



Business Intelligence 플랫폼 관리자 가이드

■ SAP BusinessObjects Business Intelligence platform 4.0 Support Package 2

2011-05-06

Copyright

© 2011 SAP AG. All rights reserved. 모든 권한 보유. SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign 및 본 문서에 언급된 기타 SAP 제품, 서비스와 해당 로고는 독일 및 기타 국가에서 사용되는 SAP AG의 상표 또는 등록 상표입니다. Business Objects, Business Objects 로고, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius 및 본 문서에 언급된 기타 Business Objects 제품, 서비스와 해당 로고는 미국 및 기타 국가에서 사용되는 Business Objects S.A.의 상표 또는 등록 상표입니다. Business Objects는 SAP 회사 중 하나입니다. 기타 언급된 제품 및 서비스 이름은 해당 기업의 상표입니다. 이 문서에 포함된 데이터는 정보 전달의 목적으로만 사용됩니다. 국가별 제품 명세는 다를 수 있습니다. 이 문서의 내용은 사전 예고 없이 변경될 수 있습니다. 이 문서는 SAP AG 및 계열사 ("SAP 그룹")에 정보 전달 목적으로만 제공되며 어떠한 것도 대표하거나 보증하지 않습니다. SAP 그룹은 이 문서의 오류나 누락 부분에 대한 책임을 지지 않습니다. SAP 그룹 제품 및 서비스 대한 보증은 해당 제품 및 서비스와 함께 제공되는 보증서에 명시된 내용으로 국한합니다. 이 문서의 어떤 내용도 추가 보증의 근거로 해석할 수 없습니다.

2011-05-06

목차

1 장	시작하기.....	17
1.1	도움말 정보...17	
1.1.1	이 도움말의 대상...17	
1.1.2	SAP BusinessObjects Business Intelligence 플랫폼 정보 ...18	
1.1.3	변수...18	
1.2	시작하기 전에...19	
1.2.1	주요 개념...19	
1.2.2	주요 관리 도구...21	
1.2.3	주요 작업...23	
2 장	아키텍처.....	27
2.1	아키텍처 개요...27	
2.1.1	시스템 개요...28	
2.1.2	데이터베이스...29	
2.1.3	서버...30	
2.1.4	웹 응용 프로그램 서버...31	
2.1.5	소프트웨어 개발 키트...32	
2.1.6	데이터 소스...36	
2.1.7	언어 지원...37	
2.1.8	인증 및 단일 로그인...38	
2.1.9	SAP 통합...40	
2.1.10	주기 관리(LCM)...41	
2.1.11	통합 버전 제어...41	
2.1.12	영구 데이터...42	
2.1.13	업그레이드 경로...42	
2.2	개념적 계층...42	
2.3	서비스 및 서버...44	
2.3.1	서비스...45	
2.3.2	서비스 범주...51	
2.3.3	서버 유형...54	
2.3.4	서버...57	
2.4	클라이언트 응용 프로그램...59	
2.4.1	SAP BusinessObjects Business Intelligence 플랫폼 클라이언트 도구와 함께 설치 ...60	
2.4.2	SAP BusinessObjects Business Intelligence 플랫폼과 함께 설치...65	
2.4.3	별도로 사용 가능...66	

2.4.4	웹 응용 프로그램 클라이언트...68
2.5	정보 워크플로...72
2.5.1	인증...72
2.5.2	일정...74
2.5.3	보기...79
2.5.4	요청 시...81

3 장 라이선스 관리.....85

3.1	라이선스 키 관리...85
3.1.1	라이선스 정보 보기...85
3.1.2	라이선스 키 추가...86
3.1.3	현재 계정 활동을 보려면...86
3.2	라이선스 측정...86
3.2.1	라이선스 감사 실행...87

4 장 사용자 및 그룹 관리.....89

4.1	계정 관리 개요...89
4.1.1	사용자 관리...89
4.1.2	그룹 관리...91
4.1.3	사용 가능한 인증 형식 ...92
4.2	Enterprise 및 일반 계정 관리...94
4.2.1	사용자 계정 만들기...94
4.2.2	사용자 계정 수정...95
4.2.3	사용자 계정 삭제...96
4.2.4	새 그룹 만들기...97
4.2.5	그룹 속성 수정...97
4.2.6	그룹 멤버 보기...98
4.2.7	하위 그룹 추가...98
4.2.8	소속 그룹 지정...99
4.2.9	그룹 삭제...99
4.2.10	Guest 계정 활성화...100
4.2.11	그룹에 사용자 추가...100
4.2.12	암호 설정 변경...101
4.2.13	사용자 및 그룹에 액세스 허용...103
4.2.14	사용자의 받은 파일함에 대한 액세스 제어...104
4.2.15	BI 실행 패드 옵션 구성...104
4.3	별칭 관리...108
4.3.1	사용자 및 타사 별칭 만들기...108
4.3.2	기존 사용자에게 대한 새 별칭 만들기...109
4.3.3	다른 사용자의 별칭 할당...110
4.3.4	별칭 삭제...110
4.3.5	별칭 비활성화...111

5 장	권한 설정.....113
5.1	BI 플랫폼에서 권한 작동 방식...113
5.1.1	액세스 수준...113
5.1.2	고급 권한 설정...114
5.1.3	상속...115
5.1.4	유형별 권한...120
5.1.5	유효한 권한 결정...122
5.2	CMC에서 개체의 보안 설정 관리...123
5.2.1	개체에 대한 사용자 권한 보기...123
5.2.2	개체의 액세스 제어 목록에 사용자 할당...124
5.2.3	개체에 대한 사용자 보안 수정...124
5.2.4	BI 플랫폼에서 최상위 폴더에 대한 권한 설정...125
5.2.5	사용자에 대한 보안 설정 확인...126
5.3	액세스 수준 작업...128
5.3.1	보기 및 요청 시 보기 액세스 수준 중에서 선택...130
5.3.2	기존 액세스 수준 복사...131
5.3.3	새 액세스 수준 만들기...131
5.3.4	액세스 수준의 이름을 변경하려면...132
5.3.5	액세스 수준 삭제...132
5.3.6	액세스 수준의 권한 수정...132
5.3.7	액세스 수준과 개체 사이의 관계 추적...134
5.3.8	여러 사이트에서 액세스 수준 관리...134
5.4	상속 무시...135
5.4.1	상속을 비활성화하려면...136
5.5	관리 위임을 위한 권한 사용...137
5.5.1	개체에 대한 사용자 권한 수정 옵션 선택...138
5.5.2	소유자 권한...140
5.6	관리 권한을 위한 권장 사항 요약...140
6 장	BI 플랫폼 보안.....141
6.1	보안 개요 ...141
6.2	재해 복구 계획...141
6.3	배포 보안 설정을 위한 일반 권장 사항...142
6.4	번들 타사 서버에 대한 보안 구성...143
6.5	활성 신뢰 관계...143
6.5.1	로그온 토큰...143
6.5.2	분산 보안의 티켓 메커니즘...144
6.6	세션 및 세션 추적...145
6.6.1	CMS 세션 추적...145
6.7	환경 보호...146
6.7.1	웹 브라우저에서 웹 서버로...146
6.7.2	웹 서버와 BI 플랫폼 간 통신...147
6.8	보안 구성 수정 사항 감사 ...147
6.9	웹 작업 감사...147

6.9.1	불법 로그인 시도 방지...147
6.9.2	암호 제한...148
6.9.3	로그온 제한...148
6.9.4	사용자 제한...149
6.9.5	Guest 계정 제한...149
6.10	처리 확장...149
6.11	BI 플랫폼의 데이터 보안 개요...150
6.11.1	데이터 처리 보안 모드...150
6.12	BI 플랫폼의 암호화 방식...153
6.12.1	클러스터 키를 사용한 작업...153
6.12.2	암호화 담당자...155
6.12.3	CMC에서 암호화 키 관리...157
6.13	SSL에 대해 서버 구성...161
6.13.1	키 및 인증서 파일 만들기...162
6.13.2	SSL 프로토콜 구성...164
6.14	BI 플랫폼 구성 요소 간의 통신 이해...169
6.14.1	BI 플랫폼 서버 및 통신 포트 개요...169
6.14.2	BI 플랫폼 구성 요소 간의 통신 ...172
6.15	BI 플랫폼의 방화벽 구성...179
6.15.1	방화벽이 사용되는 시스템을 구성하려면...179
6.15.2	방화벽을 사용하는 배포 디버깅...183
6.16	일반적인 방화벽 시나리오의 예...184
6.16.1	예제 - 별도의 네트워크에 배포된 응용 프로그램 계층...184
6.16.2	예제 - 방화벽으로 BI 플랫폼 서버와 분리된 썩(Thick) 클라이언트 및 데이터베이스 계층...187
6.17	통합 환경에 대한 방화벽 설정...189
6.17.1	SAP 통합을 위한 구체적인 방화벽 지침...190
6.17.2	JD Edwards EnterpriseOne 통합을 위한 방화벽 구성...191
6.17.3	Oracle EBS에 대한 구체적인 방화벽 지침...193
6.17.4	PeopleSoft Enterprise 통합을 위한 방화벽 구성 ...194
6.17.5	Siebel 통합을 위한 방화벽 구성...196
6.18	BI 플랫폼 및 역방향 프록시 서버 ...198
6.18.1	지원되는 역방향 프록시 서버 ...198
6.18.2	웹 응용 프로그램 배포 방법 이해 ...198
6.19	BI 플랫폼 웹 응용 프로그램에 대해 역방향 프록시 서버 구성...199
6.19.1	역방향 프록시 서버 구성에 대한 자세한 지침...199
6.19.2	역방향 프록시 서버를 구성하려면...200
6.19.3	BI 플랫폼에 대한 Apache 2.2 역방향 프록시 서버 구성 ...200
6.19.4	BI 플랫폼에 대해 WebSEAL 6.0 역방향 프록시 서버 구성 ...201
6.19.5	BI 플랫폼에 대해 Microsoft ISA 2006 구성 ...202
6.20	역방향 프록시 배포에서 BI 플랫폼에 대한 특수 구성...203
6.20.1	웹 서비스에 대해 역방향 프록시 활성화...204
6.20.2	ISA 2006의 세션 쿠키에 대한 루트 경로 활성화...206
6.20.3	SAP BusinessObjects Live Office의 역방향 프록시 활성화...208

7 장	인증.....	211
7.1	BI 플랫폼의 인증 옵션...211	
7.1.1	기본 인증...212	
7.1.2	보안 플러그 인...213	
7.1.3	BI 플랫폼에 대한 단일 로그인...213	
7.2	Enterprise 인증...216	
7.2.1	Enterprise 인증 개요...216	
7.2.2	Enterprise 인증 설정...216	
7.2.3	Enterprise 설정 변경...217	
7.2.4	신뢰할 수 있는 인증 활성화...219	
7.2.5	웹 응용 프로그램에 대한 신뢰할 수 있는 인증 구성...221	
7.3	LDAP 인증...230	
7.3.1	LDAP 인증 사용...230	
7.3.2	LDAP 인증 구성...232	
7.3.3	LDAP 그룹 매핑...243	
7.4	Windows AD 인증...248	
7.4.1	개요...248	
7.4.2	AD 인증(Kerberos) 준비...252	
7.4.3	AD 인증 단일 로그인...265	
7.4.4	AD 그룹 매핑 및 AD 인증 구성...278	
7.4.5	Windows AD 인증 문제 해결...282	
7.5	SAP 인증...284	
7.5.1	SAP 인증 구성 ...285	
7.5.2	BI 플랫폼의 사용자 계정 만들기...285	
7.5.3	SAP 권한 부여 시스템에 연결...287	
7.5.4	SAP 인증 옵션 설정...289	
7.5.5	SAP 역할 가져오기...292	
7.5.6	보안 네트워크 연결(SNC) 구성...296	
7.5.7	SAP 시스템에 대한 단일 로그인 설정...310	
7.5.8	SAP Crystal Reports 및 SAP Netweaver에 대해 SSO 구성...314	
7.6	PeopleSoft 인증...315	
7.6.1	개요...315	
7.6.2	PeopleSoft Enterprise 인증 사용...315	
7.6.3	PeopleSoft 역할을 BI 플랫폼에 매핑...316	
7.6.4	사용자 업데이트 예약...319	
7.6.5	PeopleSoft 보안 브리지 사용...321	
7.7	JD Edwards 인증...333	
7.7.1	개요...333	
7.7.2	JD Edwards EnterpriseOne 인증 사용...333	
7.7.3	JD Edwards EnterpriseOne 역할을 BI 플랫폼에 매핑...334	
7.7.4	사용자 업데이트 예약...337	
7.8	Siebel 인증...339	
7.8.1	Siebel 인증 사용...339	
7.8.2	BI 플랫폼에 역할 매핑...340	

7.8.3	사용자 업데이트 예약...343
7.9	Oracle EBS 인증...345
7.9.1	Oracle EBS 인증 사용...345
7.9.2	Oracle E-Business Suite 역할을 BI 플랫폼에 매핑...346
7.9.3	역할 매핑 해제 ...350
7.9.4	매핑된 Oracle EBS 그룹 및 사용자의 권한 사용자 지정 ...351
7.9.5	SAP Crystal Reports 및 Oracle EBS에 대한 단일 로그인(SSO) 구성...353

8 장 서버 관리.....355

8.1	서버 관리...355
8.1.1	CMC의 서버 관리 영역 작업...355
8.1.2	Windows에서 스크립트를 이용한 서버 관리 ...358
8.1.3	UNIX에서 서버 관리 ...359
8.1.4	라이선스 키 관리...359
8.1.5	라이선스 측정...361
8.1.6	서버 상태 확인 및 변경...362
8.1.7	서버 추가, 복제 또는 삭제...368
8.1.8	중앙 관리 서버 클러스터링...372
8.1.9	서버 그룹 관리...377
8.1.10	시스템 성능 평가...382
8.1.11	서버 설정 구성...387
8.1.12	서버 네트워크 설정 구성...391
8.1.13	노드 관리...400
8.1.14	SAP BusinessObjects Business Intelligence 플랫폼 배포에서 컴퓨터 이름 바꾸기 ...424
8.1.15	SAP BusinessObjects Business Intelligence 플랫폼에서 32비트 및 64비트 타사 라이브러리 사용...425
8.1.16	서버 및 노드 자리 표시자 관리...425

9 장 중앙 관리 서버(CMS) 데이터베이스 관리.....427

9.1	CMS 시스템 데이터베이스 연결 관리...427
9.2	새 CMS 데이터베이스 또는 기존 CMS 데이터베이스 선택...427
9.2.1	Windows에서 새 CMS 데이터베이스 또는 기존 데이터베이스 선택...428
9.2.2	UNIX에서 새 CMS 데이터베이스 또는 기존 데이터베이스 선택...428
9.3	CMS 시스템 데이터베이스 다시 만들기...429
9.3.1	Windows에서 CMS 시스템 데이터베이스 다시 만들기...429
9.3.2	UNIX에서 CMS 시스템 데이터베이스 다시 만들기...430
9.4	CMS 시스템 데이터베이스 간에 데이터 복사...431
9.4.1	CMS 시스템 데이터베이스 복사 준비...431
9.4.2	Windows에서 CMS 시스템 데이터베이스 복사...432
9.4.3	UNIX에 설치된 CMS에서 데이터 복사...433

10 장 웹 응용 프로그램 컨테이너 서버(WACS) 관리.....435

10.1	WACS...435
------	------------

10.1.1	웹 응용 프로그램 컨테이너 서버(WACS)...435
10.1.2	추가 WACS를 배포에 추가 또는 제거...438
10.1.3	WACS에 서비스 추가 또는 제거...442
10.1.4	HTTPS/SSL 구성...443
10.1.5	지원되는 인증 방법...448
10.1.6	WACS에 대해 AD Kerberos 구성 ...448
10.1.7	AD Kerberos 단일 로그인 구성 ...456
10.1.8	WACS 및 IT 환경...459
10.1.9	웹 응용 프로그램 속성 구성...462
10.1.10	문제 해결...463
10.1.11	WACS 속성...468
11 장	백업 및 복원.....469
11.1	시스템 백업 및 복원...469
11.1.1	시스템 백업 수행...470
11.1.2	서버 설정 백업...471
11.1.3	비즈니스 인텔리전스 콘텐츠 백업...473
11.1.4	시스템 복원...474
11.1.5	백업이 있는 경우 손실 또는 손상된 SAP BusinessObjects Business Intelligence 플랫폼 파일 복원...479
11.1.6	파일이 손실된 경우 SAP BusinessObjects Business Intelligence 플랫폼 시스템 다시 만들기...479
11.1.7	BackupCluster 및 RestoreCluster 매개 변수...480
12 장	수명 주기 관리.....483
12.1	주기 관리 콘솔...483
12.2	주기 관리 콘솔용 버전 관리 시스템...483
12.2.1	주기 관리 콘솔용 버전 관리 시스템...484
12.3	BIAR 엔진 명령줄 도구...484
12.3.1	속성 파일 사용 ...487
12.3.2	BIAR 엔진 명령줄 도구 사용...491
13 장	응용 프로그램 관리.....493
13.1	CMC를 통한 응용 프로그램 관리...493
13.1.1	개요...493
13.1.2	응용 프로그램의 일반 설정...494
13.1.3	응용 프로그램 관련 설정...496
13.2	BOE.war 속성을 통한 응용 프로그램 관리...514
13.2.1	BOE war 파일...514
13.3	BI 실행 패드 및 OpenDocument 로그인 진입점 사용자 지정...523
13.3.1	BI 실행 패드 및 OpenDocument 파일 위치...523
13.3.2	사용자 지정 로그인 페이지 정의...524
13.3.3	로그인 시 신뢰할 수 있는 인증 추가...525
13.4	BEx 웹 통합 구성 ...526

13.4.1	BEx 웹 응용 프로그램용 서버 시작 ...527
13.4.2	BEx 웹 응용 프로그램에 대해 표준 서버 시작 ...528
13.4.3	서버 설정 구성...528
13.4.4	BW 시스템에 대한 연결 확인 ...529
13.4.5	BEx Web Application Designer 및 BI 플랫폼 간 연결 구성...529
14 장	연결 및 유니버스 관리.....533
14.1	연결 관리...533
14.1.1	유니버스 연결 삭제...533
14.2	유니버스 관리...534
14.2.1	유니버스 삭제...535
15 장	모니터링.....537
15.1	모니터링 정보...537
15.2	모니터링 용어...537
15.2.1	아키텍처...538
15.3	모니터링 서버에 대한 클러스터 지원...542
15.4	메트릭...542
15.5	구성 속성...550
15.5.1	JMX 끝점 URL...553
15.6	다른 응용 프로그램과 통합...554
15.6.1	IBM Tivoli와 모니터링 응용 프로그램 통합...555
15.6.2	SAP Solution Manager와 모니터링 응용 프로그램 통합 ...558
15.7	Derby 데이터베이스용 유니버스 만들기...558
15.8	문제 해결...559
15.8.1	대시보드...559
15.8.2	경고...560
15.8.3	감시 목록...560
15.8.4	프로브...561
15.8.5	메트릭...562
15.8.6	그래프...562
16 장	감사.....563
16.1	개요...563
16.2	CMC 감사 페이지...569
16.2.1	감사 상태...569
16.2.2	감사 이벤트 구성...570
16.2.3	감사 데이터 저장소 구성 설정...573
16.3	감사 이벤트...574
16.3.1	감사 이벤트 및 세부 정보...581
17 장	플랫폼 검색.....599
17.1	개요...599

17.2	아키텍처...599
17.3	플랫폼 검색의 클러스터 지원...601
17.4	SDK 및 Open Search...601
17.4.1	플랫폼 검색 SDK...602
17.4.2	Open Search...602
17.5	응용 프로그램 속성 구성...604
17.6	검색 가능한 콘텐츠 유형...609
17.7	제안된 쿼리...611
17.8	패킷...611
17.9	다국어 지원...612
17.10	제안...613
17.11	SAP BusinessObjects Explorer의 검색 결과 연합...613
17.12	SAP NetWeaver Enterprise Search를 이용한 검색 시간 통합...613
17.12.1	SAP NetWeaver Enterprise Search에서 커넥터 만들기 ...614
17.12.2	SAP BusinessObjects Enterprise 인증의 사용자 역할 가져오기...615
17.12.3	NetWeaver Enterprise Search에서 검색...615
17.13	감사...616
17.14	인덱싱 오류 목록...617
17.15	문제 해결...618

18 장 연합621

18.1	연합...621
18.2	연합 용어...622
18.2.1	BI 응용 프로그램 ...622
18.2.2	대상 사이트 ...623
18.2.3	로컬...623
18.2.4	로컬에서 실행되는 완료된 인스턴스 ...623
18.2.5	다중 원본 사이트 ...623
18.2.6	단방향 복제 ...624
18.2.7	원본 사이트 ...624
18.2.8	원격...624
18.2.9	원격 연결...624
18.2.10	원격 일정 설정...624
18.2.11	복제...625
18.2.12	복제 작업...625
18.2.13	복제 목록...625
18.2.14	복제 개체...625
18.2.15	복제 패키지...626
18.2.16	복제 새로 고침...626
18.2.17	양방향 복제...626
18.3	보안 권한 관리...626
18.3.1	원본 사이트에 필요한 권한...627
18.3.2	대상 사이트에 필요한 권한...627
18.3.3	연합 관련 권한...628
18.3.4	개체에 대한 보안 복제...629

18.3.5	엑세스 수준을 사용하여 보안 복제...630
18.4	복제 유형 및 모드 옵션...631
18.4.1	단방향 복제 ...631
18.4.2	양방향 복제 ...631
18.4.3	원본에서 새로 고침 또는 대상에서 새로 고침...632
18.5	타사 사용자 및 그룹 복제...633
18.6	유니버스 및 유니버스 연결 복제...634
18.7	복제 목록 관리...635
18.7.1	복제 목록 만들기...636
18.7.2	복제 목록 수정...638
18.8	원격 연결 관리...639
18.8.1	원격 연결 만들기...640
18.8.2	원격 연결 수정...642
18.9	복제 작업 관리...642
18.9.1	복제 작업 만들기...643
18.9.2	복제 작업 예약...645
18.9.3	복제 작업 수정...645
18.9.4	복제 작업 후 로그 보기...646
18.10	개체 정리 관리...647
18.10.1	개체 정리 사용 방법...647
18.10.2	개체 정리 제한...648
18.10.3	개체 정리 간격...648
18.11	충돌 감지 및 해결 관리...649
18.11.1	단방향 복제 충돌 해결...650
18.11.2	양방향 복제 충돌 해결...651
18.12	연함에 웹 서비스 사용...654
18.12.1	세션 변수 ...654
18.12.2	파일 캐싱 ...655
18.12.3	사용자 지정 배포 ...655
18.13	원격 일정 설정 및 로컬에서 실행되는 인스턴스...656
18.13.1	원격 일정 설정...656
18.13.2	로컬에서 실행되는 인스턴스...658
18.13.3	인스턴스 공유...658
18.14	복제된 콘텐츠 가져오기 및 승격...659
18.14.1	복제된 콘텐츠 가져오기...659
18.14.2	복제된 콘텐츠를 가져온 후 복제 진행 ...660
18.14.3	테스트 환경의 콘텐츠 수준 올리기...661
18.14.4	대상 사이트 다시 가리키기...661
18.15	모범 사례...662
18.15.1	현재 릴리스 제한 사항...664
18.15.2	오류 메시지 문제 해결...666
19 장	ERP 환경에 대한 보완 구성.....669
19.1	SAP NetWeaver 통합 구성...669
19.1.1	SAP NetWeaver Business Warehouse(BW)와 통합...669

19.2	JD Edwards 통합 구성...727
19.2.1	SAP Crystal Reports에 대해 단일 로그인(SSO) 구성...728
19.2.2	JD Edwards 통합을 위한 Secure Sockets Layer 구성...729
19.3	PeopleSoft Enterprise 통합 구성...730
19.3.1	SAP Crystal Reports 및 PeopleSoft Enterprise에 대해 단일 로그인(SSO) 구성...730
19.3.2	Secure Sockets Layer 통신 구성...731
19.3.3	PeopleSoft 시스템용 성능 조정...733
19.4	Siebel 통합 구성...735
19.4.1	SAP BusinessObjects Business Intelligence 플랫폼과 통합하도록 Siebel 구성...735
19.4.2	Crystal Reports 메뉴 항목 만들기...736
19.4.3	Contextual Awareness...738
19.4.4	SAP Crystal Reports 및 Siebel에 대해 단일 로그인(SSO) 구성...740
19.4.5	Secure Socket Layer 통신을 위한 구성...741
20 장	로그 관리 및 구성.....743
20.1	구성 요소에서 추적 로깅...743
20.2	추적 로그 수준...743
20.3	서버에 대한 추적 구성...744
20.3.1	CMC에서 서버 추적 로그 수준 설정...745
20.3.2	CMC에서 관리되는 여러 서버에 대한 추적 로그 수준 설정...745
20.3.3	BO_trace.ini 파일을 통해 서버 추적 구성...746
20.4	웹 응용 프로그램에 대한 추적 구성...749
20.4.1	CMC에서 웹 응용 프로그램 추적 로그 수준 설정...749
20.4.2	BO_trace.ini 파일을 통해 수동으로 추적 설정 수정...750
20.5	업그레이드 관리 도구에 대한 추적 구성...755
20.5.1	업그레이드 관리 도구에 대한 추적 구성...755
21 장	SAP Solution Manager에 통합.....757
21.1	통합 개요...757
21.2	SAP Solution Manager 통합 검사 목록...757
21.3	System Landscape Directory 등록 관리...758
21.3.1	시스템 랜드스케이프에 BI 플랫폼 등록...759
21.3.2	SLD 등록이 트리거되는 시기...760
21.3.3	SLD 연결 로깅 ...760
21.4	Solution Manager Diagnostics Agent 관리...761
21.4.1	SMD(Solution Manager Diagnostics) 개요...761
21.4.2	SMD 에이전트 작업...762
21.4.3	SMAAdmin 사용자 계정...762
21.5	성능 계측 관리...763
21.5.1	BI 플랫폼용 성능 계측...763
21.5.2	BI 플랫폼용 성능 계측 설정...763
21.5.3	Web Tier를 위한 성능 계측...765
21.5.4	계측 로그 파일 ...765
21.6	SAP Passport로 추적...766

22 장	명령줄 관리.....	767
22.1	UNIX 스크립트...767	
22.1.1	스크립트 유틸리티...767	
22.1.2	스크립트 템플릿...773	
22.1.3	SAP BusinessObjects Business Intelligence 플랫폼에서 사용하는 스크립트 .774	
22.2	Windows 스크립트...776	
22.2.1	ccm.exe...776	
22.3	서버 명령줄...779	
22.3.1	명령줄 개요...779	
22.3.2	모든 서버의 표준 옵션...780	
22.3.3	중앙 관리 서버...781	
22.3.4	Crystal Reports 처리 서버 및 Crystal Reports 캐시 서버...784	
22.3.5	Dashboard Design 처리 서버와 Dashboard Design 캐시 서버...785	
22.3.6	작업 서버...786	
22.3.7	적응형 처리 서버...787	
22.3.8	Report Application Server...787	
22.3.9	Web Intelligence 처리 서버...789	
22.3.10	입력 및 출력 파일 리포지토리 서버...791	
22.3.11	이벤트 서버...793	
22.3.12	대시보드 및 대시보드 분석 서버 ...793	
23 장	권한 부록.....	795
23.1	권한 부록 소개...795	
23.2	일반 권한...795	
23.3	특정 개체 유형에 대한 권한...797	
23.3.1	폴더 권한...797	
23.3.2	범주...798	
23.3.3	메모...798	
23.3.4	Crystal 보고서...799	
23.3.5	Web Intelligence 문서...800	
23.3.6	사용자 및 그룹...801	
23.3.7	액세스 수준...802	
23.3.8	BI 작업 영역...803	
23.3.9	유니버스(.unv) 권한...804	
23.3.10	유니버스(.unx) 권한...805	
23.3.11	유니버스 개체 액세스 수준...806	
23.3.12	연결 권한...808	
23.3.13	응용 프로그램...809	
24 장	서버 속성 부록.....	821
24.1	서버 속성 부록에 대한 정보...821	
24.1.1	일반 서버 속성...821	
24.1.2	핵심 서비스 속성...824	

24.1.3	연결 서비스 속성...834	
24.1.4	Crystal Reports 서비스 속성...837	
24.1.5	분석 서비스 속성...846	
24.1.6	데이터 연합 서비스 속성...848	
24.1.7	Web Intelligence 서비스 속성...848	
24.1.8	Dashboard Design 서비스 속성...856	
25 장	서버 메트릭 부록.....	861
25.1	서버 메트릭 부록 정보...861	
25.1.1	공통 서버 메트릭 ...861	
25.1.2	중앙 관리 서버 메트릭...863	
25.1.3	연결 서버 메트릭...868	
25.1.4	이벤트 서버 메트릭...869	
25.1.5	파일 리포지토리 서버 메트릭...869	
25.1.6	적응형 처리 서버 메트릭...870	
25.1.7	웹 응용 프로그램 컨테이너 서버 메트릭...875	
25.1.8	적응형 작업 서버 메트릭...875	
25.1.9	Crystal Report Server 메트릭...878	
25.1.10	Web Intelligence 서버 메트릭...880	
25.1.11	Dashboard Design 서버 메트릭...881	
26 장	서버 및 노드 자리 표시자 부록.....	885
26.1	서버 및 노드 자리 표시자...885	
27 장	감사 데이터 저장소 스키마 부록.....	895
27.1	개요...895	
27.2	스키마 다이어그램...895	
27.3	감사 데이터 저장소 테이블...896	
A 부록	추가 정보.....	905
인덱스.....		907

장1 시작하기

1.1 도움말 정보

이 도움말에서는 BI 플랫폼을 배포 및 구성하기 위한 정보와 절차를 제공합니다. 여기에서는 일반적인 작업의 절차를 설명합니다. 또한 모든 고급 항목에 대한 개념 정보와 세부적인 기술 내용을 설명합니다.

이 제품 설치에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 설치 가이드를 참조하십시오.

1.1.1 이 도움말의 대상

이 도움말에서는 배포 및 구성 작업을 설명합니다. 여기에 설명된 내용은 다음과 같은 경우에 유용합니다.

- 최초 배포를 계획할 경우
- 최초 배포를 구성할 경우
- 기존 배포의 아키텍처를 크게 변경하려는 경우
- 시스템의 성능을 개선하려는 경우

이 도움말은 BI 플랫폼 설치 환경의 구성, 관리 및 유지 관리 작업을 담당하는 시스템 관리자를 대상으로 합니다. 운영 체제와 네트워크 환경에 대한 지식이나 웹 응용 프로그램 서버 관리 및 스크립트 작성 기술에 대한 일반적인 지식을 갖추고 있다면 여기에서 설명하는 내용을 쉽게 이해할 수 있습니다. 그러나 이 도움말의 내용은 실무 관리 경험의 수준에 상관없이 모든 사용자가 관리 작업과 기능을 이해하는 데 충분한 배경 지식과 개념 정보를 얻을 수 있도록 작성되었습니다.

1.1.2 SAP BusinessObjects Business Intelligence 플랫폼 정보

BI 플랫폼은 인트라넷, 엑스트라넷, 인터넷 또는 통합 포털과 같은 임의의 웹 응용 프로그램을 통해 최종 사용자에게 강력한 대화형 보고서를 제공하며 유연하고 확장 가능한 안정적인 솔루션입니다. BI 플랫폼을 사용하면 그 용도가 주간 판매 보고서를 배포하기 위한 것이든, 고객에게 맞춤 서비스를 제공하기 위한 것이든, 중요한 정보를 통합 포털에 통합하기 위한 것이든 상관없이 조직의 내부와 외부 사용자 모두 실질적인 이익을 얻을 수 있습니다. 보고서 작성, 분석 및 정보 전달을 목적으로 하는 이 플랫폼은 최종 사용자의 생산성을 높이고 관리에 드는 노력을 줄일 수 있는 솔루션을 제공합니다.

1.1.3 변수

이 가이드 전체에서 사용되는 변수는 다음과 같습니다.

변수	설명
<INSTALLEDIR>	BI 플랫폼이 설치된 디렉터리입니다. Windows 컴퓨터의 경우 기본 디렉터리는 C:\Program Files (x86)\SAP BusinessObjects\입니다.
<PLATFORM64DIR>	UNIX 운영 체제의 이름입니다. 허용되는 값은 다음과 같습니다. <ul style="list-style-type: none"> • aix_rs6000_64 • linux_x64 • solaris_sparcv9 • hpux_ia64
<SCRIPTDIR>	관리 BI 플랫폼의 스크립트가 위치한 디렉터리입니다. Windows 컴퓨터의 경우 <INSTALLEDIR>\win64_x64\scripts 디렉터리입니다. UNIX 컴퓨터의 경우 <INSTALLEDIR>/<PLATFORM64DIR>/scripts 디렉터리입니다.

1.2 시작하기 전에

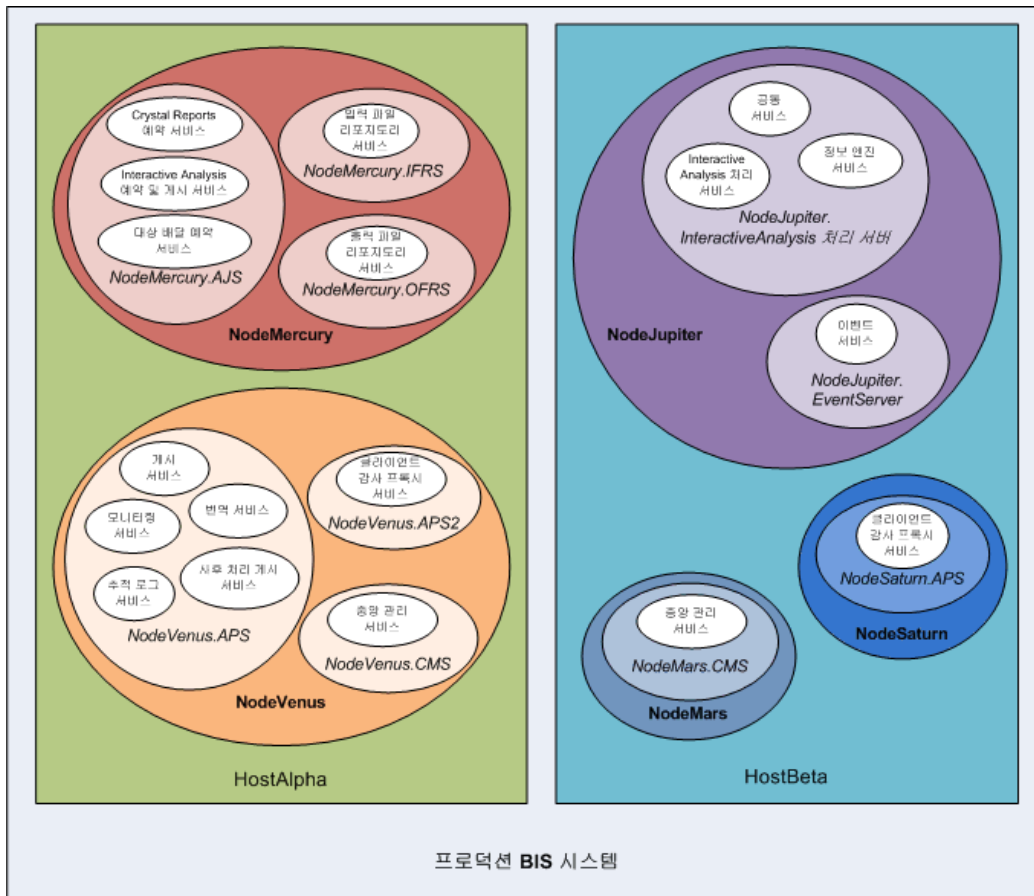
1.2.1 주요 개념

1.2.1.1 서비스 및 서버

다음 그림에서 BI 플랫폼의 가상 설치를 볼 수 있습니다.

참고:

노드, 서버 및 서비스는 예시용으로만 표시되었습니다. 서버와 서비스의 종류 뿐 아니라 호스트, 노드, 서버 및 서비스의 수는 실제 설치 시 달라질 수 있습니다.



아래에 설명된 두 개의 호스트가 ProductionBISystem이라는 클러스터를 구성합니다.

- HostAlpha라는 호스트에 BI 플랫폼이 설치되어 있고 다음 두 개의 노드를 포함하도록 구성됩니다.
 - NodeMercury: 보고서 예약 및 게시 서비스를 제공하는 적응형 작업 서버(NodeMercury.AJS), 입력 보고서를 저장하는 서비스를 제공하는 입력 파일 리포지토리 서버(NodeMercury.IFRS), 보고서 출력을 저장하는 서비스를 제공하는 출력 파일 리포지토리 서버(NodeMercury.OFRS)로 구성됩니다.
 - NodeVenus: 게시, 모니터링 및 변환 기능 서비스를 제공하는 적응형 처리 서버(NodeVenus.APS), 클라이언트 감사 서비스를 제공하는 적응형 처리 서버(NodeVenus.APS), CMS 서비스를 제공하는 중앙 관리 서버(NodeVenus.CMS)로 구성됩니다.
- 이름이 HostBeta인 호스트에는 BI 플랫폼이 설치되어 있고 다음 세 개의 노드를 포함하도록 구성됩니다.
 - NodeMars: CMS 서비스를 제공하는 중앙 관리 서버(NodeMars.CMS)로 구성됩니다.

- NodeJupiter: Web Intelligence 보고 서비스를 제공하는 Web Intelligence 처리 서버 (NodeJupiter.Web Intelligence), 파일의 보고서 모니터링 서비스를 제공하는 이벤트 서버 (NodeJupiter.EventServer)로 구성됩니다.
- NodeSaturn: 클라이언트 감사 서비스를 제공하는 적응형 처리 서버(NodeSaturn.APS)로 구성됩니다.

BI 플랫폼은 BI 플랫폼 컴퓨터에서 실행되는 두 가지 유형의 소프트웨어를 칭하는 말로 서버와 서비스라는 용어를 사용합니다.

서비스는 특정 기능을 수행하는 서버 하위 시스템입니다. 서비스는 부모 컨테이너(서버)의 프로세스 id로 서버의 메모리 공간 내에서 실행됩니다. 예를 들어 SAP BusinessObjects Web Intelligence 예약 및 게시 서비스는 적응형 작업 서버 안에서 실행되는 하위 시스템입니다.

서버라는 용어는 하나 이상의 서비스를 호스팅하는 운영 체제 수준 프로세스(일부 컴퓨터에서는 데몬이라고도 함)를 설명하는 데 사용됩니다. 예를 들어 중앙 관리 서버(CMS)와 적응 처리 서버는 서버입니다. 서버는 특정 운영 체제 계정에서 실행되고 자체 PID를 갖습니다.

노드는 동일한 호스트에서 실행되는 BI 플랫폼 서버의 컬렉션입니다. 단일 호스트에 하나 이상의 노드가 있을 수 있습니다.

BI 플랫폼을 단일 컴퓨터에 설치하거나 인트라넷에 있는 다른 컴퓨터에 배포하거나 또는 WAN(Wide Area Network)을 통해 배포할 수 있습니다.

1.2.1.2 Server Intelligence

Server Intelligence는 컬렉션 또는 서버 프로세스를 관리하기 위한 중앙 관리 콘솔(CMC)의 구성 요소로서, 일반적으로 노드라고 알려져 있습니다. CMC에서 적용된 서버 프로세스의 변경 내용은 SIA(Server Intelligence Agent)를 통해 관련 서버로 전파됩니다. SIA는 예기치 않은 상황이 발생할 경우 서버를 자동으로 다시 시작하거나 종료하는 데에도 사용되고 중앙 관리 서버(CMS)에서 노드를 관리하는 데 사용됩니다.

SIA(Server Intelligence Agent) 서버는 CMS 시스템 데이터베이스에 서버 정보를 보관하므로 필요한 경우 기본 서버 설정을 쉽게 복원하거나 동일한 설정을 적용한 서버 프로세스의 인스턴스를 중복하여 만들 수 있습니다.

1.2.2 주요 관리 도구

1.2.2.1 중앙 관리 콘솔(CMC)

중앙 관리 콘솔(CMC)은 사용자 관리, 콘텐츠 관리 및 서버 관리를 포함하여 관리 작업을 수행하는 데 사용되는 웹 기반 도구입니다. 사용자가 보안 설정을 게시 및 구성할 수도 있습니다. CMC는 웹 기반 응용 프로그램이므로 이러한 모든 관리 작업을 서버에 연결할 수 있는 모든 컴퓨터의 웹 브라우저를 통해 원격으로 수행할 수 있습니다.

모든 사용자는 CMC에 로그인하여 자신의 기본 설정을 변경할 수 있습니다. 또한 해당 권한이 명시적으로 부여되지 않은 경우 Administrators 그룹의 멤버만 관리 설정을 변경할 수 있습니다. 일부 사용자에게 보조 관리 작업을 수행할 수 있는 권한을 부여하도록 역할을 CMC에 할당할 수도 있습니다.

1.2.2.2 중앙 구성 관리자(CCM)

중앙 구성 관리자(CCM)는 두 가지 형태로 제공되는 서버 문제 해결 및 노드 관리 도구입니다. Microsoft Windows 환경에서는 CCM을 사용하여 그래픽 사용자 인터페이스(GUI) 또는 명령줄을 통해 로컬/원격 서버를 관리할 수 있습니다. UNIX 환경에서는 CCM 셸 스크립트(ccm.sh)를 사용하여 명령줄에서 서버를 관리할 수 있습니다.

CCM을 사용하면 SIA(Server Intelligence Agent) 노드를 만들고 구성할 수 있으며 웹 응용 프로그램 서버를 시작 또는 중지할 수 있습니다. 또한 Windows에서는 SSL(Secure Socket Layer) 암호화 등의 네트워크 매개 변수를 구성할 수 있습니다. 이러한 매개 변수는 노드 내에서 모든 서버에 적용됩니다.

참고:

대부분의 서버 관리 작업은 이제 CCM이 아닌 CMC를 통해 처리됩니다. 현재 CCM은 문제 해결 및 노드 구성에 사용됩니다.

1.2.2.3 리포지토리 진단 도구

리포지토리 진단 도구(RDT)를 사용하면 중앙 관리 서버(CMS) 시스템 데이터베이스와 파일 리포지토리 서버(FRS) 파일 저장소 사이에 발생할 수 있는 불일치를 검사, 진단 및 복구할 수 있습니다. RDT를 중지하기 전에 RDT를 통해 찾거나 복원할 오류의 수를 제한할 수 있습니다.

BI 플랫폼 시스템을 복원한 다음 RDT를 사용해야 합니다.

1.2.2.4 업그레이드 관리 도구

업그레이드 관리 도구(이전 이름: 가져오기 마법사)는 BI 플랫폼의 일부로 설치되며, 이전 버전의 BI 플랫폼에서 사용자, 그룹 및 폴더를 가져오는 과정을 관리자에게 안내합니다. 개체, 이벤트, 서버 그룹, 리포지토리 개체 및 달력을 가져오고 업그레이드할 수도 있습니다.

BI 플랫폼의 이전 버전을 업그레이드하는 방법에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 업그레이드 가이드를 참조하십시오.

1.2.3 주요 작업

상황에 따라 이 도움말의 특정 단원을 중점적으로 읽고 사용 가능한 다른 리소스를 찾아볼 수 있습니다. 다음과 같은 각 상황에 대한 권장 작업 목록이 있으므로 해당 항목을 읽어 보십시오.

관련 항목

- 23 페이지에서 [첫 배포 계획 또는 수행](#)"
- 24 페이지에서 [배포 구성](#)"
- 24 페이지에서 [시스템 성능 개선](#)"
- 69 페이지에서 [중앙 관리 콘솔\(CMC\)](#)"

1.2.3.1 첫 배포 계획 또는 수행

BI 플랫폼의 최초 배포를 계획하거나 수행하려면 다음 작업을 수행하고 해당 단원을 읽어 보는 것이 좋습니다.

- BI 플랫폼에 대해 알아보려면 아키텍처 개요를 읽어 보십시오.
- 요구 사항을 평가하고 가장 적합한 배포 아키텍처를 설계하려면 SAP BusinessObjects Business Intelligence 플랫폼 배포 계획 가이드를 읽어 보십시오.
- BI 플랫폼 구성 요소 간의 통신 이해
- 보안 개요
- 타사 인증을 사용할 계획인 경우 인증을 읽어 보십시오.
- BI 플랫폼 설치에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 설치 가이드를 참조하십시오.
- 설치를 완료하고 나면 서버 관리 개요를 읽어 보십시오.

관련 항목

- 27 페이지에서 [아키텍처 개요](#)"
- 169 페이지에서 [BI 플랫폼 구성 요소 간의 통신 이해](#)"
- 141 페이지에서 [보안 개요](#) "
- 211 페이지에서 [BI 플랫폼의 인증 옵션](#)"
- 355 페이지에서 [서버 관리](#)"

1.2.3.2 배포 구성

BI 플랫폼의 설치를 완료한 후 즉시 방화벽 구성 및 사용자 관리 등의 초기 구성 작업을 수행해야 하는 경우에는 다음 단원을 읽어 보는 것이 좋습니다.

관련 항목

- 355 페이지에서 [서버 관리](#)"
- 172 페이지에서 [BI 플랫폼 구성 요소 간의 통신](#) "
- 141 페이지에서 [보안 개요](#) "
- 537 페이지에서 [모니터링 정보](#)"

1.2.3.3 시스템 성능 개선

배포의 효율성을 평가하고 세부 조정을 통해 리소스를 최대화하려면 다음 단원을 읽어 보는 것이 좋습니다.

- 기존 시스템을 모니터링하려면 [모니터링](#)을 읽어 보십시오.
- CMC에서 서버 작업을 수행하는 데 필요한 일상적인 유지 관리 작업과 절차에 대한 자세한 내용은 [서버 유지 관리](#)를 참조하십시오.

관련 항목

- 537 페이지에서 [모니터링 정보](#)
- 355 페이지에서 [서버 관리](#)

1.2.3.4 CMC에서 개체로 작업

CMC에서 개체를 사용하여 작업하는 경우 다음 단원을 읽어 보십시오.

- CMC에서 사용자와 그룹을 설정하는 데 대한 자세한 내용은 [계정 관리 개요](#)를 참조하십시오.
- 개체에 대한 보안을 설정하려면 BI 플랫폼에서 권한 작동 방식을 참조하십시오.
- 개체를 사용한 작업에 대한 일반적인 내용은 SAP BusinessObjects Business Intelligence 플랫폼 사용자 가이드를 참조하십시오.

관련 항목

- 89 페이지에서 [계정 관리 개요](#)
- 113 페이지에서 [BI 플랫폼에서 권한 작동 방식](#)

장2 아키텍처

2.1 아키텍처 개요

이 단원에서는 SAP BusinessObjects Business Intelligence 플랫폼을 구성하는 전체 플랫폼 아키텍처, 시스템 및 서비스 구성 요소에 대해 간략하게 설명합니다. 이 정보를 통해 관리자는 시스템 기본 사항을 이해하고 시스템 배포, 관리 및 유지 관리 계획을 세울 수 있습니다.

SAP BusinessObjects Business Intelligence 플랫폼은 광범위한 사용자층과 배포 시나리오에 대해 높은 성능을 발휘할 수 있도록 디자인되었습니다. 예를 들어, 특화된 플랫폼 서비스는 사용자의 주문을 기준으로 데이터 액세스와 보고서 생성을 처리할 수도 있고 시간 및 이벤트를 기준으로 보고서 예약을 처리할 수도 있습니다. 특정 서버에 호스팅할 전용 서버를 만들어 프로세서 집약적인 일정 관리와 처리를 별도로 처리할 수 있습니다. 이 아키텍처는 거의 모든 BI 배포의 요구 사항을 충족하도록 설계되었으며 도구를 하나만 사용하는 몇 명 되지 않는 사용자 조직이 여러 가지 도구와 인터페이스를 필요로 하는 수만 명의 사용자 집단으로 규모를 키우더라도 충분히 대처할 만큼 유연성이 있습니다.

개발자는 웹 서비스, Java 또는 .NET 응용 프로그래밍 인터페이스(API)를 사용하여 SAP BusinessObjects Business Intelligence 플랫폼 BI를 조직의 다른 기술 시스템에 통합할 수 있습니다.

최종 사용자는 다음과 같은 특화된 도구와 응용 프로그램을 사용하여 보고서에 액세스하고, 보고서를 만들고, 편집하고, 상호 작용할 수 있습니다.

- SAP BusinessObjects Business Intelligence 플랫폼 클라이언트 도구 설치 프로그램을 통해 설치된 클라이언트
 - Web Intelligence
 - 비즈니스 뷰 관리자
 - 보고서 변환 도구
 - 유니버스 디자인 도구
 - 웹 서비스 쿼리 도구(이전 이름: Query as a Web Service)
 - 정보 디자인 도구(이전 이름: 정보 디자이너)
 - 번역 관리 도구(이전 이름: Translation Manager)
 - SAP BusinessObjects Business Intelligence 플랫폼용 위젯(이전 이름: BI Widgets)
- 별도로 사용 가능한 클라이언트
 - SAP Crystal Reports

- SAP BusinessObjects Dashboard Design(이전 이름: Xcelsius)
- SAP BusinessObjects Analysis(이전 이름: Voyager)
- BI 작업 영역(이전 이름: Dashboard Builder)

IT 부서에서는 다음과 같은 데이터 및 시스템 관리 도구를 사용할 수 있습니다.

- 보고서 뷰어
- 중앙 관리 콘솔(CMC)
- 중앙 구성 관리자(CCM)
- 리포지토리 진단 도구(RDT)
- 데이터 연합 관리 도구
- 업그레이드 관리 도구(이전 이름: 가져오기 마법사)
- 유니버스 디자인 도구(이전 이름: Universe Designer)
- SAP BusinessObjects Mobile

유연성, 신뢰성 및 확장 가능성을 제공하기 위해 SAP BusinessObjects Business Intelligence 플랫폼 구성 요소를 하나 이상의 시스템에 설치할 수 있습니다. SAP BusinessObjects Business Intelligence 플랫폼의 서로 다른 두 버전을 같은 컴퓨터에 동시에 설치할 수도 있지만, 이러한 구성은 업그레이드 프로세스의 일부로 또는 테스트용으로만 권장됩니다.

서버 프로세스를 수직 확장하여 비용을 절감하거나 수평 확장하여 성능을 향상시킬 수 있습니다. 수직 확장은 컴퓨터 한 대에서 서버 측 프로세스를 여러 개 또는 모두 실행하는 경우를 말하고, 수평 확장은 네트워크로 연결된 둘 이상의 컴퓨터에 서버 프로세스를 분산시키는 것을 말합니다. 동일한 서버 프로세스의 여러 중복 버전을 둘 이상의 시스템에서 실행하여 기본 프로세스에 문제가 발생해도 처리를 계속하도록 할 수도 있습니다.

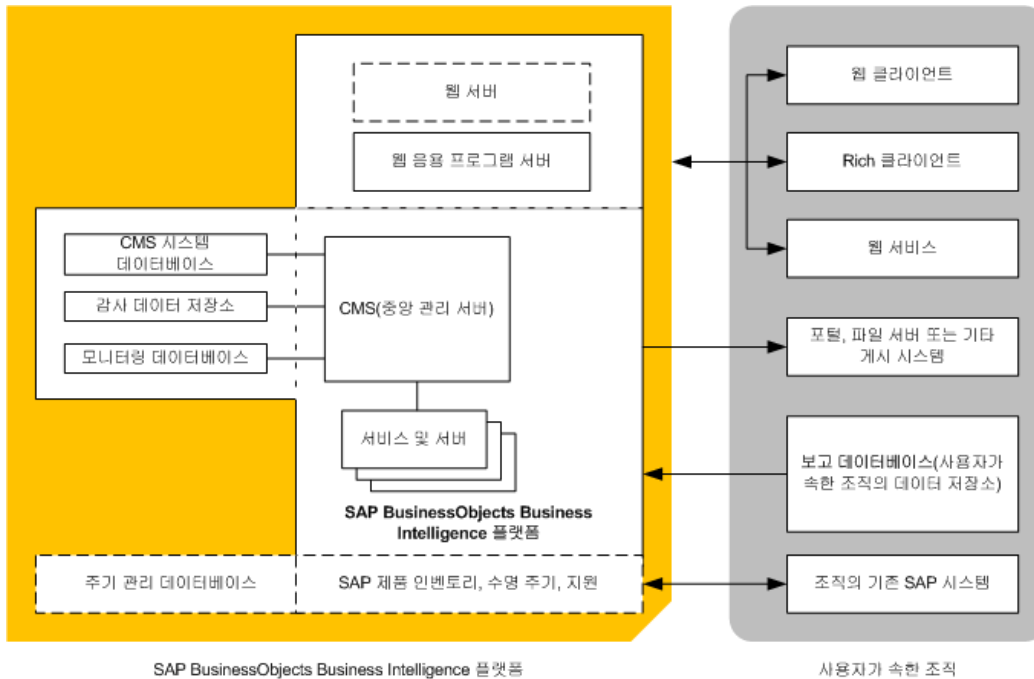
참고:

Windows 플랫폼과 Unix 또는 Linux 플랫폼을 혼합하여 사용할 수는 있지만 중앙 관리 서버(CMS) 프로세스에는 운영 체제를 혼합하여 사용하지 않는 것이 좋습니다.

2.1.1 시스템 개요

SAP BusinessObjects Business Intelligence 플랫폼은 엔터프라이즈 수준의 분석 및 보고 도구를 제공합니다. 지원되는 수많은 데이터베이스 시스템(텍스트 또는 다차원 OLAP 시스템 포함) 중 어떠한 시스템의 데이터도 분석할 수 있으며 BI 보고서를 다양한 형식으로 많은 수의 다양한 게시 시스템에 게시할 수 있습니다.

다음 그림에는 SAP BusinessObjects Business Intelligence 플랫폼과 조직의 인프라 간 관계가 나와 있습니다.



SAP BusinessObjects Business Intelligence 플랫폼은 읽기 전용 연결을 통해 조직의 데이터베이스로 데이터를 전송하며 자체 데이터베이스에 구성, 감사 및 기타 운영 정보를 저장합니다. 시스템에서 생성된 BI 보고서는 파일 시스템, 전자 메일 등의 다양한 대상으로 보내거나 웹 사이트 또는 포털을 통해 액세스할 수 있습니다.

SAP BusinessObjects Business Intelligence 플랫폼은 단일 시스템(예: 소규모 개발 또는 프로덕션 이전 테스트 환경)에 존재하거나 다양한 구성 요소(예: 대규모 프로덕션 환경)를 실행하는 많은 시스템 집합으로 범위를 확장할 수 있는 독립적인 시스템입니다.

2.1.2 데이터베이스

SAP BusinessObjects Business Intelligence 플랫폼은 다양한 여러 데이터베이스를 사용합니다.

- 보고 데이터베이스

조직의 정보를 의미합니다. 이러한 정보는 SAP BusinessObjects Business Intelligence 플랫폼에서 분석되어 보고된 소스 정보로, 보통은 관계형 데이터베이스 내에 저장되지만 텍스트 파일, Microsoft Office 문서 또는 OLAP 시스템에 포함될 수도 있습니다.

- CMS 시스템 데이터베이스

CMS 시스템 데이터베이스는 사용자, 서버, 폴더, 문서, 구성, 권한 부여, 인증 세부 정보와 같은 SAP BusinessObjects Business Intelligence 플랫폼 정보를 저장하는 데 사용됩니다. 중앙 관리 서버(CMS)에서 유지 관리하는 이 데이터베이스는 시스템 리포지토리라고도 합니다.

- 감사 데이터 저장소

감사 데이터 저장소(ADS)는 SAP BusinessObjects Business Intelligence 플랫폼에서 발생하는 추적 가능한 이벤트의 정보를 저장하는 데 사용됩니다. 이 정보는 시스템 구성 요소, 사용자 활동 또는 일일 작업의 다른 측면에 대한 용도를 모니터링하는 데 사용할 수 있습니다.

- 주기 관리 데이터베이스

주기 관리 데이터베이스는 SAP BusinessObjects Business Intelligence 플랫폼 설치뿐 아니라 업데이트와 관련된 구성 및 버전 정보를 추적합니다.

- 모니터링 데이터베이스

모니터링은 Java Derby 데이터베이스를 사용하여 시스템 구성 및 SAP 지원을 위한 구성 요소 정보를 저장합니다.

CMS 시스템 및 감사 데이터 저장소 데이터베이스와 함께 사용할 데이터베이스 서버가 없는 경우, SAP BusinessObjects Business Intelligence 플랫폼 설치 프로그램이 자동으로 설치하여 구성합니다. 데이터베이스 서버 공급업체에서 제공하는 정보를 조직의 요구 사항과 비교하여 지원되는 데이터베이스 중 어떤 데이터베이스가 자신의 조직에 가장 적합한지 따져보는 것이 좋습니다.

