



Informatica®
10.5.2

보안 가이드

Informatica 보안 가이드

10.5.2

2022년4월

© 저작권 Informatica LLC 2013, 2022

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

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.

Informatica, Informatica 로고, Informatica Cloud, 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.

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

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

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.

발행 날짜: 2022-06-22

목차

서문	11
Informatica 리소스	11
Informatica Network	11
Informatica 기술 자료	11
Informatica 설명서	11
Informatica Product Availability Matrix	12
Informatica Velocity	12
Informatica Marketplace	12
Informatica 글로벌 고객 지원 센터	12
장 1: Informatica 보안 소개	13
Informatica 보안 개요	13
하부 구조 보안	14
인증	14
보안 도메인 통신	15
보안 데이터 저장소	15
운영 보안	15
도메인 구성 리포지토리	16
보안 도메인	16
장 2: 사용자 인증	18
사용자 인증 개요	18
원시 사용자 인증	19
LDAP 사용자 인증	19
Kerberos 인증	20
Informatica 웹 응용 프로그램에 대한 SAML 인증	20
장 3: LDAP 인증	21
개요	21
LDAP 보안 도메인	21
사용자 계정 동기화	22
LDAP 디렉터리 서비스	22
보안 LDAP 인증을 위한 Azure Active Directory	23
Active Directory 사용자 계정 가져오는 작업 준비	23
LDAP 구성 생성	24
LDAP 구성을 생성하고 LDAP 서버 연결 구성	25
보안 도메인 구성	26
동기화 일정 구성	27
LDAP 디렉터리 서비스에서 중첩 그룹 사용	28
자체 서명된 SSL 인증서 사용	28

LDAP 구성 삭제.	29
------------------	----

장 4: Kerberos 인증..... 30

Kerberos 개요.	30
Informatica 도메인에서 Kerberos가 작동하는 방식.	31
Kerberos 교차 영역 인증.	33
Kerberos 단일 영역 인증의 도메인을 Kerberos 교차 영역 인증으로 변환.	33
Kerberos 인증 활성화 준비.	34
Kerberos 서비스 사용자 수준 결정.	34
Kerberos 구성 파일 구성.	35
Active Directory에서 Kerberos 사용자 계정 생성.	38
서비스 사용자 이름 및 keytab 파일 이름 형식 생성.	39
keytab 파일 생성.	44
Kerberos 인증 활성화.	47
도메인에서 Kerberos 인증 활성화.	48
도메인의 노드 업데이트.	50
Informatica 노드에서 Kerberos 활성화.	51
Informatica 노드에 keytab 파일 복사.	52
Informatica 클라이언트에 대한 Kerberos 인증 활성화.	53
Hadoop 통합을 위해 Kerberos 활성화.	54
Kerberos 인증을 사용하도록 사용자 계정 설정.	54
Active Directory의 사용자 계정을 LDAP 보안 도메인으로 가져오기.	54
원시 사용자 권한 및 사용 권한을 Kerberos 보안 도메인으로 마이그레이션.	57
Kerberos 위임.	58
Kerberos 위임 유형.	58
S4U(사용자 서비스) 확장.	59
S4U2Self로 리소스 기반 제한 위임 활성화.	59
Active Directory에서 Kerberos 주 사용자 계정에 대한 전체 위임 활성화.	59
전체 위임에서 제한 위임으로 전환.	60

장 5: Informatica 웹 응용 프로그램에 대한 SAML 인증..... 61

SAML 인증 개요.	61
기본 키 저장소 및 트러스트 저장소 디렉터리.	62
지원되는 ID 공급자.	62
SAML 인증 프로세스.	63
도메인에서 SAML 인증 활성화.	63
ID 공급자 또는 LDAP 저장소에 대한 LDAP 구성 생성.	64
어설션 서명 인증서 내보내기.	64
SAML 인증에 사용되는 트러스트 저장소로 인증서 가져오기.	64
ID 공급자 구성.	64
ID 공급자에 Informatica 웹 응용 프로그램 URL 추가.	65
도메인에서 SAML 인증 설정.	65

노드에서 SAML 인증 활성화.	65
인증 보안 강화.	66
요청 서명.	66
서명된 응답.	67
암호화된 어설션.	68
다른 ID 공급자를 사용하도록 웹 응용 프로그램 구성.	68
ID 공급자 사용 준비.	69
ID 공급자를 사용하도록 Informatica Administrator 구성.	69
Informatica 웹 응용 프로그램 구성.	70

장 6: 도메인 보안..... 73

도메인 보안 개요.	73
도메인 내에서 보안 통신.	74
서비스와 서비스 관리자를 위한 보안 통신.	74
보안 도메인 구성 리포지토리 데이터베이스.	80
보안 PowerCenter 리포지토리 데이터베이스.	83
보안 모델 리포지토리 데이터베이스.	83
워크플로우 및 세션에 대한 보안 통신.	84
웹 응용 프로그램 서비스에 대한 보안 연결.	85
웹 응용 프로그램 서비스에 대한 보안 연결을 위한 요구 사항.	85
Administrator 도구에 대한 보안 연결 활성화.	86
Informatica 웹 응용 프로그램 서비스.	86
Informatica 도메인의 암호화 그룹.	88
암호화 그룹 목록 작성.	89
새로운 암호화 그룹 유효 목록을 사용하여 Informatica 도메인 구성.	90
보안 소스 및 대상.	91
데이터 통합 서비스 소스 및 대상.	92
PowerCenter 소스 및 대상.	93
보안 데이터 저장소.	93
UNIX에서 보안 디렉터리.	93
명령줄에서 암호화 키 변경.	94
응용 프로그램 서비스 및 포트.	97

장 7: Informatica Administrator에서 보안 관리..... 100

Informatica Administrator 사용 개요.	100
사용자 보안.	101
암호화.	101
인증.	101
권한 부여.	102
보안 탭.	103
검색 섹션 사용.	103
보안 탐색기 사용.	103

그룹.....	104
사용자.....	104
역할.....	105
운영 체제 프로필.....	105
LDAP 구성.....	105
계정 관리.....	106
감사 보고서.....	106
암호 관리.....	106
암호 변경.....	107
도메인 보안 관리.....	107
사용자 보안 관리.....	108

장 8: 사용자 및 그룹..... 109

사용자 및 그룹 개요.....	109
기본 그룹.....	110
관리자 그룹.....	110
모든 사람 그룹.....	110
운영자 그룹.....	110
사용자 계정 이해.....	111
기본 관리자.....	111
도메인 관리자.....	111
응용 프로그램 클라이언트 관리자.....	111
사용자.....	112
사용자 관리.....	113
원시 사용자 생성.....	113
원시 사용자의 일반 속성 편집.....	114
원시 그룹에 원시 사용자 할당.....	114
원시 그룹에 LDAP 사용자 할당.....	114
사용자 계정 활성화 및 비활성화.....	114
원시 사용자 삭제.....	115
LDAP 사용자.....	115
사용자 계정 잠금 해제.....	115
여러 사용자를 위해 시스템 메모리 늘리기.....	116
사용자 활동 보기.....	117
그룹 관리.....	120
원시 그룹 추가.....	121
원시 그룹의 속성 편집.....	121
원시 그룹에서 다른 원시 그룹으로 이동.....	122
원시 그룹 삭제.....	122
LDAP 그룹.....	122
운영 체제 프로필 관리.....	122
PowerCenter 통합 서비스에 대한 운영 체제 프로필 속성.....	122

데이터 통합 서비스에 대한 운영 체제 프로필 속성.	124
메타데이터 액세스 서비스에 대한 운영 체제 프로필 속성.	126
운영 체제 프로필 작성.	126
운영 체제 프로필 편집.	127
사용자 또는 그룹에 기본 운영 체제 프로필 할당.	128
운영 체제 프로필 삭제.	128
보안 도메인에서 운영 체제 프로필 작업.	128
Kerberos 인증을 사용하는 도메인에서 운영 체제 프로필 작업.	129
계정 잠금.	129
계정 잠금 구성.	130
계정 잠금에 대한 규칙 및 지침.	130
장 9: 권한 및 역할.	131
권한.	131
권한 그룹.	132
역할.	132
도메인 권한.	133
보안 관리 권한 그룹.	133
도메인 관리 권한 그룹.	134
모니터링 권한 그룹.	138
도구 권한 그룹.	139
Cloud 관리 권한 그룹.	139
분석 서비스 권한.	140
콘텐츠 관리 서비스 권한.	141
데이터 통합 서비스 권한.	141
대량 수집 서비스 권한.	142
Metadata Manager 서비스 권한.	142
카탈로그 권한 그룹.	143
로드 권한 그룹.	144
모델 권한 그룹.	145
보안 권한 그룹.	145
모델 리포지토리 서비스 권한.	145
PowerCenter 리포지토리 서비스 권한.	146
도구 권한 그룹.	147
폴더 권한 그룹.	148
디자인 개체 권한 그룹.	149
소스 및 대상 권한 그룹.	152
런타임 개체 권한 그룹.	154
글로벌 개체 권한 그룹.	158
PowerExchange 수신기 서비스 권한.	160
PowerExchange 로거 서비스 권한.	160
스케줄러 서비스 권한.	161

Test Data Manager 서비스 권한.....	162
관리 권한 그룹.....	162
연결 권한 그룹.....	162
데이터 도메인 권한 그룹.....	163
데이터 마스킹 권한 그룹.....	163
데이터 하위 집합 권한 그룹.....	163
정책 권한 그룹.....	164
프로젝트 권한 그룹.....	164
규칙 권한 그룹.....	164
데이터 생성 권한 그룹.....	165
역할 관리.....	165
시스템 정의 역할.....	165
사용자 지정 역할.....	166
사용자 및 그룹에 권한 및 역할 할당.....	168
상속된 권한.....	168
탐색으로 사용자 또는 그룹에 권한 및 역할 할당.....	169
서비스에 대한 권한을 가진 사용자 보기.....	169
권한 및 역할 문제 해결.....	170
장 10: 사용 권한.....	172
사용 권한 개요.....	172
사용 권한 유형.....	173
사용 권한 검색 필터.....	174
도메인 개체 사용 권한.....	174
도메인 개체별 사용 권한.....	175
사용자 또는 그룹별 사용 권한.....	176
운영 체제 프로필 사용 권한.....	177
연결 사용 권한.....	178
연결 사용 권한 유형.....	179
기본 연결 사용 권한.....	179
연결에 대한 사용 권한 할당.....	179
연결에 대한 사용 권한 세부 정보 보기.....	180
연결에 대한 사용 권한 편집.....	180
클러스터 구성 사용 권한.....	180
응용 프로그램 및 응용 프로그램 개체 사용 권한.....	181
응용 프로그램 및 응용 프로그램 개체 사용 권한의 유형.....	181
응용 프로그램 또는 응용 프로그램 개체에 대한 사용 권한 할당.....	181
응용 프로그램 또는 응용 프로그램 개체에 대한 사용 권한 세부 정보 보기.....	182
응용 프로그램 또는 응용 프로그램 개체에 대한 사용 권한 편집.....	182
응용 프로그램 또는 응용 프로그램 개체에 대한 사용 권한 거부.....	183
SQL 데이터 서비스 사용 권한.....	183
SQL 데이터 서비스 사용 권한 유형.....	183

SQL 데이터 서비스에 대한 사용 권한 할당.....	184
SQL 데이터 서비스에 대한 사용 권한 세부 정보 보기.....	184
SQL 데이터 서비스에 대한 사용 권한 편집.....	184
SQL 데이터 서비스에 대한 사용 권한 거부.....	185
열 수준 보안.....	185
웹 서비스 사용 권한.....	187
웹 서비스 사용 권한 유형.....	187
웹 서비스에 대한 사용 권한 할당.....	188
웹 서비스에 대한 사용 권한 세부 정보 보기.....	188
웹 서비스에 대한 사용 권한 편집.....	189

장 11: 감사 보고서..... 190

감사 보고 개요.....	190
사용자 개인 정보.....	191
사용자 그룹 연관.....	191
권한.....	192
역할 연관.....	193
도메인 개체 사용 권한.....	193
감사 보고서를 위한 사용자 선택.....	194
감사 보고서를 위한 그룹 선택.....	194
감사 보고서를 위한 역할 선택.....	195

부록 A: 명령줄 권한 및 사용 권한..... 196

infacmd as 명령.....	196
infacmd cluster 명령.....	197
infacmd dis 명령.....	198
infacmd dp 명령.....	199
infacmd es 명령.....	199
infacmd ipc 명령.....	200
infacmd isp 명령.....	200
infacmd mas 명령.....	208
infacmd mi 명령.....	209
infacmd mrs 명령.....	209
infacmd ms 명령.....	211
infacmd tools 명령.....	212
infacmd ps 명령.....	212
infacmd pwx 명령.....	213
infacmd rms 명령.....	214
infacmd rtm 명령.....	214
infacmd sch 명령.....	214
infacmd sql 명령.....	215
infacmd wfs 명령.....	216

pmcmd 명령.	216
pmrep 명령.	219
부록 B: 사용자 지정 역할.	224
분석 서비스 사용자 지정 역할.	224
Metadata Manager 서비스 사용자 지정 역할.	225
운영자 사용자 지정 역할.	226
PowerCenter 리포지토리 서비스 사용자 지정 역할.	227
Test Data Manager 사용자 지정 역할.	228
인덱스.	232

서문

*Informatica 보안 가이드*에서는 Informatica 도메인에서 보안을 활성화하는 방법을 알아볼 수 있습니다. 또한 LDAP(Lightweight Directory Access Protocol), Kerberos 및 SAML(Security Assertion Markup Language)을 포함하는 다양한 인증 프로토콜을 구성 및 관리하는 방법, 사용자 및 그룹을 구성하는 방법과 사용 권한, 권한 및 역할을 사용하여 사용자 보안을 관리하는 방법에 대해서도 알아볼 수 있습니다.

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.

제 1 장

Informatica 보안 소개

이 장에 포함된 항목:

- [Informatica 보안 개요, 13](#)
- [하부 구조 보안, 14](#)
- [운영 보안, 15](#)
- [도메인 구성 리포지토리, 16](#)
- [보안 도메인, 16](#)

Informatica 보안 개요

Informatica 도메인을 보호하여 도메인이 실행되는 네트워크 안팎의 위협으로부터 보호할 수 있습니다.

Informatica 도메인에 대한 보안은 다음 유형의 보안을 포함합니다.

하부 구조 보안

하부 구조 보안은 Informatica 도메인의 서비스 및 리소스 수정 또는 무단 액세스로부터 Informatica 도메인을 보호합니다. 하부 구조 보안은 다음과 같은 양상을 포함합니다.

- Informatica 도메인에 전달되고 저장된 데이터 보호
- Informatica 도메인에 연결되는 사용자 및 서비스 인증
- 리포지토리, 소스 및 대상에 대한 관계형 데이터베이스 및 클라이언트 응용 프로그램을 포함한 외부 구성 요소에 대한 연결 보호

운영 보안

운영 보안은 Informatica 도메인의 데이터 및 서비스에 대한 액세스를 제어합니다. 운영 보안은 다음과 같은 양상을 포함합니다.

- 조직의 사용자 역할을 기반으로 데이터 및 메타데이터에 대한 사용자 액세스에 제한 설정
- 조직의 사용자 역할을 기반으로 Informatica 도메인에서 작업을 수행하기 위한 사용자 기능에 제한 설정

Informatica는 도메인 구성 리포지토리의 도메인에 액세스하기 위해 권한 부여된 사용자 목록 및 도메인 구성 정보를 저장합니다. 또한 도메인 구성 리포지토리에는 Informatica 도메인의 각 사용자에게 할당된 그룹, 역할, 권한 및 사용 권한도 포함되어 있습니다.

Informatica는 보안 도메인별로 사용자 목록을 구성합니다. 보안 도메인에는 사용자 계정 컬렉션이 포함되어 있습니다. 한 도메인이 여러 보안 도메인을 가질 수 있습니다.

하부 구조 보안

하부 구조 보안에는 사용자 및 서비스 인증, 도메인 내의 보안 통신, 보안 데이터 저장소가 포함됩니다.

인증

서비스 관리자는 도메인에서 실행하는 서비스 및 **Informatica** 클라이언트 도구에 로그인하는 사용자를 인증합니다.

Informatica 도메인을 구성하면 다음 유형의 인증을 사용할 수 있습니다.

원시 인증

원시 인증은 **Informatica** 도메인의 사용자 계정에만 사용 가능한 인증 모드입니다. **Informatica** 도메인이 원시 인증을 사용하는 경우 서비스 관리자는 도메인 구성 리포지토리에 사용자 자격 증명 및 권한을 저장하고 **Informatica** 도메인에서 모든 사용자 인증을 수행합니다.

Informatica 도메인이 원시 인증을 사용하는 경우 기본적으로 도메인에 원시 보안 도메인이 있고 모든 사용자 계정이 원시 보안 도메인에 속합니다.

Informatica는 사용자 이름 및 암호를 사용하여 **Informatica** 도메인에서 사용자 및 서비스를 인증합니다.

LDAP(Lightweight Directory Access Protocol) 인증

LDAP는 네트워크에서 사용자 및 리소스에 액세스하기 위한 소프트웨어 프로토콜입니다. **Informatica** 도메인이 LDAP 인증을 사용하는 경우 사용자 계정 및 자격 증명이 LDAP 디렉터리 서비스에 저장됩니다. 사용자 권한 및 사용 권한이 도메인 구성 리포지토리에 저장됩니다. 도메인 구성 리포지토리의 사용자 계정을 LDAP 디렉터리 서비스의 사용자 계정과 정기적으로 동기화해야 합니다.

Informatica는 사용자 이름 및 암호를 사용하여 **Informatica** 도메인에서 **informatica** 사용자 및 서비스를 인증합니다.

Kerberos 인증

Kerberos는 네트워크에서 사용자 및 서비스를 인증하기 위해 티켓을 사용하는 네트워크 인증 프로토콜입니다. **Informatica** 도메인이 Kerberos 인증을 사용하는 경우 사용자 계정 및 자격 증명이 LDAP 디렉터리 서비스일 수 있는 Kerberos 사용자 데이터베이스에 저장됩니다. 사용자 권한 및 사용 권한이 도메인 구성 리포지토리에 저장됩니다. 도메인 구성 리포지토리의 사용자 계정을 Kerberos 사용자 데이터베이스의 사용자 계정과 정기적으로 동기화해야 합니다.

Informatica는 Kerberos 티켓을 사용하여 **Informatica** 도메인에서 **Informatica** 사용자 및 서비스를 인증합니다.

SAML 기반 Single Sign-on

SAML(Security Assertion Markup Language)은 서비스 공급자와 ID 공급자 사이에 인증 및 권한 부여 정보를 교환하기 위한 XML 기반 데이터 형식입니다. SAML 기반 Single Sign-on은 Administrator 도구, Analyst 도구 및 Monitoring 도구 웹 응용 프로그램에 대해 구성할 수 있습니다.

Informatica 도메인, **Informatica** 웹 응용 프로그램은 서비스 공급자이고 Microsoft AD FS(Active Directory Federation Services)는 ID 공급자입니다. **Informatica** 웹 응용 프로그램 사용자의 계정 및 자격 증명은 Microsoft Active Directory에 저장됩니다. 계정을 Active Directory에서 **Informatica** 도메인 내의 보안 도메인으로 가져옵니다. 보안 도메인의 사용자 계정을 Active Directory 디렉터리 서비스의 사용자 계정과 정기적으로 동기화해야 합니다.

Kerberos 인증을 사용하도록 구성된 **Informatica** 도메인에서는 SAML 기반 Single Sign-on을 활성화할 수 없습니다.

보안 도메인 통신

Informatica 도메인에는 도메인 및 클라이언트 응용 프로그램의 서비스와 서비스 관리자 간에 전송되는 데이터 및 메타데이터를 보호하는 다양한 옵션이 있습니다. **Informatica**는 TCP/IP 및 HTTP 프로토콜을 사용하여 도메인의 구성 요소 간에 통신하고 SSL 인증서를 사용하여 도메인의 서비스와 서비스 관리자 간 통신을 보호합니다.

SSL/TLS 프로토콜은 공개 키 암호화를 사용하여 네트워크 트래픽을 암호화하고 암호 해독합니다. 트래픽을 암호화하고 암호 해독하는 데 사용되는 공개 키는 서명되거나 자체 서명될 수 있는 SSL 인증서에 저장됩니다. 자체 서명된 인증서는 인증서의 작성자에 의해 서명됩니다. 서명자의 ID가 확인되지 않으므로 자체 서명된 인증서는 서명된 인증서보다 덜 안전합니다. 서명된 인증서는 CA(인증 기관)에 의해 확인된 인증서를 요청한 사람의 ID가 있는 SSL 인증서입니다. **Informatica**에서는 더 높은 보안 수준을 위해 CA에서 서명한 인증서를 권장합니다.

키 저장소에는 개인 키와 인증서가 포함되어 있습니다. 이것은 자격 증명을 제공하는 데 사용됩니다. 트러스트 저장소에는 트러스트된 SSL/TLS 서버의 인증서가 포함되어 있습니다. 이것은 자격 증명을 확인하는 데 사용됩니다.

도메인의 연결을 보호하기 위해 **Informatica**는 PEM 및 JKS 형식의 키 저장소와 트러스트 저장소를 요구합니다. 다음 프로그램을 사용하여 필수 파일을 작성할 수 있습니다.

keytool

Java **keytool** 키 및 인증서 관리 유틸리티를 사용하여 SSL 인증서 또는 CSR(인증서 서명 요청)은 물론, JKS 형식의 키 저장소 및 트러스트 저장소를 생성할 수도 있습니다.

keytool 유틸리티는 도메인 노드의 다음 디렉터리에서 사용할 수 있습니다.

<Informatica installation directory>\java\bin

도메인 노드를 AIX에서 실행하는 경우 IBM JDK와 함께 제공되는 **keytool**을 사용하여 SSL 인증서 또는 CSR(인증서 서명 요청)과 키 저장소 및 트러스트 저장소를 생성할 수 있습니다.

OpenSSL

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

OpenSSL에 대한 자세한 내용은 다음 웹 사이트의 설명서를 참조하십시오.

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

보호하는 연결 유형에 따라 필요한 파일이 결정됩니다.

보안 데이터 저장소

Informatica는 도메인 구성 리포지토리에 데이터를 저장하기 전에 암호 및 보안 연결 매개 변수와 같은 중요한 데이터를 암호화합니다. 또한 **Informatica**는 구성 파일과 같은 중요한 파일을 보안 디렉터리에 저장합니다.

운영 보안

권한, 역할 및 사용 권한을 사용자 또는 사용자 그룹에 할당하여 사용자 및 그룹이 가질 수 있는 액세스 수준과 사용자 및 그룹이 도메인에서 수행할 수 있는 작업 범위를 관리할 수 있습니다.

다음 방법을 사용하여 도메인에서 사용자 및 그룹 액세스를 관리할 수 있습니다.

권한

권한에 따라 사용자가 **Informatica** 클라이언트 도구에서 수행할 수 있는 작업이 결정됩니다. 권한 집합을 사용자에게 할당하여 도메인에서 사용 가능한 서비스에 대한 액세스를 제한할 수 있습니다. 또한 그룹의 모든 사용자에게 서비스에 대한 동일한 액세스를 허용하도록 그룹에 권한을 할당할 수 있습니다.

역할

역할은 사용자 또는 그룹에 할당할 수 있는 권한 집합입니다. 역할을 사용하면 사용자에게 대한 권한 할당을 좀 더 쉽게 관리할 수 있습니다. 제한된 권한을 가진 역할을 작성하고 도메인 서비스에 제한된 액세스 권한을 가진 사용자 및 그룹에 할당합니다. 또는 관련된 권한을 가진 역할을 작성하여 동일한 수준의 액세스가 필요한 사용자 및 그룹에 할당할 수 있습니다.

사용 권한

사용 권한은 사용자의 개체에 대한 액세스 수준을 정의합니다. 특정 작업을 수행하기 위한 권한이 있는 사용자가 특정 개체에서 작업을 수행하기 위한 사용 권한이 필요할 수 있습니다. 예를 들어 응용 프로그램 서비스를 관리하기 위해 사용자는 서비스를 관리하기 위한 권한 및 특정 응용 프로그램 서비스에 대한 사용 권한이 있어야 합니다.

기본 관리자 그룹

Informatica 도메인에는 서비스에 대한 모든 권한 및 사용 권한이 포함된 시스템 정의 관리자 그룹이 있습니다. 관리자 그룹에 추가하는 사용자 계정에는 도메인의 모든 서비스 및 개체에 대한 권한 및 사용 권한이 있습니다. Informatica 서비스를 설치할 때 설치 프로그램이 관리자 그룹에 속하는 사용자 계정을 작성합니다. 처음으로 Administrator 도구에 로그인할 때 기본 관리자 계정을 사용할 수 있습니다.

도메인 구성 리포지토리

도메인 구성 리포지토리에는 도메인 구성, 사용자 권한 및 사용 권한에 대한 정보가 포함되어 있습니다.

Informatica 도메인이 원시 사용자 인증을 사용하는 경우 도메인 구성 리포지토리에는 사용자 자격 증명도 들어 있습니다. 도메인이 LDAP 또는 Kerberos 인증을 사용하는 경우 도메인 구성 리포지토리에는 사용자 자격 증명도 없습니다. 모든 LDAP 및 Kerberos 사용자 자격 증명은 Informatica 도메인을 벗어난 LDAP 디렉터리 서비스 또는 Kerberos 사용자 데이터베이스에 저장됩니다.

설치 중 Informatica 도메인을 작성할 때 설치 프로그램은 도메인 구성 리포지토리를 관계형 데이터베이스에 작성합니다. 도메인 구성 리포지토리를 작성할 데이터베이스를 지정해야 합니다. SSL 프로토콜로 보호되는 데이터베이스에 리포지토리를 작성할 수 있습니다.

보안 도메인

보안 도메인은 Informatica 도메인의 사용자 계정 및 그룹 컬렉션입니다.

Informatica 도메인은 다음 유형의 보안 도메인을 가질 수 있습니다.

원시 보안 도메인

원시 보안 도메인에는 Administrator 도구에서 작성되고 관리되는 사용자 및 그룹이 포함되어 있습니다. Informatica는 도메인 구성 리포지토리에 원시 보안 도메인의 사용자 계정에 대한 모든 자격 증명을 저장합니다. 기본적으로 설치 중에 원시 보안 도메인이 작성됩니다. 설치 후에는 추가 원시 보안 도메인을 작성하거나 원시 보안 도메인을 삭제할 수 없습니다.

Informatica 도메인이 Kerberos 인증을 사용하는 경우 도메인은 원시 보안 도메인을 사용하지 않습니다.

LDAP 보안 도메인

LDAP 보안 도메인에는 LDAP 디렉터리 서비스에서 가져온 사용자 및 그룹이 포함되어 있습니다. Informatica 도메인이 LDAP 또는 Kerberos 인증을 사용하는 경우 LDAP 보안 도메인을 작성하고 LDAP 디렉터리 서비스에서 가져오는 사용자 및 그룹을 추가할 수 있습니다.

Informatica 서비스를 설치하고 원시 또는 LDAP 인증을 사용하는 도메인을 작성하는 경우 설치 프로그램이 원시 보안 도메인은 작성하지만 LDAP 보안 도메인은 작성하지 않습니다. 설치 후 LDAP 보안 도메인을 작성할 수 있습니다.

Informatica 서비스를 설치하고 Kerberos 인증을 사용하는 도메인을 작성하는 경우 설치 프로그램이 다음 LDAP 보안 도메인을 작성합니다.

- 내부 보안 도메인. 설치 프로그램이 이름이 *_infalInternalNamespace*인 LDAP 보안 도메인을 작성합니다. *_infalInternalNamespace* 보안 도메인에는 설치 중 작성하는 기본 관리자 사용자 계정이 포함됩니다. 설치 후에는 사용자를 *_infalInternalNamespace* 보안 도메인에 추가하거나 보안 도메인을 삭제할 수 없습니다.
- 사용자 영역 보안 도메인. 설치 프로그램이 빈 LDAP 보안 도메인을 작성하고 설치 중 지정하는 Kerberos 사용자 영역과 동일한 이름을 이 도메인에 지정합니다. 설치 후 Kerberos 사용자 데이터베이스의 사용자를 사용자 영역 보안 도메인으로 가져올 수 있습니다. 사용자 영역 보안 도메인은 삭제할 수 없습니다.
Kerberos 인증을 사용하는 도메인에서 명령줄 프로그램을 실행하는 경우 보안 도메인 옵션 기본값은 설치 중 작성된 사용자 영역 보안 도메인입니다.

Informatica 도메인의 LDAP 인증 또는 Kerberos 인증 사용 여부와 관계 없이 동일한 방식으로 LDAP 보안 도메인을 작성하고 관리합니다.

제 2 장

사용자 인증

이 장에 포함된 항목:

- [사용자 인증 개요, 18](#)
- [원시 사용자 인증, 19](#)
- [LDAP 사용자 인증, 19](#)
- [Kerberos 인증, 20](#)
- [Informatica 웹 응용 프로그램에 대한 SAML 인증, 20](#)

사용자 인증 개요

Informatica 도메인에서 사용자 인증은 Informatica 서비스를 설치할 때 구성하는 인증 유형에 따라 다릅니다.

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

- 원시 사용자 인증
- LDAP 사용자 인증
- Kerberos 네트워크 인증
- SAML(Security Assertion Markup Language) 기반 single sign-on

원시 사용자 계정은 Informatica 도메인에 저장되며 해당 Informatica 도메인 내에서만 사용될 수 있습니다.

LDAP 및 Kerberos 및 사용자 계정은 LDAP 디렉터리 서비스에 저장되며 엔터프라이즈 내 응용 프로그램에 의해 공유됩니다.

SAML 기반 single sign-on은 Microsoft Active Directory에 저장된 계정 자격 증명과 대조하여 사용자를 인증합니다. 계정은 Active Directory에서 Informatica 도메인 내 보안 도메인으로 가져옵니다.

설치 중 Informatica 도메인에서 사용하기 위한 인증 유형을 선택할 수 있습니다. 설치 중에 Kerberos 인증을 활성화하는 경우, Kerberos KDC(키 배포 센터)와 함께 작동하도록 Informatica 도메인을 구성해야 합니다.

Informatica 도메인에 필요한 SPN(서비스 사용자 이름)을 Kerberos 사용자 데이터베이스에 생성해야 합니다. Kerberos 사용자 데이터베이스는 LDAP 디렉터리 서비스일 수 있습니다. 또한 SPN에 대해 키 탭 파일을 생성하고 이 파일을 Informatica 도메인에서 필요로 하는 디렉터리에 저장해야 합니다.

설치 중에 Kerberos 인증을 활성화하지 않으면 설치 프로그램이 Informatica 도메인에서 원시 인증을 사용하도록 구성합니다. 설치 후에 LDAP 서버에 대한 연결을 설정할 수 있고 원시 인증 외에 LDAP 인증을 사용하도록 Informatica 도메인을 구성할 수 있습니다.

Informatica 도메인에서는 원시 인증 및 LDAP 인증을 함께 사용할 수 있습니다. 서비스 관리자가 보안 도메인에 따라 사용자를 인증합니다. 사용자가 원시 보안 도메인에 속하는 경우 서비스 관리자는 도메인 구성 리포지토리

에서 사용자를 인증합니다. 사용자가 LDAP 보안 도메인에 속하는 경우 서비스 관리자는 인증을 위해 사용자 이름 및 암호를 LDAP 서버에 전달합니다.

원시 인증은 Kerberos 인증과 함께 사용할 수 없습니다. Informatica 도메인이 Kerberos 인증을 사용하는 경우 모든 사용자 계정이 LDAP 보안 도메인에 있어야 합니다. Kerberos 서버는 사용자가 네트워크에 로그인할 때 사용자 계정을 인증합니다. Informatica 클라이언트 응용 프로그램은 네트워크 로그인의 자격 증명을 사용하여 Informatica 도메인에서 사용자를 인증합니다. 원시 그룹 및 역할은 계속 지원됩니다.

SAML 기반 single sign-on은 Informatica 웹 응용 프로그램에 대해 설치 중에 또는 설치 후에 활성화할 수 있습니다. 하지만 모든 필수 설정 작업은 SAML 기반 single sign-on을 활성화하기 전에 완료되어야 합니다. Kerberos 인증을 사용하도록 구성된 Informatica 도메인에서는 SAML 기반 Single Sign-on을 활성화할 수 없습니다.

Informatica 도메인이 AWS EC2 인스턴스가 아닌 온-프레미스에 있는 경우 Amazon EMR과 통합하여 EMRFS 인증 프로토콜을 사용할 수 없습니다.

고유한 사이트 키를 사용하여 사용자 자격 증명 토큰을 암호화할 수 있습니다. 사용자 자격 증명 토큰을 암호화하려면 `infoEnableAdvancedEncryptionSchemeForCredential` 환경 변수를 `true`로 설정합니다. 기본 및 LDAP 사용자 인증의 경우 사용자 인증에 성공하면 사용자 암호 대신 암호화된 자격 증명 토큰이 사용됩니다.

원시 사용자 인증

Informatica 도메인이 원시 인증을 사용하는 경우 서비스 관리자는 모든 사용자 계정 정보를 저장하고 Informatica 도메인 내 모든 사용자 인증을 수행합니다. 사용자가 로그인하는 경우 서비스 관리자는 원시 보안 도메인을 사용하여 사용자 이름 및 암호를 인증합니다.

Kerberos 네트워크 인증을 사용하도록 Informatica 도메인을 구성하지 않으면 Informatica 도메인은 기본적으로 원시 보안 도메인을 포함합니다. 원시 보안 도메인은 설치할 때 작성되며 삭제할 수 없습니다. Informatica 도메인은 원시 보안 도메인을 하나만 가질 수 있습니다. Administrator 도구에서 원시 보안 도메인의 사용자 계정을 작성하고 유지 관리합니다. 서비스 관리자는 사용자 자격 증명 및 권한을 비롯한 사용자 계정에 대한 세부 정보를 도메인 구성 리포지토리에 저장합니다.

LDAP 사용자 인증

LDAP 디렉터리 서비스의 사용자가 Informatica 클라이언트 응용 프로그램에 로그인할 수 있도록 Informatica 도메인을 구성할 수 있습니다. 도메인에 대한 여러 LDAP 구성을 생성하여 각각 다른 LDAP 서버에 연결할 수 있습니다. 도메인에서 원시 사용자 인증 외에 LDAP 사용자 인증을 사용할 수 있습니다.

Informatica 도메인에서 LDAP 사용자 인증을 사용할 수 있도록 하려면 LDAP 서버에 대한 연결을 설정하고 Informatica 도메인에 액세스할 수 있는 LDAP 디렉터리 서비스의 사용자 및 그룹을 지정해야 합니다. Administrator 도구를 사용하여 LDAP 서버에 대한 연결을 설정할 수 있습니다.

LDAP 보안 도메인을 LDAP 디렉터리 서비스와 동기화하는 경우 서비스 관리자는 Informatica 도메인에 대한 액세스 권한이 있는 LDAP 사용자 계정 목록을 LDAP 보안 도메인으로 가져옵니다. 권한 및 사용 권한을 LDAP 보안 도메인의 사용자에게 할당하는 경우 서비스 관리자는 도메인 구성 리포지토리에 정보를 저장합니다. 서비스 관리자는 사용자 자격 증명을 도메인 구성 리포지토리에 저장하지 않습니다.

사용자가 로그인하는 경우 서비스 관리자는 인증을 위해 사용자 이름 및 암호를 LDAP 서버에 전달합니다.

참고: 서비스 관리자는 LDAP 디렉터리 서비스가 익명 로그인 모드에 대해 빈 암호를 허용할 수 있더라도 LDAP 사용자는 암호를 사용하여 클라이언트 응용 프로그램에 로그인해야 합니다.

Kerberos 인증

Kerberos 네트워크 인증을 사용하여 네트워크에서 사용자 및 서비스를 인증하도록 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.

Kerberos 교차 영역 인증을 사용하도록 Informatica 도메인을 구성할 수 있습니다. Kerberos 교차 영역 인증을 사용하면 한 Kerberos 영역에 속하는 Informatica 클라이언트에서 다른 Kerberos 영역에 속하는 노드 및 응용 프로그램 서비스에 인증할 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.

Informatica 웹 응용 프로그램에 대한 SAML 인증

사용자가 SAML(Security Assertion Markup Language) 인증을 사용하여 Administrator 도구, Analyst 도구, 대량 수집 도구, Metadata Manager 및 Monitoring 도구 웹 응용 프로그램에 로그인할 수 있도록 Informatica 도메인을 구성할 수 있습니다.

SAML은 서비스 공급자와 ID 공급자 간의 인증 및 권한 부여 정보 교환을 위한 XML 기반 데이터 형식입니다. Informatica 도메인에서는 Informatica 웹 응용 프로그램이 서비스 공급자입니다. Microsoft AD FS(Active Directory Federation Services)는 ID 공급자이며 조직의 Active Directory ID 저장소를 사용하여 웹 응용 프로그램 사용자를 인증합니다.

Informatica 도메인에서 SAML 기반 single sign-on을 사용할 수 있도록 하려면 Informatica 웹 응용 프로그램 사용자 계정에 대한 LDAP 보안 도메인을 생성한 다음 사용자를 Active Directory에서 도메인으로 가져와야 합니다. Administrator 도구를 사용하여 Active Directory 서버에 대한 연결을 설정한 다음 사용자를 보안 도메인으로 가져옵니다.

사용자가 Informatica 웹 응용 프로그램에 로그인 할 때 응용 프로그램이 SAML 인증 요청을 AD FS에 전송합니다. AD FS는 Active Directory에 있는 사용자 계정 정보와 대조하여 사용자의 자격 증명을 인증한 다음 사용자에게 대한 보안 관련 정보를 포함하는 SAML 어설션 토큰을 웹 응용 프로그램에 반환합니다.

Informatica 웹 응용 프로그램 사용자를 인증하는 데 사용되는 SAML 토큰을 발급하도록 AD FS를 구성합니다. 또한 AD FS에서 ID 공급자 어설션 서명 인증서를 내보낸 다음 인증서를 도메인의 각 게이트웨이 노드에 있는 Informatica 기본 트러스트 저장소 파일로 가져와야 합니다.

제 3 장

LDAP 인증

이 장에 포함된 항목:

- [개요, 21](#)
- [LDAP 보안 도메인, 21](#)
- [사용자 계정 동기화, 22](#)
- [LDAP 디렉터리 서비스, 22](#)
- [보안 LDAP 인증을 위한 Azure Active Directory, 23](#)
- [LDAP 구성 생성, 24](#)
- [LDAP 구성 삭제, 29](#)

개요

하나 이상의 LDAP 디렉터리 서비스에서 가져온 사용자가 Informatica 노드, 서비스 및 응용 프로그램 클라이언트(예: Informatica Developer 및 Informatica Analyst)에 로그인할 수 있도록 Informatica 도메인을 구성할 수 있습니다.

LDAP 디렉터리 서비스에는 계정 사용자 이름과 암호가 저장됩니다. LDAP 인증을 사용하면 모든 Informatica 사용자의 자격 증명을 단일 ID 저장소에 통합하여 계정 자격 증명을 생성하고 업데이트하는 작업을 간소화할 수 있습니다.

Informatica 도메인에서는 원시 인증과 LDAP 인증을 함께 사용할 수 있습니다. 도메인 내의 마스터 게이트웨이 노드에서 실행되는 서비스 관리자는 사용자가 속한 보안 도메인을 기반으로 사용자를 인증합니다. 사용자가 기본 원시 보안 도메인에 속하는 경우 서비스 관리자는 도메인 구성 리포지토리의 계정 정보를 바탕으로 사용자를 인증합니다. 사용자가 LDAP 보안 도메인에 속하는 경우 서비스 관리자는 인증을 위한 사용자 자격 증명을 LDAP 서버로 전달합니다.

LDAP 보안 도메인

LDAP 보안 도메인에는 LDAP 디렉터리 서비스에서 가져온 사용자 및 그룹이 포함되어 있습니다. Informatica 도메인 내에 여러 LDAP 보안 도메인을 정의할 수 있습니다. 그런 다음 LDAP 디렉터리 서비스의 계정을 보안 도메인으로 가져올 수 있습니다.

Informatica 도메인에서 Kerberos 인증을 사용하도록 구성한 경우 LDAP 보안 도메인을 생성해야 합니다. Informatica 서비스를 설치하고 Kerberos 인증을 활성화하면 Informatica 설치 프로그램이 설치 중에 지정된 Kerberos 영역의 이름으로 LDAP 보안 도메인을 생성합니다.

LDAP 보안 도메인을 생성할 때 보안 도메인에 포함할 LDAP 사용자 계정 및 그룹의 집합을 정의하는 검색 기준 및 필터링을 구성합니다. 서비스 관리자는 보안 도메인 구성을 사용하여 보안 도메인의 사용자 및 그룹을 가져오거나 LDAP 디렉터리 서비스의 사용자 및 그룹과 동기화합니다.

서비스 관리자는 LDAP 보안 도메인 내의 사용자 및 그룹을 가져오거나 동기화할 때 다음과 같은 조건을 사용합니다.

- 서비스 관리자는 사용자 검색 기준 및 필터를 사용하여 사용자 계정을 가져옵니다.
- 서비스 관리자는 그룹 검색 기준 및 필터를 사용하여 그룹을 가져옵니다.
- 서비스 관리자는 그룹 필터에 포함된 그룹과 사용자 필터에 포함된 사용자 계정을 가져옵니다.

사용자 계정 동기화

서비스 관리자는 예약된 일정에 따라 LDAP 디렉터리 서비스의 사용자 및 그룹으로 보안 도메인을 업데이트합니다. LDAP 인증을 구성할 때 동기화 일정을 설정할 수 있습니다.

서비스 관리자는 동기화 중에 다음 단계를 수행합니다.

- 보안 도메인에 대해 구성된 검색 기준 및 필터에 따라 LDAP 디렉터리 서비스에서 업데이트된 사용자 및 그룹 목록을 검색합니다.
- 보안 도메인의 LDAP 사용자 및 그룹 목록을 업데이트합니다. 보안 도메인의 LDAP 사용자가 LDAP 디렉터리 서비스에서 삭제된 경우 서비스 관리자는 사용자 개체의 소유권을 도메인 관리자 계정으로 이전합니다.

LDAP 디렉터리 서비스

LDAP 디렉터리 서비스의 사용자 계정을 Informatica 보안 도메인으로 가져올 수 있습니다.

다음과 같은 LDAP 디렉터리 서비스에서 사용자를 가져올 수 있습니다.

- IBM Tivoli Directory Server
- Microsoft Active Directory
- Microsoft Azure Active Directory
- Novell eDirectory
- OpenLDAP
- Oracle Directory Server(ODSEE)
- Oracle Unified Directory(ODU)
- Sun Java System Directory Server

참고: Kerberos 인증을 사용하는 경우 Microsoft Active Directory의 사용자만 가져올 수 있습니다.

서비스 관리자가 각 LDAP 디렉터리 서비스의 사용자를 식별하려면 특정 UID(고유 ID)가 필요합니다. 다음 테이블에는 각 LDAP 디렉터리 서비스의 기본 UID가 나열되어 있습니다.

LDAP 디렉터리 서비스	UID
IBM Tivoli Directory Server	uid
Microsoft Active Directory	sAMAccountName
Microsoft Azure Active Directory	UserPrincipalName
Novell eDirectory	uid
OpenLDAP	uid
Oracle Directory Server(ODSEE)	uid
Oracle Unified Directory(ODU)	uid
Sun Java System Directory Server	uid

보안 LDAP 인증을 위한 Azure Active Directory

Azure AD(Azure Active Directory)의 사용자를 LDAP 보안 도메인으로 가져올 수 있습니다.

Azure Active Directory Domain Services는 Azure Active Directory의 사용자 계정을 LDAP 보안 도메인으로 가져올 때 사용할 수 있는 보안 LDAP 공용 IP 주소를 제공합니다. 가져온 사용자는 자신의 LDAP 자격 증명을 사용하여 Azure Active Directory 관리 도메인의 가상 시스템에서 실행되는 Informatica 노드, 서비스 및 응용 프로그램을 로그인할 수 있습니다.

지원되는 Active Directory 버전에 대한 자세한 내용은 Informatica Network(<https://network.informatica.com/community/informatica-network/product-availability-matrices>)에서 Product Availability Matrix를 참조하십시오.

Informatica 사용자를 인증하려면 Azure Active Directory Domain Services에서 보안 LDAP(Secure Lightweight Directory Access Protocol) 인증을 활성화해야 합니다.

Informatica How To Library에서 다음 문서를 참조하면 Active Directory에서 LDAP 인증을 사용하는 프로세스를 완벽하게 파악할 수 있습니다.

- [Enabling SAML Authentication with Active Directory Federation Services in Informatica 10.4.0](#)
- [Enabling SAML Authentication with Azure Active Directory for Web Applications](#)

Active Directory 사용자 계정 가져오는 작업 준비

다음 단계를 완료하여 Azure Active Directory의 사용자 계정을 Informatica 도메인으로 가져오는 작업을 준비합니다.

1. 방화벽을 통해 Azure Active Directory 보안 LDAP 포트인 포트 636에 액세스할 수 있는지 확인합니다.
2. Azure Active Directory Domain Services에서 보안 LDAP 인증을 활성화합니다.

Azure 포털을 사용하여 Azure Active Directory Domain Services에서 보안 LDAP를 활성화할 수 있습니다. Azure Active Directory Domain Services의 보안 LDAP 구성에 대한 자세한 내용은 다음 링크를 참조하십시오.

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-admin-guide-configure-secure-ldap>

3. Azure Active Directory Domain Services에서 보안 LDAP 인증서를 구성할 때 인증서의 주체 이름이 Azure Active Directory의 FQDN(정규화된 도메인 이름)인지 확인합니다.
4. 보안 LDAP 인증서를 PFX 형식에서 PEM 형식으로 변환합니다. Java를 사용하려면 인증서가 PEM 형식이어야 합니다.
5. 모든 도메인에 사용되는 인증서를 Java cacerts 트러스트 저장소 파일로 가져옵니다. 이 파일은 도메인의 단일 게이트웨이 노드에 있는 다음 디렉터리에 있습니다.
<Informatica 설치 디렉터리>/java/jre/lib/security/
6. 가져온 인증서가 포함된 cacerts 파일을 도메인의 다른 모든 게이트웨이 노드에 있는 동일한 디렉터리로 복사합니다.
7. Azure Active Directory의 공용 IP 주소 및 Azure Active Directory의 FQDN(정규화된 도메인 이름)을 도메인에 포함된 각 게이트웨이 노드의 /etc/hosts 파일에 추가합니다. 다음 형식을 사용합니다.
<Azure Active Directory 호스트 IP 주소> ldaps.<Azure Active Directory의 FQDN>

LDAP 구성 생성

LDAP 디렉터리 서비스에서 가져온 사용자 계정 및 사용자 그룹이 Informatica 도메인에서 인증하는 데 필요한 하나 이상의 LDAP 구성을 생성할 수 있습니다.

LDAP 디렉터리 서비스에서 LDAP 사용자 및 그룹을 생성하고 관리합니다. LDAP 디렉터리 서버에 대한 연결을 설정하고 검색 필터를 사용하여 Informatica 도메인에 액세스할 수 있는 사용자 및 그룹을 지정합니다. 그런 다음 사용자 계정을 LDAP 보안 도메인으로 가져옵니다. LDAP 서버가 SSL 프로토콜을 사용하는 경우 SSL 인증서의 위치도 지정해야 합니다.

사용자를 LDAP 보안 도메인으로 가져온 다음 역할, 권한 및 사용 권한을 사용자에게 할당할 수 있습니다. LDAP 사용자 계정을 원시 그룹에 할당하여 Informatica 도메인의 역할에 따라 계정을 구성할 수 있습니다.

Administrator 도구를 사용하여 LDAP 보안 도메인에서 사용자 및 그룹을 생성, 편집 또는 삭제할 수 없습니다. LDAP 디렉터리 서비스에서 LDAP 사용자 및 그룹을 변경한 다음 LDAP 보안 도메인을 LDAP 디렉터리 서비스와 동기화해야 합니다.

LDAP 구성 대화 상자를 사용하여 LDAP 디렉터리 서비스에 대한 연결을 설정하고 사용자 계정을 가져올 LDAP 보안 도메인을 생성합니다. 또한 LDAP 구성 대화 상자를 사용하여 동기화 일정을 설정할 수 있습니다.

LDAP 구성을 생성하려면 다음 단계를 수행합니다.

1. 사용자 계정 및 그룹을 가져오려는 디렉터리 서비스가 포함된 LDAP 서버에 대한 연결을 구성합니다.
2. LDAP 디렉터리 서비스에서 가져오려는 각 사용자 계정 및 그룹 집합에 대한 LDAP 보안 도메인을 생성합니다.
3. 서비스 관리자가 LDAP 디렉터리 서비스의 신규 또는 변경된 사용자 및 그룹으로 LDAP 보안 도메인을 업데이트하는 일정을 설정합니다.

LDAP 구성을 생성하고 LDAP 서버 연결 구성

LDAP 구성을 생성하고 사용자 계정을 가져오려는 디렉터리 서비스가 포함된 LDAP 서버에 대한 연결을 구성합니다.

LDAP 서버에 대한 연결을 구성하는 경우 서비스 관리자가 사용자를 Informatica 도메인의 그룹에 할당할 때 LDAP 사용자 계정의 고유 이름 특성에서 대/소문자 구분을 무시해야 한다는 것을 나타냅니다. 서비스 관리자가 대/소문자 구분을 무시하지 않는 경우 서비스 관리자는 그룹에 속한 모든 사용자를 할당하지 않을 수도 있습니다.

LDAP 서버에서 SSL을 사용하는 경우 각 도메인 노드에 사용되는 인증서를 게이트웨이 노드 도메인의 cacerts 트러스트 저장소 파일로 가져와야 합니다. 그런 다음 가져온 인증서가 포함된 cacerts 파일을 도메인의 모든 노드에 있는 동일한 디렉터리로 복사합니다. 자세한 내용은 [“자체 서명된 SSL 인증서 사용” 페이지 28](#) 항목을 참조하십시오.

LDAP 디렉터리 서비스에 대한 연결을 설정하려면 다음 태스크를 수행합니다.

1. Administrator 도구에서 **보안** 탭을 클릭합니다.
2. **LDAP 구성** 탭을 클릭합니다.
3. **작업** 메뉴를 클릭하고 **LDAP 구성 생성**을 선택합니다.
4. **LDAP 구성 생성** 대화 상자에서 **LDAP 연결** 탭을 클릭합니다.
5. LDAP 서버에 대한 연결 속성을 구성합니다.

LDAP 서버 연결에 필요한 정보를 가져오려면 LDAP 관리자에게 문의해야 할 수 있습니다.

다음 테이블에는 LDAP 서버 구성 속성이 설명되어 있습니다.

속성	설명
LDAP 구성 이름	LDAP 구성의 이름입니다.
서버 이름	LDAP 디렉터리 서비스를 호스팅하는 시스템의 호스트 이름 또는 IP 주소입니다.
포트	LDAP 서버의 수신 포트입니다. 이것은 LDAP 디렉터리 서비스와 통신하기 위한 포트 번호입니다. 일반적으로 LDAP 서버 포트 번호는 389입니다. LDAP 서버가 SSL을 사용하는 경우 LDAP 서버 포트 번호는 636입니다. 최대 포트 번호는 65535입니다.
LDAP 디렉터리 서비스	LDAP 디렉터리 서비스의 유형입니다. 참고: Kerberos 인증을 사용하는 경우 Microsoft Active Directory Service를 선택해야 합니다.
이름	주 사용자의 DN(고유 이름)입니다. 사용자 이름은 종종 CN(일반적인 이름), O(조직) 및 C(국가)로 구성됩니다. 주 사용자 이름은 디렉터리에 대한 액세스 권한이 있는 관리 사용자입니다. LDAP 디렉터리 서비스에서 다른 사용자 항목을 읽기 위한 사용 권한이 있는 사용자를 지정합니다. Azure Active Directory에 연결하려면 주 사용자의 UPN(사용자 이름)을 지정합니다.
암호	주 사용자의 암호입니다. 익명 로그인인 경우 비워 둡니다.
SSL 인증서 사용	LDAP 서버가 SSL(보안 소켓 레이어) 프로토콜을 사용한다는 것을 나타냅니다.

속성	설명
LDAP 인증서 트러스트	서비스 관리자가 LDAP 서버의 SSL 인증서를 트러스트할 수 있는지 여부를 결정합니다. 선택하면 서비스 관리자는 SSL 인증서를 확인하지 않고 LDAP 서버에 연결합니다. 선택하지 않으면 서비스 관리자가 LDAP 서버에 연결하기 전에 SSL 인증서가 인증서 인증으로 서명되어 있는지 확인합니다.
대/소문자 구분 안 함	사용자를 그룹에 할당할 때 서비스 관리자가 고유 이름 특성의 대/소문자 구분을 무시해야 한다는 것을 나타냅니다.
그룹 멤버 자격 특성	사용자의 그룹 멤버 자격 정보가 포함된 특성의 이름입니다. 이것은 그룹의 멤버인 사용자 또는 그룹의 DN이 포함된 LDAP 그룹 개체의 특성입니다. 예를 들어 <i>member</i> 또는 <i>memberof</i> 입니다.
최대 크기	보안 도메인으로 가져올 사용자 계정의 최대 수입입니다. 예를 들어 값이 100으로 설정된 경우 최대 100개의 사용자 계정을 보안 도메인으로 가져올 수 있습니다. 가져올 사용자 수가 이 속성에 대한 값을 초과하는 경우 서비스 관리자는 오류 메시지를 생성하고 사용자를 가져오지 않습니다. 가져올 사용자가 많은 경우 이 속성을 더 높은 값으로 설정합니다. 기본값은 1000입니다.

- LDAP 서버에 대한 연결이 유효한지 확인하려면 **연결 테스트**를 클릭합니다.
- 확인**을 클릭하여 LDAP 구성을 저장합니다.

보안 도메인 구성

LDAP 디렉터리 서비스에서 가져오려는 각 사용자 계정 및 그룹 집합에 대한 LDAP 보안 도메인을 생성합니다. 검색 기준 및 필터를 설정하여 보안 도메인에 포함하려는 사용자 계정 및 그룹 집합을 정의합니다.

LDAP 디렉터리 서비스에서 가져오는 사용자 및 그룹 이름은 원시 사용자 및 그룹의 이름과 동일한 규칙을 준수해야 합니다. 이름이 원시 사용자 및 그룹 이름 규칙을 준수하지 않는 경우 서비스 관리자가 LDAP 사용자 또는 그룹을 가져오지 않습니다. 원시 사용자 이름과 달리 LDAP 사용자 이름은 대/소문자를 구분할 수 있습니다.

서비스 관리자는 사용자 검색 기준 및 필터를 사용하여 사용자 계정을 가져오고 그룹 검색 기준 및 필터를 사용하여 그룹을 가져옵니다. 서비스 관리자는 필터를 사용하여 그룹과 각 그룹에 속하는 사용자 목록을 가져옵니다.

LDAP 연결 속성을 수정하여 다른 LDAP 서버에 연결하는 경우 서비스 관리자는 기존 보안 도메인을 삭제하지 않으므로 LDAP 보안 도메인이 새 LDAP 서버에 대해 올바른지 확인해야 합니다. 서비스 관리자가 Informatica 도메인에서 사용하려는 사용자 및 그룹을 제대로 가져올 수 있도록 보안 도메인의 사용자 및 그룹 필터를 수정하거나 추가 보안 도메인을 생성합니다.

LDAP 보안 도메인을 구성하려면 다음 단계를 수행합니다.

- Administrator 도구에서 **보안** 탭을 클릭합니다.
- 작업** 메뉴를 클릭하고 **LDAP 구성**을 선택합니다.
- LDAP 구성** 대화 상자에서 **보안 도메인** 탭을 클릭합니다.
- 추가**를 클릭합니다.

다음 테이블에는 보안 도메인에 대해 설정할 수 있는 필터 속성이 설명되어 있습니다.

속성	설명
보안 도메인	LDAP 보안 도메인의 이름입니다. 이름은 대/소문자를 구분하지 않으며 도메인 내에서 고유해야 합니다. 문자열은 128자를 초과하거나 다음 특수 문자를 포함할 수 없습니다. , + / < > @ ; \ % ? 첫 번째 문자와 마지막 문자를 제외하고 이름에 ASCII 공백 문자를 포함할 수 있습니다. 다른 모든 공백 문자는 사용할 수 없습니다.
사용자 검색 기준	LDAP 디렉터리 서비스에서 사용자 이름을 검색하는 시작점 역할을 하는 항목의 DN(고유 이름)입니다. 검색하면 개체의 고유 이름의 경로에 따라 디렉터리에서 개체를 찾습니다. 예를 들어 Microsoft Active Directory에서 사용자 개체의 고유 이름이 cn=UserName,ou=OrganizationalUnit,dc=DomainName일 수 있으며 여기서 dc=DomainName으로 표시되는 일련의 상대 고유 이름이 개체의 DNS 도메인을 식별합니다.
사용자 필터	디렉터리 서비스에서 사용자를 검색하는 조건을 지정하는 LDAP 쿼리 문자열입니다. 필터에서 특성 유형, 어설션 값 및 일치 조건을 지정할 수 있습니다. 예: (objectclass=*) - 모든 개체를 검색합니다. (&(objectClass=user)(!(cn=susan))) - "susan" 이외의 모든 사용자 개체를 검색합니다. 검색 필터에 대한 자세한 내용은 LDAP 디렉터리 서비스에 대한 설명서를 참조하십시오.
그룹 검색 기준	LDAP 디렉터리 서비스에서 그룹 이름을 검색하는 시작점 역할을 하는 항목의 DN(고유 이름)입니다.
그룹 필터	디렉터리 서비스에서 그룹을 검색하는 조건을 지정하는 LDAP 쿼리 문자열입니다.

5. **미리 보기**를 클릭하여 필터 매개 변수에 속한 사용자 및 그룹 목록의 하위 집합을 봅니다.
미리 보기가 올바른 사용자 및 그룹 집합을 표시하지 않는 경우 사용자 및 그룹 필터와 검색 기준을 수정하여 올바른 사용자 및 그룹을 가져옵니다.
6. 보안 도메인의 사용자 및 그룹을 LDAP 디렉터리 서비스의 사용자 및 그룹과 즉시 동기화하려면 **지금 동기화**를 클릭합니다.
서비스 관리자가 모든 LDAP 보안 도메인의 사용자와 LDAP 디렉터리 서비스의 사용자를 동기화합니다. 동기화 프로세스를 완료하는 데 걸리는 시간은 가져오는 사용자 및 그룹 수에 따라 다릅니다.
7. **확인**을 클릭하여 보안 도메인을 저장합니다.

동기화 일정 구성

서비스 관리자가 LDAP 디렉터리 서비스의 신규 또는 변경된 사용자 및 그룹으로 LDAP 보안 도메인을 업데이트하는 일별 일정을 설정할 수 있습니다.

서비스 관리자는 LDAP 보안 도메인을 LDAP 디렉터리 서비스와 동기화할 때 LDAP 디렉터리 서비스의 사용자 필터 설정과 일치하는 모든 사용자를 보안 도메인으로 가져옵니다. 그런 다음 서비스 관리자는 그룹 필터 설정과 일치하는 모든 그룹을 가져오고 사용자를 해당하는 그룹에 연결합니다. 또한 서비스 관리자는 LDAP 디렉터리 서비스에 없는 사용자 또는 그룹을 보안 도메인에서 삭제합니다.

기본적으로 서비스 관리자가 LDAP 디렉터리 서비스와 동기화하는 시간은 예약되지 않습니다. LDAP 보안 도메인의 사용자 및 그룹 목록을 정확하게 유지하려면 서비스 관리자가 LDAP 보안 도메인을 LDAP 디렉터리 서비스와 동기화하는 시간을 예약하십시오. 서비스 관리자는 매일 설정한 시간에 LDAP 보안 도메인을 LDAP 디렉터리 서비스와 동기화합니다.

동기화에 성공하려면 동기화 일정을 설정하기 전에 다음 권장 사항을 고려하십시오.

/etc/hosts 파일에 LDAP 서버에 대한 항목이 있어야 합니다.

도메인에 있는 각 노드 게이트웨이의 /etc/hosts 파일에 LDAP 서버의 호스트 이름과 IP 주소가 포함된 항목이 있어야 합니다. 서비스 관리자가 LDAP 서버의 호스트 이름을 확인할 수 없는 경우 동기화가 실패할 수 있습니다.

동기화하는 사용자 또는 그룹 수가 100개를 초과하는 경우 LDAP에서 페이징을 활성화합니다.

100개를 초과하는 사용자 또는 그룹을 동기화하기 전에 LDAP 디렉터리 서비스에서 페이징을 활성화합니다. LDAP 디렉터리 서비스에서 페이징을 활성화하지 않으면 동기화가 실패할 수 있습니다.

대부분의 사용자가 Informatica 응용 프로그램에 로그인하지 않는 시간에 보안 도메인을 동기화합니다.

동기화 중에 서비스 관리자는 동기화하는 각 사용자 계정을 잠급니다. 동기화 중에 사용자는 Informatica 응용 프로그램 클라이언트에 로그인하지 못할 수 있습니다. 동기화가 시작될 때 응용 프로그램 클라이언트에 로그인한 사용자는 특정 태스크를 수행하지 못할 수 있습니다.

LDAP 보안 도메인과 LDAP 디렉터리 서비스의 동기화 일정을 설정하려면 다음 단계를 수행합니다.

1. Administrator 도구에서 **보안** 탭을 클릭합니다.
2. **작업** 메뉴를 클릭하고 **LDAP 구성**을 선택합니다.
3. **LDAP 구성** 대화 상자에서 **일정** 탭을 클릭합니다.
4. **추가** 단추(+)를 클릭하여 시간을 추가합니다.
동기화 일정은 24시간 형식을 사용합니다.
5. LDAP 보안 도메인의 사용자 및 그룹을 LDAP 디렉터리 서비스의 사용자 및 그룹과 즉시 동기화하려면 **지금 동기화**를 클릭합니다.
6. **확인**을 클릭하여 동기화 일정을 저장합니다.

참고: 서비스 관리자가 LDAP 디렉터리 서비스를 동기화할 때까지 기다린 후 Informatica 도메인을 다시 시작해야 일정에 설정된 동기화 시간이 손실되지 않습니다.

LDAP 디렉터리 서비스에서 중첩 그룹 사용

LDAP 보안 도메인은 중첩된 LDAP 그룹을 포함할 수 있습니다. 서비스 관리자는 다음과 같은 방식으로 작성된 중첩 그룹을 가져올 수 있습니다.

- 동일한 조직 단위(OU)에서 그룹 작성
- 그룹 간의 관계 설정

예를 들어 GroupB가 GroupA의 멤버이고 GroupD가 GroupC의 멤버인 중첩 그룹을 작성할 수 있습니다.

1. 동일한 OU에 GroupA, GroupB, GroupC 및 GroupD를 작성합니다.
2. GroupA를 편집하고 GroupB를 멤버로 추가합니다.
3. GroupC를 편집하고 GroupD를 멤버로 추가합니다.

중첩된 LDAP 그룹을 다른 방식으로 작성된 LDAP 보안 도메인으로 가져올 수 없습니다.

자체 서명된 SSL 인증서 사용

CA(인증 기관)에 의해 서명된 SSL 인증서를 사용하는 LDAP 서버에 연결할 수 있습니다. 기본적으로 서비스 관리자는 자체 서명된 인증서를 사용하는 LDAP 서버에 연결되지 않습니다.

SSL 인증서를 사용하는 LDAP 서버에 연결하려면 Java keytool 키 및 인증서 관리 유틸리티를 사용하여 모든 도메인 노드에 사용되는 인증서를 도메인의 각 게이트웨이 노드에 있는 Java cacerts 트러스트 저장소 파일로 가져

와야 합니다. 그런 다음 가져온 인증서가 포함된 **cacerts** 키 저장소 파일을 도메인의 다른 모든 노드로 복사합니다.

cacerts 트러스트 저장소 파일은 각 노드의 다음 디렉터리에 있습니다.

<Informatica 설치 디렉터리>\java\jre\lib\security

keytool 유틸리티는 각 노드의 다음 디렉터리에서 사용할 수 있습니다.

<Informatica 설치 디렉터리>\java\bin

인증서를 가져온 후 노드를 다시 시작합니다.

LDAP 구성 삭제

LDAP 구성 및 연결된 보안 도메인을 삭제하여 사용자의 도메인 액세스를 영구적으로 금지할 수 있습니다.

LDAP 구성을 삭제할 때는 LDAP 구성에 연결된 보안 도메인을 먼저 삭제해야 합니다. 서비스 관리자는 삭제된 각 LDAP 보안 도메인의 모든 사용자 계정 및 그룹을 도메인 구성 데이터베이스에서 삭제합니다.

1. Administrator 도구에서 **보안** 탭을 클릭합니다.
2. **LDAP 구성** 탭을 클릭합니다.
3. **보안 도메인** 탭을 클릭하고 **편집** 단추를 클릭합니다.
4. **LDAP 구성 편집** 대화 상자에서 보안 도메인을 선택하고 **삭제**를 클릭합니다.
5. LDAP 구성 탐색기에서 삭제할 LDAP 구성을 선택합니다.
6. **작업** 메뉴를 클릭하고 **LDAP 구성 삭제**를 선택합니다.
7. **확인**을 클릭하여 LDAP 구성 삭제를 확인합니다.

제 4 장

Kerberos 인증

이 장에 포함된 항목:

- [Kerberos 개요, 30](#)
- [Informatica 도메인에서 Kerberos가 작동하는 방식, 31](#)
- [Kerberos 교차 영역 인증, 33](#)
- [Kerberos 인증 활성화 준비, 34](#)
- [Kerberos 인증 활성화, 47](#)
- [Informatica 노드에서 Kerberos 활성화, 51](#)
- [Hadoop 통합을 위해 Kerberos 활성화, 54](#)
- [Kerberos 인증을 사용하도록 사용자 계정 설정, 54](#)
- [Kerberos 위임, 58](#)

Kerberos 개요

Kerberos는 Informatica 클라이언트, 노드 및 서비스가 네트워크 통신을 통해 안전하게 서로 연결할 수 있도록 하는 컴퓨터 네트워크 인증 프로토콜입니다.

Kerberos 인증에는 Informatica 원시 계정이 사용되지 않으므로 도메인에서 LDAP 서버에 사용자 자격 증명을 전달할 필요가 없습니다. 도메인에서 Kerberos 인증을 활성화하면 Informatica 클라이언트가 Windows 인증 프로세스 중에 생성된 Kerberos 티켓을 사용하여 도메인에서 실행되는 Informatica 서비스에 로그인합니다.

Windows 네트워크에서 실행되는 도메인에서 Kerberos 인증을 활성화할 수 있습니다. 네트워크는 Microsoft AD DS(Active Directory Domain Services)를 Kerberos 사용자 데이터베이스로 사용해야 합니다.

Informatica 도메인에서 Kerberos 인증을 활성화하려면 다음 단계를 수행합니다.

Kerberos 인증 활성화를 준비합니다.

Kerberos 인증을 활성화하기 전에 여러 작업을 완료해야 합니다. 완료해야 하는 작업에는 다음이 포함됩니다.

- Kerberos 구성 파일을 생성합니다.
- Active Directory에서 Kerberos 사용자에게 대한 계정을 생성합니다.
- SPN(서비스 사용자 이름) 및 keytab 형식을 생성합니다.
- 네트워크의 사용자 및 서비스를 인증할 때 사용되는 keytab 파일을 생성합니다.

Informatica 도메인에서 Kerberos 인증을 활성화합니다.

Informatica 서비스를 설치할 때 Informatica 도메인에서 Kerberos 인증을 활성화하거나 서비스를 설치한 후 Kerberos 인증을 활성화할 수 있습니다. 설치 중 Kerberos 인증을 활성화하지 않은 경우 Informatica 명령줄 프로그램을 사용하여 Kerberos 인증을 사용하도록 도메인을 구성할 수 있습니다.

Informatica 노드 및 클라이언트 호스트에서 Kerberos 인증을 활성화합니다.

도메인에서 Kerberos를 활성화한 후 도메인의 각 노드와 각 Informatica 클라이언트 호스트에 Kerberos 구성 파일을 복사합니다. 또한 Informatica 웹 응용 프로그램에 액세스하도록 웹 브라우저를 구성합니다.

Kerberos 인증을 사용하도록 Informatica 사용자를 설정합니다.

Kerberos 인증을 활성화한 후 Active Directory의 Informatica 사용자를 Kerberos 사용자 계정이 포함되는 LDAP 보안 도메인으로 가져옵니다. 또한 원시 사용자 계정의 그룹, 역할, 권한 및 사용 권한을 LDAP 보안 도메인의 사용자 계정으로 마이그레이션해야 합니다.

Informatica 도메인에서 Kerberos가 작동하는 방식

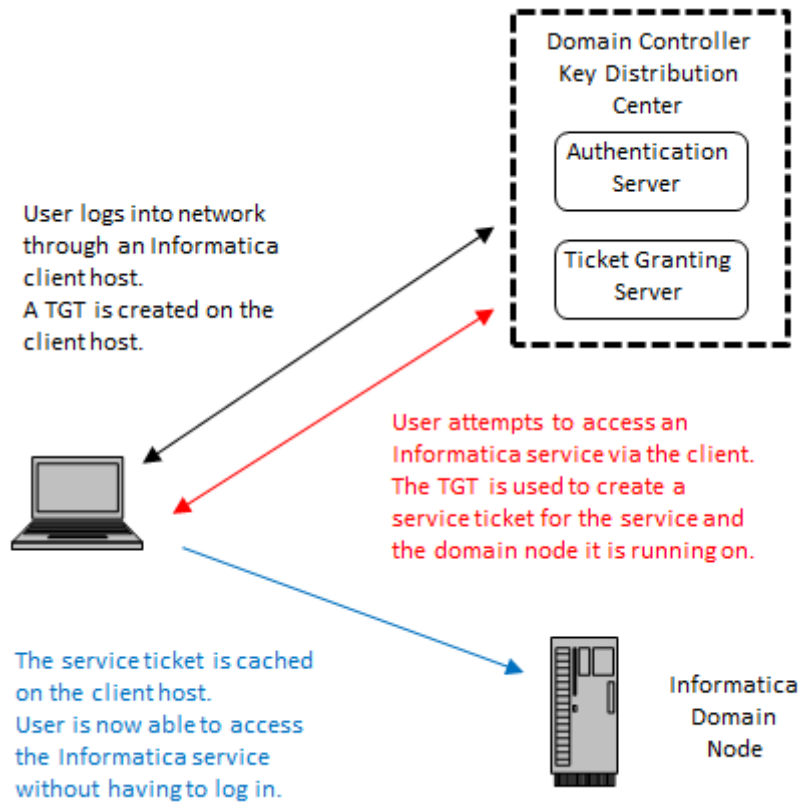
Kerberos 인증을 사용하도록 구성된 도메인에서 Informatica 클라이언트는 도메인 내의 Informatica 노드 및 응용 프로그램 서비스에 암호를 입력할 필요 없이 인증됩니다.

Kerberos 인증을 사용하는 도메인에서 노드 프로세스, 웹 응용 프로그램 프로세스 및 Informatica 응용 프로그램 서비스 등 도메인 내에서 실행되는 서비스는 Kerberos 사용자인니다. Kerberos 영역에 사용되는 Active Directory 사용자 데이터베이스에는 각 사용자의 사용자 계정이 포함됩니다.

Kerberos 인증 프로토콜은 *keytab*을 사용하여 도메인 내에서 실행되는 서비스에 연결하는 Informatica 클라이언트를 인증합니다. 사용자에 대한 *keytab*은 서비스가 실행되는 노드에 저장됩니다. *keytab*에는 Kerberos 영역 내의 서비스를 식별하는 *SPN(서비스 사용자 이름)*과 Active Directory의 *SPN*에 할당된 키가 포함됩니다.

KDC가 클라이언트에 서비스 티켓을 제공하면 클라이언트가 *SPN*에 할당된 키를 사용하여 티켓을 암호화합니다. 요청된 서비스는 이 키를 사용하여 서비스 티켓을 암호 해독합니다.

다음 이미지는 기본적인 Kerberos 인증 흐름을 보여줍니다.



다음 아웃라인은 기본적인 Kerberos 인증 흐름을 보여줍니다.

1. Informatica 클라이언트 사용자가 Informatica 클라이언트를 호스팅하는 네트워크 컴퓨터에 로그인합니다.
2. 로그인 요청이 KDC(키 배포 센터)의 구성 요소인 인증 서버로 연결됩니다. KDC는 Active Directory 도메인 내의 각 도메인 컨트롤러에서 실행되는 사용자 계정 정보에 액세스할 수 있는 네트워크 서비스입니다.
3. 인증 서버는 사용자 데이터베이스에 해당 사용자가 있는지 확인한 후 사용자 컴퓨터에 TGT(티켓 부여 티켓)라고 하는 Kerberos 토큰을 생성합니다.
4. 사용자가 Informatica 클라이언트를 통해 Informatica 도메인 내의 프로세스 또는 서비스에 액세스를 시도합니다.
5. Informatica 및 Kerberos 라이브러리는 TGT를 사용하여 KDC에서도 실행되는 티켓 부여 서버에서 요청된 서비스에 대한 서비스 티켓 및 세션 키를 요청합니다.

예를 들어 사용자가 Informatica Developer 클라이언트에서 모델 리포지토리 서비스에 액세스하면 TGT가 요청된 서비스가 실행되는 노드에 대한 서비스 티켓을 요청합니다. 또한 TGT는 모델 리포지토리 서비스에 대한 서비스 티켓도 요청합니다.

6. Kerberos는 이 서비스 티켓을 사용하여 요청된 서비스가 포함된 클라이언트를 인증합니다. Informatica 클라이언트를 호스팅하는 컴퓨터에 서비스 티켓이 캐싱되고 클라이언트가 유효한 상태의 티켓을 사용할 수 있게 됩니다. 사용자가 Informatica 클라이언트를 종료한 후 다시 시작하면 클라이언트는 동일한 티켓을 재사용하여 Informatica 도메인 내의 프로세스 및 서비스에 액세스합니다.

