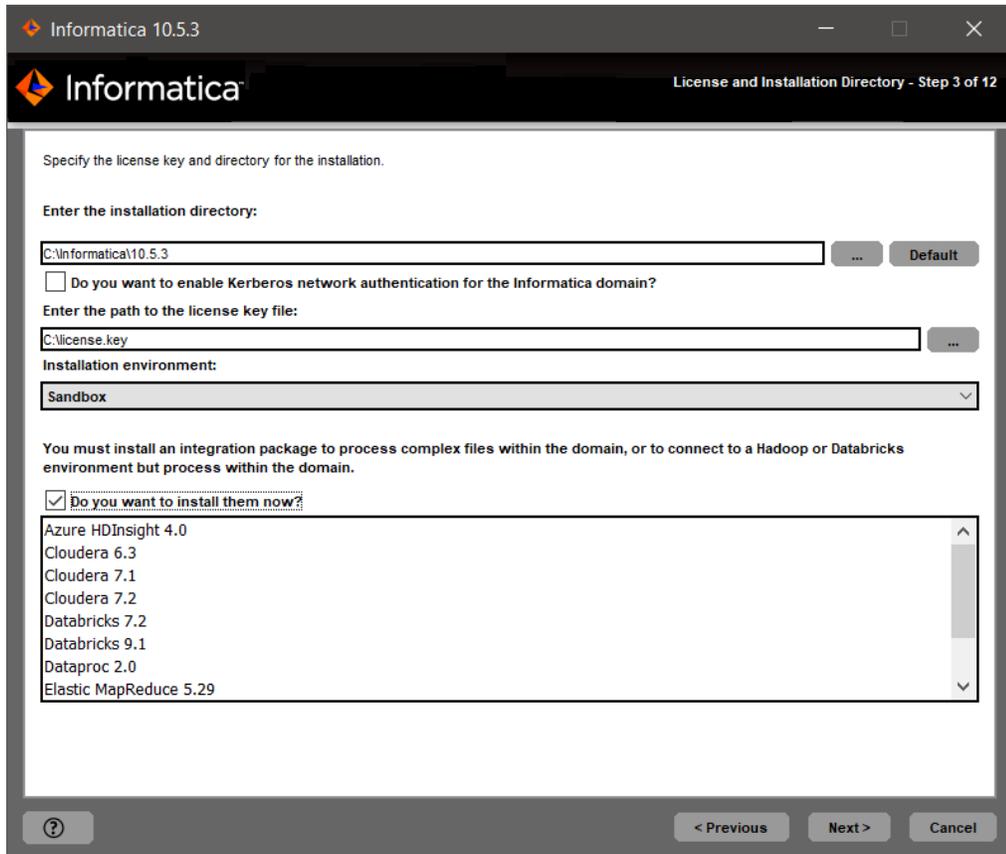
License and Installation Directory

After you verify the installation prerequisites, you can specify the installation directory.

1. On the **License and Installation Directory** page, enter the Informatica license key, installation directory, installation environment, and distribution packages.

The following table describes the license key, directory that you specify for the Informatica services installation, and the distribution packages installation:

Property	Description
License key file	Path and file name of the Informatica license key.
Installation directory	<p>Absolute path for the installation directory. The installation directory must be on the machine where you are installing Informatica. The directory names in the path must not contain spaces or the following special characters: @ * \$ # ! % () { } []</p> <p>참고: Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.</p>
Installation environment	<p>Environment type associated with the Informatica services installation.</p> <ul style="list-style-type: none"> - Set Sandbox environment for a basic environment used for proof of concept with minimal users. - Set Development environment for the design environment. - Set Test environment for high volume processing that is closest to a production environment. - Set Production environment for high volume processing with high levels of concurrency meant for end users. Advanced production environments are typically multi-node setups.
Distribution packages	<p>You can choose whether to install distribution packages through the Informatica installer.</p> <p>If you choose to install distribution packages, select one or more packages from the list that you want to install.</p>



2. Click **Next**.

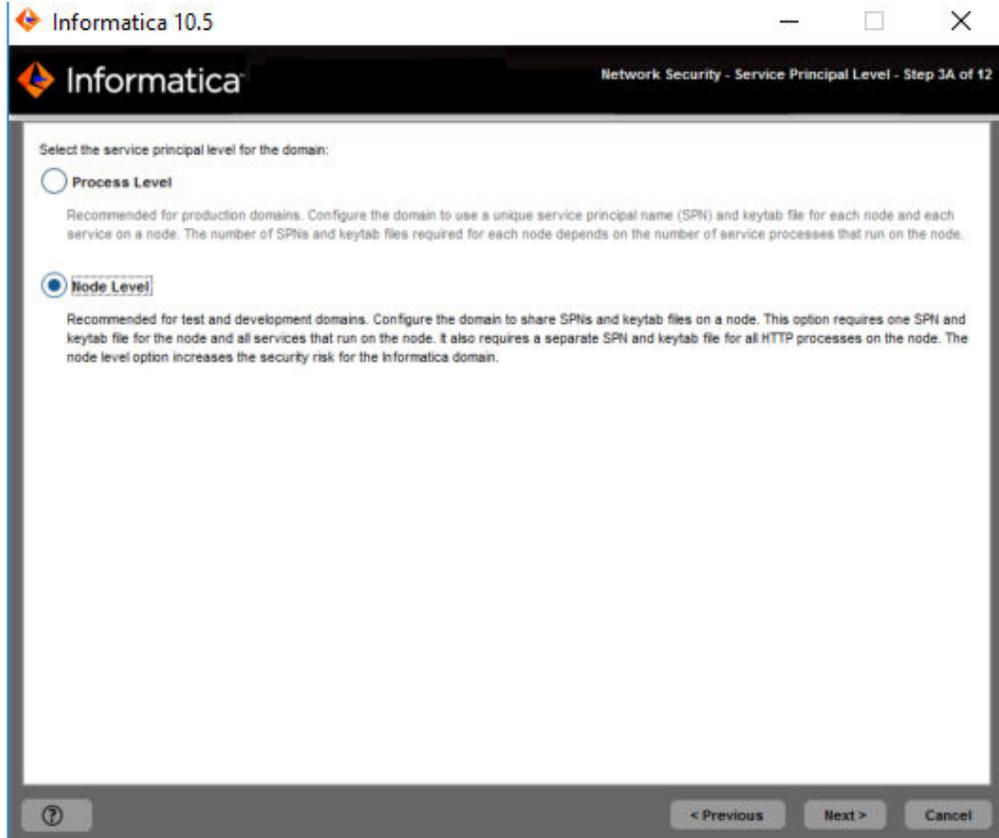
If you enabled Kerberos network authentication, the **Service Principal Level** section appears.

If you did not enable Kerberos network authentication, the **Pre-Installation Summary** section appears. Review the installation information and press **Enter** to continue. Skip to [“도메인 선택” 페이지 114](#).

네트워크 보안 - 서비스 사용자 수준

설치 디렉터리를 지정한 후에는 보안 수준을 구성할 수 있습니다.

1. Kerberos 네트워크 인증을 활성화한 경우 **네트워크 보안 - 서비스 사용자 수준**이 나타납니다.



2. **네트워크 보안 - 서비스 사용자 수준** 페이지에서 도메인에 대한 Kerberos 서비스 사용자를 설정할 수준을 선택합니다.

다음 테이블에는 사용자가 선택할 수 있는 서비스 사용자 수준이 설명되어 있습니다.

수준	설명
프로세스 수준	<p>각 노드 및 노드의 각 응용 프로그램 서비스에 대해 고유한 SPN(서비스 사용자 이름) 및 키 탭 파일을 사용하도록 도메인을 구성합니다.</p> <p>각 노드에 필요한 SPN 및 키 탭 파일의 수는 노드에서 실행되는 응용 프로그램 서비스 프로세스의 수에 따라 달라집니다. 운영 도메인 같이 높은 보안 수준이 필요한 도메인에 대해 프로세스 수준 옵션을 사용하십시오.</p>
노드 수준	<p>노드에서 SPN 및 키 탭 파일을 공유하도록 도메인을 구성합니다.</p> <p>이 옵션에는 노드에 대한 하나의 SPN과 키 탭 파일 및 노드에서 실행되는 모든 응용 프로그램 서비스가 필요합니다. 또한 노드의 모든 HTTP 프로세스에 대해 별도의 SPN 및 키 탭 파일이 필요합니다.</p> <p>테스트 및 개발 도메인 같이 높은 보안 수준이 필요하지 않은 도메인에 대해 노드 수준 옵션을 사용하십시오.</p>

3. 다음을 클릭합니다.

네트워크 보안 - Kerberos 인증 섹션이 나타납니다.

네트워크 보안 - Kerberos 인증

보안 수준을 구성한 후에는 Kerberos 인증을 구성할 수 있습니다.

1. **네트워크 보안 - Kerberos 인증** 페이지에서 Kerberos 인증에 필요한 도메인 및 키 탭 정보를 입력합니다.

The screenshot shows the 'Network Security - Kerberos Authentication - Step 3B of 12' window in Informatica 10.5. The window title is 'Informatica 10.5'. The main content area is titled 'Specify the Kerberos network authentication parameters.' and contains the following fields:

- Domain name:
- Node name:
- Node host name:
- Service realm name:
- User realm name:
- Keytab directory: ...
- Fully qualified path to the Kerberos configuration file: ...

At the bottom of the window, there are three buttons: '< Previous', 'Next >', and 'Cancel'. A help icon (?) is also visible in the bottom left corner.

다음 테이블에는 사용자가 입력해야 하는 Informatica 도메인 및 노드 정보가 설명되어 있습니다.

속성	설명
도메인 이름	작성할 도메인의 이름입니다. The name must not exceed 128 characters and must be 7-bit ASCII only. The name cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
노드 이름	Name of the node to create.
노드 호스트 이름	노드를 생성할 시스템의 정규화된 호스트 이름 또는 IP 주소입니다. 참고: The node host name cannot contain the underscore (_) character. Do not use localhost. The host name must explicitly identify the machine.

The following table describes the Kerberos realm and keytab information that you must provide:

Property	Description
Service realm name	Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example: *EAST.COMPANY.COM
User realm name	Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example: *EAST.COMPANY.COM
Keytab directory	Directory where all keytab files for the Informatica domain are stored. The name of a keytab file in the Informatica domain must follow a format set by Informatica.
Kerberos configuration file	Path and file name of the Kerberos configuration file. Informatica requires the following name for the Kerberos configuration file: <i>krb5.conf</i>

중요: Kerberos 인증으로 실행되도록 도메인을 구성하는 경우, 도메인과 노드 이름 및 노드 호스트 이름이 사용자가 Informatica Kerberos SPN 형식 생성기를 실행하여 SPN 및 키 탭 파일 이름을 생성했을 때 지정한 이름과 일치해야 합니다. 다른 도메인, 노드 또는 호스트 이름을 사용하는 경우, SPN 및 키 탭 파일 이름을 다시 생성하고 Kerberos 관리자에게 새로운 SPN을 Kerberos 사용자 데이터베이스에 추가하고 키 탭 파일을 생성하도록 요청하십시오.

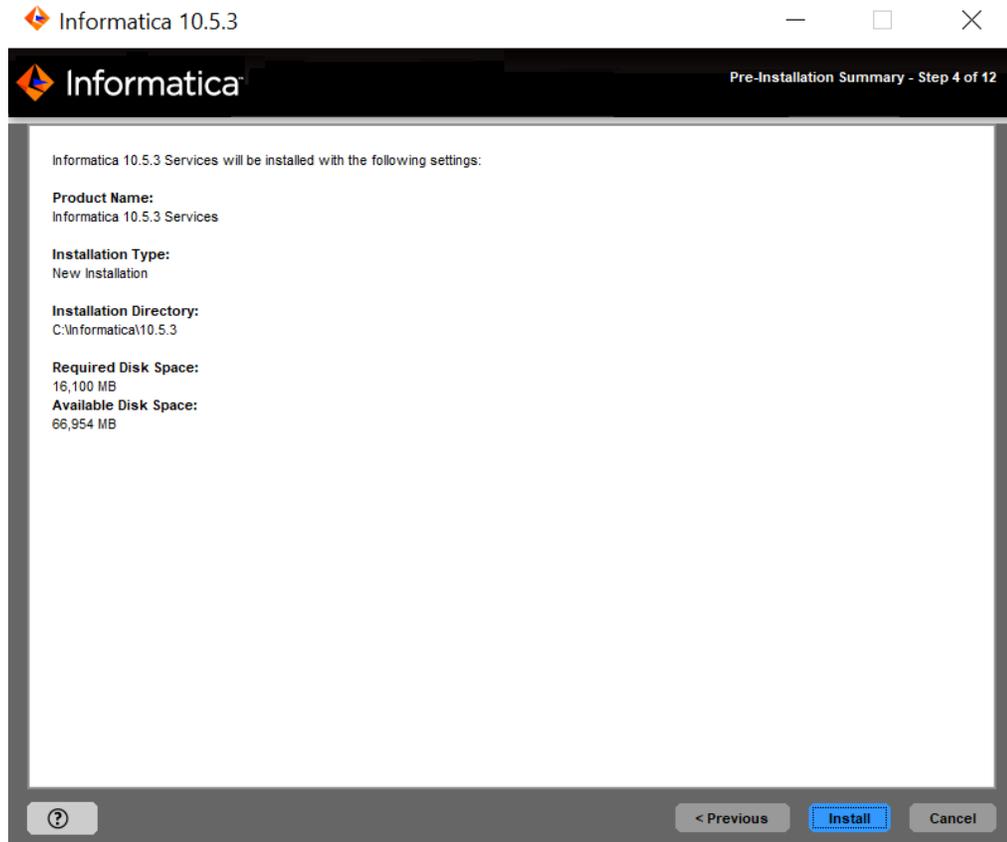
2. 다음을 클릭합니다.

사전 설치 요약 섹션이 나타납니다. 설치 정보를 검토합니다.

도메인 선택

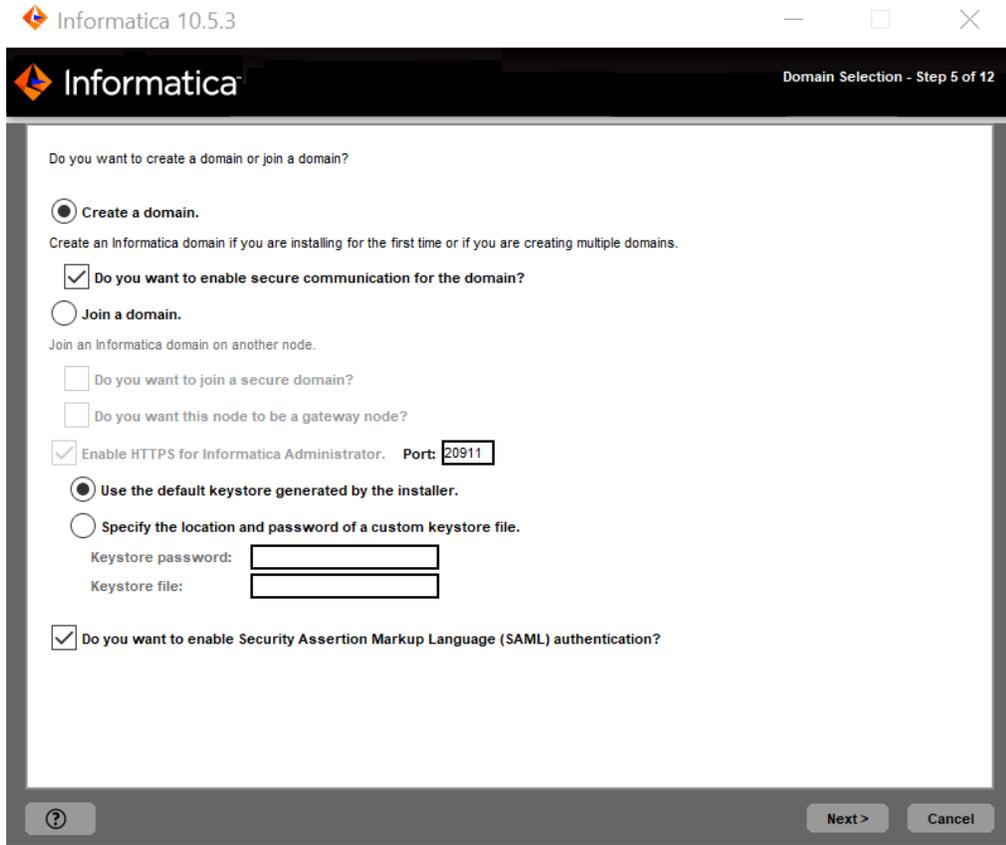
설치 전 요약 검토한 후에는 도메인 정보를 입력할 수 있습니다.

1. 설치 전 요약 페이지를 검토합니다.



2. 설치 정보를 검토하고 설치를 클릭하여 계속 진행합니다.

설치 프로그램이 설치 디렉터리로 Informatica 파일을 복사합니다. 설치 프로그램이 파일을 복사한 후 **도메인 선택** 페이지가 나타납니다.



3. **도메인 작성**을 선택합니다.

도메인을 생성하면, 생성하는 노드가 도메인의 게이트웨이 노드가 됩니다. 게이트웨이 노드에는 모든 도메인 작업을 관리하는 서비스 관리자가 포함됩니다.

4. 도메인의 서비스 간에 보안 통신을 활성화하려면 **확인란**을 선택합니다.

기본적으로, 도메인에 대한 보안 통신을 활성화하는 경우 설치 프로그램이 **Informatica Administrator**에 대한 **HTTPS** 연결을 설정합니다. 또한 보안 데이터베이스에서 도메인 구성 리포지토리를 생성할 수 있습니다.

5. **Informatica Administrator**에 대한 연결을 보호하려면 **Informatica Administrator**에 **HTTPS** 사용을 선택합니다.

The following table describes the properties that you set for a secure connection to the Administrator tool:

Property	Description
Enable HTTPS for Informatica Administrator	Select this option to secure the connection to Informatica Administrator. To use an unsecure HTTP connection, clear the option. By default, if secure communication is enabled for the domain, the installer enables this option. You can also enable this option even if you do not enable secure communication for the domain.
Port	The port to use for communication between Informatica Administrator and the Service Manager.
Use a keystore file generated by the installer	Use a self-signed keystore file generated by the installer. The installer creates a keystore file named Default.keystore in the following location: <Informatica installation directory>\tomcat\conf\
Specify a keystore file and password	Use a keystore file that you create. You can use a keystore file with a self-signed certificate or a certificate signed by a certification authority.
Keystore password	A plain-text password for the keystore file. Required if you use a keystore file that you create.
Keystore file	Path and file name of the keystore file. Required if you use a keystore file that you create.

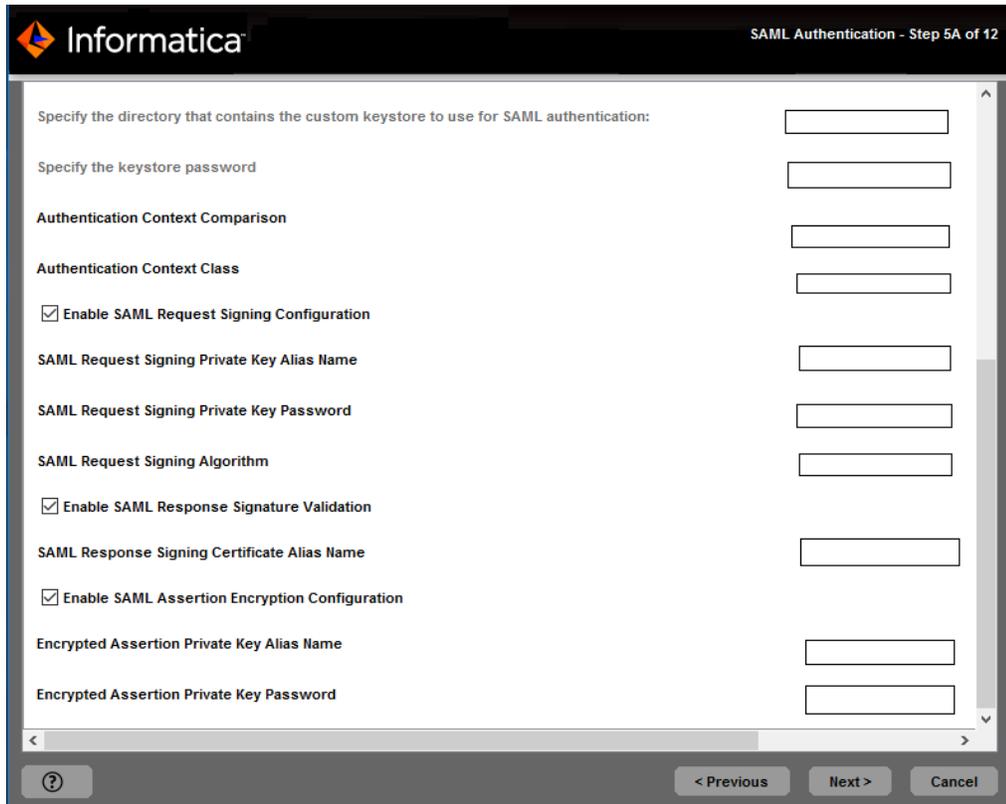
6. Informatica 도메인에서 웹 기반 Informatica 응용 프로그램에 대해 SAML(Security Assertion Markup Language) 기반 SSO(Single Sign-On) 지원을 구성하려면 SAML 인증을 활성화하는 확인란을 선택합니다.
참고: Kerberos 네트워크 인증을 활성화하는 경우 SAML 인증을 구성할 수 없습니다.
7. 다음을 클릭합니다.

SAML 인증 옵션을 활성화하는 확인란을 선택하면 **SAML 인증** 페이지가 나타납니다.

The screenshot shows a configuration window titled "Informatica 10.5.3" with a subtitle "SAML Authentication - Step 5A of 12". The window contains the following configuration options:

- Identity Provider URL**
 - Do you want to enter a relying party trust name or a service provider identifier? If you choose No, the service provider identifier will be used.
- Service Provider ID**
 - Enable SAML Assertion Signature Validation
- SAML Assertion Signing Certificate Alias Name**
 - Select the truststore for SAML authentication where you imported the identity provider assertion signing certificate
 - Use the default Informatica truststore and keystore.
 - Use a custom truststore and keystore.
 - Specify the directory that contains the custom truststore to use for SAML authentication:
 - Specify the truststore password
 - Specify the directory that contains the custom keystore to use for SAML authentication:
 - Specify the keystore password

At the bottom of the window, there are navigation buttons: a help icon (?), "< Previous", "Next >", and "Cancel".



8. 도메인의 ID 공급자 URL을 입력합니다.
9. ID 공급자에 정의된 도메인의 신뢰 당사자 트러스트 이름 또는 서비스 공급자 식별자를 지정하십시오. 아니요를 선택하는 경우 서비스 공급자 식별자가 "Informatica"로 설정됩니다.
10. IdP에서 SAML 어설션을 서명할지 여부를 지정합니다.
11. ID 공급자 어설션 서명 인증서 별칭 이름을 입력합니다.
12. 도메인에서 보안 통신을 활성화하는 데 기본 Informatica SSL 인증서를 사용할지 사용자의 SSL 사용할지 여부를 지정합니다.

다음 테이블에는 SAML 인증에 대한 SSL 인증서 옵션이 설명되어 있습니다.

옵션	설명
기본 Informatica SSL 인증서 파일을 사용합니다.	SAML 인증을 위한 기본 Informatica 트러스트 저장소 파일을 사용하려면 선택합니다.
SSL 인증서 파일의 위치를 입력하십시오.	SAML 인증을 위한 사용자 지정 트러스트 저장소 파일을 사용하려면 선택합니다. 도메인 내의 게이트웨이 노드에 대한 사용자 지정 트러스트 저장소 파일이 포함된 디렉터리를 지정하십시오. 파일에 대한 전체 경로가 아닌 디렉터리만 지정하십시오.

13. 사용자가 보안 인증서를 제공하는 경우 키 저장소 및 트러스트 저장소 파일의 위치와 암호를 지정합니다.

다음 테이블에는 트러스트 저장소 및 키 저장소 파일의 위치와 암호가 설명되어 있습니다.

속성	설명
트러스트 저장소 디렉터리	도메인 내의 게이트웨이 노드에 대한 사용자 지정 트러스트 저장소 파일이 포함된 디렉터리를 지정하십시오. 파일에 대한 전체 경로가 아닌 디렉터리만 지정하십시오.
트러스트 저장소 암호	사용자 지정 트러스트 저장소 파일에 대한 암호입니다.
키 저장소 디렉터리	사용자 지정 키 저장소 파일이 포함된 디렉터리를 지정합니다.
키 저장소 암호	사용자 지정 키 저장소 파일에 대한 암호입니다.

14. 인증 컨텍스트 비교를 지정하려면 IdP 서버와 사용자가 사용하는 인증 메커니즘의 비교 강도를 지정합니다. 지원되는 값은 **MINIMUM**, **MAXIMUM**, **BETTER** 또는 **EXACT** 옵션입니다. 기본값은 **MINIMUM**입니다.
15. 인증 컨텍스트 클래스를 설정하려면 IdP 서버를 사용하는 사용자에게 예상되는 최초 인증 메커니즘을 지정합니다. 지원되는 값은 **PASSWORD** 또는 **PASSWORDPROTECTEDTRANSPORT**입니다. 기본값은 **PASSWORD**입니다.
16. 웹 응용 프로그램이 SAML 인증 요청에 서명하도록 활성화할지 여부를 지정하시겠습니까? 기본값은 비활성화됨입니다.
17. SAML 요청에 서명하는 데 사용하는 노드 SAML 키 저장소로 가져온 개인 키의 별칭 이름을 지정하십시오.
18. SAML 요청 서명에 사용된 개인 키 액세스를 위한 암호를 지정합니다.
19. 웹 응용 프로그램이 SAML 요청을 서명하는 데 사용하는 알고리즘을 지정하십시오. 지원되는 값은 **RSA_SHA256**, **DSA_SHA1**, **DSA_SHA256**, **RSA_SHA1**, **RSA_SHA224**, **RSA_SHA384**, **RSA_SHA512**, **ECDSA_SHA1**, **ECDSA_SHA224**, **ECDSA_SHA256**, **ECDSA_SHA384**, **ECDSA_SHA512**, **RIPEMD160** 또는 **RSA_MD5**입니다.
20. IdP가 SAML 응답에 서명하도록 할지 여부를 지정하시겠습니까? 웹 응용 프로그램을 활성화하여 서명된 SAML 응답을 수신할지 여부를 선택하십시오. 기본값은 비활성화됨입니다.
21. IdP에서 SAML 어설션을 암호화할지 여부를 지정하십시오. 웹 응용 프로그램을 활성화하여 암호화된 SAML 어설션을 수신할지 여부를 선택하십시오. 기본값은 활성화됨입니다.
22. Informatica가 SAML 어설션을 암호 해독하는 데 사용하는 게이트웨이 노드 SAML 트러스트 저장소에 있는 개인 키의 별칭 이름을 지정하십시오.
23. 어설션 암호화 키를 암호 해독할 때 사용하는 개인 키 액세스를 위한 암호를 제공하십시오.
24. 다음을 클릭합니다.
도메인에 대한 보안 통신을 활성화하지 않은 경우 **도메인 구성 리포지토리** 페이지가 나타납니다. 도메인 구성 리포지토리 페이지를 설명하는 단계로 건너뛩니다. 도메인에 대한 보안 통신을 활성화하는 확인란을 선택한 경우 **도메인 보안 - 보안 통신** 페이지가 나타납니다.

도메인 보안 - 보안 통신

도메인을 구성한 후에는 도메인 보안을 구성할 수 있습니다.

1. **도메인 보안 - 보안 통신** 페이지에서 기본 Informatica SSL 인증서를 사용하거나 사용자의 SSL 인증서를 사용하여 도메인에서 보안 통신을 활성화할지 여부를 지정합니다.

Informatica 10.5.3

Informatica Domain Security - Secure Communication - Step 5B of 12

Select the SSL certificates to enable secure communication within the domain:

Use the default Informatica SSL certificates contained in the default keystore and truststore.

Use custom SSL certificates. Specify the path, file name, and passwords for the keystore and truststore files that contain the c

Keystore file directory: c:\temp

Keystore password:

Truststore file directory: c:\temp

Truststore password:

< Previous Next > Cancel

The following table describes the SSL certificate options for securing the Informatica domain:

Option	Description
Use the default Informatica SSL certificates	<p>Use the default SSL certificates provided by Informatica.</p> <p>참고: If you do not provide an SSL certificate, Informatica uses the same default private key for all Informatica installations. If you use the default Informatica keystore and truststore files, the security of your domain could be compromised. To ensure a high level of security for the domain, select the option to specify the location of the SSL certificate files.</p>
Use custom SSL certificates	<p>Specify the path of the keystore and truststore files that contain the SSL certificates.</p> <p>You can provide a self-signed certificate or a certificate issued by a certificate authority (CA). You must provide SSL certificates in PEM format and in Java Keystore (JKS) files.</p> <p>Informatica requires specific names for the SSL certificate files for the Informatica domain. You must use the same SSL certificates for all nodes in the domain.</p> <p>Store the truststore and keystore files in a directory accessible to all the nodes in the domain and specify the same keystore file directory and truststore file directory for all nodes in the same domain.</p> <p>To set the private truststore files, you must manually import the certificates. Run the keytool command in the <INFA_JDK_HOME> directory to import the private truststore certificates. For example, use the following keytool command:</p> <pre>keytool -noprompt -importkeystore -srckeystore <source truststore file path> -srcstorepass <source truststore file password> -srcalias <alias> -srcstoretype JKS -destkeystore <destination truststore file path> -deststorepass <destination truststore file password> -keypass <private key password> -deststoretype JKS</pre>

2. 사용자가 보안 인증서를 제공하는 경우 키 저장소 및 트러스트 저장소 파일의 위치와 암호를 지정합니다.

The following table describes the parameters that you must enter for the SSL certificate files:

Property	Description
Keystore file directory	Directory that contains the keystore files. The directory must contain files named infa_keystore.jks and infa_keystore.pem.
Keystore password	Password for the keystore infa_keystore.jks.
Truststore file directory	Directory that contains the truststore files. The directory must contain files named infa_truststore.jks and infa_truststore.pem.
Truststore password	Password for the infa_truststore.jks file.

3. 다음을 클릭합니다.

도메인 구성 리포트토리 페이지가 나타납니다.

도메인 구성 리포지토리

도메인 보안을 구성한 후에는 도메인 리포지토리 세부 정보를 구성할 수 있습니다.

1. **도메인 구성 리포지토리** 페이지에서 도메인 구성 리포지토리에 대한 데이터베이스 및 사용자 계정 정보를 입력합니다.

도메인 구성 리포지토리는 도메인 작업 및 사용자 인증에 대한 메타데이터를 저장합니다. 데이터베이스는 도메인의 모든 게이트웨이 노드에서 액세스할 수 있어야 합니다.

The following table describes the properties that you specify for the database and user account:

Property	Description
Database type	Database for the repository. Select one of the following databases: - Oracle - IBM DB2 - Microsoft SQL Server - PostgreSQL - Sybase ASE
Database user ID	User account for the repository database.
User password	Password for the database user account.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

If you select Microsoft SQL Server or PostgreSQL, specify the schema for the repository tables and database connection:

Property	Description
Schema name	Name of the schema that will contain the repository tables. If not selected, the installer creates the tables in the default schema.
Trusted connection	Indicates whether to connect to Microsoft SQL Server through a trusted connection. Trusted authentication uses the security credentials of the current user to make the connection to Microsoft SQL Server. If not selected, the installer uses Microsoft SQL Server authentication.

도메인에 대해 보안 통신을 활성화한 경우, SSL 프로토콜로 보호되는 데이터베이스에서 도메인 구성 리포지토리를 작성할 수 있습니다. 데이터베이스를 보호하고 3단계로 건너뛰려면 확인란을 선택합니다..

참고: Sybase 데이터베이스에 대한 보안 연결은 구성할 수 없습니다.

2. 데이터베이스 연결 정보를 입력합니다.

보안 도메인 구성 리포지토리를 작성하지 않은 경우 JDBC URL에 대한 연결 속성을 지정하거나 JDBC 연결 문자열을 제공할 수 있습니다.

- JDBC URL을 사용하여 연결 정보를 입력하려면 **JDBC URL**을 선택하고 데이터베이스 연결 속성을 지정합니다.

The following table describes the JDBC URL properties that you specify:

Property	Description
Database address	Host name and port number for the database in the format host_name:port .
Database service name	Service or database name: - Oracle: Enter the service name. - Microsoft SQL Server: Enter the database name. - IBM DB2: Enter the service name. - Sybase ASE: Enter the database name. - PostgreSQL: Enter the database name.
JDBC parameters	Optional parameters to include in the database connection string. Use the parameters to optimize database operations for the database. Verify that the parameter string is valid. The installer does not validate the parameter string before it adds the string to the JDBC URL. If not selected, the installer creates the JDBC URL string without additional parameters.

- 사용자 지정 JDBC 연결 문자열을 사용하여 연결하려면 **사용자 지정 JDBC 연결 문자열**을 선택하고 연결 문자열을 입력합니다.
3. 데이터베이스를 보호하도록 선택한 경우 사용자 지정 JDBC 연결 문자열을 사용하여 연결 정보를 입력합니다.

보안 데이터베이스에 리포지토리를 생성하는 경우 데이터베이스에 대한 트러스트 저장소 정보를 제공해야 합니다. 데이터베이스에 대한 보안 매개 변수가 포함된 JDBC 연결 문자열도 제공해야 합니다.

The following table describes the properties you must set for a secure database:

Property	Description
Database truststore file	Path and file name of the truststore file for the secure database.
Database truststore password	Password for the truststore file.
Custom JDBC Connection String	JDBC connection string to connect to the secure database, including the host name and port number and the security parameters for the database.

보안 데이터베이스의 JDBC 연결에 포함해야 하는 보안 매개 변수에 대한 자세한 내용은 [“보안 데이터베이스에 대한 연결 문자열” 페이지 94](#)을 참조하십시오.

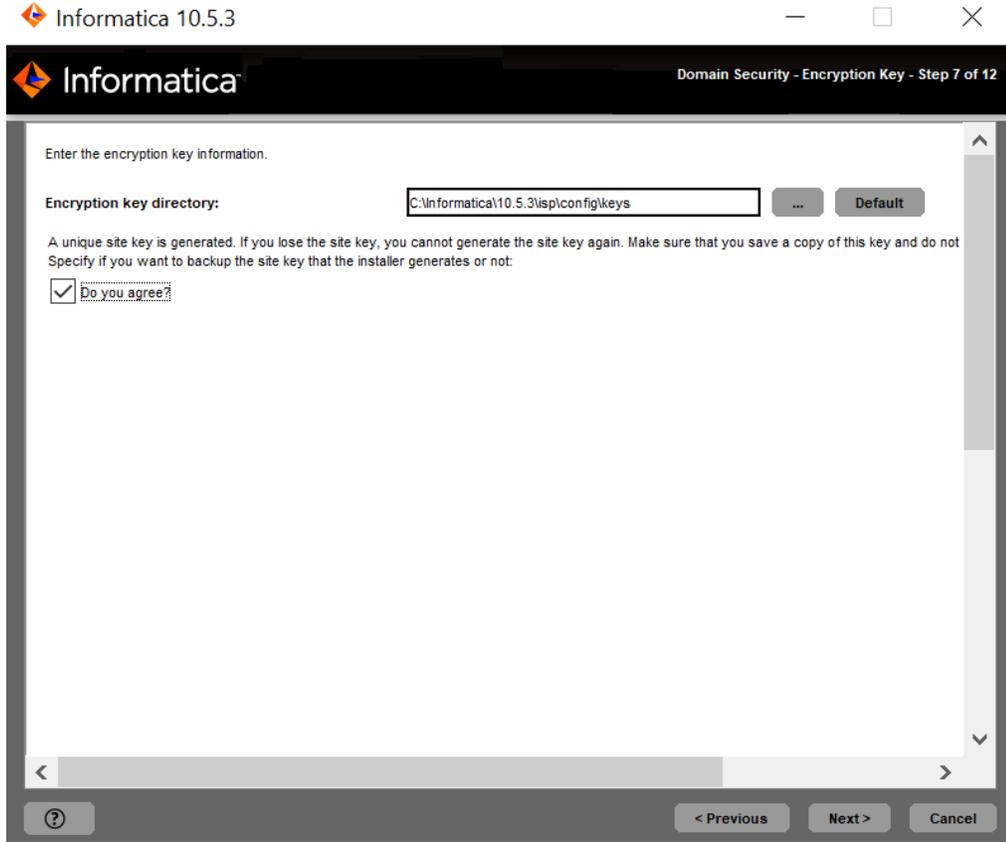
4. **연결 테스트**를 클릭하여 데이터베이스에 연결할 수 있는지 확인한 다음 **확인**을 클릭하여 계속 진행합니다.
5. **다음**을 클릭합니다.

도메인 보안 - 암호화 키 섹션이 나타납니다.

도메인 보안 - 암호화 키

도메인 리포지토리를 구성한 후에는 암호화 키를 구성할 수 있습니다.

1. **도메인 보안 - 암호화 키** 섹션에서 도메인을 생성할 때 지정해야 하는 암호화 키 매개 변수를 입력합니다.



다음 테이블에는 도메인을 생성할 때 지정해야 하는 암호화 키 매개 변수가 설명되어 있습니다.

속성	설명
암호화 키 디렉터리	도메인에 대한 암호화 키가 저장되는 디렉터리입니다. 기본적으로 암호화 키는 다음 디렉터리에 생성됩니다. <Informatica 설치 디렉터리>/isp/config/keys.
설치 프로그램에서 생성되는 사이트 키를 백업할지 여부를 지정하십시오.	고유한 사이트 키가 생성됩니다. 사이트 키를 분실하는 경우 사이트 키를 다시 생성할 수 없습니다. 이 키의 사본을 반드시 저장하고 고유한 사이트 키를 다른 사람과 공유하지 마십시오. 설치 프로그램에서 생성되는 사이트 키를 백업할지 여부를 지정하십시오. - [아니요]인 경우 1을 선택합니다. [아니요]를 선택하는 경우 설치 프로그램이 종료됩니다. - [예]인 경우 2를 선택합니다. [예]를 선택하는 경우 파일을 수동으로 백업하는데 동의하는 것입니다.

설치 프로그램이 디렉터리 및 해당 디렉터리의 파일에 대해 서로 다른 사용 권한을 설정합니다. 암호화 키 파일 및 디렉터리의 사용 권한에 대한 자세한 내용은 [“보안 파일 및 디렉터리” 페이지 98](#)를 참조하십시오.

2. 다음을 클릭합니다.

도메인 및 노드 구성 섹션이 나타납니다.

도메인 및 노드 구성

암호화 키를 구성한 후에는 도메인 및 노드를 구성할 수 있습니다.

1. 생성할 도메인 및 노드에 대한 정보를 입력합니다.

다음 테이블에는 사용자가 도메인 및 게이트웨이 노드에 대해 설정하는 속성이 설명되어 있습니다.

속성	설명
도메인 이름	<p>생성할 Informatica 도메인의 이름입니다. 기본 도메인 이름은 Domain_<MachineName>입니다.</p> <p>이름은 128자를 초과하지 않아야 하고 7비트 ASCII여야만 합니다. 이름에는 공백이나 다음과 같은 문자를 사용할 수 없습니다. ` % * + ; " ? , < > \ /</p>
노드 이름	<p>생성할 노드의 이름입니다.</p>
노드 호스트 이름	<p>노드를 생성할 시스템의 호스트 이름 또는 IP 주소입니다.</p> <p>시스템이 단일 네트워크 이름을 갖는 경우 기본 호스트 이름을 사용하십시오. 시스템이 여러 네트워크 이름을 갖는 경우 대체 네트워크 이름을 사용하도록 기본 호스트 이름을 수정할 수 있습니다.</p> <p>참고: 노드 호스트 이름에는 밑줄(_) 문자를 사용할 수 없습니다. localhost는 사용하지 마십시오. 호스트 이름은 명시적으로 시스템을 식별해야 합니다.</p>

속성	설명
노드 포트 번호	노드의 포트 번호입니다. 노드의 기본 포트 번호는 6005입니다. 시스템에서 해당 포트 번호를 사용할 수 없는 경우 사용 가능한 다음 포트 번호가 설치 프로그램에 표시됩니다.
도메인 사용자 이름	도메인 관리자의 사용자 이름입니다. 처음에 Informatica Administrator에 로그인할 때 이 사용자 이름을 사용할 수 있습니다. 다음 지침을 사용하십시오. <ul style="list-style-type: none"> - 이름은 대/소문자를 구분하지 않으며 128자를 초과할 수 없습니다. - 이름에는 탭, 줄 바꿈 문자 또는 다음과 같은 특수 문자를 사용할 수 없습니다. % * + / ? ; < > - 첫 번째 문자와 마지막 문자를 제외하고 이름에는 ASCII 공백 문자를 사용할 수 있습니다. 다른 공백 문자는 사용할 수 없습니다.

The following table describes the password complexity:

Prompt	Description
Password complexity	Select whether you want to enable password complexity. If you select Yes, the password must meet the following requirements: It must be at least eight characters long and contain at least one alphabetic character, one numeric character, and one special character.
Configure password policy	Select whether you want to configure a password policy. If you select Yes, you can configure password complexity rules. If you select No, the default Informatica password policy rules apply.
Number of special characters	The minimum number of special characters required in a password. You can use the following special characters: [! " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { } ~] You can enter a value between 0 and 255. Default is 1.
Number of alphabetic characters	The minimum number of alphabetic characters required in a password. You can enter a value between 0 and 255. Default is 1.
Number of numeric characters	The minimum number of numeric characters required in a password. You can enter a value between 0 and 255. Default is 1.
Minimum password length	The minimum number of characters required in a password. You can enter a value between 8 and 255. Default is 8.
Number of previous passwords to store	The number of consecutive previous passwords that can't be reused. You can enter a value between 0 and 12. Default is 0.
Password expiration in days	The duration of the validity of a password. If you don't want passwords to expire, set the value to 0. Default is 0.

Prompt	Description
Domain password	Password for the domain administrator. - If you don't enable password complexity, the password must be between 2 and 16 characters. - If you enable password complexity, the password must be at least eight characters long and contain at least one alphabetic character, one numeric character, and one special character. - If you configure a password policy, the password must meet the complexity rules that you set. Not available if you configure the Informatica domain to run on a network with Kerberos authentication.
Confirm password	Enter the password again to confirm. Not available if you configure the Informatica domain to run on a network with Kerberos authentication.

2. 설치 프로그램에 의해 할당된 도메인 및 노드 구성 요소에 대한 기본 포트 번호를 표시하려면 **고급 포트 구성 페이지 표시**를 활성화합니다.

 포트 구성 페이지를 표시하면 설치 프로그램이 도메인 및 노드에 할당된 기본 포트 번호를 표시합니다. 포트 번호를 수정하거나 응용 프로그램 서비스 프로세스에 대해 다른 포트 번호 범위를 지정할 수 있습니다. 포트 구성 페이지 표시를 선택하지 않으면 설치 프로그램에 기본 포트 번호가 표시되지 않으며 할당된 포트 번호를 수정할 수 없습니다.
3. 설치 중에 모델 리포지토리 서비스와 데이터 통합 서비스를 생성하는 확인란을 선택합니다.

 서비스를 구성하지 않는 경우 설치 프로그램이 모델 리포지토리 서비스 또는 데이터 통합 서비스를 새 도메인에 작성하지 않습니다. 설치 후에 **Administrator** 도구에서 서비스를 작성할 수 있습니다.

 서비스를 구성하도록 선택한 경우 설치 프로그램이 모델 리포지토리 서비스와 데이터 통합 서비스를 새 도메인에 작성합니다. 모델 리포지토리에 대한 데이터베이스를 지정하고 데이터 통합 서비스에 대한 연결을 구성해야 합니다. 기본적으로 설치가 완료되면 서비스가 시작됩니다.
4. 설치 중에 도메인 통계를 모니터링할 모니터링 모델 리포지토리 서비스를 생성할지 여부를 선택합니다.
5. 설치 중에 데이터 도메인 검색을 위한 콘텐츠 관리 서비스를 생성할지 여부를 선택합니다.
6. 설치 중에 프로파일링 웨어하우스 연결을 구성할지 여부를 선택합니다.
7. 설치 중에 **PowerCenter** 리포지토리 서비스와 **PowerCenter** 통합 서비스를 생성할지 여부를 선택합니다.

 포트 구성 페이지를 표시하도록 선택한 경우 **포트 구성** 페이지가 나타납니다.

 포트 구성 페이지를 표시하도록 선택하지 않은 경우 설치 프로그램이 **Windows 서비스 구성** 페이지를 표시합니다.

포트 구성

서비스 관리자 및 Informatica Administrator의 포트 번호를 업데이트할 수 있습니다.

1. 포트 구성 페이지를 표시하도록 선택한 경우 **포트 구성** 페이지가 나타납니다.

Informatica 10.5 Port Configuration - Step 8A of 12

Enter the port numbers for the Service Manager and Informatica Administrator.

Service Manager port: 20106

Service Manager shutdown port: 20107

Informatica Administrator port: 20108

Informatica Administrator shutdown port: 20109

Enter a range of port numbers for service processes in the node.

Minimum port number: 20114

Maximum port number: 20214

Default

< Previous Next > Cancel

2. **포트 구성** 페이지에서 노드에서 실행할 도메인 서비스 관리자 및 서비스 프로세스에 사용할 포트 번호를 입력합니다.

입력하는 포트 번호가 다른 응용 프로그램에서 사용되지 않는지 확인합니다.

The following table describes the ports that you can set:

Port	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.

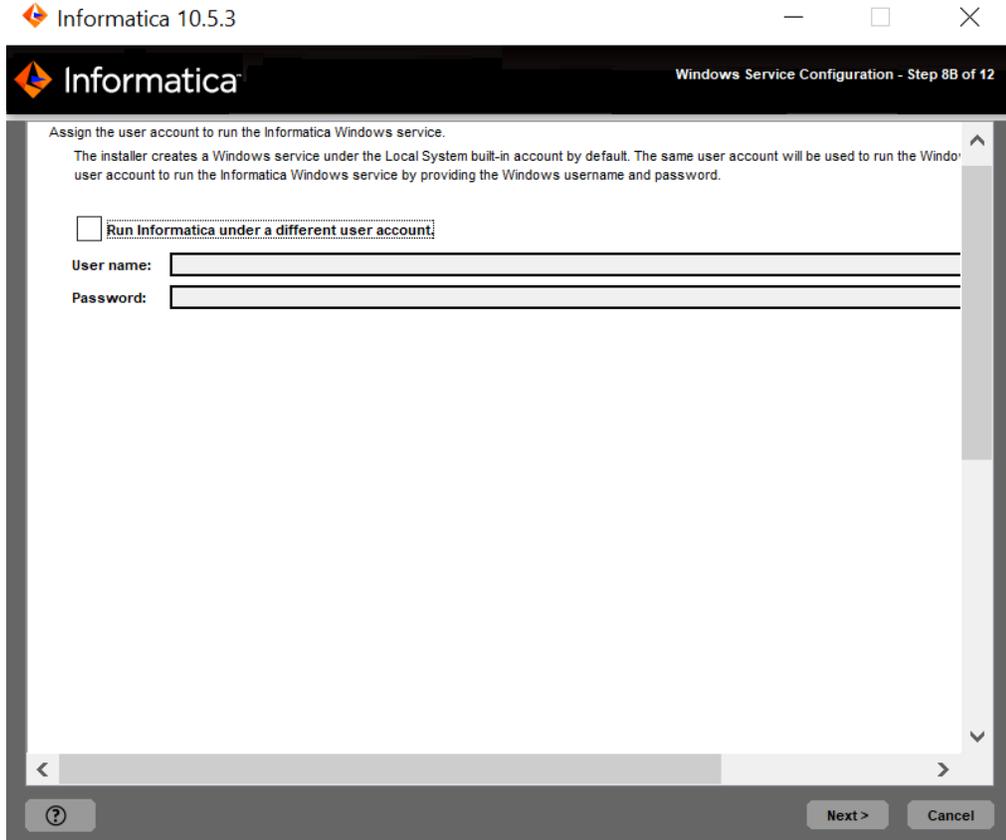
Port	Description
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.

3. 다음을 클릭합니다.

Windows 서비스 구성 페이지가 나타납니다.

Windows 서비스 구성

1. 포트 구성 페이지를 표시하도록 선택하지 않은 경우 설치 프로그램이 **Windows 서비스 구성** 페이지를 표시합니다.



2. **Windows 서비스 구성** 페이지에서 Windows 서비스를 다른 사용자 계정으로 실행할지 여부를 선택합니다. 설치 프로그램이 Informatica를 시작하기 위한 서비스를 생성합니다. 기본적으로 해당 서비스는 설치에 사용된 계정과 동일한 사용자 계정으로 실행됩니다. 다른 사용자 계정으로 Windows 서비스를 실행할 수도 있습니다.

The following table describes the properties that you set to run Informatica under a different account:

Property	Description
Run Informatica under a different user account	Indicates whether to run the Windows service under a different user account.
User name	User account with which to run the Informatica Windows service. Use the following format: <domain name>\<user account> This user account must have the Act as operating system permission.
Password	Password for the user account with which to run the Informatica Windows service.

3. 다음을 클릭합니다.

서비스를 생성하도록 선택하지 않은 경우 설치 프로그램이 **설치 후 요약** 페이지를 표시합니다. **설치 후 요약** 페이지에 설치가 완료되었는지 여부가 나타납니다.

Informatica 응용 프로그램 서비스를 구성하도록 선택한 경우 설치 프로그램이 **모델 리포지토리 서비스 데이터베이스** 페이지를 표시합니다.

모델 리포지토리 서비스 데이터베이스 구성

도메인과 노드를 구성한 후에는 모델 리포지토리 데이터베이스 속성을 구성할 수 있습니다.

1. **모델 리포지토리 서비스 데이터베이스** 페이지에서 모델 리포지토리에 대한 데이터베이스 및 사용자 계정 정보를 입력합니다.

Informatica 10.5.3

Model Repository Database - Step 9A of 12

Model Repository Service name: _____

Enter database information for the Model repository:

Database type: _____

Database user ID: _____

Database user password: _____

Is the database secure?

Database connection

() Enter the JDBC URL.

Database address: `host_name:port_no`

Database service name: `ServiceName`

JDBC parameters:

`MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true`

(●) Enter the JDBC connection string.

Next > Cancel

다음 테이블에는 사용자가 데이터베이스 및 사용자 계정에 대해 지정하는 속성이 설명되어 있습니다.

속성	설명
데이터베이스 유형	리포지토리의 데이터베이스입니다. 다음 데이터베이스 중 하나를 선택합니다. - Oracle - IBM DB2 - Microsoft SQL Server - PostgreSQL
데이터베이스 사용자 ID	리포지토리 데이터베이스의 사용자 계정입니다.
사용자 암호	데이터베이스 사용자 계정의 암호입니다.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

If you select Microsoft SQL Server or PostgreSQL, specify the schema for the repository tables and database connection:

Property	Description
Schema name	Name of the schema that will contain the repository tables. If not selected, the installer creates the tables in the default schema.
Trusted connection	Indicates whether to connect to Microsoft SQL Server through a trusted connection. Trusted authentication uses the security credentials of the current user to make the connection to Microsoft SQL Server. If not selected, the installer uses Microsoft SQL Server authentication.

도메인에 대해 보안 통신을 활성화하는 경우 **SSL** 프로토콜로 보호되는 데이터베이스에서 모델 리포지토리를 생성할 수 있습니다. 보안 모델 리포지토리를 작성하려면 **3**단계로 건너뛩니다.

2. 데이터베이스 연결 정보를 입력합니다.

보안 모델 리포지토리를 작성하지 않은 경우 **JDBC URL**에 대한 연결 속성을 지정하거나 **JDBC** 연결 문자열을 제공할 수 있습니다.

- **JDBC URL**을 사용하여 연결 정보를 입력하려면 **JDBC URL**을 선택하고 데이터베이스 연결 속성을 지정합니다.

다음 표에는 사용자가 지정해야 하는 JDBC URL 속성이 설명되어 있습니다.

속성	설명
데이터베이스 주소	host_name:port 형식으로 된 데이터베이스의 호스트 이름 및 포트 번호입니다.
데이터베이스 서비스 이름	서비스 또는 데이터베이스 이름: - Oracle: 서비스 이름을 입력합니다. - Microsoft SQL Server: 데이터베이스 이름을 입력합니다. - IBM DB2: 서비스 이름을 입력합니다. - PostgreSQL: 데이터베이스 이름을 입력합니다.
JDBC 매개 변수	데이터베이스 연결 문자열에 포함할 매개 변수(선택 사항)입니다. 데이터베이스에 대한 데이터베이스 작업을 최적화하려면 매개 변수를 사용하십시오. 매개 변수 문자열이 유효하지 확인하십시오. 설치 프로그램은 JDBC URL에 문자열을 추가하기 전에 매개 변수 문자열의 유효성을 검사하지 않습니다. 선택하지 않으면 설치 프로그램이 추가 매개 변수 없이 JDBC URL 문자열을 생성합니다.

- 사용자 지정 JDBC 연결 문자열을 사용하여 연결 정보를 입력하려면 **사용자 지정 JDBC 연결 문자열**을 선택하고 연결 문자열을 입력합니다.