2.1.3 서버

SAP BusinessObjects Business Intelligence 플랫폼은 하나 이상의 호스트에서 실행되는 여러 서버로 구성되어 있습니다. 테스트 시스템이나 개발 시스템 같이 소규모 설치인 경우에는 웹 응용 프로그램 서버, 데이터베이스 서버 및 모든 SAP BusinessObjects Business Intelligence 플랫폼 서버에 하나의 호스트를 사용할 수 있습니다.

중간 규모 및 대규모 설치의 경우 여러 개의 호스트에서 여러 서버가 실행될 수 있습니다. 예를 들어 웹 응용 프로그램 서버 호스트를 SAP BusinessObjects Business Intelligence 플랫폼 서버 호스트와 함께 사용할 수 있습니다. 이렇게 하면 SAP BusinessObjects Business Intelligence 플랫폼 서버 호스트의 리소스에 여유가 생겨서 웹 응용 프로그램 서버를 동시에 호스트할 때보다 더 많은 정보를 처리할 수 있습니다.

대규모 설치의 경우 하나의 클러스터 내에서 여러 개의 SAP BusinessObjects Business Intelligence 플랫폼 서버 호스트가 함께 작동하도록 할 수 있습니다. 예를 들어 조직에 SAP Crystal Reports 사용자가 아주 많다면 Crystal Reports 처리 서버를 여러 SAP BusinessObjects Business Intelligence 플랫폼 서버 호스트에 만들어 여러 클라이언트에서 보내는 요청을 리소스 부족 없이 처리할 수 있습니다.

여러 개의 서버를 사용할 경우 얻게 되는 이점은 다음과 같습니다.

- 성능 향상

여러 개의 SAP BusinessObjects Business Intelligence 플랫폼 서버 호스트는 보고서 정보 대기열을 한 개의 SAP BusinessObjects Business Intelligence 플랫폼 서버 호스트보다 빨리 처리할 수 있습니다.

- 부하 분산

한 서버의 부하가 클러스터 내의 다른 서버보다 높을 경우 CMS에서 자동으로 새 작업을 보다 뛰어난 리소스를 보유한 서버로 전송합니다.

- 가용성 향상

서버에서 예상치 않은 상황이 발생할 경우 상황이 해결될 때까지 CMS에서 자동으로 작업을 다른 서버로 다시 라우팅합니다.

2.1.4 웹 응용 프로그램 서버

웹 응용 프로그램 서버는 웹 브라우저 또는 서식 있는 응용 프로그램과 SAP BusinessObjects Business Intelligence 플랫폼 사이에 변환 계층 역할을 합니다. Windows, Unix 및 Linux에서 실행되는 웹 응용 프로그램 서버가 지원됩니다.

다음 웹 응용 프로그램 서버가 지원됩니다.

- JBoss
- Oracle Application Server
- Sun Java System Application Server(Unix 전용)
- SAP NetWeaver AS Java
- Tomcat
- WebLogic
- WebSphere

지원되는 웹 응용 프로그램 서버의 세부 목록은 <http://service.sap.com/bosap-support>의 Supported Platforms Guide를 참조하십시오.

SAP BusinessObjects Business Intelligence 플랫폼과 함께 사용할 웹 응용 프로그램 서버가 없는 경우에는 설치 프로그램에서 Tomcat 6 웹 응용 프로그램 서버를 설치하여 구성합니다. 웹 응용 프로그램 서버 공급업체에서 제공하는 정보를 조직의 요구 사항과 비교하여 지원되는 웹 응용 프로그램 서버 중 어떤 서버가 해당 조직에 가장 적합한지 따져보는 것이 좋습니다.

참고:

운영 환경을 구성할 때는 웹 응용 프로그램 서버를 별도의 시스템에서 호스팅하는 것이 좋습니다. 운영 환경에서 SAP BusinessObjects Business Intelligence 플랫폼과 웹 응용 프로그램 서버를 같은 호스트에서 실행하면 성능이 저하될 수 있습니다.

2.1.4.1 WACS(웹 응용 프로그램 컨테이너 서비스)

SAP BusinessObjects Business Intelligence 플랫폼 웹 응용 프로그램을 호스팅하려면 웹 응용 프로그램 서버가 필요합니다.

고급 관리 업무를 수행하는 고급 Java 웹 응용 프로그램 서버 관리자라면 지원되는 Java 웹 응용 프로그램 서버를 사용하여 SAP BusinessObjects Business Intelligence 플랫폼 웹 응용 프로그램을 호스팅하십시오. 지원되는 Windows 운영 체제를 사용하여 SAP BusinessObjects Business Intelligence 플랫폼을 호스팅하며 단순 웹 응용 프로그램 서버 설치 프로세스를 선호하거나, Java 웹 응용 프로그램 서버를 관리할 리소스가 없는 경우 SAP BusinessObjects Business Intelligence 플랫폼을 설치할 때 웹 응용 프로그램 컨테이너 서비스(WACS)를 설치할 수 있습니다.

WACS는 Java 웹 응용 프로그램 서버가 설치되어 있지 않아도 중앙 관리 콘솔(CMC), BI 실행 패드 및 웹 서비스와 같은 SAP BusinessObjects Business Intelligence 플랫폼 웹 응용 프로그램을 실행할 수 있는 SAP BusinessObjects Business Intelligence 플랫폼 서버입니다.

WACS를 사용하면 다음과 같은 몇 가지 장점이 있습니다.

- 설치, 유지 관리 및 구성에 필요한 작업이 최소화됩니다. SAP BusinessObjects Business Intelligence 플랫폼 설치 프로그램을 통해 설치 및 구성되며 별도의 추가 단계 없이 실행을 시작할 수 있습니다.
- Java 응용 프로그램 서버 관리 및 유지 관리 기술이 없어도 됩니다.
- WACS는 다른 SAP BusinessObjects Business Intelligence 플랫폼 서버와 일관되는 관리 인터페이스를 제공합니다.
- 다른 SAP BusinessObjects Business Intelligence 플랫폼 서버처럼 WACS를 전용 호스트에 설치할 수 있습니다.

참고:

전용 Java 웹 응용 프로그램 서버 대신 WACS를 사용하는 데는 몇 가지 제한 사항이 있습니다.

- WACS는 지원되는 Windows 운영 체제에서만 사용할 수 있습니다.
- WACS에서는 SAP BusinessObjects Business Intelligence 플랫폼과 함께 설치된 웹 응용 프로그램만 지원되므로 사용자 지정 웹 응용 프로그램을 WACS에 배포할 수 없습니다.
- WACS는 Apache 부하 분산 장치와 함께 사용할 수 없습니다.

WACS 이외에도 전용 웹 응용 프로그램 서버를 사용할 수 있습니다. 따라서 전용 웹 응용 프로그램 서버를 사용하여 사용자 지정 웹 응용 프로그램을 호스팅할 수 있습니다. 반면 CMC 및 다른 SAP BusinessObjects Business Intelligence 플랫폼 웹 응용 프로그램은 WACS에 의해 호스팅됩니다.

2.1.5 소프트웨어 개발 키트

소프트웨어 개발 키트(SDK)를 통해 개발자는 SAP BusinessObjects Business Intelligence 플랫폼의 여러 특성을 조직의 자체 응용 프로그램과 시스템에 통합할 수 있습니다.

SAP BusinessObjects Business Intelligence 플랫폼에는 Java 플랫폼과 .NET 플랫폼의 소프트웨어 개발용 SDK가 있습니다.

참고:

SAP BusinessObjects Business Intelligence 플랫폼 .NET SDK는 기본적으로 설치되지 않으므로 SAP Service Marketplace에서 다운로드해야 합니다.

SAP BusinessObjects Business Intelligence 플랫폼에서 지원되는 SDK는 다음과 같습니다.

- SAP BusinessObjects Business Intelligence 플랫폼 Java SDK 및 .NET SDK

SAP BusinessObjects Business Intelligence 플랫폼 SDK를 통해 응용 프로그램에서 인증, 세션 관리, 리포지토리 개체 관련 작업, 보고서 예약 및 게시, 서버 관리 등의 작업을 수행할 수 있습니다.

참고:

보안, 서버 관리 및 감사 기능에 대한 전체 액세스 권한은 Java SDK를 사용하십시오.

- Report Application Server Java SDK 및 .NET SDK

Report Application Server SDK를 통해 응용 프로그램에서 매개 변수 값 설정, 데이터 소스 변경 및 XML, PDF, Microsoft Word, Microsoft Excel 등의 다른 형식으로 내보내기를 포함하여 기존 Crystal 보고서를 열고 만들고 수정할 수 있습니다.

- 보고서 엔진 Java SDK 및 .NET SDK

보고서 엔진 SDK를 사용하면 응용 프로그램과 SAP BusinessObjects Web Intelligence로 만든 보고서가 상호 작용할 수 있습니다.

보고서 엔진 SDK에는 웹 보고서 디자인 도구를 작성하는 데 사용할 수 있는 라이브러리가 포함되어 있습니다. 이 SDK로 제작한 응용 프로그램에서는 다양한 SAP BusinessObjects Web Intelligence 문서를 조회하거나 만들고 수정할 수 있습니다. 사용자는 테이블, 차트, 조건, 필터 등의 개체를 추가, 제거 및 변경하여 문서를 수정할 수 있습니다.

- 플랫폼 검색 SDK: 플랫폼 검색 SDK는 클라이언트 응용 프로그램과 플랫폼 검색 서비스를 연결하는 인터페이스입니다. 플랫폼 검색은 플랫폼 검색 SDK의 일부로 제공되는 공용 SDK를 지원합니다.

검색 요청 매개 변수가 클라이언트 응용 프로그램을 통해 SDK 계층으로 전송되면 SDK 계층은 요청 매개 변수를 XML 인코딩 형식으로 변환하여 플랫폼 검색 서비스로 전달합니다.

- Crystal Reports Viewer Java SDK 및 .NET SDK

Viewer SDK를 통해 응용 프로그램에서 Crystal 보고서를 표시하고 내보낼 수 있습니다. 사용 가능한 뷰어는 다음과 같습니다.

- DHTML 보고서 페이지 뷰어: 데이터를 표시하고 드릴다운, 페이지 탐색, 확대/축소, 프론트, 검색, 강조 표시, 내보내기 및 인쇄를 수행할 수 있습니다.
- 부분 보고서 뷰어: 차트, 텍스트 및 필드를 포함하여 보고서의 개별 부분을 볼 수 있습니다.

- 뷰어 태그 라이브러리: JSP 페이지에서 뷰어의 동작을 사용자 지정할 수 있습니다.
- SAP BusinessObjects Business Intelligence 플랫폼 Java 소비자 SDK 및 .NET 소비자 SDK
웹 서비스 구현을 통해 사용자는 사용자 인증 및 보안, 문서 및 보고서 액세스, 예약, 게시 및 서버 관리를 처리할 수 있습니다.

참고:

SAP BusinessObjects Business Intelligence 플랫폼 JavaServer Faces 구성 요소는 더 이상 사용되지 않습니다.

광범위한 BI 기능을 응용 프로그램에 제공하기 위해 SDK를 조합해서 사용할 수 있습니다. 예를 들어, SAP BusinessObjects Business Intelligence 플랫폼에 포함된 BI 실행 패드 웹 응용 프로그램은 이러한 SDK를 사용하여 작성되었습니다.

SAP BusinessObjects Business Intelligence 플랫폼 SDK에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence Platform SDK Developer Guide, Report Application Server Java SDK 개발자 가이드, Report Application Server .NET SDK Developer Guide 및 뷰어 Java SDK 개발자 가이드(<http://service.sap.com/bosap-support>)를 참조하십시오.

2.1.5.1 웹 서비스 Java 및 .NET 소비자 SDK

SAP BusinessObjects Business Intelligence 플랫폼 웹 서비스 Java 및 .NET 소비자 SDK를 통해 사용자는 SAP BusinessObjects Business Intelligence 플랫폼 기능을 활용하는 분산 웹 서비스 응용 프로그램을 만들 수 있습니다.

웹 서비스는 SOAP(Simple Object Access Protocol)를 사용하여 원격으로 호출할 수 있는 소프트웨어 구성 요소로 이루어져 있습니다. SOAP는 특정 플랫폼, 개체 모델 또는 프로그래밍 언어에 종속되지 않으며 정보를 교환하는 프로토콜입니다.

SAP BusinessObjects Business Intelligence 플랫폼 웹 서비스에는 다음과 같은 영역의 기능이 포함되어 있습니다.

- 세션
인증 및 사용자 관리
- BI 플랫폼
예약, 게시, 검색, 사용자 및 그룹 관리, 서버 관리 서버 등의 고급 플랫폼 기능을 표시합니다.
- 보고서 엔진
SAP BusinessObjects Business Intelligence Solution과 Crystal Reports를 HTML, PDF, Excel 및 XML 형식으로 표시합니다.
- 쿼리
유니버스 의미 계층을 기반으로 임시 쿼리를 작성합니다.

SAP BusinessObjects Business Intelligence 플랫폼 웹 서비스에는 XML, SOAP, AXIS 2.0, WSDL 등의 표준이 사용됩니다. 플랫폼은 WS-Interoperability Basic Profile 1.0 웹 서비스 사양을 따릅니다.

참고:

웹 서비스 응용 프로그램은 현재 다음의 부하 분산 장치 구성에서만 지원됩니다.

1. 소스 IP 주소 지속성
2. 소스 IP 및 대상 포트 지속성(Cisco Content Services Switch에서만 사용 가능)
3. SSL 지속성.

참고:

SSL 지속성으로 인해 일부 웹 브라우저에서 보안 및 신뢰성 문제가 발생할 수 있습니다. SSL 지속성이 사용자 조직에 적절한지 여부를 판별하려면 네트워크 관리자에게 문의하십시오.

2.1.5.2 웹 서비스 쿼리 도구

웹 서비스 쿼리 도구는 쿼리를 웹 서비스로 만들어 웹을 사용하는 응용 프로그램에 통합할 수 있도록 해 주는 마법사 기반 응용 프로그램입니다. 쿼리를 저장하여 표준 쿼리의 카탈로그를 만들고 응용 프로그램 작성기에서 필요에 따라 이를 선택할 수 있습니다.

Business Intelligence(BI) 콘텐츠는 일반적으로 BI 도구의 특정 사용자 인터페이스에 바인딩됩니다. 하지만 웹 서비스 쿼리 도구의 경우에는 웹 서비스 처리가 가능한 어느 사용자 인터페이스에나 BI 콘텐츠를 전달할 수 있습니다.

웹 서비스 쿼리 도구는 모든 Microsoft Windows 응용 프로그램에서 다른 웹 서비스와 동일하게 작동하도록 만들어졌습니다. Query as a Web Service는 W3C 웹 서비스 지정 SOAP, WSDL 및 XML을 기반으로 합니다. 이 프로그램은 다음 두 가지 주요 구성 요소로 이루어져 있습니다.

- 서버 구성 요소

서버 구성 요소(SAP BusinessObjects Business Intelligence 플랫폼에 포함)는 웹 서비스 쿼리 도구 카탈로그를 저장하고 게시된 웹 서비스를 호스팅합니다.

- 클라이언트 도구

비즈니스 사용자가 쿼리를 웹 서비스로 만들어 서버에 게시하는 데 사용하는 도구입니다. 서버에 저장된 동일한 웹 서비스 쿼리 도구 카탈로그에 액세스하여 이를 공유하는 여러 컴퓨터에 클라이언트 도구를 설치할 수 있습니다. 클라이언트 도구는 웹 서비스를 통해 서버 구성 요소와 통신합니다.

웹 서비스 쿼리 도구를 통해 웹 쿼리를 다음과 같은 여러 클라이언트측 솔루션의 일부로 사용할 수 있습니다.

- Microsoft Office, Excel 및 InfoPath
- SAP NetWeaver

- OpenOffice
- 비즈니스 규칙 및 프로세스 관리 응용 프로그램
- 엔터프라이즈 서비스 버스 플랫폼

2.1.6 데이터 소스

2.1.6.1 유니버스

유니버스는 데이터 언어가 아닌 비즈니스 언어를 사용하여 데이터에 액세스하고 데이터를 조작 및 구성하는 방식으로 데이터의 복잡한 구조를 추상화합니다. 이 비즈니스 언어는 유니버스 파일에 개체로 저장됩니다. Web Intelligence와 Crystal Reports에서는 복잡한 최종 사용자 쿼리 및 분석을 간소화하는 데 필요한 사용자 작성 프로세스를 단순화하기 위해 유니버스를 사용합니다.

유니버스는 SAP BusinessObjects Business Intelligence 플랫폼의 핵심 구성 요소입니다. 모든 유니버스 개체 및 연결은 연결 서버를 통해 중앙 리포지토리에 저장되고 보호됩니다. 유니버스 디자인 도구에서 시스템에 액세스하고 유니버스를 만들려면 SAP BusinessObjects Business Intelligence 플랫폼에 로그인해야 합니다. 유니버스 액세스 및 하위 수준 보안을 디자인 환경 내에서 그룹 또는 개별 사용자 수준으로 관리할 수도 있습니다.

의미 계층을 통해 SAP BusinessObjects Web Intelligence는 OLAP(Online Analytical Processing) 및 CWM(Common Warehouse Metamodel) 데이터 소스 등 여러 개의 동기화된 데이터 공급자를 사용하여 문서를 전달할 수 있습니다.

2.1.6.2 비즈니스 뷰

비즈니스 뷰는 보고서 개발자를 위해 복잡한 데이터를 추상화하여 보고서 작성 및 상호 작용을 간소화합니다. 비즈니스 뷰를 사용하면 데이터 연결, 데이터 액세스, 비즈니스 요소 및 액세스 제어를 쉽게 분리할 수 있습니다.

비즈니스 뷰는 Crystal Reports에서만 사용할 수 있으며 Crystal 보고서 작성에 필요한 데이터 액세스 및 뷰 타임 보안을 간소화할 수 있도록 디자인되었습니다. 비즈니스 뷰를 사용하면 여러 데이터 소스를 한 개의 뷰로 결합할 수 있습니다. SAP BusinessObjects Business Intelligence 플랫폼에서는 비즈니스 뷰의 모든 기능을 지원합니다.

SAP BusinessObjects Business Intelligence 플랫폼에는 암호 관리, 서버 메트릭 및 사용자 액세스 제어 등의 작업을 위해 미리 구성된 일련의 전용 플랫폼 관리 서비스가 포함되어 있으므로 관리 기능을 분산하여 사용할 수 있습니다.

2.1.7 언어 지원

SAP BusinessObjects Business Intelligence 플랫폼 제품은 다양한 언어로 번역되고 보다 다양한 언어로 데이터를 지원합니다.

제품 인터페이스는 다음 언어로 이용할 수 있습니다.

- 체코어
- 중국어 간체
- 중국어 번체
- 덴마크어
- 네덜란드어
- 영어
- 핀란드어
- 프랑스어
- 독일어
- 이탈리아어
- 일본어
- 한국어
- 노르웨이어(북말)
- 폴란드어
- 포르투갈어
- 러시아어
- 스페인어
- 스웨덴어
- 태국어

인터페이스에서 사용할 수 있는 언어로 데이터를 지원하는 것 외에도 다음 문자 집합이 지원됩니다.

- 그리스어
- 말레이어
- 히브리어
- 아랍어

- 루마니아어
- 베트남어
- 헝가리어
- 터키어
- 힌디어

2.1.8 인증 및 단일 로그인

시스템 보안은 중앙 관리 서버(CMS), 보안 플러그 인 및 타사 인증 도구(예: SiteMinder 또는 Kerberos)를 사용하여 관리됩니다. 이러한 구성 요소에서는 사용자를 인증하고 사용자에게 SAP BusinessObjects Business Intelligence 플랫폼, 관련 폴더 및 기타 개체에 대한 액세스 권한을 부여합니다.

사용 가능한 사용자 인증 단일 로그인 보안 플러그 인은 다음과 같습니다.

- Enterprise(기본값) - 타사 인증을 위한 신뢰할 수 있는 인증 지원 포함
- LDAP
- Windows AD(Active Directory)

ERP(Enterprise Resource Planning) 시스템을 사용하는 경우 ERP 데이터에 대한 보고서가 생성될 수 있도록 단일 로그인을 사용하여 ERP 시스템에 대한 사용자 액세스를 인증합니다. ERP 시스템에 대해 지원되는 사용자 인증 단일 로그인은 다음과 같습니다.

- SAP ERP 및 Business Warehouse(BW)
- Oracle E-Business Suite(EBS)
- Siebel Enterprise
- JD Edwards Enterprise One
- PeopleSoft Enterprise

2.1.8.1 보안 플러그 인

보안 플러그 인을 사용하면 타사 시스템의 사용자 계정과 그룹을 SAP BusinessObjects Business Intelligence 플랫폼에 매핑할 수 있으므로 계정을 만들고 관리하는 작업을 자동으로 수행할 수 있습니다. 타사 사용자 계정 또는 그룹을 기존의 Enterprise 사용자 계정 또는 그룹에 매핑하거나, 외부 시스템에서 매핑되는 각 항목에 해당하는 Enterprise 사용자 계정 또는 그룹을 새로 만들 수 있습니다.

보안 플러그 인은 타사 사용자 및 그룹 목록을 동적으로 관리합니다. 따라서 LDAP(Lightweight Directory Access Protocol) 또는 Windows AD(Active Directory) 그룹을 SAP BusinessObjects

Business Intelligence 플랫폼에 매핑하면 해당 그룹에 속한 모든 사용자가 SAP BusinessObjects Business Intelligence 플랫폼에 로그인할 수 있습니다. 타사 소속 그룹에 대한 이후 변경 사항은 자동으로 전파됩니다.

SAP BusinessObjects Business Intelligence 플랫폼은 다음과 같은 보안 플러그인을 지원합니다.

- Enterprise 보안 플러그인

중앙 관리 서버(CMS)에서는 사용자 계정, 소속 그룹 및 사용자와 그룹 권한을 정의하는 개체 권한 같은 보안 정보를 처리합니다. 이를 Enterprise 인증이라고 합니다.

Enterprise 인증은 항상 활성화되어 있으며 비활성화할 수 없습니다. SAP BusinessObjects Business Intelligence 플랫폼에 사용할 고유한 계정 및 그룹을 만들어야 하는 경우 또는 LDAP 또는 Windows AD 서버에서 아직 사용자 및 그룹 계층을 설정하지 않은 경우에는 시스템 기본값인 Enterprise 인증을 사용하십시오.

신뢰할 수 있는 인증은 Java 인증 및 권한 부여 서비스(JAAS)와 같은 타사 단일 로그인 솔루션과 통합되는 Enterprise 인증의 한 구성 요소입니다. 중앙 관리 서버에 대한 신뢰가 설정된 응용 프로그램에서는 신뢰할 수 있는 인증을 사용하여 사용자가 암호를 입력하지 않고 로그인할 수 있습니다.

- LDAP 보안 플러그인
- Windows AD

참고:

사용자가 CMC를 통해 SAP BusinessObjects Business Intelligence 플랫폼 및 사용자 지정 응용 프로그램에 대해 Windows AD 인증을 구성할 수는 있지만 CMC와 BI 실행 패드 자체는 NTLM을 사용한 Windows AD 인증을 지원하지 않습니다. CMC와 BI 실행 패드는 Kerberos, LDAP, Enterprise 및 신뢰할 수 있는 인증과 함께 사용되는 Windows AD 인증 방법만 지원합니다.

2.1.8.2 ERP(Enterprise Resource Planning) 통합

ERP(Enterprise Resource Planning) 응용 프로그램은 일상의 업무와 관련된 실시간 정보를 수집하여 조직의 프로세스에서 필수적인 기능을 지원합니다. SAP BusinessObjects Business Intelligence 플랫폼은 다음 ERP 시스템에서 단일 로그인 및 보고 기능을 지원합니다.

- SAP ERP 및 Business Warehouse(BW)

참고:

ODA(OLAP Data Access), SAP BusinessObjects Analysis(이전 이름: Voyager) 또는 BW 연결을 사용하려면 먼저 SAP GUI를 설치해야 합니다.

- Siebel Enterprise
- Oracle E-Business Suite
- JD Edwards EnterpriseOne
- PeopleSoft Enterprise

참고:

- SAP ERP 및 BW 지원은 기본적으로 설치됩니다. SAP ERP 또는 BW에 대한 지원이 필요하지 않은 경우 사용자 지정/확장 설치 옵션을 사용하여 SAP 통합 지원을 선택 취소하십시오.
- Siebel Enterprise, Oracle E-Business Suite, JD Edwards EnterpriseOne 또는 PeopleSoft에 대한 지원은 기본적으로 설치되지 않습니다. 사용자 지정/확장 설치 옵션을 사용하여 SAP ERP 시스템 이외의 시스템에 대한 통합을 선택 및 설치하십시오.

SAP BusinessObjects Business Intelligence 플랫폼에서 지원하는 특정 버전에 대한 자세한 내용은 Supported Platforms Guide(service.sap.com/bosap-support)를 참조하십시오.

ERP 통합을 구성하려면 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드를 참조하십시오.

2.1.9 SAP 통합

SAP BusinessObjects Business Intelligence 플랫폼은 다음 SAP 도구를 사용하여 기존 SAP 인프라와 통합합니다.

- SAP System Landscape Directory(SLD)

SAP NetWeaver의 시스템 랜즈케이프 디렉터리는 소프트웨어 수명 주기 관리와 관련된 시스템 랜즈케이프 정보의 중심 소스입니다. SAP에서 사용 가능한 모든 설치 가능 소프트웨어 관련 정보로 구성된 디렉터리와 랜즈케이프에 이미 설치된 시스템에 대해 자동으로 업데이트된 데이터를 제공함으로써 사용자는 시스템 랜즈케이프에서 소프트웨어 수명 주기 작업을 계획하기 위한 도구 지원 기반을 마련합니다.

SAP BusinessObjects Business Intelligence 플랫폼 설치 프로그램은 서버와 프론트 엔드 구성 요소 이름, 버전 및 위치를 비롯하여 공급업체, 제품 이름 및 버전을 SLD에 등록합니다.

- SAP Solution Manager

SAP Solution Manager는 조직의 SAP 및 타사 솔루션을 구현, 지원, 운영 및 모니터링하기 위해 사용하는 통합된 콘텐츠, 도구 및 방법론을 제공하는 플랫폼입니다.

SAP 인증 통합을 사용하는 타사 소프트웨어는 중앙 리포지토리에 입력되며 SAP System Landscape Directories(SLD)로 자동 전송됩니다. 그러면 SAP 고객이 어떤 버전의 타사 제품 통합이 SAP 시스템 환경 내에서 SAP에 의해 인증되었는지 쉽게 식별할 수 있습니다. 따라서 이 서비스를 통해 SAP의 타사 제품 온라인 카탈로그 외에도 타사 제품을 확인할 수 있습니다.

SAP 고객에게는 SAP Solution Manager를 추가 요금 없이 제공하며, 여기에는 SAP 지원 및 SAP 제품 업그레이드 경로 정보에 대한 직접 액세스가 포함됩니다. SLD에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드에서 시스템 랜즈케이프에 SAP BusinessObjects Business Intelligence 플랫폼 등록을 참조하십시오.

- CTS 전송(CTS+)

CTS(Change and Transport System)는 ABAP Workbench 및 Customizing에서 개발 프로젝트를 구성한 다음 시스템 란드스케이프에서 SAP 시스템 간에 변경 내용을 전송하도록 지원합니다. 또한 란드스케이프에서 ABAP 개체를 비롯하여 Java 개체(J2EE, JEE)와 SAP별 비ABAP 기술(Web Dynpro Java 또는 SAP NetWeaver Portal)을 전송할 수 있습니다.

- CA Wily Introscope를 통한 모니터링

CA Wily Introscope는 사용자 지정 Java 응용 프로그램의 표시 유형과 백엔드 시스템으로의 연결을 포함하여 생산 시 Java 기반 SAP 모듈에서 발생할 수 있는 성능 문제를 모니터링하고 진단하는 기능을 제공하는 웹 응용 프로그램 관리 제품입니다. CA Wily Introscope를 통해 사용자는 개별 서블릿, JSP, EJB, JCO, 클래스, 메소드 등을 포함하는 NetWeaver 모듈에서 성능 병목 현상을 제거할 수 있습니다. CA Wily Introscope는 낮은 오버헤드 모니터링, 중단 간 트랜잭션 표시 유형, 분석 또는 용량 계획을 위한 기록 데이터, 사용자 지정 가능한 대시보드, 자동화된 임계값 경고 및 개방형 아키텍처를 실시간으로 제공하여 NetWeaver 환경 외부로 모니터링을 확장합니다.

2.1.10 주기 관리(LCM)

주기 관리(LCM)는 설치 제품 정보를 관리하는 것과 관련된 일련의 프로세스를 의미하며, 개발, 테스트, 프로덕션 또는 유지 관리 환경에 대한 SAP BusinessObjects Business Intelligence 플랫폼 설치 관리 절차를 수립합니다.

SAP BusinessObjects Business Intelligence 플랫폼 Lifecycle Manager는 사용자가 BI 개체의 종속성에 영향을 주지 않으면서 해당 개체를 한 시스템에서 다른 시스템으로 이동할 수 있도록 지원하는 웹 기반 도구입니다. 또한 이 도구를 사용하면 여러 개의 버전 및 종속성을 관리할 수 있으며 승격된 개체를 이전 상태로 롤백할 수도 있습니다.

LCM 도구는 SAP BusinessObjects Business Intelligence 플랫폼용 플러그 인입니다. 소스 시스템과 대상 시스템 동일한 버전의 응용 프로그램이 설치되어 있는 경우에만 BI 개체를 한 시스템에서 다른 시스템으로 승격시킬 수 있습니다.

자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 4.0용 주기 관리 콘솔 사용자 가이드를 참조하십시오.

2.1.11 통합 버전 제어

서버 시스템에서 SAP BusinessObjects Business Intelligence 플랫폼을 구성하는 파일이 지금은 버전 제어 대상으로 관리됩니다. 설치 프로그램이 Subversion 버전 제어 시스템을 설치하고 구성하거

나, 사용자가 세부 정보를 입력하여 기존 Subversion 또는 Clearcase 버전 제어 시스템을 사용할 수 있습니다.

버전 제어 시스템을 통해 구성의 다른 수정 버전과 다른 파일을 유지 및 복원할 수 있는데, 이는 과거 어느 시점의 알려진 상태로도 시스템을 항상 되돌릴 수 있음을 의미합니다.

2.1.12 영구 데이터

"영구 데이터"라는 용어는 시스템 업그레이드 중에 마이그레이션할 가치가 있는 중요한 정보를 의미합니다. 예를 들어, 중앙 관리 서버(CMS)는 구성 정보를 Windows 레지스트리 또는 구성 파일이 아닌 CMS 데이터베이스에 저장합니다.

모든 SAP BusinessObjects Business Intelligence 플랫폼 제품은 CMS 시스템 데이터베이스에 영구 데이터를 저장합니다. 따라서 업그레이드하는 경우 데이터와 구성 정보를 새 버전으로 쉽게 마이그레이션할 수 있습니다.

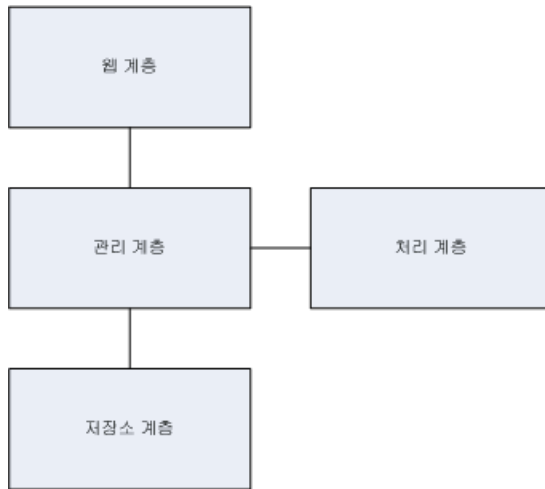
2.1.13 업그레이드 경로

SAP BusinessObjects Business Intelligence 플랫폼 이전 릴리즈에서는 업그레이드할 수 없으므로 먼저 SAP BusinessObjects Business Intelligence 플랫폼 4.0을 설치한 다음, 업그레이드 관리 도구를 사용하여 기존 시스템에서 설정 및 데이터를 마이그레이션하십시오.

이전 버전에서 업그레이드하는 방법은 SAP BusinessObjects Business Intelligence 플랫폼 업그레이드 가이드를 참조하십시오.

2.2 개념적 계층

SAP BusinessObjects Business Intelligence 플랫폼은 일련의 개념적 계층으로 생각할 수 있습니다.



- 웹 계층

웹 계층에는 Java 웹 응용 프로그램 서버에 배포된 웹 응용 프로그램이 있습니다. 웹 응용 프로그램은 웹 브라우저를 통해 최종 사용자에게 SAP BusinessObjects Business Intelligence 플랫폼 기능을 제공합니다. 웹 응용 프로그램의 예로는 중앙 관리 콘솔(CMC) 관리 웹 인터페이스, BI 실행 패드 등이 있습니다.

웹 계층에는 웹 서비스도 포함됩니다. 웹 서비스는 웹 응용 프로그램 서버를 통해 소프트웨어 도구에 세션 인증, 사용자 권한 관리, 예약, 검색, 관리, 보고서 작성 및 쿼리 관리 등의 SAP BusinessObjects Business Intelligence 플랫폼 기능을 제공합니다. 예를 들어 Live Office는 웹 서비스를 통해 SAP BusinessObjects Business Intelligence 플랫폼 보고 기능을 Microsoft Office 제품에 통합하는 제품입니다.

- 관리 계층

관리 계층에서는 SAP BusinessObjects Business Intelligence 플랫폼의 모든 구성 요소를 조직하고 관리합니다. 관리 계층은 중앙 관리 서버(CMS)와 이벤트 서버로 구성됩니다. CMS에서는 보안과 구성 정보를 유지하고 서버에 서비스 요청을 보내며 감사 관리, CMS 시스템 데이터베이스 유지 관리를 수행합니다. 이벤트 서버는 저장소 계층에서 발생하는 파일 기반 이벤트를 관리합니다.

- 처리 계층

처리 계층은 데이터를 분석하고 보고서를 만들어냅니다. 보고서 데이터가 있는 데이터베이스에 액세스하는 유일한 계층입니다.

- 저장소 계층

저장소 계층은 문서, 보고서 등의 파일을 처리합니다.

입력 파일 리포지토리 서버는 보고서에 사용할 정보가 들어가는 파일을 관리합니다. 관리되는 파일 형식은 .rpt, .car, .exe, .bat, .js, .xls, .doc, .ppt, .rtf, .txt, .pdf, .wid, .rep, .unv 등입니다.

출력 파일 리포지토리 서버는 시스템이 만든 보고서를 관리합니다. 관리되는 파일 형식은 .rpt, .csv, .xls, .doc, .rtf, .txt, .pdf, .wid, .rep 등입니다.

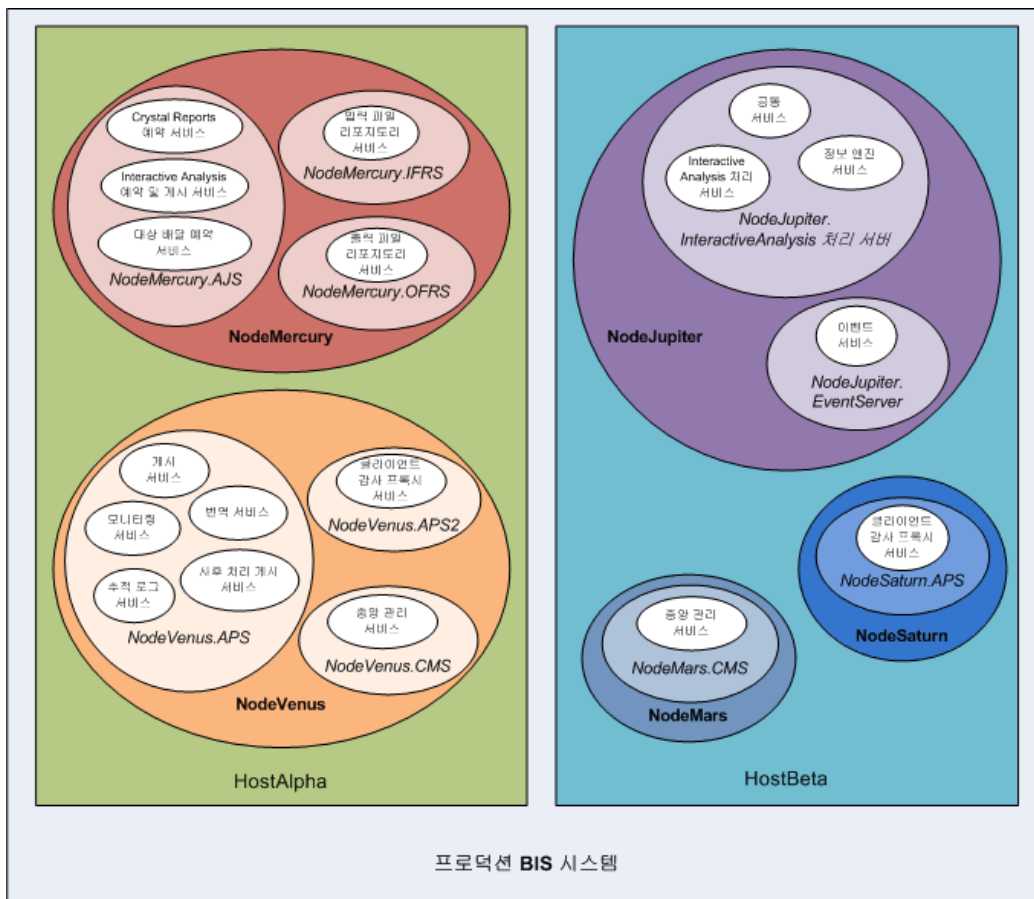
저장소 계층은 사용자가 보고서에 액세스할 때 시스템 리소스를 저장하는 보고서 캐싱도 처리합니다.

2.3 서비스 및 서버

다음 그림에서 BI 플랫폼의 가상 설치를 볼 수 있습니다.

참고:

노드, 서버 및 서비스는 예시용으로만 표시되었습니다. 서버와 서비스의 종류 뿐 아니라 호스트, 노드, 서버 및 서비스의 수는 실제 설치 시 달라질 수 있습니다.



아래에 설명된 두 개의 호스트가 ProductionBISystem이라는 클러스터를 구성합니다.

- HostAlpha라는 호스트에 BI 플랫폼이 설치되어 있고 다음 두 개의 노드를 포함하도록 구성됩니다.
 - NodeMercury: 보고서 예약 및 게시 서비스를 제공하는 적응형 작업 서버(NodeMercury.AJS), 입력 보고서를 저장하는 서비스를 제공하는 입력 파일 리포지토리 서버(NodeMercury.IFRS), 보고서 출력을 저장하는 서비스를 제공하는 출력 파일 리포지토리 서버(NodeMercury.OFRS)로 구성됩니다.

- NodeVenus: 게시, 모니터링 및 변환 기능 서비스를 제공하는 적응형 처리 서버(NodeVenus.APS), 클라이언트 감사 서비스를 제공하는 적응형 처리 서버(NodeVenus.APS), CMS 서비스를 제공하는 중앙 관리 서버(NodeVenus.CMS)로 구성됩니다.
- 이름이 HostBeta인 호스트에는 BI 플랫폼이 설치되어 있고 다음 세 개의 노드를 포함하도록 구성됩니다.
 - NodeMars: CMS 서비스를 제공하는 중앙 관리 서버(NodeMars.CMS)로 구성됩니다.
 - NodeJupiter: Web Intelligence 보고 서비스를 제공하는 Web Intelligence 처리 서버(NodeJupiter.Web Intelligence), 파일의 보고서 모니터링 서비스를 제공하는 이벤트 서버(NodeJupiter.EventServer)로 구성됩니다.
 - NodeSaturn: 클라이언트 감사 서비스를 제공하는 적응형 처리 서버(NodeSaturn.APS)로 구성됩니다.

BI 플랫폼은 BI 플랫폼 컴퓨터에서 실행되는 두 가지 유형의 소프트웨어를 칭하는 말로 서버와 서비스라는 용어를 사용합니다.

서비스는 특정 기능을 수행하는 서버 하위 시스템입니다. 서비스는 부모 컨테이너(서버)의 프로세스 id로 서버의 메모리 공간 내에서 실행됩니다. 예를 들어 SAP BusinessObjects Web Intelligence 예약 및 게시 서비스는 적응형 작업 서버 안에서 실행되는 하위 시스템입니다.

서버라는 용어는 하나 이상의 서비스를 호스팅하는 운영 체제 수준 프로세스(일부 컴퓨터에서는 데몬이라고도 함)를 설명하는 데 사용됩니다. 예를 들어 중앙 관리 서버(CMS)와 적응 처리 서버는 서버입니다. 서버는 특정 운영 체제 계층에서 실행되고 자체 PID를 갖습니다.

노드는 동일한 호스트에서 실행되는 BI 플랫폼 서버의 컬렉션입니다. 단일 호스트에 하나 이상의 노드가 있을 수 있습니다.

BI 플랫폼을 단일 컴퓨터에 설치하거나 인트라넷에 있는 다른 컴퓨터에 배포하거나 또는 WAN(Wide Area Network)을 통해 배포할 수 있습니다.

2.3.1 서비스

다음 표에 각 서비스에 대한 설명이 나와 있습니다.

테이블2-1: 서비스

서비스	서비스 범주	서버 유형	서비스 설명
적응형 연결 서비스	연결 서비스	적응형 처리 서버	연결 서비스를 제공합니다(연결 서버를 대체함).

서비스	서비스 범주	서버 유형	서비스 설명
인증 업데이트 예약 서비스	핵심 서비스	적응형 작업 서버	타사 보안 플러그 인에 대한 업데이트 동기화를 제공합니다.
BEx 웹 응용 프로그램 서비스	연결 서비스	적응형 처리 서버	BI 실행 패드와 SAP Business Warehouse(BW) Business Explorer(BEx) 웹 응용 프로그램과의 통합을 제공합니다.
BOE 웹 응용 프로그램 서비스	핵심 서비스	웹 응용 프로그램 컨테이너 서버	WACS용 웹 응용 프로그램 제공: 중앙 관리 콘솔(CMC), BI 실행 패드, Open Document가 포함됩니다.
Business Process BI 서비스	핵심 서비스	웹 응용 프로그램 컨테이너 서버	WACS용 Business Process BI 웹 서비스를 제공하며, BI 기술을 웹 응용 프로그램에 통합할 수 있습니다. Business Process BI 서비스는 더 이상 사용되지 않습니다.
중앙 관리 서비스	핵심 서비스	중앙 관리 서버	서버, 사용자, 세션 관리 및 보안(권한 부여 및 인증) 관리를 제공합니다. 클러스터가 작동하려면 적어도 하나의 중앙 관리 서비스를 클러스터에서 사용할 수 있어야 합니다.
클라이언트 감사 프록시 서비스	핵심 서비스	적응형 처리 서버	클라이언트에서 보낸 감사 이벤트를 수집하여 CMS 서버로 전달합니다.
Crystal Reports 2011 처리 서비스	Crystal Reports 서비스	Crystal Reports 처리 서버	Crystal Report 2011 보고서를 허용하고 처리하며, 보고서 간에 데이터를 공유하여 데이터베이스 액세스 횟수를 줄일 수 있습니다.

서비스	서비스 범주	서버 유형	서비스 설명
Crystal Report 2011 예약 서비스	Crystal Reports 서비 스	적응형 작업 서버	예약된 레거시 Crystal Reports 작업을 실행하 여 그 결과를 지정된 출 력 위치에 게시합니다.
Crystal Reports 2011 보기 및 수정 서비스	Crystal Reports 서비 스	RAS	RAS(Report Applica- tion Server)
Crystal Reports 캐시 서비스	Crystal Reports 서비 스	Crystal Reports 캐시 서버	Crystal Reports에서 생성된 데이터베이스 액세스 수를 제한하며 보고서 캐시를 관리하 여 보고 속도를 높입니 다.
Crystal Reports 처리 서비스	Crystal Reports 서비 스	Crystal Reports 처리 서버	Crystal 보고서를 허용 및 처리하며, 보고서 간 에 데이터를 공유하여 데이터베이스 액세스 수를 줄일 수 있습니다.
Crystal Reports 예약 서비스	Crystal Reports 서비 스	적응형 작업 서버	예약된 새 Crystal Re- ports 작업을 실행하여 그 결과를 지정된 출력 위치에 게시합니다.
사용자 지정 데이터 액 세스 서비스	연결 서비스	적응형 처리 서버	연결 서버가 필요하지 않은 데이터 소스에 동 적 연결을 제공합니다.
대시보드 분석 서비스	핵심 서비스	대시보드 분석 서버	데이터 분석을 위해 BI 작업 영역 및 모듈 기능 을 제공합니다.
Dashboard Design 캐 시 서비스	Dashboard Design 서 비스	Dashboard Design 캐 시 서버	Dashboard Design 보 고서에서 생성된 데이 터베이스 액세스 수를 제한하며 보고서 캐시 를 관리하여 보고 속도 를 높입니다.
Dashboard Design 처 리 서비스	Dashboard Design 서 비스	Dashboard Design 처 리 서버	Dashboard Design 보 고서를 허용 및 처리하 며, 보고서 간에 데이 터를 공유하여 데이터베 이스 액세스 수를 줄일 수 있습니다.

서비스	서비스 범주	서버 유형	서비스 설명
대시보드 서비스	핵심 서비스	대시보드 서버	BI 작업 영역 지원입니다.
데이터 연합 서비스	데이터 연합 서비스	적응형 처리 서버	데이터 연합 서비스입니다.
대상 배달 예약 서비스	핵심 서비스	적응형 작업 서버	예약된 작업을 실행하여 그 결과를 지정된 출력 위치(예: 파일 시스템, FTP, 전자 메일 또는 사용자의 받은 파일함)에 게시합니다.
문서 복구 서비스	Web Intelligence 서비스	적응형 처리 서버	Web Intelligence 문서 자동 저장 및 복구
DSL Bridge Service	Web Intelligence 서비스	적응형 처리 서버	이중 의미 계층(DSL) 세션을 지원합니다.
이벤트 서비스	핵심 서비스	이벤트 서버	파일 리포지토리 서버(FRS)에 대한 파일 이벤트를 모니터링하고 필요 시 실행할 보고서를 트리거합니다.
외부 데이터 액세스 서비스	연결 서비스	적응형 처리 서버	SAP BusinessObjects Business Intelligence 플랫폼에 업로드된 Excel 파일을 데이터 소스로 지원합니다.
정보 엔진 서비스	Web Intelligence 서비스	Web Intelligence 처리 서버	Web Intelligence 문서 처리에 필요한 서비스
Input Filestore 서비스	핵심 서비스	입력 파일 리포지토리 서버	입력 파일을 수신할 때 새 보고서 생성에 사용할 수 있는 게시된 보고서 및 프로그램 개체를 유지 관리합니다.
Web Intelligence 공통 서비스	Web Intelligence 서비스	Web Intelligence 처리 서버	Web Intelligence 문서 처리를 지원합니다.
Web Intelligence 핵심 서비스	Web Intelligence 서비스	Web Intelligence 처리 서버	Web Intelligence 문서 처리를 지원합니다.
Web Intelligence 모니터링 서비스	Web Intelligence 서비스	적응형 처리 서버	Web Intelligence 서버를 모니터링합니다.

서비스	서비스 범주	서버 유형	서비스 설명
Web Intelligence 처리 서비스	Web Intelligence 서비스	Web Intelligence 처리 서버	Web Intelligence 문서를 허용하고 처리합니다.
Web Intelligence 예약 서비스	Web Intelligence 서비스	적응형 작업 서버	예약된 Web Intelligence 작업 지원을 활성화합니다.
주기 관리 ClearCase 서비스	주기 관리 서비스	적응형 처리 서버	LCM에 대한 ClearCase 지원을 제공합니다.
주기 관리 예약 서비스	주기 관리 서비스	적응형 작업 서버	예약된 주기 관리 작업을 실행합니다.
주기 관리 서비스	주기 관리 서비스	적응형 처리 서버	주기 관리 핵심 서비스입니다.
모니터링 서비스	핵심 서비스	적응형 처리 서버	모니터링 기능을 제공합니다.
다차원 분석 서비스	Analysis Services	적응형 처리 서버	다차원 OLAP(Online Analytical Processing) 데이터에 대한 액세스를 제공하고, 원시 데이터를 Excel, PDF 또는 Analysis(이전 이름: Voyager) 크로스탭 및 차트에 렌더링할 수 있도록 XML로 변환합니다.
네이티브 연결 서비스	연결 서비스	연결 서버	64비트 아키텍처에 대한 네이티브 연결 서비스를 제공합니다.
네이티브 연결 서비스 (32비트)	연결 서비스	연결 서버	32비트 아키텍처에 대한 네이티브 연결 서비스를 제공합니다.
Output Filestore 서비스	핵심 서비스	출력 파일 리포지토리 서버	완성된 문서 컬렉션을 유지 관리합니다.
플랫폼 검색 예약 서비스	핵심 서비스	적응형 작업 서버	예약된 검색을 실행하여 중앙 관리 서버(CMS) 리포지토리의 모든 콘텐츠를 인덱싱합니다.

서비스	서비스 범주	서버 유형	서비스 설명
플랫폼 검색 서비스	핵심 서비스	적응형 처리 서버	BI 플랫폼에 대한 검색 기능을 제공합니다.
프로브 예약 서비스	핵심 서비스	적응형 작업 서버	예약된 프로브 작업을 제공하여 그 결과를 지정된 출력 위치에 게시합니다.
프로그램 예약 서비스	핵심 서비스	적응형 작업 서버	지정된 시간에 실행되도록 예약된 프로그램을 실행합니다.
게시 예약 서비스	핵심 서비스	적응형 작업 서버	예약된 게시 작업을 실행하여 그 결과를 지정된 출력 위치에 게시합니다.
게시 사후 처리 서비스	핵심 서비스	적응형 처리 서버	보고서가 완성된 후 보고서에 대한 작업(예: 보고서를 특정 출력 위치로 전송)을 수행합니다.
게시 서비스	핵심 서비스	적응형 처리 서버	게시 사후 처리 서비스 및 대상 작업 서비스와 협력하여 보고서를 지정된 출력 위치(예: 파일 시스템, FTP, 전자 메일 또는 사용자의 받은 파일함)에 게시합니다.
Rebean 서비스	Web Intelligence 서비스	적응형 처리 서버	Web Intelligence 및 Explorer에서 사용하는 SDK
복제 서비스	핵심 서비스	적응형 작업 서버	예약된 연합 작업을 실행하여 콘텐츠를 연합된 사이트 간에 복제합니다.
보안 쿼리 예약 서비스	핵심 서비스	적응형 작업 서버	예약된 보안 쿼리 작업을 실행합니다.
보안 토큰 서비스	핵심 서비스	적응형 처리 서버	SAP 단일 로그인 지원

서비스	서비스 범주	서버 유형	서비스 설명
단일 로그인 서비스	핵심 서비스	중앙 관리 서버	Active Directory 단일 로그인 지원입니다. 보조 서비스로, "중앙 관리 서비스"에 자동으로 추가됩니다.
추적 로그 서비스	핵심 서비스	모든 서버	추적, 로깅 및 지원 가능성 지원입니다.
변환 서비스	핵심 서비스	적응형 처리 서버	Translation Manager 클라이언트에서 입력된 InfoObject를 변환합니다.
시각적 차이 예약 서비스	주기 관리 서비스	적응형 작업 서버	예약된 시각적 차이(주기 관리) 작업을 실행하여 그 결과를 지정된 출력 위치에 게시합니다.
시각적 차이 서비스	주기 관리 서비스	적응형 처리 서버	문서가 시각적으로 문서 프로모션 및 주기 관리에 적합한지 여부를 결정합니다.
시각화 서비스	Web Intelligence 서비스	적응형 처리 서버	Web Intelligence에서 사용되는 공통 시각화 개체 모델 서비스입니다.
웹 서비스 SDK 및 QaaWS	핵심 서비스	웹 응용 프로그램 컨테이너 서버	WACS의 웹 서비스입니다.

참고:

SAP BusinessObjects Business Intelligence 플랫폼의 이후 유지 관리 릴리스에 새로운 서비스 또는 서버 유형이 추가될 수 있습니다.

2.3.2 서비스 범주

다음 표에 각 서버가 서비스 범주별로 나와 있습니다. 각 서비스에 대한 설명은 서비스를 참조하십시오.

참고:

SAP BusinessObjects Business Intelligence 플랫폼의 이후 유지 관리 릴리스에 새로운 서비스 또는 서버 유형이 추가될 수 있습니다.

테이블 2-2: 서비스(서비스 범주별)

서비스 범주	서비스	서버 유형
Analysis Services	BEx 웹 응용 프로그램 서비스	적응형 처리 서버
Analysis Services	다차원 분석 서비스	적응형 처리 서버
연결 서비스	적응형 연결 서비스	적응형 처리 서버
연결 서비스	사용자 지정 데이터 액세스 서비스	적응형 처리 서버
연결 서비스	외부 데이터 액세스 서비스	적응형 처리 서버
연결 서비스	네이티브 연결 서비스	연결 서버
연결 서비스	네이티브 연결 서비스(32비트)	연결 서버
핵심 서비스	인증 업데이트 예약 서비스	적응형 작업 서버
핵심 서비스	BOE 웹 응용 프로그램 서비스	웹 응용 프로그램 컨테이너 서버
핵심 서비스	Business Process BI 서비스	웹 응용 프로그램 컨테이너 서버
핵심 서비스	중앙 관리 서비스	중앙 관리 서버
핵심 서비스	클라이언트 감사 프록시 서비스	적응형 처리 서버
핵심 서비스	대시보드 분석 서비스	대시보드 분석 서버
핵심 서비스	대시보드 서비스	대시보드 서버
핵심 서비스	대상 배달 예약 서비스	적응형 작업 서버
핵심 서비스	이벤트 서비스	이벤트 서버
핵심 서비스	Input Filestore 서비스	입력 파일 리포지토리 서버
핵심 서비스	모니터링 서비스	적응형 처리 서버
핵심 서비스	Output Filestore 서비스	출력 파일 리포지토리 서버
핵심 서비스	플랫폼 검색 예약 서비스	적응형 작업 서버
핵심 서비스	플랫폼 검색 서비스	적응형 처리 서버
핵심 서비스	프로브 예약 서비스	적응형 작업 서버

서비스 범주	서비스	서버 유형
핵심 서비스	프로그램 예약 서비스	적응형 작업 서버
핵심 서비스	게시 예약 서비스	적응형 작업 서버
핵심 서비스	게시 사후 처리 서비스	적응형 처리 서버
핵심 서비스	게시 서비스	적응형 처리 서버
핵심 서비스	복제 서비스	적응형 작업 서버
핵심 서비스	보안 쿼리 예약 서비스	적응형 작업 서버
핵심 서비스	보안 토큰 서비스	적응형 처리 서버
핵심 서비스	단일 로그인 서비스	중앙 관리 서버
핵심 서비스	추적 로그 서비스	모든 서버
핵심 서비스	변환 서비스	적응형 처리 서버
핵심 서비스	웹 서비스 SDK 및 QaaWS	웹 응용 프로그램 컨테이너 서버
Crystal Reports 서비스	Crystal Reports 2011 처리 서비스	Crystal Reports 처리 서버
Crystal Reports 서비스	Crystal Report 2011 예약 서비스	적응형 작업 서버
Crystal Reports 서비스	Crystal Reports 2011 보기 및 수정 서비스	RAS
Crystal Reports 서비스	Crystal Reports 캐시 서비스	Crystal Reports 캐시 서버
Crystal Reports 서비스	Crystal Reports 처리 서비스	Crystal Reports 처리 서버
Crystal Reports 서비스	Crystal Reports 예약 서비스	적응형 작업 서버
Dashboard Design 서비스	Dashboard Design 캐시 서비스	Dashboard Design 캐시 서버
Dashboard Design 서비스	Dashboard Design 처리 서비스	Dashboard Design 처리 서버
데이터 연합 서비스	데이터 연합 서비스	적응형 처리 서버
주기 관리 서비스	주기 관리 ClearCase 서비스	적응형 처리 서버
주기 관리 서비스	주기 관리 예약 서비스	적응형 작업 서버
주기 관리 서비스	주기 관리 서비스	적응형 처리 서버

서비스 범주	서비스	서버 유형
주기 관리 서비스	시각적 차이 예약 서비스	적응형 작업 서버
주기 관리 서비스	시각적 차이 서비스	적응형 처리 서버
Web Intelligence 서비스	문서 복구 서비스	적응형 처리 서버
Web Intelligence 서비스	DSL Bridge Service	적응형 처리 서버
Web Intelligence 서비스	정보 엔진 서비스	Web Intelligence 처리 서버
Web Intelligence 서비스	Web Intelligence 모니터링 서비스	적응형 처리 서버
Web Intelligence 서비스	Rebean 서비스	적응형 처리 서버
Web Intelligence 서비스	시각화 서비스	적응형 처리 서버
Web Intelligence 서비스	Web Intelligence 공통 서비스	Web Intelligence 처리 서버
Web Intelligence 서비스	Web Intelligence 핵심 서비스	Web Intelligence 처리 서버
Web Intelligence 서비스	Web Intelligence 처리 서비스	Web Intelligence 처리 서버
Web Intelligence 서비스	Web Intelligence 예약 서비스	적응형 작업 서버

2.3.3 서버 유형

다음 표에는 서버 유형별 각 서버가 나와 있습니다. 각 서비스에 대한 설명은 서비스를 참조하십시오.