Kerberos 교차 영역 인증

Kerberos 교차 영역 인증을 사용하도록 Informatica 도메인을 구성할 수 있습니다. Kerberos 교차 영역 인증을 사용하면 한 Kerberos 영역에 속하는 Informatica 클라이언트에서 다른 Kerberos 영역에 속하는 노드 및 응용 프로그램 서비스에 인증할 수 있습니다.

Kerberos 교차 영역 인증을 사용하도록 도메인을 구성할 때 각 Kerberos 영역에 대한 속성을 Kerberos 구성 파일에 추가합니다. 또한 `infasetup` 명령을 실행하여 도메인 및 도메인 노드에서 Kerberos 인증을 활성화할 때 각 영역의 이름을 포함합니다.

도메인이 Kerberos 교차 영역 인증에 사용하는 Active Directory 서버는 동일한 Active Directory 포리스트에 속해야 합니다. Active Directory 포리스트는 공통의 글로벌 카탈로그, 디렉터리 스키마, 논리적 구조 및 디렉터리 구성을 공유하는 Active Directory 도메인의 그룹입니다. 글로벌 카탈로그에 연결하여 Active Directory 서버의 사용자를 LDAP 보안 도메인으로 가져올 수 있습니다.

Kerberos 도메인 간 인증을 사용하려면 포리스트의 Active Directory 서버 간에 양방향 트러스트를 활성화해야 합니다.

Kerberos 단일 영역 인증의 도메인을 Kerberos 교차 영역 인증으로 변환

사용자 인증에 단일 Kerberos 영역을 사용하는 Informatica 도메인을 변환하여 Kerberos 교차 영역 인증을 사용하게 할 수 있습니다.

Kerberos 교차 영역 인증을 사용하도록 도메인을 변환하기 전에 도메인을 버전 10.2 HotFix 2로 업그레이드해야 합니다.

또한 Active Directory 글로벌 카탈로그의 사용자 및 그룹 계정을 LDAP 보안 도메인으로 가져와야 합니다. 계정을 가져오는 경우 `samAccount` 이름 특성을 사용하는 LDAP 보안 도메인의 기존 계정이 삭제되고 사용자 이름 특성을 사용하는 새로운 계정으로 대체됩니다.

사용자는 다음과 같은 형식의 정규화된 사용자 이름을 사용하여 Informatica 클라이언트에 로그인합니다.

<사용자 이름>@<Kerberos 영역 이름>

사용자 및 그룹 계정을 가져온 후 권한, 역할 및 사용 권한을 계정에 할당합니다.

1. 도메인을 버전 10.2 HotFix 2로 업그레이드합니다.

2. 각 Kerberos 영역의 필요한 속성을 Kerberos 구성 파일에 추가합니다.

도메인의 각 노드에서 `krb5.conf` 구성 파일의 각 영역에 대한 속성을 설정합니다. 도메인의 모든 노드에서 파일을 업데이트한 후 도메인을 다시 시작합니다.

Kerberos 교차 영역 인증의 `krb5.conf` 구성 파일 구성에 대한 자세한 내용은 [“Kerberos 구성 파일 구성” 페이지 35](#)에서 확인하십시오.

3. 업데이트된 `krb5.conf` 파일을 Informatica 클라이언트를 호스팅하는 각 컴퓨터의 다음 디렉터리에 복사합니다.

<Informatica 설치 디렉터리>\clients\shared\security

4. 도메인 노드에서 `infasetup UpdateGatewayNode` 및 `infasetup UpdateWorkerNode` 명령을 실행합니다.

도메인이 사용자 인증에 사용하는 각 Kerberos 영역의 이름을 쉼표로 구분하여 `-srn` 및 `-urn` 옵션의 값으로 지정합니다.

`infasetup` 명령 실행에 대한 자세한 내용은 *Informatica 10.2 HotFix 2 명령 참조*에서 "infasetup 명령 참조" 장을 참조하십시오.

5. 도메인 내의 게이트웨이 노드에서 `UpdateKerberosConfig` 명령을 실행합니다.

도메인이 사용자 인증에 사용하는 각 Kerberos 영역의 이름을 쉼표로 구분하여 `-srn` 및 `-urn` 옵션의 값으로 지정합니다.

6. 도메인 내의 게이트웨이 노드에서 `UpdateKerberosAdminUser` 명령을 실행합니다.

도메인 관리자의 사용자 계정에 대한 정규화된 사용자 이름을 지정합니다.

7. 사용자 및 그룹 계정을 LDAP 보안 도메인으로 가져옵니다.

Active Directory 글로벌 카탈로그에 연결합니다. 글로벌 카탈로그에 연결할 때 각 Kerberos 영역에 사용되는 Active Directory 서버에서 사용자를 가져옵니다.

글로벌 카탈로그 연결 및 계정 가져오기에 대한 자세한 내용은 [“Active Directory의 사용자 계정을 LDAP 보안 도메인으로 가져오기” 페이지 54](#)에서 확인하십시오.

8. LDAP 보안 도메인으로 가져온 사용자 및 그룹 계정에 권한, 역할 및 사용 권한을 할당합니다.

권한 및 역할 할당에 대한 자세한 내용은 [장 9, “권한 및 역할” 페이지 131](#)에서 확인하십시오.

사용 권한 할당에 대한 자세한 내용은 [장 10, “사용 권한” 페이지 172](#)에서 확인하십시오.

Kerberos 인증 활성화 준비

여러 태스크를 완료하여 Informatica 도메인에서 Kerberos 인증을 활성화할 준비를 해야 합니다. 각 태스크에서 수행하는 절차는 Kerberos를 활성화하는 서비스 사용자 수준에 따라 다릅니다.

참고: 도메인에서 Kerberos 인증을 활성화한 후에는 Kerberos 인증을 비활성화할 수 없습니다. 또한 서비스 사용자 수준을 노드 수준과 프로세스 수준 간에 전환할 수 없습니다.

Kerberos 서비스 사용자 수준 결정

Kerberos 인증 활성화를 준비할 때 필요한 서비스 사용자 수준을 결정해야 합니다. 필요한 서비스 사용자 수준에 따라 도메인의 Kerberos 인증 활성화를 준비할 때 수행하는 절차가 결정됩니다.

다음 수준 중 하나에서 Kerberos 인증을 활성화할 수 있습니다.

노드 수준

도메인이 테스트 또는 개발용으로 사용되고 도메인에 높은 수준의 보안이 요구되지 않는 경우 노드 수준에서 Kerberos를 활성화할 수 있습니다. 단일의 서비스 사용자 이름과 단일의 `keytab` 파일을 노드와 노드에서 실행되는 모든 프로세스 및 서비스에 사용할 수 있습니다. 또한 노드에서 실행되는 HTTP 프로세스에 대한 SPN 및 `keytab` 파일도 생성해야 합니다.

프로세스 수준

도메인이 프로덕션용으로 사용되고 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 생성합니다. 또한 노드에서 실행되는 HTTP 프로세스에 대한 SPN 및 `keytab` 파일도 생성해야 합니다.

Kerberos를 프로세스 수준에서 활성화하면 최고 수준의 보안이 제공되지만 다수의 노드 또는 서비스를 포함하는 Informatica 도메인에서는 관리가 어려울 수 있습니다. 이 시나리오에서는 Kerberos를 노드 수준에서 활성화하는 것이 좋을 수 있습니다.

Kerberos 구성 파일 구성

Kerberos 구성 파일에서 Informatica에 필요한 속성을 설정한 후 Informatica 도메인의 각 노드에 파일을 복사합니다.

Kerberos는 구성 정보를 *krb5.conf*. *krb5.conf* 구성 파일에서 속성을 설정한 다음 Informatica 도메인의 모든 노드에 파일을 복사해야 합니다.

도메인에서 Kerberos 교차 영역 인증을 사용하는 경우 각 Kerberos 영역에 대해 필요한 속성을 입력합니다.

1. 파일의 *libdefaults* 섹션에서 다음과 같은 Kerberos 라이브러리 속성을 구성합니다.

다음 테이블에는 입력할 속성이 설명되어 있습니다.

속성	설명
default_realm	Informatica 도메인 서비스가 속하는 Kerberos 영역의 이름입니다. 해당 영역 이름은 대문자여야 합니다. 도메인에서 단일 Kerberos 영역을 인증에 사용하는 경우 서비스 영역 이름과 사용자 영역 이름이 동일해야 합니다.
forwardable	서비스에서 클라이언트 사용자 자격 증명을 다른 서비스에 위임할 수 있습니다. Informatica 도메인에서 응용 프로그램 서비스는 다른 서비스를 통해 클라이언트 사용자 자격 증명을 인증해야 합니다. true로 설정합니다.
default_tkt_enctypes	TGT(티켓 부여 티켓)에 포함되는 세션 키의 암호화 유형입니다. 이 속성은 세션 키에 특정 암호화 유형이 사용되어야 하는 경우에만 설정합니다. Kerberos KDC(키 배포 센터)가 지정한 암호화 유형을 지원하는지 확인하십시오. Kerberos 프로토콜이 사용할 암호화 유형을 선택할 수 있도록 하려면 이 속성을 설정하지 마십시오. 노드 호스트 또는 Informatica 클라이언트 호스트에서 256비트 암호화를 사용하는 경우 JCE(Java Cryptography Extension) 무한 강도 정책 파일을 모든 노드 호스트 및 Informatica 클라이언트 호스트에 설치하여 인증 문제를 방지하십시오.
rdns	서비스 사용자 이름에 사용할 호스트 이름을 정규화할 때 정방향 이름 조회와 함께 역방향 이름 조회를 사용할지 여부를 결정합니다. false로 설정합니다.
renew_lifetime	초기 티켓 요청의 기본 갱신 가능한 수명입니다.
ticket_lifetime	초기 티켓 요청의 기본 수명입니다.
udp_preference_limit	Kerberos에서 KDC에 메시지를 전송할 때 사용할 프로토콜을 결정합니다. 도메인에서 간헐적인 Kerberos 인증 실패가 발생하는 경우 TCP 프로토콜을 사용하면 1로 설정합니다.

속성	설명
dns_lookup_kdc	해당 영역 관련 정보에 나열되지 않은 경우, Kerberos 클라이언트가 DNS SRV 레코드를 사용하여 영역에 대한 KDC 및 기타 서버를 찾을지 나타냅니다. DNS는 SRV 레코드를 사용하여 특정 서비스를 호스팅하는 컴퓨터를 식별합니다. 도메인에 Kerberos가 활성화된 경우 필요합니다. admin_server 영역 속성을 설정해야 합니다. true로 설정합니다.
dns_lookup_realm	Kerberos 클라이언트가 DNS TXT 레코드를 사용하여 호스트의 Kerberos 영역을 결정할지 나타냅니다. DNS는 텍스트 또는 TXT 레코드를 사용하여 임의 텍스트를 호스트 또는 기타 이름에 연결합니다(예: 서버, 네트워크, 데이터 센터에 대한 사람이 읽을 수 있는 정보 또는 기타 회계 정보). 도메인에 Kerberos가 활성화된 경우 필요합니다. true로 설정합니다.

2. 각 Kerberos 영역을 파일의 *realms* 섹션에서 정의합니다.

다음 예는 COMPANY.COM이라는 Kerberos 영역에 대한 항목을 보여 줍니다.

```
[realms]
COMPANY.COM = {...}
```

3. 파일의 *realms* 섹션에서 각 Kerberos 영역에 대한 괄호 안에 다음과 같은 영역 속성을 입력합니다.

다음 테이블에는 입력할 속성이 설명되어 있습니다.

속성	설명
admin_server	Kerberos 관리 서버 호스트의 이름 또는 IP 주소입니다. 필요한 경우 포트 번호를 콜론으로 호스트 이름과 구분하여 포함할 수 있습니다. 기본값은 749입니다. <i>libdefaults</i> 섹션에서 dns_lookup_kdc를 구성하는 경우 필요합니다.
kdc	영역에 대한 KDC(키 배포 센터)를 실행하는 호스트의 이름 또는 IP 주소입니다. 필요한 경우 포트 번호를 콜론으로 호스트 이름과 구분하여 포함할 수 있습니다. 기본값은 88입니다.

다음 예는 Kerberos 교차 영역 구성의 각 Kerberos 영역에 대한 항목을 보여 줍니다.

```
[realms]
COMPANY.COM = {
  admin_server = KDC01.COMPANY.COM:749
  kdc = KDC01.COMPANY.COM:88
}
EAST.COMPANY.COM = {
  kdc = 10.75.141.193
  admin_server = 10.75.141.193
}
WEST.COMPANY.COM = {
  kdc = 10.78.140.111
  admin_server = 10.78.140.111
}
```

4. *domain_realms* 섹션에서 도메인 이름 또는 호스트 이름을 Kerberos 영역 이름에 매핑합니다. 도메인 이름에는 마침표(.)가 접두사로 추가됩니다.

다음 예는 Informatica 도메인에서 Kerberos 인증을 사용하지 않는 경우 Hadoop domain_realm에 대한 매개 변수를 보여 줍니다.

```
[domain_realm]
.hadoop_realm.com = HADOOP-REALM
hadoop_realm.com = HADOOP-REALM
```

다음 예는 Informatica 도메인에서 Kerberos 인증을 사용하는 경우 Hadoop domain_realm에 대한 매개 변수를 보여 줍니다.

```
[domain_realm]
.infa_ad_realm.com = INFA-AD-REALM
infa_ad_realm.com = INFA-AD-REALM
.hadoop_realm.com = HADOOP-REALM
hadoop_realm.com = HADOOP-REALM
```

5. 데이터 통합 서비스를 호스팅하는 시스템의 다음 위치에 krb5.conf 파일을 복사합니다.

- <Informatica 설치 디렉터리>/services/shared/security/
- <Informatica 설치 디렉터리>/java/jre/lib/security

다음 예는 Kerberos 구성 파일의 콘텐츠와 단일 Kerberos 영역 구성의 필요한 속성을 보여 줍니다.

```
[libdefaults]
default_realm = COMPANY.COM
forwardable = true
rdns = false
renew_lifetime = 7d
ticket_lifetime = 24h
udp_preference_limit = 1
dns_lookup_kdc = true
dns_lookup_realm = true

[realms]
COMPANY.COM = {
admin_server = KDC01.COMPANY.COM:749
kdc = KDC01.COMPANY.COM:88
}

[domain_realm]
.company.com = COMPANY.COM
company.com = COMPANY.COM
```

다음 예는 Kerberos 구성 파일의 콘텐츠와 Kerberos 교차 영역 구성의 필요한 속성을 보여 줍니다.

```
[libdefaults]
default_realm = COMPANY.COM
forwardable = true
rdns = false
renew_lifetime = 7d
ticket_lifetime = 24h
udp_preference_limit = 1
dns_lookup_kdc = true
dns_lookup_realm = true

[realms]
COMPANY.COM = {
admin_server = KDC01.COMPANY.COM:749
kdc = KDC01.COMPANY.COM:88
}
EAST.COMPANY.COM = {
kdc = 10.75.141.193
admin_server = 10.75.141.193
}
WEST.COMPANY.COM = {
kdc = 10.78.140.111
admin_server = 10.78.140.111
}

[domain_realm]
.company.com = COMPANY.COM
company.com = COMPANY.COM
.east.company.com = EAST.COMPANY.COM
east.company.com = EAST.COMPANY.COM
.west.company.com = WEST.COMPANY.COM
west.company.com = WEST.COMPANY.COM
```

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

Active Directory에서 Kerberos 사용자 계정 생성

Active Directory에서 Kerberos 사용자에게 대한 LDAP 사용자 계정을 생성합니다. Kerberos 사용자는 Kerberos 영역 내의 프로세스, 서비스 또는 사용자입니다.

krb5.conf 구성 파일의 default_tkt_enctypes 속성을 128비트 또는 256비트 AES 암호화 유형으로 설정한 경우 Active Directory에서 해당하는 암호화 유형을 사용하도록 각 계정을 구성해야 합니다.

생성하는 계정은 Kerberos를 노드 수준에서 활성화하는지, 아니면 프로세스 수준에서 활성화하는지에 따라 다릅니다.

참고: 계정 이름의 길이는 최대 20자일 수 있습니다.

노드 수준에서 필요한 계정

Active Directory의 노드 수준에서 Kerberos 인증을 활성화하는 데 필요한 LDAP 사용자 계정을 생성합니다.

노드 수준에서 Kerberos를 활성화하는 경우 Active Directory에서 다음 Kerberos 사용자 계정을 생성합니다.

노드 프로세스

도메인에서 실행되는 각 노드에 대한 계정을 생성합니다.

HTTP 프로세스

도메인의 각 노드에서 실행되는 Informatica 웹 응용 프로그램에 대한 계정을 생성합니다. 노드에서 실행되는 웹 응용 프로그램에는 Administrator 도구, Informatica Analyst 및 Catalog Administrator가 포함될 수 있습니다. 노드에서 실행되는 모든 웹 응용 프로그램이 공유하는 단일 계정을 생성합니다.

사용자 DN(고유 이름) 바인딩

Kerberos 사용자 계정이 포함된 LDAP 보안 도메인과 Active Directory를 동기화할 때 사용할 LDAP 바인딩 사용자 계정을 생성합니다.

프로세스 수준에서 필요한 계정

Active Directory의 프로세스 수준에서 Kerberos 인증을 활성화하는 데 필요한 LDAP 사용자 계정을 생성합니다.

프로세스 수준에서 Kerberos를 활성화하는 경우 Active Directory에서 다음 Kerberos 사용자 계정을 생성합니다.

노드 프로세스

도메인에서 실행되는 각 노드에 대한 계정을 생성합니다.

HTTP 프로세스

도메인의 각 노드에서 실행되는 Informatica 웹 응용 프로그램에 대한 계정을 생성합니다. 노드에서 실행되는 웹 응용 프로그램에는 Informatica Analyst 및 Catalog Administrator가 포함될 수 있습니다. 노드에서 실행되는 모든 웹 응용 프로그램이 공유하는 단일 계정을 생성합니다.

Informatica Administrator 서비스

도메인의 각 게이트웨이 노드에 Administrator 도구에 대한 계정을 생성합니다.

Informatica Application Service

도메인의 각 노드에서 실행되는 모든 Informatica Application Service에 대한 계정을 생성합니다.

사용자 DN(고유 이름) 바인딩

Kerberos 사용자 계정이 포함된 LDAP 보안 도메인과 Active Directory를 동기화할 때 사용할 LDAP 사용자 계정을 생성합니다.

서비스 사용자 이름 및 keytab 파일 이름 형식 생성

Informatica Kerberos SPN 형식 생성기 유틸리티를 사용하여 Kerberos 인증을 사용하는 데 필요한 SPN(서비스 사용자 이름) 및 keytab 파일 이름 형식을 생성합니다. Kerberos SPN 형식 생성기 유틸리티를 사용하면 SPN 및 keytab 파일 이름의 올바른 형식이 포함된 SPNKeytabFormat.txt라는 이름의 텍스트 파일이 생성됩니다.

생성하는 SPN 및 keytab 파일 이름 형식은 Kerberos를 노드 수준에서 활성화하는지, 아니면 프로세스 수준에서 활성화하는지에 따라 다릅니다.

노드 수준에서 서비스 사용자 이름 및 keytab 파일 이름 형식 생성

노드 수준에서 Kerberos 인증을 활성화하는 데 필요한 SPN 및 keytab 파일 이름에 대한 형식을 생성합니다.

Kerberos 인증을 노드 수준에서 활성화하는 경우 Informatica 도메인의 다음 프로세스에 SPN 및 keytab 파일이 필요합니다.

노드 프로세스

도메인의 모든 노드에 대한 SPN 및 keytab 파일이 필요합니다. Kerberos는 동일한 서비스 사용자 이름과 keytab을 사용하여 노드에서 실행되는 Informatica Application Service를 인증합니다.

HTTP 프로세스

도메인의 각 노드에서 실행되는 웹 응용 프로그램에 대한 SPN 및 keytab 파일이 필요합니다. 노드에서 실행되는 웹 응용 프로그램에는 Administrator 도구, Informatica Analyst 및 Catalog Administrator가 포함될 수 있습니다. Kerberos는 동일한 서비스 사용자 이름을 사용하여 노드에서 실행되는 모든 웹 응용 프로그램을 인증합니다.

1. Windows Informatica 노드 호스트에서는 SPNFormatGenerator.bat 배치 파일이 포함된 디렉터리로 이동합니다.

<Informatica 설치 디렉터리>\tools\Kerberos

UNIX Informatica 노드 호스트에서는 SPNFormatGenerator.sh 셸 파일이 포함된 디렉터리로 이동합니다.

<Informatica 설치 디렉터리>/tools/Kerberos

2. SPNFormatGenerator.bat 또는 SPNFormatGenerator.sh를 실행합니다.
3. 다음을 클릭합니다.
4. 노드 수준을 선택합니다.
5. 다음을 클릭합니다.
6. SPN 및 keytab 파일 형식을 생성하는 데 필요한 속성을 입력합니다.

다음 테이블에는 속성이 설명되어 있습니다.

프롬프트	설명
도메인 이름	Informatica 도메인의 이름입니다. 이름은 128자를 초과하지 않아야 하고 7비트 ASCII여야 합니다. 이름에는 공백이나 ` % * + ; " ? , < > \ /` 문자를 사용할 수 없습니다.
서비스 영역 이름	Kerberos 영역의 이름입니다. 해당 영역 이름은 대문자여야 합니다.

프롬프트	설명
노드 이름	Informatica 노드의 이름입니다.
노드 호스트 이름	노드 호스트의 정규화된 이름입니다. 노드 호스트 이름에는 밑줄(_) 문자를 사용할 수 없습니다. 참고: <i>localhost</i> 는 사용하지 마십시오. 호스트 이름은 명시적으로 호스트를 식별해야 합니다.

7. 다른 노드에 대해 추가적으로 SPN 형식을 생성하려면 **+노드**를 클릭하고 노드 이름 및 호스트 이름을 지정합니다.

다음 이미지는 InfaDomain 도메인에서 실행되는 여러 노드에 대한 SPN 형식 생성기 유틸리티 항목을 보여줍니다.

8. **다음**을 클릭합니다.

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

9. **완료**를 클릭하여 SPN 형식 생성기 유틸리티를 종료합니다.

프로세스 수준에서 서비스 사용자 이름 및 keytab 파일 이름 형식 생성

프로세스 수준에서 Kerberos 인증을 활성화하는 데 필요한 SPN 및 keytab 파일 이름에 대한 형식을 생성합니다.

Kerberos 인증을 프로세스 수준에서 활성화하는 경우 Informatica 도메인의 다음 프로세스 및 서비스에 SPN 및 keytab 파일이 필요합니다.

노드 프로세스

도메인의 모든 노드에 대한 SPN 및 keytab 파일이 필요합니다.

Informatica Administrator

도메인의 모든 게이트웨이 노드에 대한 Administrator 도구에 사용할 SPN 및 keytab 파일이 필요합니다.

HTTP 프로세스

도메인의 노드에서 실행되는 웹 응용 프로그램에 대한 SPN 및 keytab 파일이 필요합니다. 노드에서 실행되는 웹 응용 프로그램에는 Informatica Analyst 및 Catalog Administrator가 포함될 수 있습니다.

Informatica Application Service 프로세스

도메인의 모든 노드에서 실행되는 각 Informatica Application Service에 대한 SPN 및 keytab 파일이 필요합니다.

1. Windows Informatica 노드 호스트에서는 SPNFormatGenerator.bat 배치 파일이 포함된 디렉터리로 이동합니다.

<Informatica 설치 디렉터리>\tools\Kerberos

UNIX Informatica 노드 호스트에서는 SPNFormatGenerator.sh 셸 파일이 포함된 디렉터리로 이동합니다.

<Informatica 설치 디렉터리>/tools/Kerberos

2. SPNFormatGenerator.bat 또는 SPNFormatGenerator.sh를 실행합니다.
3. 다음을 클릭합니다.
4. 프로세스 수준을 선택합니다.
5. 다음을 클릭합니다.
6. SPN 및 keytab 파일 형식을 생성하는 데 필요한 속성을 입력합니다.

다음 테이블에는 속성이 설명되어 있습니다.

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

7. 노드에서 실행되는 Informatica Application Service에 대한 SPN 형식을 생성하려면 노드 세부 정보를 입력한 후에 서비스를 클릭합니다.

Administrator 도구에 표시된 대로 Informatica Application Service의 이름을 입력합니다. 도메인의 각 노드에서 실행되는 모든 Informatica Application Service에 대해 이 단계를 완료합니다.

8. 다른 노드에 대해 추가적으로 SPN 형식을 생성하려면 **+노드**를 클릭하고 노드 이름 및 호스트 이름을 지정합니다.

다음 이미지는 InfaDomain 도메인에서 실행되는 여러 노드 및 응용 프로그램 서비스에 대한 SPN 형식 생성기 유틸리티 항목을 보여줍니다.

9. 다음을 클릭합니다.

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

10. **완료**를 클릭하여 SPN 형식 생성기 유틸리티를 종료합니다.

서비스 사용자 이름 및 keytab 파일 이름 형식 텍스트 파일 검토

SPNKeytabFormat.txt 파일을 생성한 후 파일을 검토할 수 있습니다.

파일의 정보를 사용하여 keytab 파일을 생성하고 각 SPN을 Active Directory의 해당하는 사용자 계정에 연결합니다.

SPNKeytabFormat.txt 파일에는 다음 정보가 포함됩니다.

항목 이름

프로세스에 연결된 노드 또는 서비스를 식별합니다.

서비스 사용자 이름

SPN의 형식입니다. SPN은 대/소문자를 구분합니다.

참고: 여러 Kerberos 도메인 이름이 포함된 문자열을 입력하거나 영역 접미사 앞에 별표를 추가하여 접미사가 포함된 모든 영역을 포함하는 경우 SPN 형식에는 영역 이름이 포함되지 않습니다.

다음 테이블에는 SPN 형식이 설명되어 있습니다.

키 탭 유형	SPN 형식
NODE_SPN	isp/<노드 이름>/<도메인 이름>@<REALM NAME>
NODE_AC_SPN	_AdminConsole/<노드 이름>/<도메인 이름>@<REALM NAME>
NODE_HTTP_SPN	HTTP/<노드 호스트 이름>@<REALM NAME> 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	<응용 프로그램 서비스 이름>/<노드 이름>/<도메인 이름>@<REALM NAME>

키 탭 파일 이름

연결된 SPN에 대해 생성할 keytab 파일 이름의 형식입니다. 키 탭 파일 이름은 대/소문자를 구분합니다.

다음 테이블에는 keytab 파일 이름 형식이 설명되어 있습니다.

키 탭 유형	키 탭 파일 이름
NODE_SPN	<노드 이름>.keytab
NODE_AC_SPN	_AdminConsole.keytab
NODE_HTTP_SPN	webapp_http.keytab
SERVICE_PROCESS_SPN	<응용 프로그램 서비스 이름>.keytab

노드 수준의 서비스 사용자

다음 이미지는 노드 수준의 서비스 사용자에게 대해 생성된 SPNKeytabFormat.txt 파일의 콘텐츠를 보여줍니다.

ENTITY_NAME	SPN	KEY_TAB_NAME	KEY_TAB_TYPE
node01	isp/node01/Infadomain@COMPANY.COM	node01.keytab	NODE_SPN
node01	HTTP/US001DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN
node02	isp/node02/Infadomain@COMPANY.COM	node02.keytab	NODE_SPN
node02	HTTP/US005DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN

프로세스 수준의 서비스 사용자

다음 이미지는 프로세스 수준의 서비스 사용자에게 대해 생성된 SPNKeytabFormat.txt 파일의 콘텐츠를 보여줍니다.

ENTITY_NAME	SPN	KEY_TAB_NAME	KEY_TAB_TYPE
node01	isp/node01/Infadomain@COMPANY.COM	node01.keytab	NODE_SPN
node01	_AdminConsole/node01/Infadomain@COMPANY.COM	_AdminConsole.keytab	NODE_AC_SPN
node01	HTTP/US001DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN
node02	isp/node02/Infadomain@COMPANY.COM	node02.keytab	NODE_SPN
node02	_AdminConsole/node02/Infadomain@COMPANY.COM	_AdminConsole.keytab	NODE_AC_SPN
node02	HTTP/US005DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN
MRS_dev:node01	MRS_dev/node01/Infadomain@COMPANY.COM	MRS_dev.keytab	SERVICE_PROCESS_SPN
DIS_dev:node01	DIS_dev/node01/Infadomain@COMPANY.COM	DIS_dev.keytab	SERVICE_PROCESS_SPN
CAT_dev:node02	CAT_dev/node02/Infadomain@COMPANY.COM	CAT_dev.keytab	SERVICE_PROCESS_SPN

keytab 파일 생성

Informatica 사용자 및 서비스를 인증할 때 사용되는 **keytab** 파일을 생성합니다.

Microsoft Windows Server ktpass 유틸리티를 사용하여 Active Directory에서 생성한 각 사용자 계정에 대한 **keytab** 파일을 생성합니다. Active Directory 도메인의 내의 멤버 서버 또는 도메인 컨트롤러에 **keytab** 파일을 생성해야 합니다. Microsoft Windows 7 같은 워크스테이션 운영 체제에는 **keytab** 파일을 생성할 수 없습니다.

ktpass를 사용하여 **keytab** 파일을 생성하려면 다음 명령을 실행합니다.

```
ktpass.exe -out <keytab filename> -princ <service principal name> -mapuser <user account> [-pass <user account password>] -crypto <key types> -ptype <principal type> [-target <realm name>]
```

다음 테이블에는 명령 옵션이 설명되어 있습니다.

옵션	설명
-out	SPNKeytabFormat.txt 파일의 KEY_TAB_NAME 열에서 파일 이름을 복사합니다.
-princ	SPNKeytabFormat.txt 파일의 SPN 열에 서비스 사용자 이름이 표시됩니다. 도메인에서 Kerberos 교차 영역 인증을 사용하는 경우 서비스 사용자 이름은 모든 Kerberos 영역에서 고유해야 합니다.
-mapuser	SPN에 연결할 Active Directory 사용자 계정입니다. 계정 이름은 최대 20자일 수 있습니다.
-pass	해당하는 경우 Active Directory에 설정된 Active Directory 사용자 계정의 암호입니다.
-crypto	keytab 파일에 생성되는 키 유형을 지정합니다. 지원되는 모든 암호화 유형을 사용하려면 all로 설정합니다.
-ptype	사용자 유형입니다. KRB5_NT_PRINCIPAL로 설정합니다.
-target	Active Directory 서버가 속하는 영역의 이름입니다. 유틸리티를 실행할 때 다음 오류가 발생하는 경우 이 옵션을 포함하십시오. DsCrackNames가 이름에 0x2를 반환함

생성하는 **keytab** 파일은 Kerberos를 노드 수준에서 활성화하는지, 아니면 프로세스 수준에서 활성화하는지에 따라 다릅니다.

노드 수준에서 keytab 파일 생성

ktpass를 실행하여 노드 수준에서 **keytab** 파일을 생성하는 경우 각 Kerberos 사용자 계정을 Active Directory의 해당하는 SPN에 연결해야 합니다.

다음 테이블에는 SPNKeytabFormat.txt 예제 파일에 표시된 Kerberos 사용자 계정과 SPN 간의 연결이 나와 있습니다.

사용자 계정	키 탭 유형	서비스 사용자 이름
nodeuser01	NODE_SPN	isp/node01/InfraDomain/COMPANY.COM
httpuser01	NODE_HTTP_SPN	HTTP/US001DEV.company.com@COMPANY.COM

사용자 계정	키 탭 유형	서비스 사용자 이름
nodeuser02	NODE_SPN	isp/node02/Infadomain/COMPANY.COM
httpuser02	NODE_HTTP_SPN	HTTP/US005DEV.company.com@COMPANY.COM

LDAP 동기화 중에 Active Directory 액세스 및 검색에 사용할 LDAP 바인딩 사용자 계정의 **keytab**도 생성해야 합니다.

1. Active Directory에서 각 노드에 대해 생성한 Kerberos 사용자 계정에 대한 **keytab** 파일을 생성합니다.

SPNKeytabFormat.txt 파일의 KEY_TAB_NAME 열에서 파일 이름을 복사합니다. SPNKeytabFormat.txt 파일의 SPN 열에서 서비스 사용자 이름을 복사합니다.

다음 예는 nodeuser01이라는 Kerberos 사용자 계정에 대한 **keytab** 파일을 생성합니다.

```
ktpass.exe -out node01.keytab -princ isp/node01/Infadomain/COMPANY.COM -mapuser nodeuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

2. Active Directory에서 생성한 각 HTTP 프로세스 Kerberos 사용자 계정에 대한 **keytab** 파일을 생성합니다.

도메인에서 Kerberos 교차 영역 인증을 사용하는 경우 도메인이 사용하는 모든 Kerberos 영역에 사용자 계정이 존재할 수 있습니다.

SPNKeytabFormat.txt 파일의 KEY_TAB_NAME 열에서 **keytab** 파일 이름을 복사합니다.

SPNKeytabFormat.txt 파일의 SPN 열에서 서비스 사용자 이름을 복사합니다.

다음 예는 httpuser01이라는 Kerberos 사용자 계정에 대한 **keytab** 파일을 생성합니다.

```
ktpass.exe -out webapp_http.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser httpuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

3. LDAP 동기화 중에 Active Directory 액세스 및 검색에 사용할 LDAP 바인딩 사용자 계정의 **keytab**을 생성합니다.

-princ 옵션의 값을 <사용자 이름>@<Kerberos 영역>으로 구조화합니다. Active Directory 서버에 대한 LDAP 구성의 이름을 **keytab** 파일 이름에 포함합니다. <Active Directory LDAP configuration_name>.keytab 형식으로 **keytab** 파일 이름을 구성합니다.

다음 예는 ldapuser라는 서비스 사용자 계정에 대한 **keytab** 파일을 생성합니다.

```
ktpass.exe -out ActiveDirectoryServer1.keytab -princ ldapuser@COMPANY.COM -mapuser ldapuser -crypto all -ptype KRB5_NT_PRINCIPAL
```

프로세스 수준에서 keytab 파일 생성

ktpass를 실행하여 프로세스 수준에서 **keytab** 파일을 생성하는 경우 각 Kerberos 사용자 계정을 Active Directory의 해당하는 SPN에 연결해야 합니다.

다음 테이블에는 SPNKeytabFormat.txt 예제 파일에 표시된 Kerberos 사용자 계정과 SPN 간의 연결이 나와 있습니다.

사용자 계정	키 탭 유형	서비스 사용자 이름
nodeuser01	NODE_SPN	isp/node01/Infadomain/COMPANY.COM
admintooluser01	NODE_AC_SPN	_AdminConsole/node01/Infadomain@COMPANY.COM

사용자 계정	키 탭 유형	서비스 사용자 이름
httpuser01	NODE_HTTP_SPN	HTTP/US001DEV.company.com@COMPANY.COM
MRSdevuser01	SERVICE_PROCESS_SPN	MRS_dev/node01/Infadomain@COMPANY.COM
DISdevuser01	SERVICE_PROCESS_SPN	DIS_dev/node01/Infadomain@COMPANY.COM
nodeuser02	NODE_SPN	isp/node02/Infadomain/COMPANY.COM
admintooluser02	NODE_AC_SPN	_AdminConsole/node02/Infadomain@COMPANY.COM
httpuser02	NODE_HTTP_SPN	HTTP/US005DEV.company.com@COMPANY.COM
CATdevuser01	SERVICE_PROCESS_SPN	CAT_dev/node02/Infadomain@COMPANY.COM

LDAP 동기화 중에 Active Directory 액세스 및 검색에 사용할 LDAP 바인딩 사용자 계정의 **keytab**도 생성해야 합니다.

1. Active Directory에서 각 노드에 대해 생성한 Kerberos 사용자 계정에 대한 **keytab** 파일을 생성합니다.

SPNKeytabFormat.txt 파일의 KEY_TAB_NAME 열에서 파일 이름을 복사합니다. SPNKeytabFormat.txt 파일의 SPN 열에서 서비스 사용자 이름을 복사합니다.

다음 예는 nodeuser01이라는 Kerberos 사용자 계정에 대한 **keytab** 파일을 생성합니다.

```
ktpass.exe -out node01.keytab -princ isp/node01/Infadomain/COMPANY.COM -mapuser nodeuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

2. 생성한 각 HTTP 프로세스 Kerberos 사용자 계정에 대한 **keytab** 파일을 생성합니다.

도메인에서 Kerberos 교차 영역 인증을 사용하는 경우 도메인이 사용하는 모든 Kerberos 영역에 사용자 계정이 존재할 수 있습니다.

SPNKeytabFormat.txt 파일의 KEY_TAB_NAME 열에서 파일 이름을 복사합니다. SPNKeytabFormat.txt 파일의 SPN 열에서 서비스 사용자 이름을 복사합니다.

다음 예는 httpuser01이라는 Kerberos 사용자 계정에 대한 **keytab** 파일을 생성합니다.

```
ktpass.exe -out webapp_http.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser httpuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

3. 생성한 각 Administrator 도구 Kerberos 사용자 계정에 대한 **keytab** 파일을 생성합니다.

SPNKeytabFormat.txt 파일의 KEY_TAB_NAME 열에서 파일 이름을 복사합니다. SPNKeytabFormat.txt 파일의 SPN 열에서 서비스 사용자 이름을 복사합니다.

다음 예는 admintooluser01이라는 Kerberos 사용자 계정에 대한 **keytab** 파일을 생성합니다.

```
ktpass.exe -out _AdminConsole.keytab -princ _AdminConsole/node01/Infadomain@COMPANY.COM -mapuser admintooluser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

4. 생성한 각 Informatica Application Service Kerberos 사용자 계정에 대한 **keytab** 파일을 생성합니다.

SPNKeytabFormat.txt 파일의 KEY_TAB_NAME 열에서 파일 이름을 복사합니다. SPNKeytabFormat.txt 파일의 SPN 열에서 서비스 사용자 이름을 복사합니다.

다음 예는 MRSdevuser01이라는 서비스 Kerberos 사용자 계정에 대한 **keytab** 파일을 생성합니다.

```
ktpass.exe -out MRS_dev.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser MRSdevuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

5. LDAP 동기화 중에 Active Directory 액세스 및 검색에 사용할 LDAP 바인딩 사용자 계정의 **keytab**을 생성합니다.

-princ 옵션의 값을 <사용자 이름>@<Kerberos 영역>으로 구조화합니다. Active Directory 서버에 대한 LDAP 구성의 이름을 keytab 파일 이름에 포함합니다. <Active Directory LDAP configuration_name>.keytab 형식으로 keytab 파일 이름을 구성합니다.

다음 예는 ldapuser라는 서비스 사용자 계정에 대한 keytab 파일을 생성합니다.

```
ktpass.exe -out ActiveDirectoryServer1.keytab -princ ldapuser@COMPANY.COM -mapuser ldapuser -crypto all -ptype KRB5_NT_PRINCIPAL
```

서비스 사용자 이름 및 keytab 파일 확인

Kerberos 유틸리티를 사용하여 SPN과 keytab 파일이 유효한지 확인할 수 있습니다. 또한 이 유틸리티를 사용하여 Kerberos KDC(키 배포 센터)의 상태를 확인할 수도 있습니다.

kinit 및 *klist* 같은 Kerberos 유틸리티를 사용하여 SPN 및 keytab 파일을 보고 확인할 수 있습니다. 이 유틸리티를 사용하려면 KRB5_CONFIG 환경 변수에 Kerberos 구성 파일의 경로 및 파일 이름이 포함되어 있는지 확인하십시오. Kerberos 유틸리티 실행에 대한 자세한 내용은 Kerberos 설명서를 참조하십시오.

다음 유틸리티를 사용하여 SPN 및 키 탭 파일을 확인합니다.

kinit

kinit 유틸리티를 사용하여 KDC의 TGT(티켓 부여 티켓)를 요청하고 keytab 파일을 Kerberos 연결을 설정하는 데 사용할 수 있는지 여부를 확인할 수 있습니다. keytab 및 지정된 SPN이 올바르면 명령이 티켓을 가져온 후 지정된 캐시에 티켓을 캐싱합니다.

kinit 유틸리티는 Informatica 노드의 다음 디렉터리에서 사용할 수 있습니다.

<Informatica 설치 디렉터리>\java\jre\bin

SPN에 대한 티켓 부여 티켓을 요청하려면 다음 명령을 실행합니다.

```
kinit -c <캐시 이름> -k -t <keytab 파일 이름> <서비스 사용자 이름>
```

다음 출력 예는 지정된 키 탭 파일 및 SPN에 대한 기본 캐시에 생성된 티켓 부여 티켓을 보여줍니다.

```
Cache: \temp\krb Using principal: isp/node01/Infadomain/COMPANY.COM Using keytab: node01.keytab
Authenticated to Kerberos v5
```

klist

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

```
klist -k -t <keytab 파일 이름>
```

다음 출력 예는 키 탭 파일의 사용자를 보여줍니다.

```
Keytab name: FILE:node01.keytab KVNO Timestamp Principal ----
----- 3 12/31/16 19:00:00 MRS_dev/node01/
Infadomain@COMPANY.COM 3 12/31/16 19:00:00 MRS_dev/node01/Infadomain@COMPANY.COM 3 12/31/16 19:00:00
MRS_dev/node01/Infadomain@COMPANY.COM 3 12/31/16 19:00:00 MRS_dev/node01/Infadomain@COMPANY.COM
```

Kerberos 인증 활성화

Informatica 서비스를 설치할 때 Informatica 도메인에서 Kerberos 인증을 활성화하거나 서비스를 설치한 후 Kerberos 인증을 활성화할 수 있습니다.

Informatica 서비스를 설치할 때 Kerberos 인증을 활성화하는 방법에 대한 자세한 내용은 *Informatica 10.2 HotFix 2 설치 및 구성 가이드*를 참조하십시오.

설치 중에 Kerberos 인증을 활성화하지 않은 경우 서비스를 설치한 후 이 섹션의 단계에 따라 Informatica 명령줄 프로그램을 사용하여 Kerberos 인증을 활성화합니다.

도메인에서 Kerberos 인증 활성화

도메인 내의 게이트웨이 노드에서 Kerberos를 활성화합니다.

도메인 내의 게이트웨이 노드에서 `infasetup switchToKerberosMode` 명령을 실행하여 인증을 Kerberos 네트워크 인증으로 변경합니다.

1. 도메인과 모든 Informatica 서비스를 종료합니다. 다음 순서로 서비스를 종료합니다.

- Metadata Manager 서비스
- PowerCenter(R) 통합 서비스
- PowerCenter(R) 리포지토리 서비스
- 콘텐츠 관리 서비스
- 분석 서비스
- 데이터 통합 서비스
- 모델 리포지토리 서비스

2. 게이트웨이 노드의 명령 프롬프트에서 `infasetup` 실행 파일이 있는 디렉터리로 전환합니다.

<Informatica 설치 디렉터리>\isp\bin

3. 다음 명령을 실행합니다.

```
infasetup switchToKerberosMode -ad <administrator name> -srn <Kerberos realm names> -urn <Kerberos realm names> -spnSL <service principal level>
```


다음 테이블에는 `infasetup switchToKerberosMode` 명령의 옵션 및 인수가 설명되어 있습니다.

옵션	인수	설명
-administratorName -ad	user_name	<p>Kerberos 인증을 구성할 때 작성된 도메인 관리자 계정에 대한 사용자 이름입니다. Active Directory에 있는 계정의 이름을 지정합니다.</p> <p>Kerberos 인증을 구성한 후 이 사용자는 명령이 생성한 <code>_infalInternalNamespace</code> 보안 도메인에 포함됩니다.</p> <p>도메인에서 단일 Kerberos 영역을 사용하여 사용자를 인증하는 경우 관리자 계정으로 사용하려는 계정의 <code>samAccount</code> 이름을 지정합니다.</p> <p>도메인에서 Kerberos 교차 영역 인증을 사용하는 경우 관리자 계정으로 사용하려는 계정의 정규화된 사용자 이름(영역 이름 포함)을 지정합니다. 예를 들면 다음과 같습니다.</p> <p>sysadmin@COMPANY.COM</p>
-ServiceRealmName -srn	Kerberos_realm_name	<p>도메인에서 사용자 인증에 사용하는 Kerberos 영역의 이름입니다. 해당 영역 이름은 대문자여야 하고 대/소문자를 구분합니다.</p> <p>Kerberos 교차 영역 인증을 구성하려면 도메인이 사용자 인증에 사용하는 각 Kerberos 영역의 이름을 쉼표로 구분하여 지정합니다. 예를 들면 다음과 같습니다.</p> <p>COMPANY.COM,EAST.COMPANY.COM, WEST.COMPANY.COM</p> <p>특정 이름이 포함된 모든 영역을 포함하려면 영역 이름 앞에 별표를 와일드카드 문자로 사용합니다. 예를 들면 다음과 같습니다.</p> <p>*EAST.COMPANY.COM</p>

옵션	인수	설명
-UserRealmName -urn	Kerberos_realm_name	<p>도메인에서 사용자 인증에 사용하는 Kerberos 영역의 이름입니다. 해당 영역 이름은 대문자여야 하고 대/소문자를 구분합니다.</p> <p>Kerberos 교차 영역 인증을 구성하려면 도메인이 사용자 인증에 사용하는 각 Kerberos 영역의 이름을 쉼표로 구분하여 지정합니다. 예를 들면 다음과 같습니다.</p> <p>COMPANY.COM,EAST.COMPANY.COM, WEST.COMPANY.COM</p> <p>특정 이름이 포함된 모든 영역을 포함하려면 영역 이름 앞에 별표를 와일드카드 문자로 사용합니다. 예를 들면 다음과 같습니다.</p> <p>*EAST.COMPANY.COM</p>
-SPNShareLevel -spnSL	NODE PROCESS	<p>도메인에 대한 서비스 사용자 수준입니다.</p> <p>노드 수준에서 Kerberos를 활성화하려면 NODE로 설정합니다.</p> <p>프로세스 수준에서 Kerberos를 활성화하려면 PROCESS로 설정합니다.</p>

다음 예는 도메인 인증을 Kerberos로 변경하고 단일 Kerberos 영역을 사용하여 사용자를 인증하는 도메인에서 **sysadmin** 사용자 계정을 관리자 계정으로 설정합니다.

```
infasetup switchToKerberosMode -ad sysadmin -srn COMPANY.COM -urn COMPANY.COM -spnSL NODE
```

다음 예는 도메인 인증을 Kerberos로 변경하고 Kerberos 교차 영역 인증을 사용하는 도메인에서 **sysadmin** 사용자 계정을 관리자 계정으로 설정합니다.

```
infasetup switchToKerberosMode -ad sysadmin@COMPANY.COM -srn  
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM -urn COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM -  
spnSL NODE
```

도메인의 노드 업데이트

infasetup switchToKerberosMode 명령을 실행한 게이트웨이 노드를 제외하고 Kerberos 인증 서버 정보를 사용하여 모든 게이트웨이 및 작업자 노드를 업데이트합니다.

다음 명령을 사용하여 게이트웨이 및 작업자 노드를 업데이트합니다.

infasetup UpdateGatewayNode

UpdateGatewayNode 명령을 사용하여 도메인의 게이트웨이 노드에서 Kerberos 인증 매개 변수를 설정합니다. 도메인에 게이트웨이 노드가 여러 개 있으면 각 게이트웨이 노드에서 **UpdateGatewayNode** 명령을 실행합니다.

infasetup UpdateWorkerNode

UpdateWorkerNode 명령을 사용하여 도메인의 작업자 노드에서 Kerberos 인증 매개 변수를 설정합니다. 도메인에 작업자 노드가 여러 개 있으면 각 작업자 노드에서 **UpdateWorkerNode** 명령을 실행합니다.

1. 노드의 명령 프롬프트에서 **infasetup** 실행 파일이 있는 디렉터리로 전환합니다.

```
<Informatica 설치 디렉터리>\isp\bin
```

2. 게이트웨이 노드에 Kerberos 인증 매개 변수를 설정하려면 다음 명령을 실행합니다.

```
infasetup UpdateGatewayNode -krb <true|false> -srn <Kerberos realm names> -urn <Kerberos realm names>
```

작업자 노드에 Kerberos 인증 매개 변수를 설정하려면 다음 명령을 실행합니다.

```
infasetup UpdateWorkerNode -krb <true|false> -srn <Kerberos realm names> -urn <Kerberos realm names>
```

다음 테이블에는 노드의 Kerberos 인증을 활성화하는 데 필요한 옵션 및 인수가 설명되어 있습니다.

옵션	인수	설명
- EnableKerberos -krb	true false	Kerberos 인증을 사용하도록 Informatica 도메인을 구성합니다. Kerberos 인증을 활성화하려면 true로 설정합니다. 기본값은 false입니다.
- ServiceRealmName -srn	Kerberos_realm_name	도메인에서 사용자 인증에 사용하는 Kerberos 영역의 이름입니다. 해당 영역 이름은 대문자여야 하고 대/소문자를 구분합니다. Kerberos 교차 영역 인증을 구성하려면 도메인이 사용자 인증에 사용하는 각 Kerberos 영역의 이름을 쉼표로 구분하여 지정합니다. 예를 들면 다음과 같습니다. COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM 특정 이름이 포함된 모든 영역을 포함하려면 영역 이름 앞에 별표를 와일드카드 문자로 사용합니다. 예를 들면 다음과 같습니다. *EAST.COMPANY.COM
- UserRealmName -urn	Kerberos_realm_name	도메인에서 사용자 인증에 사용하는 Kerberos 영역의 이름입니다. 해당 영역 이름은 대문자여야 하고 대/소문자를 구분합니다. Kerberos 교차 영역 인증을 구성하려면 도메인이 사용자 인증에 사용하는 각 Kerberos 영역의 이름을 쉼표로 구분하여 지정합니다. 예를 들면 다음과 같습니다. COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM 특정 이름이 포함된 모든 영역을 포함하려면 영역 이름 앞에 별표를 와일드카드 문자로 사용합니다. 예를 들면 다음과 같습니다. *EAST.COMPANY.COM

다음 예는 Kerberos 인증을 사용하도록 작업자 노드를 업데이트합니다.

```
infasetup updateWorkerNode -krb true -srn COMPANY.COM -urn COMPANY.COM
```

다음 예는 Kerberos 교차 영역 인증을 사용하도록 작업자 노드를 업데이트합니다.

```
infasetup updateWorkerNode -krb true -srn COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM -urn  
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM
```

Informatica 노드에서 Kerberos 활성화

도메인에서 Kerberos를 활성화한 후 도메인의 각 노드에 Kerberos 구성 파일을 복사해야 합니다. 또한 Informatica 웹 응용 프로그램에 액세스하도록 웹 브라우저를 구성해야 합니다.

keytab 파일을 각 노드의 다음 디렉터리에 복사합니다.

<Informatica 설치 디렉터리>\isp\config\keys

복사하는 keytab 파일은 Kerberos 인증을 노드 수준에서 활성화하는지, 아니면 프로세스 수준에서 활성화하는지에 따라 다릅니다.

노드 수준의 keytab 파일

노드 수준에서 생성된 각 keytab 파일을 해당하는 노드에 복사합니다.

다음 테이블에는 각 keytab 파일을 복사할 노드가 나와 있습니다.

keytab 파일	노드의 위치
<노드 이름>.keytab	각 파일을 해당하는 노드에 복사합니다.
webapp_http.keytab	각 파일을 해당하는 게이트웨이 노드에 복사합니다.
ldapuser.keytab	파일을 각 게이트웨이 노드에 복사합니다.

프로세스 수준의 keytab 파일

프로세스 수준에서 생성된 각 keytab 파일을 해당하는 노드에 복사합니다.

다음 테이블에는 각 keytab 파일을 복사할 노드가 나와 있습니다.

keytab 파일	노드의 위치
<노드 이름>.keytab	각 파일을 해당하는 노드에 복사합니다.
webapp_http.keytab	각 파일을 해당하는 게이트웨이 노드에 복사합니다.
_AdminConsole.keytab	각 파일을 해당하는 게이트웨이 노드에 복사합니다.
<응용 프로그램 서비스 이름>.keytab	각 파일을 Informatica Application Service가 실행되는 해당 노드에 복사합니다.
ldapuser.keytab	파일을 각 게이트웨이 노드에 복사합니다.

Informatica 웹 응용 프로그램에 액세스하도록 웹 브라우저를 구성합니다.

Microsoft Internet Explorer 및 Google Chrome에서 Informatica 웹 응용 프로그램(예: Analyst 도구)의 URL을 신뢰할 수 있는 사이트의 목록에 추가합니다.

Chrome 버전 41 이상을 사용 중인 경우 AuthServerWhitelist 및 AuthNegotiateDelegateWhitelist 정책도 설정해야 합니다.

Informatica 노드에 keytab 파일 복사

keytab 파일을 생성한 후 각 keytab 파일을 해당하는 노드에 복사합니다.

keytab 파일을 각 노드의 다음 디렉터리에 복사합니다.

<Informatica 설치 디렉터리>\isp\config\keys

복사하는 keytab 파일은 Kerberos 인증을 노드 수준에서 활성화하는지, 아니면 프로세스 수준에서 활성화하는지에 따라 다릅니다.

노드 수준의 keytab 파일

노드 수준에서 생성된 각 keytab 파일을 해당하는 노드에 복사합니다.

다음 테이블에는 각 **keytab** 파일을 복사할 노드가 나와 있습니다.

keytab 파일	노드의 위치
<노드 이름>.keytab	각 파일을 해당하는 노드에 복사합니다.
webapp_http.keytab	각 파일을 해당하는 노드에 복사합니다.
ldapuser.keytab	파일을 각 게이트웨이 노드에 복사합니다.

프로세스 수준의 **keytab** 파일

프로세스 수준에서 생성된 각 **keytab** 파일을 해당하는 노드에 복사합니다.

다음 테이블에는 각 **keytab** 파일을 복사할 노드가 나와 있습니다.

keytab 파일	노드의 위치
<노드 이름>.keytab	각 파일을 해당하는 노드에 복사합니다.
webapp_http.keytab	각 파일을 해당하는 노드에 복사합니다.
_AdminConsole.keytab	각 파일을 해당하는 노드에 복사합니다.
<응용 프로그램 서비스 이름>.keytab	각 파일을 Informatica Application Service가 실행되는 해당 노드에 복사합니다.
ldapuser.keytab	파일을 각 노드에 복사합니다.

Informatica 클라이언트에 대한 Kerberos 인증 활성화

Informatica 클라이언트를 호스팅하는 각 컴퓨터에 **Kerberos** 구성 파일을 복사한 후 구성 파일을 가리키도록 환경 변수를 설정합니다. 또한 **Informatica** 웹 응용 프로그램에 액세스하도록 클라이언트 브라우저를 설정해야 합니다.

Kerberos 인증을 사용하여 실행하도록 **Informatica** 도메인을 구성한 후 **Informatica** 클라이언트 도구에서 다음 태스크를 수행하십시오.

각 **Informatica** 클라이언트 호스트에 **Kerberos** 구성 파일을 복사합니다.

PowerCenter Client 또는 **Informatica Developer** 클라이언트(Developer tool) 같은 **Informatica** 클라이언트를 호스팅하는 각 컴퓨터에 **krb5.conf** 파일을 복사합니다. 각 호스트의 다음 디렉터리에 파일을 복사합니다.

<Informatica 설치 디렉터리>\clients\shared\security

각 **Informatica** 클라이언트 호스트에서 **KRB5_CONFIG** 환경 변수를 설정합니다.

KRB5_CONFIG 환경 변수를 **Informatica** 클라이언트(예: **PowerCenter Client** 및 **Developer tool**)를 호스팅하는 각 컴퓨터의 **Kerberos** 구성 파일 경로 및 이름으로 설정합니다.

Informatica 웹 응용 프로그램에 액세스하도록 웹 브라우저를 구성합니다.

Microsoft Internet Explorer 및 **Google Chrome**에서 **Informatica** 웹 응용 프로그램(예: **Analyst** 도구)의 URL을 신뢰할 수 있는 사이트의 목록에 추가합니다.

Chrome 버전 41 이상을 사용 중인 경우 **AuthServerWhitelist** 및 **AuthNegotiateDelegateWhitelist** 정책도 설정해야 합니다.

Hadoop 통합을 위해 Kerberos 활성화

Kerberos가 활성화된 클러스터에서 매핑을 실행하고 Developer tool에서 메타데이터를 보려면 Administrator 도구 및 각 Developer tool 시스템에서 구성 태스크를 수행해야 합니다.

다음 태스크를 수행합니다.

- Kerberos 구성 파일 구성
- 사용자 인증 아티팩트 생성
- Informatica 도메인에 대한 Kerberos 인증 속성 구성
- 각 Developer tool 시스템으로 구성 파일 가져오기
- Developer tool 시스템에 대한 Kerberos 자격 증명 파일 생성

이러한 태스크를 수행하는 방법을 보려면 *Data Engineering 관리자 가이드*에서 Kerberos 인증을 사용한 매핑 실행에 대한 장을 읽으십시오.

Kerberos 인증을 사용하도록 사용자 계정 설정

도메인에서 Kerberos 인증을 활성화한 후 Active Directory의 Informatica 사용자 계정을 Kerberos 사용자 계정이 포함되는 LDAP 보안 도메인으로 가져옵니다. 또한 원시 보안 도메인의 그룹, 역할, 권한 및 사용 권한을 Kerberos 사용자 계정이 포함되는 LDAP 보안 도메인의 해당하는 Active Directory 사용자 계정으로 마이그레이션해야 합니다.

Active Directory의 사용자 계정을 LDAP 보안 도메인으로 가져오기

Active Directory의 사용자 계정을 LDAP 보안 도메인으로 가져옵니다.

도메인에서 Kerberos 인증을 활성화하면 Kerberos 영역과 이름이 같은 빈 LDAP 보안 도메인이 생성됩니다. Active Directory의 사용자 계정을 이 LDAP 보안 도메인으로 가져오거나 사용자 계정을 다른 LDAP 보안 도메인으로 가져올 수 있습니다.

Administrator 도구를 사용하여 Kerberos 인증을 사용하는 사용자 계정을 Active Directory에서 LDAP 보안 도메인으로 가져옵니다.

Kerberos 교차 영역 인증을 구성하려면 Active Directory 글로벌 카탈로그에 연결합니다. 글로벌 카탈로그에 연결할 때 각 Kerberos 영역에 사용되는 Active Directory 서버에서 사용자를 가져옵니다.

1. 도메인과 모든 Informatica 서비스를 시작합니다.
2. 도메인에서 Kerberos 인증을 활성화할 때 지정한 관리자 계정으로 Windows에 로그인합니다.
3. Administrator 도구에 로그인합니다. `_infalnternalNamespace`를 보안 도메인으로 선택합니다.
4. Administrator 도구에서 **보안** 탭을 클릭합니다.
5. **작업** 메뉴를 클릭하고 **LDAP 구성**을 선택합니다.
6. **LDAP 구성** 대화 상자에서 **LDAP 연결** 탭을 클릭합니다.
7. Active Directory에 대한 연결 속성을 구성합니다.

LDAP 서버 연결에 필요한 정보를 가져오려면 LDAP 관리자에게 문의해야 할 수 있습니다.

다음 테이블에는 LDAP 서버 구성 속성이 설명되어 있습니다.

속성	설명
서버 이름	Active Directory 서버의 호스트 이름 또는 IP 주소입니다. Kerberos 교차 영역 인증을 구성하려면 Active Directory 글로벌 카탈로그 호스트에 연결합니다. 정규화된 호스트 이름을 지정합니다. 예를 들면 다음과 같습니다. host.company.local
포트	Active Directory 서버의 수신 대기 포트입니다. 기본값은 389입니다. 기본 SSL 포트는 636입니다. Kerberos 교차 영역 인증을 구성하려면 Active Directory 글로벌 카탈로그 포트에 연결합니다. 기본값은 3268입니다. 기본 SSL 포트는 3269입니다.
LDAP 디렉터리 서비스	Microsoft Active Directory 서비스를 선택합니다.
이름	Active Directory의 계정을 LDAP 보안 도메인과 동기화하기 위해 Active Directory에서 생성한 바인딩 사용자 계정을 지정합니다. 도메인에서 Kerberos 인증이 활성화되었기 때문에 계정 암호를 입력하는 옵션은 표시되지 않습니다. 도메인에서 Kerberos 교차 영역 인증을 사용하는 경우 Active Directory 사용자 데이터베이스가 속하는 영역의 이름을 포함합니다.
SSL 인증서 사용	LDAP 서버가 SSL(보안 소켓 레이어) 프로토콜을 사용한다는 것을 나타냅니다.
LDAP 인증서 트러스트	서비스 관리자가 LDAP 서버의 SSL 인증서를 트러스트할 수 있는지 여부를 결정합니다. 선택하면 서비스 관리자는 SSL 인증서를 확인하지 않고 LDAP 서버에 연결합니다. 선택하지 않으면 서비스 관리자가 LDAP 서버에 연결하기 전에 SSL 인증서가 인증서 인증으로 서명되어 있는지 확인합니다.
대/소문자 구분 안 함	사용자를 그룹에 할당할 때 서비스 관리자가 고유 이름 특성의 대/소문자 구분을 무시해야 한다는 것을 나타냅니다.
그룹 멤버 자격 특성	사용자의 그룹 멤버 자격 정보가 포함된 특성의 이름입니다. 이것은 그룹의 멤버인 사용자 또는 그룹의 DN이 포함된 LDAP 그룹 개체의 특성입니다. 예를 들어 <i>member</i> 또는 <i>memberof</i> 입니다.
최대 크기	보안 도메인으로 가져올 사용자 계정의 최대 수입니다. 예를 들어 값이 100으로 설정된 경우 최대 100개의 사용자 계정을 보안 도메인으로 가져올 수 있습니다. 가져올 사용자 수가 이 속성에 대한 값을 초과하는 경우 서비스 관리자는 오류 메시지를 생성하고 사용자를 가져오지 않습니다. 가져올 사용자가 많은 경우 이 속성을 더 높은 값으로 설정합니다. 기본값은 1000입니다.

8. **LDAP 구성** 대화 상자에서 **보안 도메인** 탭을 클릭합니다.
9. **추가**를 클릭합니다.

다음 테이블에는 보안 도메인에 대해 설정할 수 있는 필터 속성이 설명되어 있습니다.

속성	설명
보안 도메인	Active Directory의 사용자 계정을 가져올 LDAP 보안 도메인의 이름입니다.
사용자 검색 기준	Active Directory에서 사용자 이름을 검색하는 시작점 역할을 하는 항목의 DN(고유 이름)입니다. 검색하면 개체의 고유 이름의 경로에 따라 디렉터리에서 개체를 찾습니다. 예를 들어 example.com Windows 도메인에서 Informatica 사용자 계정이 포함되는 USERS 컨테이너를 검색하려면 CN=USERS,DC=EXAMPLE,DC=COM을 지정합니다.
사용자 필터	디렉터리 서비스에서 사용자를 검색하는 조건을 지정하는 LDAP 쿼리 문자열입니다. 필터에서 특성 유형, 어설션 값 및 일치 조건을 지정할 수 있습니다. 예: (objectclass=*) - 모든 개체를 검색합니다. (&(objectClass=user)(!(cn=susan))) - "susan" 이외의 모든 사용자 개체를 검색합니다. 검색 필터에 대한 자세한 내용은 LDAP 디렉터리 서비스에 대한 설명서를 참조하십시오.
그룹 검색 기준	LDAP 디렉터리 서비스에서 그룹 이름을 검색하는 시작점 역할을 하는 항목의 DN(고유 이름)입니다.
그룹 필터	디렉터리 서비스에서 그룹을 검색하는 조건을 지정하는 LDAP 쿼리 문자열입니다.

다음 이미지는 Active Directory의 LDAP 사용자를 도메인에서 Kerberos를 활성화할 때 생성한 LDAP 보안 도메인으로 가져올 때 필요한 정보를 보여줍니다.

LDAP Configuration

Fields marked with an asterisk (*) are required.

LDAP Connectivity **Security Domains** Schedule

You can specify multiple security domains for LDAP users and groups. Click Add to add a new security domain. + Add

▼ Add new Security Domain Preview Cancel

Security Domain *	COMPANY.COM
User search base	CN=USERS,DC=COMPANY,DC=COM
User filter	
Group search base	
Group filter	

Synchronize Now OK Cancel

10. **지금 동기화**를 클릭합니다.

서비스 관리자가 모든 LDAP 보안 도메인의 사용자와 LDAP 디렉터리 서비스의 사용자를 동기화합니다. 동기화 프로세스를 완료하는 데 걸리는 시간은 가져오는 사용자 및 그룹 수에 따라 다릅니다.

11. **확인**을 클릭하여 LDAP 보안 도메인을 저장합니다.

원시 사용자 권한 및 사용 권한을 Kerberos 보안 도메인으로 마이그레이션

Informatica 도메인에 원시 보안 도메인의 사용자 계정이 있는 경우 Kerberos 보안 도메인의 해당 Active Directory 사용자 계정에 동일한 그룹, 역할, 권한 및 사용 권한이 있어야 합니다. 원시 사용자의 그룹, 역할, 권한 및 사용 권한을 Kerberos LDAP 보안 도메인의 해당하는 사용자 계정으로 마이그레이션합니다.

1. 원시 사용자 계정 목록을 검토하고 Kerberos 인증을 위해 LDAP 보안 도메인으로 마이그레이션하려는 계정을 결정합니다.

Informatica 도메인의 사용자 계정을 나열하려면 다음 명령을 실행합니다.

```
infacmd isp ListAllUsers
```

Kerberos 보안 도메인으로 마이그레이션하려는 각 원시 사용자 계정은 Kerberos 인증을 위해 사용하는 Active Directory 서비스에 해당 계정이 있어야 합니다.

2. 사용자 마이그레이션 파일을 생성합니다.

사용자 마이그레이션 파일은 원시 사용자 및 동일한 그룹, 역할, 권한 및 사용 권한을 요구하는 해당 Kerberos 사용자 목록이 들어 있는 일반 텍스트 파일입니다.

다음 형식을 사용하여 사용자 마이그레이션 파일의 항목을 나열합니다.

```
Native/<source user name>,<LDAP security domain>/<target user name>
```

다음 예는 COMPANY.COM 보안 도메인으로 마이그레이션할 목록의 사용자가 포함된 사용자 마이그레이션 파일을 보여줍니다.

```
Native/User1,COMPANY.COM/User1
Native/User2,COMPANY.COM/User2
Native/User3,COMPANY.COM/User3
```

3. `infacmd isp migrateUsers` 명령을 실행하여 원시 보안 도메인의 계정 권한 및 사용 권한을 Kerberos 보안 도메인의 계정으로 마이그레이션합니다.

사용자에 대한 그룹, 역할, 권한 및 사용 권한을 마이그레이션하려면 다음 명령을 실행합니다.

```
infacmd isp migrateUsers -dn <domain name> -un <administrator user name> -pd <administrator password> -sdn <security domain> -umf <user migration file>
```

다음 테이블에는 명령에 대한 옵션이 설명되어 있습니다.

옵션	설명
-DomainName -dn	Informatica 도메인의 이름입니다.
-UserName -un	도메인에 연결하기 위한 사용자 이름입니다. <code>infasetup switchToKerberosMode</code> 명령에서 지정한 관리자 계정의 사용자 이름을 지정합니다.
-Password -pd	관리자 계정에 대한 암호입니다.

옵션	설명
-SecurityDomain -sdn	도메인에 연결할 때 사용되는 관리자 계정의 LDAP 보안 도메인입니다. _infaInternalNamespace를 지정합니다.
-UserMigrationFile -umf	사용자 마이그레이션 파일의 경로 및 파일 이름입니다. 명령이 중복 소스 사용자 이름 또는 대상 사용자 이름이 포함된 항목은 건너뜁니다.

다음 예는 um_s.txt 사용자 마이그레이션 파일에 따라 사용자의 그룹, 역할, 권한 및 사용 권한을 마이그레이션합니다.

```
infacmd isp migrateUsers -dn InfaDomain -un nodeuser01 -pd password -sdn _infaInternalNamespace -umf C:\Infa\um_s.txt
```

이 명령은 원시 사용자에 대한 연결 개체 사용 권한으로 LDAP 사용자에게 할당된 연결 개체 사용 권한을 덮어씁니다. 이 명령은 원시 사용자 및 해당 LDAP 사용자에 대한 그룹, 역할, 권한 및 도메인 개체 권한을 병합합니다.

migrateUsers 명령을 실행하면 명령을 실행한 디렉터리에 infacmd_uml_date_time.txt라는 이름의 상세한 로그 파일이 생성됩니다.

Kerberos 위임

Kerberos 위임을 사용하면 Kerberos 서비스에서 Kerberos 클라이언트 사용자를 가장하고 클라이언트 사용자를 대신하여 다른 서비스에 대한 서비스 티켓을 받을 수 있습니다.

Informatica 도메인의 서비스에서 작업을 완료하려면 다른 서비스에 연결해야 합니다. 위임된 인증을 통해 다른 서비스에 연결할 수 있습니다. 위임된 인증에서 사용자가 서비스에 의해 인증되면 서비스는 해당 자격 증명을 사용하여 다른 서비스에 연결합니다. 예를 들어 pmcmd 사용자가 Power Center 통합 서비스에 액세스하는 경우 서비스는 pmcmd 사용자 역할로 Power Center 리포지토리 서비스에 인증합니다.

Kerberos 위임 유형

위임된 인증을 사용하는 경우 다음 위임 유형 중 하나를 선택할 수 있습니다.

전체 위임

전체 위임은 Kerberos 위임의 초기 구현입니다. 이 위임 방법에서는 클라이언트가 Kerberos 인증 후에 TGT(허용 티켓)를 서비스에 전달합니다. 서비스는 TGT를 사용하여 네트워크의 다른 서비스에 액세스하기 위한 서비스 티켓을 받습니다. 이러한 유형의 위임은 안전한 것으로 간주되지 않습니다. 서버에서 클라이언트 ID를 사용하여 액세스할 수 있는 서비스를 관리자가 제어할 수 없기 때문입니다. 전체 위임은 제한 없는 위임이라고도 합니다.

리소스 기반 제한 위임

리소스 기반 제한 위임을 통해 관리자는 서비스의 클라이언트 ID 사용을 제한할 수 있습니다. 이 위임 방법에서는 클라이언트가 TGT를 서버로 전달하지 않습니다. 이 방법에서는 서비스가 신뢰할 수 있는 사용자와 인증을 위임할 수 있는 사용자를 지정합니다.

제한 위임은 서비스에서 사용자를 대신하여 Kerberos 서비스 티켓을 받는 데 사용되는 S4U(사용자 서비스)라고 하는 Kerberos 프로토콜 확장을 사용합니다.

참고: 단일 도메인에서 제한 위임과 전체 위임을 모두 사용할 수는 없습니다. 전체 위임 또는 제한 위임 중 하나를 사용하도록 도메인을 구성할 수 있습니다.

S4U(사용자 서비스) 확장

S4U(사용자 서비스) 확장을 사용하면 서비스에서 사용자를 대신하여 Kerberos 서비스 티켓을 받을 수 있습니다. 다음은 2가지 유형의 S4U 확장입니다.

- S4U2Self(자체 사용자 서비스). 이 확장을 사용하면 서비스에서 클라이언트 사용자를 대신하여 자체 서비스에 대한 서비스 티켓을 받을 수 있습니다.
- S4U2Proxy(프록시 사용자 서비스). 이 확장을 사용하면 서비스에서 클라이언트 사용자를 대신하여 다른 서비스에 대한 서비스 티켓을 받을 수 있습니다. S4U2proxy를 수행하려면 서비스에 서비스 자체에 대한 서비스 티켓이 필요합니다. 서비스 티켓은 클라이언트 사용자가 제시하거나 S4U2Self 확장을 통해 받을 수 있습니다.

S4U 확장에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

S4U2Self로 리소스 기반 제한 위임 활성화

krb5.conf 파일의 libdefaults 섹션에서 forwardable 플래그가 true로 설정되어 있는지 확인하십시오.

리소스 기반 제한 위임은 powershell 명령을 통해서만 구성할 수 있습니다. KDC 계정의 속성을 변경하는 데 필요한 권한을 가진 사용자, 가급적이면 KDC 관리자로 powershell을 시작해야 합니다.

S4U2Self로 리소스 기반 제한 위임을 활성화하려면 KDC 서버의 모든 Informatica 키 탭 계정에 대해 다음 단계를 수행하십시오.

1. 사용자 계정을 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.

속성 대화 상자가 나타납니다.

2. 위임 탭에서 위임용으로 이 컴퓨터 트러스트 안 함을 선택합니다.
3. 적용을 클릭합니다.

4. 다음 명령을 실행하여 PrincipalsAllowedToDelegateToAccount 특성을 설정합니다.

```
$IntermediateService = Get-ADUser -Identity <중간 서버 계정의 samAccountName> -Properties *  
Set-ADUser -Identity <대상 서버 계정의 samAccountName> -PrincipalsAllowedToDelegateToAccount  
$IntermediateService1, $IntermediateService2, $IntermediateService3
```

참고: 쉼표로 구분된 값을 사용하여 PrincipalsAllowedToDelegateToAccount 특성에 여러 계정을 추가할 수 있습니다.

5. PrincipalsAllowedToDelegateToAccount 특성을 설정 해제하려면 다음 명령을 실행합니다.

```
Set-ADUser -Identity <대상 서버 계정의 samAccountName> PrincipalsAllowedToDelegateToAccount $null
```

6. PrincipalsAllowedToDelegateToAccount 목록의 기존 사용자를 보려면 다음 명령을 실행합니다.

```
$FormatEnumerationLimit=-1  
Get-ADUser -Identity <sam 계정 이름> -properties  
PrincipalsAllowedToDelegateToAccount
```

참고: 기본적으로 powershell 명령 출력은 출력에서 서비스 사용자 목록에 있는 값 4개를 보여줍니다. 사용자의 전체 목록을 표시하려면 이 매개 변수를 -1로 설정합니다.

Active Directory에서 Kerberos 주 사용자 계정에 대한 전체 위임 활성화

ktpass 명령을 사용하여 키 탭 파일을 생성합니다.

전체 위임을 사용하려면 LDAP 동기화 중에 Active Directory 액세스 및 검색에 사용되는 LDAP 바인딩 사용자 계정을 제외하고, 생성한 모든 계정에 대해 위임을 활성화해야 합니다.

전체 위임을 활성화하려면 각 사용자 계정에 대해 다음 단계를 수행하십시오.

1. 사용자 계정을 마우스 오른쪽 단추로 클릭하고 **속성**을 선택합니다.
속성 대화 상자가 나타납니다.
2. 위임 탭에서 **모든 서비스에 대한 위임용으로 이 사용자 트러스트(Kerberos만)**를 선택합니다.
3. **적용**을 클릭합니다.
전체 위임이 활성화됩니다.