IBM DB2

```
jdbc:Informatica:db2://<호스트 이름>:<포트 번호>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<호스트 이름>:<포트 번호>;ServiceName=
```

Oracle Connection Manager를 통해 Oracle 데이터베이스에 연결하려면 다음 연결 문자열을 사용합니다.

```
jdbc:Informatica:oracle:TNSNamesFile=<tnsnames.ora 파일에 대한 정규화된 경로>;TNSServerName=<TNS 이름>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<호스트 이름>:<포트 번호>;SelectMethod=cursor;DatabaseName=
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

Active Directory 인증을 사용하는 Azure SQL Database

```
"jdbc:informatica: sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;LoginTimeout=<seconds>"
```

PostgreSQL

```
jdbc:Informatica:postgresql://<호스트 이름>:<포트 번호>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLsv1.2;
```

데이터베이스 시스템에 필요한 모든 연결 매개 변수가 연결 문자열에 포함되어 있는지 확인합니다.

3. 보안 모델 리포지토리를 생성할지 여부를 선택합니다.

보안 데이터베이스에 리포지토리를 생성하는 경우 데이터베이스에 대한 트러스트 저장소 정보를 제공해야 합니다. 데이터베이스에 대한 보안 매개 변수가 포함된 JDBC 연결 문자열도 제공해야 합니다.

The following table describes the properties you must set for a secure database:

Property	Description
Database truststore file	Path and file name of the truststore file for the secure database.
Database truststore password	Password for the truststore file.
Custom JDBC Connection String	JDBC connection string to connect to the secure database, including the host name and port number and the security parameters for the database.

보안 데이터베이스의 JDBC 연결에 포함해야 하는 보안 매개 변수에 대한 자세한 내용은 [“보안 데이터베이스에 대한 연결 문자열” 페이지 94](#)을 참조하십시오.

4. **연결 테스트**를 클릭하여 데이터베이스에 연결할 수 있는지 확인한 다음 **확인**을 클릭하여 계속 진행합니다.

5. **다음**을 클릭합니다.

서비스 매개 변수 섹션이 나타납니다.

모니터링 모델 리포지토리 서비스 데이터베이스 구성

모델 리포지토리 데이터베이스를 구성한 후에는 모니터링 모델 리포지토리 데이터베이스 속성을 구성할 수 있습니다.

1. 도메인 통계 모니터링을 위한 모니터링 모델 리포지토리 서비스를 생성하도록 선택한 경우 **모니터링을 위한 모델 리포지토리 데이터베이스** 페이지가 나타납니다.

The screenshot shows the 'Model Repository Database for monitoring - Step 9B of 12' configuration window in Informatica 10.5.3. The window contains the following fields and options:

- monitoring Model Repository Service name: [Text Field]
- Enter database information for the monitoring Model repository:
- Database type: [Text Field]
- Database user ID: [Text Field]
- Database user password: [Text Field]
- Is the database secure?
- Database connection:
 - Enter the JDBC URL.
 - Database address: [Text Field with placeholder 'host_name:port_no']
 - Database service name: [Text Field with placeholder 'ServiceName']
 - Enter the JDBC connection string.
 - [Text Field]
- JDBC parameters:
 - JDBC parameters: [Text Field with placeholder 'MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true']

Navigation buttons at the bottom include a question mark icon, 'Next >', and 'Cancel'.

2. 모니터링을 위한 모델 리포지토리 데이터베이스 페이지에서 모니터링 모델 리포지토리에 대한 데이터베이스 및 사용자 계정 정보를 입력합니다.

속성	설명
데이터베이스 유형	리포지토리의 데이터베이스입니다. 다음 데이터베이스 중 하나를 선택합니다. - Oracle - IBM DB2 - Microsoft SQL Server - PostgreSQL
데이터베이스 사용자 ID	리포지토리 데이터베이스의 사용자 계정입니다. 신뢰할 수 있는 Microsoft SQL Server 연결을 위해 Windows NT 사용자 이름을 입력할 수 있습니다.
사용자 암호	데이터베이스 사용자 계정의 암호입니다. 신뢰할 수 있는 Microsoft SQL Server 연결을 위해 Windows NT 암호를 입력할 수 있습니다.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

If you select Microsoft SQL Server or PostgreSQL, specify the schema for the repository tables and database connection:

Property	Description
Schema name	Name of the schema that will contain the repository tables. If not selected, the installer creates the tables in the default schema.
Trusted connection	Indicates whether to connect to Microsoft SQL Server through a trusted connection. Trusted authentication uses the security credentials of the current user to make the connection to Microsoft SQL Server. If not selected, the installer uses Microsoft SQL Server authentication.

3. 데이터베이스 연결 정보를 입력합니다.

JDBC URL에 대한 연결 속성을 지정하거나 JDBC 연결 문자열을 제공할 수 있습니다.

- JDBC URL을 사용하여 연결 정보를 입력하려면 **JDBC URL**을 선택하고 데이터베이스 연결 속성을 지정합니다.
다음 표에는 사용자가 지정해야 하는 JDBC URL 속성이 설명되어 있습니다.

속성	설명
데이터베이스 주소	<호스트 이름>:<포트 번호> 형식으로 된 데이터베이스의 호스트 이름 및 포트 번호입니다.
데이터베이스 서비스 이름	서비스 또는 데이터베이스 이름: - Oracle: 서비스 이름을 입력합니다. - Microsoft SQL Server: 데이터베이스 이름을 입력합니다. - IBM DB2: 서비스 이름을 입력합니다. - PostgreSQL: 데이터베이스 이름을 입력합니다.
JDBC 매개 변수	데이터베이스 연결 문자열에 포함할 매개 변수(선택 사항)입니다. 데이터베이스에 대한 데이터베이스 작업을 최적화하려면 매개 변수를 사용하십시오. 매개 변수 문자열이 유효한지 확인하십시오. 설치 프로그램은 JDBC URL에 문자열을 추가하기 전에 매개 변수 문자열의 유효성을 검사하지 않습니다. 선택하지 않으면 설치 프로그램이 추가 매개 변수 없이 JDBC URL 문자열을 생성합니다.

- 사용자 지정 JDBC 연결 문자열을 사용하여 연결 정보를 입력하려면 **사용자 지정 JDBC 연결 문자열**을 선택하고 연결 문자열을 입력합니다.

4. **연결 테스트**를 클릭하여 데이터베이스에 연결할 수 있는지 확인한 다음 **확인**을 클릭하여 계속 진행합니다.
5. **다음**을 클릭합니다.

서비스 매개 변수 섹션이 나타납니다.

데이터 통합 서비스

모델 리포지토리 데이터베이스를 구성한 후에는 응용 프로그램 서비스에 대한 서비스 매개 변수를 구성할 수 있습니다.

1. 데이터 통합 서비스 페이지에서 데이터 통합 서비스 속성을 구성합니다.

The following table describes services parameters that you must set:

Port	Description
Data Integration Service name	Name of the Data Integration Service to create in the Informatica domain.
HTTP protocol type	Type of connection to the Data Integration Service. Select one of the following options: - HTTP. Requests to the service uses an HTTP connection. - HTTPS. Requests to the service uses a secure HTTP connection. - HTTP&HTTPS. Requests to the service can use either an HTTP or HTTPS connection.
HTTP port	Port number to used for the Data Integration Service. Default is 6030.

2. HTTPS 연결을 선택하는 경우 데이터 통합 서비스에 대한 연결의 보안에 기본 Informatica SSL 인증서를 사용할지 사용자의 SSL 인증서를 사용할지를 지정합니다.

다음 테이블에는 데이터 통합 서비스 보안을 위한 SSL 인증서 옵션이 설명되어 있습니다.

옵션	설명
기본 Informatica SSL 인증서 파일을 사용합니다.	Use the default SSL certificates provided by Informatica. 참고: If you do not provide an SSL certificate, Informatica uses the same default private key for all Informatica installations. If you use the default Informatica keystore and truststore files, the security of your domain could be compromised. To ensure a high level of security for the domain, select the option to specify the location of the SSL certificate files.
SSL 인증서 파일의 위치를 입력하십시오.	Specify the path of the keystore and truststore files that contain the SSL certificates.

사용자가 인증서를 제공하는 경우 키 저장소 및 트러스트 저장소 파일의 위치와 암호를 지정합니다.

The following table describes the parameters that you must enter for the SSL certificate files:

Property	Description
Keystore file	Required. Path and file name of the keystore file that contains the private keys and SSL certificates for the database.
Keystore password	Required. Password for the keystore file for the secure database.
Truststore file	Required. Path and file name of the truststore file that contains the public key for the database.
Truststore password	Required. Password for the truststore file for the secure database.

3. 다음을 클릭합니다.

설치 프로그램이 데이터 통합 서비스를 생성합니다.

콘텐츠 관리 서비스 매개 변수 및 데이터베이스

데이터 통합 서비스를 구성한 후에는 콘텐츠 관리 서비스에 대한 매개 변수를 구성할 수 있습니다.

1. 설치 중에 콘텐츠 관리 서비스를 생성하도록 선택한 경우 **콘텐츠 관리 서비스** 페이지가 나타납니다.

2. 콘텐츠 관리 서비스 매개 변수를 입력합니다.

다음 테이블에는 사용자가 설정해야 하는 서비스 매개 변수가 설명되어 있습니다.

포트	설명
콘텐츠 관리 서비스 이름	Informatica 도메인에 생성할 콘텐츠 관리 서비스의 이름입니다.
HTTP 프로토콜	콘텐츠 관리 서비스에 대한 연결 유형입니다. 다음 옵션 중 하나를 선택합니다. - HTTP. 서비스를 요청할 때 HTTP 연결을 사용합니다. - HTTPS. 서비스를 요청할 때 보안 HTTP 연결을 사용합니다.
HTTP 포트	콘텐츠 관리 서비스에 사용할 포트 번호입니다. 기본값은 8105입니다.

3. HTTPS 연결을 선택하는 경우 콘텐츠 관리 서비스에 대한 연결의 보안에 기본 Informatica SSL 인증서를 사용하지 않으면 사용자의 SSL 인증서를 사용할지를 지정합니다.

다음 테이블에는 콘텐츠 관리 서비스 보안을 위한 SSL 인증서 옵션이 설명되어 있습니다.

옵션	설명
기본 Informatica SSL 인증서 파일을 사용합니다.	Use the default SSL certificates provided by Informatica. 참고: SSL 인증서를 제공하지 않을 경우 Informatica에서는 모든 Informatica 설치에 동일한 기본 개인 키를 사용합니다. 기본 Informatica 키 저장소 파일을 사용하는 경우 도메인의 보안이 침해될 수 있습니다. 도메인의 보안 수준을 높이려면 SSL 인증서 파일의 위치를 지정하는 옵션을 선택하십시오.
SSL 인증서 파일의 위치를 입력하십시오.	사용자가 제공하는 SSL 인증서를 사용합니다. 키 저장소 파일의 위치를 지정해야 합니다.

사용자가 인증서를 제공하는 경우 키 저장소 파일의 위치와 암호를 지정합니다.

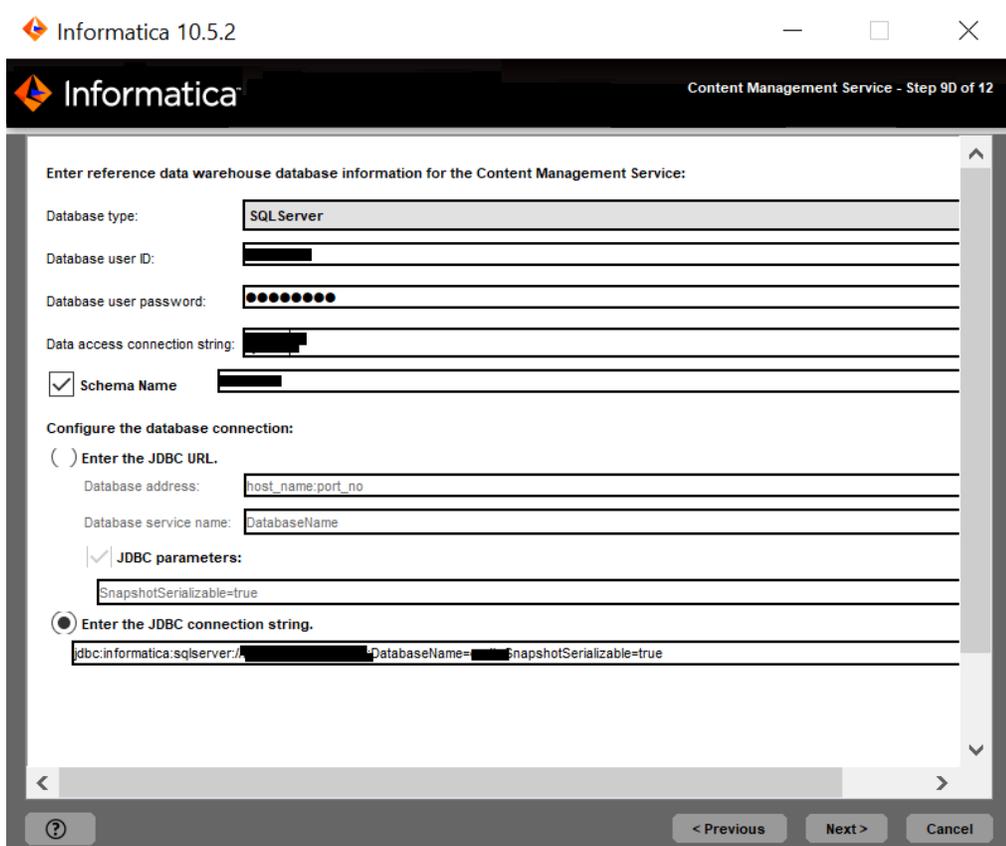
다음 테이블에는 SSL 인증서 파일에 대해 입력해야 하는 매개 변수가 설명되어 있습니다.

속성	설명
키 저장소 파일	필수 사항입니다. 데이터베이스의 개인 키 및 SSL 인증서를 포함하는 키 저장소 파일의 경로 및 파일 이름입니다.
키 저장소 암호	필수 사항입니다. 보안 데이터베이스에 대한 키 저장소 파일의 암호입니다.

콘텐츠 관리 서비스의 키 저장소 인증서 유형은 Administrator 도구에 사용되는 인증서 유형에 따라 달라집니다.

- Administrator 도구에 기본 키 저장소 인증서를 사용한 경우 콘텐츠 관리 서비스에 대해 기본 또는 사용자 지정 키 저장소 인증서를 사용할 수 있습니다.
- Administrator 도구에 사용자 지정 키 저장소 인증서를 사용한 경우 콘텐츠 관리 서비스에 대해 사용자 지정 키 저장소 인증서를 사용해야 합니다.

4. 다음을 클릭합니다.



5. 콘텐츠 관리 서비스 페이지에서 참조 데이터 웨어하우스 데이터베이스에 대한 데이터베이스 및 사용자 계정 정보를 입력합니다.

다음 테이블에는 사용자가 데이터베이스 및 사용자 계정에 대해 지정하는 속성이 설명되어 있습니다.

속성	설명
데이터베이스 유형	참조 데이터 웨어하우스의 데이터베이스입니다. 다음 데이터베이스 중 하나를 선택합니다. <ul style="list-style-type: none"> - Oracle - IBM DB2 - Microsoft SQL Server - Microsoft Azure SQL Database - JDBC를 사용하는 PostgreSQL
데이터베이스 사용자 ID	참조 데이터 웨어하우스 데이터베이스의 사용자 계정입니다.
사용자 암호	데이터베이스 사용자 계정의 암호입니다.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

If you select Microsoft SQL Server or PostgreSQL, specify the schema for the repository tables and database connection:

Property	Description
Schema name	Name of the schema that will contain the repository tables. If not selected, the installer creates the tables in the default schema.
Trusted connection	Indicates whether to connect to Microsoft SQL Server through a trusted connection. Trusted authentication uses the security credentials of the current user to make the connection to Microsoft SQL Server. If not selected, the installer uses Microsoft SQL Server authentication.

6. 데이터베이스 연결 정보를 입력합니다.

JDBC URL에 대한 연결 속성을 지정하거나 JDBC 연결 문자열을 제공할 수 있습니다.

- JDBC URL을 사용하여 연결 정보를 입력하려면 **JDBC URL**을 선택하고 데이터베이스 연결 속성을 지정합니다.

속성	설명
데이터베이스 주소	<호스트 이름>:<포트 번호> 형식으로 된 데이터베이스의 호스트 이름 및 포트 번호입니다.
데이터베이스 서비스 이름	서비스 또는 데이터베이스 이름: - Oracle: 서비스 이름을 입력합니다. - Microsoft SQL Server: 데이터베이스 이름을 입력합니다. - IBM DB2: 서비스 이름을 입력합니다.
JDBC 매개 변수	데이터베이스 연결 문자열에 포함시킬 매개 변수(선택 사항)입니다. 데이터베이스에 대한 데이터베이스 작업을 최적화하려면 매개 변수를 사용하십시오. 매개 변수 문자열이 유효한지 확인하십시오. 설치 프로그램은 JDBC URL에 문자열을 추가하기 전에 매개 변수 문자열의 유효성을 검사하지 않습니다. 선택하지 않으면 설치 프로그램이 추가 매개 변수 없이 JDBC URL 문자열을 생성합니다.

- 사용자 지정 JDBC 연결 문자열을 사용하여 연결 정보를 입력하려면 **사용자 지정 JDBC 연결 문자열**을 선택하고 연결 문자열을 입력합니다.

7. **연결 테스트**를 클릭하여 데이터베이스에 연결할 수 있는지 확인한 다음 **확인**을 클릭하여 계속 진행합니다.

8. **다음**을 클릭합니다.

프로파일링 웨어하우스 연결 데이터베이스

콘텐츠 관리 서비스를 구성한 후에는 데이터 프로파일링 웨어하우스 데이터베이스를 구성할 수 있습니다.

1. 데이터 프로파일링 웨어하우스의 데이터베이스 유형을 선택합니다.

다음 테이블에는 데이터 프로파일링 웨어하우스의 데이터베이스가 나열되어 있습니다.

프롬프트	설명
데이터베이스 유형	데이터 프로파일링 웨어하우스의 데이터베이스 유형입니다. 다음 옵션 중에서 선택하십시오. <ul style="list-style-type: none"> - Oracle - Microsoft SQL Server - IBM DB2

2. 데이터베이스 사용자 계정의 속성을 입력합니다.

다음 테이블에는 데이터베이스 사용자 계정의 속성이 나와 있습니다.

속성	설명
데이터베이스 사용자 ID	데이터 프로파일링 웨어하우스 사용자 계정의 이름입니다.
데이터베이스 사용자 암호	데이터 프로파일링 웨어하우스 사용자 계정의 암호입니다.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

3. 스키마 이름을 지정하려면 **1**을 누릅니다. 스키마 이름을 지정하지 않으려면 **2**를 누릅니다. 기본값은 **2**입니다. **Microsoft SQL Server**를 선택하는 경우 리포지토리 테이블의 스키마 및 데이터베이스 연결을 지정합니다. 스키마 이름을 지정하지 않으면 설치 프로그램이 기본 스키마에 테이블을 생성합니다.
4. **JDBC URL** 정보를 사용하여 **JDBC** 연결 정보를 입력하려면 **1**을 누릅니다. 사용자 지정 **JDBC** 연결 문자열을 사용하여 **JDBC** 연결 정보를 입력하려면 **2**를 누릅니다.
 - a. **JDBC** 연결 정보를 입력합니다.
 - **JDBC URL** 정보를 사용하여 연결 정보를 입력하려면 **JDBC URL** 속성을 지정합니다.

다음 테이블에는 데이터베이스 연결 정보가 설명되어 있습니다.

프롬프트	설명
데이터베이스 호스트 이름	데이터베이스의 호스트 이름입니다.
데이터베이스 포트 번호	데이터베이스의 포트 번호입니다.
데이터베이스 서비스 이름	서비스 또는 데이터베이스 이름: <ul style="list-style-type: none"> - Oracle: 서비스 이름을 입력합니다. - Microsoft SQL Server: 데이터베이스 이름을 입력합니다. - IBM DB2: 서비스 이름을 입력합니다.
JDBC 매개 변수 구성	추가적인 JDBC 매개 변수를 연결 문자열에 추가할지 여부를 선택합니다. 1 - 예 2 - 아니요 예를 선택하는 경우 매개 변수를 입력하거나 Enter 키를 눌러 기본값을 수락합니다. 아니요를 선택하는 경우 설치 프로그램이 매개 변수 없이 JDBC 연결 문자열을 생성합니다.

- 사용자 지정 JDBC 연결 문자열을 사용하여 연결 정보를 입력하려면 연결 문자열을 입력합니다. JDBC 연결 문자열에 다음 구문을 사용합니다.

IBM DB2

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

데이터베이스 시스템에 필요한 모든 연결 매개 변수가 연결 문자열에 포함되어 있는지 확인합니다.

5. 데이터 액세스 연결 문자열을 입력합니다.

PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스

PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스를 구성할 수 있습니다.

1. 설치 중에 PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스를 생성하도록 선택한 경우 **PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스** 페이지가 나타납니다.

2. PowerCenter 리포지토리에 사용하도록 구성할 데이터베이스를 선택합니다.
다음 테이블에는 PowerCenter 리포지토리에 사용하도록 구성할 수 있는 데이터베이스가 나와 있습니다.

프롬프트	설명
데이터베이스 유형	PowerCenter 리포지토리의 데이터베이스 유형입니다. 다음 옵션 중에서 선택하십시오. 1 - Oracle 2 - Microsoft SQL Server 3 - PostgreSQL 4 - IBM DB2 5 - Sybase ASE

3. 데이터베이스 사용자 계정의 속성을 입력합니다.

다음 테이블에는 데이터베이스 사용자 계정의 속성이 나와 있습니다.

속성	설명
데이터베이스 사용자 ID	PowerCenter 리포지토리 데이터베이스 사용자 계정의 이름입니다.
사용자 암호	PowerCenter 데이터베이스 사용자 계정의 암호입니다.
데이터베이스 서비스 이름	PowerCenter의 서비스 또는 데이터베이스 이름입니다. - Oracle: 서비스 이름을 입력합니다. - Microsoft SQL Server: 데이터베이스 이름을 입력합니다. - PostgreSQL: 데이터베이스 이름을 입력합니다. - IBM DB2: 데이터베이스 이름을 입력합니다. - Sybase ASE: 데이터베이스 이름을 입력합니다.
데이터베이스 호스트 이름	PowerCenter 리포지토리 데이터베이스를 입력합니다.

4. 생성할 PowerCenter 리포지토리 서비스의 이름을 입력합니다.
5. 생성할 PowerCenter 통합 서비스의 이름을 입력합니다.
6. PowerCenter 리포지토리 서비스 코드 페이지를 선택합니다. 기본값은 7비트 ASCII입니다.
7. PowerCenter 통합 서비스 코드 페이지를 선택합니다. 기본값은 7비트 ASCII입니다.
8. 다음을 클릭합니다.
9. 완료를 클릭하여 설치 프로그램을 닫습니다.

설치 프로그램이 PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스를 생성하고 서비스를 시작합니다.

설치 후 요약 페이지에 설치가 완료되었는지 여부가 나타납니다. 또한 설치된 구성 요소 및 해당 구성의 상태도 요약에 표시됩니다.

설치 후 요약 섹션에 설치가 완료되었는지 여부가 나타납니다. 설치된 구성 요소 및 해당 구성의 상태도 요약에 표시됩니다.

도메인에 가입

여러 시스템에서 설치하는 중이며 다른 시스템에 도메인을 이미 생성한 경우 도메인에 가입할 수 있습니다.

설치 프로그램 실행

설치 프로그램을 실행하려면 다음 단계를 수행하십시오.

1. 시스템 사용자 계정으로 시스템에 로그인하십시오.
2. 기타 모든 응용 프로그램을 닫으십시오.
3. 설치 파일의 디렉터리 루트로 이동하고 관리자 권한으로 `install.bat`를 실행합니다.

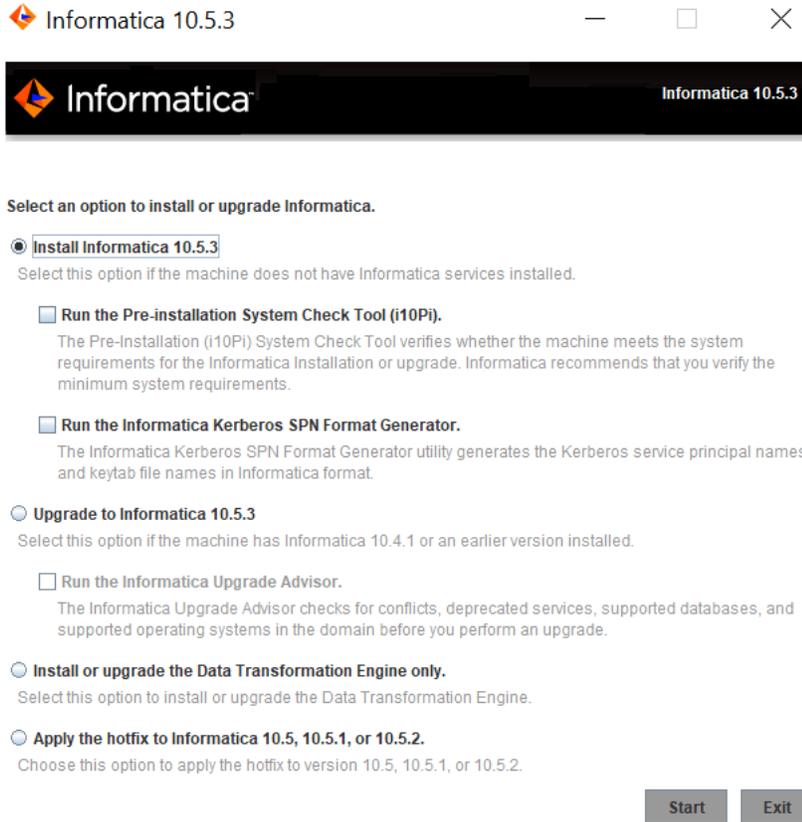
관리자로 이 파일을 실행하려면 `install.bat` 파일을 마우스 오른쪽 단추로 클릭하고 **관리자 권한으로 실행**을 선택합니다.

참고: 관리자 권한으로 설치 프로그램을 실행하지 않는 경우 Windows 시스템 관리자가 Informatica 설치 디렉터리의 파일을 액세스할 때 문제가 발생할 수 있습니다.

Informatica 10.5.3 페이지가 나타납니다.

Informatica 설치 프로그램 시작

1. Informatica 10.5.2 Informatica 10.5.3 설치를 선택합니다.



Informatica는 Informatica 서비스 설치 프로세스를 용이하게 하기 위한 유틸리티를 제공합니다. Informatica 서비스를 설치하기 전에 다음 유틸리티를 실행하십시오.

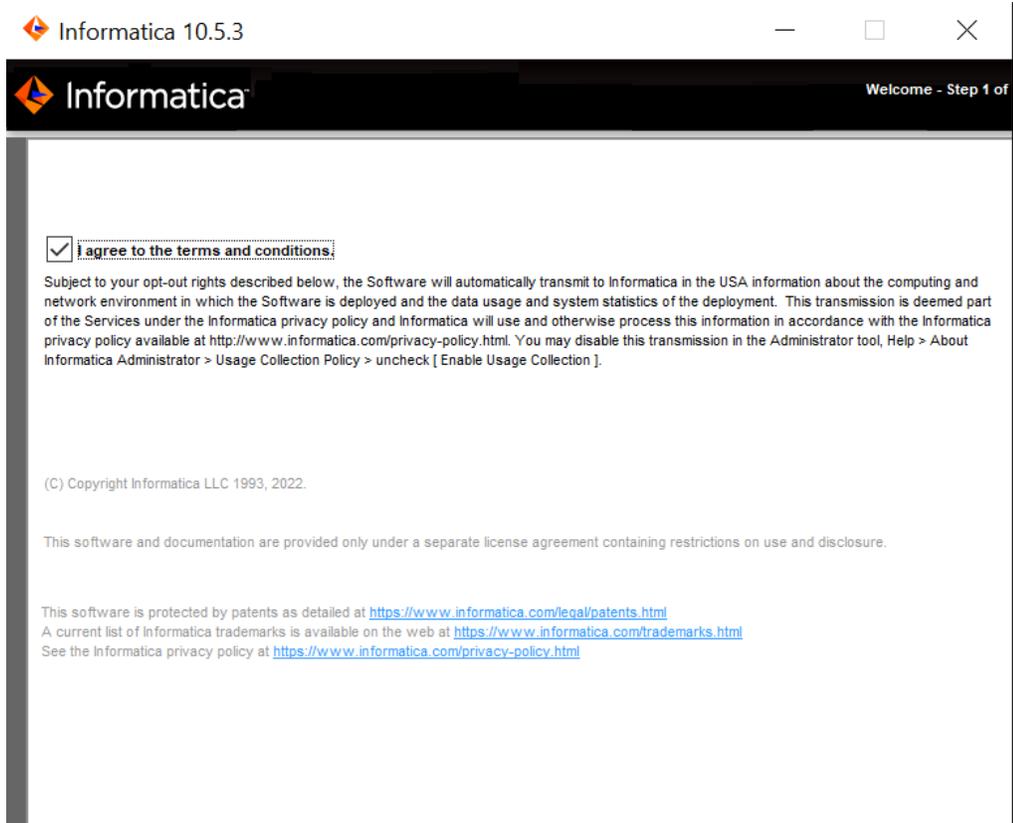
- 설치 전 시스템 검사 도구(i10Pi). Informatica 서비스를 설치할 시스템이 설치를 위한 시스템 요구 사항을 충족하는지 확인합니다.
설치 전 시스템 검사 도구(i10Pi) 실행에 대한 자세한 내용은 [“설치 전 시스템 검사 도구\(i10Pi\) 실행\(그래픽 모드\)” 페이지 102](#)을 참조하십시오.
- Informatica Kerberos SPN 형식 생성기. Kerberos 인증이 포함된 네트워크에서 Informatica 서비스를 실행하는 데 필요한 Kerberos 서비스 사용자 이름과 키 탭 파일 이름 목록을 생성합니다.

Informatica 서비스를 설치하기 전에 설치 프로그램을 사용하여 유틸리티를 실행할 수 있습니다. 유틸리티 실행을 마친 후 설치 프로그램을 다시 시작하여 다음 유틸리티를 실행하거나 Informatica 서비스를 설치합니다.

2. 시작을 클릭합니다.
시작 섹션이 나타납니다.

시작 - 약관 및 조건에 동의

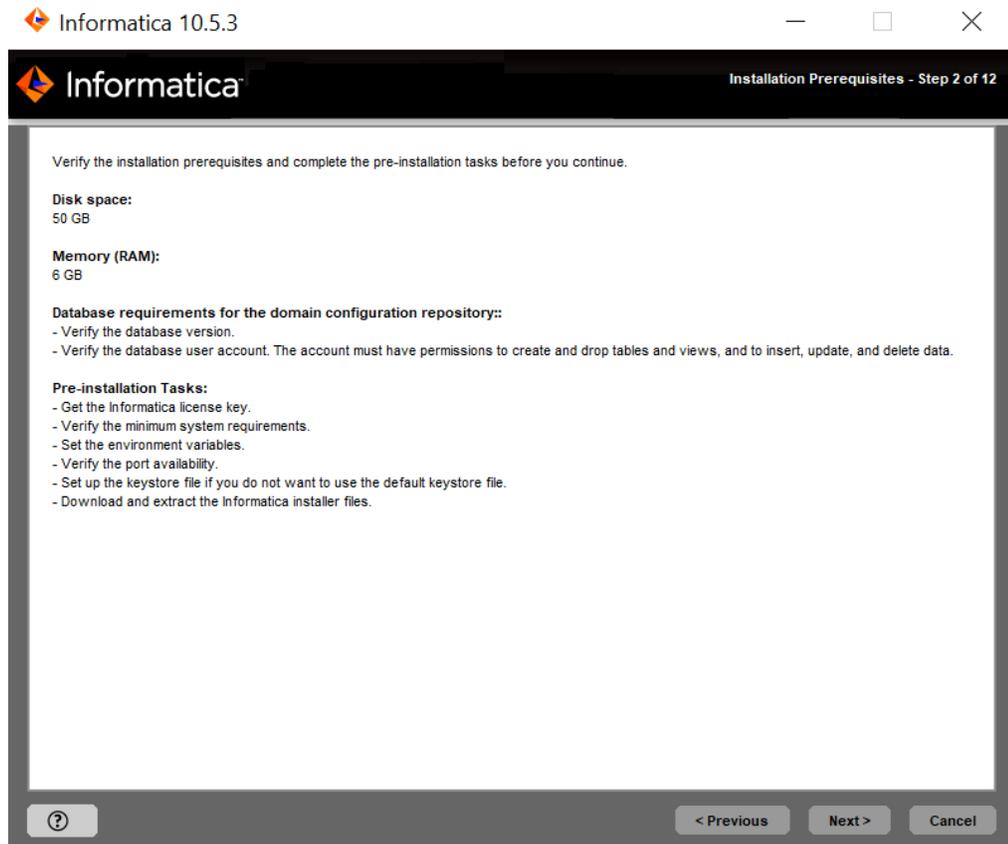
1. Informatica 설치 및 제품 사용 툴킷의 약관을 읽고 **약관을 읽고 동의함**을 선택합니다.



Informatica DiscoveryIQ는 데이터 사용에 대한 루틴 보고서와 시스템 통계를 Informatica로 전송하는 제품 사용 도구입니다. Informatica DiscoveryIQ에서는 사용자가 Informatica 도메인을 설치 및 구성한 후 15분이 지나면 데이터를 Informatica로 업로드합니다. 이후부터는 도메인에서 30일마다 데이터를 전송합니다. Administrator 도구에서 사용 통계를 비활성화하도록 선택할 수 있습니다.

2. 다음을 클릭합니다.

설치 선행 조건 페이지에 설치 요구 사항이 표시됩니다. 설치를 계속하기 전에 모든 요구 사항이 충족되었는지 확인합니다.



3. 다음을 클릭합니다.

라이선스 및 설치 디렉터리 섹션이 나타납니다.

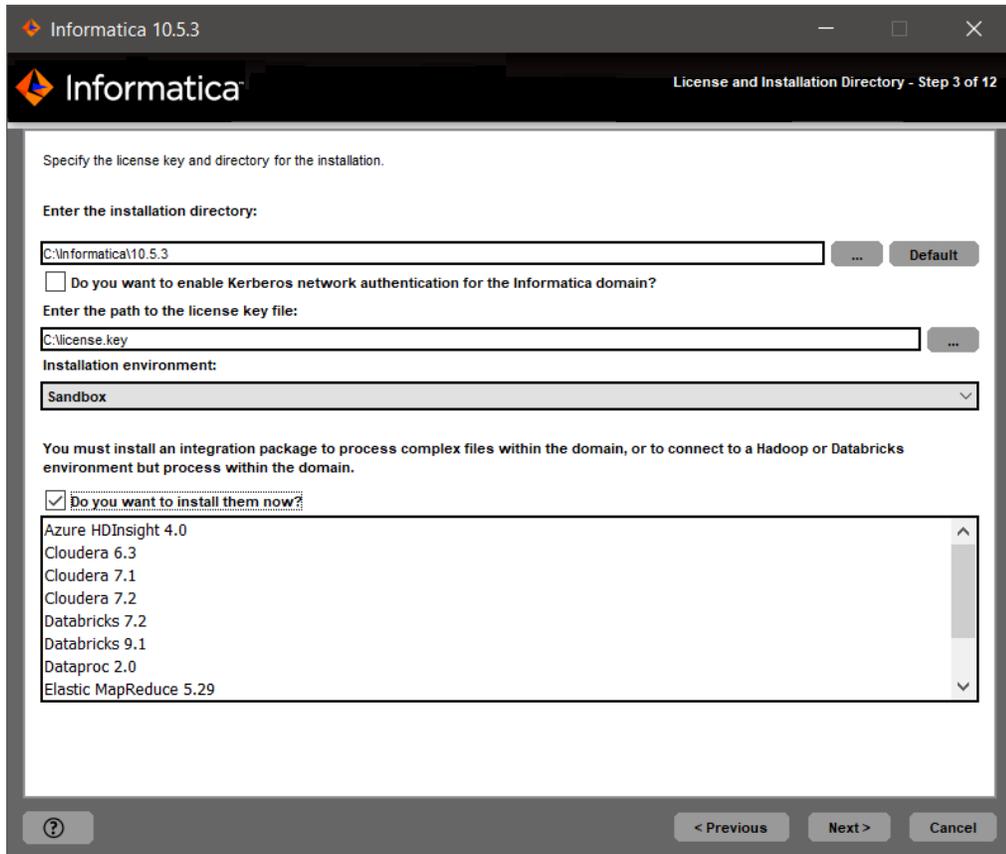
License and Installation Directory

After you verify the installation prerequisites, you can specify the installation directory.

1. On the **License and Installation Directory** page, enter the Informatica license key, installation directory, installation environment, and distribution packages.

The following table describes the license key, directory that you specify for the Informatica services installation, and the distribution packages installation:

Property	Description
License key file	Path and file name of the Informatica license key.
Installation directory	<p>Absolute path for the installation directory. The installation directory must be on the machine where you are installing Informatica. The directory names in the path must not contain spaces or the following special characters: @ * \$ # ! % () { } []</p> <p>참고: Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.</p>
Installation environment	<p>Environment type associated with the Informatica services installation.</p> <ul style="list-style-type: none"> - Set Sandbox environment for a basic environment used for proof of concept with minimal users. - Set Development environment for the design environment. - Set Test environment for high volume processing that is closest to a production environment. - Set Production environment for high volume processing with high levels of concurrency meant for end users. Advanced production environments are typically multi-node setups.
Distribution packages	<p>You can choose whether to install distribution packages through the Informatica installer.</p> <p>If you choose to install distribution packages, select one or more packages from the list that you want to install.</p>



2. Click **Next**.

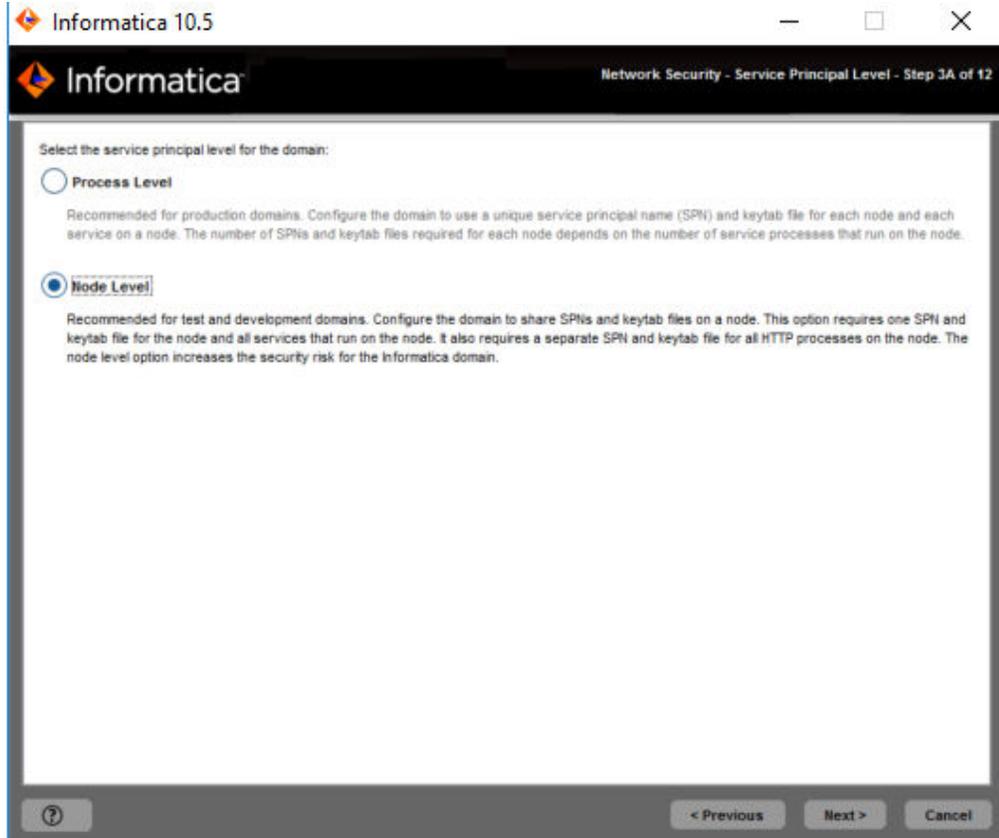
If you enabled Kerberos network authentication, the **Service Principal Level** section appears.

If you did not enable Kerberos network authentication, the **Pre-Installation Summary** section appears. Review the installation information and press **Enter** to continue. Skip to [“도메인 선택” 페이지 114](#).

네트워크 보안 - 서비스 사용자 수준

설치 디렉터리를 지정한 후에는 보안 수준을 구성할 수 있습니다.

1. Kerberos 네트워크 인증을 활성화한 경우 **네트워크 보안 - 서비스 사용자 수준**이 나타납니다.



2. **네트워크 보안 - 서비스 사용자 수준** 페이지에서 도메인에 대한 Kerberos 서비스 사용자를 설정할 수준을 선택합니다.

다음 테이블에는 사용자가 선택할 수 있는 서비스 사용자 수준이 설명되어 있습니다.

수준	설명
프로세스 수준	<p>각 노드 및 노드의 각 응용 프로그램 서비스에 대해 고유한 SPN(서비스 사용자 이름) 및 키 탭 파일을 사용하도록 도메인을 구성합니다.</p> <p>각 노드에 필요한 SPN 및 키 탭 파일의 수는 노드에서 실행되는 응용 프로그램 서비스 프로세스의 수에 따라 달라집니다. 운영 도메인 같이 높은 보안 수준이 필요한 도메인에 대해 프로세스 수준 옵션을 사용하십시오.</p>
노드 수준	<p>노드에서 SPN 및 키 탭 파일을 공유하도록 도메인을 구성합니다.</p> <p>이 옵션에는 노드에 대한 하나의 SPN과 키 탭 파일 및 노드에서 실행되는 모든 응용 프로그램 서비스가 필요합니다. 또한 노드의 모든 HTTP 프로세스에 대해 별도의 SPN 및 키 탭 파일이 필요합니다.</p> <p>테스트 및 개발 도메인 같이 높은 보안 수준이 필요하지 않은 도메인에 대해 노드 수준 옵션을 사용하십시오.</p>

3. 다음을 클릭합니다.

네트워크 보안 - Kerberos 인증 섹션이 나타납니다.

네트워크 보안 - Kerberos 인증

보안 수준을 구성한 후에는 Kerberos 인증을 구성할 수 있습니다.

1. 네트워크 보안 - Kerberos 인증 페이지에서 Kerberos 인증에 필요한 도메인 및 키 탭 정보를 입력합니다.

다음 테이블에는 사용자가 입력해야 하는 Informatica 도메인 및 노드 정보가 설명되어 있습니다.

속성	설명
도메인 이름	작성할 도메인의 이름입니다. The name must not exceed 128 characters and must be 7-bit ASCII only. The name cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
노드 이름	Name of the node to create.
노드 호스트 이름	노드를 생성할 시스템의 정규화된 호스트 이름 또는 IP 주소입니다. 참고: The node host name cannot contain the underscore (_) character. Do not use localhost. The host name must explicitly identify the machine.

The following table describes the Kerberos realm and keytab information that you must provide:

Property	Description
Service realm name	Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example: *EAST.COMPANY.COM
User realm name	Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example: *EAST.COMPANY.COM
Keytab directory	Directory where all keytab files for the Informatica domain are stored. The name of a keytab file in the Informatica domain must follow a format set by Informatica.
Kerberos configuration file	Path and file name of the Kerberos configuration file. Informatica requires the following name for the Kerberos configuration file: <i>krb5.conf</i>

중요: Kerberos 인증으로 실행되도록 도메인을 구성하는 경우, 도메인과 노드 이름 및 노드 호스트 이름이 사용자가 Informatica Kerberos SPN 형식 생성기를 실행하여 SPN 및 키 탭 파일 이름을 생성했을 때 지정한 이름과 일치해야 합니다. 다른 도메인, 노드 또는 호스트 이름을 사용하는 경우, SPN 및 키 탭 파일 이름을 다시 생성하고 Kerberos 관리자에게 새로운 SPN을 Kerberos 사용자 데이터베이스에 추가하고 키 탭 파일을 생성하도록 요청하십시오.

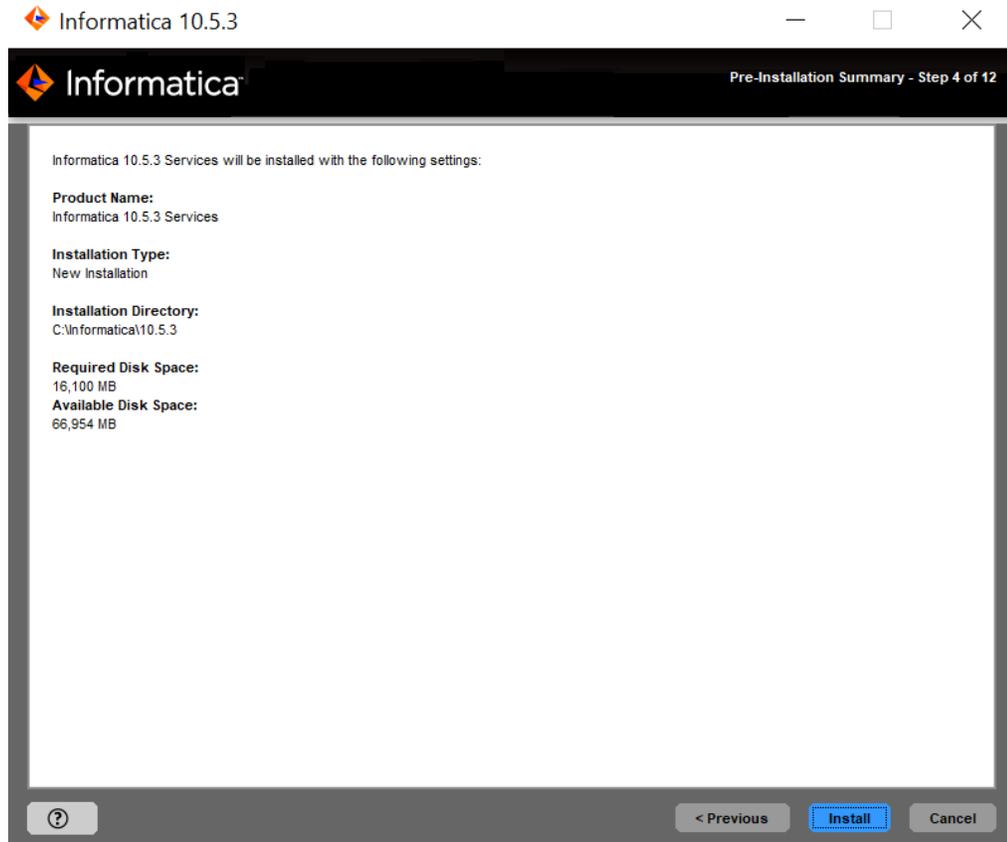
2. 다음을 클릭합니다.

사전 설치 요약 섹션이 나타납니다. 설치 정보를 검토합니다.

도메인 선택

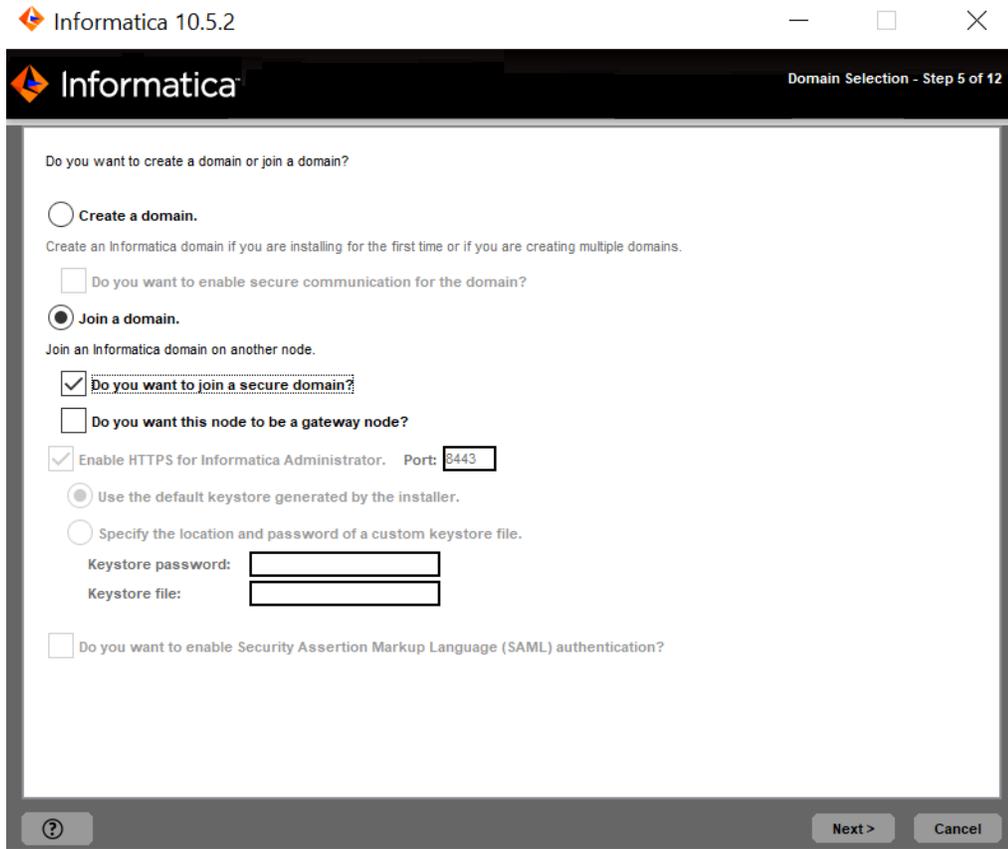
설치 전 요약 검토한 후에는 도메인 정보를 입력할 수 있습니다.

1. 설치 전 요약 페이지를 검토합니다.



2. 설치 정보를 검토하고 설치를 클릭하여 계속 진행합니다.

설치 프로그램이 설치 디렉터리로 Informatica 파일을 복사합니다. 설치 프로그램이 파일을 복사한 후 **도메인 선택** 페이지가 나타납니다.



3. **도메인에 가입**을 선택합니다.

사용자가 설치한 시스템의 노드에 설치 프로그램이 가입합니다.

도메인을 생성하면, 생성하는 노드가 도메인의 게이트웨이 노드가 됩니다. 게이트웨이 노드에는 모든 도메인 작업을 관리하는 서비스 관리자가 포함됩니다.

4. 가입하려는 도메인에서 보안 통신 옵션이 활성화되었는지 여부를 지정합니다.

1을 눌러 비보안 도메인에 가입하거나 **2**를 눌러 보안 도메인에 가입합니다.

5. 생성할 노드 유형을 선택합니다.

1을 눌러 게이트웨이 노드를 구성하거나 **2**를 눌러 작업자 노드를 구성합니다.

노드를 게이트웨이로 구성한 경우, Informatica Administrator에 대한 보안 HTTPS 연결을 활성화할 수 있습니다.

6. Informatica Administrator에 HTTPS 연결을 사용하는 경우 이 연결을 보호하는 데 사용할 HTTPS 포트 번호를 입력하십시오.

7. 도메인에서 SAML 인증을 활성화하는 데 기본 Informatica SSL 인증서를 사용할지 또는 사용자의 SSL 인증서를 사용할지 선택합니다.

다음 테이블에는 SAML 인증에 대한 SSL 인증서 옵션이 설명되어 있습니다.

옵션	설명
기본 Informatica SSL 인증서 파일을 사용합니다.	SAML 인증을 위한 기본 Informatica 트러스트 저장소 파일을 사용하려면 선택합니다.
SSL 인증서 파일의 위치를 입력하십시오.	SAML 인증을 위한 사용자 지정 트러스트 저장소 파일을 사용하려면 선택합니다. 도메인 내의 게이트웨이 노드에 대한 사용자 지정 트러스트 저장소 파일이 포함된 디렉터리를 지정하십시오. 파일에 대한 전체 경로가 아닌 디렉터리만 지정하십시오.

8. Informatica 도메인에서 웹 기반 Informatica 응용 프로그램에 대해 SAML(Security Assertion Markup Language) 기반 SSO(Single Sign-On) 지원을 구성하려면 SAML 인증을 활성화하는 확인란을 선택합니다.
참고: Kerberos 네트워크 인증을 활성화하는 경우 SAML 인증을 구성할 수 없습니다.
9. 다음을 클릭합니다.

SAML 인증 옵션을 활성화하는 확인란을 선택하면 **SAML 인증** 페이지가 나타납니다.

The screenshot shows the Informatica 10.5.3 SAML Authentication configuration window, Step 5A of 12. The window title is "Informatica 10.5.3" and the page title is "SAML Authentication - Step 5A of 12". The main content area is titled "Identity Provider URL" and contains the following configuration options:

- Do you want to enter a relying party trust name or a service provider identifier? If you choose No, the service provider identifier will be used.
- Service Provider ID**
- Enable SAML Assertion Signature Validation
- SAML Assertion Signing Certificate Alias Name**
- Select the truststore for SAML authentication where you imported the identity provider assertion signing certificate
 - Use the default Informatica truststore and keystore.
 - Use a custom truststore and keystore.
- Specify the directory that contains the custom truststore to use for SAML authentication:
- Specify the truststore password
- Specify the directory that contains the custom keystore to use for SAML authentication:
- Specify the keystore password

At the bottom of the window, there are navigation buttons: a help icon (?), "< Previous", "Next >", and "Cancel".

Informatica SAML Authentication - Step 5A of 12

Specify the directory that contains the custom keystore to use for SAML authentication:

Specify the keystore password

Authentication Context Comparison

Authentication Context Class

Enable SAML Request Signing Configuration

SAML Request Signing Private Key Alias Name

SAML Request Signing Private Key Password

SAML Request Signing Algorithm

Enable SAML Response Signature Validation

SAML Response Signing Certificate Alias Name

Enable SAML Assertion Encryption Configuration

Encrypted Assertion Private Key Alias Name

Encrypted Assertion Private Key Password

< Previous Next > Cancel

10. 도메인의 ID 공급자 URL을 입력합니다.
11. ID 공급자에 정의된 도메인의 신뢰 당사자 트러스트 이름 또는 서비스 공급자 식별자를 지정하십시오. 아니요를 선택하는 경우 서비스 공급자 식별자가 "Informatica"로 설정됩니다.
12. IdP에서 SAML 어설션을 서명할지 여부를 지정합니다.
13. ID 공급자 어설션 서명 인증서 별칭 이름을 입력합니다.
14. 도메인에서 보안 통신을 활성화하는 데 기본 Informatica SSL 인증서를 사용할지 사용자의 SSL 사용할지 여부를 지정합니다.

다음 테이블에는 SAML 인증에 대한 SSL 인증서 옵션이 설명되어 있습니다.

옵션	설명
기본 Informatica SSL 인증서 파일을 사용합니다.	SAML 인증을 위한 기본 Informatica 트러스트 저장소 파일을 사용하려면 선택합니다.
SSL 인증서 파일의 위치를 입력하십시오.	SAML 인증을 위한 사용자 지정 트러스트 저장소 파일을 사용하려면 선택합니다. 도메인 내의 게이트웨이 노드에 대한 사용자 지정 트러스트 저장소 파일이 포함된 디렉터리를 지정하십시오. 파일에 대한 전체 경로가 아닌 디렉터리만 지정하십시오.

15. 사용자가 보안 인증서를 제공하는 경우 키 저장소 및 트러스트 저장소 파일의 위치와 암호를 지정합니다.

다음 테이블에는 트러스트 저장소 및 키 저장소 파일의 위치와 암호가 설명되어 있습니다.

속성	설명
트러스트 저장소 디렉터리	도메인 내의 게이트웨이 노드에 대한 사용자 지정 트러스트 저장소 파일이 포함된 디렉터리를 지정하십시오. 파일에 대한 전체 경로가 아닌 디렉터리만 지정하십시오.
트러스트 저장소 암호	사용자 지정 트러스트 저장소 파일에 대한 암호입니다.
키 저장소 디렉터리	사용자 지정 키 저장소 파일이 포함된 디렉터리를 지정합니다.
키 저장소 암호	사용자 지정 키 저장소 파일에 대한 암호입니다.

16. 인증 컨텍스트 비교를 지정하려면 IdP 서버와 사용자가 사용하는 인증 메커니즘의 비교 강도를 지정합니다. 지원되는 값은 MINIMUM, MAXIMUM, BETTER 또는 EXACT 옵션입니다. 기본값은 MINIMUM입니다.
17. 인증 컨텍스트 클래스를 설정하려면 IdP 서버를 사용하는 사용자에게 예상되는 최초 인증 메커니즘을 지정합니다.
지원되는 값은 PASSWORD 또는 PASSWORDPROTECTEDTRANSPORT입니다. 기본값은 PASSWORD입니다.
18. 웹 응용 프로그램이 SAML 인증 요청에 서명하도록 활성화할지 여부를 지정하시겠습니까?
기본값은 비활성화됨입니다.
19. SAML 요청에 서명하는 데 사용하는 노드 SAML 키 저장소로 가져온 개인 키의 별칭 이름을 지정하십시오.
20. SAML 요청 서명에 사용된 개인 키 액세스를 위한 암호를 지정합니다.
21. 웹 응용 프로그램이 SAML 요청을 서명하는 데 사용하는 알고리즘을 지정하십시오.
지원되는 값은 RSA_SHA256, DSA_SHA1, DSA_SHA256, RSA_SHA1, RSA_SHA224, RSA_SHA384, RSA_SHA512, ECDSA_SHA1, ECDSA_SHA224, ECDSA_SHA256, ECDSA_SHA384, ECDSA_SHA512, RIPEMD160 또는 RSA_MD5입니다.
22. IdP가 SAML 응답에 서명하도록 할지 여부를 지정하시겠습니까?
웹 응용 프로그램을 활성화하여 서명된 SAML 응답을 수신할지 여부를 선택하십시오. 기본값은 비활성화됨입니다.
23. IdP에서 SAML 어설션을 암호화할지 여부를 지정하십시오.
웹 응용 프로그램을 활성화하여 암호화된 SAML 어설션을 수신할지 여부를 선택하십시오. 기본값은 활성화됨입니다.
24. Informatica가 SAML 어설션을 암호 해독하는 데 사용하는 게이트웨이 노드 SAML 트러스트 저장소에 있는 개인 키의 별칭 이름을 지정하십시오.
25. 어설션 암호화 키를 암호 해독할 때 사용하는 개인 키 액세스를 위한 암호를 제공하십시오.
26. 다음을 클릭합니다.
도메인에 대한 보안 통신을 활성화하지 않은 경우 **도메인 구성** 페이지가 나타납니다. 도메인 구성 리포트토리 페이지를 설명하는 단계로 건너뛩니다. 도메인에 대한 보안 통신을 활성화하는 확인란을 선택한 경우 **도메인 보안 - 보안 통신** 페이지가 나타납니다.

도메인 보안 - 보안 연결

도메인을 구성한 후에는 도메인 보안을 구성할 수 있습니다.

1. **도메인 보안 - 보안 통신** 페이지에서 기본 Informatica SSL 인증서를 사용하거나 사용자의 SSL 인증서를 사용하여 도메인에서 보안 통신을 활성화할지 여부를 지정합니다.

Informatica 10.5.3

Informatica Domain Security - Secure Communication - Step 5B of 12

Select the SSL certificates to enable secure communication within the domain:

Use the default Informatica SSL certificates contained in the default keystore and truststore.

Use custom SSL certificates. Specify the path, file name, and passwords for the keystore and truststore files that contain the c...

Keystore file directory: c:\temp

Keystore password:

Truststore file directory: c:\temp

Truststore password:

< Previous Next > Cancel

The following table describes the SSL certificate options for securing the Informatica domain:

Option	Description
Use the default Informatica SSL certificates	Use the default SSL certificates provided by Informatica. 참고: If you do not provide an SSL certificate, Informatica uses the same default private key for all Informatica installations. If you use the default Informatica keystore and truststore files, the security of your domain could be compromised. To ensure a high level of security for the domain, select the option to specify the location of the SSL certificate files.
Use custom SSL certificates	Specify the path of the keystore and truststore files that contain the SSL certificates. You can provide a self-signed certificate or a certificate issued by a certificate authority (CA). You must provide SSL certificates in PEM format and in Java Keystore (JKS) files. Informatica requires specific names for the SSL certificate files for the Informatica domain. You must use the same SSL certificates for all nodes in the domain. Store the truststore and keystore files in a directory accessible to all the nodes in the domain and specify the same keystore file directory and truststore file directory for all nodes in the same domain. To set the private truststore files, you must manually import the certificates. Run the keytool command in the <INFA_JDK_HOME> directory to import the private truststore certificates. For example, use the following keytool command: <pre>keytool -noprompt -importkeystore -srckeystore <source truststore file path> -srcstorepass <source truststore file password> -srcalias <alias> -srcstoretype JKS -destkeystore <destination truststore file path> -deststorepass <destination truststore file password> -keypass <private key password> -deststoretype JKS</pre>

2. 사용자가 보안 인증서를 제공하는 경우 키 저장소 및 트러스트 저장소 파일의 위치와 암호를 지정합니다.

The following table describes the parameters that you must enter for the SSL certificate files:

Property	Description
Keystore file directory	Directory that contains the keystore files. The directory must contain files named infa_keystore.jks and infa_keystore.pem.
Keystore password	Password for the keystore infa_keystore.jks.
Truststore file directory	Directory that contains the truststore files. The directory must contain files named infa_truststore.jks and infa_truststore.pem.
Truststore password	Password for the infa_truststore.jks file.

3. 다음을 클릭합니다.
도메인 구성 섹션이 나타납니다.

도메인 구성

도메인 보안을 구성한 후에는 도메인 리포지토리 연결 세부 정보를 구성할 수 있습니다.

- ▶ 가입할 도메인에 대한 정보를 입력합니다.

다음 테이블에는 사용자가 도메인에 대해 지정하는 속성이 설명되어 있습니다.

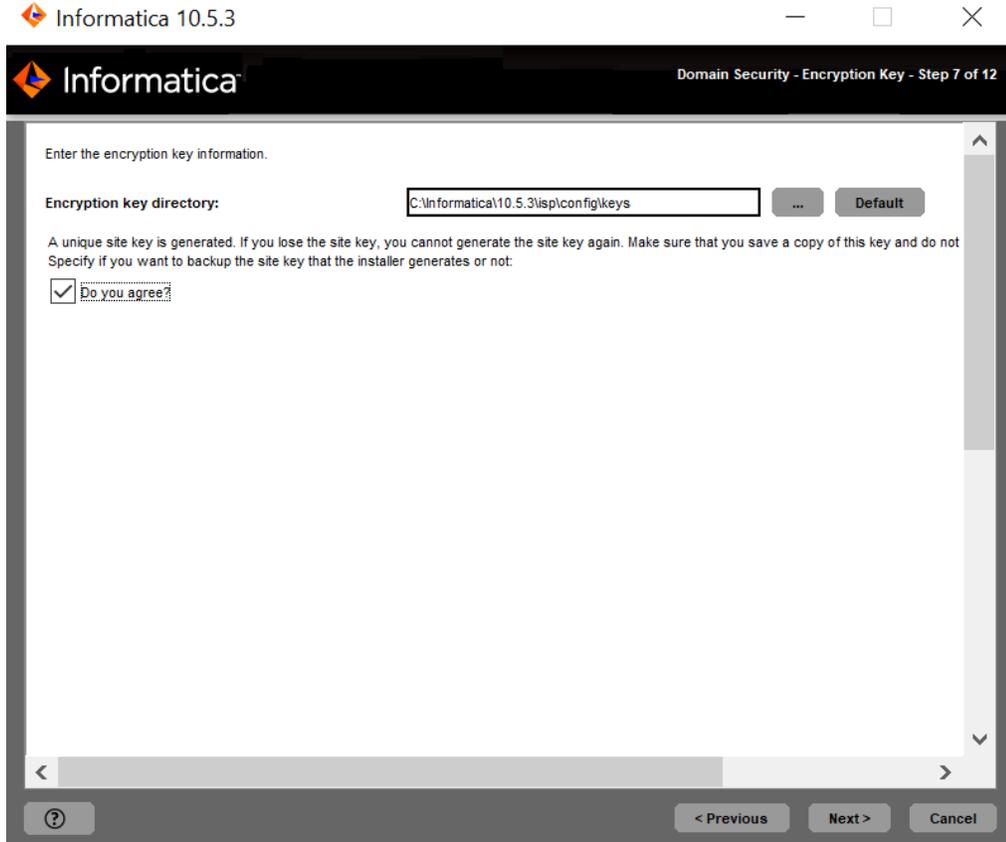
속성	설명
도메인 이름	가입할 도메인의 이름입니다.
게이트웨이 노드 호스트	도메인의 게이트웨이 노드를 호스팅하는 시스템의 호스트 이름입니다.
게이트웨이 노드 포트	게이트웨이 노드의 포트 번호입니다.
도메인 사용자 이름	가입할 도메인에 대한 관리자의 사용자 이름입니다.
도메인 암호	도메인 관리자의 암호입니다.
보안 도메인 이름	보안 도메인의 이름입니다.

도메인 보안 - 암호화 키 섹션이 나타납니다.

도메인 보안 - 암호화 키

도메인 리포지토리를 구성한 후에는 암호화 키를 구성할 수 있습니다.

1. **도메인 보안 - 암호화 키** 섹션에서 도메인을 생성할 때 지정해야 하는 암호화 키 매개 변수를 입력합니다.



다음 테이블에는 도메인을 생성할 때 지정해야 하는 암호화 키 매개 변수가 설명되어 있습니다.

속성	설명
암호화 키 디렉터리	도메인에 대한 암호화 키가 저장되는 디렉터리입니다. 기본적으로 암호화 키는 다음 디렉터리에 생성됩니다. <Informatica 설치 디렉터리>/isp/config/keys.
설치 프로그램에서 생성되는 사이트 키를 백업할지 여부를 지정하십시오.	고유한 사이트 키가 생성됩니다. 사이트 키를 분실하는 경우 사이트 키를 다시 생성할 수 없습니다. 이 키의 사본을 반드시 저장하고 고유한 사이트 키를 다른 사람과 공유하지 마십시오. 설치 프로그램에서 생성되는 사이트 키를 백업할지 여부를 지정하십시오. - [아니요]인 경우 1을 선택합니다. [아니요]를 선택하는 경우 설치 프로그램이 종료됩니다. - [예]인 경우 2를 선택합니다. [예]를 선택하는 경우 파일을 수동으로 백업하는데 동의하는 것입니다.

설치 프로그램이 디렉터리 및 해당 디렉터리의 파일에 대해 서로 다른 사용 권한을 설정합니다. 암호화 키 파일 및 디렉터리의 사용 권한에 대한 자세한 내용은 [“보안 파일 및 디렉터리” 페이지 98](#)를 참조하십시오.

2. 다음을 클릭합니다.

도메인 및 노드 구성 섹션이 나타납니다.

도메인 가입 노드 구성

암호화 키를 구성한 후에는 가입 도메인 및 노드를 구성할 수 있습니다.

1. 가입할 도메인 및 노드에 대한 정보를 입력합니다.

다음 테이블에는 현재 노드에 대해 설정해야 하는 속성이 설명되어 있습니다.

속성	설명
노드 호스트 이름	가입할 노드가 있는 시스템의 호스트 이름 또는 IP 주소입니다. 시스템이 단일 네트워크 이름을 갖는 경우 기본 호스트 이름을 사용하십시오. 시스템이 여러 네트워크 이름을 갖는 경우 대체 네트워크 이름을 사용하도록 기본 호스트 이름을 수정할 수 있습니다. 참고: 노드 호스트 이름에는 밑줄(_) 문자를 사용할 수 없습니다. localhost는 사용하지 마십시오. 호스트 이름은 명시적으로 시스템을 식별해야 합니다.
노드 이름	가입할 노드의 이름입니다.
노드 포트 번호	노드의 포트 번호입니다. 노드의 기본 포트 번호는 6005입니다. 시스템에서 해당 포트 번호를 사용할 수 없는 경우 사용 가능한 다음 포트 번호가 설치 프로그램에 표시됩니다.

2. 설치 프로그램에 의해 할당된 도메인 및 노드 구성 요소에 대한 고급 포트 구성을 표시할지 여부를 선택합니다.

포트 구성 옵션을 비활성화하면 설치 프로그램이 포트 구성을 표시하지 않습니다. 포트 구성 옵션을 활성화한 경우 **포트 구성** 섹션이 나타납니다. 도메인 구성 요소에 할당된 기본 포트 번호가 표시됩니다. 도메인 및 노드 구성 요소에 사용할 포트 번호를 지정할 수 있습니다. 노드에서 실행될 서비스 프로세스에 사용할 포트 번호의 범위도 지정할 수 있습니다. 기본 포트 번호를 사용하거나 새 포트 번호를 지정할 수 있습니다. 입력하는 포트 번호가 다른 응용 프로그램에서 사용되지 않는지 확인합니다.

3. 모델 리포지토리 서비스 및 데이터 통합 서비스 생성 여부를 선택합니다.

서비스 생성을 선택하면 **모델 리포지토리 서비스** 및 **데이터 통합 서비스** 섹션이 나타납니다.

4. PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스 생성 여부를 선택합니다.

서비스 생성을 선택하면 **PowerCenter 리포지토리 서비스** 및 **PowerCenter 통합 서비스** 섹션이 나타납니다.

설치 후 요약 섹션에 설치가 완료되었는지 여부가 나타납니다. 또한 설치된 구성 요소 및 해당 구성의 상태도 요약에 표시됩니다.

포트 구성

서비스 관리자 및 Informatica Administrator의 포트 번호를 업데이트할 수 있습니다.

1. 포트 구성 페이지를 표시하도록 선택한 경우 **포트 구성** 페이지가 나타납니다.

Informatica 10.5.2

Informatica Port Configuration - Step 8A of 12

Enter the port number for the Service Manager.

Service Manager port: 13242

Service Manager shutdown port: 13243

Enter a range of port numbers for service processes in the node.

Minimum port number: 13250

Maximum port number: 13350

< Previous Next > Cancel

2. **포트 구성** 페이지에서 노드에서 실행할 도메인 서비스 관리자 및 서비스 프로세스에 사용할 포트 번호를 입력합니다.

입력하는 포트 번호가 다른 응용 프로그램에서 사용되지 않는지 확인합니다.

The following table describes the ports that you can set:

Port	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.

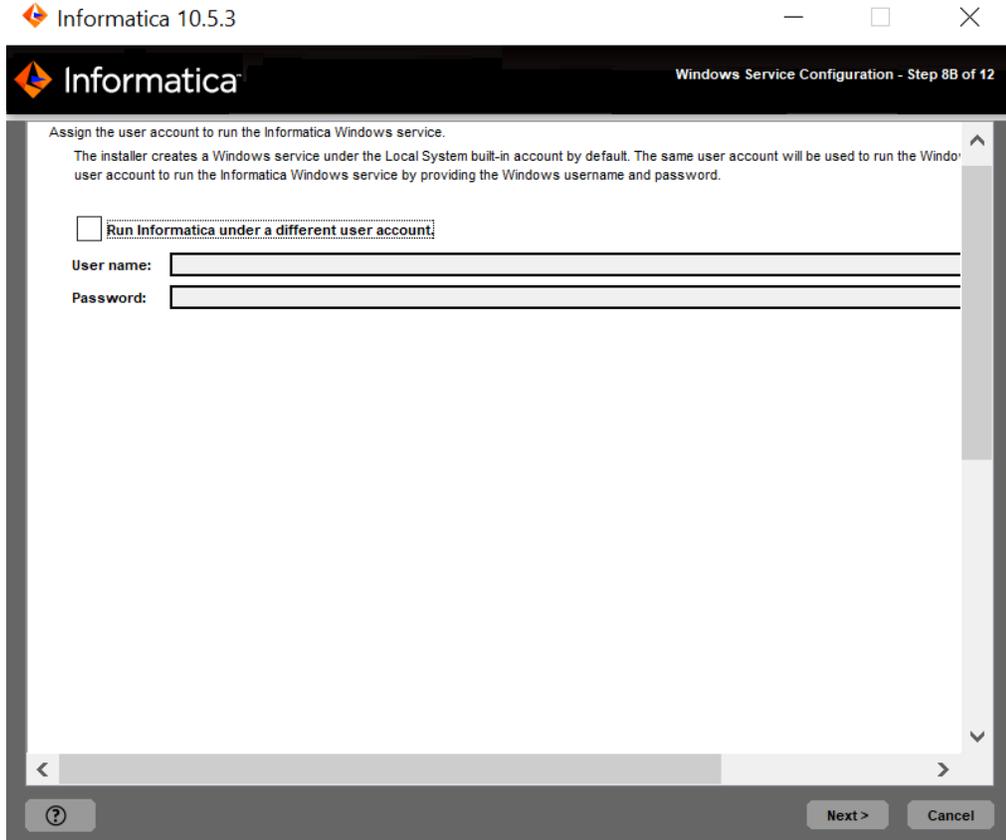
Port	Description
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.

3. 다음을 클릭합니다.

Windows 서비스 구성 페이지가 나타납니다.

Windows 서비스 구성

1. 포트 구성 페이지를 표시하도록 선택하지 않은 경우 설치 프로그램이 **Windows 서비스 구성** 페이지를 표시합니다.



2. **Windows 서비스 구성** 페이지에서 Windows 서비스를 다른 사용자 계정으로 실행할지 여부를 선택합니다. 설치 프로그램이 Informatica를 시작하기 위한 서비스를 생성합니다. 기본적으로 해당 서비스는 설치에 사용된 계정과 동일한 사용자 계정으로 실행됩니다. 다른 사용자 계정으로 Windows 서비스를 실행할 수도 있습니다.

The following table describes the properties that you set to run Informatica under a different account:

Property	Description
Run Informatica under a different user account	Indicates whether to run the Windows service under a different user account.
User name	User account with which to run the Informatica Windows service. Use the following format: <domain name>\<user account> This user account must have the Act as operating system permission.
Password	Password for the user account with which to run the Informatica Windows service.

3. 다음을 클릭합니다.

서비스를 생성하도록 선택하지 않은 경우 설치 프로그램이 **설치 후 요약** 페이지를 표시합니다. **설치 후 요약** 페이지에 설치가 완료되었는지 여부가 나타납니다.

Informatica 응용 프로그램 서비스를 구성하도록 선택한 경우 설치 프로그램이 **모델 리포지토리 서비스 데이터베이스** 페이지를 표시합니다.

모델 리포지토리 서비스 데이터베이스 구성

도메인과 노드를 구성한 후에는 모델 리포지토리 데이터베이스 속성을 구성할 수 있습니다.

1. **모델 리포지토리 서비스 데이터베이스** 페이지에서 모델 리포지토리에 대한 데이터베이스 및 사용자 계정 정보를 입력합니다.

The screenshot shows the 'Model Repository Database - Step 9A of 12' configuration window in Informatica 10.5.3. The window contains the following fields and options:

- Model Repository Service name: [Text input field]
- Enter database information for the Model repository:
 - Database type: [Text input field]
 - Database user ID: [Text input field]
 - Database user password: [Text input field]
- Is the database secure?
- Database connection:
 - Enter the JDBC URL.
 - Database address: [Text input field with placeholder 'host_name:port_no']
 - Database service name: [Text input field with placeholder 'ServiceName']
 - JDBC parameters: [Text input field with placeholder 'MaxPooledStatements=20,CatalogOptions=0,BatchPerformanceWorkaround=true']
 - Enter the JDBC connection string. [Text input field]

At the bottom of the window, there are navigation buttons: a question mark icon, 'Next >', and 'Cancel'.

다음 테이블에는 사용자가 데이터베이스 및 사용자 계정에 대해 지정하는 속성이 설명되어 있습니다.

속성	설명
데이터베이스 유형	리포지토리의 데이터베이스입니다. 다음 데이터베이스 중 하나를 선택합니다. - Oracle - IBM DB2 - Microsoft SQL Server - PostgreSQL
데이터베이스 사용자 ID	리포지토리 데이터베이스의 사용자 계정입니다.
사용자 암호	데이터베이스 사용자 계정의 암호입니다.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

If you select Microsoft SQL Server or PostgreSQL, specify the schema for the repository tables and database connection:

Property	Description
Schema name	Name of the schema that will contain the repository tables. If not selected, the installer creates the tables in the default schema.
Trusted connection	Indicates whether to connect to Microsoft SQL Server through a trusted connection. Trusted authentication uses the security credentials of the current user to make the connection to Microsoft SQL Server. If not selected, the installer uses Microsoft SQL Server authentication.

도메인에 대해 보안 통신을 활성화하는 경우 **SSL** 프로토콜로 보호되는 데이터베이스에서 모델 리포지토리를 생성할 수 있습니다. 보안 모델 리포지토리를 작성하려면 **3**단계로 건너뛩니다.

2. 데이터베이스 연결 정보를 입력합니다.

보안 모델 리포지토리를 작성하지 않은 경우 **JDBC URL**에 대한 연결 속성을 지정하거나 **JDBC 연결 문자열**을 제공할 수 있습니다.

- **JDBC URL**을 사용하여 연결 정보를 입력하려면 **JDBC URL**을 선택하고 데이터베이스 연결 속성을 지정합니다.

다음 표에는 사용자가 지정해야 하는 JDBC URL 속성이 설명되어 있습니다.

속성	설명
데이터베이스 주소	host_name:port 형식으로 된 데이터베이스의 호스트 이름 및 포트 번호입니다.
데이터베이스 서비스 이름	서비스 또는 데이터베이스 이름: - Oracle: 서비스 이름을 입력합니다. - Microsoft SQL Server: 데이터베이스 이름을 입력합니다. - IBM DB2: 서비스 이름을 입력합니다. - PostgreSQL: 데이터베이스 이름을 입력합니다.
JDBC 매개 변수	데이터베이스 연결 문자열에 포함할 매개 변수(선택 사항)입니다. 데이터베이스에 대한 데이터베이스 작업을 최적화하려면 매개 변수를 사용하십시오. 매개 변수 문자열이 유효하지 확인하십시오. 설치 프로그램은 JDBC URL에 문자열을 추가하기 전에 매개 변수 문자열의 유효성을 검사하지 않습니다. 선택하지 않으면 설치 프로그램이 추가 매개 변수 없이 JDBC URL 문자열을 생성합니다.

- 사용자 지정 JDBC 연결 문자열을 사용하여 연결 정보를 입력하려면 **사용자 지정 JDBC 연결 문자열**을 선택하고 연결 문자열을 입력합니다.

IBM DB2