테이블2-3: 서버(서버 유형별)

서버 유형	서비스	서비스 범주
적응형 작업 서버	인증 업데이트 예약 서비스	핵심 서비스
적응형 작업 서버	Crystal Report 2011 예약 서비스	Crystal Reports 서비스
적응형 작업 서버	Crystal Reports 예약 서비스	Crystal Reports 서비스
적응형 작업 서버	대상 배달 예약 서비스	핵심 서비스

서버 유형	서비스	서비스 범주
적응형 작업 서버	주기 관리 예약 서비스	주기 관리 서비스
적응형 작업 서버	플랫폼 검색 예약 서비스	핵심 서비스
적응형 작업 서버	프로브 예약 서비스	핵심 서비스
적응형 작업 서버	프로그램 예약 서비스	핵심 서비스
적응형 작업 서버	게시 예약 서비스	핵심 서비스
적응형 작업 서버	복제 서비스	핵심 서비스
적응형 작업 서버	보안 쿼리 예약 서비스	핵심 서비스
적응형 작업 서버	시각적 차이 예약 서비스	주기 관리 서비스
적응형 작업 서버	Web Intelligence 예약 서비스	Web Intelligence 서비스
적응형 처리 서버	적응형 연결 서비스	연결 서비스
적응형 처리 서버	BEx 웹 응용 프로그램 서비스	Analysis Services
적응형 처리 서버	클라이언트 감사 프록시 서비스	핵심 서비스
적응형 처리 서버	사용자 지정 데이터 액세스 서비스	연결 서비스
적응형 처리 서버	데이터 연합 서비스	데이터 연합 서비스
적응형 처리 서버	문서 복구 서비스	Web Intelligence 서비스
적응형 처리 서버	DSL Bridge Service	Web Intelligence 서비스
적응형 처리 서버	외부 데이터 액세스 서비스	연결 서비스
적응형 처리 서버	Web Intelligence 모니터링 서비스	Web Intelligence 서비스
적응형 처리 서버	주기 관리 ClearCase 서비스	주기 관리 서비스
적응형 처리 서버	주기 관리 콘솔 서비스	주기 관리 서비스
적응형 처리 서버	모니터링 서비스	핵심 서비스
적응형 처리 서버	다차원 분석 서비스	Analysis Services
적응형 처리 서버	플랫폼 검색 서비스	핵심 서비스
적응형 처리 서버	게시 사후 처리 서비스	핵심 서비스
적응형 처리 서버	게시 서비스	핵심 서비스
적응형 처리 서버	Rebean 서비스	Web Intelligence 서비스

서버 유형	서비스	서비스 범주
적응형 처리 서버	보안 토큰 서비스	핵심 서비스
적응형 처리 서버	변환 서비스	핵심 서비스
적응형 처리 서버	시각적 차이 서비스	주기 관리 서비스
적응형 처리 서버	시각화 서비스	Web Intelligence 서비스
모든 서버	추적 로그 서비스	핵심 서비스
중앙 관리 서버	중앙 관리 서비스	핵심 서비스
중앙 관리 서버	단일 로그인 서비스	핵심 서비스
연결 서버	네이티브 연결 서비스	연결 서비스
연결 서버	네이티브 연결 서비스(32비트)	연결 서비스
Crystal Reports 캐시 서버	Crystal Reports 캐시 서비스	Crystal Reports 서비스
Crystal Reports 처리 서버	Crystal Reports 2011 처리 서비스	Crystal Reports 서비스
Crystal Reports 처리 서버	Crystal Reports 처리 서비스	Crystal Reports 서비스
대시보드 분석 서버	대시보드 분석 서비스	핵심 서비스
Dashboard Design 캐시 서버	Dashboard Design 캐시 서비스	Dashboard Design 서비스
Dashboard Design 처리 서버	Dashboard Design 처리 서비스	Dashboard Design 서비스
대시보드 서버	대시보드 서비스	핵심 서비스
이벤트 서버	이벤트 서비스	핵심 서비스
입력 파일 리포지토리 서버	Input Filestore 서비스	핵심 서비스
출력 파일 리포지토리 서버	Output Filestore 서비스	핵심 서비스
RAS	Crystal Reports 2011 보기 및 수정 서비스	Crystal Reports 서비스
웹 응용 프로그램 컨테이너 서버	BOE 웹 응용 프로그램 서비스	핵심 서비스
웹 응용 프로그램 컨테이너 서버	Business Process BI 서비스	핵심 서비스
웹 응용 프로그램 컨테이너 서버	웹 서비스 SDK 및 QaaWS	핵심 서비스

서버 유형	서비스	서비스 범주
Web Intelligence 처리 서버	정보 엔진 서비스	Web Intelligence 서비스
Web Intelligence 처리 서버	Web Intelligence 공통 서비스	Web Intelligence 서비스
Web Intelligence 처리 서버	Web Intelligence 핵심 서비스	Web Intelligence 서비스
Web Intelligence 처리 서버	Web Intelligence 처리 서비스	Web Intelligence 서비스

2.3.4 서버

서버는 호스트의 SIA(Server Intelligence Agent)에서 실행되는 서비스 컬렉션입니다. 서버 유형은 서버 내에서 실행되는 서비스에 따라 표시됩니다. 서버는 중앙 관리 콘솔(CMC)에서 만들 수 있습니다. 다음 표에는 CMC에서 만들 수 있는 여러 유형의 서버가 나와 있습니다.

서버	설명
적응형 작업 서버	예약된 작업을 처리하는 일반 서버입니다. 작업 서버를 SAP BusinessObjects Business Intelligence 플랫폼에 추가하는 경우 보고서, 문서, 프로그램 또는 게시를 처리하여 그 결과를 여러 대상으로 보내도록 작업 서버를 구성할 수 있습니다.
적응형 처리 서버	<p>다양한 소스로부터 받은 요청을 처리하는 서비스를 호스팅하는 일반 서버입니다.</p> <p>참고: 설치 프로그램은 호스트 시스템당 하나의 적응형 처리 서버(APS)를 설치합니다. 설치한 기능에 따라 이 APS는 모니터링 서비스, 주기 관리 서비스, 다차원 분석 서비스(MDAS), 게시 서비스 등과 같은 많은 수의 서비스를 호스팅할 수 있습니다.</p> <p>운영 환경을 설치하는 경우에는 기본 APS를 사용하지 마십시오. 대신 설치 프로세스가 완료되면 시스템 크기 조정을 수행하여 다음을 확인하는 것이 좋습니다.</p> <ul style="list-style-type: none"> • APS 서비스의 유형 및 개수 • 여러 APS 서버에 서비스 배포 • 최적의 APS 서비스 수 여러 개의 APS 서버는 중복성, 뛰어난 성능, 높은 안정성을 제공합니다. • 여러 노드에 APS 서버 배포 <p>크기 조정 프로세스를 통해 확인된 APS 서버 인스턴스를 새로 만듭니다.</p> <p>예를 들어, 크기 조정 결과에 따라 서비스 범주당 하나의 APS를 만들어야 하는 한다면 8개의 APS 서버를 만들어야 합니다. Analysis Services, 연결 서비스, 핵심 서비스, Crystal Reports 서비스, Dashboard Design 서비스, 데이터 연합 서비스, 주기 관리 서비스 및 Web Intelligence 서비스의 각 서비스 범주마다 하나씩 만들어집니다.</p>
중앙 관리 서버 (CMS)	SAP BusinessObjects Business Intelligence 플랫폼에 대한 정보로 구성된 데이터베이스(CMS 시스템 데이터베이스 내) 및 감사 대상 사용자 작업(감사 데이터 저장소 내)을 유지 관리합니다. 모든 플랫폼 서비스는 CMS를 통해 관리됩니다. CMS는 또한 문서가 저장되는 시스템 파일에 대한 액세스 및 사용자, 사용자 그룹, 보안 수준(인증 및 권한 부여 포함), 콘텐츠에 대한 정보도 제어합니다.
연결 서버	소스 데이터에 대한 데이터베이스 액세스를 제공하며, 관계형 데이터베이스, OLAP 및 기타 형식을 지원합니다. 연결 서버에서는 다양한 데이터 소스와의 연결 및 상호 작용을 처리하고 클라이언트에 공통 기능 집합을 제공합니다.
Crystal Reports 캐시 서버	클라이언트에서 페이지 서버로 전달되는 보고서 요청을 가로칩니다. 캐시 서버에서 캐시된 보고서 페이지로 요청을 처리할 수 없는 경우에는 요청이 Crystal Reports 처리 서버로 전달됩니다. 이렇게 요청을 전달받은 서버에서는 보고서를 실행하여 그 결과를 반환합니다. 그러면 캐시 서버에서는 나중에 사용할 수 있도록 보고서 페이지를 캐시합니다.

서버	설명
Crystal Reports 처리 서버	보고서를 처리하고 EPF(Encapsulated Page Format) 페이지를 생성하여 페이지 요청에 응답합니다. EPF의 주요 이점은 전체 보고서를 반환할 필요 없이 요청된 페이지만 반환하면 되도록 요청된 페이지에 대한 선별적인 액세스를 지원한다는 점입니다. 따라서 대형 보고서의 경우 시스템 성능을 향상시키고 불필요한 네트워크 트래픽을 줄일 수 있습니다.
대시보드 분석 서버	회사 및 개인 BI 작업 영역 모듈 콘텐츠를 만들고 관리하기 위해 BI 작업 영역 구성 요소에서 사용하는 서버 프로세스입니다.
대시보드 서버	BI 작업 영역 구성 요소에서 회사 및 개인 대시보드를 만들고 관리하는 데 사용됩니다. BI 작업 영역에 제공되는 대시보드 관리 기능을 통해 조직은 비즈니스 활동을 모니터링하고 이해할 수 있습니다.
Dashboard Design 캐시 서버	클라이언트에서 대시보드 서버로 전달되는 보고서 요청을 가로챍니다. 캐시 서버에서 캐시된 보고서 페이지로 요청을 처리할 수 없는 경우에는 요청이 대시보드 서버로 전달됩니다. 이렇게 요청을 전달받은 서버에서는 보고서를 실행하여 그 결과를 반환합니다. 그러면 캐시 서버에서는 나중에 사용할 수 있도록 보고서 페이지를 캐시합니다.
Dashboard Design 처리 서버	보고서를 처리하고 EPF(Encapsulated Page Format) 페이지를 생성하여 Dashboard Design 요청에 응답합니다. EPF의 주요 이점은 전체 보고서를 반환할 필요 없이 요청된 페이지만 반환하면 되도록 요청된 페이지에 대한 선별적인 액세스를 지원한다는 점입니다. 따라서 대형 보고서의 경우 시스템 성능을 향상시키고 불필요한 네트워크 트래픽을 줄일 수 있습니다.
이벤트 서버	보고서를 실행하는 트리거 역할을 할 수 있는 이벤트용 시스템을 모니터링합니다. 이벤트 트리거를 설정할 경우 이벤트 서버에서 조건을 모니터링하여 이벤트가 발생한 경우 이를 CMS에 알립니다. 그러면 CMS에서 이벤트 발생 시 실행되도록 설정된 작업을 시작할 수 있습니다.
파일 리포지토리 서버	내보낸 보고서, 네이티브가 아닌 형식으로 가져온 파일 등의 파일 시스템 개체를 만드는 일을 담당합니다. 입력 FRS는 관리자 또는 최종 사용자가 시스템에 게시한 보고서 및 프로그램 개체를 저장합니다. 출력 FRS는 작업 서버에서 생성한 모든 보고서 인스턴스를 관리합니다.
Web Intelligence 처리 서버	SAP BusinessObjects Web Intelligence 문서를 처리합니다.
Report Application Server	사용자가 SAP Crystal Reports Server Embedded 소프트웨어 개발 키트(SDK)를 통해 Crystal 보고서를 만들고 수정할 수 있는 임시 보고서 작성 기능을 제공합니다.

2.4 클라이언트 응용 프로그램

유형이 다른 두 가지 데스크톱 응용 프로그램을 사용하여 SAP BusinessObjects Business Intelligence 플랫폼과 상호 작용할 수 있습니다.

- 데스크톱 응용 프로그램

이러한 응용 프로그램은 지원되는 Microsoft Windows 운영 체제에서 설치해야 하며 데이터를 처리하고 보고서를 로컬로 만들 수 있습니다.

참고:

SAP BusinessObjects Business Intelligence 플랫폼 설치 프로그램에서는 더 이상 데스크톱 응용 프로그램을 설치하지 않습니다. 서버에 데스크톱 응용 프로그램을 설치하려면 독립 실행형 SAP BusinessObjects Business Intelligence 플랫폼 클라이언트 도구 설치 프로그램을 사용하십시오.

데스크톱 클라이언트를 통해 사용자는 일부 BI 보고서 처리를 개별 클라이언트 컴퓨터에서 별도로 처리할 수 있습니다. 대부분의 데스크톱 응용 프로그램은 데스크톱에 설치된 드라이버를 통해 조직의 데이터에 직접 액세스하며 CORBA 또는 암호화된 CORBA SSL을 통해 SAP BusinessObjects Business Intelligence 플랫폼 배포와 통신합니다.

이러한 종류의 응용 프로그램으로는 Crystal Reports와 Live Office 등이 있습니다.

참고:

Live Office는 다양한 기능의 응용 프로그램이지만 HTTP를 통해 SAP BusinessObjects Business Intelligence 플랫폼 웹 서비스와 상호 작용합니다.

- 웹 응용 프로그램

이러한 응용 프로그램은 웹 응용 프로그램 서버에서 호스팅되고 Windows, Macintosh, Unix 및 Linux 운영 체제에서 지원되는 웹 브라우저를 사용하여 액세스할 수 있습니다.

따라서 데스크톱 소프트웨어 제품을 배포해야 하는 문제 없이 대규모 사용자 그룹에 Business Intelligence(BI) 액세스를 제공할 수 있습니다. 통신은 SSL 암호화(HTTPS) 여부에 관계 없이 HTTP를 통해 수행됩니다.

이러한 종류의 응용 프로그램으로는 BI 실행 패드, SAP BusinessObjects Web Intelligence, 중앙 관리 콘솔(CMC), 보고서 뷰어 등이 있습니다.

2.4.1 SAP BusinessObjects Business Intelligence 플랫폼 클라이언트 도구와 함께 설치

2.4.1.1 Web Intelligence Desktop

Web Intelligence Desktop은 비즈니스 사용자가 SAP BusinessObjects Business Intelligence 플랫폼 액세스 여부에 관계 없이 임시 분석 및 보고 기능을 수행할 수 있는 도구입니다.

이 도구를 사용하면 비즈니스 사용자는 끌어서 놓기 인터페이스에서 친숙한 비즈니스 용어를 사용하여 관계형, OLAP(Online Analytical Processing), 스프레드시트 또는 텍스트 파일 소스의 데이터를 액세스 및 결합할 수 있습니다. 워크플로를 통해 매우 광범위하거나 세부적인 질문을 분석하고, 분석 워크플로에서 언제든지 추가 질문을 할 수 있습니다.

Web Intelligence Desktop 사용자는 중앙 관리 서버(CMS)에 연결할 수 없을 때에도 Web Intelligence 문서 파일(.wid)로 작업을 계속할 수 있습니다.

2.4.1.2 비즈니스 뷰 관리자

비즈니스 뷰 관리자를 통해 사용자는 기본 데이터베이스의 복잡성을 단순화하는 의미 계층 개체를 작성할 수 있습니다.

비즈니스 뷰 관리자는 데이터 연결, 동적 데이터 연결, 데이터 기반, 비즈니스 요소, 비즈니스 뷰 및 관계형 뷰를 만들 수 있습니다. 또한 보고서에서 상세 열과 행 수준 보안을 개체에 설정할 수 있습니다.

디자이너는 여러 데이터 소스에 대한 연결 작성, 테이블 조인, 필드 이름에 별칭 지정 및 계산된 필드 만들기를 수행한 후에 이 간소화된 구조를 비즈니스 뷰로 사용할 수 있습니다. 그리고 나면 보고서 디자이너와 사용자는 데이터에서 직접 자체 쿼리를 작성하는 대신, 비즈니스 뷰를 보고서의 기준으로 사용할 수 있습니다.

2.4.1.3 보고서 변환 도구

보고서 변환 도구는 보고서를 Web Intelligence 형식으로 변환하여 중앙 관리 서버(CMS)에 게시합니다.

보고서는 CMS 폴더인 공용, 즐겨찾기 또는 받은 파일함에서 검색할 수 있습니다. 변환된 보고서는 원본 Web Intelligence 보고서와 동일한 폴더 또는 다른 폴더에 게시됩니다. 보고서 변환 도구를 통해 Web Intelligence의 모든 기능과 보고서가 변환되는 것은 아닙니다. 변환 수준은 원본 보고서의 기능에 따라 달라집니다. 일부 기능으로 인해 보고서가 변환되지 않을 수도 있으며, 다른 기능은 변환 중에 도구를 통해 수정되고 다시 구현되거나 제거됩니다.

또한 보고서 변환 도구를 사용하여 변환된 보고서를 감사할 수 있습니다. 보고서를 감사하면 보고서 변환 도구를 통해 전부 변환할 수 없는 보고서를 식별하고 그 이유를 파악할 수 있습니다.

2.4.1.4 유니버스 디자인 도구

유니버스 디자인 도구(이전 이름: Universe Designer)를 통해 데이터 디자이너는 여러 소스의 데이터를 의미 계층으로 결합하여 최종 사용자에게서 데이터베이스 복잡성을 감출 수 있습니다. 또한 기술적 언어가 아닌 비즈니스 언어를 사용하여 데이터를 액세스, 조작 및 구성함으로써 데이터의 복잡성을 추상화합니다.

유니버스 디자인 도구에는 데이터베이스의 테이블을 선택하고 표시하는 데 사용되는 그래픽 인터페이스가 제공됩니다. 데이터베이스 테이블은 스키마 다이어그램에서 테이블 기호로 표시됩니다. 이 인터페이스를 사용하여 디자이너는 테이블을 조작하고 테이블 사이에 조인을 만들며 별칭 테이블을 만들고 컨텍스트를 만들거나 스키마의 루프를 해결할 수 있습니다.

메타데이터 소스에서 유니버스를 만들 수도 있습니다. 유니버스 디자인 도구는 만드는 마지막 과정에서 유니버스를 생성하는 데 사용됩니다.

2.4.1.5 웹 서비스 쿼리 도구

웹 서비스 쿼리 도구(이전 이름: Query as a Web Service)를 통해 Business Intelligence(BI) 쿼리를 사용자 지정 웹 응용 프로그램에서 사용할 수 있습니다. 비즈니스 사용자는 유니버스 연결에서 자신의 쿼리를 만들고 이 쿼리가 웹 응용 프로그램에 통합될 수 있도록 웹 서비스로 게시합니다.

웹 서비스 쿼리 도구는 비즈니스를 위한 새 클라이언트 솔루션을 제공합니다. 예를 들어 SAP BusinessObjects Dashboard Design(이전 이름: Xcelsius)을 사용하여 여러 종류의 데이터 소스를 하나의 신뢰할 수 있는 BI 뷰로 합칠 수 있습니다.

웹 서비스 쿼리 도구는 다음과 같은 여러 클라이언트측 솔루션과도 사용할 수 있습니다.

- Microsoft Office, Excel 및 InfoPath
- SAP NetWeaver

- OpenOffice
- 비즈니스 규칙 및 프로세스 관리 응용 프로그램
- Enterprise Services

2.4.1.6 정보 디자인 도구

정보 디자인 도구(이전 이름: 정보 디자이너)는 디자이너가 관계형 및 OLAP 소스에서 메타데이터를 추출, 정의 및 조작하여 SAP BusinessObjects 유니버스를 만들고 배포할 수 있도록 해주는 SAP BusinessObjects 메타데이터 디자인 환경입니다.

2.4.1.7 번역 관리 도구

SAP BusinessObjects Business Intelligence 플랫폼은 다국어 문서 및 유니버스를 지원합니다. 다국어 문서에는 유니버스 메타데이터 및 문서 프롬프트의 지역화 버전이 포함되어 있습니다. 예를 들어, 사용자는 선택한 언어로 동일한 유니버스에서 보고서를 만들 수 있습니다.

번역 관리 도구(이전 이름: Translation Manager)는 다국어 유니버스를 정의하고 유니버스와 Web Intelligence 문서 및 프롬프트의 변환을 관리합니다.

번역 관리 도구에서 수행할 수 있는 기능은 다음과 같습니다.

- 다른 언어 사용자를 위해 유니버스 또는 SAP BusinessObjects Web Intelligence 문서 변환
- 문서의 메타데이터 언어 부분과 적절한 변환 내용 정의 외부 XLIFF 형식 생성 및 번역된 정보를 얻기 위한 XLIFF 파일 가져오기
- 변환할 유니버스 또는 SAP BusinessObjects Web Intelligence 문서 구조 표시
- XLIFF 파일을 가져오고 내보내서 사용자 인터페이스 또는 외부 변환 도구를 통해 메타데이터를 변환할 수 있습니다.
- 다국어 문서를 만듭니다.

2.4.1.8 데이터 연합 관리 도구

데이터 연합 관리 도구(이전 이름: Data Federator)는 사용이 간편한 데이터 연합 서비스 관리 기능을 제공하는 Rich Client 응용 프로그램입니다.

SAP BusinessObjects Business Intelligence 플랫폼에 완벽히 통합된 데이터 연합 서비스를 통해 서로 다른 데이터 소스에 쿼리를 배포하여 다중 소스 유니버스를 사용하고 단일 데이터 연합을 통해 데이터를 통합할 수 있습니다.

데이터 연합 관리 도구를 통해 데이터 연합 쿼리를 최적화하고 데이터 연합 쿼리 엔진을 세밀하게 조정하여 성능을 최적화할 수 있습니다.

데이터 연합 관리 도구는 다음 작업을 수행하는 데 사용됩니다.

- SQL 쿼리를 테스트합니다.
- 연합 쿼리를 각 소스에 배포하는 방법을 자세히 설명하는 최적화 계획을 시각화합니다.
- 통계를 계산하고 시스템 매개 변수를 설정하여 데이터 연합 서비스를 세밀하게 조정하고 성능을 최적화합니다.
- 커넥터 수준에서의 데이터 소스별 쿼리 실행 방식을 제어하는 속성을 관리합니다.
- 실행 중인 SQL 쿼리를 모니터링합니다.
- 실행된 쿼리의 기록을 찾아봅니다.

2.4.1.9 SAP BusinessObjects Business Intelligence 플랫폼용 위젯

위젯은 자주 사용하는 기능에 빠르고 간편하게 액세스할 수 있도록 하고 바탕 화면에서 시각적 정보를 제공하는 소형 응용 프로그램입니다. SAP BusinessObjects Business Intelligence 플랫폼용 위젯(이전 이름: BI Widgets)을 사용할 경우 조직에서는 SAP BusinessObjects Business Intelligence 플랫폼에 있는 기존 비즈니스 인텔리전스(BI) 콘텐츠에 액세스할 수 있으며, 사용자는 SAP NetWeaver Application Server에 XBCML(Extensible Business Client Markup Language) 위젯으로 등록된 Web Dynpro 응용 프로그램을 바탕화면 위젯으로 추가할 수 있습니다.

사용자의 바탕화면에서 XBCML 위젯을 렌더링하기 위해 SAP Web Dynpro Flex 클라이언트가 사용됩니다. SAP Web Dynpro Flex 클라이언트는 위젯 렌더링에 사용되는 Adobe Flex 기반의 렌더링 엔진입니다. Web Dynpro 응용 프로그램 구성 방법에 대한 자세한 내용은 SAP BusinessObjects용 위젯 사용자 가이드의 SAP NetWeaver Application Server에서 위젯 사용 항목을 참조하십시오.

참고:

XBCML 위젯에 대한 SAP Web Dynpro Flex 클라이언트 지원은 릴리스 7.0 EhP2 SP3부터 제공됩니다. 지정된 이 릴리스의 XBCML 위젯에서 발견된 Flex 클라이언트 문제에 대해서만 Flex 클라이언트 대기열이 지정됩니다.

SAP BusinessObjects Business Intelligence 플랫폼용 위젯으로 Web Intelligence 문서, Dashboard Design 모델 및 Web Dynpro 응용 프로그램과 같은 기존의 콘텐츠를 검색하거나 찾아본 후 정보를 자신의 컴퓨터로 복사하여 필요할 때 즉시 사용할 수 있습니다.

위젯으로서, 콘텐츠는 위젯 프레임워크에서 다음과 같은 기능을 가져옵니다.

- 사용자 제어 크기 및 위치 지정
- 자동 새로 고침
- 맨 위 응용 프로그램 창으로 설정(선택 사항)
- 전체 SAP BusinessObjects Business Intelligence 플랫폼 보안(Web Intelligence 부분 보고서 및 Dashboard Design 모델만 해당)
- 디스플레이 저장
- 데이터 컨텍스트 상태 저장(Web Intelligence 부분 보고서만 해당)
- 상세 보고서에 대한 Web Intelligence OpenDocument 링크(Web Intelligence 문서만 해당)
- 탭으로 구분된 뷰(Dashboard Design 모델만 해당)

2.4.2 SAP BusinessObjects Business Intelligence 플랫폼과 함께 설치

2.4.2.1 중앙 구성 관리자(CCM)

중앙 구성 관리자(CCM)는 두 가지 형태로 제공되는 서버 문제 해결 및 노드 관리 도구입니다. Microsoft Windows 환경에서는 CCM을 사용하여 그래픽 사용자 인터페이스(GUI) 또는 명령줄을 통해 로컬/원격 서버를 관리할 수 있습니다. UNIX 환경에서는 CCM 셸 스크립트(ccm.sh)를 사용하여 명령줄에서 서버를 관리할 수 있습니다.

CCM을 사용하면 SIA(Server Intelligence Agent) 노드를 만들고 구성할 수 있으며 웹 응용 프로그램 서버를 시작 또는 중지할 수 있습니다. 또한 Windows에서는 SSL(Secure Socket Layer) 암호화 등의 네트워크 매개 변수를 구성할 수 있습니다. 이러한 매개 변수는 노드 내에서 모든 서버에 적용됩니다.

참고:

대부분의 서버 관리 작업은 이제 CCM이 아닌 CMC를 통해 처리됩니다. 현재 CCM은 문제 해결 및 노드 구성에 사용됩니다.

2.4.2.2 업그레이드 관리 도구

업그레이드 관리 도구(이전 이름: 가져오기 마법사)는 BI 플랫폼의 일부로 설치되며, 이전 버전의 BI 플랫폼에서 사용자, 그룹 및 폴더를 가져오는 과정을 관리자에게 안내합니다. 개체, 이벤트, 서버 그룹, 리포지토리 개체 및 달력을 가져오고 업그레이드할 수도 있습니다.

BI 플랫폼의 이전 버전을 업그레이드하는 방법에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 업그레이드 가이드를 참조하십시오.

2.4.2.3 리포지토리 진단 도구

리포지토리 진단 도구(RDT)를 사용하면 중앙 관리 서버(CMS) 시스템 데이터베이스와 파일 리포지토리 서버(FRS) 파일 저장소 사이에 발생할 수 있는 불일치를 검사, 진단 및 복구할 수 있습니다.

복구 상태와 완료된 작업을 보고할 수도 있습니다. 파일 시스템과 데이터베이스 사이의 동기화를 확인하려면 사용자가 맨 처음 핫 백업을 완료한 이후 RDT를 사용해야 합니다. 복원 후 및 SAP BusinessObjects Business Intelligence 플랫폼 서비스를 시작하기 전에 사용할 수도 있습니다. 사용자는 RDT를 중지하기 전까지 RDT를 통해 찾거나 복원할 오류의 수를 제한할 수도 있습니다.

2.4.3 별도로 사용 가능

2.4.3.1 SAP BusinessObjects Analysis, Microsoft Office용 에디션

SAP BusinessObjects Analysis, Microsoft Office용 에디션은 고급 기능이 추가된 Business Explorer(BEx)의 대체 솔루션으로 비즈니스 분석가는 이 솔루션을 통해 다차원 OLAP(online analytical processing) 데이터를 탐색할 수 있습니다.

분석가는 비즈니스 질문에 신속하게 응답한 후 자신의 분석과 작업 영역을 다른 사용자와 분석으로 공유할 수 있습니다.

SAP BusinessObjects Analysis, Microsoft Office용 에디션을 사용하여 분석가는 다음 작업을 수행할 수 있습니다.

- 데이터베이스 관리자의 도움 없이 재무 시스템에 저장된 추세, 특이값 및 세부 정보 검색
- 크고 작은 다차원 데이터 집합의 효율적인 검색을 통해 비즈니스 질문 해결
- 조직 내에 있는 모든 범위의 OLAP 데이터 소스에 액세스 및 간단하고 직관적인 인터페이스를 통해 결과 공유
- 동일한 분석에서 서로 다른 여러 OLAP 소스에 액세스하여 비즈니스 및 하나의 추세가 다른 추세에 미치는 상호 영향을 포괄적으로 관찰
- 비즈니스 동인 질의, 분석, 비교 및 예측
- 포괄적인 범위의 비즈니스 및 시간 계산 사용

2.4.3.2 SAP Crystal Reports

SAP Crystal Reports 소프트웨어를 사용하면 사용자가 데이터 소스에서 대화형 보고서를 디자인할 수 있습니다.

2.4.3.3 SAP BusinessObjects Dashboard Design

SAP BusinessObjects Dashboard Design(이전 이름: Xcelsius)은 데이터를 시각화하고 동적인 대화형 대시보드를 만드는 데 사용되는 도구입니다. 데이터와 수식은 포함된 Excel 스프레드시트로 가져오거나 직접 입력합니다. Flash 인터페이스는 다양한 분석 및 대시보드를 표시할 수 있는 캔버스를 제공합니다.

데이터는 SAP BusinessObjects Business Intelligence 플랫폼에서 동적으로 업데이트할 수 있으며, PowerPoint, PDF 또는 Flash 등의 표준 형식을 사용하여 데이터 소비자가 볼 수 있는 다양한 형식으로 내보낼 수 있습니다.

2.4.3.4 SAP BusinessObjects Explorer

SAP BusinessObjects Explorer는 강력한 검색 기능을 사용하여 회사 데이터에서 신속하게 비즈니스 관련 질문에 대한 답변을 직접 검색할 수 있도록 해주는 데이터 검색 응용 프로그램입니다.

SAP BusinessObjects Explorer를 설치하면 SAP BusinessObjects Business Intelligence 플랫폼 중앙 구성 관리자(CCM) 및 중앙 관리 콘솔(CMC)에 다음 서버가 추가됩니다.

- Explorer 마스터 서버: 모든 Explorer 서버를 관리합니다.
- Explorer 인덱싱 서버: 정보 공간 데이터 및 메타데이터의 인덱싱을 제공하고 관리합니다.
- Explorer 검색 서버: 검색 쿼리를 처리하고 결과를 반환합니다.
- Explorer 탐색 서버: 데이터 검색, 필터링 및 집계 등의 정보 공간 탐색 및 분석 기능을 제공하고 관리합니다.

2.4.4 웹 응용 프로그램 클라이언트

웹 응용 프로그램 클라이언트는 웹 응용 프로그램 서버에 있으며 클라이언트 웹 브라우저에서 액세스됩니다. 웹 응용 프로그램은 SAP BusinessObjects Business Intelligence 플랫폼을 설치할 때 자동으로 배포됩니다.

웹 응용 프로그램은 사용자가 웹 브라우저에서 간편하게 액세스할 수 있으며, 조직 네트워크 외부의 사용자 액세스를 허용할 필요가 있을 때 SSL 암호화를 통해 통신을 안전하게 관리할 수 있습니다.

Java 웹 응용 프로그램은 번들 WDeploy 명령줄 도구를 사용하여 초기 설치 후에 재구성하거나 배포할 수도 있으며, 이렇게 하면 다음의 두 가지 방법으로 웹 응용 프로그램을 웹 응용 프로그램 서버에 배포할 수 있습니다.

1. 독립 실행형 모드

동적 콘텐츠와 정적 콘텐츠를 모두 제공하는 웹 응용 프로그램 서버에 모든 웹 응용 프로그램 리소스를 배포합니다. 이 배열은 소규모 설치에 적합합니다.

2. 분할 모드

웹 응용 프로그램의 정적 콘텐츠(HTML, 이미지, CSS)는 전용 웹 서버에 배포되는 반면, 동적 콘텐츠(JSP)는 웹 응용 프로그램 서버에 배포됩니다. 이 배열은 정적 웹 콘텐츠를 제공함으로써 웹 응용 프로그램 서버 공간을 확보할 수 있다는 이점을 지닌 대규모 설치에 적합합니다.

WDeploy에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 웹 응용 프로그램 배포 가이드를 참조하십시오.

2.4.4.1 중앙 관리 콘솔(CMC)

중앙 관리 콘솔(CMC)은 사용자 관리, 콘텐츠 관리 및 서버 관리를 포함하여 관리 작업을 수행하는 데 사용되는 웹 기반 도구입니다. 사용자가 보안 설정을 게시 및 구성할 수도 있습니다. CMC는 웹 기반 응용 프로그램이므로 이러한 모든 관리 작업을 서버에 연결할 수 있는 모든 컴퓨터의 웹 브라우저를 통해 원격으로 수행할 수 있습니다.

모든 사용자는 CMC에 로그인하여 자신의 기본 설정을 변경할 수 있습니다. 또한 해당 권한이 명시적으로 부여되지 않은 경우 Administrators 그룹의 멤버만 관리 설정을 변경할 수 있습니다. 일부 사용자에게 보조 관리 작업을 수행할 수 있는 권한을 부여하도록 역할을 CMC에 할당할 수도 있습니다.

2.4.4.2 BI 실행 패드

BI 실행 패드(이전 이름: InfoView)는 최종 사용자가 게시된 Business Intelligence(BI) 보고서를 보고 예약하고 추적하기 위해 액세스하는 웹 기반 인터페이스입니다. BI 실행 패드를 사용하면 보고서, 분석, 대시보드, 점수 카드 및 전략 맵을 비롯한 모든 유형의 Business Intelligence에 액세스하고 상호 작용하고 내보낼 수 있습니다.

BI 실행 패드를 통해 사용자는 다음 항목을 관리할 수 있습니다.

- BI 카탈로그 탐색 및 검색
- BI 콘텐츠 액세스(만들기, 편집 및 보기)
- BI 콘텐츠 일정 설정 및 게시

2.4.4.3 BI 작업 영역

BI 작업 영역(이전 이름: Dashboard Builder)에서는 모듈(데이터 템플릿) 및 BI 작업 영역(하나 이상의 모듈의 데이터 표시)을 사용하여 비즈니스 활동과 성능을 추적할 수 있습니다. 모듈과 BI 작업 영역에는 조건이 변경되어 이에 따라 비즈니스 규칙을 조정해야 할 때 필요한 정보가 제공됩니다. BI 작업 영역과 모듈 관리를 통해 주요 비즈니스 데이터를 추적하고 분석할 수 있으며 통합된 공동 작업 및 워크플로 기능을 통해 그룹 의사 결정과 분석에도 활용할 수 있습니다. 다음은 BI 작업 영역에서 제공하는 기능입니다.

- 탭 기반 찾아보기
- 페이지 만들기: BI 작업 영역 및 모듈 관리
- 포인트 후 클릭 응용 프로그램 작성기
- 자세한 데이터 분석을 위한 모듈 간 콘텐츠 연결

참고:

BI 작업 영역 기능을 사용하려면 BI 작업 영역 사용 계약이 포함된 SAP BusinessObjects Business Intelligence 플랫폼 라이선스를 구입해야 합니다.

2.4.4.4 보고서 뷰어

보고서 뷰어는 다른 플랫폼과 다른 브라우저를 지원하고 다음 두 개의 범주 중 하나에 속합니다.

- 클라이언트측 보고서 뷰어(Active X 뷰어, Java 뷰어)

클라이언트측 보고서 뷰어는 사용자의 브라우저에 다운로드된 후 설치됩니다. 사용자가 보고서를 요청하면 응용 프로그램 서버는 요청을 처리하고 SAP BusinessObjects Business Intelligence 플랫폼에서 보고서 페이지를 검색합니다. 그런 다음 응용 프로그램 서버는 보고서 페이지를 클라이언트측 뷰어에 전달합니다. 이 뷰어에서는 보고서 페이지를 처리하여 브라우저에 표시합니다.

- 제로 클라이언트 보고서 뷰어(DHTML 뷰어)

제로 클라이언트 보고서 뷰어는 웹 응용 프로그램 서버에 있습니다. 사용자가 보고서를 요청하면 웹 응용 프로그램 서버는 SAP BusinessObjects Business Intelligence 플랫폼에서 보고서 페이지를 검색하고 DHTML 페이지를 만들어 웹 브라우저에 표시합니다.

모든 보고서 뷰어는 보고서 요청을 처리하고 웹 브라우저에 나타나는 보고서 페이지를 표시합니다.

각 보고서 뷰어에서 제공하는 특정 기능 또는 플랫폼 지원에 대한 자세한 내용은 BI 실행 패드 사용자 가이드, Report Application Server .NET SDK Developer Guide 또는 Viewers Java SDK Developer Guide를 참조하십시오.

2.4.4.5 SAP BusinessObjects Web Intelligence

SAP BusinessObjects Web Intelligence는 단일 웹 기반 제품에서 관계형 데이터 소스에 대한 쿼리, 보고 및 분석 기능을 제공하는 웹 기반 도구입니다.

이 도구를 통해 사용자는 보고서를 만들고 임시 쿼리를 수행하고 데이터를 분석하고 끌어 놓기 인터페이스에서 보고서 서식을 지정할 수 있습니다. Web Intelligence는 기본 데이터 소스를 간단히 표시합니다.

보고서를 지원되는 웹 포털에 게시할 수도 있고 BusinessObjects Live Office를 사용하여 Microsoft Office 응용 프로그램에 게시할 수도 있습니다.

2.4.4.6 SAP BusinessObjects Analysis, OLAP 에디션

SAP BusinessObjects Analysis, OLAP 에디션(이전 이름: Voyager)은 다차원 데이터 작업을 수행하는 데 필요한 BI 실행 패드 포털의 OLAP(Online Analytical Processing) 도구입니다. 단일 작업 영역 내의 서로 다른 OLAP 데이터 소스에서 정보를 결합할 수도 있습니다. 지원되는 OLAP 공급자에는 SAP BW 및 Microsoft Analysis Services가 포함됩니다.

Analysis OLAP 기능 집합은 SAP Crystal Reports(운영 보고를 위한 OLAP 큐브로의 직접 데이터 액세스)와 SAP BusinessObjects Web Intelligence(OLAP 데이터 소스의 유니버스로 임시 분석 보고)의 요소가 결합되어 구성됩니다. 또한, 다양한 비즈니스 및 시간 계산 기능을 제공하며 OLAP 데이터를 가능한 한 간단하게 분석하는 데 도움이 되도록 시간 슬라이더 같은 기능을 포함하고 있습니다.

참고:

Analysis, OLAP 에디션 웹 응용 프로그램은 Java 웹 응용 프로그램으로만 사용할 수 있습니다. .NET의 경우에는 해당하는 응용 프로그램이 없습니다.

2.4.4.7 SAP BusinessObjects Mobile

SAP BusinessObjects Mobile을 통해 사용자는 무선 장치의 데스크톱 클라이언트에서 사용할 수 있는 것과 동일한 Business Intelligence(BI) 보고서, 메트릭 및 실시간 데이터에 원격으로 액세스할 수 있습니다. 콘텐츠가 모바일 장치에 최적화되므로 사용자는 추가 교육 없이도 친숙한 보고서에 쉽게 액세스하고 탐색 및 분석을 수행할 수 있습니다.

SAP BusinessObjects Mobile을 사용하여 관리 및 정보 작업자는 항상 최신 정보를 볼 수 있고 최신 정보를 사용하여 의사 결정을 수행할 수 있습니다. 영업 및 현장 서비스 직원은 언제 어디서나 필요한 고객, 제품 및 작업 주문 정보를 정확하게 제공할 수 있습니다.

SAP BusinessObjects Mobile은 BlackBerry, Windows Mobile, Symbian 등의 다양한 모바일 장치를 지원합니다.

모바일 설치, 구성 및 배포에 대한 자세한 내용은 SAP BusinessObjects Mobile 설치 및 배포 가이드를 참조하십시오. SAP BusinessObjects Mobile 사용에 대한 자세한 내용은 SAP BusinessObjects Mobile 사용 가이드를 참조하십시오.

2.5 정보 워크플로

로그인, 보고서 예약 또는 보고서 조회와 같은 작업을 SAP BusinessObjects Business Intelligence 플랫폼에서 수행할 경우, 정보가 시스템을 통해 전달되고 서버는 정보를 서로 주고 받습니다. 다음 단원에서는 SAP BusinessObjects Business Intelligence 플랫폼 시스템에서 발생할 수 있는 일부 프로세스 흐름에 대해 설명합니다.

2.5.1 인증

2.5.1.1 SAP BusinessObjects Business Intelligence 플랫폼 로그인

이 워크플로에서는 사용자가 웹 브라우저에서 SAP BusinessObjects Business Intelligence 플랫폼에 로그인하는 과정을 설명합니다.

1. 브라우저가 웹 서버를 거쳐 웹 응용 프로그램 서버로 로그인 요청을 보냅니다.
2. 웹 응용 프로그램 서버가 요청이 로그인 요청임을 확인합니다. 웹 응용 프로그램 서버가 인증을 위해 사용자 이름, 암호 및 인증 유형을 CMS로 보냅니다.

3. CMS가 적절한 데이터베이스를 기준으로 사용자 이름과 암호의 유효성을 검사합니다. 이 경우에는 Enterprise 인증이 사용되며 사용자 자격 증명이 CMS 시스템 데이터베이스를 기준으로 인증됩니다.
4. 유효성 검사가 끝나면 CMS가 메모리에 해당 사용자를 위한 세션을 만듭니다.
5. CMS가 웹 응용 프로그램 서버에 응답을 보내 유효성 검사가 완료되었음을 알립니다. 웹 응용 프로그램 서버는 메모리에 사용자 세션의 로그인 토큰을 생성합니다. 그런 다음 웹 응용 프로그램 서버는 로그인 토큰을 사용하여 CMS에 대해 사용자의 유효성을 검사합니다.
6. 웹 응용 프로그램 서버가 HTML 페이지를 생성하여 클라이언트로 보냅니다. 웹 응용 프로그램 서버는 사용자 컴퓨터로 응답을 다시 보냅니다. 사용자 컴퓨터에서는 이러한 응답이 웹 클라이언트에 렌더링됩니다.

2.5.1.2 SIA 시작

SIA(Server Intelligence Agent)는 호스트 운영 체제에서 자동으로 시작하도록 구성하거나, 중앙 구성 관리자(CCM)에서 수동으로 시작할 수 있습니다.

SIA는 중앙 관리 서버(CMS)에서 관리하는 서버 관련 정보를 검색합니다. SIA가 로컬 CMS를 사용하고 해당 CMS가 실행되지 않은 경우, SIA는 CMS를 시작합니다. SIA가 원격 CMS를 사용하는 경우 CMS에 연결을 시도합니다.

SIA가 시작되면 다음 이벤트가 순서대로 수행됩니다.

1. SIA는 CMS의 위치를 찾기 위해 캐시를 검토합니다.
 - a. SIA가 로컬 CMS를 시작하도록 구성되고 CMS가 실행 중이 아니면 SIA는 CMS를 시작하고 연결합니다.
 - b. SIA가 실행 중인 CMS(로컬 또는 원격)를 사용하도록 구성된 경우 캐시에서 첫 번째 CMS로의 연결을 시도합니다. CMS를 현재 사용할 수 없는 경우 캐시에서 다음 CMS로의 연결을 시도합니다. 캐시된 CMS 중 아무 것도 사용할 수 없는 경우 SIA는 CMS를 사용할 수 있게 될 때까지 기다립니다.
2. CMS는 SIA의 ID가 유효한지 확인합니다.
3. SIA가 성공적으로 CMS에 연결되면 서버 목록을 관리하도록 요청합니다.
SIA는 관리하는 서버 관련 정보를 저장하지 않습니다. SIA에서 관리되는 서버를 나타내는 구성 정보는 CMS 시스템 데이터베이스에 저장되고 시작 시 SIA에 의해 CMS에서 검색됩니다.
4. CMS는 SIA에서 관리되는 서버 목록이 있는지 CMS 시스템 데이터베이스를 쿼리합니다. 각 서버의 구성도 검색됩니다.
5. CMS는 서버 목록과 구성을 SIA로 반환합니다.
6. 자동으로 시작되도록 구성된 각 서버의 경우 SIA는 적절한 구성을 적용하여 시작하고 상태를 모니터링합니다. SIA에 의해 시작된 각 서버는 SIA에서 사용된 것과 동일한 CMS를 사용하도록 구성됩니다.
SIA와 함께 자동으로 시작되도록 구성되지 않은 서버는 시작되지 않습니다.

2.5.1.3 SIA 종료

SIA(Server Intelligence Agent)는 호스트 운영 체제에서 자동으로 중지하도록 구성하거나, 중앙 구성 관리자(CCM)에서 수동으로 중지할 수 있습니다.

SIA가 종료되면 다음 단계가 수행됩니다.

1. CMS는 SIA에게 중지하라고 알립니다.
2. SIA는 CMS에게 종료되고 있다고 알립니다.
 - a. 운영 체제가 종료되어 SIA가 중지된 경우 SIA는 서버가 중지되도록 요청합니다. 25초 이내에 중지되지 않는 서버는 강제 종료됩니다.
 - b. SIA가 수동으로 중지되고 있으면 관리되는 서버가 기존 작업의 처리를 완료할 때까지 기다립니다. 관리되는 서버는 새 작업을 허용하지 않습니다. 모든 작업이 완료되면 서버가 중지됩니다. 모든 서버가 중지되면 SIA도 중지됩니다.

참고:

강제 종료 중에 SIA는 모든 관리되는 서버에게 즉시 중지하라고 알립니다.

2.5.2 일정

2.5.2.1 SAP Crystal 보고서 예약

이 워크플로는 사용자가 SAP Crystal 보고서를 이후 시간에 실행하도록 예약하는 프로세스에 대해 설명합니다.

1. 웹 클라이언트가 일반적으로 웹 서버를 통해 URL 요청 방식으로 일정 요청을 웹 응용 프로그램 서버에 제출합니다.
2. 웹 응용 프로그램 서버가 URL 요청을 해석하여 이 요청이 일정 요청임을 확인합니다. 웹 응용 프로그램 서버가 일정 시간, 데이터베이스 로그인 값, 매개 변수 값, 대상, 서식을 지정된 CMS로 보냅니다.

3. 중앙 관리 서버(CMS)가 사용자에게 개체를 예약할 권한이 있는지 확인합니다. 사용자에게 충분한 권한이 있는 경우 CMS는 CMS 시스템 데이터베이스에 새 레코드를 추가합니다. 또한 보류 중인 일정 목록에 인스턴스를 추가합니다.

2.5.2.2 SAP Crystal 보고서를 즉시 실행하도록 예약

이 워크플로는 사용자가 SAP Crystal 보고서를 즉시 실행하도록 예약하는 프로세스에 대해 설명합니다.

1. 사용자가 보고서를 예약하면 요청이 웹 응용 프로그램 서버로 전송됩니다.
2. 웹 응용 프로그램 서버가 요청을 중앙 관리 서버(CMS)로 전달합니다.
3. CMS가 사용자에게 보고서를 예약할 수 있는 적절한 권한이 있는지 여부를 확인합니다.
4. 사용자에게 보고서를 예약할 수 있는 적절한 권한이 있는 경우 CMS는 예약된 개체 요청을 CMS 시스템 데이터베이스로 커밋합니다.
5. 예약 시간이 되면 CMS가 각 Crystal Reports 작업 서버에 대해 구성된 허용된 최대 작업 수를 기준으로 사용 가능한 Crystal Reports 작업 서버를 찾습니다.
6. CMS가 작업 정보를 Crystal Reports 작업 서버로 보냅니다.
7. Crystal Reports 작업 서버가 이 보고서가 저장된 입력 파일 리포지토리 서버(FRS)의 위치를 확인합니다. 그런 다음 Crystal Reports 작업 서버는 입력 FRS에 보고서 템플릿을 요청합니다.
8. 입력 FRS가 보고서 템플릿을 찾아 Crystal Reports 작업 서버로 스트리밍합니다.
9. 보고서 템플릿이 Crystal Reports 작업 서버의 임시 디렉터리에 저장됩니다.
10. Crystal Reports 작업 서버가 자식 프로세스(JobServerChild.exe)를 시작하여 보고서 실행을 조정합니다.
11. JobServerChild.exe가 ProcReport.dll을 시작하고 Crystal Reports 작업 서버에서 받은 모든 인스턴스를 전달합니다. ProcReport.dll이 Crpe32.dll을 호출합니다.
12. Crpe32.dll이 다음 작업을 완료하면 보고서가 작성됩니다.
 - 보고서를 엽니다.
 - 프로덕션 데이터베이스에 연결합니다.
 - 보고서를 처리합니다.
 - 보고서 인스턴스를 만들어 저장합니다.
 - 보고서를 다시 JobServerChild.exe로 전달합니다.
13. Crystal Reports 작업 서버가 CMS의 작업 상태를 주기적으로 업데이트합니다. 이때 상태는 보고서 처리 중으로 표시됩니다.
14. JobServerChild.exe가 보고서 인스턴스를 출력 FRS로 업로드합니다.
15. 출력 FRS가 JobServerChild.exe에 보고서가 성공적으로 저장되었음을 알립니다.
16. JobServerChild.exe가 Crystal Reports 작업 서버에 보고서 작성이 완료되었음을 알립니다.
17. 보고서 작업 서버가 CMS의 작업 상태를 업데이트합니다. JobServerChild.exe가 메모리에서 자동으로 지워집니다.

18. CMS가 메모리에 작업 상태를 업데이트한 다음 인스턴스 정보를 CMS 시스템 데이터베이스에 씁니다.

2.5.2.3 예약된 SAP Crystal 보고서 실행

이 워크플로는 예약된 SAP Crystal 보고서를 예정된 시간에 실행하는 프로세스에 대해 설명합니다.

1. 중앙 관리 서버(CMS)가 해당 시간에 실행되는 예약된 SAP Crystal 보고서가 있는지 확인하기 위해 CMS 시스템 데이터베이스를 검사합니다.
2. 예약된 작업 시간이 되면 CMS가 각 Crystal Reports 작업 서버에 구성된 허용된 최대 작업 수를 기준으로 사용 가능한 Crystal Reports 작업 서버를 찾습니다. CMS는 작업 정보를 Crystal Reports 작업 서버로 보냅니다. CMS가 Crystal Reports 작업 서버로 보내는 정보는 보고서 ID, 서식, 대상, 로그인 정보, 매개 변수, 선택 수식입니다.
3. Crystal Reports 작업 서버가 입력 FRS(파일 리포지토리 서버)와 통신하여 요청된 보고서 ID에 따라 보고서 템플릿을 가져옵니다.
4. Crystal Reports 작업 서버가 JobChildserver 프로세스를 시작합니다.
5. Enterprise 인프라를 통해 입력 파일 리포지토리 서버에서 템플릿을 받으면 자식 프로세스(JobChildserver)가 ProcReport.dll을 시작합니다. ProcReport.dll에는 CMS에서 Crystal Reports 작업 서버로 전달된 모든 매개 변수가 포함되어 있습니다.
6. ProcReport.dll이 전달된 모든 매개 변수에 따라 보고서를 처리하는 Crpe32.dll을 시작합니다.
7. 보고서가 처리되는 동안 보고서 내에 정의된 데이터베이스 서버에서 레코드가 검색됩니다.
8. Crystal Reports 작업 서버가 CMS의 작업 상태를 주기적으로 업데이트합니다. 이때 상태는 처리 중으로 표시됩니다.
9. 보고서를 Crystal Reports 작업 서버의 메모리로 컴파일한 후에는 PDF(Portable Document Format)와 같은 다른 형식으로 내보내야 합니다. PDF로 내보내는 경우 PDF.dll이 사용됩니다.
10. 또한 데이터가 저장된 보고서를 기본 위치에 제출해야 합니다. 그러면 출력 FRS로 전송됩니다.
11. 이 프로세스가 완료되면 Crystal Reports 작업 서버에서 CMS의 작업 상태를 업데이트합니다. 이때 상태는 성공으로 보고됩니다.
12. CMS가 메모리에 작업 상태를 업데이트한 다음 인스턴스 정보를 CMS 시스템 데이터베이스에 씁니다.

2.5.2.4 SAP BusinessObjects Web Intelligence 문서 예약

이 워크플로에서는 사용자가 SAP BusinessObjects Web Intelligence 문서를 나중에 실행하도록 예약하는 과정에 대해 설명합니다.

1. 사용자가 문서 일정을 설정하면 요청이 웹 서버로 전송됩니다. 웹 서버가 문서 일정 요청을 웹 응용 프로그램 서버로 전달합니다.
2. 웹 응용 프로그램 서버가 문서 일정 요청을 CMS로 전달합니다.
3. CMS가 사용자에게 문서를 예약할 수 있는 적절한 권한이 있는지 여부를 확인합니다.
4. 관련된 모든 예약 정보가 포함된 SAP BusinessObjects Web Intelligence 문서의 인스턴스가 CMS에 만들어집니다.
5. 사용자에게 문서를 예약할 적절한 권한이 있는 경우 다른 예약 매개 변수를 설정합니다.
6. CMS가 예약된 개체 요청을 시스템 데이터베이스에 커밋합니다.

2.5.2.5 예약된 SAP BusinessObjects Web Intelligence, OLAP 에디션 문서 실행

이 워크플로에서는 예약된 SAP BusinessObjects Web Intelligence 문서를 예정된 시간에 실행하는 과정에 대해 설명합니다.

1. 중앙 관리 서버(CMS)에서는 CMS 시스템 데이터베이스를 확인하여 실행 예정된 SAP BusinessObjects Web Intelligence 작업이 있는지 확인합니다.
2. 예약 시간이 되면 CMS는 SAP BusinessObjects Web Intelligence 예약 및 게시 서비스가 실행되는 적응형 작업 서버에 예약 요청과 이 예약에 대한 모든 정보를 전송합니다.
3. 적응형 작업 서버(Web Intelligence 예약 및 게시 서비스)는 각 SAP BusinessObjects Business Web Intelligence 처리 서버에 구성된 허용된 최대 작업 수를 참고하여 사용 가능한 Web Intelligence 처리 서버를 찾습니다.
4. SAP BusinessObjects Web Intelligence 처리 서버는 문서와 이 문서의 기반이 되는 유니버스 메타계층 파일을 보관하는 입력 파일 리포지토리 서버(FRS)의 위치를 찾습니다. 그리고 SAP BusinessObjects Web Intelligence 처리 서버가 입력 FRS의 문서를 요청합니다. 입력 FRS는 SAP BusinessObjects Web Intelligence 문서 및 해당 문서의 기반이 되는 유니버스 파일을 찾은 후 SAP BusinessObjects Business Web Intelligence 처리 서버로 이를 보냅니다.
5. SAP BusinessObjects Web Intelligence 문서가 SAP BusinessObjects Web Intelligence 처리 서버의 임시 디렉터리에 저장됩니다. SAP BusinessObjects Web Intelligence 처리 서버의 메모리에서 이 문서가 열립니다. QT.dll이 문서의 기반이 되는 유니버스에서 SQL을 생성합니다. 연결 서버(SAP BusinessObjects Web Intelligence 프로세스 서버의 구성 요소)가 데이터베이스에 연결됩니다. 쿼리 데이터는 QT.dll을 통해 문서가 처리되는 문서 엔진으로 다시 전달됩니다. 성공한 새 인스턴스가 만들어집니다.
6. SAP BusinessObjects Web Intelligence 처리 서버가 이 문서 인스턴스를 출력 FRS에 업로드합니다.
7. SAP BusinessObjects Web Intelligence 처리 서버는 문서 작성이 완료되었음을 적응형 작업 서버(SAP BusinessObjects Web Intelligence 예약 및 게시 서비스)에 알립니다. 문서가 대상(파일 시스템, FTP, SMTP 또는 받은 파일함)으로 이동하기로 예약되어 있는 경우 적응형 작업 서버가 출력 FRS에서 처리된 문서를 검색하여 지정된 대상으로 배달합니다. 이 예에서는 문서 이동이 예약되어 있지 않다고 가정합니다.

8. 적응형 작업 서버(Web Intelligence 예약 및 게시 서비스)가 CMS의 작업 상태를 업데이트합니다.
9. CMS가 메모리에 작업 상태를 업데이트한 다음 인스턴스 정보를 CMS 시스템 데이터베이스에 씁니다.

2.5.2.6 개체 예약

이 워크플로는 사용자가 개체 실행을 예약하는 프로세스에 대해 설명합니다.