전체 위임에서 제한 위임으로 전환

전체 위임을 사용 중인데 제한 위임으로 전환하려면 다음 단계를 수행하십시오.

1. 도메인을 종료합니다.
2. KDC 서버의 **keytab** 계정과 연결된 기존 Active Directory 사용자의 경우 [“S4U2Self로 리소스 기반 제한 위임 활성화” 페이지 59](#)합니다.
3. 도메인을 시작합니다.

제 5 장

Informatica 웹 응용 프로그램에 대한 SAML 인증

이 장에 포함된 항목:

- [SAML 인증 개요, 61](#)
- [SAML 인증 프로세스, 63](#)
- [도메인에서 SAML 인증 활성화, 63](#)
- [인증 보안 강화, 66](#)
- [다른 ID 공급자를 사용하도록 웹 응용 프로그램 구성, 68](#)

SAML 인증 개요

Informatica 웹 응용 프로그램에 대한 SAML(Security Assertion Markup Language) 인증을 구성할 수 있습니다.

SAML(Security Assertion Markup Language)은 서비스 공급자와 ID 공급자 간의 인증 정보 교환을 위한 XML 기반 데이터 형식입니다. Informatica 도메인에서는 Informatica 웹 응용 프로그램이 서비스 공급자입니다.

다음 Informatica 웹 응용 프로그램에서 SAML 인증을 사용하도록 구성할 수 있습니다.

- Informatica Administrator
- Informatica Analyst
- 대량 수집 도구
- Metadata Manager
- Enterprise Data Catalog
- Enterprise Data Preparation
- Data Privacy Management

참고: Kerberos 인증을 사용하도록 구성된 Informatica 도메인에는 SAML 인증을 사용할 수 없습니다.

도메인에서 SAML 인증을 활성화하면 도메인에 구성된 ID 공급자가 이 도메인에서 실행되는 모든 웹 응용 프로그램에 기본적으로 사용됩니다. 그러나 다른 ID 공급자를 사용하도록 도메인에서 실행되는 웹 응용 프로그램을 구성할 수 있습니다. 예를 들어 Informatica Administrator의 ID 공급자로 AD FS를 사용하도록 구성하고, Informatica Analyst에서는 PingFederate를 ID 공급자로 사용하도록 구성할 수 있습니다.

다른 ID 공급자를 사용하도록 웹 응용 프로그램을 구성하는 방법에 대한 자세한 내용은 [“다른 ID 공급자를 사용하도록 웹 응용 프로그램 구성” 페이지 68](#)에서 확인하십시오.

기본 키 저장소 및 트러스트 저장소 디렉터리

Informatica 배포의 <Informatica 설치 디렉터리>\services\shared\security 디렉터리에 기본 키 저장소 및 트러스트 저장소 파일이 포함되어 있습니다.

기본 키 저장소 및 트러스트 저장소는 설정 및 개념 증명 사용 사례에만 사용하는 것이 좋습니다. 프로덕션 환경을 보호하려면 다음 지침을 사용하십시오.

- 기본 디렉터리가 아닌 위치에 SAML 인증을 위한 사용자 지정 키 저장소 및 트러스트 저장소를 구성합니다.
<Informatica 설치 디렉터리>\services\shared\security
- 기본 키 저장소 및 트러스트 저장소를 사용하여 다른 서비스 또는 클라이언트를 구성할 수 없습니다.
- SAML 인증을 활성화하는 경우 키 저장소 또는 트러스트 저장소 인증서 파일과 개인 키를 기본 디렉터리로 가져옵니다.
<Informatica 설치 디렉터리>\services\shared\security
- 키 저장소 또는 트러스트 저장소에 별칭을 할당하는 경우 Informatica가 개인 키 인증 및 인증서 서명에 사용하는 "Informatica LLC"를 사용하지 마십시오.
- 기본 SAML 키 저장소 또는 트러스트 저장소 수정은 기본 디렉터리가 SAML 키 저장소 및 트러스트 저장소 디렉터리로 구성되어 있고 기본 키 저장소 또는 트러스트 저장소에서 개인 키 및 인증서 항목을 가져오려는 경우에만 허용됩니다.

기본 키 저장소 및 트러스트 저장소의 새 항목에 대한 별칭으로 "Informatica LLC"를 사용할 수 없습니다. 사용자 지정 키 저장소-트러스트 저장소 항목의 별칭으로는 "Informatica LLC"를 사용할 수 있습니다.

기본 키 저장소 및 트러스트 저장소 파일에는 파일 삭제 또는 교체, 키 저장소 또는 트러스트 저장소의 암호 변경, Informatica 생성 개인 키 및 서명 인증서 수정, 제거 또는 교체를 포함한 다른 작업은 허용되지 않습니다.

지원되는 ID 공급자

지원되는 ID 공급자를 사용하여 웹 응용 프로그램의 도메인에서 SAML 인증을 관리할 수 있습니다.

Informatica는 다음 ID 공급자를 지원합니다. H2L(How-to Library) 문서 링크를 클릭하여 각 ID 공급자와 도메인 간의 통합 지침을 확인하십시오.

ID 공급자	H2L(How-to Library) 문서
Microsoft AD FS(Active Directory Federation Services)	SAML Authentication with Active Directory Federation Services in Informatica 10.4.0
PingFederate	SAML Authentication with PingFederate in Informatica 10.4.0
F5 Big-IP	SAML Authentication with F5 Networks BIG-IP in Informatica 10.4.1
NetScaler	SAML Authentication with NetScaler for Web Applications
Oracle Access Manager(OAM)	SAML Authentication with Oracle Access Manager for Web Applications
Okta SSO	SAML Authentication with Okta SSO for Web Applications
Azure Active Directory	SAML Authentication with Azure Active Directory for Web Applications

이러한 ID 공급자의 지원되는 버전에 대한 자세한 내용은 Informatica Network(<https://network.informatica.com/community/informatica-network/product-availability-matrices>)에서 Product Availability Matrix를 참조하십시오.

SAML 인증 프로세스

Informatica 웹 응용 프로그램과 ID 공급자는 인증 정보를 교환하여 Informatica 도메인에서 SAML 인증을 활성화합니다.

다음 단계에서는 기본 SAML 인증 흐름에 대해 설명합니다.

1. 사용자가 Informatica 웹 응용 프로그램에 액세스합니다.
2. 사용자는 응용 프로그램 로그인 페이지에서 SAML 인증에 사용되는 LDAP 사용자 계정이 포함된 보안 도메인을 선택한 다음 로그인 단추를 클릭합니다.
사용자가 원시 보안 도메인을 선택하는 경우 사용자는 사용자 이름과 암호를 제공하고 응용 프로그램에 로그인합니다.
3. ID 공급자 구성에 따라 첫 번째 인증에 필요한 자격 증명을 제공하라는 메시지가 표시됩니다.
4. ID 공급자는 사용자의 자격 증명에 대한 유효성을 검사하고 사용자에게 세션을 생성합니다.
또한 ID 공급자는 대상 웹 응용 프로그램 URL의 유효성을 검사한 다음 사용자의 ID 정보가 포함된 SAML 토큰을 사용하여 웹 응용 프로그램으로 사용자를 리디렉션합니다.
5. 응용 프로그램은 SAML 토큰 및 사용자 ID 정보의 유효성을 검사하고 사용자 세션을 생성한 다음 사용자 로그인 프로세스를 완료합니다.

후속 인증에는 브라우저의 기존 사용자 세션이 사용됩니다. SAML 인증을 사용하도록 구성된 다른 Informatica 웹 응용 프로그램에 액세스하려는 경우 사용자는 응용 프로그램 로그인 페이지에서 LDAP 보안 도메인을 선택합니다. 사용자가 사용자 이름이나 암호를 제공할 필요가 없습니다.

사용자는 동일한 브라우저 세션에서 실행되는 모든 Informatica 웹 응용 프로그램에 로그인된 상태로 유지됩니다. 하지만 사용자가 Informatica 웹 응용 프로그램에서 로그아웃하면 동일한 브라우저 세션에서 실행되는 다른 Informatica 웹 응용 프로그램에서도 로그아웃됩니다.

도메인에서 SAML 인증 활성화

도메인에서 SAML 인증을 사용하도록 ID 공급자, Informatica 도메인 및 도메인의 노드를 구성합니다.

도메인에서 실행되는 지원되는 Informatica 웹 응용 프로그램에 대해 SAML 인증을 구성하려면 다음 태스크를 수행합니다.

1. LDAP 구성을 생성하여 Informatica 웹 응용 프로그램 사용자 계정이 포함된 LDAP ID 저장소에 연결합니다. 또한 LDAP 보안 도메인을 생성한 다음 사용자 계정을 보안 도메인으로 가져옵니다.
2. ID 공급자에서 어설션 서명 인증서를 내보냅니다.
3. 어설션 서명 인증서를 도메인의 각 게이트웨이 노드에 있는 트러스트 저장소 파일로 가져옵니다. Informatica 기본 트러스트 저장소 파일 또는 사용자 지정 트러스트 저장소 파일로 인증서를 가져올 수 있습니다.
4. ID 공급자에 포함된 하나 이상의 신뢰 당사자 트러스트 또는 서비스 공급자를 추가합니다.
5. 각 Informatica 웹 응용 프로그램의 URL을 ID 공급자에 추가합니다.
6. 도메인에서 SAML 인증을 활성화합니다.
7. 도메인의 모든 노드에서 SAML 인증을 활성화합니다.

참고: Informatica에서 지원하는 여러 SAML ID 공급자에 대해 H2L(How-To Library) 문서의 자세한 통합 단계를 수행할 수 있습니다. 문서 링크는 [“지원되는 ID 공급자” 페이지 62](#) 항목을 참조하십시오.

ID 공급자 또는 LDAP 저장소에 대한 LDAP 구성 생성

Administrator 도구를 사용하여 ID 공급자 또는 **SAML** 인증을 사용하는 웹 응용 프로그램 사용자 계정이 포함된 LDAP 저장소에 대한 LDAP 구성을 생성합니다.

LDAP 구성을 생성할 때 사용자 계정에 대한 보안 도메인을 생성한 다음 계정을 보안 도메인으로 가져옵니다. 계정을 보안 도메인으로 가져온 후에는 적절한 **Informatica** 도메인 역할, 권한 및 사용 권한을 보안 도메인에 있는 계정에 할당합니다.

LDAP 구성 생성에 대한 자세한 내용은 [“LDAP 구성 생성” 페이지 24](#)에서 확인하십시오.

어설션 서명 인증서 내보내기

ID 공급자는 서비스 공급자에게 어설션 서명 인증서 형태의 신뢰성 어설션을 보냅니다.

서명된 어설션에는 ID 공급자 관리자가 선택한 알고리즘을 사용하여 ID 공급자가 생성하는 서명이 포함됩니다. **Informatica**는 도메인 관리자가 **SAML** 트러스트 저장소로 가져온 해당 공용 인증서를 사용하여 서명을 확인합니다.

서명된 어설션을 활성화하는 것이 좋습니다.

서명된 어설션을 활성화하려면 ID 공급자의 어설션 서명 인증서를 내보냅니다.

SAML 인증에 사용되는 트러스트 저장소로 인증서 가져오기

ID 공급자에 사용되는 어설션 서명 인증서를 **Informatica** 도메인 내의 모든 게이트웨이 노트에 대한 **SAML** 인증에 사용되는 트러스트 저장소 파일에 가져옵니다.

기본 **Informatica** 트러스트 저장소 파일 또는 사용자 지정 트러스트 저장소 파일로 인증서를 가져올 수 있습니다.

ID 공급자 구성

Informatica 웹 응용 프로그램에 **SAML** 토큰을 발급하도록 ID 공급자를 구성합니다.

다음 작업을 수행하여 ID 공급자를 구성하십시오.

- ID 공급자의 도메인에 대한 신뢰 당사자 트러스트를 추가합니다. 신뢰 당사자 트러스트로 정의하면 ID 공급자가 도메인에서 실행되는 **Informatica** 웹 응용 프로그램의 인증 요청을 허용할 수 있습니다.
- ID 저장소의 LDAP 특성이 ID 공급자에서 발급한 **SAML** 토큰에 사용된 해당 유형과 매핑되도록 LDAP 특성을 클레임으로 보내기 규칙을 편집합니다.

도메인에서 **SAML** 인증을 활성화할 때 신뢰 당사자 트러스트의 이름을 제공합니다. 엔터프라이즈 내의 서로 다른 조직이 사용하는 도메인에서 **SAML** 인증을 사용할 수 있도록 하려면 보안 요구 사항에 따라 ID 공급자에 여러 신뢰 당사자 트러스트를 생성해야 할 수 있습니다.

Informatica는 "**Informatica**"를 기본 신뢰 당사자 트러스트 이름으로 인식합니다. "**Informatica**"를 신뢰 당사자 트러스트 이름으로 사용하는 단일 신뢰 당사자를 생성하는 경우 도메인에서 **SAML** 인증을 활성화할 때 신뢰 당사자 트러스트 이름을 제공하지 않아도 됩니다.

참고: ID 공급자에서 모든 문자열은 URL을 포함하여 대/소문자를 구분합니다.

ID 공급자에 Informatica 웹 응용 프로그램 URL 추가

SAML 인증을 사용하는 각 Informatica 웹 응용 프로그램의 URL을 ID 공급자에 추가합니다.

응용 프로그램에서 전송한 인증 요청을 ID 공급자에서 허용할 수 있도록 Informatica 웹 응용 프로그램의 URL을 제공합니다. URL을 제공하면 ID 공급자에서 사용자를 인증한 후에 응용 프로그램에 SAML 토큰도 보낼 수 있습니다.

도메인에서 SAML 인증 설정

SAML 인증은 기존 Informatica 도메인에서 활성화하거나 도메인을 생성할 때 설정할 수 있습니다.

도메인에서 SAML 인증을 활성화하면 이 도메인에서 실행되는 모든 웹 응용 프로그램에 도메인에서 SAML 인증을 활성화할 때 지정한 기본 ID 공급자가 사용됩니다.

다음 옵션 중 하나를 선택합니다.

Informatica 설치 프로그램을 실행할 때 SAML 인증을 활성화합니다.

설치 프로세스의 일환으로 도메인을 구성할 때 SAML 인증을 활성화하고 ID 공급자 URL을 지정할 수 있습니다.

기존 도메인에서 SAML 인증을 활성화합니다.

기존 Informatica 도메인에서 SAML 인증을 활성화하려면 `infasetup updateDomainSamlConfig` 명령을 사용합니다. 이 명령은 도메인 내 모든 게이트웨이 노드에서 실행할 수 있습니다.

도메인을 생성할 때 SAML 인증을 활성화합니다.

도메인을 생성할 때 SAML 인증을 활성화하려면 `infasetup defineDomain` 명령을 사용합니다.

명령 사용에 대한 지침은 *Informatica 명령 참조*를 참조하십시오.

노드에서 SAML 인증 활성화

Informatica 도메인의 모든 게이트웨이 및 작업자 노드에서 SAML 인증을 구성해야 합니다.

다음 옵션 중 하나를 선택하여 게이트웨이 노드에서 SAML 인증을 구성합니다.

시스템에서 게이트웨이 노드를 정의할 때 SAML 인증을 활성화합니다.

`infasetup DefineGatewayNode` 명령을 사용하여 게이트웨이 노드에서 SAML 인증을 활성화합니다.

SAML 인증을 사용하는 도메인에 가입할 게이트웨이 노드를 구성할 때 SAML 인증을 활성화합니다.

`infasetup UpdateGatewayNode` 명령을 사용하여 게이트웨이 노드에서 SAML 인증을 활성화합니다.

작업자 노드를 게이트웨이 노드로 변환할 때 SAML 인증을 활성화합니다.

`isp SwitchToGatewayNode` 명령을 사용하여 노드에서 SAML 인증을 활성화합니다.

다음 옵션 중 하나를 선택하여 작업자 노드에서 SAML 인증을 구성합니다.

시스템에서 작업자 노드를 정의할 때 SAML 인증을 활성화합니다.

`infasetup DefineWorkerNode` 명령을 사용하여 작업자 노드에서 SAML 인증을 활성화합니다.

SAML 인증을 사용하는 도메인에 가입할 작업자 노드를 구성할 때 SAML 인증을 활성화합니다.

`infasetup UpdateWorkerNode` 명령을 사용하여 작업자 노드에서 SAML 인증을 활성화합니다.

명령 사용에 대한 지침은 *Informatica 명령 참조*를 참조하십시오.

인증 보안 강화

요청 서명, 서명된 응답 또는 암호화된 어설션을 활성화하여 인증 보안을 강화할 수 있습니다.

요청 서명

서명된 인증 요청에는 요청 자체의 신뢰성을 확인하는 서명이 포함됩니다. 서비스 공급자 역할을 하는 Informatica는 ID 공급자에게 인증 요청을 보냅니다. 요청의 무결성을 유지하기 위해 인증 요청에 서명할 수 있습니다.

Informatica는 개인 키를 사용하여 SAML 요청에 서명하고 ID 공급자는 해당 공용 인증서를 사용하여 서명을 확인합니다.

Informatica는 HTTP-리디렉션을 통해 SAML 인증 요청을 보냅니다. 요청에는 URL 매개 변수에 서명을 넣는 deflate 인코딩이 사용됩니다.

서명된 응답

ID 공급자는 서비스 공급자의 인증 요청에 응답합니다. 서명된 응답에는 ID 공급자 관리자가 선택한 알고리즘을 사용하여 ID 공급자가 생성하는 서명이 포함됩니다. Informatica는 도메인 관리자가 SAML 트러스트 저장소로 가져온 해당 공용 인증서를 사용하여 서명을 확인합니다.

서명된 어설션 및 암호화된 어설션

ID 공급자는 서비스 공급자에게 신뢰성 어설션을 보냅니다.

서명된 어설션에는 ID 공급자 관리자가 선택한 알고리즘을 사용하여 ID 공급자가 생성하는 서명이 포함됩니다. Informatica는 도메인 관리자가 SAML 트러스트 저장소로 가져온 해당 공용 인증서를 사용하여 서명을 확인합니다. 서명된 어설션을 활성화하는 것이 좋습니다.

Informatica 관리자는 비대칭 키(공개-개인 키)를 생성합니다.

ID 공급자는 ID 공급자가 생성한 대칭 키인 어설션 암호화 키를 사용하여 어설션을 암호화할 수 있습니다.

암호화된 어설션을 활성화할 경우 ID 공급자는 보안 관리자가 ID 공급자로 가져온 공용 인증서를 사용하여 대칭 키도 암호화합니다. SAML 응답에는 암호화된 어설션과 암호화된 대칭 키가 포함됩니다. 서비스 공급자 역할을 하는 Informatica는 Informatica 관리자가 SAML 키 저장소로 가져오는 개인 키를 사용하여 암호화된 대칭 키를 해독합니다. 대칭 키를 얻은 후 Informatica는 암호화된 어설션을 해독합니다.

이 섹션의 단계에 따라 요청 서명, 암호화된 어설션 또는 서명된 응답을 활성화하십시오.

요청 서명

infasetup을 사용하여 설치-업그레이드 프로세스 도중 또는 설치-업그레이드 후에 요청 서명을 활성화할 수 있습니다.

설치 또는 업그레이드 프로세스 중에 설치 유틸리티에서 **서명된 요청** 옵션을 선택합니다.

설치 또는 업그레이드 프로세스 후에 infasetup을 사용하여 요청 서명을 설정합니다.

Administrator 도구 또는 웹 응용 프로그램 사용자 인터페이스를 사용하여 웹 응용 프로그램에 대한 요청 서명을 구성할 수도 있습니다.

infasetup

infasetup을 사용하려면 infasetup updateDomainSamlConfig 명령에 다음 옵션을 사용합니다.

```
[<-SignSamlRequest|-ssr> sign_saml_request]
[<-RequestSigningPrivateKeyAlias|-rspa> saml_request_signing_private_key_alias]
[<-RequestSigningPrivateKeyPassword|-rspw> saml_request_signing_private_key_password]
```

```
[<-RequestSigningAlgorithm|-rsa> saml_request_signing_algorithm]
```

이러한 명령에 대한 자세한 내용은 *Informatica 명령 참조*를 참조하십시오.

Administrator 도구

Administrator 도구에서 요청 서명을 구성합니다.

1. 도메인 탐색기에서 도메인 노드를 선택합니다.
2. 노드 속성의 **SAML 구성** 섹션에서 **편집** 아이콘을 클릭합니다.
3. **서명 요청 활성화**를 선택합니다.
4. 다음 속성을 입력합니다.
 - 서명 개인 키 별칭
 - 서명 개인 키 암호
 - 서명 알고리즘
5. **확인**을 클릭합니다.
6. 도메인을 다시 시작하십시오.

서명된 응답

ID 공급자가 서비스 공급자의 인증 요청 응답에 서명할 수 있도록 서명된 응답을 활성화합니다.

infasetup을 사용하여 설치-업그레이드 프로세스 도중 또는 설치-업그레이드 후에 서명된 응답을 활성화할 수 있습니다.

설치 또는 업그레이드 프로세스 도중에 설치 유틸리티에서 **서명된 응답** 옵션을 선택합니다.

설치 또는 업그레이드 프로세스 후에 infasetup을 사용하여 응답 서명을 설정합니다.

Administrator 도구 또는 웹 응용 프로그램 사용자 인터페이스를 사용하여 웹 응용 프로그램에 대한 서명된 응답을 구성할 수도 있습니다.

참고: Okta SSO ID 공급자는 서명된 응답을 지원하지 않습니다.

infasetup

infasetup을 사용하려면 infasetup updateDomainSamlConfig 명령에 다음 옵션을 사용합니다.

```
[<-SamlResponseSigned|-srs> saml_response_signed]
```

```
[<-ResponseSigningCertificateAlias|-rsca> idp_response_signing_certificate_alias]
```

이러한 명령에 대한 자세한 내용은 *Informatica 명령 참조*를 참조하십시오.

Administrator 도구

Administrator 도구에서 응답 서명을 구성합니다.

1. 도메인 탐색기에서 도메인 노드를 선택합니다.
2. 노드 속성의 **SAML 구성** 섹션에서 **편집** 아이콘을 클릭합니다.
3. **응답 서명 활성화**를 선택합니다.
4. 응답 서명 인증서 별칭 속성을 입력합니다.
5. **확인**을 클릭합니다.

6. 도메인을 다시 시작하십시오.

암호화된 어설션

암호화된 어설션을 활성화하면 ID 공급자가 대칭 키를 사용하여 신뢰성 어설션을 암호화할 수 있습니다.

infasetup을 사용하여 설치-업그레이드 프로세스 도중 또는 설치-업그레이드 후에 어설션 서명 또는 암호화된 어설션을 활성화할 수 있습니다.

설치 또는 업그레이드 프로세스 도중에 설치 유틸리티에서 **어설션 암호화** 옵션을 선택합니다.

설치 또는 업그레이드 프로세스 후에 **infasetup**을 사용하여 암호화된 어설션을 설정합니다.

Administrator 도구 또는 웹 응용 프로그램 사용자 인터페이스를 사용하여 웹 응용 프로그램에 대한 서명된 응답을 구성할 수도 있습니다.

infasetup

infasetup을 사용하려면 **infasetup updateDomainSamlConfig** 명령에 다음 옵션을 사용합니다.

```
[<-SamlAssertionEncrypted|-sae> saml_assertion_encrypted]
[<-EncryptedAssertionPrivateKeyAlias|-eapa> saml_encrypted_assertion_private_key_alias]
[<-EncryptedAssertionPrivateKeyPassword|-eapp> saml_encrypted_assertion_private_key_password]
```

이러한 명령에 대한 자세한 내용은 *Informatica 명령 참조*를 참조하십시오.

Administrator 도구

Administrator 도구에서 암호화된 어설션을 구성합니다.

1. 도메인 탐색기에서 도메인 노드를 선택합니다.
2. 노드 속성의 **SAML 구성** 섹션에서 **편집** 아이콘을 클릭합니다.
3. **어설션 암호화 활성화**를 선택합니다.
4. 다음 속성을 입력합니다.
 - 암호화 어설션 개인 키 별칭
 - 암호화 어설션 개인 키 암호
5. **확인**을 클릭합니다.
6. 도메인을 다시 시작하십시오.

다른 ID 공급자를 사용하도록 웹 응용 프로그램 구성

다른 ID 공급자를 사용하도록 도메인에서 실행되는 **Informatica** 웹 응용 프로그램을 구성할 수 있습니다. 예를 들어 **Informatica Administrator**의 ID 공급자로 **AD FS**를 사용하도록 구성하고, **Informatica Analyst**에서는 **PingFederate**를 ID 공급자로 사용하도록 구성할 수 있습니다.

도메인에서 **SAML** 인증을 활성화하면 이 도메인에서 실행되는 모든 웹 응용 프로그램에 도메인에서 **SAML** 인증을 활성화할 때 지정한 기본 ID 공급자가 사용됩니다. 예를 들어 **AD FS**를 ID 공급자로 구성하는 경우 다른 ID 공급자를 사용하도록 웹 응용 프로그램을 구성하지 않는 한 모든 웹 응용 프로그램의 ID 공급자로 **AD FS**가 사용됩니다.

다음 옵션 중 하나를 사용하여 SAML 인증을 활성화하는 경우 기본 ID 공급자를 지정할 수 있습니다.

- 도메인을 생성하고 Informatica 서비스를 설치하는 경우.
- `infasetup defineDomain` 명령을 실행하여 도메인을 생성하는 경우.
- `infasetup updateDomainSamlConfig` 명령을 실행하여 기존 도메인에서 SAML 인증을 활성화하는 경우.

Administrator 도구를 사용하여 다른 ID 공급자를 사용하도록 웹 응용 프로그램을 구성할 수 있습니다. 다른 ID 공급자를 사용하도록 Administrator 도구 또는 모니터링 응용 프로그램을 구성하려면 응용 프로그램이 실행되는 노드에서 SAML 구성을 수정합니다. 다른 웹 응용 프로그램에서 다른 ID 공급자를 사용하도록 구성하려면 응용 프로그램 프로세스 내에서 SAML 구성을 수정합니다.

ID 공급자 사용 준비

Informatica 웹 응용 프로그램에서 ID 공급자 사용을 준비하려면 다음 태스크를 완료합니다.

1. Informatica 웹 응용 프로그램 사용자 계정이 포함된 ID 공급자 저장소에 대한 LDAP 구성을 생성합니다. 또한 LDAP 보안 도메인을 생성한 다음 사용자 계정을 보안 도메인으로 가져옵니다.
2. ID 공급자에서 ID 공급자 어설션 서명 인증서를 내보냅니다.
3. ID 공급자 어설션 서명 인증서를 도메인의 각 게이트웨이 노드에 있는 트러스트 저장소 파일로 가져옵니다. Informatica 기본 트러스트 저장소 파일 또는 사용자 지정 트러스트 저장소 파일로 인증서를 가져올 수 있습니다.
별칭 이름을 변경하는 경우 해당하는 인증서를 각 게이트웨이 노드의 트러스트 저장소 파일로 가져온 다음 노드를 다시 시작합니다.
4. ID 공급자에서 하나 이상의 신뢰 당사자 트러스트로 추가하고 LDAP 특성을 ID 공급자에서 발급한 보안 토큰에 사용된 해당 유형과 매핑합니다.
5. Informatica 웹 응용 프로그램의 URL을 ID 공급자에 추가합니다.

ID 공급자를 사용하도록 Informatica Administrator 구성

Administrator 도구에서 SAML ID 공급자를 사용하도록 Administrator 도구 또는 모니터링 응용 프로그램을 구성할 수 있습니다. 응용 프로그램이 실행되는 노드의 ID 공급자를 사용하도록 Administrator 도구 또는 모니터링 응용 프로그램을 구성할 수 있습니다.

1. Administrator 도구에서 **서비스 및 노드** 탭을 클릭합니다.
2. 도메인 탐색기에서 Administrator 도구와 모니터링 응용 프로그램이 실행되는 게이트웨이 노드를 선택합니다.
3. SAML 구성 옆의 편집 아이콘을 클릭합니다.
4. 응용 프로그램에서 ID 공급자를 사용하는 데 필요한 속성을 입력합니다.
다음 테이블에는 입력할 수 있는 속성이 설명되어 있습니다.

속성	설명
ID 공급자 URL	선택 사항입니다. ID 공급자 서버의 URL입니다. 전체 URL 문자열을 지정해야 합니다.
서비스 공급자 ID	선택 사항입니다. ID 공급자에 정의된 도메인의 신뢰 당사자 트러스트 이름 또는 서비스 공급자 식별자입니다.

속성	설명
어설션 서명 인증서 별칭	선택 사항입니다. ID 공급자 어설션 서명 인증서를 SAML 인증에 사용되는 트러스트 저장소 파일로 가져올 때 지정한 별칭 이름입니다. 별칭 이름을 변경하는 경우 해당하는 인증서를 각 게이트웨이 노드의 트러스트 저장소 파일로 가져온 다음 노드를 다시 시작합니다.
클록 스큐 허용 오차	선택 사항입니다. ID 공급자 호스트 시스템 클록과 마스터 게이트웨이 노드의 시스템 클록 간에 허용되는 시간 차이입니다. 선택 사항입니다. ID 공급자를 통해 발급된 SAML 토큰의 수명은 ID 공급자 호스트 시스템 클록에 따라 설정됩니다. ID 공급자를 통해 발급된 SAML 토큰의 수명은 토큰에 설정된 시작 시간 또는 종료 시간이 마스터 게이트웨이 노드의 시스템 클록에 지정된 시간(초) 내에 있는 경우 유효합니다. 값은 0~600초여야 합니다. 도메인에 구성된 값을 사용하려면 -1로 설정합니다. 기본값은 120초입니다.

다음 이미지는 Administrator 도구에서 AD FS를 ID 공급자로 사용하는 구성을 보여 줍니다. 속성에 대한 값을 지정하지 않으면 기본 SAML 구성에 설정된 값이 도메인에 사용됩니다.

Edit SAML Configuration

Fields marked with an asterisk (*) are required.

Web Application ID * monitoring

Identity Provider URL

Service Provider ID

Assertion Signing Certificate Alias

Clock Skew Tolerance -1

Web Application ID * AdministratorConsole

Identity Provider URL https://server.company.com/adfs/ls/

Service Provider ID ADFS_Prod

Assertion Signing Certificate Alias adfs_cert

Clock Skew Tolerance 240

OK Cancel

5. **확인**을 클릭합니다.
6. 응용 프로그램을 다시 시작합니다.

Informatica 웹 응용 프로그램 구성

Administrator 도구에서 SAML ID 공급자를 사용하도록 Informatica 웹 응용 프로그램을 구성할 수 있습니다.

1. Administrator 도구에서 **서비스 및 노드** 탭을 클릭합니다.
2. 도메인 탐색기에서 응용 프로그램 또는 응용 프로그램 서비스를 선택합니다.
 - ID 공급자를 사용하도록 Analyst 도구 응용 프로그램을 구성하려면 분석 서비스를 선택하고 **프로세스** 탭을 클릭합니다.

- ID 공급자를 사용하도록 대량 수집 도구 응용 프로그램을 구성하려면 대량 수집 서비스를 선택하고 **프로세스** 탭을 클릭합니다.
 - ID 공급자를 사용하도록 **Metadata Manager** 응용 프로그램을 구성하려면 **Metadata Manager** 서비스를 선택하고 **속성** 탭을 클릭합니다.
 - ID 공급자를 사용하도록 **Enterprise Data Catalog** 응용 프로그램 또는 **Catalog Administrator** 응용 프로그램을 구성하려면 카탈로그 서비스를 선택하고 **프로세스** 탭을 클릭합니다.
 - ID 공급자를 사용하도록 **Enterprise Data Preparation** 응용 프로그램을 구성하려면 **Enterprise Data Preparation** 서비스를 선택하고 **프로세스** 탭을 클릭합니다.
 - ID 공급자를 사용하도록 **Data Privacy Management** 응용 프로그램을 구성하려면 **Data Privacy Management Service**를 선택하고 **프로세스** 탭을 클릭합니다.
3. **SAML 구성** 옆의 편집 아이콘을 클릭합니다.
4. 웹 응용 프로그램에서 ID 공급자를 사용하는 데 필요한 속성을 입력합니다.
- 다음 테이블에는 입력할 수 있는 속성이 설명되어 있습니다.

속성	설명
ID 공급자 URL	선택 사항입니다. ID 공급자 서버의 URL입니다. 전체 URL 문자열을 지정해야 합니다.
서비스 공급자 ID	선택 사항입니다. ID 공급자에 정의된 도메인의 신뢰 당사자 트러스트 이름 또는 서비스 공급자 식별자입니다.
어설션 서명 인증서 별칭	선택 사항입니다. ID 공급자 어설션 서명 인증서를 SAML 인증에 사용되는 트러스트 저장소 파일로 가져올 때 지정한 별칭 이름입니다. 별칭 이름을 변경하는 경우 해당하는 인증서를 각 게이트웨이 노드의 트러스트 저장소 파일로 가져온 다음 노드를 다시 시작합니다.
클록 스큐 허용 오차	선택 사항입니다. ID 공급자 호스트 시스템 클록과 마스터 게이트웨이 노드의 시스템 클록 간에 허용되는 시간 차이입니다. 선택 사항입니다. ID 공급자를 통해 발급된 SAML 토큰의 수명은 ID 공급자 호스트 시스템 클록에 따라 설정됩니다. ID 공급자를 통해 발급된 SAML 토큰의 수명은 토큰에 설정된 시작 시간 또는 종료 시간이 마스터 게이트웨이 노드의 시스템 클록에 지정된 시간(초) 내에 있는 경우 유효합니다. 값은 0~600초여야 합니다. 기본값은 120초입니다.

다음 이미지는 Enterprise Data Catalog에서 PingFederate를 ID 공급자로 사용하는 구성을 보여 줍니다.

Edit Ldadmin SAML Configuration X

Fields marked with an asterisk (*) are required.

Web Application ID	catalog_service_ldmadmin
IDP URL	https://10.70.140.70:9031/idp/startSSO.saml2
Service Provider ID	PingFed_Dev
Assertion Signing Certificate Alias	pingfed_cert
Clock Skew Tolerance	240

? OK Cancel

5. **확인**을 클릭합니다.
6. SAML ID 공급자를 사용하도록 응용 프로그램을 구성한 후 응용 프로그램 또는 응용 프로그램 서비스를 다시 시작합니다.

제 6 장

도메인 보안

이 장에 포함된 항목:

- [도메인 보안 개요, 73](#)
- [도메인 내에서 보안 통신, 74](#)
- [웹 응용 프로그램 서비스에 대한 보안 연결, 85](#)
- [Informatica 도메인의 암호화 그룹, 88](#)
- [보안 소스 및 대상, 91](#)
- [보안 데이터 저장소, 93](#)
- [응용 프로그램 서비스 및 포트, 97](#)

도메인 보안 개요

도메인의 구성 요소 간 보안 통신 및 도메인과 클라이언트 구성 요소 간 보안 통신을 구성하도록 Informatica 도메인의 옵션을 활성화할 수 있습니다.

다른 옵션을 활성화하여 도메인의 특정 구성 요소를 보호할 수 있습니다. 도메인의 모든 구성 요소를 보호할 필요는 없습니다. 예를 들어 도메인의 서비스 간 통신은 보호할 수 있지만 모델 리포지토리 서비스와 리포지토리 데이터베이스 간의 연결은 보호할 수 없습니다.

Informatica는 TCP/IP 및 HTTP 프로토콜을 사용하여 도메인의 구성 요소 간에 통신합니다. 도메인은 SSL 인증서를 사용하여 구성 요소 간 통신을 보호합니다.

Informatica 서비스를 설치할 때 도메인의 서비스 및 Administrator 도구에 대해 보안 통신을 활성화할 수 있습니다. 설치 후 Administrator 도구 또는 명령줄에서 도메인의 보안 통신을 구성할 수 있습니다.

설치 중 설치 프로그램이 암호화 키를 생성하여 도메인에 저장되는 암호와 같은 중요한 데이터를 암호화합니다. 설치 프로그램이 암호화 키를 생성하는 데 사용하는 키워드를 제공할 수 있습니다. 설치 후 중요한 데이터의 암호화 키를 변경할 수 있습니다. 암호화된 데이터를 업데이트하려면 리포지토리 콘텐츠를 업그레이드해야 합니다.

다음 영역에서 보안 통신을 활성화할 수 있습니다.

도메인

도메인에서 옵션을 선택하여 다음 구성 요소에 대한 보안 통신을 활성화할 수 있습니다.

- 서비스 관리자, 도메인의 서비스와 Informatica 클라이언트 도구 간
- 도메인과 도메인 구성 리포지토리 간
- 리포지토리 서비스와 리포지토리 데이터베이스 간

- PowerCenter 통합 서비스와 DTM 프로세스 간

웹 응용 프로그램 서비스

웹 응용 프로그램 서비스(예: 분석 서비스 또는 REST 작업 헵 서비스)와 브라우저 간의 연결을 보호할 수 있습니다.

소스 및 대상

데이터 통합 서비스 및 PowerCenter 통합 서비스와 소스 및 대상 데이터베이스 간의 보안 통신을 활성화할 수 있습니다.

데이터 저장소

Informatica는 도메인에서 데이터를 저장할 때 암호와 같은 중요한 데이터를 암호화합니다. Informatica는 설치 중 제공하는 키워드를 기반으로 암호화 키를 생성합니다. Informatica는 암호화 키를 사용하여 도메인에 저장되는 중요한 데이터를 암호화하고 암호 해독합니다.

도메인 내에서 보안 통신

보안 통신 옵션을 사용하여 서비스 간의 연결 및 서비스와 도메인의 서비스 관리자 간의 연결을 보호할 수 있습니다. 또한 워크플로우에 대해 보안을 활성화하고 도메인에서 작성되는 리포지토리에 대해 보안 데이터베이스를 사용할 수 있습니다.

도메인을 보호한 후에 보안 도메인 작업을 위한 Informatica 클라이언트 응용 프로그램을 구성합니다.

키 저장소 및 트러스트 저장소의 기본 디렉터리

Informatica 배포의 기본 키 저장소 및 트러스트 저장소 파일은 다음 기본 디렉터리에 포함됩니다.

<Informatica 설치 디렉터리>\services\shared\security

기본 키 저장소 및 트러스트 저장소는 설정 및 개념 증명 사용 사례에만 사용하는 것이 좋습니다.

프로덕션 환경을 보호하려면 다음 지침을 사용하십시오.

- 보안 통신을 구성할 때 기본 디렉터리에 있는 파일을 수정, 교체 또는 삭제하지 마십시오.
<Informatica 설치 디렉터리>\services\shared\security
- 기본 디렉터리가 아닌 위치에 보안 통신을 위한 사용자 지정 키 저장소 및 트러스트 저장소를 구성합니다.
<Informatica 설치 디렉터리>\services\shared\security
- 기본 키 저장소 및 트러스트 저장소를 사용하여 다른 서비스 또는 클라이언트를 구성할 수 없습니다.

서비스와 서비스 관리자를 위한 보안 통신

설치 중 도메인 내의 보안 통신을 구성할 수 있습니다. 설치 후 명령줄에서 또는 Administrator 도구에서 도메인에 대한 보안 통신을 구성할 수 있습니다.

Informatica는 도메인을 보호하는 데 사용할 수 있는 SSL 인증서를 제공합니다. 하지만 프로덕션 환경의 도메인과 같이 높은 보안 수준이 필요한 도메인에 대해서는 사용자 지정 SSL 인증서를 제공해야 합니다. 사용하려는 SSL 인증서가 포함된 키 저장소 및 트러스트 파일을 지정합니다.

참고: Informatica는 평가 목적으로 SSL 인증서를 제공합니다. SSL 인증서를 제공하지 않을 경우 Informatica에서는 모든 Informatica 설치에 동일한 기본 개인 키를 사용합니다. 도메인의 보안이 손상될 수 있습니다. 도메인에 높은 수준의 보안이 적용되도록 SSL 인증서를 제공합니다. 제공하는 인증서는 자체 서명된 것일 수도 있고 CA(인증 기관)에서 생성된 것일 수도 있습니다.

도메인에 대한 보안 통신을 구성하는 경우 다음 구성 요소 간의 연결을 보호합니다.

- 도메인에서 실행되는 모든 서비스와 서비스 관리자
- 데이터 통합 서비스와 모델 리포지토리 서비스
- 데이터 통합 서비스와 워크플로우 프로세스
- PowerCenter 통합 서비스와 PowerCenter 리포지토리 서비스
- 도메인 서비스, Informatica 클라이언트 도구 및 명령줄 프로그램

도메인 내의 보안 통신을 위한 요구 사항

도메인 내에서 보안 통신을 활성화하기 전에 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. 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.

설치 중에 보안 통신을 활성화하는 경우 키 저장소와 트러스트 저장소가 설치 프로그램에서 액세스할 수 있는 디렉터리에 있어야 합니다.

설치 후에 보안 통신을 활성화하는 경우 키 저장소와 트러스트 저장소가 명령줄 프로그램에서 액세스할 수 있는 디렉터리에 있어야 합니다.

HSTS(HTTP Strict Transport Security) 응답 헤더를 적용했습니다.

MITM(man-in-the-middle: 가로채기) 보안 위협을 방지하기 위해 도메인에서 HSTS 응답 헤더를 활성화하도록 선택할 수 있습니다. HSTS 응답 헤더를 활성화하면 HTTPS로의 HTTP 리디렉션을 중지하고 보안 URL(HTTPS)에만 액세스하도록 할 수 있습니다.

중요: Informatica는 HTTP와 HTTPS 모두에서 실행되는 여러 애플리케이션과 서비스를 지원합니다. 이 옵션을 활성화하면 HTTP URL을 사용하여 응용 프로그램이나 서비스에 액세스할 수 없습니다.

이 옵션을 활성화하려면 `INFA_HSTS_HEADER_ENABLED` 환경 변수를 `true`로 설정하고 `infa_truststore`의 인증서와 Informatica Administrator 키 저장소를 브라우저로 가져옵니다.

기본 및 사용자 지정 트러스트 저장소 파일 사용 지침

설치 프로그램은 기본 `infa_truststore.jks` 및 키 저장소 파일을 각 노드의 `<Informatica 설치 디렉터리>/services/shared/security` 디렉터리에 배치합니다. 설치 및 개념 증명에 기본 트러스트 저장소를 사용할 수 있지만

기본 트러스트 저장소 및 키 저장소 파일은 제한된 보안을 제공합니다. 프로덕션에는 보안 통신 및 SAML 인증을 위해 사용자 지정 트러스트 저장소 및 키 저장소 파일을 사용하는 것이 좋습니다.

사용자 지정 트러스트 저장소 및 키 저장소 파일을 사용자 지정 디렉터리에 배치하십시오. 트러스트 저장소 파일 이름은 `infa_truststore.jks`여야 합니다.

기본 파일을 덮어쓰거나 삭제하거나 이동하지 마십시오. 기본 트러스트 저장소 및 `keyst.ore` 파일, 사용자 지정 트러스트 저장소 및 키 저장소 파일을 `<Informatica 설치 디렉터리>/services/shared/security` 디렉터리에 배치하지 마십시오.

새 인증서 및 개인 키에 대한 별칭을 생성하는 경우 기본 트러스트 저장소 및 키 저장소 파일에 사용되는 기본 "Informatica LLC" 이름을 사용하지 마십시오.

인증서 및 사용자 지정 트러스트 저장소/키 저장소 파일 생성 지침

Java `keytool` 키 및 인증서 관리 유틸리티를 사용하여 SSL 인증서 또는 CSR(인증서 서명 요청)은 물론, JKS 형식의 키 저장소 및 트러스트 저장소를 생성할 수도 있습니다.

`keytool`은 도메인 노드의 다음 디렉터리에서 사용할 수 있습니다.

```
<Informatica installation directory>\java\bin
```

도메인 노드를 AIX에서 실행하는 경우 IBM JDK와 함께 제공되는 `keytool`을 사용하여 SSL 인증서 또는 CSR(인증서 서명 요청)과 키 저장소 및 트러스트 저장소를 생성할 수 있습니다.

1. 인증서 파일을 Informatica 도메인 내 게이트웨이 노드의 로컬 폴더에 복사합니다.
2. 명령줄에서 노드의 `keytool` 유틸리티 위치로 이동합니다.
3. `keytool` 유틸리티를 실행하여 인증서를 가져옵니다.
4. 노드를 다시 시작하십시오.

다음 단계

사용자 지정 키 저장소와 트러스트 저장소를 생성하고 브라우저에서 인증서를 가져오는 방법에 대한 자세한 내용은 Informatica How-To Library 문서 "Informatica 도메인에서 보안 통신을 위해 키 저장소 및 트러스트 저장소 파일을 작성하는 방

법"(<https://docs.informatica.com/data-integration/shared-content-for-data-integration/h2l/how-to-create-keystore-and-truststore-files-for-secure-communication/abstract.html>)을 참조하십시오.

도메인을 보호한 후에 보안 도메인 작업을 위한 Informatica 클라이언트 응용 프로그램을 구성합니다.

명령줄에서 도메인에 대한 보안 통신 활성화

`infacmd` 및 `infasetup` 명령을 사용하여 도메인에 대한 보안 통신을 활성화합니다. 보안 통신을 활성화한 후 변경 내용을 적용하려면 도메인을 다시 시작해야 합니다.

SSL 인증서 파일을 사용하려면 `infasetup` 명령을 실행할 때 키 저장소 파일을 지정합니다.

명령줄에서 보안 도메인 통신을 구성하려면 다음 명령을 사용합니다.

```
infacmd isp UpdateDomainOptions
```

`UpdateDomainOptions` 명령을 사용하여 도메인에 대한 보안 통신 모드를 설정합니다.

```
infasetup UpdateGatewayNode
```

도메인의 게이트웨이 노드에서 서비스 관리자에 대해 보안 통신을 활성화하려면 `UpdateGatewayNode` 명령을 사용합니다. 도메인에 게이트웨이 노드가 여러 개 있으면 각 게이트웨이 노드에서 `UpdateGatewayNode` 명령을 실행합니다.

infasetup UpdateWorkerNode

도메인의 작업자 노드에서 서비스 관리자에 대해 보안 통신을 활성화하려면 **UpdateWorkerNode** 명령을 사용합니다. 도메인에 작업자 노드가 여러 개 있으면 각 작업자 노드에서 **UpdateWorkerNode** 명령을 실행합니다.

1. 보호하려는 도메인이 실행 중인지 확인합니다.
2. 도메인을 업데이트합니다.

필요한 옵션 및 인수를 사용하여 다음 명령을 실행합니다.

- Windows: `infacmd isp UpdateDomainOptions`
- UNIX: `infacmd.sh isp UpdateDomainOptions`

도메인에 대한 보안 통신을 구성하려면 **infacmd** 명령을 실행할 때 다음 옵션을 포함합니다.

옵션	인수	설명
-DomainOptions -do	option_name=value	다음 옵션을 설정하여 도메인에 대한 보안 통신을 구성합니다. TLSMode=True

3. 도메인을 종료합니다.
infasetup 명령을 실행하기 전에 도메인이 종료되어야 합니다.

4. 필요한 옵션 및 인수와 함께 **infasetup**을 실행합니다.

다음 명령을 입력합니다.

- Windows: `infasetup UpdateGatewayNode` 또는 `infasetup UpdateWorkerNode`
- UNIX: `infasetup.sh UpdateGatewayNode` 또는 `infasetup.sh UpdateWorkerNode`

노드에서 보안 통신을 구성하려면 다음 옵션과 함께 명령을 실행합니다.

옵션	인수	설명
-EnableTLS -tls	enable_tls	Informatica 도메인 서비스에 대해 보안 통신을 구성합니다.
-NodeKeystore -nk	node_keystore_directory	Informatica의 기본 SSL 인증서를 사용할 경우에는 선택 사항입니다. 사용자 자신의 SSL 인증서를 사용할 경우에는 필수 사항입니다. 키 저장소 파일이 포함된 디렉터리입니다. Informatica 도메인은 PEM 형식 및 Java 키 저장소(JKS) 파일 유형의 SSL 인증서를 필요로 합니다. 이 디렉터리에 PEM 및 JKS 형식의 키 저장소 파일이 포함되어 있어야 합니다. 키 저장소 파일의 이름은 <code>nfa_keystore.jks</code> 및 <code>infa_keystore.pem</code> 이어야 합니다. 동일한 키 저장소 파일을 여러 노드에 사용할 수 있습니다.
-NodeKeystorePass -nkp	node_keystore_password	Informatica의 기본 SSL 인증서를 사용할 경우에는 선택 사항입니다. 사용자 자신의 SSL 인증서를 사용할 경우에는 필수 사항입니다. <code>infa_keystore.jks</code> 파일의 암호입니다.

옵션	인수	설명
-NodeTruststore -nt	node_truststore_directory	Informatica의 기본 SSL 인증서를 사용할 경우에는 선택 사항입니다. 트러스트 저장소 파일이 포함된 디렉터리입니다. 동일한 트러스트 저장소 파일을 여러 노드에 사용할 수 있습니다.
-NodeTruststorePass -ntp	node_truststore_password	Informatica의 기본 SSL 인증서를 사용할 경우에는 선택 사항입니다. infa_truststore.jks 파일의 암호입니다.

5. 도메인의 각 노드에서 **infasetup** 명령을 실행합니다.

도메인에 게이트웨이 노드가 여러 개 있으면 각 게이트웨이 노드에서 **infasetup UpdateGatewayNode**를 실행합니다. 작업자 노드가 여러 개 있으면 각 작업자 노드에서 **infasetup UpdateWorkerNode**를 실행합니다. 도메인의 모든 노드에 대해 동일한 키 저장소 파일을 사용해야 합니다.

6. 도메인을 다시 시작합니다.

Administrator 도구에서 도메인에 대한 보안 통신 활성화

Administrator 도구를 사용하여 도메인에 대한 보안 통신을 활성화할 수 있습니다. **Administrator** 도구에서 보안 통신을 활성화할 때 노드를 업데이트하는 **infasetup** 명령도 실행해야 합니다.

Administrator 도구에서 보안 통신 옵션을 활성화할 때 각 노드에서 **Informatica** 구성 파일을 업데이트하는 **infasetup** 명령도 실행해야 합니다. 사용할 SSL 인증서 파일을 지정하려면 **infasetup** 명령을 실행할 때 키 저장소 파일을 지정합니다.

각 노드에서 **Informatica** 구성 파일을 업데이트하려면 다음 명령을 사용합니다.

infasetup UpdateGatewayNode

도메인의 게이트웨이 노드에서 서비스 관리자에 대해 보안 통신을 활성화하려면 **UpdateGatewayNode** 명령을 사용합니다. 도메인에 게이트웨이 노드가 여러 개 있으면 각 게이트웨이 노드에서 **UpdateGatewayNode** 명령을 실행합니다.

infasetup UpdateWorkerNode

도메인의 작업자 노드에서 서비스 관리자에 대해 보안 통신을 활성화하려면 **UpdateWorkerNode** 명령을 사용합니다. 도메인에 작업자 노드가 여러 개 있으면 각 작업자 노드에서 **UpdateWorkerNode** 명령을 실행합니다.

Administrator 도구에서 보안 도메인 통신을 활성화하려면 다음 단계를 수행합니다.

1. **Administrator** 도구에서 도메인을 선택합니다.
2. 콘텐츠 패널에서 **속성** 보기를 클릭합니다.
3. **일반 속성** 섹션으로 이동하고 **편집**을 클릭합니다.
4. **일반 속성 편집** 창에서 **보안 통신 활성화**를 선택합니다.
5. **확인**을 클릭합니다.
6. 도메인을 종료합니다.

infasetup 명령을 실행하기 전에 도메인이 종료되어야 합니다.

7. 필요한 옵션 및 인수와 함께 **infasetup**을 실행합니다.

다음 명령을 입력합니다.

- Windows: `infasetup UpdateGatewayNode` 또는 `infasetup UpdateWorkerNode`
- UNIX: `infasetup.sh UpdateGatewayNode` 또는 `infasetup.sh UpdateWorkerNode`

노드에서 보안 통신을 구성하려면 다음 옵션과 함께 명령을 실행합니다.

옵션	인수	설명
-EnableTLS -tls	enable_tls	Informatica 도메인 서비스에 대해 보안 통신을 구성합니다.
-NodeKeystore -nk	node_keystore_directory	Informatica의 기본 SSL 인증서를 사용할 경우에는 선택 사항입니다. 사용자 자신의 SSL 인증서를 사용할 경우에는 필수 사항입니다. 키 저장소 파일이 포함된 디렉터리입니다. Informatica 도메인은 PEM 형식 및 Java 키 저장소(JKS) 파일 유형의 SSL 인증서를 필요로 합니다. 이 디렉터리에 PEM 및 JKS 형식의 키 저장소 파일이 포함되어 있어야 합니다. 키 저장소 파일의 이름은 <code>nfa_keystore.jks</code> 및 <code>infa_keystore.pem</code> 이어야 합니다. 동일한 키 저장소 파일을 여러 노드에 사용할 수 있습니다.
-NodeKeystorePass -nkp	node_keystore_password	Informatica의 기본 SSL 인증서를 사용할 경우에는 선택 사항입니다. 사용자 자신의 SSL 인증서를 사용할 경우에는 필수 사항입니다. <code>infa_keystore.jks</code> 파일의 암호입니다.
-NodeTruststore -nt	node_truststore_directory	Informatica의 기본 SSL 인증서를 사용할 경우에는 선택 사항입니다. 트러스트 저장소 파일이 포함된 디렉터리입니다. 동일한 트러스트 저장소 파일을 여러 노드에 사용할 수 있습니다.
-NodeTruststorePass -ntp	node_truststore_password	Informatica의 기본 SSL 인증서를 사용할 경우에는 선택 사항입니다. <code>infa_truststore.jks</code> 파일의 암호입니다.

8. 도메인의 각 노드에서 `infasetup` 명령을 실행합니다.

도메인에 게이트웨이 노드가 여러 개 있으면 각 게이트웨이 노드에서 `infasetup UpdateGatewayNode`를 실행합니다. 작업자 노드가 여러 개 있으면 각 작업자 노드에서 `infasetup UpdateWorkerNode`를 실행합니다. 도메인의 모든 노드에 대해 동일한 키 저장소 파일을 사용해야 합니다.

9. 도메인을 다시 시작하십시오.

보안 도메인 작업을 위한 Informatica 클라이언트 응용 프로그램 구성

도메인 내에서 보안 통신을 활성화하면 도메인과 Informatica 클라이언트 응용 프로그램(예: Developer tool) 간의 연결도 보호됩니다. 환경 변수에서 도메인을 보호하는 데 사용하는 트러스트 저장소 파일의 위치와 암호를 지정해야 할 수 있습니다. 환경 변수는 도메인 내에서 서비스에 액세스하는 클라이언트 응용 프로그램을 호스팅하는 시스템에서 설정합니다.

Informatica 도메인을 보호하는 데 사용되는 SSL 인증서는 `infa_truststore.jks` 및 `infa_truststore.pem`이라는 트러스트 저장소 파일에 포함됩니다. 트러스트 저장소 파일은 각 클라이언트 호스트에서 사용할 수 있어야 합니다.

각 클라이언트 호스트에 다음의 환경 변수를 설정해야 할 수 있습니다.

INFA_TRUSTSTORE

이 변수는 `infa_truststore.jks` 및 `infa_truststore.pem` 트러스트 저장소 파일을 포함하는 디렉터리에 대해 설정합니다.

INFA_TRUSTSTORE_PASSWORD

이 변수는 트러스트 저장소의 암호에 대해 설정합니다. 이 암호는 암호화되어야 합니다. 명령줄 프로그램 `pmpasswd`를 사용하여 암호를 암호화하십시오.

Informatica는 도메인을 보호하는 데 사용할 수 있는 기본 트러스트 저장소 파일에 SSL 인증서를 제공합니다. Informatica 클라이언트를 설치할 경우 설치 프로그램에서 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` 파일이 기본 디렉터리에 있으면 `INFA_TRUSTSTORE` 또는 `INFA_TRUSTSTORE_PASSWORD` 환경 변수를 설정할 필요가 없습니다.

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 제공하는 경우 인증서를 `infa_truststore.jks` 및 `infa_truststore.pem`이라는 트러스트 저장소 파일로 가져온 다음 트러스트 저장소 파일을 각 클라이언트 호스트에 복사합니다. 파일의 위치와 트러스트 저장소 암호를 지정해야 합니다.

중요: 컴퓨팅 클러스터로 처리를 푸시하고 데이터 통합 서비스를 그리드에서 실행하는 경우 인증서를 한 번 가져온 후 그리드의 각 데이터 통합 서비스에 복사합니다. 인증서를 가져올 때마다 인증서 콘텐츠는 동일하지만 다른 16진수 값이 지정됩니다. 따라서 그리드에서 실행되는 동시 매핑이 초기화 오류로 인해 실패합니다.

기본 Informatica 트러스트 저장소 파일을 기본 디렉터리에서 사용자 고유의 트러스트 저장소 파일로 바꿉니다.

기본 `infa_truststore.jks` 및 `infa_truststore.pem` 트러스트 저장소 파일을 기본 Informatica 디렉터리에서 사용자 고유의 트러스트 저장소 파일로 바꾸는 경우 트러스트 저장소 암호를 반드시 지정해야 합니다. 트러스트 저장소 파일은 기본 트러스트 저장소 파일과 이름이 같아야 합니다.

기본 Informatica SSL 인증서를 사용하지만 트러스트 저장소 파일이 기본 Informatica 디렉터리에 없는 경우

기본 Informatica SSL 인증서를 사용하지만 기본 `infa_truststore.jks` 및 `infa_truststore.pem` 트러스트 저장소 파일이 기본 디렉터리에 없으면 파일의 위치와 트러스트 저장소 암호를 지정해야 합니다.

보안 도메인 구성 리포지토리 데이터베이스

Informatica 도메인 구성 리포지토리는 구성 정보 및 사용자 계정 권한 및 사용 권한을 저장합니다. Informatica 도메인을 작성할 때 도메인 구성 리포지토리를 작성해야 합니다.

SSL 프로토콜로 보호되는 데이터베이스에서 도메인 구성 리포지토리를 작성할 수 있습니다. SSL 프로토콜은 트러스트 저장소 파일에 저장된 SSL 인증서를 사용합니다. 보안 데이터베이스 액세스에 대한 액세스에는 데이터베이스에 대한 인증서가 포함된 트러스트 저장소가 필요합니다.

Informatica 서비스를 설치하고 도메인을 작성할 때 보안 도메인 구성 리포지토리 데이터베이스를 작성할 수 있습니다. 설치 중 보안 도메인 구성 리포지토리 구성에 대한 자세한 내용은 Informatica 설치 가이드를 참조하십시오.

설치 후 명령줄에서 보안 도메인 구성 리포지토리 데이터베이스를 구성할 수 있습니다.

참고: 설치한 다음 보안 도메인 구성 리포지토리 데이터베이스를 구성하기 전에 도메인에 대한 보안 통신을 활성화해야 합니다.

다음 데이터베이스에서 보안 도메인 구성 리포지토리를 작성할 수 있습니다.

- Oracle
- Microsoft SQL Server
- IBM DB2

보안 도메인 구성 리포지토리 데이터베이스 구성

설치 후 도메인 구성 리포지토리를 보안 데이터베이스로 변경할 수 있습니다. 도메인에 대한 보안 통신을 활성화한 경우에만 보안 도메인 구성 리포지토리 데이터베이스를 사용할 수 있습니다.

도메인 구성 리포지토리 데이터베이스를 변경하려면 도메인을 종료해야 합니다. **infasetup** 명령을 사용하여 도메인 구성 리포지토리 데이터베이스를 백업하고 보안 데이터베이스에서 복원합니다. 보안 데이터베이스에서 도메인 구성 리포지토리를 복원하는 경우 보안 데이터베이스에 보안 매개 변수를 지정합니다. 그런 다음 도메인 구성 리포지토리 정보를 사용하여 게이트웨이 노드를 업데이트합니다.

리포지토리 데이터베이스를 백업 및 복원하고 게이트웨이 노드를 업데이트하려면 다음 명령을 사용합니다.

infasetup BackupDomain

BackupDomain 옵션을 사용하여 도메인 구성 리포지토리 데이터베이스에서 데이터를 백업합니다.

infasetup RestoreDomain

RestoreDomain 옵션을 사용하여 도메인 구성 리포지토리 데이터를 보안 데이터베이스에 복원합니다.

infasetup UpdateGatewayNode

UpdateGatewayNode 옵션을 사용하여 도메인의 게이트웨이 노드에서 도메인 구성 리포지토리 설정을 업데이트합니다.

도메인 구성 리포지토리를 보안 데이터베이스로 변경하려면 다음 단계를 완료합니다.

1. 도메인에 대한 보안 통신이 활성화되었는지 확인합니다.

도메인 구성 리포지토리에 보안 데이터베이스를 사용할 수 있으려면 도메인이 안전해야 합니다.

2. 도메인을 종료합니다.

3. **infasetup BackupDomain** 명령을 실행하고 데이터베이스 연결 정보를 지정합니다.

BackupDomain 명령을 실행하는 경우 **infasetup**은 대부분의 도메인 구성 데이터베이스 테이블을 사용자가 지정하는 파일 이름에 백업합니다.

참고: Java 메모리 오류가 발생하면서 **infasetup** 백업 또는 복원 명령이 실패하는 경우 **infasetup**에 대해 사용 가능한 시스템 메모리를 늘립니다. 시스템 메모리를 늘리려면 **INFA_JAVA_CMD_OPTS** 환경 변수에서 **-Xmx** 값을 설정합니다.

4. 데이터베이스 백업 유틸리티를 사용하여 **infasetup** 명령이 백업하지 않는 추가 리포지토리 테이블을 수동으로 백업합니다.

다음 테이블의 콘텐츠를 백업합니다.

- ISP_RUN_LOG

5. 보안 데이터베이스에서 도메인 구성 리포지토리를 복원하려면 **infasetup RestoreDomain** 명령을 실행하고 데이터베이스 연결 정보를 지정합니다.

연결 정보 외에 보안 데이터베이스에 필요한 다음 옵션을 지정합니다.

옵션	인수	설명
-DatabaseTlsEnabled -dbtls	database_tls_enabled	필수. 도메인 구성 리포지토리가 복원되는 데이터베이스가 보안 데이터베이스인지 나타냅니다. 이 옵션을 True로 설정합니다.
- DatabaseTruststoreLocation -dbtl	database_truststore_location	필수. 데이터베이스의 SSL 인증서를 포함하는 트러스트 저장소 파일의 경로 및 파일 이름입니다.
- DatabaseTruststorePassword -dbtp	database_truststore_password	필수. 보안 데이터베이스에 대한 데이터베이스 트러스트 저장소 파일의 암호입니다.

연결 문자열에서 다음 보안 매개 변수를 포함시킵니다.

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.

기본값은 True입니다.

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.

- 데이터베이스 복원 유틸리티를 사용하여 수동으로 백업한 리포지토리 테이블을 복원합니다.
다음 테이블을 복원합니다.
 - ISP_RUN_LOG
- 보안 도메인 구성 리포지토리에 대한 정보를 사용하여 도메인에서 노드를 업데이트하려면 infasetup UpdateGatewayNode 명령을 실행하고 보안 데이터베이스 연결 정보를 지정합니다.

노드 옵션 외에 보안 데이터베이스에 필요한 다음 옵션을 지정합니다.

옵션	인수	설명
-DatabaseTlsEnabled -dbtls	database_tls_enabled	필수. 도메인 구성 리포지토리에 사용되는 데이터베이스가 보안 데이터베이스라는 것을 나타냅니다. 이 옵션을 True로 설정합니다.
- DatabaseConnectionString -cs	database_connection_string	필수. 보안 데이터베이스에 연결하기 위해 사용하는 연결 문자열입니다. 연결 문자열에 5 단계에서 infasetup RestoreDomain 명령을 실행했을 때 연결 문자열에 포함된 보안 매개 변수를 포함해야 합니다.
- DatabaseTruststorePassword -dbtp	database_truststore_password	필수. 보안 데이터베이스에 대한 데이터베이스 트러스트 저장소 파일의 암호입니다.

도메인에 게이트웨이 노드가 여러 개 있으면 각 게이트웨이 노드에서 infasetup UpdateGatewayNode를 실행합니다.

8. 도메인을 다시 시작하십시오.

보안 PowerCenter 리포지토리 데이터베이스

PowerCenter 리포지토리 서비스를 작성할 때 SSL 프로토콜로 보호되는 데이터베이스에서 연결된 PowerCenter 리포지토리를 작성할 수 있습니다.

PowerCenter 리포지토리 서비스는 원시 연결을 통해 PowerCenter 리포지토리 데이터베이스에 연결합니다.

보안 데이터베이스에서 PowerCenter 리포지토리를 작성할 때 데이터베이스 클라이언트 파일에 데이터베이스에 대한 보안 연결 정보가 포함되었는지 확인합니다. 예를 들어 보안 Oracle 데이터베이스에서 PowerCenter 리포지토리를 작성하는 경우 보안 연결 정보가 포함된 Oracle 데이터베이스 tnsnames.ora 및 sqlnet.ora 클라이언트 파일을 구성합니다.

보안 모델 리포지토리 데이터베이스

모델 리포지토리 서비스를 작성할 때 SSL 프로토콜로 보호되는 데이터베이스에서 관련된 모델 리포지토리를 작성할 수 있습니다.

모델 리포지토리 서비스는 JDBC 드라이버를 통해 모델 리포지토리 데이터베이스에 연결됩니다.

1. SSL 프로토콜로 보호되는 데이터베이스를 설정합니다.
2. Administrator 도구에서 모델 리포지토리 서비스를 작성합니다.
3. 새 모델 리포지토리 서비스 대화 상자에서 모델 리포지토리 서비스에 대한 일반 속성을 입력하고 다음을 클릭합니다.
4. 모델 리포지토리 서비스에 대한 데이터베이스 속성 및 JDBC 연결 문자열을 입력합니다.

보안 데이터베이스에 연결하려면 보안 JDBC 매개 변수 필드에 보안 데이터베이스 매개 변수를 입력합니다. Informatica는 보안 JDBC 매개 변수 필드 값을 중요한 데이터로 다루고 암호화된 매개 변수 문자열을 저장합니다.

다음 목록에는 보안 데이터베이스 매개 변수가 설명되어 있습니다.

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.

기본값은 True입니다.

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. 데이터베이스의 SSL 인증서를 포함하는 트러스트 저장소 파일의 경로 및 파일 이름입니다. 트러스트 저장소 파일에 대한 경로가 없는 경우 Informatica는 다음 기본 디렉터리에서 파일을 찾습니다. <InformaticaInstallationDirectory>/tomcat/bin

TrustStorePassword

필수. 보안 데이터베이스에 대한 트러스트 저장소 파일의 암호입니다.

참고: Informatica는 보안 JDBC 매개 변수를 JDBC 연결 문자열에 추가합니다. 보안 JDBC 매개 변수를 연결 문자열에 직접 포함시키는 경우 **보안 JDBC 매개 변수** 필드에 매개 변수를 입력하지 마십시오.

5. 연결을 테스트하여 보안 리포지토리 데이터베이스에 대한 연결이 유효한지 확인합니다.
6. 프로세스를 완료하여 모델 리포지토리 서비스를 작성합니다.

워크플로우 및 세션에 대한 보안 통신

기본적으로 도메인에 대한 보안 통신 옵션을 활성화하는 경우 Informatica는 데이터 통합 서비스 및 PowerCenter 통합 서비스와 DTM 프로세스 간의 연결을 보호합니다.

또한 그리드에서 PowerCenter 세션을 실행하는 경우 DTM 프로세스 간의 데이터 통신을 보호하기 위해 옵션을 활성화할 수 있습니다.

PowerCenter 세션에서 DTM 프로세스 간의 보안 데이터 통신을 활성화하려면 PowerCenter 통합 서비스에 대한 **데이터 암호화 활성화** 옵션을 선택합니다.

참고: PowerCenter 세션은 DTM 프로세스가 보안 모드에서 실행되는 경우 CPU 및 메모리가 더 많이 필요합니다. PowerCenter 세션의 DTM 프로세스 간 보안 데이터 통신을 활성화하기 전에 추가 로드를 위해 도메인 리소스가 충분한지 확인합니다.

PowerCenter DTM 프로세스에 대한 보안 통신 활성화

그리드에서 실행되는 PowerCenter 세션의 DTM 프로세스 간 연결을 보호하려면 PowerCenter 통합 서비스를 구성하여 DTM 프로세스의 데이터 암호화를 활성화합니다.

1. Administrator 도구의 탐색기에서 PowerCenter 통합 서비스를 선택합니다.
2. 콘텐츠 패널에서 속성 보기를 클릭합니다.
3. PowerCenter 통합 서비스 속성 섹션으로 이동하고 편집을 클릭합니다.
4. **PowerCenter 통합 서비스 속성 편집** 창에서 **데이터 암호화 활성화**를 선택합니다.
5. **확인**을 클릭합니다.

그리드에서 PowerCenter 세션을 실행하는 경우 DTM 프로세스는 다른 DTM 프로세스와 통신할 때 암호화된 데이터를 보냅니다.

웹 응용 프로그램 서비스에 대한 보안 연결

웹 응용 프로그램 서비스와 브라우저 간에 전송되는 데이터를 보호하려면 웹 응용 프로그램 서비스와 브라우저 간의 연결을 보호해야 합니다.

다음 연결을 보호할 수 있습니다.

Administrator 도구에 대한 연결

Administrator 도구와 브라우저 간의 연결을 보호할 수 있습니다.

웹 응용 프로그램 서비스에 대한 연결

다음 웹 응용 프로그램 서비스와 브라우저 간의 연결을 보호할 수 있습니다.

- 분석 서비스
- Metadata Manager 서비스
- REST 작업 힙 서비스
- Test Data Manager 서비스
- 웹 서비스 힙 콘솔 서비스

웹 응용 프로그램 서비스에 대한 보안 연결을 위한 요구 사항

웹 응용 프로그램 서비스에 대한 연결을 보호하기 전에 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. 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 액세스 가능한 디렉터리에 있습니다.

키 저장소가 Administrator 도구 및 명령줄 프로그램에서 액세스할 수 있는 디렉터리에 있어야 합니다.

Administrator 도구에 대한 보안 연결 활성화

설치 후 명령줄에서 Administrator 도구에 대한 보안 연결을 구성할 수 있습니다.

브라우저와 Informatica Administrator 서비스 간의 보안 연결에 대한 속성을 사용하여 도메인에서 게이트웨이 노드를 업데이트해야 합니다.

보안 연결 속성을 사용하여 게이트웨이 노드를 업데이트하려면 다음 명령을 실행합니다. `infasetup UpdateGatewayNode`

다음 옵션을 포함합니다.

옵션	인수	설명
-HttpsPort -hs	AdminConsole_https_port	Informatica Administrator 서비스에 대한 보안 연결에 사용할 포트 번호입니다.
-KeystoreFile -kf	AdminConsole_Keystore_File	Informatica Administrator 서비스에 대한 HTTPS 연결에 사용할 키 저장소 파일의 경로 및 파일 이름입니다.
-KeystorePass -kp	AdminConsole_Keystore_Password	키 저장소 파일의 암호입니다

도메인에 여러 게이트웨이 노드가 있는 경우 각 게이트웨이 노드에서 명령을 실행합니다.

Informatica 웹 응용 프로그램 서비스

웹 응용 프로그램 서비스를 작성하거나 구성할 때 웹 응용 프로그램 서비스에 대한 보안 연결을 구성합니다. 각 응용 프로그램 서비스에는 보안 HTTPS 연결에 대한 특정 속성이 포함됩니다.

Analyst 도구에 대한 보안

분석 서비스를 작성할 때 Analyst 도구에 대해 보안 HTTPS 속성을 구성할 수 있습니다.

브라우저와 분석 서비스 간의 연결을 보호하려면 다음 분석 서비스 속성을 구성합니다.

속성	설명
보안 통신 활성화	Analyst 도구와 분석 서비스 간의 보안 연결을 활성화하도록 선택합니다.
HTTPS 포트	TLS(Transport Layer Security) 프로토콜을 활성화할 때 Informatica Analyst 웹 응용 프로그램이 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 <i>changeit</i> 를 사용합니다.
SSL 프로토콜	이 필드는 비워 두는 것이 좋습니다. 활성화된 TLS 버전은 이 값에 따라 다릅니다. 필드를 비워 두면 사용할 수 있는 가장 높은 버전의 TLS가 활성화됩니다. 값을 입력하면 이전 버전의 TLS가 활성화될 수 있습니다. 이 동작은 환경에서 사용 중인 Java 버전에 따라 다릅니다. 자세한 내용은 Java 버전의 설명서를 참조하십시오.

REST 작업 협 서비스에 대한 보안

REST 작업 협 서비스를 사용하는 경우 REST 작업 협에 대한 보안 HTTPS 속성을 구성할 수 있습니다.

브라우저와 REST 작업 협 서비스 사이의 연결을 보호하려면 다음 REST 작업 협 서비스 속성을 구성합니다.

속성	설명
HTTP 포트	REST 작업 협 서비스가 HTTP 프로토콜을 사용하는 경우 서비스 프로세스에 대한 고유한 HTTP 포트 번호입니다. 기본값은 6555입니다.
HTTPS 포트	TLS(Transport Layer Security) 프로토콜을 활성화하는 경우 REST 작업 협 서비스가 실행되는 포트 번호입니다. HTTP 포트 번호와 다른 포트 번호를 사용하십시오.
TLS(Transport Layer Security) 설정	REST 작업 협 서비스와 REST 클라이언트 간의 보안 연결을 활성화하려면 선택합니다.
키 저장소 파일	디지털 인증서가 포함된 키 저장소 파일이 저장되는 디렉터리입니다.
키 저장소 암호	키 저장소 파일에 대한 일반 텍스트 암호입니다. 이 속성이 설정되지 않은 경우 REST 작업 협 서비스는 기본 암호를 사용합니다.
SSL 프로토콜	필드를 비워 두면 사용할 수 있는 가장 높은 버전의 TLS가 활성화됩니다. 활성화되는 TLS 버전은 이 값에 따라 달라집니다. 값을 입력하면 이전 버전의 TLS가 활성화될 수 있습니다. 이 동작은 환경에서 사용 중인 Java 버전에 따라 다릅니다. 자세한 내용은 Java 버전의 설명서를 참조하십시오.