```
jdbc:Informatica:db2://<호스트 이름>:<포트 번호>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<호스트 이름>:<포트 번호>;ServiceName=
```

Oracle Connection Manager를 통해 Oracle 데이터베이스에 연결하려면 다음 연결 문자열을 사용합니다.

```
jdbc:Informatica:oracle:TNSNamesFile=<tnsnames.ora 파일에 대한 정규화된 경로>;TNSServerName=<TNS 이름>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<호스트 이름>:<포트 번호>;SelectMethod=cursor;DatabaseName=
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

Active Directory 인증을 사용하는 Azure SQL Database

```
"jdbc:informatica: sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;LoginTimeout=<seconds>"
```

PostgreSQL

```
jdbc:Informatica:postgresql://<호스트 이름>:<포트 번호>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLV1.2;
```

데이터베이스 시스템에 필요한 모든 연결 매개 변수가 연결 문자열에 포함되어 있는지 확인합니다.

3. 보안 모델 리포지토리를 생성할지 여부를 선택합니다.

보안 데이터베이스에 리포지토리를 생성하는 경우 데이터베이스에 대한 트러스트 저장소 정보를 제공해야 합니다. 데이터베이스에 대한 보안 매개 변수가 포함된 JDBC 연결 문자열도 제공해야 합니다.

The following table describes the properties you must set for a secure database:

Property	Description
Database truststore file	Path and file name of the truststore file for the secure database.
Database truststore password	Password for the truststore file.
Custom JDBC Connection String	JDBC connection string to connect to the secure database, including the host name and port number and the security parameters for the database.

보안 데이터베이스의 JDBC 연결에 포함해야 하는 보안 매개 변수에 대한 자세한 내용은 [“보안 데이터베이스에 대한 연결 문자열” 페이지 94](#)을 참조하십시오.

4. **연결 테스트**를 클릭하여 데이터베이스에 연결할 수 있는지 확인한 다음 **확인**을 클릭하여 계속 진행합니다.

5. **다음**을 클릭합니다.

서비스 매개 변수 섹션이 나타납니다.

데이터 통합 서비스

모델 리포지토리 데이터베이스를 구성한 후에는 응용 프로그램 서비스에 대한 서비스 매개 변수를 구성할 수 있습니다.

1. 데이터 통합 서비스 페이지에서 데이터 통합 서비스 속성을 구성합니다.

The following table describes services parameters that you must set:

Port	Description
Data Integration Service name	Name of the Data Integration Service to create in the Informatica domain.
HTTP protocol type	Type of connection to the Data Integration Service. Select one of the following options: - HTTP. Requests to the service uses an HTTP connection. - HTTPS. Requests to the service uses a secure HTTP connection. - HTTP&HTTPS. Requests to the service can use either an HTTP or HTTPS connection.
HTTP port	Port number to used for the Data Integration Service. Default is 6030.

2. HTTPS 연결을 선택하는 경우 데이터 통합 서비스에 대한 연결의 보안에 기본 Informatica SSL 인증서를 사용할지 사용자의 SSL 인증서를 사용할지를 지정합니다.

다음 테이블에는 데이터 통합 서비스 보안을 위한 SSL 인증서 옵션이 설명되어 있습니다.

옵션	설명
기본 Informatica SSL 인증서 파일을 사용합니다.	Use the default SSL certificates provided by Informatica. 참고: If you do not provide an SSL certificate, Informatica uses the same default private key for all Informatica installations. If you use the default Informatica keystore and truststore files, the security of your domain could be compromised. To ensure a high level of security for the domain, select the option to specify the location of the SSL certificate files.
SSL 인증서 파일의 위치를 입력하십시오.	Specify the path of the keystore and truststore files that contain the SSL certificates.

사용자가 인증서를 제공하는 경우 키 저장소 및 트러스트 저장소 파일의 위치와 암호를 지정합니다.

The following table describes the parameters that you must enter for the SSL certificate files:

Property	Description
Keystore file	Required. Path and file name of the keystore file that contains the private keys and SSL certificates for the database.
Keystore password	Required. Password for the keystore file for the secure database.
Truststore file	Required. Path and file name of the truststore file that contains the public key for the database.
Truststore password	Required. Password for the truststore file for the secure database.

3. 다음을 클릭합니다.

설치 프로그램이 데이터 통합 서비스를 생성합니다.

PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스

PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스를 구성할 수 있습니다.

1. 설치 중에 PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스를 생성하도록 선택한 경우 **PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스** 페이지가 나타납니다.

2. PowerCenter 리포지토리에 사용하도록 구성할 데이터베이스를 선택합니다.
다음 테이블에는 PowerCenter 리포지토리에 사용하도록 구성할 수 있는 데이터베이스가 나와 있습니다.

프롬프트	설명
데이터베이스 유형	PowerCenter 리포지토리의 데이터베이스 유형입니다. 다음 옵션 중에서 선택하십시오. 1 - Oracle 2 - Microsoft SQL Server 3 - PostgreSQL

3. 데이터베이스 사용자 계정의 속성을 입력합니다.

다음 테이블에는 데이터베이스 사용자 계정의 속성이 나와 있습니다.

속성	설명
데이터베이스 사용자 ID	PowerCenter 리포지토리 데이터베이스 사용자 계정의 이름입니다.
사용자 암호	PowerCenter 데이터베이스 사용자 계정의 암호입니다.
데이터베이스 서비스 이름	PowerCenter의 서비스 또는 데이터베이스 이름입니다. - Oracle: 서비스 이름을 입력합니다. - Microsoft SQL Server: 데이터베이스 이름을 입력합니다. - PostgreSQL: 데이터베이스 이름을 입력합니다.
데이터베이스 호스트 이름	PowerCenter 리포지토리 데이터베이스를 입력합니다.

4. 생성할 PowerCenter 리포지토리 서비스의 이름을 입력합니다.
5. 생성할 PowerCenter 통합 서비스의 이름을 입력합니다.
6. PowerCenter 리포지토리 서비스 코드 페이지를 선택합니다. 기본값은 7비트 ASCII입니다.
7. PowerCenter 통합 서비스 코드 페이지를 선택합니다. 기본값은 7비트 ASCII입니다.
8. 다음을 클릭합니다.
9. 완료를 클릭하여 설치 프로그램을 닫습니다.
 설치 프로그램이 PowerCenter 리포지토리 서비스 및 PowerCenter 통합 서비스를 생성하고 서비스를 시작합니다.
 설치 후 요약 페이지에 설치가 완료되었는지 여부가 나타납니다. 또한 설치된 구성 요소 및 해당 구성의 상태도 요약에 표시됩니다.
 설치 후 요약 섹션에 설치가 완료되었는지 여부가 나타납니다. 또한 설치된 구성 요소 및 해당 구성의 상태도 요약에 표시됩니다.

제 10 장

자동 설치 프로그램 실행

이 장에 포함된 항목:

- [자동 모드에서 설치, 229](#)
- [속성 파일의 암호 암호화, 230](#)

자동 모드에서 설치

사용자 상호 작용 없이 설치하려면 자동 모드로 설치하십시오. 설치 옵션을 지정하려면 속성 파일을 사용합니다. 설치 프로그램은 이 파일을 읽어 설치 옵션을 확인합니다. 자동 모드 설치를 사용하여 네트워크의 여러 시스템에 서비스를 설치하거나 시스템 간에 설치를 표준화할 수 있습니다.

서비스를 설치하려는 시스템의 하드 디스크에 설치 파일을 복사하십시오. 원격 시스템에 설치하는 경우 원격 시스템에서 파일을 액세스하고 생성할 수 있는지 확인하십시오.

자동 모드에서 설치하려면 다음 태스크를 완료하십시오.

1. 암호 암호화 유틸리티를 실행하여 설치 속성 파일의 암호를 암호화합니다.
2. 설치 속성 파일을 구성하고 속성 파일에 설치 옵션을 지정합니다.
3. 설치 속성 파일을 사용하여 설치 프로그램을 실행합니다.

속성 파일 구성

자동 모드에서 **Informatica** 서비스를 설치하는 데 필요한 구성 속성이 포함되는 속성 파일을 구성합니다.

Informatica는 두 가지 버전의 속성 파일을 제공합니다. 두 파일 중 하나를 사용하여 설치 옵션을 지정할 수 있습니다.

자동 입력 속성 파일

자동 입력 속성 파일에는 자동 모드에서 **Informatica** 서비스를 설치하는 데 필요한 구성 속성이 포함됩니다. 파일의 각 속성에 대해 설정할 적절한 값을 고려하려면 이 파일을 사용합니다.

기본 자동 입력 속성 파일

기본 자동 입력 속성 파일에는 다수의 구성 속성에 대한 기본값이 포함됩니다. 파일의 아래쪽 부분에 속성이 나열됩니다. 기본 속성 값을 사용하여 **Informatica** 서비스를 설치할 계획인 경우 이 파일을 사용합니다.

이 파일에는 다음 옵션에 대한 기본값으로 설정된 속성이 포함됩니다.

- 응용 프로그램 서비스 이름
- SSL(Secure Sockets Layer) 인증

- Kerberos 인증
- 도메인 및 노드 구성 요소에 대한 포트 번호 할당

자동 모드에서 Informatica 서비스를 설치하는 데 필요한 구성 속성이 포함되는 속성 파일을 구성하려면 다음 단계를 수행합니다.

1. 설치 파일을 포함하는 디렉터리의 루트로 이동합니다.
2. 필요한 경우 암호 암호화 유틸리티를 실행하여 .properties 파일의 암호를 암호화합니다.
3. SilentInput.properties 파일의 백업 사본을 생성합니다.
4. SilentInput.properties 파일 또는 SilentInput_Default.properties 파일을 엽니다.
5. 파일에 포함된 속성을 구성합니다.
6. SilentInput.properties라는 이름으로 파일을 저장합니다.

설치 프로그램 실행

속성 파일을 구성한 후 명령 프롬프트를 열어 자동 설치를 시작하십시오.

1. 명령 프롬프트를 엽니다.
2. 설치 파일을 포함하는 디렉터리의 루트로 이동합니다.
3. 편집하고 다시 저장한 SilentInput.properties 파일이 이 디렉터리에 있는지 확인합니다.
4. 자동 설치를 실행합니다. Linux에서 silentInstall.sh를 실행합니다.

자동 설치 프로그램이 백그라운드에서 실행됩니다. 이 프로세스에는 다소 시간이 걸릴 수 있습니다.

Informatica_<버전>_Services_InstallLog<타임스탬프>.log 파일이 설치 디렉터리에 생성되면 자동 설치가 완료된 것입니다.

속성 파일을 잘못 구성하거나 설치 디렉터리에 액세스할 수 없는 경우 자동 설치가 실패합니다. 설치 로그 파일을 살펴보고 오류를 수정하십시오. 그런 다음 자동 설치를 다시 실행하십시오.

속성 파일의 암호 암호화

설치 프로그램에 포함된 유틸리티를 사용하면 자동 모드에서 설치 프로그램을 실행할 때 옵션을 지정하기 위해 사용하는 속성 파일의 암호를 암호화할 수 있습니다. Informatica에서는 암호를 암호화하는 데 다중 256비트 키를 통한 AES 암호화가 사용됩니다.

이 유틸리티는 암호화하려는 각 암호에 대해 실행해야 합니다. 유틸리티를 실행할 때 명령 프롬프트에 일반 텍스트로 암호 값을 지정합니다. 그러면 유틸리티가 암호화된 형식의 암호를 출력으로 생성합니다. 출력에는 =INSTALLER:CIPHER:AES:256=이라는 접두사가 포함됩니다.

접두사를 포함한 전체 출력 문자열을 복사하여 속성 파일에 암호 속성 값으로 붙여 넣습니다. 자동 모드에서 설치 프로그램을 실행하면 설치 프레임워크가 암호를 해독합니다.

1. 다음 유틸리티 디렉터리로 이동합니다.
<설치 디렉터리>/properties/utils/passwd_encryption
2. 유틸리티를 실행합니다. <암호> 값으로 암호화할 일반 텍스트 암호를 지정합니다.
 - Linux 및 UNIX에서 다음 명령을 실행합니다.
sh install.sh <암호>

- Windows에서 다음 명령을 실행합니다.

```
install.bat <암호>
```

3. 출력에서 암호화된 암호 문자열을 복사하여 `.properties` 파일에 해당 암호 값으로 붙여 넣습니다.

다음 예에서는 `DOMAIN_PSSWD` 속성의 값으로 설정된 암호화된 암호를 보여 줍니다.

```
DOMAIN_PSSWD==INSTALLER:CIPHER:AES:256=mjkjDR2kzFJiizfRWIOPg==
```

제 11 장

문제 해결

이 장에 포함된 항목:

- [설치 문제 해결 개요, 232](#)
- [실패한 설치 프로그램 프로세스 다시 시작, 232](#)
- [설치 로그 파일 문제 해결, 233](#)
- [도메인 및 노드 문제 해결, 235](#)
- [Informatica Developer 문제 해결, 237](#)

설치 문제 해결 개요

이 섹션의 항목은 Informatica 설치 프로세스 중에 발생할 수 있는 가능한 문제를 해결하는 방법에 대한 정보를 제공합니다. 항목에 포함된 예는 일반적인 문제 해결 방법을 설명하며, 설치 문제의 가능한 모든 원인을 포괄적으로 제공하지 않습니다.

실패한 설치 프로그램 프로세스 다시 시작

설치 프로세스가 중간에 중지되는 경우 실패 또는 종료 지점에서 설치를 다시 시작할 수 있습니다.

UNIX 또는 Linux에서 설치 프로세스가 실패할 경우 이전 서비스 구성에서 다시 시작하고 해당 서비스 설치에 대해 마지막으로 입력한 세부 정보를 복구할 수 있습니다. 네트워크가 중단되거나 전체 설치 프로세스가 완료되기 전에 설치를 종료하거나 입력한 정보가 잘못된 경우 설치 프로세스가 실패할 수 있습니다.

설치를 다시 시작할 때 다음 지침을 고려하십시오.

설치 프로그램을 다시 시작할 수 있는 경우

서비스가 실패하거나 서비스 생성 중에 설치 프로세스가 실패하는 경우 서버 설치 프로그램을 사용하여 설치 프로세스를 다시 시작할 수 있습니다. 설치 프로세스를 다시 시작하려면 설치 로그에서 하나 이상의 서비스가 생성되어 있으며 도메인이 설정되고 실행되는지 확인해야 합니다. 예를 들어 모델 리포지토리 서비스가 생성되었는지 확인하려면 서버 로그에 다음과 같은 형식의 서비스 생성 성공 텍스트가 있는지 확인합니다.

```
SUCCESS: MRS Service [mrs_name] is created. Command ran successfully.
```

설치를 다시 시작하려면 설치 프로그램을 다시 실행합니다.

서비스를 생성하는 동안 설치 프로그램을 다시 시작하면 서비스 생성 상태, 서비스 이름, 서비스 활성화 또는 비활성화 상태 같은 모든 서비스 및 데이터베이스 관련 정보가 설치 프로그램에 유지됩니다. 이전에 입력한 값을 확인하고 사용하거나 서비스에 대한 새 값을 지정하고 설치 프로세스를 다시 시작할 수 있습니다.

설치 프로그램을 다시 시작할 수 없는 경우

다음과 같은 경우에는 설치 프로그램을 다시 시작할 수 없습니다.

- 서비스가 생성된 후 서비스를 구성하기 위해 설치 프로그램을 실행하는 경우
- 서비스 구성 마법사를 실행하는 경우
- 도메인에 가입하는 경우

설치 프로그램을 다시 시작하기 전에

설치 프로세스가 중간에 중지되는 경우 실패 또는 종료 지점에서 설치를 다시 시작할 수 있습니다.

설치 프로그램을 다시 시작하기 전에 다음 선행 조건을 완료합니다.

1. 설치 디렉터리에 있는 설치 로그 파일에서 도메인과 하나 이상의 서비스가 생성되어 있는지 확인합니다. 설치 프로그램 로그 파일 이름은 다음과 같은 구문으로 나타납니다. `Informatica_<버전>_Services_<타임스탬프>.log`
2. 사용자 설치 디렉터리의 도구 폴더에 있는 `installInst.obj` 개체 파일이 삭제되지 않았는지 확인합니다.
3. 자동 설치 프로그램을 통해 다시 시작하려는 경우 `SilentInput.properties` 파일에서 `RESUME_INSTALLATION`을 `true`로 설정해야 합니다.

설치 프로그램 다시 시작

선행 조건을 완료한 후에는 설치 프로그램을 다시 시작할 수 있습니다.

1. 명령 프롬프트를 열고 설치 파일의 위치로 이동합니다.
2. 콘솔 설치 프로그램 또는 자동 설치 프로그램을 실행합니다.
3. 정규 설치 프로그램이 실행되면 이전 설치 프로그램을 다시 시작할지 여부를 묻는 메시지가 표시될 수 있습니다.
 - 설치를 다시 시작하지 않으려면 아니요를 나타내는 1을 입력합니다. 기본값은 1입니다.
 - 설치를 다시 시작하려면 예를 나타내는 2를 입력합니다.설치를 다시 시작하기 전에 서비스 유효성을 검사해야 합니다.

설치 로그 파일 문제 해결

다음 로그 파일을 사용하여 Informatica 설치 관련 문제를 해결할 수 있습니다.

설치 로그 파일

설치 프로그램은 설치 도중 및 이후에 로그 파일을 생성합니다. 이러한 로그를 사용하면 설치 프로그램에 의해 완료된 태스크 및 설치 중에 발생한 오류에 대해 자세한 정보를 얻을 수 있습니다. 설치 로그 파일에는 다음 로그가 포함됩니다.

- 디버그 로그
- 파일 설치 로그

서비스 관리자 로그 파일

서비스 관리자가 노드에서 시작될 때 생성되는 로그 파일입니다.

디버그 로그 파일

설치 프로그램은 작업 및 오류를 디버그 로그 파일에 씁니다. 로그 파일의 이름은 설치한 Informatica 구성 요소에 따라 달라집니다.

디버그 로그에는 도메인, 노드 및 응용 프로그램 서비스를 작성하는 데 사용되는 `infacmd` 및 `infasetup` 명령의 출력이 포함됩니다. 또한 응용 프로그램 서비스 시작에 대한 정보도 포함됩니다.

다음 테이블에는 디버그 로그 파일의 속성이 설명되어 있습니다.

속성	설명
로그 파일 이름	<ul style="list-style-type: none">- Informatica_<버전>_Services_<타임스탬프>.log- Informatica_<Version>_Client_<timestamp>.log- Informatica_<Version>_Services_Upgrade_<timestamp>.log- Informatica_<Version>_Client_Upgrade_<timestamp>.log
위치	설치 디렉터리입니다.
사용	설치 프로그램에 의해 수행된 작업 및 설치 오류에 대한 자세한 정보를 얻습니다. 설치하는 동안 설치 프로그램에서 정보를 이 파일에 씁니다. 설치 프로그램에서 오류가 발생하면 이 로그를 사용하여 오류를 해결할 수 있습니다.
콘텐츠	설치 프로그램에 의해 수행되는 각 작업에 대한 자세한 요약, 설치 프로그램에 입력한 정보, 설치 프로그램에 의해 사용되는 각 명령줄 명령 및 해당 명령에 의해 반환되는 오류 코드입니다.

파일 설치 로그 파일

파일 설치 로그 파일에는 설치된 파일에 대한 정보가 포함됩니다.

다음 테이블에는 설치 로그 파일의 속성이 설명되어 있습니다.

속성	설명
로그 파일 이름	<ul style="list-style-type: none">- Informatica_<버전>_Services_InstallLog.log- Informatica_<버전>_Client_InstallLog.log
위치	설치 디렉터리입니다.
사용	설치된 파일과 작성된 레지스트리 항목에 대한 정보를 가져옵니다.
콘텐츠	생성된 디렉터리, 설치된 파일과 실행된 명령의 이름 및 설치된 각 파일의 상태입니다.

서비스 관리자 로그 파일

설치 프로그램은 Informatica 서비스를 시작하고, Informatica 서비스는 해당 노드의 서비스 관리자를 시작합니다. 서비스 관리자는 노드의 시작 상태를 나타내는 로그 파일을 생성합니다. Informatica 서비스가 시작되지 않고 Informatica Administrator에 로그인할 수 없는 경우 문제를 해결하려면 이 파일을 사용하십시오. 서비스 관리자 로그 파일은 각 노드에서 작성됩니다.

다음 테이블에는 서비스 관리자에 의해 생성되는 파일이 설명되어 있습니다.

속성	설명
catalina.out	서비스 관리자를 실행하는 JVM(Java Virtual Machine)의 로그 이벤트입니다. 예를 들어 설치 중에 사용 가능했던 포트가 서비스 관리자 시작 시에 이미 사용되고 있을 수 있습니다. 서비스 관리자를 시작하는 동안 사용할 수 없었던 포트에 대한 자세한 정보를 얻으려면 이 로그를 사용하십시오. catalina.out 파일은 다음 디렉터리에 있습니다. <Informatica 설치 디렉터리>/logs/<노드 이름>/catalina.out
node.log	노드에서 서비스 관리자를 시작하는 중에 생성된 로그 이벤트입니다. 이 로그를 사용하면 노드의 서비스 관리자가 시작하지 못한 이유에 대한 자세한 정보를 얻을 수 있습니다. 예를 들어 30초가 지난 후에도 서비스 관리자가 도메인 구성 데이터베이스에 연결되지 않으면 서비스 관리자가 시작되지 않습니다. node.log 파일은 /tomcat/logs 디렉터리에 있습니다.

참고: 서비스 관리자는 로그 관리자를 사용할 수 없는 경우에도 **node.log**를 사용하여 이벤트를 기록합니다. 예를 들어 서비스 관리자가 실행되는 시스템에서 사용 가능한 디스크 공간이 부족하여 로그 이벤트 파일을 쓸 수 없으면 로그 관리자를 사용할 수 없게 됩니다.

도메인 및 노드 문제 해결

Informatica를 설치하는 동안 도메인 및 노드를 작성하고 구성하는 경우 설치 프로그램에서 오류가 발생할 수 있습니다.

도메인 구성 리포지토리 작성

도메인을 작성하는 경우, 설치 프로그램은 도메인 메타데이터 저장을 위한 도메인 구성 리포지토리를 작성합니다. 설치 프로그램은 설치 중에 입력한 옵션을 사용하여 구성 메타데이터를 도메인 구성 리포지토리에 추가합니다. 설치 프로그램은 데이터베이스와 통신하기 위해 JDBC를 사용합니다. 따라서 Informatica 서비스를 설치하는 시스템에서 ODBC 또는 원시 연결을 구성할 필요는 없습니다.

설치 프로그램은 연결 정보를 확인하기 위해 도메인 구성 리포지토리 데이터베이스에 테이블을 작성하고 삭제합니다. 이 데이터베이스의 사용자 계정에는 해당 데이터베이스에 대한 작성 권한이 있어야 합니다. 각 도메인은 별도의 도메인 구성 리포지토리를 가져야 합니다.

도메인 생성 또는 가입

설치 프로그램은 도메인을 생성하는지 아니면 도메인에 가입하는지에 따라 서로 다른 태스크를 완료합니다.

- **도메인 생성.** 설치 프로그램은 `infasetup DefineDomain` 명령을 실행하여 도메인 구성 창에서 입력되는 정보에 따라 도메인 및 해당 도메인의 게이트웨이 노드를 현재 시스템에 생성합니다.
- **도메인에 가입.** 설치 프로그램은 `infasetup DefineWorkerNode` 명령을 실행하여 현재 시스템에 노드를 생성하고 `infacmd AddDomainNode` 명령을 실행하여 도메인에 노드를 추가합니다. 설치 프로그램은 도메인 구성 창에 입력한 정보를 사용하여 명령을 실행합니다.

게이트웨이 노드를 사용할 수 없으면 `infasetup` 및 `infacmd` 명령이 실패하게 됩니다. 게이트웨이 노드를 사용할 수 없는 경우 Informatica Administrator에 로그인할 수 없습니다.

예를 들어 연결 테스트를 클릭하여 연결 테스트를 통과했지만 다음을 클릭하기 전에 데이터베이스를 사용할 수 없게 되면 `DefineDomain` 명령이 실패합니다. 또한 호스트 이름 또는 IP 주소가 현재 시스템에 속하지 않는 경우

에도 DefineDomain 명령이 실패할 수 있습니다. 도메인 구성을 위해 지정된 데이터베이스를 사용할 수 있고 호스트 이름이 올바른지 확인한 후 다시 시도하십시오.

AddDomainNode 명령이 실패한 경우 게이트웨이 노드에서 Informatica 서비스가 실행 중인지 확인하고 다시 시도하십시오.

Informatica 시작

설치 프로그램은 infaservice를 실행하여 Informatica 서비스를 시작합니다. Informatica가 시작되지 못할 경우 문제를 해결하려면 설치 디버그 로그와 node.log 및 catalina.out 서비스 관리자 로그 파일에 있는 정보를 사용하여 오류 원인을 식별하십시오.

도메인을 작성하는 경우 Informatica 서비스 시작 이후에 Informatica Administrator에 로그인하여 도메인을 사용할 수 있는지 확인하십시오. 도메인에 가입하는 경우 Informatica 서비스 시작 이후에 Informatica Administrator에 로그인하여 노드가 성공적으로 작성되고 시작되었는지 확인하십시오.

Informatica는 다음과 같은 이유로 인해 시작되지 못할 수 있습니다.

- **서비스 관리자의 시스템 메모리가 부족합니다.** Informatica를 시작하고 서비스 관리자를 실행하는 JRE(Java Runtime Environment)가 시스템 메모리 부족으로 인해 시작되지 못할 수 있습니다. INFA_JAVA_OPTS 환경 변수를 설정하여 Informatica에 의해 사용되는 시스템 메모리의 양을 구성하십시오. UNIX에서는 Informatica를 시작할 때 메모리 구성을 설정할 수 있습니다.
- **도메인 구성 데이터베이스를 사용할 수 없습니다.** 게이트웨이 노드의 서비스 관리자가 30초 이내에 도메인 구성 데이터베이스에 연결되지 않으면 Informatica가 노드에서 시작되지 않습니다. 도메인 구성 리포지토리를 사용할 수 있는지 확인하십시오.
- **Informatica 설치 디렉터리의 일부 폴더에 적절한 실행 권한이 없습니다.** Informatica 설치 디렉터리에 실행 권한을 부여합니다.

도메인에 Ping 수행

설치 프로그램은 설치를 계속하기 전에 infacmd Ping 명령을 실행하여 도메인을 사용할 수 있는지 확인합니다. 라이선스 개체가 도메인에 추가되려면 해당 도메인을 사용할 수 있어야 합니다. Ping 명령이 실패하면 게이트웨이 노드에서 Informatica를 시작하십시오.

라이선스 추가

설치 프로그램은 infacmd AddLicense 명령을 실행하여 Informatica 라이선스 키 파일을 읽고 라이선스 개체를 도메인에 생성합니다. Informatica Administrator에서 응용 프로그램 서비스를 실행하려면 유효한 라이선스 개체가 도메인에 있어야 합니다.

충분 라이선스를 사용하고 도메인에 가입하는 경우, 충분 라이선스의 일련 번호는 도메인에 있는 기존 라이선스 개체의 일련 번호와 일치해야 합니다. 일련 번호가 일치하지 않으면 AddLicense 명령이 실패하게 됩니다.

설치에 사용된 라이선스 키 파일의 일련 번호, 버전, 만료 날짜, 운영 체제 및 연결 옵션 같은 콘텐츠에 대한 자세한 정보는 설치 디버그 로그에서 얻을 수 있습니다. 도메인의 기존 라이선스에 대한 자세한 정보는 Informatica Administrator에서 얻을 수 있습니다.

Informatica Developer 문제 해결

Informatica Developer로 작업할 때 다음 팁을 고려하십시오.

Informatica Developer 시작 실패

이 문제는 Java의 jvm.dll에 MSVCR100.dll이 필요한 경우 발생할 수 있습니다.

이 문제를 해결하려면 Microsoft 웹 사이트에서 Microsoft Visual C++ Studio 2010 재배포 가능 패키지를 다운로드하십시오.

파트 IV: 서비스를 설치한 후에

이 파트에 포함된 장:

- [도메인 구성 완료, 239](#)
- [응용 프로그램 서비스를 작성하기 위한 준비, 244](#)
- [응용 프로그램 서비스 생성 및 구성, 253](#)

제 12 장

도메인 구성 완료

이 장에 포함된 항목:

- [도메인 구성 완료 검사 목록, 239](#)
- [도메인 구성 완료 개요, 239](#)
- [로컬 설정 및 코드 페이지 호환성 확인, 240](#)
- [UNIX 또는 Linux에서 환경 변수 구성, 241](#)

도메인 구성 완료 검사 목록

이 장에는 설치 후에 완료해야 하는 도메인 구성 태스크에 대한 정보가 포함되어 있습니다. 도메인 구성 태스크를 추적하는 데 이 검사 목록을 사용하십시오.