1. 사용자가 개체를 예약하면 요청이 웹 서버로 전송됩니다.
2. 웹 서버가 개체 일정 요청을 웹 응용 프로그램 서버로 전달합니다.
3. 웹 응용 프로그램 서버가 요청을 중앙 관리 서버(CMS)로 전달합니다.
4. CMS가 사용자에게 개체를 예약할 적절한 권한이 있는지 확인합니다.
5. 사용자에게 개체를 예약할 적절한 권한이 있는 경우 CMS는 예약된 개체 요청을 CMS 시스템 데이터베이스로 커밋합니다.
6. 예약 시간이 되면 CMS가 각 프로그램 작업 서버에 구성된 허용된 최대 작업 수를 기반으로 사용 가능한 프로그램 작업 서버를 찾습니다.
7. CMS가 작업 정보를 프로그램 작업 서버로 보냅니다.
8. 프로그램 작업 서버가 입력 파일 리포지토리 서버와 통신하여 프로그램 개체를 요청합니다.
9. 입력 파일 리포지토리 서버가 프로그램 개체를 프로그램 작업 서버로 다시 반환합니다.
10. 프로그램 작업 서버가 예약된 개체를 시작합니다.
11. 프로그램 작업 서버가 CMS의 작업 상태를 주기적으로 업데이트합니다. 이때 상태는 프로그램 처리 중으로 보고됩니다.
12. 프로그램 작업 서버가 로그 파일을 출력 파일 리포지토리 서버로 보냅니다.
13. 출력 파일 리포지토리 서버가 개체 로그 파일을 보내 개체가 성공적으로 예약되었음을 프로그램 작업 서버에 알립니다.
14. 프로그램 작업 서버가 CMS의 작업 상태를 업데이트합니다.
15. CMS가 메모리에 작업 상태를 업데이트한 다음 개체 인스턴스 정보를 CMS 시스템 데이터베이스에 씁니다.

2.5.2.7 개체를 즉시 실행하도록 예약

이 워크플로에서는 사용자가 개체를 즉시 실행하도록 예약하는 과정에 대해 설명합니다.

1. 사용자가 개체를 예약하면 요청이 웹 서버로 전송됩니다.

2. 웹 서버가 개체 일정 요청을 웹 응용 프로그램 서버로 전달합니다.
3. 웹 응용 프로그램 서버가 요청을 중앙 관리 서버(CMS)로 전달합니다.
4. CMS가 사용자에게 개체를 예약할 적절한 권한이 있는지 확인합니다.
5. 사용자에게 개체를 예약할 적절한 권한이 있는 경우 CMS는 예약된 개체 요청을 CMS 시스템 데이터베이스로 커밋합니다.
6. 예약 시간이 되면 CMS가 각 프로그램 작업 서버에 구성된 허용된 최대 작업 수를 기반으로 사용할 가능한 프로그램 작업 서버를 찾습니다.
7. CMS가 작업 정보를 프로그램 작업 서버로 보냅니다.
8. 프로그램 작업 서버가 입력 파일 리포지토리 서버와 통신하여 프로그램 개체를 요청합니다.
9. 입력 파일 리포지토리 서버가 프로그램 개체를 프로그램 작업 서버로 다시 반환합니다.
10. 프로그램 작업 서버가 예약된 개체를 시작합니다.
11. 프로그램 작업 서버가 CMS의 작업 상태를 주기적으로 업데이트합니다. 이때 상태는 프로그램 처리 중으로 보고됩니다.
12. 프로그램 작업 서버가 로그 파일을 출력 파일 리포지토리 서버로 보냅니다.
13. 출력 파일 리포지토리 서버가 개체 로그 파일을 보내 개체가 성공적으로 예약되었음을 프로그램 작업 서버에 알립니다.
14. 프로그램 작업 서버가 CMS의 작업 상태를 업데이트합니다.
15. CMS가 메모리에 작업 상태를 업데이트한 다음 개체 인스턴스 정보를 CMS 시스템 데이터베이스에 씁니다.

2.5.3 보기

2.5.3.1 SAP Crystal 보고서 보기

이 워크플로는 보고서가 캐시 서버에 아직 없을 때 사용자가 SAP Crystal 보고서의 페이지를 요청하는 프로세스에 대해 설명합니다.

1. 사용자가 웹 서버를 통해 보기 요청을 웹 응용 프로그램 서버로 보냅니다.
2. 웹 응용 프로그램 서버가 이 요청을 보고서 페이지를 보기 위한 요청으로 인식합니다. 사용자에게 보고서를 볼 수 있는 충분한 권한이 있는지 확인하기 위해 웹 응용 프로그램 서버가 중앙 관리 서버(CMS)를 검사합니다.
3. CMS가 사용자에게 보고서를 볼 적절한 권한이 있는지 확인합니다.

4. CMS가 사용자에게 보고서를 볼 수 있는 충분한 권한이 있음을 확인하는 응답을 웹 응용 프로그램 서버에 보냅니다.
5. 웹 응용 프로그램 서버가 요청된 보고서 페이지에 대한 요청을 Crystal Reports 캐시 서버로 보냅니다.
6. Crystal Reports 캐시 서버가 캐시 디렉터리에 요청된 파일이 있는지 확인합니다.
7. 캐시 디렉터리에 요청된 EPF 파일이 없습니다.
8. Crystal Reports 캐시 서버가 이 요청을 Crystal Reports 페이지 서버로 보냅니다.
9. Crystal Reports 페이지 서버가 출력 파일 리포지토리 서버(FRS)를 쿼리하여 요청된 보고서 인스턴스가 있는지 확인합니다.
10. 출력 FRS가 요청된 보고서 인스턴스를 Crystal Reports 페이지 서버로 보냅니다.
11. Crystal Reports 페이지 서버가 보고서 인스턴스를 열고 보고서를 검사하여 보고서에 데이터가 있는지 확인합니다.
12. Crystal Reports 페이지 서버가 보고서에 데이터가 포함되어 있음을 확인한 후 프로덕션 데이터베이스에 연결하지 않고 요청된 보고서 페이지에 대한 파일을 만듭니다.
13. Crystal Reports 페이지 서버가 EPF 파일을 Crystal Reports 캐시 서버로 보냅니다.
14. Crystal Reports 캐시 서버가 EPF 파일을 캐시 디렉터리에 씁니다.
15. Crystal Reports 캐시 서버가 요청된 페이지를 웹 응용 프로그램 서버로 보냅니다.
16. 웹 응용 프로그램 서버가 파일을 웹 서버로 전달합니다.
17. 웹 서버가 요청된 페이지를 보고서 뷰어로 보냅니다.

2.5.3.2 캐시된 SAP Crystal 보고서 보기

이 워크플로는 보고서가 캐시 서버에 이미 있을 때 사용자가 SAP Crystal 보고서의 페이지를 요청하는 프로세스에 대해 설명합니다.

1. 웹 클라이언트가 URL 형식으로 보기 요청을 웹 응용 프로그램 서버로 보냅니다.
2. 웹 응용 프로그램 서버가 요청을 해석하여 이 요청이 선택된 보고서 인스턴스의 첫 번째 페이지를 보기 위한 요청임을 확인합니다. 웹 응용 프로그램 서버가 중앙 관리 서버(CMS)로 요청을 보내 사용자에게 인스턴스를 볼 수 있는 권한이 있는지 확인합니다.
3. CMS가 CMS 시스템 데이터베이스를 검사하여 사용자 권한을 확인합니다.
4. CMS가 사용자에게 인스턴스를 볼 수 있는 충분한 권한이 있음을 확인하는 응답을 웹 응용 프로그램 서버에 보냅니다.
5. 웹 응용 프로그램 서버가 보고서 인스턴스의 첫 번째 페이지에 대한 요청을 Crystal Reports 캐시 서버로 보냅니다. Crystal Reports 캐시 서버가 이 페이지가 존재하는지 확인합니다. 이 페이지가 존재하는 경우 Crystal Reports 캐시 서버는 웹 응용 프로그램 서버로 이 페이지를 반환합니다.
6. 페이지가 렌더링되어 표시되는 웹 클라이언트로 웹 응용 프로그램 서버가 페이지를 보냅니다.

2.5.3.3 SAP Analysis, OLAP 에디션 작업 영역 표시

이 워크플로에서는 사용자가 SAP Analysis, OLAP 에디션(이전 이름: Voyager) 작업 영역을 요청하는 프로세스에 대해 설명합니다.

1. 웹 클라이언트가 새 작업 영역을 보기 위해 웹 서버를 통해 요청을 웹 응용 프로그램 서버로 보냅니다. 웹 클라이언트가 DHTML AJAX 기술(비동기 JavaScript와 XML)을 사용하여 웹 응용 프로그램 서버와 통신합니다. AJAX 기술을 사용하면 부분 페이지 업데이트가 가능하므로 새 요청 각각에 대해 새 페이지를 렌더링할 필요가 없습니다.
2. 웹 응용 프로그램 서버가 요청을 변환한 다음 중앙 관리 서버(CMS)로 보내 사용자가 새 작업 영역을 보거나 만들 수 있는 권한이 있는지 여부를 확인합니다.
3. CMS가 CMS 시스템 데이터베이스에서 사용자의 자격 증명을 검색합니다.
4. 사용자가 작업 영역을 보거나 만들 수 있는 경우 CMS는 웹 응용 프로그램 서버에 대해 자격 증명을 확인합니다. 이와 동시에 사용 가능한 하나 이상의 MDAS(Multi-Dimensional Analysis Server) 목록도 보냅니다.
5. 웹 응용 프로그램 서버가 사용 가능한 선택 사항 목록에서 MDAS를 선택하고 CORBA 요청을 서버로 보내 새 작업 영역을 만들거나 기존 작업 영역을 새로 고칠 수 있도록 적절한 OLAP 서버를 찾습니다.
6. MDAS 서버는 입력 파일 리포지토리 서버(FRS)와 통신하여 기본 OLAP 데이터베이스 및 이와 함께 저장된 초기 OLAP 쿼리에 대한 정보가 들어 있는 적절한 작업 영역 문서를 검색해야 합니다. 입력 FRS가 기본 디렉터리에서 적절한 Advanced Analyzer 작업 영역을 검색한 다음 이 작업 영역을 다시 MDAS로 스트리밍합니다.
7. MDAS 서버가 작업 영역을 열고 쿼리를 공식화한 후 OLAP 데이터베이스 서버로 보냅니다. MDAS에는 OLAP 데이터 소스에 맞게 구성된 적절한 OLAP 데이터베이스 클라이언트가 있어야 합니다. 웹 클라이언트 쿼리는 적절한 OLAP 쿼리로 변환되어야 합니다. OLAP 데이터베이스 서버가 쿼리 결과를 다시 MDAS로 보냅니다.
8. MDAS는 작성, 보기, 인쇄 또는 내보내기 요청에 따라 결과를 사전 렌더링하므로 Java WAS는 렌더링을 보다 신속하게 마칠 수 있습니다. MDAS가 렌더링된 결과의 XML 패키지를 웹 응용 프로그램 서버로 다시 보냅니다.
9. 웹 응용 프로그램 서버가 작업 영역을 렌더링하고 웹 서버를 통해 서식이 지정된 페이지 또는 페이지의 일부를 웹 클라이언트로 보냅니다. 웹 클라이언트가 업데이트된 요청 페이지나 새로 요청된 페이지를 표시합니다. 이것이 Java 또는 ActiveX 구성 요소를 다운로드하지 않아도 되는 제로 클라이언트 솔루션입니다.

2.5.4 요청 시

2.5.4.1 요청 시 SAP Crystal 보고서 보기

이 워크플로는 사용자가 요청 시 SAP Crystal 보고서 페이지를 요청하는 프로세스에 대해 설명합니다.

1. 웹 클라이언트가 일반적으로 웹 서버를 통해 URL 요청 방식으로 요청 시 보기 요청을 웹 응용 프로그램 서버로 보냅니다.
2. 웹 응용 프로그램 서버가 URL 요청에서 전송된 요청된 페이지와 값을 해석하여 이 요청이 선택된 보고서 개체의 첫 번째 페이지를 보기 위한 요청임을 확인합니다.
3. 웹 응용 프로그램 서버가 중앙 관리 서버(CMS)로 요청을 보내 사용자에게 개체를 볼 수 있는 권한이 있는지 확인합니다. CMS가 CMS 시스템 데이터베이스를 검사하여 사용자 권한을 확인합니다.
4. CMS가 사용자에게 개체를 볼 수 있는 충분한 권한이 있음을 확인하는 응답을 웹 응용 프로그램 서버에 보냅니다.
5. 웹 응용 프로그램 서버가 보고서 개체의 첫 번째 페이지에 대한 요청을 Crystal Reports 캐시 서버로 보냅니다.
6. Crystal Reports 캐시 서버가 이 페이지가 존재하는지 확인합니다. 보고서가 요청 시 보고서 공유에 대한 요구 사항(매개 변수, 데이터베이스 로그인, 다른 요청 시 요청의 설정 시간 이내)을 충족하지 않을 경우 Crystal Reports 캐시 서버는 Crystal Reports 처리 서버가 페이지를 생성하도록 요청을 보냅니다.
7. Crystal Reports 처리 서버가 입력 파일 리포지토리 서버에 보고서 개체를 요청합니다. 입력 파일 리포지토리 서버가 개체 복사본을 Crystal Reports 처리 서버로 스트리밍합니다. Crystal Reports 처리 서버가 메모리에 있는 보고서를 열고 이 보고서에 데이터가 포함되어 있는지 확인합니다.
8. 보고서 개체에 데이터가 없다고 가정할 경우 데이터를 쿼리하기 위해서는 Crystal Reports 처리 서버에서 데이터베이스에 연결해야 합니다.
9. Crystal Reports 처리 서버가 페이지를 Crystal Reports 캐시 서버로 보냅니다. 나중에 새 보기 요청이 있을 수 있으므로 Crystal Reports 캐시 서버가 캐시 디렉터리에 페이지 복사본을 저장합니다.
10. Crystal Reports 캐시 서버가 페이지를 웹 응용 프로그램 서버로 보냅니다.
11. 웹 응용 프로그램 서버가 .epf 페이지를 웹 서버로 보냅니다. 웹 서버가 페이지를 사용자 컴퓨터로 보냅니다. 사용자 컴퓨터에서는 이러한 페이지가 웹 클라이언트의 뷰어에서 렌더링됩니다.

2.5.4.2 요청 시 SAP BusinessObjects Web Intelligence 문서 표시

이 워크플로에서는 요청 시 사용자가 SAP BusinessObjects Web Intelligence 문서를 보는 과정에 대해 설명합니다.

1. 웹 브라우저가 웹 서버를 통해 보기 요청을 웹 응용 프로그램 서버로 보냅니다.
2. 웹 응용 프로그램 서버가 이 요청이 Web Intelligence 문서에 대한 것임을 확인하고 요청을 중앙 관리 서버(CMS)로 보내 사용자에게 문서를 볼 수 있는 적절한 권한이 있는지 확인합니다.
3. CMS가 사용자에게 문서를 볼 수 있는 충분한 권한이 있음을 확인하는 응답을 웹 응용 프로그램 서버에 보냅니다.
4. 웹 응용 프로그램 서버가 문서 요청을 Web Intelligence 처리 서버로 보냅니다.
5. Web Intelligence 처리 서버가 입력 파일 리포지토리 서버(FRS)에 문서 외에 요청된 문서가 작성된 유니버스 파일을 요청합니다. 유니버스 파일에는 행 및 열 수준 보안을 비롯한 메타 계층 정보가 포함되어 있습니다.
6. 입력 FRS가 문서 사본 및 요청된 문서가 작성된 유니버스 파일을 Web Intelligence 처리 서버로 스트리밍합니다.
7. Web Intelligence 보고서 엔진이 메모리에 있는 문서를 엽니다.
8. Web Intelligence 보고서 엔진에서는 QT 구성 요소(inproc)와 ConnectionServer(inproc)를 사용합니다. QT 구성 요소는 SQL을 생성/유효성 검사/다시 생성하고 데이터베이스에 연결하여 쿼리를 실행합니다. 연결 서버는 SQL을 사용하여 데이터베이스에서 문서가 처리되는 보고서 엔진으로 데이터를 가져옵니다.
9. Web Intelligence 처리 서버가 보기 가능한 요청된 문서 페이지를 웹 응용 프로그램 서버로 보냅니다. 웹 응용 프로그램 서버가 이 보기 가능한 페이지를 웹 서버로 전달합니다. 웹 서버는 이 보기 가능한 페이지를 사용자 컴퓨터로 보냅니다. 사용자 컴퓨터에서는 이러한 페이지가 웹 브라우저에 렌더링됩니다.

2.5.4.3 기본 보기 형식이 웹 Java로 설정된 경우 요청 시 SAP Crystal 보고서 보기

이 워크플로는 기본 보기 형식이 웹 Java로 설정되어 있을 때 사용자가 SAP Crystal 보고서를 보는 프로세스에 대해 설명합니다.

1. 웹 클라이언트가 웹 서버를 통해 요청 시 보기 요청을 웹 응용 프로그램 서버로 보냅니다.
2. 웹 응용 프로그램 서버가 URL 요청에서 전송된 요청된 페이지와 값을 해석하여 이 요청이 선택된 보고서 개체의 첫 번째 페이지를 보기 위한 요청임을 확인합니다.
3. 웹 응용 프로그램 서버가 중앙 관리 서버(CMS)로 요청을 보내 사용자에게 개체를 볼 수 있는 권한이 있는지 확인합니다. CMS가 CMS 시스템 데이터베이스를 검사하여 사용자 권한을 확인합니다.
4. CMS가 사용자에게 개체를 볼 수 있는 충분한 권한이 있음을 확인하는 응답을 웹 응용 프로그램 서버에 보냅니다.
5. 웹 응용 프로그램 서버가 보고서 개체의 첫 번째 페이지에 대한 요청을 Crystal Reports 캐시 서버로 보냅니다.
6. Crystal Reports 캐시 서버가 이 페이지가 존재하는지 확인합니다. 보고서가 요청 시 보고서 공유에 대한 요구 사항(매개 변수, 데이터베이스 로그인, 다른 요청 시 요청의 설정 시간 이내)을 충족하지 않을 경우 Crystal Reports 캐시 서버는 Crystal Reports 처리 서버가 페이지를 생성하도록 요청을 보냅니다.

7. Crystal Reports 처리 서버가 입력 파일 리포지토리 서버에 보고서 개체를 요청합니다. 입력 파일 리포지토리 서버가 개체 복사본을 Crystal Reports 처리 서버로 스트리밍합니다. Crystal Reports 처리 서버가 메모리에 있는 보고서를 열고 이 보고서에 데이터가 포함되어 있는지 확인합니다.
8. 보고서 개체에 데이터가 없다고 가정할 경우 데이터를 쿼리하기 위해서는 Crystal Reports 처리 서버에서 데이터베이스에 연결해야 합니다.
9. Crystal Reports 처리 서버가 .epf 페이지를 Crystal Reports 캐시 서버로 보냅니다. 나중에 새 보기 요청이 있을 수 있으므로 Crystal Reports 캐시 서버에서는 캐시 디렉터리에 .epf 페이지 복사본을 저장합니다. 또한 이 단계에서는 .etf 페이지가 생성되어 Crystal Reports 캐시 서버로 전송될 수 있습니다. 보고서의 첫 번째 페이지가 생성될 때와 보고서가 그룹화될 때 .etf 페이지(보고서의 왼쪽 창 그룹 트리 탐색)가 생성됩니다. 보고서당 .etf는 하나만 있지만 이 .etf 페이지의 크기는 상당할 수 있습니다.
10. Crystal Reports 캐시 서버가 .epf 페이지를 웹 응용 프로그램 서버로 보냅니다.
11. 웹 응용 프로그램 서버가 .epf 페이지를 웹 서버로 보냅니다. 웹 서버는 .epf 페이지를 사용자 컴퓨터로 보냅니다. 사용자 컴퓨터에서는 이러한 페이지가 웹 클라이언트의 뷰어에서 렌더링됩니다.

장3 라이선스 관리

3.1 라이선스 키 관리

이 단원에서는 BI 플랫폼 배포에 필요한 라이선스 키를 관리하는 방법에 대해 설명합니다.

관련 항목

- 359 페이지에서 [라이선스 정보 보기](#)"
- 360 페이지에서 [라이선스 키 추가](#)"
- 360 페이지에서 [현재 계정 활동을 보려면](#)"

3.1.1 라이선스 정보 보기

CMC의 라이선스 키 관리 영역에서는 역할(BI Viewer 및 BI Analyst)에 따라 각 키와 관련된 동시 라이선스, 명명된 라이선스 및 프로세서 라이선스 수를 확인할 수 있습니다.

1. CMC의 라이선스 키 관리 영역으로 이동합니다.
2. 라이선스 키를 선택합니다.

선택한 키와 관련된 자세한 정보가 라이선스 키 정보 영역에 나타납니다. 추가 라이선스 키를 구입하려면 SAP 영업 담당자에게 문의하십시오.

관련 항목

- 359 페이지에서 [라이선스 키 관리](#)"
- 360 페이지에서 [라이선스 키 추가](#)"
- 360 페이지에서 [현재 계정 활동을 보려면](#)"

3.1.2 라이선스 키 추가

평가판 제품을 업그레이드할 경우에는 새 라이선스 키 또는 정품 인증 키코드를 추가하기 전에 평가용 키를 삭제해야 합니다.

1. CMC의 라이선스 키 관리 영역으로 이동합니다.
2. 키 추가 필드에 키를 입력합니다.
3. 추가를 클릭합니다.

목록에 키가 추가됩니다.

관련 항목

- 359 페이지에서 [라이선스 정보 보기](#)"
- 360 페이지에서 [현재 계정 활동을 보려면](#)"

3.1.3 현재 계정 활동을 보려면

1. CMC의 설정 관리 영역으로 이동합니다.
2. 전역 시스템 메트릭 보기를 클릭합니다.

이 섹션에는 추가 작업 메트릭과 함께 현재 사용하는 라이선스 정보가 표시됩니다.

관련 항목

- 359 페이지에서 [라이선스 키 관리](#)"
- 360 페이지에서 [라이선스 키 추가](#)"
- 359 페이지에서 [라이선스 정보 보기](#)"

3.2 라이선스 측정

BOLMT(BusinessObjects License Measurement Tool)는 BI 플랫폼 라이선스 데이터를 수집 및 저장하는 데 사용되는 Java 명령줄 유틸리티입니다. 출력 XML 문서에는 라이선스 배포 측정값이 포함되어 있으며 이 문서는 라이선스 감사의 일부로 통합되도록 SAP GLAS(Global License Auditing Services)로 전송됩니다.

시스템 관리자는 라이선스 감사가 요청될 때마다 모든 BI 플랫폼 클러스터에 대해 BOLMT를 설치하고 실행합니다. BOLMT에서는 명명된 역할 기반 동시 사용자 라이선스에 대한 사용 측정값을 수집합니다.

관리자는 XML 문서에 대한 특정 출력 디렉토리를 지정하고 시스템 사용자를 식별하는 데 사용할 수 있는 정보를 포함하지 않도록 출력 문서를 구성할 수 있습니다.

3.2.1 라이선스 감사 실행

라이선스 감사를 수행하려면 관리자 권한이 필요하며 BI 플랫폼 설치의 BOLMT.jar 파일이 포함된 디렉터리에 액세스해야 합니다.

1. 명령줄 콘솔을 엽니다.
2. BI 플랫폼을 설치하는 데 필요한 Java 실행 파일이 포함된 디렉터리로 디렉토리를 변경합니다.
기본적으로 이 파일은 [INSTALLDIR]WSAP BusinessObjects Enterprise XI 4.0WjavaWlib 디렉터리에 설치됩니다.
3. BOLMT.jar를 실행합니다.
-jar BOLMT.jar [options] <outputFile>과 같은 형식으로 실행 명령을 입력합니다
아래 표에서는 사용 가능한 옵션에 대해 간략하게 설명합니다.

옵션	설명
-c --cms	중앙 관리 서버(CMS)의 이름 식별자 및 포트 번호를 지정합니다. cm sname:port number로 지정합니다. 이 설정이 지정되어 있지 않으면 기본적으로 로컬 호스트에 대한 CMS 설정이 사용됩니다.
-p --password	CMS에 연결하는 데 사용되는 관리자 계정 암호를 지정합니다.
-a--auth	사용자를 CMS에 연결하는 인증 방법을 지정합니다. 기본 방법은 secEnterprise로 지정된 Enterprise입니다.
-s--sanitize	출력 감사 문서에서 사용자를 식별하는 데 사용할 수 있는 개인 정보를 필터링하도록 지정합니다.

참고:

출력 파일은 항상 명령줄의 마지막 인수로 지정됩니다. 이 설정은 선택 사항입니다. 지정된 인수가 없는 경우 해당 출력이 콘솔의 표준 출력이 됩니다. 또한 명령줄 인수로 스크립트에 출력을 파이프할 수도 있습니다.

예제

```
C:\WProgram Files (x86)\WSAP
Business Objects\WSAP BusinessObjects Enterprise XI 4.0\Wjava\lib>"C:\WProgram Files
(x86)\WSAP Business Objects\WSAP BusinessObjects Enterprise XI 4.0\Wwin64_x64\Wsapjvm\Wbin
Wjava.exe" -jar BOLMT.jar --cms=mycms:6400 -uAdministrator
-p=7juujg --auth=secEnterprise --sanitize audit.xml
```


장4 사용자 및 그룹 관리

4.1 계정 관리 개요

계정 관리는 사용자 및 그룹 정보 작성, 매핑, 변경 및 구성에 관련된 모든 작업이라고 할 수 있습니다. 중앙 관리 콘솔(CMC)의 사용자 및 그룹 관리 영역을 사용하여 이러한 작업을 중앙에서 수행할 수 있습니다.

사용자 계정과 그룹이 만들어지면 개체를 추가하고 권한을 지정할 수 있습니다. 사용자는 로그인한 후 BI 실행 패드 또는 사용자 지정 웹 응용 프로그램을 사용하여 개체를 볼 수 있습니다.

4.1.1 사용자 관리

사용자 및 그룹 관리 영역에서는 사용자가 BI 플랫폼에 액세스하는 데 필요한 모든 항목을 지정할 수 있습니다. 기본 사용자 계정 표에 요약되어 있는 두 개의 기본 사용자 계정도 볼 수 있습니다.

테이블4-1: 기본 사용자 계정

계정 이름	설명
관리자	이 사용자는 관리자 및 Everyone 그룹에 속합니다. 관리자는 모든 BI 플랫폼 응용 프로그램(예: CMC, CCM, 게시 마법사 및 BI 실행 패드)에서 모든 작업을 수행할 수 있습니다.
Guest	이 사용자는 Everyone 그룹에 속합니다. 이 계정은 기본적으로 활성화되고 시스템에서 암호가 할당되지 않습니다. 이 사용자에게 암호를 할당하면 BI 실행 패드에 대한 단일 로그온을 사용할 수 없게 됩니다.

계정 이름	설명
SMAAdmin	SAP Solution Manager에서 BI 플랫폼 구성 요소에 액세스하는 데 사용하는 읽기 전용 계정입니다.

4.1.1.1 역할 기반 라이선스

사용자 역할 기반 라이선스 체계에서는 다음 두 가지 역할을 BI 플랫폼 사용자에게 할당할 수 있습니다.

- BI Analyst
- BI Viewer

각 역할은 BI 플랫폼 응용 프로그램에 대한 특정 액세스 수준과 함께 제공됩니다. 이 사용자 역할에 대한 액세스 수준을 수정하거나 무시할 수 없습니다. 사용자 역할은 BI 플랫폼에서 만든 새 사용자 계정 또는 타사 디렉터리 서비스(예: Windows AD 또는 LDAP)에서 가져온 기존 사용자에게 적용됩니다.

참고:

사용자 역할을 소속 그룹과 혼동해서는 안 됩니다. 사용 가능한 두 역할 중 하나를 사용자에게 할당하면 응용 프로그램에 대해 미리 정의된 권한이 자동으로 해당 사용자에게 할당됩니다. 특정 그룹 액세스 수준과 사용자를 연결하려면 해당 사용자를 원하는 그룹에 추가해야 합니다.

라이선스 체계에 대한 자세한 내용을 보려면 CMC에서 라이선스 키를 클릭하고, 각 사용자 역할의 액세스 권한에 대한 자세한 내용은 SAP Business Objects 계정 관리자에게 문의하십시오.

4.1.1.1.1 BI Analyst 역할

BI Analyst 역할은 BI 플랫폼 시스템에 콘텐츠를 만드는 사용자를 위해 만든 것으로, 보고서를 편집 또는 작성하거나, 유니버스를 디자인 및 관리하거나, CMC에서 관리 작업을 수행하는 사용자에게 할당해야 합니다.

4.1.1.1.2 BI Viewer 역할

BI Viewer 역할은 주로 콘텐츠 소비자를 위해 만들었습니다. 이 사용자는 보고서를 볼 수만 있고 콘텐츠를 수정할 수는 없습니다.

BI Viewer 역할에 할당된 사용자는 콘텐츠를 만들고, 보고서를 수정하며 시스템에서 일반 관리 작업을 수행할 수 없습니다. 따라서 BI Viewer 역할은 다음을 수행해야 하는 사용자에게 할당할 수 없습니다.

- 보고서 만들기
- 보고서 업데이트 또는 수정
- CMC를 사용하여 관리 작업 수행

참고:

BI Viewer 사용자는 CMC에 액세스할 수 없습니다.

4.1.2 그룹 관리

그룹은 같은 계정 권한을 공유하는 사용자들의 집합이므로 부서, 역할 또는 위치에 따라 그룹을 만들 수 있습니다. 그룹을 사용하면 각 사용자 계정에 대한 권한을 개별적으로 수정하는 대신 사용자에게 대한 권한을 그룹으로 한 번에 변경할 수 있습니다. 또한 개체 권한을 하나 이상의 그룹에 할당할 수도 있습니다.

사용자 및 그룹 영역에서는 여러 사용자에게 보고서 또는 폴더에 대한 액세스 권한을 제공하는 그룹을 만들 수 있습니다. 이렇게 하면 각 사용자 계정을 개별적으로 수정하는 대신 한 번만 변경하면 됩니다. 기본 그룹 계정 표에 요약되어 있는 여러 가지 기본 그룹 계정도 볼 수 있습니다.

CMC에서 사용 가능한 그룹을 보려면 트리 패널에서 그룹 목록을 클릭합니다. 또는 그룹 계층 구조를 클릭하여 사용 가능한 모든 그룹의 계층 구조 목록을 표시할 수 있습니다.

테이블4-2: 기본 그룹 계정

계정 이름	설명
관리자	이 그룹의 멤버는 모든 BI 플랫폼 응용 프로그램 (CMC, CCM, 게시 마법사 및 BI 실행 패드)에서 모든 작업을 수행할 수 있습니다. 기본적으로 관리자 그룹에는 Administrator 사용자만 포함됩니다.
Everyone	모든 사용자는 Everyone 그룹의 멤버입니다.
QaaWS 그룹 디자이너	이 그룹의 구성원은 Query as a Web Service에 액세스할 수 있습니다.
보고서 변환 도구 사용자	이 그룹의 멤버는 보고서 변환 도구 응용 프로그램에 액세스할 수 있습니다.
변환기	이 그룹의 구성원은 Translation Manager 응용 프로그램에 액세스할 수 있습니다.
유니버스 디자이너 사용자	이 그룹에 속한 사용자에게는 Universe Designer 폴더 및 Connections 폴더에 대한 액세스 권한이 부여됩니다. 이러한 사용자는 Designer 응용 프로그램에 대한 사용자의 액세스 권한을 제어할 수 있습니다. 필요에 따라 이 그룹에 사용자를 추가해야 합니다. 기본적으로 이 그룹에는 사용자가 포함되어 있지 않습니다.

관련 항목

- 113 페이지에서 [BI 플랫폼에서 권한 작동 방식](#)"
- 103 페이지에서 [사용자 및 그룹에 액세스 허용](#)"

4.1.3 사용 가능한 인증 형식

BI 플랫폼에서 사용자 계정과 그룹을 설정하기 전에 사용할 인증 형식을 결정해야 합니다. 인증 형식 표에는 조직에서 사용하는 보안 도구에 따라 사용할 수 있는 인증 옵션이 요약되어 있습니다.

테이블4-3: 인증 형식

인증 형식	설명
Enterprise	BI 플랫폼에 사용할 고유한 계정 및 그룹을 만들어야 하는 경우 또는 LDAP 디렉터리 서버 또는 Windows AD 서버에서 아직 사용자 및 그룹 계층을 설정하지 않은 경우에는 시스템 기본값인 Enterprise 인증을 사용하십시오.
LDAP	LDAP 디렉터리 서버를 설정하는 경우 BI 플랫폼에서 기존의 LDAP 사용자 계정과 그룹을 사용할 수 있습니다. LDAP 계정을 BI 플랫폼에 매핑하면 사용자는 LDAP 사용자 이름과 암호를 사용하여 BI 플랫폼 응용 프로그램에 액세스할 수 있습니다. 이렇게 하면 BI 플랫폼에서 개별 사용자 및 그룹 계정을 다시 만들 필요가 없습니다.
Windows AD	BI 플랫폼에서 기존 Windows AD 사용자 계정 및 그룹을 사용할 수 있습니다. AD 계정을 BI 플랫폼에 매핑하면 사용자는 AD 사용자 이름과 암호를 사용하여 BI 플랫폼 응용 프로그램에 로그인할 수 있습니다. 이렇게 하면 BI 플랫폼에서 개별 사용자 및 그룹 계정을 다시 만들 필요가 없습니다.
SAP	BI 플랫폼 계정에 기존 SAP 역할을 매핑할 수 있습니다. SAP 역할을 매핑한 후 사용자는 SAP 자격 증명을 사용하여 BI 플랫폼 응용 프로그램에 로그인할 수 있습니다. 이렇게 하면 BI 플랫폼에서 개별 사용자 및 그룹 계정을 다시 만들 필요가 없습니다.
Oracle EBS	BI 플랫폼 계정에 기존 Oracle EBS 역할을 매핑할 수 있습니다. Oracle EBS 역할을 매핑한 후 사용자는 SAP 자격 증명을 사용하여 BI 플랫폼 응용 프로그램에 로그인할 수 있습니다. 이렇게 하면 BI 플랫폼에서 개별 사용자 및 그룹 계정을 다시 만들 필요가 없습니다.
Siebel	BI 플랫폼 계정에 기존 Siebel 역할을 매핑할 수 있습니다. Siebel 역할을 매핑한 후 사용자는 Siebel 자격 증명을 사용하여 BI 플랫폼 응용 프로그램에 로그인할 수 있습니다. 이렇게 하면 BI 플랫폼에서 개별 사용자 및 그룹 계정을 다시 만들 필요가 없습니다.

인증 형식	설명
PeopleSoft Enterprise	BI 플랫폼 계정에 기존 PeopleSoft 역할을 매핑할 수 있습니다. PeopleSoft 역할을 매핑한 후 사용자는 PeopleSoft 자격 증명을 사용하여 BI 플랫폼 응용 프로그램에 로그인할 수 있습니다. 이렇게 하면 BI 플랫폼에서 개별 사용자 및 그룹 계정을 다시 만들 필요가 없습니다.
JD Edwards EnterpriseOne	BI 플랫폼 계정에 기존 JD Edwards 역할을 매핑할 수 있습니다. JD Edwards 역할을 매핑한 후 사용자는 JD Edwards 자격 증명을 사용하여 BI 플랫폼 응용 프로그램에 로그인할 수 있습니다. 이렇게 하면 BI 플랫폼에서 개별 사용자 및 그룹 계정을 다시 만들 필요가 없습니다.

4.2 Enterprise 및 일반 계정 관리

Enterprise 인증은 BI 플랫폼의 기본 인증 방법이므로 시스템을 처음 설치할 때 자동으로 설정됩니다. 사용자 및 그룹을 추가하고 관리할 때 BI 플랫폼의 데이터베이스에 사용자 및 그룹 정보가 유지됩니다.

참고:

사용자가 BI 플랫폼 이외의 페이지로 이동하거나 웹 브라우저를 닫아 해당 플랫폼에서 자신의 웹 세션을 로그오프하더라도 사용자의 Enterprise 세션은 로그오프되지 않고 라이선스가 계속 유지됩니다. Enterprise 세션은 약 24시간이 지나면 제한 시간 초과로 종료됩니다. 사용자의 Enterprise 세션을 끝내고 다른 사용자를 위해 라이선스를 반환하려면 사용자가 플랫폼에서 로그아웃해야 합니다.

4.2.1 사용자 계정 만들기

새 사용자를 만들 경우 사용자의 속성을 지정하고 사용자가 속할 그룹을 하나 이상 선택합니다.

1. CMC의 사용자 및 그룹 관리 영역으로 이동합니다.
2. 관리 > 새로 만들기 > 새 사용자를 클릭합니다.
새 사용자 대화 상자가 나타납니다.

3. Enterprise 사용자 만들기

- a. 인증 형식 목록에서 Enterprise를 선택합니다.
- b. 계정 이름, 전체 이름, 전자 메일 및 설명 정보를 입력합니다.

팁:

설명 영역을 사용하여 사용자 또는 계정에 대한 추가 정보를 포함할 수 있습니다.

- c. 암호 정보 및 설정을 지정합니다.
4. 다른 인증 유형을 이용해 로그인할 사용자를 만들려면 인증 유형 목록에서 알맞은 옵션을 선택하고 계정 이름을 입력합니다.
5. SAP BusinessObjects Business Intelligence 플랫폼 사용권 계약에 명시된 옵션에 따라 사용자 계정 지정 방법을 지정합니다.

사용권 계약이 사용자 역할을 기반으로 하는 경우 다음 옵션 중 하나를 선택합니다.

- BI Viewer: BI Viewer 역할의 모든 계정에 대한 BI 플랫폼 응용 프로그램 액세스 권한이 사용권 계약에 정의됩니다. 사용자는 BI Viewer 역할용으로 정의된 응용 프로그램 워크플로에만 액세스할 수 있습니다. 액세스 권한은 일반적으로 비즈니스 인텔리전스 문서를 보는 것으로 제한됩니다. 이 역할은 일반적으로 플랫폼 응용 프로그램을 통해 콘텐츠를 사용하는 사용자에게 적합합니다.
- BI Analyst: BI Analyst 역할의 모든 계정에 대한 BI 플랫폼 응용 프로그램 액세스 권한이 사용권 계약에 정의됩니다. 사용자는 BI Analyst 역할에 대해 정의된 모든 응용 프로그램 워크플로에 액세스할 수 있습니다. 액세스 권한에는 비즈니스 인텔리전스 문서를 보고 수정하는 것이 포함됩니다. 이 역할은 일반적으로 플랫폼 응용 프로그램의 콘텐츠를 만들고 수정하는 사용자에게 적합합니다.

사용권 계약이 사용자 역할을 기반으로 하지 않는 경우 사용자 계정에 대한 연결 유형을 지정합니다.

- 동시에 연결 가능한 사용자 수를 정의하는 사용권 계약에 해당하는 사용자인 경우 동시 사용자를 선택합니다.
- 특정 사용자에게 라이선스를 할당하는 사용권 계약에 해당하는 사용자인 경우 명명된 사용자를 선택합니다. 명명된 사용자 라이선스는 현재 연결된 다른 사용자의 수에 관계없이 BI 플랫폼에 액세스해야 하는 사용자에게 유용합니다.

6. 만들기 및 닫기를 클릭합니다.

사용자가 시스템에 추가되고 자동으로 Everyone 그룹에 추가됩니다. 사용자용 받은 파일함이 Enterprise 별칭과 함께 자동으로 만들어집니다. 이제 그룹에 사용자를 추가하고 사용자에게 대한 권한을 지정할 수 있습니다.

관련 항목

- 113 페이지에서 [BI 플랫폼에서 권한 작동 방식](#)
- 90 페이지에서 [역할 기반 라이선스](#)

4.2.2 사용자 계정 수정

이 절차를 사용하여 사용자의 속성 또는 소속 그룹을 수정할 수 있습니다.

참고:

설정을 변경하는 동안 로그인한 사용자에게는 변경 내용이 적용됩니다.

1. CMC의 사용자 및 그룹 관리 영역으로 이동합니다.
2. 속성을 변경하려는 사용자를 선택합니다.
3. 관리 > 속성을 클릭합니다.

사용자에 대한 속성 대화 상자가 나타납니다.

4. 사용자의 속성을 수정합니다.

계정을 처음 만들었을 때 사용 가능했던 모든 옵션뿐만 아니라 계정 사용 안 함 확인란을 선택하여 계정을 사용하지 않도록 설정할 수 있습니다.

참고:

사용자가 다음 번에 로그인하기 전까지는 사용자 계정에 대한 변경 내용이 표시되지 않습니다.

5. 저장 후 닫기를 클릭합니다.

관련 항목

- 109 페이지에서 [기존 사용자에게 새 별칭 만들기](#)

4.2.3 사용자 계정 삭제

이 절차를 사용하여 사용자의 계정을 삭제할 수 있습니다. 계정이 삭제된 사용자가 로그인하면 오류 메시지가 나타납니다. 사용자 계정을 삭제하면 사용자의 즐겨찾기 폴더, 개인 범주 및 수신함도 함께 삭제됩니다.

사용자가 나중에 다시 계정에 액세스해야 할 수도 있다고 판단되면 계정을 삭제하는 대신 선택한 사용자의 속성 페이지에서 계정 사용 안 함 확인란을 선택하면 됩니다.

참고:

사용자 계정을 삭제하더라도 해당 사용자가 BI 플랫폼에 다시 로그인할 수 없는 것은 아닙니다. 타사 시스템에도 사용자 계정이 있고 이 계정이 BI 플랫폼에 매핑된 타사 그룹에 속한 경우 사용자는 계속하여 로그인할 수 있습니다.

1. CMC의 사용자 및 그룹 관리 영역으로 이동합니다.
2. 삭제할 사용자를 선택합니다.
3. 관리 > 삭제를 클릭합니다.

삭제 확인 대화 상자가 나타납니다.

4. 확인을 클릭합니다.
사용자 계정이 삭제됩니다.

관련 항목

- 95 페이지에서 [사용자 계정 수정](#)"
- 96 페이지에서 [사용자 계정 삭제](#)"
- 111 페이지에서 [별칭 비활성화](#)"

4.2.4 새 그룹 만들기

1. CMC의 사용자 및 그룹 관리 영역으로 이동합니다.
2. 관리 > 새로 만들기 > 새 그룹을 클릭합니다.
새 사용자 그룹 만들기 대화 상자가 나타납니다.
3. 그룹 이름과 설명을 입력합니다.
4. 확인을 클릭합니다.

새 그룹을 만든 후에는 사용자 또는 하위 그룹을 추가하거나 소속 그룹을 지정하여 새 그룹을 하위 그룹으로 만들 수 있습니다. 하위 그룹을 만들면 조직의 수준이 추가되므로 BI 플랫폼 콘텐츠에 대한 사용자의 액세스를 제어할 수 있도록 개체 권한을 설정할 때 유용합니다.

4.2.5 그룹 속성 수정

설정을 변경하여 그룹의 속성을 수정할 수 있습니다.

참고:

그룹에 속한 사용자는 다음 번에 로그인할 때 그룹 수정의 영향을 받습니다.

1. CMC의 사용자 및 그룹 관리 영역에서 그룹을 선택합니다.
2. 관리 > 속성을 클릭합니다.
속성 대화 상자가 나타납니다.
3. 그룹의 속성을 수정합니다.
다른 대화 상자에 액세스하여 다른 속성을 수정하려면 탐색 목록에서 링크를 클릭합니다.

- 그룹에 대한 제목이나 설명을 변경하려면 속성을 클릭합니다.
 - 그룹에 대해 사용자가 갖고 있는 권한을 수정하려면 사용자 보안을 클릭합니다.
 - 그룹 멤버에 대한 프로필 값을 수정하려면 프로필 값을 클릭합니다.
 - 그룹을 다른 그룹에 하위 그룹으로 추가하려면 소속 그룹을 클릭합니다.
4. 저장을 클릭합니다.

4.2.6 그룹 멤버 보기

이 절차를 사용하여 특정 그룹에 속한 사용자를 볼 수 있습니다.

1. CMC의 사용자 및 그룹 관리 영역으로 이동합니다.
2. 트리 패널에서 그룹 계층 구조를 확장합니다.
3. 트리 패널에서 그룹을 선택합니다.

참고:

그룹에 속한 사용자가 많은 경우 또는 그룹이 타사 디렉터리에 매핑된 경우에는 목록을 표시하는데 몇 분 정도의 시간이 소요됩니다.

그룹에 속한 사용자의 목록이 표시됩니다.

4.2.7 하위 그룹 추가

한 그룹을 다른 그룹에 추가할 수 있습니다. 이렇게 추가한 그룹은 하위 그룹이 됩니다.

참고:

하위 그룹을 추가하는 작업은 소속 그룹을 지정하는 작업과 유사합니다.

1. CMC의 사용자 및 그룹 관리 영역에서 다른 그룹에 하위 그룹으로 추가하려는 그룹을 선택합니다.
2. 작업 > 그룹 조인을 클릭합니다.
그룹 조인 대화 상자가 나타납니다.
3. 첫 번째 그룹을 추가하려는 그룹을 사용 가능한 그룹 목록에서 대상 그룹 목록으로 이동합니다.
4. 확인을 클릭합니다.

관련 항목

- 99 페이지에서 [소속 그룹 지정](#)

4.2.8 소속 그룹 지정

그룹을 다른 그룹에 포함시킬 수 있습니다. 다른 그룹에 포함된 그룹을 하위 그룹이라고 합니다. 하위 그룹이 추가된 그룹은 부모 그룹입니다. 하위 그룹에는 부모 그룹의 권한이 상속됩니다.

1. CMC의 사용자 및 그룹 관리 영역에서 다른 그룹에 추가하려는 그룹을 클릭합니다.
2. 작업 > 소속 그룹을 클릭합니다.
소속 그룹 대화 상자가 나타납니다.
3. 그룹 조인을 클릭합니다.
그룹 조인 대화 상자가 나타납니다.
4. 첫 번째 그룹을 추가하려는 그룹을 사용 가능한 그룹에서 대상 그룹 목록으로 이동합니다.
부모 그룹과 관련된 모든 권한이 새로 만든 그룹에 상속됩니다.
5. 확인을 클릭합니다.
소속 그룹 대화 상자로 돌아오면 부모 그룹 목록에 부모 그룹이 표시됩니다.

4.2.9 그룹 삭제

그룹이 더 이상 필요하지 않은 경우 그룹을 삭제할 수 있습니다. Administrator 및 Everyone 기본 그룹은 삭제할 수 없습니다.

참고:

- 삭제한 그룹에 속한 사용자는 다음 번에 로그인할 때 변경 내용의 영향을 받습니다.
- 삭제한 그룹에 속한 사용자는 그룹에서 상속한 모든 권한을 잃습니다.

Windows AD 사용자 그룹 같은 타사 인증 그룹을 삭제하려면 CMC의 인증 관리 영역을 사용합니다.

1. CMC의 사용자 및 그룹 관리 영역으로 이동합니다.
2. 삭제하려는 그룹을 선택합니다.
3. 관리 > 삭제를 클릭합니다.
삭제 확인 대화 상자가 나타납니다.
4. 확인을 클릭합니다.
그룹이 삭제됩니다.

4.2.10 Guest 계정 활성화

Guest 계정으로 BI 플랫폼에 로그인할 수 없도록 이 계정은 기본적으로 비활성화되어 있습니다. 이러한 기본 설정을 사용하면 BI 플랫폼의 익명 단일 로그인 기능도 사용할 수 없게 되므로 사용자는 유효한 사용자 이름과 암호를 입력하여 BI 실행 패드에 액세스해야 합니다.

자신의 계정이 없는 사용자도 BI 실행 패드에 액세스할 수 있도록 Guest 계정을 활성화하려면 다음 작업을 수행합니다.

1. CMC의 사용자 및 그룹 관리 영역으로 이동합니다.
2. 탐색 패널에서 사용자 목록을 클릭합니다.
3. Guest를 선택합니다.
4. 관리 > 속성을 클릭합니다.
속성 대화 상자가 나타납니다.
5. 계정 사용 안 함 확인란의 선택을 취소합니다.
6. 저장 후 닫기를 클릭합니다.

4.2.11 그룹에 사용자 추가

다음과 같은 방법으로 그룹에 사용자를 추가할 수 있습니다.

- 그룹을 선택한 다음 작업 > 그룹에 구성원 추가를 클릭합니다.
- 사용자를 선택한 다음 작업 > 소속 그룹을 클릭합니다.
- 사용자를 선택한 다음 작업 > 그룹 조인을 클릭합니다.

다음 절차에서는 이러한 방법을 사용하여 그룹에 사용자를 추가하는 방법을 설명합니다.

관련 항목

- 99 페이지에서 [소속 그룹 지정](#)

4.2.11.1 하나 이상의 그룹에 사용자 추가

1. CMC의 사용자 및 그룹 관리 영역으로 이동합니다.
2. 그룹에 추가하려는 사용자를 선택합니다.
3. 작업 > 그룹 조인을 클릭합니다.

참고:

시스템의 모든 BI 플랫폼 사용자는 Everyone 그룹에 속합니다.

그룹 조인 대화 상자가 나타납니다.

4. 사용자를 추가하려는 그룹을 사용 가능한 그룹 목록에서 대상 그룹 목록으로 이동합니다.

팁:

여러 그룹을 선택하려면 Shift + 키를 누른 채 클릭하거나 Ctrl + 키를 누른 채 클릭합니다.

5. 확인을 클릭합니다.

4.2.11.2 그룹에 하나 이상의 사용자 추가

1. CMC의 사용자 및 그룹 관리 영역에서 그룹을 선택합니다.
2. 작업 > 그룹에 구성원 추가를 클릭합니다.
추가 대화 상자가 나타납니다.
3. 사용자 목록을 클릭합니다.
사용 가능한 사용자/그룹 목록이 새로 고쳐지고 시스템의 모든 사용자 계정이 표시됩니다.
4. 그룹에 추가하려는 사용자를 사용 가능한 사용자/그룹 목록에서 선택한 사용자/그룹 목록으로 이동합니다.

팁:

- 여러 사용자를 선택하려면 Shift + 키를 누른 채 클릭하거나 Ctrl + 키를 누른 채 클릭합니다.
- 특정 사용자를 검색하려면 검색 필드를 사용합니다.
- 시스템에 사용자가 많은 경우 이전 및 다음 단추를 클릭하여 사용자 목록을 탐색할 수 있습니다.

5. 확인을 클릭합니다.

4.2.12 암호 설정 변경

CMC에서 특정 사용자 또는 시스템의 모든 사용자에게 대한 암호 설정을 변경할 수 있습니다. 아래에 나열된 다양한 제한 사항은 Enterprise 계정에만 적용됩니다. 즉 LDAP 또는 Windows AD와 같은 외부 사용자 데이터베이스에 매핑된 계정에는 적용되지 않습니다. 그러나 외부 시스템을 사용하는 경우 일반적으로 이와 비슷한 제한을 외부 계정에 적용할 수 있습니다.

4.2.12.1 사용자 암호 설정 변경

1. CMC의 사용자 및 그룹 관리 영역으로 이동합니다.
2. 암호 설정을 변경하려는 사용자를 선택합니다.
3. 관리 > 속성을 클릭합니다.
속성 대화 상자가 나타납니다.
4. 변경할 암호 설정과 관련된 확인란을 선택하거나 선택을 취소합니다.
다음과 같은 옵션을 사용할 수 있습니다.
 - 암호가 만료되지 않음
 - 다음 로그인할 때 반드시 암호 변경
 - 암호 변경할 수 없음
5. 저장 후 단기를 클릭합니다.

4.2.12.2 일반 암호 설정 변경

1. CMC의 인증 관리 영역으로 이동합니다.
2. Enterprise를 두 번 클릭합니다.
Enterprise 대화 상자가 나타납니다.
3. 사용할 각 암호 설정에 대한 확인란을 선택하고 필요한 경우 값을 지정합니다.
다음 표에는 구성할 수 있는 각 설정에 대한 최소값과 최대값이 나와 있습니다.

테이블4-4: 암호 설정

암호 설정	최소값	권장 최대값
암호에 대/소문자를 혼용해야 함	N/A	N/A
N개 이상의 문자를 포함해야 함	0자	64자
N일마다 암호를 변경해야 함	1일	100일
최근 N개의 암호는 다시 사용할 수 없음	암호 1개	암호 100개
암호를 변경하려면 N분을 기다려야 함	0분	100분
로그온에 N번 실패하면 계정을 사용할 수 없음	1번 실패	100번 실패
실패한 로그온 횟수를 N분 후에 재설정	1분	100분
N분 후에 계정을 다시 사용할 수 있음	0분	100분

4. 업데이트를 클릭합니다.

4.2.13 사용자 및 그룹에 액세스 허용

다른 사용자와 그룹에 사용자 및 그룹 관리자 액세스 권한을 부여할 수 있습니다. 관리자 권한에는 개체 보기, 편집 및 삭제, 개체 인스턴스 보기, 삭제 및 일시 중지 등이 포함됩니다. 예를 들면 문제 해결 및 시스템 유지 관리를 위하여 IT 부서에 개체를 편집하고 삭제할 수 있는 액세스 권한을 부여할 수 있습니다.

관련 항목

- 124 페이지에서 [개체의 액세스 제어 목록에 사용자 할당](#)"

4.2.14 사용자의 받은 파일함에 대한 액세스 제어

사용자를 추가하면 사용자에게 대한 받은 파일함이 자동으로 만들어집니다. 받은 파일함의 이름은 사용자와 동일합니다. 기본적으로 사용자 및 관리자만 사용자의 받은 파일함에 액세스할 수 있습니다.

관련 항목

- 78 페이지에서 [개체를 즉시 실행하도록 예약](#)"
- 123 페이지에서 [CMC에서 개체의 보안 설정 관리](#)"

4.2.15 BI 실행 패드 옵션 구성

관리자는 사용자가 BI 실행 패드 응용 프로그램에 액세스하는 방식을 구성할 수 있습니다. BOE.war 파일의 속성을 구성하여 사용자의 로그인 화면에 표시될 정보를 지정할 수 있습니다. 또한 CMC에서 특정 그룹에 대한 BI 실행 패드 기본 설정을 지정할 수도 있습니다.

4.2.15.1 BI 실행 패드 로그인 화면 구성

기본적으로 BI 실행 패드 로그인 화면에서는 사용자에게 사용자 이름과 암호를 입력하라는 메시지를 표시합니다. 원하는 경우 사용자에게 CMS 이름과 인증 형식을 요청하도록 이 화면을 구성할 수도 있습니다. 이 설정을 변경하려면 BOE.war 파일에 대한 BI 실행 패드 속성을 편집해야 합니다.

4.2.15.1.1 BI 실행 패드 로그인 화면 구성

BI 실행 패드 기본 설정을 수정하려면 BOE.war 파일에 대한 사용자 지정 BI 실행 패드 속성을 설정해야 합니다. 이 파일은 웹 응용 프로그램 서버를 호스팅하는 컴퓨터에 배포됩니다.

1. BI 플랫폼 설치 위치의 다음 디렉터리로 이동합니다.

<INSTALLDIR>WSAP BusinessObjects Enterprise XI
4.0WwarfilesWwebappsWBOEWWEB-INFWconfigWcustomW

참고:

BI 플랫폼과 함께 설치되는 Tomcat 버전을 사용 중인 경우 C:WProgram Files (x86)WSAP BusinessObjectsWTomcat6WwebappsWBOEWWEB-INFWconfigWcustom 디렉터리에도 액세스할 수 있습니다.

- 지원되는 다른 웹 응용 프로그램 서버를 사용하는 경우 해당 웹 응용 프로그램 서버의 설명서를 참조하여 적절한 경로를 결정합니다.

2. 새 파일을 만듭니다.

참고:

메모장이나 기타 텍스트 편집 유틸리티를 사용하십시오.

3. 파일을 다음 이름으로 저장합니다.

BIlaunchpad.properties

4. BI 실행 패드 로그인 화면에 인증 옵션을 포함시키려면 다음을 추가합니다.

```
authentication.visible=true
```

5. 기본 인증 유형을 변경하려면 다음을 수행합니다.

```
authentication.default=<authentication>
```

<authentication>을 다음 옵션 중 하나로 바꿉니다.

인증 형식	<authentication> 값
Enterprise	secEnterprise
LDAP	secLDAP
Windows AD	secWinAD
SAP	secSAPR3

6. BI 실행 패드 로그인 화면에서 CMS 이름을 묻는 메시지를 표시하려면 다음을 추가합니다.

```
cms.visible=true
```

7. 파일을 저장하고 닫습니다.
8. 웹 응용 프로그램 서버를 다시 시작합니다.

WDeploy를 사용하여 웹 응용 프로그램 서버에 BOE.war 파일을 다시 배포하십시오. WDeploy 사용에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 웹 응용 프로그램 배포 가이드를 참조하십시오.