웹 서비스 협 콘솔에 대한 보안

웹 서비스 협 서비스를 작성할 때 웹 서비스 협 콘솔에 대해 보안 HTTPS 속성을 구성할 수 있습니다.

브라우저와 웹 서비스 협 서비스 사이의 연결을 보호하려면 다음 웹 서비스 협 서비스 속성을 구성합니다.

속성	설명
URL 구성표	웹 서비스 협에 대해 구성하는 보안 프로토콜을 나타냅니다. - HTTP. HTTP에서만 웹 서비스 협을 실행합니다. - HTTPS. HTTPS에서만 웹 서비스 협을 실행합니다. - HTTP 및 HTTPS. HTTP 및 HTTPS 모드에서 웹 서비스 협을 실행합니다.
허브 포트 번호 (https)	HTTPS에서 웹 서비스 협에 대한 포트 번호입니다. 선택한 URL 구성표가 HTTPS를 포함하는 경우 나타납니다. HTTPS에서 웹 서비스 협을 실행하기로 선택하는 경우 필요합니다. 기본값은 7343입니다.

속성	설명
키 저장소 파일	HTTPS 연결에 필요한 키 및 인증서가 포함된 키 저장소 파일의 파일 이름 및 경로입니다.
키 저장소 암호	키 저장소 파일의 암호입니다 이 속성이 설정되지 않은 경우 웹 서비스 헉은 기본 암호 <i>changeit</i> 를 사용합니다.

Metadata Manager에 대한 보안

Metadata Manager 서비스를 작성할 때 Metadata Manager 웹 응용 프로그램에 대해 보안 HTTPS 속성을 구성할 수 있습니다.

브라우저와 Metadata Manager 서비스 간의 연결을 보호하려면 다음 Metadata Manager 서비스 속성을 구성합니다.

속성	설명
SSL(Secure Sockets Layer) 설정	Metadata Manager 웹 응용 프로그램에 대해 보안 연결을 구성함을 나타냅니다. 참고: 이 속성은 Metadata Manager 서비스를 작성할 때 표시됩니다. 기존 Metadata Manager 서비스에 대한 연결을 보호하려면 URL 구성표 구성 속성을 HTTPS로 설정하십시오.
포트 번호	Metadata Manager 응용 프로그램이 실행되는 포트 번호입니다. 기본값은 10250입니다.
키 저장소 파일	키 저장소 파일에는 Metadata Manager 웹 응용 프로그램에 대해 보안 연결을 구성할 경우에 필요한 키와 인증서가 포함되어 있습니다. 참고: Metadata Manager 서비스는 RSA 암호화를 사용합니다. 따라서 RSA 알고리즘으로 생성된 보안 인증서를 사용하는 것이 좋습니다.
키 저장소 암호	키 저장소 파일의 암호입니다.

Informatica 도메인의 암호화 그룹

Informatica 도메인이 Informatica 도메인 내의 연결을 암호화할 때 사용하는 암호화 그룹을 구성할 수 있습니다. Informatica 도메인에서 도메인 외부의 리소스를 대상으로 하는 연결은 암호화 그룹 구성의 영향을 받지 않습니다.

Informatica 도메인에 대한 보안 통신 또는 웹 응용 프로그램 서비스에 대한 보안 연결을 활성화하면 Informatica 도메인에서는 암호화 그룹을 사용하여 트래픽을 암호화합니다.

Informatica에서는 다음과 같은 목록에 기반하여 암호화 그룹의 유효 목록을 작성합니다.

차단 목록

Informatica 도메인에서 차단할 암호화 그룹의 목록입니다. 암호화 그룹을 차단 목록에 추가하면 Informatica 도메인은 해당 암호화 그룹을 유효 목록에서 제거합니다. 기본 목록에 있는 암호화 그룹을 차단 목록에 추가할 수 있습니다.

기본 목록

Informatica 도메인에서 기본적으로 지원하는 암호화 그룹 목록입니다. 허용 목록 또는 차단 목록을 구성하지 않으면 Informatica 도메인은 기본 목록을 유효 목록으로 사용합니다.

자세한 내용은 [“암호화 그룹 기본 목록” 페이지 89](#)을 참조하십시오.

허용 목록

Informatica 도메인이 지원할 암호화 그룹의 목록입니다. 암호화 그룹을 허용 목록에 추가하면 Informatica 도메인은 해당 암호화 그룹을 유효 목록에 추가합니다. 기본 목록에 있는 암호화 그룹은 허용 목록에 추가할 필요가 없습니다.

Informatica에서는 허용 목록의 암호화 그룹을 기본 목록에 추가하고 차단 목록에 있는 암호화 그룹을 기본 목록에서 제거하여 유효 목록을 작성합니다.

유효 목록에 대해 다음 지침을 고려하십시오.

- 웹 클라이언트에 대한 보안 연결을 위해 사용자 지정 유효 목록을 사용하려면 Informatica 도메인이 도메인 내에서 보안 통신을 사용해야 합니다. 도메인이 보안 통신을 사용하지 않으면 Informatica는 기본 목록을 유효 목록으로 사용합니다.
- 유효 목록은 Informatica 도메인 내의 연결만 제어합니다. 데이터 소스에 대한 연결에는 유효 목록이 사용되지 않습니다.
- 유효 목록에는 TLS v1.1 또는 1.2에서 지원하는 암호화 그룹이 하나 이상 포함되어야 합니다.
- 유효 목록은 Windows, Java Runtime Environment 및 OpenSSL에 대해 유효한 암호화 그룹이어야 합니다.

암호화 그룹 목록 작성

특정 암호화 그룹을 사용하도록 Informatica 도메인을 구성하려면 지원할 추가 암호화 그룹을 지정하는 허용 목록을 생성합니다. 차단할 암호화 그룹을 지정하는 차단 목록도 생성할 수 있습니다.

네트워크 보안 관리자와 협의하여 Informatica 도메인에 적합한 암호화 그룹을 결정하십시오.

암호화 그룹 목록은 쉼표로 구분된 목록이어야 합니다. 목록의 암호화 그룹에 대해 IANA(Internet Assigned Numbers Authority) 이름을 사용합니다. 또는 Java 정규식을 사용할 수 있습니다.

허용 목록과 차단 목록은 `infasetup`을 사용하여 구성할 수 있습니다. 목록을 명령줄 매개 변수에 직접 제공하거나, 쉼표로 구분된 목록이 포함된 일반 텍스트 파일을 지정할 수 있습니다.

다음 샘플 텍스트는 암호화 그룹 두 개가 포함된 목록을 보여 줍니다.

```
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

Informatica 도메인을 작성할 때 해당 도메인의 암호화 그룹 허용 목록 및 차단 목록을 구성할 수 있습니다. `infasetup`을 사용하여 Informatica 도메인, 게이트웨이 노드 및 작업자 노드를 생성합니다. `infasetup` 명령에 대한 자세한 내용은 *Informatica 명령 참조*를 참조하십시오.

기존 Informatica 도메인의 허용 목록 및 차단 목록을 구성할 수도 있습니다.

암호화 그룹 기본 목록

기본적으로 Informatica 도메인은 도메인 내의 보안 통신 및 안전한 클라이언트 연결을 위해 다음과 같은 암호화 그룹을 사용합니다.

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256

새로운 암호화 그룹 유효 목록을 사용하여 Informatica 도메인 구성

Informatica 도메인에서 사용하는 암호화 그룹을 구성하려면 동일한 허용 목록과 차단 목록을 사용하여 Informatica 도메인, 모든 게이트웨이 노드 및 모든 작업자 노드를 업데이트해야 합니다.

참고: 차단 목록, 허용 목록 및 유효 목록에 대한 변경 내용은 누적되지 않습니다. Informatica에서는 사용자가 명령을 실행할 때 차단 목록, 기본 목록 및 허용 목록에 기반하여 새 유효 목록을 작성합니다. 새 유효 목록은 이전 목록을 덮어씁니다.

암호화 그룹의 새 유효 목록을 사용하여 기존 Informatica 도메인을 구성하려면 다음 단계를 수행하십시오.

1. Informatica 도메인을 종료합니다.

2. 필요한 경우 `infasetup listDomainCiphers` 명령을 실행하여 도메인 또는 노드에서 지원하거나 차단하는 암호화 그룹의 목록을 봅니다.

예를 들어 다음 명령을 실행하여 모든 암호화 그룹 목록을 봅니다.

```
infasetup listDomainCiphers -l ALL -dc true
```

3. 게이트웨이 노드에서 `infasetup updateDomainCiphers` 명령을 실행하고 허용 목록, 차단 목록 또는 둘 모두를 지정합니다.

예를 들어 다음 명령을 실행하여 유효 목록에 암호화 그룹 하나를 추가하고 유효 목록에서 암호화 그룹 두 개를 제거합니다.

```
infasetup updateDomainCiphers -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl  
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

4. 각 게이트웨이 노드에서 `infasetup updateGatewayNode` 명령을 실행하고 허용 목록, 차단 목록 또는 둘 모두를 지정합니다.

도메인에서 사용하는 것과 동일한 허용 목록 및 차단 목록을 사용합니다.

예를 들어 다음 명령을 실행합니다.

```
infasetup updateGatewayNode -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl  
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

5. Informatica 도메인에서 사용하는 것과 동일한 암호화 그룹 집합을 사용하여 각 작업자 노드를 업데이트합니다.

도메인에서 사용하는 것과 동일한 허용 목록 및 차단 목록을 사용합니다.

예를 들어 다음 명령을 실행합니다.

```
infasetup updateWorkerNode -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl  
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

6. Informatica 도메인을 시작합니다.

7. 필요한 경우 `infacmd isp listDomainCiphers` 명령을 실행하여 도메인 또는 노드에서 사용하는 암호화 그룹 목록을 봅니다.

예를 들어 다음 명령을 실행하여 도메인에서 사용하는 암호화 그룹 유효 목록을 봅니다.

```
infacmd isp listDomainCiphers -l EFFECTIVE
```

보안 소스 및 대상

Informatica는 관계형 데이터베이스에 연결하는 연결 개체를 소스 또는 대상으로 사용합니다. SSL 인증서로 보호되는 관계형 데이터베이스에 대한 연결 개체를 작성할 수 있습니다.

워크플로우 관리자에서 **PowerCenter** 연결 개체를 작성합니다. **Developer tool** 또는 **Administrator** 도구에서 데이터 서비스, **Data Quality** 또는 프로파일링 연결을 작성합니다.

다음 데이터베이스의 소스 또는 대상을 보호하기 위한 연결을 작성할 수 있습니다.

- Oracle
- Microsoft SQL Server
- IBM DB2

데이터 통합 서비스 소스 및 대상

데이터 통합 서비스에 대한 연결 개체를 작성하여 매핑, 데이터 프로필, 성과 기록표 또는 **SQL** 데이터 서비스를 처리하는 경우 **SSL** 프로토콜로 보호되는 데이터베이스에 대한 연결을 정의할 수 있습니다.

데이터 통합 서비스는 **JDBC** 드라이버를 통해 소스 또는 대상 데이터베이스에 연결됩니다. 보안 리포지토리 데이터베이스에 대한 연결을 구성하는 경우 **JDBC** 연결 문자열에 보안 연결 매개 변수를 포함해야 합니다.

1. 소스 또는 대상으로 사용할 **SSL** 프로토콜로 보호되는 데이터베이스를 설정합니다.
2. **Administrator** 도구에서 연결을 작성합니다.
3. **새 연결** 대화 상자에서 연결 유형을 선택하고 **확인**을 클릭합니다.

보안 DB2, Microsoft SQL Server 또는 Oracle 데이터베이스에 대한 연결을 작성할 수 있습니다.

4. **새 연결 - 1/3단계** 대화 상자에서 연결에 대한 속성을 입력하고 **다음**을 클릭합니다.
5. **새 연결 - 2/3단계** 페이지에서 데이터베이스에 대한 연결 문자열을 입력합니다.

보안 데이터베이스에 연결하려면 **고급 JDBC 보안 옵션** 필드에 보안 데이터베이스 매개 변수를 입력합니다. Informatica는 **고급 JDBC 보안 옵션** 필드 값을 중요한 데이터로 다루고 암호화된 매개 변수 문자열을 저장합니다.

다음 목록에는 보안 데이터베이스 매개 변수가 설명되어 있습니다.

EncryptionMethod

필수 사항입니다. 네트워크를 통해 전송되는 경우 데이터가 암호화되었는지를 나타냅니다. 이 매개 변수는 **SSL**로 설정되어야 합니다.

ValidateServerCertificate

선택 사항입니다. Informatica가 데이터베이스 서버에서 보낸 인증서에 대해 유효성을 검사하는지 여부를 나타냅니다.

이 매개 변수를 **True**로 설정하면 데이터베이스 서버에서 보낸 인증서에 대해 Informatica에서 유효성을 검사합니다. **HostNameInCertificate** 매개 변수를 지정하면 Informatica에서 인증서의 호스트 이름에 대한 유효성도 검사합니다.

이 매개 변수를 **False**로 설정하면 데이터베이스 서버에서 보낸 인증서에 대해 Informatica에서 유효성을 검사하지 않습니다. Informatica에서 사용자가 지정한 트러스트 저장소 정보를 모두 무시합니다.

기본값은 **True**입니다.

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.

TrustStore

필수. 데이터베이스의 **SSL** 인증서를 포함하는 트러스트 저장소 파일의 경로 및 파일 이름입니다.

TrustStorePassword

필수. 보안 데이터베이스에 대한 트러스트 저장소 파일의 암호입니다.

참고: Informatica에서 보안 JDBC 매개 변수를 연결 문자열에 추가합니다. 보안 JDBC 매개 변수를 연결 문자열에 직접 포함시키는 경우 **고급 JDBC 보안 옵션** 필드에 매개 변수를 입력하지 마십시오.

6. 연결을 테스트하여 보안 데이터베이스에 대한 연결이 유효한지 확인합니다.
7. 프로세스를 완료하여 관계형 연결을 작성합니다.

PowerCenter 소스 및 대상

PowerCenter 세션에 대해 연결 개체를 작성할 때 SSL 프로토콜로 보호되는 데이터베이스에 대한 연결을 정의할 수 있습니다.

원시 연결 또는 ODBC 드라이버를 통해 관계형 PowerCenter 소스 및 대상에 연결할 수 있습니다.

원시 연결을 통해 보안 관계형 소스 또는 대상에 연결하는 경우 데이터베이스 클라이언트에 보안 데이터베이스에 대한 연결 정보가 포함되었는지 확인합니다. 예를 들어 보안 Oracle 데이터베이스에서 PowerCenter 대상에 연결하는 경우 보안 데이터베이스에 대한 연결 정보로 Oracle 데이터베이스 클라이언트 파일 *tnsnames.ora*를 구성합니다.

ODBC 드라이버를 통해 보안 관계형 소스 또는 대상에 연결하는 경우 데이터베이스 클라이언트에 보안 데이터베이스에 대한 연결 정보가 포함되고 ODBC 데이터 소스가 보안 데이터베이스에 대한 연결을 제대로 정의하는지 확인합니다.

보안 데이터 저장소

Informatica는 도메인 구성 리포지토리에 데이터를 저장하기 전에 암호 및 보안 연결 매개 변수와 같은 중요한 데이터를 암호화합니다. Informatica는 제공하는 키워드를 사용하여 중요한 데이터를 암호화하는 암호화 키를 작성합니다.

설치 중 도메인의 암호화 키를 생성하려면 사용할 설치 프로그램에 키워드를 제공해야 합니다. 도메인의 모든 노드는 동일한 암호화 키를 사용해야 합니다. 여러 노드에 설치할 경우, 설치 프로그램은 도메인의 모든 노드에 대해 동일한 암호화 키를 사용합니다. 설치 중 도메인의 암호화 키 생성에 대한 자세한 내용은 Informatica 설치 가이드를 참조하십시오.

설치 후 도메인의 암호화 키를 변경할 수 있습니다. 암호화 키를 생성하고 도메인의 암호화 키를 변경하는 **infasetup** 명령을 실행합니다. 도메인의 암호화 키를 변경한 다음 암호화된 데이터를 업데이트하려면 도메인의 리포지토리 콘텐츠를 업그레이드해야 합니다.

참고: 도메인 이름, 암호화 키의 키워드 및 암호화 키 파일을 안전한 위치에 보관해야 해야 합니다. 도메인 이름, 키워드 및 암호화 키는 도메인의 암호화 키를 변경하거나 리포지토리를 다른 도메인으로 이동할 때 필요합니다. 암호화 키 파일을 잃어 버린 경우 암호화 키를 다시 생성하려면 키워드가 필요합니다. 키워드 및 암호화 키를 잃어 버린 경우 도메인의 암호화 키를 변경하거나 다른 도메인으로 리포지토리를 이동할 수 없습니다.

UNIX에서 보안 디렉터리

Informatica를 설치할 때 설치 프로그램이 도메인 암호화 키 파일과 같이 제한된 액세스가 필요한 Informatica 파일을 저장할 디렉터리를 작성합니다. UNIX에서는 설치 프로그램이 해당 디렉터리 및 해당 디렉터리의 파일에 대해 다양한 사용 권한을 할당합니다.

기본적으로 설치 프로그램이 Informatica 설치 디렉터리 내에 다음 디렉터리를 작성하여 암호화 키를 저장합니다. <INFA_HOME>/isp/config/keys

/keys 디렉터리에는 노드에 대한 암호화 키 파일이 포함됩니다. Kerberos 인증을 사용하도록 도메인을 구성하는 경우 해당 디렉터리에 Kerberos 키 탭 파일도 포함됩니다.

설치 중 암호화 파일을 저장하는 다른 디렉터리를 지정할 수 있습니다. 설치 프로그램은 기본 디렉터리와 동일한 사용 권한을 지정된 디렉터리에 할당합니다.

/keys 디렉터리 및 디렉터리의 파일에는 다음 사용 권한이 있습니다.

디렉터리 사용 권한

디렉터리의 소유자는 디렉터리에 대해 `-wx` 사용 권한을 갖지만, `r` 사용 권한은 갖지 않습니다. 디렉터리의 소유자는 설치 프로그램을 실행하는 데 사용되는 사용자 계정입니다. 소유자 속해 있는 그룹 또한 디렉터리에 대해 `-wx` 사용 권한을 갖지만, `r` 사용 권한은 갖지 않습니다.

사용자 계정 *ediqa*가 디렉터리를 소유하며 *infaadmin* 그룹에 속해 있는 예를 들어 보겠습니다. *ediqa* 사용자 계정 및 *infaadmin* 그룹은 다음 사용 권한을 갖고 있습니다. `-wx-wx---`

ediqa 사용자 계정 및 *infaadmin* 그룹은 해당 디렉터리에서 파일에 쓰고 파일을 실행할 수 있습니다. 이 사용자 계정과 그룹은 디렉터리에 있는 파일의 목록을 표시할 수 없지만 이름을 사용하여 특정 파일을 나열할 수는 있습니다.

디렉터리에 있는 파일의 이름을 알고 있으면 해당 파일을 디렉터리에서 다른 위치로 복사할 수 있습니다. 파일의 이름을 알지 못하면 파일을 복사하기 전에 읽기 권한을 포함하도록 디렉터리에 대한 사용 권한을 변경해야 합니다. 명령 `chmod 730`을 사용하면 디렉터리 및 하위 디렉터리의 소유자에게 읽기 권한을 부여할 수 있습니다.

*siteKey*라는 암호화 키 파일을 도메인의 다른 노드에서 액세스할 수 있도록 하기 위해 이 파일을 임시 디렉터리로 복사해야 하는 경우를 예로 들어 보겠습니다. `<Informatica 설치 디렉터리>/isp/config` 디렉터리에서 `chmod 730` 명령을 실행하여 `rw-x-wx---` 사용 권한을 할당합니다. 그러면 암호화 키 파일을 `/keys` 하위 디렉터리에서 다른 디렉터리로 복사할 수 있습니다.

파일 복사를 완료한 후에 해당 디렉터리에 대한 사용 권한을 다시 쓰기 및 실행 사용 권한으로 변경하십시오. 명령 `chmod 330`을 사용하면 읽기 권한을 제거할 수 있습니다.

참고: `-R` 옵션을 사용하여 디렉터리에 대한 사용 권한과 파일에 대한 사용 권한을 함께 변경하지 마십시오. 디렉터리와 해당 디렉터리의 파일은 서로 다른 사용 권한을 갖고 있습니다.

파일 사용 권한

디렉터리에 있는 파일의 소유자는 해당 파일에 대해 `rw-x` 사용 권한을 갖습니다. 디렉터리에 있는 파일의 소유자는 설치 프로그램을 실행하는 데 사용되는 사용자 계정입니다. 소유자가 속해 있는 그룹 또한 디렉터리의 파일에 대해 `rw-x` 사용 권한을 갖습니다.

소유자 및 그룹은 파일에 대해 모든 권한을 가지며 디렉터리의 파일을 표시하거나 편집할 수 있습니다.

참고: 파일을 나열하거나 편집하려면 해당 파일의 이름을 알고 있어야 합니다.

명령줄에서 암호화 키 변경

설치 후 명령줄에서 도메인에 대한 암호화 키를 변경할 수 있습니다. 암호화 키를 변경하려면 도메인을 종료해야 합니다.

`infasetup` 명령을 사용하여 암호화 키를 생성하고 도메인을 구성하여 새 암호화 키를 사용합니다.

다음 `infasetup` 명령은 암호화 키를 생성하고 변경합니다.

`generateEncryptionKey`

이름이 *sitekey*인 파일에 암호화 키를 생성합니다. 암호화 키를 위해 지정된 디렉터리에 *sitekey*라는 파일이 있는 경우 Informatica는 파일 이름을 *siteKey_old*로 바꿉니다.

`migrateEncryptionKey`

Informatica 도메인에 중요한 데이터를 저장하는 데 사용되는 암호화 키를 변경합니다.

도메인의 암호화 키를 변경하려면 다음 단계를 완료합니다.

1. 도메인을 종료합니다.
2. 암호화 키를 변경하기 전에 도메인을 백업합니다.

암호화 키를 변경할 때 문제가 발생하는 경우 도메인을 복구할 수 있도록 도메인을 백업한 다음 `infasetup` 명령을 실행합니다.

3. 도메인의 암호화 키를 생성하려면 `infasetup generateEncryptionKey` 명령을 실행합니다.

암호화 키를 생성하려면 `encryptionKeyLocation` 옵션을 지정합니다.

옵션	인수	설명
<code>-encryptionKeyLocation</code> <code>-kl</code>	<code>encryption_key_location</code>	현재 암호화 키가 들어 있는 디렉터리입니다. 암호화 파일의 이름은 <i>sitekey</i> 입니다. Informatica에서 현재 <i>sitekey</i> 인 파일 이름을 <i>sitekey_old</i> 로 바꾸고 동일한 디렉터리에 이름이 <i>sitekey</i> 인 새 파일에 암호화 키를 생성합니다.

참고: 설치 프로그램에서 설치 및 업그레이드 중에 암호화 키가 생성됩니다. 암호화 파일 사이트 키를 생성할 때 키워드 및 도메인 이름 옵션은 필요하지 않습니다. 고유한 사이트 키의 복사본을 저장해야 합니다. 사이트 키를 분실하는 경우 사이트 키를 다시 생성할 수 없습니다. 고유한 사이트 키를 다른 사람과 공유하지 마십시오.

4. 도메인의 암호화 키를 변경하려면 `infasetup migrateEncryptionKey` 명령을 실행하고 이전 및 새 암호화 키의 위치를 지정합니다.

도메인의 암호화 키를 변경하는 데 필요한 다음 옵션을 지정합니다.

옵션	인수	설명
-LocationOfEncryptionKeys -loc	location_of_encryption_keys	<p>이름이 <i>siteKey_old</i>인 이전 암호화 키 파일 및 이름이 <i>siteKey</i>인 새 암호화 키 파일이 저장되는 디렉터리입니다.</p> <p>디렉터리에는 이전 및 새 암호화 키 파일이 포함되어 있어야 합니다. 이전 및 새 암호화 키 파일이 다른 디렉터리에 저장되는 경우 암호화 키 파일을 동일한 디렉터리에 복사합니다.</p> <p>도메인에 여러 노드가 있는 경우 이 디렉터리가 <code>migrateEncryptionKey</code> 명령을 실행하는 도메인의 노드에 액세스할 수 있어야 합니다.</p> <p>다중 노드 도메인을 마이그레이션하는 경우 도메인의 모든 노드에 동일한 암호화 키를 사용해야 합니다. 도메인의 암호화 키를 변경하려면 도메인의 모든 노드에서 <code>infasetup migrateEncryptionKey</code> 명령을 실행합니다.</p> <p>참고: UNIX에서는 파일 이름 <i>siteKey_old</i>의 대/소문자를 구분합니다. 이전 암호화 키 파일의 이름을 수동으로 바꾸는 경우 파일 이름의 대/소문자가 올바른지 확인합니다.</p>
-IsDomainMigrated -mig	is_domain_migrated	<p>도메인이 최신 암호화 키를 사용하도록 업데이트되었는지 여부를 나타냅니다.</p> <p>처음으로 <code>migrateEncryptionKey</code> 명령을 실행하는 경우 이 옵션을 <code>False</code>로 설정하면 도메인이 이전 암호화 키를 사용한다는 것을 나타냅니다.</p> <p>처음 실행 이후 <code>migrateEncryptionKey</code> 명령을 실행하여 도메인에서 다른 노드를 업데이트하는 경우 이 옵션을 <code>True</code>로 설정하면 도메인이 업데이트되어 최신 암호화 키를 사용한다는 것을 나타냅니다. 또는 이 옵션 없이 <code>migrateEncryptionKey</code> 명령을 실행할 수 있습니다.</p> <p>기본값은 <code>True</code>입니다.</p>

5. 도메인의 각 노드에서 `infasetup` 명령을 실행합니다.

도메인에 여러 노드가 있는 경우 각 노드에서 `infasetup migrateEncryptionKey`를 실행합니다. 작업자 노드에서 명령을 실행하기 전에 게이트웨이 노드에서 명령을 실행합니다. 처음으로 명령을 실행한 이후에는 `IsDomainMigrated` 옵션을 생략할 수 있습니다.

6. 도메인을 다시 시작합니다.

새 암호화 키로 리포지토리의 중요한 데이터를 업데이트하고 암호화하려면 도메인에서 모든 리포지토리 서비스를 업그레이드해야 합니다. 도메인을 업그레이드한 후 사이트 키도 마이그레이션해야 합니다.

7. 모든 모델 리포지토리 서비스, **PowerCenter** 리포지토리 서비스 및 **Metadata Manager** 서비스를 업그레이드합니다.

Administrator 도구 또는 명령 프롬프트에서 모델 리포지토리 서비스 및 PowerCenter 리포지토리 서비스를 업그레이드할 수 있습니다. Administrator 도구에서 Metadata Manager 서비스를 업그레이드할 수 있습니다.

참고: 업그레이드를 수행하려면 Metadata Manager 서비스가 비활성화되어 있어야 합니다.

Administrator 도구에서 서비스를 업그레이드하려면 헤더 영역에서 **관리 > 업그레이드**를 선택합니다. 여러 서비스를 선택하는 경우 Administrator 도구가 올바른 순서로 서비스를 업그레이드합니다.

명령 프롬프트에서 서비스를 업그레이드하려면 다음 명령을 사용합니다.

리포지토리 서비스 유형	명령
모델 리포지토리 서비스	infacmd mrs UpgradeContents
PowerCenter 리포지토리 서비스	pmrep Upgrade

응용 프로그램 서비스 및 포트

Informatica 도메인의 Informatica 도메인 서비스와 응용 프로그램 서비스에는 고유한 포트가 있습니다.

Informatica 도메인

다음 테이블에는 사용자가 설정할 수 있는 포트가 설명되어 있습니다.

포트	설명
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 HTTPS 포트	기본 포트는 없습니다. 서비스를 생성할 때 필수 포트 번호를 입력합니다. 이 포트를 0으로 설정하면 Administrator 도구에 대한 HTTPS 연결이 비활성화됩니다.
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.

분석 서비스

다음 테이블에는 분석 서비스에 연결된 기본 포트가 나열되어 있습니다.

유형	기본 포트
분석 서비스(HTTP)	8085
분석 서비스(HTTPS)	기본 포트는 없습니다. 서비스를 생성할 때 필수 포트 번호를 입력합니다.

콘텐츠 관리 서비스

다음 테이블에는 콘텐츠 관리 서비스에 연결된 기본 포트가 나열되어 있습니다.

유형	기본 포트
콘텐츠 관리 서비스(HTTP)	8105
콘텐츠 관리 서비스(HTTPS)	기본 포트는 없습니다. 서비스를 생성할 때 필수 포트 번호를 입력합니다.

데이터 통합 서비스

다음 표에는 데이터 통합 서비스에 연결된 기본 포트가 나열되어 있습니다.

유형	기본 포트
데이터 통합 서비스(HTTP 프록시)	8080
데이터 통합 서비스(HTTP)	8095
데이터 통합 서비스(HTTPS)	기본 포트는 없습니다. 서비스를 생성할 때 필수 포트 번호를 입력합니다.
프로파일링 웨어하우스 데이터베이스	기본 포트는 없습니다. 데이터베이스 포트 번호를 입력합니다.

메타데이터 액세스 서비스

다음 테이블에는 메타데이터 액세스 서비스에 연결된 기본 포트가 나열되어 있습니다.

유형	기본 포트
메타데이터 액세스 서비스(HTTP)	7080 메타데이터 액세스 서비스는 연속 포트 번호를 사용하여 여러 Hadoop 배포에 연결합니다.
메타데이터 액세스 서비스(HTTPS)	기본 포트는 없습니다. 서비스를 생성할 때 필수 포트 번호를 입력합니다. 메타데이터 액세스 서비스는 연속 포트 번호를 사용하여 여러 Hadoop 배포에 연결합니다.

Metadata Manager 서비스

다음 테이블에는 Metadata Manager 서비스에 연결된 기본 포트가 나열되어 있습니다.

유형	기본 포트
Metadata Manager 서비스(HTTP)	10250
Metadata Manager 서비스(HTTPS)	기본 포트는 없습니다. 서비스를 생성할 때 필수 포트 번호를 입력합니다.

PowerExchange® Listener 서비스

DBMOVER 파일의 SVCNODE 문에서 지정하는 동일한 포트 번호를 사용하십시오.

노드에서 실행할 둘 이상의 수신기 서비스를 정의하는 경우 각 서비스에 대해 고유한 SVCNODE 포트 번호를 정의해야 합니다.

PowerExchange Logger 서비스

DBMOVER 파일의 SVCNODE 문에서 지정하는 동일한 포트 번호를 사용하십시오.

노드에서 실행할 둘 이상의 수신기 서비스를 정의하는 경우 각 서비스에 대해 고유한 SVCNODE 포트 번호를 정의해야 합니다.

웹 서비스 협 서비스

다음 테이블에는 웹 서비스 협 서비스에 연결된 기본 포트가 나열되어 있습니다.

유형	기본 포트
웹 서비스 협 서비스(HTTP)	7333
웹 서비스 협 서비스(HTTPS)	7343

제 7 장

Informatica Administrator에서 보안 관리

이 장에 포함된 항목:

- [Informatica Administrator 사용 개요, 100](#)
- [사용자 보안, 101](#)
- [보안 탭, 103](#)
- [암호 관리, 106](#)
- [도메인 보안 관리, 107](#)
- [사용자 보안 관리, 108](#)

Informatica Administrator 사용 개요

Informatica Administrator는 Informatica 도메인 및 Informatica 보안을 관리하는 데 사용할 수 있는 도구입니다.

Administrator 도구를 통해 다음과 같은 유형의 작업을 완료합니다.

- **도메인 관리 작업.** 로그, 도메인 개체, 사용자 사용 권한 및 도메인 보고서를 관리합니다. 노드 진단을 생성하고 업로드합니다. 데이터 통합 서비스 작업 및 응용 프로그램을 모니터링합니다. 도메인 개체에는 응용 프로그램 서비스, 노드, 그리드, 폴더, 데이터베이스 연결, 운영 체제 프로파일 및 라이선스가 포함됩니다.
- **보안 관리 작업.** 사용자, 그룹, 역할 및 사용 권한을 관리합니다.

Administrator 도구에는 다음과 같은 탭이 포함됩니다.

- **관리.** 도메인과 도메인 내 개체의 속성을 보고 편집합니다.
- **모니터링.** 각 데이터 통합 서비스에 대한 프로파일 작업, 성과 기록표 작업, 미리보기 작업, 매핑 작업, SQL 데이터 서비스, 웹 서비스 및 워크플로우의 상태를 봅니다.
- **모니터링.** 각 데이터 통합 서비스에 대한 프로파일 작업, 미리보기 작업, 매핑 작업, SQL 데이터 서비스 및 웹 서비스의 상태를 봅니다.
- **로그.** 도메인 및 도메인 내 서비스에 대한 로그 이벤트를 봅니다.
- **보고서.** 웹 서비스 보고서 또는 라이선스 관리 보고서를 실행합니다.
- **보안.** 사용자, 그룹, 역할 및 사용 권한을 관리합니다.
- **클라우드.** Informatica Cloud® 조직에 대한 정보를 봅니다.

Administrator 도구에는 다음과 같은 헤더 항목이 있습니다.

- **로그아웃.** Administrator 도구에서 로그아웃합니다.
- **관리.** 계정을 관리합니다.
- **도움말.** 현재 탭에 대한 도움말에 액세스하고 Informatica 버전을 확인합니다.

사용자 보안

서비스 관리자 및 일부 응용 프로그램 서비스는 응용 프로그램 클라이언트에서 사용자 보안을 제어합니다. 응용 프로그램 클라이언트에는 Informatica Administrator, Informatica Analyst, Informatica Developer, Metadata Manager 및 PowerCenter 클라이언트가 포함되어 있습니다.

서비스 관리자 및 응용 프로그램 서비스는 다음 기능을 수행하여 사용자 보안을 제어합니다.

암호화

응용 프로그램 클라이언트에 로그인하는 경우 서비스 관리자는 암호를 암호화합니다.

인증

응용 프로그램 클라이언트에 로그인하는 경우 서비스 관리자는 사용자 이름 및 암호 또는 사용자 인증 토큰에 따라 사용자 계정을 인증합니다.

권한 부여

응용 프로그램 클라이언트에서 개체를 요청하는 경우 서비스 관리자 및 일부 응용 프로그램 서비스는 권한, 역할, 사용 권한에 따라 요청을 권한 부여합니다.

또한 도메인 및 응용 프로그램 서비스에 대한 보안 연결을 위해 HTTPS를 사용할 수 있습니다. 다음 응용 프로그램 서비스는 Informatica 도메인에서 HTTPS 연결을 제공합니다.

- 데이터 통합 서비스
- 분석 서비스
- 콘텐츠 관리 서비스
- 메타데이터 액세스 서비스
- Metadata Manager 서비스
- 웹 서비스 헵 서비스

암호화

Informatica는 응용 프로그램 클라이언트에서 서비스 관리자로 보낸 암호를 암호화합니다. Informatica는 다양한 128비트 키를 사용하는 AES 암호화를 사용하여 암호를 암호화하고 도메인 구성 데이터베이스에 암호화된 암호를 저장합니다. 응용 프로그램 클라이언트에서 서비스 관리자로 보낸 암호를 암호화하도록 HTTPS를 구성합니다.

인증

서비스 관리자는 응용 프로그램 클라이언트에 로그인하는 사용자를 인증합니다.

응용 프로그램 클라이언트에 처음 로그인할 때 사용자 이름, 암호 및 보안 도메인을 입력합니다. 보안 도메인은 Informatica 도메인의 사용자 계정 및 그룹 컬렉션입니다.

선택하는 보안 도메인에 따라 서비스 관리자가 사용자 계정을 인증하기 위해 사용하는 인증 방법이 결정됩니다.

- 원시. 원시 사용자로 응용 프로그램 클라이언트에 로그인하는 경우 서비스 관리자는 사용자 이름 및 암호를 도메인 구성 데이터베이스의 사용자 계정에 대해 인증합니다.
- LDAP(Lightweight Directory Access Protocol). LDAP 사용자로 응용 프로그램 클라이언트에 로그인하는 경우 서비스 관리자는 인증을 위해 사용자 이름 및 암호를 외부 LDAP 디렉터리 서비스에 전달합니다.

Single Sign-On

응용 프로그램 클라이언트에 로그인한 다음 서비스 관리자를 통해 다른 응용 프로그램 클라이언트를 시작하거나 응용 프로그램 클라이언트에서 여러 리포지토리에 액세스할 수 있습니다. 추가 응용 프로그램 클라이언트 또는 리포지토리에 로그인하지 않아도 됩니다.

처음으로 서비스 관리자가 사용자 계정을 인증할 때 계정에 대해 암호화된 인증 토큰을 작성하고 인증 토큰을 응용 프로그램 클라이언트로 반환합니다. 인증 토큰에는 사용자 이름, 보안 도메인 및 만료 시간이 포함되어 있습니다. 서비스 관리자는 만료 시간 전에 정기적으로 인증 토큰을 갱신합니다.

응용 프로그램 클라이언트에서 여러 리포지토리에 액세스하는 경우 응용 프로그램 클라이언트는 사용자 인증을 위해 인증 토큰을 서비스 관리자에게 보냅니다.

한 웹 응용 프로그램 클라이언트에서 다른 웹 응용 프로그램 클라이언트를 시작하는 경우 해당 응용 프로그램 클라이언트가 인증 토큰을 다음 응용 프로그램 클라이언트로 전달합니다. 다음 웹 응용 프로그램 클라이언트는 사용자 인증을 위해 인증 토큰을 서비스 관리자에게 보냅니다. 각 웹 응용 프로그램 클라이언트에서 별도로 로그아웃해야 합니다. 예를 들어 Administrator 도구에서 Analyst 도구를 여는 경우 Analyst 도구와 Administrator 도구에서 별도로 로그아웃해야 합니다.

참고: Administrator 도구, Analyst 도구 및 모니터링 도구 간에 Single Sign-On을 사용하려면 정규화된 도메인 이름을 모든 노드의 호스트 파일에 추가해야 합니다.

Single Sign-On을 사용하여 클라이언트 도구에서 웹 응용 프로그램 클라이언트에 연결할 수 없습니다. 예를 들어 Developer tool에서 Administrator 도구를 실행하는 경우 Administrator 도구에 로그인해야 합니다.

권한 부여

서비스 관리자가 도메인 개체에 대한 사용자 요청을 권한 부여합니다. 요청은 Administrator 도구에서 발생할 수 있습니다. 다음 응용 프로그램 서비스는 다른 개체에 대한 사용자 요청을 권한 부여합니다.

- 데이터 통합 서비스
- Metadata Manager 서비스
- 모델 리포지토리 서비스
- PowerCenter 리포지토리 서비스

원시 사용자 및 그룹을 작성하거나 LDAP 사용자 및 그룹을 가져오는 경우 서비스 관리자는 도메인 구성 데이터베이스의 정보를 다음 리포지토리에 저장합니다.

- 모델 리포지토리
- PowerCenter 리포지토리
- Metadata Manager의 PowerCenter 리포지토리

서비스 관리자는 다음 이벤트가 발생할 때 리포지토리와 도메인 구성 데이터베이스 간의 사용자 및 그룹 정보를 동기화합니다.

- Metadata Manager 서비스, 모델 리포지토리 서비스 또는 PowerCenter 리포지토리 서비스를 다시 시작합니다.
- 원시 사용자 또는 그룹을 추가 또는 제거합니다.

- 서비스 관리자가 도메인 구성 데이터베이스의 LDAP 사용자 및 그룹 목록을 LDAP 디렉터리 서비스의 사용자 및 그룹 목록과 동기화합니다.

응용 프로그램 클라이언트에서 사용자 및 그룹에 사용 권한을 할당하면 응용 프로그램 서비스는 사용자 및 그룹 정보와 함께 사용 권한 할당을 적절한 리포지토리에 저장합니다.

응용 프로그램 클라이언트에서 개체를 요청하면 적절한 응용 프로그램 서비스가 요청을 권한 부여합니다. 예를 들어 Informatica Developer에서 프로젝트를 편집하는 경우 모델 리포지토리 서비스가 권한, 역할 및 사용 권한 할당에 따라 요청을 권한 부여합니다.

보안 탭

Administrator 도구의 보안 탭에서 Informatica 보안을 관리합니다.

보안 탭에는 다음 구성 요소가 포함됩니다.

- 검색 섹션. 이름으로 사용자, 그룹 또는 역할을 검색합니다.
- Navigator. 탐색기는 왼쪽 창에 나타나고 그룹, 사용자 및 역할을 표시합니다.
- 콘텐츠 패널. 콘텐츠 패널에는 탐색기에서 선택한 개체와 콘텐츠 패널에서 선택한 탭에 따라 속성 및 옵션이 표시됩니다.
- 보안 작업 메뉴. 그룹, 사용자 또는 역할을 작성하거나 삭제하는 옵션을 포함합니다. LDAP 구성 및 운영 체제 프로필을 관리할 수 있습니다. 또한 서비스에 대한 권한이 있는 사용자를 볼 수 있습니다.

검색 섹션 사용

검색 섹션을 사용하여 이름으로 사용자, 그룹 및 역할을 검색합니다. 검색은 대/소문자를 구분하지 않습니다.

1. 검색 섹션에서 사용자, 그룹 또는 역할을 검색할지 여부를 선택합니다.
2. 검색할 이름 전체 또는 일부를 입력합니다.

이름에 별표(*)를 포함시켜 검색에서 와일드카드 문자로 사용할 수 있습니다. 예를 들어 “ad”로 시작하는 모든 개체를 검색하려면 “ad*”를 입력합니다. “ad”로 끝나는 모든 개체를 검색하려면 “*ad”를 입력합니다.

3. 실행을 클릭합니다.

검색 결과 섹션이 나타나고 최대 100개의 개체가 표시됩니다. 검색에서 100개가 넘는 개체가 반환되는 경우 더 구체적인 검색 조건을 지정하여 검색 결과를 줄이십시오.

4. 검색 결과 섹션에서 개체를 선택하면 해당 개체에 대한 정보가 콘텐츠 패널에 표시됩니다.

보안 탐색기 사용

보안 탭의 콘텐츠 패널에 탐색기가 나타납니다. 탐색기에서 개체를 선택하면 콘텐츠 패널에 개체에 대한 정보가 표시됩니다.

보안 탭의 탐색기에는 사용자가 보고 있는 내용에 따라 다음 섹션 중 하나가 표시됩니다.

- 그룹 섹션. 그룹의 속성, 그룹에 할당된 사용자와 그룹에 할당된 역할 및 권한을 보려면 그룹을 선택합니다.
- 사용자 섹션. 사용자의 속성, 사용자가 속한 그룹과 사용자에게 할당된 역할 및 권한을 보려면 사용자를 선택합니다.
- 역할 섹션. 역할의 속성, 역할이 할당된 사용자 및 그룹, 역할에 할당된 권한을 보려면 역할을 선택합니다.

- 운영 프로필 섹션. 운영 체제 프로필의 속성과 운영 체제 프로필을 사용하는 사용자 및 그룹에 할당된 사용 권한을 보려면 운영 프로필을 선택합니다.
- LDAP 구성 섹션. LDAP 서버 연결 세부 정보, LDAP 디렉터리 서비스에서 가져온 사용자와 그룹이 포함된 LDAP 보안 도메인 및 LDAP 동기화 일정을 보려면 구성을 선택합니다.

탐색기에서 다양한 방법으로 태스크를 완료할 수 있습니다. 다음 방법 중 하나를 사용하여 그룹, 사용자 및 역할을 관리할 수 있습니다.

- **작업** 메뉴를 클릭합니다. 탐색기의 각 섹션에는 그룹, 사용자, 역할, 운영 체제 프로필 또는 LDAP 구성을 관리하기 위한 작업 메뉴가 포함되어 있습니다.
- 마우스 오른쪽 단추로 개체 클릭. 탐색기에서 개체를 마우스 오른쪽 단추로 클릭하면 작업 메뉴에서 사용할 수 있는 옵션이 표시됩니다.
- 키보드 바로 가기를 사용합니다. 탐색기의 여러 섹션으로 이동하려면 키보드 단축키를 사용합니다.

그룹

그룹은 동일한 권한, 역할 및 사용 권한을 가질 수 있는 사용자 및 그룹의 컬렉션입니다.

탐색기의 그룹 섹션에서 그룹은 보안 도메인 폴더를 구성합니다. 보안 도메인은 **Informatica** 도메인의 사용자 계정 및 그룹 컬렉션입니다. 원시 인증에서는 **Administrator** 도구에서 생성하고 관리하는 사용자 및 그룹이 포함된 원시 보안 도메인을 사용합니다. LDAP 인증에서는 LDAP 디렉터리 서비스에서 가져온 사용자 및 그룹이 포함된 LDAP 보안 도메인을 사용합니다.

탐색기의 그룹 섹션에서 보안 도메인 폴더를 선택하면 콘텐츠 패널에 해당 보안 도메인에 속한 모든 그룹이 표시됩니다.

탐색기에서 그룹을 선택하면 콘텐츠 패널에 다음과 같은 탭이 표시됩니다.

- 개요. 그룹의 일반 속성과 그룹에 할당된 사용자를 표시합니다.
- 권한. 도메인 및 도메인의 응용 프로그램 서비스에 대해 그룹에 할당된 권한과 역할을 표시합니다.
- 사용 권한. 그룹 내의 사용자가 노드, 그리드 및 응용 프로그램 서비스를 포함하여 도메인 개체에 대해 태스크를 수행할 수 있는 액세스 수준을 표시합니다. 또한 그룹 내의 사용자가 연결 개체 및 운영 체제 프로필에 대해 태스크를 수행해야 하는 액세스 수준도 표시합니다.

사용자

Informatica 도메인의 계정이 있는 사용자는 다음 응용 프로그램 클라이언트에 로그인할 수 있습니다.

- Informatica Administrator
- PowerCenter 클라이언트
- Informatica Developer
- Informatica Analyst
- Metadata Manager

탐색기의 사용자 섹션에서 사용자는 보안 도메인 폴더를 구성합니다. 보안 도메인은 **Informatica** 도메인의 사용자 계정 및 그룹 컬렉션입니다. 원시 인증에서는 **Administrator** 도구에서 생성하고 관리하는 사용자 및 그룹이 포함된 원시 보안 도메인을 사용합니다. LDAP 인증에서는 LDAP 디렉터리 서비스에서 가져온 사용자 및 그룹이 포함된 LDAP 보안 도메인을 사용합니다.

탐색기의 사용자 섹션에서 보안 도메인 폴더를 선택하면 콘텐츠 패널에 해당 보안 도메인에 속한 모든 사용자가 표시됩니다.

탐색기에서 사용자를 선택하면 콘텐츠 패널에 다음과 같은 탭이 표시됩니다.

- 개요. 사용자의 일반 속성과 사용자가 속한 모든 그룹을 표시합니다.
- 권한. 도메인 및 도메인의 응용 프로그램 서비스에 대해 사용자에게 할당된 권한과 역할을 표시합니다.
- 사용 권한. 사용자가 노드, 그리드 및 응용 프로그램 서비스를 포함하여 도메인 개체에 대해 태스크를 수행할 수 있는 액세스 수준을 표시합니다. 또한 사용자가 연결 개체 및 운영 체제 프로필에 대해 태스크를 수행해야 하는 액세스 수준도 표시합니다.

역할

역할은 사용자 또는 그룹에 할당한 권한의 컬렉션입니다. 권한은 사용자가 수행할 수 있는 작업을 결정합니다. 역할을 도메인 및 도메인의 응용 프로그램 서비스에 대한 사용자 및 그룹에 할당합니다.

탐색기의 역할 섹션에서 역할은 다음과 같은 폴더로 구성됩니다.

- 시스템 정의 역할. 편집하거나 삭제할 수 없는 역할을 포함합니다. 관리자 역할은 시스템 정의 역할입니다.
- 사용자 지정 역할. 작성하고, 편집하고, 삭제할 수 있는 역할을 포함합니다. Administrator 도구는 직접 편집하고 사용자 및 그룹에 할당할 수 있는 몇 가지 사용자 지정 역할을 포함합니다.

탐색기의 역할 섹션에서 폴더를 선택하면 콘텐츠 패널에 해당 폴더에 속한 모든 역할이 표시됩니다.

탐색기에서 역할을 선택하면 콘텐츠 패널에 다음과 같은 탭이 표시됩니다.

- 개요. 역할의 일반 속성과 도메인 및 응용 프로그램 서비스에 대해 할당된 역할이 있는 사용자 및 그룹을 표시합니다.
- 권한. 도메인 및 응용 프로그램 서비스에 대해 역할에 할당된 권한을 표시합니다.

운영 체제 프로필

운영 체제 프로필은 데이터 통합 서비스 및 PowerCenter 통합 서비스가 매핑, 워크플로우 및 프로파일링 작업을 실행할 때 사용하는 보안 메커니즘입니다.

탐색기의 운영 체제 프로필 섹션에는 도메인에 구성된 운영 체제 프로필이 나열됩니다.

탐색기에서 운영 체제 프로필을 선택하면 콘텐츠 패널에 다음과 같은 탭이 표시됩니다.

- 속성. 데이터 통합 서비스, PowerCenter 통합 서비스 또는 이 두 응용 프로그램 서비스에 대해 구성된 운영 체제 프로필의 일반 속성을 표시합니다.
- 사용 권한. 운영 체제 프로필을 사용하는 사용자 및 그룹에 할당된 사용 권한을 표시합니다. 운영 체제 프로필이 사용자 또는 그룹에 할당된 기본 프로필인지 여부도 표시됩니다.

LDAP 구성

하나 이상의 LDAP 디렉터리 서비스에서 가져온 사용자 및 그룹을 활성화하여 Informatica 노드, 서비스 및 응용 프로그램 클라이언트에 로그인하도록 Informatica 도메인을 구성할 수 있습니다.

탐색기의 LDAP 구성 섹션은 도메인에서 사용하는 LDAP 구성을 나열합니다.

LDAP 구성을 선택하면 LDAP 구성 탭 아래에 다음과 같은 탭이 나타납니다.

- 개요. 사용자와 그룹을 가져오려는 디렉터리 서비스가 있는 LDAP 서버에 대한 연결 세부 정보를 나열합니다.
- 보안 도메인. LDAP 디렉터리 서비스에서 가져온 사용자와 그룹이 있는 LDAP 보안 도메인에 대한 세부 정보를 나열합니다.
- 일정. 서비스 관리자가 LDAP 디렉터리 서비스의 사용자와 그룹이 있는 보안 도메인을 업데이트하는 시기를 지정하는 동기화 일정에 대한 세부 정보를 나열합니다.

계정 관리

Informatica 도메인의 보안을 개선하기 위해 지정된 수의 로그인 시도 실패 후 사용자 및 관리자 계정 잠금을 적용할 수 있습니다.

계정 관리 페이지의 계정 잠금 구성 섹션에는 사용자 계정 및 관리자 계정에 대해 계정 잠금이 활성화되었는지 여부가 표시됩니다. 또한 이 섹션에는 허용되는 최대 로그인 시도 실패 횟수가 표시됩니다.

페이지의 잠긴 원시 사용자 섹션에는 원시 보안 도메인의 잠긴 사용자 계정이 나열됩니다. 원시 보안 도메인의 사용자 계정을 잠금 해제할 수 있습니다.

페이지의 잠긴 LDAP 사용자 섹션에는 LDAP 보안 도메인의 잠긴 사용자 계정이 나열됩니다. **Informatica** 도메인의 사용자 계정을 잠금 해제할 수 있습니다. 그러나 LDAP 관리자가 LDAP 서버에서 사용자 계정을 잠금 해제해야 합니다. 사용자는 LDAP 관리자가 사용자 계정을 잠금 해제할 때까지 **Informatica** 도메인에 로그인할 수 없습니다.

감사 보고서

감사 보고서는 **Informatica** 도메인의 사용자 및 그룹에 대한 정보와 각 사용자 또는 그룹에 할당된 권한, 역할 및 사용 권한에 대한 정보를 제공합니다.

보고서 유형 선택 메뉴에서 생성할 감사 보고서를 선택합니다. 다음과 같은 감사 보고서를 생성할 수 있습니다.

사용자 개인 정보

도메인의 사용자 계정에 대한 연락처 정보 및 상태 세부 정보를 표시합니다. 보고서를 생성하려는 사용자 또는 그룹을 선택할 수 있습니다.

사용자 그룹 연관

사용자와 사용자가 속하는 그룹에 대한 정보를 표시합니다. 보고서를 생성하려는 사용자 또는 그룹을 선택할 수 있습니다.

권한

도메인의 사용자 및 그룹에 할당된 권한에 대한 정보를 표시합니다. 보고서를 생성하려는 사용자 또는 그룹을 선택할 수 있습니다.

역할

도메인의 사용자 및 그룹에 할당된 역할에 대한 정보를 표시합니다. 보고서를 생성하려는 역할을 선택할 수 있습니다.

도메인 개체 사용 권한

사용자 및 그룹이 사용 권한을 가진 도메인 개체에 대한 정보를 표시합니다. 보고서를 생성하려는 사용자 또는 그룹을 선택할 수 있습니다.

암호 관리

암호 변경 응용 프로그램을 통해 암호를 변경할 수 있습니다.

암호 변경 응용 프로그램은 **Administrator** 도구에서 또는 다음 URL을 사용하여 열 수 있습니다. <http://<정규화된 호스트 이름>:<포트>/passwordchange/>

서비스 관리자는 작업자 노드와 연결된 사용자 암호를 사용하여 도메인 사용자를 인증합니다. 하나 이상의 작업자 노드와 연결된 사용자 암호를 변경한 경우 서비스 관리자가 각 작업자 노드에 대해 암호를 업데이트합니다.

서비스 관리자는 실행되고 있지 않은 노드를 업데이트할 수 없습니다. 실행되고 있지 않은 노드인 경우 서비스 관리자는 해당 노드가 다시 시작될 때 암호를 업데이트합니다.

참고: LDAP 사용자 계정인 경우 LDAP 디렉터리 서비스에서 암호를 변경합니다.

원시 사용자 계정에 대해 암호 복잡성을 활성화하는 경우 다음 지침에 따라 암호를 생성하거나 변경합니다.

- 암호 길이가 8자 이상이어야 합니다.
- 다음과 같은 영문자, 숫자 및 영숫자 이외 문자의 조합이어야 합니다.
! \ " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { | } ~

암호에 특수 문자를 사용하면 셸이 이러한 문자를 다르게 해석하는 경우가 있습니다. 예를 들어 \$는 변수로 해석됩니다. 이 경우 이스케이프 문자를 사용하여 특수 문자를 이스케이프합니다.

암호 변경

언제라도 원시 사용자 계정의 암호를 변경합니다. 다른 사람이 작성한 사용자 계정인 경우 Administrator 도구에 처음 로그인할 때 암호를 변경합니다.

1. Administrator 도구 헤더 영역에서 **관리 > 암호 변경**을 클릭합니다.
새 브라우저 창에서 암호 변경 응용 프로그램이 열립니다.
2. **암호** 상자에 현재 암호를 입력하고 **새 암호** 및 **암호 확인** 상자에 새 암호를 입력합니다.
3. **업데이트**를 클릭합니다.

도메인 보안 관리

Informatica 도메인 구성 요소가 다른 구성 요소와의 연결을 암호화할 때 SSL(Secure Sockets Layer) 프로토콜 또는 TLS(Transport Layer Security) 프로토콜을 사용하도록 구성할 수 있습니다. 도메인 구성 요소에 SSL 또는 TLS를 활성화하면 보안 통신을 사용할 수 있습니다.

보안 통신은 다음과 같은 방법으로 구성할 수 있습니다.

도메인 내 서비스 간 보안 통신

도메인 내 서비스 간의 보안 통신을 구성할 수 있습니다.

도메인과 외부 구성 요소 간의 보안 통신

Informatica 도메인 구성 요소와 웹 브라우저 또는 웹 서비스 클라이언트 간의 보안 통신을 구성할 수 있습니다.

보안 통신을 구성하는 각 방법은 다른 방법과 별개입니다. 한 구성 요소 집합에 보안 통신을 구성한 경우 다른 모든 집합에 보안 통신을 구성할 필요가 없습니다.

참고: 보안 도메인을 비보안 도메인으로 변경하거나 비보안 도메인을 보안 도메인으로 변경할 경우 Developer 도구 및 PowerCenter 클라이언트 도구에서 도메인 구성을 삭제하고 클라이언트에서 도메인을 다시 구성해야 합니다.

사용자 보안 관리

도메인 안의 사용자 보안은 권한 및 사용 권한을 통해 관리합니다.

권한은 사용자가 도메인 개체에 완료할 수 있는 작업을 결정합니다. 사용 권한은 사용자의 도메인 개체에 대한 액세스 수준을 정의합니다. 도메인 개체에는 도메인, 폴더, 노드, 그리드, 라이선스, 데이터베이스 연결, 운영 체제 프로필 및 응용 프로그램 서비스가 포함됩니다.

특정 작업을 완료할 도메인 권한이 있는 사용자라 하더라도 특정 개체에 대한 작업을 완료하려면 해당하는 사용 권한이 필요할 수 있습니다. 예를 들어 서비스 관리 도메인 권한은 응용 프로그램 서비스를 편집할 수 있는 권한을 사용자에게 제공합니다. 그러나 사용자가 응용 프로그램 서비스를 편집하려면 해당 응용 프로그램 서비스에 대한 사용 권한도 있어야 합니다. 서비스 관리 도메인 권한과 개발 리포지토리 서비스에 대한 사용 권한이 있지만 프로덕션 리포지토리 서비스에 대한 사용 권한이 없는 사용자는 개발 리포지토리 서비스를 편집할 수 있지만 프로덕션 리포지토리 서비스는 편집할 수 없습니다.

Administrator 도구에 로그인하려면 사용자에게 **Informatica Administrator** 액세스 도메인 권한이 있어야 합니다. **Informatica Administrator** 액세스 권한과 개체에 대한 사용 권한이 있지만 개체 유형을 수정할 수 있는 도메인 권한이 없는 사용자는 개체를 보기만 할 수 있습니다. 예를 들어 노드에 대한 사용 권한이 있지만 노드 및 그리드 관리 권한이 없는 사용자는 노드 속성을 볼 수 있지만 노드를 구성하거나 종료하거나 제거할 수 없습니다.

사용자가 사용 권한이 없는 개체를 탐색기에서 선택한 경우 해당 개체에 대한 사용 권한이 거부되었음을 나타내는 메시지가 콘텐츠 패널에 표시됩니다.

제 8 장

사용자 및 그룹

이 장에 포함된 항목:

- [사용자 및 그룹 개요, 109](#)
- [기본 그룹, 110](#)
- [사용자 계정 이해, 111](#)
- [사용자 관리, 113](#)
- [그룹 관리, 120](#)
- [운영 체제 프로필 관리, 122](#)
- [계정 잠금, 129](#)

사용자 및 그룹 개요

Informatica 도메인에서 응용 프로그램 서비스 및 개체에 액세스하고 응용 프로그램 클라이언트를 사용하려면 사용자 계정이 있어야 합니다.

설치 중 기본 관리자 사용자 계정이 작성됩니다. 기본 관리자 계정을 사용하여 **Informatica** 도메인에 로그인하고 응용 프로그램 서비스, 도메인 개체 및 다른 사용자 계정을 관리합니다. 설치 후 **Informatica** 도메인에 로그인하는 경우 암호를 변경하여 **Informatica** 도메인 및 응용 프로그램을 보호합니다.

Informatica의 사용자 계정 관리는 다음 키 구성 요소와 관련됩니다.

- 사용자. **Informatica** 도메인에서 다른 유형의 사용자 계정을 설정할 수 있습니다. 사용자는 할당된 역할, 권한 및 사용 권한에 따라 태스크를 수행할 수 있습니다.
- 인증. 사용자가 응용 프로그램 클라이언트에 로그인하는 경우 서비스 관리자는 **Informatica** 도메인에서 사용자 계정을 인증하고 사용자가 응용 프로그램 클라이언트를 사용할 수 있는지 확인합니다. **Informatica** 도메인은 원시 또는 **LDAP** 인증을 사용하여 사용자를 인증합니다. 서비스 관리자는 보안 도메인에 따라 사용자 계정 및 그룹을 구성합니다. 사용자가 속한 보안 도메인에 따라 사용자를 인증합니다.
- 그룹. 사용자 그룹을 설정하고 다른 역할, 권한 및 사용 권한을 각 그룹에 할당할 수 있습니다. 그룹에 할당된 역할, 권한 및 사용 권한에 따라 그룹의 사용자가 **Informatica** 도메인에서 수행할 수 있는 태스크가 결정됩니다.
- 권한 및 역할. 권한에 따라 사용자가 응용 프로그램 클라이언트에서 수행할 수 있는 작업이 결정됩니다. 역할은 사용자 및 그룹에 할당할 수 있는 권한의 컬렉션입니다. 역할 또는 권한을 도메인 및 도메인의 응용 프로그램 서비스의 사용자 및 그룹에 할당합니다.
- 운영 체제 프로필. **UNIX** 또는 **Linux**에서 통합 서비스를 실행하는 경우 운영 체제 프로필을 사용하도록 통합 서비스를 구성할 수 있습니다. 운영 체제 프로필을 사용하여 보안을 강화하고 사용자의 런타임 환경을 격리합니다. **Administrator** 도구의 보안 탭에서 운영 체제 프로필을 작성하고 관리할 수 있습니다.

- 계정 잠금. 계정 잠금을 구성하면 사용자가 Administrator 도구 또는 Developer tool 및 Analyst 도구와 같은 응용 프로그램 클라이언트에서 잘못된 로그인을 지정하는 경우 사용자 계정을 잠글 수 있습니다. 또한 사용자 계정을 잠금 해제할 수도 있습니다.

기본 그룹

Informatica 도메인에는 설치 중 작성되는 사용자 그룹 집합이 있습니다.

기본적으로 Informatica 도메인에는 설치 후 다음과 같은 사용자 그룹이 생깁니다.

- 관리자
- 모든 사람
- 운영자

관리자 그룹

Informatica 도메인에는 Administrator라는 이름의 기본 그룹이 포함됩니다. 설치 중 작성된 기본 관리자 계정이 이 그룹에 속합니다.

관리자 그룹에는 도메인 및 모든 응용 프로그램 서비스에 대한 관리자 사용 권한 및 권한이 있습니다. 관리자 그룹에서 사용자를 추가하거나 제거할 수 있습니다. 관리자 그룹의 모든 사용자는 설치 시 작성되는 기본 관리자와 동일한 사용 권한 및 권한을 가지고 있습니다.

관리자 그룹에서 기본 관리자 계정을 삭제할 수 없고 관리자 그룹을 삭제할 수 없습니다.

모든 사람 그룹

Informatica 도메인에는 모든 사람이라는 기본 그룹이 포함되어 있습니다. 도메인의 모든 사용자가 이 그룹에 속합니다.

기본적으로 모든 사람 그룹은 어떤 권한도 갖지 않습니다. 권한, 역할 및 사용 권한을 모든 사람 그룹에 할당하면 동일한 액세스를 모든 사용자에게 부여할 수 있습니다.

모든 사람 그룹에서 다음 태스크를 수행할 수 없습니다.

- 모든 사람 그룹 편집 또는 삭제
- 모든 사람 그룹에서 사용자 추가 또는 사용자 제거
- 모든 사람 그룹으로 그룹 이동

운영자 그룹

Informatica 도메인에는 운영자라는 이름의 기본 그룹이 포함됩니다.

기본적으로 운영자 그룹에는 도메인의 모든 개체에 대한 사용 권한이 있습니다. 운영자 역할을 운영자 그룹에 할당하고 도메인의 운영자 사용자를 관리하는 데 사용할 수 있습니다.

운영자 그룹에서 다음과 같은 태스크를 수행할 수 있습니다.

- 그룹에 권한 및 역할 할당
- 그룹에서 사용자 추가 또는 사용자 제거
- 그룹으로 그룹 이동

- 그룹 편집 또는 삭제

사용자 계정 이해

Informatica 도메인에는 다음 유형의 계정이 있을 수 있습니다.

- 기본 관리자
- 도메인 관리자
- 응용 프로그램 클라이언트 관리자
- 사용자

기본 관리자

Informatica 서비스를 설치할 때 설치 프로그램은 제공하는 사용자 이름 및 암호를 사용하여 기본 관리자를 작성합니다. 처음으로 **Administrator** 도구에 로그인할 때 기본 관리자 계정을 사용할 수 있습니다.

기본 관리자에는 도메인 및 모든 응용 프로그램 서비스에 대한 관리자 사용 권한 및 권한이 있습니다.

기본 관리자는 다음 태스크를 수행할 수 있습니다.

- 도메인에서 노트, 응용 프로그램 서비스, 관리자 및 사용자 계정을 비롯한 모든 개체 작성, 구성 및 관리
- 다른 도메인 관리자 및 응용 프로그램 클라이언트 관리자가 작성한 모든 개체 및 사용자 계정 구성 및 관리
- 응용 프로그램 클라이언트에 로그인

기본 관리자의 사용자 이름 또는 권한을 비활성화하거나 수정할 수 없습니다. 기본 관리자 암호는 변경할 수 있습니다.

도메인 관리자

도메인 관리자는 도메인에서 개체를 작성하고 관리할 수 있습니다.

도메인 관리자는 **Administrator** 도구에 로그인하고 도메인에서 응용 프로그램 서비스를 작성 및 구성할 수 있습니다. 그러나 기본적으로 도메인 관리자는 응용 프로그램 클라이언트에 로그인할 수 없습니다. 기본 관리자는 명시적으로 응용 프로그램 서비스에 대한 도메인 관리자 전체 사용 권한 및 권한을 제공해야 응용 프로그램 클라이언트에 로그인하고 관리 태스크를 수행할 수 있습니다.

도메인 관리자를 작성하려면 사용자에게 도메인에 대한 관리자 역할을 할당합니다.

응용 프로그램 클라이언트 관리자

응용 프로그램 클라이언트 관리자는 응용 프로그램 클라이언트에서 개체를 작성하고 관리할 수 있습니다. 응용 프로그램 클라이언트의 관리자 계정을 작성해야 합니다. 관리자 권한을 제한하고 응용 프로그램 클라이언트를 보호하려면 각 응용 프로그램 클라이언트에 대해 별도의 관리자 계정을 작성합니다.

기본적으로 응용 프로그램 클라이언트 관리자는 도메인에 대한 사용 권한 또는 권한이 없습니다. 도메인에 대한 사용 권한 또는 권한이 없으면 응용 프로그램 클라이언트 관리자가 **Administrator** 도구에 로그인하여 응용 프로그램 서비스를 관리할 수 없습니다.

다음과 같은 응용 프로그램 클라이언트 관리자를 설정할 수 있습니다.

Informatica Analyst 관리자

Informatica Analyst에 전체 사용 권한 및 권한이 있습니다. Informatica Analyst 관리자는 Informatica Analyst에 로그인하여 프로젝트 및 프로젝트의 개체를 작성 및 관리하고 응용 프로그램 클라이언트에서 모든 태스크를 수행할 수 있습니다.

Informatica Analyst 관리자를 작성하려면 사용자에게 분석 서비스 및 관련된 모델 리포지토리 서비스에 대한 관리자 역할을 할당합니다.

Informatica Developer 관리자

Informatica Developer에 전체 사용 권한 및 권한이 있습니다. Informatica Developer 관리자는 Informatica Developer에 로그인하여 프로젝트 및 프로젝트의 개체를 작성 및 관리하고 응용 프로그램 클라이언트에서 모든 태스크를 수행할 수 있습니다.

Informatica Developer 관리자를 작성하려면 사용자에게 모델 리포지토리 서비스에 대한 관리자 역할을 할당합니다.

Metadata Manager 관리자

Metadata Manager에 전체 사용 권한 및 권한이 있습니다. Metadata Manager 관리자는 Metadata Manager에 로그인하여 Metadata Manager 개체를 작성 및 관리하고 응용 프로그램 클라이언트에서 모든 태스크를 수행할 수 있습니다.

Metadata Manager 관리자를 작성하려면 사용자에게 Metadata Manager 서비스에 대한 관리자 역할을 할당합니다.

테스트 데이터 관리자

Test Data Manager에 전체 사용 권한 및 권한이 있습니다. Test Data Manager 관리자는 Test Data Manager에 로그인하여 Test Data Manager 개체를 작성 및 관리하고 응용 프로그램 클라이언트에서 모든 태스크를 수행할 수 있습니다.

테스트 데이터 관리자를 작성하려면 사용자에게 Test Data Manager 서비스에 대한 관리자 역할을 할당합니다.

PowerCenter 클라이언트 관리자

PowerCenter 클라이언트의 모든 개체에 대한 전체 사용 권한 및 권한이 있습니다. PowerCenter 클라이언트 관리자는 PowerCenter 클라이언트에 로그인하여 PowerCenter 리포지토리 개체를 관리하고 PowerCenter 클라이언트에서 모든 태스크를 수행할 수 있습니다. PowerCenter 클라이언트 관리자는 pmrep 및 pmcmd 명령줄 프로그램에서 모든 태스크를 수행할 수도 있습니다.

PowerCenter 클라이언트 관리자를 작성하려면 사용자에게 PowerCenter 리포지토리 서비스에 대한 관리자 역할을 할당합니다.

사용자

Informatica 도메인의 계정이 있는 사용자는 응용 프로그램 클라이언트에서 태스크를 수행할 수 있습니다.

일반적으로 기본 관리자 또는 도메인 관리자가 Informatica 도메인에서 사용자 계정을 작성 및 관리하고 역할, 권한 및 사용 권한을 할당합니다. 그러나 필요한 도메인 권한 및 사용 권한을 가진 사용자는 사용자 계정을 작성하고 역할, 사용 권한 및 권한을 할당할 수 있습니다.

사용자는 할당된 권한 및 사용 권한에 따라 응용 프로그램 클라이언트에서 태스크를 수행할 수 있습니다.

사용자 관리

원시 보안 도메인에서 사용자를 작성, 편집 및 삭제할 수 있습니다. LDAP 보안 도메인에서 사용자 계정의 속성을 삭제 또는 수정할 수 없습니다. LDAP 그룹에 대한 사용자 할당을 수정할 수 없습니다.

역할, 사용 권한 및 권한을 원시 보안 도메인 또는 LDAP 보안 도메인의 사용자 계정에 할당할 수 있습니다. 사용자에게 할당된 역할, 사용 권한 및 권한에 따라 Informatica 도메인에서 사용자가 수행할 수 있는 태스크가 결정됩니다.

또한 사용자 계정을 잠금 해제할 수도 있습니다.

원시 사용자 생성

보안 탭에서 원시 사용자를 추가, 편집 또는 삭제합니다.

1. Administrator 도구에서 보안 탭을 클릭합니다.
2. 보안 작업 메뉴에서 사용자 생성을 클릭합니다.
3. 사용자에게 다음 세부 정보를 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. < > “
전자 메일	사용자의 전자 메일 주소입니다. 전자 메일 주소는 다음 특수 문자를 포함할 수 없습니다. < > “ UserName@Domain 형식으로 전자 메일 주소를 입력합니다.
전화	사용자의 전화 번호입니다. 전화 번호는 다음 특수 문자를 포함할 수 없습니다. < > “

4. 확인을 클릭하여 사용자 계정을 저장합니다.

사용자 계정을 생성하면 세부 정보 패널에 사용자에게 할당된 사용자 계정 및 그룹의 속성이 표시됩니다.

원시 사용자의 일반 속성 편집

원시 사용자의 로그인 이름은 변경할 수 없습니다. 원시 사용자 계정의 암호 및 다른 세부 정보는 변경할 수 있습니다.

1. **Administrator** 도구에서 보안 탭을 클릭합니다.
2. 탐색기의 사용자 섹션에서 원시 사용자 계정을 선택하고 편집을 클릭합니다.
3. 암호를 변경하려면 암호 변경을 선택합니다.
보안 탭에서 암호 및 암호 확인 필드를 지웁니다.
4. 새 암호를 입력하고 확인합니다.
5. 필요에 따라 전체 이름, 설명, 전자 메일 및 전화번호를 수정합니다.
6. 확인을 클릭하여 변경 내용을 저장합니다.

원시 그룹에 원시 사용자 할당

보안 탭에서 원시 사용자를 원시 그룹에 할당합니다.

1. **Administrator** 도구에서 보안 탭을 클릭합니다.
2. 탐색기의 사용자 섹션에서 원시 사용자 계정을 선택하고 **편집**을 클릭합니다.
3. 그룹 탭을 클릭합니다.
4. 원시 사용자를 그룹에 할당하려면 모든 그룹 열에서 그룹 이름을 선택하고 **추가**를 클릭합니다.
중첩 그룹이 모든 그룹 열에 표시되지 않는 경우 각 그룹을 확장하여 중첩된 모든 그룹을 표시합니다.
원시 사용자를 둘 이상의 그룹에 할당할 수 있습니다. 동시에 여러 그룹을 선택하려면 **Ctrl** 또는 **Shift** 키를 사용합니다.
5. 원시 사용자를 그룹에서 제거하려면 할당된 그룹 열에서 그룹을 선택하고 **제거**를 클릭합니다.
6. **확인**을 클릭하여 그룹 할당을 저장합니다.

원시 그룹에 LDAP 사용자 할당

LDAP 사용자 계정을 원시 그룹에 할당할 수 있습니다. LDAP 그룹에 대한 LDAP 사용자 계정 할당은 변경할 수 없습니다.

1. **Administrator** 도구에서 **보안** 탭을 클릭합니다.
2. 탐색기의 그룹 섹션에서 원시 그룹을 선택하고 **편집**을 클릭합니다.
3. **사용자** 탭을 클릭합니다.
4. LDAP 사용자를 그룹에 할당하려면 모든 사용자 열에서 LDAP 사용자를 선택하고 **추가**를 클릭합니다.
5. LDAP 사용자를 그룹에서 제거하려면 할당된 사용자 열에서 LDAP 사용자를 선택하고 **제거**를 클릭합니다.
6. **확인**을 클릭하여 사용자 할당을 저장합니다.

사용자 계정 활성화 및 비활성화

활성 계정이 있는 사용자는 응용 프로그램 클라이언트에 로그인하고 해당 사용 권한 및 권한에 따라 태스크를 수행할 수 있습니다. 사용자가 응용 프로그램 클라이언트에 일시적으로 액세스하지 못하도록 하려면 사용자 계정을 비활성화하면 됩니다. 원시 또는 LDAP 보안 도메인에서 사용자 계정을 활성화하거나 비활성화할 수 있습니다. 사용자 계정을 비활성화하는 경우 사용자는 응용 프로그램 클라이언트에 로그인할 수 없습니다.