- 로컬 설정 및 코드 페이지 호환성을 확인합니다.
 - 도메인 구성 데이터베이스가 도메인에 작성한 응용 프로그램 서비스의 코드 페이지와 호환되는지 확인합니다.
 - Administrator 도구 및 Informatica 클라이언트 도구에 액세스하는 시스템의 로컬 설정이 도메인에 있는 리포지토리의 코드 페이지와 호환되는지 확인합니다.
 - 로컬 환경 변수를 구성합니다.
- 다음 환경 변수를 구성합니다.
 - 메모리, 도메인 및 위치 설정을 저장하기 위한 Informatica 환경 변수
 - 데이터 통합 서비스를 실행하는 시스템에 있는 라이브러리 경로 환경 변수
 - Kerberos 환경 변수(Kerberos 인증을 통해 네트워크에서 실행되도록 Informatica 도메인을 구성하는 경우)

도메인 구성 완료 개요

Informatica 서비스를 설치한 후 응용 프로그램 서비스를 작성하기 전에 도메인 서비스 구성을 완료하십시오. 도메인 구성에는 코드 페이지 확인, 도메인에 대한 환경 변수 구성 및 방화벽 구성 등의 태스크가 포함됩니다.

로캘 설정 및 코드 페이지 호환성 확인

응용 프로그램 서비스의 코드 페이지는 도메인의 코드 페이지와 호환되어야 합니다.

로캘 설정 및 코드 페이지를 확인하고 구성하십시오.

도메인 구성 데이터베이스가 도메인에 작성한 응용 프로그램 서비스의 코드 페이지와 호환되는지 확인합니다.

서비스 관리자는 도메인의 사용자 목록을 각 응용 프로그램 서비스의 사용자 및 그룹 목록과 동기화합니다. 도메인의 사용자 이름에 응용 프로그램 서비스의 코드 페이지에서 인식하지 못하는 문자가 있으면 문자가 올바르게 변환되지 않고 불일치가 발생합니다.

Administrator 도구 및 Informatica 클라이언트 도구에 액세스하는 시스템의 로캘 설정이 도메인에 있는 리포지토리의 코드 페이지와 호환되는지 확인합니다.

로캘 설정이 리포지토리 코드 페이지와 호환되지 않으면 응용 프로그램 서비스를 작성할 수 없습니다.

로캘 환경 변수 구성

로캘 설정이 리포지토리의 코드 페이지와 호환 가능한지 확인하십시오. 로캘 설정이 리포지토리 코드 페이지와 호환되지 않으면 응용 프로그램 서비스를 생성할 수 없습니다.

UNIX 또는 Linux 코드 페이지를 설정하려면 LANG, LC_CTYPE 또는 LC_ALL을 사용하십시오.

운영 체제 유형별로 동일한 로캘에 대해 서로 다른 값을 필요로 합니다. 로캘 변수의 값은 대/소문자를 구분합니다.

다음 명령을 사용하여 로캘 환경 변수의 값이 리포지토리에 사용할 코드 페이지의 유형 및 시스템에 대한 언어 설정과 호환되는지 확인하십시오.

```
locale -a
```

이 명령은 운영 체제에 설치된 언어와 기존 로캘 설정을 반환합니다.

다음 로캘 환경 변수를 설정하십시오.

Linux에서의 로캘

Linux를 제외한 모든 UNIX 운영 체제에는 각 로캘에 대한 고유한 값이 있습니다. Linux에서는 같은 로캘을 나타내는 여러 값을 허용합니다. 예를 들어 “utf8”, “UTF-8”, “UTF8” 및 “utf-8”은 Linux 시스템에서 같은 로캘을 나타냅니다. Informatica는 Linux 시스템에서 각 로캘에 대한 특정 값을 사용하도록 요구합니다. 모든 Linux 시스템에 대해 LANG 환경 변수를 적절하게 설정해야 합니다.

Oracle 데이터베이스 클라이언트의 로캘

Oracle 데이터베이스 클라이언트의 경우 로그인할 때 데이터베이스 클라이언트와 서버가 사용할 로캘로 NLS_LANG를 설정하십시오. 로캘 설정은 언어, 지역 및 문자 집합으로 구성되어 있습니다. NLS_LANG의 값은 구성에 따라 다릅니다.

예를 들어 이 값이 american_america.UTF8인 경우 다음 명령으로 C 셸에서 변수를 설정하십시오.

```
setenv NLS_LANG american_america.UTF8
```

데이터베이스에서 다중 바이트 문자를 읽으려면 다음 명령을 사용하여 변수를 설정하십시오.

```
setenv NLS_LANG=american_america.AL32UTF8
```

데이터 통합 서비스가 Oracle 데이터를 올바르게 읽을 수 있도록 데이터 통합 서비스 시스템에 올바른 변수를 설정해야 합니다.

UNIX 또는 Linux에서 환경 변수 구성

Informatica는 응용 프로그램 서비스를 실행하고 클라이언트에 연결할 때 환경 변수를 사용하여 구성 정보를 저장합니다. Informatica 요구 사항을 충족하도록 환경 변수를 구성하십시오.

환경 변수가 잘못 구성되면 Informatica 도메인이나 노드가 시작되지 못하거나 Informatica 클라이언트 및 도메인 간에 연결 문제가 발생할 수 있습니다.

환경 변수를 구성하려면 Informatica를 설치하는 데 사용한 시스템 사용자 계정으로 로그인해야 합니다.

Informatica 환경 변수 구성

메모리, 도메인 및 위치 설정을 저장하기 위한 Informatica 환경 변수를 구성할 수 있습니다.

다음 환경 변수를 설정하십시오.

INFA_JAVA_OPTS

기본적으로 Informatica에서는 최대 512MB의 시스템 메모리를 사용합니다.

다음 테이블에는 도메인의 사용자 및 서비스 수에 따른 최대 힙 크기 설정에 대한 최소 요구 사항이 나열되어 있습니다.

도메인 사용자 수	최대 힙 크기 (1~5개 서비스)	최대 힙 크기 (6~10개 서비스)
1,000명 미만	512MB(기본값)	1024MB
5,000	2048MB	3072MB
10,000	3072MB	5120MB
20,000	5120MB	6144MB
30,000	5120MB	6144MB

참고: 이 테이블의 최대 힙 크기 설정은 도메인의 응용 프로그램 서비스 수에 따른 것입니다.

도메인에 1,000명 이상의 사용자가 있는 경우 도메인의 사용자 수를 기반으로 최대 힙 크기를 업데이트하십시오.

INFA_JAVA_OPTS 환경 변수를 사용하여 Informatica에 의해 사용되는 시스템 메모리의 양을 구성할 수 있습니다. 예를 들어 C 셸에서 Informatica 데몬에 대해 1GB의 시스템 메모리를 구성하려면 다음 명령을 사용하십시오.

```
setenv INFA_JAVA_OPTS "-Xmx1024m"
```

변경 사항이 적용되도록 노드를 다시 시작하십시오.

INFA_DOMAINS_FILE

설치 프로그램이 Informatica 설치 디렉터리에 domains.inf 파일을 작성합니다. domains.inf 파일에는 도메인 이름, 도메인 호스트 이름 및 도메인 호스트 포트 번호를 비롯한 도메인의 게이트웨이 노드에 대한 연결 정보가 포함되어 있습니다.

INFA_DOMAINS_FILE 변수의 값을 domains.inf 파일의 경로 및 파일 이름으로 설정하십시오.

Informatica 서비스를 설치하는 시스템에 INFA_DOMAINS_FILE 변수를 구성하십시오.

INFA_HOME

INFA_HOME을 사용하여 Informatica 설치 디렉터리를 지정하십시오. Informatica 디렉터리 구조를 수정하는 경우 Informatica 설치 디렉터리 또는 설치된 Informatica 파일이 있는 디렉터리의 위치로 환경 변수를 설정해야 합니다.

예를 들어 모든 Informatica 디렉터리에 대해 소프트링크를 사용합니다. 모든 Informatica 응용 프로그램이나 서비스에서 실행해야 하는 기타 Informatica 구성 요소를 찾을 수 있도록 INFA_HOME을 구성하려면 INFA_HOME을 Informatica 설치 디렉터리 위치로 설정하십시오.

INFA_TRUSTSTORE

도메인에 대한 보안 통신을 활성화하는 경우, SSL 인증서의 트러스트 저장소 파일을 포함하는 디렉터리로 INFA_TRUSTSTORE 변수를 설정하십시오. 이 디렉터리에는 `infa_truststore.jks` 및 `infa_truststore.pem`이라는 트러스트 저장소 파일이 포함되어 있어야 합니다.

Informatica에 의해 제공되는 기본 SSL 인증서 또는 사용자 자신이 제공한 인증서를 사용할 경우 INFA_TRUSTSTORE 변수를 설정해야 합니다.

INFA_TRUSTSTORE_PASSWORD

도메인에 대한 보안 통신을 활성화하고 사용할 SSL 인증서를 지정하는 경우, 해당 SSL 인증서를 포함하는 `infa_truststore.jks`의 암호로 INFA_TRUSTSTORE_PASSWORD 변수를 설정하십시오. 이 암호는 암호화되어야 합니다. 명령줄 프로그램 `pmpasswd`를 사용하여 암호를 암호화하십시오.

라이브러리 경로 환경 변수 구성

데이터 통합 서비스 프로세스를 실행하는 시스템에 라이브러리 경로 환경 변수를 구성합니다. 변수 이름 및 요구 사항은 플랫폼 및 데이터베이스에 따라 달라집니다.

LD_LIBRARY_PATH 환경 변수를 구성합니다.

다음 테이블에는 데이터베이스별로 LD_LIBRARY_PATH에 대해 설정하는 값이 설명되어 있습니다.

데이터베이스	값
Oracle	<데이터베이스 경로>/lib
IBM DB2	<데이터베이스 경로>/lib
Sybase ASE	"\${SYBASE_OCS}/lib:\${SYBASE_ASE}/lib:\${LD_LIBRARY_PATH}"
Informix	<데이터베이스 경로>/lib
Teradata	<데이터베이스 경로>/lib
ODBC	<CLOSEDODBCHOME>/lib
PostgreSQL	\$PGHOME/lib:\${LD_LIBRARY_PATH}

Kerberos 환경 변수 구성

Kerberos 인증을 통해 네트워크에서 실행되도록 Informatica 도메인을 구성하는 경우, Kerberos 구성 및 자격 증명 캐시 환경 변수를 설정해야 합니다.

다음 환경 변수를 설정하십시오.

KRB5_CONFIG

Kerberos 구성 파일의 경로 및 파일 이름을 저장하려면 KRB5_CONFIG 환경 변수를 사용합니다. Kerberos 구성 파일의 이름은 *krb5.conf*입니다. Informatica 도메인의 각 노드에서 KRB5_CONFIG 환경 변수를 설정해야 합니다.

KRB5CCNAME

Kerberos 사용자 자격 증명 캐시의 경로 및 파일 이름으로 KRB5CCNAME 환경 변수를 설정합니다. Kerberos SSO(Single Sign-On)에서는 사용자 계정에 대해 Kerberos 자격 증명 캐시가 필요합니다.

사용자 자격 증명을 캐싱하는 경우 *forwardable* 옵션을 사용해야 합니다. 예를 들어 *kinit*를 사용하여 사용자 자격 증명을 가져오고 캐싱하는 경우, *-f* 옵션을 사용하여 전달 가능한 티켓을 요청해야 합니다.

제 13 장

응용 프로그램 서비스를 작성하기 위한 준비

이 장에 포함된 항목:

- [응용 프로그램 서비스 생성 준비를 위한 검사 목록, 244](#)
- [분석 서비스용 디렉터리 작성, 245](#)
- [웹 응용 프로그램 서비스에 대한 보안 연결을 위한 키 저장소 작성, 245](#)
- [Informatica Administrator에 로그인, 246](#)
- [연결 작성, 247](#)

응용 프로그램 서비스 생성 준비를 위한 검사 목록

이 장에는 분석 서비스, 데이터 통합 서비스 및 콘텐츠 관리 서비스를 생성하거나 구성하기 전에 완료해야 하는 태스크가 포함되어 있습니다. 서비스를 구성하는 경우, 생성하는 연결 및 디렉터리에 기반하여 속성을 구성해야 합니다. 구성 태스크를 추적하는 데 이 검사 목록을 사용하십시오.

- 분석 서비스에 대해 다음 디렉터리를 생성합니다.
 - 플랫폼 파일 캐시
 - 임시 비즈니스 용어집 파일
 - 용어집 자산
- 데이터 통합 서비스에 대해 다음 연결을 생성합니다.
 - 데이터 개체 캐시 데이터베이스
 - 워크플로우 데이터베이스
 - 프로파일링 웨어하우스
- 콘텐츠 관리 서비스에 대해 다음 연결을 생성합니다.
 - 참조 데이터 웨어하우스

분석 서비스용 디렉터리 작성

분석 서비스를 작성하기 전에 **Analyst** 도구에서 임시 파일을 저장할 디렉터리를 작성해야 합니다.

다음 디렉터리는 분석 서비스가 실행되는 노드에 작성합니다.

플랫 파일 캐시 디렉터리

Analyst 도구가 업로드된 플랫 파일을 저장하는 플랫 파일 캐시의 디렉터리를 작성합니다. 데이터 통합 서비스에서도 이 디렉터리에 액세스할 수 있어야 합니다. 분석 서비스와 데이터 통합 서비스가 서로 다른 노드에서 실행되는 경우에는 공유 디렉터리를 사용하도록 플랫 파일 디렉터리를 구성합니다. 데이터 통합 서비스가 기본 및 백업 노드 또는 그리드에서 실행되는 경우에는 각 데이터 통합 서비스 프로세스가 공유 디렉터리의 파일에 액세스할 수 있어야 합니다.

예를 들어 모든 분석 서비스 및 데이터 통합 서비스 프로세스가 액세스할 수 있는 "flatfilecache"라는 디렉터리를 다음 매핑된 드라이브에 작성할 수 있습니다.

```
F:\shared\<<Informatica installation directory>\server
```

참조 테이블 또는 플랫 파일 소스를 가져올 경우, **Analyst** 도구는 이 디렉터리에 있는 파일을 사용하여 참조 테이블 또는 플랫 파일 데이터 개체를 작성합니다.

임시 내보내기 파일 디렉터리

비즈니스 용어집 내보내기 프로세스가 작성하는 임시 비즈니스 용어집 파일을 저장할 디렉터리를 작성합니다. 분석 서비스를 실행하는 노드에 디렉터리를 작성합니다.

예를 들어 "exportfiledirectory"라는 디렉터리를 다음 위치에 작성할 수 있습니다.<Informatica 설치 디렉터리>/server

자산 첨부 파일 디렉터리

콘텐츠 관리자가 용어집 자산에 첨부 파일을 추가하는 파일을 저장할 디렉터리를 작성합니다. 분석 서비스를 실행하는 노드에 디렉터리를 작성합니다.

예를 들어 "attachmentdirectory"라는 디렉터리를 다음 위치에 작성할 수 있습니다.<Informatica 설치 디렉터리>/server

웹 응용 프로그램 서비스에 대한 보안 연결을 위한 키 저장소 작성

Informatica 도메인과 분석 서비스 같은 웹 응용 프로그램 서비스 간 연결의 보안을 유지할 수 있습니다. **Informatica**에서는 네트워크 트래픽을 암호화하기 위해 **SSL/TLS** 프로토콜을 사용합니다. 연결의 보안을 유지하려면 필요한 파일을 작성해야 합니다.

웹 응용 프로그램 서비스에 대한 연결의 보안을 유지하려면 먼저 다음 요구 사항이 충족되었는지 확인합니다.

CSR(인증서 서명 요청)과 개인 키를 작성했습니다.

keytool 또는 OpenSSL을 사용하여 CSR과 개인 키를 작성할 수 있습니다.

RSA 암호화를 사용하는 경우 512비트를 초과하여 사용해야 합니다.

서명된 SSL 인증서가 있습니다.

인증서는 자체 서명되었거나 CA에서 서명했을 수 있습니다. **Informatica**는 CA 서명 인증서를 권장합니다.

인증서를 JKS 형식의 키 저장소로 가져왔습니다.

키 저장소에는 하나의 인증서만 포함되어 있어야 합니다. 각 웹 응용 프로그램 서비스에 대해 고유한 인증서를 사용하는 경우 각 인증서에 대해 별도의 키 저장소를 작성합니다. 또는 공유 인증서 및 키 저장소를 사용할 수 있습니다.

Administrator 도구에 대해 설치 프로그램에서 생성한 SSL 인증서를 사용하는 경우 인증서를 JKS 형식의 키 저장소로 가져올 필요가 없습니다.

키 저장소가 액세스 가능한 디렉터리에 있습니다.

키 저장소는 Administrator 도구에서 액세스할 수 있는 디렉터리에 있어야 합니다.

Informatica Administrator에 로그인

Informatica Administrator 웹 응용 프로그램에 로그인하려면 사용자 계정이 있어야 합니다.

Informatica 도메인이 Kerberos 인증을 사용하는 네트워크에서 실행되는 경우 Informatica 웹 응용 프로그램에 대한 액세스를 허용하도록 브라우저를 구성해야 합니다. Microsoft Internet Explorer, Microsoft Edge 및 Google Chrome에서 Informatica 웹 응용 프로그램의 URL을 신뢰할 수 있는 사이트의 목록에 추가합니다. Safari에서 Informatica 웹 응용 프로그램의 인증서를 키체인에 추가합니다. Windows에서 Chrome 버전 86.0.42x 이상을 사용 중인 경우 AuthServerWhitelist 및 AuthNegotiateDelegateWhitelist 정책도 설정해야 합니다.

1. Microsoft Internet Explorer 또는 Google Chrome 브라우저를 시작합니다.
2. 주소 필드에 Administrator 도구의 URL을 입력합니다.
 - 보안 연결을 사용하도록 Administrator 도구가 구성되지 않은 경우 다음 URL을 입력합니다.
http://<fully qualified hostname>:<http port>/administrator/
 - 보안 연결을 사용하도록 Administrator 도구가 구성된 경우 다음 URL을 입력합니다.
https://<fully qualified hostname>:<https port>/administrator/

URL에서 호스트 이름 및 포트는 마스터 게이트웨이 노드의 호스트 이름 및 포트 번호를 나타냅니다. 도메인에 대해 보안 통신을 구성한 경우, Administrator 도구에 액세스하려면 URL에 HTTPS를 사용해야 합니다.

Kerberos 인증을 사용하면 네트워크에서 SSO(Single Sign-On)를 사용합니다. 사용자 이름 및 암호를 입력하여 Administrator 도구에 로그인하지 않아도 됩니다.

3. Kerberos 인증을 사용하지 않는 경우에는 사용자 계정의 사용자 이름, 암호 및 보안 도메인을 입력하고 **로그인**을 클릭합니다.

Informatica 도메인에 LDAP 보안 도메인이 포함된 경우 **보안 도메인** 필드가 나타납니다. 자신의 사용자 계정이 속한 보안 도메인을 알지 못하는 경우 Informatica 도메인 관리자에게 문의하십시오.

참고: 도메인 관리자가 제공한 사용자 이름 및 암호를 사용하여 처음 로그인하는 경우에는 보안을 유지할 수 있도록 암호를 변경하십시오.

Informatica Administrator 로그인 문제 해결

Informatica 도메인이 Kerberos 인증을 사용하는 경우 Administrator 도구에 로그인할 때 다음과 같은 문제가 발생할 수 있습니다.

도메인 게이트웨이 노드를 작성한 시스템에서 Administrator 도구에 로그인할 수 없습니다.

Administrator 도구를 설치한 후 도메인 게이트웨이 노드를 작성한 시스템에서 Administrator 도구에 로그인할 수 없는 경우 브라우저 캐시를 지우십시오. Administrator 도구를 설치한 후 처음 로그인하는 경우 설치 중에 작성한 Administrator 사용자 계정으로만 로그인할 수 있습니다. 브라우저 캐시에 다른 사용자 자격 증명이 저장되어 있는 경우 로그인이 실패할 수 있습니다.

Administrator 도구에 로그인한 후 빈 페이지가 나타납니다.

Administrator 도구에 로그인한 후 빈 페이지가 나타나는 경우 Informatica 도메인에 사용되는 서비스 사용자에게 모든 사용자 계정에 대한 위임을 활성화했는지 확인합니다. 위임을 활성화하려면 Microsoft Active Directory 서비스에서 SPN을 설정한 각 사용자 계정에 대해 **모든 서비스에 대한 위임용으로 이 사용자 트러스트(Kerberos만)** 옵션을 설정합니다.

연결 작성

Administrator 도구에서 응용 프로그램 서비스가 액세스하는 데이터베이스에 대한 연결을 생성합니다. 응용 프로그램 서비스를 구성하는 동안 연결 세부 정보를 지정해야 합니다.

데이터베이스 연결을 작성할 때 데이터베이스 연결 속성을 지정하고 연결을 테스트하십시오.

다음 테이블에는 응용 프로그램 서비스가 연결된 데이터베이스에 액세스하려면 먼저 생성해야 하는 데이터베이스 연결이 설명되어 있습니다.

데이터베이스 연결	설명
데이터 개체 캐시 데이터베이스	데이터 개체 캐시에 액세스하려면 데이터 통합 서비스를 위해 데이터 개체 캐시 연결을 작성합니다.
워크플로우 데이터베이스	워크플로우 런타임 메타데이터를 저장하려면 데이터 통합 서비스에 대한 워크플로우 데이터베이스 연결을 작성합니다.
프로파일링 웨어하우스 데이터베이스	프로필 및 성과 기록표를 작성 및 실행하려면 데이터 통합 서비스를 위해 프로파일링 웨어하우스 데이터베이스 연결을 작성합니다. 분석 서비스의 런타임 속성을 구성할 때 데이터 통합 서비스의 이 인스턴스를 사용합니다. 참고: Microsoft SQL Server 데이터베이스를 프로파일링 웨어하우스로 사용하려면 Microsoft SQL Server 연결을 구성할 때 Microsoft SQL Server 연결 속성 대화 상자에서 공급자 유형으로 ODBC를 선택하고 DSN 사용 옵션을 선택 취소합니다.
참조 데이터 웨어하우스	참조 테이블 데이터를 저장하려면 콘텐츠 관리 서비스에 대한 참조 데이터 웨어하우스 연결을 작성합니다.

IBM DB2 연결 속성

DB2 for LUW 데이터베이스의 테이블에 액세스하려면 DB2 for LUW 연결을 사용하십시오.

다음 테이블에는 DB2 for LUW 연결 속성이 설명되어 있습니다.

속성	설명
사용자 이름	데이터베이스 사용자 이름입니다.
암호	사용자 이름의 암호입니다.
메타데이터 액세스를 위한 연결 문자열	실제 데이터 개체를 가져오기 위한 연결 문자열입니다. 다음 연결 문자열을 사용하십시오. jdbc:informatica:db2://<호스트>:50000;databaseName=<dbname>

속성	설명
데이터 액세스를 위한 연결 문자열	데이터를 미리 보고 매핑을 실행하기 위한 연결 문자열입니다. DB2 클라이언트에 구성된 별칭의 dbname을 입력하십시오.
코드 페이지	데이터베이스 코드 페이지입니다.
환경 SQL	선택 사항입니다. 데이터베이스에 연결할 때 데이터베이스 환경을 설정하는 SQL 명령을 입력합니다. 데이터 통합 서비스에서 데이터베이스에 연결할 때마다 연결 환경 SQL을 실행합니다.
트랜잭션 SQL	선택 사항입니다. 데이터베이스에 연결할 때 데이터베이스 환경을 설정하는 SQL 명령을 입력합니다. 데이터 통합 서비스에서 각 트랜잭션을 시작할 때 트랜잭션 환경 SQL을 실행합니다.
다시 시도 기간	이 속성은 나중에 사용하기 위해 예약되어 있습니다.
테이블스페이스	DB2 for LUW 데이터베이스의 테이블스페이스 이름입니다.
SQL 식별자 문자	특수 문자 및 예약된 SQL 키워드(예: WHERE)를 식별하는 데 사용되는 문자의 유형입니다. 데이터 통합 서비스에서 특수 문자와 예약된 SQL 키워드 주변에 선택된 문자를 배치합니다. 데이터 통합 서비스에서 대/소문자가 혼합된 식별자 지원 속성에도 이 문자를 사용합니다.
대/소문자가 혼합된 식별자 지원	활성화할 경우, 연결에서 테이블, 보기, 스키마, 동의어 및 열 이름 개체에 대해 SQL을 생성 및 실행할 때 데이터 통합 서비스에서 이러한 개체 주위에 식별자 문자를 배치합니다. 개체의 이름이 대/소문자가 혼합되거나 소문자일 경우 사용합니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.

Microsoft Azure SQL Database 연결 속성

Azure SQL Data Warehouse 연결을 사용하여 Microsoft Azure SQL 데이터베이스의 테이블에 액세스합니다.

다음 테이블에는 Microsoft Azure SQL Database 연결 속성이 설명되어 있습니다.

속성	설명
Azure DW JDBC URL	Microsoft Azure SQL Database에 대한 연결 문자열입니다.
Azure DW JDBC 사용자 이름	데이터베이스 사용자 이름입니다.
Azure DW JDBC 암호	사용자 이름의 암호입니다.
Azure DW JDBC 스키마 이름	데이터베이스에 있는 스키마의 이름입니다.
Azure Storage 유형	
Azure Blob 계정 이름	
Azure Blob 계정 키	
ADLS Gen2 저장소 계정 이름	
ADLS Gen2 계정 키	

속성	설명
Blob 끝점	
VNet 규칙	

참고: Microsoft SQL Server 연결을 사용하여 Microsoft SQL Server 데이터베이스의 테이블에 액세스하면 Developer tool에서 해당 테이블의 동의어가 표시되지 않습니다.

Microsoft SQL Server 연결 속성

Microsoft SQL Server 데이터베이스의 테이블에 액세스하려면 Microsoft SQL Server 연결을 사용하십시오. 다음 테이블에는 Microsoft SQL Server 연결 속성이 설명되어 있습니다.

속성	설명
사용자 이름	데이터베이스 사용자 이름입니다.
암호	사용자 이름의 암호입니다.
트러스트된 연결 사용	선택 사항입니다. 활성화된 경우, 데이터 통합 서비스가 Windows 인증을 사용하여 Microsoft SQL Server 데이터베이스에 액세스합니다. 데이터 통합 서비스를 시작하는 사용자 이름은 Microsoft SQL Server 데이터베이스에 대한 액세스 권한을 갖는 유효한 Windows 사용자여야 합니다.
메타데이터 액세스를 위한 연결 문자열	실제 데이터 개체를 가져오기 위한 연결 문자열입니다. 다음 연결 문자열을 사용하십시오. <code>jdbc:informatica:sqlserver://<host>:<port>;databaseName=<dbname></code>
데이터 액세스를 위한 연결 문자열	데이터를 미리 보고 매핑을 실행하기 위한 연결 문자열입니다. <code><ServerName>@<DBName></code> 을 입력하십시오.
도메인 이름	선택 사항입니다. Microsoft SQL Server가 실행되는 도메인의 이름입니다.
패킷 크기	필수. ODBC 연결을 Microsoft SQL Server에 맞춰 최적화합니다. 성능을 높이려면 패킷 크기를 늘리십시오. 기본값은 0입니다.
코드 페이지	데이터베이스 코드 페이지입니다.
소유자 이름	스키마 소유자의 이름입니다. 프로파일링 웨어하우스 데이터베이스 또는 데이터 개체 캐시 데이터베이스에 대한 연결을 위해 지정합니다.
스키마 이름	데이터베이스에 있는 스키마의 이름입니다. 프로파일링 웨어하우스 또는 데이터 개체 캐시 데이터베이스에 대한 연결을 위해 지정합니다. 스키마 이름이 데이터베이스 사용자 이름과 다를 경우 프로파일링 웨어하우스에 대한 스키마 이름을 지정해야 합니다. 스키마 이름이 데이터베이스 사용자 이름과 다르고 외부 도구를 사용하여 캐시를 관리하는 경우 데이터 개체 캐시 데이터베이스의 스키마 이름을 지정해야 합니다.
환경 SQL	선택 사항입니다. 데이터베이스에 연결할 때 데이터베이스 환경을 설정하는 SQL 명령을 입력합니다. 데이터 통합 서비스에서 데이터베이스에 연결할 때마다 연결 환경 SQL을 실행합니다.

속성	설명
트랜잭션 SQL	선택 사항입니다. 데이터베이스에 연결할 때 데이터베이스 환경을 설정하는 SQL 명령을 입력합니다. 데이터 통합 서비스에서 각 트랜잭션을 시작할 때 트랜잭션 환경 SQL을 실행합니다.
다시 시도 기간	이 속성은 나중에 사용하기 위해 예약되어 있습니다.
SQL 식별자 문자	특수 문자 및 예약된 SQL 키워드(예: WHERE)를 식별하는 데 사용되는 문자의 유형입니다. 데이터 통합 서비스에서 특수 문자와 예약된 SQL 키워드 주변에 선택된 문자를 배치합니다. 데이터 통합 서비스에서 대/소문자가 혼합된 식별자 지원 속성에도 이 문자를 사용합니다.
대/소문자가 혼합된 식별자 지원	활성화할 경우, 연결에서 테이블, 보기, 스키마, 동의어 및 열 이름 개체에 대해 SQL을 생성 및 실행할 때 데이터 통합 서비스에서 이러한 개체 주위에 식별자 문자를 배치합니다. 개체의 이름이 대/소문자가 혼합되거나 소문자일 경우 사용합니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.

참고: Microsoft SQL Server 연결을 사용하여 Microsoft SQL Server 데이터베이스의 테이블에 액세스하면 Developer tool에서 해당 테이블의 동의어가 표시되지 않습니다.

Oracle 연결 속성

Oracle 데이터베이스의 테이블에 액세스하려면 Oracle 연결을 사용하십시오.

다음 테이블에는 Oracle 연결 속성이 설명되어 있습니다.

속성	설명
사용자 이름	데이터베이스 사용자 이름입니다.
암호	사용자 이름의 암호입니다.
메타데이터 액세스를 위한 연결 문자열	실제 데이터 개체를 가져오기 위한 연결 문자열입니다. 다음 연결 문자열을 사용하십시오. jdbc:informatica:oracle://<host>:1521;SID=<sid> Oracle Connection Manager를 통해 Oracle에 연결하려면 다음 연결 문자열을 사용합니다. jdbc:Informatica:oracle:TNSNamesFile=<tnsnames.ora 파일의 정규화된 경로>;TNSServerName=<TNS 서버 이름>;
데이터 액세스를 위한 연결 문자열	데이터를 미리 보고 매핑을 실행하기 위한 연결 문자열입니다. TNSNAMES 항목에 있는 dbname.world를 입력하십시오.
코드 페이지	데이터베이스 코드 페이지입니다.
환경 SQL	선택 사항입니다. 데이터베이스에 연결할 때 데이터베이스 환경을 설정하는 SQL 명령을 입력합니다. 데이터 통합 서비스에서 데이터베이스에 연결할 때마다 연결 환경 SQL을 실행합니다.
트랜잭션 SQL	선택 사항입니다. 데이터베이스에 연결할 때 데이터베이스 환경을 설정하는 SQL 명령을 입력합니다. 데이터 통합 서비스에서 각 트랜잭션을 시작할 때 트랜잭션 환경 SQL을 실행합니다.
다시 시도 기간	이 속성은 나중에 사용하기 위해 예약되어 있습니다.

속성	설명
병렬 모드	선택 사항입니다. 대량 모드에서 데이터를 테이블로 로드할 때 병렬 처리를 활성화합니다. 기본값은 비활성화됩니다.
SQL 식별자 문자	특수 문자 및 예약된 SQL 키워드(예: WHERE)를 식별하는 데 사용되는 문자의 유형입니다. 데이터 통합 서비스에서 특수 문자와 예약된 SQL 키워드 주변에 선택된 문자를 배치합니다. 데이터 통합 서비스에서 대/소문자가 혼합된 식별자 지원 속성에도 이 문자를 사용합니다.
대/소문자가 혼합된 식별자 지원	활성화할 경우, 연결에서 테이블, 보기, 스키마, 동의어 및 열 이름 개체에 대해 SQL을 생성 및 실행할 때 데이터 통합 서비스에서 이러한 개체 주위에 식별자 문자를 배치합니다. 개체의 이름이 대/소문자가 혼합되거나 소문자일 경우 사용합니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.

PostgreSQL 연결 속성

JDBC 연결을 사용하여 PostgreSQL 데이터베이스의 테이블에 액세스합니다.

다음 테이블에는 Oracle 연결 속성이 설명되어 있습니다.

속성	설명
사용자 이름	데이터베이스 사용자 이름입니다.
암호	사용자 이름의 암호입니다.
JDBC 드라이버 클래스 이름	
연결 문자열	데이터베이스의 데이터 및 메타데이터를 읽는 데 사용할 연결 문자열입니다. 다음 형식으로 연결 문자열을 정의합니다. <code>jdbc:informatica:postgresql://<host>:<port>;Database=<id></code>
환경 SQL	선택 사항입니다. 데이터베이스에 연결할 때 데이터베이스 환경을 설정하는 SQL 명령을 입력합니다. 데이터 통합 서비스에서 데이터베이스에 연결할 때마다 연결 환경 SQL을 실행합니다.
트랜잭션 SQL	선택 사항입니다. 데이터베이스에 연결할 때 데이터베이스 환경을 설정하는 SQL 명령을 입력합니다. 데이터 통합 서비스에서 각 트랜잭션을 시작할 때 트랜잭션 환경 SQL을 실행합니다.
대/소문자가 혼합된 식별자 지원	활성화한 경우 연결에서 테이블, 보기, 스키마, 동의어 및 열 이름에 대해 SQL을 생성하고 실행할 때 데이터 통합 서비스는 이러한 개체 주위에 식별자 문자를 배치합니다. 개체 이름에 대/소문자가 혼합되어 있거나 소문자 이름이 있으면 사용합니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.
SQL 식별자 문자	특수 문자 및 예약된 SQL 키워드(예: WHERE)를 식별하는 데 사용하는 문자의 유형입니다. 데이터 통합 서비스는 특수 문자 및 예약된 SQL 키워드 주위에 특정 문자를 배치합니다. 또한 데이터 통합 서비스에서는 대/소문자가 혼합된 식별자 지원 속성에 대해서도 이 문자를 사용합니다.
Sqoop 커넥터 사용	
Sqoop 인수	

연결 작성

Administrator 도구에서 관계형 데이터베이스, 소셜 미디어 및 파일 시스템 연결을 작성할 수 있습니다.

1. Administrator 도구에서 **관리** 탭을 클릭합니다.
2. **연결** 보기를 클릭합니다.
3. 탐색기에서 도메인을 선택합니다.
4. 탐색기에서 **작업 > 새로 만들기 > 연결**을 클릭합니다.
새 연결 대화 상자가 나타납니다.
5. **새 연결** 대화 상자에서 연결 유형을 선택한 다음 **확인**을 클릭합니다.
새 연결 마법사가 표시됩니다.
6. 연결 속성을 입력합니다.
입력하는 연결 속성은 연결 유형에 따라 다릅니다. **다음**을 클릭하여 **새 연결** 마법사의 다음 페이지로 이동합니다.
7. 연결 속성을 입력한 후에 **연결 테스트**를 클릭하여 연결을 테스트할 수 있습니다.
8. **마침**을 클릭합니다.

제 14 장

응용 프로그램 서비스 생성 및 구성

이 장에 포함된 항목:

- [응용 프로그램 생성 및 구성을 위한 검사 목록, 253](#)
- [응용 프로그램 서비스 생성 및 구성 개요, 253](#)
- [모델 리포지토리 서비스 작성 및 구성, 254](#)
- [데이터 통합 서비스 작성 및 구성, 259](#)
- [PowerCenter 리포지토리 서비스 작성 및 구성, 262](#)
- [PowerCenter 통합 서비스 작성 및 구성, 266](#)
- [Metadata Manager 서비스 작성 및 구성, 268](#)
- [콘텐츠 관리 서비스 작성 및 구성, 272](#)
- [분석 서비스 작성 및 구성, 274](#)
- [검색 서비스 작성 및 구성, 276](#)

응용 프로그램 생성 및 구성을 위한 검사 목록

이 장에는 응용 프로그램 서비스 생성 및 구성을 위한 지침이 포함되어 있습니다. 설치 중에 서비스를 생성했다 라도 일부 서비스를 구성해야 할 수 있습니다. 응용 프로그램 서비스 구성의 완료 여부를 추적하는 데 이 검사 목록을 사용하십시오.

- 응용 프로그램 서비스 계획을 위한 메모를 검토합니다.
- 설치 중에 생성한 서비스를 식별하고, 해당 서비스에 대한 추가적인 구성을 완료합니다.
- 도메인에 필요한 기타 서비스를 생성하고 구성합니다.

응용 프로그램 서비스 생성 및 구성 개요

설치 프로그램을 실행할 때 서비스를 생성하지 않은 경우 Administrator 도구를 사용하여 응용 프로그램 서비스를 생성합니다.

일부 응용 프로그램 서비스는 다른 응용 프로그램 서비스에 종속됩니다. 이러한 종속형 응용 프로그램 서비스를 작성하는 경우 실행되는 다른 응용 프로그램 서비스의 이름을 제공해야 합니다. 서비스를 작성해야 하는 순서를 결정하려면 응용 프로그램 서비스 종속성을 검토합니다. 예를 들어 데이터 통합 서비스를 생성하려면 먼저 모델 리포지토리 서비스를 생성해야 합니다.

응용 프로그램 서비스를 작성하기 전에는 설치 및 구성 프로세스에 따라 요구되는 선행 조건 태스크를 완료했는지 확인합니다.

모델 리포지토리 서비스 작성 및 구성

모델 리포지토리 서비스는 모델 리포지토리를 관리하는 응용 프로그램 서비스입니다. 모델 리포지토리는 Informatica 클라이언트 및 응용 프로그램 서비스에서 작성한 메타데이터를 관계형 데이터베이스에 저장하여 클라이언트와 서비스 간의 협업을 가능하게 합니다.

Informatica 클라이언트 도구 또는 응용 프로그램 서비스에서 모델 리포지토리 개체에 액세스하는 경우, 해당 클라이언트 또는 서비스가 모델 리포지토리 서비스로 요청을 보냅니다. 모델 리포지토리 서비스 프로세스는 모델 리포지토리 데이터베이스 테이블에서 메타데이터를 가져오고, 삽입하고, 업데이트합니다.

모델 리포지토리 서비스 생성

Administrator 도구에서 서비스 작성 마법사를 사용하여 서비스를 작성합니다.

- Administrator 도구에서 **관리** 탭을 클릭합니다.
- 작업 > 새로 만들기 > **모델 리포지토리 서비스**를 클릭합니다.
새 모델 리포지토리 서비스 대화 상자가 나타납니다.
- 새 모델 리포지토리 서비스 - 1/2단계 페이지에서 다음 속성을 입력합니다.

속성	설명
이름	서비스의 이름입니다. 이름은 대/소문자를 구분하지 않으며 도메인 내에서 고유해야 합니다. 이름은 128자를 초과하거나 @로 시작할 수 없습니다. 또한 공백이나 다음과 같은 특수 문자를 포함할 수도 없습니다. ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
설명	서비스에 대한 설명. 설명은 765자를 초과할 수 없습니다.
위치	서비스가 작성되는 도메인 및 폴더입니다. 다른 폴더를 선택하려면 찾아보기 를 클릭합니다. 서비스를 작성한 후 이동할 수 있습니다.
라이선스	서비스를 사용할 수 있도록 해주는 라이선스 개체입니다.
노드	서비스가 실행되는 노드입니다.
백업 노드	라이선스에 고가용성이 포함된 경우, 기본 노드를 사용할 수 없을 때 서비스가 실행될 수 있는 노드입니다.

- 다음을 클릭합니다.
새 모델 리포지토리 서비스 - 2/2단계 페이지가 나타납니다.

5. 모델 리포지토리 데이터베이스에 대한 다음 속성을 입력합니다.

속성	설명
데이터베이스 유형	리포지토리 데이터베이스의 유형입니다.
사용자 이름	리포지토리에 대한 데이터베이스 사용자 이름입니다. 신뢰할 수 있는 Microsoft SQL Server 연결을 위해 Windows NT 사용자 이름을 입력할 수 있습니다.
암호	데이터베이스 사용자에게 대한 리포지토리 데이터베이스 암호입니다. 신뢰할 수 있는 Microsoft SQL Server 연결을 위해 Windows NT 암호를 입력할 수 있습니다.
데이터베이스 스키마	Microsoft SQL Server 및 PostgreSQL에 사용할 수 있습니다. 모델 리포지토리 테이블이 포함될 스키마의 이름입니다.
데이터베이스 테이블스페이스	IBM DB2에 사용할 수 있습니다. 테이블이 생성될 테이블스페이스의 이름입니다. 다중 파티션 IBM DB2 데이터베이스의 경우 테이블스페이스에는 노드 하나와 파티션 하나가 포함되어야 합니다.

6. 서비스가 모델 리포지토리 데이터베이스에 연결하는 데 사용하는 JDBC 연결 문자열을 입력합니다.

선택한 데이터베이스 유형에 대해 다음과 같은 연결 문자열 구문을 사용합니다.

데이터베이스 유형	연결 문자열 구문
IBM DB2	"jdbc:informatica:db2://<호스트 이름>:<포트 번호>;DatabaseName=<데이터베이스 이름>;BatchPerformanceWorkaround=true;DynamicSections=3000"
Microsoft SQL Server	<ul style="list-style-type: none"> - 기본 인스턴스를 사용하는 Microsoft SQL Server "jdbc:informatica:sqlserver://<호스트 이름>:<포트 번호>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true" - 명명된 인스턴스를 사용하는 Microsoft SQL Server "jdbc:informatica:sqlserver://<호스트 이름>\<명명된 인스턴스 이름>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true" - Microsoft Azure. jdbc:informatica:sqlserver://<host_name>:<port_number>;DatabaseName=<database_name>;SnapshotSerializable=true;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.<hostnameincertificate>;ValidateServerCertificate=true - Active Directory 인증을 사용하는 Azure SQL Database. "jdbc:informatica:sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostnameInCertificate=*.database.windows.net;loginTimeout=<seconds>" <p>참고: Microsoft SQL Server에서 모델 리포지토리 데이터베이스에 대한 Windows NT 자격 증명을 지정한 경우 NTLM을 인증 방법으로 포함하도록 연결 문자열 구문을 지정합니다.</p> <ul style="list-style-type: none"> - Windows NT 자격 증명에 있는 기본 인스턴스를 사용하는 Microsoft SQL Server: "jjdbc:informatica:sqlserver://<호스트 이름>:<포트 번호>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;authenticationMethod=NTLM" - Windows NT 자격 증명에 있는 명명된 인스턴스를 사용하는 Microsoft SQL Server: "jjdbc:informatica:sqlserver://<호스트 이름>\<명명된 인스턴스 이름>;DatabaseName=<데이터베이스 이름>;SnapshotSerializable=true;authenticationMethod=NTLM"
Oracle	"jdbc:informatica:oracle://<호스트 이름>:<포트 번호>;SID=<데이터베이스 이름>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true"
PostgreSQL	"jdbc:informatica:postgresql://<호스트 이름>:<포트 번호>;DatabaseName= "

7. 모델 리포지토리 데이터베이스를 SSL 프로토콜로 보안하는 경우 **보안 JDBC 매개 변수** 필드에 보안 데이터베이스 매개 변수를 입력해야 합니다.

세미콜론 문자(;)로 구분된 이름=값 쌍으로 매개 변수를 입력합니다. 예:

```
param1=value1;param2=value2
```

다음 보안 데이터베이스 매개 변수를 입력하십시오.

보안 데이터베이스 매개 변수	설명
EncryptionMethod	필수 사항입니다. 네트워크를 통해 전송되는 경우 데이터가 암호화되었는지를 나타냅니다. 이 매개 변수는 SSL로 설정되어야 합니다.
ValidateServerCertificate	선택 사항입니다. Informatica가 데이터베이스 서버에서 보낸 인증서에 대해 유효성을 검사하는지 여부를 나타냅니다. 이 매개 변수를 True로 설정하면 데이터베이스 서버에서 보낸 인증서에 대해 Informatica에서 유효성을 검사합니다. HostNameInCertificate 매개 변수를 지정하면 Informatica에서 인증서의 호스트 이름에 대한 유효성도 검사합니다. 이 매개 변수를 False로 설정하면 데이터베이스 서버에서 보낸 인증서에 대해 Informatica에서 유효성을 검사하지 않습니다. Informatica에서 사용자가 지정한 트러스트 저장소 정보를 모두 무시합니다.
HostNameInCertificate	선택 사항입니다. 보안 데이터베이스를 호스팅하는 시스템의 호스트 이름입니다. 호스트 이름을 지정하면 Informatica에서 SSL 인증서의 호스트 이름에 대해 연결 문자열에 포함된 호스트 이름의 유효성을 검사합니다.
cryptoProtocolVersion	필수 사항입니다. 보안 데이터베이스에 연결하는 데 사용할 암호화 프로토콜을 지정합니다. 데이터베이스 서버에 사용되는 암호화 프로토콜을 기반으로 매개 변수를 cryptoProtocolVersion=TLSv1.1 또는 cryptoProtocolVersion=TLSv1.2로 설정할 수 있습니다.
TrustStore	필수 사항입니다. 데이터베이스의 SSL 인증서를 포함하는 트러스트 저장소 파일의 경로 및 파일 이름입니다. 트러스트 저장소 파일에 대한 경로가 없는 경우 Informatica는 다음 기본 디렉터리에서 파일을 찾습니다. <Informatica 설치 디렉터리>/tomcat/bin
TrustStorePassword	필수 사항입니다. 보안 데이터베이스에 대한 트러스트 저장소 파일의 암호입니다.

참고: Informatica는 보안 JDBC 매개 변수를 JDBC 연결 문자열에 추가합니다. 보안 JDBC 매개 변수를 직접 연결 문자열에 포함할 경우 **보안 JDBC 매개 변수** 필드에 매개 변수를 입력하지 마십시오.

8. **연결 테스트**를 클릭하여 데이터베이스에 연결할 수 있는지 확인합니다.
9. **지정된 연결 문자열에 콘텐츠가 없습니다. 새 콘텐츠를 작성하십시오.**를 선택합니다.
10. **마침**을 클릭합니다.

도메인이 모델 리포지토리 서비스를 생성하고, 지정된 데이터베이스에 모델 리포지토리의 콘텐츠를 생성하고, 서비스를 활성화합니다.

마법사를 통해 서비스를 작성한 후 속성을 편집하거나 다른 속성을 구성할 수 있습니다.

모델 리포지토리 서비스를 생성한 후

모델 리포지토리 서비스를 생성한 후에는 다음 태스크를 수행합니다.

- 도메인에서 Kerberos 인증을 사용하지 않는 경우 모델 리포지토리 사용자를 생성합니다.
- 다른 응용 프로그램 서비스를 생성합니다.

모델 리포지토리 사용자 작성

모델 리포지토리 서비스에 종속된 응용 프로그램 서비스를 생성하는 경우 모델 리포지토리 서비스의 이름과 이 모델 리포지토리 사용자의 이름을 제공합니다.

Kerberos 인증을 사용하지 않는 도메인에서는 모델 리포지토리 서비스에 대해 요청하는 다른 응용 프로그램 서비스를 인증하기 위해 사용자 계정을 사용합니다. 따라서 모델 리포지토리 서비스에 대해 사용자 계정을 생성하고 사용자에게 관리자 역할을 할당해야 합니다.

1. Administrator 도구에서 **보안** 탭을 클릭합니다.
2. 보안 작업 메뉴에서 **사용자 작성**을 클릭하여 원시 사용자 계정을 작성합니다.

참고: 도메인에서 LDAP 인증을 설정하려면 모델 리포지토리 사용자에게 대해 LDAP 사용자 계정을 사용하면 됩니다.

3. 사용자에게 다음 속성을 입력합니다.

속성	설명
로그인 이름	사용자 계정의 로그인 이름입니다. 사용자 계정의 로그인 이름은 해당 계정이 속한 보안 도메인 내에서 고유해야 합니다. 이름은 대/소문자를 구분하지 않으며 128자를 초과할 수 없습니다. 이름에는 탭, 줄 바꿈 문자 또는 다음과 같은 특수 문자를 사용할 수 없습니다. , + " \ < > ; / * % ? & 첫 번째 문자와 마지막 문자를 제외하고 이름에는 ASCII 공백 문자를 사용할 수 있습니다. 다른 모든 공백 문자는 사용할 수 없습니다.
암호	사용자 계정에 대한 암호입니다. 암호의 길이는 1~80자여야 합니다.
암호 확인	확인을 위해 암호를 다시 입력합니다. 암호를 수동으로 다시 입력해야 합니다. 암호를 복사해서 붙여 넣지 마십시오.
전체 이름	사용자 계정의 전체 이름입니다. 전체 이름에는 다음과 같은 특수 문자를 포함할 수 없습니다. < > “
설명	사용자 계정에 대한 설명입니다. 설명은 765자를 초과하거나 다음 특수 문자를 포함할 수 없습니다. < > “

4. **확인**을 클릭합니다.
사용자 속성이 나타납니다.
5. **권한** 탭을 클릭합니다.
6. **편집**을 클릭합니다.
역할 및 권한 편집 대화 상자가 나타납니다.
7. **역할** 탭에서 모델 리포지토리 서비스를 확장합니다.
8. **시스템 정의 역할**에서 관리자를 선택하고 **확인**을 클릭합니다.

기타 서비스 작성

모델 리포지토리 서비스를 작성한 후에는 모델 리포지토리 서비스에 종속된 응용 프로그램 서비스를 작성합니다.

종속형 서비스는 다음 순서대로 작성합니다.

1. 데이터 통합 서비스
2. 분석 서비스
3. 콘텐츠 관리 서비스
4. 검색 서비스

데이터 통합 서비스 작성 및 구성

Analyst 도구 또는 Developer tool에서 데이터 프로필, SQL 데이터 서비스 및 매핑을 미리 보거나 실행하면 해당 클라이언트 도구가 데이터 통합 서비스로 요청을 보내어 데이터 통합 작업을 수행합니다. 명령줄 프로그램 또는 외부 클라이언트에서 SQL 데이터 서비스, 매핑 및 워크플로우를 실행하면 해당 명령이 데이터 통합 서비스로 요청을 보냅니다.

데이터 통합 서비스 작성

Administrator 도구에서 서비스 작성 마법사를 사용하여 서비스를 작성합니다.

데이터 통합 서비스를 생성하기 전에 다음 서비스를 생성했는지 확인합니다:

모델 리포지토리 서비스

1. Administrator 도구에서 **관리** 탭을 클릭합니다.
2. **서비스 및 노드** 보기를 클릭합니다.
3. 도메인 탐색기에서 도메인을 선택합니다.
4. **작업 > 새로 만들기 > 데이터 통합 서비스**를 클릭합니다.
새 **데이터 통합 서비스** 마법사가 나타납니다.
5. **새 데이터 통합 서비스 - 1/14단계** 페이지에서 다음 속성을 입력합니다.

속성	설명
이름	서비스의 이름입니다. 이름은 대/소문자를 구분하지 않으며 도메인 내에서 고유해야 합니다. 이름은 128자를 초과하거나 @로 시작할 수 없습니다. 또한 공백이나 다음과 같은 특수 문자를 포함할 수도 없습니다. ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
설명	서비스에 대한 설명. 설명은 765자를 초과할 수 없습니다.
위치	서비스가 작성되는 도메인 및 폴더입니다. 다른 폴더를 선택하려면 찾아보기 를 클릭합니다. 서비스를 작성한 후 이동할 수 있습니다.
라이선스	서비스를 사용할 수 있도록 해주는 라이선스 개체입니다.

속성	설명
할당	노드에서 실행할 서비스를 구성하려면 노드 를 선택합니다. 라이선스에 그리드가 포함된 경우에는 서비스를 작성한 후 그리드를 작성하고 그리드에서 실행할 서비스를 할당할 수 있습니다.
노드	서비스가 실행되는 노드입니다.
백업 노드	라이선스에 고가용성이 포함된 경우, 기본 노드를 사용할 수 없을 때 서비스가 실행될 수 있는 노드입니다.
모델 리포지토리 서비스	서비스와 연결할 모델 리포지토리 서비스입니다.
사용자 이름	서비스가 모델 리포지토리 서비스에 액세스하는 데 필요한 사용자 이름입니다. 작성한 모델 리포지토리 사용자를 입력합니다.
암호	모델 리포지토리 사용자의 암호입니다.
보안 도메인	모델 리포지토리 사용자에 대한 LDAP 보안 도메인입니다. Informatica 도메인에 LDAP 보안 도메인이 포함된 이 필드가 나타납니다. Kerberos 인증이 있는 도메인에서는 사용할 수 없습니다.

6. 다음을 클릭합니다.

새 데이터 통합 서비스 - 2/14단계 페이지가 나타납니다.

7. 데이터 통합 서비스에 사용할 HTTP 포트 번호를 입력합니다.

8. 나머지 보안 속성에 대해 기본값을 그대로 사용합니다. 데이터 통합 서비스를 작성한 후 보안 속성을 구성할 수 있습니다.

9. **서비스 활성화**를 선택합니다.

데이터 통합 서비스를 활성화하려면 모델 리포지토리 서비스가 실행되고 있어야 합니다.

10. **플러그 인 구성 페이지로 이동**이 선택되지 않았는지 확인합니다.