4.2.15.2 그룹에 대한 BI 실행 패드 기본 설정 구성

관리자가 특정 사용자 그룹에 대한 BI 실행 패드 기본 설정을 구성할 수 있습니다. 이런 기본 설정은 그룹에 속한 모든 사용자에게 대한 기본 BI 실행 패드 기본 설정입니다.

참고:

사용자가 스스로의 기본 설정을 구성한 경우 관리자가 정의한 모든 설정은 BI 실행 패드의 보기에 반영되지 않습니다. 사용자는 언제든지 자신의 기본 설정에서 관리자가 정의한 기본 설정으로 전환하여 업데이트된 설정을 사용할 수 있습니다.

기본적으로, 어떤 사용자 그룹에 대해서도 BI 실행 패드 기본 설정이 구성되지 않습니다. 관리자는 다음에 대한 기본 설정을 지정할 수 있습니다.

- 홈 탭
- 문서 - 시작 위치
- 폴더
- 범주
- 페이지당 개체 수
- 문서 탭에 표시되는 열
- BI 실행 패드에 문서를 표시하는 방법 - 탭이나 새 창을 통해

4.2.15.2.1 그룹에 대한 BI 실행 패드 기본 설정 구성

1. CMC의 사용자 및 그룹 관리 영역으로 이동합니다.
2. 그룹 목록에서 그룹을 선택합니다.
3. 작업 > BI 실행 패드 기본 설정을 클릭합니다.
BI 실행 패드 기본 설정 대화 상자가 나타납니다.
4. 정의된 기본 설정 없음을 선택 취소합니다.

5. 사용자의 초기 뷰 설정

- 사용자가 처음 로그인할 때 홈 탭을 표시하려면 홈 탭을 클릭하고 다음 옵션 중 하나를 선택합니다.

옵션	설명
기본 홈 탭	BI 플랫폼의 기본 홈 탭을 표시합니다.
홈 탭 선택	<p>특정 웹 사이트를 홈 탭으로 표시합니다.</p> <p>홈 탭 찾아보기를 클릭합니다. 사용자 지정 홈 탭 선택 창에서 리포지토리 개체를 선택하고 열기를 클릭합니다.</p> <p>참고: 이미 리포지토리에 추가된 개체만 선택할 수 있습니다.</p>

- 사용자가 처음 로그인할 때 문서 탭을 표시하려면 문서를 클릭한 다음 기본적으로 열리는 서랍 및 노드를 지정합니다. 다음 중에서 선택할 수 있습니다.

서랍	노드 옵션
내 문서	<p>문서 탭에 표시하려면 다음 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 즐겨찾기 • 개인 범주 • 내 받은 파일함
폴더	<p>다음 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 공용 폴더: 문서 탭에 공용 폴더가 표시됩니다. • 공용 폴더 선택 <p>폴더 찾아보기를 클릭하여 문서 탭에 표시할 특정 공용 폴더를 선택합니다.</p>
범주	<p>다음 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 회사 범주: 문서 탭에 회사 범주가 표시됩니다. • 회사 범주 선택 <p>폴더 찾아보기를 클릭하여 문서 탭에 표시할 특정 회사 범주를 선택합니다.</p>

예를 들어 처음 로그인했을 때 사용자의 BI 받은 파일함에 대해 내 문서 서랍이 열리도록 하려면 내 문서를 클릭한 다음 내 받은 파일함을 클릭합니다.

6. 문서 탭에 표시된 열 선택에서 사용자의 목록 패널의 각 개체에 대해 보려는 요약 정보를 선택합니다.

- 유형
- 마지막 실행
- 인스턴스
- 설명

- 작성자
 - 만든 날짜
 - 위치(범주)
 - 받은 날짜(받은 파일함)
 - 보낸 사람(받은 파일함)
7. 문서 확인 위치 설정에서 사용자가 문서를 보는 방법을 선택합니다.
 사용자는 BI 실행 패드 내의 새 탭 또는 새 웹 브라우저 창에서 보도록 문서를 열 수 있습니다.
8. 페이지당 최대 항목 수 설정 필드에 숫자를 입력하여 사용자가 개체 목록을 볼 때 페이지당 표시되는 최대 개체 수를 지정합니다.
9. 저장 후 단기를 클릭합니다.
- 지정된 기본 설정은 2단계에서 선택한 그룹의 사용자에게 대한 기본 설정입니다. 하지만, 사용자가 기본 설정을 구성할 수 있는 권한이 있는 경우에는 고유의 BI 실행 패드 기본 설정을 만들 수 있습니다. 사용자가 기본 설정을 수정하지 못하게 하려면 사용자에게 기본 설정 구성 권한을 부여하면 안 됩니다.

4.3 별칭 관리

사용자가 BI 플랫폼에 계정을 여러 개 가지고 있는 경우 별칭 할당 기능을 사용하여 이러한 계정을 연결할 수 있습니다. 이 기능은 사용자가 Enterprise에 매핑된 타사 계정 및 Enterprise 계정을 가지고 있는 경우에 유용합니다.

별칭을 할당받은 사용자는 타사 사용자 이름 및 암호를 사용하거나 Enterprise 사용자 이름 및 암호를 사용하여 로그인할 수 있습니다. 따라서 별칭을 사용하면 사용자가 둘 이상의 인증 형식을 통해 로그인할 수 있습니다.

CMC에서 별칭 정보는 사용자의 속성 대화 상자 아래쪽에 표시됩니다. 사용자는 Enterprise, LDAP 또는 Windows AD 별칭을 조합하여 사용할 수 있습니다.

4.3.1 사용자 및 타사 별칭 만들기

사용자를 만들고 Enterprise 이외의 인증 형식을 선택하면 BI 플랫폼에서 새 사용자가 만들어지고 이 사용자에게 대해 타사 별칭이 만들어집니다.

참고:

시스템에서 타사 별칭을 만들려면 다음 조건을 충족해야 합니다.

- CMC에서 인증 도구를 사용할 수 있어야 합니다.
 - 계정 이름의 형식이 인증 형식에 필요한 형식과 일치해야 합니다.
 - 타사 인증 도구에 사용자 계정이 있어야 하며 이 계정이 BI 플랫폼에 이미 매핑된 그룹에 속해야 합니다.
1. CMC의 사용자 및 그룹 관리 영역으로 이동합니다.
 2. 관리 > 새로 만들기 > 새 사용자를 클릭합니다.
새 사용자 대화 상자가 나타납니다.
 3. 사용자의 인증 유형(예: Windows AD)을 선택합니다.
 4. 사용자의 타사 계정 이름(예: bsmith)을 입력합니다.
 5. 사용자의 연결 유형을 선택합니다.
 6. 만들기 및 닫기를 클릭합니다.
- 사용자가 BI 플랫폼에 추가되고 선택한 인증 형식에 대한 별칭이 지정됩니다(예: secWindowsAD:ENTERPRISE:bsmith). 필요한 경우 사용자에게 별칭을 추가, 할당 및 다시 할당할 수 있습니다.

4.3.2 기존 사용자에게 대한 새 별칭 만들기

기존 BI 플랫폼 사용자에게 대해 별칭을 만들 수 있습니다. 별칭은 Enterprise 별칭 또는 타사 인증 도구의 별칭일 수 있습니다.

참고:

시스템에서 타사 별칭을 만들려면 다음 조건을 충족해야 합니다.

- CMC에서 인증 도구를 사용할 수 있어야 합니다.
 - 계정 이름의 형식이 인증 형식에 필요한 형식과 일치해야 합니다.
 - 타사 인증 도구에 사용자 계정이 있어야 하며 이 계정이 플랫폼에 매핑된 그룹에 속해야 합니다.
1. CMC의 사용자 및 그룹 관리 영역으로 이동합니다.
 2. 별칭을 추가하려는 사용자를 선택합니다.
 3. 관리 > 속성을 클릭합니다.
속성 대화 상자가 나타납니다.
 4. 새 별칭을 클릭합니다.
 5. 인증 유형을 선택합니다.
 6. 사용자의 계정 이름을 입력합니다.
 7. 업데이트를 클릭합니다.

사용자에 대해 별칭이 만들어집니다. CMC에서 사용자를 확인할 때 최소한 두 개의 별칭(이전에 사용자에게 할당된 별칭과 방금 만든 별칭)이 표시됩니다.

8. 저장 후 단기를 클릭하여 속성 대화 상자를 닫습니다.

4.3.3 다른 사용자의 별칭 할당

사용자에게 별칭을 할당할 때는 다른 사용자의 타사 별칭을 현재 표시된 사용자에게 할당합니다. Enterprise 별칭은 할당하거나 다시 할당할 수 없습니다.

참고:

사용자에게 별칭이 하나 뿐이고 다른 사용자에게 이 마지막 별칭을 할당하면 사용자 계정 및 이 계정에 대한 즐겨찾기 폴더, 개인 범주와 수신함이 삭제됩니다.

1. CMC의 사용자 및 그룹 관리 영역으로 이동합니다.
2. 별칭을 할당하려는 사용자를 선택합니다.
3. 관리 > 속성을 클릭합니다.
속성 대화 상자가 나타납니다.
4. 별칭 할당을 클릭합니다.
5. 할당하려는 별칭을 갖고 있는 사용자 계정을 입력하고 지금 찾기를 클릭합니다.
6. 할당하려는 별칭을 사용 가능한 별칭 목록에서 사용자 이름에 추가할 별칭 목록으로 이동합니다.
여기서 사용자 이름은 별칭을 할당하려는 사용자의 이름입니다.

팁:

별칭을 여러 개 선택하려면 Shift + 키를 누른 채 클릭하거나 Ctrl + 키를 누른 채 클릭합니다.

7. 확인을 클릭합니다.

4.3.4 별칭 삭제

별칭을 삭제하면 시스템에서 별칭이 제거됩니다. 사용자에게 별칭이 하나 뿐인 경우 이 별칭을 삭제하면 사용자 계정 및 이 계정에 대한 즐겨찾기 폴더, 개인 범주와 수신함이 자동으로 삭제됩니다.

참고:

사용자의 별칭을 삭제하더라도 사용자가 BI 플랫폼에 다시 로그인할 수 없는 것은 아닙니다. 타사 시스템에 아직 사용자 계정이 있고 이 계정이 BI 플랫폼에 매핑된 그룹에 속하는 경우 사용자가 BI 플랫폼

폼에 로그인할 수 있습니다. CMC의 인증 관리 영역에서 인증 도구에 대해 선택한 업데이트 옵션에 따라 새 사용자가 만들어지거나 기존 사용자에게 별칭이 할당됩니다.

1. CMC의 사용자 및 그룹 관리 영역으로 이동합니다.
2. 삭제하려는 별칭을 갖고 있는 사용자를 선택합니다.
3. 관리 > 속성을 클릭합니다.
속성 대화 상자가 나타납니다.
4. 삭제하려는 별칭 옆에 있는 별칭 삭제 단추를 클릭합니다.
5. 정말로 삭제할지 확인하는 메시지가 나타나면 확인을 클릭합니다.
별칭이 삭제됩니다.
6. 저장 후 단기를 클릭하여 속성 대화 상자를 닫습니다.

4.3.5 별칭 비활성화

특정 인증 방법과 연결된 사용자 별칭을 비활성화하면 사용자가 이 인증 방법을 사용하여 BI 플랫폼에 로그인하지 못하도록 할 수 있습니다. 사용자가 플랫폼에 액세스하지 못하도록 하려면 해당 사용자의 모든 별칭을 비활성화합니다.

참고:

시스템에서 사용자를 삭제하더라도 해당 사용자가 BI 플랫폼에 다시 로그인할 수 없는 것은 아닙니다. 타사 시스템에 아직 사용자 계정이 있고 이 계정이 플랫폼에 매핑된 그룹에 속해 있는 경우 사용자가 계속 시스템에 로그인할 수 있습니다. 사용자가 자신의 별칭 중 하나를 사용하여 플랫폼에 더 이상 로그인하지 못하도록 하는 가장 좋은 방법은 별칭을 비활성화하는 것입니다.

1. CMC의 사용자 및 그룹 관리 영역으로 이동합니다.
2. 비활성화하려는 별칭을 갖고 있는 사용자를 선택합니다.
3. 관리 > 속성을 클릭합니다.
속성 대화 상자가 나타납니다.
4. 비활성화하려는 별칭의 사용 확인란을 선택 취소합니다.
비활성화할 각 별칭에 대해 이 단계를 반복합니다.
5. 저장 후 단기를 클릭합니다.
사용자는 방금 비활성화한 인증 형식을 사용하여 더 이상 로그인할 수 없습니다.

관련 항목

- 110 페이지에서 [별칭 삭제](#)

장5 권한 설정

5.1 BI 플랫폼에서 권한 작동 방식

권한은 개체, 사용자, 응용 프로그램, 서버 및 BI 플랫폼의 기타 기능에 대한 사용자의 액세스를 제어하는 기본 단위입니다. 또한 사용자가 개체에서 수행할 수 있는 개별 작업을 지정하여 시스템을 안전하게 하는 중요한 역할을 담당합니다. 그 밖에도 권한을 통해 BI 플랫폼 콘텐츠에 대한 액세스를 제어하고, 사용자 및 그룹 관리를 서로 다른 부서에 위임하고, IT 담당자에게 서버 및 서버 그룹을 관리하기 위한 액세스 권한을 제공할 수 있습니다.

권한은 액세스를 수행하는 사용자와 그룹이 아니라 보고서와 폴더 같은 개체에 설정되는 것입니다. 예를 들어, 폴더 영역에서 관리자에게 특정 폴더에 대한 액세스 권한을 부여하려면, 해당 폴더에 대한 액세스 제어 목록, 즉 개체에 대한 액세스 권한을 가진 사용자 목록에 관리자를 추가합니다. 사용자 및 그룹 영역에서 관리자 권한 설정을 구성하는 방법으로는 관리자에게 액세스 권한을 부여할 수 없습니다. 사용자 및 그룹 영역에서 구성하는 관리자 권한 설정은 다른 사용자(예: 위임된 관리자)에게 시스템 내 개체로서의 관리자에게 액세스할 수 있도록 권한을 부여하는 데 사용됩니다. 이런 식으로 사용자는 보다 높은 수준의 권한을 관리하는 다른 사용자의 개체와 같은 역할을 하게 됩니다.

개체에 대한 각 권한은 부여되거나, 거부되거나, 지정되지 않을 수 있습니다. BI 플랫폼 보안 모델은 권한을 지정되지 않은 상태로 둘 경우 해당 권한이 거부되도록 디자인되었습니다. 또한 사용자나 그룹에 대해 특정 권한이 부여되는 동시에 거부되도록 설정된 경우 해당 권한은 거부됩니다. 이와 같은 거부 기반 디자인은 명시적으로 허용하지 않은 권한이 사용자와 그룹에 자동으로 부여되는 것을 방지합니다.

이 규칙에는 중요한 예외가 한 가지 있습니다. 하위 개체에 대해 명시적으로 설정된 권한이 상위 개체에서 상속된 권한과 충돌하는 경우, 상위 개체에 대해 설정된 권한이 상속 권한을 무시합니다. 이러한 예외는 그룹의 멤버인 사용자에게도 적용됩니다. 사용자가 자신이 속한 사용자 그룹에 거부된 권한을 명시적으로 부여받으면 이 사용자에게 설정된 권한이 상속 권한을 무시합니다.

관련 항목

- 118 페이지에서 [권한 무시](#)"

5.1.1 액세스 수준

액세스 수준은 사용자가 가장 자주 필요로 하는 권한 그룹입니다. 필요한 개별 권한을 하나씩 설정하는 것이 아니라 관리자가 빠르고 일치되게 공통 보안 수준을 설정할 수 있게 합니다.

BI 플랫폼에는 미리 정의된 여러 개의 액세스 수준이 제공됩니다. 미리 정의된 액세스 수준의 기반이 되는 모델은 보기에서 시작하여 모든 권한에 이르기까지 권한이 증가하는 방식으로 구성되며, 각 액세스 수준은 이전 수준에 허용되는 권한을 기반으로 설정되어 있습니다.

사용자는 고유의 액세스 수준을 만들고 사용자 지정할 수도 있으며, 그런 경우 보안과 관련된 관리 비용과 유지 관리 비용을 현저히 줄일 수 있습니다. 관리자가 판매 관리자와 판매 직원, 두 개의 그룹을 관리해야 하는 경우를 가정합니다. 두 그룹 모두 BI 플랫폼 시스템에 있는 5개의 보고서에 액세스해야 하지만, 판매 관리자가 판매 직원보다 더 많은 권한이 필요합니다. 미리 정의된 액세스 수준은 두 그룹 중 어느 쪽의 요구도 충족시키지 못합니다. 관리자는 두 그룹을 보안 주체로서 각 보고서에 추가하고 5개의 위치별로 그룹의 권한을 수정하는 대신, Sales Managers와 Sales Employees라는 2개의 새로운 액세스 수준을 만들 수 있습니다. 그런 다음, 두 그룹을 모두 보안 주체로서 보고서에 추가하고 각 그룹에 액세스 수준을 할당합니다. 권한 수정이 필요한 경우 관리자는 액세스 수준을 수정할 수 있습니다. 액세스 수준이 5개의 보고서 모두에서 두 그룹 모두에 대해 적용되므로 그룹이 보고서에 대해 가진 권한이 신속하게 업데이트됩니다.

관련 항목

- 128 페이지에서 [액세스 수준 작업](#)"


5.1.2 고급 권한 설정





CMC에서 고급 권한을 설정하여 개체 보안에 필요한 모든 권한을 얻을 수 있습니다. 이러한 고급 권한을 사용하면 개체에 대한 보안을 세부 수준에서 정의하여 유연성을 높일 수 있습니다.

예를 들어, 특정 개체나 개체 집합에 대한 보안 주체의 권한을 사용자 지정해야 하는 경우 고급 권한 설정을 사용할 수 있습니다. 이후에 그룹 구성원을 변경하거나 폴더 보안 수준을 변경하는 경우 고급 권한을 사용하면 사용자 또는 그룹에 허용되지 말아야 할 권한이 변경되지 않도록 명시적으로 거부할 수 있다는 점이 특히 중요합니다.

다음 표에는 고급 권한을 설정할 때 적용할 수 있는 옵션이 요약되어 있습니다.

테이블5-1: 권한 옵션

아이콘	권한 옵션	설명
	허가됨	보안 주체에게 권한을 부여합니다.

아이콘	권한 옵션	설명
	거부됨	보안 주체에 대해 권한을 거부합니다.
	지정되지 않음	보안 주체에 대해 권한을 지정하지 않습니다. 지정되지 않음으로 설정된 권한은 기본적으로 거부됩니다.
	개체에 적용	권한을 개체에 적용합니다. 이 옵션은 허가됨 또는 거부됨을 클릭했을 때 사용할 수 있습니다.
	하위 개체에 적용	권한을 하위 개체에 적용합니다. 이 옵션은 허가됨 또는 거부됨을 클릭했을 때 사용할 수 있습니다.

관련 항목

- 120 페이지에서 [유형별 권한](#)"

5.1.3 상속

사용자가 개체에 대한 액세스를 제어할 수 있도록 권한을 개체에 설정하지만 모든 개체에 대해 사용할 수 있는 모든 권한의 명시적 값을 설정하는 것은 비효율적입니다. 100개의 권한과 1000명의 사용자, 10,000 개의 개체가 있는 시스템이 있다고 가정해 봅시다. 여기서 각 개체에 대해 권한을 명시적으로 설정하려면 CMS의 메모리에 수십억 개의 권한을 저장할 수 있어야 하고 특히 관리자가 각각의 권한을 수동으로 설정해야 합니다.

상속 패턴을 통해 이 비효율성 문제를 해결할 수 있습니다. 상속을 사용하면 시스템의 개체에 대해 사용자 권한을 여러 그룹과 하위 그룹의 구성원 조합 및 상위 폴더 및 하위 폴더에서 권한을 상속한 개체에서 가져옵니다. 이러한 사용자는 그룹의 구성원으로서 권한을 상속받을 수 있고 하위 그룹은 상위 그룹에서 권한을 상속받을 수 있으며 사용자와 그룹 모두 상위 폴더에서 권한을 상속받을 수 있습니다.

기본적으로 폴더에 대한 권한이 있는 사용자나 그룹은 이후에 그 폴더에 게시되는 모든 개체에 대해서도 동일한 권한을 상속받습니다. 따라서 권한을 설정하는 가장 좋은 방법은 먼저 폴더 수준에서 사용자와 그룹에 대한 적절한 권한을 설정한 다음 그 폴더에 개체를 게시하는 것입니다.

BI 플랫폼에서는 그룹 상속과 폴더 상속이라는 두 가지 유형의 상속을 인식합니다.

5.1.3.1 그룹 상속

그룹 상속을 사용하면 그룹 구성원이 된 사용자에게 그룹의 권한을 상속할 수 있습니다. 그룹 상속은 조직의 현재 보안 규칙에 부합하는 그룹으로 모든 사용자를 편성하려는 경우에 특히 유용합니다.

그룹 상속 예제 1에서는 그룹 상속 작동 방법을 볼 수 있습니다. 빨강 그룹은 파란 그룹의 하위 그룹이므로 파란 그룹의 권한을 상속받습니다. 이 경우, 빨강 그룹은 권한 1이 부여되었으며 나머지 권한은 지정되지 않은 상태로 권한을 상속받습니다. 빨강 그룹의 모든 멤버는 이러한 권한을 상속받습니다. 또한 하위 그룹에 설정된 다른 권한은 해당 그룹의 멤버가 상속받습니다. 이 예제에서 녹색 사용자는 빨강 그룹의 멤버이므로 1번 권한은 부여된 상태로 상속받고 2, 3, 4, 6 권한은 지정되지 않은 상태로, 5번 권한은 거부된 상태로 상속받습니다.

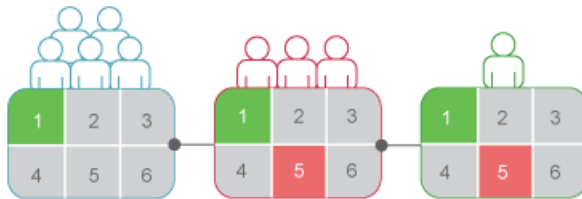


그림 5-1: 그룹 상속 예제 1

두 개 이상의 그룹에 속한 사용자에게 대해 그룹 상속이 활성화된 경우 시스템에서 자격 증명을 확인할 때는 모든 상위 그룹의 권한이 검토됩니다. 상위 그룹에서 명시적으로 거부된 권한은 사용자에게 대해서도 거부되고 전혀 지정되지 않은 상태인 권한도 사용자에게 대해 거부되므로, 사용자에게는 하나 이상의 그룹에서 명시적으로 또는 여러 액세스 수준에 걸쳐 허용된 권한과 명시적으로 거부되지 않은 권한만 허용됩니다.

그룹 상속 예제 2에서 녹색 사용자는 서로 연관되지 않은 두 그룹의 멤버입니다. 파란 그룹에서는 1번 권한과 5번 권한을 “부여됨”으로 상속받고 나머지 권한은 지정되지 않은 상태로 상속받습니다. 그러나 녹색 사용자는 빨강 그룹에도 속하므로 빨강 그룹은 5번 권한을 명시적으로 거부하고 파란 그룹에서 녹색 사용자가 받은 5번 권한에 대한 상속은 무시됩니다.

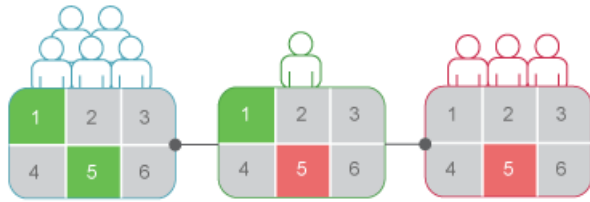


그림 5-2: 그룹 상속 예제 2

관련 항목

- 118 페이지에서 [권한 무시](#)"

5.1.3.2 폴더 상속

폴더 상속을 사용하면 개체의 상위 폴더에서 허용된 모든 권한을 사용자가 상속받을 수 있습니다. 폴더 상속은 조직의 현재 보안 규칙을 반영하는 폴더 계층으로 BI 플랫폼 콘텐츠를 구성하려는 경우에 특히 유용합니다. 예를 들어 Sales Reports라는 폴더를 만들고 이 폴더에 대한 요청 시 보기 액세스 수준을 Sales 그룹에 부여한 경우를 가정해 봅니다. 기본적으로 Sales Reports 폴더에 대한 권한이 있는 모든 사용자는 이후에 이 폴더에 게시되는 보고서에 대해서도 동일한 권한을 상속받습니다. 따라서 Sales 그룹에는 모든 보고서에 대한 요청 시 보기 액세스 수준이 부여되며, 폴더 수준에서 이 개체 권한을 한 번만 설정하면 됩니다.

폴더 상속 예제에서 빨강 그룹이 폴더에 대해 가지는 권한이 설정되었습니다. 1번 권한과 5번 권한은 부여되었고 나머지는 지정되지 않고 남아 있습니다. 폴더 상속을 활성화하면 빨강 그룹의 멤버는 폴더 수준의 그룹 권한과 동일한 개체 수준의 권한을 가지게 됩니다. 1번 권한과 5번 권한은 부여됨으로 상속받고 나머지는 지정되지 않고 남아 있습니다.

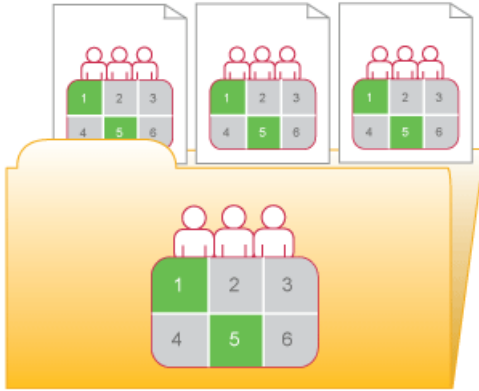


그림 5-3: 폴더 상속 예제

관련 항목

- 118 페이지에서 [권한 무시](#)"

5.1.3.3 권한 무시

권한 재정의는 하위 개체에 대해 설정된 권한이 상위 개체에 설정된 권한을 무시하는 권한 동작입니다. 권한 무시는 다음과 같은 경우에 발생합니다.

- 일반적으로 하위 개체에 설정된 권한이 상위 개체에 설정된 동등한 권한을 무시합니다.
- 일반적으로 하위 그룹 또는 그룹 멤버에 대해 설정된 권한이 그룹에 설정된 동등한 권한을 무시합니다.

개체에 대한 사용자 지정 권한을 설정하기 위해 상속을 비활성화할 필요가 없습니다. 하위 개체는 자신에 대해 명시적으로 설정된 권한을 제외하고는 상위 개체의 권한 설정을 상속받습니다. 또한, 상위 개체에 대한 권한 설정이 변경되면 이는 하위 개체에 적용됩니다.

권한 무시 예제 1에서는 권한 무시가 상위 개체와 하위 개체에 작동하는 방식을 보여 줍니다. 파란색 사용자는 폴더 내용을 편집할 수 있는 권한이 거부된 상태이며, 이 권한 설정은 하위 폴더에 상속됩니다. 그러나 관리자가 하위 폴더에 있는 문서에 대한 편집 권한을 파란색 사용자에게 부여합니다. 그러면 폴더와 하위 폴더에서 상속된 권한이 무시되고 파란색 사용자가 문서에 대해 부여받은 편집 권한이 적용됩니다.

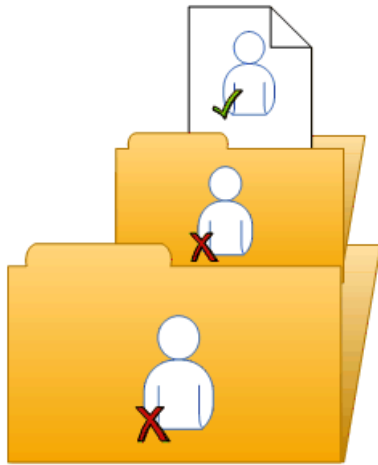


그림 5-4: 권한 무시 예제 1

권한 무시 예제 2에서는 권한 무시가 멤버와 그룹에 작동하는 방식을 보여 줍니다. 파란색 그룹은 폴더 편집 권한이 거부된 상태이며, 이 권한 설정은 파란색 하위 그룹에 상속됩니다. 그러나 관리자가 폴더에 대한 편집 권한을 파란색 그룹과 파란색 하위 그룹의 멤버인 파란색 사용자에게 부여합니다. 그러면 파란색 그룹과 파란색 하위 그룹에서 상속된 권한이 무시되고 파란색 사용자가 폴더에 대해 부여받은 편집 권한이 적용됩니다.

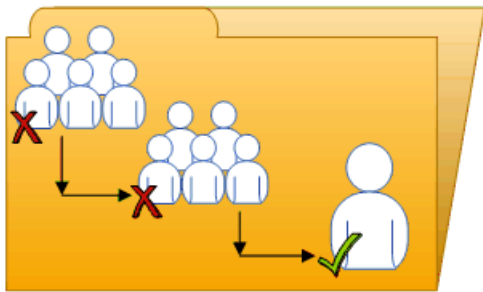


그림 5-5: 권한 무시 예제 2

복합 권한 무시에서는 권한 무시의 영향이 다소 명확하지 않은 상황을 보여 줍니다. 자주색 사용자는 하위 그룹 1A와 2A의 멤버이며, 이들 하위 그룹은 각각 그룹 1과 그룹 2에 속해 있습니다. 그룹 1과 그룹 2 모두 폴더에 대한 편집 권한을 가지고 있습니다. 1A는 그룹 1이 가진 편집 권한을 상속받고, 2A는 관리자에 의해 편집 권한이 거부되었습니다. 이런 경우 권한 무시로 인해 2A의 권한 설정이 그룹 2에 대한 권한 설정을 무시합니다. 그 결과, 자주색 사용자는 1A와 2A로부터 서로 상반된 권한 설정을 상속받습니다. 1A와 2A는 상위-하위 관계가 아니므로 권한 무시가 발생하지 않습니다. 다시 말해 두 하위 그룹의 상태가 동등하므로 한 하위 그룹의 권한 설정이 다른 하위 그룹의 설정을 무시하지 않습니다. 따라서 BI 플랫폼의 거부 기반 권한 모델 때문에 자주색 사용자는 편집 권한이 거부됩니다.

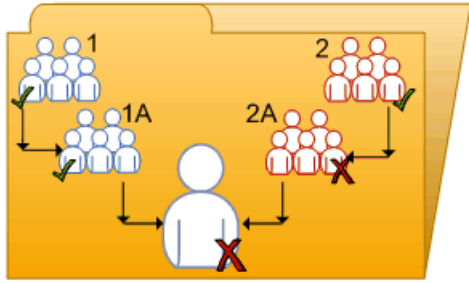


그림 5-6: 복합 권한 무시

권한 무시를 사용하면 상속된 모든 권한 설정을 삭제하지 않고도 하위 개체의 권한 설정을 약간 조정할 수 있습니다. 판매 관리자가 기밀 폴더에 있는 기밀 보고서를 봐야 하는 경우를 생각해 볼 수 있습니다. 판매 관리자는 판매 그룹에 속해 있고, 이 그룹에 대해서는 기밀 폴더 및 그 콘텐츠에 대한 액세스 권한이 거부되어 있습니다. 관리자가 기밀 폴더에 대한 보기 권한을 이 관리자에게 부여하고 판매 그룹에 대해서는 해당 권한을 계속 거부합니다. 이 경우 판매 관리자가 판매 그룹의 구성원으로서 상속하는 거부된 권한 대신 이 관리자에게 부여된 보기 권한이 유효하게 적용됩니다.

5.1.3.4 권한의 범위

권한의 범위는 권한 상속의 범위를 제어하는 기능을 가리킵니다. 권한의 범위를 정의하려면 권한을 개체에 적용할지 그 하위 개체에 적용할지 아니면 둘 다에 적용할지 결정해야 합니다. 기본적으로 권한의 범위는 개체 및 하위 개체 모두를 대상으로 확장됩니다.

권한의 범위를 사용하면 공유 위치에 있는 개인 콘텐츠를 보호할 수 있습니다. 재무 부서에서 Expense Claims 폴더를 공유하고 있고 이 폴더에 각 직원별로 Personal Expense Claims 하위 폴더가 포함되어 있는 경우를 가정해 봅시다. 직원들은 Expense Claims 폴더를 보고 여기에 개체를 추가할 수 있어야 할 뿐만 아니라 각자의 Personal Expense Claims 하위 폴더에 들어 있는 내용을 보호할 필요도 있습니다. 관리자는 모든 직원에게 Expense Claims 폴더에 대한 보기 및 추가 권한을 부여하고 이러한 권한의 범위를 Expense Claims 폴더로만 제한합니다. 즉 Expense Claims 폴더의 하위 개체에는 보기 및 추가 권한이 적용되지 않습니다. 그런 다음 관리자는 직원들에게 각자의 Personal Expense Claims 하위 폴더에 대한 보기 및 추가 권한을 부여합니다.

권한의 범위를 사용하면 위임된 관리자가 갖는 유효한 권한을 제한할 수도 있습니다. 예를 들어 위임된 관리자가 폴더에 대한 권한 보안 수정 및 편집 권한을 갖도록 하되 이러한 권한의 범위를 폴더로만 제한하고 폴더의 하위 개체에는 적용되지 않도록 할 수 있습니다. 위임된 관리자는 해당 폴더의 하위 개체 중 하나에 대해 이러한 권한을 다른 사용자에게 부여할 수 없습니다.

5.1.4 유형별 권한

유형별 권한은 Crystal 보고서, 폴더 또는 액세스 수준과 같은 특정 개체 유형에만 영향을 주는 권한입니다. 유형별 권한은 다음과 같이 구성됩니다.

- 개체 유형에 대한 일반 권한

이 권한은 개체 추가, 삭제, 편집 등 일반 전역 권한과 동일하지만 일반 전역 권한 설정을 무시하도록 특정 개체 유형에 대해 설정할 수 있습니다.

- 개체 유형에 대한 특정 권한

이 권한은 특정 개체 유형에만 사용할 수 있습니다. 예를 들면, Crystal 보고서에 대해서는 보고서 데이터 내보내기 권한이 나타나지만 Word 문서에 대해서는 나타나지 않습니다.

다이어그램 유형별 권한 예제에서는 유형별 권한이 작동하는 방식을 보여 줍니다. 여기서 권한 3은 개체 편집 권한을 나타냅니다. 파란색 그룹은 최상위 폴더에 대해서는 편집 권한이 거부되며 폴더와 하위 폴더의 Crystal 보고서에 대해서는 편집 권한이 부여됩니다. 이러한 편집 권한은 Crystal 보고서에 한정되며 일반 전역 수준의 권한 설정을 무시합니다. 그 결과, 파란색 그룹 멤버는 Crystal 보고서에 대한 편집 권한을 갖지만 하위 폴더의 XLF 파일에 대해서는 권한이 없습니다.

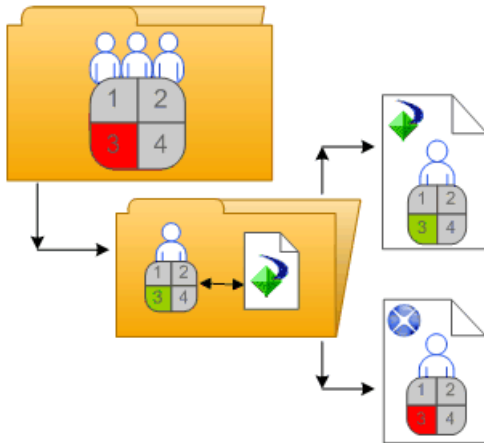


그림 5-7: 유형별 권한 예제

유형별 권한은 개체 유형에 따라 사용자의 권한을 제한하므로 유용합니다. 직원이 폴더에 개체를 추가할 수 있지만 하위 폴더를 만들 수는 없도록 설정하려는 경우를 생각해 봅시다. 이를 위해 관리자는 폴더에 대한 일반 전역 수준에서 추가 권한을 허용하고 폴더 개체 유형에 대해서는 추가 권한을 거부합니다.

권한은 적용되는 개체 유형에 따라 다음과 같이 분류됩니다.

- 일반

이 권한은 모든 개체에 영향을 미칩니다.

- 내용

이 권한은 특정 콘텐츠 개체 유형에 따라 분류됩니다. 콘텐츠 개체 유형으로는 Crystal Reports 및 Adobe Acrobat PDF가 있습니다.

- 응용 프로그램

이 권한은 적용되는 BI 플랫폼 응용 프로그램에 따라 분류됩니다. 이러한 응용 프로그램에는 CMC와 BI 실행 패드가 있습니다.

- 시스템

이 권한은 적용되는 시스템 핵심 구성 요소에 따라 분류됩니다. 이러한 시스템 핵심 구성 요소에는 달력, 이벤트, 사용자와 그룹이 있습니다.

유형별 권한은 콘텐츠, 응용 프로그램 및 시스템 컬렉션에 있으며 각 컬렉션 내에서 다시 개체 유형에 따라 여러 범주로 분류됩니다.

5.1.5 유효한 권한 결정

개체에 대한 권한을 설정할 때는 다음 고려 사항을 염두에 두어야 합니다.

- 각 액세스 수준은 일부 권한은 부여하고, 일부 권한은 거부하고, 다른 권한은 지정하지 않은 채로 둡니다. 사용자에게 허용되는 액세스 수준이 여러 개인 경우 시스템에서는 유효한 권한을 집계하고 지정되지 않은 모든 권한은 기본적으로 거부합니다.
- 개체의 사용자에게 다중 액세스 수준을 할당하는 경우 그 사용자는 각 액세스 수준에서 허용하는 권한의 조합을 부여받습니다. 다중 액세스 수준의 사용자에게는 두 가지 액세스 수준이 할당됩니다. 그 중 한 액세스 수준은 사용자에게 권한 3과 4를 부여하고, 다른 액세스 수준은 권한 3만 부여합니다. 이 사용자의 유효한 권한은 3과 4입니다.

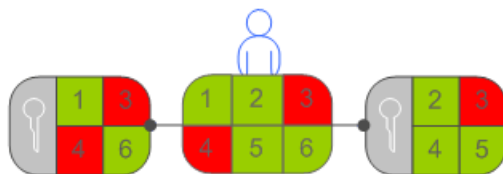


그림 5-8: 다중 액세스 수준

- 고급 권한을 액세스 수준과 조합하여 개체의 사용자에게 대한 권한 설정을 사용자 지정할 수 있습니다. 예를 들어 고급 권한과 액세스 수준을 개체의 사용자에게 모두 명시적으로 할당하는 경우 고급 권한이 액세스 수준의 권한과 충돌하면 액세스 수준의 권한은 무시한 채 고급 권한이 사용됩니다.

고급 권한은 동일한 사용자의 동일한 개체에 설정되었을 경우에만 액세스 수준의 동등 권한을 재정의할 수 있습니다. 예를 들어 일반 전역 수준의 고급 추가 권한 집합은 액세스 수준의 일반 추가 권한 설정을 재정의할 수 있지만, 액세스 수준에 포함된 유형별 추가 권한 설정을 재정의할 수는 없습니다.

그러나 고급 권한이 항상 액세스 수준보다 우선하는 것은 아닙니다. 예를 들어 부모 개체에 대한 편집 권한은 사용자에게 거부됩니다. 자식 개체에 대해서는 사용자에게 편집 권한을 부여한 액세스

스 수준이 해당 사용자에게 할당됩니다. 따라서 사용자는 자식 개체에 대한 편집 권한을 갖게 됩니다. 자식 개체에 대해 설정된 권한이 부모 개체에 대해 설정된 권한을 재정의하기 때문입니다.

- 권한을 재정의하면 부모 개체로부터 상속받은 권한 대신 자식 개체에 대해 설정된 권한을 적용할 수 있습니다.

5.2 CMC에서 개체의 보안 설정 관리

CMC의 관리 메뉴에서 보안 옵션을 사용하여 대부분의 개체에 대한 보안 설정을 관리할 수 있습니다. 이러한 옵션을 사용하면 개체에 대한 액세스 제어 목록에 사용자를 할당할 수 있고, 사용자가 보유한 권한을 볼 수 있고, 개체에 대해 사용자가 갖고 있는 권한을 수정할 수 있습니다.

구체적인 보안 관리 세부 사항은 어떤 보안이 필요한지와 권한을 설정하려는 개체의 유형이 무엇인지에 따라 다릅니다. 그러나 일반적으로 다음 작업의 워크플로는 매우 비슷하게 진행됩니다.

- 개체에 대한 사용자의 권한을 봅니다.
- 개체에 대한 액세스 제어 목록에 사용자를 할당하고 해당 사용자에게 부여할 권한과 액세스 수준을 지정합니다.
- BI 플랫폼에서 최상위 폴더에 대한 권한을 설정합니다.

5.2.1 개체에 대한 사용자 권한 보기

일반적으로 이 워크플로에 따라 개체에 대한 사용자의 권한을 봅니다.

1. 보안 설정을 보려는 개체를 선택합니다.
2. 관리 > 사용자 보안을 클릭합니다.
사용자 보안 대화 상자가 나타나고 개체에 대한 액세스 제어 목록이 표시됩니다.
3. 액세스 제어 목록에서 사용자를 선택하고 보안 보기를 클릭합니다.

권한 탐색기가 시작되고 개체에 대한 사용자의 유효한 권한 목록이 표시됩니다. 권한 탐색기에서 다음 작업을 수행할 수도 있습니다.

- 해당 권한을 보려는 다른 사용자를 찾을 수 있습니다.
- 표시되는 권한을 다음 항목을 기준으로 필터링할 수 있습니다.
 - 할당된 권한
 - 허용된 권한
 - 할당되지 않은 권한
 - 액세스 수준

- 개체 형식
- 권한 이름
- 표시되는 권한의 목록을 다음 항목을 기준으로 오름차순이나 내림차순으로 정렬할 수 있습니다.
 - 컬렉션
 - 유형
 - 권한 이름
 - 권한 상태(허용됨, 거부됨 또는 지정되지 않음)

또한 소스 옆에 있는 링크 중 하나를 클릭하여 상속된 권한의 소스를 표시할 수 있습니다.

5.2.2 개체의 액세스 제어 목록에 사용자 할당

액세스 제어 목록은 개체에 대한 권한이 허용되거나 거부된 사용자를 지정하는 데 사용됩니다. 액세스 제어 목록에 사용자를 할당하고 개체에 대해 사용자가 갖는 권한을 지정하려면 일반적으로 여기에서 설명하는 워크플로를 따릅니다.

1. 사용자를 추가하려는 개체를 선택합니다.
2. 관리 > 사용자 보안을 클릭합니다.
사용자 보안 대화 상자가 나타나고 액세스 제어 목록이 표시됩니다.
3. 보안 주체 추가를 클릭합니다.
보안 주체 추가 대화 상자가 나타납니다.
4. 사용자로 추가하려는 사용자 및 그룹을 사용 가능한 사용자/그룹 목록에서 선택한 사용자/그룹 목록으로 이동합니다.
5. 보안 추가 및 할당을 클릭합니다.
6. 사용자에게 부여하려는 액세스 수준을 선택합니다.
7. 폴더 또는 그룹 상속을 사용할지 여부를 선택합니다.

필요한 경우 세부 수준에서 권한을 수정하여 액세스 수준의 특정 권한을 재정의할 수도 있습니다.

관련 항목

- 124 페이지에서 [개체에 대한 사용자 보안 수정](#)

5.2.3 개체에 대한 사용자 보안 수정

일반적으로 사용자에게 권한을 할당하는 데는 액세스 수준을 사용하는 것이 좋습니다. 그러나 경우에 따라서는 액세스 수준의 특정 권한을 별도로 재정의해야 할 수도 있습니다. 고급 권한을 사용하면 사용자가 이미 갖고 있는 액세스 수준에 더해 사용자의 권한을 사용자 지정할 수 있습니다. 일반적으로 이 워크플로에 따라 개체에 대한 고급 권한을 사용자에게 할당합니다.

1. 개체에 대한 액세스 제어 목록에 사용자를 할당합니다.
2. 사용자를 추가했으면 관리 > 사용자 보안으로 이동하여 개체에 대한 액세스 제어 목록을 표시합니다.
3. 액세스 제어 목록에서 사용자를 선택하고 보안 할당을 클릭합니다.
보안 할당 대화 상자가 나타납니다.
4. 고급 탭을 클릭합니다.
5. 권한 추가/제거를 클릭합니다.
6. 사용자의 권한을 수정합니다.
사용 가능한 모든 권한이 권한 목록에 요약되어 있습니다.

관련 항목

- 124 페이지에서 [개체의 액세스 제어 목록에 사용자 할당](#)

5.2.4 BI 플랫폼에서 최상위 폴더에 대한 권한 설정

일반적으로 이 워크플로에 따라 BI 플랫폼에서 최상위 폴더에 대한 권한을 설정합니다.

참고:

이번 릴리스에서는 컨테이너 폴더에 대한 보기 권한이 있어야 해당 폴더를 탐색하고 그 하위 개체를 볼 수 있습니다. 즉, 폴더에 있는 개체를 보려면 최상위 폴더에 대한 보기 권한이 사용자에게 있어야 합니다. 사용자의 보기 권한을 제한하려면 특정 폴더에 대한 사용자 보기 권한을 허용하고 권한이 해당 폴더에만 적용되도록 권한의 범위를 설정하면 됩니다.

1. 권한을 설정하려는 최상위 폴더가 있는 CMC 영역으로 이동합니다.
2. 관리 > 최상위 보안 > 모든 개체를 클릭합니다.
여기에서 개체는 최상위 폴더의 내용을 나타냅니다. 확인 메시지가 나타나면 확인을 클릭합니다.
사용자 보안 대화 상자가 나타나고 최상위 폴더에 대한 액세스 제어 목록이 표시됩니다.
3. 최상위 폴더에 대한 액세스 제어 목록에 사용자를 할당합니다.
4. 필요한 경우 사용자에게 고급 권한을 할당합니다.

관련 항목

- 124 페이지에서 [개체의 액세스 제어 목록에 사용자 할당](#)"
- 124 페이지에서 [개체에 대한 사용자 보안 수정](#)"

5.2.5 사용자에게 대한 보안 설정 확인

경우에 따라서는 사용자의 액세스가 허용 또는 거부된 개체가 무엇인지 알아야 할 수도 있습니다. 보안 쿼리를 사용하여 이를 확인할 수 있습니다. 보안 쿼리를 통해 사용자가 특정 권한을 가지고 있는 대상 개체를 확인하고 사용자 권한을 관리할 수 있습니다. 각 보안 쿼리에 다음 정보를 제공합니다.

- 쿼리 사용자

보안 쿼리를 실행할 대상 사용자나 그룹을 지정합니다. 각 보안 쿼리별로 사용자 하나씩 지정할 수 있습니다.

- 쿼리 권한

보안 쿼리를 실행할 대상 권한, 이 권한의 상태, 권한이 설정된 대상 개체 유형 등을 지정합니다. 예를 들어 사용자가 새로 고칠 수 있는 모든 보고서에 대한 보안 쿼리 또는 사용자가 내보낼 수 없는 모든 보고서에 대한 보안 쿼리를 실행할 수 있습니다.

- 쿼리 컨텍스트

보안 쿼리가 검색할 CMC 영역을 지정합니다. 각 영역에 대해 보안 쿼리에 하위 개체를 포함할지 여부를 선택할 수 있습니다. 보안 쿼리에는 최대 4개 영역이 포함될 수 있습니다.

보안 쿼리를 실행하면 트리 패널의 보안 쿼리 아래 있는 쿼리 결과 영역에 결과가 표시됩니다. 보안 쿼리를 구체화하려면 첫 번째 쿼리 결과 내에서 두 번째 쿼리를 실행합니다.

보안 쿼리를 사용하면 사용자에게 특정 권한이 있는 대상 개체를 볼 수 있으며 이러한 권한을 수정하려는 경우 개체의 위치를 알 수 있으므로 유용합니다. 판매 직원이 판매 관리자로 승진하는 경우를 가정합니다. 판매 관리자는 자신이 이전에 보기 권한만 가지고 있던 Crystal 보고서에 대해 일정 설정 권한이 필요하며, 이러한 보고서는 서로 다른 폴더에 들어 있습니다. 이런 경우, 관리자는 판매 관리자가 모든 폴더의 Crystal 보고서를 볼 수 있도록 보안 쿼리를 실행하고 이 쿼리에 하위 개체를 포함시킵니다. 보안 쿼리를 실행한 후 관리자는 판매 관리자가 보기 권한을 가지고 있는 모든 Crystal 보고서를 쿼리 결과 영역에서 볼 수 있습니다. 세부 정보 패널에 각 Crystal 보고서의 위치가 나타나므로 관리자는 각 보고서를 찾고 보고서에 대한 판매 관리자의 권한을 수정할 수 있습니다.

5.2.5.1 보안 쿼리 실행

1. 세부 정보 패널의 사용자 및 그룹 영역에서 보안 쿼리를 실행할 대상 사용자 또는 그룹을 선택합니다.
2. 관리 > 도구 > 보안 쿼리 만들기를 클릭합니다.

보안 쿼리 만들기: Nina

쿼리 보안 주제

이 쿼리는 다음 보안 주제의 개체를 검색합니다.

Nina

쿼리 권한

이 쿼리는 위의 보안 주제가 다음 권한을 모두 갖는 개체를 검색합니다.

☐ 승인을 받아 쿼리 안 함

컬렉션	유형	권한 이름	상태
일반	일반	사용자가 소유한 폴더에 개체 추가	✓
일반	일반	폴더에 개체 추가	✓

쿼리 컨텍스트

이 쿼리는 CMC의 다음 섹션에서만 개체를 검색합니다.

☒ 폴더 (모두) ☒ 쿼리 하위 개체

보안 쿼리 만들기 대화 상자가 나타납니다.

3. 쿼리 보안 주제 영역의 사용자가 올바른지 확인합니다.
다른 사용자에 대해 보안 쿼리를 실행하려면 찾아보기를 클릭하고 다른 사용자를 선택합니다. 쿼리 보안 주제 찾아보기 대화 상자에서 사용자 목록 또는 그룹 목록을 확장하고 사용자를 찾거나 이름을 기준으로 사용자를 검색합니다. 작업을 마쳤으면 확인을 클릭하여 보안 쿼리 만들기 대화 상자로 돌아갑니다.
4. 쿼리 권한 영역에서 권한을 지정하고 쿼리를 실행하려는 각 권한의 상태를 지정합니다.
 - 사용자가 개체에 가지고 있는 특정 권한에 대해 쿼리를 실행하려는 경우 찾아보기를 클릭하고 보안 쿼리를 실행하려는 각 권한의 상태를 설정한 다음 확인을 클릭합니다.

팁:
각 권한 옆에 있는 삭제 단추를 클릭하여 특정 권한을 쿼리에서 삭제할 수 있고, 머리글 행에 있는 삭제 단추를 클릭하면 쿼리에서 모든 권한을 삭제할 수 있습니다.

 - 일반 보안 쿼리를 실행하려는 경우 승인을 받아 쿼리 안 함 확인란을 선택합니다.
그러면 BI 플랫폼에서는 액세스 제어 목록에 사용자가 있는 모든 개체에 대해 일반 보안 쿼리를 실행합니다. 이 경우 사용자가 개체에 대해 어떤 권한을 가지고 있는지는 상관이 없습니다.
5. 쿼리 컨텍스트 영역에서 쿼리할 CMC 영역을 지정합니다.

- a. 목록 옆에 있는 확인란을 선택합니다.
- b. 목록에서 쿼리하려는 CMC 영역을 선택합니다.
영역 내의 더 구체적인 위치(예를 들어, 폴더 아래의 특정 폴더)를 쿼리하려면 찾아보기를 클릭하여 쿼리 컨텍스트 찾아보기 대화 상자를 엽니다. 세부 정보 창에서 쿼리하려는 폴더를 선택하고 확인을 클릭합니다. 보안 쿼리 대화 상자로 돌아오면 사용자가 지정한 폴더가 대화 상자의 목록 아래 표시됩니다.
- c. 쿼리 하위 개체를 선택합니다.
- d. 쿼리하려는 각 CMC 영역에 대해 위 단계를 반복합니다.

참고:

영역을 최대 네 개까지 쿼리할 수 있습니다.

6. 확인을 클릭합니다.
보안 쿼리가 실행되고 쿼리 결과 영역으로 이동합니다.
7. 쿼리 결과를 보려면 트리 패널에서 보안 쿼리를 확장하고 쿼리 결과를 클릭합니다.

팁:

쿼리 결과는 사용자의 이름에 따라 나열됩니다.

쿼리 결과가 세부 정보 패널에 표시됩니다.

사용자가 로그오프하기 전까지는 단일 사용자 세션의 모든 보안 쿼리 결과가 쿼리 결과 영역에 유지됩니다. 내용을 수정하여 쿼리를 다시 실행하려면 작업 > 쿼리 편집을 클릭합니다. 쿼리를 선택하고 작업 > 쿼리 다시 실행을 클릭하면 동일한 쿼리를 다시 실행할 수 있습니다. 보안 쿼리 결과를 유지하려면 작업 > 내보내기를 클릭하여 보안 쿼리 결과를 CSV 파일로 내보냅니다.

5.3 액세스 수준 작업

다음과 같은 액세스 수준 작업을 수행할 수 있습니다.

- 기존 액세스 수준을 복사한 다음 복사본을 변경하고 이름을 바꾼 후 새로운 액세스 수준으로 저장합니다.
- 액세스 수준을 만들고, 이름을 바꾸며, 삭제합니다.
- 액세스 수준에서 권한을 수정합니다.
- 시스템 내에서 액세스 수준과 다른 객체 간의 관계를 추적합니다.
- 여러 사이트에서 액세스 수준을 복제하고 관리합니다.
- BI 플랫폼에서 미리 정의된 액세스 수준을 사용하여 다수의 사용자에게 대해 빠르고 일정하게 권한을 설정합니다.

다음 표에서는 미리 정의된 액세스 수준에 포함된 권한을 요약하여 보여 줍니다.

테이블5-2: 미리 정의된 액세스 수준

액세스 수준	설명	포함된 권한
보기	폴더 수준으로 설정하면 사용자는 폴더, 폴더 안의 개체 및 각 개체에 대해 생성된 인스턴스가 표시됩니다. 개체 수준으로 설정하면 사용자는 개체, 개체의 기록 및 개체에 대해 생성된 인스턴스가 표시됩니다.	<ul style="list-style-type: none"> 개체 보기 문서 인스턴스 보기
일정	사용자는 특정 데이터 소스에 대해 반복적으로 실행되도록 개체에 일정을 설정하여 인스턴스를 만들 수 있습니다. 사용자는 자신이 소유한 인스턴스의 일정을 보거나 삭제 또는 일시 중지할 수 있습니다. 또한 다른 형식과 대상을 예약하고, 매개 변수 및 데이터베이스 로그인 정보를 설정하고, 작업을 처리할 서버를 선택하고, 폴더에 내용을 추가하고, 개체 또는 폴더를 복사할 수도 있습니다.	보기 액세스 수준 권한 및 다음 권한 <ul style="list-style-type: none"> 문서 실행 일정 설정 작업을 처리할 서버 그룹 정의 다른 폴더에 개체 복사 대상에 보내도록 일정 설정 보고서 데이터 인쇄 보고서 데이터 내보내기 사용자가 소유한 개체 편집 사용자가 소유한 인스턴스 삭제 사용자가 소유한 문서 인스턴스 일시 중지 및 다시 시작
요청 시 보기	사용자는 필요할 때 데이터 소스를 기준으로 데이터를 새로 고칠 수 있습니다.	일정 액세스 수준 권한 및 다음 권한 <ul style="list-style-type: none"> 보고서 데이터 새로 고침
모든 권한	사용자에게는 개체의 모든 관리 권한이 있습니다.	다음을 포함한 모든 사용 가능한 권한 <ul style="list-style-type: none"> 폴더에 개체 추가 개체 편집 개체에 대한 사용자의 권한 수정 개체 삭제 인스턴스 삭제

다음 표에서는 액세스 수준에 대한 특정 작업을 수행하는 데 필요한 권한을 요약하여 보여 줍니다.

액세스 수준 작업	필요한 권한
액세스 수준 만들기	<ul style="list-style-type: none"> 액세스 수준 최상위 폴더에 대한 추가 권한
액세스 수준에서 세부 권한 보기	<ul style="list-style-type: none"> 액세스 수준에 대한 보기 권한
사용자에게 개체에 대한 액세스 수준 할당	<ul style="list-style-type: none"> 액세스 수준에 대한 보기 권한 액세스 수준에 대한 보안 할당을 위해 액세스 수준 사용 권한 개체에 대한 권한 수정 권한 또는 개체와 사용자에게 대한 권한 보안 수정 권한 <p>참고: 권한 보안 수정 권한이 부여된 사용자가 다른 사용자에게 액세스 수준을 할당하려면 동일한 액세스 수준이 자신에게도 할당되어 있어야 합니다.</p>
액세스 수준 수정	<ul style="list-style-type: none"> 액세스 수준에 대한 보기 및 편집 권한
액세스 수준 삭제	<ul style="list-style-type: none"> 액세스 수준에 대한 보기 및 삭제 권한
액세스 수준 복제	<ul style="list-style-type: none"> 액세스 수준에 대한 보기 권한 액세스 수준에 대한 복사 권한 액세스 수준 최상위 폴더에 대한 추가 권한

5.3.1 보기 및 요청 시 보기 액세스 수준 중에서 선택

웹을 통해 보고서를 만드는 경우에는 라이브 데이터와 저장된 데이터 중 무엇을 사용할지 신중하게 결정해야 합니다. 둘 중 어느 것을 선택하더라도 BI 플랫폼에서는 가능한 빨리 첫 페이지를 표시하므로 나머지 데이터가 처리되는 동안 보고서를 볼 수 있습니다. 이 단원에서는 이를 선택할 때 사용할 수 있는 2개의 미리 정의된 액세스 수준의 차이점에 대해 설명합니다.