사용자 계정을 비활성화하려면 탐색기의 사용자 섹션에서 사용자 계정을 선택하고 비활성화를 클릭합니다. 비활성화된 사용자 계정을 선택하면 보안 탭에 사용자 계정이 비활성화되었다는 메시지가 표시됩니다. 사용자 계정이 비활성화되면 활성화 단추를 사용할 수 있습니다. 사용자 계정을 활성화하려면 활성화를 클릭합니다.

기본 관리자 계정은 비활성화할 수 없습니다.

참고: 서비스 관리자가 LDAP 디렉터리 서비스에서 사용자 계정을 가져오는 경우 사용자 계정이 활성화되거나 비활성화되었다는 것을 나타내는 LDAP 특성은 가져오지 않습니다. 서비스 관리자는 모든 사용자 계정을 활성화된 사용자 계정으로 가져옵니다. 사용자가 응용 프로그램 클라이언트에 액세스하지 않도록 하려면

Administrator 도구에서 LDAP 사용자 계정을 비활성화해야 합니다. 이후에 LDAP 서버와 동기화하는 동안 사용자 계정은 **Administrator** 도구에서 설정된 활성화 또는 비활성화 상태를 유지합니다.

원시 사용자 삭제

원시 사용자 계정을 삭제하려면 탐색기의 사용자 섹션에서 사용자 계정 이름을 마우스 오른쪽 단추로 클릭하고 사용자 삭제를 선택합니다. 사용자 계정을 삭제할 것인지 확인합니다.

기본 관리자 계정은 삭제할 수 없습니다. **Administrator** 도구에 로그인하는 경우에는 사용자 계정을 삭제할 수 없습니다.

PowerCenter의 사용자 삭제

PowerCenter 리포지토리에서 개체를 소유하는 사용자를 삭제하면 사용자가 폴더, 연결 개체, 배포 그룹, 레이블 또는 쿼리에 대해 가진 소유권이 제거됩니다. 사용자를 삭제하고 나면 기본 관리자가 삭제된 사용자가 소유했던 모든 개체의 소유자가 됩니다.

삭제된 사용자가 이전에 소유했던 버전 지정 개체의 기록을 보면 삭제된 사용자의 이름에 "삭제됨"이라는 단어가 접두사로 표시됩니다.

Metadata Manager 사용자 삭제

바로 가기 및 폴더를 소유하는 사용자를 삭제하는 경우 **Metadata Manager**는 사용자의 개인 폴더를 기본 관리자가 소유한 삭제된 사용자라는 이름의 폴더로 이동합니다. 삭제된 사용자의 개인 폴더에는 사용자가 작성한 모든 바로 가기 및 폴더가 포함되어 있습니다. 공유된 폴더는 사용자를 삭제한 후에도 여전히 공유됩니다.

삭제된 사용자 폴더에 동일한 사용자 이름을 가진 폴더가 있는 경우 **Metadata Manager**는 추가 폴더의 이름을 "<사용자 이름> 사본"으로 지정합니다.

LDAP 사용자

Administrator 도구에서 LDAP 사용자를 추가, 편집 또는 삭제할 수 없습니다. LDAP 디렉터리 서비스에서 LDAP 사용자 계정을 관리해야 합니다.

사용자 계정 잠금 해제

도메인 관리자는 도메인에 대해 잠긴 사용자 계정을 잠금 해제할 수 있습니다. 사용자가 원시 사용자인 경우 관리자는 사용자가 도메인에 다시 로그인하기 전에 해당 암호를 재설정하도록 요청할 수 있습니다.

사용자는 해당 계정 암호가 재설정된 경우 알림을 받도록 도메인에 구성된 유효한 전자 메일 주소가 있어야 합니다.

사용자가 LDAP 인증 서버에 대해 잠긴 경우 LDAP 관리자는 LDAP 서버에서 사용자 계정을 잠금 해제해야 합니다.

1. **Administrator** 도구에서 **보안** 탭을 클릭합니다.

2. **계정 관리**를 클릭합니다.

계정 관리자 페이지에 다음과 같이 잠긴 사용자 목록이 표시됩니다.

잠긴 원시 사용자

잠긴 원시 보안 도메인에 사용자 계정을 포함합니다.

잠긴 LDAP 사용자

잠긴 LDAP 보안 도메인의 사용자 계정을 포함합니다.

3. 잠금을 해제하려는 사용자를 선택합니다.

4. **사용자 잠금 해제 및 암호 재설정**을 선택하고 계정을 잠금 해제한 후 사용자에게 대한 새 암호를 생성합니다.

사용자는 전자 메일로 새 암호를 받습니다.

5. **선택한 사용자 잠금 해제** 단추를 클릭합니다.

여러 사용자를 위해 시스템 메모리 늘리기

Informatica 도메인 다시 시작, LDAP 사용자 동기화, 일부 `infacmd` 및 `infasetup` 명령 처리 시간은 Informatica 도메인의 사용자 수에 따라 비례적으로 증가합니다.

사용자 수는 다음 명령의 처리 시간에 영향을 미칩니다.

- `infasetup BackupDomain, DeleteDomain` 및 `RestoreDomain`
- `infacmd isp ExportDomainObjects, ExportUsersandGroups, ImportDomainObjects` 및 `ImportUsersandGroups`
- `infacmd tools ExportObjects` 및 `ImportObjects`

도메인에 많은 사용자가 있는 경우 Informatica 서비스, `infasetup` 및 `infacmd`에서 사용되는 시스템 메모리를 늘려야 할 수도 있습니다. 최대 힙 크기를 늘리려면 다음 환경 변수를 구성하고 값을 메가바이트로 지정합니다.

- `INFA_JAVA_OPTS`. Informatica 서비스에서 사용되는 최대 힙 크기를 결정합니다. Informatica 서비스가 설치되는 각 노드에서 구성합니다.
- `ICMD_JAVA_OPTS`. `infacmd`에서 사용되는 최대 힙 크기를 결정합니다. `infacmd`를 실행하는 각 시스템에서 구성합니다.
- `INFA_JAVA_CMD_OPTS`. `infasetup`에서 사용되는 최대 힙 크기를 결정합니다. `infasetup`을 실행하는 각 시스템에서 구성합니다.

예를 들어 UNIX에서 `INFA_JAVA_OPTS` 환경 변수에 대해 2048MB의 시스템 메모리를 구성하려면 다음 명령을 사용합니다.

```
setenv INFA_JAVA_OPTS "-Xmx2048m"
```

Windows에서는 변수를 시스템 변수로 구성합니다.

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

도메인 사용자 수	최대 힙 크기 (1~5개 서비스)	최대 힙 크기 (6~10개 서비스)
20,000	5120MB	6144MB
30,000	5120MB	6144MB

참고: 이 테이블의 최대 힙 크기 설정은 도메인의 응용 프로그램 서비스 수에 따른 것입니다.

이러한 환경 변수를 구성한 후 노드를 다시 시작하여 변경 내용을 적용합니다.

사용자 활동 보기

Administrator 도구의 로그 탭에서 사용자 활동 로그를 볼 수 있습니다. 사용자 활동 로그를 확인하여 **Informatica** 클라이언트 응용 프로그램의 로그인 시도를 검토합니다. 또한 로그를 확인하여 사용자가 서비스, 노드, 사용자, 그룹 또는 역할을 생성하거나 업데이트하거나 제거한 시기를 파악할 수도 있습니다.

사용자 활동 로그와 **Administrator** 도구의 로그 탭에 대한 자세한 내용은 *Informatica Administrator 가이드*를 참조하십시오.

`infacmd isp getUserActivityLog` 명령을 사용하여 사용자 활동 로그 데이터를 볼 수도 있습니다. `infacmd isp getUserActivityLog` 명령은 다음 구문을 사용합니다.

```
infacmd isp getUserActivityLog -dn domain_name -un user_name -pd password
```

`infacmd isp getUserActivityLog` 명령을 사용하려면 관리자 역할 또는 관리자 그룹의 멤버가 필요합니다. `isp getUserActivityLog` 명령에 대한 자세한 내용은 *Informatica 명령 참조*를 참조하십시오.

사용자 활동 로그 데이터에는 **Informatica** 클라이언트의 성공 및 실패한 사용자 로그인 시도가 포함됩니다. 클라이언트의 로그인 요청에 사용자 지정 속성이 설정된 경우 로그 데이터에 사용자 지정 속성도 포함됩니다.

참고: Kerberos 인증을 사용하도록 구성된 도메인의 사용자 로그인 시도는 사용자 활동 로그에 포함되지 않습니다.

사용자 활동 데이터에는 **Informatica** 클라이언트의 각 로그인 시도에 대한 다음 속성이 포함됩니다.

- 응용 프로그램 이름
- 응용 프로그램 버전
- 응용 프로그램 호스트의 호스트 이름 또는 IP 주소

다음 선택 필터에 따라 로그 이벤트를 볼 수 있습니다.

- 사용자 이름
- 보안 도메인
- 날짜 및 시간
- 시간 순
- 활동 코드
- 활동 텍스트

명령 프롬프트에 로그 이벤트를 표시하거나 다음 형식 중 하나의 파일에 이벤트를 기록할 수 있습니다.

- 이진
- 텍스트
- XML

이진 형식으로 로그를 인쇄하는 경우 `infacmd isp convertUserActivityLog` 명령을 사용하여 텍스트 또는 XML 형식으로 변환할 수 있습니다. `infacmd isp convertUserActivityLog` 명령 사용에 대한 자세한 내용은 *Informatica 명령 참조*를 참조하십시오.

사용자 활동 코드

사용자 활동 로그에는 각 활동의 성공 또는 실패를 나타내는 코드가 포함됩니다.

유효한 활동 코드는 다음과 같습니다.

- CCM_10437. 활동이 성공했음을 나타냅니다.
- CCM_10438. 활동이 실패했음을 나타냅니다.
- CCM_10778. 사용자 지정 속성을 사용한 로그인 시도가 성공했음을 나타냅니다.
- CCM_10779. 사용자 지정 속성을 사용한 로그인 시도가 실패했음을 나타냅니다.
- CCM_10786. 사용자 지정 속성을 사용하지 않은 로그인 시도가 성공했음을 나타냅니다.
- CCM_10787. 사용자 지정 속성을 사용하지 않은 로그인 시도가 실패했음을 나타냅니다.

사용자 활동 로그 필터

하나 이상의 필터를 사용하여 특정 사용자, 날짜 또는 이벤트에 대한 로그 이벤트를 검색합니다.

`infacmd isp getUserActivityLog` 명령에 대해 하나 이상의 다음 매개 변수를 사용하여 로그 이벤트를 필터링합니다.

사용자 및 보안 도메인

선택 사항입니다. 로그 이벤트를 가져올 사용자의 목록입니다. 여러 사용자는 공백으로 구분합니다. 단일 보안 도메인 또는 모든 보안 도메인의 여러 사용자에 대한 로그를 보려면 와일드카드 기호(*)를 사용합니다. 예를 들어 다음 문자열은 이 옵션에 대해 올바른 값입니다.

```
user:Native
"user:*"
"user*"
"*_users_*"
"*:Native"
```

다음 매개 변수를 `getUserActivityLog` 명령에 추가하여 사용자 또는 보안 도메인에 따른 로그 이벤트를 필터링합니다.

```
-usrs <UserName>:<SecurityDomain>
```

예를 들어 다음 매개 변수를 추가하여 모든 보안 도메인에서 `User1`이라는 사용자에 대한 사용자 활동을 검색합니다.

```
-usrs "User1:*
```

날짜 및 시간

선택 사항입니다. 로그 이벤트를 보려는 날짜 범위입니다.

시작 날짜 이전의 날짜를 종료 날짜로 입력하는 경우 명령이 로그 이벤트를 반환하지 않습니다.

다음 형식 중 하나로 날짜 및 시간을 입력합니다.

- MM/dd/yyyy
- MM/dd/yyyy HH:mm:ss
- yyyy-MM-dd
- yyyy-MM-dd HH:mm:ss

다음 매개 변수를 `getUserActivityLog` 명령에 추가하여 시작 날짜 또는 종료 날짜로 로그를 필터링합니다.

`-sd <start_date> -ed <end_date>`

예를 들어 다음 매개 변수를 추가하여 2014년 1월 1일에서 2014년 2월 3일 사이의 사용자 활동을 검색합니다.

`-sd 01/01/2014 -ed 02/03/2014`

활동 코드

선택 사항입니다. 활동 코드에 따라 로그 이벤트를 반환합니다.

여러 활동 코드에 대한 로그 이벤트를 검색하려면 와일드카드 기호(*)를 사용합니다. 올바른 활동 코드에는 다음이 포함됩니다.

- CCM_10437. 활동이 성공했음을 나타냅니다.
- CCM_10438. 활동이 실패했음을 나타냅니다.
- CCM_10778. 사용자 지정 속성을 사용한 로그인 시도가 성공했음을 나타냅니다.
- CCM_10779. 사용자 지정 속성을 사용한 로그인 시도가 실패했음을 나타냅니다.
- CCM_10786. 사용자 지정 속성을 사용하지 않은 로그인 시도가 성공했음을 나타냅니다.
- CCM_10787. 사용자 지정 속성을 사용하지 않은 로그인 시도가 실패했음을 나타냅니다.

다음 매개 변수를 `getUserActivityLog` 명령에 추가하여 활동 코드로 필터링합니다.

`-ac <activity_code>`

예를 들어 다음 매개 변수를 추가하여 성공한 로그 이벤트를 검색합니다.

`-ac CCM_10437`

와일드카드 기호를 사용하는 경우 인수를 따옴표로 묶습니다.

활동 텍스트

선택 사항입니다. 활동 텍스트에 있는 문자열에 따라 로그 이벤트를 반환합니다.

다음 매개 변수를 `getUserActivityLog` 명령에 추가하여 활동 텍스트로 필터링합니다.

`-atxt <activity_text>`

여러 이벤트에 대한 로그를 검색하려면 와일드카드 기호(*)를 사용합니다. 예를 들어 다음 매개 변수는 설명에 "Enabling service" 구가 포함된 모든 로그 이벤트를 반환합니다.

`-atxt "*Enabling service*"`

와일드카드 기호를 사용하는 경우 인수를 따옴표로 묶습니다.

시간 순

선택 사항입니다. 로그 이벤트를 반대 시간 순으로 인쇄합니다. 이 매개 변수를 지정하지 않을 경우 명령이 로그 이벤트를 시간 순으로 표시합니다.

다음 매개 변수를 `getUserActivityLog` 명령에 추가하여 최신 이벤트를 먼저 인쇄합니다.

`-ro true`

사용자 활동 로그 이벤트 쓰기 및 보기

infacmd isp getUserActivityLog 명령을 사용하면 사용자 활동 로그 이벤트를 파일에 쓰거나 명령줄에 표시할 수 있습니다. 내보낸 로그 이벤트 파일의 사용 계획 방법에 따른 형식으로 사용자 활동 로그 이벤트를 씁니다.

로그 파일 쓰기 및 보기

사용자 활동 로그 이벤트를 파일에 쓰려면 출력 파일 매개 변수 **-lo**와 함께 명령을 실행합니다.

-lo output_file_name

출력 형식을 지정하지 않으면 명령이 텍스트 파일에 로그 이벤트를 씁니다. 예를 들어 다음 명령을 실행하여 로그 이벤트를 이름이 **log.txt**인 파일에 씁니다.

```
infacmd isp getUserActivityLog -dn TestDomain -un Administrator -pd Administrator -lo log.txt
```

출력 형식을 지정하려면 형식 매개 변수 **-fm**과 함께 명령을 실행합니다.

-fm output_format_BIN_TEXT_XML

유효한 형식은 다음과 같습니다.

- 이진(바이너리). 이진 형식으로 로그 이벤트를 백업하려면 이진 형식을 사용합니다. Informatica 글로벌 고객 지원 센터에 로그 이벤트를 전송하려면 이 형식을 사용해야 할 수 있습니다.
- 텍스트. 텍스트 편집기에서 로그 이벤트를 분석하려는 경우 텍스트 형식을 사용합니다.
- XML. XML을 사용하는 외부 도구에서 로그 이벤트를 분석하거나 XSLT와 같은 XML 도구를 사용하려는 경우 XML 형식을 사용합니다.

텍스트 또는 XML을 출력 형식으로 지정하고 출력 파일을 지정하지 않는 경우 명령은 명령줄에 텍스트 또는 XML 로그를 표시합니다.

이진을 출력 형식으로 지정하는 경우 출력 파일 이름을 제공해야 합니다.

예를 들어 다음 명령을 실행하여 로그 이벤트를 이름이 **log.xml**인 파일에 인쇄합니다.

```
infacmd isp getUserActivityLog -dn TestDomain -un Administrator -pd Administrator -fm xml -lo log.xml
```

로그 파일 변환

getUserActivity 명령을 사용하여 로그 이벤트를 이진 파일에 쓰는 경우 파일을 텍스트 또는 XML 형식으로 변환할 수 있습니다.

다음 명령을 실행하여 검색한 이진 로그를 텍스트 또는 XML 형식으로 변환합니다.

```
infacmd isp convertUserActivityLogFile -in BIN_input_file_name -fm output_format_TEXT_XML -lo output_file_name
```

예를 들어 다음 명령을 실행하여 이름이 **log.bin**인 이진 입력 파일을 XML 형식으로 변환하고 이름이 **convertedLog.xml**인 파일에 출력합니다.

```
infacmd isp convertUserActivityLogFile -in log.bin -fm XML -lo convertedLog.xml
```

명령줄에 로그를 표시하려면 출력 파일 이름을 생략합니다.

형식을 생략하는 경우 명령은 텍스트 형식을 사용합니다.

그룹 관리

원시 보안 도메인에서 그룹을 작성, 편집 및 삭제할 수 있습니다.

원시 또는 LDAP 보안 도메인에서 그룹에 역할, 권한 및 사용 권한을 할당할 수 있습니다. LDAP 보안 도메인에서 그룹 계정의 속성을 삭제하거나 수정할 수 없습니다. 그룹에 할당된 역할, 사용 권한 및 권한에 따라 그룹의 사용자가 Informatica 도메인에서 수행할 수 있는 태스크가 결정됩니다.

원시 그룹 추가

보안 탭에서 원시 그룹을 추가, 편집 또는 제거합니다.

원시 그룹은 원시 또는 LDAP 사용자 계정 또는 다른 원시 그룹을 포함할 수 있습니다. 여러 수준의 원시 그룹을 작성할 수 있습니다. 예를 들어 Finance 그룹이 OfficeSupplies 그룹이 포함된 AccountsPayable 그룹을 포함합니다. Finance 그룹은 AccountsPayable 그룹의 상위 그룹이고 AccountsPayable 그룹은 OfficeSupplies 그룹의 상위 그룹입니다. 각 그룹은 다른 원시 그룹을 포함할 수 있습니다.

1. Administrator 도구에서 보안 탭을 클릭합니다.
2. 보안 작업 메뉴에서 그룹 작성을 클릭합니다.
3. 그룹에 대한 다음 정보를 입력합니다.

속성	설명
이름	그룹의 이름입니다. 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.
상위 그룹	새 그룹이 속한 그룹입니다. 그룹 작성을 클릭하기 전에 원시 그룹을 선택하는 경우 선택한 그룹이 상위 그룹입니다. 그렇지 않은 경우 상위 그룹 필드에 새 그룹이 그룹에 속하지 않음을 나타내는 원시가 표시됩니다.
설명	그룹에 대한 설명입니다. 그룹 설명이 765자를 초과하거나 다음 특수 문자를 포함할 수 없습니다. < > “

4. 찾아보기를 클릭하여 다른 상위 그룹을 선택합니다.
둘 이상의 그룹 및 하위 그룹 수준을 작성할 수 있습니다.
5. 확인을 클릭하여 그룹을 저장합니다.

원시 그룹의 속성 편집

그룹을 작성한 후 그룹의 설명 및 그룹의 사용자 목록을 변경할 수 있습니다. 그룹 이름 또는 그룹의 상위를 변경할 수 없습니다. 그룹의 상위를 변경하려면 그룹을 다른 그룹으로 이동해야 합니다.

1. Administrator 도구에서 보안 탭을 클릭합니다.
2. 탐색기의 그룹 섹션에서 원시 그룹을 선택하고 편집을 클릭합니다.
3. 그룹의 설명을 변경합니다.
4. 그룹의 사용자 목록을 변경하려면 사용자 탭을 클릭합니다.
사용자 탭에는 도메인의 사용자 목록 및 그룹에 할당된 사용자 목록이 표시됩니다.
5. 사용자를 그룹에 할당하려면 모든 사용자 열의 사용자 계정을 선택하고 추가를 클릭합니다.
6. 사용자를 그룹에서 제거하려면 할당된 사용자 열에서 사용자 계정을 선택하고 제거를 클릭합니다.
7. 확인을 클릭하여 변경 내용을 저장합니다.

원시 그룹에서 다른 원시 그룹으로 이동

원시 보안 도메인에서 사용자 그룹을 구성하려면 중첩 그룹을 설정하고 한 그룹을 다른 그룹으로 이동할 수 있습니다.

원시 그룹을 다른 원시 그룹으로 이동하려면 탐색기의 그룹 섹션에서 원시 그룹 이름을 마우스 오른쪽 단추로 클릭하고 그룹 이동을 선택합니다.

원시 그룹 삭제

원시 그룹을 삭제하려면 탐색기의 그룹 섹션에서 그룹 이름을 마우스 오른쪽 단추로 클릭하고 그룹 삭제를 선택합니다.

그룹을 삭제하면 그룹의 사용자는 그룹의 멤버 자격 및 그룹에서 상속받은 모든 사용 권한 또는 권한을 잃게 됩니다.

그룹을 삭제하면 서비스 관리자는 그룹에 속한 모든 그룹 및 하위 그룹을 삭제합니다.

LDAP 그룹

LDAP 그룹을 추가, 편집 또는 삭제하거나 Administrator 도구에서 LDAP 그룹에 대한 사용자 할당을 수정할 수 없습니다. LDAP 디렉터리 서비스에서 그룹 및 사용자 할당을 관리해야 합니다.

운영 체제 프로필 관리

Administrator 도구의 보안 탭 또는 명령줄에서 운영 체제 프로필을 작성 및 관리합니다. 운영 체제 프로필을 작성, 편집 및 삭제할 수 있습니다. 사용자 및 그룹에 기본 운영 체제 프로필을 할당하거나 변경할 수 있습니다.

데이터 통합 서비스가 운영 체제 프로필을 사용하도록 구성된 경우 데이터 통합 서비스는 운영 체제 프로필을 사용하여 매핑, 프로필 및 워크플로우를 실행합니다. PowerCenter 통합 서비스가 운영 체제 프로필을 사용하도록 구성된 경우 PowerCenter 통합 서비스는 운영 체제 프로필을 사용하여 워크플로우를 실행합니다.

보안 탭의 **운영 체제 프로필** 보기에서 운영 체제 프로필을 작성, 편집 및 삭제합니다.

다음 단계를 완료하여 운영 체제 프로필을 작성합니다.

1. 운영 체제 프로필 이름과 시스템 사용자 이름을 입력합니다.
2. 통합 서비스를 선택하고 운영 체제 프로필 속성을 구성합니다.
3. 필요한 경우 운영 체제 프로필에 대한 사용 권한을 할당합니다.

운영 체제 프로필을 작성한 후 사용자 및 그룹을 운영 체제 프로필에 할당하고 기본 프로필을 사용자 및 그룹에 할당할 수 있습니다.

PowerCenter 통합 서비스에 대한 운영 체제 프로필 속성

세션 속성 및 매개 변수 파일에서 설정된 서비스 프로세스 변수로 운영 체제 프로필 설정을 재정의합니다.

다음 테이블에는 **PowerCenter** 통합 서비스에 대한 운영 체제 프로파일 속성이 설명되어 있습니다.

속성	설명
이름	운영 체제 프로파일의 읽기 전용 이름입니다. 이름은 128자를 초과할 수 없습니다. 공백이나 다음 특수 문자를 포함할 수 없습니다. \ / : * ? " < > [] = + ; ,
시스템 사용자 이름	PowerCenter 통합 서비스가 실행되는 시스템에 있는 운영 체제 사용자의 읽기 전용 이름입니다. PowerCenter 통합 서비스는 운영 체제 프로파일에서 정의된 시스템 사용자의 시스템 액세스를 사용하여 워크플로우를 실행합니다.
\$PMRootDir	노드를 통해 액세스할 수 있는 루트 디렉터리입니다. 이는 다른 서비스 프로세스 변수의 루트 디렉터리입니다. 다음 특수 문자를 포함할 수 없습니다. * ? < > " ,
\$PMSessionLogDir	세션 로그의 디렉터리입니다. 다음 특수 문자를 포함할 수 없습니다. * ? < > " , 기본값은 \$PMRootDir/SessLogs입니다.
\$PMBadFileDir	거부 파일의 디렉터리입니다. 다음 특수 문자를 포함할 수 없습니다. * ? < > " , 기본값은 \$PMRootDir/BadFiles입니다.
\$PMCacheDir	인덱스 및 데이터 캐시 파일의 디렉터리입니다. 캐시 디렉터리가 PowerCenter 통합 서비스 프로세스에 대해 로컬인 드라이브인 경우 성능을 향상시킬 수 있습니다. 캐시 파일에 대해 매핑되거나 마운팅된 드라이브를 사용하지 마십시오. 다음 특수 문자를 포함할 수 없습니다. * ? < > " , 기본값은 \$PMRootDir/Cache입니다.
\$PMTargetFileDir	대상 파일의 디렉터리입니다. 다음 특수 문자를 포함할 수 없습니다. * ? < > " , 기본값은 \$PMRootDir/TgtFiles입니다.
\$PMSourceFileDir	소스 파일의 디렉터리입니다. 다음 특수 문자를 포함할 수 없습니다. * ? < > " , 기본값은 \$PMRootDir/SrcFiles입니다.
\$PmExtProcDir	외부 프로시저의 디렉터리입니다. 다음 특수 문자를 포함할 수 없습니다. * ? < > " , 기본값은 \$PMRootDir/ExtProc입니다.
\$PMTempDir	임시 파일의 디렉터리입니다. 다음 특수 문자를 포함할 수 없습니다. * ? < > " , 기본값은 \$PMRootDir/Temp입니다.
\$PMLookupFileDir	조회 파일의 디렉터리입니다. 다음 특수 문자를 포함할 수 없습니다. * ? < > " , 기본값은 \$PMRootDir/LkpFiles입니다.

속성	설명
\$PMStorageDir	런타임 파일의 디렉터리입니다. 워크플로우 복구 파일이 PowerCenter 통합 서비스 속성에서 구성된 \$PMStorageDir에 저장됩니다. 세션 복구 파일이 운영 체제 프로필에 구성된 \$PMStorageDir에 저장됩니다. 다음 특수 문자를 포함할 수 없습니다. * ? < > " , 기본값은 \$PMRootDir/Storage입니다.
환경 변수	런타임 시 통합 서비스에서 사용하는 환경 변수의 이름 및 값입니다. 운영 체제 프로필 속성에서 LD_LIBRARY_PATH 환경 변수를 지정하는 경우 통합 서비스는 이 변수의 값을 해당 LD_LIBRARY_PATH 환경 변수에 추가합니다. 통합 서비스는 LD_LIBRARY_PATH 환경 변수 값을 사용하여 운영 체제 프로필에 대해 생성된 하위 프로세스의 환경 변수를 설정합니다. 운영 체제 프로필 속성에서 LD_LIBRARY_PATH 환경 변수를 지정하지 않는 경우 통합 서비스는 해당 LD_LIBRARY_PATH 환경 변수를 사용합니다.

데이터 통합 서비스에 대한 운영 체제 프로필 속성

다음 테이블에는 데이터 통합 서비스에 대한 운영 체제 프로필 속성이 설명되어 있습니다.

속성	설명
이름	운영 체제 프로필의 읽기 전용 이름입니다. 이름은 128자를 초과할 수 없습니다. 공백이나 다음 특수 문자를 포함할 수 없습니다. % * + \ / ? ; < >
시스템 사용자 이름	데이터 통합 서비스가 실행되는 시스템에 있는 운영 체제 사용자의 읽기 전용 이름입니다. 데이터 통합 서비스는 운영 체제 사용자의 시스템 액세스를 사용하여 매핑, 워크플로우 및 프로파일링 작업을 실행합니다.
\$DISRootDir	노드를 통해 액세스할 수 있는 루트 디렉터리입니다. 이는 다른 서비스 프로세스 변수의 루트 디렉터리입니다. 다음 특수 문자를 포함할 수 없습니다. * ? < > " , []
\$DISTempDir	작업 실행 시 작성되는 임시 파일에 대한 디렉터리입니다. 다음 특수 문자를 포함할 수 없습니다. * ? < > " , [] 기본값은 <루트 디렉터리>/disTemp입니다. 참고: 데이터 통합 서비스가 여러 운영 체제 프로필을 사용하도록 구성된 경우 각 프로필에 대해 별도의 디렉터리를 사용하면 디스크 공간이 과도하게 사용되므로 모든 프로필에 대해 공통 디렉터리를 지정하십시오.
\$DISCacheDir	변환할 인덱스 및 데이터 캐시 파일의 디렉터리입니다. 다음 특수 문자를 포함할 수 없습니다. * ? < > " , [] 기본값은 <루트 디렉터리>/cache입니다.
\$DISSourceDir	매핑에 사용되는 소스 플랫 파일의 디렉터리입니다. 다음 특수 문자를 포함할 수 없습니다. * ? < > " , [] 기본값은 <루트 디렉터리>/source입니다.

속성	설명
\$DISTargetDir	매핑에 사용되는 대상 플랫폼 파일의 디렉터리입니다. 다음 특수 문자를 포함할 수 없습니다. * ? < > " , [] 기본값은 <루트 디렉터리>/target입니다.
\$DISRejectedFilesDir	거부 파일의 디렉터리입니다. 거부 파일은 매핑을 실행할 때 거부되었던 행을 포함합니다. 다음 특수 문자를 포함할 수 없습니다. * ? < > " , [] 기본값은 <루트 디렉터리>/reject입니다.
\$DISLogDir	로그의 디렉터리입니다. 다음 특수 문자를 포함할 수 없습니다. * ? < > " , [] 기본값은 <루트 디렉터리>/disLogs입니다.
Hadoop 가장 속성 활성화	데이터 통합 서비스가 Hadoop 가장 사용자를 사용하여 Hadoop 환경에서 매핑, 워크플로우 및 프로파일링 작업을 실행함을 나타냅니다. 기본 Hadoop 가장 사용자는 로그인한 사용자입니다. 다른 Hadoop 가장 사용자를 지정하려면 지정된 사용자를 Hadoop 가장 사용자로 사용 을 선택하고 사용자 이름을 입력합니다.
환경 변수	런타임 시 통합 서비스에서 사용하는 환경 변수의 이름 및 값입니다. 운영 체제 프로파일 속성에서 LD_LIBRARY_PATH 환경 변수를 지정하는 경우 통합 서비스는 이 변수의 값을 해당 LD_LIBRARY_PATH 환경 변수에 추가합니다. 통합 서비스는 LD_LIBRARY_PATH 환경 변수 값을 사용하여 운영 체제 프로파일에 대해 생성된 하위 프로세스의 환경 변수를 설정합니다. 운영 체제 프로파일 속성에서 LD_LIBRARY_PATH 환경 변수를 지정하지 않는 경우 통합 서비스는 해당 LD_LIBRARY_PATH 환경 변수를 사용합니다. 참고: AIX에서 데이터 통합 서비스가 운영 체제 프로파일을 사용하여 매핑, 프로파일 및 워크플로우를 성공적으로 실행하려면 LD_LIBRARY_PATH 환경 변수를 INFA_HOME/services/shared/bin으로 설정해야 합니다.
플랫 파일 캐시 디렉터리	Analyst 도구가 업로드된 플랫 파일을 저장하는 플랫 파일 캐시의 디렉터리입니다. 분석 서비스가 운영 체제 프로파일을 사용하는 데이터 통합 서비스에 연결하는 경우, 운영 체제 프로파일 지정된 운영 체제 사용자에게 이 플랫 파일 캐시 디렉터리에 대한 액세스 권한이 있어야 합니다. 참조 테이블 또는 플랫 파일 소스를 가져올 경우, Analyst 도구는 이 디렉터리에 있는 파일을 사용하여 참조 테이블 또는 플랫 파일 데이터 개체를 작성합니다. 플랫 파일 위치를 변경하는 경우 분석 서비스를 다시 시작합니다.

메타데이터 액세스 서비스에 대한 운영 체제 프로필 속성

다음 테이블에는 메타데이터 액세스 서비스에 대한 운영 체제 프로필 속성이 설명되어 있습니다.

속성	설명
이름	운영 체제 프로필의 읽기 전용 이름입니다. 이름은 128자를 초과할 수 없습니다. 공백이나 다음 특수 문자를 포함할 수 없습니다. % * + \ / ? ; < >
시스템 사용자 이름	메타데이터 액세스 서비스가 실행되는 시스템에 있는 운영 체제 사용자의 읽기 전용 이름입니다. 메타데이터 액세스 서비스를 사용하면 Developer tool에서 운영 체제 사용자의 시스템 액세스 권한을 사용하여 Hadoop 연결 정보에 액세스한 후 메타데이터를 가져오고 미리 볼 수 있습니다.
Hadoop 가장 속성 활성화	메타데이터 액세스 서비스가 메타데이터를 가져오고 미리 보기 위해 Hadoop 가장 사용자를 사용함을 나타냅니다. 기본 Hadoop 가장 사용자는 로그인한 사용자입니다. 다른 Hadoop 가장 사용자를 지정하려면 지정된 사용자 를 Hadoop 가장 사용자로 사용을 선택하고 사용자 이름을 입력합니다.

운영 체제 프로필 작성

운영 체제 프로필을 작성하고 이를 사용자 및 그룹에 할당하여 보안을 강화하고 런타임 사용자 환경을 격리합니다. 하나 이상의 운영 체제 프로필을 작성할 수 있습니다. PowerCenter 통합 서비스는 운영 체제 프로필을 사용하여 워크플로우를 실행합니다. 데이터 통합 서비스는 운영 체제 프로필을 사용하여 매핑, 프로필 및 워크플로우를 실행합니다. 메타데이터 액세스 서비스는 운영 체제 프로필을 사용하여 Hadoop 연결 정보에 액세스한 후 메타데이터를 가져오고 미리 봅니다.

1. Administrator 도구에서 **보안** 탭을 클릭합니다.
2. 보안 작업 메뉴에서 **운영 체제 프로필 작성**을 클릭합니다.
운영 체제 프로필 작성 - 1/3단계 대화 상자가 나타납니다.
3. 운영 체제 프로필에 대해 다음 일반 속성을 입력합니다.

속성	설명
이름	운영 체제 프로필의 이름입니다. 이름은 대/소문자를 구분하지 않으며 도메인 내에서 고유해야 합니다. 이름은 128자를 초과하거나 @로 시작할 수 없습니다. 또한 다음 특수 문자를 포함할 수 없습니다. % * + \ / ? ; < > 첫 번째 문자와 마지막 문자를 제외하고 이름에 ASCII 공백 문자를 포함할 수 있습니다. 다른 모든 공백 문자는 사용할 수 없습니다.
시스템 사용자 이름	통합 서비스가 실행되는 시스템에 존재하는 운영 체제 사용자의 이름입니다. 통합 서비스는 운영 체제 프로필에 대해 정의된 시스템 사용자의 시스템 액세스를 사용하여 워크플로우 또는 작업을 실행합니다. 참고: 운영 체제 프로필을 작성할 때 시스템 사용자 이름을 루트로 지정하거나 uid==0 인 루트가 아닌 사용자를 사용할 수 없습니다.

4. **다음**을 클릭합니다.
운영 체제 프로필 구성 - 2/3단계 대화 상자가 나타납니다.
5. 운영 체제 프로필을 사용할 서비스를 선택합니다.

- PowerCenter 통합 서비스
 - 데이터 통합 서비스
 - 메타데이터 액세스 서비스
6. 선택한 서비스에 대한 운영 체제 프로파일 속성을 구성합니다. 메타데이터 액세스 서비스에 대한 운영 체제 프로파일 생성하려면 메타데이터 액세스 서비스와 함께 데이터 통합 서비스를 선택하고 데이터 통합 서비스에 대한 \$DISRootDir 변수를 지정해야 합니다.
 7. 서비스가 디자인 타임 또는 런타임 시 Hadoop 환경에 액세스하는 경우 다음과 같이 Hadoop 가장 속성을 구성합니다.
 - a. **Hadoop 가장 속성 활성화**를 선택합니다.
 - b. 로그인한 사용자를 사용하도록 선택하거나 Hadoop 가장 사용자를 지정하여 Hadoop 작업을 실행합니다.
 8. 필요한 경우 환경 변수를 구성합니다.
 9. 분석 서비스가 운영 체제 프로파일 사용하는 데이터 통합 서비스에 연결하는 경우 분석 서비스 속성을 구성합니다.
 10. 다음을 클릭합니다.

그룹 및 사용자를 운영 체제 프로필에 할당 - 3/3단계 대화 상자가 나타납니다.
 11. **그룹** 탭에서 그룹을 운영 체제 프로필에 다음과 같이 할당합니다.
 - a. 특정 그룹을 운영 체제 프로필에 할당하려면 하나 이상의 그룹을 선택하고 **추가**를 클릭합니다.
 - b. 사용 가능한 모든 그룹을 운영 체제 프로필에 할당하려면 **모두 추가**를 클릭합니다.
 12. 필요한 경우 운영 체제 프로필을 하나 이상의 그룹에 기본 프로파일로 할당합니다. 기본 프로필을 할당하려면 선택한 그룹 목록의 그룹에 대해 **기본 프로파일**을 선택합니다.
 13. **사용자** 탭에서 사용자를 운영 체제 프로필에 다음과 같이 할당합니다.
 - a. 특정 사용자를 운영 체제 프로필에 할당하려면 하나 이상의 사용자를 선택하고 **추가**를 클릭합니다.
 - b. 사용 가능한 모든 사용자를 운영 체제 프로필에 할당하려면 **모두 추가**를 클릭합니다.
 14. 필요한 경우 운영 체제 프로필을 하나 이상의 사용자에게 기본 프로파일로 할당합니다. 기본 프로필을 할당하려면 선택한 사용자 목록의 사용자에게 대해 **기본 프로파일**을 선택합니다.
 15. **마침**을 클릭합니다.

운영 체제 프로필을 작성하고 나면 세부 정보 패널에 운영 체제 프로파일의 속성과 프로필이 할당된 그룹 및 사용자가 표시됩니다.

운영 체제 프로파일 편집

운영 체제 프로필을 편집하여 운영 체제 프로파일 속성을 변경할 수 있습니다.

운영 체제 프로필을 작성한 다음 이름 또는 시스템 사용자 이름을 편집할 수 없습니다. 운영 체제 프로필에 지정된 운영 체제 사용자를 사용하지 않으려면 운영 체제 프로필을 삭제합니다.

1. Administrator 도구에서 **보안** 탭을 클릭합니다.
2. **운영 체제 프로파일** 보기를 선택합니다.
3. 운영 체제 프로필을 선택합니다.
4. **속성** 탭에서 **편집**을 클릭합니다.

속성 편집 대화 상자가 나타납니다.
5. 구성하려는 데이터 통합 서비스, PowerCenter 통합 서비스 또는 메타데이터 액세스 서비스를 선택합니다.
6. 서비스 속성을 편집합니다.

7. **확인**을 클릭합니다.

사용자 또는 그룹에 기본 운영 체제 프로필 할당

사용자 또는 그룹에서 둘 이상의 운영 체제 프로필에 액세스할 수 있을 때 작업 및 워크플로우 실행을 위해 통합 서비스에서 사용하는 기본 운영 체제 프로필을 할당합니다. 직접 사용 권한이 있는 운영 체제 프로필을 사용자 또는 그룹에 기본 프로필로 할당할 수 있습니다. 사용자 또는 그룹은 기본 운영 체제 프로필을 하나만 가질 수 있습니다. 하지만 동일한 운영 체제 프로필을 둘 이상의 사용자 또는 그룹에 기본 프로필로 할당할 수 있습니다.

1. 보안 탭에서 **사용자** 또는 **그룹** 보기를 선택합니다.
2. 탐색기에서 사용자 또는 그룹을 선택합니다.
3. 콘텐츠 패널에서 **사용 권한** 보기를 선택합니다.
4. **운영 체제 프로필** 탭을 클릭합니다.
5. **기본 운영 체제 프로필 할당 또는 변경** 단추를 클릭합니다.
기본 운영 체제 프로필 할당 또는 변경 대화 상자가 나타납니다.
6. **기본 운영 체제 프로필** 목록에서 프로필을 선택합니다. 또는 목록에서 **기본 운영 체제 프로필을 할당하지 않음**을 선택하여 사용자 또는 그룹에 할당된 기본 프로필을 제거합니다.
7. **확인**을 클릭합니다.

세부 정보 패널에서 **기본 프로필** 열이 운영 체제 프로필에 대해 **예(직접)**를 표시합니다.

운영 체제 프로필 삭제

운영 체제 프로필을 삭제하려면 탐색기의 운영 체제 프로필 섹션에서 운영 체제 프로필 이름을 마우스 오른쪽 단추로 클릭하고 **프로필 삭제**를 선택합니다.

운영 체제 프로필을 삭제한 후 운영 체제 프로필이 기본 프로필로 할당되었던 사용자와 그룹에 다른 운영 체제 프로필을 할당합니다. PowerCenter 통합 서비스에서 운영 체제 프로필을 사용하는 경우, 운영 체제 프로필이 할당되었던 리포지토리 폴더와 워크플로우에 다른 운영 체제 프로필을 할당합니다.

보안 도메인에서 운영 체제 프로필 작업

보안 통신이 활성화된 Informatica 도메인에서 운영 체제 프로필을 사용할 수 있습니다.

보안 통신이 활성화된 도메인에서 운영 체제 프로필을 사용하는 경우 다음 규칙 및 지침을 고려하십시오.

- 운영 체제 프로필에 대해 다음 환경 변수를 설정해야 합니다.

INFA_TRUSTSTORE

값을 보안 도메인에 대한 SSL 인증서의 트러스트 저장소 파일이 포함된 디렉터리로 설정합니다. 디렉터리에는 **infa_truststore.pem**이라는 트러스트 저장소 파일이 포함되어 있어야 합니다.

INFA_TRUSTSTORE_PASSWORD

사용자 지정 트러스트 저장소를 사용하는 경우 값을 보안 도메인을 위한 SSL 인증서를 포함하는 **infa_truststore.pem**에 대한 암호로 설정합니다. 이 암호는 암호화되어야 합니다. 명령줄 프로그램 **pmpasswd**를 사용하여 암호를 암호화하십시오.

- 또한 PowerCenter 통합 서비스가 그리드의 세션 옵션을 사용하는 경우 운영 체제 프로필에 대해 다음 환경 변수를 설정해야 합니다.

INFA_KEYSTORE

값을 보안 도메인에 대한 SSL 인증서의 키 저장소 파일이 포함된 디렉터리로 설정합니다. 디렉터리에는 **infa_keystore.pem**이라는 키 저장소 파일이 포함되어 있어야 합니다.

Administrator 도구에서 운영 체제 프로필에 대한 환경 변수를 설정할 수 있습니다. 운영 체제 프로필에 대한 환경 변수를 설정하려면 **보안 > 운영 체제 프로필**을 클릭합니다. 운영 체제 프로필의 속성을 편집하고 환경 변수를 설정합니다.

Kerberos 인증을 사용하는 도메인에서 운영 체제 프로필 작업

Kerberos 인증을 사용하는 네트워크에서 실행되는 Informatica 도메인에서 운영 체제 프로필을 사용할 수 있습니다.

Kerberos 인증을 사용하는 네트워크에서 실행되는 도메인에서 운영 체제 프로필을 사용하는 경우 다음 규칙 및 지침을 고려하십시오.

- 운영 체제 프로필의 사용자 계정은 Kerberos 인증에 사용되는 Active Directory 서비스의 사용자여야 하고 Informatica 도메인의 LDAP 보안 도메인으로 가져와야 합니다.
- 사용자 계정에는 운영 체제 프로필 사용자 계정에 액세스할 수 있는 Kerberos 자격 증명 캐시 파일이 있어야 합니다. 각 운영 체제 프로필 사용자 계정에는 별도의 자격 증명 캐시 파일이 있어야 합니다.
- 운영 체제 프로필 사용자 계정에 대한 자격 증명 캐시 파일은 전달 가능해야 합니다. 예를 들어 *kinit* 유틸리티를 사용하여 자격 증명 캐시 파일을 작성하는 경우 *-f* 옵션을 포함해야 합니다.
- 운영 체제 프로필을 사용하는 워크플로우를 실행하는 경우 운영 체제 프로필 사용자 계정에 대한 자격 증명 캐시 파일이 사용 가능해야 합니다.
- 운영 체제 프로필 사용자 계정에 대한 자격 증명 캐시 파일에는 항상 최신 자격 증명이 있어야 합니다. *cron* 과 같은 작업 스케줄러 유틸리티를 실행하면 자격 증명 캐시 파일에서 사용자 자격 증명을 정기적으로 업데이트할 수 있습니다.
- 운영 체제 프로필에 대해 다음 환경 변수를 설정해야 합니다.

INFA_OSPI_SECURITY_DOMAIN

운영 체제 프로필의 사용자 계정이 포함된 보안 도메인 이름에 값을 설정합니다. 사용자 계정이 Kerberos의 사용자 영역 보안 도메인에 있는 경우 이 변수를 설정하지 않아도 됩니다. Kerberos의 사용자 영역 보안 도메인은 설치 중 작성된 보안 도메인으로, Kerberos 사용자 영역과 이름이 동일합니다.

KRB5_CONFIG

Kerberos 구성 파일의 경로 및 파일 이름에 값을 설정합니다. Kerberos 구성 파일의 이름은 *krb5.conf* 입니다.

KRB5CCNAME

운영 체제 프로필 사용자 계정에 대한 Kerberos 자격 증명 캐시 파일의 파일 이름 및 경로에 대한 값을 설정합니다.

Administrator 도구에서 운영 체제 프로필에 대한 환경 변수를 설정할 수 있습니다. 운영 체제 프로필에 대한 환경 변수를 설정하려면 **보안 > 운영 체제 프로필**을 클릭합니다. 운영 체제 프로필의 속성을 편집하고 환경 변수를 설정합니다.

계정 잠금

Informatica 도메인에서 보안을 향상시키기 위해 관리자는 여러 번의 로그인 실패한 도메인 사용자 계정(다른 관리자 사용자 포함)을 잠글 수 있습니다.

관리자는 사용자 계정을 잠그기 전에 사용자에게 허용되는 로그인 실패 횟수를 지정할 수 있습니다. 계정이 잠긴 경우 관리자는 Informatica 도메인에서 해당 계정을 잠금 해제할 수 있습니다.

관리자가 사용자 계정을 잠금 해제할 때 관리자는 "사용자 잠금 해제 및 암호 재설정" 옵션을 선택하여 사용자 암호를 재설정할 수 있습니다. 관리자는 전자 메일을 사용자에게 보내 사용자가 도메인에 다시 로그인하기 전에 암호를 변경하도록 요청할 수 있습니다. 암호가 재설정된 경우 도메인이 사용자에게 전자 메일을 보내도록 설정하기 위해 도메인의 전자 메일 서버 설정을 구성합니다.

사용자가 Informatica 도메인 및 LDAP 서버에 대해 잠긴 경우 Informatica Administrator는 Informatica 도메인에서 사용자 계정을 잠금 해제할 수 있습니다. 또한 사용자는 LDAP 관리자가 LDAP 서버에서 사용자 계정을 잠금 해제할 때까지 Informatica 도메인에 로그인할 수 없습니다.

참고: Informatica 도메인이 Kerberos 네트워크 인증을 사용하는 경우 사용자 계정에 대한 잠금을 구성할 수 없습니다. 계정 관리 보기는 Administrator 도구의 보안 탭에서 사용할 수 없습니다.

계정 잠금 구성

계정 잠금 옵션을 선택하여 여러 번의 로그인이 실패한 Informatica 도메인의 사용자 계정을 잠급니다.

1. Administrator 도구에서 **보안 > 계정 관리**를 클릭합니다.
2. **계정 잠금 구성** 섹션에서 **편집**을 클릭합니다.
3. 다음 속성을 설정합니다.

속성	설명
계정 잠금 활성화	지정된 횟수만큼 로그인이 실패한 Informatica 도메인 사용자 계정의 잠금을 적용합니다. 기본적으로 이 옵션은 관리자 사용자 계정의 잠금은 적용하지 않습니다. 관리자 사용자 계정에 대한 잠금을 적용하려면 관리자 계정 잠금 활성화 옵션을 선택해야 합니다.
관리자 계정 잠금 활성화	지정된 횟수만큼 로그인이 실패한 Informatica 도메인 관리자 사용자 계정의 잠금을 적용합니다. 관리자 사용자 계정에 대한 잠금을 적용하려면 계정 잠금 활성화 옵션을 선택해야 합니다.
최대 로그인 시도 횟수	사용자 계정이 Informatica 도메인에서 잠기기 전에 허용되는 최대 연속 로그인 실패 횟수를 지정합니다.

계정 잠금에 대한 규칙 및 지침

Informatica 사용자에게 계정 잠금을 적용할 때 다음 규칙 및 지침을 고려하십시오.

- 응용 프로그램 서비스가 사용자 계정에서 실행되고 잘못된 암호가 응용 프로그램 서비스에 제공되는 경우 응용 프로그램 서비스가 시작하려고 할 때 사용자 계정이 잠길 수 있습니다. 데이터 통합 서비스, 웹 서비스 힙 서비스 및 PowerCenter 통합 서비스는 모델 리포지토리 서비스 또는 PowerCenter 리포지토리 서비스에 대해 인증하기 위해 사용자 이름 및 암호를 사용하는 복원 응용 프로그램 서비스입니다. 로그인이 실패한 후 데이터 통합 서비스, 웹 서비스 힙 서비스 또는 PowerCenter 통합 서비스가 계속 다시 시작하려고 시도하는 경우 도메인은 결국 관련된 사용자 계정을 잠급니다.
- LDAP 사용자 계정이 Informatica 도메인 및 LDAP 인증 서버에 대해 잠긴 경우 Informatica 도메인 관리자는 Informatica 도메인에서 계정을 잠금 해제할 수 있습니다. LDAP 관리자는 LDAP 서버에서 사용자 계정을 잠금 해제할 수 있습니다.
- Informatica 도메인 및 LDAP 서버에서 계정 잠금을 활성화하는 경우 Informatica 도메인 및 LDAP 서버에서 로그인 실패에 대해 동일한 임계값을 구성하여 계정 잠금 정책에 대한 혼란을 방지합니다.
- 계정 잠금이 Informatica 도메인에서 활성화되지 않았는데 사용자가 잠긴 경우 사용자가 LDAP 서버에서 잠기지 않았는지 확인합니다.

제 9 장

권한 및 역할

이 장에 포함된 항목:

- [권한, 131](#)
- [역할, 132](#)
- [도메인 권한, 133](#)
- [분석 서비스 권한, 140](#)
- [콘텐츠 관리 서비스 권한, 141](#)
- [데이터 통합 서비스 권한, 141](#)
- [대량 수집 서비스 권한, 142](#)
- [Metadata Manager 서비스 권한, 142](#)
- [모델 리포지토리 서비스 권한, 145](#)
- [PowerCenter 리포지토리 서비스 권한, 146](#)
- [PowerExchange 수신기 서비스 권한, 160](#)
- [PowerExchange 로거 서비스 권한, 160](#)
- [스케줄러 서비스 권한, 161](#)
- [Test Data Manager 서비스 권한, 162](#)
- [역할 관리, 165](#)
- [사용자 및 그룹에 권한 및 역할 할당, 168](#)
- [서비스에 대한 권한을 가진 사용자 보기, 169](#)
- [권한 및 역할 문제 해결, 170](#)

권한

권한에 따라 사용자가 응용 프로그램 클라이언트에서 수행할 수 있는 작업이 결정됩니다. Informatica에는 다음 권한이 포함되어 있습니다.

- 도메인 권한. 사용자가 Administrator 도구, infacmd 및 pmrep 명령줄 프로그램을 사용하여 Informatica 도메인에서 수행할 수 있는 작업을 결정할 수 있습니다.
- 분석 서비스 권한. 사용자가 Informatica Analyst를 사용하여 수행할 수 있는 작업을 결정합니다.
- 콘텐츠 관리 서비스 권한. 사용자가 Informatica Developer tool 및 Informatica Analyst 도구의 참조 테이블을 사용하여 수행할 수 있는 작업을 결정합니다.

- 데이터 통합 서비스 권한. 사용자가 **Administrator** 도구 및 **infacmd** 명령줄 프로그램을 사용하여 수행할 수 있는 응용 프로그램에 대한 작업을 결정합니다. 또한 이 권한은 사용자가 프로필 결과를 드릴다운하고 내보낼 수 있는지 여부를 결정합니다.
- 대량 수집 서비스 권한. 사용자가 대량 수집 도구를 사용하여 수행할 수 있는 작업을 결정합니다.
- **Metadata Manager** 서비스 권한. 사용자가 **Metadata Manager**를 사용하여 수행할 수 있는 작업을 결정합니다.
- 모델 리포지토리 서비스 권한. 사용자가 **Informatica Analyst** 및 **Informatica Developer**를 사용하여 수행할 수 있는 프로젝트에 대한 작업을 결정합니다.
- **PowerCenter** 리포지토리 서비스 권한. 사용자가 **Repository Manager**, 디자이너, 워크플로우 관리자, **Workflow Monitor**, **pmrep** 및 **pmcmd** 명령줄 프로그램을 사용하여 수행할 수 있는 **PowerCenter** 리포지토리 작업을 결정합니다.
- **PowerExchange** 응용 프로그램 서비스 권한. 사용자가 **infacmd pwx** 명령을 사용하여 **PowerExchange Listener** 서비스 및 **PowerExchange Logger** 서비스에서 수행할 수 있는 작업을 결정합니다.
- 스케줄러 서비스 권한. 사용자가 스케줄러 서비스를 사용하여 수행할 수 있는 작업을 결정할 수 있습니다.
- **Test Data Manager** 서비스 권한. 사용자가 **Test Data Manager**를 사용하여 수행할 수 있는 데이터 검색, 데이터 마스킹, 데이터 하위 집합 및 **Test Data Generation** 태스크를 결정합니다.

권한을 응용 프로그램 서비스의 사용자 및 그룹에 할당합니다. 다른 권한을 동일한 서비스 유형의 각 응용 프로그램 서비스에 대한 사용자에게 할당할 수 있습니다.

Administrator 도구의 **보안 탭**에서 권한을 사용자 및 그룹에 할당합니다.

Administrator 도구는 권한을 수준으로 구성합니다. 권한은 그 권한이 포함하는 권한 아래 나열됩니다. 일부 권한은 다른 권한을 포함합니다. 권한을 사용자 및 그룹에 할당하는 경우 **Administrator** 도구는 포함된 권한도 할당합니다.

권한 그룹

도메인 및 응용 프로그램 서비스 권한은 권한 그룹으로 구성됩니다. 권한 그룹은 일반 사용자 작업을 정의하는 권한 조직입니다. 예를 들어 도메인 권한은 다음 권한 그룹을 포함합니다.

- 도구. **Administrator** 도구에 로그인을 위한 권한을 포함합니다.
- 보안 관리. 사용자, 그룹, 역할 및 권한 관리를 위한 권한을 포함합니다.
- 도메인 관리. 도메인, 폴더, 노드, 그리드, 라이선스 및 응용 프로그램 서비스 관리를 위한 권한을 포함합니다.

팁: 권한을 사용자 및 사용자 그룹에 할당할 때 권한 그룹을 선택하여 그룹의 모든 권한을 할당할 수 있습니다.

역할

역할은 사용자 또는 그룹에 할당한 권한의 컬렉션입니다. 사용자가 개발자, 관리자, 기본 사용자 또는 고급 사용자이든 조직 내의 각 사용자에게는 특정한 역할이 있습니다.

예를 들어 **PowerCenter** 개발자 역할에는 개발자가 수행하는 모든 **PowerCenter** 리포지토리 서비스 권한 또는 작업이 포함됩니다.

역할을 도메인 및 도메인의 응용 프로그램 서비스에 대한 사용자 및 그룹에 할당합니다.

팁: 사용자를 그룹으로 구성한 다음 역할 및 사용 권한을 그룹에 할당하는 경우 사용자 관리 태스크를 간소화할 수 있습니다. 예를 들어 사용자가 조직에서 위치를 변경하는 경우 사용자를 다른 그룹으로 이동합니다. 새 사용자가 해당 조직에 들어오면 해당 사용자를 그룹에 추가합니다. 사용자는 그룹에 할당된 역할 및 사용 권한을 상

속받습니다. 권한, 역할 및 사용 권한을 재할당하지 않아도 됩니다. 자세한 내용은 다음 Informatica How-To Library 문서를 참조하십시오. [Using Groups and Roles to Manage Access Controls](#).

도메인 권한

도메인 권한에 따라 사용자가 Administrator 도구와 infacmd 및 pmrep 명령줄 프로그램을 사용하여 수행할 수 있는 작업이 결정됩니다.

다음 테이블에는 각 도메인 권한 그룹이 설명되어 있습니다.

권한 그룹	설명
보안 관리	사용자, 그룹, 역할 및 권한 관리를 위한 권한을 포함합니다.
도메인 관리	도메인, 폴더, 노드, 그리드, 라이선스, 응용 프로그램 서비스, 연결 및 클러스터 구성 관리를 위한 권한을 포함합니다.
모니터링	모니터링 통계 및 보고서 구성, 통합 개체에 대한 모니터링 보기 및 모니터링 액세스를 위한 권한을 포함합니다.
도구	Administrator 도구에 로그인을 위한 권한을 포함합니다.
Cloud 관리	Administrator 도구에서 Informatica Cloud 조직을 추가하고 보기 위한 권한을 포함합니다.

보안 관리 권한 그룹

보안 관리 권한 그룹의 권한 및 도메인 개체 사용 권한에 따라 사용자가 수행할 수 있는 보안 관리 작업이 결정됩니다.

일부 보안 관리 태스크는 권한 또는 사용 권한이 아닌 관리자 역할에 따라 결정됩니다. 도메인의 관리자 역할이 할당된 사용자는 다음 태스크를 완료할 수 있습니다.

- 운영 체제 프로필을 작성, 편집 및 삭제합니다.
- 운영 체제 프로필에 대한 권한 부여

참고: Administrator 도구에서 보안 관리 태스크를 완료하려면 사용자에게 Informatica Administrator 액세스 권한도 있어야 합니다.

권한 및 역할 부여 권한

권한 및 역할 부여 권한이 할당된 사용자는 권한 및 역할을 사용자 및 그룹에 할당할 수 있습니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 권한 및 역할 부여 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한 대상	설명
도메인 또는 응용 프로그램 서비스	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> - 권한 및 역할을 도메인 또는 응용 프로그램 서비스의 사용자 및 그룹에 할당 - 사용자 및 그룹에 할당된 권한 및 역할을 편집 및 제거

사용자, 그룹 및 역할 관리 권한

사용자, 그룹 및 역할 관리 권한이 할당된 사용자는 LDAP 인증을 구성하고 사용자, 그룹 및 역할을 관리할 수 있습니다.

사용자, 그룹 및 역할 관리 권한에는 권한 및 역할 부여 권한이 포함됩니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 사용자, 그룹 및 역할 관리 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한 대상	설명
-	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none">- 도메인에 대한 LDAP 인증 구성- 사용자, 그룹, 역할 작성, 편집 및 삭제- LDAP 사용자 및 그룹 가져오기
운영 체제 프로필	사용자가 운영 체제 프로필 속성을 편집할 수 있습니다.

도메인 관리 권한 그룹

사용자가 수행할 수 있는 도메인 관리 작업은 도메인 관리 그룹의 권한 및 도메인 개체에 대한 사용 권한에 따라 다릅니다.

일부 도메인 관리 태스크는 권한 또는 사용 권한이 아닌 관리자 역할에 따라 결정됩니다. 도메인의 관리자 역할이 할당된 사용자는 다음 태스크를 완료할 수 있습니다.

- 도메인 속성 구성
- 클러스터 구성 설정
- 도메인에 대한 사용 권한 부여
- 로그 이벤트 관리 및 제거
- 도메인 알림 수신
- 라이선스 보고서 실행
- 사용자 활동 로그 이벤트 보기
- 도메인을 종료합니다.
- 서비스 업그레이드 마법사 액세스

권한이 아닌 도메인 개체 사용 권한이 할당된 사용자는 일부 도메인 관리 태스크를 완료할 수 있습니다. 다음 테이블에는 도메인 개체 사용 권한만 할당된 경우 사용자가 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한 대상	설명
도메인	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none">- 도메인 속성 및 로그 이벤트 보기- 모니터링 설정을 구성합니다.
폴더	사용자가 폴더 속성을 볼 수 있습니다.
응용 프로그램 서비스	사용자가 응용 프로그램 서비스 속성 및 로그 이벤트를 볼 수 있습니다.
라이선스 개체	사용자가 라이선스 개체 속성을 볼 수 있습니다.

사용 권한 대상	설명
그리드	사용자가 그리드 속성을 볼 수 있습니다.
노드	사용자가 노드 속성을 볼 수 있습니다.
웹 서비스 헵	사용자가 웹 서비스 보고서를 실행할 수 있습니다.

참고: Administrator 도구에서 도메인 관리 태스크를 완료하려면 사용자에게 Informatica Administrator 액세스 권한도 있어야 합니다.

서비스 실행 관리 권한

서비스 실행 관리 권한이 할당된 사용자는 응용 프로그램 서비스를 활성화 및 비활성화하고 응용 프로그램 서비스 알림을 받을 수 있습니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 서비스 실행 관리 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한 대상	설명
응용 프로그램 서비스	<p>사용자가 다음 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> 응용 프로그램 서비스 및 서비스 프로세스 활성화 및 비활성화. Metadata Manager 서비스를 활성화하고 비활성화하려면 사용자에게 연결된 PowerCenter 통합 서비스 및 PowerCenter 리포지토리 서비스에 대한 사용 권한도 있어야 합니다. 응용 프로그램 서비스 알림 받기

서비스 관리 권한

서비스 관리 권한이 할당된 사용자는 응용 프로그램 서비스 및 라이선스 개체에 대한 사용 권한을 작성, 구성, 이동, 제거 및 부여할 수 있습니다.

서비스 관리 권한에는 서비스 실행 관리 권한이 포함됩니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 서비스 관리 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한 대상	설명
도메인 또는 상위 폴더	사용자가 라이선스 개체를 작성할 수 있습니다.
도메인 또는 상위 폴더, 응용 프로그램 서비스가 실행되는 노드 또는 그리드, 라이선스 개체, 연결된 응용 프로그램 서비스	사용자가 응용 프로그램 서비스를 작성할 수 있습니다.
응용 프로그램 서비스	<p>사용자가 다음 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> 응용 프로그램 서비스 구성 응용 프로그램 서비스에 대한 사용 권한 부여
원래 폴더 및 대상 폴더	사용자가 한 폴더에서 다른 폴더로 응용 프로그램 서비스 또는 라이선스 개체를 이동할 수 있습니다.

사용 권한 대상	설명
도메인 또는 상위 폴더 및 응용 프로그램 서비스	사용자가 응용 프로그램 서비스를 제거할 수 있습니다.
분석 서비스	사용자가 감사 내역 테이블을 작성하고 삭제할 수 있습니다.
Metadata Manager 서비스	<p>사용자가 다음 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> - Metadata Manager 리포지토리 콘텐츠 백업. - Metadata Manager 리포지토리 콘텐츠 삭제. - Metadata Manager 서비스의 콘텐츠 업그레이드 <p>참고: Metadata Manager 리포지토리 콘텐츠를 작성 또는 복원하려면 사용자가 기본 관리자 그룹에 속해야 합니다.</p>
Metadata Manager 서비스 PowerCenter 리포지토리 서비스	사용자가 Metadata Manager에 대한 PowerCenter 리포지토리를 복원할 수 있습니다.
모델 리포지토리 서비스	<p>사용자가 다음 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> - 모델 리포지토리 콘텐츠 작성 및 삭제 - 검색 인덱스 작성, 삭제 및 다시 인덱싱 - 작업 메뉴 또는 명령줄에서 모델 리포지토리 서비스의 콘텐츠를 업그레이드합니다. 사용자에게 모델 리포지토리 서비스에 대한 프로젝트 작성, 편집, 삭제 권한 및 프로젝트에 대한 쓰기 권한도 있어야 합니다.
PowerCenter 통합 서비스	사용자가 안전 모드에서 PowerCenter 통합 서비스를 실행할 수 있습니다.
PowerCenter 리포지토리 서비스	<p>사용자가 다음 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> - PowerCenter 리포지토리 백업, 복원 및 업그레이드 - PowerCenter 리포지토리에 대한 데이터 연계 구성 - 다른 PowerCenter 리포지토리에서 콘텐츠 복사 - 사용자 연결 닫기 및 PowerCenter 리포지토리 잠금 해제 - PowerCenter 리포지토리 콘텐츠 작성 및 삭제 - PowerCenter Repository Manager에서 재사용 가능 메타데이터 확장 작성, 편집 및 삭제 - PowerCenter 리포지토리에 대한 버전 제어 활성화 - PowerCenter 리포지토리 도메인 관리 - PowerCenter Repository Manager의 리포지토리 수준에서 개체 버전의 고급 제거 수행 - PowerCenter 리포지토리 플러그인 등록 및 등록 해제 - 제외 모드에서 PowerCenter 리포지토리 실행 - 사용자에게 PowerCenter 리포지토리 알림 전송 - PowerCenter 리포지토리 통계 업데이트 - PowerCenter 리포지토리 서비스의 콘텐츠 업그레이드
Test Data Manager 서비스	<p>사용자가 다음 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> - Test Data Manager 리포지토리 콘텐츠 작성 및 삭제 - Test Data Manager 서비스의 콘텐츠 업그레이드
라이선스 개체	<p>사용자가 다음 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> - 라이선스 개체 편집 - 라이선스 개체에 대한 사용 권한 부여
라이선스 개체 및 응용 프로그램 서비스	사용자가 응용 프로그램 서비스에 라이선스를 할당할 수 있습니다.
도메인 또는 상위 폴더 및 라이선스 개체	사용자가 라이선스 개체를 제거할 수 있습니다.

노드 및 그리드 관리 권한

노드 및 그리드 관리 권한이 할당된 사용자는 노드 및 그리드에 대한 사용 권한을 작성, 구성, 이동, 제거, 종료 및 부여할 수 있습니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 노드 및 그리드 관리 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한 대상	설명
도메인 또는 상위 폴더	사용자가 노드를 작성할 수 있습니다.
도메인 또는 상위 폴더 및 그리드에 할당된 노드	사용자가 그리드를 작성할 수 있습니다.
노드 또는 그리드	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none">- 노드 및 그리드 구성 및 종료- 노드 및 그리드에 대한 권한 부여
원래 폴더 및 대상 폴더	사용자가 한 폴더에서 다른 폴더로 노드 및 그리드를 이동할 수 있습니다.
도메인 또는 상위 폴더 및 노드 또는 그리드	사용자가 노드 및 그리드를 제거할 수 있습니다.

도메인 폴더 관리 권한

도메인 폴더 관리 권한이 할당된 사용자는 도메인 폴더에 대한 사용 권한을 작성, 편집, 이동, 제거 및 부여할 수 있습니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 도메인 폴더 관리 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한 대상	설명
도메인 또는 상위 폴더	사용자가 폴더를 작성할 수 있습니다.
폴더	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none">- 폴더 편집- 폴더에 대한 사용 권한 부여
원래 폴더 및 대상 폴더	사용자가 상위 폴더에서 다른 폴더로 폴더를 이동할 수 있습니다.
도메인 또는 제거되는 상위 폴더 및 폴더	사용자가 폴더를 제거할 수 있습니다.

연결 관리 권한

연결 관리 권한이 할당된 사용자는 Administrator 도구, Analyst 도구, Developer 도구 및 infacmd 명령줄 프로그램에서 연결을 작성, 편집 및 삭제할 수 있습니다. 또한 사용자는 Developer 도구에서 연결을 복사하고 Administrator 도구 및 infacmd 명령줄 프로그램에서 연결에 대한 사용 권한을 부여할 수 있습니다.

연결 관리 권한이 할당된 사용자는 Administrator 도구 및 infacmd 명령줄 프로그램에서 클러스터 구성을 생성하고 새로 고치고 삭제할 수 있으며 구성 속성을 설정하고 지울 수 있습니다.

연결 관리 권한이 아닌 연결 사용 권한이 할당된 사용자는 다음 연결 관리 작업을 수행할 수 있습니다.

- 암호를 제외한 모든 연결 메타데이터 보기. 연결에 대한 읽기 권한이 필요합니다.
- 데이터를 미리 보거나 매핑, 성과 기록표 또는 프로필 실행. 연결에 대한 실행 권한이 필요합니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 연결 관리 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
-	또한 사용자는 연결과 클러스터 구성을 생성할 수 있습니다.
연결에 대한 쓰기	사용자가 연결을 복사, 편집 및 삭제할 수 있습니다.
연결에 대한 부여	사용자가 연결에 대한 사용 권한을 부여 및 취소할 수 있습니다.
클러스터 구성에 대한 쓰기	사용자는 클러스터 구성을 생성하고 새로 고치고 삭제할 수 있습니다. 사용자는 클러스터 구성 속성을 설정하고 지울 수 있습니다.

모니터링 권한 그룹

모니터링 권한 그룹의 권한에 따라 모니터링을 보고 구성할 수 있는 사용자가 결정됩니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 모니터링 관리 그룹의 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

상위 권한	권한	사용 권한 대상	설명
모니터링 관리	모니터링 구성	도메인	사용자가 모니터링 설정을 구성할 수 있습니다.
모니터링 관리	보고서 및 통계 설정	도메인	사용자가 모니터링 통계 및 보고서를 구성할 수 있습니다.
보기	사용자가 속한 그룹에 있는 모든 사용자의 작업 보기	도메인	그룹의 사용자는 그룹의 다른 사용자가 실행하는 작업을 모니터링할 수 있습니다. 사용자가 여러 그룹에 속하는 경우 사용자는 모든 그룹의 작업을 볼 수 있습니다.
사용자가 속한 그룹에 있는 모든 사용자의 작업 보기	다른 사용자의 작업 보기	도메인	사용자가 다른 사용자의 작업을 볼 수 있습니다.
보기	통계 보기	도메인	사용자가 도메인 개체에 대한 요약 통계 보기 및 통계를 볼 수 있습니다. 참고: Kerberos 인증을 사용하는 도메인에서 사용자가 요약 통계 보기 및 도메인 개체에 대한 통계를 보려면 모니터링 모델 리포지토리 서비스에 대한 관리자 역할도 있어야 합니다.
보기	보고서 보기	도메인	사용자가 도메인 개체에 대한 보고서를 볼 수 있습니다.
모니터링 액세스	Analyst 도구에서 액세스	도메인	사용자가 Analyst 도구의 작업 상태 작업 공간에 액세스할 수 있습니다.

상위 권한	권한	사용 권한 대상	설명
모니터링 액세스	Developer tool에서 액세스	도메인	사용자가 Developer tool에서 모니터링 도구에 액세스할 수 있습니다.
모니터링 액세스	Administrator 도구에서 액세스	도메인	사용자가 Administrator 도구의 모니터 탭에 액세스할 수 있습니다.
해당 없음	작업에 대해 동작 수행	도메인	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> - 작업 중단 - 매핑 작업 다시 시작 - 작업 로그 보기

모니터링 도구에 액세스하는 경우에는 사용자에게 Informatica Administrator 액세스 권한이 없어도 됩니다.

도구 권한 그룹

도메인 도구 그룹의 권한에 따라 Administrator 도구에 액세스할 수 있는 사용자가 결정됩니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 도구 그룹의 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

권한	설명
Informatica Administrator 액세스	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> - Administrator 도구에 로그인합니다. - Administrator 도구에서 고유한 사용자 계정 관리 - 로그 이벤트 내보내기

사용자에게 Informatica Administrator 액세스 권한이 있어야 Administrator 도구에서 태스크를 완료할 수 있습니다. infacmd 명령을 실행하거나 모니터링 도구에 액세스하는 경우에는 사용자에게 Informatica Administrator 액세스 권한이 없어도 됩니다.

Cloud 관리 권한 그룹

Cloud 관리 그룹의 권한에 따라 Informatica Cloud 조직을 보고 구성할 수 있는 사용자가 결정됩니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 Cloud 관리 그룹의 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

권한	사용 권한 대상	설명
조직 보기	도메인	사용자가 Informatica Cloud 조직 과 연결된 보안 에이전트 및 클라우드 연결을 볼 수 있습니다.
조직 관리	도메인	사용자가 Administrator 도구에서 Informatica Cloud 조직을 추가할 수 있습니다.

분석 서비스 권한

분석 서비스 권한에 따라 라이선스 사용자가 **Analyst** 도구를 사용하여 프로젝트에 대해 수행할 수 있는 작업이 결정됩니다.

다음 테이블에는 권한 및 프로젝트 및 프로젝트의 개체를 관리하기 위해 필요한 사용 권한이 나열되어 있습니다.