11. 다음을 클릭합니다.

새 데이터 통합 서비스 - 3/14단계 페이지가 나타납니다.

12. **작업 실행 옵션** 속성을 다음 값 중 하나로 설정합니다.

- 서비스 프로세스. SQL 데이터 서비스 및 웹 서비스 작업을 실행할 때 구성합니다. 데이터 통합 서비스가 서비스 프로세스에서 작업을 실행하는 경우 일반적으로 SQL 데이터 서비스 및 웹 서비스 작업이 더 나은 성능을 구현합니다.
- 별도의 로컬 프로세스. 매핑, 프로필 및 워크플로우 작업을 실행할 때 구성합니다. 데이터 통합 서비스가 별도의 로컬 프로세스에서 작업을 실행하는 경우, 하나의 작업에 대한 예기치 않은 중단이 다른 모든 작업에 영향을 미치는 것은 아니기 때문에 안정성이 높아집니다.

서비스를 작성한 후 데이터 통합 서비스가 그리드에서 실행되도록 구성한 경우에는 개별 원격 프로세스에서 작업을 실행하도록 서비스를 구성할 수 있습니다.

13. 나머지 실행 옵션에 대해 기본값을 그대로 사용하고 **다음**을 클릭합니다.

새 데이터 통합 서비스 - 4/14단계 페이지가 나타납니다.

14. 데이터 통합 서비스에 대해 데이터 개체 캐시 데이터베이스를 작성한 경우, **선택**을 클릭하여 캐시 연결을 선택합니다. 데이터베이스에 액세스하기 위해 해당 서비스에 대해 작성한 데이터 개체 캐시 연결을 선택합니다.

15. 이 페이지의 나머지 속성에 대해 기본값을 그대로 사용하고 **다음**을 클릭합니다.

새 데이터 통합 서비스 - 5/14단계 페이지가 나타납니다.

16. 최적의 성능을 위해 사용하려고 계획한 데이터 통합 서비스 모듈을 활성화합니다.
다음 테이블에는 활성화할 수 있는 데이터 통합 서비스 모듈이 나열되어 있습니다.

모듈	설명
웹 서비스 모듈	웹 서비스 작업 매핑을 실행합니다.
매핑 서비스 모듈	매핑 및 미리보기를 실행합니다.
프로파일링 서비스 모듈	프로필 및 성과 기록표를 실행합니다.
SQL 서비스 모듈	타사 클라이언트 도구에서 SQL 데이터 서비스로 SQL 쿼리를 실행합니다.
Workflow Orchestration Service 모듈	워크플로우를 실행합니다.

17. 다음을 클릭합니다.

새 데이터 통합 서비스 - 6/14단계 페이지가 나타납니다.

HTTP 요청을 데이터 통합 서비스로 리디렉션하도록 HTTP 프록시 서버 속성을 구성합니다. 데이터 통합 서비스에 요청을 보낼 수 있는 웹 서비스 클라이언트 시스템을 필터링하도록 HTTP 구성 속성을 구성할 수 있습니다. 서비스를 작성한 후 이러한 속성을 구성할 수 있습니다.

18. HTTP 프록시 서버 및 HTTP 구성 속성에 대해 기본값을 그대로 사용하고 다음을 클릭합니다.

새 데이터 통합 서비스 - 7/14단계 페이지가 나타납니다.

데이터 통합 서비스는 결과 집합 캐시 속성을 통해 SQL 데이터 서비스 쿼리 및 웹 서비스 요청에 대해 캐시된 결과를 사용합니다. 서비스를 작성한 후 속성을 구성할 수 있습니다.

19. 결과 집합 캐시 속성에 대해 기본값을 그대로 사용하고 다음을 클릭합니다.

새 데이터 통합 서비스 - 8/14단계 페이지가 나타납니다.

20. 데이터 통합 서비스에 대해 프로파일링 웨어하우스 데이터베이스를 작성한 경우, 프로파일링 서비스 모듈을 선택합니다.

21. 데이터 통합 서비스에 대해 워크플로우 데이터베이스를 작성한 경우, Workflow Orchestration Service 모듈을 선택합니다.

22. 나머지 모듈이 선택되지 않았는지 확인합니다.

서비스를 작성한 후 나머지 모듈에 대한 속성을 구성할 수 있습니다.

23. 다음을 클릭합니다.

새 데이터 통합 서비스 - 11/14단계 페이지가 나타납니다.

24. 데이터 통합 서비스에 대해 프로파일링 웨어하우스 데이터베이스를 작성한 경우, **선택**을 클릭하여 데이터베이스 연결을 선택합니다. 데이터베이스에 액세스하기 위해 해당 서비스에 대해 작성한 프로파일링 웨어하우스 연결을 선택합니다.

25. 프로파일링 웨어하우스 데이터베이스에 콘텐츠가 있는지 여부를 선택합니다.

새 프로파일링 웨어하우스 데이터베이스를 작성한 경우 **지정된 연결 문자열에 콘텐츠가 없습니다**를 선택합니다.

26. 다음을 클릭합니다.

새 데이터 통합 서비스 - 12/14단계 페이지가 나타납니다.

27. 고급 프로파일링 속성에 대해 기본값을 그대로 사용하고 다음을 클릭합니다.

새 데이터 통합 서비스 - 14/14단계 페이지가 나타납니다.

28. 데이터 통합 서비스에 대해 워크플로우 데이터베이스를 작성한 경우, **선택**을 클릭하여 데이터베이스 연결을 선택합니다. 데이터베이스에 액세스하기 위해 해당 서비스에 대해 작성한 워크플로우 데이터베이스 연결을 선택합니다.

29. **마침**을 클릭합니다.

도메인이 데이터 통합 서비스를 작성하고 활성화합니다.

마법사를 통해 서비스를 작성한 후 속성을 편집하거나 다른 속성을 구성할 수 있습니다.

데이터 통합 서비스를 작성한 후

데이터 통합 서비스를 작성한 후에는 다음 태스크를 수행합니다.

- 호스트 파일 구성을 확인합니다.
- 다른 응용 프로그램 서비스를 작성합니다.

호스트 파일 구성 확인

작업을 별도의 프로세스로 실행하도록 UNIX 또는 Linux에서 데이터 통합 서비스를 구성한 경우 해당 서비스가 실행되는 노드의 호스트 파일에 **localhost** 항목이 포함되어 있는지 확인합니다. **localhost** 항목이 포함되어 있지 않은 경우 데이터 통합 서비스에 대해 **별도의 프로세스로 작업 실행** 속성이 활성화되어 있으면 작업이 실패하게 됩니다.

기타 서비스 작성

데이터 통합 서비스를 작성한 후에는 데이터 통합 서비스에 종속된 응용 프로그램 서비스를 작성합니다.

종속형 서비스는 다음 순서대로 작성합니다.

1. 콘텐츠 관리 서비스
2. 분석 서비스
3. 검색 서비스

PowerCenter 리포지토리 서비스 작성 및 구성

PowerCenter 리포지토리 서비스는 PowerCenter 리포지토리를 관리하는 응용 프로그램 서비스입니다.

PowerCenter 리포지토리는 PowerCenter 클라이언트 및 응용 프로그램 서비스에서 작성된 메타데이터를 관계형 데이터베이스에 저장합니다.

PowerCenter 클라이언트 또는 PowerCenter 통합 서비스에서 PowerCenter 리포지토리 개체에 액세스하는 경우, 해당 클라이언트 또는 서비스가 PowerCenter 리포지토리 서비스로 요청을 보냅니다. PowerCenter 리포지토리 서비스 프로세스는 PowerCenter 리포지토리 데이터베이스 테이블에서 메타데이터를 가져오고, 삽입하고, 업데이트합니다.

PowerCenter 리포지토리 서비스 작성

Administrator 도구에서 서비스 작성 마법사를 사용하여 서비스를 작성합니다.

1. Administrator 도구에서 **관리** 탭을 클릭합니다.

- 작업 > 새로 만들기 > **PowerCenter 리포지토리 서비스**를 클릭합니다.
새 **PowerCenter 리포지토리 서비스** 대화 상자가 나타납니다.
- 새 **PowerCenter 리포지토리 서비스 - 1/2단계** 페이지에서 다음 속성을 입력합니다.

속성	설명
이름	서비스의 이름입니다. 이름은 대/소문자를 구분하지 않으며 도메인 내에서 고유해야 합니다. 이름은 128자를 초과하거나 @로 시작할 수 없습니다. 또한 공백이나 다음과 같은 특수 문자를 포함할 수도 없습니다. ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
설명	서비스에 대한 설명. 설명은 765자를 초과할 수 없습니다.
위치	서비스가 작성되는 도메인 및 폴더입니다. 다른 폴더를 선택하려면 찾아보기 를 클릭합니다. 서비스를 작성한 후 이동할 수 있습니다.
라이선스	서비스를 사용할 수 있도록 해주는 라이선스 개체입니다.
노드	서비스가 실행되는 노드입니다.
기본 노드	라이선스에 고가용성이 포함된 경우 서비스가 기본적으로 실행되는 노드입니다. 고가용성이 포함된 라이선스를 선택한 경우 필요합니다.
백업 노드	라이선스에 고가용성이 포함된 경우, 기본 노드를 사용할 수 없을 때 서비스가 실행될 수 있는 노드입니다.

- 다음을 클릭합니다.
새 **PowerCenter 리포지토리 서비스 - 2/2단계** 페이지가 나타납니다.
- PowerCenter 리포지토리 데이터베이스**에 대한 다음 속성을 입력합니다.

속성	설명
데이터베이스 유형	리포지토리 데이터베이스의 유형입니다.
사용자 이름	리포지토리에 대한 데이터베이스 사용자 이름입니다.
암호	PowerCenter 리포지토리 데이터베이스 사용자의 암호입니다. 7비트 ASCII여야 합니다.
연결 문자열	리포지토리 데이터베이스에 액세스하기 위해 PowerCenter 리포지토리 서비스에서 사용하는 원시 연결 문자열입니다. 지원되는 각 데이터베이스에 대해 다음 원시 연결 문자열 구문을 사용하십시오. <ul style="list-style-type: none"> - servername@databasename(Microsoft SQL Server 및 Sybase) - databasename.world(Oracle) - databasename(IBM DB2)

속성	설명
코드 페이지	리포지토리 데이터베이스 코드 페이지입니다. PowerCenter 리포지토리 서비스에서는 데이터베이스 코드 페이지에 인코딩된 문자 집합을 사용하여 데이터를 기록합니다. PowerCenter 리포지토리 서비스를 작성한 후에는 PowerCenter 리포지토리 서비스 속성의 코드 페이지를 변경할 수 없습니다.
테이블스페이스 이름	모든 리포지토리 데이터베이스 테이블을 작성할 테이블스페이스 이름입니다. 테이블스페이스 이름에 공백을 사용할 수 없습니다. IBM DB2 및 Sybase 데이터베이스에 사용할 수 있습니다. IBM DB2 EEE 리포지토리에서 리포지토리 성능을 개선하려면 노드가 1개 있는 테이블스페이스 이름을 지정하십시오.

- 지정된 연결 문자열에 콘텐츠가 없습니다. 새 콘텐츠를 작성하십시오.를 선택합니다.
- 필요에 따라 글로벌 리포지토리 작성을 선택합니다.
서비스를 작성한 후에는 로컬 리포지토리를 글로벌 리포지토리로 승격할 수 있지만 글로벌 리포지토리를 로컬 리포지토리로 변경할 수는 없습니다.
- 라이선스에 팀 기반 개발 옵션이 있는 경우 필요에 따라 리포지토리에 대한 버전 제어를 활성화할 수 있습니다.
서비스를 작성한 후에는 버전이 없는 리포지토리를 버전이 있는 리포지토리로 변환할 수 있지만 버전이 있는 리포지토리를 버전이 없는 리포지토리로 변환할 수는 없습니다.
- 마침을 클릭합니다.
도메인이 PowerCenter 리포지토리 서비스를 작성하고, 서비스를 시작하고, PowerCenter 리포지토리의 콘텐츠를 작성합니다.
마법사를 통해 서비스를 작성한 후 속성을 편집하거나 다른 속성을 구성할 수 있습니다.

PowerCenter 리포지토리 서비스를 작성한 후

PowerCenter 리포지토리 서비스를 작성한 후에는 다음 태스크를 수행합니다.

- PowerCenter 리포지토리 서비스가 보통 모드에서 실행되도록 구성합니다.
- 도메인에서 Kerberos 인증을 사용하지 않는 경우 PowerCenter 리포지토리 사용자를 작성합니다.
- 다른 응용 프로그램 서비스를 작성합니다.

보통 모드로 PowerCenter 리포지토리 서비스 실행

PowerCenter 리포지토리 서비스를 작성하고 나면 제외 모드에서 시작되고 액세스가 관리자로 제한됩니다. 다른 사용자에게 액세스 권한을 부여하려면 서비스가 보통 작동 모드에서 실행되도록 서비스 속성을 편집합니다.

- Administrator 도구에서 **관리** 탭을 클릭합니다.
- 탐색기에서 PowerCenter 리포지토리 서비스를 선택합니다.
- 속성을 클릭합니다.
- 리포지토리 속성 편집을 클릭합니다.
- 작동 모드 필드에서 보통을 선택합니다.
- 확인을 클릭합니다.
변경 내용을 적용하려면 PowerCenter 리포지토리 서비스를 재사용해야 합니다.
- 작업 > 서비스 재사용을 선택합니다.

PowerCenter 리포지토리 사용자 작성

Kerberos 인증을 사용하지 않는 도메인에서는 PowerCenter 리포지토리 서비스에 대해 요청하는 다른 응용 프로그램 서비스를 인증하기 위해 사용자 계정을 사용합니다. 따라서 PowerCenter 리포지토리 서비스에 대해 사용자 계정을 작성하고 사용자에게 관리자 역할을 할당해야 합니다.

PowerCenter 리포지토리 서비스에 종속된 응용 프로그램 서비스를 작성하는 경우 PowerCenter 리포지토리 서비스의 이름과 이 PowerCenter 리포지토리 사용자의 이름을 제공합니다.

1. Administrator 도구에서 **보안** 탭을 클릭합니다.
2. 보안 작업 메뉴에서 **사용자 작성**을 클릭하여 원시 사용자 계정을 작성합니다.

참고: 도메인에서 LDAP 인증을 설정하려면 PowerCenter 리포지토리 사용자에게 대해 LDAP 사용자 계정을 사용하면 됩니다.

3. 사용자에게 다음 속성을 입력합니다.

속성	설명
로그인 이름	<p>사용자 계정의 로그인 이름입니다. 사용자 계정의 로그인 이름은 해당 계정이 속한 보안 도메인 내에서 고유해야 합니다.</p> <p>이름은 대/소문자를 구분하지 않으며 128자를 초과할 수 없습니다. 이름에는 탭, 줄 바꿈 문자 또는 다음과 같은 특수 문자를 사용할 수 없습니다.</p> <p>, + " \ < > ; / * % ? &</p> <p>첫 번째 문자와 마지막 문자를 제외하고 이름에는 ASCII 공백 문자를 사용할 수 있습니다. 다른 모든 공백 문자는 사용할 수 없습니다.</p>
암호	<p>사용자 계정에 대한 암호입니다. 암호의 길이는 1~80자여야 합니다.</p>
암호 확인	<p>확인을 위해 암호를 다시 입력합니다. 암호를 수동으로 다시 입력해야 합니다. 암호를 복사해서 붙여 넣지 마십시오.</p>
전체 이름	<p>사용자 계정의 전체 이름입니다. 전체 이름에는 다음과 같은 특수 문자를 포함할 수 없습니다.</p> <p>< > “</p>
설명	<p>사용자 계정에 대한 설명입니다. 설명은 765자를 초과하거나 다음 특수 문자를 포함할 수 없습니다.</p> <p>< > “</p>

4. **확인**을 클릭합니다.
사용자 속성이 나타납니다.
5. **권한** 탭을 클릭합니다.
6. **편집**을 클릭합니다.
역할 및 권한 편집 대화 상자가 나타납니다.
7. **역할** 탭에서 PowerCenter 리포지토리 서비스를 확장합니다.
8. **시스템 정의 역할**에서 관리자를 선택하고 **확인**을 클릭합니다.

기타 서비스 작성

PowerCenter 리포지토리 서비스를 작성한 후에는 PowerCenter 리포지토리 서비스에 종속된 응용 프로그램 서비스를 작성합니다.

다음과 같은 응용 프로그램 서비스를 작성할 수 있습니다.

1. PowerCenter 통합 서비스
2. Metadata Manager 서비스
3. 웹 서비스 힙 서비스

PowerCenter 통합 서비스 작성 및 구성

PowerCenter 통합 서비스는 PowerCenter 클라이언트를 위해 워크플로우 및 세션을 실행하는 응용 프로그램 서비스입니다.

PowerCenter 클라이언트에서 워크플로우를 실행하면 해당 클라이언트가 PowerCenter 통합 서비스로 요청을 보냅니다. PowerCenter 통합 서비스는 PowerCenter 리포지토리 서비스에 연결하여 PowerCenter 리포지토리에서 메타데이터를 가져온 후, 세션 및 워크플로우를 실행하고 모니터링합니다.

PowerCenter 통합 서비스 작성

Administrator 도구에서 서비스 작성 마법사를 사용하여 서비스를 작성합니다.

PowerCenter 통합 서비스를 생성하기 전에 다음 서비스를 생성했는지 확인합니다:

PowerCenter 리포지토리 서비스

1. Administrator 도구에서 **관리** 탭을 클릭합니다.
2. **작업 > 새로 만들기 > PowerCenter 통합 서비스**를 클릭합니다.
새 **PowerCenter 통합 서비스** 대화 상자가 나타납니다.
3. 새 **PowerCenter 통합 서비스 - 1/2단계** 페이지에서 다음 속성을 입력합니다.

속성	설명
이름	서비스의 이름입니다. 이름은 대/소문자를 구분하지 않으며 도메인 내에서 고유해야 합니다. 이름은 128자를 초과하거나 @로 시작할 수 없습니다. 또한 공백이나 다음과 같은 특수 문자를 포함할 수도 없습니다. <code>` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []</code>
설명	서비스에 대한 설명. 설명은 765자를 초과할 수 없습니다.
위치	서비스가 작성되는 도메인 및 폴더입니다. 다른 폴더를 선택하려면 찾아보기 를 클릭합니다. 서비스를 작성한 후 이동할 수 있습니다.
라이선스	서비스를 사용할 수 있도록 해주는 라이선스 개체입니다.
노드	서비스가 실행되는 노드입니다.

속성	설명
할당	노드에서 실행할 서비스를 구성하려면 노드 를 선택합니다. 라이선스에 그리드가 포함된 경우에는 서비스를 작성한 후 그리드를 작성하고 그리드에서 실행할 서비스를 할당할 수 있습니다.
기본 노드	라이선스에 고가용성이 포함된 경우 서비스가 기본적으로 실행되는 노드입니다. 고가용성이 포함된 라이선스를 선택한 경우 필요합니다.
백업 노드	라이선스에 고가용성이 포함된 경우, 기본 노드를 사용할 수 없을 때 서비스가 실행될 수 있는 노드입니다.

4. 다음을 클릭합니다.
5. 새 **PowerCenter 통합 서비스 - 2/2단계** 페이지에서 다음 속성을 입력합니다.

속성	설명
PowerCenter 리포지토리 서비스	서비스와 연결할 PowerCenter 리포지토리 서비스입니다.
사용자 이름	서비스가 PowerCenter 리포지토리 서비스에 액세스하는 데 필요한 사용자 이름입니다. 작성한 PowerCenter 리포지토리 사용자를 입력합니다. PowerCenter 리포지토리 서비스를 서비스와 연결할 경우 필요합니다. Kerberos 인증이 있는 도메인에서는 사용할 수 없습니다.
암호	PowerCenter 리포지토리 사용자와 연결된 암호입니다. Kerberos 인증이 있는 도메인에서는 사용할 수 없습니다.
보안 도메인	PowerCenter 리포지토리 사용자에 대한 LDAP 보안 도메인입니다. Informatica 도메인에 LDAP 보안 도메인이 포함된 경우 보안 도메인 필드가 나타납니다. PowerCenter 리포지토리 서비스를 서비스와 연결할 경우 필요합니다. Kerberos 인증이 있는 도메인에서는 사용할 수 없습니다.

6. PowerCenter 통합 서비스가 문자 데이터를 처리하는 방법을 결정하는 데이터 이동 모드를 선택합니다. ASCII 또는 유니코드를 선택합니다. 기본값은 ASCII입니다.
ASCII 모드에서 PowerCenter 통합 서비스는 7비트 ASCII 및 EBCDIC 문자를 인식하고 각 문자를 단일 바이트로 저장합니다. 유니코드 모드에서 PowerCenter 통합 서비스는 지원되는 코드 페이지에 의해 정의된 다중 바이트 문자 집합을 인식합니다. 소스 또는 대상이 8비트 또는 다중 바이트 문자 집합이고 문자 데이터를 포함하는 경우 유니코드 모드를 사용하십시오.
7. **마침**을 클릭합니다.
8. **코드 페이지 지정** 대화 상자에서 PowerCenter 통합 서비스의 코드 페이지를 할당합니다. PowerCenter 통합 서비스의 코드 페이지는 연결된 리포지토리의 코드 페이지와 호환되어야 합니다.
9. **확인**을 클릭합니다.
도메인이 PowerCenter 통합 서비스를 작성합니다. 서비스를 작성하는 중에는 도메인이 PowerCenter 통합 서비스를 활성화하지 않습니다.
10. PowerCenter 통합 서비스를 활성화하려면 탐색기에서 해당 서비스를 선택하고 **작업 > 서비스 활성화**를 클릭합니다. PowerCenter 통합 서비스를 활성화하려면 PowerCenter 리포지토리 서비스가 실행되고 있어야 합니다.

마법사를 통해 서비스를 작성한 후 속성을 편집하거나 다른 속성을 구성할 수 있습니다.

PowerCenter 통합 서비스를 작성한 후

PowerCenter 통합 서비스를 작성한 후에는 PowerCenter 통합 서비스에 종속된 Metadata Manager 서비스를 작성합니다.

Metadata Manager 서비스 작성 및 구성

Metadata Manager 서비스는 Informatica 도메인에서 Metadata Manager 웹 클라이언트를 실행하는 응용 프로그램 서비스입니다. Metadata Manager 서비스는 Metadata Manager에 액세스할 수 있는 사용자와 서비스 구성 요소 간의 연결을 관리합니다.

메타데이터를 Metadata Manager 웨어하우스로 로드하면 Metadata Manager 서비스가 PowerCenter 통합 서비스에 연결합니다. PowerCenter 통합 서비스는 PowerCenter 리포지토리의 워크플로우를 실행하여 메타데이터 소스에서 읽은 후 해당 메타데이터를 Metadata Manager 웨어하우스로 로드합니다. Metadata Manager를 사용하여 메타데이터를 찾아보고 분석할 경우 Metadata Manager 서비스에서 Metadata Manager 리포지토리에 있는 메타데이터에 액세스합니다.

Metadata Manager 서비스 작성

Administrator 도구에서 서비스 작성 마법사를 사용하여 서비스를 작성합니다.

Metadata Manager 서비스를 작성하기 전에 다음 서비스를 작성하고 활성화했는지 확인합니다.

PowerCenter 리포지토리 서비스

PowerCenter 통합 서비스

- Administrator 도구에서 **관리** 탭을 클릭합니다.
- 작업 > 새로 만들기 > Metadata Manager 서비스**를 클릭합니다.
새 **Metadata Manager 서비스** 대화 상자가 표시됩니다.
- 새 **Metadata Manager 서비스 - 1/3단계** 페이지에서 다음 속성을 입력합니다.

속성	설명
이름	서비스의 이름입니다. 이름은 대/소문자를 구분하지 않으며 도메인 내에서 고유해야 합니다. 이름은 128자를 초과하거나 @로 시작할 수 없습니다. 또한 공백이나 다음과 같은 특수 문자를 포함할 수도 없습니다. ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () [
설명	서비스에 대한 설명. 설명은 765자를 초과할 수 없습니다.
위치	서비스가 작성되는 도메인 및 폴더입니다. 다른 폴더를 선택하려면 찾아보기 를 클릭합니다. 서비스를 작성한 후 이동할 수 있습니다.
라이선스	서비스를 사용할 수 있도록 해주는 라이선스 개체입니다.
노드	서비스가 실행되는 노드입니다.

4. 연결된 리포지토리 서비스의 다음 속성을 지정합니다.

속성	설명
연결된 통합 서비스	Metadata Manager 웨어하우스로 메타데이터를 로드하기 위해 Metadata Manager에서 사용되는 PowerCenter 통합 서비스를 선택합니다.
리포지토리 사용자 이름	서비스가 PowerCenter 리포지토리 서비스에 액세스하는 데 필요한 사용자 이름입니다. 작성한 PowerCenter 리포지토리 사용자를 입력합니다. PowerCenter 리포지토리 서비스를 서비스와 연결할 경우 필요합니다. Kerberos 인증이 있는 도메인에서는 사용할 수 없습니다.
리포지토리 암호	PowerCenter 리포지토리 사용자와 연결된 암호입니다. Kerberos 인증이 있는 도메인에서는 사용할 수 없습니다.
보안 도메인	PowerCenter 리포지토리 사용자에 대한 LDAP 보안 도메인입니다. Informatica 도메인에 LDAP 보안 도메인이 포함된 경우 보안 도메인 필드가 나타납니다. PowerCenter 리포지토리 서비스를 서비스와 연결할 경우 필요합니다. Kerberos 인증이 있는 도메인에서는 사용할 수 없습니다.

5. 다음을 클릭합니다.

새 **Metadata Manager** 서비스 - 2/3단계 페이지가 나타납니다.

6. Metadata Manager 리포지토리에 대한 다음 데이터베이스 속성을 입력합니다.

속성	설명
데이터베이스 유형	리포지토리 데이터베이스의 유형입니다.
코드 페이지	Metadata Manager 리포지토리 코드 페이지입니다. Metadata Manager 서비스 및 Metadata Manager 응용 프로그램은 데이터를 Metadata Manager 리포지토리에 기록할 때 리포지토리 코드 페이지에 인코딩된 문자 집합을 사용합니다. Metadata Manager 서비스를 활성화하려면 반드시 코드 페이지를 먼저 지정해야 합니다.
연결 문자열	Metadata Manager 리포지토리 데이터베이스의 원시 연결 문자열입니다. Metadata Manager 서비스는 연결 문자열을 사용하여 PowerCenter 리포지토리의 Metadata Manager 리포지토리에 대한 연결 개체를 작성합니다. 지원되는 각 데이터베이스에 대해 다음 원시 연결 문자열 구문을 사용하십시오. - servername@databasename(Microsoft SQL Server) - databasename.world(Oracle) - databasename(IBM DB2)
데이터베이스 사용자	리포지토리에 대한 데이터베이스 사용자 이름입니다.
데이터베이스 암호	Metadata Manager 리포지토리 데이터베이스 사용자의 암호입니다. 7비트 ASCII여야 합니다.

속성	설명
테이블스페이스 이름	모든 리포지토리 데이터베이스 테이블을 작성할 테이블스페이스 이름입니다. 테이블스페이스 이름에 공백을 사용할 수 없습니다. IBM DB2 데이터베이스에 사용할 수 있습니다. IBM DB2 EEE 리포지토리에서 리포지토리 성능을 개선하려면 노드가 1개 있는 테이블스페이스 이름을 지정하십시오.
데이터베이스 호스트 이름	데이터베이스 서버를 호스팅하는 시스템 이름입니다.
데이터베이스 포트	데이터베이스 서버 수신기 서비스를 구성하는 포트 번호입니다.
SID/서비스 이름	Oracle 데이터베이스입니다. JDBC 연결 문자열에서 SID 또는 서비스 이름을 사용하지 여부를 지정합니다. Oracle RAC 데이터베이스의 경우 Oracle SID 또는 Oracle 서비스 이름 중에서 선택합니다. 그 외의 Oracle 데이터베이스의 경우 Oracle SID를 선택합니다.
데이터베이스 이름	데이터베이스 서버의 이름입니다. Oracle 데이터베이스의 전체 서비스 이름 또는 SID, IBM DB2 데이터베이스의 서비스 이름, Microsoft SQL Server 데이터베이스의 데이터베이스 이름을 지정합니다.

7. 데이터베이스 연결 URL에 매개 변수를 추가하려면 **추가 JDBC 매개 변수 필드**에서 추가 매개 변수를 구성합니다. 세미콜론 문자(;)로 구분된 이름=값 쌍으로 매개 변수를 입력합니다. 예를 들어 `param1=value1;param2=value2`와 같습니다.

이 속성을 사용하여 다음 매개 변수를 지정할 수 있습니다.

매개 변수	설명
백업 서버 위치	Oracle RAC 같이 고가용성 데이터베이스 서버를 사용할 경우 백업 서버의 위치를 입력하십시오.
Oracle ASO(Advanced Security Option) 매개 변수	Metadata Manager 리포지토리가 ASO를 사용하는 Oracle 데이터베이스인 경우 다음 추가 매개 변수를 입력하십시오. <code>EncryptionLevel=[encryption level];EncryptionTypes=[encryption types];DataIntegrityLevel=[data integrity level];DataIntegrityTypes=[data integrity types]</code> 참고: 매개 변수 값은 Metadata Manager 서비스가 실행되는 시스템에 있는 <code>sqlnet.ora</code> 파일의 값과 일치해야 합니다.
Microsoft SQL Server에 대한 인증 정보	Windows 인증을 사용하여 사용자 자격 증명을 인증하고 Microsoft SQL Server 리포지토리에 대한 트러스트된 연결을 설정하려면 다음 텍스트를 입력하십시오. <code>AuthenticationMethod=ntlm;LoadLibraryPath=[directory containing DDJDBCx64Auth04.dll]. jdbc:informatica:sqlserver://[host]:[port];DatabaseName=[DB name]; AuthenticationMethod=ntlm;LoadLibraryPath=[directory containing DDJDBCx64Auth04.dll]</code> 트러스트된 연결을 사용하여 Microsoft SQL Server 데이터베이스에 연결한 경우 Metadata Manager 서비스는 서비스를 실행하는 시스템에 로그인한 사용자의 자격 증명을 사용하여 리포지토리에 연결합니다. 트러스트된 연결을 사용하여 Metadata Manager 서비스를 Windows 서비스로 시작하려면 트러스트된 사용자 계정으로 로그인하도록 Windows 서비스 속성을 구성합니다.

8. **Metadata Manager** 리포지토리 데이터베이스가 보안 통신을 사용하도록 구성되어 있으면 **보안 JDBC 매개 변수** 필드에서 추가 JDBC 매개 변수를 구성할 수 있습니다.

이 속성을 사용하여 암호와 같은 보안 연결 매개 변수를 지정합니다. **Administrator** 도구는 **Metadata Manager** 서비스 속성에 보안 매개 변수 또는 매개 변수 값을 표시하지 않습니다. 세미콜론 문자(;)로 구분된 이름=값 쌍으로 매개 변수를 입력합니다. 예를 들어 `param1=value1;param2=value2`와 같습니다. 다음 보안 데이터베이스 매개 변수를 입력하십시오.

보안 데이터베이스 매개 변수	설명
EncryptionMethod	필수 사항입니다. 네트워크를 통해 전송되는 경우 데이터가 암호화되었는지를 나타냅니다. 이 매개 변수는 SSL로 설정되어야 합니다.
TrustStore	필수. 데이터베이스 서버의 SSL 인증서를 포함하는 트러스트 저장소 파일의 경로 및 파일 이름입니다.
TrustStorePassword	필수. 트러스트 저장소 파일에 액세스하는 데 사용되는 암호입니다.
HostNameInCertificate	보안 데이터베이스를 호스팅하는 시스템의 호스트 이름입니다. 호스트 이름을 지정하면 Metadata Manager 서비스에서 SSL 인증서의 호스트 이름에 대해 연결 문자열에 포함된 호스트 이름의 유효성을 검사합니다.
ValidateServerCertificate	선택 사항입니다. Informatica가 데이터베이스 서버에서 보낸 인증서에 대해 유효성을 검사하는지 여부를 나타냅니다. 이 매개 변수를 True로 설정하면 데이터베이스 서버에서 보낸 인증서에 대해 Informatica에서 유효성을 검사합니다. HostNameInCertificate 매개 변수를 지정하면 Informatica에서 인증서의 호스트 이름에 대한 유효성도 검사합니다. 이 매개 변수를 False로 설정하면 데이터베이스 서버에서 보낸 인증서에 대해 Informatica에서 유효성을 검사하지 않습니다. Informatica에서 사용자가 지정한 트러스트 저장소 정보를 모두 무시합니다.
KeyStore	Metadata Manager 서비스에서 데이터베이스 서버에 전송하는 SSL 인증서가 포함된 키 저장소 파일의 경로 및 파일 이름입니다.
KeyStorePassword	키 저장소 파일에 액세스하는 데 사용되는 암호입니다.

9. 다음을 클릭합니다.

새 Metadata Manager 서비스 - 3/3단계 페이지가 나타납니다.

10. 서비스에 사용할 HTTP 포트 번호를 입력합니다.
11. **Metadata Manager** 서비스와의 보안 통신을 활성화하려면 **보안 소켓 계층 활성화**를 선택합니다. 다음 속성을 입력하여 서비스에 대한 보안 통신을 구성합니다.

속성	설명
HTTPS 포트	서비스에 대한 보안 연결에 사용할 포트 번호입니다. HTTP 포트 번호와 다른 포트 번호를 사용하십시오.
키 저장소 파일	개인 또는 공용 키 쌍 및 연결된 인증서를 포함하는 키 저장소 파일의 경로와 파일 이름입니다. 서비스에 HTTPS 연결을 사용할 경우 필요합니다.
키 저장소 암호	키 저장소 파일에 대한 일반 텍스트 암호입니다.

12. **마침**을 클릭합니다.

도메인이 **Metadata Manager** 서비스를 작성합니다. 서비스를 작성하는 중에는 도메인이 **Metadata Manager** 서비스를 활성화하지 않습니다.

13. **Metadata Manager** 서비스를 활성화하려면 탐색기에서 해당 서비스를 선택하고 **작업 > 서비스 활성화**를 클릭합니다. **Metadata Manager** 서비스를 활성화하려면 **PowerCenter** 리포지토리 서비스 및 **PowerCenter** 통합 서비스를 실행 중이어야 합니다.

마법사를 통해 서비스를 작성한 후 속성을 편집하거나 다른 속성을 구성할 수 있습니다.

Metadata Manager 서비스를 작성한 후

Metadata Manager 서비스를 작성한 후에는 다음 태스크를 수행합니다.

- **Metadata Manager** 리포지토리에 대한 콘텐츠를 작성합니다.
- 다른 응용 프로그램 서비스를 작성합니다.

Metadata Manager 서비스를 작성하는 경우 리포지토리 테이블을 작성하고 메타데이터 소스의 모델을 가져옵니다.

1. 탐색기에서 **Metadata Manager** 서비스를 선택합니다.
2. **작업 > 리포지토리 콘텐츠 > 작성**을 클릭합니다.
3. **확인**을 클릭합니다.

Metadata Manager 서비스를 작성한 후에는 **Metadata Manager** 서비스에 종속된 응용 프로그램 서비스를 작성합니다.

콘텐츠 관리 서비스 작성 및 구성

콘텐츠 관리 서비스는 참조 데이터를 관리하는 응용 프로그램 서비스입니다. 참조 데이터 개체에는 소스 데이터에 대해 데이터 품질 작업을 수행하는 동안 검색할 수 있는 데이터 값의 집합이 포함되어 있습니다. 또한 콘텐츠 관리 서비스는 규칙 사양을 맵셋으로 컴파일합니다. 규칙 사양 개체는 비즈니스 규칙의 데이터 요구 사항을 논리적 형태로 기술합니다.

콘텐츠 관리 서비스는 데이터 통합 서비스를 사용해 매핑을 실행하여 참조 테이블과 외부 데이터 소스 간에 데이터를 전달합니다. 또한 콘텐츠 관리 서비스는 다음 유형의 참조 데이터와 함께 변환, 매핑 사양 및 규칙 사양을 제공합니다.

- 주소 참조 데이터
- ID 채우기
- 확률 모델 및 분류자 모델
- 참조 테이블

콘텐츠 관리 서비스 작성

Administrator 도구에서 서비스 작성 마법사를 사용하여 서비스를 작성합니다.

콘텐츠 관리 서비스를 작성하기 전에 다음 서비스를 작성하고 활성화했는지 확인합니다.

- 모델 리포지토리 서비스
- 데이터 통합 서비스

1. Administrator 도구에서 **관리** 탭을 클릭합니다.
2. **작업 > 새로 만들기 > 콘텐츠 관리 서비스**를 클릭합니다.
새 **콘텐츠 관리 서비스** 대화 상자가 나타납니다.
3. **새 콘텐츠 관리 서비스 - 1/2단계** 페이지에서 다음 속성을 입력합니다.

속성	설명
이름	서비스의 이름입니다. 이름은 대/소문자를 구분하지 않으며 도메인 내에서 고유해야 합니다. 이름은 128자를 초과하거나 @로 시작할 수 없습니다. 또한 공백이나 다음과 같은 특수 문자를 포함할 수도 없습니다. ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () [
설명	서비스에 대한 설명. 설명은 765자를 초과할 수 없습니다.
위치	서비스가 작성되는 도메인 및 폴더입니다. 다른 폴더를 선택하려면 찾아보기 를 클릭합니다. 서비스를 작성한 후 이동할 수 있습니다.
라이선스	서비스를 사용할 수 있도록 해주는 라이선스 개체입니다.
노드	서비스가 실행되는 노드입니다.
HTTP 포트	콘텐츠 관리 서비스에 사용할 HTTP 포트 번호입니다.
데이터 통합 서비스	서비스와 연결할 데이터 통합 서비스입니다. 데이터 통합 서비스 및 콘텐츠 관리 서비스는 같은 노드에서 실행되어야 합니다.
모델 리포지토리 서비스	서비스와 연결할 모델 리포지토리 서비스입니다.
사용자 이름	서비스가 모델 리포지토리 서비스에 액세스하는 데 필요한 사용자 이름입니다. 작성한 모델 리포지토리 사용자를 입력합니다.
암호	모델 리포지토리 사용자의 암호입니다.
보안 도메인	모델 리포지토리 사용자에게 대한 LDAP 보안 도메인입니다. Informatica 도메인에 LDAP 보안 도메인이 포함된 이 필드가 나타납니다. Kerberos 인증이 있는 도메인에서는 사용할 수 없습니다.
참조 데이터 위치	콘텐츠 관리 서비스가 참조 데이터 웨어하우스에 액세스하도록 작성한 참조 데이터 웨어하우스 연결입니다. 선택 을 클릭하여 연결을 선택합니다.

4. **다음**을 클릭합니다.
새 **콘텐츠 관리 서비스 - 2/2단계** 페이지가 나타납니다.
5. 보안 속성에 대해 기본값을 그대로 사용합니다.
6. **서비스 활성화**를 선택합니다.
콘텐츠 관리 서비스를 활성화하려면 모델 리포지토리 서비스 및 데이터 통합 서비스가 실행되고 있어야 합니다.
7. **마침**을 클릭합니다.
도메인이 콘텐츠 관리 서비스를 작성하고 활성화합니다.
마법사를 통해 서비스를 작성한 후 속성을 편집하거나 다른 속성을 구성할 수 있습니다.

분석 서비스 작성 및 구성

분석 서비스는 Informatica 도메인에서 Analyst 도구를 실행하는 응용 프로그램 서비스입니다. 분석 서비스는 Analyst 도구에 액세스할 수 있는 사용자와 서비스 구성 요소 간의 연결을 관리합니다.

분석 서비스 작성

Administrator 도구에서 서비스 작성 마법사를 사용하여 서비스를 작성합니다.

분석 서비스를 작성하기 전에 다음 서비스를 작성하고 활성화했는지 확인합니다.

- 모델 리포지토리 서비스
- 데이터 통합 서비스

1. Administrator 도구에서 **관리** 탭을 클릭합니다.
2. **작업 > 새로 만들기 > 분석 서비스**를 클릭합니다.
새 분석 서비스 대화 상자가 나타납니다.
3. **새 분석 서비스 - 1/6단계** 페이지에서 다음 속성을 입력합니다.

속성	설명
이름	서비스의 이름입니다. 이름은 대/소문자를 구분하지 않으며 도메인 내에서 고유해야 합니다. 이름은 128자를 초과하거나 @로 시작할 수 없습니다. 또한 공백이나 다음과 같은 특수 문자를 포함할 수도 없습니다. ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
설명	서비스에 대한 설명. 설명은 765자를 초과할 수 없습니다.
위치	서비스가 작성되는 도메인 및 폴더입니다. 다른 폴더를 선택하려면 찾아보기 를 클릭합니다. 서비스를 작성한 후 이동할 수 있습니다.
라이선스	서비스를 사용할 수 있도록 해주는 라이선스 개체입니다.
노드	서비스가 실행되는 노드입니다.

4. **다음**을 클릭합니다.
새 분석 서비스 - 2/6단계 페이지가 나타납니다.
5. Analyst 도구에서 분석 서비스와 통신하는 데 사용되는 HTTP 포트 번호를 입력합니다.
6. Analyst 도구에서 분석 서비스와 보안 통신을 수행하도록 하려면 **보안 통신 활성화**를 선택합니다.
다음 속성을 입력하여 분석 서비스에 대한 보안 통신을 구성합니다.

속성	설명
HTTPS 포트	보안 통신을 활성화하는 경우 Analyst 도구가 실행되는 포트 번호입니다. HTTP 포트 번호와 다른 포트 번호를 사용하십시오.
키 저장소 파일	디지털 인증서가 포함된 키 저장소 파일이 저장되는 디렉터리입니다.

속성	설명
키 저장소 암호	키 저장소 파일에 대한 일반 텍스트 암호입니다. 이 속성이 설정되지 않은 경우 분석 서비스는 기본 암호 changeit를 사용합니다.
SSL 프로토콜	선택 사항입니다. 사용할 프로토콜을 나타냅니다. 이 속성을 SSL로 설정합니다.

7. **서비스 활성화**를 선택합니다.
분석 서비스를 활성화하려면 모델 리포지토리 서비스 및 데이터 통합 서비스가 실행되고 있어야 합니다.
8. **다음**을 클릭합니다.
새 분석 서비스 - 3/6단계 페이지가 나타납니다.
9. 다음 속성을 입력하여 모델 리포지토리 서비스와 분석 서비스를 연결합니다.

설명	속성
모델 리포지토리 서비스	서비스와 연결할 모델 리포지토리 서비스입니다.
사용자 이름	서비스가 모델 리포지토리 서비스에 액세스하는 데 필요한 사용자 이름입니다. 작성한 모델 리포지토리 사용자를 입력합니다.
암호	모델 리포지토리 사용자의 암호입니다.
보안 도메인	모델 리포지토리 사용자에 대한 LDAP 보안 도메인입니다. Informatica 도메인에 LDAP 보안 도메인이 포함된 이 필드가 나타납니다. Kerberos 인증이 있는 도메인에서는 사용할 수 없습니다.

10. **Analyst** 도구 사용자가 휴먼 태스크 데이터에 대한 작업을 수행하도록 활성화하려면 **데이터 통합 서비스** 속성을 워크플로우를 실행하도록 구성하는 데이터 통합 서비스로 설정합니다.
Analyst 도구 사용자가 휴먼 태스크 레코드를 다룰 필요가 없으면 이 속성을 구성하지 마십시오.
11. **다음**을 클릭합니다.
새 분석 서비스 - 4/6단계 페이지가 나타납니다.
12. 분석 서비스에 대해 다음과 같은 런타임 속성을 입력합니다.

속성	설명
데이터 통합 서비스	서비스와 연결할 데이터 통합 서비스입니다. 분석 서비스는 데이터 통합 서비스에 대한 연결을 관리하고, 이 데이터 통합 서비스를 통해 사용자는 데이터 미리보기, 매핑 사양, 성과 기록표 및 프로필 작업을 Analyst 도구에서 수행할 수 있습니다. 분석 서비스를 워크플로우를 실행하도록 구성된 데이터 통합 서비스와 연결할 수 있습니다. 또는 분석 서비스를 다른 작업을 위한 또 다른 데이터 통합 서비스와 연결할 수도 있습니다.
플랫 파일 캐시 디렉터리	Analyst 도구가 업로드된 플랫 파일을 저장하는 플랫 파일 캐시의 디렉터리입니다. 데이터 통합 서비스에서도 이 디렉터리에 액세스할 수 있어야 합니다. 분석 서비스와 데이터 통합 서비스가 서로 다른 노드에서 실행되는 경우에는 공유 디렉터리를 사용하도록 플랫 파일 디렉터리를 구성합니다.

13. **다음**을 클릭합니다.
새 분석 서비스 - 5/6단계 페이지가 나타납니다.

14. 비즈니스 용어집 내보내기 프로세스에서 작성하는 비즈니스 용어집 파일을 저장할 임시 디렉터리와 콘텐츠 관리자에서 용어집 자산에 첨부하는 파일을 저장할 디렉터리를 입력합니다. 이러한 디렉터리는 분석 서비스를 실행하는 노드에 있어야 합니다.

15. **마침**을 클릭합니다.

도메인이 분석 서비스를 작성하고 활성화합니다.

마법사를 통해 서비스를 작성한 후 속성을 편집하거나 다른 속성을 구성할 수 있습니다.

분석 서비스를 생성한 후

분석 서비스를 생성한 후에는 분석 서비스에 종속된 검색 서비스를 생성합니다.

검색 서비스 작성 및 구성

검색 서비스는 **Analyst** 도구에서 검색을 수행하고 데이터 개체, 매핑 사양, 성과 기록표와 같은 프로파일링 웨어하우스 및 모델 리포지토리의 검색 결과를 반환합니다.

기본적으로 검색 서비스는 데이터 개체, 매핑 사양, 프로필, 참조 테이블, 규칙, 성과 기록표 및 비즈니스 용어집 용어와 같은 모델 리포지토리의 검색 결과를 반환합니다. 프로파일링 웨어하우스의 열 프로필 결과 및 도메인 검색 결과가 검색 결과에 포함될 수도 있습니다.

검색 서비스 작성

Administrator 도구에서 서비스 작성 마법사를 사용하여 서비스를 작성합니다.

검색 서비스를 작성하기 전에 다음 서비스를 작성하고 활성화했는지 확인합니다.

모델 리포지토리 서비스

데이터 통합 서비스

분석 서비스

1. **Administrator** 도구에서 **관리** 탭을 클릭합니다.
2. **작업 > 새로 만들기 > 검색 서비스**를 클릭합니다.
새 검색 서비스 대화 상자가 나타납니다.
3. **새 검색 서비스 - 1/2단계** 페이지에서 다음 속성을 입력합니다.

속성	설명
이름	서비스의 이름입니다. 이름은 대/소문자를 구분하지 않으며 도메인 내에서 고유해야 합니다. 이름은 128자를 초과하거나 @로 시작할 수 없습니다. 또한 공백이나 다음과 같은 특수 문자를 포함할 수도 없습니다. ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
설명	서비스에 대한 설명. 설명은 765자를 초과할 수 없습니다.

속성	설명
위치	서비스가 작성되는 도메인 및 폴더입니다. 다른 폴더를 선택하려면 찾아보기 를 클릭합니다. 서비스를 작성한 후 이동할 수 있습니다.
라이선스	서비스를 사용할 수 있도록 해주는 라이선스 개체입니다.
노드	서비스가 실행되는 노드입니다.

- 다음을 클릭합니다.
새 검색 서비스 - 2/2 단계 페이지가 나타납니다.
- 검색 서비스에 대해 다음과 같은 검색 속성을 입력합니다.

설명	속성
포트 번호	검색 서비스에 사용할 포트 번호입니다.
인덱스 위치	검색 인덱스 파일이 포함된 디렉터리입니다. 검색 서비스가 실행되는 시스템의 디렉터리를 입력하십시오. 디렉터리가 존재하지 않는 경우 Informatica는 검색 서비스를 작성할 때 디렉터리를 작성합니다.
추출 간격	검색 서비스가 업데이트된 콘텐츠를 추출 및 인덱싱하는 간격(초)입니다. 기본값은 60초입니다.
모델 리포지토리 서비스	서비스와 연결할 모델 리포지토리 서비스입니다.
사용자 이름	서비스가 모델 리포지토리 서비스에 액세스하는 데 필요한 사용자 이름입니다. 작성한 모델 리포지토리 사용자를 입력합니다.
암호	모델 리포지토리 사용자의 암호입니다.
보안 도메인	모델 리포지토리 사용자에 대한 LDAP 보안 도메인입니다. Informatica 도메인에 LDAP 보안 도메인이 포함된 이 필드가 나타납니다. Kerberos 인증이 있는 도메인에서는 사용할 수 없습니다.

- 마침**을 클릭합니다.
도메인이 검색 서비스를 작성합니다. 서비스를 작성하는 중에는 도메인이 검색 서비스를 활성화하지 않습니다. 검색 서비스를 활성화해야 사용자가 **Analyst** 도구 및 **Business Glossary Desktop**에서 검색을 수행할 수 있습니다.
- 검색 서비스를 활성화하려면 탐색기에서 해당 서비스를 선택하고 **작업 > 서비스 활성화**를 클릭합니다.
검색 서비스를 활성화하려면 모델 리포지토리 서비스, 데이터 통합 서비스 및 분석 서비스가 실행되고 있어야 합니다.

마법사를 통해 서비스를 작성한 후 속성을 편집하거나 다른 속성을 구성할 수 있습니다.

파트 V: Informatica 클라이언트 설치

이 파트에 포함된 장:

- [클라이언트 설치, 279](#)
- [자동 모드에서 설치, 286](#)

제 15 장

클라이언트 설치

이 장에 포함된 항목:

- [클라이언트 설치 개요, 279](#)
- [설치하기 전에 , 280](#)
- [클라이언트 설치, 281](#)
- [설치한 후에, 282](#)
- [PowerCenter 클라이언트 시작, 284](#)
- [Developer 도구 시작, 284](#)

클라이언트 설치 개요

Windows에서 Informatica 클라이언트를 그래픽 또는 자동 모드로 설치할 수 있습니다.

설치 준비를 위해 설치 전 태스크를 완료하십시오. 여러 시스템에 Informatica 클라이언트를 설치할 수 있습니다.

클라이언트 설치 프로그램을 실행할 경우 다음 Informatica 클라이언트 도구를 선택할 수 있습니다.

Informatica Developer

Informatica Developer는 데이터 개체를 작성하고 매핑을 작성 및 실행하고 가상 데이터베이스를 작성할 때 사용하는 클라이언트 응용 프로그램입니다.

PowerCenter 클라이언트

PowerCenter 클라이언트는 PowerCenter 리포지토리, 매핑 및 세션을 관리하기 위해 사용할 수 있는 도구 집합입니다.

참고: 동일한 설치 디렉터리에 Informatica 서비스와 PowerCenter 클라이언트를 설치하면 PowerCenter 클라이언트를 제거할 때 서비스 바이너리가 제거되므로 Informatica 서비스와 PowerCenter 클라이언트를 서로 다른 설치 디렉터리에 설치할 것을 권장합니다.

설치하기 전에

Informatica 클라이언트를 Windows에 설치하기 전에 시스템 및 타사 소프트웨어의 최소 요구 사항이 충족되는지 확인하십시오. Informatica 클라이언트를 설치할 시스템이 올바르게 구성되어 있지 않으면 설치에 실패할 수 있습니다.

Verify Installer Package Checksum

Before you run the client installer, verify the install package integrity through the cksum command. The cksum command calculates the checksum value for the installer.

Verify the checksum for the specific installer files against the checksum of the installation files downloaded from the Informatica Electronic Software Download site.

다음 테이블에는 Windows의 Informatica 클라이언트에 대한 체크섬 및 파일 크기가 나와 있습니다.

파일	체크섬 값	파일 크기
informatica_1053_client_winem-64t.zip	590321451	3139423400

A checksum mismatch can occur when there are data errors during download due to network issues or when data corruption occurs in the file on disk. For more information about the checksum errors, see [HOW TO: Identify file errors after downloading Informatica installation files.](#)

시스템 요구 사항 확인

클라이언트를 설치하기 전에 클라이언트를 설치하고 실행하기 위한 다음 설치 요구 사항이 충족되는지 확인합니다.

임시 파일의 디스크 공간

설치 프로그램은 하드 디스크에 임시 파일을 씁니다. 설치를 지원할 1GB 디스크 공간이 시스템에 있는지 확인하십시오. 설치가 완료되면 설치 프로그램이 임시 파일을 삭제하고 디스크 공간을 해제합니다.

설치 권한

클라이언트를 설치하는 데 사용하는 사용자 계정이 설치 디렉터리 및 Windows 레지스트리에 대해 쓰기 권한을 갖는지 확인합니다.

최소 시스템 요구 사항

다음 테이블에는 클라이언트를 실행하기 위한 최소 시스템 요구 사항이 나와 있습니다.

프로세서	RAM	디스크 공간
1 CPU	1GB	6GB

Informatica Developer에 대한 타사 요구 사항 확인

Developer tool을 설치하기 전에 다음 타사 설치 요구 사항을 확인하십시오.

- .NET Framework 4.0 이상을 설치합니다. 데이터 프로세서 또는 계층-관계 변환을 사용하려는 경우 Developer tool을 설치하기 전에 .NET Framework를 설치해야 합니다.

- Developer tool을 사용하거나 설치하기 전에 Microsoft Visual C++ 재배포 가능 패키지(x64)의 최신 버전을 설치합니다. Microsoft 웹사이트에서 다운로드할 수 있습니다.