요청 시 보기 액세스 수준

주문형 보고서를 작성하면 사용자는 데이터베이스 서버의 라이브 데이터에 실시간으로 액세스할 수 있습니다. 라이브 데이터를 사용하면 지속적으로 변하는 데이터를 최신으로 유지하여 사용자가 항상 정확한 정보에 액세스할 수 있습니다. 예를 들어, 배송되는 제품을 지속적으로 추적해야 하는 대형 물류 센터의 관리자에게는 라이브 보고서 형식으로 정보를 제공하는 방법이 적절합니다.

그러나 모든 보고서에 라이브 데이터를 제공하기 전에 모든 사용자가 데이터베이스 서버에 항상 액세스할 수 있도록 설정할지 여부를 결정해야 합니다. 데이터가 가끔 변경되거나 단속적으로 변경되는 경우 데이터베이스에 대한 요청이 많아지면 네트워크 트래픽이 증가하고 서버 리소스가 소모될 뿐입니다. 이런 경우에는 사용자가 데이터베이스 서버에 액세스하지 않고도 항상 최신 데이터(보고서 인스턴스)를 볼 수 있도록 주기적으로 보고서 일정을 설정하는 것이 좋습니다.

데이터베이스에 대해 보고서를 새로 고치려면 사용자에게 요청 시 보기 권한이 있어야 합니다.

보기 액세스 수준

지정된 시간에 보고서가 실행되도록 일정을 설정하면 네트워크 트래픽 및 데이터베이스 서버 접속 횟수를 줄일 수 있습니다. 보고서가 실행되면 사용자는 추가로 데이터베이스에 접속하지 않고도 필요에 따라 보고서 인스턴스를 볼 수 있습니다.

보고서 인스턴스는 지속적으로 업데이트되지 않는 데이터를 처리하는 데 유용합니다. 사용자가 보고서 인스턴스를 탐색하고 열 또는 차트에서 세부 데이터를 보기 위해 드릴다운하는 경우 데이터베이스 서버에 직접 액세스하는 대신 저장된 데이터에 액세스하게 됩니다. 따라서 저장된 데이터를 사용하는 보고서는 네트워크를 통한 데이터 전송을 최소화할 뿐만 아니라 데이터베이스 서버의 작업 로드도 줄입니다.

예를 들어, 매출 데이터베이스가 하루에 한 번 업데이트되는 경우에는 주기에 맞게 보고서를 실행할 수 있습니다. 이렇게 하면 판매 담당자는 보고서를 열 때마다 데이터베이스에 액세스하지 않고도 최신 매출 데이터를 볼 수 있습니다.

보고서 인스턴스를 표시하려면 사용자에게 보기 권한만 있으면 됩니다.

5.3.2 기존 액세스 수준 복사

기존 액세스 수준 중 하나와 크게 다르지 않은 액세스 수준이 필요한 경우에는 복사를 통해 액세스 수준을 만드는 것이 좋습니다.

1. 액세스 수준 영역으로 이동합니다.
2. 세부 정보 패널에서 액세스 수준을 선택합니다.

팁:

새 액세스 수준에 필요한 것과 비슷한 권한이 포함되어 있는 액세스 수준을 선택합니다.

3. 구성 > 복사를 클릭합니다.
선택한 액세스 수준의 복사본이 세부 정보 패널에 나타납니다.

5.3.3 새 액세스 수준 만들기

기존의 모든 액세스 수준과 상당히 다른 액세스 수준이 필요한 경우에는 액세스 수준을 새로 만드는 것이 좋습니다.

1. 액세스 수준 영역으로 이동합니다.

2. 관리 > 새로 만들기 > 액세스 수준 만들기를 클릭합니다.
새 액세스 수준 만들기 대화 상자가 나타납니다.
3. 새 액세스 수준에 대한 제목과 설명을 입력한 다음 확인을 클릭합니다.
액세스 수준 영역으로 돌아옵니다. 새 액세스 수준이 세부 정보 패널에 표시됩니다.

5.3.4 액세스 수준의 이름을 변경하려면

1. 세부 정보 패널의 액세스 수준 영역에서 이름을 변경하려는 액세스 수준을 선택합니다.
2. 관리 > 속성을 클릭합니다.
속성 대화 상자가 나타납니다.
3. 액세스 수준의 새 이름을 제목 필드에 입력하고 저장 후 단기를 클릭합니다.
액세스 수준 영역으로 돌아옵니다.

5.3.5 액세스 수준 삭제

1. 세부 정보 패널의 액세스 수준 영역에서 삭제하려는 액세스 수준을 선택합니다.
2. 관리 > 액세스 수준 삭제를 클릭합니다.

참고:

미리 정의된 액세스 수준은 삭제할 수 없습니다.

해당 액세스 수준의 영향을 받는 개체에 대한 정보가 대화 상자에 표시됩니다. 액세스 수준을 삭제하지 않으려면 취소를 클릭하여 대화 상자를 닫습니다.

3. 삭제를 클릭합니다.
액세스 수준이 삭제되고 액세스 수준 영역으로 돌아옵니다.

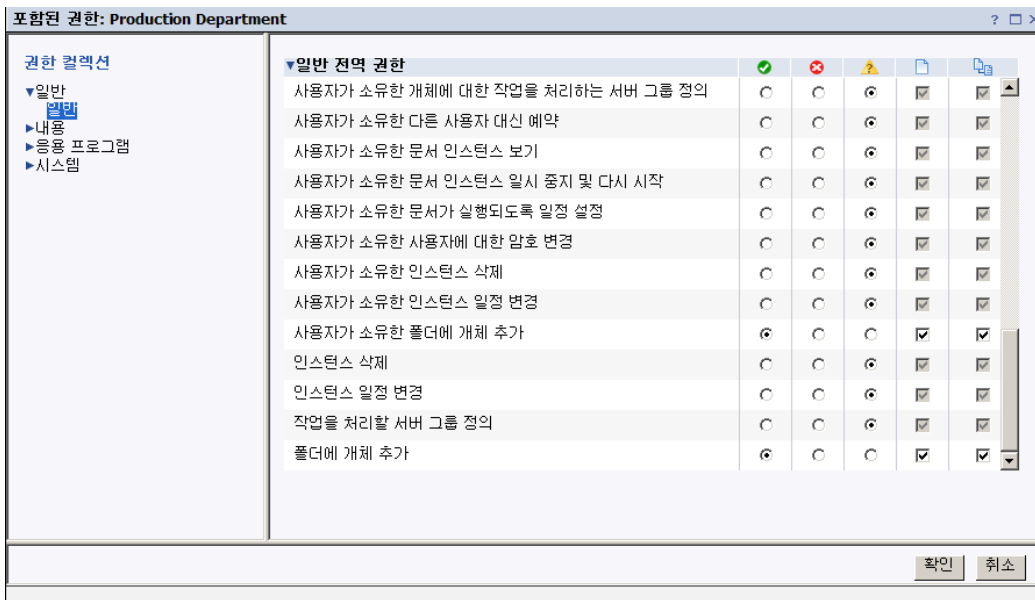
5.3.6 액세스 수준의 권한 수정

액세스 수준에 대해 권한을 설정하려면 먼저 유형에 상관없이 모든 개체에 적용되는 일반 전역 권한을 설정한 다음 특정 개체 유형을 기반으로 일반 설정을 재정의하려는 조건을 지정합니다.

1. 세부 정보 패널의 액세스 수준 영역에서 권한을 수정하려는 액세스 수준을 선택합니다.
2. 작업 > 포함된 권한을 클릭합니다.

포함된 권한 대화 상자가 나타나고 유효한 권한의 목록이 표시됩니다.

3. 권한 추가/제거를 클릭합니다.



탐색 목록에 있는 액세스 수준에 대한 권한 컬렉션이 포함된 권한 대화 상자에 표시됩니다. 기본적으로 일반 전역 권한 섹션이 확장되어 있습니다.

4. 일반 전역 권한을 설정합니다.
각 권한의 상태를 허가됨, 거부됨 또는 지정되지 않음으로 설정할 수 있습니다. 해당 권한을 개체에만 적용할지 하위 개체에만 적용할지 아니면 둘 다에 적용할지도 선택할 수 있습니다.
5. 액세스 수준의 유형별 권한을 설정하려면 탐색 목록에서 권한 컬렉션을 클릭한 다음 권한을 설정하려는 개체 유형에 적용되는 하위 컬렉션을 클릭합니다.
6. 설정을 마쳤으면 확인을 클릭합니다.
유효한 권한의 목록이 다시 표시됩니다.

관련 항목

- 123 페이지에서 [CMC에서 개체의 보안 설정 관리](#)"
- 120 페이지에서 [유형별 권한](#)"

5.3.7 액세스 수준과 개체 사이의 관계 추적

액세스 수준을 수정하거나 삭제하기 전에 먼저, 액세스 레벨을 변경하면 CMC 내의 개체에 부정적인 영향을 미치지 않는지 확인해야 합니다. 액세스 수준에 대해 관계 쿼리를 실행하면 됩니다.

관계 쿼리를 사용하면 액세스 수준의 영향을 받는 개체를 한곳에서 간편하게 볼 수 있으므로 권한 관리에 유용합니다. 회사가 조직 재구성을 통해서 A 부서와 B 부서, 두 개의 부서를 C 부서로 병합하는 경우를 가정합니다. 관리자는 A 부서와 B 부서가 더 이상 존재하지 않을 것이므로 이들 부서에 대한 액세스 수준을 삭제하기로 결정합니다. 관리자는 삭제하기 전에 두 액세스 수준 모두에 대해 관계 쿼리를 실행합니다. 관리자는 쿼리 결과 영역에서 액세스 수준 삭제 시 영향을 받게 될 개체를 볼 수 있습니다. 액세스 수준 삭제 이전에 개체에 대한 권한 수정이 필요한 경우 CMC 내 개체의 위치를 세부 정보 패널에서 확인할 수 있습니다.

참고:

- 영향을 받는 개체 목록을 보려면 해당 개체에 대한 보기 권한이 있어야 합니다.
- 액세스 수준에 대해서만 관계 쿼리를 수행한 결과로는 액세스 수준이 명시적으로 할당된 개체가 반환됩니다. 상속 설정으로 인해 해당 액세스 수준을 사용하는 개체는 쿼리 결과에 표시되지 않습니다.

5.3.8 여러 사이트에서 액세스 수준 관리

액세스 수준은 원본 사이트에서 대상 사이트로 복제할 수 있는 개체 중 하나입니다. 복제 개체의 액세스 제어 목록에 액세스 수준이 표시되면 해당 액세스 수준을 복제할 수 있습니다. 예를 들어 Crystal 보고서에 대한 액세스 수준 A를 사용자에게 부여하고 사이트 간에 Crystal 보고서를 복제하면 액세스 수준 A도 복제됩니다.

참고:

대상 사이트에 이름이 같은 액세스 수준이 이미 있으면 액세스 수준이 복제되지 않습니다. 이러한 경우 복제하기 전에 사용자나 대상 사이트 관리자가 액세스 수준 중 하나의 이름을 변경해야 합니다.

사이트 간에 액세스 수준을 복제한 후에는 이 단원에서 설명하는 관리 관련 사항을 고려해야 합니다.

원본 사이트에서 복제된 액세스 수준 수정

원본 사이트에서 복제된 액세스 수준을 수정하면 일정에 따라 다음 번에 복제를 실행할 때 대상 사이트에서 액세스 수준이 업데이트됩니다. 양방향 복제 시나리오에서는 대상 사이트에서 복제된 액세스 수준을 수정하면 원본 사이트에서도 액세스 수준이 변경됩니다.

참고:

사이트 중 하나에서 액세스 수준을 변경할 때는 다른 사이트의 개체에 악영향을 주지 않는지 확인해야 합니다. 변경 작업을 수행하기 전에 사이트 관리자에게 문의하여 복제된 액세스 수준에 대한 관계 쿼리를 실행하도록 요청하십시오.

대상 사이트에서 복제된 액세스 수준 수정

참고:

이는 단방향 복제에만 해당합니다.

대상 사이트에서 복제된 액세스 수준을 변경해도 원본 사이트에는 반영되지 않습니다. 예를 들어 원본 사이트에서 복제된 액세스 수준의 Crystal 보고서 일정을 설정하는 권한이 거부되었더라도 대상 사이트 관리자는 이러한 권한을 허용할 수 있습니다. 따라서 액세스 수준 이름과 복제된 개체 이름이 같더라도 이러한 개체에 대해 사용자가 갖는 유효 권한은 대상 사이트마다 다를 수 있습니다.

원본 사이트와 대상 사이트 사이에 복제된 액세스 수준이 다른 경우 일정에 따라 다음 번에 복제 작업이 실행될 때 유효 권한의 차이가 감지됩니다. 원본 사이트 액세스 수준을 적용하여 대상 사이트 액세스 수준을 재정의할 수도 있고, 대상 사이트 액세스 수준을 그대로 유지할 수도 있습니다. 그러나 원본 사이트 액세스 수준을 적용하여 대상 사이트 액세스 수준을 재정의하지 않으면 복제 대기 중인 개체 중 해당 액세스 수준을 사용하는 어떠한 개체도 복제되지 않습니다.

사용자가 대상 사이트에서 복제된 액세스 수준을 수정할 수 없도록 제한하려면 대상 사이트 사용자를 액세스 수준에 사용자로 추가하고 해당 사용자에게 보기 권한만 부여합니다. 이렇게 하면 대상 사이트 사용자는 액세스 수준을 볼 수는 있지만 권한 설정을 수정하거나 다른 사용자에게 할당할 수 없습니다.

관련 항목

- 621 페이지에서 [연합](#)"
- 134 페이지에서 [액세스 수준과 개체 사이의 관계 추적](#)"

5.4 상속 무시

상속을 사용하면 개별 개체에 대해 권한을 설정하지 않고도 보안 설정을 관리할 수 있습니다. 하지만 권한이 상속되지 않도록 해야 하는 경우도 있습니다. 예를 들면 객 개체별로 권한을 사용자 지정하려는 경우가 그렇습니다. 이런 경우 개체의 액세스 제어 목록에서 특정 사용자에게 권한을 비활성화할 수 있습니다. 이때 그룹 상속이나 폴더 상속 중 어느 쪽을 비활성화할지 아니면 두 가지 모두를 비활성화할지 선택할 수 있습니다.

참고:

상속이 무시되면 모든 권한에 대해서도 무시되며, 일부에 대해서는 상속을 해제하고 다른 일부에 대해서는 상속을 유지할 수는 없습니다. 즉, 모든 권한에 대해서 상속이 해제되는 것입니다.

상속 무시 다이어그램에서 그룹 상속 및 폴더 상속은 기본적으로 적용됩니다. 빨강 사용자는 1번 권한과 5번 권한을 부여됨으로, 2, 3, 4번 권한을 지정되지 않음으로, 6번 권한을 명시적으로 거부됨으로 상속받습니다. 그룹에 대해 폴더 수준으로 설정된 이러한 권한은 빨강 사용자 및 그룹 내 모든 다른

멤버가 폴더 개체 권한 A와 B를 가지게 됨을 의미합니다. 폴더 수준에서 상속이 무시되는 경우 해당 폴더에서 개체에 대한 빨강 사용자의 모든 권한은 관리자가 새 권한을 할당하기 전까지 해제됩니다.

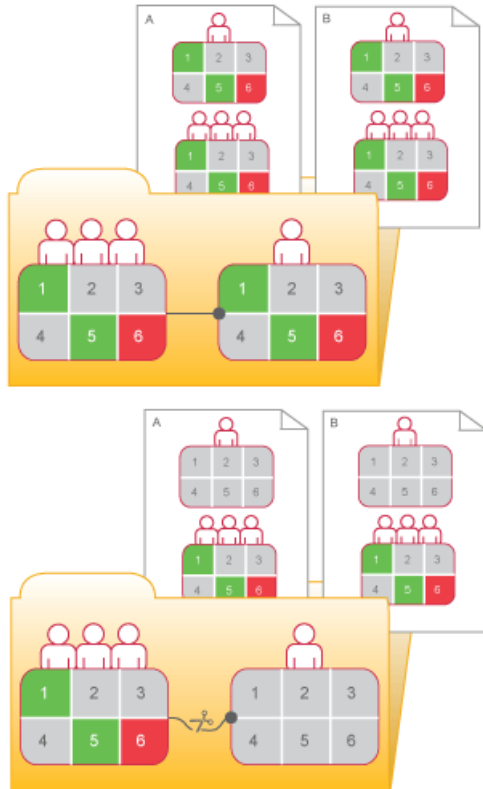


그림 5-9: 상속 무시

5.4.1 상속을 비활성화하려면

여기에서 설명하는 절차에 따라 개체의 액세스 제어 목록에서 사용자에게 대한 그룹 또는 폴더 상속을 비활성화하거나 두 가지 상속을 모두 비활성화할 수 있습니다.

1. 상속을 비활성화할 개체를 선택합니다.
2. 관리 > 사용자 보안을 클릭합니다.
사용자 보안 대화 상자가 나타납니다.
3. 상속을 비활성화할 사용자를 선택하고 보안 할당을 클릭합니다.
보안 할당 대화 상자가 나타납니다.
4. 상속 설정을 구성합니다.

- 그룹 상속(사용자가 소속 그룹으로부터 상속하는 권한)을 비활성화하려면 부모 그룹에서 상속 확인란의 선택을 취소합니다.
- 폴더 상속(개체가 폴더로부터 상속하는 권한 설정)을 비활성화하려면 부모 폴더에서 상속 확인란의 선택을 취소합니다.

5. 확인을 클릭합니다.

5.5 관리 위임을 위한 권한 사용

또한 권한을 통해 개체 및 설정에 대한 액세스를 제어하고, 조직 내의 직무별 그룹 사이에 관리 작업을 분담시킬 수 있습니다. 예를 들어, 서로 다른 부서의 직원들이 각자 자기 부서의 사용자 및 그룹을 관리하도록 할 수 있습니다. 또는 전사적인 수준의 BI 플랫폼 관리 작업은 관리자 한 명이 담당하는 대신 서버 관리는 모두 IT 부서의 직원들이 처리하도록 할 수도 있습니다.

그룹 구조 및 폴더 구조가 위임된 관리 보안 구조와 일치한다고 가정할 경우, 위임된 관리자 권한을 전체 사용자 그룹에 부여해야 하지만 위임된 관리자에게 관리 대상 사용자에 대한 전체 권한을 부여해서는 안 됩니다. 예를 들어 위임된 관리자는 사용자 특성을 편집하거나 이를 다른 그룹에 다시 할당하지 못하도록 해야 할 수 있습니다.

위임된 관리자를 위한 권한 표에는 위임된 관리자가 일반적인 작업을 수행하는 데 필요한 권한이 요약되어 있습니다.

테이블5-3: 위임된 관리자를 위한 권한

위임된 관리자의 작업	위임된 관리자에게 필요한 권한
새 사용자 만들기	최상위 사용자 폴더에 대한 추가 권한
새 그룹 만들기	최상위 사용자 그룹 폴더에 대한 추가 권한
통제되는 그룹 및 그룹 내의 개별 사용자 삭제	관련 그룹에 대한 삭제 권한
위임된 관리자가 만든 사용자만 삭제	최상위 사용자 폴더에 대한 소유자 삭제 권한
위임된 관리자가 만든 사용자 및 그룹만 삭제	최상위 사용자 그룹 폴더에 대한 소유자 삭제 권한

위임된 관리자의 작업	위임된 관리자에게 필요한 권한
위임된 관리자가 만든 사용자만 조작(해당 그룹에 사용자를 추가하는 경우 포함)	최상위 사용자 폴더에 대한 소유자 편집 및 소유자 권한 보안 수정 권한
위임된 관리자가 만든 그룹만 조작(해당 그룹에 사용자를 추가하는 경우 포함)	최상위 사용자 그룹 폴더에 대한 소유자 편집 및 소유자 권한 보안 수정 권한
관리되는 그룹의 사용자 암호 수정	관련 그룹에 대한 암호 편집 권한
위임된 관리자가 만든 사용자의 암호만 수정	최상위 사용자 폴더 또는 관련 그룹에 대한 소유자 암호 편집 권한 참고: 그룹에 대한 소유자 암호 편집 권한 설정은 사용자를 관련 그룹에 추가할 때만 사용자에게 적용됩니다.
사용자 이름, 설명, 다른 특성 수정 및 다른 그룹에 사용자 다시 할당	관련 그룹에 대한 편집 권한
위임된 관리자가 만든 사용자에 대해서만 사용자 이름, 설명, 기타 특성 수정 및 다른 그룹에 사용자 다시 할당	최상위 사용자 폴더 또는 관련 그룹에 대한 소유자 편집 권한 참고: 관련 그룹에 대한 소유자 편집 권한 설정은 사용자를 관련 그룹에 추가할 때만 사용자에게 적용됩니다.

5.5.1 개체에 대한 사용자 권한 수정 옵션 선택

위임된 관리를 설정할 경우 제어할 사용자에게 대해 위임된 관리자 권한을 부여합니다. 위임된 관리자에게 모든 권한을 부여해도 되지만 고급 권한 설정을 사용하여 권한 수정 권한을 보류하고 위임된 관리자에게 권한 보안 수정 권한을 대신 부여하는 것이 좋습니다. 권한 상속 설정 수정 권한 대신 권한 상속 설정을 안전하게 수정 권한을 관리자에게 부여할 수도 있습니다. 이들 권한 사이의 차이점은 아래에 요약되어 있습니다.

개체에 대한 사용자 권한 수정

이 권한이 있으면 사용자는 그 개체에 대한 모든 사용자의 권한을 수정할 수 있습니다. 예를 들어 A 사용자가 개체에 대해 개체 보기 및 개체에 대한 사용자 권한 수정 권한을 갖고 있는 경우 A 사용자는 자신이나 다른 사용자가 이 개체에 대한 모든 권한을 갖도록 해당 개체에 대한 권한을 변경할 수 있습니다.

개체에 대한 사용자 권한을 안전하게 수정합니다.

이 권한이 있을 경우 사용자는 자신에게 이미 부여된 권한만 부여 또는 거부하거나 지정되지 않은 상태로 되돌릴 수 있습니다. 예를 들어, A 사용자가 보기 및 개체에 대한 사용자 권한을 안전하게 수정합니다. 권한을 갖고 있는 경우 A 사용자는 자신에게 다른 권한을 추가로 부여할 수 없고 이들 두 권한(보기 및 개체에 대한 사용자 권한을 안전하게 수정합니다.)만 다른 사용자에게 부여 또는 거부할 수 있습니다. 또한 A 사용자는 자신이 개체에 대한 사용자 권한을 안전하게 수정합니다. 권한을 갖고 있는 개체에 대해서만 사용자의 권한을 변경할 수 있습니다.

A 사용자가 O 개체의 B 사용자에게 권한을 수정하기 위해서는 다음과 같은 권한을 가지고 있어야 합니다.

- A 사용자가 O 개체에 대해 개체에 대한 사용자 권한을 안전하게 수정합니다. 권한을 갖고 있어야 합니다.
- A 사용자가 B 사용자에게 변경하려는 각 권한 또는 액세스 수준이 A 사용자에게 부여되어 있어야 합니다.
- A 사용자가 B 사용자에게 개체에 대한 사용자 권한을 안전하게 수정합니다. 권한을 갖고 있어야 합니다.
- 액세스 수준이 할당되는 경우 A 사용자가 b 사용자와 관련하여 변경되는 액세스 수준에 대해 액세스 수준 할당 권한을 갖고 있어야 합니다.

권한의 범위를 지정하면 위임된 관리자가 할당할 수 있는 유효한 권한을 추가로 제한할 수 있습니다. 예를 들어, 위임된 관리자가 폴더에 대한 권한 보안 수정 및 편집 권한을 갖도록 하되 이러한 권한의 범위를 폴더로만 제한하고 폴더의 하위 개체에는 적용되지 않도록 할 수 있습니다. 실제로, 위임된 관리자는 폴더에 대해서만 편집 권한을 부여할 수 있으며(하위 개체에 대해서는 불가능) 이는 개체에 적용하는 범위에서만 가능합니다. 반면에, 위임된 관리자에게 폴더에 대해 하위 개체에 적용 범위에서만 편집 권한이 부여된 경우 해당 관리자는 다른 사용자에게 폴더 하위 개체에 대해 두 범위 모두에서 편집 권한을 부여할 수 있습니다. 하지만 폴더 자체에 대해서는 하위 개체에 적용 범위에서만 편집 권한을 부여할 수 있습니다.

또한 위임된 관리자는 개체에 대한 사용자 권한을 안전하게 수정합니다. 권한을 가지고 있지 않은 다른 사용자들을 위해 해당 그룹에 대한 권한을 수정할 수 없습니다. 이러한 제약은 예를 들어, 같은 폴더에 대한 서로 다른 사용자 그룹에 권한을 부여하는 두 명의 위임된 관리자가 있을 때 한 명의 위임된 관리자가 다른 위임된 관리자가 관리하는 그룹에 대한 액세스를 거부할 수 없도록 하려는 경우에 유용합니다. 이는 권한 보안 수정 권한을 통해 적용됩니다. 위임된 관리자에게는 일반적으로 서로에 대한 권한 보안 수정 권한이 없기 때문입니다.

권한 상속 설정을 안전하게 수정

이 권한을 사용하면 위임된 관리자가 액세스할 수 있는 개체와 관련하여 이 위임된 관리자가 다른 사용자의 상속 설정을 수정하도록 할 수 있습니다. 다른 사용자의 상속 설정을 수정할 수 있으려면 위임된 관리자가 개체 및 대상 사용자의 사용자 계정에 대해 이 권한을 갖고 있어야 합니다.

5.5.2 소유자 권한

소유자 권한은 확인된 개체의 소유자에게만 적용되는 권한입니다. BI 플랫폼에서 개체의 소유자는 개체를 만든 사용자이고, 해당 사용자가 시스템에서 삭제되면 소유권은 관리자에게 되돌아 갑니다.

소유자 권한은 소유자를 기준으로 보안을 관리하는 데 유용합니다. 예를 들어 여러 사용자가 문서를 만들고 볼 수 있지만 본인 소유의 문서만 수정 또는 삭제할 수 있는 폴더 또는 폴더 계층을 만들려고 합니다. 또한 소유자 권한은 다른 사람의 인스턴스가 아닌 본인이 만든 보고서의 인스턴스를 조작하는 데 유용합니다. 액세스 수준 일정을 설정하는 경우 이 권한을 사용하면 사용자가 본인 소유의 인스턴스만 편집하고 삭제하고 일정을 다시 설정하도록 할 수 있습니다.

소유자 권한은 상응하는 일반 권한과 유사하게 적용됩니다. 그러나 소유자 권한은 사용자에게 소유자 권한을 부여하고 일반 권한을 부여하지 않았거나 일반 권한을 지정하지 않은 경우에만 유효합니다.

5.6 관리 권한을 위한 권장 사항 요약

권한을 관리할 때는 다음 고려 사항을 염두에 두어야 합니다.

- 어디에서나 가능한 액세스 수준을 사용합니다. 이와 같이 미리 정의된 권한 집합을 사용하면 일반적인 사용자 요구 사항과 관련된 권한을 함께 그룹화하여 관리를 간소화할 수 있습니다.
- 최상위 폴더에 대한 권한 및 액세스 수준을 설정합니다. 상속을 활성화하면 최소한의 관리 조정으로 시스템 전체에 이러한 권한이 아래로 전달됩니다.
- 가능하면 항상 상속이 무시되지 않도록 하십시오. 이렇게 하면 BI 플랫폼에 추가한 콘텐츠를 보호하기 위한 작업을 수행하는 데 필요한 시간을 줄일 수 있습니다.
- 폴더 수준에서 사용자와 그룹에 대한 적절한 권한을 설정한 다음 그 폴더에 개체를 게시합니다. 기본적으로 폴더에 대한 권한이 있는 사용자나 그룹은 이후에 그 폴더에 게시되는 모든 개체에 대해서도 동일한 권한을 상속받습니다.
- 사용자를 사용자 그룹으로 묶어 구성하고, 전체 그룹에 액세스 수준과 권한을 할당하고, 필요한 경우 특정 구성원에게 별도의 액세스 수준과 권한을 할당합니다.
- 시스템의 각 관리자에 대해 개별 administrator 계정을 만들고 이를 Administrators 그룹에 추가하면 시스템 변경에 따른 책임 소재를 더욱 명확히 할 수 있습니다.
- 기본적으로 Everyone 그룹에는 BI 플랫폼의 최상위 폴더에 대한 매우 제한된 권한이 부여됩니다. 설치 후에 Everyone 그룹 구성원의 권한을 검토하고 적절한 보안을 할당하는 것이 좋습니다.

장6 BI 플랫폼 보안

6.1 보안 개요

이 단원에서는 BI 플랫폼이 엔터프라이즈 보안 관련 사항을 다루는 방식에 대해 자세히 설명합니다. 관리자와 시스템 설계자는 여기에서 보안에 관련된 일반적인 문제를 해결하는 데 도움이 되는 정보를 얻을 수 있습니다.

BI 플랫폼 아키텍처는 오늘날의 업무와 조직에 영향을 미치는 여러 가지 보안 관련 문제를 고려하여 디자인되었습니다. 현재 릴리스는 분산 보안, 단일 로그인, 리소스 액세스 보안, 단위별 개체 권한 같은 기능을 지원할 뿐만 아니라 권한이 없는 사용자의 액세스를 차단하기 위한 타사의 인증 기능을 지원합니다.

BI 플랫폼은 SAP BusinessObjectsEnterprise 제품군의 구성 요소 수를 늘리기 위한 프레임워크를 제공하므로, 이 단원에서는 보안 특징 및 관련 기능에 대한 자세한 설명을 통해 프레임워크 자체의 보안 강화 및 유지 관리 방법을 보여 줍니다. 이를 위해 자세한 절차를 설명하는 대신 개념적인 내용을 주로 설명하고 주요 절차에 대한 링크를 제공합니다.

시스템 보안 개념에 대해 간략히 소개한 후 다음 항목에서 자세한 내용을 다룹니다.

- 암호화 및 데이터 처리 보안 모델을 사용하여 데이터를 보호하는 방법
- BI 플랫폼 배포 시 SSL(Secure Sockets Layer)을 설정하는 방법
- BI 플랫폼에 방화벽을 설치하고 방화벽을 유지 관리하는 지침
- 역방향 프록시 서버 구성

6.2 재해 복구 계획

재해가 발생하는 경우에도 비즈니스가 중단 없이 최대한 지속될 수 있도록 BI 플랫폼에서 조직의 투자를 보호하려면 특정 단계를 수행해야 합니다. 이 단원에서는 조직에 대한 재해 복구 계획의 기초를 마련하는 데 사용할 지침을 제공합니다.

일반 지침

- 정기 시스템 백업을 수행한 다음 필요에 따라 일부 백업 미디어 복사본을 오프사이트에 복사합니다.
- 모든 소프트웨어 미디어를 안전하게 보관합니다.
- 모든 라이선스 문서를 안전하게 보관합니다.

특정 지침

재해 복구 계획의 관점에서 특별히 주의해야 하는 시스템 리소스에는 다음 세 가지가 있습니다.

- 파일 리포지토리 서버의 콘텐츠: 전용 콘텐츠(예: 보고서)가 포함됩니다. 이 콘텐츠는 정기적으로 백업해야 합니다. 재해가 발생할 경우 정기적인 백업 프로세스 이외에는 이러한 콘텐츠를 다시 생성할 수 있는 방법이 없습니다.
- CMS에서 사용하는 시스템 데이터베이스: 이 리소스에는 매우 중요한 배포 메타데이터(예: 사용자 정보, 보고서, 특정 조직에만 적용되는 기타 중요 정보)가 모두 포함됩니다.
- 데이터베이스 정보 키 파일(.dbinfo 파일): 이 리소스에는 시스템 데이터베이스에 대한 마스터 키가 포함되어 있습니다. 어떤 이유로 이 키를 사용할 수 없는 경우 시스템 데이터베이스에 액세스할 수 없습니다. BI 플랫폼을 배포한 후에는 이 리소스에 대한 암호를 안전하고 알려진 위치에 보관하는 것이 좋습니다. 암호가 없으면 파일을 다시 생성할 수 없으므로 시스템 데이터베이스에 액세스할 수 없습니다.

6.3 배포 보안 설정을 위한 일반 권장 사항

다음은 BI 플랫폼 배포 시 보안을 설정할 때 권장되는 지침입니다.

- 방화벽을 사용하여 CMS와 다른 시스템 구성 요소 간 통신을 보호합니다. 가능하면 CMS를 항상 방화벽 뒤에 숨기십시오. 시스템 데이터베이스만이라도 방화벽 뒤에 안전하게 있도록 합니다.
- 파일 리포지토리 서버에 암호화를 추가합니다. 시스템이 작동되어 실행 중인 경우 전용 콘텐츠가 이 서버에 저장됩니다. OS를 암호화를 추가하거나 타사 도구를 사용하십시오.
- 역방향 프록시 서버를 웹 응용 프로그램 서버 앞에 배포하여 웹 응용 프로그램 서버를 단일 IP 주소 뒤에 감춥니다. 이 구성의 경우 비공개 웹 응용 프로그램 서버로 보내야 할 모든 인터넷 트래픽을 역방향 프록시 서버를 통해 라우팅하여 개인 IP 주소를 숨깁니다.
- 회사 암호 정책을 엄격하게 적용합니다. 사용자 암호를 정기적으로 변경하도록 하십시오.
- BI 플랫폼에서 제공하는 시스템 데이터베이스 및 웹 응용 프로그램 서버를 설치하려는 경우, 관련 설명서를 참조하여 이러한 구성 요소가 적절한 보안 구성으로 배포되도록 합니다.
- 배포 환경에서 클라이언트와 서버 간의 모든 네트워크 통신에 SSL(Secure Sockets Layer) 프로토콜을 사용합니다.
- 중앙 관리 콘솔(CMC)에 대한 액세스는 로컬 액세스로만 제한해야 합니다. CMC 배포 옵션에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 웹 응용 프로그램 배포 가이드를 참조하십시오.

관련 항목

- 172 페이지에서 [BI 플랫폼 구성 요소 간 통신을 위한 요구 사항](#)

- 198 페이지에서 [BI 플랫폼 및 역방향 프록시 서버 "](#)
- 164 페이지에서 [SSL 프로토콜 구성"](#)
- 148 페이지에서 [암호 제한"](#)
- 143 페이지에서 [번들 타사 서버에 대한 보안 구성"](#)

6.4 번들 타사 서버에 대한 보안 구성

BI 플랫폼과 함께 제공되는 타사 서버 구성 요소를 설치하려는 경우, 다음 번들 구성 요소에 대한 설명서를 검토하는 것이 좋습니다.

- Microsoft SQL Server 2008 Express Edition: Windows 플랫폼에서 이 시스템 데이터베이스의 보안을 유지하는 방법에 대한 자세한 내용은 <http://msdn.microsoft.com/en-us/library/bb283235%28v=sql.100%29.aspx>를 참조하십시오.
- IBM DB2 Express: UNIX 플랫폼에서 이 시스템 데이터베이스의 보안을 유지하는 방법에 대한 자세한 내용은 http://publib.boulder.ibm.com/infocenter/db2luw/v9r7/index.jsp?nav=/2_를 참조하십시오.
- Apache Tomcat 6.0: 이 웹 응용 프로그램 서버 보안에 대한 자세한 내용은 <http://tomcat.apache.org/tomcat-6.0-doc/index.html>을 참조하십시오.

6.5 활성 신뢰 관계

네트워크로 연결된 환경에서 두 도메인 사이의 신뢰 관계는 일반적으로 한 도메인에서 인증된 사용자를 다른 도메인에서 정확하게 식별할 수 있도록 하는 관계입니다. 신뢰 관계를 사용하면 보안을 유지한 채 사용자가 자격 증명을 매번 입력하지 않고도 여러 도메인의 리소스에 액세스할 수 있습니다.

BI 플랫폼 환경에서 활성 신뢰 관계는 각 사용자가 시스템 간의 리소스에 일관되게 액세스할 수 있도록 유사한 방식으로 작동합니다. 사용자가 인증되고 활성 세션이 부여되면 다른 모든 BI 플랫폼 구성 요소에서는 자격 증명을 다시 요구하지 않은 채 사용자의 요청과 작업을 처리할 수 있습니다. 이와 같이 활성 신뢰 관계는 BI 플랫폼의 분산형 보안에 대한 기반을 형성합니다.

6.5.1 로그인 토큰

로그온 토큰은 고유의 사용법 특성을 정의하고 사용자의 세션 정보가 포함되어 있는 인코딩된 문자열입니다. 로그온 토큰의 사용법 특성은 로그온 토큰을 생성할 때 지정합니다. 이러한 특성을 사용하면 로그온 토큰에 제한 사항을 적용하여 악의적인 사용자가 로그온 토큰을 사용할 수 있는 가능성을 줄일 수 있습니다. 현재 로그온 토큰의 사용 특성은 다음과 같습니다.

- 분 수

이 특성은 로그온 토큰의 수명을 제한합니다.

- 로그온 수

이 특성은 BI 플랫폼에 로그인하는 데 로그온 토큰을 사용할 수 있는 횟수를 제한합니다.

이러한 두 특성은 악의적인 사용자가 정식 사용자에게서 가로챈 로그온 토큰을 사용하여 BI 플랫폼에 무단으로 액세스하지 못하도록 합니다.

참고:

공용 네트워크로 연결하고 연결에 SSL 또는 신뢰할 수 있는 인증을 사용하지 않는 경우처럼 브라우저와 응용 프로그램 또는 웹 서버 간 네트워크가 보안되지 않은 경우 쿠키에 로그온 토큰을 저장하면 잠재적인 보안 위험이 있을 수 있습니다. 브라우저와 응용 프로그램 또는 웹 서버 간 보안 위험을 줄일 수 있도록 SSL(Secure Sockets Layer)을 사용하는 것이 좋습니다.

로그온 쿠키를 비활성화한 경우 웹 서버나 웹 브라우저의 제한 시간이 경과하면 사용자에게 로그온 화면이 표시됩니다. 이 쿠키를 활성화한 경우에는 서버나 브라우저의 제한 시간이 경과하더라도 사용자가 시스템에 자동으로 다시 로그인됩니다. 그러나 상태 정보가 웹 세션에 묶여 있으므로 사용자의 상태가 손실됩니다. 예를 들어 사용자가 탐색 트리를 확장하고 특정 항목을 선택했다라도 트리가 원래대로 돌아갑니다.

BI 플랫폼의 경우 기본값은 웹 클라이언트에서 로그온 토큰을 활성화하는 것이지만 BI 실행 패드에 대해 로그온 토큰을 비활성화할 수 있습니다. 클라이언트에서 로그온 토큰을 비활성화하면 사용자 세션이 웹 서버나 웹 브라우저 제한 시간에 의해 제한됩니다. 해당 세션이 만료되면 사용자가 BI 플랫폼에 다시 로그인해야 합니다.

6.5.2 분산 보안의 티켓 메커니즘

많은 사용자를 지원해야 하는 엔터프라이즈 시스템에는 일반적으로 분산 보안이 필요합니다. 엔터프라이즈 시스템은 신뢰 전송(사용자 대신 다른 구성 요소가 작동하도록 만드는 기능) 같은 기능을 지원하기 위해 분산 보안을 필요로 할 수 있습니다.

BI 플랫폼은 Kerberos 티켓 메커니즘과 비슷한 티켓 메커니즘을 구현하여 분산형 보안을 처리합니다. CMS는 특정 사용자 대신 작업을 수행하도록 구성 요소에 권한을 부여하는 티켓을 허용합니다. BI 플랫폼에서는 이 티켓을 로그온 토큰이라고 합니다.

로그온 토큰은 웹에서 가장 일반적으로 사용됩니다. BI 플랫폼에서 사용자를 먼저 인증하면 사용자는 CMS에서 로그인 토큰을 받습니다. 사용자의 웹 브라우저에서는 이 로그인 토큰을 캐시합니다. 사용자가 새로운 요청을 보낼 때 다른 BI 플랫폼 구성 요소가 사용자의 웹 브라우저에서 로그인 토큰을 읽을 수 있습니다.

6.6 세션 및 세션 추적

일반적으로 세션은 두 컴퓨터 사이에 정보를 교환할 수 있게 하는 클라이언트-서버 연결입니다. 세션의 상태는 세션의 특성, 구성 또는 내용을 설명하는 데이터의 집합입니다. 웹에서 클라이언트-서버 연결을 설정하면 HTTP의 기본 특성에 따라 각 세션의 지속 기간이 한 페이지 분량의 정보로 제한됩니다. 따라서 사용자의 웹 브라우저에는 웹 페이지 하나가 표시되는 동안에만 각 세션의 상태가 메모리에 유지됩니다. 한 웹 페이지에서 다른 웹 페이지로 이동하면 첫 번째 세션의 상태가 삭제되고 다음 세션의 상태로 바뀝니다. 따라서 웹 사이트와 웹 응용 프로그램에서는 한 세션의 정보를 다른 세션에서 다시 사용해야 하는 경우 세션 상태를 별도로 저장해야 합니다.

BI 플랫폼은 다음과 같은 두 가지 일반적인 방법을 사용하여 세션 상태를 저장합니다.

- 쿠키 - 쿠키는 클라이언트 쪽에서 세션 상태를 저장하는 작은 텍스트 파일입니다. 사용자의 웹 브라우저에서는 나중에 사용할 수 있도록 쿠키를 캐시합니다. BI 플랫폼 로그인 토큰은 이러한 방법 중 하나입니다.
- 세션 변수 - 세션 변수는 서버 쪽에서 세션 상태를 저장하는 메모리의 일부입니다. BI 플랫폼이 시스템에서 활성 ID를 사용자에게 부여할 때 사용자의 인증 형식 같은 정보가 세션 변수에 저장됩니다. 세션이 유지되는 동안에는 시스템에서 이 정보를 입력하라는 메시지를 사용자에게 다시 표시하거나 다음 요청을 완료하는 데 필요한 어떠한 작업도 반복할 필요가 없습니다.

Java 배포에서는 세션이 .jsp 요청을 처리하는 데 사용되고 .NET 배포에서는 세션이 .aspx 요청을 처리하는 데 사용됩니다.

참고:

이상적으로는 사용자가 시스템에서 활성 상태인 동안 세션 변수가 시스템에 유지되어야 합니다. 또한 보안을 강화하고 리소스 사용을 최소화하기 위해 사용자가 시스템에서 작업을 마치는 즉시 세션 변수가 삭제되어야 합니다. 그러나 웹 브라우저와 웹 서버 사이의 상호 작용은 상태 비저장 환경에서 이루어질 수 있으므로 사용자가 명시적으로 로그오프하지 않는 경우 사용자가 시스템에서 나간 시점을 파악하기 힘들 수 있습니다. 이 문제를 해결하기 위해 BI 플랫폼에서는 세션 추적을 구현합니다.

6.6.1 CMS 세션 추적

CMS는 간단한 추적 알고리즘을 구현합니다. 사용자가 로그인하면 CMS 세션이 부여됩니다. 이 세션은 사용자가 로그오프하거나 웹 응용 프로그램 서버 세션 변수가 해제될 때까지 유지됩니다.

웹 응용 프로그램 서버 세션은 해당 세션이 활성 상태임을 CMS에 반복하여 통보하도록 디자인되어 있으므로 웹 응용 프로그램 서버 세션이 유지되는 동안 CMS 세션도 함께 유지됩니다. 웹 응용 프로그램 서버 세션이 10분 동안 CMS와 통신하지 못하면 CMS에서 CMS 세션이 해제됩니다. 이렇게 하면 클라이언트 쪽 구성 요소가 비정기적으로 중지되는 경우를 처리할 수 있습니다.

6.7 환경 보호

환경 보호란 클라이언트와 서버 구성 요소가 통신하는 전체 환경에 대한 보안을 의미합니다. 인터넷과 웹 기반 시스템은 그 융통성과 다양한 기능 덕분에 더욱 널리 사용되고 있는 추세이지만 그 운영 환경의 보안 문제는 해결하기가 쉽지 않습니다. BI 플랫폼을 배포하는 경우 환경 보호는 두 가지 통신 영역으로 나누어 생각해 볼 수 있습니다.

6.7.1 웹 브라우저에서 웹 서버로

웹 브라우저와 웹 서버 사이에 데이터를 전달하는 경우에는 일반적으로 일정한 수준의 보안이 필요합니다. 이를 위한 보안 조치에는 대개 두 가지 일반적인 작업이 포함됩니다.

- 데이터 통신이 보호되고 있는지 확인
- 유효한 사용자만 웹 서버에서 정보를 검색할 수 있는지 확인

참고:

일반적으로 이러한 작업은 SSL(Secure Sockets Layer) 프로토콜 및 기타 관련 메커니즘을 비롯한 여러 가지 보안 메커니즘을 통해 웹 서버에서 처리됩니다. 브라우저와 응용 프로그램 또는 웹 서버 간 보안 위험을 줄일 수 있도록 SSL(Secure Sockets Layer)을 사용하는 것이 좋습니다.

웹 브라우저와 웹 서버 간의 통신에는 BI 플랫폼과는 별도로 보안을 적용해야 합니다. 클라이언트 연결을 보호하는 방법에 대한 자세한 내용은 웹 서버 설명서를 참조하십시오.

6.7.2 웹 서버와 BI 플랫폼 간 통신

방화벽은 일반적으로 웹 서버와 나머지 회사 인트라넷(BI 플랫폼 포함) 간 통신 영역을 보호하는 데 사용됩니다. 이 플랫폼은 IP 필터링 또는 정적 네트워크 주소 변환(NAT)을 지원합니다. 지원되는 환경에는 여러 개의 방화벽, 웹 서버 또는 응용 프로그램 서버가 포함될 수 있습니다.

6.8 보안 구성 수정 사항 감사

다음에 대한 기본 보안 구성 변경 사항은 BI 플랫폼에서 감사되지 않습니다.

- 웹 응용 프로그램에 대한 속성 파일(BOE, 웹 서비스)
- TrustedPrincipal.conf
- BI 실행 패드 및 Open Document에서 수행되는 사용자 지정

일반적으로 CMC 외부에서 수행되는 보안 구성 수정 사항은 감사되지 않습니다. 중앙 구성 관리자(CCM)를 통해 수정된 사항도 감사되지 않습니다. CMC를 통해 커밋된 변경 사항은 감사할 수 있습니다.

6.9 웹 작업 감사

BI 플랫폼에서는 웹 작업을 기록하고 사용자가 그 세부 내용을 조사하거나 모니터링할 수 있도록 하여 시스템에 대한 상세한 정보를 제공합니다. 웹 응용 프로그램 서버에서는 기록하려는 시간, 날짜, IP 주소, 포트 번호 등의 웹 특성을 선택할 수 있습니다. 감사 데이터는 디스크에 기록되고 쉼표로 구분된 텍스트 파일에 저장되므로 보고서의 데이터를 추출하거나 다른 응용 프로그램으로 가져오는 작업을 쉽게 수행할 수 있습니다.

6.9.1 불법 로그인 시도 방지

보안 시스템이 아무리 잘 구축되어 있더라도 하나 이상의 공격 취약점이 존재하기 마련입니다. 사용자가 시스템에 접속하는 지점이 바로 여기에 해당합니다. 이러한 지점을 완벽하게 보호하기는 거의 불가능합니다. 유효한 사용자 이름과 암호를 단순히 추측하는 것만으로도 시스템을 "해킹"할 수 있기 때문입니다.

BI 플랫폼에서는 악의적인 사용자가 시스템에 대한 액세스 권한을 얻을 가능성을 낮추는 여러 가지 기술을 구현합니다. 아래에 나열된 다양한 제한 사항은 Enterprise 계정에만 적용됩니다. 즉 LDAP 또는 Windows AD와 같은 외부 사용자 데이터베이스에 매핑된 계정에는 적용되지 않습니다. 그러나 외부 시스템을 사용하는 경우 일반적으로 이와 비슷한 제한을 외부 계정에 적용할 수 있습니다.

6.9.2 암호 제한

암호 제한으로 인해 기본 Enterprise 인증을 인증하는 사용자는 상대적으로 복잡한 암호를 만들 수 있습니다. 사용할 수 있는 옵션은 다음과 같습니다.

- 암호에 대/소문자를 혼용해야 함

이 옵션을 적용하면 대문자, 소문자, 숫자 또는 문장 부호 중 적어도 두 가지 이상을 암호에 포함시켜야 합니다.

- N개 이상의 문자를 포함해야 함

암호의 복잡한 정도를 설정할 때 그 최소 수준을 강화하면 악의적인 사용자가 유효한 사용자 암호를 쉽게 추측하지 못하도록 할 수 있습니다.

6.9.3 로그인 제한

로그인 제한은 주로 사전 공격(dictionary attack)을 방어하는 데 사용됩니다. 사전 공격은 악의적인 사용자가 유효한 사용자 이름을 획득하고 사전의 모든 단어를 시도하여 암호를 알아내는 방법입니다. 하드웨어의 속도가 향상됨에 따라 해킹 프로그램을 사용하여 분 당 수백만 개의 암호를 시도할 수 있습니다. 사전 공격을 방지하기 위해 BI 플랫폼에서는 각 로그인 시도 간에 0.5-1.0초의 지연 시간을 적용하는 내부 메커니즘을 사용합니다. 또한 플랫폼에서 제공하는 사용자 지정 가능한 여러 가지 옵션을 통해 사전 공격의 위험을 줄일 수 있습니다.

- 로그인에 N번 실패하면 계정을 사용할 수 없음

- 실패한 로그인 횟수를 N분 후에 재설정
- N분 후에 계정을 다시 사용할 수 있음

6.9.4 사용자 제한

사용자 제한으로 인해 기본 Enterprise 인증을 인증하는 사용자는 일반적인 기준에 따라 새 암호를 만들 수 있습니다. 사용할 수 있는 옵션은 다음과 같습니다.

- N일마다 암호를 변경해야 함
- 최근 N개의 암호는 다시 사용할 수 없음
- 암호를 변경하려면 N분을 기다려야 함

이러한 옵션은 여러 가지 방식으로 유용하게 사용할 수 있습니다. 먼저, 사전 공격을 시도하는 악의적인 사용자는 매번 암호를 다시 변경하여 공격을 시작해야 합니다. 또한, 사용자가 처음 로그인할 때마다 암호가 변경되므로 악의적인 사용자는 특정 암호가 변경되는 시기를 쉽게 확인할 수 없습니다. 뿐만 아니라, 악의적인 사용자가 다른 사용자의 자격 증명을 알아내거나 기타 다른 방식으로 획득한 경우에도 이러한 자격 증명은 제한된 시간 동안만 유효합니다.

6.9.5 Guest 계정 제한

BI 플랫폼은 Guest 계정에 대해 익명의 단일 로그인을 지원합니다. 따라서 사용자 이름과 암호를 지정하지 않고 BI 플랫폼에 연결하면 시스템에서 사용자가 자동으로 Guest 계정으로 로그인됩니다. Guest 계정에 암호를 할당하거나 Guest 계정을 완전히 비활성화하면 이러한 기본 동작이 수행되지 않습니다.

6.10 처리 확장

BI 플랫폼에서는 보고서 작성 환경을 더욱 안전하게 보호하기 위해 사용자 지정된 처리 확장을 사용할 수 있습니다. 처리 확장은 특정한 BI 플랫폼 보기 또는 일정 요청을 시스템에서 처리하기 전에 이러한 요청에 사용자의 비즈니스 논리를 적용하는 동적으로 로드되는 코드 라이브러리입니다.

처리 확장에 대한 지원을 통해 BI 플랫폼 관리 SDK는 근본적으로 개발자가 요청을 가로챌 수 있도록 하는 "핸들"을 노출합니다. 개발자는 보고서를 처리하기 전에 요청에 선택 수식을 첨부할 수 있습니다.

행 수준 보안을 적용하는 보고서 처리 확장을 일반적인 경우의 예로 들 수 있습니다. 이 유형의 보안은 하나 이상의 데이터베이스 테이블에서 행을 기준으로 데이터 액세스를 제한합니다. 개발자는 작업 서버, 처리 서버 또는 Report Application Server를 통해 요청을 처리하기 전에 보고서에 대한 보기 또는 예약 요청을 가로채는 동적으로 로드되는 라이브러리를 작성합니다. 개발자의 코드는 먼저 처리하려는 작업을 소유한 사용자를 확인한 다음 타사 시스템에서 사용자의 데이터 액세스 권한을 조회합니다. 그런 다음 코드는 데이터베이스에서 반환되는 데이터를 제한하기 위해 레코드 선택 수식을 생성하고 이를 보고서에 첨부합니다. 이 경우 처리 확장은 사용자 지정된 행 수준 보안을 BI 플랫폼 환경에 통합하기 위한 수단으로 사용됩니다.

팁:

처리 확장을 활성화하여 적절한 BI 플랫폼 서버 구성 요소에서 처리 확장을 런타임에 동적으로 로드하도록 구성합니다. SDK에는 개발자가 처리 확장을 작성하는 데 사용할 수 있는 API가 자세한 설명과 함께 포함되어 있습니다. 자세한 내용은 제품 배포에 들어 있는 개발자 설명서를 참조하십시오.

6.11 BI 플랫폼의 데이터 보안 개요

BI 플랫폼 시스템의 관리자는 다음을 사용하여 기밀 데이터 보안 방식을 관리합니다.

- CMS에 대한 응용 프로그램과 클라이언트의 액세스권한을 결정하는 클러스터 수준의 보안 설정. 이 설정은 중앙 구성 관리자를 통해 관리가 이루어집니다.
- CMS 리포지토리에 대한 액세스 권한 및 리포지토리 내에서 개체를 암호화/암호 해독하는데 사용되는 키를 제어하는 이중 키 암호화 시스템. CMS 리포지토리로의 액세스 권한은 중앙 구성 관리자를 통해 설정되며, 중앙 관리 콘솔에는 암호화 키를 위한 전용 관리 영역이 있습니다.

관리자는 이 기능을 통해 BI 플랫폼 배포를 특정 데이터 보안 준수 수준으로 설정하고 CMS 리포지토리 내에서 데이터 암호화 및 암호 해독에 사용되는 암호화 키를 관리할 수 있습니다.

6.11.1 데이터 처리 보안 모드

BI 플랫폼은 두 가지 데이터 처리 보안 모드에서 작동이 가능합니다.

- 기본 데이터 처리 보안 모드. 일부의 경우, 이 모드에서 실행되는 시스템은 하드코딩된 암호화 키를 사용하며 특정 표준을 준수하지 않습니다. 기본 모드는 이전 버전의 BI 플랫폼 클라이언트 도구 및 응용 프로그램과 호환이 가능합니다.
- FIPS(Federal Information Processing Standard), 특히 FIPS 140-2에서 규정한 지침을 충족하기 위해 디자인된 데이터 보안 모드. 이 모드에서는 FIPS 호환 알고리즘 및 암호화 모듈을 사용하여 기밀 데이터를 보호합니다. 플랫폼이 FIPS 호환 모드에서 실행되면 FIPS 지침을 충족하지 않는 모든 클라이언트 도구 및 응용 프로그램은 자동으로 비활성화됩니다. 플랫폼 클라이언트 도구 및 응용 프로그램은 FIPS 2 표준을 준수하도록 설계되었습니다. SAP BusinessObjects Business Intelligence 플랫폼 4.0이 FIPS 호환 모드에서 실행되면 이전 버전의 클라이언트와 응용 프로그램은 작동하지 않습니다.

데이터 처리 모드는 시스템 사용자에게 명시적으로 표시됩니다. 두 가지 데이터 처리 보안 모드에서 기밀 데이터는 내부 암호화 엔진에서 백그라운드로 암호화 및 해독됩니다.

다음 환경에서 FIPS 호환 모드를 사용하는 것이 좋습니다.

- SAP BusinessObjects Business Intelligence 플랫폼 4.0 배포가 다른 레거시 BI 플랫폼 클라이언트 도구 또는 응용 프로그램을 사용하거나 상호 작용할 필요가 없을 경우.
- 조직의 데이터 처리 표준 및 지침이 하드코딩된 암호화 키의 사용을 금지하는 경우.
- 조직에서 FIPS 140-2 규정에 따라 기밀 데이터를 보호해야 하는 경우.

데이터 처리 보안 모드는 Windows와 UNIX 모두에서 중앙 구성 관리자를 통해 설정합니다. 클러스터 환경의 모든 노드는 동일한 모드로 설정해야 합니다.