권한	사용 권한	설명
프로필 및 성과 기록표 실행	프로젝트에 대한 읽기 관계형 데이터 소스 연결에 대한 실행	사용자가 Analyst 도구에서 라이선스 사용자의 프로필 및 성과 기록표를 실행할 수 있습니다.
매핑 사양 액세스	프로젝트에 대한 읽기	사용자가 Analyst 도구에서 라이선스 사용자의 매핑 사양에 액세스할 수 있습니다.
매핑 사양 결과 로드	프로젝트에 대한 쓰기	사용자가 라이선스 사용자의 매핑 사양 결과를 테이블 또는 플랫폼 파일에 로드할 수 있습니다. 참고: 이 권한을 선택하면 매핑 사양 액세스 권한도 기본적으로 부여합니다.
용어집 관리	-	사용자가 비즈니스 용어집을 관리할 수 있습니다.
용어집 보기	-	사용자가 라이브러리 작업 공간에서 게시된 Business Glossary 자산을 볼 수 있습니다. 이는 용어집 보안 작업 공간에서 용어집 및 용어집 자산에 대한 읽기 권한을 제공하는 것과 동일합니다.
작업 공간 액세스	-	사용자가 Analyst 도구에서 다음 작업 공간에 액세스할 수 있습니다. - 디자인 작업 공간 - 검색 작업 공간 - 용어집 작업 공간 - 성과 기록표 작업 공간 참고: 이 권한을 선택하면 Analyst 도구에서 프로젝트에 대한 액세스 권한도 부여합니다. 사용자에게 이 권한이 없는 경우 프로젝트에 액세스하려면 사용자에게 디자인 작업 공간 , 검색 작업 공간 , 용어집 작업 공간 또는 성과 기록표 작업 공간 권한 중 하나가 있어야 합니다.
디자인 작업 공간	-	사용자가 디자인 작업 공간에 액세스할 수 있습니다.
검색 작업 공간	-	사용자가 검색 작업 공간에 액세스할 수 있습니다.
용어집 작업 공간	-	사용자가 용어집 작업 공간에 액세스할 수 있습니다.
성과 기록표 작업 공간	-	사용자가 성과 기록표 작업 공간에 액세스할 수 있습니다.

콘텐츠 관리 서비스 권한

콘텐츠 관리 서비스 권한에 따라 라이선스 사용자가 참조 테이블에서 수행할 수 있는 작업이 결정됩니다.

다음 테이블에는 참조 테이블을 관리하기 위해 필요한 권한 및 사용 권한이 나열되어 있습니다.

권한	사용 권한	설명
참조 테이블 작성	프로젝트에 대한 쓰기	<ul style="list-style-type: none"> - Analyst 및 Developer 도구에서 참조 테이블 작성 - infacmd rtm 가져오기를 사용하여 참조 테이블 작성 - 참조 테이블 개체를 모델 리포지토리로 가져오기 - Analyst 및 Developer 도구에서 참조 테이블 복사 - 프로필 데이터에서 참조 테이블 작성 참고: 기본적으로 작성 권한은 편집 권한도 부여합니다.
참조 테이블 데이터 및 메타데이터 편집	프로젝트에 대한 읽기	<ul style="list-style-type: none"> - Developer 도구 및 Analyst 도구에서 참조 테이블 데이터 값 편집 - 참조 테이블에 프로필 데이터 추가 - 참조 테이블에서 열 추가 또는 삭제, 열 이름, 설명 및 기본값과 같은 참조 테이블 메타데이터 변경

데이터 통합 서비스 권한

데이터 통합 서비스 권한에 따라 Administrator 도구 및 infacmd 명령줄 프로그램을 사용하여 사용자가 응용 프로그램에서 수행할 수 있는 작업이 결정됩니다. Analyst 도구 및 Developer 도구를 사용하여 사용자가 프로필 결과를 드릴다운하고 내보낼 수 있는지 여부도 결정됩니다.

다음 테이블에는 사용자가 응용 프로그램 관리 권한 그룹의 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

권한 이름	설명
응용 프로그램 관리	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> - 파일에 응용 프로그램 백업 및 복원 - 데이터 통합 서비스에 응용 프로그램 배포 및 이름 충돌 해결 - 배포 후 응용 프로그램 시작 - 응용 프로그램 찾기 - 응용 프로그램에서 개체 시작 또는 중지 - 응용 프로그램 속성 구성

다음 테이블에는 필요한 사용 권한 및 사용자가 프로파일링 관리 권한 그룹의 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

권한 이름	사용 권한 대상	설명
결과 드릴다운 및 내보내기	프로젝트에 대한 읽기 또한 관계형 데이터 소스 연결에 대한 실행이 라이브 데이터에서 드릴다운하는 데 필요합니다.	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> - 프로파일링 결과 드릴다운 - 프로파일링 결과 내보내기

대량 수집 서비스 권한

대량 수집 서비스 권한은 사용자가 대량 수집 도구를 사용하여 수행할 수 있는 작업을 결정합니다.

다음 테이블에는 사용자가 대량 수집 서비스 관련 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

권한	설명
대량 수집 사양 액세스	사용자는 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none">- 모든 대량 수집 사양 찾기- 대량 수집 사양 편집- 대량 수집 사양 실행- 대량 수집 사양 삭제

참고: 도메인에서 대량 수집 사양 액세스 권한 또는 관리자 역할이 할당되지 않은 사용자는 자신이 직접 생성한 대량 수집 사양에 대해서만 이러한 작업을 수행할 수 있습니다.

Metadata Manager 서비스 권한

Metadata Manager 서비스 권한에 따라 사용자가 Metadata Manager를 사용하여 수행할 수 있는 Metadata Manager 작업이 결정됩니다.

다음 테이블에는 각 Metadata Manager 권한 그룹이 설명되어 있습니다.

권한 그룹	설명
카탈로그	Metadata Manager 인터페이스의 찾기보기 페이지에서 개체를 관리하기 위한 권한을 포함합니다.
로드	Metadata Manager 인터페이스의 로드 페이지에서 개체를 관리하기 위한 권한을 포함합니다.
모델	Metadata Manager 인터페이스의 모델 페이지에서 개체를 관리하기 위한 권한을 포함합니다.
보안	Metadata Manager 인터페이스의 보안 페이지에서 개체를 관리하기 위한 권한을 포함합니다.

카탈로그 권한 그룹

카탈로그 권한 그룹의 권한에 따라 사용자가 **Metadata Manager** 응용 프로그램의 **찾아보기** 탭에서 수행할 수 있는 태스크가 결정됩니다. 특정 작업을 수행하기 위한 권한이 있는 사용자는 특정 개체에 대한 작업을 수행하기 위한 사용 권한도 필요합니다. **Metadata Manager** 응용 프로그램의 **보안** 탭에서 사용 권한을 구성합니다.

다음 테이블에는 카탈로그 권한 그룹의 권한 및 개체에 대한 태스크를 수행하기 위해 필요한 사용 권한이 나열되어 있습니다.

권한	포함되는 권한	사용 권한	설명
바로 가기 공유	해당 없음	쓰기	사용자가 바로 가기가 포함된 폴더를 다른 사용자 및 그룹과 공유할 수 있습니다.
연계 보기	해당 없음	읽기	사용자가 다음 작업을 수행할 수 있습니다. - 메타데이터 개체, 범주 및 비즈니스 용어에서 데이터 연계 분석 실행 - PowerCenter Designer에서 데이터 연계 분석 실행. 사용자에게 PowerCenter 리포지토리 폴더에 대한 읽기 권한도 있어야 합니다.
관련 카탈로그 보기	해당 없음	읽기	사용자가 관련된 카탈로그를 볼 수 있습니다.
프로필 결과 보기	해당 없음	읽기	사용자가 관계형 소스의 카탈로그에서 메타데이터 개체에 대한 프로파일링 정보를 볼 수 있습니다.
카탈로그 보기	해당 없음	읽기	사용자가 다음 작업을 수행할 수 있습니다. - 메타데이터 카탈로그에서 리소스 및 메타데이터 개체 보기 - 메타데이터 카탈로그 검색
관계 보기	해당 없음	읽기	사용자가 메타데이터 개체, 범주 및 비즈니스 용어에 대한 관계를 볼 수 있습니다.
관계 관리	관계 보기	쓰기	사용자가 사용자 지정 메타데이터 개체, 범주 및 비즈니스 용어에 대한 관계를 작성, 편집 및 삭제할 수 있습니다.
설명 보기	해당 없음	읽기	사용자가 메타데이터 개체, 범주 및 비즈니스 용어에 대한 설명을 볼 수 있습니다.
설명 게시	설명 보기	쓰기	사용자가 메타데이터 개체, 범주 및 비즈니스 용어에 대한 설명을 추가할 수 있습니다.
설명 삭제	- 설명 게시 - 설명 보기	쓰기	사용자가 메타데이터 개체, 범주 및 비즈니스 용어에 대한 설명을 삭제할 수 있습니다.
링크 보기	해당 없음	읽기	사용자가 메타데이터 개체, 범주 및 비즈니스 용어에 대한 링크를 볼 수 있습니다.
링크 관리	링크 보기	쓰기	사용자가 메타데이터 개체, 범주 및 비즈니스 용어에 대한 링크를 작성, 편집 및 삭제할 수 있습니다.

권한	포함되는 권한	사용 권한	설명
용어집 보기	해당 없음	읽기	사용자가 다음 작업을 수행할 수 있습니다. - 용어집 보기에서 비즈니스 용어집 보기 - 비즈니스 용어집 검색
개체 관리	해당 없음	쓰기	사용자가 다음 작업을 수행할 수 있습니다. - 카탈로그에서 메타데이터 개체 편집 - 사용자 지정 메타데이터 개체 작성, 편집 및 삭제. 사용자에게 모델 보기 권한도 있어야 합니다. - 사용자 지정 메타데이터 리소스 작성, 편집 및 삭제. 사용자에게 리소스 관리 권한도 있어야 합니다.

로드 권한 그룹

로드 권한 그룹의 권한에 따라 사용자가 **Metadata Manager** 응용 프로그램의 **로드** 탭에서 수행할 수 있는 테스트가 결정됩니다. 특정 작업을 수행하기 위한 권한이 있는 사용자는 특정 개체에 대한 작업을 수행하기 위한 사용 권한도 필요합니다. **Metadata Manager** 응용 프로그램의 **보안** 탭에서 사용 권한을 구성합니다.

다음 표에는 **Metadata Manager** 웨어하우스에서 리소스의 인스턴스를 관리하는 데 필요한 권한과 사용 권한이 나열되어 있습니다.

권한	포함되는 권한	사용 권한	설명
리소스 보기	-	읽기	사용자가 다음 작업을 수행할 수 있습니다. - Metadata Manager 웨어하우스의 리소스 및 리소스 속성 보기 - 리소스 구성 내보내기 - Metadata Manager 에이전트 설치 프로그램 다운로드
리소스 로드	리소스 보기	쓰기	사용자가 다음 작업을 수행할 수 있습니다. - Metadata Manager 웨어하우스로 리소스의 메타데이터 로드* - 데이터 연계를 위해 연결된 리소스의 개체 간 링크 작성 - 리소스에 대한 검색 인덱싱 구성 - 리소스 구성 가져오기
일정 관리	리소스 보기	쓰기	사용자가 다음 작업을 수행할 수 있습니다. - 일정 작성 및 편집 - 리소스에 일정 추가
메타데이터 제거	리소스 보기	쓰기	사용자가 Metadata Manager 웨어하우스에서 리소스에 대한 메타데이터를 제거할 수 있습니다.
리소스 관리	- 메타데이터 제거 - 리소스 보기	쓰기	사용자가 리소스를 작성, 편집 및 삭제할 수 있습니다.
* Business Glossary 리소스의 메타데이터를 로드하려면 리소스 로드, 리소스 관리 및 모델 보기 권한이 필요합니다.			

모델 권한 그룹

모델 권한 그룹의 권한에 따라 사용자가 **Metadata Manager** 응용 프로그램의 **모델** 탭에서 수행할 수 있는 태스크가 결정됩니다. 모델에 대한 사용 권한을 구성할 수 없습니다.

다음 테이블에는 모델을 관리하기 위해 필요한 권한이 나열되어 있습니다.

권한	포함되는 권한	사용 권한	설명
모델 보기	-	-	사용자가 모델 및 클래스를 열고 모델 및 클래스 속성을 볼 수 있습니다. 클래스의 관계 및 특성을 봅니다.
모델 관리	모델 보기	-	사용자가 사용자 지정 모델을 작성, 편집 및 삭제할 수 있습니다. 패키징된 모델 및 범용 모델에 특성을 추가합니다.
모델 가져오기/내보내기	모델 보기	-	사용자가 사용자 지정 모델을 가져오고 내보낼 수 있습니다. 수정된 패키지 모델 및 범용 모델을 가져오고 내보냅니다.

보안 권한 그룹

보안 권한 그룹의 권한에 따라 사용자가 **Metadata Manager** 응용 프로그램의 **보안** 탭에서 수행할 수 있는 태스크가 결정됩니다.

기본적으로 보안 권한 그룹의 카탈로그 사용 권한 관리 권한이 **Metadata Manager** 서비스에서 관리자 또는 관리자 역할이 있는 사용자에게 할당됩니다. 카탈로그 사용 권한 관리 권한을 다른 사용자에게 할당할 수 있습니다.

다음 표에는 **Metadata Manager** 보안을 관리하기 위해 필요한 권한과 사용 권한이 나열되어 있습니다.

권한	포함되는 권한	사용 권한	설명
카탈로그 사용 권한 관리	-	모든 권한	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none">- 리소스, 메타데이터 개체, 범주 및 비즈니스 용어에 대한 사용자 및 그룹 사용 권한 할당- 리소스, 메타데이터 개체, 범주 및 비즈니스 용어에 대한 사용 권한 편집

모델 리포지토리 서비스 권한

모델 리포지토리 서비스 권한에 따라 사용자가 **Informatica Analyst** 및 **Informatica Developer**를 사용하여 프로젝트에 대해 수행할 수 있는 작업이 결정됩니다.

모델 리포지토리 개체 사용 권한에 따라 사용자가 프로젝트의 개체에 대해 완료할 수 있는 태스크가 결정됩니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 모델 리포지토리 서비스 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

권한	사용 권한	설명
해당 없음	프로젝트에 대한 읽기	사용자가 프로젝트 및 프로젝트의 개체를 볼 수 있습니다.
해당 없음	프로젝트에 대한 쓰기	사용자가 프로젝트의 개체를 작성, 편집 및 삭제할 수 있습니다.
해당 없음	프로젝트에 대한 부여	사용자가 사용자 및 그룹의 프로젝트에 대한 사용 권한을 부여 및 취소할 수 있습니다.
분석 액세스	해당 없음	사용자가 Analyst 도구에서 모델 리포지토리에 액세스할 수 있습니다.
Developer 액세스	해당 없음	사용자가 Developer tool에서 모델 리포지토리에 액세스할 수 있습니다.
프로젝트 작성, 편집 및 삭제	해당 없음	사용자가 프로젝트를 작성할 수 있습니다.
프로젝트 작성, 편집 및 삭제	프로젝트에 대한 쓰기	<p>사용자가 다음 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> - 프로젝트 편집 - 사용자가 프로젝트를 작성한 경우 프로젝트 삭제 - 모델 리포지토리 서비스의 콘텐츠 업그레이드. 작업 메뉴 또는 명령줄에서 서비스를 업그레이드하려면 사용자에게 도메인에 대한 서비스 관리 권한 및 모델 리포지토리 서비스에 대한 사용 권한도 있어야 합니다. 서비스 업그레이드 마법사를 사용하여 서비스를 업그레이드하려면 사용자에게 도메인에 대한 관리자 역할도 있어야 합니다.
데이터 도메인 관리	해당 없음	사용자가 데이터 도메인 용어집에서 데이터 도메인을 작성, 편집 및 삭제할 수 있습니다. 이 권한은 데이터 도메인 관리 권한 그룹의 일부입니다.
알림 관리	해당 없음	사용자가 성과 기록표 알림을 구성할 수 있습니다. 이 권한은 프로파일링 관리 권한 그룹의 일부입니다.
팀 기반 개발 관리	해당 없음	사용자가 모델 리포지토리 개체의 잠금 또는 잠금 해제 상태를 관리할 수 있습니다. 모델 리포지토리가 버전 제어 시스템과 통합된 경우 사용자가 개체의 체크 아웃 또는 체크 인 상태를 관리할 수 있습니다. 또한 사용자가 체크 아웃된 개체의 소유권을 관리할 수 있습니다.
보안 세부 정보 표시	해당 없음	<p>사용자가 다음 세부 정보를 볼 수 있습니다.</p> <ul style="list-style-type: none"> - 사용자가 읽기 권한을 가지고 있지 않은 프로젝트의 이름입니다. - 오류 및 경고 메시지 세부 정보입니다.

PowerCenter 리포지토리 서비스 권한

PowerCenter 리포지토리 서비스 권한에 따라 사용자가 PowerCenter Repository Manager, 디자이너, 워크플로우 관리자, 워크플로우 모니터, pmrep 및 pmcmd 명령줄 프로그램을 사용하여 수행할 수 있는 PowerCenter 리포지토리 작업이 결정됩니다.

다음 테이블에는 PowerCenter 리포지토리 서비스에 대한 각 권한 그룹이 설명되어 있습니다.

권한 그룹	설명
도구	PowerCenter 클라이언트 도구 및 명령줄 프로그램에 액세스하기 위한 권한이 포함됩니다.
폴더	리포지토리 폴더를 관리하기 위한 권한이 포함됩니다.
디자인 개체	비즈니스 구성 요소, 매핑 매개 변수 및 변수, 매핑, 맵렛, 변환 및 사용자 정의 함수를 관리하기 위한 권한이 포함됩니다.
소스 및 대상	큐브, 차원, 소스 정의 및 대상 정의를 관리하기 위한 권한이 포함됩니다.
런타임 개체	세션 구성 개체, 태스크, 워크플로우 및 worklet을 관리하기 위한 권한이 포함됩니다.
글로벌 개체	연결 개체, 배포 그룹, 레이블 및 쿼리를 관리하기 위한 권한이 포함됩니다.

Repository Manager에서 다음 작업을 수행하려면 사용자에게 서비스 관리 도메인 권한 및 PowerCenter 리포지토리 서비스에 대한 사용 권한이 있어야 합니다.

- PowerCenter 리포지토리 수준에서 개체 버전의 고급 제거 수행
- 재사용 가능 메타데이터 확장 작성, 편집 및 삭제

도구 권한 그룹

PowerCenter 리포지토리 서비스 도구 권한 그룹의 권한에 따라 사용자가 액세스할 수 있는 PowerCenter 클라이언트 도구 및 명령줄 프로그램이 결정됩니다.

다음 테이블에는 사용자가 도구 그룹의 권한에 대해 수행할 수 있는 작업이 나열되어 있습니다.

권한	사용 권한	설명
디자이너 액세스	-	사용자가 디자이너를 사용하여 PowerCenter 리포지토리에 연결할 수 있습니다.
Repository Manager 액세스	-	사용자가 다음 작업을 수행할 수 있습니다. - Repository Manager를 사용하여 PowerCenter 리포지토리에 연결 - <i>pmrep</i> 명령 실행
워크플로우 관리자 액세스	-	사용자가 다음 작업을 수행할 수 있습니다. - 워크플로우 관리자를 사용하여 PowerCenter 리포지토리에 연결 - 워크플로우 관리자에서 PowerCenter 통합 서비스 제거
워크플로우 모니터 액세스	-	사용자가 다음 작업을 수행할 수 있습니다. - 워크플로우 모니터를 사용하여 PowerCenter 리포지토리에 연결 - 워크플로우 모니터에서 PowerCenter 통합 서비스에 연결

참고: PowerCenter 통합 서비스가 안전 모드에서 실행되는 경우 사용자는 연결된 PowerCenter 리포지토리 서비스에 대해 관리자 역할이 있어야 합니다.

도구 권한 그룹의 적절한 권한이 PowerCenter 클라이언트 도구 및 명령줄 프로그램에서 태스크를 완료하는 모든 사용자에게 대해 필요합니다. 예를 들어 Repository Manager에서 폴더를 작성하려면 사용자에게 폴더 작성 및 Repository Manager 액세스 권한이 있어야 합니다.

사용자에게 도구 권한 그룹의 권한 및 PowerCenter 리포지토리 개체에 대한 사용 권한이 있지만 개체 유형을 수정하기 위한 권한이 없는 경우 개체에 대한 일부 작업은 여전히 수행할 수 있습니다. 예를 들어 어떤 사용자에게

계 **Repository Manager** 액세스 권한과 일부 폴더에 대한 읽기 권한이 있습니다. 해당 사용자는 폴더 권한 그룹의 권한은 없습니다. 해당 사용자는 폴더에서 개체를 보고 폴더를 비교할 수 있습니다.

폴더 권한 그룹

폴더 관리 작업은 폴더 권한 그룹의 권한, **PowerCenter** 리포지토리 개체 사용 권한 및 도메인 개체 사용 권한에 따라 결정됩니다. 사용자는 **Repository Manager** 및 **pmrep** 명령줄 프로그램에서 폴더 관리 작업을 수행합니다.

일부 폴더 관리 태스크는 권한 또는 사용 권한이 아닌 폴더 소유권 및 관리자 역할에 따라 결정됩니다. 폴더 소유자 또는 **PowerCenter** 리포지토리 서비스의 관리자 역할이 할당된 사용자는 다음 폴더 관리 태스크를 완료할 수 있습니다.

- **PowerCenter** 통합 서비스가 운영 체제 프로필을 사용하는 경우 폴더에 운영 체제 프로필을 할당. 운영 체제 프로필에 대한 사용 권한이 필요합니다.
- 폴더 소유자 변경
- 폴더 사용 권한 구성
- 폴더 삭제
- 공유할 폴더 지정
- 폴더 이름 및 설명 편집

권한이 아닌 폴더 사용 권한이 할당된 사용자는 몇 가지 폴더 관리 작업을 수행할 수 있습니다. 다음 테이블에는 폴더 사용 권한만 할당된 경우 사용자가 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
폴더에 대한 읽기	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> - 폴더 비교 - 폴더에서 개체 보기

참고: 폴더에 대한 작업을 수행하려면 사용자에게 **Repository Manager** 액세스 권한도 있어야 합니다.

폴더 작성 권한

폴더 작성 권한이 할당된 사용자는 **PowerCenter** 리포지토리 폴더를 작성할 수 있습니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 폴더 작성 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
-	사용자가 폴더를 작성할 수 있습니다.

폴더 복사 권한

폴더 복사 권한이 할당된 사용자는 한 PowerCenter 리포지토리 내에서 또는 다른 PowerCenter 리포지토리로 폴더를 복사할 수 있습니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 폴더 복사 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
폴더에 대한 읽기	사용자가 동일한 PowerCenter 리포지토리 내에서 또는 다른 PowerCenter 리포지토리에 폴더를 복사할 수 있습니다. 사용자에게 대상 리포지토리에서 폴더 작성 권한도 있어야 합니다.

폴더 버전 관리

팁 기반 개발 옵션이 있는 경우 사용자에게 버전이 지정된 PowerCenter 리포지토리의 폴더 버전 관리 권한을 할당합니다. 사용자는 폴더 상태를 변경하고 폴더 수준에서 개체 버전의 고급 제거를 수행할 수 있습니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 폴더 버전 관리 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
폴더에 대한 읽기 및 쓰기	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none">- 폴더 상태 변경- 폴더 수준에서 개체 버전의 고급 제거 수행

디자인 개체 권한 그룹

디자인 개체 권한 그룹의 권한과 PowerCenter 리포지토리 개체 사용 권한에 따라 사용자가 다음 디자인 개체에 대해 수행할 수 있는 작업이 결정됩니다.

- 비즈니스 구성 요소
- 매핑 매개 변수 및 변수
- 매핑
- 맵렛
- 변환
- 사용자 정의 함수

권한이 아닌 사용 권한이 할당된 사용자는 디자인 개체에 대해 일부 작업을 수행할 수 있습니다. 다음 테이블에는 사용 권한만 할당된 경우 사용자가 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
폴더에 대한 읽기	<p>사용자가 다음 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> - 디자인 개체 비교 - 디자인 개체를 이미지로 복사 - 디자인 개체 내보내기 - 사용자 지정 변환 및 외부 프로시저에 대한 코드 생성 - PowerCenter 리포지토리 알림 메시지 받기 - 디자인 개체에 대한 데이터 연계 실행 사용자에게 Metadata Manager 서비스에 대한 연계 보기 권한 및 Metadata Manager 카탈로그의 메타데이터 개체에 대한 읽기 사용 권한도 있어야 합니다. - 디자인 개체 검색 - 디자인 개체, 디자인 개체 종속성 및 디자인 개체 기록 보기
공유 폴더에 대한 읽기 대상 폴더에 대한 읽기 및 쓰기	<p>사용자가 바로 가기를 작성할 수 있습니다.</p>

참고: 디자인 개체에 대한 작업을 수행하려면 사용자에게 도구 권한 그룹의 적절한 권한도 있어야 합니다.

디자인 개체 작성, 편집 및 삭제 권한

디자인 개체 작성, 편집 및 삭제 권한이 할당된 사용자는 비즈니스 구성 요소, 매핑 매개 변수, 매핑 변수, 매핑, 맵렛, 변환 및 사용자 정의 함수를 작성, 편집 및 삭제할 수 있습니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 디자인 개체 작성, 편집 및 삭제 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
원래 폴더에 대한 읽기 대상 폴더에 대한 읽기 및 쓰기	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> - 한 폴더에서 다른 폴더로 디자인 개체 복사 - 디자인 개체를 다른 PowerCenter 리포지토리로 복사. 사용자에게 대상 리포지토리의 디자인 개체 작성, 편집 및 삭제 권한도 있어야 합니다.
폴더에 대한 읽기 및 쓰기	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> - 버전이 지정된 디자인 개체에 대한 설명 변경 - 체크 인 및 고유한 사용자 계정으로 체크 아웃된 디자인 개체의 체크 아웃 실행 취소 - 디자인 개체 체크 아웃 - 동일한 폴더에서 디자인 개체 복사 및 붙여넣기 - 데이터 프로파일 작성, 편집, 삭제 및 프로파일 관리자 실행. 사용자에게 런타임 개체 작성, 편집 및 삭제 권한도 있어야 합니다. - 디자인 개체 작성, 편집 및 삭제 - SAP ABAP 프로그램 생성 및 정리 - 비즈니스 콘텐츠 통합 매핑 생성. 사용자에게 소스 및 대상 작성, 편집 및 삭제 권한도 있어야 합니다. - 디자이너를 사용하여 디자인 개체 가져오기. 사용자에게 소스 및 대상 작성, 편집 및 삭제 권한도 있어야 합니다. - Repository Manager를 사용하여 디자인 개체 가져오기. 사용자에게 런타임 개체 작성, 편집, 삭제 권한과 소스 및 대상 작성, 편집, 삭제 권한도 있어야 합니다. - 이전 디자인 개체 버전으로 되돌리기 - 매핑, 맵렛 및 사용자 정의 함수의 유효성 검사

디자인 개체 버전 관리

템 기반 개발 옵션이 있는 경우 사용자에게 버전이 지정된 PowerCenter 리포지토리의 디자인 개체 버전 관리 권한을 할당합니다. 사용자는 상태를 변경하고 디자인 개체 버전을 복구 및 제거할 수 있습니다. 사용자는 체크 인하고 다른 사용자가 수행한 체크 아웃을 실행 취소할 수도 있습니다.

디자인 개체 버전 관리 권한에는 디자인 개체 작성, 편집 및 삭제 권한이 포함됩니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 디자인 개체 버전 관리 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
폴더에 대한 읽기 및 쓰기	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> - 디자인 개체 상태 변경 - 체크 인 및 다른 사용자가 체크 아웃한 디자인 개체 체크 아웃 실행 취소 - 디자인 개체 버전 제거 - 삭제된 디자인 개체 복구

소스 및 대상 권한 그룹

소스 및 대상 권한 그룹의 권한과 PowerCenter 리포지토리 개체 권한의 사용 권한에 따라 사용자가 다음 소스 및 대상 개체에서 수행할 수 있는 작업이 결정됩니다.

- 큐브
- 차원
- 소스 정의
- 대상 정의

권한이 아닌 사용 권한이 할당된 사용자는 소스 및 대상 개체에 대해 일부 작업을 수행할 수 있습니다. 다음 테이블에는 사용 권한만 할당된 경우 사용자가 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
폴더에 대한 읽기	<p>사용자가 다음 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> - 소스 및 대상 개체 비교 - 소스 및 대상 개체 내보내기 - 소스 및 대상 데이터 미리 보기 - PowerCenter 리포지토리 알림 메시지 받기 - 소스 및 대상 개체에서 데이터 연계 실행. 사용자에게 Metadata Manager 서비스에 대한 연계 보기 권한 및 Metadata Manager 카탈로그의 메타데이터 개체에 대한 읽기 사용 권한도 있어야 합니다. - 소스 및 대상 개체 검색 - 소스 및 대상 개체, 소스 및 대상 개체 종속성, 소스 및 대상 개체 기록 보기
공유 폴더에 대한 읽기 대상 폴더에 대한 읽기 및 쓰기	바로 가기 작성

참고: 소스 및 대상 개체에서 작업을 수행하려면 사용자에게 도구 권한 그룹의 적절한 권한도 있어야 합니다.

소스 및 대상 작성, 편집 및 삭제 권한

소스 및 대상 작성, 편집 및 삭제 권한이 할당된 사용자는 큐브, 차원, 소스 정의 및 대상 정의를 작성, 편집 및 삭제할 수 있습니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 소스 및 대상 작성, 편집 및 삭제 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
원래 폴더에 대한 읽기 대상 폴더에 대한 읽기 및 쓰기	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> - 소스 및 대상 개체를 다른 폴더에 복사 - 소스 및 대상 개체를 다른 PowerCenter 리포지토리에 복사. 사용자에게 대상 리포지토리의 소스 및 대상 작성, 편집 및 삭제 권한도 있어야 합니다.
폴더에 대한 읽기 및 쓰기	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> - 버전이 지정된 소스 또는 대상 개체에 대한 설명 변경 - 체크 인 및 고유한 사용자 계정으로 체크 아웃된 소스 및 대상 개체 체크 아웃 실행 취소 - 소스 및 대상 개체 체크 아웃 - 동일한 폴더에서 소스 및 대상 개체 복사 및 붙여넣기 - 소스 및 대상 개체 작성, 편집 및 삭제 - SAP 함수 가져오기 - 디자이너를 사용하여 소스 및 대상 개체 가져오기. 사용자에게 디자인 개체 작성, 편집 및 삭제 권한도 있어야 합니다. - Repository Manager를 사용하여 소스 및 대상 개체 가져오기. 사용자에게 디자인 개체 작성, 편집, 삭제 및 런타임 개체 작성, 편집, 삭제 권한도 있어야 합니다. - SQL을 작성 및 실행하여 관계형 데이터베이스에서 대상 작성 - 이전 소스 또는 대상 개체 버전으로 되돌리기

소스 및 대상 버전 관리 권한

템 기반 개발 옵션이 있는 경우 사용자에게 버전이 지정된 PowerCenter 리포지토리의 소스 및 대상 버전 관리 권한을 할당합니다. 사용자는 상태를 변경하고 소스 및 대상 개체 버전을 복구 및 제거할 수 있습니다. 사용자는 체크 인하고 다른 사용자가 수행한 체크 아웃을 실행 취소할 수도 있습니다.

소스 및 대상 버전 관리 권한에는 소스 및 대상 작성, 편집 및 삭제 권한이 포함됩니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 소스 및 대상 버전 관리 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
폴더에 대한 읽기 및 쓰기	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> - 소스 및 대상 개체 상태 변경 - 체크 인 및 다른 사용자가 체크 아웃한 소스 및 대상 개체의 체크 아웃 실행 취소 - 소스 및 대상 개체 버전 제거 - 삭제된 소스 및 대상 개체 복구

런타임 개체 권한 그룹

런타임 개체 권한 그룹의 권한, **PowerCenter** 리포지토리 개체 사용 권한 및 도메인 개체 사용 권한에 따라 사용자가 다음 런타임 개체에서 수행할 수 있는 작업이 결정됩니다.

- 세션 구성 개체
- 작업
- 워크플로우
- Worklet

일부 런타임 개체 태스크는 권한 또는 사용 권한이 아닌 관리자 역할에 따라 결정됩니다. **PowerCenter** 리포지토리 서비스의 관리자 역할이 할당된 사용자는 워크플로우 관리자의 탐색기에서 **PowerCenter** 통합 서비스를 삭제할 수 있습니다.

권한이 아닌 사용 권한이 할당된 사용자는 런타임 개체에 대해 일부 작업을 수행할 수 있습니다. 다음 테이블에는 사용 권한만 할당된 경우 사용자가 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
폴더에 대한 읽기	<p>사용자가 다음 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> - 런타임 개체 비교 - 런타임 개체 내보내기 - PowerCenter 리포지토리 알림 메시지 받기 - 런타임 개체 검색 - 세션에서 매핑 매개 변수 및 변수 사용 - 런타임 개체, 런타임 개체 종속성 및 런타임 개체 기록 보기
폴더에 대한 읽기 및 실행	<p>고유한 사용자 계정으로 시작한 태스크 및 워크플로우 중지 및 중단</p> <p>PowerCenter 통합 서비스가 안전 모드에서 실행되는 경우 사용자는 연결된 PowerCenter 리포지토리 서비스에 대해 관리자 역할이 있어야 합니다.</p>

참고: 런타임 개체에서 작업을 수행하려면 사용자에게 도구 권한 그룹의 적절한 권한도 있어야 합니다.

런타임 개체 작성, 편집 및 삭제 권한

런타임 개체 작성, 편집 및 삭제 권한이 할당된 사용자는 세션 구성 개체, 태스크, 워크플로우 및 **worklet**을 작성, 편집 및 삭제할 수 있습니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 런타임 개체 작성, 편집 및 삭제 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
원래 폴더에 대한 읽기 대상 폴더에 대한 읽기 및 쓰기	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> - 한 폴더에서 다른 폴더로 태스크, 워크플로우 또는 worklet 복사 - 다른 PowerCenter 리포지토리로 태스크, 워크플로우 또는 worklet 복사. 사용자에게 대상 리포지토리의 런타임 개체 작성, 편집 및 삭제 권한도 있어야 합니다.
폴더에 대한 읽기 및 쓰기	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> - PowerCenter 통합 서비스를 워크플로우 속성의 워크플로우에 할당 - 서비스 수준을 워크플로우에 할당 - 버전이 지정된 런타임 개체에 대한 설명 변경 - 체크 인 및 고유한 사용자 계정으로 체크 아웃된 런타임 개체의 체크 아웃 실행 취소 - 런타임 개체 체크 아웃 - 동일한 폴더에서 태스크, 워크플로우 및 worklet 복사 및 붙여넣기 - 데이터 프로필 작성, 편집, 삭제 및 프로필 관리자 실행. 사용자에게 디자인 개체 작성, 편집 및 삭제 권한도 있어야 합니다. - 세션 구성 개체 작성, 편집 및 삭제 - 태스크, 워크플로우, worklet 삭제 및 유효성 검사 - Repository Manager를 사용하여 런타임 개체 가져오기. 사용자에게 디자인 개체 작성, 편집, 삭제 권한과 소스 및 대상 작성, 편집, 삭제 권한도 있어야 합니다. - 워크플로우 관리자를 사용하여 런타임 개체 가져오기 - 이전 개체 버전으로 되돌리기
폴더에 대한 읽기 및 쓰기 연결 개체에 대한 읽기	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> - 태스크, 워크플로우, worklet 작성 및 편집 - 연결을 사용하는 모든 세션에 대해 관계형 데이터베이스 연결 바꾸기

런타임 개체 버전 관리 권한

팀 기반 개발 옵션이 있는 경우 사용자에게 버전이 지정된 PowerCenter 리포지토리의 런타임 개체 버전 관리 권한을 할당합니다. 사용자는 상태를 변경하고 런타임 개체 버전을 복구 및 제거할 수 있습니다. 사용자는 체크 인하고 다른 사용자가 수행한 체크 아웃을 실행 취소할 수도 있습니다.

런타임 개체 버전 관리 권한에는 런타임 개체 작성, 편집 및 삭제 권한이 포함됩니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 런타임 개체 버전 관리 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
폴더에 대한 읽기 및 쓰기	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> - 런타임 개체의 상태 변경 - 체크 인 및 다른 사용자가 체크 아웃한 런타임 개체의 체크 아웃 실행 취소 - 런타임 개체 버전 제거 - 삭제된 런타임 개체 복구

런타임 개체 모니터링 권한

런타임 개체 모니터링 권한이 할당된 사용자는 워크플로우 모니터에서 워크플로우 및 태스크를 모니터링할 수 있습니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 런타임 개체 모니터링 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	사용자에게 부여하는 기능
폴더에 대한 읽기	사용자가 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> - 워크플로우 모니터에서 런타임 개체의 속성 보기 - 워크플로우 모니터에서 세션 및 워크플로우 로그 보기 - 워크플로우 모니터에서 런타임 개체 및 성능 세부 정보 보기 PowerCenter 통합 서비스가 안전 모드에서 실행되는 경우 사용자는 연결된 PowerCenter 리포지토리 서비스에 대해 관리자 역할이 있어야 합니다.

런타임 개체 실행 권한

런타임 개체 실행 권한이 할당된 사용자는 태스크 및 워크플로우를 시작, 콜드 시작 및 복구할 수 있습니다.

런타임 개체 실행 권한에는 런타임 개체 모니터링 권한이 포함됩니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 런타임 개체 실행 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
폴더에 대한 읽기 및 실행	사용자가 서비스 메뉴 또는 탐색기를 사용하여 PowerCenter 통합 서비스를 워크플로우에 할당할 수 있습니다.
폴더에 대한 읽기, 쓰기 및 실행 연결 개체에서 읽기 및 실행	사용자가 디버그 세션 인스턴스를 작성하거나 기존의 재사용 가능 세션을 사용하여 매핑을 디버그할 수 있습니다. 사용자에게 런타임 개체 작성, 편집 및 삭제 권한도 있어야 합니다. PowerCenter 통합 서비스가 안전 모드에서 실행되는 경우 사용자는 연결된 PowerCenter 리포지토리 서비스에 대해 관리자 역할이 있어야 합니다.

사용 권한	설명
폴더에 대한 읽기 및 실행 연결 개체에서 읽기 및 실행	사용자가 기존의 재사용 불가능 세션을 사용하여 매핑을 디버그할 수 있습니다. PowerCenter 통합 서비스가 안전 모드에서 실행되는 경우 사용자는 연결된 PowerCenter 리포지토리 서비스에 대해 관리자 역할이 있어야 합니다.
폴더에 대한 읽기 및 실행 연결 개체에서 읽기 및 실행	사용자가 다음 작업을 수행할 수 있습니다. - 태스크 및 워크플로우 시작, 콜드 시작 및 재시작 - 고유한 사용자 계정으로 시작한 태스크 및 워크플로우 복구 PowerCenter 통합 서비스가 운영 체제 프로필을 사용하는 경우 사용자에게 운영 체제 프로필에 대한 사용 권한도 있어야 합니다. PowerCenter 통합 서비스가 안전 모드에서 실행되는 경우 사용자는 연결된 PowerCenter 리포지토리 서비스에 대해 관리자 역할이 있어야 합니다.

런타임 개체 실행 관리 권한

런타임 개체 실행 관리 권한이 할당된 사용자는 워크플로우를 스케줄링하고 스케줄링 취소할 수 있습니다. 사용자는 다른 사용자가 시작한 태스크 및 워크플로우를 중지, 중단 및 복구할 수도 있습니다.

런타임 개체 실행 관리 권한에는 런타임 개체 실행 권한 및 런타임 개체 모니터링 권한이 포함됩니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 런타임 개체 실행 관리 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
폴더에 대한 읽기 및 실행	사용자가 워크플로우 및 세션 로그 항목을 잘라낼 수 있습니다.
폴더에 대한 읽기 및 실행	사용자가 다음 작업을 수행할 수 있습니다. - 다른 사용자가 시작한 태스크 및 워크플로우 중지 및 중단 - 자동으로 복구된 태스크 중지 및 중단 - 워크플로우 스케줄링 취소 PowerCenter 통합 서비스가 안전 모드에서 실행되는 경우 사용자는 연결된 PowerCenter 리포지토리 서비스에 대해 관리자 역할이 있어야 합니다.
폴더에 대한 읽기 및 실행 연결 개체에서 읽기 및 실행	사용자가 다음 작업을 수행할 수 있습니다. - 다른 사용자가 시작한 태스크 및 워크플로우 복구 - 자동으로 복구된 태스크 복구 PowerCenter 통합 서비스가 운영 체제 프로필을 사용하는 경우 사용자에게 운영 체제 프로필에 대한 사용 권한도 있어야 합니다. PowerCenter 통합 서비스가 안전 모드에서 실행되는 경우 사용자는 연결된 PowerCenter 리포지토리 서비스에 대해 관리자 역할이 있어야 합니다.
폴더에 대한 읽기, 쓰기 및 실행 연결 개체에서 읽기 및 실행	사용자가 다음 작업을 수행할 수 있습니다. - 워크플로우 > 스케줄러 메뉴에서 재사용 가능 스케줄러 작성 및 편집 - 워크플로우 속성에서 재사용 불가능 스케줄러 편집 - 워크플로우 속성에서 재사용 가능 스케줄러 편집. 사용자에게 런타임 개체 작성, 편집 및 삭제 권한도 있어야 합니다. PowerCenter 통합 서비스가 운영 체제 프로필을 사용하는 경우 사용자에게 운영 체제 프로필에 대한 사용 권한도 있어야 합니다. PowerCenter 통합 서비스가 안전 모드에서 실행되는 경우 사용자는 연결된 PowerCenter 리포지토리 서비스에 대해 관리자 역할이 있어야 합니다.

글로벌 개체 권한 그룹

글로벌 개체 권한 그룹의 권한과 **PowerCenter** 리포지토리 개체 사용 권한에 따라 사용자가 다음 글로벌 개체에서 수행할 수 있는 작업이 결정됩니다.

- 연결 개체
- 배포 그룹
- 레이블
- 쿼리

일부 글로벌 개체 태스크는 권한 또는 사용 권한이 아닌 글로벌 개체 소유권 및 관리자 역할에 따라 결정됩니다. 글로벌 개체 소유자 또는 **PowerCenter** 리포지토리 서비스에 대한 관리자 역할이 할당된 사용자는 다음 글로벌 개체 태스크를 완료할 수 있습니다.

- 글로벌 개체 사용 권한 구성
- 글로벌 개체 소유자 변경
- 글로벌 개체 삭제

권한이 아닌 사용 권한이 할당된 사용자는 글로벌 개체에 대해 일부 작업을 수행할 수 있습니다. 다음 테이블에는 사용 권한만 할당된 경우 사용자가 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
연결 개체에 대한 읽기	사용자가 연결 개체를 볼 수 있습니다.
배포 그룹에 대한 읽기	사용자가 배포 그룹을 볼 수 있습니다.
레이블에 대한 읽기	사용자가 레이블을 볼 수 있습니다.
쿼리에 대한 읽기	사용자가 개체 쿼리를 볼 수 있습니다.
연결 개체에 대한 읽기 및 쓰기	사용자가 연결 개체를 편집할 수 있습니다.
레이블에 대한 읽기 및 쓰기	사용자가 레이블을 편집하고 잠글 수 있습니다.
쿼리에 대한 읽기 및 쓰기	사용자가 개체 쿼리를 편집하고 유효성을 검사할 수 있습니다.
쿼리에 대한 읽기 및 실행	사용자가 개체 쿼리를 실행할 수 있습니다.
폴더에 대한 읽기 레이블에 대한 읽기 및 실행	사용자가 레이블을 적용하고 레이블 참조를 제거할 수 있습니다.

참고: 글로벌 개체에서 작업을 수행하려면 사용자에게 도구 권한 그룹의 적절한 권한도 있어야 합니다.

연결 작성 권한

연결 작성 권한에 할당된 사용자는 연결 개체를 작성할 수 있습니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 연결 작성 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
-	사용자가 연결 개체를 작성하고 복사할 수 있습니다.

배포 그룹 관리 권한

팀 기반 개발 옵션이 있는 경우 버전이 지정된 **PowerCenter** 리포지토리의 배포 그룹 관리 권한이 할당된 사용자는 배포 그룹을 작성, 편집, 복사 및 롤백할 수 있습니다. 버전이 지정되지 않은 리포지토리에서 사용자는 배포 그룹을 작성, 편집 및 복사할 수 있습니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 배포 그룹 관리 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
-	사용자가 배포 그룹을 작성할 수 있습니다.
배포 그룹에 대한 읽기 및 쓰기	사용자가 다음 작업을 수행할 수 있습니다. - 배포 그룹 편집 - 배포 그룹에서 개체 제거
원래 폴더에 대한 읽기 배포 그룹에 대한 읽기 및 쓰기	사용자가 개체를 배포 그룹에 추가할 수 있습니다.
원래 폴더에 대한 읽기 대상 폴더에 대한 읽기 및 쓰기 배포 그룹에 대한 읽기 및 실행	사용자가 배포 그룹을 복사할 수 있습니다.
대상 폴더에 대한 읽기 및 쓰기	사용자가 배포 그룹을 롤백할 수 있습니다.

배포 그룹 실행 권한

배포 그룹 실행 권한이 할당된 사용자는 대상 폴더에 대한 쓰기 권한 없이 배포 그룹을 복사할 수 있습니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 배포 그룹 실행 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
원래 폴더에 대한 읽기 배포 그룹에 대한 실행	사용자가 배포 그룹을 복사할 수 있습니다.

레이블 작성 권한

팀 기반 개발 옵션이 있는 경우 버전이 지정된 **PowerCenter** 리포지토리의 레이블 작성 권한이 할당된 사용자는 레이블을 작성할 수 있습니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 레이블 작성 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
-	사용자가 레이블을 작성할 수 있습니다.

쿼리 작성 권한

쿼리 작성 권한이 할당된 사용자는 개체 쿼리를 작성할 수 있습니다.

다음 테이블에는 필요한 사용 권한 및 사용자가 쿼리 작성 권한으로 수행할 수 있는 작업이 나열되어 있습니다.

사용 권한	설명
-	사용자가 개체 쿼리를 작성할 수 있습니다.

PowerExchange 수신기 서비스 권한

PowerExchange 수신기 서비스 권한에 따라 사용자가 실행할 수 있는 `infacmd pwx` 명령이 결정됩니다.

다음 테이블에는 정보 명령 권한 그룹의 PowerExchange 수신기 서비스 권한이 설명되어 있습니다.

권한 이름	설명
listtask	<code>infacmd pwx ListTaskListener</code> 명령을 실행합니다.

다음 테이블에는 관리 명령 권한 그룹의 각 PowerExchange 수신기 서비스 권한이 설명되어 있습니다.

권한 이름	설명
닫기	<code>infacmd pwx CloseListener</code> 명령을 실행합니다.
closeforce	<code>infacmd pwx CloseForceListener</code> 명령을 실행합니다.
stoptask	<code>infacmd pwx StopTaskListener</code> 명령을 실행합니다.

PowerExchange 로거 서비스 권한

PowerExchange 로거 서비스 권한에 따라 사용자가 실행할 수 있는 `infacmd pwx` 명령이 결정됩니다.

다음 테이블에는 정보 명령 권한 그룹의 각 PowerExchange 로거 서비스 권한이 설명되어 있습니다.

권한 이름	설명
displayall	<code>infacmd pwx DisplayAllLogger</code> 명령을 실행합니다.
displaycpu	<code>infacmd pwx DisplayCPULogger</code> 명령을 실행합니다.
displaycheckpoints	<code>infacmd pwx DisplayCheckpointsLogger</code> 명령을 실행합니다.
displayevents	<code>infacmd pwx DisplayEventsLogger</code> 명령을 실행합니다.
displaymemory	<code>infacmd pwx DisplayMemoryLogger</code> 명령을 실행합니다.

권한 이름	설명
displayrecords	infacmd pwx DisplayRecordsLogger 명령을 실행합니다.
displaystatus	infacmd pwx DisplayStatusLogger 명령을 실행합니다.

다음 테이블에는 관리 명령 권한 그룹의 각 **PowerExchange** 로거 서비스 권한이 설명되어 있습니다.

권한 이름	설명
condense	infacmd pwx CondenseLogger 명령을 실행합니다.
fileswitch	infacmd pwx FileSwitchLogger 명령을 실행합니다.
shutdown	infacmd pwx ShutDownLogger 명령을 실행합니다.

스케줄러 서비스 권한

스케줄러 서비스 권한에 따라 사용자가 일정 및 예약된 작업에서 수행할 수 있는 작업이 결정됩니다.

다음 테이블에는 스케줄러 서비스 권한 및 필요한 사용 권한이 설명되어 있습니다.

권한	설명	사용 권한이 필요한 대상
일정 작성	사용자가 일정을 작성할 수 있습니다. 일정을 작성하려면 사용자에게 데이터 통합 서비스에 대한 응용 프로그램 관리 권한도 필요합니다.	<ul style="list-style-type: none"> - 스케줄러 서비스 - 사용자가 예약하려는 작업을 실행하는 데이터 통합 서비스
일정 편집	사용자가 일정을 편집하고 일시 중지하고 다시 시작할 수 있습니다. 일정을 편집하려면 사용자에게 데이터 통합 서비스에 대한 응용 프로그램 관리 권한도 필요합니다.	<ul style="list-style-type: none"> - 스케줄러 서비스 - 사용자가 예약하려는 작업을 실행하는 데이터 통합 서비스
일정 삭제	사용자가 일정을 삭제할 수 있습니다.	스케줄러 서비스
일정 보기	사용자가 일정 보기 및 일정을 볼 수 있습니다.	스케줄러 서비스

Test Data Manager 서비스 권한

Test Data Manager 서비스 권한에 따라 사용자가 Test Data Manager를 사용하여 수행할 수 있는 작업이 결정됩니다. Administrator 도구의 **보안** 탭에서 권한을 구성합니다.

다음 테이블에는 각 Test Data Manager 권한 그룹이 설명되어 있습니다.

권한 그룹	설명
관리	연결, 암호 문구, 역할 생성 및 관리, Informatica Administrator의 사용자 및 사용자 그룹에 권한 할당, 리포지토리 관리, 라이선스 추가, 워크플로우 및 프로젝트 특성 설정을 위한 권한을 포함합니다. 참고: 사용자 및 그룹을 생성하려면 기본 Informatica Administrator 사용자는 보안 관리 권한을 테스트 데이터 관리자 사용자에게 할당해야 합니다.
데이터 도메인	Test Data Manager에서 데이터 도메인을 보고 관리하기 위한 권한을 포함합니다.
데이터 마스킹	Test Data Manager에서 마스킹 규칙 및 정책 할당을 보고 관리하기 위한 권한을 포함합니다.
정책	Test Data Manager에서 정책을 보고 관리하기 위한 권한을 포함합니다.
프로젝트	Test Data Manager에서 프로젝트 보기 및 관리, 메타데이터 감사 및 가져오기, 계획 및 워크플로우 실행을 위한 권한을 포함합니다.

관리 권한 그룹

관리 권한 그룹의 권한에 따라 테스트 데이터 관리자가 수행할 수 있는 관리 태스크가 결정됩니다.

다음 테이블에는 관리 권한 그룹의 권한 및 개체에 대한 태스크를 수행하기 위해 필요한 사용 권한이 나열되어 있습니다.

연결 권한 그룹

연결 권한 그룹의 권한에 따라 사용자가 TDM 작업 영역의 연결 페이지에서 수행할 수 있는 태스크가 결정됩니다. 다음 테이블에는 연결 권한 그룹의 권한 및 개체에서 태스크를 수행하기 위해 필요한 사용 권한이 나열되어 있습니다.

권한	포함되는 권한	사용 권한	설명
연결 보기	-	읽기	사용자가 TDM 작업 영역에서 연결 및 테스트 연결을 볼 수 있습니다.
연결 관리	연결 보기	쓰기	사용자가 TDM 작업 영역의 연결 페이지에서 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> - 연결 작성 - 연결 편집 - 연결 삭제 - 연결 보기 - 연결 테스트

데이터 도메인 권한 그룹

데이터 도메인 권한 그룹의 권한에 따라 사용자가 **Test Data Manager**의 정책 페이지에서 데이터 도메인에 대해 수행할 수 있는 태스크가 결정됩니다.

다음 테이블에는 데이터 도메인 권한 그룹의 권한 및 개체에서 태스크를 수행하기 위해 필요한 사용 권한이 나열되어 있습니다.

권한	포함되는 권한	사용 권한	설명
데이터 도메인 보기	-	읽기	사용자가 Test Data Manager에서 데이터 도메인을 볼 수 있습니다.
데이터 도메인 관리	데이터 도메인 보기	쓰기	사용자가 Test Data Manager에서 데이터 도메인에 대한 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none">- 데이터 도메인 작성- 데이터 도메인 편집- 데이터 도메인 삭제- 데이터 도메인 보기

데이터 마스킹 권한 그룹

데이터 마스킹 권한 그룹의 권한에 따라 사용자가 프로젝트 | 정의 | **Test Data Manager**의 데이터 마스킹 보기에서 수행할 수 있는 태스크가 결정됩니다. 규칙 및 정책을 이 보기의 테이블 열에 할당할 수 있습니다.

다음 테이블에는 데이터 마스킹 권한 그룹의 권한 및 개체에서 태스크를 수행하기 위해 필요한 사용 권한이 나열되어 있습니다.

권한	포함되는 권한	사용 권한	설명
데이터 마스킹 보기	-	읽기	사용자가 Test Data Manager에서 데이터 마스킹 할당을 볼 수 있습니다.
데이터 마스킹 관리	데이터 마스킹 보기	쓰기	사용자가 Test Data Manager에서 다음 데이터 마스킹 할당 작업을 수행할 수 있습니다. <ul style="list-style-type: none">- 규칙 및 정책 할당 추가- 규칙 및 정책 할당 삭제- 규칙 속성 재정의- 데이터 마스킹 할당 보기

데이터 하위 집합 권한 그룹

데이터 하위 집합 권한 그룹의 권한에 따라 사용자가 **Test Data Manager**에서 데이터 하위 집합 개체에 대해 수행할 수 있는 태스크가 결정됩니다.

다음 테이블에는 데이터 하위 집합 권한 그룹의 권한 및 개체에 대한 태스크를 수행하기 위해 필요한 사용 권한이 나열되어 있습니다.

정책 권한 그룹

정책 권한 그룹의 권한에 따라 사용자가 **Test Data Manager**에서 정책에 대해 수행할 수 있는 태스크가 결정됩니다.

다음 테이블에는 정책 권한 그룹의 권한 및 개체에서 태스크를 수행하기 위해 필요한 사용 권한이 나열되어 있습니다.

권한	포함되는 권한	사용 권한	설명
정책 보기	-	읽기	사용자가 Test Data Manager에서 정책을 볼 수 있습니다.
정책 관리	정책 보기	쓰기	사용자가 Test Data Manager에서 다음 정책 작업을 수행할 수 있습니다. <ul style="list-style-type: none">- 정책 작성- 정책 편집- 정책 삭제- 정책 보기

프로젝트 권한 그룹

프로젝트 권한 그룹의 권한에 따라 사용자가 **Test Data Manager**에서 프로젝트에 대해 수행할 수 있는 태스크가 결정됩니다.

다음 테이블에는 프로젝트 권한 그룹의 권한 및 개체에 대한 태스크를 수행하기 위해 필요한 사용 권한이 나열되어 있습니다.

참고: 프로젝트 관리 권한이 있는 사용자가 각 구성 요소를 사용하여 계획을 작성할 수 있으려면 최소한 다음 수준의 권한이 있어야 합니다.

- 관리 권한 그룹에서 연결 보기. 계획을 작성하기 위해
- 데이터 하위 집합 권한 그룹에서 데이터 하위 집합 보기. 하위 집합 구성 요소로 계획을 작성하기 위해
- 규칙 권한 그룹에서 마스킹 규칙 보기. 마스킹 구성 요소로 계획을 작성하기 위해

규칙 권한 그룹

다음 테이블에는 데이터 마스킹 권한 그룹의 권한 및 개체에서 태스크를 수행하기 위해 필요한 사용 권한이 나열되어 있습니다.

데이터 생성 권한 그룹

데이터 생성 권한 그룹의 권한에 따라 사용자가 **Test Data Manager**에서 수행할 수 있는 **Test Data Generation** 태스크가 결정됩니다.

다음 테이블에는 데이터 생성 권한 그룹의 권한 및 개체에 대한 태스크를 수행하기 위해 필요한 사용 권한이 나열되어 있습니다.

권한	포함되는 권한	사용 권한	설명
데이터 생성 보기	-	읽기	사용자가 Test Data Manager 에서 데이터 생성 규칙 할당을 볼 수 있습니다.
데이터 생성 관리	데이터 생성 보기	쓰기	사용자가 Test Data Manager 에서 다음 데이터 생성 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> - 데이터 생성 규칙 할당 보기 - 데이터 생성 규칙 할당 추가 - 데이터 생성 규칙 할당 삭제 - 데이터 생성 규칙 할당 재정의

역할 관리

역할은 사용자 및 그룹에 할당할 수 있는 권한의 컬렉션입니다. 다음 유형의 역할을 할당할 수 있습니다.

- 시스템 정의. 편집하거나 삭제할 수 없는 역할입니다.
- 사용자 지정. 작성, 편집 및 삭제할 수 있는 역할입니다.

역할에는 도메인 또는 응용 프로그램 서비스 유형의 권한이 포함됩니다. 역할을 도메인 또는 도메인의 각 응용 프로그램 서비스의 사용자 또는 그룹에 할당합니다. 예를 들어 **PowerCenter** 리포지토리 서비스에 대한 권한이 포함된 개발자 역할을 작성할 수 있습니다. 도메인에는 여러 **PowerCenter** 리포지토리 서비스가 포함될 수 있습니다. 개발자 역할을 개발 **PowerCenter** 리포지토리 서비스의 사용자에게 할당할 수 있습니다. 다른 역할을 프로덕션 **PowerCenter** 리포지토리 서비스의 해당 사용자에게 할당할 수 있습니다.

탐색기의 역할 섹션에서 역할을 선택하는 경우 도메인 및 응용 프로그램 서비스에 대한 역할이 직접 할당된 모든 사용자 및 그룹을 볼 수 있습니다. 사용자 및 그룹 또는 서비스에 따라 역할 할당을 볼 수 있습니다. 할당 섹션에 나열된 사용자 또는 그룹으로 이동하려면 사용자 또는 그룹을 마우스 오른쪽 단추로 클릭하고 항목 탐색을 선택합니다.

시스템 정의 역할 및 사용자 지정 역할을 검색할 수 있습니다.

시스템 정의 역할

시스템 정의 역할은 편집하거나 삭제할 수 없는 역할입니다. 관리자 역할은 시스템 정의 역할입니다.

도메인, 분석 서비스, 데이터 통합 서비스, 대량 수집 서비스, **Metadata Manager** 서비스, 모델 리포지토리 서비스 또는 **PowerCenter** 리포지토리 서비스에 대한 관리자 역할을 사용자 또는 그룹에 할당하는 경우 사용자 또는 그룹에 서비스에 대한 모든 권한이 부여됩니다. 관리자 역할은 사용 권한 검사를 바이패스합니다. 관리자 역할이 있는 사용자는 서비스에서 관리되는 모든 개체에 액세스할 수 있습니다.

관리자 역할

도메인, 데이터 통합 서비스 또는 **PowerCenter** 리포지토리 서비스에 대한 관리자 역할을 사용자 또는 그룹에 할당하는 경우 사용자 또는 그룹은 권한이나 사용 권한이 아닌 관리자 역할에 의해 결정되는 일부 태스크를 완료할 수 있습니다.

도메인, 데이터 통합 서비스 또는 **PowerCenter** 리포지토리 서비스의 모든 권한을 사용자 또는 그룹에 할당한 다음 모든 도메인 또는 **PowerCenter** 리포지토리 개체에 대한 전체 사용 권한을 사용자 또는 그룹에 부여할 수 있습니다. 그러나 이 사용자 또는 그룹은 관리자 역할에 의해 결정되는 태스크를 완료할 수 없습니다.

예를 들어 도메인에 대한 관리자 역할이 할당된 사용자는 **Administrator** 도구에서 도메인 속성을 구성할 수 있습니다. 모든 도메인 권한 및 도메인에 대한 사용 권한이 할당된 사용자는 도메인 속성을 구성할 수 없습니다.

다음 테이블에는 도메인, 데이터 통합 서비스, 대량 수집 서비스 및 **PowerCenter** 리포지토리 서비스에 대한 관리자 역할에 의해 결정되는 태스크가 나열되어 있습니다.

서비스	태스크
도메인	<ul style="list-style-type: none"> - 도메인 속성 구성 - 클러스터 구성 설정 - 운영 체제 프로파일 작성 - 운영 체제 프로파일 삭제 - 도메인 및 운영 체제 프로파일에 대한 사용 권한 부여 - 로그 이벤트 관리 및 제거 - 도메인 알림 수신 - 라이선스 보고서 실행 - 사용자 활동 로그 이벤트 보기 - 도메인을 종료합니다. - 서비스 업그레이드 마법사 액세스
데이터 통합 서비스	<ul style="list-style-type: none"> - 작업 메뉴를 사용하여 데이터 통합 서비스 업그레이드
대량 수집 서비스	<ul style="list-style-type: none"> - 모든 대량 수집 사양을 찾아봅니다. - 대량 수집 사양을 편집합니다. - 대량 수집 사양을 실행합니다. - 대량 수집 사양을 삭제합니다.
PowerCenter 리포지토리 서비스	<ul style="list-style-type: none"> - PowerCenter 통합 서비스가 운영 체제 프로파일을 사용하는 경우 리포지토리 폴더에 운영 체제 프로파일 할당* - 폴더 및 글로벌 개체의 소유자 변경* - 폴더 및 글로벌 개체 사용 권한 구성* - PowerCenter 통합 서비스가 안전 모드로 실행될 때 PowerCenter 클라이언트에서 PowerCenter 통합 서비스에 연결 - 워크플로우 관리자의 탐색기에서 PowerCenter 통합 서비스 삭제 - 폴더 및 글로벌 개체 삭제* - 공유되는 폴더 지정* - 폴더의 이름 및 설명 편집* <p>*PowerCenter 리포지토리 폴더 소유자 또는 글로벌 개체 소유자도 이러한 태스크를 완료할 수 있습니다.</p>

사용자 지정 역할

사용자 지정 역할은 편집하거나 삭제할 수 있는 역할입니다.

기본적으로 **Administrator** 도구에는 다음과 같은 사용자 지정 역할이 포함됩니다.

- 분석 서비스 사용자 지정 역할
- **Metadata Manager** 서비스 사용자 지정 역할

- 운영자 사용자 지정 역할
- PowerCenter 리포지토리 서비스 사용자 지정 역할
- Test Data Manager 서비스 사용자 지정 역할

이러한 역할에 대한 권한을 편집하거나 역할을 삭제할 수 있습니다. 고유한 사용자 지정 역할을 작성할 수도 있습니다.

사용자 지정 역할 작성

사용자 지정 역할을 작성할 때 권한을 도메인 또는 응용 프로그램 서비스 유형에 대한 역할에 할당합니다. 역할은 하나 이상의 서비스에 대한 권한을 포함할 수 있습니다.

1. **Administrator** 도구에서 보안 탭을 클릭합니다.
2. 보안 작업 메뉴에서 역할 작성을 클릭합니다.
역할 작성 대화 상자가 나타납니다.
3. 역할에 대해 다음 속성을 입력합니다.

속성	설명
이름	역할의 이름입니다. 역할 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.
설명	역할에 대한 설명입니다. 설명은 765자를 초과할 수 없고 탭, 줄바꿈 문자 또는 다음 특수 문자를 포함할 수 없습니다. < > "

4. 권한 탭을 클릭합니다.
5. 도메인 또는 응용 프로그램 서비스 유형을 확장합니다.
6. 도메인 또는 응용 프로그램 서비스 유형에 대한 역할에 할당할 권한을 선택합니다.
7. 확인을 클릭합니다.

사용자 지정 역할의 속성 편집

사용자 지정 역할을 편집할 때 역할에 대한 설명을 변경할 수 있습니다. 역할의 이름은 변경할 수 없습니다.

1. **Administrator** 도구에서 보안 탭을 클릭합니다.
2. 탐색기의 역할 섹션에서 역할을 선택합니다.
3. 편집을 클릭합니다.
4. 역할의 설명을 변경하고 확인을 클릭합니다.

사용자 지정 역할에 할당된 권한 편집

각 응용 프로그램 서비스 유형 및 도메인에 대해 사용자 지정 역할에 할당된 권한을 변경할 수 있습니다.

1. **Administrator** 도구에서 보안 탭을 클릭합니다.
2. 탐색기의 역할 섹션에서 역할을 선택합니다.
3. 권한 탭을 클릭합니다.
4. 편집을 클릭합니다.

역할 및 권한 편집 대화 상자가 나타납니다.

5. 도메인 또는 응용 프로그램 서비스 유형을 확장합니다.
6. 권한을 역할에 할당하려면 도메인 또는 응용 프로그램 서비스 유형에 대한 권한을 선택합니다.
7. 권한을 역할에서 제거하려면 도메인 또는 응용 프로그램 서비스 유형에 대한 권한을 지웁니다.
8. 단계를 반복하여 각 서비스 유형에 대한 권한을 변경합니다.
9. 확인을 클릭합니다.

사용자 지정 역할 삭제

사용자 지정 역할을 삭제하는 경우 이 역할이 할당된 모든 사용자 또는 그룹에서 사용자 지정 역할 및 이 역할에 포함된 모든 권한이 제거됩니다.

사용자 지정 역할을 삭제하려면 탐색기의 역할 섹션에서 역할을 마우스 오른쪽 단추로 클릭하고 역할 삭제를 선택합니다. 역할을 삭제할 것인지 확인합니다.

사용자 및 그룹에 권한 및 역할 할당

다음 항목을 사용자 및 그룹에 할당하여 사용자가 수행할 수 있는 작업을 결정합니다.

- 권한. 권한에 따라 사용자가 응용 프로그램 클라이언트에서 수행할 수 있는 작업이 결정됩니다.
- 역할. 역할은 권한의 컬렉션입니다. 역할을 사용자 또는 그룹에 할당할 때 역할에 속한 권한 컬렉션을 할당합니다.

권한 및 역할을 사용자 및 그룹에 할당하는 경우 다음 규칙 및 지침을 사용합니다.

- 권한 및 역할을 도메인 및 도메인에서 실행되는 각 응용 프로그램 서비스의 사용자 및 그룹에 할당합니다.
다음 상황에서는 권한 및 역할을 **Metadata Manager** 서비스 또는 **PowerCenter** 리포지토리 서비스의 사용자 및 그룹에 할당할 수 없습니다.
 - 응용 프로그램 서비스가 비활성화되어 있습니다.
 - **PowerCenter** 리포지토리 서비스가 제외 모드에서 실행되고 있습니다.
- 동일한 서비스 유형의 각 응용 프로그램 서비스에 대한 서로 다른 권한 및 역할을 사용자 또는 그룹에 할당할 수 있습니다.
- 역할은 도메인 및 여러 응용 프로그램 서비스 유형에 대한 권한을 포함할 수 있습니다. 한 응용 프로그램 서비스에 대한 역할을 사용자 또는 그룹에 할당하면 해당 응용 프로그램 서비스 유형에 대한 권한이 사용자 또는 그룹에 할당됩니다.

사용자에게 할당된 권한 또는 역할을 변경하면 사용자가 다음에 로그인할 때 변경된 권한 또는 역할이 적용됩니다.

참고: 기본 관리자 사용자 계정에 할당된 권한 또는 역할은 편집할 수 없습니다.

상속된 권한

사용자 또는 그룹은 다음 개체에서 권한을 상속받을 수 있습니다.

- 그룹. 권한을 그룹에 할당하면 모든 하위 그룹 및 그룹에 속한 사용자가 권한을 상속받습니다.
- 역할. 역할을 사용자에 할당하면 사용자가 역할에 속한 권한을 상속받습니다. 역할을 그룹에 할당하면 그룹과 모든 하위 그룹, 그룹에 속한 사용자가 역할에 속한 권한을 상속받습니다. 하위 그룹 및 사용자는 역할을 상속받지 않습니다.

그룹 또는 역할에서 상속된 권한은 취소할 수 없습니다. 그룹 또는 역할에서 상속되지 않은 추가 권한을 사용자 또는 그룹에 할당할 수 있습니다.

사용자 또는 그룹의 권한 탭에 각 응용 프로그램 서비스 및 도메인의 사용자 또는 그룹에 할당된 모든 역할 및 권한이 표시됩니다. 도메인 또는 서비스에 대해 할당된 역할 및 권한을 보려면 도메인 또는 응용 프로그램 서비스를 확장합니다. 할당된 역할 및 권한에 대한 추가 정보를 표시하려면 다음 항목을 클릭합니다.

- 할당된 역할의 이름. 세부 정보 패널에 역할 세부 정보를 표시합니다.
- 할당된 역할의 정보 아이콘. 해당 역할로 상속된 모든 권한을 강조 표시합니다.

역할 또는 그룹에서 상속된 권한에는 상속 아이콘이 표시됩니다. 상속된 권한에 대한 도구 설명에 사용자가 권한을 상속받은 역할 또는 그룹이 표시됩니다.

탐색으로 사용자 또는 그룹에 권한 및 역할 할당

1. **Administrator** 도구에서 보안 탭을 클릭합니다.
2. 탐색기에서 사용자 또는 그룹을 선택합니다.
3. 권한 탭을 클릭합니다.
4. 편집을 클릭합니다.
역할 및 권한 편집 대화 상자가 나타납니다.
5. 역할을 할당하려면 역할 탭에서 도메인 또는 응용 프로그램 서비스를 확장합니다.
6. 역할을 부여하려면 도메인 또는 응용 프로그램 서비스의 사용자 또는 그룹에 할당할 역할을 선택합니다.
선택한 도메인 또는 응용 프로그램 서비스 유형에 대한 권한이 포함된 역할을 선택할 수 있습니다.
7. 역할을 취소하려면 사용자 또는 그룹에 할당된 역할을 지웁니다.
8. [5 - 7](#) 단계를 반복하여 다른 서비스에 대해 역할을 할당합니다.
9. 권한을 할당하려면 권한 탭을 클릭합니다.
10. 도메인 또는 응용 프로그램 서비스를 확장합니다.
11. 권한을 부여하려면 도메인 또는 응용 프로그램 서비스의 사용자 또는 그룹에 할당할 권한을 선택합니다.
12. 권한을 취소하려면 사용자 또는 그룹에 할당된 권한을 지웁니다.
그룹 또는 역할에서 상속된 권한은 취소할 수 없습니다.
13. [10 - 12](#) 단계를 반복하여 다른 서비스에 대해 권한을 할당합니다.
14. 확인을 클릭합니다.

서비스에 대한 권한을 가진 사용자 보기

도메인 또는 응용 프로그램 서비스에 대한 권한을 가진 모든 사용자를 볼 수 있습니다.

1. **Administrator** 도구에서 보안 탭을 클릭합니다.
2. 보안 작업 메뉴에서 서비스 사용자 권한을 클릭합니다.
서비스 대화 상자가 나타납니다.
3. 도메인 또는 응용 프로그램 서비스를 선택합니다.
세부 정보 패널에 도메인 또는 응용 프로그램 서비스에 대한 권한을 가진 모든 사용자가 표시됩니다.
4. 사용자 이름을 마우스 오른쪽 단추로 클릭하고 항목 탐색을 클릭하여 사용자로 이동합니다.

권한 및 역할 문제 해결

권한 또는 역할을 기존 **Metadata Manager 서비스** 또는 **PowerCenter 리포지토리 서비스**의 사용자에게 할당할 수 없습니다.

다음 상황에서는 권한 및 역할을 기존 **Metadata Manager 서비스** 또는 **PowerCenter 리포지토리 서비스**의 사용자 및 그룹에 할당할 수 없습니다.

- 응용 프로그램 서비스가 비활성화되어 있습니다.
- **PowerCenter 리포지토리 서비스**가 제외 모드에서 실행되고 있습니다.

그룹에서 권한을 제거했습니다. 그룹의 일부 사용자에게 해당 권한이 여전히 있는 이유가 무엇입니까?

다음 방법을 사용하면 사용자에게 권한을 할당할 수 있습니다.

- 사용자에게 직접 권한 할당
- 사용자에게 역할 할당
- 사용자가 속한 그룹에 권한 또는 역할 할당

권한을 그룹에서 제거하면 해당 그룹에 속한 사용자에게 권한이 직접 할당되거나 할당된 역할에서 권한을 상속받을 수 있습니다.

모든 도메인 권한 및 모든 도메인 개체에 대한 사용 권한이 할당되었지만 **Administrator 도구**에서 일부 태스크를 완료할 수 없습니다.

일부 **Administrator** 도구 태스크는 권한 또는 사용 권한이 아닌 관리자 역할에 따라 결정됩니다. 도메인에 대한 모든 사용 권한을 할당받고 모든 도메인 개체에 대한 전체 사용 권한을 부여받을 수 있습니다. 그러나 관리자 역할에 의해 결정되는 태스크는 완료할 수 없습니다.

응용 프로그램 서비스에 대한 관리자 역할이 할당되었지만 **Administrator 도구**에서 응용 프로그램 서비스를 구성할 수 없습니다.

응용 프로그램 서비스에 대한 관리자 역할이 있으면 응용 프로그램 클라이언트 관리자입니다. 응용 프로그램 클라이언트 관리자는 응용 프로그램 클라이언트에 대한 전체 사용 권한 및 권한을 가집니다.

그러나 응용 프로그램 클라이언트 관리자에게는 **Informatica** 도메인에 대한 사용 권한 또는 권한이 없습니다. 응용 프로그램 클라이언트 관리자는 **Administrator** 도구에 로그인하여 관리자 권한이 있는 응용 프로그램 클라이언트에 대한 서비스를 관리할 수 없습니다.

Administrator 도구에서 응용 프로그램 서비스를 관리하려면 적절한 도메인 권한 및 사용 권한이 있어야 합니다.

PowerCenter 리포지토리 서비스에 대한 관리자 역할이 할당되었지만 **Repository Manager**를 사용하여 개체의 고급 제거를 수행하거나 재사용 가능 메타데이터 확장을 작성할 수 없습니다.

Repository Manager에서 다음 작업을 수행하려면 **Administrator** 도구에서 **PowerCenter 리포지토리 서비스**에 대한 서비스 관리 도메인 권한 및 사용 권한이 있어야 합니다.

- **PowerCenter 리포지토리** 수준에서 개체 버전의 고급 제거 수행
- 재사용 가능 메타데이터 확장 작성, 편집 및 삭제

내 권한으로 응용 프로그램 클라이언트에서 개체를 편집할 수 있어야 하는데 메타데이터를 편집할 수 없습니다.

응용 프로그램 클라이언트에서 필요한 개체 사용 권한이 없을 수 있습니다. 특정 작업을 수행하는 권한이 있어도 특정 개체에서 작업을 수행하기 위한 사용 권한이 필요할 수도 있습니다.