PowerCenter 클라이언트에 대한 타사 요구 사항 확인

PowerCenter 클라이언트 설치에는 Mapping Architect for Visio 및 Mapping Analyst for Excel이 포함됩니다. PowerCenter 클라이언트를 설치하기 전에 Mapping Architect for Visio와 Mapping Analyst for Excel에 대한 타사 요구 사항을 모두 확인하십시오.

Mapping Architect for Visio에 대한 타사 요구 사항 확인

Visio용 매핑 아키텍처를 사용하려는 경우, PowerCenter 클라이언트 설치 전에 다음과 같은 타사 소프트웨어를 설치하십시오.

- Microsoft Visio 버전 2007 또는 2010
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4.0

중요: 올바른 버전 및 서비스 팩 수준으로 Microsoft .NET Framework를 설치하지 않으면 Mapping Architect for Visio가 제대로 설치되지 않습니다.

Mapping Analyst for Excel에 대한 타사 요구 사항 확인

Mapping Analyst for Excel에는 메타데이터 메뉴 또는 리본을 Microsoft Excel에 추가하는 Excel 추가 기능이 포함됩니다. 이 추가 기능은 Excel 2016에 대해서만 설치할 수 있습니다. Mapping Analyst for Excel을 사용하려는 경우, PowerCenter 클라이언트 설치 전에 다음과 같은 타사 소프트웨어를 설치하십시오.

- Microsoft Office Excel 버전 2016
- Java 버전 1.8 이상

클라이언트 설치

클라이언트 도구를 설치하려면 다음 단계를 수행합니다.

1. 기타 모든 응용 프로그램을 닫습니다.
2. 설치 파일의 디렉터리 루트로 이동하고 관리자 권한으로 `install.bat`를 실행합니다.
관리자로 이 파일을 실행하려면 `install.bat` 파일을 마우스 오른쪽 단추로 클릭하고 **관리자 권한으로 실행**을 선택합니다.
참고: 관리자 권한으로 설치 프로그램을 실행하지 않는 경우 Windows 시스템 관리자가 Informatica 설치 디렉터리의 파일을 액세스할 때 문제가 발생할 수 있습니다.
루트 디렉터리에서 `install.bat` 파일을 실행할 때 문제가 발생할 경우 다음 파일을 실행하십시오. <설치 프로그램 파일 디렉터리>\client\install.exe
3. **Informatica <버전> 클라이언트 설치**를 선택하고 **다음**을 클릭합니다.
4. **설치 선행 조건** 페이지에 시스템 요구 사항이 표시됩니다. 설치를 계속하기 전에 모든 설치 요구 사항이 충족되었는지 확인합니다.
5. **설치 디렉터리** 페이지에서 설치 디렉터리의 절대 경로를 입력합니다.

설치 디렉터리는 현재 컴퓨터에 있어야 합니다. 경로의 최대 길이는 260자 미만이어야 합니다. 경로의 디렉터리 이름에 공백이나 다음과 같은 특수 문자가 있어서는 안 됩니다. @|* \$ # ! % () { } [] , ; ' "

참고: Informatica는 설치 디렉터리 경로에 영숫자 문자를 사용할 것을 권장합니다. á 또는 €와 같은 특수 문자를 사용할 경우 런타임에 예기치 않은 결과가 발생할 수 있습니다.

6. If you want to install distribution packages through the Informatica installer, select the check box.
7. If you choose to install distribution packages, select one or more packages from the list that you want to install.
8. 다음을 클릭합니다.
9. **설치 전 요약** 페이지에서 설치 정보를 검토하고 **설치**를 클릭합니다.
설치 프로그램이 Developer tool 파일을 설치 디렉터리에 복사합니다.
설치 후 요약 페이지에 설치가 완료되었는지 여부가 나타납니다.
10. **완료**를 클릭하여 설치 프로그램을 닫습니다.

설치 로그 파일을 확인하면 설치 프로그램에서 수행한 태스크에 대한 자세한 정보를 볼 수 있습니다.

설치한 후에

클라이언트 도구를 설치한 후에는 다른 언어를 설치하고, 도메인 내에 보안 통신을 활성화하고, 이 도구를 시작할 수 있습니다.

언어 설치

시스템 로캘 이외의 언어로 보거나 UTF-8 코드 페이지를 사용하는 리포지토리로 작업을 수행하려면 Informatica 클라이언트와 함께 사용할 다른 언어를 Windows에 추가로 설치합니다.

참고: PowerCenter 클라이언트를 설치하고 이 언어 설치 태스크를 수행한 경우 태스크를 반복할 필요가 없습니다.

Windows IME(입력기)를 사용하려는 경우에도 언어를 설치해야 합니다.

1. **시작 > 설정 > 제어판**을 클릭하십시오.
2. **국가별 옵션**을 클릭하십시오.
3. 시스템의 언어 설정 아래에서 설치하려는 언어를 선택합니다.
4. **적용**을 클릭합니다.

언어를 설치할 때 시스템 로캘을 변경한 경우 Windows 시스템을 다시 시작하십시오.

보안 도메인을 위한 클라이언트 구성

도메인 내에서 보안 통신을 활성화하면 도메인과 Informatica 클라이언트 응용 프로그램 간의 연결도 보호됩니다. 사용되는 트러스트 저장소 파일에 따라 각 클라이언트 호스트의 환경 변수에 트러스트 저장소 파일의 위치와 암호를 지정해야 할 수 있습니다.

각 클라이언트 호스트에 다음의 환경 변수를 설정해야 할 수 있습니다.

INFA_TRUSTSTORE

이 변수를 SSL 인증서의 트러스트 저장소 파일을 포함하는 디렉터리로 설정하십시오. 이 디렉터리에는 이름이 infa_truststore.jks 및 infa_truststore.pem인 트러스트 저장소 파일이 포함되어야 합니다.

INFA_TRUSTSTORE_PASSWORD

이 변수를 `infa_truststore.jks` 파일의 암호로 설정하십시오. 이 암호는 암호화되어야 합니다. 명령줄 프로그램 `pmpasswd`를 사용하여 암호를 암호화하십시오.

Informatica는 도메인을 보호하는 데 사용할 수 있는 SSL 인증서를 제공합니다. Informatica 클라이언트를 설치할 경우 설치 프로그램이 환경 변수를 설정하고 기본적으로 다음 디렉터리에 트러스트 저장소 파일을 설치합니다. <Informatica 설치 디렉터리>\clients\shared\security

기본 Informatica SSL 인증서를 사용하고 `infa_truststore.jks` 및 `infa_truststore.pem`이 기본 디렉터리에 있는 경우에는 `INFA_TRUSTSTORE` 또는 `INFA_TRUSTSTORE_PASSWORD` 환경 변수를 설정하지 않아도 됩니다.

다음 시나리오에서는 `INFA_TRUSTSTORE` 및 `INFA_TRUSTSTORE_PASSWORD` 환경 변수를 각 클라이언트 호스트에 설정해야 합니다.

사용자 지정 SSL 인증서를 사용하여 도메인을 보호하는 경우

도메인을 보호하는 데 사용할 SSL 인증서를 제공할 경우 `infa_truststore.jks` 및 `infa_truststore.pem` 트러스트 저장소 파일을 각 클라이언트 호스트에 복사합니다. 파일의 위치와 트러스트 저장소 암호를 지정해야 합니다.

기본 Informatica SSL 인증서를 사용하지만 트러스트 저장소 파일이 기본 Informatica 디렉터리에 없는 경우

기본 Informatica SSL 인증서를 사용하지만 `infa_truststore.jks` 및 `infa_truststore.pem` 트러스트 저장소 파일이 기본 Informatica 디렉터리에 없는 경우에는 파일의 위치와 트러스트 저장소 암호를 지정해야 합니다.

Developer tool 작업 공간 디렉터리 구성

사용자가 로그인한 시스템에 작업 공간 메타데이터를 쓰도록 Informatica Developer를 구성하십시오.

참고: PowerCenter 클라이언트를 설치하고 이 태스크를 수행한 경우 이 태스크를 반복할 필요가 없습니다.

1. 다음 디렉터리로 이동합니다. <Informatica 설치 디렉터리>\clients\DeveloperClient\configuration\
2. `config.ini` 파일을 찾습니다.
3. `config.ini` 파일의 백업 사본을 작성합니다.
4. 텍스트 편집기를 사용하여 `config.ini` 파일을 엽니다.
5. `osgi.instance.area.default` 변수를 `config.ini` 파일의 끝에 추가하고 이 변수를 작업 공간 메타데이터를 저장하려는 디렉터리 위치로 설정합니다. 파일 경로에 ANSI 아닌 문자가 포함될 수 없습니다. 작업 공간 디렉터리의 폴더 이름에 숫자 기호(#) 문자가 포함될 수 없습니다. 작업 공간 디렉터리의 폴더 이름에 공백이 포함되어 있으면 전체 디렉터리를 큰따옴표로 묶습니다.

- 로컬 시스템에서 Informatica Developer를 실행하는 경우, 이 변수를 작업 공간 디렉터리의 절대 경로로 설정합니다.

```
osgi.instance.area.default=<Drive>/<WorkspaceDirectory>
```

또는

```
osgi.instance.area.default=<Drive>\\<WorkspaceDirectory>
```

- 원격 시스템에서 Informatica Developer를 실행하는 경우, 이 변수를 로컬 시스템의 디렉터리 위치로 설정합니다.

```
osgi.instance.area.default=\\\\<LocalMachine>/<WorkspaceDirectory>
```

또는

```
osgi.instance.area.default=\\\\<LocalMachine>\\<WorkspaceDirectory>
```

사용자에게 로컬 작업 공간 디렉터리에 대한 쓰기 권한이 있어야 합니다.

Informatica Developer는 작업 공간 메타데이터를 작업 공간 디렉터리에 씁니다. 로컬 시스템에서 Informatica Developer에 로그인하는 경우, Informatica Developer는 작업 공간 메타데이터를 로컬 시스템에 씁니다. 로그인한 시스템에 작업 공간 디렉터리가 없으면 Informatica Developer가 파일을 쓸 때 디렉터리를 작성합니다.

Informatica Developer를 시작할 때 작업 공간 디렉터리를 재정의할 수 있습니다.

PowerCenter 클라이언트 시작

PowerCenter 클라이언트를 시작할 때 PowerCenter 리포지토리에 연결하십시오.

1. Windows 시작 메뉴에서 **프로그램 > Informatica [버전] > 클라이언트 > [클라이언트 도구 이름]**을 클릭합니다.
PowerCenter 클라이언트 도구를 처음 실행할 때 리포지토리를 추가하고 해당 리포지토리에 연결해야 합니다.
2. **리포지토리 > 리포지토리 추가**를 클릭합니다.
리포지토리 추가 대화 상자가 나타납니다.
3. 리포지토리 및 사용자 이름을 입력합니다.
4. **확인**을 클릭합니다.
리포지토리가 탐색기에 표시됩니다.
5. **리포지토리 > 연결**을 클릭합니다.
리포지토리에 연결 대화 상자가 표시됩니다.
6. 연결 설정 섹션에서 **추가**를 클릭하여 도메인 연결 정보를 추가합니다.
도메인 추가 대화 상자가 나타납니다.
7. 도메인 이름, 게이트웨이 호스트 및 게이트웨이 포트 번호를 입력합니다.
8. **확인**을 클릭합니다.
9. **리포지토리에 연결** 대화 상자에서 관리자 사용자의 암호를 입력합니다.
10. 보안 도메인을 선택합니다.
11. **연결**을 클릭합니다.
리포지토리에 연결한 후 개체를 작성할 수 있습니다.

Developer 도구 시작

Developer 도구를 시작할 때 모델 리포지토리에 연결하십시오. 모델 리포지토리는 Developer 도구에서 작성되는 메타데이터를 저장합니다. 모델 리포지토리 서비스에서 모델 리포지토리를 관리합니다. 프로젝트를 작성하기 전에 이 리포지토리에 연결하십시오.

1. Windows 시작 메뉴에서 **프로그램 > Informatica [버전] > 클라이언트 > Developer 클라이언트 > Informatica Developer 실행**을 클릭합니다.
Developer 도구를 처음 실행하면 시작 페이지에 여러 아이콘이 표시됩니다. 이후에는 Developer 도구를 실행할 때 시작 페이지가 나타나지 않습니다.
2. **작업 영역**을 클릭합니다.
작성되는 개체를 저장할 리포지토리를 Developer 도구를 처음 시작할 때 선택해야 합니다.
3. **파일 > 리포지토리에 연결**을 클릭합니다.
리포지토리에 연결 대화 상자가 표시됩니다.

4. **Developer** 도구에서 도메인을 구성하지 않은 경우 **도메인 구성**을 클릭하여 도메인을 구성합니다.
모델 리포지토리 서비스에 액세스하도록 도메인을 구성해야 합니다.
 5. **추가**를 클릭하여 도메인을 추가합니다.
새 도메인 대화 상자가 표시됩니다.
 6. 도메인 이름, 호스트 이름 및 포트 번호를 입력합니다.
 7. **마침**을 클릭합니다.
 8. **확인**을 클릭합니다.
 9. **리포지토리에 연결** 대화 상자에서 **찾아보기**를 클릭한 후 모델 리포지토리 서비스를 선택합니다.
 10. **확인**을 클릭합니다.
 11. **다음**을 클릭합니다.
 12. 사용자 이름 및 암호를 입력하십시오.
 13. **마침**을 클릭합니다.
- Developer** 도구의 개체 탐색기 보기에 모델 리포지토리가 추가됩니다. 다음에 **Developer** 도구를 실행할 때 동일한 리포지토리에 연결할 수 있습니다.

제 16 장

자동 모드에서 설치

이 장에 포함된 항목:

- [자동 모드에서 설치 개요, 286](#)
- [Configure the Properties File, 286](#)
- [자동 설치 프로그램 실행, 287](#)

자동 모드에서 설치 개요

사용자 상호 작용 없이 **Informatica** 클라이언트를 설치하려면 자동 모드로 설치하십시오.

설치 옵션을 지정하려면 속성 파일을 사용합니다. 설치 프로그램은 이 파일을 읽어 설치 옵션을 확인합니다. 자동 모드 설치를 사용하여 네트워크의 여러 시스템에 **Informatica** 클라이언트를 설치하거나 시스템 간에 설치를 표준화할 수 있습니다.

자동 모드에서 설치하려면 다음 태스크를 완료하십시오.

1. 설치 속성 파일을 구성하고 속성 파일에 설치 옵션을 지정합니다.
2. 설치 속성 파일을 사용하여 설치 프로그램을 실행합니다.

Configure the Properties File

Informatica provides a sample properties file that includes the properties required by the installer. Customize the sample properties file to create a properties file and specify the options for your installation. Then run the silent installation.

The sample SilentInput.properties file is stored in the installer download location.

1. Go to the root of the directory that contains the installation files.
2. Locate the sample SilentInput.properties file.
3. Create a backup copy of the SilentInput.properties file.
4. Use a text editor to open and modify the values of the properties in the file.

The following table describes the installation properties that you can modify:

Property Name	Description
INSTALL_TYPE	Indicates whether to install or upgrade the Informatica clients. If the value is 0, the Informatica clients are installed in the directory you specify. If the value is 1, the Informatica clients are upgraded. Default is 0.
USER_INSTALL_DIR	Informatica client installation directory.
DXT_COMP	Indicates whether to install Informatica Developer. If the value is 1, the Developer tool will be installed. If the value is 0, the Developer tool will not be installed. Default is 1.
INSTALL_HADOOP_LIBRARIES	Determines whether to install distribution packages through the installer. Set the value to true if you want to install distribution packages through the installer. Set the value to false if you don't need distribution packages or if you want to install them later.
SELECTED_HADOOP_LIBRARIES	Determines the distribution packages that you want to install from the supported packages list. Enter the distribution packages that you want to install, separating multiple packages with a comma.

5. Save the properties file.

자동 설치 프로그램 실행

속성 파일을 구성한 후 명령 프롬프트를 열어 자동 설치를 시작하십시오.

1. 명령 프롬프트를 엽니다.
2. 설치 파일을 포함하는 디렉터리의 루트로 이동합니다.
3. 편집하고 다시 저장한 **SilentInput.properties** 파일이 이 디렉터리에 있는지 확인합니다.
4. 자동 설치를 실행하기 위해 **silentInstall.bat**를 실행합니다.

자동 설치 프로그램이 백그라운드에서 실행됩니다. 이 프로세스에는 다소 시간이 걸릴 수 있습니다. **Informatica_<버전>_Client_InstallLog<타임스탬프>.log** 파일이 설치 디렉터리에 생성되면 자동 설치가 완료된 것입니다.

속성 파일을 잘못 구성하거나 설치 디렉터리에 액세스할 수 없는 경우 자동 설치가 실패합니다. 설치 로그 파일을 살펴보고 오류를 수정하십시오. 그런 다음 자동 설치를 다시 실행하십시오.

파트 VI: 제거

이 파트에 포함된 장:

- [제거, 289](#)

제 17 장

제거

이 장에 포함된 항목:

- [Informatica 제거 개요, 289](#)
- [제거 규칙 및 지침, 289](#)
- [콘솔 모드에서 Informatica 서버 제거, 290](#)
- [자동 모드에서 Informatica 서버 제거, 290](#)
- [그래픽 모드에서 Informatica 서버 제거, 291](#)
- [Informatica 클라이언트 제거, 291](#)

Informatica 제거 개요

Informatica 서버 또는 클라이언트를 시스템에서 제거하려면 Informatica를 제거하십시오.

Informatica 제거 프로세스는 시스템에서 모든 Informatica 파일을 삭제하고 모든 Informatica 구성을 지웁니다. 제거 프로세스에서 Informatica와 함께 설치되지 않은 파일은 삭제하지 않습니다. 설치 프로세스에서 임시 디렉터리를 작성하는 경우를 예로 들어 보겠습니다. 제거 프로그램은 이러한 디렉터리를 기록해 두지 않기 때문에 해당 디렉터리를 삭제할 수 없습니다. 이러한 디렉터리를 완전히 제거하려면 수동으로 삭제해야 합니다.

중요: Informatica 서비스와 PowerCenter 클라이언트를 동일한 설치 디렉터리에 설치한 경우 PowerCenter 클라이언트를 제거할 때 서비스 바이너리가 제거됩니다.

제거 규칙 및 지침

Informatica 구성 요소를 제거할 경우 다음 규칙 및 지침을 사용하십시오.

- Informatica 서버 제거 모드는 Informatica 서버 설치를 위해 사용한 모드에 따라 달라집니다. Informatica 서버를 콘솔 모드에서 설치한 경우를 예로 들어 보겠습니다. 이 경우 제거 프로그램을 실행하면 제거 프로그램이 콘솔 모드에서 실행됩니다. Informatica 클라이언트 제거 모드는 Informatica 클라이언트 설치를 위해 사용한 모드에 따라 달라지지 않습니다. Informatica 클라이언트를 자동 모드에서 설치한 경우를 예로 들어 보겠습니다. 이 경우 제거 프로그램을 실행하면 제거 프로그램은 그래픽 또는 자동 모드에서 실행될 수 있습니다.
- Informatica를 제거해도 Informatica 리포지토리는 영향을 받지 않습니다. 제거 프로그램이 제거하는 것은 Informatica 파일입니다. 제거 프로그램은 데이터베이스에서 리포지토리를 제거하지 않습니다. 리포지토리를 이동해야 하는 경우, 리포지토리를 백업한 후에 다른 데이터베이스에 리포지토리를 복원할 수 있습니다.

- Informatica를 제거해도 도메인 구성 데이터베이스에서 메타데이터 테이블이 제거되지는 않습니다. 동일한 도메인 구성 데이터베이스 및 사용자 계정을 사용하여 Informatica를 다시 설치할 경우, 수동으로 테이블을 제거하거나 테이블 덮어쓰기를 선택해야 합니다. `infasetup BackupDomain` 명령을 사용하면 메타데이터 테이블을 덮어쓰기 전에 도메인 구성 데이터베이스를 백업할 수 있습니다. 메타데이터 테이블을 수동으로 제거하려면 제거 프로그램을 실행하기 전에 `infasetup DeleteDomain` 명령을 사용하십시오.
- Informatica를 제거하면 Informatica 설치 디렉터리에서 모든 설치 파일 및 하위 디렉터리가 제거됩니다. Informatica를 제거하기 전에 모든 Informatica 서비스 및 프로세스를 중지하고 설치 디렉터리의 모든 파일이 닫혀 있는지 확인하십시오. 제거 프로세스가 끝나면 제거하지 못한 파일 및 디렉터리의 이름이 제거 프로그램에 표시됩니다.
- Informatica 서버를 설치하면 Informatica 개발 플랫폼 API를 사용하여 작성된 타사 어댑터에 필요한 파일 및 라이브러리를 위해 다음 폴더가 작성됩니다.
<Informatica 설치 디렉터리>/services/shared/extensions
Informatica 서버를 제거하면 이 폴더 및 해당 폴더 아래에 작성된 모든 하위 폴더가 삭제됩니다. 어댑터 파일이 /extensions 폴더에 저장되어 있으면 제거를 시작하기 전에 해당 폴더를 백업하십시오.
- 컴퓨터에서 제거를 수행하는 경우 제거하기 전에 ODBC 폴더를 백업해야 합니다. 제거가 완료된 후에 해당 폴더를 복원하십시오.

콘솔 모드에서 Informatica 서버 제거

Informatica 서버를 콘솔 모드에서 설치한 경우, Informatica 서버를 콘솔 모드에서 제거하십시오.

제거 프로그램을 실행하기 전에 모든 Informatica 서비스 및 프로세스를 중지하고 설치 디렉터리의 모든 파일이 닫혀 있는지 확인하십시오. 제거 프로세스는 열려 있는 파일이나 실행 중인 프로세스 또는 서비스에서 사용하고 있는 파일을 제거할 수 없습니다.

1. 다음 디렉터리로 이동합니다.

```
<Informatica 설치 디렉터리>/Uninstaller_Server
```

2. 다음 명령을 입력하여 제거 프로그램을 실행합니다.

```
./uninstaller.sh
```

Informatica 서버를 콘솔 모드에서 설치한 경우, 제거 프로그램이 콘솔 모드에서 시작됩니다.

자동 모드에서 Informatica 서버 제거

Informatica 서버를 자동 모드에서 설치한 경우에는 자동 모드에서 제거해야 합니다.

제거 프로그램을 실행하기 전에 모든 Informatica 서비스 및 프로세스를 중지하고 설치 디렉터리의 모든 파일이 닫혀 있는지 확인하십시오. 제거 프로세스는 열려 있는 파일이나 실행 중인 프로세스 또는 서비스에서 사용하고 있는 파일을 제거할 수 없습니다.

1. 다음 디렉터리로 이동합니다.

```
<Informatica 설치 디렉터리>/Uninstaller_Server
```

2. 다음 명령을 입력하여 자동 제거 프로그램을 실행합니다.

```
./uninstaller.sh
```

Informatica 서버를 자동 모드에서 설치한 경우, 제거 프로그램이 자동 모드에서 시작됩니다. 자동 설치 제거 프로그램은 백그라운드에서 실행됩니다. 이 프로세스에는 다소 시간이 걸릴 수 있습니다. 설치 디렉터리에 액세스할 수 없는 경우 자동 설치 제거가 실패합니다.

Informatica 서버를 제거한 후에 나머지 폴더 및 파일을 Informatica 설치 디렉터리에서 삭제합니다. 예를 들면 다음과 같습니다.

- Informatica_<버전>_Services_InstallLog.log 파일
- Informatica_<버전>_Services_<타임스탬프>.log 파일

그래픽 모드에서 Informatica 서버 제거

제거 프로그램을 실행하기 전에 모든 Informatica 서비스 및 프로세스를 중지하고 설치 디렉터리의 모든 파일이 닫혀 있는지 확인하십시오. 제거 프로세스는 열려 있는 파일이나 실행 중인 프로세스 또는 서비스에서 사용하고 있는 파일을 제거할 수 없습니다.

1. **시작 > 프로그램 파일 > Informatica [버전] > 서버 > 제거 프로그램**을 클릭합니다.
제거 페이지가 표시됩니다.
2. **제거**를 클릭하여 제거를 시작합니다.
설치 프로그램에서 해당 디렉터리의 모든 Informatica 파일을 삭제하면 **제거 후 요약** 페이지가 표시됩니다.
3. **완료**를 클릭하여 제거 프로그램을 닫습니다.

Informatica 서버를 제거한 후에 나머지 폴더 및 파일을 Informatica 설치 디렉터리에서 삭제합니다. 예를 들면 다음과 같습니다.

- Informatica_<버전>_Client_InstallLog.log 파일
- Informatica_<버전>_Client.log 파일

시스템에서 로그아웃하고 다시 로그인합니다. 그런 다음 Informatica 전용 CLASSPATH 및 PATH 환경 변수를 지웁니다.

Informatica 클라이언트 제거

Windows에서 Informatica 클라이언트를 그래픽 모드 및 자동 모드로 제거할 수 있습니다.

Informatica 클라이언트를 제거하면 설치 프로그램이 설치 도중 작성하는 환경 변수 INFA_TRUSTSTORE를 제거하지 않습니다. 이후 버전의 Informatica 클라이언트를 설치하는 경우 환경 변수가 SSL 인증서의 새 값을 가리키도록 환경 변수를 편집해야 합니다.

그래픽 모드에서 Informatica 클라이언트 제거

Informatica 클라이언트를 그래픽 모드에서 설치한 경우, Informatica 클라이언트를 그래픽 모드에서 제거하십시오.

1. **시작 > 프로그램 파일 > Informatica [버전] > 클라이언트 > 제거 프로그램**을 클릭합니다.
제거 페이지가 표시됩니다.
2. **다음**을 클릭합니다.

응용 프로그램 클라이언트 제거 선택 페이지가 표시됩니다.

3. 제거하려는 클라이언트 응용 프로그램을 선택하고 **제거**를 클릭합니다.
4. **완료**를 클릭하여 제거 프로그램을 닫습니다.

설치가 완료되면 **제거 후 요약** 페이지에 제거 결과가 표시됩니다.

Informatica 클라이언트를 제거한 후에 나머지 폴더 및 파일을 Informatica 설치 디렉터리에서 삭제합니다. 예를 들면 다음과 같습니다.

- Informatica_<버전>_Client_InstallLog.log 파일
- Informatica_<버전>_Client.log 파일

시스템에서 로그아웃하고 다시 로그인합니다. 그런 다음 Informatica 전용 CLASSPATH 및 PATH 환경 변수를 지웁니다.

자동 모드에서 Informatica 클라이언트 제거

Informatica 클라이언트를 자동 모드에서 설치한 경우, Informatica 클라이언트를 자동 모드에서 제거하십시오.

속성 파일 생성

Informatica는 설치 프로그램에 필요한 속성이 포함된 샘플 속성 파일을 제공합니다.

샘플 속성 파일을 사용자 지정하여 속성 파일을 생성하고 제거에 필요한 옵션을 지정하십시오. 그런 다음 자동 제거를 실행하십시오.

1. <Informatica 설치 디렉터리>/Uninstaller_Client로 이동합니다.
2. 샘플 SilentInput.properties 파일을 찾습니다.
3. SilentInput.properties 파일의 백업 사본을 생성합니다.
4. 텍스트 편집기를 사용하여 속성 파일을 열고 해당 파일에서 값을 수정합니다.

다음 테이블에는 수정할 수 있는 속성이 설명되어 있습니다.

속성 이름	설명
DXT_COMP	Informatica Developer를 제거할지 여부를 나타냅니다. 이 값이 1이면 Developer tool이 제거됩니다. 이 값이 0이면 Developer tool이 제거되지 않습니다. 기본값은 1입니다.

5. SilentInput.properties 파일을 저장합니다.

자동 제거 프로그램 실행

속성 파일을 구성한 후에 자동 제거를 실행하십시오.

1. <Informatica 설치 디렉터리>/Uninstaller_Client로 이동합니다.
2. 자동 제거를 실행하려면 uninstaller.bat 또는 uninstaller.exe 파일을 두 번 클릭합니다.

자동 설치 제거 프로그램은 백그라운드에서 실행됩니다. 이 프로세스에는 다소 시간이 걸릴 수 있습니다. 속성 파일을 잘못 구성하거나 설치 디렉터리에 액세스할 수 없는 경우 자동 제거가 실패합니다.

Informatica 클라이언트를 제거한 후에 나머지 폴더 및 파일을 Informatica 설치 디렉터리에서 삭제합니다. 예를 들면 다음과 같습니다.

- Informatica_<버전>_Client_InstallLog.log 파일
- Informatica_<버전>_Client.log 파일

시스템에서 로그아웃하고 다시 로그인합니다. 그런 다음 Informatica 전용 CLASSPATH 및 PATH 환경 변수를 지웁니다.

부록 A

Informatica 서비스 시작 및 중지

이 부록에 포함된 항목:

- [Informatica 서비스 시작 및 중지 개요, 294](#)
- [Informatica 서비스 시작 및 중지 \(콘솔 사용\), 294](#)
- [Informatica Administrator에서 Informatica 중지, 295](#)
- [제어판에서 Informatica 시작 또는 중지, 295](#)
- [시작 메뉴에서 Informatica 시작 또는 중지, 295](#)
- [명령 프롬프트에서 Informatica 시작 또는 중지, 295](#)
- [Informatica 시작 또는 중지에 대한 규칙 및 지침, 296](#)

Informatica 서비스 시작 및 중지 개요

Informatica 서비스는 해당 노드의 서비스 관리자를 실행하고, 서비스 관리자는 모든 도메인 기능을 관리하고 노드에서 실행되도록 구성된 응용 프로그램 서비스를 시작합니다. Informatica를 시작 또는 중지하는 데 사용되는 방법은 운영 체제에 따라 달라집니다. 노드를 종료하기 위해 Informatica Administrator를 사용할 수 있습니다. 노드를 종료하면 해당 노드에서 Informatica가 중지됩니다.

또한 Informatica 서비스는 Informatica Administrator 도구를 실행합니다. Informatica Administrator는 Informatica 도메인 개체 및 사용자 계정을 관리하는 데 사용됩니다. Informatica 사용자의 사용자 계정을 작성하고 도메인에 응용 프로그램 서비스를 작성 및 구성하려면 Informatica Administrator에 로그인하십시오.

Informatica 서비스 시작 및 중지 (콘솔 사용)

infaservice.sh를 실행하여 Informatica 데몬을 시작 및 중지합니다. 기본적으로 infaservice.sh는 다음 디렉터리에 설치됩니다.

```
<Informatica installation directory>/tomcat/bin
```

1. infaservice.sh가 있는 디렉터리로 이동합니다.
2. 명령 프롬프트에서 다음 명령을 입력하여 데몬을 시작합니다.

```
infaservice.sh startup
```

데몬을 중지하려면 다음 명령을 입력합니다.

```
infaservice.sh shutdown
```

참고: 소프트 링크를 사용하여 `infaservice.sh`의 위치를 지정하는 경우, `INFA_HOME` 환경 변수를 Informatica 설치 디렉터리의 위치로 설정합니다.

Informatica Administrator에서 Informatica 중지

Informatica Administrator를 사용하여 노드를 종료하면 해당 노드에서 Informatica 서비스가 중지됩니다.

실행 중인 프로세스를 중단하거나 서비스 종료 전에 프로세스가 완료되도록 허용할 수 있습니다. 노드를 종료하고 해당 노드에서 실행 중인 리포지토리 서비스 프로세스를 중단하면 리포지토리에 아직 쓰여지지 않은 변경 내용이 손실될 수 있습니다. 통합 서비스 프로세스를 실행하는 노드를 중단하면 해당 워크플로우가 중단됩니다.

1. Informatica Administrator에 로그인합니다.
2. 탐색기에서 종료할 노드를 선택합니다.
3. 도메인 탭의 **작업** 메뉴에서 **노드 종료**를 선택합니다.

제어판에서 Informatica 시작 또는 중지

Informatica Windows 서비스를 시작하거나 중지하기 위한 절차는 다른 모든 Windows 서비스와 동일합니다.

1. Windows 제어판을 엽니다.
2. **관리 도구**를 선택합니다.
3. 서비스를 마우스 오른쪽 단추로 클릭하고 **관리자 권한으로 실행**을 선택합니다.
4. Informatica 서비스를 마우스 오른쪽 단추로 클릭합니다.
5. 해당 서비스가 실행 중이면 **중지**를 클릭합니다.
해당 서비스가 중지되어 있으면 **시작**을 클릭합니다.

시작 메뉴에서 Informatica 시작 또는 중지

Windows 시작 메뉴에서 Informatica를 시작하려면 **프로그램 > Informatica [버전] > 서버**를 클릭합니다. Informatica 서비스 시작을 마우스 오른쪽 단추로 클릭하고 **관리자 권한으로 실행**을 선택합니다.

Windows 시작 메뉴에서 Informatica를 중지하려면 **프로그램 > Informatica [버전] > 서버**를 클릭합니다. Informatica 서비스 중지를 마우스 오른쪽 단추로 클릭하고 **관리자 권한으로 실행**을 선택합니다.

명령 프롬프트에서 Informatica 시작 또는 중지

명령줄에서 `infaservice.bat`를 실행하여 Windows의 Informatica 서비스를 시작하고 중지할 수 있습니다.

기본적으로 `infaservice.bat`는 다음 디렉터리에 설치됩니다.

<Informatica 설치 디렉터리>\tomcat\bin

1. 관리자로서 명령 프롬프트를 엽니다.
2. `infaservice.bat`가 있는 디렉터리로 이동합니다.
3. 다음 명령을 입력하여 **Informatica** 서비스를 시작합니다.
`infaservice.bat startup`
다음 명령을 입력하여 **Informatica** 서비스를 중지합니다.
`infaservice.bat shutdown`

Informatica 시작 또는 중지에 대한 규칙 및 지침

노드에서 **Informatica**를 시작 및 중지할 경우 다음 규칙 및 지침을 고려하십시오.

- 노드를 종료하면 도메인에서 해당 노드를 사용할 수 없게 됩니다. 게이트웨이 노드를 종료한 경우 도메인에 다른 게이트웨이 노드가 없으면 해당 도메인을 사용할 수 없습니다.
- **Informatica**를 시작할 때 노드의 서비스에 의해 사용되는 포트를 사용할 수 있는지 확인하십시오. 예를 들어 노드에서 **Informatica**를 중지한 경우, **Informatica**를 다시 시작하기 전에 시스템의 다른 프로세스에서 해당 포트를 사용하지 않는지 확인하십시오. 포트를 사용할 수 없는 경우 **Informatica**가 시작되지 않습니다.
- **Informatica Administrator**를 사용하지 않고 노드를 종료하면 해당 노드에서 실행 중인 모든 프로세스가 중단됩니다. 노드를 종료하기 전에 모든 프로세스가 완료될 때까지 대기하려면 **Informatica Administrator**를 사용하십시오.
- 도메인에 있는 2개의 노드 중 하나가 응용 프로그램 서비스의 기본 노드로 구성되고 다른 노드는 백업 노드로 구성되어 있는 경우, 백업 노드를 시작하기 전에 기본 노드에서 **Informatica**를 시작하십시오. 그렇지 않으면 기본 노드가 아니라 백업 노드에서 응용 프로그램 서비스가 실행됩니다.

부록 B

배포 패키지 관리

이 부록에 포함된 항목:

- [Managing Distribution Packages Overview, 297](#)
- [Before You Begin, 297](#)
- [Install or Remove Distribution Packages in Console Mode, 298](#)
- [Install or Remove Distribution Packages in Silent Mode, 299](#)
- [After You Install, 300](#)

Managing Distribution Packages Overview

You can use Integration Package Manager (the package manager) to install and remove distribution packages from the Informatica service and client machines.

A distribution package is a set of distribution binaries that you install within the domain for the following processing requirements:

- To push processing to the Hadoop or Databricks environment.
- To process complex files within the Informatica domain.
- To connect to the Hadoop or Databricks environment when you process within the Informatica domain.

You can install distribution packages if you didn't do so during the upgrade or install process or if you want to add a distribution package. You can remove a distribution package if you want to use a different package or if you installed a package that you don't use.

When you install or remove distribution packages, verify that you perform the operation on all service and client machines.

Before You Begin

Before you run the package manager, perform tasks such as setting environment variables and downloading files.

1. Shut down the Informatica services.

2. Set one of the following environment variables:

Variable	Description
INFA_JDK_HOME	Location of the folder containing the supported Java Development Kit (JDK). Set the INFA_JDK_HOME environment variable in the following scenarios: <ul style="list-style-type: none"> - Informatica domain is on Windows or Linux - Informatica client
INFA_JRE_HOME	Location of the folder containing the supported Java Runtime Environment (JRE). If the Informatica domain is on AIX, set the INFA_JRE_HOME environment variable.

3. Verify that the user that runs the package manager has read and write permissions on the Informatica installation directory and execute permissions on the executable file.
4. Download the following files from the Informatica Electronic Software Download site:
 - [Integration Package Manager](#)
 - [Distribution packages](#)
5. Extract the Integration Package Manager ZIP files to a local drive.
6. Copy the ZIP files of distribution packages that you need to the following location: <Integration Package Manager directory>/source

참고: The package manager fails if the ZIP files for distribution packages aren't available in the source directory.

Install or Remove Distribution Packages in Console Mode

You can run the package manager in console mode to install or remove distribution packages.

1. From the package manager directory, run one of the following commands:
 - `./Server.sh console` for Linux or UNIX
 - `Server.bat console` for Windows
 - `Client.bat console` for client

참고: To run the command on Windows, use the administrator command prompt.

2. Enter the installation directory of the services or client and press **Enter**.
3. Choose the operation type and press **Enter**.
 - Select 1 to remove existing distribution packages.
 - Select 2 to install one or more distribution packages.

The console lists the distribution packages that you can install or remove.

4. Enter the distribution packages that you want to install or remove, separating multiple packages with a comma, and press **Enter**.

5. Verify the installation or removal status in the package manager log file.

You can find the log file in the following location: <Integration Package Manager directory>/IntegrationPackageManager_<date and timestamp>.log

Install or Remove Distribution Packages in Silent Mode

You can run the package manager in silent mode to install or remove distribution packages. The silent input properties file contains the properties for the package manager to run in silent mode for service and clients. Set the appropriate value for each property in the file.

1. Find the IntegrationPackageManager.properties file in the following location: <Integration Package Manager directory>/
2. Edit the properties file in a text editor.

The following table describes the properties that you can modify:

Property Name	Description
USER_INSTALL_DIR	The installation directory of the service or client.
OPERATION_TYPE	The operation that you want to perform: <ul style="list-style-type: none">- Set to DELETE to remove existing distribution packages.- Set to EXTRACT to install one or more distribution packages.
SELECTED_HADOOP_LIBRARIES	Lists the distribution packages and versions. Enter the distribution packages that you want to install or remove. Separate multiple packages with a comma.

3. Save the properties file.
4. From the package manager directory, run one of the following commands:
 - ./Server.sh silent for Linux or UNIX
 - Server.bat silent for Windows
 - Client.bat silent for client

참고: To run the command on Windows, use the administrator command prompt.

5. Verify the installation or removal status in the package manager log file.

You can find the log file in the following location: <Integration Package Manager directory>/IntegrationPackageManager_<date and timestamp>.log

After You Install

To use the distribution packages that are installed using the package manager, configure the property or environment variable in service and client machines.

Configure the Developer Tool

After you install the distribution packages in the Developer tool, update the developerCore.ini file with the installed distribution package.

1. Find the developerCore.ini file in the following location: <Informatica installation directory>\clients\DeveloperClient
2. Edit the file to update the following property:
-DINFA_HADOOP_DIST_DIR=hadoop\<Hadoop distribution name>_<version>
For example,
-DINFA_HADOOP_DIST_DIR=hadoop\CDH_7.1
3. Restart the Developer tool.

Configure Environment Variables

Some adapters require environment variables for the Data Integration Service and Metadata Access Service to access the distribution packages. For more information, see [Configure environment variables to process complex files](#).

부록 C

UNIX 또는 Linux에서 데이터베이스에 연결

이 부록에 포함된 항목:

- [UNIX 또는 Linux에서 데이터베이스에 연결 개요, 301](#)
- [IBM DB2 범용 데이터베이스에 연결, 302](#)
- [Informix 데이터베이스에 연결, 304](#)
- [Microsoft SQL Server 데이터베이스에 연결, 305](#)
- [Netezza 데이터베이스에 연결, 306](#)
- [Oracle 데이터베이스에 연결, 308](#)
- [PostgreSQL 데이터베이스에 연결, 310](#)
- [Sybase ASE 데이터베이스에 연결, 314](#)
- [Teradata 데이터베이스에 연결, 316](#)
- [JDBC 데이터 소스에 연결, 318](#)
- [ODBC 데이터 소스에 연결, 319](#)
- [샘플 `odbc.ini` 파일, 321](#)

UNIX 또는 Linux에서 데이터베이스에 연결 개요

원시 연결을 사용하려면 액세스할 데이터베이스의 데이터베이스 클라이언트 소프트웨어를 설치 및 구성해야 합니다. 응용 프로그램 서비스와 데이터베이스 간에 호환성을 보장하려면 데이터베이스 버전과 호환되는 클라이언트 소프트웨어를 설치하고 적절한 데이터베이스 클라이언트 라이브러리를 사용하십시오. 성능을 개선하려면 원시 연결을 사용하십시오.

Informatica 설치에는 DataDirect ODBC 드라이버가 포함됩니다. 이전 버전의 드라이버를 사용하여 기존 ODBC 데이터 소스를 작성한 경우 새 드라이버를 사용하여 새 ODBC 데이터 소스를 작성해야 합니다.

Informatica에서 제공하는 DataDirect ODBC 드라이버 또는 수준 2 이상과 호환되는 타사 ODBC 드라이버를 사용하여 ODBC 연결을 구성하십시오.

Informatica 도메인의 다음 서비스에 대해 데이터베이스 연결을 구성해야 합니다.

- PowerCenter 리포지토리 서비스
- 모델 리포지토리 서비스
- 데이터 통합 서비스

- 분석 서비스

Linux 또는 UNIX에서 데이터베이스에 연결하는 경우 원시 드라이버를 사용하여 IBM DB2, Oracle 또는 Sybase ASE 데이터베이스에 연결합니다. ODBC를 사용하여 다른 소스 및 대상에 연결할 수 있습니다.

IBM DB2 범용 데이터베이스에 연결

원시 연결의 경우 IBM DB2 데이터베이스 서버 버전에 해당하는 IBM DB2 CAE(Client Application Enabler) 버전을 설치하십시오. Informatica와 데이터베이스 간 호환성을 보장하려면 적절한 데이터베이스 클라이언트 라이브러리를 사용하십시오.

원시 연결 구성

IBM DB2 데이터베이스에 대한 원시 연결을 구성하여 성능을 개선할 수 있습니다.

다음 단계에서는 원시 연결을 구성하기 위한 지침을 제공합니다. 특정한 지침은 데이터베이스 설명서를 참조하십시오.

1. 데이터 통합 서비스, PowerCenter 통합 서비스 또는 PowerCenter 리포지토리 서비스 프로세스가 실행되는 시스템에서 연결을 구성하려면 서비스 프로세스를 시작할 수 있는 사용자로 시스템에 로그인합니다.
2. DB2INSTANCE, INSTHOME, DB2DIR 및 PATH 환경 변수를 설정합니다.

UNIX IBM DB2 소프트웨어에는 연결된 사용자 계정(주로 db2admin)이 항상 있으며, 이 계정은 데이터베이스 구성의 홀더 역할을 합니다. 이 사용자가 DB2 인스턴스를 소유합니다.

DB2INSTANCE. 인스턴스 홀더의 이름입니다.

Bourne 셸 사용:

```
$ DB2INSTANCE=db2admin; export DB2INSTANCE
```

C 셸 사용:

```
$ setenv DB2INSTANCE db2admin
```

INSTHOME. db2admin 홈 디렉터리 경로입니다.

Bourne 셸 사용:

```
$ INSTHOME=~db2admin
```

C 셸 사용:

```
$ setenv INSTHOME ~db2admin>
```

DB2DIR. IBM DB2 CAE 설치 디렉터리를 가리키도록 변수를 설정합니다. 예를 들어 클라이언트가 /opt/IBM/db2/V9.7 디렉터리에 설치된 경우 다음을 수행하십시오.

Bourne 셸 사용:

```
$ DB2DIR=/opt/IBM/db2/V9.7; export DB2DIR
```

C 셸 사용:

```
$ setenv DB2DIR /opt/IBM/db2/V9.7
```

PATH IBM DB2 명령줄 프로그램을 실행하려면 DB2 bin 디렉터리를 포함하도록 변수를 설정합니다.

Bourne 셸 사용:

```
$ PATH=${PATH}:$DB2DIR/bin; export PATH
```

C 셸 사용:

```
$ setenv PATH ${PATH}:$DB2DIR/bin
```

3. DB2 lib 디렉터리를 포함하도록 공유 라이브러리 변수를 설정합니다.

IBM DB2 클라이언트 소프트웨어에는 데이터 통합 서비스, PowerCenter 통합 서비스 및 PowerCenter 리포지토리 서비스 프로세스가 동적으로 로드하는 여러 개의 공유 라이브러리 구성 요소가 포함되어 있습니다. 서비스가 런타임에 공유 라이브러리를 찾을 수 있도록 공유 라이브러리 환경 변수를 설정합니다.

공유 라이브러리 경로는 Informatica 설치 디렉터리 (*server_dir*)도 포함해야 합니다.

운영 체제에 맞게 공유 라이브러리 환경 변수를 설정합니다.

다음 표에는 각 운영 체제별로 공유 라이브러리 변수가 설명되어 있습니다.

운영 체제	변수
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

예를 들어 Linux의 경우 다음 구문을 사용하십시오.

- Bourne 셸 사용:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:%HOME/server_dir:%DB2DIR/lib; export LD_LIBRARY_PATH
```

- C 셸 사용:

```
$ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:%HOME/server_dir:%DB2DIR/lib
```

AIX의 경우:

- Bourne 셸 사용:

```
$ LIBPATH=${LIBPATH}:%HOME/server_dir:%DB2DIR/lib; export LIBPATH
```

- C 셸 사용:

```
$ setenv LIBPATH ${LIBPATH}:%HOME/server_dir:%DB2DIR/lib
```

4. 일련의 셸 명령을 완전하게 포함하도록 *.cshrc* 또는 *.profile*을 편집합니다. 파일을 저장한 후에 로그아웃했다가 다시 로그인하거나 *source* 명령을 실행합니다.

Bourne 셸 사용:

```
$ source .profile
```

C 셸 사용:

```
$ source .cshrc
```

5. 데이터 통합 서비스, PowerCenter 통합 서비스 또는 PowerCenter 리포지토리 서비스 프로세스가 실행되는 시스템과 같은 시스템에 DB2 데이터베이스가 있는 경우, DB2 인스턴스를 원격 인스턴스로 구성합니다. 다음 명령을 실행하여 해당 데이터베이스에 대한 원격 항목이 있는지 확인합니다.

```
DB2 LIST DATABASE DIRECTORY
```

이 명령은 DB2 클라이언트에서 액세스할 수 있는 모든 데이터베이스 및 데이터베이스의 구성 속성을 나열합니다. 이 명령이 “Directory entry type”이 “Remote”인 항목을 나열하면 7로 건너뛵니다.

6. 데이터베이스가 원격으로 구성되어 있지 않으면 다음 명령을 실행하여 TCP/IP 노드가 호스트를 위한 목록에 포함되어 있는지 확인합니다.

```
DB2 LIST NODE DIRECTORY
```

노드 이름이 비어 있으면 원격 데이터베이스를 설정할 때 노드 이름을 작성할 수 있습니다. 다음 명령을 사용하여 원격 데이터베이스를 설정하고 필요하면 노드를 작성합니다.

```
db2 CATALOG TCP/IP NODE <nodename> REMOTE <hostname_or_address> SERVER <port number>
```

다음 명령을 실행하여 데이터베이스를 카탈로그에 포함시킵니다.

```
db2 CATALOG DATABASE <dbname> as <dbalias> at NODE <nodename>
```

이러한 명령에 대한 자세한 내용은 데이터베이스 설명서를 참조하십시오.

7. DB2 데이터베이스에 연결할 수 있는지 확인합니다. DB2 명령줄 프로세서를 실행하고 해당 명령을 실행합니다.

```
CONNECT TO <dbalias> USER <username> USING <password>
```

연결이 성공적이면 `CONNECT RESET` 또는 `TERMINATE` 명령으로 정리합니다.

Informix 데이터베이스에 연결

UNIX 또는 Linux에서 ODBC를 사용하여 Informix 데이터베이스에 연결합니다.

ODBC 연결 구성

Informix 데이터베이스에 대한 ODBC 연결을 구성할 수 있습니다.

다음 단계에서는 ODBC 연결을 구성하기 위한 지침을 제공합니다. 특정한 지침은 데이터베이스 설명서를 참조하십시오.

1. ODBC_HOME 환경 변수를 ODBC 설치 디렉터리로 설정합니다. 예를 들면 다음과 같습니다.

Bourne 셸 사용:

```
$ ODBC_HOME=<Informatica server home>/ODBC7.1; export ODBC_HOME
```

C 셸 사용:

```
$ setenv ODBC_HOME <Informatica server home>/ODBC7.1
```

2. ODBCINI 환경 변수를 `odbc.ini` 파일의 위치로 설정합니다. 예를 들어 `odbc.ini` 파일이 `$ODBC_HOME` 디렉터리에 있으면 다음을 수행하십시오.

Bourne 셸 사용:

```
ODBCINI=$ODBC_HOME/odbc.ini; export ODBCINI
```

C 셸 사용:

```
$ setenv ODBCINI $ODBC_HOME/odbc.ini
```

3. `$ODBC_HOME` 디렉터리에 있는 기존 `odbc.ini` 파일을 편집하거나 이 `odbc.ini` 파일을 UNIX 홈 디렉터리에 복사한 후 편집합니다.

```
$ cp $ODBC_HOME/odbc.ini $HOME/.odbc.ini
```

4. [ODBC 데이터 소스] 섹션 아래에 Informix 데이터 소스에 대한 항목을 추가하고 해당 데이터 소스를 구성합니다. 예를 들면 다음과 같습니다.