6.11.1.1 Windows에서 FIPS 호환 모드 설정

BI 플랫폼 설치 시 기본적으로 FIPS 호환 모드가 해제되어 있습니다. 아래 지침을 사용하여 배포의 모든 노드에 FIPS 호환 모드를 설정하십시오.

1. CCM을 시작하려면 프로그램 > SAP BusinessObjects Enterprise XI 4.0 > SAP BusinessObjects Enterprise > 중앙 구성 관리자를 선택합니다.
2. CCM에서 Server Intelligence Agent를 마우스 오른쪽 단추로 클릭하고 중지를 선택합니다.

주의:

SIA 상태가 중지됨으로 표시된 다음 3단계를 진행합니다.

3. SIA를 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.
속성 대화 상자가 열리고 속성 탭이 표시됩니다.
4. 명령 필드에 -fips를 추가하고 적용을 클릭합니다.
5. 확인을 클릭하여 속성 대화 상자를 닫습니다.
6. SIA를 다시 시작합니다.

SIA가 FIPS 호환 모드에서 작동합니다.

BI 플랫폼 배포의 모든 SIA에서 FIPS 호환 모드를 설정해야 합니다.

6.11.1.2 UNIX에서 FIPS 호환 모드 설정

다음 절차를 실행하기 전에 BI 플랫폼 배포 환경의 모든 노드를 중지해야 합니다.

BI 플랫폼 설치 시 기본적으로 FIPS 호환 모드가 해제되어 있습니다. 아래 지침을 사용하여 배포의 모든 노드에 FIPS 호환 모드를 설정하십시오.

1. UNIX 컴퓨터에서 BI 플랫폼이 설치된 디렉터리로 이동합니다.
2. sap_bobj 디렉터리로 변경합니다.
3. ccm.config를 입력하고Enter 키를 누릅니다.
ccm.config파일이 로드됩니다.
4. -fips를 노드 실행 명령 매개 변수에 추가합니다.
노드 실행 명령 매개 변수가 [node nameLaunch]로 표시됩니다.
5. 변경 사항을 저장하고 종료합니다.
6. 노드를 다시 시작합니다.

노드가 FIPS 호환 모드에서 작동합니다.

BI 플랫폼 배포 환경의 모든 노드에서 FIPS 호환 모드를 설정해야 합니다.

6.11.1.3 Windows에서 FIPS 호환 모드 해제

다음 절차를 실행하기 전에 BI 플랫폼 배포의 모든 서버를 중지해야 합니다.

배포가 FIPS 호환 모드에서 실행 중인 경우 다음 지침을 사용하여 설정을 해제하십시오.

1. CCM에서 Server Intelligence Agent를 마우스 오른쪽 단추로 클릭하고 중지를 선택합니다.

주의:

노드 상태가 중지됨으로 표시되면 2단계로 진행합니다.

2. SIA를 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.
속성 대화 상자가 열리고 속성 탭이 표시됩니다.
3. 명령 필드에서 -fips를 제거하고 적용을 클릭합니다.
4. 확인을 클릭하여 속성 대화 상자를 닫습니다.
5. SIA를 다시 시작합니다.

6.12 BI 플랫폼의 암호화 방식

기밀 데이터

BI 플랫폼 암호화 방식은 CMS 리포지토리에 저장된 기밀 데이터를 보호하도록 설계되었습니다. 기밀 데이터에는 사용자 자격 증명, 데이터 소스 연결 데이터 및 암호를 저장한 기타 정보 개체가 포함됩니다. 이 데이터는 개인 정보가 손상되지 않도록 보호하고 액세스 제어를 관리할 수 있도록 암호화됩니다. 모든 필수 암호화 리소스(암호화 엔진, RSA 라이브러리 포함)는 기본적으로 각각의 BI 플랫폼 배포 환경에 설치됩니다.

BI 플랫폼 시스템에서는 다음과 같은 두 가지 키 암호화 체계가 사용됩니다.

암호화 키

기밀 데이터의 암호화 및 암호 해독은 내부 암호화 엔진과 상호 작용하는 SDK를 통해 백그라운드에서 처리됩니다. 시스템 관리자는 특정 데이터 블록을 직접 암호화 또는 암호 해독하지 않고 대칭 암호화 키를 통해 데이터를 관리합니다.

BI 플랫폼에서는 암호화 키로 알려져 있는 대칭 암호 키를 사용하여 기밀 데이터를 암호화/암호 해독합니다. 중앙 관리 콘솔에는 암호화 키를 위한 전용 관리 영역이 있습니다. 암호화 키(Cryptographic Keys)를 사용하여 키를 보고, 생성하고, 비활성화하고, 해지하고, 삭제할 수 있습니다. 시스템에서는 기밀 데이터의 암호를 해독하는데 필요한 데이터가 삭제되지 않도록 합니다.

클러스터 키

클러스터 키는 CMS 리포지토리에 저장된 암호화 키를 보호하는 대칭 키 래핑 키입니다. 클러스터 키는 대칭 키 알고리즘을 사용하여 CMS 리포지토리에 대한 액세스 제어의 수준을 유지 관리합니다. BI 플랫폼의 각 노드는 설치 설정 단계에서 클러스터 키를 할당 받습니다. 시스템 관리자는 CCM에서 클러스터 키를 재설정할 수 있습니다.

6.12.1 클러스터 키를 사용한 작업

BI 플랫폼을 설치하는 과정에서 Server Intelligence Agent용 클러스터 키가 8자로 생성됩니다. 이 키는 CMS 리포지토리에서 모든 암호화 키를 암호화하는데 사용됩니다. 올바른 클러스터 키가 없으면 CMS에 액세스할 수 없습니다. 클러스터 키는 dbinfo 파일에 암호화된 형식으로 저장됩니다. 기본 Windows 설치에서는 파일이 C:\Program Files (x86)\WSAP BusinessObjects\WSAP BusinessObjects Enterprise XI 4.0\win64_x64 디렉터리에 저장됩니다. Unix 시스템에서는 파일이 <INSTALLDIR>/sap_bobj/enterprise_xi40/의 플랫폼 디렉터리에 저장됩니다.

Unix 플랫폼	경로
AIX	<INSTALLDIR>/sap_bobj/enterprise_xi40/ aix_rs6000/
Solaris	<INSTALLDIR>/sap_bobj/enterprise_xi40/ solaris_sparc/
Linux	<INSTALLDIR>/sap_bobj/enterprise_xi40/ linux_x86/
HP_UX	<INSTALLDIR>/sap_bobj/enterprise_xi40/ hpux_pa-risc/

파일 이름을 정하는 규칙은 _boe_<sia_name>.dbinfo와 같은 형식에 따르며, 여기서 <sia_name>은 클러스터에 대한 서버 인텔리전스 에이전트의 이름입니다.

참고:

제공된 노드의 클러스터 키는 dbinfo 파일에서 검색할 수 없습니다. 시스템 관리자는 신중하고 주의를 기울여 클러스터 키를 보호하는 것이 좋습니다.

관리 권한이 있는 사용자만 클러스터 키를 재설정할 수 있습니다. 필요 시 CCM을 사용하여 배포한 모든 노드의 8자 클러스터 키를 재설정하십시오. 새 클러스터키가 자동으로 CMS 리포지토리 내의 암호화 키를 보호하기 위해 사용됩니다.

6.12.1.1 Windows에서 클러스터 키 재설정

클러스터 키를 재설정하기 전에 Server Intelligence Agent에서 관리하는 모든 서버를 중지해야 합니다.

다음의 절차에 따라 노드에 대한 클러스터 키를 재설정합니다.

1. CCM을 시작하려면 프로그램 > SAP BusinessObjects Enterprise XI 4.0 > SAP BusinessObjects Enterprise > 중앙 구성 관리자를 선택합니다.
2. CCM에서 Server Intelligence Agent(SIA)를 마우스 오른쪽 단추로 클릭하고 중지를 선택합니다.

주의:

SIA 상태가중지됨으로 표시된 다음 3단계를 진행합니다.

3. Server Intelligence Agent(SIA)를 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.
속성 대화 상자가 열립니다.
4. 구성 탭을 클릭합니다.
5. CMS 시스템 데이터베이스 구성에서 변경을 클릭합니다.
경고 메시지가 표시됩니다.
6. 계속하려면 예를 클릭합니다.
클러스터 키 변경 대화 상자가 열립니다.
7. 새 클러스터 키와 새 클러스터 키 확인 필드에 동일한 8자의 클러스터 키를 입력합니다.

참고:

Windows 플랫폼의 경우 클러스터 키는 반드시 대소문자의 조합이 포함되어야 합니다. 또는 사용자가 임의의 키를 생성할 수도 있습니다. 임의의 키는 FIPS와의 호환성을 위해 필수적입니다.

8. 새 키를 시스템에 제출하려면 확인을 클릭합니다.
클러스터 키가 재설정되었다는 확인 메시지가 표시됩니다.
9. SIA를 다시 시작합니다.

다중 노드 클러스터에서는 BI 플랫폼의 모든 SIA에 대해 클러스터 키를 새 키로 재설정해야 합니다.

6.12.1.2 UNIX에서 클러스터 키 재설정

노드에 대한 클러스터 키를 재설정하기 전에 노드에서 관리하는 모든 서버를 중지해야 합니다.

1. UNIX 컴퓨터에서 BI 플랫폼이 설치된 디렉터리로 이동합니다.
2. `sap bobj` 디렉터리로 변경합니다.
3. `cmsdbsetup.sh`를 입력하고 Enter 키를 누릅니다.
CMS 데이터베이스 설정 화면이 표시됩니다.
4. 노드의 이름을 입력하고 Enter 키를 누릅니다.
5. 2를 입력해 클러스터 키를 변경합니다.
경고 메시지가 표시됩니다.
6. 계속하려면 예를 클릭합니다.
7. 제공되는 필드에서 8자의 새 클러스터 키를 입력하고 Enter 키를 누릅니다.

참고:

UNIX 플랫폼에서는 제한 없이 8자의 모든 조합이 클러스터 키로 유효합니다.

8. 나타나는 필드에 새 클러스터 키를 다시 입력한 다음 Enter 키를 누릅니다.
클러스터 키가 재설정 되었음을 알리는 메시지가 표시됩니다.
9. 노드를 다시 시작합니다.

같은 클러스터 키를 사용하려면 BI 플랫폼 배포의 모든 노드를 재설정해야 합니다.

6.12.2 암호화 담당자

CMC에서 암호화 키를 관리하려면 암호화 담당자 그룹의 멤버여야 합니다. BI 플랫폼의 기본 관리자 계정도 암호화 담당자 그룹의 멤버입니다. 필요 시 이 계정을 사용하여 사용자를 암호화 담당자 그룹에 추가하십시오. 이 그룹의 구성원은 제한된 수의 사용자로 제한하는 것이 좋습니다.

참고:

사용자가 Administrators 그룹에 추가되면 암호화 키에 관한 관리 작업을 수행하기 위한 필수 권한을 상속하지 않습니다.

6.12.2.1 암호화 담당자 그룹에 사용자 추가

BI 플랫폼에 사용자 계정이 있어야 암호화 담당자 그룹에 해당 사용자를 추가할 수 있습니다.

참고:

사용자를 암호화 담당자 그룹에 추가하려면 Administrators 그룹과 암호화 담당자 그룹 모두의 멤버여야 합니다.

1. CMC의 사용자 및 그룹 관리 영역에서 암호화 담당자 그룹을 선택합니다.
2. 작업 > 그룹에 구성원 추가를 클릭합니다.
추가 대화 상자가 열립니다.
3. 사용자 목록을 클릭합니다.
사용 가능한 사용자/그룹 목록이 새로 고쳐지고 시스템의 모든 사용자 계정이 표시됩니다.
4. 암호화 담당자 그룹에 추가하려는 사용자 계정을 사용 가능한 사용자/그룹 목록에서 선택한 사용자/그룹 목록으로 이동합니다.

팁:

특정 사용자를 검색하려면 검색 필드를 사용합니다.

5. 확인을 클릭합니다.

암호화 담당자 그룹의 멤버로 새로 추가된 계정은 CMC의 암호화 키 관리 영역에 대한 액세스 권한이 부여됩니다.

6.12.2.2 CMC에서 암호화 키 보기

CMC 응용 프로그램에는 BI 플랫폼 시스템에서 사용하는 암호화 키 전용 관리 영역이 있습니다. 이 영역에는 암호화 담당자 그룹의 멤버만 액세스할 수 있습니다.

1. CMC를 시작하려면 프로그램 > SAP BusinessObjects XI 4.0 > SAP BusinessObjects Enterprise > SAP BusinessObjects Enterprise 중앙 관리 콘솔로 이동합니다.
CMC 홈 페이지가 열립니다.
2. 암호화 키 탭을 클릭합니다.
암호화 키 관리 영역이 표시됩니다.
3. 자세한 정보를 보려는 암호화 키를 두 번 클릭합니다.

관련 항목

- 158 페이지에서 [암호화 키와 관련된 개체 보기](#)"

6.12.3 CMC에서 암호화 키 관리

암호화 담당자는 암호화 키 관리 영역을 통해 CMS 리포지토리에 저장된 중요한 데이터를 보호할 때 사용하는 키에 대해 확인, 만들기, 비활성화, 해지 및 삭제 작업을 수행할 수 있습니다.

시스템에 현재 정의된 모든 암호화 키는 암호화 키 관리 영역에 목록으로 표시됩니다. 각 키에 대한 기본 정보는 다음 테이블에 설명된 머리글 아래 표시됩니다.

머리글	설명
제목	암호화 키의 이름 식별자
상태	키의 현재 상태
마지막 변경	암호화 키와 관련된 마지막 변경의 날짜 및 시간
개체	키와 연결된 개체 수

관련 항목

- 158 페이지에서 [암호화 키 상태 "](#)
- 159 페이지에서 [새 암호화 키 만들기"](#)
- 161 페이지에서 [시스템에서 암호화 키 삭제"](#)
- 160 페이지에서 [암호화 키 해지"](#)
- 158 페이지에서 [암호화 키와 관련된 개체 보기"](#)
- 159 페이지에서 [암호화 키를 손상됨으로 표시 "](#)

6.12.3.1 암호화 키 상태

다음 표에는 BI 플랫폼의 암호화 키에서 가능한 모든 상태 옵션이 나와 있습니다.

상태	설명
활성	시스템에서 하나의 암호화 키만 활성으로 지정될 수 있습니다. 이 키는 CMS 데이터베이스에 저장될 현재의 기밀 데이터를 암호화하는데 사용됩니다. 또한 개체 목록의 모든 개체를 암호 해독하는데도 사용됩니다. 새로운 암호화 키가 만들어지면 현재 활성인 상태가 비활성화된 상태로 되돌아갑니다. 활성 키는 시스템에서 삭제할 수 없습니다.
비활성화된	비활성화된 키는 암호화 데이터에서 더 이상 사용되지 않습니다. 그러나 개체 목록의 모든 개체를 암호 해독하는데 사용될 수 있습니다. 한 번 비활성화된 키는 다시 활성화할 수 없습니다. 비활성화된 것으로 표시된 키는 시스템에서 삭제할 수 없습니다. 삭제하려면 키의 상태를 해지된으로 변경해야 합니다.
손상됨	안전하지 않아 보이는 암호화 키는 손상된 것으로 표시할 수 있습니다. 이러한 키에 플래그를 지정하면 나중에 해당 키와 관련된 데이터 개체를 다시 암호화할 수 있습니다. 키가 일단 손상된 것으로 표시되면 상태가 해지된 후에 시스템에서 삭제할 수 있습니다.
해지	암호화 키가 해지되면 현재 해당 키와 관련된 모든 개체가 현재 "활성"인 암호화 키를 사용하여 다시 암호화되는 프로세스가 실행됩니다. 키가 해지되면 시스템에서 안전하게 삭제할 수 있습니다. 해지 메커니즘을 통해 CMS 데이터베이스의 데이터를 언제라도 해독할 수 있습니다. 한 번 해지된 키는 다시 활성화할 수 없습니다.
비활성화된: 키 다시 입력 프로세스	암호화 키가 해지 처리되는 중임을 나타냅니다. 프로세스가 완료되면 키가 해지로 표시됩니다.
비활성화된: 키 다시 입력 일시 중단됨	암호화 키를 해지하는 프로세스가 일시 중단되었음을 나타냅니다. 보통 해당 프로세스가 의도적으로 일시 중단되었거나 키와 관련된 데이터 개체를 사용할 수 없을 때 발생합니다.
해지-손상됨	손상된 것으로 표시된 키의 경우 그와 이전에 관련되었던 모든 데이터가 다른 키로 암호화 될 경우 해지-손상됨으로 플래그가 지정됩니다. 비활성화된 키가 손상된 것으로 표시되면 작업을 수행하지 않거나 키를 해지해야 합니다. 손상된 키가 해지되면 삭제할 수 있습니다.

6.12.3.2 암호화 키와 관련된 개체 보기

1. CMC의 암호화 키 관리 영역에서 키를 선택합니다.
2. 관리 > 속성을 클릭합니다.
암호화 키의 속성 대화 상자가 열립니다.
3. 속성 대화 상자 왼쪽의 탐색 창에서 개체 목록을 클릭합니다.
암호화 키와 관련된 모든 개체가 탐색 창의 오른쪽에 나열됩니다.

팁:

특정 개체를 찾으려면 검색 기능을 사용하십시오.

6.12.3.3 새 암호화 키 만들기

주의:

새 암호화 키를 만들 때 시스템에서 자동으로 현재의 활성 키를 비활성화합니다. 키를 비활성화하고 나면 이 키는 다시 활성 키로 복원할 수 없습니다.

1. CMC의 암호화 키 관리 영역에서 관리 > 새로 만들기 > 암호화 키를 클릭합니다.
새 암호화 키 만들기 대화 상자가 열리고 경고 메시지가 표시됩니다.
2. 계속을 눌러 새 암호화 키를 만듭니다.
3. 새 암호화 키의 이름과 설명을 입력하고 확인을 클릭하여 정보를 저장합니다.
암호화 키 관리 영역에 새 키가 유일한 활성 키로 목록에 표시됩니다. 이전의 활성 키는 비활성화됨으로 변해 있습니다.

CMS 데이터베이스에서 만들어지고 저장되는 중요한 새 데이터는 모두 이 새 암호화 키로 암호화됩니다. 필요한 경우 이전 키를 해지하고 새 활성 키로 이전 키의 모든 데이터 개체를 재암호화할 수 있습니다.

6.12.3.4 암호화 키를 손상됨으로 표시

암호화 키가 어떤 이유로든 더 이상 안전하지 않다고 판단되면 손상됨으로 표시할 수 있습니다. 이는 추적에 도움이 되며 이 키와 연결된 데이터 개체를 파악할 수 있습니다. 암호화 키는 손상됨으로 표시하기 전에 반드시 비활성화되어야 합니다.

참고:

키를 해지한 후에도 손상됨으로 표시할 수 있습니다.

1. CMC의 암호화 키 관리 영역으로 이동합니다.
2. 손상됨으로 표시할 암호화 키를 선택합니다.
3. 작업 > 손상됨으로 표시를 클릭합니다.
손상됨으로 표시 대화 상자에서 경고 메시지가 표시됩니다.
4. 계속을 클릭합니다.
5. 손상됨으로 표시 대화 상자에서 다음 옵션 중 하나를 선택합니다.
 - 예: 손상된 키와 연결된 모든 데이터 개체를 재암호화하는 프로세스를 시작합니다.
 - 아니요: 손상됨으로 표시 대화 상자가 닫히고 암호화 키 관리 영역에서 암호화 키가 손상됨으로 표시됩니다.

참고:

아니요를 선택하면 중요한 데이터와 손상된 키 간의 연결 상태를 계속 유지하며 연결된 개체의 암호 해독을 위해 손상된 키가 사용됩니다.

관련 항목

- 160 페이지에서 [암호화 키 해지](#)"
- 158 페이지에서 [암호화 키 상태](#) "
- 158 페이지에서 [암호화 키와 관련된 개체 보기](#)"

6.12.3.5 암호화 키 해지

비활성화된 상태인 암호화 키에 연결된 데이터 개체는 여전히 이 키를 사용할 수 있습니다. 암호화된 개체와 비활성화된 키의 연결을 끊기 위해서는 다음 절차에 따라 키를 해지해야 합니다.

1. 암호화 키 관리 영역에 표시된 키 목록에서 해지할 키를 선택합니다.
2. 작업 > 키 해지를 클릭합니다.
키 해지 대화 상자가 열리고 경고 메시지가 표시됩니다.
3. 확인을 클릭하여 암호화 키를 해지합니다.
이 키에 연결되었던 모든 개체를 현재 활성 키로 암호화하는 프로세스가 시작됩니다. 연결된 데이터 개체가 너무 많은 경우에는 재암호화 과정이 완료될 때까지 비활성화된: 키 다시 지정 진행 중으로 표시됩니다.

암호화 키를 해지하고 나면 암호 해독에 이 키를 필요로 하는 중요한 데이터 개체는 없으므로 시스템에서 키를 안전하게 제거할 수 있습니다.

6.12.3.6 시스템에서 암호화 키 삭제

BI 플랫폼에서 암호화 키를 삭제하려면 먼저 해당 키를 필요로 하는 데이터가 시스템에 없어야 합니다. 이는 CMS 리포지토리에 저장된 모든 중요 데이터를 언제든지 해독할 수 있도록 보장하기 위한 제한입니다.

암호화 키를 해지한 후에는 다음과 같이 시스템에서 키를 삭제하십시오.

1. CMC의 암호화 키 관리 영역으로 이동합니다.
2. 삭제할 암호화 키를 선택합니다.
3. 관리 > 삭제를 클릭합니다.
키 삭제 대화 상자에서 경고 메시지가 표시됩니다.
4. 삭제를 클릭하여 시스템에서 암호화 키를 제거합니다.
삭제한 키는 이제 CMC의 암호화 키 관리 영역에 표시되지 않습니다.

참고:

암호화 키를 시스템에서 삭제하고 나면 이를 복원할 수 없습니다.

관련 항목

- 160 페이지에서 [암호화 키 해지](#)
- 158 페이지에서 [암호화 키 상태](#)

6.13 SSL에 대해 서버 구성

BI 플랫폼 배포 환경에서 클라이언트와 서버 사이의 모든 네트워크 통신에 SSL(Secure Sockets Layer) 프로토콜을 사용할 수 있습니다.

모든 서버 통신에 대한 SSL을 설정하려면 다음 단계를 수행해야 합니다.

- SSL을 활성화하여 BI 플랫폼을 배포합니다.
- 배포 환경의 각 컴퓨터에 대한 키와 인증서 파일을 만듭니다.

- 웹 응용 프로그램 서버와 CCM(Central Configuration Manager)에서 이러한 파일의 위치를 구성합니다.

참고:

Crystal Reports 또는 디자이너와 같은 짙(thick) 클라이언트를 사용하고 있는 경우 이러한 짙(thick) 클라이언트에서 CMS에 연결하려면 해당 클라이언트를 SSL로 구성해야 합니다. 그렇지 않으면 SSL로 구성된 CMS를 같은 방식으로 구성되지 않은 짙(thick) 클라이언트에서 연결할 때 오류가 발생하게 됩니다.

6.13.1 키 및 인증서 파일 만들기

서버 통신을 위한 SSL 프로토콜을 설정하려면 SSLC 명령줄 도구를 사용하여 배포 환경의 각 컴퓨터에 대한 키 파일과 인증서 파일을 만듭니다.

참고:

- Crystal Reports와 같은 짙(thick) 클라이언트 구성 요소를 실행하는 컴퓨터를 비롯하여 배포의 모든 컴퓨터에 대해 인증서와 키를 만들어야 합니다. 이러한 클라이언트 컴퓨터의 경우 sslconfig 명령줄 도구를 사용하여 구성합니다.
- 최상의 보안을 위해 모든 개인 키를 보호하고 보안되지 않은 통신 채널을 통해 전송하지 말아야 합니다.
- 이전 버전의 BI 플랫폼에 대해 만들어진 인증서는 SAP BusinessObjects Business Intelligence 플랫폼 4.0에서 사용할 수 없습니다. 이러한 인증서는 다시 만들어야 합니다.

6.13.1.1 컴퓨터의 키와 인증서 파일을 만들려면

1. SSLC.exe 명령줄 도구를 실행합니다.

SSLC 도구는 BI 플랫폼 소프트웨어와 함께 설치됩니다. 예를 들어, Windows의 경우 이 도구는 기본적으로 <INSTALLDIR>WSAP BusinessObjects Enterprise XI 4.0\Win64_x64에 설치됩니다.

2. 다음 명령을 입력합니다.

```
sslc req -config sslc.cnf -new -out cacert.req
```

이 명령을 실행하면 CA(인증 기관) 인증서 요청(cacert.req) 및 개인 키(privkey.pem)의 두 가지 파일이 작성됩니다.

3. 개인 키의 암호를 해독하려면 다음 명령을 입력합니다.

이 명령을 실행하면 서명된 인증서가 들어 있는 servercert.pem 파일이 작성됩니다.

10. 다음 명령을 사용하여 인증서를 DER 인코딩된 인증서로 변환합니다.

```
sslc x509 -in cacert.pem -out cacert.der -outform DER
```

```
sslc x509 -in servercert.pem -out servercert.der -outform DER
```

참고:

CA 인증서(cacert.der) 및 해당 개인 키(cakey.pem)는 배포 당 한 번만 생성해야 합니다. 동일한 배포에 속한 컴퓨터는 모두 동일한 CA 인증서를 공유해야 합니다. 다른 인증서는 모두 임의의 CA 인증서 개인 키로 서명해야 합니다.

11. 생성된 개인 키를 암호 해독하는 데 사용되는 일반 텍스트 passphrase를 저장하기 위한 텍스트 파일(passphrase.txt)을 만듭니다.
12. BI 플랫폼 배포 환경에서 컴퓨터로 액세스할 수 있는 동일한 디렉터리 ((d:/ssl))의 안전한 위치에 다음 키 및 인증서 파일을 저장합니다.
 - 신뢰할 수 있는 인증서 파일(cacert.der)
 - 생성된 서버 인증서 파일(servercert.der)
 - 서버 키 파일(server.key)
 - passphrase 파일

이 위치는 웹 응용 프로그램 서버와 CCM의 SSL을 구성하는 데 사용됩니다.

6.13.2 SSL 프로토콜 구성

배포 환경에서 각 컴퓨터에 대한 키와 인증서를 만들고 이러한 파일을 안전한 위치에 저장한 다음 이 안전한 위치를 통해 중앙 구성 관리자(CCM) 및 웹 응용 프로그램 서버를 제공해야 합니다.

또한 웹 응용 프로그램 서버 및 티켓 클라이언트 응용 프로그램을 실행하는 컴퓨터용 SSL 프로토콜을 구성하기 위한 특정 단계도 구현해야 합니다.

6.13.2.1 CCM에서 SSL 프로토콜 구성

1. CCM에서 Server Intelligence Agent를 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.
2. 속성 대화 상자에서 프로토콜 탭을 클릭합니다.

3. SSL 사용을 선택합니다.
4. 키와 인증서 파일이 저장된 디렉터리의 파일 경로를 입력합니다.

필드	설명
SSL 인증서 폴더	필요한 모든 SSL 인증서와 파일이 있는 폴더입니다 예: d:\Wssl
서버 SSL 인증서 파일	서버 SSL 인증서를 저장하는 데 사용되는 파일의 이름입니다. 기본적으로 servercert.der입니다.
SSL 신뢰할 수 있는 인증서 파일	SSL 신뢰할 수 있는 인증서를 저장하는 데 사용되는 파일의 이름입니다. 기본적으로 cacert.der입니다.
SSL 개인 키 파일	인증서에 액세스하는 데 사용되는 SSL 개인 키 파일의 이름입니다. 기본적으로 server.key입니다.
SSL 개인 키 암호 파일	개인 키에 액세스하는 데 사용되는 암호를 포함하는 텍스트 파일의 이름입니다. 기본적으로 passphrase.txt입니다.

참고:

서버가 실행되고 있는 컴퓨터에 대한 디렉터리를 제공해야 합니다.

6.13.2.2 UNIX에서 SSL 프로토콜 구성

SIA에 대해 SSL 프로토콜을 구성하려면 serverconfig.sh 스크립트를 사용해야 합니다. 이 스크립트는 서버 정보를 보고 설치 환경에서 서버를 추가하거나 삭제하는 데 사용할 수 있는 텍스트 기반의 프로그램을 제공합니다. serverconfig.sh 스크립트는 설치 환경의 sap_bobj 디렉터리에 설치됩니다.

1. ccm.sh 스크립트를 사용하여 SIA 및 모든 SAP BusinessObjects 서버의 작동을 중지합니다.
2. serverconfig.sh 스크립트를 실행합니다.
3. 3 - Server Intelligence Agent 수정을 선택하고 Enter 키를 누릅니다.
4. 대상 SIA를 지정하고 Enter 키를 누릅니다.
5. 서버 SSL 구성 수정 옵션을 선택합니다.
6. ssl을 선택합니다.

메시지가 표시되면 SSL 인증서 위치를 지정합니다.

7. BI 플랫폼 배포 환경이 SIA 클러스터일 경우 SIA마다 1-6단계를 반복합니다.
8. ccm.sh 스크립트로 SIA를 시작한 다음 서버가 시작될 때까지 기다립니다.

6.13.2.3 웹 응용 프로그램 서버에 대한 SSL 프로토콜을 구성하려면

1. J2EE 웹 응용 프로그램 서버가 있으면 다음 시스템 속성을 설정하여 Java SDK를 실행합니다. 예를 들면 다음과 같습니다.

```
-Dbusinessobjects.orb.ocl.protocol=ssl -DcertDir=d:\Wssl -DtrustedCert=cacert.der  
-DsslCert=clientcert.der -DsslKey=client.key -Dpassphrase=passphrase.txt
```

다음 표에는 이러한 예에 해당하는 설명이 나열되어 있습니다.

예제	설명
DcertDir=d:\Wssl	모든 인증서와 키를 저장할 디렉터리입니다.
DtrustedCert=cacert.der	신뢰할 수 있는 인증서 파일입니다. 두 개 이상 지정할 경우 세미콜론으로 구분합니다.
DsslCert=clientcert.der	SDK에서 사용하는 인증서입니다.
DsslKey=client.key	SDK 인증서의 개인 키입니다.
Dpassphrase=passphrase.txt	개인 키의 암호를 저장하는 파일입니다.

2. IIS 웹 응용 프로그램 서버가 있으면 명령줄에서 sslconfig 도구를 실행하고 구성 단계를 수행합니다.

6.13.2.4 씹(Thick) 클라이언트 구성

다음 절차를 수행하기 전에 필요한 SSL 리소스(예: 인증서 및 개인 키)를 모두 알려진 디렉터리에 만들고 저장해야 합니다.

아래 절차에서는 다음 SSL 리소스를 만들기 위한 지침을 따랐다고 가정합니다.

SSL 리소스	
SSL 인증서 폴더	d:\Wssl
서버 SSL 인증서 파일 이름	servercert.der
SSL 신뢰할 수 있는 인증서 또는 루트 인증서 파일 이름	cacert.der
SSL 개인 키 파일 이름	server.key
SSL 개인 키 파일에 액세스하는 데 사용되는 암호를 포함하는 파일	passphrase.txt

위 리소스를 만들었으면 다음 지침에 따라 중앙 구성 관리자(CCM) 또는 업그레이드 관리 도구 등의 썩(thick) 클라이언트 응용 프로그램을 구성하십시오.

1. 썩(thick) 클라이언트 응용 프로그램이 작동하고 있지 않은지 확인합니다.

참고:

서버가 실행되고 있는 컴퓨터에 대한 디렉터리를 제공해야 합니다.

2. sslconfig.exe 명령줄 도구를 실행합니다.

SSLC 도구는 BI 플랫폼 소프트웨어와 함께 설치됩니다. 예를 들어, Windows의 경우 이 도구는 기본적으로 <INSTALLDIR>WSAP BusinessObjects Enterprise XI 4.0\Win64_x64에 설치됩니다.

3. 다음 명령을 입력합니다.

```
sslconfig.exe -dir d:\WSSL -mycert servercert.der -rootcert cacert.der -mykey server.key
-passphrase passphrase.txt -protocol ssl
```

4. 썩(thick) 클라이언트 웹 응용 프로그램을 다시 시작합니다.

관련 항목

- 162 페이지에서 [컴퓨터의 키와 인증서 파일을 만들려면](#)

6.13.2.4.1 번역 관리 도구에 대해 SSL 로그인 구성

사용자가 번역 관리 도구에서 SSL 로그인을 사용할 수 있게 하려면 SSL 리소스에 대한 정보를 도구의 구성 파일(.ini)에 추가해야 합니다.

1. <INSTALLDIR>WSAP BusinessObjects Enterprise XI 4.0\Win32_x86 디렉터리에서 TransMgr.ini 파일을 찾습니다..
2. 텍스트 편집기를 사용하여 TransMgr.ini 파일을 엽니다.

3. 다음 매개 변수를 추가합니다.

```
-Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=D:\WSSLCert
-DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key
-Dpassphrase=passphrase.txt -jar program.jar
```

4. 파일을 저장하고 텍스트 편집기를 닫습니다.

이제 사용자가 SSL을 사용하여 번역 관리 도구에 로그인할 수 있습니다.

6.13.2.4.2 보고서 변환 도구에 대해 SSL 구성

다음 절차를 수행하기 전에 필요한 SSL 리소스(예: 인증서 및 개인 키)를 모두 알려진 디렉터리에 만들고 저장해야 합니다. 또한 BI 플랫폼 배포의 일부로 보고서 변환 도구를 설치해야 합니다.

아래 절차에서는 다음 SSL 리소스를 만들기 위한 지침을 따랐다고 가정합니다.

SSL 리소스	
SSL 인증서 폴더	d:\Wssl
서버 SSL 인증서 파일 이름	servercert.der
SSL 신뢰할 수 있는 인증서 또는 루트 인증서 파일 이름	cacert.der
SSL 개인 키 파일 이름	server.key
SSL 개인 키 파일에 액세스하는 데 사용되는 암호를 포함하는 파일	passphrase.txt

위 리소스를 만들었으면 다음 지침에 따라 보고서 변환 도구에서 작동하도록 SSL을 구성하십시오.

1. 보고서 변환 도구를 호스팅하는 컴퓨터에 Windows 환경 변수 BOBJ_MIGRATION을 만듭니다.

팁:

변수는 원하는 값으로 설정할 수 있습니다.

2. 텍스트 편집기를 사용하여 다음 디렉터리에 있는 migration.bat 파일을 엽니다.

<INSTALLDIR>\WSAP BusinessObjects Enterprise XI 4.0\Win32_x86\scripts\W.

3. 다음 줄을 찾습니다.

```
start "" "%JRE%\bin\Wjavaw" -Xmx512m -Xss10m -jar "%SHAREDIR%\Wlib\Wmigration.jar"
```

4. -Xss10m 매개 변수 뒤에 다음을 추가합니다.

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir=C:\ssl
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
```



```
-Dpassphrase=passphrase.txt
-Dbusinessobjects.migration
```

참고:

각 매개 변수 사이에 공백이 있는지 확인하십시오.

5. 파일을 저장하고 텍스트 편집기를 닫습니다.

이제 사용자가 SSL을 사용하여 보고서 변환 도구에 액세스할 수 있습니다.

관련 항목

- 162 페이지에서 [컴퓨터의 키와 인증서 파일을 만들려면](#)

6.14 BI 플랫폼 구성 요소 간의 통신 이해

BI 플랫폼 시스템 전체를 동일한 보안 서브넷에만 배포한 경우에는 방화벽을 별도로 구성할 필요가 없습니다. 그러나 하나 이상의 방화벽으로 분리된 각기 다른 서브넷에 일부 구성 요소를 배포할 수도 있습니다.

방화벽을 사용하여 작동하도록 시스템을 구성하려면 먼저 BI 플랫폼 서버, 리치 클라이언트 및 SAP BusinessObjects SDK를 호스팅하는 웹 응용 프로그램 서버 사이의 통신에 대해 이해해야 합니다.

관련 항목

- 179 페이지에서 [BI 플랫폼의 방화벽 구성](#)
- 184 페이지에서 [일반적인 방화벽 시나리오의 예](#)

6.14.1 BI 플랫폼 서버 및 통신 포트 개요

방화벽과 함께 시스템을 배포하는 경우 BI 플랫폼 서버와 통신 포트를 이해하고 있어야 합니다.

6.14.1.1 BI 플랫폼 서버별 요청 포트 바인딩

BI 플랫폼 서버(예: 입력 파일 리포지토리 서버)는 시작 시 요청 포트에 바인딩됩니다. 서버, 리치 클라이언트, 웹 응용 프로그램 서버에 호스팅된 SDK를 포함한 다른 BI 플랫폼 구성 요소에서는 이 요청 포트를 사용하여 서버와 통신할 수 있습니다.

특정 포트 번호를 사용하도록 구성되지 않은 경우에는 서버가 시작 또는 재시작될 때 동적으로 요청 포트 번호를 선택합니다. 방화벽을 지나 다른 BI 플랫폼 구성 요소와 통신하는 서버에 대해서는 특정 요청 포트 번호를 구성해야 합니다.

6.14.1.2 BI 플랫폼 서버별 CMS 등록

BI 플랫폼 서버가 시작되면 CMS에 등록됩니다. 서버를 등록할 때 CMS에 기록되는 사항은 다음과 같습니다.

- 서버의 호스트 컴퓨터의 호스트 이름 또는 IP 주소
- 서버의 요청 포트 번호

6.14.1.3 CMS에서 두 개의 포트 사용

중앙 관리 서버(CMS)에서는 요청 포트와 이름 서버 포트라는 두 개의 포트를 사용합니다. 요청 포트는 기본적으로 동적으로 선택됩니다. 이름 서버 포트는 기본적으로 6400입니다.

모든 BI 플랫폼 서버 및 클라이언트 응용 프로그램은 이름 서버 포트에서 CMS와 처음 연결을 시도합니다. CMS는 요청 포트의 값을 반환하여 이 초기 접촉에 응답합니다. 서버는 이후에 이어지는 CMS와의 통신에 이 요청 포트를 사용합니다.

6.14.1.4 중앙 관리 서버(CMS)에서 제공하는 등록된 서비스 디렉터리

CMS는 등록된 서비스의 디렉터리를 제공합니다. 웹 서비스, 리치 클라이언트, 웹 응용 프로그램 서버에서 호스팅되는 SDK 등의 기타 BI 플랫폼 구성 요소는 CMS에 연결하여 특정 서비스에 대한 참조를 요청할 수 있습니다. 서비스의 참조에는 서비스의 요청 포트 번호와 서버의 호스트 컴퓨터 및 서비스 ID의 호스트 이름 또는 IP 주소가 포함됩니다.

BI 플랫폼 구성 요소와 이 구성 요소가 사용하는 서버가 서로 다른 서브넷에 위치할 수도 있습니다. 서비스 참조에 포함된 호스트 이름이나 IP 주소를 구성 요소의 컴퓨터에서 라우팅할 수 있어야 합니다.

참고:

BI 플랫폼 서버에 대한 참조에는 기본적으로 서버 컴퓨터의 호스트 이름이 포함됩니다. 컴퓨터에 여러 개의 호스트 이름이 있으면 기본 호스트 이름이 선택됩니다. 참조에 호스트 이름 대신 IP 주소가 포함되도록 서버를 구성할 수 있습니다.

관련 항목

- 172 페이지에서 [BI 플랫폼 구성 요소 간의 통신](#) "

6.14.1.5 중앙 관리 서버(CMS)와 통신하는 SIA(Server Intelligence Agent)

SIA(Server Intelligence Agent)와 중앙 관리 서버(CMS)가 서로 통신할 수 없는 경우에는 배포 작업을 수행할 수 없습니다. 방화벽 포트가 모든 SIA와 클러스터 내 모든 CMS 간의 통신을 허용하도록 구성되어 있는지 확인하십시오.

6.14.1.6 데이터 계층 및 CMS와 통신하는 작업 서버 자식 프로세스

대부분의 작업 서버에서는 보고서 생성 같은 작업을 처리하기 위해 자식 프로세스를 만듭니다. 작업 서버는 하나 이상의 하위 프로세스를 만듭니다. 자식 프로세스 각각에는 고유한 요청 포트가 있습니다.

기본적으로 각 자식 프로세스의 요청 포트는 작업 서버를 통해 동적으로 선택됩니다. 포트 번호의 범위를 지정하고 작업 서버가 그 범위 내에서 포트를 선택하도록 할 수 있습니다.

모든 자식 프로세스는 CMS와 통신합니다. 이 통신이 방화벽을 지나는 경우에는 다음을 수행해야 합니다.

- -requestJSChildPorts<lowestport>-<highestport> 및 -requestPort<port> 매개 변수를 서버의 명령줄에 추가하여 작업 서버에서 선택할 수 있는 포트 번호 범위를 지정합니다. 포트 범위는 -maxJobs에 지정된 자식 프로세스의 최대 개수를 허용할 수 있을 정도로 충분히 커야 합니다.
- 방화벽에서 지정된 포트 범위를 엽니다.

대부분의 자식 프로세스는 데이터 계층과 통신합니다. 예를 들어, 자식 프로세스가 보고 데이터베이스에 연결하여 데이터를 추출하고 보고서의 값을 계산할 수 있습니다. 작업 서버 자식 프로세스가 방화벽을 지나 데이터 계층과 통신하는 경우에는 다음을 수행해야 합니다.

- 작업 서버 컴퓨터의 임의의 포트에서 데이터베이스 서버 컴퓨터의 데이터베이스 수신 포트에 연결되는 통신 경로를 방화벽에 엮습니다.

관련 항목

- 779 페이지에서 [명령줄 개요](#)"

6.14.2 BI 플랫폼 구성 요소 간의 통신

브라우저 클라이언트, 리치 클라이언트, 서버, 웹 응용 프로그램 서버에서 호스팅되는 SDK 등의 BI 플랫폼 구성 요소는 일반적인 워크플로 도중 네트워크를 통해 서로 통신합니다. 방화벽으로 분리되어 있는 서로 다른 서브넷에 SAP BusinessObjects 제품을 배포하려면 이러한 워크플로를 이해해야 합니다.

6.14.2.1 BI 플랫폼 구성 요소 간 통신을 위한 요구 사항

다음과 같은 일반적인 요구 사항을 충족하도록 BI 플랫폼을 배포해야 합니다.

1. 모든 서버가 해당 서버의 요청 포트에서 다른 모든 BI 플랫폼 서버와의 통신을 시작할 수 있어야 합니다.
2. CMS에는 두 개의 포트가 사용됩니다. 모든 BI 플랫폼 서버, 리치 클라이언트 및 SDK를 호스팅하는 웹 응용 프로그램 서버가 두 포트 모두에서 중앙 관리 서버(CMS)와의 통신을 시작할 수 있어야 합니다.
3. 모든 작업 서버 하위 프로세스가 CMS와 통신할 수 있어야 합니다.
4. 짙(Thick) 클라이언트가 입력 및 출력 파일 리포지토리 서버에 있는 요청 포트와의 통신을 시작할 수 있어야 합니다.
5. 짙(Thick) 클라이언트 및 웹 응용 프로그램에서 감사를 사용할 수 있는 경우 이들이 클라이언트 감사 프록시 서비스를 호스팅하는 적응형 처리 서버에 있는 요청 포트와의 통신을 시작할 수 있어야 합니다.
6. 일반적으로 SDK를 호스팅하는 웹 응용 프로그램 서버는 모든 BI 플랫폼 서버의 요청 포트와 통신할 수 있어야 합니다.

참고:

웹 응용 프로그램 서버에서는 배포에 사용되는 BI 플랫폼 서버와만 통신하면 됩니다. 예를 들어 Crystal Reports가 사용되지 않는 경우 웹 응용 프로그램 서버에서는 Crystal Reports 캐시 서버와 통신할 필요가 없습니다.

7. 작업 서버에서는 `-requestJSChildPorts <port range>` 명령을 통해 지정된 포트 번호를 사용합니다. 명령줄에 범위가 지정되지 않은 경우 임의의 포트 번호가 사용됩니다. 작업 서버가 다른 컴퓨터에 있는 CMS, FTP 또는 메일 서버와 통신할 수 있게 하려면 `-requestJSChildPorts`에 지정된 범위의 모든 포트를 방화벽에서 개방하십시오.
8. CMS가 CMS 데이터베이스 수신 포트와 통신할 수 있어야 합니다.
9. 연결 서버, 대부분의 작업 서버 하위 프로세스, 모든 시스템 데이터 및 감사 처리 서버가 보고 데이터베이스 수신 포트와의 통신을 시작할 수 있어야 합니다.

관련 항목

- 173 페이지에서 [BI 플랫폼 포트 요구 사항](#) "

6.14.2.2 BI 플랫폼 포트 요구 사항

이 단원에는 BI 플랫폼 서버, 씹(Thick) 클라이언트, SDK를 호스팅하는 웹 응용 프로그램 서버 및 타사 소프트웨어 응용 프로그램에 사용되는 통신 포트가 나와 있습니다. 방화벽을 포함하여 BI 플랫폼을 배포하는 경우 이 정보를 사용하면 방화벽에서 열어야 할 포트의 수를 최소화할 수 있습니다.

6.14.2.2.1 BI 플랫폼 응용 프로그램의 포트 요구 사항

다음 표에는 BI 플랫폼 응용 프로그램에서 사용되는 서버 및 포트 번호가 나와 있습니다.

제품	클라이언트 응용 프로그램	관련 서버	서버 포트 요구 사항
Crystal Reports	SAP Crystal Reports 2011 디자이너	CMS 입력 FRS 출력 FRS Crystal Reports 2011 Report Application Server(RAS) Crystal Reports 2011 처리 서버 Crystal Reports 캐시 서버	CMS 이름 서버 포트(기본값: 6400) CMS 요청 포트 입력 FRS 요청 포트 출력 FRS 요청 포트 Crystal Reports 2011 Report Application Server 요청 포트 Crystal Reports 2011 처리 서버 요청 포트 Crystal Reports 캐시 서버 요청 포트
Crystal Reports	SAP Crystal Reports for Enterprise 디자이너	CMS 입력 FRS 출력 FRS Crystal Reports 처리 서버 Crystal Reports 캐시 서버	CMS 이름 서버 포트(기본값: 6400) CMS 요청 포트 입력 FRS 요청 포트 출력 FRS 요청 포트 Crystal Reports 처리 서버 요청 포트 Crystal Reports 캐시 서버 요청 포트
Dashboard Design	SAP BusinessObjects Dashboard Design	CMS 입력 FRS 출력 FRS 특정 데이터 소스 연결에 필요한 Dashboard Design, Live Office 및 QaaWS 웹 서비스를 호스팅하는 웹 서비스 공급자 응용 프로그램(dswebobje.war)	CMS 이름 서버 포트(기본값: 6400) CMS 요청 포트 입력 FRS 요청 포트 출력 FRS 요청 포트 HTTP 포트(기본값: 80)
Live Office	Live Office 클라이언트	Live Office 웹 서비스를 호스팅하는 웹 서비스 공급자 응용 프로그램(dswebobje.war)	HTTP 포트(기본값: 80)

제품	클라이언트 응용 프로그램	관련 서버	서버 포트 요구 사항
BI 플랫폼	SAP BusinessObjects Web Intelligence Desktop	CMS 입력 FRS	CMS 이름 서버 포트(기본값: 6400) CMS 요청 포트 입력 FRS 요청 포트
BI 플랫폼	유니버스 디자인 도구	CMS 입력 FRS 연결 서버	CMS 이름 서버 포트(기본값: 6400) CMS 요청 포트 입력 FRS 요청 포트 연결 서버 포트
BI 플랫폼	비즈니스 뷰 관리자	CMS 입력 FRS	CMS 이름 서버 포트(기본값: 6400) CMS 요청 포트 입력 FRS 요청 포트

제품	클라이언트 응용 프로그램	관련 서버	서버 포트 요구 사항
BI 플랫폼	중앙 구성 관리자(CCM)	CMS SIA(Server Intelligence Agent)	<p>CCM에서 원격 BI 플랫폼 서버를 관리하려면 다음 포트를 열어 두어야 합니다.</p> <p>CMS 이름 서버 포트(기본값: 6400)</p> <p>CMS 요청 포트</p> <p>CCM에서 원격 SIA 프로세스를 관리하려면 다음 포트를 열어 두어야 합니다.</p> <p>Microsoft 디렉터리 서비스(TCP 포트 445)</p> <p>NetBIOS 세션 서비스(TCP 포트 139)</p> <p>NetBIOS 데이터그램 서비스(UDP 포트 138)</p> <p>NetBIOS 이름 서비스(UDP 포트 137)</p> <p>DNS(TCP/UDP 포트 53)</p> <p>위에 나와 있는 포트 중 일부는 필요하지 않을 수도 있습니다. 자세한 내용은 Windows 관리자에게 문의하십시오.</p>
BI 플랫폼	SIA(Server Intelligence Agent)	CMS가 포함된 모든 BI 플랫폼 서버	<p>SIA 요청 포트(기본값: 6410)</p> <p>CMS 이름 서버 포트(기본값: 6400)</p> <p>CMS 요청 포트</p>
BI 플랫폼	보고서 변환 도구	CMS 입력 FRS	<p>CMS 이름 서버 포트(기본값: 6400)</p> <p>CMS 요청 포트</p> <p>입력 FRS 요청 포트</p>

제품	클라이언트 응용 프로그램	관련 서버	서버 포트 요구 사항
BI 플랫폼	리포지토리 진단 도구	CMS 입력 FRS 출력 FRS	CMS 이름 서버 포트(기본값: 6400) CMS 요청 포트 입력 FRS 요청 포트 출력 FRS 요청 포트
BI 플랫폼	웹 응용 프로그램 서버에서 호스팅되는 BI 플랫폼 SDK	배포된 제품에 필요한 모든 BI 플랫폼 서버 예를 들어 SDK가 CMS에서 Crystal 보고서를 검색하여 통신하는 경우 Crystal Reports 2011 처리 서버 요청 포트와의 통신이 필요합니다.	CMS 이름 서버 포트(기본값: 6400) CMS 요청 포트 필요한 각 서버의 요청 포트 (예: Crystal Reports 2011 처리 서버 요청 포트)
BI 플랫폼	웹 서비스 공급자(dswebobje.war)	웹 서비스를 액세스하는 제품에 필요한 모든 BI 플랫폼 서버 예를 들어 SAP BusinessObjects Dashboard Design이 웹 서비스 공급자를 통해 Enterprise 데이터 소스 연결에 액세스하는 경우 Dashboard Design 캐시 및 처리 서버 요청 포트와의 통신이 필요합니다.	CMS 이름 서버 포트(기본값: 6400) CMS 요청 포트 필요한 각 서버의 요청 포트 (예: Dashboard Design 캐시 서버 및 Dashboard Design 처리 서버 요청 포트)
BI 플랫폼	SAP BusinessObjects Analysis, OLAP용 에디션	CMS 다차원 분석 서비스를 호스팅하는 적응형 처리 서버 입력 FRS 출력 FRS	CMS 이름 서버 포트(기본값: 6400) CMS 요청 포트 적응 처리 서버 요청 포트 입력 FRS 요청 포트 출력 FRS 요청 포트

6.14.2.2.2 타사 응용 프로그램의 포트 요구 사항

다음 표에는 SAP Business Objects 제품에 사용되는 타사 소프트웨어가 나와 있습니다. 여기에는 몇몇 소프트웨어 공급업체의 특정 예가 포함되어 있지만 각 공급업체별로 포트 요구 사항이 다르다는 점을 염두에 두어야 합니다.

타사 응용 프로그램	타사 제품을 사용하는 SAP Business Objects 구성 요소	타사 응용 프로그램 포트 요구 사항	설명
CMS 시스템 데이터베이스	중앙 관리 서버(CMS)	데이터베이스 서버 수신 포트	CMS는 CMS 시스템 데이터베이스와 통신하는 유일한 서버입니다.
CMS 감사 데이터베이스	중앙 관리 서버(CMS)	데이터베이스 서버 수신 포트	CMS는 CMS 감사 데이터베이스와 통신하는 유일한 서버입니다.
보고 데이터베이스	연결 서버 모든 작업 서버 자식 프로세스 모든 처리 서버	데이터베이스 서버 수신 포트	이러한 서버는 보고 데이터베이스에서 정보를 검색합니다.
웹 응용 프로그램 서버	모든 SAP Business Objects 웹 서비스 및 웹 응용 프로그램(예: BI 실행 패드 및 CMC)	HTTP 포트와 HTTPS 포트. 예를 들어, Tomcat의 기본 HTTP 포트는 8080이고 기본 HTTPS 포트는 443입니다.	HTTPS 포트는 보안 HTTP 통신을 사용하는 경우에만 필요합니다.
FTP 서버	모든 작업 서버	FTP 인(포트 21) FTP 아웃(포트 22)	작업 서버에서는 FTP로 보내기를 허용하기 위해 FTP 포트를 사용합니다.

타사 응용 프로그램	타사 제품을 사용하는 SAP Business Objects 구성 요소	타사 응용 프로그램 포트 요구 사항	설명
전자 메일 서버	모든 작업 서버	SMTP(포트 25)	작업 서버에서는 전자 메일로 보내기를 허용하기 위해 SMTP 포트를 사용합니다.
작업 서버에서 콘텐츠를 보낼 수 있는 대상 UNIX 서버	모든 작업 서버	rexec 아웃(포트 512) (UNIX에만 해당) rsh 아웃(포트 514)	(UNIX에만 해당) 작업 서버에서는 디스크로 보내기를 허용하기 위해 이들 포트를 사용합니다.
인증 서버	CMS SDK를 호스팅하는 웹 응용 프로그램 서버 모든 씹(Thick) 클라이언트(예: Live Office)	타사 인증을 위한 연결 포트. 예를 들어, Oracle LDAP 서버의 연결 서버는 사용자가 ldap.ora 파일에 정의합니다.	사용자 자격 증명은 타사 인증 서버에 저장됩니다. 여기에 나열된 CMS, SDK 및 씹(Thick) 클라이언트는 사용자가 로그인할 때 타사 인증 서버와 통신해야 합니다.

6.15 BI 플랫폼의 방화벽 구성

이 단원에서는 방화벽이 구현된 환경에서 BI 플랫폼 시스템을 사용할 수 있도록 구성하는 단계별 지침을 제공합니다.

6.15.1 방화벽이 사용되는 시스템을 구성하려면

1. 방화벽을 지나 통신해야 하는 BI 플랫폼 구성 요소를 결정합니다.
2. 방화벽을 지나 통신해야 하는 각 BI 플랫폼 서버에 대한 요청 포트를 구성합니다.

3. -requestJSChildPorts<lowestport>-<highestport> 및 -requestPort<port> 매개 변수를 서버의 명령줄에 추가하여 방화벽을 지나 통신해야 하는 작업 서버 하위 항목에 대한 포트 번호를 구성합니다.
4. 이전 단계에서 구성한 BI 플랫폼 서버의 요청 포트 및 작업 서버 포트 범위에 대한 통신을 허용하도록 방화벽을 구성합니다.
5. (옵션) 방화벽을 지나 통신해야 하는 BI 플랫폼 서버를 호스팅하는 각 시스템에서 hosts 파일을 구성합니다.

관련 항목

- 172 페이지에서 [BI 플랫폼 구성 요소 간의 통신](#) "
- 397 페이지에서 [포트 번호 구성](#) "
- 779 페이지에서 [명령줄 개요](#) "
- 180 페이지에서 [방화벽 규칙 지정](#) "
- 181 페이지에서 [NAT를 사용하는 방화벽에 대한 호스트 파일 구성](#) "

6.15.1.1 방화벽 규칙 지정

BI 플랫폼 구성 요소 간에 필요한 트래픽을 허용하도록 방화벽을 구성해야 합니다. 이러한 규칙을 지정하는 방법에 대한 자세한 내용은 방화벽 설명서를 참조하십시오.

방화벽을 지나는 통신 경로 각각에 대해 인바운드 액세스 규칙을 하나씩 지정합니다. 방화벽 너머의 모든 BI 플랫폼 서버에 대해 액세스 규칙을 지정할 필요는 없습니다.

서버 포트 상자에 지정한 포트 번호를 사용합니다. 시스템의 각 서버에 사용되는 포트 번호는 서로 중복되지 않아야 합니다. 일부 Business Objects 서버에는 여러 개의 포트가 사용됩니다.

참고:

NAT를 사용하는 방화벽을 지나도록 BI 플랫폼을 배포한 경우에는 모든 컴퓨터의 각 서버에 고유한 요청 포트 번호가 필요합니다. 즉, 전체 배포에서 여러 서버가 동일한 요청 포트를 공유할 수 없습니다.

참고:

아웃바운드 액세스 규칙은 지정할 필요가 없습니다. BI 플랫폼 서버에서는 웹 응용 프로그램 서버나 클라이언트 응용 프로그램에 대한 통신을 시작하지 않습니다. BI 플랫폼 서버에서는 동일한 클러스터에 있는 다른 플랫폼 서버에 대한 통신을 시작할 수 있습니다. 아웃바운드 방화벽 환경에서 클러스터 서버를 통한 배포는 지원되지 않습니다.

예제

이 예제에서는 웹 응용 프로그램 서버와 BI 플랫폼 서버 사이의 방화벽에 대한 인바운드 액세스 규칙을 보여 줍니다. 여기서는 CMS에 대해 두 개의 포트, 즉 입력 FRS(파일 리포지토리 서버)에 사용

되는 포트와 출력 FRS에 사용되는 포트를 엽니다. 요청 포트 번호는 서버의 CMC 구성 페이지에 있는 포트 상자에 지정한 포트 번호입니다.

소스 컴퓨터	포트	대상 컴퓨터	포트	작업
웹 응용 프로그램 서버	모두 가능	CMS	6400	허용
웹 응용 프로그램 서버	모두 가능	CMS	<요청 포트 번호>	허용
웹 응용 프로그램 서버	모두 가능	입력 FRS	<요청 포트 번호>	허용
웹 응용 프로그램 서버	모두 가능	출력 FRS	<요청 포트 번호>	허용
모두 가능	모두 가능	CMS	모두 가능	거부
모두 가능	모두 가능	기타 플랫폼 서버	모두 가능	거부

관련 항목

- 172 페이지에서 [BI 플랫폼 구성 요소 간의 통신](#) "

6.15.1.2 NAT를 사용하는 방화벽에 대한 호스트 파일 구성

이 단계는 BI 플랫폼 서버가 통신할 때 NAT(Network Address Translation)를 사용하는 방화벽을 통과해야 하는 경우에만 필요합니다. 이 단계를 통해 클라이언트 컴퓨터에서 서버의 호스트 이름을 라우트 가능한 IP 주소에 매핑할 수 있습니다.

참고:

DNS(Domain Name System)를 사용하는 컴퓨터에 BI 플랫폼을 배포할 수 있습니다. 이 경우 서버 컴퓨터 호스트 이름을 각 컴퓨터의 hosts 파일 대신 DNS 서버의 외부 라우트 가능한 IP 주소에 매핑할 수 있습니다.

NAT 이해

방화벽은 내부 네트워크를 무단 액세스로부터 보호할 목적으로 배포됩니다. NAT(Network Address Translation)를 사용하는 방화벽에서는 내부 네트워크의 IP 주소를 외부 네트워크에 사용되는 다른 주소에 매핑할 수 있습니다. 이와 같은 주소 변환을 사용하면 외부 네트워크로부터 내부 IP 주소를 숨겨 보안을 강화할 수 있습니다.

서버, 썩(Thick)클라이언트, SDK를 호스팅하는 웹 응용 프로그램 서버 같은 BI 플랫폼 구성 요소에서는 서비스 참조를 사용하여 서버에 연결합니다. 서비스 참조에는 서버 컴퓨터의 호스트 이름이 포함됩니다. 이 호스트 이름을 BI 플랫폼 구성 요소의 컴퓨터에서 라우트할 수 있어야 합니다. 즉, 구성 요소 컴퓨터에 있는 hosts 파일을 통해 서버 컴퓨터의 호스트 이름을 서버 컴퓨터의 외부 IP 주소에 매핑해야 합니다. 서버 컴퓨터의 외부 IP 주소는 방화벽 바깥쪽에서 라우트할 수 있는 반면 내부 IP 주소는 라우트할 수 없습니다.

hosts 파일을 구성하는 방법은 Windows와 UNIX에서 각각 다릅니다.

6.15.1.2.1 Windows에서 hosts 파일 구성

1. NAT(Network Address Translation)를 사용하는 방화벽을 통해 통신해야 하는 BI 플랫폼 구성 요소가 실행되는 컴퓨터를 모두 찾습니다.
2. 이전 단계에서 찾은 각 컴퓨터에서 메모장 같은 텍스트 편집기를 사용하여 hosts 파일을 엽니다. hosts 파일은 `\\WINNT\\system32\\drivers\\etc\\hosts`에 있습니다.
3. hosts 파일의 지침에 따라 방화벽으로 보호된 환경에서 BI 플랫폼 서버를 하나 이상 실행하는 각 컴퓨터에 대한 항목을 추가합니다. 서버 컴퓨터의 호스트 이름이나 정규화된 도메인 이름을 외부 IP 주소에 매핑합니다.
4. hosts 파일을 저장합니다.

6.15.1.2.2 UNIX에서 hosts 파일 구성

참고:

먼저 hosts 파일을 참조하여 도메인 이름을 확인한 다음 DNS를 참조하도록 UNIX 운영 체제를 구성해야 합니다. 자세한 내용은 UNIX 시스템 설명서를 참조하십시오.

1. NAT(Network Address Translation)를 사용하는 방화벽을 통해 통신해야 하는 BI 플랫폼 구성 요소가 실행되는 컴퓨터를 모두 찾습니다.
2. vi 같은 편집기를 사용하여 hosts 파일을 엽니다. hosts 파일은 `/etc` 디렉터리에 있습니다.

3. hosts 파일의 지침에 따라 방화벽으로 보호된 환경에서 BI 플랫폼 서버를 하나 이상 실행하는 각 컴퓨터에 대한 항목을 추가합니다. 서버 컴퓨터의 호스트 이름이나 정규화된 도메인 이름을 외부 IP 주소에 매핑합니다.
4. hosts 파일을 저장합니다.

6.15.2 방화벽을 사용하는 배포 디버깅

방화벽 사용 중에 하나 이상의 BI 플랫폼 서버가 작동하지 않을 경우 예상되는 포트가 방화벽에서 열려 있더라도 이벤트 로그를 통해 포트 또는 IP 주소에서 수신을 시도 중인 서버가 어떤 것인지 확인해야 합니다. 그런 다음 해당 방화벽에서 해당 포트를 열거나 중앙 관리 콘솔(CMC)에서 서버가 수신을 시도하는 포트 번호 또는 IP 주소를 변경할 수 있습니다.

BI 플랫폼 서버를 시작할 때마다 서버에서는 바인딩하려는 각 요청 포트에 대해 다음과 같은 정보를 이벤트 로그에 기록합니다.

- 서버 - 서버의 이름 및 서버가 정상적으로 시작되었는지 여부.
- 게시된 주소 - 다른 서버가 이 서버와 통신하기 위해 사용할 이름 서비스에 게시된 IP 주소와 포트 조합 목록

서버가 성공적으로 포트에 바인딩되면 로그 파일에도 수신 중인 포트, IP 주소 및 서버 수신 포트가 표시됩니다. 서버가 포트에 바인딩되지 못하면 로그 파일에 포트 수신 실패, IP 주소 및 서버가 수신을 시도했으나 실패한 포트가 표시됩니다.

중앙 관리 서버가 시작되면 서버의 이름 서비스 포트에 대해 게시된 주소, 수신 포트 및 수신 실패 정보도 기록됩니다.

참고:

서버가 자동 할당된 포트를 사용하고 올바르게 않은 호스트 이름이나 IP 주소를 사용하도록 구성되면 이벤트 로그에 서버가 호스트 이름 또는 IP 주소 및 포트 0을 수신하는데 실패했음이 표시됩니다. 지정된 호스트 이름이나 IP 주소가 올바르게 않을 경우 호스트 운영 체제가 포트를 할당할 수 있기 전에 서버가 실패합니다.

예제

다음 예는 두 개의 요청 포트 및 이름 서비스 포트를 수신 중인 중앙 관리 서버에 대한 항목을 보여줍니다.