제외 모드에서 실행 중인 새 PowerCenter 리포지토리 서비스에 연결하기 위한 pmrep를 사용할 수 없습니다.

서비스 관리자가 PowerCenter 리포지토리의 사용자 및 그룹 목록과 도메인 구성 데이터베이스의 목록을 동기화하지 않았을 수도 있습니다. 사용자 및 그룹 목록을 동기화하려면 PowerCenter 리포지토리 서비스를 다시 시작합니다.

PowerCenter 리포지토리 서비스에 대한 폴더 권한 그룹의 모든 권한이 할당되고 폴더에 대한 읽기, 쓰기 및 실행 사용 권한이 있습니다. 그러나 폴더에 대한 사용 권한을 구성할 수 없습니다.

PowerCenter 리포지토리 서비스에 대한 관리자 역할이 할당된 사용자 또는 폴더 소유자만 다음과 같은 폴더 관리 태스크를 완료할 수 있습니다.

- PowerCenter 통합 서비스가 운영 체제 프로필을 사용하는 경우 폴더에 운영 체제 프로필을 할당. 운영 체제 프로필에 대한 사용 권한이 필요합니다.
- 폴더 소유자 변경
- 폴더 사용 권한 구성
- 폴더 삭제
- 공유할 폴더 지정
- 폴더 이름 및 설명 편집

Metadata Manager 서비스에 대한 관리자 역할이 할당되었지만 Metadata Manager 리포지토리를 작성 또는 복원할 수 없습니다.

Metadata Manager 리포지토리를 작성하거나 복원하려면 기본 관리자 그룹에 있어야 합니다. 기본 관리자 그룹의 사용자는 응용 프로그램 서비스에 대한 관리자 역할이 할당된 사용자보다 더 많은 권한을 가집니다.

Metadata Manager 서비스에 대한 리소스 로드 권한을 부여받았지만 Business Glossary 리소스를 로드하려고 하면 "권한 부족" 오류가 나타납니다.

Business Glossary 리소스를 로드하려면 리소스 로드, 리소스 관리 및 모델 보기 권한이 필요합니다. 로드하려는 비즈니스 용어집 리소스에 대한 쓰기 권한도 있어야 합니다.

제 10 장

사용 권한

이 장에 포함된 항목:

- [사용 권한 개요, 172](#)
- [도메인 개체 사용 권한, 174](#)
- [연결 사용 권한, 178](#)
- [클러스터 구성 사용 권한, 180](#)
- [응용 프로그램 및 응용 프로그램 개체 사용 권한, 181](#)
- [SQL 데이터 서비스 사용 권한, 183](#)
- [웹 서비스 사용 권한, 187](#)

사용 권한 개요

사용 권한 및 권한으로 사용자 보안을 관리합니다. 사용 권한은 개체에 대한 사용자 및 그룹의 액세스 수준을 정의합니다.

사용자에게 특정 작업을 수행하는 권한이 있더라도 사용자는 특정 개체에 대한 작업을 수행하기 위한 사용 권한이 필요할 수도 있습니다.

예를 들어 사용자에게 서비스 관리 도메인 권한 및 개발 **PowerCenter** 리포지토리 서비스에 대한 사용 권한은 있지만 프로덕션 **PowerCenter** 리포지토리 서비스에 대한 사용 권한은 없습니다. 사용자는 개발 **PowerCenter** 리포지토리 서비스를 편집하거나 제거할 수 있지만 프로덕션 **PowerCenter** 리포지토리 서비스는 편집하거나 제거할 수 없습니다. 응용 프로그램 서비스를 관리하려면 사용자에게 서비스 관리 도메인 권한 및 응용 프로그램 서비스에 대한 사용 권한이 있어야 합니다.

여러 도구를 사용하여 다음 개체에 대한 사용 권한을 구성합니다.

개체 유형	도구	설명
응용 프로그램 및 응용 프로그램 개체	Administrator 도구	응용 프로그램 및 응용 프로그램 개체(예: 매핑 및 워크플로우)에 대한 사용 권한을 할당할 수 있습니다.
연결 개체	Administrator 도구 Analyst 도구 Developer tool	Administrator 도구, Analyst 도구 또는 Developer tool에서 정의된 연결에 대한 사용 권한을 할당할 수 있습니다. 이러한 도구는 연결 사용 권한을 공유합니다.

개체 유형	도구	설명
도메인 개체	Administrator 도구	다음 도메인 개체에 대한 사용 권한을 할당할 수 있습니다. 도메인, 폴더, 노드, 그리드, 라이선스, 응용 프로그램 서비스 및 운영 체제 프로필.
Metadata Manager 카탈로그 개체	Metadata Manager	Metadata Manager 폴더 및 카탈로그 개체에 대한 사용 권한을 할당할 수 있습니다.
모델 리포지토리 프로젝트	Analyst 도구 Developer tool	Analyst 도구 및 Developer tool에서 정의된 프로젝트에 대한 사용 권한을 할당할 수 있습니다. 이러한 도구는 프로젝트 사용 권한을 공유합니다.
PowerCenter 리포지토리 개체	PowerCenter 클라이언트	PowerCenter 폴더, 배포 그룹, 레이블, 쿼리 및 연결 개체에 대한 사용 권한을 할당할 수 있습니다.
SQL 데이터 서비스 개체	Administrator 도구	SQL 데이터 서비스, 가상 스키마, 가상 테이블 및 가상 저장 프로시저와 같은 SQL 데이터 개체에 대한 사용 권한을 할당할 수 있습니다.
웹 서비스 개체	Administrator 도구	웹 서비스 또는 웹 서비스 작업에 대한 사용 권한을 할당할 수 있습니다.

사용 권한 유형

사용자 및 그룹은 도메인에서 다음과 같은 유형의 사용 권한을 가질 수 있습니다.

직접 사용 권한

사용자 또는 그룹에 직접 할당된 사용 권한입니다. 사용자 및 그룹에게 개체에 대한 권한이 있는 경우 해당 개체에 대해 적합한 사용 권한이 있으면 관리 태스크를 수행할 수도 있습니다. 직접 사용 권한을 편집할 수 있습니다.

상속된 사용 권한

사용자가 상속받는 사용 권한입니다. 사용자에게 도메인 또는 폴더에 대한 사용 권한이 있는 경우 사용자는 도메인 또는 폴더의 모든 개체에 대한 사용 권한을 상속받습니다. 그룹에 도메인 개체에 대한 사용 권한이 있는 경우 그룹에 속한 모든 하위 그룹 및 사용자는 도메인 개체에 대한 사용 권한을 상속받습니다. 예를 들어 도메인에 여러 노드가 포함된 **Nodes**라는 이름의 폴더가 있습니다. 폴더에 그룹 사용 권한을 할당하면 그룹에 속한 모든 하위 그룹 및 사용자는 폴더 및 폴더의 모든 노드에 대한 사용 권한을 상속받습니다.

상속된 사용 권한은 취소할 수 없습니다. 또한 관리자 역할이 할당된 사용자 또는 그룹에서 사용 권한을 취소할 수 없습니다. 관리자 역할은 사용 권한 검사를 바이패스합니다. 관리자 역할이 있는 사용자는 모든 개체에 액세스할 수 있습니다.

일부 개체 유형에 대해 상속된 사용 권한을 거부할 수 있습니다. 사용 권한을 거부하려면 사용자 및 그룹이 이미 가지고 있을 사용 권한에 예외를 구성합니다.

유효 사용 권한

사용자 또는 그룹에 대한 모든 사용 권한의 상위 집합입니다. 직접 사용 권한과 상속된 사용 권한을 포함합니다.

사용 권한 세부 정보를 보면 유효한 사용 권한의 출처를 볼 수 있습니다. 사용 권한 세부 정보에는 사용자 또는 그룹에 할당된 직접 사용 권한, 상위 그룹에 할당된 직접 사용 권한 및 상위 개체에서 상속된 사용 권한이 표시됩니다. 또한 사용 권한 세부 정보에는 사용자 또는 그룹에 사용 권한 검사를 바이패스하는 관리자 역할이 할당되었는지 여부가 표시됩니다.

사용 권한 검색 필터

사용자 또는 그룹에 대해 사용 권한 할당, 사용 권한 세부 정보 보기 또는 사용 권한 편집을 수행할 때 검색 필터를 사용하여 사용자 또는 그룹을 검색할 수 있습니다.

사용자 또는 그룹의 사용 권한을 관리할 때 다음 검색 필터를 사용할 수 있습니다.

보안 도메인

사용자 또는 그룹을 검색할 보안 도메인을 선택합니다.

패턴 문자열

사용자 또는 그룹을 검색하려면 문자열을 입력합니다. **Administrator** 도구에서 검색 문자열이 포함된 모든 이름을 반환합니다. 문자열은 대/소문자를 구분하지 않습니다. 예를 들어 문자열 "DA"는 "iasdaemon," "daphne" 및 "DA_AdminGroup"을 반환할 수 있습니다.

또한 사용자 또는 그룹 목록을 정렬할 수 있습니다. 열 이름을 마우스 오른쪽 단추로 클릭하여 오름차순 또는 내림차순으로 열을 정렬합니다.

도메인 개체 사용 권한

도메인 내에서 사용자 보안을 관리하기 위한 권한 및 사용 권한을 구성합니다. 사용 권한은 사용자의 도메인 개체에 대한 액세스 수준을 정의합니다. **Administrator** 도구에 로그인하려면 사용자에게 하나 이상의 도메인 개체에 대한 사용 권한이 있어야 합니다. 사용자에게 개체에 대한 사용 권한은 있지만 개체 유형을 수정하는 기능을 부여하는 도메인 권한이 없는 경우 사용자는 개체를 볼 수만 있습니다.

예를 들어 사용자에게 노드에 대한 사용 권한은 있지만 노드 및 그리드 관리 권한이 없는 경우 사용자는 노드 속성을 볼 수 있지만 노드를 구성, 종료 또는 제거할 수 없습니다.

다음 유형의 도메인 개체에 대한 사용 권한을 구성할 수 있습니다.

도메인 개체 유형	사용 권한 설명
도메인	Administrator 도구 사용자는 도메인의 모든 개체에 액세스할 수 있습니다. 사용자에게 도메인에 대한 사용 권한이 있는 경우 사용자는 도메인의 모든 개체에 대한 사용 권한을 상속받습니다.
폴더	Administrator 도구 사용자는 Administrator 도구에서 폴더의 모든 개체에 액세스할 수 있습니다. 사용자에게 폴더에 대한 사용 권한이 있는 경우 사용자는 폴더의 모든 개체에 대한 사용 권한을 상속받습니다.
노드	Administrator 도구 사용자는 노드 속성을 보고 편집할 수 있습니다. 권한이 없는 경우 사용자는 응용 프로그램 서비스를 정의하거나 그리드를 작성할 때 노드를 사용할 수 없습니다.
그리드	Administrator 도구 사용자는 그리드 속성을 보고 편집할 수 있습니다. 권한이 없는 경우 사용자는 그리드를 데이터 통합 서비스 또는 PowerCenter 통합 서비스에 할당할 수 없습니다.
라이선스	Administrator 도구 사용자는 라이선스 속성을 보고 편집할 수 있습니다. 권한이 없는 경우 사용자는 응용 프로그램 서비스를 작성할 때 라이선스를 사용할 수 없습니다.

도메인 개체 유형	사용 권한 설명
응용 프로그램 서비스	Administrator 도구 사용자는 응용 프로그램 서비스 속성을 보고 편집할 수 있습니다.
운영 체제 프로필	운영 체제 프로필과 연결된 Informatica 개발자, 분석가 및 운영자는 매핑, 프로필 및 워크플로우를 실행할 수 있습니다. PowerCenter 사용자는 운영 체제 프로필과 관련된 워크플로우를 실행할 수 있습니다. 워크플로우를 실행하는 사용자에게 워크플로우에 할당된 운영 체제 프로필에 대한 사용 권한이 없는 경우 워크플로우가 실패합니다.

다음 방법을 사용하여 도메인 개체 사용 권한을 관리할 수 있습니다.

- 도메인 개체에 대한 사용 권한 관리. 도메인 개체의 사용 권한 보기를 사용하여 여러 사용자 또는 그룹의 개체에 대한 사용 권한을 할당하고 편집합니다.
- 사용자 또는 그룹에서 사용 권한 관리. 권한 관리 대화 상자를 사용하여 특정 사용자 또는 그룹의 도메인 개체에 대한 사용 권한을 할당하고 편집합니다.

참고: 운영 체제 프로필에 대한 사용 권한은 다른 도메인 개체에 대한 사용 권한을 구성하는 것과 다르게 구성합니다.

도메인 개체별 사용 권한

도메인 개체의 **사용 권한** 보기를 사용하여 여러 사용자 또는 그룹에 대해 도메인 개체에 대한 사용 권한을 할당하고 보고 편집합니다.

도메인 개체에 대한 사용 권한 할당

도메인 개체에 대한 사용 권한을 할당할 때 개체에 대한 사용자 및 그룹 액세스 권한을 부여합니다.

1. 관리 탭에서 **서비스 및 노드** 보기를 선택합니다.
2. 탐색기에서 도메인 개체를 선택합니다.
3. 콘텐츠 패널에서 **사용 권한** 보기를 선택합니다.
4. **그룹** 또는 **사용자** 탭을 클릭합니다.
5. **작업 > 권한 할당**을 클릭합니다.
사용 권한 할당 대화 상자에 개체에 대한 사용 권한이 없는 모든 사용자 또는 그룹이 표시됩니다.
6. 사용자 및 그룹을 검색하는 필터 조건을 입력하고 **필터** 단추를 클릭합니다.
7. 사용자 또는 그룹을 선택하고 **다음**을 클릭합니다.
8. **허용**을 선택하고 **마침**을 클릭합니다.

도메인 개체에 대한 사용 권한 세부 정보 보기

사용 권한 세부 정보를 보면 유효한 사용 권한의 출처를 볼 수 있습니다.

1. 관리 탭에서 **서비스 및 노드** 보기를 선택합니다.
2. 탐색기에서 도메인 개체를 선택합니다.
3. 콘텐츠 패널에서 **사용 권한** 보기를 선택합니다.
4. **그룹** 또는 **사용자** 탭을 클릭합니다.

5. 사용자 및 그룹을 검색하는 필터 조건을 입력하고 **필터** 단추를 클릭합니다.
6. 사용자 또는 그룹을 선택하고 **작업 > 권한 세부 정보 보기**를 클릭합니다.
권한 세부 정보 대화 상자가 나타납니다. 대화 상자에 사용자 또는 그룹에 할당된 직접 사용 권한, 상위 그룹에 할당된 직접 사용 권한, 상위 개체에서 상속된 사용 권한을 표시합니다. 또한 사용 권한 세부 정보에는 사용자 또는 그룹에 사용 권한 검사를 바이패스하는 관리자 역할이 할당되었는지 여부가 표시됩니다.
7. **닫기**를 클릭합니다.
8. 또는 **사용 권한 편집**을 클릭하여 직접 사용 권한을 편집합니다.

도메인 개체에 대한 사용 권한 편집

사용자 또는 그룹에 대해 도메인 개체에 대한 직접 사용 권한을 편집할 수 있습니다. 상속된 사용 권한 또는 고유한 사용 권한은 취소할 수 없습니다.

참고: 개체에 대한 직접 사용 권한을 취소하는 경우 사용자 또는 그룹은 상위 그룹 또는 개체에서 여전히 사용 권한을 상속받을 수 있습니다.

1. 관리 탭에서 **서비스 및 노드** 보기를 선택합니다.
2. 탐색기에서 도메인 개체를 선택합니다.
3. 콘텐츠 패널에서 **사용 권한** 보기를 선택합니다.
4. **그룹** 또는 **사용자** 탭을 클릭합니다.
5. 사용자 및 그룹을 검색하는 필터 조건을 입력하고 **필터** 단추를 클릭합니다.
6. 사용자 또는 그룹을 선택하고 **작업 > 직접 사용 권한 편집**을 클릭합니다.
직접 사용 권한 편집 대화 상자가 나타납니다.
7. 개체에 대한 사용 권한을 할당하려면 **허용**을 선택합니다.
8. 개체에 대한 사용 권한을 취소하려면 **취소**를 선택합니다.
권한 세부 정보 보기를 클릭하여 사용 권한이 직접 할당되거나 상속되었는지 볼 수 있습니다.
9. **확인**을 클릭합니다.

사용자 또는 그룹별 사용 권한

사용 권한 관리 대화 상자를 사용하여 특정 사용자 또는 그룹에 대한 도메인 개체 사용 권한을 보고 할당하고 편집합니다.

사용자 또는 그룹에 대한 사용 권한 세부 정보 보기

사용 권한 세부 정보를 보면 유효한 사용 권한의 출처를 볼 수 있습니다.

1. Administrator 도구에서 **보안** 탭을 클릭합니다.
2. **그룹** 탭 또는 **사용자** 탭을 클릭합니다.
3. 사용자 또는 그룹을 선택합니다.
4. **사용 권한** 탭을 클릭합니다.

사용자 또는 그룹에 대한 사용 권한 할당 및 편집

사용자 또는 그룹에 대한 도메인 개체 사용 권한을 편집할 때 사용 권한을 할당하고 기존의 직접 사용 권한을 편집할 수 있습니다. 상속된 사용 권한 또는 고유한 사용 권한은 취소할 수 없습니다.

권한 세부 정보 보기를 클릭하여 사용 권한이 직접 할당되거나 상속되었는지 볼 수 있습니다. 개체에 대한 사용 권한을 취소하는 경우 사용자 또는 그룹은 상위 그룹 또는 개체에서 여전히 사용 권한을 상속받을 수 있습니다.

1. Administrator 도구에서 **보안** 탭을 클릭합니다.
2. **그룹** 탭 또는 **사용자** 탭을 클릭합니다.
3. 사용자 또는 그룹을 선택합니다.
4. **사용 권한** 탭을 클릭합니다.
5. 도메인 개체를 선택하고 **직접 사용 권한 편집**을 클릭합니다.
6. 개체에 대한 사용 권한을 할당하려면 **허용**을 선택합니다.
7. 개체에 대한 사용 권한을 취소하려면 **취소**를 선택합니다.
8. **확인**을 클릭합니다.

운영 체제 프로필 사용 권한

Administrator 도구의 보안 페이지에서 운영 체제 프로필에 대한 사용 권한을 할당하고, 보고, 편집합니다.

관리자 그룹에는 모든 운영 체제 프로필에 대한 사용 권한이 있습니다.

운영 체제 프로필에 대한 사용 권한 할당

운영 체제 프로필에 대한 사용 권한을 할당하면 Informatica 사용자는 운영 체제 프로필을 사용하여 매핑, 프로필 및 워크플로우를 실행합니다. PowerCenter 사용자는 운영 체제 프로필에 할당된 워크플로우를 실행합니다.

1. Administrator 도구에서 **보안** 탭을 클릭합니다.
2. **운영 체제 프로필** 탭을 클릭합니다.
3. 운영 체제 프로필을 선택하고 **사용 권한** 탭을 클릭합니다.
4. **그룹** 탭 또는 **사용자** 탭을 클릭하고 **직접 사용 권한 편집**을 선택합니다.
5. 도메인 개체를 선택하고 **직접 사용 권한 편집**을 클릭합니다.
6. 개체에 대한 사용 권한을 할당하려면 **허용**을 선택합니다.
7. 개체에 대한 사용 권한을 취소하려면 **취소**를 선택합니다.
8. **확인**을 클릭합니다.

운영 체제 프로필에 대한 사용 권한 세부 정보 보기

사용 권한 세부 정보를 보면 유효한 사용 권한의 출처를 볼 수 있습니다.

1. **보안** 탭에서 **운영 체제 프로필** 보기를 선택합니다.
2. 운영 체제 프로필을 선택하고 **사용 권한** 탭을 클릭합니다.
3. **그룹** 또는 **사용자** 보기를 선택합니다.
4. 사용자 및 그룹을 검색하는 필터 조건을 입력하고 **필터** 단추를 클릭합니다.
5. 사용자 또는 그룹을 선택하고 **사용 권한 세부 정보 보기**를 클릭합니다.

권한 세부 정보 대화 상자가 나타납니다. 대화 상자에 사용자 또는 그룹에 할당된 직접 사용 권한, 상위 그룹에 할당된 직접 사용 권한, 상위 개체에서 상속된 사용 권한을 표시합니다. 또한 사용 권한 세부 정보에는 사용자 또는 그룹에 사용 권한 검사를 바이패스하는 관리자 역할이 할당되었는지 여부가 표시됩니다.

6. 닫기를 클릭합니다.
7. 또는 **사용 권한 편집**을 클릭하여 직접 사용 권한을 편집합니다.

운영 체제 프로필에 대한 사용 권한 편집

사용자 또는 그룹의 운영 체제 프로필에 대한 직접 사용 권한을 편집할 수 있습니다. 상속된 사용 권한 또는 고유한 사용 권한은 취소할 수 없습니다.

참고: 개체에 대한 직접 사용 권한을 취소하는 경우 사용자 또는 그룹은 상위 그룹 또는 개체에서 여전히 사용 권한을 상속받을 수 있습니다.

1. **보안** 탭에서 **운영 체제 프로필** 보기를 선택합니다.
2. 운영 체제 프로필을 선택하고 **사용 권한** 탭을 클릭합니다.
3. **그룹** 또는 **사용자** 보기를 선택합니다.
4. 사용자 및 그룹을 검색하는 필터 조건을 입력하고 **필터** 단추를 클릭합니다.
5. 사용자 또는 그룹을 선택하고 **직접 사용 권한 편집**을 클릭합니다.
직접 사용 권한 편집 대화 상자가 나타납니다.
6. 운영 체제 프로필에 대한 사용 권한을 할당하려면 **허용**을 선택합니다.
7. 운영 체제 프로필에 대한 사용 권한을 취소하려면 **취소**를 선택합니다.
권한 세부 정보 보기를 클릭하여 사용 권한이 직접 할당되거나 상속되었는지 볼 수 있습니다.
8. **확인**을 클릭합니다.

연결 사용 권한

사용 권한에 따라 연결에 대한 사용자 또는 그룹 액세스 수준이 제어됩니다.

Analyst 도구, **Developer** 도구 또는 **Administrator** 도구에서 연결에 대한 사용 권한을 구성할 수 있습니다.

하나의 도구에서 사용자 또는 그룹에 할당된 연결 사용 권한은 다른 도구에서도 적용됩니다. 예를 들어 **Developer** 도구에서 **ConnectionA**에 대해 **GroupA** 사용 권한을 부여합니다. **Analyst** 도구 및 **Administrator** 도구에서도 **GroupA**에는 **ConnectionA**에 대한 사용 권한이 있습니다.

하나의 도구에서 사용자 또는 그룹에 할당된 연결 사용 권한은 다른 도구에서도 적용됩니다. 예를 들어 **Developer** 도구에서 **ConnectionA**에 대해 **GroupA** 사용 권한을 부여합니다. **Administrator** 도구에서도 **GroupA**에는 **ConnectionA**에 대한 사용 권한이 있습니다.

다음과 같은 **Informatica** 구성 요소는 연결 사용 권한을 사용합니다.

- **Administrator** 도구. 연결에 대해 읽기, 쓰기 및 실행 사용 권한을 적용합니다.
- **Analyst** 도구. 연결에 대해 읽기, 쓰기 및 실행 사용 권한을 적용합니다.
- **Informatica** 명령줄 인터페이스. 연결에 대해 읽기, 쓰기 및 부여 사용 권한을 적용합니다.
- **Developer** 도구. 연결에 대해 읽기, 쓰기 및 실행 사용 권한을 적용합니다.
 SQL 데이터 서비스의 경우 **Developer** 도구는 연결 사용 권한을 적용하지 않습니다. 대신 열 수준 및 통과 보안 적용하여 데이터에 대한 액세스를 제한합니다.
- 데이터 통합 서비스. 사용자가 데이터를 미리 보거나 매핑, 성과 기록표 또는 프로필을 실행하려는 경우 실행 사용 권한을 적용합니다.

참고: 프로파일링 웨어하우스, 데이터 개체 캐시 데이터베이스 또는 모델 리포지토리 등 연결에 대한 사용 권한을 할당할 수 없습니다.

연결 사용 권한 유형

여러 사용 권한 유형을 사용자에게 할당하여 다음 작업을 수행할 수 있습니다.

작업	사용 권한 유형
연결 이름, 유형, 설명, 연결 문자열 및 사용자 이름과 같은 암호를 제외한 모든 연결 메타데이터를 봅니다.	읽기
암호를 포함하여 모든 연결 메타데이터를 편집합니다. 연결 삭제 쓰기 권한이 있는 사용자는 읽기 권한을 상속받습니다.	쓰기
연결에서 정의된 기본 데이터 소스의 물리적 데이터에 액세스합니다. 사용자는 데이터 미리 보기, 매핑 실행, 워크플로우 매핑 태스크에서 매핑 실행, 성과 기록표 실행 또는 연결을 사용하는 프로필 실행을 수행할 수 있습니다.	실행
연결에 대한 사용 권한을 부여하고 취소합니다.	권한 부여

기본 연결 사용 권한

도메인 관리자에게는 모든 연결에 대한 모든 사용 권한이 있습니다. 연결을 작성하는 사용자에게는 연결에 대한 읽기, 쓰기, 실행 및 부여 권한이 있습니다. 기본적으로 모든 사용자에게는 연결에 대해 다음 작업을 수행하기 위한 권한이 있습니다.

- 연결 이름, 유형 및 설명과 같은 기본 연결 메타데이터 보기
- Developer 도구에서 매핑의 연결 사용
- 연결의 개체에 대해 Analyst 도구에서 프로필 작성

연결에 대한 사용 권한 할당

연결에 대한 사용 권한을 할당할 때 사용자 또는 그룹의 연결에 대한 액세스 수준을 정의합니다.

1. 관리 탭에서 **연결** 보기를 선택합니다.
2. 탐색기에서 연결을 선택합니다.
3. 콘텐츠 패널에서 **사용 권한** 보기를 선택합니다.
4. **그룹** 또는 **사용자** 탭을 클릭합니다.
5. **작업 > 사용 권한 할당**을 클릭합니다.

사용 권한 할당 대화 상자에 연결에 대한 사용 권한이 없는 모든 사용자 또는 그룹이 표시됩니다.

6. 사용자 및 그룹을 검색하는 필터 조건을 입력하고 **필터** 단추를 클릭합니다.
7. 사용자 또는 그룹을 선택하고 **다음**을 클릭합니다.
8. 할당할 각 사용 권한 유형에 대해 **허용**을 선택합니다.
9. **마침**을 클릭합니다.

연결에 대한 사용 권한 세부 정보 보기

사용 권한 세부 정보를 보면 유효한 사용 권한의 출처를 볼 수 있습니다.

1. 관리 탭에서 **연결** 보기를 선택합니다.
2. 탐색기에서 연결을 선택합니다.
3. 콘텐츠 패널에서 **사용 권한** 보기를 선택합니다.
4. **그룹** 또는 **사용자** 탭을 클릭합니다.
5. 사용자 또는 그룹을 선택하고 **작업 > 사용 권한 세부 정보 보기**를 클릭합니다.

사용 권한 세부 정보 보기 대화 상자가 나타납니다. 대화 상자에 사용자 또는 그룹에 할당된 직접 사용 권한 및 상위 그룹에 할당된 직접 사용 권한이 표시됩니다. 또한 사용 권한 세부 정보에는 사용자 또는 그룹에 사용 권한 검사를 바이패스하는 관리자 역할이 할당되었는지 표시됩니다.

6. **닫기**를 클릭합니다.
7. 또는 **사용 권한 편집**을 클릭하여 직접 사용 권한을 편집합니다.

연결에 대한 사용 권한 편집

사용자 또는 그룹에 대해 연결에 대한 직접 사용 권한을 편집할 수 있습니다. 상속된 사용 권한 또는 고유한 사용 권한은 취소할 수 없습니다.

참고: 개체에 대한 직접 사용 권한을 취소하는 경우 사용자 또는 그룹은 상위 그룹 또는 개체에서 여전히 사용 권한을 상속받을 수 있습니다.

1. 관리 탭에서 **연결** 보기를 선택합니다.
2. 탐색기에서 연결을 선택합니다.
3. 콘텐츠 패널에서 **사용 권한** 보기를 선택합니다.
4. **그룹** 또는 **사용자** 탭을 클릭합니다.
5. 사용자 및 그룹을 검색하는 필터 조건을 입력하고 **필터** 단추를 클릭합니다.
6. 사용자 또는 그룹을 선택하고 **작업 > 직접 사용 권한 편집**을 클릭합니다.

직접 사용 권한 편집 대화 상자가 나타납니다.

7. 사용 권한을 허용 또는 취소할 수 있습니다.
 - 사용 권한을 할당하려면 **허용**을 선택합니다.
 - 단일 사용 권한을 취소하려면 **허용**을 지웁니다.
 - 모든 사용 권한을 취소하려면 **취소**를 선택합니다.

권한 세부 정보 보기를 클릭하여 사용 권한이 직접 할당되거나 상속되었는지 볼 수 있습니다.

8. **확인**을 클릭합니다.

클러스터 구성 사용 권한

사용 권한에 따라 클러스터 구성에 대한 사용자 또는 그룹 액세스 수준이 제어됩니다.

Administrator 도구와 Informatica 명령줄 인터페이스에서 클러스터 구성에 대한 사용 권한을 구성할 수 있습니다.

클러스터 구성에 대한 다음 사용 권한을 사용자 또는 그룹에 설정할 수 있습니다.

- 읽기. 사용자 또는 그룹 멤버는 클러스터 구성을 볼 수 있습니다.
- 쓰기. 사용자 또는 그룹 멤버는 클러스터 구성을 편집할 수 있습니다. 읽기 권한이 포함됩니다.
- 실행. 사용자 또는 그룹 멤버는 Hadoop 환경에서 맵핑을 실행할 수 있습니다.
- 권한 부여. 사용자 또는 그룹 멤버는 클러스터 구성에 대한 사용 권한을 다른 사용자 및 그룹에 부여할 수 있습니다. 읽기 권한이 포함됩니다.
- 모두. 사용자는 허용되는 모든 사용 권한을 상속합니다.

기본적으로 모든 사용자는 클러스터 구성 이름을 볼 수 있습니다.

응용 프로그램 및 응용 프로그램 개체 사용 권한

사용 권한은 응용 프로그램 및 응용 프로그램 개체(예: 맵핑, 워크플로우)에 대한 사용자 또는 그룹의 액세스 수준을 제어합니다.

Administrator 도구 또는 명령줄에서 응용 프로그램 및 응용 프로그램 개체 사용 권한을 구성할 수 있습니다.

응용 프로그램 및 응용 프로그램 개체 사용 권한의 유형

사용자 및 그룹에 보기 사용 권한, 부여 사용 권한 및 실행 사용 권한을 할당할 수 있습니다.

다음 사용 권한을 사용자 및 그룹에 할당할 수 있습니다.

보기 사용 권한

응용 프로그램 및 응용 프로그램 개체를 봅니다.

부여 사용 권한

응용 프로그램 및 응용 프로그램 개체에 대한 사용 권한을 부여하고 취소합니다.

실행 사용 권한

응용 프로그램 및 응용 프로그램 개체를 실행합니다.

참고: Administrator 도구 또는 명령줄에서 시작, 중지 또는 백업과 같은 응용 프로그램 작업을 수행하려면 사용자에게 해당 응용 프로그램에 대한 응용 프로그램 관리 권한 및 실행 사용 권한이 있어야 합니다.

응용 프로그램 또는 응용 프로그램 개체에 대한 사용 권한 할당

응용 프로그램 또는 응용 프로그램 개체에 대한 사용 권한을 할당할 때 응용 프로그램 또는 응용 프로그램 개체에 대한 사용자 또는 그룹의 액세스 수준을 정의합니다.

1. 관리 탭에서 **서비스 및 노드** 보기를 선택합니다.
2. 탐색기에서 데이터 통합 서비스를 선택합니다.
3. 콘텐츠 패널에서 **응용 프로그램** 보기를 선택합니다.
4. 응용 프로그램, 맵핑 또는 워크플로우를 선택합니다.
5. 세부 정보 패널에서 **그룹 사용 권한** 또는 **사용자 사용 권한** 보기를 선택합니다.
6. **사용 권한 할당** 단추를 클릭합니다.

사용 권한 할당 대화 상자에 응용 프로그램 또는 응용 프로그램 개체에 대한 사용 권한이 없는 모든 사용자 또는 그룹이 표시됩니다.

7. 사용자 및 그룹을 검색하는 필터 조건을 입력하고 **필터** 단추를 클릭합니다.
8. 사용자 또는 그룹을 선택하고 **다음**을 클릭합니다.
9. 할당할 각 사용 권한 유형에 대해 **허용**을 선택합니다.
10. **마침**을 클릭합니다.

응용 프로그램 또는 응용 프로그램 개체에 대한 사용 권한 세부 정보 보기

사용 권한 세부 정보를 보면 유효한 사용 권한의 출처를 볼 수 있습니다.

1. 관리 탭에서 **서비스 및 노드** 보기를 선택합니다.
2. 탐색기에서 데이터 통합 서비스를 선택합니다.
3. 콘텐츠 패널에서 **응용 프로그램** 보기를 선택합니다.
4. 응용 프로그램, 매핑 또는 워크플로우를 선택합니다.
5. 세부 정보 패널에서 **그룹 사용 권한** 또는 **사용자 사용 권한** 보기를 선택합니다.
6. 사용자 및 그룹을 검색하는 필터 조건을 입력하고 **필터** 단추를 클릭합니다.
7. 사용자 또는 그룹을 선택하고 **사용 권한 세부 정보 보기** 단추를 클릭합니다.

권한 세부 정보 대화 상자가 나타납니다. 대화 상자에 사용자 또는 그룹에 할당된 직접 사용 권한, 상위 그룹에 할당된 직접 사용 권한, 상위 개체에서 상속된 사용 권한을 표시합니다. 또한 사용 권한 세부 정보에는 사용자 또는 그룹에 사용 권한 검사를 바이패스하는 관리자 역할이 할당되었는지 여부가 표시됩니다.

8. **닫기**를 클릭합니다.
9. 또는 **사용 권한 편집**을 클릭하여 직접 사용 권한을 편집합니다.

응용 프로그램 또는 응용 프로그램 개체에 대한 사용 권한 편집

사용자 또는 그룹에 대해 응용 프로그램 또는 응용 프로그램 개체에 대한 직접 사용 권한을 편집할 수 있습니다. 상속된 사용 권한 또는 고유한 사용 권한은 취소할 수 없습니다.

참고: 개체에 대한 직접 사용 권한을 취소하는 경우 사용자 또는 그룹은 상위 그룹 또는 개체에서 여전히 권한을 상속받을 수 있습니다.

1. 관리 탭에서 **서비스 및 노드** 보기를 선택합니다.
2. 탐색기에서 데이터 통합 서비스를 선택합니다.
3. 콘텐츠 패널에서 **응용 프로그램** 보기를 선택합니다.
4. 응용 프로그램 또는 응용 프로그램 개체를 선택합니다.
5. 세부 정보 패널에서 **그룹 사용 권한** 또는 **사용자 사용 권한** 보기를 선택합니다.
6. 사용자 및 그룹을 검색하는 필터 조건을 입력하고 **필터** 단추를 클릭합니다.
7. 사용자 또는 그룹을 선택하고 **직접 사용 권한 편집** 단추를 클릭합니다.

직접 사용 권한 편집 대화 상자가 나타납니다.

8. 사용 권한을 허용 또는 취소할 수 있습니다.
 - 사용 권한을 할당하려면 **허용**을 선택합니다.
 - 단일 사용 권한을 취소하려면 **허용**을 지웁니다.
 - 모든 사용 권한을 취소하려면 **취소**를 선택합니다.

권한 세부 정보 보기를 클릭하여 사용 권한이 직접 할당되거나 상속되었는지 볼 수 있습니다.

9. **확인**을 클릭합니다.

응용 프로그램 또는 응용 프로그램 개체에 대한 사용 권한 거부

응용 프로그램 및 응용 프로그램 개체에 대한 사용 권한을 명시적으로 거부할 수 있습니다. 사용 권한을 거부하면 유효한 사용 권한에 예외를 적용합니다.

SQL 데이터 서비스 사용 권한

최종 사용자는 JDBC 또는 ODBC 클라이언트 도구를 통해 SQL 데이터 서비스에 연결할 수 있습니다. 연결되면 사용자가 SQL 데이터 서비스의 가상 테이블에서 SQL 쿼리를 실행하거나 SQL 데이터 서비스에서 가상 저장 프로시저를 실행할 수 있습니다. 사용 권한에 따라 SQL 데이터 서비스에 대한 사용자 액세스 수준이 제어됩니다.

사용자 및 그룹에게 다음 SQL 데이터 서비스 개체에 대한 사용 권한을 할당할 수 있습니다.

- SQL 데이터 서비스
- 가상 테이블
- 가상 저장 프로시저

SQL 데이터 서비스 개체에 대한 사용 권한을 할당할 때 사용자 또는 그룹은 SQL 데이터 서비스 개체에 속하는 모든 개체에 대해 동일한 사용 권한을 상속합니다. 예를 들어 사용자에게 SQL 데이터 서비스에 대한 선택 권한을 할당하는 경우가 있습니다. 그러면 사용자가 SQL 데이터 서비스의 모든 가상 테이블에 대한 선택 권한을 상속합니다.

일부 SQL 데이터 서비스 개체에 대한 사용자 및 그룹의 사용 권한을 거부할 수 있습니다. 사용 권한을 거부하려면 사용자 및 그룹이 이미 가지고 있을 사용 권한에 예외를 구성합니다. 예를 들어 가상 테이블의 열에는 사용 권한을 할당할 수 없지만 사용자가 해당 열을 포함하는 SQL SELECT 문을 실행하지 못하도록 거부할 수 있습니다.

SQL 데이터 서비스 사용 권한 유형

다음 사용 권한을 사용자 및 그룹에 할당할 수 있습니다.

- 부여 사용 권한. 사용자가 Administrator 도구 또는 *infacmd* 명령줄 프로그램을 사용하여 SQL 데이터 서비스 개체에 대해 사용 권한을 부여 및 취소할 수 있습니다.
- 실행 사용 권한. 사용자가 JDBC 또는 ODBC 클라이언트 도구를 사용하여 SQL 데이터 서비스에서 가상 저장 프로시저를 실행할 수 있습니다.
- 선택 사용 권한. 사용자가 JDBC 또는 ODBC 클라이언트 도구를 사용하여 SQL 데이터 서비스의 가상 테이블에서 SQL SELECT 문을 실행할 수 있습니다.

일부 사용 권한은 모든 SQL 데이터 서비스 개체에 적용할 수 없습니다.

다음 테이블에는 각 SQL 데이터 서비스 개체에 대한 사용 권한이 설명되어 있습니다.

개체	부여 사용 권한	실행 사용 권한	선택 사용 권한
SQL 데이터 서비스	SQL 데이터 서비스 및 SQL 데이터 서비스의 모든 개체에 대한 사용 권한을 부여하고 취소합니다.	SQL 데이터 서비스에서 모든 가상 저장 프로시저를 실행합니다.	SQL 데이터 서비스의 모든 가상 테이블에서 SQL SELECT 문을 실행합니다.
가상 테이블	가상 테이블에 대한 사용 권한을 부여하고 취소합니다.	-	가상 테이블에서 SQL SELECT 문을 실행합니다.
가상 저장 프로시저	가상 저장 프로시저에 대한 사용 권한을 부여하고 취소합니다.	가상 저장 프로시저를 실행합니다.	-

SQL 데이터 서비스에 대한 사용 권한 할당

SQL 데이터 서비스 개체에 대한 사용 권한을 할당할 때 사용자 또는 그룹의 개체에 대한 액세스 수준을 정의합니다.

1. 관리 탭에서 **서비스 및 노드** 보기를 선택합니다.
2. 탐색기에서 데이터 통합 서비스를 선택합니다.
3. 콘텐츠 패널에서 **응용 프로그램** 보기를 선택합니다.
4. SQL 데이터 서비스 개체를 선택합니다.
5. 세부 정보 패널에서 **그룹 사용 권한** 또는 **사용자 사용 권한** 보기를 선택합니다.
6. **권한 할당** 단추를 클릭합니다.

사용 권한 할당 대화 상자에 SQL 데이터 서비스 개체에 대한 사용 권한이 없는 모든 사용자 또는 그룹이 표시됩니다.

7. 사용자 및 그룹을 검색하는 필터 조건을 입력하고 **필터** 단추를 클릭합니다.
8. 사용자 또는 그룹을 선택하고 **다음**을 클릭합니다.
9. 할당할 각 사용 권한 유형에 대해 **허용**을 선택합니다.
10. **마침**을 클릭합니다.

SQL 데이터 서비스에 대한 사용 권한 세부 정보 보기

사용 권한 세부 정보를 보면 유효한 사용 권한의 출처를 볼 수 있습니다.

1. 관리 탭에서 **서비스 및 노드** 보기를 선택합니다.
2. 탐색기에서 데이터 통합 서비스를 선택합니다.
3. 콘텐츠 패널에서 **응용 프로그램** 보기를 선택합니다.
4. SQL 데이터 서비스 개체를 선택합니다.
5. 세부 정보 패널에서 **그룹 사용 권한** 또는 **사용자 사용 권한** 보기를 선택합니다.
6. 사용자 및 그룹을 검색하는 필터 조건을 입력하고 **필터** 단추를 클릭합니다.
7. 사용자 또는 그룹을 선택하고 **권한 세부 정보 보기** 단추를 클릭합니다.

권한 세부 정보 대화 상자가 나타납니다. 대화 상자에 사용자 또는 그룹에 할당된 직접 사용 권한, 상위 그룹에 할당된 직접 사용 권한, 상위 개체에서 상속된 사용 권한을 표시합니다. 또한 사용 권한 세부 정보에는 사용자 또는 그룹에 사용 권한 검사를 바이패스하는 관리자 역할이 할당되었는지 여부가 표시됩니다.

8. **닫기**를 클릭합니다.
9. 또는 **사용 권한 편집**을 클릭하여 직접 사용 권한을 편집합니다.

SQL 데이터 서비스에 대한 사용 권한 편집

사용자 또는 그룹에 대해 SQL 데이터 서비스에 대한 직접 사용 권한을 편집할 수 있습니다. 상속된 사용 권한 또는 고유한 사용 권한은 취소할 수 없습니다.

참고: 개체에 대한 직접 사용 권한을 취소하는 경우 사용자 또는 그룹은 상위 그룹 또는 개체에서 여전히 사용 권한을 상속받을 수 있습니다.

1. 관리 탭에서 **서비스 및 노드** 보기를 선택합니다.
2. 탐색기에서 데이터 통합 서비스를 선택합니다.
3. 콘텐츠 패널에서 **응용 프로그램** 보기를 선택합니다.
4. SQL 데이터 서비스 개체를 선택합니다.

5. 세부 정보 패널에서 **그룹 사용 권한** 또는 **사용자 사용 권한** 보기를 선택합니다.
6. 사용자 및 그룹을 검색하는 필터 조건을 입력하고 **필터** 단추를 클릭합니다.
7. 사용자 또는 그룹을 선택하고 **직접 사용 권한 편집** 단추를 클릭합니다.
직접 사용 권한 편집 대화 상자가 나타납니다.
8. 사용 권한을 허용 또는 취소할 수 있습니다.
 - 사용 권한을 할당하려면 **허용**을 선택합니다.
 - 단일 사용 권한을 취소하려면 **허용**을 지웁니다.
 - 모든 사용 권한을 취소하려면 **취소**를 선택합니다.**권한 세부 정보 보기**를 클릭하여 사용 권한이 직접 할당되거나 상속되었는지 볼 수 있습니다.
9. **확인**을 클릭합니다.

SQL 데이터 서비스에 대한 사용 권한 거부

일부 SQL 데이터 서비스 개체에 대한 사용 권한을 명시적으로 거부할 수 있습니다. SQL 데이터 서비스의 개체에 대한 사용 권한을 거부하는 경우 유효한 사용 권한에 예외를 적용합니다.

사용 권한을 거부하려면 다음 `infacmd` 명령 중 하나를 사용합니다.

- `infacmd sql SetStoredProcedurePermissions`. 저장 프로시저 수준에서 실행 또는 부여 사용 권한을 거부합니다.
- `infacmd sql SetTablePermissions`. 가상 테이블 수준에서 선택 및 부여 사용 권한을 거부합니다.
- `infacmd sql SetColumnPermissions`. 열 수준에서 선택 사용 권한을 거부합니다.

각 열에는 사용 권한(-ap)을 적용하고 사용 권한을 거부(-dp)하기 위한 옵션이 있습니다.

`SetColumnPermissions` 명령은 사용 권한 적용 옵션을 포함하지 않습니다.

참고: Administrator 도구에서 사용 권한을 거부할 수 없습니다.

데이터 통합 서비스는 가상 데이터베이스에서 저장 프로시저 및 SQL 쿼리를 실행하기 전에 사용 권한을 확인합니다. 데이터 통합 서비스는 SQL 데이터 서비스 수준에서 시작하는 사용자 또는 그룹에 대한 사용 권한을 검사합니다. 사용 권한이 SQL 데이터 서비스의 상위 개체에 적용되는 경우 하위 개체가 사용 권한을 상속받습니다. 데이터 통합 서비스는 열 수준에서 거부된 사용 권한을 확인합니다.

열 수준 보안

관리자는 SQL 데이터 개체의 가상 테이블에 있는 열에 대한 액세스를 거부할 수 있습니다. 관리자는 제한된 열에 대한 쿼리에 데이터 통합 서비스 동작을 구성할 수 있습니다.

사용자가 사용자에게 사용 권한이 없는 열을 쿼리하는 경우 다음 결과가 발생할 수 있습니다.

- 쿼리가 데이터 대신 대체 값을 반환합니다. 쿼리가 반환하는 각 행의 대체 값을 반환합니다. 대체 값은 쿼리에서 요청한 열 값을 바꿉니다. 쿼리가 필터 또는 조인을 포함하는 경우 대체 결과가 결과에 표시됩니다.
- 쿼리가 권한 없음 오류와 함께 실패합니다.

SQL 데이터 서비스에 대한 보안 구성에 대한 자세한 내용은 Informatica 방법 라이브러리 문서 "SQL 데이터 서비스에 대한 보안 구성 방법"을 참조하십시오.

https://kb.informatica.com/h2l/HowTo%20Library/1/0266_ConfiguringSecurityForSQLDataServices.pdf.

제한된 열

열 수준 보안을 구성하는 경우 사용자가 쿼리에서 제한된 열을 선택할 때 수행되는 작업을 결정하는 열 옵션을 설정합니다. 제한된 데이터를 기본값으로 대체할 수 있습니다. 또는 사용자가 제한된 열을 선택하는 경우 쿼리를 실패로 처리할 수 있습니다.

예를 들어 관리자는 **Employee** 테이블에서 **salary** 열에 대한 사용자 액세스를 거부합니다. 관리자는 **salary** 열에 대한 대체 값으로 **100,000**을 구성합니다. 사용자가 **SQL** 쿼리에서 **salary** 열을 선택하면 데이터 통합 서비스가 각 행의 **salary**에 대해 **100,000**을 반환합니다.

infacmd sql UpdateColumnOptions 명령을 실행하여 열 옵션을 구성합니다. **Administrator** 도구에서는 열 옵션을 설정할 수 없습니다.

infacmd sql UpdateColumnOptions를 실행할 때 다음 옵션을 입력합니다.

ColumnOptions.DenyWith=옵션

제한된 열 값을 대체할지 쿼리를 실패로 처리할지 여부를 결정합니다. 열 값을 대체하는 경우 값을 **Null**로 대체하거나 상수 값으로 대체할 수 있습니다. 다음 옵션 중 하나를 입력합니다.

- 오류. **SQL** 쿼리에서 제한된 열을 선택할 경우 쿼리가 실패하고 오류가 반환됩니다.
- **NULL**. 각 행의 제한된 열에 대해 **Null** 값을 반환합니다.
- 값. 각 행의 제한된 열 위치에 상수 값을 반환합니다. **ColumnOptions.InsufficientPermissionValue** 옵션에서 상수 값을 구성합니다.

ColumnOptions.InsufficientPermissionValue=값

제한된 열 값을 상수로 대체합니다. 기본값은 빈 문자열입니다. 데이터 통합 서비스가 열을 빈 문자열로 대체하지만 열이 숫자 또는 날짜인 경우 쿼리가 오류를 반환합니다. **DenyWith** 옵션에 대한 값을 구성하지 않은 경우 데이터 통합 서비스는 **InsufficientPermissionValue** 옵션을 무시합니다.

열에 대한 대체 값을 구성하려면 다음 구문이 포함된 명령을 입력합니다.

```
infacmd sql UpdateColumnOptions -dn empDomain -sn DISService -un Administrator -pd Adminpass -sqlds employee_APP.employees_SQL -t Employee -c Salary -o ColumnOptions.DenyWith=VALUE ColumnOptions.InsufficientPermissionValue=100000
```

제한된 열에 대해 어떤 옵션도 구성하지 않는 경우 기본적으로 쿼리를 실패로 처리하지 않습니다. 쿼리가 실행되고 데이터 통합 서비스가 열 값을 **NULL**로 대체합니다.

열 수준 보안 추가

infacmd sql SetColumnPermissions 명령을 사용하여 열 수준 보안을 구성합니다. **Administrator** 도구에서는 열 수준 보안을 설정할 수 없습니다.

Employee 테이블에는 **FirstName**, **LastName**, **Dept** 및 **Salary** 열이 포함되어 있습니다. 사용자가 **Employee** 테이블에는 액세스할 수 있지만 **salary** 열에 액세스하지 않도록 제한합니다.

salary 열에서 사용자를 제한하려면 데이터 통합 서비스를 비활성화하고 다음 명령과 유사한 **infacmd**를 입력합니다.

```
infacmd sql SetColumnPermissions -dn empDomain -sn DISService -un Administrator -pd Adminpass -sqlds employee_APP.employees -t Employee -c Salary -Tom -dp SQL_Select
```

다음 **SQL** 문은 **salary** 열에서 **NULL**을 반환합니다.

```
Select * from Employee  
Select LastName, Salary from Employee
```

기본 동작은 **Null** 값을 반환하는 것입니다.

웹 서비스 사용 권한

최종 사용자는 웹 서비스 클라이언트를 통해 웹 서비스 요청을 보내고 웹 서비스 응답을 받을 수 있습니다. 사용 권한에 따라 웹 서비스에 대한 사용자 액세스 수준이 제어됩니다.

사용자 및 그룹에 다음 웹 서비스 개체에 대한 사용 권한을 할당할 수 있습니다.

- 웹 서비스
- REST 웹 서비스 리소스
- SOAP 웹 서비스 작업

웹 서비스 개체에 대한 사용 권한을 할당하면 사용자 또는 그룹에 웹 서비스 개체에 속한 모든 개체에 대한 동일한 사용 권한이 상속됩니다. 예를 들어 웹 서비스에 대한 사용자 실행 권한을 할당합니다. 사용자는 웹 서비스의 웹 서비스 작업에 대한 실행 사용 권한을 상속받습니다.

사용자 및 그룹에 대해 웹 서비스 작업에 대한 사용 권한을 거부할 수 있습니다. 사용 권한을 거부하려면 사용자 및 그룹이 이미 가지고 있을 사용 권한에 예외를 구성합니다. 예를 들어 사용자에게 3개의 작업이 있는 웹 서비스에 대한 실행 사용 권한이 있습니다. 사용자가 웹 서비스에 속한 한 개의 웹 서비스 작업을 실행하는 것을 거부할 수 있습니다.

웹 서비스 사용 권한 유형

관리자는 웹 서비스 사용 권한을 다음 유형의 사용자 및 그룹에 할당합니다.

- 웹 서비스 소비자. 웹 서비스에 요청을 전송하고 웹 서비스로부터 응답을 수신하는 원시 도메인 사용자입니다. 이 사용자에게는 웹 서비스에 대한 실행 사용 권한이 있어야 합니다.
- 웹 서비스 관리자. 관리자로 로그인하고 웹 서비스 속성을 편집하고 다른 사용자에게 사용 권한을 부여할 수 있는 사용자입니다.
- 웹 서비스 운영자. 관리자로 로그인하고 웹 서비스를 모니터링하고 웹 서비스를 시작하거나 중지할 수 있는 사용자입니다.

관리자는 다음 사용 권한을 사용자 및 그룹에 할당할 수 있습니다.

- 부여 사용 권한. 사용자는 **Administrator** 도구 또는 *infacmd* 명령줄 프로그램을 사용하여 웹 서비스 개체에 대한 사용 권한을 관리할 수 있습니다.
- 실행 사용 권한. 사용자가 웹 서비스 요청을 전송하고 웹 서비스 응답을 수신할 수 있습니다.

다음 테이블에는 각 SOAP 웹 서비스 개체에 대한 사용 권한이 설명되어 있습니다.

개체	부여 사용 권한	실행 사용 권한
SOAP 웹 서비스	웹 서비스 및 웹 서비스 내 모든 웹 서비스 작업에 대한 사용 권한을 부여하고 취소합니다.	웹 서비스 요청을 전송하고 웹 서비스 내 모든 웹 서비스 작업에서 웹 서비스 응답을 수신합니다.
SOAP 웹 서비스 작업	웹 서비스 작업에 대한 사용 권한을 부여, 취소 및 거부합니다.	웹 서비스 요청을 전송하고 웹 서비스 작업에서 웹 서비스 응답을 수신합니다.

다음 테이블에는 각 REST 웹 서비스 개체에 대한 사용 권한이 설명되어 있습니다.

개체	부여 사용 권한	실행 사용 권한
REST 웹 서비스	REST 웹 서비스 및 웹 서비스 내 모든 웹 서비스 리소스에 대한 사용 권한을 부여하고 취소합니다.	웹 서비스 요청을 전송하고 REST 웹 서비스 내 모든 웹 서비스 리소스에서 웹 서비스 응답을 수신합니다.
REST 리소스	REST 웹 서비스 리소스에 대한 사용 권한을 부여, 취소 및 거부합니다.	웹 서비스 요청을 전송하고 REST 웹 서비스 리소스에서 웹 서비스 응답을 수신합니다.

웹 서비스에 대한 사용 권한 할당

웹 서비스 개체에 대한 사용 권한을 할당할 때 사용자 또는 그룹의 개체에 대한 액세스 수준을 정의합니다.

1. 관리 탭에서 **서비스 및 노드** 보기를 선택합니다.
2. 탐색기에서 데이터 통합 서비스를 선택합니다.
3. 콘텐츠 패널에서 **응용 프로그램** 보기를 선택합니다.
4. 웹 서비스 개체를 선택합니다.
5. 세부 정보 패널에서 **그룹 사용 권한** 또는 **사용자 사용 권한** 보기를 선택합니다.
6. **권한 할당** 단추를 클릭합니다.
사용 권한 할당 대화 상자에 SQL 데이터 서비스 개체에 대한 사용 권한이 없는 모든 사용자 또는 그룹이 표시됩니다.
7. 사용자 및 그룹을 검색하는 필터 조건을 입력하고 **필터** 단추를 클릭합니다.
8. 사용자 또는 그룹을 선택하고 **다음**을 클릭합니다.
9. 할당할 각 사용 권한 유형에 대해 **허용**을 선택합니다.
10. **마침**을 클릭합니다.

웹 서비스에 대한 사용 권한 세부 정보 보기

사용 권한 세부 정보를 보면 유효한 사용 권한의 출처를 볼 수 있습니다.

1. 관리 탭에서 **서비스 및 노드** 보기를 선택합니다.
2. 탐색기에서 데이터 통합 서비스를 선택합니다.
3. 콘텐츠 패널에서 **응용 프로그램** 보기를 선택합니다.
4. 웹 서비스 개체를 선택합니다.
5. 세부 정보 패널에서 **그룹 사용 권한** 또는 **사용자 사용 권한** 보기를 선택합니다.
6. 사용자 및 그룹을 검색하는 필터 조건을 입력하고 **필터** 단추를 클릭합니다.
7. 사용자 또는 그룹을 선택하고 **권한 세부 정보 보기** 단추를 클릭합니다.

권한 세부 정보 대화 상자가 나타납니다. 대화 상자에 사용자 또는 그룹에 할당된 직접 사용 권한, 상위 그룹에 할당된 직접 사용 권한, 상위 개체에서 상속된 사용 권한을 표시합니다. 또한 사용 권한 세부 정보에는 사용자 또는 그룹에 사용 권한 검사를 바이패스하는 관리자 역할이 할당되었는지 여부가 표시됩니다.

8. **닫기**를 클릭합니다.
9. 또는 **사용 권한 편집**을 클릭하여 직접 사용 권한을 편집합니다.

웹 서비스에 대한 사용 권한 편집

사용자 또는 그룹에 대해 웹 서비스에 대한 직접 사용 권한을 편집할 수 있습니다. 웹 서비스 개체에 대한 사용 권한을 편집할 때 개체에 대한 사용 권한을 거부할 수 있습니다. 상속된 사용 권한 또는 고유한 사용 권한은 취소할 수 없습니다.

참고: 개체에 대한 직접 사용 권한을 취소하는 경우 사용자 또는 그룹은 상위 그룹 또는 개체에서 여전히 사용 권한을 상속받을 수 있습니다.

1. 관리 탭에서 **서비스 및 노드** 보기를 선택합니다.
2. 탐색기에서 데이터 통합 서비스를 선택합니다.
3. 콘텐츠 패널에서 **응용 프로그램** 보기를 선택합니다.
4. 웹 서비스 개체를 선택합니다.
5. 세부 정보 패널에서 **그룹 사용 권한** 또는 **사용자 사용 권한** 보기를 선택합니다.
6. 사용자 및 그룹을 검색하는 필터 조건을 입력하고 **필터** 단추를 클릭합니다.
7. 사용자 또는 그룹을 선택하고 **직접 사용 권한 편집** 단추를 클릭합니다.

직접 사용 권한 편집 대화 상자가 나타납니다.

8. 사용 권한을 허용 또는 취소할 수 있습니다.
 - 사용 권한을 할당하려면 **허용**을 선택합니다.
 - 웹 서비스 개체에 대한 사용 권한을 거부하려면 **거부**를 선택합니다.
 - 단일 사용 권한을 취소하려면 **허용**을 지웁니다.
 - 모든 사용 권한을 취소하려면 **취소**를 선택합니다.

권한 세부 정보 보기를 클릭하여 사용 권한이 직접 할당되거나 상속되었는지 볼 수 있습니다.

9. **확인**을 클릭합니다.

제 11 장

감사 보고서

이 장에 포함된 항목:

- [감사 보고 개요, 190](#)
- [사용자 개인 정보, 191](#)
- [사용자 그룹 연관, 191](#)
- [권한, 192](#)
- [역할 연관, 193](#)
- [도메인 개체 사용 권한, 193](#)
- [감사 보고서를 위한 사용자 선택, 194](#)
- [감사 보고서를 위한 그룹 선택, 194](#)
- [감사 보고서를 위한 역할 선택, 195](#)

감사 보고 개요

감사 보고서를 사용하여 Informatica 도메인의 사용자 및 그룹에 대한 정보와 이들에게 할당된 권한 및 사용 권한에 대한 정보를 봅니다.

다음과 같은 감사 보고서를 생성할 수 있습니다.

사용자 개인 정보

사용자 상태를 포함하여 도메인의 사용자 계정에 대한 정보를 표시합니다. 보고서를 생성하려는 사용자 또는 그룹을 선택할 수 있습니다.

사용자 그룹 연관

사용자와 사용자가 속하는 그룹에 대한 정보를 표시합니다. 보고서를 생성하려는 사용자 또는 그룹을 선택할 수 있습니다.

권한

도메인의 사용자 및 그룹에 할당된 권한에 대한 정보를 표시합니다. 보고서를 생성하려는 사용자 또는 그룹을 선택할 수 있습니다.

역할

도메인의 사용자 및 그룹에 할당된 역할에 대한 정보를 표시합니다. 보고서를 생성하려는 역할을 선택할 수 있습니다.

도메인 개체 사용 권한

사용자 및 그룹이 사용 권한을 가진 도메인 개체에 대한 정보를 표시합니다. 보고서를 생성하려는 사용자 또는 그룹을 선택할 수 있습니다.

CSV, 텍스트 또는 PDF 파일을 비롯하여 다른 형식으로 감사 보고서를 생성할 수 있습니다. 또한 화면에서 보고서를 볼 수 있습니다.

Administrator 도구 또는 명령줄에서 감사 보고서를 생성할 수 있습니다. 명령줄에서 감사 보고서를 실행하려면 `infacmd aud` 명령줄 프로그램을 실행합니다.

사용자 개인 정보

사용자 개인 정보 보고서에는 도메인의 사용자 계정 상태 및 연락처 정보가 표시됩니다.

그룹에 대해 보고서를 실행하는 경우 보고서에 그룹별로 사용자 목록이 구성되고 각 그룹에 대한 그룹 이름 및 보안 도메인이 표시됩니다. 보고서에 중첩 그룹이 별도로 표시됩니다.

사용자 개인 정보 보고서에는 다음 정보가 표시됩니다.

로그인 이름

사용자 계정의 로그인 이름입니다.

전체 이름

사용자 계정의 전체 이름입니다.

보안 도메인

사용자가 속한 보안 도메인입니다.

설명

사용자 계정에 대한 설명입니다.

전자 메일 ID

사용자 계정의 전자 메일 주소입니다.

전화

사용자 계정의 전화 번호입니다.

계정 잠금

계정이 잠겨있는지 여부를 나타냅니다. 보고서는 계정이 잠긴 경우 예를 표시하고 계정이 잠겨 있지 않은 경우 아니오를 표시합니다.

계정 비활성화됨

계정이 비활성화되어 있는지 여부를 나타냅니다. 보고서는 계정이 비활성화된 경우 예를 표시하고 계정이 활성화된 경우 아니오를 표시합니다.

사용자 그룹 연관

사용자 그룹 연관 보고서에는 사용자 및 해당 연관 그룹에 대한 정보가 표시됩니다.

사용자에 대해 보고서를 실행하는 경우 보고서에 사용자 및 사용자가 속한 그룹의 목록이 표시됩니다.

사용자 그룹 연관 보고서에는 다음 정보가 표시됩니다.

로그인 이름

사용자 계정의 로그인 이름입니다.

전체 이름

사용자 계정의 전체 이름입니다.

보안 도메인

사용자 계정이 속한 보안 도메인입니다.

그룹 이름

사용자가 속한 그룹의 이름입니다.

그룹 경로

그룹이 단일 그룹인 경우 그룹 경로에 그룹 이름이 표시됩니다. 그룹이 중첩 그룹인 경우 그룹 경로에 중첩 그룹의 계층 내 해당 그룹의 위치가 표시됩니다.

그룹 보안 도메인

사용자가 속한 그룹의 보안 도메인입니다.

그룹에 대해 보고서를 실행하는 경우 보고서에 그룹별로 사용자 목록이 구성되고 각 그룹에 대한 그룹 이름 및 보안 도메인이 표시됩니다. 보고서에 중첩 그룹이 별도로 표시됩니다. 각 그룹별로, 보고서에 그룹에 속한 사용자 및 하위 그룹 목록이 표시됩니다.

사용자 그룹 연관 보고서에는 그룹에 속한 사용자에 대한 다음 정보가 표시됩니다.

로그인 이름

사용자 계정의 로그인 이름입니다.

전체 이름

사용자 계정의 전체 이름입니다.

보안 도메인

사용자 계정이 속한 보안 도메인입니다.

사용자 그룹 연관 보고서에는 그룹에 속한 하위 그룹에 대한 다음 정보가 표시됩니다.

그룹 이름

그룹의 이름입니다.

보안 도메인

그룹이 속한 보안 도메인입니다.

그룹 경로

그룹이 단일 그룹인 경우 그룹 경로에 그룹 이름이 표시됩니다. 그룹이 중첩 그룹인 경우 그룹 경로에 중첩 그룹의 계층 내 해당 그룹의 위치가 표시됩니다.

권한

권한 보고서는 사용자, 그룹, 사용자 및 그룹에 할당된 권한을 표시합니다.

사용자에 대해 보고서를 실행하는 경우 보고서는 사용자 목록 및 각 사용자에게 할당된 권한을 표시합니다. 그룹에 대해 보고서를 실행하는 경우 보고서는 그룹 목록 및 각 그룹에 할당된 권한을 표시합니다.

권한 보고서에는 다음 정보가 표시됩니다.

권한 이름

권한의 이름입니다.

권한 경로

권한이 포함된 권한 그룹의 계층입니다.

개체 이름

권한이 허용된 개체의 이름입니다.

개체 유형

권한이 허용된 개체의 유형입니다.

역할 연관

역할 연관 보고서에는 역할 목록과 역할이 할당된 사용자 및 그룹이 표시됩니다.

역할 연관 보고서에는 다음 정보가 표시됩니다.

로그인 이름

역할이 할당된 사용자 계정의 로그인 이름입니다. 사용자 목록에 대해 표시합니다.

전체 이름

역할이 할당된 사용자 계정의 전체 이름입니다. 사용자 목록에 대해 표시합니다.

그룹 이름

역할이 할당된 그룹의 이름입니다. 그룹 목록에 대해 표시합니다.

보안 도메인

사용자 또는 그룹이 속한 보안 도메인입니다.

개체 이름

역할의 권한 집합이 허용된 개체 이름입니다.

개체 유형

역할의 권한 집합이 허용된 개체 유형입니다.

도메인 개체 사용 권한

도메인 개체 사용 권한 보고서에는 사용자 및 그룹과 사용자 및 그룹이 사용 권한을 가진 개체가 표시됩니다.

사용자에 대해 보고서를 실행하는 경우 보고서에 사용자 및 사용자가 사용 권한을 가진 개체 목록이 표시됩니다.

그룹에 대해 보고서를 실행하는 경우 보고서에 그룹 및 그룹이 사용 권한을 가진 개체 목록이 표시됩니다.

도메인 개체 사용 권한 보고서에는 다음 정보가 표시됩니다.

개체 이름

사용자 또는 그룹이 사용 권한을 가진 개체의 이름입니다.

개체 유형

사용자 또는 그룹이 사용 권한을 가진 개체의 유형입니다.

개체 경로

리포지토리에서 개체의 위치입니다.

감사 보고서를 위한 사용자 선택

여러 사용자에 대해 감사 보고서를 생성할 수 있습니다.

1. Administrator 도구에서 **보안 > 감사 보고서**를 클릭합니다.
2. **보고서 유형 선택** 목록에서 실행하려는 감사 보고서 유형을 선택합니다.
3. **보고서 생성 대상** 목록에서 **사용자**를 선택하고 **이동**을 클릭합니다.
사용자 선택 대화 상자가 나타납니다. 기본적으로 사용자 아이콘이 선택되고 모든 사용 가능한 사용자 목록이 표시됩니다. 목록에 사용자의 전체 이름 및 사용자가 속한 보안 도메인이 표시됩니다.
4. **사용 가능한 사용자** 목록에서 보고서를 실행하려는 사용자를 선택합니다.
여러 사용자를 선택하려면 Shift 키 또는 Ctrl 키를 사용합니다.
5. 그룹별로 사용자를 선택하려면 **그룹** 아이콘을 클릭합니다.
사용 가능한 그룹 목록에 도메인의 모든 그룹이 표시되고 멤버 목록에 그룹의 멤버인 사용자가 표시됩니다. 멤버 목록에서 보고서를 실행하려는 사용자를 선택합니다. 여러 그룹에서 사용자를 선택할 수 있습니다.
6. **추가**를 클릭합니다.
모든 사용자에 대해 보고서를 실행하려면 사용자 아이콘을 클릭한 다음 사용자를 선택하지 않고 **모두 추가**를 클릭합니다.
그룹의 모든 사용자에 대해 보고서를 실행하려면 그룹 아이콘을 클릭합니다. 그룹을 선택하고 멤버 목록에서 사용자를 선택하지 않고 **모두 추가**를 클릭합니다.
선택한 사용자가 **선택한 사용자** 목록으로 이동합니다.
7. **보고서 출력 형식** 목록에서 보고서를 보려는 형식을 선택합니다.
기본적으로 보고서가 화면에 표시됩니다.
또한 다음 형식 중 하나로 감사 보고서를 볼 수 있습니다.
 - 텍스트. 열에 나열된 값을 사용하는 텍스트 파일로 감사 보고서를 생성합니다.
 - CSV. 쉼표로 구분된 값을 사용하는 텍스트 파일로 감사 보고서를 생성합니다.
 - PDF. .pdf 형식으로 감사 보고서를 생성합니다. 보고서를 보려면 Acrobat Reader를 설치해야 합니다.
8. **보고서 생성**을 클릭합니다.

감사 보고서를 위한 그룹 선택

여러 그룹에 대해 감사 보고서를 실행할 수 있습니다.

1. Administrator 도구에서 **보안 > 감사 보고서**를 클릭합니다.
2. **보고서 유형 선택** 목록에서 실행하려는 감사 보고서 유형을 선택합니다.
3. **보고서 생성 대상** 목록에서 **그룹**을 선택하고 **이동**을 클릭합니다.
그룹 선택 대화 상자가 나타납니다. 그룹 목록이 보안 도메인으로 구성됩니다.

4. **사용 가능한 그룹** 목록에서 보고서를 실행하려는 그룹을 선택합니다.
여러 그룹을 선택하려면 **Shift** 키 또는 **Ctrl** 키를 사용합니다.
5. **추가**를 클릭합니다.
모든 그룹에 대해 보고서를 실행하려면 그룹을 선택하지 않고 **모두 추가**를 클릭합니다.
선택한 그룹이 **선택한 그룹** 목록으로 이동합니다.
6. **보고서 출력 형식** 목록에서 보고서를 보려는 형식을 선택합니다.
기본적으로 보고서가 화면에 표시됩니다.
또한 다음 형식 중 하나로 감사 보고서를 실행할 수 있습니다.
 - 텍스트. 열에 나열된 값을 사용하는 텍스트 파일로 감사 보고서를 생성합니다.
 - CSV. 쉼표로 구분된 값을 사용하는 텍스트 파일로 감사 보고서를 생성합니다.
 - PDF. .pdf 형식으로 감사 보고서를 생성합니다. 보고서를 보려면 Acrobat Reader를 설치해야 합니다.
7. **보고서 생성**을 클릭합니다.

감사 보고서를 위한 역할 선택

역할 연관 보고서를 실행하는 경우 보고서를 실행하려는 역할을 선택해야 합니다.

1. Administrator 도구에서 **보안 > 감사 보고서**를 클릭합니다.
2. **보고서 유형 선택** 목록에서 **역할 연관** 보고서를 선택합니다.
3. **보고서 생성 대상** 목록에서 **역할**을 선택하고 **이동**을 클릭합니다.
역할 선택 대화 상자가 나타납니다. 시스템 정의 역할 목록은 사용자 지정 역할 목록과 별도로 표시됩니다.
4. **사용 가능한 역할** 목록에서 보고서를 실행하려는 역할을 선택합니다.
여러 역할을 선택하려면 **Shift** 키 또는 **Ctrl** 키를 사용합니다.
5. **추가**를 클릭합니다.
모든 역할에 대해 보고서를 실행하려면 역할을 선택하지 않고 **모두 추가**를 클릭합니다.
선택한 역할이 **선택한 역할** 목록으로 이동합니다.
6. **보고서 출력 형식** 목록에서 보고서를 보려는 형식을 선택합니다.
기본적으로 보고서가 화면에 표시됩니다.
또한 다음 형식 중 하나로 감사 보고서를 실행할 수 있습니다.
 - 텍스트. 열에 나열된 값을 사용하는 텍스트 파일로 감사 보고서를 생성합니다.
 - CSV. 쉼표로 구분된 값을 사용하는 텍스트 파일로 감사 보고서를 생성합니다.
 - PDF. .pdf 형식으로 감사 보고서를 생성합니다. 보고서를 보려면 Acrobat Reader를 설치해야 합니다.
7. **보고서 생성**을 클릭합니다.

부록 A

명령줄 권한 및 사용 권한

이 부록에 포함된 항목:

- [infacmd as 명령, 196](#)
- [infacmd cluster 명령, 197](#)
- [infacmd dis 명령, 198](#)
- [infacmd dp 명령, 199](#)
- [infacmd es 명령, 199](#)
- [infacmd ipc 명령, 200](#)
- [infacmd isp 명령, 200](#)
- [infacmd mas 명령, 208](#)
- [infacmd mi 명령, 209](#)
- [infacmd mrs 명령, 209](#)
- [infacmd ms 명령, 211](#)
- [infacmd tools 명령, 212](#)
- [infacmd ps 명령, 212](#)
- [infacmd pwx 명령, 213](#)
- [infacmd rms 명령, 214](#)
- [infacmd rtm 명령, 214](#)
- [infacmd sch 명령, 214](#)
- [infacmd sql 명령, 215](#)
- [infacmd wfs 명령, 216](#)
- [pmcmd 명령, 216](#)
- [pmrep 명령, 219](#)

infacmd as 명령

infacmd as 명령을 실행하려면 나열된 도메인 권한, 분석 서비스 권한 및 도메인 개체 사용 권한 집합 중 하나가 있어야 합니다.

다음 표에는 *infacmd as* 명령에 필요한 권한 및 사용 권한이 나열되어 있습니다.

infacmd as 명령	권한 그룹	권한 이름	사용 권한
CreateAuditTables	도메인 관리	서비스 관리	분석 서비스가 실행되는 도메인 또는 노드
CreateService	도메인 관리	서비스 관리	분석 서비스가 실행되는 도메인 또는 노드
DeleteAuditTables	도메인 관리	서비스 관리	분석 서비스가 실행되는 도메인 또는 노드
ListServiceOptions	-	-	분석 서비스
ListServiceProcessOptions	-	-	분석 서비스
UpdateServiceOptions	도메인 관리	서비스 관리	분석 서비스가 실행되는 도메인 또는 노드
UpdateServiceProcessOptions	도메인 관리	서비스 관리	분석 서비스가 실행되는 도메인 또는 노드

infacmd cluster 명령

infacmd cluster 명령을 실행하려면 사용자에게 나열된 도메인 권한 및 클러스터 구성 사용 권한 집합 중 하나가 있어야 합니다.