```
[Informix Wire Protocol]
Driver=/export/home/Informatica/10.0.0/ODBC7.1/lib/DWifc127.so
Description=DataDirect 7.1 Informix Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
CancelDetectInterval=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
HostName=<Informix_host>
LoadBalancing=0
LogonID=
Password=
PortNumber=<Informix_server_port>
ReportCodePageConversionErrors=0
ServerName=<Informix_server>
TrimBlankFromIndexName=1
```

5. \$ODBCHOME 디렉터리에서 스크립트 `odbc.sh` 또는 `odbc.csh`를 실행하여 PATH 및 공유 라이브러리 환경 변수를 설정합니다.

Bourne 셸 사용:

```
sh odbc.sh
```

C 셸 사용:

```
source odbc.csh
```

6. ODBC 데이터 소스를 사용하여 Informix 데이터베이스에 연결할 수 있는지 확인합니다. 연결이 실패하면 데이터베이스 설명서를 참조하십시오.

Microsoft SQL Server 데이터베이스에 연결

UNIX 또는 Linux 시스템에서 Microsoft SQL Server 데이터베이스에 연결하려면 Microsoft SQL Server 연결을 사용합니다.

ODBC를 통한 SSL 인증 구성

DataDirect New SQL Server Wire Protocol 드라이버를 사용하여 ODBC를 통한 SSL 인증을 Microsoft SQL Server에 대해 구성할 수 있습니다.

1. `odbc.ini` 파일을 열고 ODBC 데이터 소스 및 DataDirect New SQL Server Wire Protocol 드라이버에 대한 항목을 [ODBC 데이터 소스] 섹션 아래에 추가합니다.
2. SSL을 구성하기 위해 `odbc.ini` 파일에 특성을 추가합니다.

다음 표에는 SSL 인증을 구성할 때 `odbc.ini` 파일에 추가해야 하는 특성이 나열되어 있습니다.

특성	설명
EncryptionMethod	드라이버와 데이터베이스 서버 간에 전송되는 데이터를 암호화하기 위해 드라이버가 사용하는 방법입니다. SSL을 사용하여 데이터를 암호화하려면 값을 1로 설정합니다.
ValidateServerCertificate	SSL 암호화가 활성화된 경우 드라이버가 데이터베이스 서버에 의해 전송되는 인증서의 유효성을 검사할지 여부를 결정합니다. 드라이버가 서버 인증서의 유효성을 검사하도록 하려면 값을 1로 설정합니다.
트러스트 저장소	트러스트 저장소 파일의 위치 및 이름입니다. 트러스트 저장소 파일에는 드라이버가 SSL 서버 인증에 사용하는 CA(인증 기관)의 목록이 포함되어 있습니다.
TrustStorePassword	트러스트 저장소 파일의 콘텐츠에 액세스하기 위한 암호입니다.
HostNameInCertificate	선택 사항입니다. 드라이버가 인증서에 포함된 호스트 이름의 유효성을 검사할 수 있도록 하기 위해 SSL 관리자가 설정하는 호스트 이름입니다.

Microsoft SQL Server의 사용자 지정 속성 구성

Microsoft SQL Server의 사용자 지정 속성을 구성하여 대량 로드 성능을 개선할 수 있습니다.

1. PowerCenter 클라이언트를 실행하고 워크플로우 관리자에 연결합니다.
2. 워크플로우를 열고 구성하려는 세션을 선택합니다.

3. **개체 구성** 탭을 클릭합니다.
4. **기본 버퍼 블록 크기** 값을 5MB로 변경합니다. 다음 명령을 사용할 수도 있습니다. `$INFA_HOME/server/bin/./pmrep massupdate -t session_config_property -n "Default buffer block size" -v "5MB" -f <folderName>`
크기가 1KB인 행의 처리량을 최적화하려면 버퍼 블록 크기를 5MB로 설정해야 합니다.
5. **속성** 탭을 클릭합니다.
6. 세션에 관계형 대상이 포함되어 있으면 **커밋 간격**을 100000으로 변경합니다.
7. **DTM 버퍼 크기**를 설정합니다. 최적의 DTM 버퍼 크기는 ((10 x 블록 버퍼 크기) x 파티션 수)입니다.

Netezza 데이터베이스에 연결

PowerCenter 통합 서비스 프로세스가 실행되는 시스템에 Netezza ODBC 드라이버를 설치하고 구성합니다. Informatica 제품과 함께 제공되는 DataDirect 드라이버 패키지의 DataDirect 드라이버 관리자를 사용하여 `odbc.ini` 파일에 Netezza 데이터 소스 세부 정보를 구성합니다.

ODBC 연결 구성

Netezza 데이터베이스에 대한 ODBC 연결을 구성할 수 있습니다.

다음 단계에서는 ODBC 연결을 구성하기 위한 지침을 제공합니다. 특정한 지침은 데이터베이스 설명서를 참조하십시오.

1. 통합 서비스 프로세스에 대한 연결을 구성하려면 서비스 프로세스를 시작할 수 있는 사용자로 시스템에 로그인합니다.
2. `ODBCHOME`, `NZ_ODBC_INI_PATH` 및 `PATH` 환경 변수를 설정합니다.

ODBCHOME. 변수를 ODBC 설치 디렉터리로 설정합니다. 예:

Bourne 셸 사용:

```
$ ODBCHOME=<Informatica server home>/ODBC7.1; export ODBCHOME
```

C 셸 사용:

```
$ setenv ODBCHOME =<Informatica server home>/ODBC7.1
```

PATH. 변수를 `ODBCHOME/bin` 디렉터리로 설정합니다. 예:

Bourne 셸 사용:

```
PATH="{PATH}:%ODBCHOME/bin"
```

C 셸 사용:

```
$ setenv PATH {PATH}:%ODBCHOME/bin
```

NZ_ODBC_INI_PATH. `odbc.ini` 파일이 포함된 디렉터리를 가리키도록 변수를 설정합니다. 예를 들어 `odbc.ini` 파일이 `%ODBCHOME` 디렉터리에 있으면 다음을 수행하십시오.

Bourne 셸 사용:

```
NZ_ODBC_INI_PATH=%ODBCHOME; export NZ_ODBC_INI_PATH
```

C 셸 사용:

```
$ setenv NZ_ODBC_INI_PATH %ODBCHOME
```

3. 공유 라이브러리 환경 변수를 설정합니다.

공유 라이브러리 경로는 ODBC 라이브러리를 포함해야 합니다. 또한 이 경로는 Informatica 서비스 설치 디렉터리(server_dir)도 포함해야 합니다.

운영 체제에 맞게 공유 라이브러리 환경 변수를 설정합니다. Netezza 라이브러리 폴더를 <NetezzaInstallationDir>/lib64로 설정합니다.

다음 표에는 각 운영 체제별로 공유 라이브러리 변수가 설명되어 있습니다.

운영 체제	변수
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

예를 들어 Linux의 경우 다음 구문을 사용하십시오.

- Bourne 셸 사용:

```
$ LD_LIBRARY_PATH="${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib:<NetezzaInstallationDir>/lib64"
export LD_LIBRARY_PATH
```

- C 셸 사용:

```
$ setenv LD_LIBRARY_PATH "${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib:<NetezzaInstallationDir>/lib64"
```

AIX의 경우

- Bourne 셸 사용:

```
$ LIBPATH=${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib:<NetezzaInstallationDir>/lib64; export LIBPATH
```

- C 셸 사용:

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib:<NetezzaInstallationDir>/lib64
```

4. 기존 odbc.ini 파일을 편집하거나 odbc.ini 파일을 홈 디렉터리에 복사한 후 편집합니다.

이 파일은 \$ODBCHOME 디렉터리에 있습니다.

```
$ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
```

[ODBC 데이터 소스] 섹션 아래에 Netezza 데이터 소스에 대한 항목을 추가하고 해당 데이터 소스를 구성합니다.

예:

```
[NZZSQL]
Driver = /export/home/appsqa/thirdparty/netezza/lib64/libnzodbc.so
Description = NetezzaSQL ODBC
Servername = netezza1.informatica.com
Port = 5480
Database = infa
Username = admin
Password = password
Debuglogging = true
StripCRLF = false
Prefetch = 256
Protocol = 7.0
ReadOnly = false
ShowSystemTables = false
Socket = 16384
DateFormat = 1
TranslationDLL =
TranslationName =
TranslationOption =
NumericAsChar = false
```

Netezza 연결에 대한 자세한 내용은 Netezza ODBC 드라이버 설명서를 참조하십시오.

5. `odbc.ini` 파일에서 마지막 항목이 `InstallDir`인지 확인하고 해당 항목을 ODBC 설치 디렉터리로 설정합니다.
예:
`InstallDir=<Informatica install directory>/<ODBCHOME directory>`
6. 일련의 셸 명령을 완전하게 포함하도록 `.cshrc` 또는 `.profile` 파일을 편집합니다.
7. Informatica 서비스를 다시 시작합니다.

Oracle 데이터베이스에 연결

원시 연결의 경우 Oracle 데이터베이스 서버 버전에 해당하는 Oracle 클라이언트 버전을 설치하십시오. Informatica와 데이터베이스 간 호환성을 보장하려면 적절한 데이터베이스 클라이언트 라이브러리를 사용하십시오.

Oracle 클라이언트 및 Oracle 데이터베이스 서버의 호환 가능한 버전을 설치해야 합니다. 동일한 버전의 Oracle 클라이언트가 필요한 모든 시스템에도 해당 클라이언트를 설치해야 합니다. 호환성을 확인하려면 Oracle에 문의하십시오.

원시 연결 구성

Oracle 데이터베이스에 대한 원시 연결을 구성하여 성능을 개선할 수 있습니다.

다음 단계는 Oracle Net Services 또는 Net8을 통한 원시 연결 구성에 대한 지침을 제공합니다. 특정한 지침은 데이터베이스 설명서를 참조하십시오.

1. 데이터 통합 서비스, PowerCenter 통합 서비스 또는 PowerCenter 리포지토리 서비스 프로세스에 대해 연결을 구성하려면 서버 프로세스를 시작할 수 있는 사용자로 시스템에 로그인합니다.
2. `ORACLE_HOME`, `NLS_LANG`, `TNS_ADMIN` 및 `PATH` 환경 변수를 설정합니다.

ORACLE_HOME. 변수를 Oracle 클라이언트 설치 디렉터리로 설정합니다. 클라이언트가 `/HOME2/oracle` 디렉터리에 설치된 경우를 예로 들어 보겠습니다. 변수를 다음과 같이 설정합니다.

Bourne 셸 사용:

```
$ ORACLE_HOME=/HOME2/oracle; export ORACLE_HOME
```

C 셸 사용:

```
$ setenv ORACLE_HOME /HOME2/oracle
```

NLS_LANG. 변수를 데이터베이스 클라이언트 및 서버가 로그인에 사용하도록 할 로캘(언어, 지역 및 문자 집합)로 설정합니다. 이 변수의 값은 구성에 따라 달라집니다. 예를 들어 값이 `american_america.UTF8`이면 변수를 다음과 같이 설정하십시오.

Bourne 셸 사용:

```
$ NLS_LANG=american_america.UTF8; export NLS_LANG
```

C 셸 사용:

```
$ NLS_LANG american_america.UTF8
```

이 변수의 값을 결정하려면 관리자에게 문의하십시오.

ORA_SDTZ. 데이터 통합 서비스가 현지 시간이 포함된 타임스탬프를 읽거나 쓸 때의 기본 세션 시간대를 설정하려면 `ORA_SDTZ` 환경 변수를 지정하십시오.

`ORA_SDTZ` 환경 변수는 다음 값 중 하나로 설정할 수 있습니다.

- 운영 체제 현지 시간대('OS_TZ')

- 데이터베이스 시간대('DB_TZ')
- UTC의 절대 오프셋(예: '-05:00')
- 시간대 영역 이름(예: 'America/Los_Angeles')

Informatica 서버가 실행되는 시스템에서 환경 변수를 설정할 수 있습니다.

TNS_ADMIN. tnsnames.ora 파일이 Oracle 클라이언트 설치 위치와 동일한 위치에 없을 경우 TNS_ADMIN 환경 변수를 tnsnames.ora 파일이 상주하는 디렉터리로 설정하십시오. 예를 들어 파일이 /HOME2/oracle/files 디렉터리에 있으면 변수를 다음과 같이 설정하십시오.

Bourne 셸 사용:

```
$ TNS_ADMIN=$HOME2/oracle/files; export TNS_ADMIN
```

C 셸 사용:

```
$ setenv TNS_ADMIN=$HOME2/oracle/files
```

참고: 기본적으로 tnsnames.ora 파일은 다음 디렉터리에 저장됩니다. \$ORACLE_HOME/network/admin.

PATH Oracle 명령줄 프로그램을 실행하려면 Oracle bin 디렉터리를 포함하도록 변수를 설정합니다.

Bourne 셸 사용:

```
$ PATH=${PATH}:$ORACLE_HOME/bin; export PATH
```

C 셸 사용:

```
$ setenv PATH ${PATH}:ORACLE_HOME/bin
```

3. 공유 라이브러리 환경 변수를 설정합니다.

Oracle 클라이언트 소프트웨어에는 데이터 통합 서비스, PowerCenter 통합 서비스 및 PowerCenter 리포지토리 서비스 프로세스가 동적으로 로드하는 여러 개의 공유 라이브러리 구성 요소가 포함되어 있습니다. 런타임 중에 공유 라이브러리를 찾으려면 공유 라이브러리 환경 변수를 설정합니다.

공유 라이브러리 경로는 Informatica 설치 디렉터리(server_dir)도 포함해야 합니다.

공유 라이브러리 환경 변수를 LD_LIBRARY_PATH로 설정합니다.

예를 들어 다음 구문을 사용하십시오.

- Bourne 셸 사용:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$ORACLE_HOME/lib; export LD_LIBRARY_PATH
```

- C 셸 사용:

```
$ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:$HOME/server_dir:$ORACLE_HOME/lib
```

4. 일련의 셸 명령을 완전하게 포함하도록 .cshrc 또는 .profile을 편집합니다. 파일을 저장한 후에 로그아웃했다가 다시 로그인하거나 source 명령을 실행합니다.

Bourne 셸 사용:

```
$ source .profile
```

C 셸 사용:

```
$ source .cshrc
```

5. Oracle 클라이언트가 데이터베이스에 액세스하도록 구성되어 있는지 확인합니다.

SQL*Net Easy Configuration 유틸리티를 사용하거나 기존 tnsnames.ora 파일을 홈 디렉터리로 복사한 후 수정합니다.

tnsnames.ora 파일은 다음 디렉터리에 저장됩니다. \$ORACLE_HOME/network/admin.

Oracle 연결 문자열(일반적으로 databasename.world)에 대한 올바른 구문을 입력합니다.

다음은 샘플 tnsnames.ora 파일입니다. 데이터베이스에 대한 정보를 입력하십시오.

```
mydatabase.world =
  (DESCRIPTION
  (ADDRESS_LIST =
```

```

        (ADDRESS =
          (COMMUNITY = mycompany.world
           (PROTOCOL = TCP)
           (Host = mymachine)
           (Port = 1521)
          )
        )
      )
    (CONNECT_DATA =
      (SID = MYORA7)
      (GLOBAL_NAMES = mydatabase.world)
    )
  )
)

```

다음은 Oracle Connection Manager를 사용하여 Oracle에 연결할 샘플 tnsnames.ora 파일입니다.

```

ORCL19C_CMAN =
(description=
(address_list=
(source_route=yes)
(address=(protocol=tcp)(host=inh74ocm.mycompany.com)(port=1521))
(address=(protocol=tcp)(host=inh74oradb.mycompany.com)(port=1521))
)
(connect_data=
(service_name=ORCL19C.mycompany.com)
)
)

```

6. Oracle 데이터베이스에 연결할 수 있는지 확인합니다.

Oracle 데이터베이스에 연결하려면 SQL*Plus를 실행하고 연결 정보를 입력합니다. 데이터베이스에 연결하지 못한 경우 모든 연결 정보를 올바르게 입력했는지 확인합니다.

tnsnames.ora 파일에 정의된 대로 사용자 이름 및 연결 문자열을 입력합니다.

PostgreSQL 데이터베이스에 연결

원시 연결의 경우 PostgreSQL 데이터베이스 서버 버전에 해당하는 PostgreSQL 클라이언트 버전을 설치하십시오.

Informatica와 데이터베이스 간 호환성을 보장하려면 적절한 데이터베이스 클라이언트 라이브러리를 사용하십시오.

PostgreSQL 클라이언트 및 PostgreSQL 데이터베이스 서버의 호환 가능한 버전을 설치해야 합니다. 동일한 버전의 PostgreSQL 클라이언트가 필요한 모든 시스템에도 해당 클라이언트를 설치해야 합니다. 호환성을 확인하려면 PostgreSQL에 문의하십시오.

Configuring Native Connectivity

You can configure native connectivity to a PostgreSQL database to increase performance.

The following steps provide a guideline for configuring native connectivity through PostgreSQL. For specific instructions, see the database documentation.

1. To configure connectivity for the PowerCenter Integration Service and PowerCenter Repository Service process, log in to the machine as a user who can start the server process.
2. To configure PostgreSQL database for the PowerCenter repository, set values for the PostgreSQL database host, port, and service name for the pg_service.conf file in the following format:

```

[PCRS_DB_SERVICE_NAME]
host=Database host IP
port=Database port
dbname=PowerCenter Repository Service database service name

```

Ensure that the entries for the [PCRS_DB_SERVICE_NAME] matches the information for the PowerCenter Repository Service. To securely connect to PostgreSQL for the PowerCenter repository, set the security property along with the remaining required database properties in the pg_service.conf file in the following format: sslmode=require

3. Set the PGSERVICEFILE, PGHOME, and PATH environment variables.

PGSERVICEFILE. Set the variable to the pg_service.conf file that contains the connection parameters for PostgreSQL database connection. For example, set the variable as follows:

Using a Bourne shell:

```
$ export PGSERVICEFILE; PGSERVICEFILE=<pg_service.conf file
directory>/pg_service.conf
```

Using a C shell:

```
$ setenv PGSERVICEFILE <pg_service.conf file
directory>/pg_service.conf
```

PGHOME. Set the variable to the PostgreSQL installation path where you have installed the PostgreSQL client. For example, set the variable as follows:

Using a Bourne shell:

```
$ export PGHOME; PGHOME=/usr/pgsql-10
```

Using a C shell:

```
$ setenv PGHOME /usr/pgsql-10
```

PATH. To run the PostgreSQL command line programs, set the variable to include the PostgreSQL client directory, psql. For example, set the variable as follows:

Using a Bourne shell:

```
$ export PATH; PATH=${PATH}:${PGHOME}
```

Using a C shell:

```
$ setenv PATH ${PGHOME}:${PATH}
```

4. Set the shared library environment variable.

The PostgreSQL client software contains a number of shared library components that the PowerCenter Integration Service and PowerCenter Repository Service processes load dynamically. To locate the shared libraries during run time, set the shared library environment variable.

The shared library path must also include the Informatica installation directory (server_dir).

Set the shared library environment variable to LD_LIBRARY_PATH.

For example, use the following syntax:

- Using a Bourne shell:

```
$ export LD_LIBRARY_PATH; LD_LIBRARY_PATH $PGHOME/lib
$ LD_LIBRARY_PATH <InstallationDirectory>/server/bin:${LD_LIBRARY_PATH}
```

- Using a C shell:

```
$ setenv LD_LIBRARY_PATH $PGHOME/lib
$ setenv LD_LIBRARY_PATH <InstallationDirectory>/server/bin:${LD_LIBRARY_PATH}
```

5. Verify that you can connect to the PostgreSQL database.

To connect to the PostgreSQL database, launch the psql utility and enter the connectivity information.

ODBC 연결 구성

UNIX 또는 Linux의 PostgreSQL 데이터베이스에 대한 ODBC 연결을 구성할 수 있습니다.

DataDirect PostgreSQL 유선 프로토콜 드라이버를 사용하여 ODBC를 통해 PostgreSQL에 대한 연결을 구성할 수 있습니다.

PostgreSQL에 대한 ODBC 연결을 구성하기 위한 지침은 다음 태스크를 검토하십시오.

1. PostgreSQL에 대한 환경 변수 설정
2. ODBC.ini 파일에서 ODBC 연결 구성
3. PostgreSQL 데이터 소스 이름으로 PowerCenter 리포지토리 업데이트
4. ODBC 데이터 소스와 PostgreSQL 연결 확인

특정한 지침은 데이터베이스 설명서를 참조하십시오.

1단계. 환경 변수 설정

1. Administrator 도구에서 **관리 > 서비스 및 노드**를 클릭합니다.
2. 도메인 탐색기에서 PowerCenter 리포지토리 서비스를 선택합니다.
3. 콘텐츠 패널에서 프로세스 보기를 클릭합니다. 환경 변수 섹션에서 변수 이름을 POSTGRES_ODBC로 설정하고 값을 1로 설정합니다.

2단계. ODBC 연결 구성

1. ODBCHOME 환경 변수를 ODBC 설치 디렉터리로 설정합니다. 예:

Bourne 셸 사용:

```
$ ODBCHOME=<Informatica 서버 홈>/ODBC7.1; export ODBCHOME
```

C 셸 사용:

```
$ setenv ODBCHOME <Informatica 서버 홈>/ODBC7.1
```

2. \$ODBCHOME 디렉터리에 있는 기존 `odbc.ini` 파일을 편집하거나 `odbc.ini` 파일을 UNIX 홈 디렉터리에 복사한 후 편집합니다.

```
$ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
```

3. `odbc.ini` 파일을 열고 DataDirect PostgreSQL 유선 프로토콜 데이터 소스에 대한 항목을 추가합니다.

PostgreSQL 데이터베이스에 연결할 데이터 소스 이름, 드라이버 경로, 호스트 이름 및 포트 번호를 구성합니다. 예:

```
[PostgreSQL Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWpsql27.so
Description=DataDirect 7.1 PostgreSQL Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=2048
EnableDescribeParam=1
EncryptionMethod=1
ExtendedColumnMetadata=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
FetchTWSasTime=0
```

```

GSSClient=native
HostName=<PostgreSQL_host>
HostNameInCertificate=<Host name in SSL certificate>
InitializationString=
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<PostgreSQL_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TransactionErrorBehavior=1
TrustStore=<Path of the truststore certificates>
TrustStorePassword=<Password of the truststore certificates>
ValidateServerCertificate=1
XMLDescribeType=-10

```

4. PATH 환경 변수를 설정합니다.

Bourne 셸 사용:

```
$ PATH=${PATH}:%ODBCHOME/bin; export PATH
```

C 셸 사용:

```
$ setenv PATH ${PATH}:%ODBCHOME/bin
```

5. 운영 체제에 맞게 공유 라이브러리 환경 변수를 설정합니다.

다음 표에는 각 운영 체제별로 공유 라이브러리 변수가 설명되어 있습니다.

예를 들어 Linux의 경우 다음 구문을 사용하여 LD_LIBRARY_PATH를 설정합니다.

- Bourne 셸 사용:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:%HOME/server_dir :%ODBCHOME/lib; export LD_LIBRARY_PATH
```

- C 셸 사용:

```
$ setenv LD_LIBRARY_PATH %HOME/server_dir:%ODBCHOME/lib:%LD_LIBRARY_PATH
```

예를 들어 AIX의 경우 다음 구문을 사용하여 LIBPATH를 설정합니다.

- Bourne 셸 사용:

```
$ LIBPATH=${LIBPATH}:%HOME/server_dir :%ODBCHOME/lib; export LIBPATH
```

- C 셸 사용:

```
$ setenv LIBPATH ${LIBPATH}:%HOME/server_dir :%ODBCHOME/lib
```

3단계. PowerCenter 리포지토리 데이터베이스 속성 업데이트

1. Administrator 도구에서 PowerCenter 리포지토리 서비스를 선택합니다.
2. 데이터베이스 속성 섹션에서 ODBC.ini 파일의 PostgreSQL에 지정한 것과 동일한 데이터 소스 이름을 입력합니다.
3. 변경 내용을 저장합니다.

4단계. PostgreSQL 연결 확인

1. ODBC 데이터 소스를 사용하여 PostgreSQL 데이터베이스에 연결할 수 있는지 확인합니다.
2. 연결이 실패하면 데이터베이스 설명서를 참조하십시오.

Sybase ASE 데이터베이스에 연결

원시 연결의 경우 데이터베이스 버전에 해당하는 **Open Client** 버전을 설치하십시오. **Informatica**와 데이터베이스 간 호환성을 보장하려면 적절한 데이터베이스 클라이언트 라이브러리를 사용하십시오.

Sybase ASE 데이터베이스 서버와 호환 가능한 **Open Client** 버전을 설치합니다. 또한 **Sybase ASE** 데이터베이스 및 **Informatica**를 호스트하는 시스템에 동일한 버전의 **Open Client**를 설치해야 합니다. 호환성을 확인하려면 **Sybase**에 문의하십시오.

Sybase ASE 리포지토리를 작성, 복원 또는 업그레이드할 경우 데이터베이스 수준에서 *allow nulls by default*를 **TRUE**로 설정하십시오. 이 옵션을 설정하면 열의 기본 **null** 유형이 **SQL** 표준과 호환되는 **null**로 변경됩니다.

원시 연결 구성

Sybase ASE 데이터베이스에 대한 원시 연결을 구성하여 성능을 개선할 수 있습니다.

다음 단계에서는 원시 연결을 구성하기 위한 지침을 제공합니다. 특정한 지침은 데이터베이스 설명서를 참조하십시오.

1. 데이터 통합 서비스, **PowerCenter** 통합 서비스 또는 **PowerCenter** 리포지토리 서비스 프로세스에 대한 연결을 구성하려면 서버 프로세스를 시작할 수 있는 사용자로 시스템에 로그인합니다.
2. **SYBASE** 및 **PATH** 환경 변수를 설정합니다.

SYBASE. 변수를 **Sybase Open Client** 설치 디렉터리로 설정합니다. 예를 들어 클라이언트가 **/usr/sybase** 디렉터리에 설치된 경우 다음을 수행하십시오.

Bourne 셸 사용:

```
$ SYBASE=/usr/sybase; export SYBASE
```

C 셸 사용:

```
$ setenv SYBASE /usr/sybase
```

PATH **Sybase** 명령줄 프로그램을 실행하려면 **Sybase OCS bin** 디렉터리를 포함하도록 변수를 설정합니다.

Bourne 셸 사용:

```
$ PATH=${PATH}:/usr/sybase/OCS-15_0/bin; export PATH
```

C 셸 사용:

```
$ setenv PATH ${PATH}:/usr/sybase/OCS-15_0/bin
```

3. 공유 라이브러리 환경 변수를 설정합니다.

Sybase Open Client 소프트웨어에는 데이터 통합 서비스, **PowerCenter** 통합 서비스 및 **PowerCenter** 리포지토리 서비스 프로세스가 동적으로 로드하는 여러 개의 공유 라이브러리 구성 요소가 포함되어 있습니다. 서비스가 런타임에 공유 라이브러리를 찾을 수 있도록 공유 라이브러리 환경 변수를 설정합니다.

공유 라이브러리 경로는 **Informatica** 서비스 설치 디렉터리 (*server_dir*)도 포함해야 합니다.

운영 체제에 맞게 공유 라이브러리 환경 변수를 설정합니다.

다음 표에는 각 운영 체제별로 공유 라이브러리 변수가 설명되어 있습니다.

운영 체제	변수
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

예를 들어 Linux의 경우 다음 구문을 사용하십시오.

- Bourne 셸 사용:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/home/server_dir:/sybase/OCS-15_0/lib:/sybase/OCS-15_0/lib3p:/sybase/OCS-15_0/lib3p64; export LD_LIBRARY_PATH
```

- C 셸 사용:

```
$ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:/home/server_dir:/sybase/OCS-15_0/lib:/sybase/OCS-15_0/lib3p:/sybase/OCS-15_0/lib3p64;
```

AIX의 경우

- Bourne 셸 사용:

```
$ LIBPATH=${LIBPATH}:/home/server_dir:/sybase/OCS-15_0/lib:/sybase/OCS-15_0/lib3p:/sybase/OCS-15_0/lib3p64; export LIBPATH
```

- C 셸 사용:

```
$ setenv LIBPATH ${LIBPATH}:/home/server_dir:/sybase/OCS-15_0/lib:/sybase/OCS-15_0/lib3p:/sybase/OCS-15_0/lib3p64;
```

4. 일련의 셸 명령을 완전하게 포함하도록 .cshrc 또는 .profile을 편집합니다. 파일을 저장한 후에 로그아웃했다가 다시 로그인하거나 source 명령을 실행합니다.

Bourne 셸 사용:

```
$ source .profile
```

C 셸 사용:

```
$ source .cshrc
```

5. \$SYBASE 디렉터리에 저장된 Sybase 인터페이스 파일에서 Sybase ASE 서버 이름을 확인합니다.

6. 필요한 경우 SSL 활성화 Sybase ASE 데이터베이스에 연결하려면 다음 태스크를 수행합니다.

- Sybase 드라이버 속성에서 데이터 소스 이름을 구성할 때 **보안** 탭에서 다음 보안 특성을 지정합니다.

특성	설명
암호화 방법	네트워크를 통해 전송되는 경우 데이터가 암호화되었는지를 나타냅니다. SSL을 선택합니다.
서버 인증서 유효성 검사	SSL 암호화가 활성화된 경우 데이터베이스 서버에서 보낸 인증서에 대해 Informatica에서 유효성을 검사하는지를 나타냅니다.
트러스트 저장소	트러스트 저장소 파일의 위치 및 이름입니다.
트러스트 저장소 암호	트러스트 저장소 파일의 콘텐츠에 액세스하기 위한 암호입니다.
인증서의 호스트 이름	인증서에 포함된 호스트 이름의 유효성을 검사할 수 있도록 하기 위해 SSL 관리자가 설정하는 호스트 이름입니다.

- Sybase ASE 클라이언트의 trusted.txt 파일에 Sybase ASE 서버 인증서를 추가합니다.

- 다음 Sybase ASE 서버 연결 세부 정보를 Sybase 인터페이스 파일에 추가합니다.

```
<server_instance_name>
  master tcp ether <host name> <port number> ssl="CN='common_name'"
  query tcp ether <host name> <port number> ssl="CN='common_name'"
```

7. Sybase ASE 데이터베이스에 연결할 수 있는지 확인합니다.

Sybase ASE 데이터베이스에 연결하려면 ISQL을 실행하고 연결 정보를 입력합니다. 데이터베이스에 연결하지 못한 경우 모든 연결 정보를 올바르게 입력했는지 확인합니다.

사용자 이름 및 데이터베이스 이름은 대/소문자를 구분합니다.

Teradata 데이터베이스에 연결

데이터 통합 서비스 또는 PowerCenter 통합 서비스 프로세스가 실행되는 시스템에 원시 클라이언트 소프트웨어를 설치하고 구성합니다. Informatica와 데이터베이스 간 호환성을 보장하려면 적절한 데이터베이스 클라이언트 라이브러리를 사용하십시오.

Teradata 클라이언트, Teradata ODBC 드라이버 및 다른 Teradata 클라이언트 소프트웨어를 설치합니다. 이러한 소프트웨어는 Teradata 데이터 통합 서비스 또는 PowerCenter 통합 서비스가 실행되는 시스템에서 필요할 수 있습니다. ODBC 연결도 구성해야 합니다.

참고: Teradata의 권장 사항에 따라 Informatica는 ODBC를 사용하여 Teradata에 연결합니다. ODBC는 Teradata용 원시 인터페이스입니다.

ODBC 연결 구성

Teradata 데이터베이스에 대한 ODBC 연결을 구성할 수 있습니다.

다음 단계에서는 ODBC 연결을 구성하기 위한 지침을 제공합니다. 특정한 지침은 데이터베이스 설명서를 참조하십시오.

1. 통합 서비스 프로세스에 대한 연결을 구성하려면 서비스 프로세스를 시작할 수 있는 사용자로 시스템에 로그인합니다.
2. TERADATA_HOME, ODBC_HOME 및 PATH 환경 변수를 설정합니다.

TERADATA_HOME. 변수를 Teradata 드라이버 설치 디렉터리로 설정합니다. 기본값은 다음과 같습니다.

Bourne 셸 사용:

```
$ TERADATA_HOME=/opt/teradata/client/<version>; export TERADATA_HOME
```

C 셸 사용:

```
$ setenv TERADATA_HOME /opt/teradata/client/<version>
```

ODBC_HOME. 변수를 ODBC 설치 디렉터리로 설정합니다. 예:

Bourne 셸 사용:

```
$ ODBC_HOME=$INFA_HOME/ODBC<version>; export ODBC_HOME
```

C 셸 사용:

```
$ setenv ODBC_HOME $INFA_HOME/ODBC<version>
```

PATH *ddtestlib* 유틸리티를 실행하려면 DataDirect ODBC 드라이버 관리자가 드라이버 파일을 로드할 수 있는지 확인하고 다음과 같이 변수를 설정합니다.

Bourne 셸 사용:

```
PATH="{PATH}:%ODBC_HOME/bin:%TERADATA_HOME/bin"
```

C 셸 사용:

```
$ setenv PATH "{PATH}:%ODBC_HOME/bin:%TERADATA_HOME/bin"
```

3. 공유 라이브러리 환경 변수를 설정합니다.

Teradata 소프트웨어에는 통합 서비스 프로세스가 동적으로 로드하는 여러 개의 공유 라이브러리 구성 요소가 포함되어 있습니다. 서비스가 런타임에 공유 라이브러리를 찾을 수 있도록 공유 라이브러리 환경 변수를 설정합니다.

공유 라이브러리 경로는 Informatica 서비스 설치 디렉터리 (*server_dir*)도 포함해야 합니다.

운영 체제에 맞게 공유 라이브러리 환경 변수를 설정합니다.

다음 표에는 각 운영 체제별로 공유 라이브러리 변수가 설명되어 있습니다.

운영 체제	변수
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

예를 들어 Linux의 경우 다음 구문을 사용하십시오.

- Bourne 셸 사용:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib:
$TERADATA_HOME/lib64:$TERADATA_HOME/odbc_64/lib";
export LD_LIBRARY_PATH
```

- C 셸 사용:

```
$ setenv LD_LIBRARY_PATH "${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib:$TERADATA_HOME/lib64:
$TERADATA_HOME/odbc_64/lib"
```

AIX의 경우

- Bourne 셸 사용:

```
$ LIBPATH=${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib:$TERADATA_HOME/lib64:$TERADATA_HOME/odbc_64/
lib; export LIBPATH
```

- C 셸 사용:

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib:$TERADATA_HOME/lib64:
$TERADATA_HOME/odbc_64/lib
```

4. 기존 odbc.ini 파일을 편집하거나 odbc.ini 파일을 홈 디렉터리에 복사한 후 편집합니다.

이 파일은 \$ODBCHOME 디렉터리에 있습니다.

```
$ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
```

[ODBC 데이터 소스] 섹션 아래에 Teradata 데이터 소스에 대한 항목을 추가하고 해당 데이터 소스를 구성합니다.

예를 들어 Teradata Parallel Transporter 유틸리티 버전 15.10의 경우 다음과 같습니다.

```
MY_TERADATA_SOURCE=Teradata Driver
[MY_TERADATA_SOURCE]
Driver=/opt/teradata/client/15.10/lib64/tdata.so
Description=NCR 3600 running Teradata V1R5.2
DBCName=208.199.59.208
DateTimeFormat=AAA
SessionMode=ANSI
DefaultDatabase=
Username=
Password=
```

예를 들어 Teradata Parallel Transporter 유틸리티 버전 16.20의 경우 다음과 같습니다.

```
MY_TERADATA_SOURCE=Teradata Driver
[dwtera]
```

```

Driver=/opt/teradata/client/16.20/lib64/tdataodbc_sb64.so
Description=NCR 3600 running Teradata V1R5.2
DBCName=tdvbe1510
LastName=
Username=
Password=
Database=
DefaultDatabase=
UseNativeLOBSupport=Yes
CharacterSet=UTF8
SessionMode=ANSI

```

5. Teradata 데이터 ODBC 구성에서 `DateTimeFormat`을 AAA로 설정합니다.
6. 필요에 따라 `SessionMode`를 ANSI로 설정합니다. ANSI 세션 모드를 사용하면 행 오류가 발생할 경우 Teradata가 트랜잭션을 롤백하지 않습니다.
Teradata 세션 모드를 선택한 경우 행 오류가 발생할 때 Teradata가 트랜잭션을 롤백합니다. Teradata 모드에서 통합 서비스 프로세스는 이 롤백을 감지할 수 없으며 세션 로그에서 롤백을 보고하지 않습니다.
7. 단일 Teradata 데이터베이스에 대한 연결을 구성하려면 `DefaultDatabase` 이름을 입력합니다. 기본 데이터베이스에 대한 단일 연결을 작성하려면 사용자 이름과 암호를 입력합니다. 동일한 ODBC DSN을 사용하여 여러 데이터베이스에 연결하려면 `DefaultDatabase` 필드를 비워 둡니다.
Teradata 연결에 대한 자세한 내용은 Teradata ODBC 드라이버 설명서를 참조하십시오.
8. `odbc.ini`에서 마지막 항목이 `InstallDir`인지 확인하고 해당 항목을 `odbc` 설치 디렉터리로 설정합니다.
예:

```
InstallDir=<Informatica installation directory>/ODBC<version>
```
9. 일련의 셸 명령을 완전하게 포함하도록 `.cshrc` 또는 `.profile`을 편집합니다.
10. 파일을 저장한 후에 로그아웃했다가 다시 로그인하거나 `source` 명령을 실행합니다.
Bourne 셸 사용:

```
$ source .profile
```


C 셸 사용:

```
$ source .cshrc
```
11. 사용하는 각 데이터 소스에 대해 `odbc.ini`에 있는 해당 데이터 소스 항목의 `Driver=<parameter>` 아래에서 파일 이름을 확인하여 적어 둡니다. `ddtestlib` 유틸리티를 사용하여 DataDirect ODBC 드라이버 관리자가 드라이버 파일을 로드할 수 있는지 확인합니다.
예를 들어 해당 드라이버 항목이 있는 경우 다음을 수행하십시오.

```
Driver=/u01/app/teradata/td-tuf611/odbc/drivers/tdata.so
```


다음 명령을 실행합니다.

```
ddtestlib /u01/app/teradata/td-tuf611/odbc/drivers/tdata.so
```
12. BTEQ 또는 다른 Teradata 클라이언트 도구를 사용하여 연결을 테스트합니다.

JDBC 데이터 소스에 연결

데이터 통합 서비스에서 관계형 대상에 쓰기 작업을 수행할 수 있도록 하려면 관계형 대상이 있는 매핑을 실행하는 모든 클라이언트 시스템과 데이터 통합 서비스 호스트에 JDBC 드라이버 `.jar` 파일을 다운로드합니다.

드라이버 `.jar` 파일은 데이터베이스 공급업체로부터 받을 수 있습니다. 예를 들어 Oracle 데이터베이스에 액세스하려면 Oracle 웹 사이트에서 `ojdbc.jar` 파일을 다운로드합니다.

1. 데이터 통합 서비스 시스템의 `<Informatica 설치 디렉터리 directory>/externaljdbcjars` 디렉터리에 JDBC 드라이버 `.jar` 파일을 배치합니다. 그런 다음 데이터 통합 서비스를 재사용합니다.

2. Developer tool을 호스트하는 시스템의 <Informatica 설치 디렉터리>\\externaljdbcjars 디렉터리에 JDBC 드라이버 .jar 파일을 배치합니다. 그런 다음 Developer tool을 재사용합니다.

ODBC 데이터 소스에 연결

데이터 통합 서비스, PowerCenter 통합 서비스 및 PowerCenter 리포지토리 서비스가 실행되는 시스템에 원시 클라이언트 소프트웨어를 설치하고 구성합니다. 또한 ODBC 드라이버에 필요한 기본 클라이언트 액세스 소프트웨어를 설치 및 구성합니다. Informatica와 데이터베이스 간 호환성을 확보하려면 적합한 데이터베이스 클라이언트 라이브러리를 사용합니다.

Informatica 설치에는 DataDirect ODBC 드라이버가 포함됩니다. odbc.ini 파일에 이전 버전의 ODBC 드라이버를 사용하는 연결이 포함되어 있으면 연결 정보를 업데이트하여 새 드라이버를 사용합니다. Windows에 있는 ODBC 데이터 소스를 지정하려면 시스템 DSN을 사용합니다.

1. 응용 프로그램 서비스가 실행되는 시스템에서 서비스 프로세스를 시작할 수 있는 사용자로 로그인합니다.
2. ODBCHOME 및 PATH 환경 변수를 설정합니다.

ODBCHOME. DataDirect ODBC 설치 디렉터리로 설정합니다. 설치 디렉터리가 /export/home/Informatica/10.0.0/ODBC7.1인 경우를 예로 들어 보겠습니다.

Bourne 셸 사용:

```
$ ODBCHOME=/export/home/Informatica/10.0.0/ODBC7.1; export ODBCHOME
```

C 셸 사용:

```
$ setenv ODBCHOME /export/home/Informatica/10.0.0/ODBC7.1
```

PATH *ddtestlib* 같은 ODBC 명령줄 프로그램을 실행하려면 odbc bin 디렉터리를 포함하도록 변수를 설정합니다.

Bourne 셸 사용:

```
$ PATH=${PATH}:${ODBCHOME}/bin; export PATH
```

C 셸 사용:

```
$ setenv PATH ${PATH}:${ODBCHOME}/bin
```

ddtestlib 유틸리티를 실행하여 DataDirect ODBC 드라이버 관리자가 드라이버 파일을 로드할 수 있는지 확인합니다.

3. 공유 라이브러리 환경 변수를 설정합니다.

ODBC 소프트웨어에는 서비스 프로세스가 동적으로 로드하는 여러 개의 공유 라이브러리 구성 요소가 포함되어 있습니다. 서비스가 런타임에 공유 라이브러리를 찾을 수 있도록 공유 라이브러리 환경 변수를 설정합니다.

공유 라이브러리 경로는 Informatica 설치 디렉터리 (*server_dir*)도 포함해야 합니다.

운영 체제에 맞게 공유 라이브러리 환경 변수를 설정합니다.

다음 표에는 각 운영 체제별로 공유 라이브러리 변수가 설명되어 있습니다.

운영 체제	변수
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

예를 들어 Linux의 경우 다음 구문을 사용하십시오.

- Bourne 셸 사용:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib; export LD_LIBRARY_PATH
```

- C 셸 사용:

```
$ setenv LD_LIBRARY_PATH $HOME/server_dir:$ODBCHOME:${LD_LIBRARY_PATH}
```

AIX의 경우

- Bourne 셸 사용:

```
$ LIBPATH=${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib; export LIBPATH
```

- C 셸 사용:

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib
```

4. 기존 `odbc.ini` 파일을 편집하거나 `odbc.ini` 파일을 홈 디렉터리에 복사한 후 편집합니다.

이 파일은 `$ODBCHOME` 디렉터리에 있습니다.

```
$ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
```

[ODBC 데이터 소스] 섹션 아래에 ODBC 데이터 소스에 대한 항목을 추가하고 해당 데이터 소스를 구성합니다.

예:

```
MY_MSSQLSERVER_ODBC_SOURCE=<Driver name or data source description>
[MY_SQLSERVER_ODBC_SOURCE]
Driver=<path to ODBC drivers>
Description=DataDirect 8.0 SQL Server Wire Protocol
Database=<SQLServer_database_name>
LogonID=<username>
Password=<password>
Address=<TCP/IP address>,<port number>
QuoteId=No
AnsiNPW=No
ApplicationsUsingThreads=1
```

ODBC 데이터 소스를 하나 이상 구성한 경우 이 파일이 이미 존재할 수 있습니다.

5. `odbc.ini`에서 마지막 항목이 `InstallDir`인지 확인하고 해당 항목을 `odbc` 설치 디렉터리로 설정합니다.

예:

```
InstallDir=/export/home/Informatica/10.0.0/ODBC7.1
```

6. 홈 디렉터리에서 `odbc.ini` 파일을 사용할 경우 `ODBCINI` 환경 변수를 설정합니다.

Bourne 셸 사용:

```
$ ODBCINI=$HOME/.odbc.ini; export ODBCINI
```

C 셸 사용:

```
$ setenv ODBCINI $HOME/.odbc.ini
```

7. 일련의 셸 명령을 완전하게 포함하도록 `.cshrc` 또는 `.profile`을 편집합니다. 파일을 저장한 후에 로그아웃했다가 다시 로그인하거나 `source` 명령을 실행합니다.

Bourne 셸 사용:

```
$ source .profile
```

C 셸 사용:

```
$ source .cshrc
```

8. `odbc.ini` 파일에서 데이터 소스에 대해 지정한 드라이버 파일을 DataDirect ODBC 드라이버 관리자가 로드할 수 있는지 `ddtestlib` 유틸리티를 사용하여 확인합니다.

예를 들어 해당 드라이버 항목이 있는 경우 다음을 수행하십시오.

```
Driver = /export/home/Informatica/10.0.0/ODBC7.1/lib/DWxxxxnn.so
```

다음 명령을 실행합니다.

```
ddtestlib /export/home/Informatica/10.0.0/ODBC7.1/lib/DWxxxxnn.so
```

9. ODBC 드라이버에 필요한 기본 클라이언트 액세스 소프트웨어를 설치 및 구성합니다.

참고: 일부 ODBC 드라이버는 자동으로 포함되며 .odbc.ini 파일 내에 모든 정보가 있지만, 대부분은 그렇지 않습니다. 예를 들어 ODBC 드라이버를 사용하여 Sybase IQ에 액세스하려면 Sybase IQ 네트워크 클라이언트 소프트웨어를 설치하고 적절한 환경 변수를 설정해야 합니다.

Informatica ODBC 드라이버(DWxxxxnn.so)를 사용하려면 PATH 및 공유 라이브러리 경로 환경 변수를 수동으로 설정해야 합니다. 또는 \$ODBCHOME 폴더의 odbc.sh 또는 odbc.csh 스크립트를 실행합니다. 이 스크립트는 Informatica에 의해 제공되는 ODBC 드라이버에 대해 필요한 PATH 및 공유 라이브러리 경로 환경 변수를 설정합니다.

샘플 odbc.ini 파일

다음 샘플은 ODBC.ini 파일의 ODBC 드라이버에 대한 항목을 보여 줍니다.

```
[ODBC Data Sources]
SQL Server Legacy Wire Protocol=DataDirect 7.1 SQL Server Legacy Wire Protocol
DB2 Wire Protocol=DataDirect 7.1 DB2 Wire Protocol
Informix Wire Protocol=DataDirect 7.1 Informix Wire Protocol
Oracle Wire Protocol=DataDirect 8.0 Oracle Wire Protocol
Sybase Wire Protocol=DataDirect 7.1 Sybase Wire Protocol
SQL Server Wire Protocol=DataDirect 8.0 SQL Server Wire Protocol
MySQL Wire Protocol=DataDirect 7.1 MySQL Wire Protocol
PostgreSQL Wire Protocol=DataDirect 7.1 PostgreSQL Wire Protocol
Greenplum Wire Protocol=DataDirect 7.1 Greenplum Wire Protocol

[ODBC]
IANAAppCodePage=4
InstallDir=/
```

```

DefaultIsolationLevel=1
DynamicSections=1000
EnableBulkLoad=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
GrantAuthid=PUBLIC
GrantExecute=1
GSSClient=native
HostNameInCertificate=
IpAddress=<DB2_server_host>
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
#Location applies to z/OS and iSeries only
Location=<location_name>
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
PackageCollection=NULLID
PackageNamePrefix=DD
PackageOwner=
Pooling=0
ProgramID=
QueryTimeout=0
ReportCodePageConversionErrors=0
TcpPort=50000
TrustStore=
TrustStorePassword=
UseCurrentSchema=0
ValidateServerCertificate=1
WithHold=1
XMLDescribeType=-10

[Informix Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWifc127.so
Description=DataDirect 7.1 Informix Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
CancelDetectInterval=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
HostName=<Informix_host>
LoadBalancing=0
LogonID=
Password=
PortNumber=<Informix_server_port>
ServerName=<Informix_server>
TrimBlankFromIndexName=1
UseDelimitedIdentifiers=0

[Oracle Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWora28.so
Description=DataDirect 8.0 Oracle Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
AccountingInfo=
Action=
ApplicationName=
ArraySize=60000
AuthenticationMethod=1
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=

```

```

CachedCursorLimit=32
CachedDescLimit=0
CatalogIncludesSynonyms=1
CatalogOptions=0
ClientHostName=
ClientID=
ClientUser=
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
DataIntegrityLevel=0
DataIntegrityTypes=MD5,SHA1
DefaultLongDataBuffLen=1024
DescribeAtPrepare=0
EditionName=
EnableBulkLoad=0
EnableDescribeParam=0
EnableNcharSupport=0
EnableScrollableCursors=1
EnableStaticCursorsForLongData=0
EnableTimestampWithTimeZone=0
EncryptionLevel=0
EncryptionMethod=0
EncryptionTypes=AES128,AES192,AES256,DES,3DES112,3DES168,RC4_40,RC4_56,RC4_128,
RC4_256
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTAsTimestamp=0
GSSClient=native
HostName=<Oracle_server>
HostNameInCertificate=
InitializationString=
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LocalTimeZoneOffset=
LockTimeOut=-1
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Module=
Password=
Pooling=0
PortNumber=<Oracle_server_port>
ProcedureRetResults=0
ProgramID=
QueryTimeout=0
ReportCodePageConversionErrors=0
ReportRecycleBin=0
ServerName=<server_name in tnsnames.ora>
ServerType=0
ServiceName=
SID=<Oracle_System_Identifier>
TimestampEscapeMapping=0
TNSNamesFile=<tnsnames.ora_filename>
TrustStore=
TrustStorePassword=
UseCurrentSchema=1
ValidateServerCertificate=1
WireProtocolMode=2

[Sybase Wire Protocol]
Driver=/

```

```

ArraySize=50
AuthenticationMethod=0
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
Charset=
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
CursorCacheSize=1
Database=<database_name>
DefaultLongDataBuffLen=1024
EnableBulkLoad=0
EnableDescribeParam=0
EnableQuotedIdentifiers=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
GSSClient=native
HostNameInCertificate=
InitializationString=
Language=
LoadBalancing=0
LoadBalanceTimeout=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
NetworkAddress=<Sybase_host,Sybase_server_port>
OptimizePrepare=1
PacketSize=0
Password=
Pooling=0
QueryTimeout=0
RaiseErrorPositionBehavior=0
ReportCodePageConversionErrors=0
SelectMethod=0
ServicePrincipalName=
TruncateTimeTypeFractions=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1
WorkStationID=

[SQL Server Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWsqls28.so
Description=DataDirect 8.0 SQL Server Wire Protocol
AlternateServers=
AlwaysReportTriggerResults=0
AnsiNPW=1
ApplicationName=
ApplicationUsingThreads=1
AuthenticationMethod=1
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadOptions=2
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
EnableBulkLoad=0
EnableQuotedIdentifiers=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0

```

```

FetchTWFSasTime=1
GSSClient=native
HostName=<SQL_Server_host>
HostNameInCertificate=
InitializationString=
Language=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
PacketSize=-1
Password=
Pooling=0
PortNumber=<SQL_Server_server_port>
QueryTimeout=0
ReportCodePageConversionErrors=0
SnapshotSerializable=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1
WorkStationID=
XML Describe Type=-10

[MySQL Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWmysql27.so
Description=DataDirect 7.1 MySQL Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=1024
EnableDescribeParam=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
HostName=<MySQL_host>
HostNameInCertificate=
InteractiveClient=0
LicenseNotice=You must purchase commercially licensed MySQL database software or
a MySQL Enterprise subscription in order to use the DataDirect Connect for ODBC
for MySQL Enterprise driver with MySQL software.
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LogonID=
LoginTimeout=15
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<MySQL_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TreatBinaryAsChar=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1

[PostgreSQL Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWpsql27.so
Description=DataDirect 7.1 PostgreSQL Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0

```

```

ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=2048
EnableDescribeParam=1
EncryptionMethod=1
ExtendedColumnMetadata=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
FetchTWFSasTime=0
GSSClient=native
HostName=<PostgreSQL_host>
HostNameInCertificate=<Host name in SSL certificate>
InitializationString=
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<PostgreSQL_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TransactionErrorBehavior=1
TrustStore=<Path of the truststore certificates>
TrustStorePassword=<Password of the truststore certificates>
ValidateServerCertificate=1
XMLDescribeType=-10

[Greenplum Wire Protocol]
Driver=~/Informatica installation directory/ODBC7.1/lib/DWgplm27.so
Description=DataDirect 7.1 Greenplum Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=2048
EnableDescribeParam=0
EnableKeysetCursors=0
EncryptionMethod=0
ExtendedColumnMetadata=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
FetchTWFSasTime=0
HostName=<Greenplum_host>
InitializationString=
KeyPassword=
KeysetCursorOptions=0
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<Greenplum_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0

```

```
TransactionErrorBehavior=1  
XMLDescribeType=-10
```

참고: 타사 드라이버를 사용하는 경우 ODBC.ini 파일의 DSN 항목을 사용자 지정해야 할 수 있습니다. DSN 항목에 대한 자세한 내용은 해당하는 타사 드라이버 설명서를 참조하십시오.

부록 D

Windows에서 데이터베이스에 연결

이 부록에 포함된 항목:

- [Windows에서 데이터베이스에 연결 개요, 328](#)
- [Windows에서 IBM DB2 범용 데이터베이스에 연결, 329](#)
- [Windows에서 Informix 데이터베이스에 연결, 329](#)
- [Windows에서 Microsoft Access 및 Microsoft Excel에 연결, 330](#)
- [Windows에서 Microsoft SQL Server 데이터베이스에 연결, 330](#)
- [Windows에서 Netezza 데이터베이스에 연결, 332](#)
- [Windows에서 Oracle 데이터베이스에 연결, 333](#)
- [PostgreSQL 데이터베이스에 연결, 334](#)
- [Windows에서 Sybase ASE 데이터베이스에 연결, 335](#)
- [Windows에서 Teradata 데이터베이스에 연결, 337](#)

Windows에서 데이터베이스에 연결 개요

클라이언트, 서비스 및 도메인의 기타 구성 요소 간에 통신을 활성화하려면 연결을 구성하십시오.

원시 연결을 사용하려면 액세스할 데이터베이스의 데이터베이스 클라이언트 소프트웨어를 설치 및 구성해야 합니다. 응용 프로그램 서비스와 데이터베이스 간에 호환성을 보장하려면 데이터베이스 버전과 호환되는 클라이언트 소프트웨어를 설치하고 적절한 데이터베이스 클라이언트 라이브러리를 사용하십시오. 성능을 개선하려면 원시 연결을 사용하십시오.

Informatica 설치에는 **DataDirect ODBC** 드라이버가 포함됩니다. 이전 버전의 드라이버를 사용하여 기존 ODBC 데이터 소스를 작성한 경우 새 드라이버를 사용하여 새 ODBC 데이터 소스를 작성해야 합니다.

Informatica에서 제공하는 **DataDirect ODBC** 드라이버 또는 수준 2 이상과 호환되는 타사 ODBC 드라이버를 사용하여 ODBC 연결을 구성하십시오.

Informatica 설치에는 **DataDirect JDBC** 드라이버가 포함됩니다. 추가 단계를 수행하지 않고 이 드라이버를 사용할 수 있습니다. 타사 공급업체의 JDBC 유형 4 드라이버를 다운로드하여 소스 및 대상에 연결할 수도 있습니다. JDBC 3.0 이상인 타사 JDBC 드라이버를 사용할 수 있습니다.

Informatica 도메인의 다음 서비스에 대해 데이터베이스 연결을 구성해야 합니다.

- PowerCenter 리포지토리 서비스
- 모델 리포지토리 서비스
- 데이터 통합 서비스

- 분석 서비스

Windows에서 IBM DB2 범용 데이터베이스에 연결

원시 연결의 경우 IBM DB2 데이터베이스 서버 버전에 해당하는 IBM DB2 CAE(Client Application Enabler) 버전을 설치하십시오. Informatica와 데이터베이스 간 호환성을 보장하려면 적절한 데이터베이스 클라이언트 라이브러리를 사용하십시오.

원시 연결 구성

IBM DB2 데이터베이스에 대한 원시 연결을 구성하여 성능을 개선할 수 있습니다.

다음 단계에서는 원시 연결을 구성하기 위한 지침을 제공합니다. 특정한 지침은 데이터베이스 설명서를 참조하십시오.

1. IBM DB2 CAE(Client Application Enabler)에서 다음 환경 변수를 설정했는지 확인합니다.


```
DB2HOME=C:\IBM\SQLLIB
DB2INSTANCE=DB2
DB2CODEPAGE=1208 (Sometimes required. Use only if you encounter problems. Depends on the locale, you may use other values.)
```
2. PATH 환경 변수에 IBM DB2 bin 디렉터리가 포함되는지 확인합니다. 예:


```
PATH=C:\WINNT\SYSTEM32;C:\SQLLIB\BIN;...
```
3. 액세스할 데이터베이스에 연결하도록 IBM DB2 클라이언트를 구성합니다. IBM DB2 클라이언트를 구성하려면 다음을 수행하십시오.
 - a. IBM DB2 Configuration Assistant를 실행합니다.
 - b. 데이터베이스 연결을 추가합니다.
 - c. 연결을 바인딩합니다.
4. IBM DB2 명령줄 프로세서에서 다음 명령을 실행하여 IBM DB2 데이터베이스에 연결할 수 있는지 확인합니다.


```
CONNECT TO <dbalias> USER <username> USING <password>
```
5. 연결이 성공하면 TERMINATE 명령을 실행하여 데이터베이스에서 연결을 해제합니다. 연결이 실패하면 데이터베이스 설명서를 참조하십시오.

Windows에서 Informix 데이터베이스에 연결

Windows에서 ODBC를 사용하여 Informix 데이터베이스에 연결합니다. Informatica와 함께 설치되는 DataDirect ODBC 드라이버를 사용하여 ODBC 데이터 소스를 작성합니다. Informatica와 데이터베이스 간 호환성을 보장하려면 적절한 데이터베이스 클라이언트 라이브러리를 사용하십시오.

참고: Informatica에서 제공하는 DataDirect ODBC 드라이버를 사용할 경우 데이터베이스 클라이언트가 필요하지 않습니다. ODBC Wire 프로토콜의 경우 데이터베이스에 연결하기 위한 데이터베이스 클라이언트 소프트웨어가 필요하지 않습니다.

ODBC 연결 구성

Informix 데이터베이스에 대한 ODBC 연결을 구성할 수 있습니다.

다음 단계에서는 ODBC 연결을 구성하기 위한 지침을 제공합니다. 특정한 지침은 데이터베이스 설명서를 참조하십시오.

1. Informatica에서 제공하는 Informix용 DataDirect ODBC Wire 프로토콜 드라이버를 사용하여 ODBC 데이터 소스를 작성합니다.
2. ODBC 데이터 소스를 사용하여 Informix 데이터베이스에 연결할 수 있는지 확인합니다.

Windows에서 Microsoft Access 및 Microsoft Excel에 연결

Windows에서 Informatica 구성 요소에 대한 연결을 구성합니다.

데이터 통합 서비스 및 PowerCenter 통합 서비스 프로세스가 실행되는 시스템에 Microsoft Access 또는 Excel을 설치합니다. 액세스할 Microsoft Access 또는 Excel 데이터에 대한 ODBC 데이터 소스를 작성합니다.

ODBC 연결 구성

Microsoft Access 또는 Excel 데이터베이스에 대한 ODBC 연결을 구성할 수 있습니다.

다음 단계에서는 ODBC 연결을 구성하기 위한 지침을 제공합니다. 특정한 지침은 데이터베이스 설명서를 참조하십시오.

1. Microsoft에서 제공하는 드라이버를 사용하여 ODBC 데이터 소스를 작성합니다.
2. 빈 문자열이나 Null 사용을 방지하려면 데이터베이스 연결을 작성할 때 사용자 이름에 대해 PmNullUser 예약어 및 암호에 대해 PmNullPasswd 예약어를 사용합니다.

Windows에서 Microsoft SQL Server 데이터베이스에 연결

ODBC 또는 OLEDB 공급자 유형을 통해 Microsoft SQL Server 데이터베이스에 연결할 수 있습니다.

원시 연결 구성

ODBC(기본값) 또는 OLEDB 공급자 유형을 사용하여 Microsoft SQL Server 데이터베이스에 대한 원시 연결을 구성할 수 있습니다.

ODBC 공급자 유형을 선택하면 DSN 사용 옵션을 활성화하여 Microsoft ODBC 관리자에 구성되어 있는 DSN을 연결 문자열로 사용할 수 있습니다. DSN 사용 옵션을 활성화하지 않은 경우에는 연결 속성에 서버 이름과 데이터베이스 이름을 지정해야 합니다.

OLEDB 공급자 유형을 선택하면 Microsoft SQL Server 2012 Native Client를 반드시 설치하여 Microsoft SQL Server 데이터베이스에 대한 원시 연결을 구성해야 합니다. 데이터베이스에 연결할 수 없는 경우 모든 연결 정보를 올바르게 입력했는지 확인하십시오.

Microsoft SQL Server 2012 Native Client는 다음 Microsoft 웹 사이트에서 다운로드할 수 있습니다.
<http://www.microsoft.com/en-in/download/details.aspx?id=29065>.

업그레이드한 후에는 Microsoft SQL Server 연결이 기본적으로 OLEDB 공급자 유형으로 설정됩니다. ODBC 공급자 유형을 사용하도록 모든 Microsoft SQL Server 연결을 업그레이드하는 것이 좋습니다. 다음 명령을 사용하면 ODBC 공급자 유형을 사용하도록 모든 Microsoft SQL Server 연결을 업그레이드할 수 있습니다.

- PowerCenter를 사용하는 경우에는 `pmrep upgradeSqlServerConnection` 명령을 실행하십시오.
- Informatica 플랫폼을 사용하는 경우에는 `infacmd.sh isp upgradeSQLSConnection` 명령을 실행하십시오.

자세한 연결 지침은 데이터베이스 설명서를 참조하십시오.

Microsoft SQL Server에 대한 규칙 및 지침

Windows에서 Microsoft SQL Server 데이터베이스를 대상으로 ODBC 연결을 구성하는 경우 다음과 같은 규칙 및 지침을 고려하십시오.

- DSN 미사용 연결, 즉 데이터 소스 이름을 사용하지 않고 Microsoft SQL Server 연결을 사용하려면 `odbcinst.ini` 환경 변수를 구성해야 합니다.
- DSN 연결을 사용하는 경우에는 ODBC DSN에 "EnableQuotedIdentifiers=1" 항목을 추가해야 합니다. 이 항목을 추가하지 않으면 데이터 미리보기 및 매핑 실행이 실패합니다.
- DSN 연결을 사용하는 경우 DataDirect 관련 속성을 구성할 수 있습니다. Data Direct 관련 속성을 구성하고 사용하는 방법에 대한 자세한 내용은 DataDirect 설명서를 참조하십시오.
- Microsoft Windows 플랫폼에서는 DSN 미사용 Microsoft SQL Server 연결에 Microsoft SQL Server NTLM 인증을 사용할 수 있습니다.
- Microsoft SQL Server 테이블에 UUID 데이터 유형이 포함되어 있고, 데이터를 SQL 테이블에서 읽고 플랫폼 파일에 쓰는 경우에는 OLE DB 및 ODBC 연결 유형 사이에 데이터 형식이 일관되지 않을 수 있습니다.
- DSN 미사용 연결에는 SSL 연결을 사용할 수 없습니다. SSL을 사용하려면 DSN 연결을 반드시 사용해야 합니다. DSN 사용 옵션을 활성화하고 `odbc.ini` 파일에 SSL 옵션을 구성하십시오.
- Microsoft SQL Server에서 Kerberos 인증을 사용하는 경우에는 Informatica Kerberos 라이브러리를 가리키도록 GSSClient 속성을 설정해야 합니다. 경로 및 파일 이름으로 `<Informatica 설치 디렉터리>/server/bin/libgssapi_krb5.so.2`를 사용하십시오. DSN 연결의 경우에는 `odbc.ini`의 DSN 항목 섹션에 GSSClient 속성을 위한 항목을 작성하고, DSN 미사용 연결의 경우에는 `odbcinst.ini`의 SQL Server 옵션 프로토콜 섹션에 GSSClient 속성을 위한 항목을 작성하십시오.
- DataDirect ODBC 드라이버를 사용하여 Microsoft SQL Server에 연결하는 경우 10진수 데이터는 데이터베이스 테이블의 소수 자릿수 값에 따라 대상 데이터베이스 내에서 반올림됩니다. 예를 들어 소수 자릿수가 5인 경우 대상 10진수 데이터는 소수점 이하 5번째 자리로 반올림됩니다. 소수 자릿수가 5인 경우 입력 값 12.3456789는 대상 10진수 값 12.34568로 반올림됩니다.
- Microsoft SQL Server 원시 클라이언트를 사용하여 Microsoft SQL Server 데이터베이스에 대한 원시 연결을 구성하는 경우 10진수 데이터는 대상 데이터베이스 테이블에 지정된 소수 자릿수에 따라 잘립니다. 예를 들어 소수 자릿수가 5인 경우 10진수 데이터는 소수점 이하 5번째 자리 다음에 잘립니다. 소수 자릿수가 5인 경우 입력 값 12.3456789는 대상 10진수 값 12.34567로 잘립니다.

Microsoft SQL Server의 사용자 지정 속성 구성

Microsoft SQL Server의 사용자 지정 속성을 구성하여 대량 로드 성능을 개선할 수 있습니다.

1. PowerCenter 클라이언트를 실행하고 워크플로우 관리자에 연결합니다.
2. 워크플로우를 열고 구성하려는 세션을 선택합니다.
3. 개체 구성 탭을 클릭합니다.

4. 기본 버퍼 블록 크기 값을 5MB로 변경합니다. 다음 명령을 사용할 수도 있습니다. `$INFA_HOME/server/bin/.pmrep massupdate -t session_config_property -n "Default buffer block size" -v "5MB" -f <folderName>`
크기가 1KB인 행의 처리량을 최적화하려면 버퍼 블록 크기를 5MB로 설정해야 합니다.
5. 속성 탭을 클릭합니다.
6. 세션에 관계형 대상이 포함되어 있으면 커밋 간격을 100000으로 변경합니다.
7. DTM 버퍼 크기를 설정합니다. 최적의 DTM 버퍼 크기는 ((10 x 블록 버퍼 크기) x 파티션 수)입니다.

Windows에서 Netezza 데이터베이스에 연결

PowerCenter 통합 서비스 프로세스가 실행되고 PowerCenter 클라이언트를 설치한 시스템에 ODBC를 설치 및 구성하십시오. Windows에서 다음 Informatica 구성 요소에 대한 연결을 구성해야 합니다.

- **PowerCenter 통합 서비스.** PowerCenter 통합 서비스 프로세스가 실행되는 시스템에 Netezza ODBC 드라이버를 설치합니다. Microsoft ODBC 데이터 소스 관리자를 사용하여 ODBC 연결을 구성합니다.
- **PowerCenter 클라이언트.** Netezza 데이터베이스에 액세스하는 PowerCenter 클라이언트 시스템 각각에 Netezza ODBC 드라이버를 설치합니다. Microsoft ODBC 데이터 소스 관리자를 사용하여 ODBC 연결을 구성합니다. 워크플로우 관리자를 사용하여 Netezza 데이터베이스에 대한 데이터베이스 연결 개체를 작성합니다.

ODBC 연결 구성

Netezza 데이터베이스에 대한 ODBC 연결을 구성할 수 있습니다.

다음 단계에서는 ODBC 연결을 구성하기 위한 지침을 제공합니다. 특정한 지침은 데이터베이스 설명서를 참조하십시오.

1. 액세스할 Netezza 데이터베이스마다 ODBC 데이터 소스를 작성합니다.

ODBC 데이터 소스를 작성하려면 Netezza에서 제공하는 드라이버를 사용하십시오.

로컬 시스템 계정 로그온으로 Informatica 서비스를 시작한 경우 시스템 DSN을 작성합니다. 이 계정 로그인 옵션을 선택하여 Informatica 서비스를 시작한 경우 사용자 DSN을 작성합니다.

데이터 소스를 작성한 후 데이터 소스의 속성을 구성하십시오.

2. 새 ODBC 데이터 소스에 대한 이름을 입력합니다.
3. Netezza 서버에 대한 IP 주소/호스트 이름 및 포트 번호를 입력합니다.
4. 데이터베이스 개체를 작성할 Netezza 스키마의 이름을 입력합니다.
5. ODBC 로그 파일에 대한 경로 및 파일 이름을 구성합니다.
6. Netezza 데이터베이스에 연결할 수 있는지 확인합니다.

Microsoft ODBC 데이터 소스 관리자를 사용하여 데이터베이스에 대한 연결을 테스트할 수 있습니다. 연결을 테스트하려면 Netezza 데이터 소스를 선택하고 구성을 클릭하십시오. 테스트 탭에서 연결 테스트를 클릭하고 Netezza 스키마에 대한 연결 정보를 입력합니다.

Windows에서 Oracle 데이터베이스에 연결

원시 연결의 경우 Oracle 데이터베이스 서버 버전에 해당하는 Oracle 클라이언트 버전을 설치하십시오. Informatica와 데이터베이스 간 호환성을 보장하려면 적절한 데이터베이스 클라이언트 라이브러리를 사용하십시오.

Oracle 클라이언트 및 Oracle 데이터베이스 서버의 호환 가능한 버전을 설치해야 합니다. 동일한 버전의 Oracle 클라이언트가 필요한 모든 시스템에도 해당 클라이언트를 설치해야 합니다. 호환성을 확인하려면 Oracle에 문의하십시오.

원시 연결 구성

Oracle 데이터베이스에 대한 원시 연결을 구성하여 성능을 개선할 수 있습니다.

다음 단계에서는 Oracle Net Services 또는 Net8을 통한 원시 연결 구성에 대한 지침을 제공합니다. 자세한 연결 지침은 데이터베이스 설명서를 참조하십시오.

1. Oracle 홈 디렉터리가 설정되어 있는지 확인합니다.

예를 들면 다음과 같습니다.

```
ORACLE_HOME=C:\Oracle
```

2. PATH 환경 변수에 Oracle bin 디렉터리가 포함되는지 확인합니다.

예를 들어, Net8을 설치한 경우 경로에 다음 항목이 포함될 수 있습니다.

```
PATH=C:\ORANT\BIN;
```

3. 액세스할 데이터베이스에 연결하도록 Oracle 클라이언트를 구성합니다.

SQL*Net Easy Configuration 유틸리티를 실행하거나 기존 tnsnames.ora 파일을 홈 디렉터리로 편집한 후 수정합니다.

참고: 기본적으로 tnsnames.ora 파일은 다음 디렉터리에 저장됩니다. <OracleInstallationDir>\network\admin.

Oracle 연결 문자열(일반적으로 databasename.world)에 대한 올바른 구문을 입력합니다. 여기서 입력한 SID가 Oracle 서버에 정의된 데이터베이스 서버 인스턴스 ID와 일치하는지 확인합니다.

다음은 샘플 tnsnames.ora 파일입니다. 데이터베이스에 대한 정보를 입력하십시오.

```
mydatabase.world =
  (DESCRIPTION
    (ADDRESS_LIST =
      (ADDRESS =
        (COMMUNITY = mycompany.world
          (PROTOCOL = TCP)
          (Host = mymachine)
          (Port = 1521)
        )
      )
    )
  (CONNECT_DATA =
    (SID = MYORA7)
    (GLOBAL_NAMES = mydatabase.world)
  )
)
```

다음은 Oracle Connection Manager를 사용하여 Oracle에 연결할 샘플 tnsnames.ora 파일입니다.

```
ORCL19C_CMAN =
  (description=
    (address_list=
      (source_route=yes)
      (address=(protocol=tcp)(host=inh74ocm.mycompany.com)(port=1521))
      (address=(protocol=tcp)(host=inh74oradb.mycompany.com)(port=1521))
    )
  (connect_data=
    (service_name=ORCL19C.mycompany.com)
  )
)
```

4. **NLS_LANG** 환경 변수를 데이터베이스 클라이언트 및 서버가 로그인과 함께 사용하도록 할 언어, 국가 및 문자 집합을 포함한 로캘로 설정합니다.
이 변수의 값은 구성에 따라 달라집니다. 예를 들어, 값이 **american_america.UTF8**일 경우 변수를 다음과 같이 설정해야 합니다.

```
NLS_LANG=american_america.UTF8;
```

이 변수의 값을 확인하려면 데이터베이스 관리자에게 문의하십시오.
5. 데이터 통합 서비스가 현지 시간이 포함된 타임스탬프를 읽거나 쓸 때의 기본 세션 시간대를 설정하려면 **ORA_SDTZ** 환경 변수를 지정하십시오.
ORA_SDTZ 환경 변수는 다음 값 중 하나로 설정할 수 있습니다.
 - 운영 체제 현지 시간대('OS_TZ')
 - 데이터베이스 시간대('DB_TZ')
 - UTC의 절대 오프셋(예: '-05:00')
 - 시간대 영역 이름(예: 'America/Los_Angeles')**Informatica** 서버가 실행되는 시스템에서 환경 변수를 설정할 수 있습니다.
6. **tnsnames.ora** 파일이 Oracle 클라이언트 설치 위치와 동일한 위치에 없을 경우 **TNS_ADMIN** 환경 변수를 **tnsnames.ora** 파일이 상주하는 디렉터리로 설정하십시오.
예를 들어, **tnsnames.ora** 파일이 C:\oracle\files 디렉터리에 있는 경우 변수를 다음과 같이 설정하십시오.

```
TNS_ADMIN= C:\oracle\files
```
7. Oracle 데이터베이스에 연결할 수 있는지 확인합니다.
데이터베이스에 연결하려면 **SQL*Plus**를 실행하고 연결 정보를 입력합니다. 데이터베이스에 연결하지 못한 경우 모든 연결 정보를 올바르게 입력했는지 확인합니다.
tnsnames.ora 파일에 정의된 연결 문자열을 사용하십시오.

PostgreSQL 데이터베이스에 연결

원시 연결의 경우 PostgreSQL 데이터베이스 서버 버전에 해당하는 PostgreSQL 클라이언트 버전을 설치하십시오.

Informatica와 데이터베이스 간 호환성을 보장하려면 적절한 데이터베이스 클라이언트 라이브러리를 사용하십시오.

PostgreSQL 클라이언트 및 PostgreSQL 데이터베이스 서버의 호환 가능한 버전을 설치해야 합니다. 동일한 버전의 PostgreSQL 클라이언트가 필요한 모든 시스템에도 해당 클라이언트를 설치해야 합니다. 호환성을 확인하려면 PostgreSQL에 문의하십시오.

원시 연결 구성

PostgreSQL 데이터베이스에 대한 원시 연결을 구성하여 성능을 개선할 수 있습니다.

다음 단계에서는 PostgreSQL을 통해 원시 연결을 구성하기 위한 지침을 제공합니다. 특정한 지침은 데이터베이스 설명서를 참조하십시오.

1. **PowerCenter** 통합 서비스 및 **PowerCenter** 리포지토리 서비스 프로세스에 대해 연결을 구성하려면 서버 프로세스를 시작할 수 있는 사용자로 시스템에 로그인합니다.

- PowerCenter 리포지토리에 대한 PostgreSQL 데이터베이스를 설치하려면 `pg_service.conf` 파일에 대한 PostgreSQL 데이터베이스 호스트, 포트 및 서비스 이름의 값을 다음 형식으로 설정합니다.

```
[PCRS_DB_SERVICE_NAME]
host=Database host IP
port=Database port
dbname=PowerCenter Repository Service database service name
```

PowerCenter 리포지토리에 대한 PostgreSQL에 안전하게 연결하려면 `sslmode`를 `require`로 설정하고 `pg_service.conf` 파일의 나머지 필수 데이터베이스 속성을 `sslmode=require` 형식으로 설정합니다.

- `PGSERVICEFILE`, `PGHOME` 및 `PATH` 환경 변수를 설정합니다.

PGSERVICEFILE. 변수를 PostgreSQL 데이터베이스 연결에 대한 연결 매개 변수가 포함된 `pg_service.conf` 파일로 설정합니다. 예를 들어 다음과 같이 변수를 설정합니다.

Bourne 셸 사용:

```
$ export PGSERVICEFILE; PGSERVICEFILE=<InstallationDirectory>/pg_service.conf
```

C 셸 사용:

```
$ setenv PGSERVICEFILE <InstallationDirectory>/pg_service.conf
```

PGHOME. 변수를 PostgreSQL 클라이언트가 설치된 PostgreSQL 설치 경로로 설정합니다. 예를 들어 다음과 같이 변수를 설정합니다.

Bourne 셸 사용:

```
$ export PGHOME; PGHOME=/usr/pgsql-10
```

C 셸 사용:

```
$ setenv PGHOME /usr/pgsql-10
```

PATH PostgreSQL 명령줄 프로그램을 실행하려면 PostgreSQL 클라이언트 디렉터리 `psql`을 포함하도록 변수를 설정합니다. 예를 들어 다음과 같이 변수를 설정합니다.

Bourne 셸 사용:

```
$ export PATH; PATH=${PATH}:${PGHOME}
```

C 셸 사용:

```
$ setenv PATH ${PGHOME}:${PATH}
```

- PostgreSQL 데이터베이스에 연결할 수 있는지 확인합니다.

PostgreSQL 데이터베이스에 연결하려면 `psql` 유틸리티를 시작하고 연결 정보를 입력합니다.

ODBC 연결 구성

Windows의 PostgreSQL 데이터베이스에 대한 ODBC 연결을 구성할 수 있습니다.

다음 단계에서는 ODBC 연결을 구성하기 위한 지침을 제공합니다.

- Informatica에서 제공하는 PostgreSQL용 DataDirect ODBC 7.1 유선 프로토콜 드라이버를 사용하여 ODBC 데이터 소스를 생성합니다.
- ODBC 데이터 소스를 사용하여 PostgreSQL 데이터베이스에 연결할 수 있는지 확인합니다.

특정한 지침은 데이터베이스 설명서를 참조하십시오.

Windows에서 Sybase ASE 데이터베이스에 연결

원시 연결의 경우 데이터베이스 버전에 해당하는 Open Client 버전을 설치하십시오. Informatica와 데이터베이스 간 호환성을 보장하려면 적절한 데이터베이스 클라이언트 라이브러리를 사용하십시오.

Sybase ASE 데이터베이스 서버와 호환 가능한 Open Client 버전을 설치합니다. 또한 Sybase ASE 데이터베이스 및 Informatica를 호스트하는 시스템에 동일한 버전의 Open Client를 설치해야 합니다. 호환성을 확인하려면 Sybase에 문의하십시오.

Sybase ASE 리포트토리를 작성, 복원 또는 업그레이드할 경우 데이터베이스 수준에서 *allow nulls by default* 를 TRUE로 설정하십시오. 이 옵션을 설정하면 열의 기본 null 유형이 SQL 표준과 호환되는 null로 변경됩니다.

원시 연결 구성

Sybase ASE 데이터베이스에 대한 원시 연결을 구성하여 성능을 개선할 수 있습니다.

다음 단계에서는 원시 연결을 구성하기 위한 지침을 제공합니다. 특정한 지침은 데이터베이스 설명서를 참조하십시오.

1. SYBASE 환경 변수가 Sybase ASE 디렉터리를 참조하는지 확인합니다.

예:

```
SYBASE=C:\SYBASE
```

2. PATH 환경 변수에 Sybase OCS 디렉터리가 포함되는지 확인합니다.

예:

```
PATH=C:\SYBASE\OCS-15_0\BIN;C:\SYBASE\OCS-15_0\DLL
```

3. 액세스할 데이터베이스에 연결하도록 Sybase Open Client를 구성합니다.

SQLEDIT를 사용하여 Sybase 클라이언트를 구성하거나, 기존 SQL.INI 파일(%SYBASE%\INI 디렉터리에 있음)을 복사하여 필요한 사항을 변경합니다.

NLWNSCK를 Net-Library 드라이버를 선택하고 Sybase ASE 서버 이름을 포함합니다.

Sybase ASE 서버에 대한 호스트 이름 및 포트 번호를 입력합니다. 호스트 이름 및 포트 번호를 모르는 경우 시스템 관리자에게 확인하십시오.

4. 필요한 경우 SSL 활성화 Sybase ASE 데이터베이스에 연결하려면 다음 태스크를 수행합니다.

- Sybase 드라이버 속성에서 데이터 소스 이름을 구성할 때 **보안** 탭에서 다음 보안 특성을 지정합니다.

특성	설명
암호화 방법	네트워크를 통해 전송되는 경우 데이터가 암호화되었는지를 나타냅니다. SSL을 선택합니다.
서버 인증서 유효성 검사	SSL 암호화가 활성화된 경우 데이터베이스 서버에서 보낸 인증서에 대해 Informatica에서 유효성을 검사하는지를 나타냅니다.
트러스트 저장소	트러스트 저장소 파일의 위치 및 이름입니다.
트러스트 저장소 암호	트러스트 저장소 파일의 콘텐츠에 액세스하기 위한 암호입니다.
인증서의 호스트 이름	인증서에 포함된 호스트 이름의 유효성을 검사할 수 있도록 하기 위해 SSL 관리자가 설정하는 호스트 이름입니다.

- Sybase ASE 클라이언트의 trusted.txt 파일에 Sybase ASE 서버 인증서를 추가합니다.
- 다음 Sybase ASE 서버 연결 세부 정보를 SQL.INI 파일에 추가합니다.

```
<server_instance_name>
  master tcp ether <host name> <port number> ssl="CN='common_name'"
  query tcp ether <host name> <port number> ssl="CN='common_name'"
```

5. Sybase ASE 데이터베이스에 연결할 수 있는지 확인합니다.

데이터베이스에 연결하려면 ISQL을 실행하고 연결 정보를 입력합니다. 데이터베이스에 연결하지 못한 경우 모든 연결 정보를 올바르게 입력했는지 확인합니다.

사용자 이름 및 데이터베이스 이름은 대/소문자를 구분합니다.

Windows에서 Teradata 데이터베이스에 연결

데이터 통합 서비스 및 PowerCenter 통합 서비스 프로세스가 실행되고 Informatica Developer 및 PowerCenter Client를 설치한 시스템에서 원시 클라이언트 소프트웨어를 설치 및 구성하십시오. Informatica 와 데이터베이스 간 호환성을 보장하려면 적절한 데이터베이스 클라이언트 라이브러리를 사용하십시오. Windows에서 다음 Informatica 구성 요소에 대한 연결을 구성해야 합니다.

- **통합 서비스.** 데이터 통합 서비스 및 PowerCenter 통합 서비스가 실행되는 시스템에서 필요한 Teradata 클라이언트, Teradata ODBC 드라이버 및 기타 Teradata 클라이언트 소프트웨어를 설치하십시오. ODBC 연결도 구성해야 합니다.
- **Informatica Developer.** Teradata에 액세스하는 Developer 도구를 호스트하는 시스템에서 필요한 Teradata 클라이언트, Teradata ODBC 드라이버 및 기타 Teradata 클라이언트 소프트웨어를 설치하십시오. ODBC 연결도 구성해야 합니다.
- **PowerCenter 클라이언트.** Teradata에 액세스하는 PowerCenter Client 시스템에서 필요한 Teradata 클라이언트, Teradata ODBC 드라이버 및 기타 Teradata 클라이언트 소프트웨어를 설치하십시오. 워크플로우 관리자를 사용하여 Teradata 데이터베이스에 대한 데이터베이스 연결 개체를 작성합니다.

참고: Teradata의 권장 사항에 따라 Informatica는 ODBC를 사용하여 Teradata에 연결합니다. ODBC는 Teradata용 원시 인터페이스입니다.

ODBC 연결 구성

Teradata 데이터베이스에 대한 ODBC 연결을 구성할 수 있습니다.

다음 단계에서는 ODBC 연결을 구성하기 위한 지침을 제공합니다. 특정한 지침은 데이터베이스 설명서를 참조하십시오.

1. 액세스할 Teradata 데이터베이스마다 ODBC 데이터 소스를 작성합니다.

ODBC 데이터 소스를 작성하려면 Teradata에서 제공하는 드라이버를 사용하십시오.

로컬 시스템 계정 로그온으로 Informatica 서비스를 시작한 경우 시스템 DSN을 작성합니다. 이 계정 로그인 옵션을 선택하여 Informatica 서비스를 시작한 경우 사용자 DSN을 작성합니다.

2. 새 ODBC 데이터 소스에 대한 이름과 Teradata 서버의 이름 또는 해당 IP 주소를 입력합니다.

단일 Teradata 데이터베이스에 대한 연결을 구성하려면 DefaultDatabase 이름을 입력합니다. 기본 데이터베이스에 대한 단일 연결을 작성하려면 사용자 이름과 암호를 입력합니다. 동일한 ODBC 데이터 소스를 사용하여 여러 데이터베이스에 연결하려면 DefaultDatabase 필드 및 사용자 이름/암호 필드를 비워 두십시오.

3. 옵션 대화 상자에서 날짜 옵션을 구성합니다.

Teradata 옵션 대화 상자에서 날짜/시간 형식에 대해 AAA를 지정합니다.

4. 옵션 대화 상자에서 세션 모드를 구성합니다.

대상 데이터 소스를 작성한 경우 ANSI 세션 모드를 선택합니다. ANSI 세션 모드를 선택한 경우 행 오류가 발생할 때 Teradata가 트랜잭션을 롤백하지 않습니다. Teradata 세션 모드를 선택한 경우 행 오류가 발생할

때 Teradata가 트랜잭션을 롤백합니다. Teradata 모드에서 통합 서비스가 롤백을 감지할 수 없고 이를 세션 로그에 보고하지 않습니다.

5. Teradata 데이터베이스에 연결할 수 있는지 확인합니다.

연결을 테스트하려면 WinDDI, BTEQ, Teradata Administrator 또는 Teradata SQL Assistant 같은 Teradata 클라이언트 프로그램을 사용하십시오.

부록 E

DB2 데이터베이스의 DynamicSections 매개 변수 업데이트

이 부록에 포함된 항목:

- [DynamicSections 매개 변수 개요, 339](#)
- [DynamicSections 매개 변수 설정, 339](#)

DynamicSections 매개 변수 개요

IBM DB2 패키지에는 데이터베이스 서버에서 실행할 SQL 문이 포함되어 있습니다. DB2 데이터베이스의 DynamicSections 매개 변수에 따라 데이터베이스 드라이버가 패키지 1개에 보유할 수 있는 최대 실행 가능한 명령문 수가 결정됩니다. DB2 패키지에서 더 많은 수의 실행 가능한 명령문을 허용하기 위해 DynamicSections 매개 변수 값을 늘릴 수 있습니다. DynamicSections 매개 변수를 수정하려면 BINDADD 권한을 가진 시스템 관리자 사용자 계정을 사용하여 데이터베이스에 연결합니다.

DynamicSections 매개 변수 설정

DataDirect Connect for JDBC 유틸리티를 사용하여 DB2 데이터베이스에서 DynamicSections 매개 변수의 값을 올리십시오.

DataDirect Connect for JDBC 유틸리티를 사용하여 DynamicSections 매개 변수를 업데이트하려면 다음 테스트를 완료하십시오.

- DataDirect Connect for JDBC 유틸리티를 다운로드하고 설치합니다.
- Test for JDBC 도구를 실행합니다.

DDconnect JDBC 유틸리티 다운로드 및 설치

DataDirect 다운로드 웹 사이트에 있는 DataDirect Connect for JDBC 유틸리티를 DB2 데이터베이스 서버에 대한 액세스 권한을 갖는 시스템으로 다운로드합니다. 유틸리티 파일의 콘텐츠를 추출하고 설치 프로그램을 실행합니다.

1. DataDirect 다운로드 사이트로 이동합니다.
<http://www.datadirect.com/support/product-documentation/downloads>
2. IBM DB2 데이터 소스용 Connect for JDBC 드라이버를 선택합니다.
3. DataDirect Connect for JDBC 유틸리티를 다운로드하기 위해 등록합니다.
4. DB2 데이터베이스 서버에 대한 액세스 권한을 갖는 시스템으로 유틸리티를 다운로드합니다.
5. 유틸리티 파일의 콘텐츠를 임시 디렉터리에 추출합니다.
6. 파일을 추출한 디렉터리에서 설치 프로그램을 실행합니다.

설치 프로그램이 `testforjdbc`라는 폴더를 설치 디렉터리에 작성합니다.

Test for JDBC 도구 실행

DataDirect Connect for JDBC 유틸리티를 설치한 후 Test for JDBC 도구를 실행하여 DB2 데이터베이스에 연결하십시오. BINDADD 권한이 있는 시스템 관리자 사용자 계정을 사용하여 데이터베이스에 연결해야 합니다.

1. DB2 데이터베이스에서 BINDADD 권한이 있는 시스템 관리자 사용자 계정을 설정합니다.
2. DataDirect Connect for JDBC 유틸리티를 설치한 디렉터리에서 Test for JDBC 도구(`testforjdbc`)를 실행합니다.
3. Test for JDBC 도구 창에서 Press Here to Continue(계속하려면 여기 누르기)를 클릭합니다.
4. Connection(연결) > Connect to DB(DB에 연결)를 클릭합니다.
5. Database(데이터베이스) 필드에 다음 텍스트를 입력합니다.

```
jdbc:datadirect:db2://  
HostName:PortNumber;databaseName=DatabaseName;CreateDefaultPackage=TRUE;ReplacePackage=TRUE;DynamicSections=3000
```

*HostName*은 DB2 데이터베이스 서버를 호스팅하는 시스템 이름입니다.

*PortNumber*는 데이터베이스의 포트 번호입니다.

*DatabaseName*은 DB2 데이터베이스 이름입니다.

6. User Name(사용자 이름) 및 Password(암호) 필드에서 DB2 데이터베이스에 연결하는 데 사용하는 시스템 관리자 사용자 이름과 암호를 입력합니다.
7. Connect(연결)를 클릭한 다음 창을 닫습니다.

인덱스

A

AddLicense (infacmd)
문제 해결 [236](#)

B

패치 요구 사항

설치 [26](#)

Windows [38](#)

포트

도메인 [27, 39](#)

요구 사항 [27, 39](#)

응용 프로그램 서비스 [27, 39](#)

포트 요구 사항

설치 요구 사항 [27, 39](#)

프로파일링 웨어하우스

IBM DB2 데이터베이스 요구 사항 [58](#)

Microsoft SQL Server 데이터베이스 요구 사항 [59](#)

Oracle 데이터베이스 요구 사항 [59](#)

데이터베이스 요구 사항 [58](#)

호스트 파일

데이터 통합 서비스 [262](#)

환경 변수

INFA_TRUSTSTORE [282](#)

INFA_TRUSTSTORE_PASSWORD [282](#)

LANG [240](#)

LANG_C [240](#)

LC_ALL [240](#)

LC_CTYPE [240](#)

UNIX [241](#)

UNIX 데이터베이스 클라이언트 [77](#)

UNIX에서 구성 [242](#)

UNIX에서의 라이브러리 경로 [242](#)

구성 [241](#)

데이터베이스 클라이언트 [77](#)

로컬 [240](#)

설치 [32, 42](#)

클라이언트 구성 [282](#)

C

catalina.out

설치 문제 해결 [234](#)

D

dbs2 연결

데이터베이스 연결 테스트 [77](#)

Developer tool

타사 소프트웨어 요구 사항 [280](#)

DISPLAY

환경 변수 [42](#)

H

HTTPS

설치 요구 사항 [33, 43](#)

I

i10Pi

UNIX [99](#)

Windows [102](#)

IATEMPDIR

환경 변수 [32, 42](#)

IBM DB2

DB2CODEPAGE 설정 [329](#)

DB2INSTANCE 설정 [329](#)

단일 노드 테이블스페이스 [73](#)

통합 서비스에 연결(Windows) [302, 329](#)

IBM DB2 데이터베이스 요구 사항

Metadata Manager 리포지토리 [63](#)

PowerCenter 리포지토리 [73](#)

데이터 개체 캐시 [57](#)

도메인 리포지토리 [50, 68](#)

모델 리포지토리 데이터베이스 [50, 68](#)

워크플로우 리포지토리 [60](#)

참조 데이터 웨어하우스 [55](#)

프로파일링 웨어하우스 [58](#)

infacmd

개체에 ping 수행 [236](#)

도메인에 노드 추가 [235](#)

infasetup

도메인 정의 [235](#)

작업자 노드 정의 [235](#)

Informatica Administrator

로그인 [246](#)

Informatica Developer

로컬 시스템 [283](#)

로컬 작업 공간 디렉터리 구성 [283](#)

언어 설치 [282](#)

원격 시스템 [283](#)

Informatica 서버

제거 [289](#)

Informatica 서비스

UNIX에서 시작 및 중지 [294](#)

그래픽 모드에서 설치 [155](#)

문제 해결 [236](#)

자동 모드에서 설치 [229](#)

Informatica 클라이언트

그래픽 모드에서 설치 [281](#)

자동 모드에서 설치 [286](#)

제거 [289, 291](#)

Informix

- 통합 서비스에 연결(UNIX) [304](#)
- 통합 서비스에 연결(Windows) [329](#)

isql

- 데이터베이스 연결 테스트 [77](#)

J

JDBC

- 연결(Windows) [328](#)
- JDBC 데이터 소스
연결(UNIX) [318](#)

JRE_HOME

- 환경 변수 [32](#), [42](#)

K

Kerberos SPN 형식 생성기 [83](#)

Kerberos 인증

- SPN 형식 생성 [82](#)
- 구성 파일 [81](#)
- 문제 해결 [246](#)
- 서비스 사용자 이름 생성 [86](#)
- 키 탭 파일 생성 [86](#)
- 키 탭 파일 이름 형식 생성 [82](#)

L

LANG

- 로컬 환경 변수 [32](#), [42](#)
- 환경 변수 [240](#)

LC_ALL

- 로컬 환경 변수 [32](#), [42](#)
- 환경 변수 [240](#)

LC_CTYPE

- 환경 변수 [240](#)

Linux

- 데이터베이스 클라이언트 환경 변수 [77](#)

localhost

- 데이터 통합 서비스 [262](#)

M

Metadata Manager 리포지토리

- IBM DB2 데이터베이스 요구 사항 [63](#)
- IBM DB2 데이터베이스 최적화 [63](#)
- Microsoft SQL Server 데이터베이스 요구 사항 [64](#)
- Oracle 데이터베이스 요구 사항 [65](#)
- 시스템 임시 테이블스페이스 [63](#)
- 합 크기 [63](#)

Metadata Manager 서비스

- 구성 [268](#)
- 리포지토리 콘텐츠 작성 [272](#)
- 분할 도메인 [66](#)
- 분할 도메인 고려 사항 [66](#)
- 작성 [268](#)
- 작성한 후 [272](#)

Metadata Manager를 위한 분할 도메인

- 고려 사항 [66](#)
- 정의 [66](#)

Microsoft Access

- 통합 서비스에 연결 [330](#)

Microsoft Azure SQL Database 요구 사항

- 데이터 개체 캐시 [57](#)

Microsoft Azure SQL Database 요구 사항 (계속)

- 도메인 구성 리포지토리 [51](#), [69](#)
- 워크플로우 데이터베이스 [60](#)
- 참조 데이터 웨어하우스 [55](#)

Microsoft Excel

- PmNullPasswd 사용 [330](#)
- PmNullUser 사용 [330](#)
- 통합 서비스에 연결 [330](#)

Microsoft SQL Server

- UNIX에서 연결 [305](#)
- 통합 서비스에 연결 [330](#)

Microsoft SQL Server 데이터베이스 요구 사항

- Metadata Manager 리포지토리 [64](#)
- PowerCenter 리포지토리 [73](#)
- 데이터 개체 캐시 [57](#)
- 도메인 구성 리포지토리 [51](#), [69](#)
- 워크플로우 리포지토리 [60](#)
- 참조 데이터 웨어하우스 [55](#)
- 프로파일링 웨어하우스 [59](#)

N

Netezza

- Informatica 클라이언트에 연결(UNIX) [306](#)
- Informatica 클라이언트에서 연결(Windows) [332](#)
- 통합 서비스에 연결(UNIX) [306](#)
- 통합 서비스에서 연결(Windows) [332](#)

node.log

- 설치 문제 해결 [234](#)

노드

- 문제 해결 [235](#)

대상 데이터베이스

- JDBC를 통해 연결(UNIX) [318](#)
- ODBC를 통한 연결(UNIX) [319](#)

데이터 개체 캐시

- IBM DB2 데이터베이스 요구 사항 [57](#)
- Microsoft Azure SQL Database 요구 사항 [57](#)
- Microsoft SQL Server 데이터베이스 요구 사항 [57](#)
- Oracle 데이터베이스 요구 사항 [58](#)
- 데이터베이스 요구 사항 [57](#)

데이터 통합 서비스

- 구성 [259](#)
- 작성 [259](#)
- 작성한 후 [262](#)
- 호스트 파일 구성 [262](#)

데이터베이스

- IBM DB2에 연결 [302](#), [329](#)
- Informix에 연결 [304](#), [329](#)
- Microsoft Access에 연결 [330](#)
- Microsoft SQL Server에 연결 [330](#)
- Netezza에 연결(UNIX) [306](#)
- Netezza에 연결(Windows) [332](#)
- Oracle에 연결 [308](#), [333](#)
- PostgreSQL에 연결 [310](#), [334](#)
- Sybase ASE에 연결 [314](#), [335](#)
- Teradata에 연결(UNIX) [316](#)
- Teradata에 연결(Windows) [337](#)
- 리포지토리 [48](#)
- 연결 테스트 [77](#)
- 연결(UNIX) [301](#)
- 연결(Windows) [328](#)

데이터베이스 사용자 계정

- 설정에 대한 지침 [48](#)

데이터베이스 연결

- 생성 [247](#)

데이터베이스 요구 사항

PowerCenter 리포지토리 [72](#)

데이터 개체 캐시 [57](#)

모델 리포지토리 [68](#)

워크플로우 데이터베이스 [59](#)

참조 데이터 웨어하우스 [54](#)

프로파일링 웨어하우스 [58](#)

데이터베이스 준비

리포지토리 [48](#)

데이터베이스 클라이언트

IBM DB2 클라이언트 응용 프로그램 활성화 프로그램 [76](#)

Microsoft SQL Server 원시 클라이언트 [76](#)

Oracle 클라이언트 [76](#)

PostgreSQL 클라이언트 [76](#)

Sybase Open Client [76](#)

구성 [77](#)

환경 변수 [77](#)

도메인

개요 [19](#)

구성 [239](#)

포트 [27, 39](#)

도메인 구성 리포지토리

IBM DB2 데이터베이스 요구 사항 [50, 68](#)

Microsoft Azure SQL Database 요구 사항 [51, 69](#)

Microsoft SQL Server 데이터베이스 요구 사항 [51, 69](#)

Oracle 데이터베이스 요구 사항 [51](#)

PostgreSQL 데이터베이스 요구 사항 [52](#)

Sybase ASE 데이터베이스 요구 사항 [52](#)

데이터베이스 준비 [49](#)

문제 해결 [235](#)

디버그 로그

설치 문제 해결 [234](#)

라이브러리 경로

환경 변수 [32](#)

라이브러리 요구 사항

Windows [38](#)

라이선스

추가 [236](#)

라이선스 키

확인 [36, 46](#)

로그 파일

catalina.out [234](#)

node.log [234](#)

디버그 로그 [234](#)

설치 [233](#)

설치 로그 [234](#)

유형 [233](#)

로그인

문제 해결 [246](#)

로컬 환경 변수

구성 [240](#)

리포지토리

데이터베이스 준비 [48](#)

데이터베이스 클라이언트 설치 [76](#)

원시 연결 구성 [76](#)

리포지토리 콘텐츠 생성

Metadata Manager 서비스 [272](#)

모델 리포지토리

IBM DB2 데이터베이스 요구 사항 [50, 68](#)

Oracle 데이터베이스 요구 사항 [70](#)

PostgreSQL 데이터베이스 요구 사항 [70](#)

데이터베이스 요구 사항 [68](#)

사용자 [258](#)

모델 리포지토리 서비스

구성 [254](#)

생성 [254](#)

작성한 후 [257](#)

문제 해결

Informatica 서비스 [236](#)

Kerberos 인증 [246](#)

도메인 가입 [235](#)

도메인 구성 리포지토리 [235](#)

도메인 생성 [235](#)

도메인에 Ping 수행 [236](#)

라이선스 [236](#)

로그인 [246](#)

보안 도메인

클라이언트 구성 [282](#)

보통 모드

PowerCenter 리포지토리 서비스 [264](#)

분석 서비스

구성 [274](#)

선행 조건 [245](#)

임시 디렉터리 [245](#)

작성 [274](#)

작성한 후 [276](#)

사용자 계정

PowerCenter 리포지토리 [265](#)

UNIX [33](#)

Windows [43](#)

모델 리포지토리 [258](#)

사용자 이름

형식 지정 [86](#)

샘플

odbc.ini 파일 [321](#)

서비스

Windows에서의 설치 전 태스크 [37](#)

서비스 관리자

로그 파일 [234](#)

서비스 사용자 이름

Kerberos 인증 [82](#)

생성 [86](#)

설치

파일 백업 이후 [31, 42](#)

설치 로그

설명 [234](#)

설치 요구 사항

응용 프로그램 서비스 요구 사항 [30, 40](#)

키 저장소 파일 [33, 43](#)

트러스트 저장소 파일 [33, 43](#)

포트 요구 사항 [27, 39](#)

환경 변수 [32, 42](#)

설치 전

UNIX에서의 i10Pi [99](#)

Windows에서의 i10Pi [102](#)

Windows에서의 서비스 [37](#)

소스 데이터베이스

JDBC를 통해 연결(UNIX) [318](#)

ODBC를 통한 연결(UNIX) [319](#)

시스템 요구 사항

응용 프로그램 서비스 [30, 40](#)

최소 [25, 38](#)

언어

클라이언트 도구 [282](#)

업그레이드

파일 백업 이후 [31, 42](#)

연결

IBM DB2 속성 [247](#)

JDBC를 사용하여 Windows [328](#)

Microsoft Azure SQL Database 속성 [248](#)

Microsoft Excel을 통한 서비스에 [330](#)

Microsoft SQL Server 속성 [249](#)

Oracle 속성 [250](#)

PostgreSQL 속성 [251](#)

연결 (계속)

- UNIX 데이터베이스 [301](#)
- Windows 데이터베이스 [328](#)
- 데이터베이스 연결 작성 [247](#), [252](#)
- 통합 서비스를 IBM DB2에(Windows) [302](#), [329](#)
- 통합 서비스를 Informix에(UNIX) [304](#)
- 통합 서비스를 Informix에(Windows) [329](#)
- 통합 서비스를 JDBC 데이터 소스에(UNIX) [318](#)
- 통합 서비스를 Microsoft Access에 [330](#)
- 통합 서비스를 Microsoft SQL Server에 [330](#)
- 통합 서비스를 ODBC 데이터 소스에(UNIX) [319](#)
- 통합 서비스를 Oracle에(UNIX) [308](#)
- 통합 서비스를 Oracle에(Windows) [333](#)
- 통합 서비스를 PostgreSQL에 연결(UNIX) [310](#)
- 통합 서비스를 PostgreSQL에 연결(Windows) [334](#)
- 통합 서비스를 Sybase ASE에(UNIX) [314](#)
- 통합 서비스를 Sybase ASE에(Windows) [335](#)

워크플로우

- IBM DB2 데이터베이스 요구 사항 [60](#)
- Microsoft SQL Server 데이터베이스 요구 사항 [60](#)
- Oracle 데이터베이스 요구 사항 [61](#)
- 데이터베이스 요구 사항 [59](#)

워크플로우 데이터베이스

- Microsoft Azure SQL Database 요구 사항 [60](#)
- PostgreSQL 데이터베이스 요구 사항 [61](#)

응용 프로그램 서비스

- 콘텐츠 관리 서비스 [54](#)
- Metadata Manager 서비스 [62](#)
- 검색 서비스 [75](#)
- 데이터 통합 서비스 [56](#), [71](#)
- 모니터링 모델 리포지토리 서비스 [71](#)
- 모델 리포지토리 서비스 [67](#), [72](#)
- 분석 서비스 [53](#)
- 설치 요구 사항 [30](#), [40](#)
- 제품 [48](#)
- 포트 [27](#), [39](#)

자동 모드

- Informatica 서비스 설치 [229](#)
- Informatica 클라이언트 설치 [286](#)

작동 모드

- PowerCenter 리포지토리 서비스 [264](#)

제거

- 규칙 및 지침 [289](#)

참조 데이터 웨어하우스

- IBM DB2 데이터베이스 요구 사항 [55](#)
- Microsoft Azure SQL Database 요구 사항 [55](#)
- Microsoft SQL Server 데이터베이스 요구 사항 [55](#)
- Oracle 데이터베이스 요구 사항 [55](#)
- 데이터베이스 요구 사항 [54](#)

최소 시스템 요구 사항

- 노드 [30](#), [40](#)

최적화

- PowerCenter 리포지토리 [73](#)

코드 페이지 호환성

- 로컬 [240](#)
- 응용 프로그램 서비스 [240](#)

콘텐츠 관리 서비스

- 구성 [272](#)
- 작성 [272](#)

클라이언트

- 보안 도메인을 위한 구성 [282](#)

클라이언트를 설치하기 전에

- 개요 [280](#)
- 설치 요구 사항 확인 [280](#)
- 최소 시스템 요구 사항 확인 [280](#)

키 저장소 파일

- 설치 요구 사항 [33](#), [43](#)

키 탭 파일

- Kerberos 인증 [82](#), [86](#)
- 타사 소프트웨어 요구 사항
- Developer tool [280](#)
- PowerCenter Client [281](#)
- 테이블스페이스
- 단일 노드 [73](#)
- 트러스트 저장소 파일
- 설치 요구 사항 [33](#), [43](#)
- 파일 백업
- 설치 전 [31](#), [42](#)
- 업그레이드 전 [31](#), [42](#)

O

ODBC 데이터 소스

- 연결(UNIX) [319](#)
- 연결(Windows) [328](#)

odbc.ini 파일

- 샘플 [321](#)

Oracle

- 통합 서비스에 연결(UNIX) [308](#)
- 통합 서비스에 연결(Windows) [333](#)

Oracle Net Services

- 통합 서비스를 Oracle에 연결하는 데 사용(UNIX) [308](#)
- 통합 서비스를 Oracle에 연결하는 데 사용(Windows) [333](#)

Oracle 데이터베이스 요구 사항

- Metadata Manager 리포지토리 [65](#)
- PowerCenter 리포지토리 [73](#)
- 데이터 개체 캐시 [58](#)
- 도메인 구성 리포지토리 [51](#)
- 모델 리포지토리 [70](#)
- 워크플로우 리포지토리 [61](#)
- 참조 데이터 웨어하우스 [55](#)
- 프로파일링 웨어하우스 [59](#)

P

PATH

- 환경 변수 [32](#)

pg_service.conf

- PostgreSQL database requirements [74](#)

PGSERVICEFILE environment variable

- PostgreSQL database requirements [74](#)

Ping (infacmd)

- 문제 해결 [236](#)

PostgreSQL

- 통합 서비스에 연결(UNIX) [310](#)
- 통합 서비스에 연결(Windows) [334](#)

PostgreSQL database requirements

- pg_service.conf [74](#)
- PGSERVICEFILE environment variable [74](#)
- PowerCenter repository [74](#)

PostgreSQL 데이터베이스 요구 사항

- 도메인 구성 리포지토리 [52](#)
- 모델 리포지토리 [70](#)
- 워크플로우 데이터베이스 [61](#)

PowerCenter repository

- PostgreSQL database requirements [74](#)

PowerCenter 리포지토리

- IBM DB2 데이터베이스 요구 사항 [73](#)
- IBM DB2 데이터베이스 최적화 [73](#)
- Microsoft SQL Server 데이터베이스 요구 사항 [73](#)
- Oracle RAC [73](#)
- Oracle 데이터베이스 요구 사항 [73](#)
- Sybase ASE 데이터베이스 요구 사항 [75](#)

PowerCenter 리포지토리 *(계속)*

데이터베이스 요구 사항 [72](#)
사용자 [265](#)

PowerCenter 리포지토리 서비스

구성 [262](#)
보통 모드 [264](#)
작성 [262](#)
작성한 후 [264](#)

PowerCenter 클라이언트

타사 소프트웨어 요구 사항 [281](#)

PowerCenter 통합 서비스

구성 [266](#)
작성 [266](#)
작성한 후 [268](#)

S

SPN [82](#)

sqlplus

데이터베이스 연결 테스트 [77](#)

Sybase ASE

통합 서비스에 연결(UNIX) [314](#)
통합 서비스에 연결(Windows) [335](#)

Sybase ASE 데이터베이스 요구 사항

PowerCenter 리포지토리 [75](#)
도메인 구성 리포지토리 [52](#)

T

Teradata

Informatica 클라이언트에 연결(UNIX) [316](#)
Informatica 클라이언트에 연결(Windows) [337](#)
통합 서비스에 연결(UNIX) [316](#)
통합 서비스에 연결(Windows) [337](#)

U

UNIX

i10Pi [99](#)

UNIX *(계속)*

Informatica 서비스 시작 및 중지 [294](#)

JDBC 데이터 소스에 연결 [318](#)

Kerberos SPN 형식 생성기 [83](#)

ODBC 데이터 소스에 연결 [319](#)

데이터베이스 클라이언트 변수 [77](#)

데이터베이스 클라이언트 환경 변수 [77](#)

라이브러리 경로 [242](#)

사용자 계정 [33](#)

설치 전 [99](#)

환경 변수 [241](#)

W

Windows

i10Pi [102](#)

그래픽 모드에서 Informatica 서비스 설치 [155](#)

그래픽 모드에서 Informatica 클라이언트 설치 [281](#)

라이브러리 요구 사항 [38](#)

사용자 계정 [43](#)

설치 전 [102](#)

패치 요구 사항 [38](#)

ㄱ

개요

클라이언트를 설치하기 전에 [280](#)

검색 서비스

구성 [276](#)

작성 [276](#)

구성

Kerberos 파일 [81](#)

UNIX에서의 환경 변수 [242](#)

도메인 [239](#)

환경 변수 [241](#)

그래픽 모드

Informatica 서비스 설치 [155](#)

Informatica 클라이언트 설치 [281](#)