다음 테이블에는 *infacmd cluster* 명령에 필요한 권한 및 사용 권한이 나열되어 있습니다.

infacmd cluster 명령	권한 그룹	권한 이름	사용 권한
clearConfigurationProperties	도메인 관리	연결 관리	클러스터 구성에 대한 쓰기
createConfiguration	도메인 관리	연결 관리	클러스터 구성에 대한 쓰기
deleteConfiguration	도메인 관리	연결 관리	클러스터 구성에 대한 쓰기
exportConfiguration(중요한 속성 포함)	-	-	클러스터 구성에 대한 쓰기
exportConfiguration(중요한 속성 제외)	-	-	클러스터 구성에 대한 읽기
listAssociatedConnections	-	-	-
listConfigurations	-	-	-
listConfigurationGroupPermissions	-	-	-

infacmd cluster 명령	권한 그룹	권한 이름	사용 권한
listConfigurationProperties	-	-	클러스터 구성에 대한 읽기
listConfigurationSets	-	-	클러스터 구성에 대한 읽기
listConfigurationUserPermissions	-	-	-
refreshConfiguration	도메인 관리	연결 관리	클러스터 구성에 대한 쓰기
setConfigurationPermissions	-	-	클러스터 구성에 대한 권한 부여
setConfigurationProperties	도메인 관리	연결 관리	클러스터 구성에 대한 쓰기

infacmd dis 명령

infacmd dis 명령을 실행하려면 나열된 도메인 권한, 데이터 통합 서비스 권한 및 도메인 개체 사용 권한 집합 중 하나가 있어야 합니다.

다음 표에는 *infacmd as* 명령에 필요한 권한 및 사용 권한이 나열되어 있습니다.

infacmd dis 명령	권한 그룹	권한 이름	사용 권한
BackupApplication	응용 프로그램 관리	응용 프로그램 관리	응용 프로그램
CancelDataObjectCache Refresh	-	-	-
CreateService	도메인 관리	서비스 관리	데이터 통합 서비스가 실행되는 도메인 또는 노드
DeployApplication	응용 프로그램 관리	응용 프로그램 관리	응용 프로그램
ListApplicationObjects	-	-	-
ListApplications	-	-	-
ListComputeOptions	도메인 관리	서비스 관리	데이터 통합 서비스
ListDataObjectOptions	-	-	-
ListServiceOptions	도메인 관리	서비스 관리	데이터 통합 서비스
ListServiceProcessOptions	도메인 관리	서비스 관리	데이터 통합 서비스
PurgeDataObjectCache	-	-	-

infacmd dis 명령	권한 그룹	권한 이름	사용 권한
RefreshDataObjectCache	-	-	-
RenameApplication	응용 프로그램 관리	응용 프로그램 관리	응용 프로그램
RestoreApplication	응용 프로그램 관리	응용 프로그램 관리	응용 프로그램
StartApplication	응용 프로그램 관리	응용 프로그램 관리	응용 프로그램
StopApplication	응용 프로그램 관리	응용 프로그램 관리	응용 프로그램
stopBlazeService	응용 프로그램 관리	응용 프로그램 관리	응용 프로그램
UndeployApplication	응용 프로그램 관리	응용 프로그램 관리	응용 프로그램
UpdateApplication	응용 프로그램 관리	응용 프로그램 관리	응용 프로그램
UpdateApplicationOptions	응용 프로그램 관리	응용 프로그램 관리	응용 프로그램
UpdateDataObjectOptions	응용 프로그램 관리	응용 프로그램 관리	-
UpdateComputeOptions	도메인 관리	서비스 관리	데이터 통합 서비스
UpdateServiceOptions	도메인 관리	서비스 관리	데이터 통합 서비스
UpdateServiceProcessOptions	도메인 관리	서비스 관리	데이터 통합 서비스

infacmd dp 명령

다음 infacmd dp 명령을 실행하려면 원시 사용자인거나 관리 역할이 할당된 사용자여야 합니다.

- startSparkJobServer
- stopSparkJobServer

infacmd es 명령

다음 infacmd es 명령을 실행하려면 도메인에 대한 관리자 역할이 있어야 합니다.

- ListServiceOptions
- UpdateServiceOptions
- UpdateSMTPOptions

infacmd ipc 명령

infacmd ipc 명령을 실행하려면 나열된 모델 리포지토리 개체 사용 권한 중 하나가 있어야 합니다.

다음 표에는 *infacmd ipc* 명령에 필요한 권한 및 사용 권한이 나열되어 있습니다.

infacmd ipc 명령	권한 그룹	권한 이름	사용 권한
ExportToPC	-	-	내보낼 참조 테이블을 작성하는 폴더에 대한 읽기
genReuseReportFromPC	도구	Repository Manager 액세스	-

infacmd isp 명령

infacmd isp 명령을 실행하려면 나열된 도메인 권한, 서비스 권한, 도메인 개체 권한 및 연결 사용 권한 집합 중 하나가 있어야 합니다.

다음 테이블에는 *infacmd isp* 명령에 필요한 권한 및 사용 권한이 나열되어 있습니다.

infacmd isp 명령	권한 그룹	권한 이름	사용 권한 대상
AddAlertUser(다른 사용자)	보안 관리	사용자, 그룹 및 역할 관리	-
AddAlertUser(자신의 사용자 계정)	-	-	-
AddConnectionPermissions	-	-	연결에 대한 부여
AddDomainLink*	-	-	-
AddDomainNode	도메인 관리	노드 및 그리드 관리	도메인 및 노드
AddGroupPrivilege	보안 관리	권한 및 역할 부여	도메인, Metadata Manager 서비스, 모델 리포지토리 서비스 또는 PowerCenter 리포지토리 서비스.
AddLicense	도메인 관리	서비스 관리	도메인 또는 상위 폴더
AddNodeResource	도메인 관리	노드 및 그리드 관리	노드
AddRolePrivilege	보안 관리	사용자, 그룹 및 역할 관리	-
AddServiceLevel*	-	-	-

infacmd isp 명령	권한 그룹	권한 이름	사용 권한 대상
AddUserToGroup	보안 관리	사용자, 그룹 및 역할 관리	-
AssignGroupPermission(응용 프로그램 서비스 또는 라이선스 개체)	도메인 관리	서비스 관리	응용 프로그램 서비스 또는 라이선스 개체
AssignGroupPermission(도메인)*	-	-	-
AssignGroupPermission(폴더)	도메인 관리	도메인 폴더 관리	폴더
AssignGroupPermission(노드 및 그리드)	도메인 관리	노드 및 그리드 관리	노드 또는 그리드
AssignGroupPermission(운영 체제 프로필)*	-	-	-
AssignISTOMMService	도메인 관리	서비스 관리	Metadata Manager 서비스
AssignLicense	도메인 관리	서비스 관리	라이선스 개체 및 응용 프로그램 서비스
AssignRSToWSHubService	도메인 관리	서비스 관리	PowerCenter 리포지토리 서비스 및 웹 서비스 협
AssignRoleToGroup	보안 관리	권한 및 역할 부여	도메인, Metadata Manager 서비스, 모델 리포지토리 서비스 또는 PowerCenter 리포지토리 서비스.
AssignRoleToUser	보안 관리	권한 및 역할 부여	도메인, Metadata Manager 서비스, 모델 리포지토리 서비스 또는 PowerCenter 리포지토리 서비스.
AssignUserPermission(응용 프로그램 서비스 또는 라이선스 개체)	도메인 관리	서비스 관리	응용 프로그램 서비스 또는 라이선스 개체
AssignUserPermission(도메인)*	-	-	-
AssignUserPermission(폴더)	도메인 관리	도메인 폴더 관리	폴더
AssignUserPermission(노드 또는 그리드)	도메인 관리	노드 및 그리드 관리	노드 또는 그리드
AssignUserPermission(운영 체제 프로필)*	-	-	-
AssignUserPrivilege	보안 관리	권한 및 역할 부여	도메인, Metadata Manager 서비스, 모델 리포지토리 서비스 또는 PowerCenter 리포지토리 서비스.
AssignedToLicense	도메인 관리	서비스 관리	라이선스 개체 및 응용 프로그램 서비스

infacmd isp 명령	권한 그룹	권한 이름	사용 권한 대상
ConvertLogFile	-	-	도메인 또는 응용 프로그램 서비스
CreateConnection*	-	-	-
CreateFolder	도메인 관리	도메인 폴더 관리	도메인 또는 상위 폴더
CreateGrid	도메인 관리	노드 및 그리드 관리	그리드에 할당된 도메인 또는 상위 폴더 및 노드
CreateGroup	보안 관리	사용자, 그룹 및 역할 관리	-
CreateIntegrationService	도메인 관리	서비스 관리	도메인 또는 상위 폴더, PowerCenter 통합 서비스가 실행되는 노드 또는 그리드, 라이선스 개체 및 연결된 PowerCenter 리포지토리 서비스
CreateMMService	도메인 관리	서비스 관리	도메인 또는 상위 폴더, Metadata Manager 서비스가 실행되는 노드, 라이선스 개체, 연결된 PowerCenter 통합 서비스 및 PowerCenter 리포지토리 서비스
CreateOSProfile*	-	-	-
CreateRepositoryService	도메인 관리	서비스 관리	도메인 또는 상위 폴더, PowerCenter 리포지토리 서비스가 실행되는 노드 및 라이선스 개체
CreateRole	보안 관리	사용자, 그룹 및 역할 관리	-
CreateSAPBWService	도메인 관리	서비스 관리	도메인 또는 상위 폴더, SAP BW 서비스가 실행되는 노드 또는 그리드, 라이선스 개체 및 연결된 PowerCenter 통합 서비스
CreateUser	보안 관리	사용자, 그룹 및 역할 관리	-
CreateWSHubService	도메인 관리	서비스 관리	도메인 또는 상위 폴더, 웹 서비스 협이 실행되는 노드 또는 그리드, 라이선스 개체 및 연결된 PowerCenter 리포지토리 서비스
DisableNodeResource	도메인 관리	노드 및 그리드 관리	노드
DisableService(Metadata Manager 서비스)	도메인 관리	서비스 실행 관리	Metadata Manager 서비스 및 연결된 PowerCenter 통합 서비스 및 PowerCenter 리포지토리 서비스
DisableService(다른 모든 응용 프로그램 서비스)	도메인 관리	서비스 실행 관리	응용 프로그램 서비스

infacmd isp 명령	권한 그룹	권한 이름	사용 권한 대상
DisableServiceProcess	도메인 관리	서비스 실행 관리	응용 프로그램 서비스
DisableUser	보안 관리	사용자, 그룹 및 역할 관리	-
EditUser	보안 관리	사용자, 그룹 및 역할 관리	-
EnableNodeResource	도메인 관리	노드 및 그리드 관리	노드
EnableService(Metadata Manager 서비스)	도메인 관리	서비스 실행 관리	Metadata Manager 서비스 및 연결된 PowerCenter 통합 서비스 및 PowerCenter 리포지토리 서비스
EnableService(다른 모든 응용 프로그램 서비스)	도메인 관리	서비스 실행 관리	응용 프로그램 서비스
EnableServiceProcess	도메인 관리	서비스 실행 관리	응용 프로그램 서비스
EnableUser	보안 관리	사용자, 그룹 및 역할 관리	-
ExportDomainObjects(연결)	도메인 관리	연결 관리	연결에 대한 읽기
ExportDomainObjects(사용자, 그룹 및 역할)	보안 관리	사용자, 그룹 및 역할 관리	-
ExportUsersAndGroups	보안 관리	사용자, 그룹 및 역할 관리	-
GetFolderInfo	-	-	폴더
GetLastError	-	-	응용 프로그램 서비스
GetLog	-	-	도메인 또는 응용 프로그램 서비스
GetNodeName	-	-	노드
GetServiceOption	-	-	응용 프로그램 서비스
GetServiceProcessOption	-	-	응용 프로그램 서비스
GetServiceProcessStatus	-	-	응용 프로그램 서비스
GetServiceStatus	-	-	응용 프로그램 서비스
GetSessionLog	런타임 개체	모니터링	리포지토리 폴더에 대한 읽기
GetWorkflowLog	런타임 개체	모니터링	리포지토리 폴더에 대한 읽기

infacmd isp 명령	권한 그룹	권한 이름	사용 권한 대상
도움말	-	-	-
ImportDomainObjects(연결)	도메인 관리	연결 관리	연결에 대한 쓰기
ImportDomainObjects(사용자, 그룹 및 역할)	보안 관리	사용자, 그룹 및 역할 관리	-
ImportUsersAndGroups	보안 관리	사용자, 그룹 및 역할 관리	-
ListAlertUsers	-	-	도메인
ListAllGroups	-	-	-
ListAllRoles	-	-	-
ListAllUsers	-	-	-
ListConnectionOptions	-	-	연결에 대한 읽기
ListConnectionPermissions	-	-	-
ListConnectionPermissions(그룹 기준)	-	-	-
ListConnectionPermissions(사용자 기준)	-	-	-
ListConnections	-	-	-
ListDomainLinks	-	-	도메인
ListDomainOptions	-	-	도메인
ListFolders	-	-	폴더
ListGridNodes	-	-	-
ListGroupPermissions	-	-	-
ListGroupPrivilege	보안 관리	권한 및 역할 부여	도메인, Metadata Manager 서비스, 모델 리포지토리 서비스 또는 PowerCenter 리포지토리 서비스.
ListGroupsForUser	-	-	도메인
ListLDAPConnectivity	보안 관리	사용자, 그룹 및 역할 관리	-
ListLicenses	-	-	라이선스 개체
ListNodeOptions	-	-	노드
ListNodeResources	-	-	노드

infacmd isp 명령	권한 그룹	권한 이름	사용 권한 대상
ListNodes	-	-	-
ListPlugins	-	-	-
ListRepositoryLDAPConfiguration	-	-	도메인
ListRolePrivileges	-	-	-
ListSMTPOptions	-	-	도메인
ListSecurityDomains	보안 관리	사용자, 그룹 및 역할 관리	-
ListServiceLevels	-	-	도메인
ListServiceNodes	-	-	응용 프로그램 서비스
ListServicePrivileges	-	-	-
ListServices	-	-	-
ListUserPermissions	-	-	-
ListUserPrivilege	보안 관리	권한 및 역할 부여	도메인, Metadata Manager 서비스, 모델 리포지토리 서비스 또는 PowerCenter 리포지토리 서비스.
MoveFolder	도메인 관리	도메인 폴더 관리	원래 폴더 및 대상 폴더
MoveObject(응용 프로그램 서비스 또는 라이선스 개체)	도메인 관리	서비스 관리	원래 폴더 및 대상 폴더
MoveObject(노드 또는 그리드)	도메인 관리	노드 및 그리드 관리	원래 폴더 및 대상 폴더
Ping	-	-	-
PurgeLog*	-	-	-
RemoveAlertUser(다른 사용자)	보안 관리	사용자, 그룹 및 역할 관리	-
RemoveAlertUser(자신의 사용자 계정)	-	-	-
RemoveConnection	-	-	연결에 대한 쓰기
RemoveConnectionPermissions	-	-	연결에 대한 부여
RemoveDomainLink*	-	-	-
RemoveFolder	도메인 관리	도메인 폴더 관리	도메인 또는 제거되는 상위 폴더 및 폴더

infacmd isp 명령	권한 그룹	권한 이름	사용 권한 대상
RemoveGrid	도메인 관리	노드 및 그리드 관리	도메인 또는 상위 폴더 및 그리드
RemoveGroup	보안 관리	사용자, 그룹 및 역할 관리	-
RemoveGroupPrivilege	보안 관리	권한 및 역할 부여	도메인, Metadata Manager 서비스, 모델 리포지토리 서비스 또는 PowerCenter 리포지토리 서비스.
RemoveLicense	도메인 관리	서비스 관리	도메인 또는 상위 폴더 및 라이선스 개체
RemoveNode	도메인 관리	노드 및 그리드 관리	도메인 또는 상위 폴더 및 노드
RemoveNodeResource	도메인 관리	노드 및 그리드 관리	노드
RemoveOSProfile*	-	-	-
RemoveRole	보안 관리	사용자, 그룹 및 역할 관리	-
RemoveRolePrivilege	보안 관리	사용자, 그룹 및 역할 관리	-
RemoveService	도메인 관리	서비스 관리	도메인 또는 상위 폴더 및 응용 프로그램 서비스
RemoveServiceLevel*	-	-	-
RemoveUser	보안 관리	사용자, 그룹 및 역할 관리	-
RemoveUserFromGroup	보안 관리	사용자, 그룹 및 역할 관리	-
RemoveUserPrivilege	보안 관리	권한 및 역할 부여	도메인, Metadata Manager 서비스, 모델 리포지토리 서비스 또는 PowerCenter 리포지토리 서비스.
RenameConnection	-	-	연결에 대한 쓰기
ResetPassword(다른 사용자)	보안 관리	사용자, 그룹 및 역할 관리	-
ResetPassword(자신의 사용자 계정)	-	-	-
RunCPUProfile	도메인 관리	노드 및 그리드 관리	노드
SetConnectionPermission	-	-	연결에 대한 부여

infacmd isp 명령	권한 그룹	권한 이름	사용 권한 대상
SetLDAPConnectivity	보안 관리	사용자, 그룹 및 역할 관리	-
SetRepositoryLDAPConfiguration	-	-	도메인
ShowLicense	-	-	라이선스 개체
ShutdownNode	도메인 관리	노드 및 그리드 관리	노드
SwitchToGatewayNode*	-	-	-
SwitchToWorkerNode*	-	-	-
UnAssignISMMService	도메인 관리	서비스 관리	PowerCenter 통합 서비스 및 Metadata Manager 서비스
UnAssignRoleFromGroup	보안 관리	권한 및 역할 부여	도메인, Metadata Manager 서비스, 모델 리포지토리 서비스 또는 PowerCenter 리포지토리 서비스.
UnAssignRoleFromUser	보안 관리	권한 및 역할 부여	도메인, Metadata Manager 서비스, 모델 리포지토리 서비스 또는 PowerCenter 리포지토리 서비스.
UnassignLicense	도메인 관리	서비스 관리	라이선스 개체 및 응용 프로그램 서비스
UnassignRSWSHubService	도메인 관리	서비스 관리	PowerCenter 리포지토리 서비스 및 웹 서비스 협
UnassociateDomainNode	도메인 관리	노드 및 그리드 관리	노드
UpdateConnection	-	-	연결에 대한 쓰기
UpdateDomainOptions*	-	-	-
UpdateFolder	도메인 관리	도메인 폴더 관리	폴더
UpdateGatewayInfo*	-	-	-
UpdateGrid	도메인 관리	노드 및 그리드 관리	그리드 및 노드
UpdateIntegrationService	도메인 관리	서비스 관리	PowerCenter 통합 서비스
UpdateLicense	도메인 관리	서비스 관리	라이선스 개체
UpdateMMService	도메인 관리	서비스 관리	Metadata Manager 서비스

infacmd isp 명령	권한 그룹	권한 이름	사용 권한 대상
UpdateNodeOptions	도메인 관리	노드 및 그리드 관리	노드
UpdateNodeRole	도메인 관리	노드 및 그리드 관리	노드
UpdateOSProfile	보안 관리	사용자, 그룹 및 역할 관리	운영 체제 프로파일
UpdateRepositoryService	도메인 관리	서비스 관리	PowerCenter 리포지토리 서비스
UpdateSAPBWService	도메인 관리	서비스 관리	SAP BW 서비스
UpdateSMTPOptions*	-	-	-
UpdateServiceLevel*	-	-	-
UpdateServiceProcess	도메인 관리	서비스 관리	PowerCenter 통합 서비스 PowerCenter 통합 서비스에 추가된 각 노드
UpdateWSHubService	도메인 관리	서비스 관리	웹 서비스 헵
generateHadoopConnectionFromHiveConnection	-	-	-
listMonitoringOptions	모니터링	모니터링 구성	도메인
purgeMonitoringData	모니터링	모니터링 구성	도메인
updateMonitoringOptions	모니터링	모니터링 구성	도메인
*이러한 명령을 실행하려면 도메인에 대한 관리자 역할이 사용자에게 할당되어 있어야 합니다.			

infacmd mas 명령

infacmd mas 명령을 실행하려면 사용자에게 나열된 도메인 권한, 메타데이터 액세스 서비스 권한 및 도메인 개체 사용 권한 집합 중 하나가 있어야 합니다.

다음 테이블에는 *infacmd mas* 명령에 필요한 권한 및 사용 권한이 나열되어 있습니다.

infacmd dis 명령	권한 그룹	권한 이름	사용 권한
CreateService	도메인 관리	서비스 관리	메타데이터 액세스 서비스가 실행되는 도메인 또는 노드
ListServiceOptions	도메인 관리	서비스 관리	메타데이터 액세스 서비스
ListServiceProcessOptions	도메인 관리	서비스 관리	메타데이터 액세스 서비스
UpdateServiceOptions	도메인 관리	서비스 관리	메타데이터 액세스 서비스
UpdateServiceProcessOptions	도메인 관리	서비스 관리	메타데이터 액세스 서비스

infacmd mi 명령

사용자가 다음 *infacmd mi* 명령을 실행하려면 대량 수집 서비스에서 관리자 역할이 할당되어야 합니다.

- clearSamlConfig
- updateSamlConfig

infacmd mrs 명령

infacmd mrs 명령을 실행하려면 나열된 도메인 권한, 모델 리포지토리 서비스 권한 및 모델 리포지토리 개체 사용 권한 집합 중 하나가 있어야 합니다.

사용자가 소유한 개체에서 잠금 및 버전 관리 작업과 관련된 다음과 같은 명령을 실행할 수 있습니다. 다른 사용자가 소유한 개체에서 명령을 실행하려면 팀 기반 개발 관리 권한이 필요합니다.

- CheckInObject
- ListCheckedOutObjects
- ListLockedObjects
- UndoCheckout
- UnlockObject

다음 표에는 *infacmd mrs* 명령에 필요한 권한 및 사용 권한이 나열되어 있습니다.

infacmd mrs 명령	권한 그룹	권한 이름	사용 권한
BackupContents	도메인 관리	서비스 관리	모델 리포지토리 서비스가 실행되는 도메인 또는 노드
CheckInObject	도메인 관리	팀 기반 개발 관리	모델 리포지토리 서비스
CreateContents	도메인 관리	서비스 관리	모델 리포지토리 서비스가 실행되는 도메인 또는 노드
CreateFolder	도메인 관리	Developer tool: - Developer 액세스 Analyst 도구: - 분석 액세스 - 검색 작업 공간 액세스	모델 리포지토리 서비스
CreateProject	도메인 관리	프로젝트 작성, 편집 및 삭제	모델 리포지토리 서비스
CreateService	도메인 관리	서비스 관리	모델 리포지토리 서비스가 실행되는 도메인 또는 노드
DeleteContents	도메인 관리	서비스 관리	모델 리포지토리 서비스가 실행되는 도메인 또는 노드
DeleteFolder	도메인 관리	Developer tool: - Developer 액세스 Analyst 도구: - 분석 액세스 - 검색 작업 공간 액세스	모델 리포지토리 서비스
DeleteProject	도메인 관리	프로젝트 작성, 편집 및 삭제	모델 리포지토리 서비스
ListBackupFiles	도메인 관리	서비스 관리	모델 리포지토리 서비스가 실행되는 도메인 또는 노드
ListCheckedOutObjects	도메인 관리	팀 기반 개발 관리	모델 리포지토리 서비스
ListFolders	도메인 관리	서비스 관리	모델 리포지토리 서비스가 실행되는 도메인 또는 노드
ListLockedObjects	도메인 관리	팀 기반 개발 관리	모델 리포지토리 서비스
ListProjects	도메인 관리	Developer tool: - Developer 액세스 Analyst 도구: - 분석 액세스 - 검색 작업 공간 액세스	모델 리포지토리 서비스가 실행되는 도메인 또는 노드

infacmd mrs 명령	권한 그룹	권한 이름	사용 권한
ListServiceOptions	-	-	모델 리포지토리 서비스
ListServiceProcessOptions	-	-	모델 리포지토리 서비스
PopulateVCS	도메인 관리	팀 기반 개발 관리	모델 리포지토리 서비스
ReassignCheckedOutObject	도메인 관리	팀 기반 개발 관리	모델 리포지토리 서비스
RebuildDependencyGraph	-	-	모델 리포지토리 서비스
RenameFolder	도메인 관리	Developer tool: - Developer 액세스 Analyst 도구: - 분석 액세스 - 검색 작업 공간 액세스	모델 리포지토리 서비스
RestoreContents	도메인 관리	서비스 관리	모델 리포지토리 서비스가 실행되는 도메인 또는 노드
UndoCheckout	도메인 관리	팀 기반 개발 관리	모델 리포지토리 서비스
UnlockObject	도메인 관리	팀 기반 개발 관리	모델 리포지토리 서비스
UpdateServiceOptions	도메인 관리	서비스 관리	모델 리포지토리 서비스
UpdateServiceProcessOptions	도메인 관리	서비스 관리	모델 리포지토리 서비스
UpgradeContents	모델 리포지토리 서비스 관리	서비스 관리	모델 리포지토리 서비스

infacmd ms 명령

infacmd ms 명령을 실행하려면 나열된 도메인 개체 사용 권한 집합 중 하나가 있어야 합니다.

다음 표에는 *infacmd ms* 명령에 필요한 권한 및 사용 권한이 나열되어 있습니다.

infacmd ms 명령	권한 그룹	권한 이름	사용 권한
deleteMappingPersistedOutputs	-	-	응용 프로그램에서 실행
getRequestLog	-	-	-
listMappingParams	-	-	-

infacmd ms 명령	권한 그룹	권한 이름	사용 권한
listMappingPersistedOutputs	-	-	응용 프로그램에서 보기
listMappings	-	-	-
runMapping	-	-	매핑에서 사용하는 연결 개체에 대한 실행

infacmd tools 명령

infacmd tools 명령을 실행하려면 사용자에게 나열된 모델 리포지토리 개체 사용 권한 중 하나가 있어야 합니다.

다음 테이블에는 *infacmd tools* 명령에 필요한 사용 권한이 나열되어 있습니다.

infacmd tools 명령	권한 그룹	권한 이름	사용 권한
ExportObjects	-	-	프로젝트에 대한 읽기
ImportObjects	-	-	프로젝트에 대한 쓰기

infacmd ps 명령

infacmd ps 명령을 실행하려면 나열된 프로파일링 권한 및 도메인 개체 사용 권한 집합 중 하나가 있어야 합니다.

다음 표에는 *infacmd ps* 명령에 필요한 권한 및 사용 권한이 나열되어 있습니다.

infacmd ps 명령	권한 그룹	권한 이름	사용 권한
CreateWH	-	-	-
DropWH	-	-	-
실행	-	-	프로젝트에 대한 읽기 소스 연결 개체에 대한 실행
목록	-	-	프로젝트에 대한 읽기
제거	-	-	프로젝트에 대한 읽기 및 쓰기

infacmd pwx 명령

infacmd pwx 명령을 실행하려면 나열된 PowerExchange 응용 프로그램 서비스 사용 권한 및 권한 집합 중 하나가 있어야 합니다.

다음 표에는 *infacmd pwx* 명령에 필요한 권한 및 사용 권한이 나열되어 있습니다.

infacmd pwx 명령	권한 그룹	권한 이름	사용 권한
CloseForceListener	관리 명령	closeforce	-
CloseListener	관리 명령	close	-
CondenseLogger	관리 명령	condense	-
CreateListenerService	도메인 관리	서비스 관리	PowerExchange 응용 프로그램 서비스가 실행되는 도메인 또는 노드
CreateLoggerService	도메인 관리	서비스 관리	PowerExchange 응용 프로그램 서비스가 실행되는 도메인 또는 노드
DisplayAllLogger	정보 명령	displayall	-
DisplayCPULogger	정보 명령	displaycpu	-
DisplayEventsLogger	정보 명령	displayevents	-
DisplayMemoryLogger	정보 명령	displaymemory	-
DisplayRecordsLogger	정보 명령	displayrecords	-
DisplayStatusLogger	정보 명령	displaystatus	-
FileSwitchLogger	관리 명령	fileswitch	-
ListTaskListener	정보 명령	listtask	-
ShutDownLogger	관리 명령	shutdown	-
StopTaskListener	관리 명령	stoptask	-
UpdateListenerService	도메인 관리	서비스 관리	PowerExchange 응용 프로그램 서비스가 실행되는 도메인 또는 노드
UpdateLoggerService	도메인 관리	서비스 관리	PowerExchange 응용 프로그램 서비스가 실행되는 도메인 또는 노드

infacmd rms 명령

infacmd rms 명령을 실행하려면 나열된 도메인 권한 및 사용 권한 집합 중 하나가 있어야 합니다.

다음 테이블에는 *infacmd rms* 명령에 필요한 권한 및 사용 권한이 나열되어 있습니다.

infacmd rms 명령	권한 그룹	권한 이름	사용 권한 대상
ListComputeNodeAttributes	도메인 관리	-	리소스 관리자 서비스
ListServiceOptions	도메인 관리	-	리소스 관리자 서비스
SetComputeNodeAttributes	도메인 관리	서비스 관리	리소스 관리자 서비스
UpdateServiceOptions	도메인 관리	서비스 관리	리소스 관리자 서비스

infacmd rtm 명령

infacmd rtm 명령을 실행하려면 나열된 모델 리포지토리 서비스 권한 및 도메인 개체 사용 권한 집합 중 하나가 있어야 합니다.

다음 표에는 *infacmd rtm* 명령에 필요한 권한 및 사용 권한이 나열되어 있습니다.

infacmd rtm 명령	권한 그룹	권한 이름	사용 권한
Deployimport	-	-	-
내보내기	-	-	내보낼 참조 테이블을 포함하는 프로젝트에 대한 읽기
가져오기	-	-	참조 테이블을 가져올 프로젝트에 대한 읽기 및 쓰기

infacmd sch 명령

infacmd sch 명령을 실행하려면 나열된 권한 및 사용 권한 집합 중 하나가 있어야 합니다.

다음 테이블에는 **infacmd sch** 명령에 필요한 권한 및 사용 권한이 나열되어 있습니다.

infacmd sch 명령	권한 그룹	권한 이름	사용 권한 대상
CreateSchedule	스케줄러 권한	일정 작성	스케줄러 서비스
DeleteSchedule	스케줄러 권한	일정 삭제	스케줄러 서비스
ListSchedule	스케줄러 권한	일정 보기	스케줄러 서비스
ListServiceOptions	도메인 권한	서비스 관리	스케줄러 서비스
ListServiceProcessOptions	도메인 권한	서비스 관리	스케줄러 서비스
PauseAll	스케줄러 권한	일정 편집	스케줄러 서비스
PauseSchedule	스케줄러 권한	일정 편집	스케줄러 서비스
ResumeAll	스케줄러 권한	일정 편집	스케줄러 서비스
ResumeSchedule	스케줄러 권한	일정 편집	스케줄러 서비스
UpdateSchedule	스케줄러 권한	일정 편집	스케줄러 서비스
UpdateService	도메인 권한	서비스 관리	스케줄러 서비스
UpdateServiceProcess	도메인 권한	서비스 관리	스케줄러 서비스
업그레이드	도메인 권한	서비스 관리	스케줄러 서비스

infacmd sql 명령

infacmd sql 명령을 실행하려면 나열된 도메인 권한, 데이터 통합 서비스 권한 및 도메인 개체 사용 권한 집합 중 하나가 있어야 합니다.

다음 표에는 **infacmd sql** 명령에 필요한 권한 및 사용 권한이 나열되어 있습니다.

infacmd sql 명령	권한 그룹	권한 이름	사용 권한
ExecuteSQL	-	-	SQL 문에서 액세스할 개체에 따라 다름
ListColumnPermissions	-	-	-
ListSQLDataServiceOptions	-	-	-
ListSQLDataServicePermissions	-	-	-
ListSQLDataServices	-	-	-
ListStoredProcedurePermissions	-	-	-

infacmd sql 명령	권한 그룹	권한 이름	사용 권한
ListTableOptions	-	-	-
ListTablePermissions	-	-	-
PurgeTableCache	-	-	-
RefreshTableCache	-	-	-
RenameSQLDataService	응용 프로그램 관리	응용 프로그램 관리	-
SetColumnPermissions	-	-	개체에 대한 부여
SetSQLDataServicePermissions	-	-	개체에 대한 부여
SetStoredProcedurePermissions	-	-	개체에 대한 부여
SetTablePermissions	-	-	개체에 대한 부여
StartSQLDataService	응용 프로그램 관리	응용 프로그램 관리	-
StopSQLDataService	응용 프로그램 관리	응용 프로그램 관리	-
UpdateColumnOptions	응용 프로그램 관리	응용 프로그램 관리	-
UpdateSQLDataServiceOptions	응용 프로그램 관리	응용 프로그램 관리	-
UpdateTableOptions	응용 프로그램 관리	응용 프로그램 관리	-

infacmd wfs 명령

infacmd wfs 명령은 권한 또는 사용 권한 없이 실행할 수 있습니다.

pmcmd 명령

pmcmd 명령을 실행하려면 나열된 **PowerCenter** 리포지토리 서비스 권한 및 **PowerCenter** 리포지토리 개체 사용 권한 집합 중 하나가 있어야 합니다.

PowerCenter 통합 서비스를 안전 모드에서 실행하는 경우 다음 명령을 실행하려면 연결된 **PowerCenter** 리포지토리 서비스에 대한 관리자 역할이 있어야 합니다.

- aborttask
- abortworkflow
- getrunningssessionsdetails
- getservicedetails
- getsessionstatistics

- gettaskdetails
- getworkflowdetails
- recoverworkflow
- scheduleworkflow
- starttask
- startworkflow
- stoptask
- stopworkflow
- unscheduleworkflow

다음 표에는 *pmcmd* 명령에 필요한 권한 및 사용 권한이 나열되어 있습니다.

pmcmd 명령	권한 그룹	권한 이름	사용 권한
aborttask(자신의 사용자 계정에서 시작된 태스크)	-	-	폴더에 대한 읽기 및 실행
aborttask(다른 사용자가 시작한 태스크)	런타임 개체	실행 관리	폴더에 대한 읽기 및 실행
abortworkflow(자신의 사용자 계정에서 시작된 워크플로우)	-	-	폴더에 대한 읽기 및 실행
abortworkflow(다른 사용자가 시작한 워크플로우)	런타임 개체	실행 관리	폴더에 대한 읽기 및 실행
connect	-	-	-
disconnect	-	-	-
종료	-	-	-
getrunningessionsdetails	런타임 개체	모니터링	-
getservicedetails	런타임 개체	모니터링	폴더에 대한 읽기
getserviceproperties	-	-	-
getsessionstatistics	런타임 개체	모니터링	폴더에 대한 읽기
gettaskdetails	런타임 개체	모니터링	폴더에 대한 읽기
getworkflowdetails	런타임 개체	모니터링	폴더에 대한 읽기
도움말	-	-	-
pingservice	-	-	-

pmcmd 명령	권한 그룹	권한 이름	사용 권한
recoverworkflow(자신의 사용자 계정에서 시작된 워크플로우)	런타임 개체	실행	폴더에 대한 읽기 및 실행 연결 개체에서 읽기 및 실행 운영 체제 프로필에 대한 사용 권한(해당하는 경우)
recoverworkflow(다른 사용자가 시작한 워크플로우)	런타임 개체	실행 관리	폴더에 대한 읽기 및 실행 연결 개체에서 읽기 및 실행 운영 체제 프로필에 대한 사용 권한(해당하는 경우)
scheduleworkflow	런타임 개체	실행 관리	폴더에 대한 읽기 및 실행 연결 개체에서 읽기 및 실행 운영 체제 프로필에 대한 사용 권한(해당하는 경우)
setfolder	-	-	폴더에 대한 읽기
setnowait	-	-	-
setwait	-	-	-
showsettings	-	-	-
starttask	런타임 개체	실행	폴더에 대한 읽기 및 실행 연결 개체에서 읽기 및 실행 운영 체제 프로필에 대한 사용 권한(해당하는 경우)
startworkflow	런타임 개체	실행	폴더에 대한 읽기 및 실행 연결 개체에서 읽기 및 실행 운영 체제 프로필에 대한 사용 권한(해당하는 경우)
stoptask(자신의 사용자 계정에서 시작된 태스크)	-	-	폴더에 대한 읽기 및 실행
stoptask(다른 사용자가 시작한 태스크)	런타임 개체	실행 관리	폴더에 대한 읽기 및 실행
stopworkflow(자신의 사용자 계정에서 시작된 워크플로우)	-	-	폴더에 대한 읽기 및 실행
stopworkflow(다른 사용자가 시작한 워크플로우)	런타임 개체	실행 관리	폴더에 대한 읽기 및 실행
unscheduleworkflow	런타임 개체	실행 관리	폴더에 대한 읽기 및 실행
unsetfolder	-	-	폴더에 대한 읽기
버전	-	-	-

pmcmd 명령	권한 그룹	권한 이름	사용 권한
waittask	런타임 개체	모니터링	폴더에 대한 읽기
waitworkflow	런타임 개체	모니터링	폴더에 대한 읽기

pmrep 명령

다음 명령을 제외한 모든 *pmrep* 명령을 실행하려면 Repository Manager 액세스 권한이 있어야 합니다.

- Run
- Create
- Restore
- Upgrade
- Version
- Help

pmrep 명령을 실행하려면 나열된 도메인 권한, PowerCenter 리포지토리 서비스 권한, 도메인 개체 사용 권한 및 PowerCenter 리포지토리 개체 사용 권한 집합 중 하나가 있어야 합니다.

다음 명령을 실행하려면 개체 소유자이거나 PowerCenter 리포지토리 서비스에 대한 관리자 역할이 있어야 합니다.

- AssignPermission
- ChangeOwner
- CreateQuery
- DeleteConnection
- DeleteDeploymentGroup
- DeleteFolder
- DeleteLabel
- DeleteQuery
- ModifyFolder(소유자 변경, 사용 권한 구성, 공유 폴더 지정 또는 폴더 이름/설명 편집을 위한 폴더 수정)

다음 표에는 *pmrep* 명령에 필요한 권한 및 사용 권한이 나열되어 있습니다.

pmrep 명령	권한 그룹	권한 이름	사용 권한
AddToDeploymentGroup	글로벌 개체	배포 그룹 관리	원래 폴더에 대한 읽기 배포 그룹에 대한 읽기 및 쓰기
ApplyLabel	-	-	폴더에 대한 읽기 레이블에 대한 읽기 및 실행
AssignPermission	-	-	-

pmrep 명령	권한 그룹	권한 이름	사용 권한
BackUp	도메인 관리	서비스 관리	PowerCenter 리포지토리 서비스에 대한 사용 권한
ChangeOwner	-	-	-
CheckIn(자신의 체크아웃에 대한 체크인)	디자인 개체	작성, 편집 및 삭제	폴더에 대한 읽기 및 쓰기
CheckIn(자신의 체크아웃에 대한 체크인)	소스 및 대상	작성, 편집 및 삭제	폴더에 대한 읽기 및 쓰기
CheckIn(자신의 체크아웃에 대한 체크인)	런타임 개체	작성, 편집 및 삭제	폴더에 대한 읽기 및 쓰기
CheckIn(다른 사용자의 체크아웃에 대한 체크인)	디자인 개체	버전 관리	폴더에 대한 읽기 및 쓰기
CheckIn(다른 사용자의 체크아웃에 대한 체크인)	소스 및 대상	버전 관리	폴더에 대한 읽기 및 쓰기
CheckIn(다른 사용자의 체크아웃에 대한 체크인)	런타임 개체	버전 관리	폴더에 대한 읽기 및 쓰기
CleanUp	-	-	-
ClearDeploymentGroup	글로벌 개체	배포 그룹 관리	배포 그룹에 대한 읽기 및 쓰기
연결	-	-	-
생성	도메인 관리	서비스 관리	PowerCenter 리포지토리 서비스에 대한 사용 권한
CreateConnection	글로벌 개체	연결 작성	-
CreateDeploymentGroup	글로벌 개체	배포 그룹 관리	-
CreateFolder	폴더	생성	-
CreateLabel	글로벌 개체	레이블 생성	-
CreateQuery	글로벌 개체	쿼리 생성	-
삭제	도메인 관리	서비스 관리	PowerCenter 리포지토리 서비스에 대한 사용 권한
DeleteConnection	-	-	-
DeleteDeploymentGroup	-	-	-
DeleteFolder	-	-	-
DeleteLabel	-	-	-
DeleteObject	디자인 개체	작성, 편집 및 삭제	폴더에 대한 읽기 및 쓰기

pmrep 명령	권한 그룹	권한 이름	사용 권한
DeleteObject	소스 및 대상	작성, 편집 및 삭제	폴더에 대한 읽기 및 쓰기
DeleteObject	런타임 개체	작성, 편집 및 삭제	폴더에 대한 읽기 및 쓰기
DeleteQuery	-	-	-
DeployDeploymentGroup	글로벌 개체	배포 그룹 관리	원래 폴더에 대한 읽기 대상 폴더에 대한 읽기 및 쓰기 배포 그룹에 대한 읽기 및 실행
DeployFolder	폴더	원래 리포지토리에 대한 복사 대상 리포지토리에 대한 생성	폴더에 대한 읽기
ExecuteQuery	-	-	쿼리에 대한 읽기 및 실행
종료	-	-	-
FindCheckout	-	-	폴더에 대한 읽기
GetConnectionDetails	-	-	연결 개체에 대한 읽기
도움말	-	-	-
KillUserConnection	도메인 관리	서비스 관리	PowerCenter 리포지토리 서비스에 대한 사용 권한
ListConnections	-	-	연결 개체에 대한 읽기
ListObjectDependencies	-	-	폴더에 대한 읽기
ListObjects	-	-	폴더에 대한 읽기
ListTablesBySess	-	-	폴더에 대한 읽기
ListUserConnections	도메인 관리	서비스 관리	PowerCenter 리포지토리 서비스에 대한 사용 권한
ModifyFolder(소유자 변경, 사용 권한 구성, 공유 폴더 지정 또는 폴더 이름/설명 편집을 위한 폴더 수정)	-	-	-
ModifyFolder(상태 변경을 위한 폴더 수정)	폴더	버전 관리	폴더에 대한 읽기 및 쓰기
알림	도메인 관리	서비스 관리	PowerCenter 리포지토리 서비스에 대한 사용 권한
ObjectExport	-	-	폴더에 대한 읽기
ObjectImport	디자인 개체	작성, 편집 및 삭제	폴더에 대한 읽기 및 쓰기

pmrep 명령	권한 그룹	권한 이름	사용 권한
ObjectImport	소스 및 대상	작성, 편집 및 삭제	폴더에 대한 읽기 및 쓰기
ObjectImport	런타임 개체	작성, 편집 및 삭제	폴더에 대한 읽기 및 쓰기
PurgeVersion	디자인 개체	버전 관리	폴더에 대한 읽기 및 쓰기 쿼리 이름을 지정한 경우 쿼리에 대한 읽기, 쓰기 및 실행
PurgeVersion	소스 및 대상	버전 관리	폴더에 대한 읽기 및 쓰기 쿼리 이름을 지정한 경우 쿼리에 대한 읽기, 쓰기 및 실행
PurgeVersion	런타임 개체	버전 관리	폴더에 대한 읽기 및 쓰기 쿼리 이름을 지정한 경우 쿼리에 대한 읽기, 쓰기 및 실행
PurgeVersion(폴더 수준의 개체 제거를 위한 버전 제 거)	폴더	버전 관리	폴더에 대한 읽기 및 쓰기
PurgeVersion(리포지토리 수준의 개체 제거를 위한 버 전 제거)	도메인 관리	서비스 관리	PowerCenter 리포지토리 서비스 에 대한 사용 권한
등록	도메인 관리	서비스 관리	PowerCenter 리포지토리 서비스 에 대한 사용 권한
RegisterPlugin	도메인 관리	서비스 관리	PowerCenter 리포지토리 서비스 에 대한 사용 권한
복원	도메인 관리	서비스 관리	PowerCenter 리포지토리 서비스 에 대한 사용 권한
RollbackDeployment	글로벌 개체	배포 그룹 관리	대상 폴더에 대한 읽기 및 쓰기
실행	-	-	-
ShowConnectionInfo	-	-	-
SwitchConnection	런타임 개체	작성, 편집 및 삭제	폴더에 대한 읽기 및 쓰기 연결 개체에 대한 읽기
TruncateLog	런타임 개체	실행 관리	폴더에 대한 읽기 및 실행
UndoCheckout(자신의 체 크아웃에 대한 체크아웃 실 행 취소)	디자인 개체	작성, 편집 및 삭제	폴더에 대한 읽기 및 쓰기
UndoCheckout(자신의 체 크아웃에 대한 체크아웃 실 행 취소)	소스 및 대상	작성, 편집 및 삭제	폴더에 대한 읽기 및 쓰기

pmrep 명령	권한 그룹	권한 이름	사용 권한
UndoCheckout(자신의 체크아웃에 대한 체크아웃 실행 취소)	런타임 개체	작성, 편집 및 삭제	폴더에 대한 읽기 및 쓰기
UndoCheckout(다른 사용자의 체크아웃에 대한 체크아웃 실행 취소)	디자인 개체	버전 관리	폴더에 대한 읽기 및 쓰기
UndoCheckout(다른 사용자의 체크아웃에 대한 체크아웃 실행 취소)	소스 및 대상	버전 관리	폴더에 대한 읽기 및 쓰기
UndoCheckout(다른 사용자의 체크아웃에 대한 체크아웃 실행 취소)	런타임 개체	버전 관리	폴더에 대한 읽기 및 쓰기
등록 해제	도메인 관리	서비스 관리	PowerCenter 리포지토리 서비스에 대한 사용 권한
UnregisterPlugin	도메인 관리	서비스 관리	PowerCenter 리포지토리 서비스에 대한 사용 권한
UpdateConnection	-	-	연결 개체에 대한 읽기 및 쓰기
UpdateEmailAddr	런타임 개체	작성, 편집 및 삭제	폴더에 대한 읽기 및 쓰기
UpdateSeqGenVals	디자인 개체	작성, 편집 및 삭제	폴더에 대한 읽기 및 쓰기
UpdateSrcPrefix	런타임 개체	작성, 편집 및 삭제	폴더에 대한 읽기 및 쓰기
UpdateStatistics	도메인 관리	서비스 관리	PowerCenter 리포지토리 서비스에 대한 사용 권한
UpdateTargPrefix	런타임 개체	작성, 편집 및 삭제	폴더에 대한 읽기 및 쓰기
업그레이드	도메인 관리	서비스 관리	PowerCenter 리포지토리 서비스에 대한 사용 권한
유효성 검사	디자인 개체	작성, 편집 및 삭제	폴더에 대한 읽기 및 쓰기
유효성 검사	런타임 개체	작성, 편집 및 삭제	폴더에 대한 읽기 및 쓰기
버전	-	-	-

부록 B

사용자 지정 역할

이 부록에 포함된 항목:

- [분석 서비스 사용자 지정 역할, 224](#)
- [Metadata Manager 서비스 사용자 지정 역할, 225](#)
- [운영자 사용자 지정 역할, 226](#)
- [PowerCenter 리포지토리 서비스 사용자 지정 역할, 227](#)
- [Test Data Manager 사용자 지정 역할, 228](#)

분석 서비스 사용자 지정 역할

분석 서비스 Business Glossary 소비자는 분석 서비스의 사용자 지정 역할입니다.

다음 표에는 분석 서비스 Business Glossary 소비자 사용자 지정 역할에 할당된 기본 권한이 나열되어 있습니다.

권한 그룹	권한 이름
작업 공간 액세스	용어집 작업 공간

Metadata Manager 서비스 사용자 지정 역할

Metadata Manager 서비스 사용자 지정 역할에는 Metadata Manager 고급 사용자, Metadata Manager 기본 사용자 및 Metadata Manager 중간 사용자 역할이 포함됩니다.

Metadata Manager 고급 사용자

다음 표에는 Metadata Manager 고급 사용자 사용자 지정 역할에 할당된 기본 권한이 나열되어 있습니다.

권한 그룹	권한 이름
카탈로그	<ul style="list-style-type: none">- 바로 가기 공유- 연계 보기- 관련 카탈로그 보기- 보고서 보기- 프로필 결과 보기- 카탈로그 보기- 관계 보기- 관계 관리- 설명 보기- 설명 게시- 설명 삭제- 링크 보기- 링크 관리- 용어집 보기- 개체 관리
로드	<ul style="list-style-type: none">- 리소스 보기- 리소스 로드- 일정 관리- 메타데이터 제거- 리소스 관리
모델	<ul style="list-style-type: none">- 모델 보기- 모델 관리- 모델 가져오기/내보내기
보안	카탈로그 사용 권한 관리

Metadata Manager 기본 사용자

다음 테이블에는 Metadata Manager 기본 사용자 사용자 지정 역할에 할당된 기본 권한이 나열되어 있습니다.

권한 그룹	권한 이름
카탈로그	<ul style="list-style-type: none">- 연계 보기- 관련 카탈로그 보기- 카탈로그 보기- 관계 보기- 설명 보기- 링크 보기
모델	모델 보기

Metadata Manager 중간 사용자

다음 테이블에는 Metadata Manager 중간 사용자 사용자 지정 역할에 할당된 기본 권한이 나열되어 있습니다.

권한 그룹	권한 이름
카탈로그	<ul style="list-style-type: none"> - 연계 보기 - 관련 카탈로그 보기 - 보고서 보기 - 프로필 결과 보기 - 카탈로그 보기 - 관계 보기 - 설명 보기 - 설명 게시 - 설명 삭제 - 링크 보기 - 링크 관리 - 용어집 보기
로드	<ul style="list-style-type: none"> - 리소스 보기 - 리소스 로드
모델	모델 보기

운영자 사용자 지정 역할

운영자 사용자 지정 역할에는 응용 프로그램 서비스 관리, 예약 및 모니터링을 위한 권한이 포함됩니다.

다음 테이블에는 운영자 사용자 지정 역할에 할당된 기본 권한이 나열되어 있습니다.

권한 그룹	권한 이름
응용 프로그램 관리	응용 프로그램 관리
도메인 관리	서비스 실행 관리
모델 리포지토리 서비스 관리	팀 기반 개발 관리
모니터링	<p>모니터링 권한 그룹에는 다음과 같은 권한이 포함됩니다.</p> <ul style="list-style-type: none"> - 보기: 다른 사용자의 작업 보기 - 보기: 통계 보기 - 보기: 보고서 보기 - 모니터링 액세스: Analyst 도구에서 액세스 - 모니터링 액세스: Developer tool에서 액세스 - 모니터링 액세스: Administrator 도구에서 액세스 - 작업에 대해 동작 수행 <p>참고: Kerberos 인증을 사용하는 도메인에서 사용자는 모니터링을 위해 구성된 모델 리포지토리 서비스에 대한 관리자 역할도 있어야 합니다.</p>

권한 그룹	권한 이름
스케줄러	스케줄러 권한 그룹에는 다음과 같은 권한이 포함됩니다. <ul style="list-style-type: none"> - 예약된 작업 관리: 일정 작성 - 예약된 작업 관리: 일정 삭제 - 예약된 작업 관리: 일정 편집 - 예약된 작업 관리: 일정 보기
도구	Informatica Administrator 액세스

PowerCenter 리포지토리 서비스 사용자 지정 역할

PowerCenter 리포지토리 서비스 사용자 지정 역할에는 PowerCenter 연결 관리자, PowerCenter 개발자, PowerCenter 운영자 및 PowerCenter 리포지토리 폴더 관리자가 포함됩니다.

PowerCenter 연결 관리자

다음 표에는 PowerCenter 연결 관리자 사용자 지정 역할에 할당된 기본 권한이 나열되어 있습니다.

권한 그룹	권한 이름
도구	워크플로우 관리자 액세스
글로벌 개체	연결 작성

PowerCenter 개발자

다음 테이블에는 PowerCenter 개발자 사용자 지정 역할에 할당된 기본 권한이 나열되어 있습니다.

권한 그룹	권한 이름
도구	<ul style="list-style-type: none"> - 디자이너 액세스 - 워크플로우 관리자 액세스 - Workflow Monitor 액세스
디자인 개체	<ul style="list-style-type: none"> - 작성, 편집 및 삭제 - 버전 관리
소스 및 대상	<ul style="list-style-type: none"> - 작성, 편집 및 삭제 - 버전 관리
런타임 개체	<ul style="list-style-type: none"> - 작성, 편집 및 삭제 - 실행 - 버전 관리 - 모니터링

PowerCenter 운영자

다음 테이블에는 PowerCenter 운영자 사용자 지정 역할에 할당된 기본 권한이 나열되어 있습니다.

권한 그룹	권한 이름
도구	Workflow Monitor 액세스
런타임 개체	<ul style="list-style-type: none">- 실행- 실행 관리- 모니터링

PowerCenter 리포지토리 폴더 관리자

다음 표에는 PowerCenter 리포지토리 폴더 관리자 사용자 지정 역할에 할당된 기본 권한이 나열되어 있습니다.

권한 그룹	권한 이름
도구	Repository Manager 액세스
폴더	<ul style="list-style-type: none">- 복사- 작성- 버전 관리
글로벌 개체	<ul style="list-style-type: none">- 배포 그룹 관리- 배포 그룹 실행- 레이블 작성- 쿼리 작성

Test Data Manager 사용자 지정 역할

Test Data Manager 사용자 지정 역할에는 테스트 데이터 관리자, 테스트 데이터 개발자, 테스트 데이터 프로젝트 DBA, 테스트 데이터 프로젝트 개발자, 테스트 데이터 프로젝트 소유자, 테스트 데이터 위험 관리자, 테스트 데이터 전문가 및 테스트 엔지니어가 포함됩니다.

테스트 데이터 관리자

다음 테이블에는 테스트 데이터 관리자 사용자 지정 역할에 할당된 기본 권한이 나열되어 있습니다.

권한 그룹	권한 이름
프로젝트	프로젝트 감사
관리	<ul style="list-style-type: none">- 연결 보기- 연결 관리- 기본 설정 관리

테스트 데이터 개발자

다음 테이블에는 테스트 데이터 개발자 사용자 지정 역할에 할당된 기본 권한이 나열되어 있습니다.

권한 그룹	권한 이름
정책	<ul style="list-style-type: none">- 정책 보기- 정책 관리
데이터 도메인	<ul style="list-style-type: none">- 데이터 도메인 보기- 데이터 도메인 관리
프로젝트	프로젝트 감사

테스트 데이터 프로젝트 DBA

다음 테이블에는 테스트 데이터 프로젝트 DBA 사용자 지정 역할에 할당된 기본 권한이 나열되어 있습니다.

권한 그룹	권한 이름
프로젝트	<ul style="list-style-type: none">- 프로젝트 보기- 프로젝트 실행- 프로젝트 모니터링- 프로젝트 감사
관리	<ul style="list-style-type: none">- 연결 보기- 연결 관리

테스트 데이터 프로젝트 개발자

다음 테이블에는 테스트 데이터 프로젝트 개발자 사용자 지정 역할에 할당된 기본 권한이 나열되어 있습니다.

권한 그룹	권한 이름
정책	정책 보기
데이터 도메인	데이터 도메인 보기
프로젝트	<ul style="list-style-type: none">- 프로젝트 보기- 프로젝트 검색- 프로젝트 실행- 프로젝트 모니터링- 프로젝트 감사- 메타데이터 가져오기
데이터 마스킹	<ul style="list-style-type: none">- 데이터 마스킹 보기- 데이터 마스킹 관리
데이터 하위 집합	<ul style="list-style-type: none">- 데이터 하위 집합 보기- 데이터 하위 집합 관리
관리	<ul style="list-style-type: none">- 연결 보기- 연결 관리

테스트 데이터 프로젝트 소유자

다음 테이블에는 테스트 데이터 프로젝트 소유자 사용자 지정 역할에 할당된 기본 권한이 나열되어 있습니다.

권한 그룹	권한 이름
정책	정책 보기
데이터 도메인	데이터 도메인 보기
프로젝트	<ul style="list-style-type: none">- 프로젝트 보기- 프로젝트 관리- 프로젝트 검색- 프로젝트 실행- 프로젝트 모니터링- 프로젝트 감사- 메타데이터 가져오기
데이터 마스킹	<ul style="list-style-type: none">- 데이터 마스킹 보기- 데이터 마스킹 관리
데이터 하위 집합	<ul style="list-style-type: none">- 데이터 하위 집합 보기- 데이터 하위 집합 관리
관리	<ul style="list-style-type: none">- 연결 보기- 연결 관리

테스트 데이터 위험 관리자

다음 테이블에는 테스트 데이터 위험 관리자 사용자 지정 역할에 할당된 기본 권한이 나열되어 있습니다.

권한 그룹	권한 이름
정책	정책 보기
데이터 도메인	데이터 도메인 보기
프로젝트	프로젝트 감사

테스트 데이터 전문가

다음 테이블에는 테스트 데이터 전문가 사용자 지정 역할에 할당된 기본 권한이 나열되어 있습니다.

권한 그룹	권한 이름
정책	정책 보기
데이터 도메인	<ul style="list-style-type: none">- 데이터 도메인 보기- 데이터 도메인 관리

권한 그룹	권한 이름
프로젝트	<ul style="list-style-type: none"> - 프로젝트 보기 - 프로젝트 관리 - 프로젝트 검색 - 프로젝트 실행 - 프로젝트 모니터링 - 프로젝트 감사 - 메타데이터 가져오기
데이터 마스킹	<ul style="list-style-type: none"> - 데이터 마스킹 보기 - 데이터 마스킹 관리
데이터 하위 집합	<ul style="list-style-type: none"> - 데이터 하위 집합 보기 - 데이터 하위 집합 관리
관리	<ul style="list-style-type: none"> - 연결 보기 - 연결 관리

테스트 엔지니어

다음 테이블에는 테스트 엔지니어 사용자 지정 역할에 할당된 기본 권한이 나열되어 있습니다.

권한 그룹	권한 이름
프로젝트	<ul style="list-style-type: none"> - 프로젝트 보기 - 프로젝트 모니터링

인덱스

A

as

명령별 권한 [196](#)
명령별 사용 권한 [196](#)

B

폴더

권한 [148](#)
사용 권한 [174](#)

폴더 권한 그룹

설명 [148](#)

필터

getUserActivityLog [118](#)

환경 변수

INFA_TRUSTSTORE [79](#)

INFA_TRUSTSTORE_PASSWORD [79](#)

C

cacerts 트러스트 저장소 파일 [28](#)

Cloud 관리 권한 그룹

도메인 [139](#)

cluster

명령별 권한 [197](#)
명령별 사용 권한 [197](#)

convertUserActivityLog

사용자 활동 로그 [117](#)

D

dis

명령별 권한 [198](#)
명령별 사용 권한 [198](#)

E

es

명령별 권한 [199](#)
명령별 사용 권한 [199](#)

G

getUserActivityLog

사용자 활동 로그 [117](#)

필터 [118](#)

I

ID 공급자

single sign-on에 대한 구성 [64](#)

Informatica Administrator

개요 [100](#)

검색 [103](#)

보안 페이지 [103](#)

탐색기 [103](#)

탭, 보기 [100](#)

Informatica Analyst

관리자 [111](#)

Informatica Developer

관리자 [111](#)

Informatica 도메인

권한 [108](#)

사용 권한 [108](#)

사용자 보안 [108](#)

사용자, 관리 [113](#)

ipc

명령별 권한 [200](#)

명령별 사용 권한 [200](#)

isp

명령별 권한 [200](#)

명령별 사용 권한 [200](#)

K

Kerberos 인증

서비스 사용자 이름 [39](#)

keytab [39](#)

LDAP 동기화 [54](#)

SPN keytab 형식 파일 [42](#)

개요 [30, 31](#)

교차 영역 인증 [33](#)

노드 수준 [34](#)

서비스 사용자 계정 [38](#)

설명 [20](#)

프로세스 수준 [34](#)

keytool 유틸리티 [28](#)

L

LDAP 구성

삭제 [29](#)

LDAP 그룹

가져오기 [24](#)

관리 [120](#)

LDAP 디렉터리 서비스

중첩 그룹 [28](#)

LDAP 보안 도메인

설명 [19, 20](#)

LDAP 사용자
가져오기 [24](#)
관리 [113](#)
그룹에 할당 [114](#)
활성화 [114](#)
LDAP 인증
Azure Active Directory [23](#)
디렉터리 서비스 [24](#)
설명 [19](#), [101](#)
설정 [24](#)
자체 서명된 SSL 인증서 [28](#)
중첩 그룹 [28](#)
지원되는 디렉터리 서비스 [22](#)

M

mas
명령별 권한 [208](#)
명령별 사용 권한 [208](#)
Metadata Manager
관리자 [111](#)
Metadata Manager 서비스
권한 [142](#)
권한 부여 [102](#)
권한이 있는 사용자 [169](#)
사용자 동기화 [102](#)
사용자 지정 역할 [225](#)
Metadata Manager 서비스 권한
권한 그룹 찾아보기 [143](#)
로드 권한 그룹 [144](#)
모델 권한 그룹 [145](#)
보안 권한 그룹 [145](#)
mrs
명령별 권한 [209](#)
명령별 사용 권한 [209](#)
ms
명령별 권한 [211](#)
명령별 사용 권한 [211](#)

N

네트워크 보호
관리 [113](#)
그룹에 할당 [114](#)
동기화 [102](#)
노드
사용 권한 [174](#)
대상
권한 [152](#)
데이터 통합 서비스
권한 [141](#)
권한 부여 [102](#)
도구 권한 그룹
PowerCenter 리포지토리 서비스 [147](#)
도메인 [139](#)
도메인
관리 권한 [134](#)
관리자 [111](#)
관리자 역할 [166](#)
권한 [133](#)
권한이 있는 사용자 [169](#)
보안 관리 권한 [133](#)
사용자 동기화 [102](#)
사용자 보안 [108](#)

도메인 개체
사용 권한 [174](#)
도메인 관리 권한 그룹
설명 [134](#)
도메인 관리자
설명 [111](#)
도메인 사용 권한
상속 [173](#)
유효 [173](#)
직접 [173](#)
동기화
LDAP 사용자 [24](#)
네트워크 보호 [102](#)
디자인 개체
권한 [149](#)
설명 [149](#)
디자인 개체 권한 그룹
설명 [149](#)
라이선스
사용 권한 [174](#)
런타임 개체
권한 [154](#)
설명 [154](#)
런타임 개체 권한 그룹
설명 [154](#)
레이블
PowerCenter에 대한 권한 [158](#)
로그인 활동
보기 [117](#)
로드 권한 그룹
설명 [144](#)
매핑
사용 권한 [181](#)
상속된 사용 권한 [181](#)
명령줄 프로그램
권한 [196](#)
모니터링 권한 그룹
도메인 [138](#)
모델 권한 그룹
설명 [145](#)
모델 리포지토리 서비스
권한 [145](#)
권한 부여 [102](#)
권한이 있는 사용자 [169](#)
사용자 동기화 [102](#)
모든 사람 그룹
설명 [110](#)
배포 그룹
PowerCenter에 대한 권한 [158](#)
변경
사용자 계정의 암호 [107](#)
보안
권한 [108](#), [131](#), [133](#)
사용 권한 [108](#)
암호 [113](#)
역할 [132](#)
보안 관리 권한 그룹
설명 [133](#)
보안 권한 그룹
설명 [145](#)
보안 도메인
LDAP [19](#), [20](#)
LDAP 삭제 [29](#)
원시 [19](#)
클라이언트 구성 [79](#)
보안 페이지
Informatica Administrator [103](#)

보안 페이지 (계속)

탐색기 [103](#)

분석 서비스

권한 [140](#)

사용자 지정 역할 [224](#)

사용 권한

as 명령 [196](#)

cluster 명령 [197](#)

dis 명령 [198](#)

es 명령 [199](#)

ipc 명령 [200](#)

isp 명령 [200](#)

mas 명령 [208](#)

mrs 명령 [209](#)

ms 명령 [211](#)

pmcmd 명령 [216](#)

pmrep 명령 [219](#)

ps 명령 [212](#)

pxw 명령 [213](#)

rms 명령 [214](#)

rtm 명령 [214](#)

sch 명령 [214](#)

SQL 데이터 서비스 [183](#)

sql 명령 [215](#)

tools 명령 [212](#)

wfs 명령 [216](#)

가상 스키마 [183](#)

가상 저장 프로시저 [183](#)

가상 테이블 [183](#)

검색 필터 [174](#)

권한 작업 [172](#)

그리드 [174](#)

노드 [174](#)

도메인 개체 [174](#)

라이선스 [174](#)

매핑 [181](#)

상속 [173](#)

설명 [172](#)

연결 [178](#)

운영 체제 프로필 [174](#), [177](#)

워크플로우 [181](#)

웹 서비스 [187](#)

웹 서비스 작업 [187](#)

유형 [173](#)

유효 [173](#)

응용 프로그램 [181](#)

응용 프로그램 서비스 [174](#)

직접 [173](#)

폴더 [174](#)

사용자

개요 [104](#)

권한, 할당 [168](#)

다수 [116](#)

시스템 메모리 [116](#)

역할, 할당 [168](#)

올바르지 않은 문자 [113](#)

유효한 이름 [113](#)

사용자 계정

개요 [111](#)

기본값 [111](#)

설치 중 작성 [111](#)

암호 변경 [107](#)

활성화 [114](#)

사용자 보안

설명 [101](#)

사용자 설명

올바르지 않은 문자 [113](#)

사용자 지정 역할

Metadata Manager 서비스 [225](#)

PowerCenter 리포지토리 서비스 [227](#)

권한, 할당 [167](#)

분석 서비스 [224](#)

사용자 및 그룹에 할당 [168](#)

삭제 [168](#)

생성 [167](#)

설명 [165](#), [166](#)

운영자 [226](#)

편집 [167](#)

사용자 활동 로그

convertUserActivityLog [117](#)

getUserActivityLog [117](#)

출력 형식 [117](#)

활동 코드 [118](#)

상속된 권한

설명 [168](#)

상속된 사용 권한

설명 [173](#)

상위 그룹

설명 [121](#)

서비스 관리자

single sign-on [102](#)

권한 부여 [102](#)

인증 [101](#)

소스

권한 [152](#)

소스 및 대상 권한 그룹

설명 [152](#)

스케줄러 서비스

권한 [161](#)

시스템 메모리

늘리기 [116](#)

시스템 정의 역할

관리자 [165](#)

사용자 및 그룹에 할당 [168](#)

설명 [165](#)

암호

기본 관리자에 대한 변경 [111](#)

사용자 계정의 암호 변경 [107](#)

요구 사항 [113](#)

원시 사용자 [113](#)

암호화 그룹

구성 [88](#)

역할

개요 [105](#)

관리 [165](#)

관리자 [165](#)

문제 해결 [170](#)

사용자 지정 [166](#)

설명 [132](#)

할당 [168](#)

연결

기본 사용 권한 [179](#)

사용 권한 [178](#)

사용 권한 유형 [179](#)

연결 개체

PowerCenter에 대한 권한 [158](#)

열 수준 보안

열 제한 [186](#)

운영 체제 프로필

개요 [105](#)

관리 [122](#)

기본값 [128](#)

사용 권한 [174](#), [177](#)

삭제 [128](#)

운영 체제 프로필 (계속)

속성, PowerCenter 통합 서비스 [122](#)

속성, 데이터 통합 서비스 [122](#), [124](#)

속성, 메타데이터 액세스 서비스 [126](#)

작성 [126](#)

편집 [122](#)

운영자}

사용자 지정 역할 [226](#)

워크플로우

사용 권한 [181](#)

상속된 사용 권한 [181](#)

원시 그룹

관리 [120](#)

다른 그룹으로 이동 [122](#)

사용자, 할당 [114](#)

삭제 [122](#)

추가 [121](#)

편집 [121](#)

원시 보안 도메인

설명 [19](#)

원시 사용자

관리 [113](#)

그룹에 할당 [114](#)

삭제 [115](#)

암호 [113](#)

추가 [113](#)

편집 [114](#)

활성화 [114](#)

원시 인증

설명 [19](#), [101](#)

웹 서비스

사용 권한 [187](#)

사용 권한 유형 [187](#)

웹 서비스 리소스

사용 권한 [187](#)

웹 서비스 작업

사용 권한 [187](#)

유효한 사용 권한

설명 [173](#)

유효한 이름

그룹/ [121](#)

사용자 계정 [113](#)

응용 프로그램

사용 권한 [181](#)

응용 프로그램 서비스

권한 부여 [102](#)

사용 권한 [174](#)

사용자 동기화 [102](#)

인증

Kerberos [20](#)

LDAP [19](#), [24](#), [101](#)

서비스 관리자 [101](#)

원시 [19](#), [101](#)

중첩 그룹

LDAP 디렉터리 서비스 [28](#)

LDAP 인증 [28](#)

직접 사용 권한

설명 [173](#)

참조 테이블 메타데이터 편집

권한 [141](#)

참조 테이블 작성

권한 [141](#)

콘텐츠 관리 서비스

권한 [141](#)

클라이언트 구성

보안 도메인 [79](#)

탐색기

보안 페이지 [103](#)

P

pmcmd

명령별 권한 [216](#)

명령별 사용 권한 [216](#)

pmrep

명령별 권한 [219](#)

명령별 사용 권한 [219](#)

PowerCenter 리포지토리 서비스

관리자 역할 [166](#)

권한 [146](#)

권한 부여 [102](#)

권한이 있는 사용자 [169](#)

사용자 동기화 [102](#)

사용자 지정 역할 [227](#)

PowerCenter 보안

관리 [103](#)

PowerCenter 클라이언트

관리자 [111](#)

PowerExchange 로거 서비스

권한 [160](#)

PowerExchange 수신기 서비스

권한 [160](#)

ps

명령별 권한 [212](#)

명령별 사용 권한 [212](#)

powx

명령별 권한 [213](#)

명령별 사용 권한 [213](#)

R

rms

명령별 권한 [214](#)

명령별 사용 권한 [214](#)

rtm

명령별 권한 [214](#)

명령별 사용 권한 [214](#)

S

SAML(Security Assertion Markup Language)

게이트웨이 노드에서 활성화 [65](#)

도메인에서 활성화 [65](#)

서명된 응답 [66](#), [67](#)

암호화된 어설션 [68](#)

어설션 서명 또는 암호화 [66](#)

요청 서명 [66](#)

지원 [61](#)

sch

명령별 권한 [214](#)

명령별 사용 권한 [214](#)

single sign-on

개요 [61](#)

구성 [63](#)

설명 [102](#)

sql

명령별 권한 [215](#)

명령별 사용 권한 [215](#)

SQL 데이터 서비스

사용 권한 [183](#)

SQL 데이터 서비스 (계속)
사용 권한 유형 [183](#)
상속된 사용 권한 [183](#)
SSL 인증서
LDAP 인증 [28](#)

T

Test Data Manager
관리자 [111](#)
tools
명령별 권한 [212](#)
명령별 사용 권한 [212](#)

U

UpdateColumnOptions
열 값 대체 [186](#)

W

wfs
명령별 권한 [216](#)
명령별 사용 권한 [216](#)

ㄱ

가상 스키마
사용 권한 [183](#)
상속된 사용 권한 [183](#)
가상 저장 프로시저
사용 권한 [183](#)
상속된 사용 권한 [183](#)
가상 테이블
사용 권한 [183](#)
상속된 사용 권한 [183](#)
감사 보고서
- 그룹 [194](#)
- 사용자 [194](#), [195](#)
개요 [106](#)
설명 [190](#)
개체 쿼리
PowerCenter에 대한 권한 [158](#)
검색 섹션
Informatica Administrator [103](#)
검색 필터
사용 권한 [174](#)
계정
암호 변경 [107](#)
계정 관리
개요 [106](#)
관리자
기본값 [111](#)
도메인 [111](#)
역할 [165](#)
응용 프로그램 클라이언트 [111](#)
권한
as 명령 [196](#)
cluster 명령 [197](#)
dis 명령 [198](#)
es 명령 [199](#)
Informatica Cloud 관리 [139](#)
ipc 명령 [200](#)

권한 (계속)
isp 명령 [200](#)
mas 명령 [208](#)
Metadata Manager 서비스 [142](#)
mrs 명령 [209](#)
ms 명령 [211](#)
pmcmd 명령 [216](#)
pmrep 명령 [219](#)
PowerCenter 글로벌 개체 [158](#)
PowerCenter 리포지토리 서비스 [146](#)
PowerCenter 리포지토리 서비스 도구 [147](#)
PowerExchange 로거 서비스 [160](#)
PowerExchange 수신기 서비스 [160](#)
ps 명령 [212](#)
pwx 명령 [213](#)
rms 명령 [214](#)
rtm 명령 [214](#)
sch 명령 [214](#)
sql 명령 [215](#)
tools 명령 [212](#)
wfs 명령 [216](#)
대상 [152](#)
데이터 통합 서비스 [141](#)
도메인 [133](#)
도메인 관리 [134](#)
도메인 도구 [139](#)
디자인 개체 [149](#)
런타임 개체 [154](#)
명령줄 프로그램 [196](#)
모니터링 [138](#)
모델 리포지토리 서비스 [145](#)
문제 해결 [170](#)
보안 관리 [133](#)
분석 서비스 [140](#)
사용 권한 작업 [172](#)
상속 [168](#)
설명 [131](#)
소스 [152](#)
스케줄러 서비스 [161](#)
콘텐츠 관리 서비스 [141](#)
폴더 [148](#)
할당 [168](#)
권한 그룹
Informatica Cloud 관리 [139](#)
글로벌 개체 [158](#)
도구 [139](#), [147](#)
도메인 관리 [134](#)
디자인 개체 [149](#)
런타임 개체 [154](#)
로드 [144](#)
모니터링 [138](#)
모델 [145](#)
보안 [145](#)
보안 관리 [133](#)
설명 [132](#)
소스 및 대상 [152](#)
찾아보기 [143](#)
폴더 [148](#)
권한 그룹 찾아보기
설명 [143](#)
권한 부여
Metadata Manager 서비스 [102](#)
PowerCenter 리포지토리 서비스 [102](#)
데이터 통합 서비스 [102](#)
모델 리포지토리 서비스 [102](#)
서비스 관리자 [102](#)
응용 프로그램 서비스 [102](#)

그룹

개요 [104](#)

권한, 할당 [168](#)

역할, 할당 [168](#)

그룹 설명

올바르지 않은 문자 [121](#)

그룹/

관리 [120](#)

기본 모든 사람 [110](#)

동기화 [102](#)

상위 그룹 [121](#)

올바르지 않은 문자 [121](#)

그룹/ (계속)

유효한 이름 [121](#)

그리드

사용 권한 [174](#)

글로벌 개체

PowerCenter에 대한 권한 [158](#)

글로벌 개체 권한 그룹

설명 [158](#)

기본 관리자

설명 [111](#)

수정 [111](#)

암호, 변경 [111](#)