```
Server mynode.cms1 successfully started.
Request Port :
  Published Address(es): mymachine.corp.com:11032, mymachine.corp.com:8765
  Listening on port(s): [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:11032, 10.90.172.216:8765
Name Service Port :
  Published Address(es): mymachine.corp.com:6400
  Listening on port(s): [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:6400, 10.90.172.216:6400
```

6.15.2.1 방화벽을 사용하는 배포 디버깅

1. 이벤트 로그에서 서버가 지정한 포트에 바인딩되었는지 확인합니다.
서버가 바인딩에 실패한 경우 서버와 같은 컴퓨터에서 실행 중인 다른 프로세스 간의 포트 충돌 때문일 수 있습니다. 수신 실패 항목은 서버에서 수신하려는 포트를 나타냅니다. netstat과 같은 유틸리티를 실행하여 포트를 점유한 프로세스를 확인한 다음 다른 프로세스 또는 서버가 다른 포트를 수신하도록 구성합니다.
2. 서버가 포트에 바인딩할 수 있는 경우 수신 대상 항목은 서버가 수신 중인 포트를 나타냅니다. 서버에서 포트를 수신 중임에도 올바르게 작동하지 않을 경우 방화벽에서 포트가 열려 있는지 확인하거나, 열려 있는 포트를 수신하도록 서버를 구성합니다.

참고:

배포의 모든 중앙 관리 서버(CMS)가 사용할 수 없는 포트 또는 IP 주소를 수신하는 경우 CMS가 시작되지 않으며 CMC에 로그인할 수 없습니다. CMS가 수신하는 포트 번호 또는 IP 주소를 바꾸려면 중앙 구성 관리자(CCM)를 사용하여 올바른 포트 번호나 IP 주소를 지정해야 합니다.

관련 항목

- 397 페이지에서 [포트 번호 구성](#)

6.16 일반적인 방화벽 시나리오의 예

이 단원에서는 일반적인 방화벽 배포 시나리오의 예를 제공합니다.

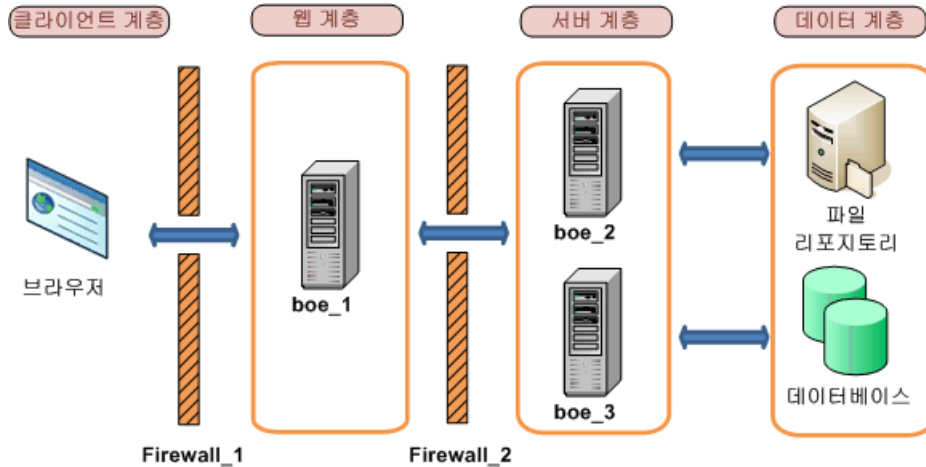
6.16.1 예제 - 별도의 네트워크에 배포된 응용 프로그램 계층

이 예제에서는 웹 응용 프로그램 서버와 다른 BI 플랫폼 서버가 방화벽으로 분리되어 있는 배포 환경에서 이러한 서버가 함께 작동하도록 방화벽과 BI 플랫폼을 구성하는 방법을 보여 줍니다.

이 예제에서 BI 플랫폼 구성 요소는 다음과 같은 시스템에 걸쳐 배포되어 있습니다.

- 컴퓨터 boe_1은 웹 응용 프로그램 서버와 SDK를 호스팅합니다.
- 컴퓨터 boe_2는 중앙 관리 서버, 입력 파일 리포지토리 서버, 출력 파일 리포지토리 서버 및 이벤트 서버를 비롯한 인텔리전스 계층 서버를 호스팅합니다.
- 컴퓨터 boe_3은 적응형 작업 서버, Web Intelligence 처리 서버, Report Application Server, Crystal Reports 캐시 서버 및 Crystal Reports 처리 서버를 비롯한 처리 계층 서버를 호스팅합니다.

그림 6-1: 별도의 네트워크에 배포된 응용 프로그램 계층



6.16.1.1 별도의 네트워크에 배포된 응용 프로그램 계층 구성

다음 단계에서는 이 예제를 구성하는 방법을 설명합니다.

- 이 예제에는 다음과 같은 통신 요구 사항이 적용됩니다.
 - SDK를 호스팅하는 웹 응용 프로그램 서버에서 두 개 포트 모두를 통해 CMS와 통신할 수 있어야 합니다.
 - SDK를 호스팅하는 웹 응용 프로그램 서버에서 모든 BI 플랫폼 서버와 통신할 수 있어야 합니다.
 - 브라우저에서 웹 응용 프로그램 서버의 http 또는 https 요청 포트에 액세스할 수 있어야 합니다.
 - 웹 응용 프로그램에서 boe_2 및 boe_3 컴퓨터의 모든 BI 플랫폼 서버와 통신해야 합니다. 이들 컴퓨터의 각 서버에 대해 포트 번호를 구성합니다. 1,025에서 65,535 사이에 있고 다른 곳에 사용되지 않은 임의의 포트를 사용할 수 있습니다.
- 이 예제를 위해 선택한 포트 번호는 다음 표에 나와 있는 것과 같습니다.

서버	포트 번호
중앙 관리 서버	6400
중앙 관리 서버	6411
입력 파일 리포지토리 서버	6415
출력 파일 리포지토리 서버	6420
이벤트 서버	6425
적응형 작업 서버	6435
Crystal Reports 캐시 서버	6440
Web Intelligence 처리 서버	6460
Report Application Server	6465
Crystal Reports 처리 서버	6470

3. 이전 단계에서 구성한 웹 응용 프로그램 서버와 서버의 고정된 포트에 대해 통신을 허용하도록 방화벽 Firewall_1과 Firewall_2를 구성합니다.

이 예제에서는 Tomcat 응용 프로그램 서버에 대해 HTTP 포트를 엽니다.

테이블6-6: Firewall_1 구성

포트	대상 컴퓨터	포트	작업
모두 가능	boe_1	8080	허용

Firewall_2 구성

소스 컴퓨터	포트	대상 컴퓨터	포트	작업
boe_1	모두 가능	boe_2	6400	허용
boe_1	모두 가능	boe_2	6411	허용
boe_1	모두 가능	boe_2	6415	허용
boe_1	모두 가능	boe_2	6420	허용
boe_1	모두 가능	boe_2	6425	허용
boe_1	모두 가능	boe_3	6435	허용
boe_1	모두 가능	boe_3	6440	허용

소스 컴퓨터	포트	대상 컴퓨터	포트	작업
boe_1	모두 가능	boe_3	6460	허용
boe_1	모두 가능	boe_3	6465	허용
boe_1	모두 가능	boe_3	6470	허용

4. 이 방화벽에는 NAT가 활성화되어 있지 않으므로 hosts 파일을 구성할 필요가 없습니다.

관련 항목

- 397 페이지에서 [포트 번호 구성](#)"
- 169 페이지에서 [BI 플랫폼 구성 요소 간의 통신 이해](#)"

6.16.2 예제 – 방화벽으로 BI 플랫폼 서버와 분리된 썩(Thick) 클라이언트 및 데이터베이스 계층

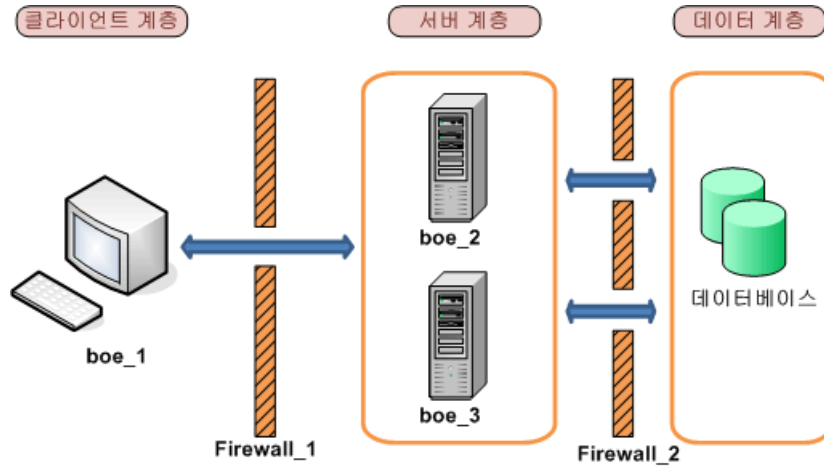
이 예제에서는 다음과 같은 배포 시나리오에서 서버가 함께 작동하도록 방화벽과 BI 플랫폼을 구성하는 방법을 보여 줍니다.

- 썩(Thick) 클라이언트와 BI 플랫폼 서버가 하나의 방화벽으로 분리된 경우
- BI 플랫폼 서버와 데이터베이스 계층이 하나의 방화벽으로 분리된 경우

이 예제에서는 BI 플랫폼 구성 요소가 다음과 같은 시스템에 배포되어 있습니다.

- 컴퓨터 boe_1은 게시 마법사를 호스팅합니다. 게시 마법사는 BI 플랫폼 썩(Thick) 클라이언트입니다.
- 컴퓨터 boe_2는 중앙 관리 서버(CMS), 입력 파일 리포지토리 서버, 출력 파일 리포지토리 서버 및 이벤트 서버를 비롯한 인텔리전스 계층 서버를 호스팅합니다.
- 컴퓨터 boe_3은 적응형 작업 서버, Web Intelligence 처리 서버, Report Application Server, Crystal Reports 처리 서버 및 Crystal Reports 캐시 서버를 비롯한 처리 계층 서버를 호스팅합니다.
- 컴퓨터 Databases는 CMS 시스템, 감사 데이터베이스 및 보고 데이터베이스를 호스팅합니다. 두 데이터베이스를 모두 동일한 데이터베이스 서버에 배포할 수도 있고 각기 다른 데이터베이스 서버에 배포할 수도 있습니다. 이 예제에서는 CMS 데이터베이스와 보고 데이터베이스가 모두 동일한 데이터베이스 서버에 배포됩니다. 데이터베이스 서버 수신 포트는 MySQL 서버의 기본 수신 포트인 3306입니다.

그림 6-2: 별도의 네트워크에 배포된 리치 클라이언트 및 데이터베이스 계층



6.16.2.1 방화벽으로 BI 플랫폼 서버와 분리된 계층 구성

다음 단계에서는 이 예제를 구성하는 방법을 설명합니다.

- 이 예제에는 다음과 같은 통신 요구 사항이 적용됩니다.
 - 게시 마법사가 두 포트 모두에서 CMS와의 통신을 시작할 수 있어야 합니다.
 - 게시 마법사가 입력 파일 리포지토리 서버 및 출력 파일 리포지토리 서버와의 통신을 시작할 수 있어야 합니다.
 - 연결 서버와 모든 작업 서버 자식 프로세스 및 모든 처리 서버에서 보고 데이터베이스 서버의 수신 포트에 액세스할 수 있어야 합니다.
 - CMS에서CMS 데이터베이스 서버의 데이터베이스 수신 포트에 액세스할 수 있어야 합니다.
- CMS, 입력 FRS 및 출력 FRS에 대해 특정 포트를 구성합니다. 1,025에서 65,535 사이에 있고 다른 곳에 사용되지 않은 임의의 포트를 사용할 수 있습니다.

이 예제를 위해 선택한 포트 번호는 다음 표에 나와 있는 것과 같습니다.

서버	포트 번호
중앙 관리 서버	6411
입력 파일 리포지토리 서버	6415
출력 파일 리포지토리 서버	6416

- 어느 포트에서나 통신을 시작할 수 있도록 작업 서버와 데이터베이스 서버 사이의 방화벽을 구성할 것이므로 작업 서버 자식에 대한 포트 범위는 구성할 필요가 없습니다.

4. 이전 단계에서 구성한 플랫폼 서버의 고정된 포트에 대해 통신을 허용하도록 Firewall_1을 구성합니다. 포트 6400은 CMS 이름 서버 포트의 기본 포트 번호이므로 이전 단계에서 명시적으로 구성할 필요가 없었습니다.

포트	대상 컴퓨터	포트	작업
모두 가능	boe_2	6400	허용
모두 가능	boe_2	6411	허용
모두 가능	boe_2	6415	허용
모두 가능	boe_2	6416	허용

데이터베이스 서버 수신 포트에 대한 통신을 허용하도록 Firewall_2를 구성합니다. boe_2의 CMS는 CMS 시스템 및 감사 데이터베이스에 액세스할 수 있어야 하고, boe_3의 작업 서버는 시스템 및 감사 데이터베이스에 액세스할 수 있어야 합니다. 이들 서버와 CMS 사이의 통신은 방화벽을 지나지 않고 이루어지므로 작업 서버 지식 프로세스에 대한 포트 범위는 구성하지 않았습니다.

소스 컴퓨터	포트	대상 컴퓨터	포트	작업
boe_2	모두 가능	Databases	3306	허용
boe_3	모두 가능	Databases	3306	허용

5. 이 방화벽에는 NAT가 활성화되어 있지 않으므로 hosts 파일을 구성할 필요가 없습니다.

관련 항목

- 169 페이지에서 [BI 플랫폼 구성 요소 간의 통신 이해](#)
- 179 페이지에서 [BI 플랫폼의 방화벽 구성](#)

6.17 통합 환경에 대한 방화벽 설정

이 단원에서는 다음 ERP 환경과 통합되는 BI 플랫폼 배포 환경에 대한 구체적인 고려 사항과 포트 설정을 자세히 설명합니다.

- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

BI 플랫폼 구성 요소에는 브라우저 클라이언트, 리치 클라이언트, 서버 및 웹 응용 프로그램 서버에 호스팅되는 SDK가 포함됩니다. 시스템 구성 요소는 여러 컴퓨터에 설치할 수 있습니다. 방화벽과 함께 작동하도록 시스템을 구성하기 전에 BI 플랫폼과 ERP 구성 요소 간의 통신에 대한 기본적인 내용을 이해하는 것이 좋습니다.

BI 플랫폼 서버의 포트 요구 사항

BI 플랫폼의 해당 서버에는 다음 포트가 필요합니다.

서버 포트 요구 사항
<ul style="list-style-type: none"> • 중앙 관리 서버 이름 서버 포트 • 중앙 관리 서버 요청 포트 • 입력 FRS 요청 포트 • 출력 FRS 요청 포트 • Report Application Server 요청 포트 • Crystal Reports 캐시 서버 요청 포트 • Crystal Reports 페이지 서버 요청 포트 • Crystal Reports 처리 서버 요청 포트

6.17.1 SAP 통합을 위한 구체적인 방화벽 지침

사용자의 BI 플랫폼 배포 환경은 다음과 같은 통신 규칙을 준수해야 합니다.

- CMS는 SAP 시스템 게이트웨이 포트에서 SAP 시스템과의 통신을 시작할 수 있어야 합니다.
- Crystal Reports 작업 서버 및 Crystal Reports 처리 서버와 데이터 액세스 구성 요소는 SAP 시스템 게이트웨이 포트에서 SAP 시스템과의 통신을 시작할 수 있어야 합니다.
- BW 게시자 구성 요소는 SAP 시스템 게이트웨이 포트에서 SAP 시스템과의 통신을 시작할 수 있어야 합니다.
- SAP Enterprise Portal 측에 배포된 BI 플랫폼 구성 요소(예: iView 및 KMC)는 HTTP/HTTPS 포트에서 BI 플랫폼 웹 응용 프로그램과의 통신을 시작할 수 있어야 합니다.
- 웹 응용 프로그램 서버는 SAP 시스템 게이트웨이 서비스에서 통신을 시작할 수 있어야 합니다.
- Crystal Reports는 SAP 시스템 디스패처 포트에서 SAP 시스템 게이트웨이 포트와의 통신을 시작할 수 있어야 합니다.

SAP 게이트웨이 서비스가 수신 대기 중인 포트는 설치 중에 지정한 것과 같습니다.

참고:

SAP 시스템에 연결하는 데 구성 요소에 SAP 라우터가 필요한 경우, SAP 라우터 문자열을 사용하여 구성 요소를 구성할 수 있습니다. 예를 들어, 역할 및 사용자를 가져오도록 SAP 권한 부여 시스템을 구성하는 경우 SAP 라우터 문자열을 응용 프로그램 서버의 이름 대신 사용할 수 있습니다. 이렇게 하면 SAP 라우터를 통해 CMS가 SAP 시스템과 통신하게 됩니다.

관련 항목

- 674 페이지에서 [로컬 SAP 게이트웨이 설치](#)"

6.17.1.1 자세한 포트 요구 사항

SAP에 대한 포트 요구 사항

BI 플랫폼은 SAP JCO(SAP Java Connector)를 사용하여 SAP NetWeaver(ABAP)와 통신합니다. 다음 포트가 사용 가능한지 확인하고 이러한 포트를 구성해야 합니다.

- SAP 게이트웨이 서비스 수신 대기 포트(예: 3300)
- SAP 디스패처 서비스 수신 대기 포트(예: 3200)

다음 표에서는 필요한 특정 포트 구성을 요약해서 설명합니다.

원본 컴퓨터	포트	대상 컴퓨터	포트	작업
SAP	모두 가능	BI 플랫폼 웹 응용 프로그램 서버	웹 서비스 HTTP/HTTPS 포트	허용
SAP	모두 가능	CMS	CMS 이름 서버 포트	허용
SAP	모두 가능	CMS	CMS 요청 포트	허용
웹 응용 프로그램 서버	모두 가능	SAP	SAP 시스템 게이트웨이 서비스 포트	허용
중앙 관리 서버 (CMS)	모두 가능	SAP	SAP 시스템 게이트웨이 서비스 포트	허용
Crystal Reports	모두 가능	SAP	SAP 시스템 게이트웨이 서비스 포트 및 SAP 시스템 디스패처 포트	허용

6.17.2 JD Edwards EnterpriseOne 통합을 위한 방화벽 구성

JD Edwards 소프트웨어와 통신할 BI 플랫폼 배포 환경은 다음과 같은 일반 통신 규칙을 준수해야 합니다.

- 중앙 관리 콘솔 웹 응용 프로그램이 JDENET 포트 및 무작위로 선택된 포트를 통해 JD Edwards EnterpriseOne과의 통신을 시작할 수 있어야 합니다.
- 데이터 연결 클라이언트 측 구성 요소를 포함하는 Crystal Reports가 JDENET 포트를 통해 JD Edwards EnterpriseOne과의 통신을 시작할 수 있어야 합니다. 데이터 검색을 위해 JD Edwards EnterpriseOne 측이 제어할 수 없는 임의의 포트를 통해 드라이버와 통신할 수 있어야 합니다.
- 중앙 관리 서버가 JDENET 포트 및 무작위로 선택된 포트를 통해 JD Edwards EnterpriseOne과의 통신을 시작할 수 있어야 합니다.
- JDENET 포트 번호는 JDENET 섹션 아래에 있는 JD Edwards EnterpriseOne Application Server 구성 파일(JDE.INI)에서 찾을 수 있습니다.

6.17.2.1 BI 플랫폼 서버의 포트 요구 사항

제품	서버 포트 요구 사항
SAP BusinessObjects Business Intelligence 플랫폼	<ul style="list-style-type: none"> • BI 플랫폼 로그인 서버 포트

6.17.2.2 JD Edwards EnterpriseOne의 포트 요구 사항

제품	포트 요구 사항	설명
JD Edwards EnterpriseOne	JDENET 포트 및 무작위로 선택된 포트	BI 플랫폼과 JD Edwards EnterpriseOne 응용 프로그램 서버 간 통신에 사용됩니다.

6.17.2.3 JD Edwards와 통신하도록 웹 응용 프로그램 서버 구성

이 단원에서는 웹 응용 프로그램 서버와 다른 BI 플랫폼 서버가 방화벽으로 분리되어 있는 배포 시나리오에서 이러한 서버가 함께 작동하도록 방화벽과 BI 플랫폼을 구성하는 방법을 보여 줍니다.

BI 플랫폼 서버 및 클라이언트의 방화벽 구성에 대한 자세한 내용은 이 가이드의 BI 플랫폼 포트 요구 사항 단원을 참조하십시오. 표준 방화벽 구성 이외에도 JD Edwards 서버와 통신하려면 몇 개의 추가 포트를 열어야 합니다.

테이블6-14: JD Edwards EnterpriseOne Enterprise의 경우

소스 컴퓨터	포트	대상 컴퓨터	포트	작업
JD Edwards EnterpriseOne에 대한 보안 연결 기능이 있는 CMS	모두 가능	JD Edwards EnterpriseOne	모두 가능	허용
JD Edwards EnterpriseOne에 대한 데이터 연결 기능이 있는 BI 플랫폼 서버	모두 가능	JD Edwards EnterpriseOne	모두 가능	허용
JD Edwards EnterpriseOne에 대한 클라이언트 측 데이터 연결 기능이 있는 Crystal Reports	모두 가능	JD Edwards EnterpriseOne	모두 가능	허용
웹 응용 프로그램 서버	모두 가능	JD Edwards EnterpriseOne	모두 가능	허용

6.17.3 Oracle EBS에 대한 구체적인 방화벽 지침

BI 플랫폼 배포 환경에서는 다음 구성 요소가 Oracle 데이터베이스 수신기 포트와의 통신을 시작할 수 있어야 합니다.

- BI 플랫폼 웹 구성 요소
- CMS(특히 Oracle EBS 보안 플러그 인)
- BI 플랫폼 백엔드 서버(특히 EBS Data Access 구성 요소)
- Crystal Reports(특히 EBS Data Access 구성 요소)

참고:

위에 언급한 모든 Oracle 데이터베이스 수신기 포트의 기본값은 1521입니다.

6.17.3.1 자세한 포트 요구 사항

BI 플랫폼에 대한 표준 방화벽 구성 이외에도 몇 개의 추가 포트를 열어야 통합된 Oracle EBS 환경에서 작동할 수 있습니다.

소스 컴퓨터	포트	대상 컴퓨터	포트	작업
웹 응용 프로그램 서버	모두 가능	Oracle EBS	Oracle 데이터베이스 포트	허용
Oracle EBS에 대한 보안 연결 기능이 있는 CMS	모두 가능	Oracle EBS	Oracle 데이터베이스 포트	허용
Oracle EBS에 대한 서버 측 데이터 연결 기능이 있는 BI 플랫폼 서버	모두 가능	Oracle EBS	Oracle 데이터베이스 포트	허용
Oracle EBS에 대한 클라이언트 측 데이터 연결 기능이 있는 Crystal Reports	모두 가능	Oracle EBS	Oracle 데이터베이스 포트	허용

6.17.4 PeopleSoft Enterprise 통합을 위한 방화벽 구성

PeopleSoft 엔터프라이즈와 통신하는 BI 플랫폼의 배포 환경은 다음과 같은 일반적인 통신 규칙을 준수해야 합니다.

- 보안 연결 구성 요소를 포함하는 중앙 관리 서버(CMS)가 PeopleSoft QAS(Query Acces) 웹 서비스와의 통신을 시작할 수 있어야 합니다.
- 데이터 연결 구성 요소를 포함하는 BI 플랫폼 서버가 PeopleSoft QAS 웹 서비스와의 통신을 시작할 수 있어야 합니다.
- 데이터 연결 클라이언트 구성 요소를 포함하는 Crystal Reports가 PeopleSoft QAS 웹 서비스와의 통신을 시작할 수 있어야 합니다.
- Enterprise Management(EPM) Bridge가 CMS 및 입력 파일 리포지토리 서버와 통신할 수 있어야 합니다.
- EPM Bridge가 ODBC 연결을 사용하여 PeopleSoft 데이터베이스와 통신할 수 있어야 합니다.

웹 서비스 포트 번호는 PeopleSoft Enterprise 도메인 이름에 지정된 포트와 동일합니다.

6.17.4.1 BI 플랫폼 서버의 포트 요구 사항

제품	서버 포트 요구 사항
SAP BusinessObjects Business Intelligence 플랫폼	<ul style="list-style-type: none"> BI 플랫폼 로그인 서버 포트

6.17.4.2 PeopleSoft의 포트 요구 사항

제품	포트 요구 사항	설명
PeopleSoft Enterprise: People Tools 8.46 이상	웹 서비스 HTTP/HTTPS 포트	이 포트는 PeopleSoft Enterprise for People Tools 8.46 이상의 솔루션에 SOAP 연결을 사용하는 경우에 필요합니다

6.17.4.3 BI 플랫폼과 PeopleSoft의 방화벽 구성

이 단원에서는 웹 응용 프로그램 서버와 다른 BI 플랫폼 서버가 방화벽으로 분리되어 있는 배포 시나리오에서 BI 플랫폼과 PeopleSoft Enterprise가 함께 작동하도록 구성하는 방법을 보여 줍니다.

BI 플랫폼 서버와 클라이언트의 방화벽 구성에 대한 자세한 내용은 BusinessObjects Business Intelligence 플랫폼 관리자 가이드를 참조하십시오.

BI 플랫폼의 방화벽 구성 외에 추가 구성을 일부 수행해야 합니다.

테이블6-18: PeopleSoft Enterprise: PeopleTools 8.46 이상의 경우

소스 컴퓨터	포트	대상 컴퓨터	포트	작업
PeopleSoft에 대한 보안 연결 기능이 있는 CMS	모두 가능	PeopleSoft	PeopleSoft 웹 서비스 HTTP/HTTPS 포트	허용
PeopleSoft에 대한 데이터 연결 기능이 있는 BI 플랫폼 서버	모두 가능	PeopleSoft	PeopleSoft 웹 서비스 HTTP/HTTPS 포트	허용
PeopleSoft에 대한 클라이언트 측 데이터 연결 기능이 있는 CrystalReports	모두 가능	PeopleSoft	PeopleSoft 웹 서비스 HTTP/HTTPS 포트	허용
EPM Bridge	모두 가능	CMS	CMS 이름 서버 포트	허용
EPM Bridge	모두 가능	CMS	CMS 요청 포트	허용
EPM Bridge	모두 가능	입력 파일 리포지토리 서버	입력 FRS 포트	허용
EPM Bridge	모두 가능	PeopleSoft	PeopleSoft 데이터베이스 포트	허용

6.17.5 Siebel 통합을 위한 방화벽 구성

이 단원에서는 방화벽으로 분리되어 있는 BI 플랫폼과 Siebel eBusiness 응용 프로그램 시스템 간의 통신에 사용되는 포트를 보여 줍니다.

- 웹 응용 프로그램이 Siebel용 BI 플랫폼 로그인 서버와의 통신을 시작할 수 있어야 합니다. Siebel용 엔터프라이즈 로그인 서버의 경우 다음 세 개의 포트가 필요합니다.
 1. Echo(TCP) 포트 7 - 로그인 서버에 대한 액세스 확인용
 2. Siebel용 BI 플랫폼 로그인 서버 포트(기본값: 8448) - CORBA IOR 수신 포트용
 3. 임의 POA 포트 - 제어할 수 없는 CORBA 통신용. 따라서 모든 포트가 열려 있어야 합니다.

- CMS가 Siebel용 BI 플랫폼 로그인 서버와의 통신을 시작할 수 있어야 합니다. 개별 로그인 서버마다 CORBA IOR 수신 포트가 구성되어 있습니다(예: 8448). 또한 BI 플랫폼을 설치할 때까지는 알려지지 않은 임의의 POA 포트 번호를 열어야 합니다.
- Siebel용 BI 플랫폼 로그인 서버가 SCBroker(Siebel Connection Broker) 포트(예: 2321)와의 통신을 시작할 수 있어야 합니다.
- BI 플랫폼 백엔드 서버(Siebel Data Access 구성 요소)가 SCBroker(Siebel Connection Broker) 포트(예: 2321)와의 통신을 시작할 수 있어야 합니다.
- Crystal Reports(Siebel Data Access 구성 요소)가 SCBroker(Siebel Connection Broker) 포트(예: 2321)와의 통신을 시작할 수 있어야 합니다.

포트에 대한 자세한 설명

이 단원에는 BI 플랫폼에서 사용되는 포트 목록이 나와 있습니다. 방화벽을 사용하는 BI 플랫폼을 배포하는 경우 이 정보를 이용하여 Siebel 통합을 위한 방화벽에서 열어야 할 포트 수를 최소화할 수 있습니다.

테이블6-19: BI 플랫폼 서버의 포트 요구 사항

제품	서버 포트 요구 사항
SAP BusinessObjects Business Intelligence 플랫폼	<ul style="list-style-type: none"> • BI 플랫폼 로그인 서버 포트

테이블6-20: Siebel의 포트 요구 사항

제품	포트 요구 사항	설명
Siebel eBusiness Application	2321	기본 SCBroker(Siebel Connection Broker) 포트

Siebel 통합을 위한 BI 플랫폼 방화벽 구성

이 단원에서는 웹 응용 프로그램 서버와 다른 플랫폼 서버가 방화벽으로 분리되어 있는 배포 시나리오에서 Siebel과 BI 플랫폼이 함께 작동하도록 방화벽을 구성하는 방법을 보여 줍니다.

소스 컴퓨터	포트	대상 컴퓨터	포트	작업
웹 응용 프로그램 서버	모두 가능	Siebel에 대한 BI 플랫폼 로그인 서버	모두 가능	허용
CMS	모두 가능	Siebel에 대한 BI 플랫폼 로그인 서버	모두 가능	허용
Siebel에 대한 BI 플랫폼 로그인 서버	모두 가능	Siebel	SCBroker 포트	허용

소스 컴퓨터	포트	대상 컴퓨터	포트	작업
Siebel에 대한 서버 측 데이터 연결 기능이 있는 BI 플랫폼 서버	모두 가능	Siebel	SCBroker 포트	허용
Siebel에 대한 클라이언트 측 데이터 연결 기능이 있는 CrystalReports	모두 가능	Siebel	SCBroker 포트	허용

6.18 BI 플랫폼 및 역방향 프록시 서버

하나 이상의 역방향 프록시 서버가 있는 환경에 BI 플랫폼을 배포할 수 있습니다. 역방향 프록시 서버는 일반적으로 단일 IP 주소만 전면에 내세운 채 웹 응용 프로그램 서버를 감출 목적으로 웹 응용 프로그램 서버 앞에 배포됩니다. 이 구성에서는 비공개 웹 응용 프로그램 서버로 보내야 할 모든 인터넷 트래픽을 역방향 프록시 서버를 통해 라우팅하여 개인 IP 주소를 숨깁니다.

역방향 프록시 서버는 공용 URL을 내부 URL로 변환하므로 내부 네트워크에 배포된 BI 플랫폼 웹 응용 프로그램의 URL을 사용하여 이 서버를 구성해야 합니다.

6.18.1 지원되는 역방향 프록시 서버

BI 플랫폼에서 지원되는 역방향 프록시 서버는 다음과 같습니다.

- IBM Tivoli Access Manager WebSEAL 6
- Apache 2.2
- Microsoft ISA 2006

6.18.2 웹 응용 프로그램 배포 방법 이해

BI 플랫폼 웹 응용 프로그램은 웹 응용 프로그램 서버에 배포되며, WDeploy 도구를 통해 설치 중 자동으로 배포됩니다. 이 도구를 통해 BI 플랫폼을 배포한 후 응용 프로그램을 수동으로 배포할 수도 있습니다. 웹 응용 프로그램은 기본 Windows 설치의 다음 디렉터리에 있습니다.

C:\Program Files (x86)\WSAP BusinessObjects\WSAP BusinessObjects Enterprise XI 4.0\Warfiles\Webapps

WDeploy로 다음 두 개의 특정 WAR 파일을 배포할 수 있습니다.

- BOE: 중앙 관리 콘솔(CMC), BI 실행 패드, Open Document가 포함되어 있습니다.
- dswsbobje: 웹 서비스 응용 프로그램이 포함되어 있습니다.

웹 응용 프로그램 서버가 역방향 프록시 서버 뒤에 있는 경우 WAR 파일의 올바른 컨텍스트 경로를 사용하여 역방향 프록시 서버를 구성해야 합니다. BI 플랫폼의 기능을 모두 표시하려면 배포된 모든 BI 플랫폼의 WAR 파일에 대해 컨텍스트 경로를 구성합니다.

6.19 BI 플랫폼 웹 응용 프로그램에 대해 역방향 프록시 서버 구성

BI 플랫폼 웹 응용 프로그램이 역방향 프록시 서버 뒤에 배포된 환경에서는 들어오는 URL 요청을 올바른 웹 응용 프로그램에 매핑하도록 역방향 프록시 서버를 구성해야 합니다.

이 단원에서는 지원되는 역방향 프록시 서버 중 일부에 대한 구체적인 구성 예제를 제공합니다. 자세한 내용은 역방향 프록시 서버 공급업체의 설명서를 참조하십시오.

6.19.1 역방향 프록시 서버 구성에 대한 자세한 지침

WAR 파일 구성

BI 플랫폼 웹 응용 프로그램은 웹 응용 프로그램 서버에 WAR 파일로 배포됩니다. 배포에 필요한 WAR 파일에 대한 지시문을 역방향 프록시 서버에서 구성해야 합니다. WDeploy를 사용하여 BOE 또는 dswsbobje WAR 파일을 배포할 수 있습니다. WDeploy에 대한 자세한 내용은 BI 플랫폼 웹 응용 프로그램 배포 가이드를 참조하십시오.

사용자 지정 구성 디렉터리에 BOE 속성 지정

BOE.war 파일에는 전역 속성 및 응용 프로그램별 속성이 포함되어 있습니다. 이러한 속성을 수정해야 하는 경우 사용자 지정 구성 디렉터리를 사용하십시오. 기본적으로 이 디렉터리는 C:\WProgram Files (x86)\WSAP BusinessObjects\WSAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOEW\WEB-INF\config\custom에 있습니다.

config\default 디렉터리의 속성은 수정하지 마십시오.

참고:

BI 플랫폼과 함께 제공되는 일부 웹 응용 프로그램 서버(예: Tomcat 버전)에서는 BOE.war에 직접 액세스할 수 있습니다. 이 경우 WAR 파일의 배포를 취소하지 않고 사용자 지정 설정을 직접 구성할 수 있습니다. BOE.war에 액세스할 수 없는 경우에는 파일을 배포 취소하고 사용자 지정한 다음 다시 배포해야 합니다.

'/' 문자의 일관된 사용

역방향 프록시 서버에 컨텍스트 경로를 정의할 때는 브라우저 URL을 입력할 때와 같은 방식을 사용합니다. 예를 들어, 지시문에서 역방향 프록시 서버의 미리 경로 끝에 '/'가 포함되어 있으면 브라우저 URL의 끝에도 '/'를 입력합니다.

역방향 프록시 서버의 지시문에서 소스 및 대상 URL에 '/' 문자를 일관되게 사용해야 합니다. '/' 문자를 소스 URL의 끝에 추가했으면 대상 URL의 끝에도 추가해야 합니다.

6.19.2 역방향 프록시 서버를 구성하려면

지원되는 역방향 프록시 서버의 백그라운드에서 작업하려면 BI 플랫폼 웹 응용 프로그램에 대해 아래 단계를 수행해야 합니다.

1. 공급업체의 지침과 배포의 네트워크 토폴로지에 따라 역방향 프록시 서버를 올바르게 설정합니다.
2. 필요한 BI 플랫폼 WAR 파일을 확인합니다.
3. 각 BI 플랫폼 WAR 파일에 대해 역방향 프록시 서버를 구성합니다. 각 유형의 역방향 프록시 서버마다 지정된 규칙이 다릅니다.
4. 필요한 구성을 모두 수행합니다. 일부 웹 응용 프로그램은 특정 웹 응용 프로그램 서버에 배포될 때 특별한 구성을 필요로 합니다.

6.19.3 BI 플랫폼에 대한 Apache 2.2 역방향 프록시 서버 구성

이 단원에서는 BI 플랫폼 및 Apache 2.2를 함께 사용하도록 구성하는 데 필요한 워크플로를 제공합니다.

1. BI 플랫폼과 Apache 2.2를 각기 별개의 컴퓨터에 설치해야 합니다.
2. 공급업체의 설명서에 따라 Apache 2.2를 설치하고 역방향 프록시 서버로 구성합니다.
3. 역방향 프록시 서버 뒤에 배포된 모든 WAR 파일에 대해 ProxyPass를 구성합니다.
4. 역방향 프록시 서버 뒤에 배포된 모든 웹 응용 프로그램에 대해 ProxyPassReverseCookiePath를 구성합니다.

6.19.4 BI 플랫폼에 대해 WebSEAL 6.0 역방향 프록시 서버 구성

이 단원에서는 BI 플랫폼과 WebSEAL 6.0을 함께 사용할 수 있도록 구성하는 방법을 설명합니다.

이 구성에는 내부 웹 응용 프로그램 서버나 웹 서버에 호스팅된 모든 BI 플랫폼 웹 응용 프로그램을 단일 탑재 지점으로 매핑하는 단일 표준 집합을 만드는 방법을 사용하는 것이 좋습니다.

1. BI 플랫폼과 WebSEAL 6.0을 각기 별개의 컴퓨터에 설치해야 합니다.
BI 플랫폼과 WebSEAL 6.0을 동일한 컴퓨터에 배포할 수도 있지만 이 방법은 사용하지 않는 것이 좋습니다. 이 배포 시나리오를 구성하는 데 필요한 지침은 WebSEAL 6.0 공급업체의 설명서를 참조하십시오.
2. 공급업체의 설명서에 따라 WebSeal 6.0을 설치하고 구성합니다.
3. WebSeal pdadmin 명령줄 유틸리티를 시작합니다. sec_master 같은 보안 도메인에 관리 권한이 있는 사용자로 로그인합니다.
4. pdadmin sec_master 프롬프트에 다음 명령을 입력합니다.

```
server task <instance_name-webseald-host_name>create -t
<type> -h <host_name> -p <port> <junction_point>
```

다음은 각 요소에 대한 설명입니다.

- <instance_name-webseald-host_name>은 설치된 WebSEAL 인스턴스의 전체 서버 이름입니다. 이 전체 서버 이름으로는 server list 명령의 출력에 표시되는 것과 같은 형식을 사용합니다.
- <type>은 집합 유형입니다. 집합이 내부 HTTP 포트에 매핑되는 경우에는 tcp를 사용합니다. 집합이 내부 HTTPS 포트에 매핑되는 경우에는 ssl을 사용합니다.
- <host_name>은 요청을 수신할 내부 서버의 DNS 호스트 이름이나 IP 주소입니다.
- <port>는 요청을 수신할 내부 서버의 TCP 포트입니다.
- <junction_point>는 내부 서버의 문서 공간이 탑재되는 WebSEAL 보호 개체 공간의 디렉터리입니다.

예제

```
server task default-webseald-webseal.rp.sap.com
create -t tcp -h 10.50.130.123 -p 8080/hr
```

6.19.5 BI 플랫폼에 대해 Microsoft ISA 2006 구성

이 단원에서는 BI 플랫폼과 ISA 2006을 함께 사용할 수 있도록 구성하는 방법을 설명합니다.

이 구성에는 내부 웹 응용 프로그램 서버나 웹 서버에 호스팅된 모든 BI 플랫폼 WAR 파일을 단일 탑재 지점으로 매핑하는 단일 표준 집합을 만드는 방법을 사용하는 것이 좋습니다. 웹 응용 프로그램 서버에 따라서는 응용 프로그램 서버를 추가로 구성해야 ISA 2006과 호환될 수 있습니다.

1. BI 플랫폼과 ISA 2006을 각기 별개의 컴퓨터에 설치해야 합니다.
BI 플랫폼과 ISA 2006을 동일한 컴퓨터에 배포할 수도 있지만 이 방법은 사용하지 않는 것이 좋습니다. 이러한 배포 시나리오를 구성하는 방법은 ISA 2006 설명서를 참조하십시오.
2. 공급업체의 설명서에 따라 ISA 2006을 설치하고 구성합니다.
3. ISA Server 관리 유틸리티를 시작합니다.
4. 탐색 패널을 사용하여 새 게시 규칙을 시작합니다.
 - a. 다음 위치로 이동합니다.
배열 > MachineName > 방화벽 설정 > 새로 만들기 > 웹 사이트 게시 규칙
 - 기억:**
MachineName을 ISA 2006이 설치된 컴퓨터의 이름으로 바꿉니다.
 - b. 웹 게시 규칙 이름에 규칙 이름을 입력하고 다음을 클릭합니다.
 - c. 규칙 동작으로 허용을 선택하고 다음을 클릭합니다.
 - d. 게시 유형으로 단일 웹 사이트 또는 부하 분산 장치 게시를 선택하고 다음을 클릭합니다.
 - e. ISA 서버와 게시된 웹 사이트 사이의 연결 유형을 선택하고 다음을 클릭합니다.
예를 들어, 보안되지 않은 연결을 사용하여 게시된 웹 서버 또는 서버 팜에 연결을 선택합니다.
 - f. 내부 사이트 이름에 게시하는 웹 사이트의 내부 이름(예: BI 플랫폼을 호스팅하는 컴퓨터 이름)을 입력하고 다음을 클릭합니다.
 - 참고:**
ISA 2006을 호스팅하는 컴퓨터에서 대상 서버에 연결할 수 없는 경우 컴퓨터 이름 또는 IP 주소를 사용하여 게시된 서버에 연결을 선택하고 해당 필드에 이름이나 IP 주소를 입력합니다.
 - g. 공개 이름 정보에서 도메인 이름(예: 모든 도메인 이름)을 선택하고 내부 게시 정보(예: /*)를 지정합니다. 다음을 클릭합니다.
이제 들어오는 웹 요청을 모니터링할 새 웹 수신기를 만들어야 합니다.
5. 새로 만들기를 클릭하여 새 웹 수신기 정의 마법사를 시작합니다.

- a. 웹 수신기 이름에 이름을 입력하고 다음을 클릭합니다.
 - b. ISA 서버와 게시된 웹 사이트 사이의 연결 유형을 선택하고 다음을 클릭합니다.
예를 들어, 클라이언트와의 SSL 보안 연결 필요 없음을 선택합니다.
 - c. 웹 수신기 IP 주소 섹션에서 아래 항목을 선택하고 다음을 클릭합니다.
 - 내부
 - 외부
 - 로컬 호스트
 - 모든 네트워크
 이제 HTTP를 통해서만 게시하도록 ISA Server가 구성되었습니다.
 - d. 인증 설정 옵션을 선택하고 다음, 마침을 차례로 클릭합니다.
이제 웹 게시 규칙에 따라 새 수신기가 구성되었습니다.
6. 사용자 집합,에서 다음을 클릭한 다음 완료를 클릭합니다.
 7. 적용을 클릭하여 웹 게시 규칙의 모든 설정을 저장하고 ISA 2006 구성을 업데이트합니다.
이제 웹 게시 규칙의 속성을 업데이트하여 웹 응용 프로그램의 경로를 매핑해야 합니다.
 8. 탐색 패널에서 앞서 구성한 방화벽 설정을 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.
 9. 경로 탭에서 추가를 클릭하여 SAP BusinessObjects 웹 응용 프로그램의 경로를 매핑합니다.
 10. 공개 이름 탭에서 다음 웹 사이트에 대한 요청을 선택하고 추가를 클릭합니다.
 11. 공개 이름 대화 상자에 ISA 2006 서버 이름을 입력하고 확인을 클릭합니다.
 12. 적용을 클릭하여 웹 게시 규칙의 모든 설정을 저장하고 ISA 2006 구성을 업데이트합니다.
 13. 다음 URL에 액세스하여 연결을 확인합니다.

http://<ISA Server 호스트 이름>:<웹 수신기 포트 번호>/<응용 프로그램의 외부 경로>

예: http://myISAserver:80/Product/BOE/CMC

참고:

브라우저를 몇 차례 새로 고쳐야 할 수 있습니다.

방금 구성한 규칙에 대한 HTTP 정책을 수정해야 CMC에 로그인할 수 있습니다. ISA Server 관리 유틸리티에서 작성한 규칙을 마우스 오른쪽 단추로 클릭하고 HTTP 구성을 선택합니다. 이제 URL 보호 영역에서 정규화 확인의 선택을 취소해야 합니다.

BI 플랫폼에 원격으로 액세스하려면 액세스 규칙을 만들어야 합니다.

6.20 역방향 프록시 배포에서 BI 플랫폼에 대한 특수 구성

일부 BI 플랫폼 제품은 역방향 프록시 배포에서 올바르게 작동하기 위해 추가 구성을 필요로 합니다. 이 단원에서는 추가 구성을 수행하는 방법을 설명합니다.

6.20.1 웹 서비스에 대해 역방향 프록시 활성화

이 단원에서는 웹 서비스에 대해 역방향 프록시를 활성화하는 데 필요한 절차에 대해 설명합니다.

6.20.1.1 Tomcat 6에서 역방향 프록시 사용

Tomcat 웹 응용 프로그램 서버에서 역방향 프록시를 활성화하려면 server.xml 파일을 수정해야 합니다. 이를 위해서는 proxyPort를 역방향 프록시 서버 수신 포트로 설정하고 새 proxyName을 추가하는 등의 수정 작업을 수행해야 합니다. 이 단원에서는 구체적인 절차를 설명합니다.

1. Tomcat 실행을 중지합니다.
2. Tomcat의 server.xml을 엽니다.

Windows의 경우 server.xml은 C:\Program Files (x86)\WSAP BusinessObjects\Tomcat6\conf에 있습니다.

UNIX의 경우 server.xml은 <CATALINA_HOME>/conf에 있습니다. <CATALINA_HOME>의 기본 값은 <INSTALLDIR>/bobje/tomcat55입니다.

3. server.xml 파일에서 다음 섹션을 찾습니다.

```
<!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
<!--See proxy documentation for more information about using
this.-->
<!--
<Connector port="8082"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false"
acceptCount="100" debug="0" connectionTimeout="20000"
proxyPort="80" disableUploadTimeout="true" />
-->
```

4. <!-- and -->를 제거하여 Connector 요소의 주석을 없앱니다.
5. 역방향 프록시 서버 수신 포트가 되도록 proxyPort의 값을 수정합니다.
6. Connector의 특성 목록에 새 proxyName 특성을 추가합니다. proxyName의 값은 Tomcat에서 올바른 IP 주소로 확인할 수 있는 프록시 서버 이름이어야 합니다.

예:

```
<!--Define a Proxied HTTP/1.1 Connector on port 8082 -->
<!--See proxy documentation for more information about using
this.-->
<Connector port="8082"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false"
```

```
acceptCount="100" debug="0" connectionTimeout="20000"
proxyName="my_reverse_proxy_server.domain.com"
proxyPort="ReverseProxyServerPort"
disableUploadTimeout="true" />
```

여기서 my_reverse_proxy_server.domain.com과 ReverseProxyServerPort 자리에는 올바른 역방향 프록시 서버 이름과 해당 수신 포트를 대신 입력합니다.

7. server.xml 파일을 저장하고 닫습니다.
8. Tomcat을 다시 시작합니다.
9. 역방향 프록시 서버에서 해당 가상 경로를 올바른 Tomcat 커넥터 포트에 매핑하는지 확인합니다. 위의 예제에서 포트는 8082입니다.

다음 예제에서는 Tomcat에 배포된 Business Objects 웹 서비스에 대해 역방향 프록시를 사용하는 Apache HTTP Server 2.2의 샘플 구성을 보여 줍니다.

```
ProxyPass /XI3.0/dswsbobje http://internalServer:8082/dswsbobje
ProxyPassReverseCookiePath /dswsbobje /XI3.0/dswsbobje
```

웹 서비스를 사용하려면 커넥터의 프록시 이름과 포트 번호가 확인되어야 합니다.

6.20.1.2 Tomcat 이외의 웹 응용 프로그램 서버에서 웹 서비스에 대해 역방향 프록시 활성화

다음 절차를 수행하려면 선택한 웹 응용 프로그램 서버에 맞게 BI 플랫폼 웹 응용 프로그램을 구성해야 합니다. wsresources는 대/소문자를 구분합니다.

1. 웹 응용 프로그램 서버를 중지합니다.
2. dsws.properties 파일에서 Web Services의 외부 URL을 지정합니다.

이 파일은 dswsbobje 웹 응용 프로그램에 있습니다. 예를 들어 외부 URL이 http://my_reverse_proxy_server.domain.com/dswsbobje/인 경우 dsws.properties 파일에서 다음 속성을 업데이트합니다.

- wsresource1=ReportEngine|reportengine web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/ReportEngine
- wsresource2=BICatalog|bicatalog web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/BICatatalog
- wsresource3=Publish|publish web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/Publish
- wsresource4=QueryService|query web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/QueryService
- wsresource5=BIPlatform|BIPlatform web service|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/BIPlatform

- wsresource6=LiveOffice|Live Office web service|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/LiveOffice

3. dsws.properties 파일을 저장하고 닫습니다.
4. 웹 응용 프로그램 서버를 다시 시작합니다.
5. 역방향 프록시 서버에서 해당 가상 경로를 올바른 웹 응용 프로그램 서버 커넥터 포트에 매핑하는지 확인합니다. 다음 예제에서는 선택한 웹 응용 프로그램 서버에 배포된 BI 플랫폼 웹 서비스에 대해 역방향 프록시를 사용하는 Apache HTTP Server 2.2의 샘플 구성을 보여 줍니다.

```
ProxyPass /SAP/dswsbobje http://internalServer:<listening port> /dswsbobje
```

```
ProxyPassReverseCookiePath /dswsbobje /SAP/dswsbobje
```

여기서 <listening port>는 웹 응용 프로그램 서버의 수신 포트입니다.

6.20.2 ISA 2006의 세션 쿠키에 대한 루트 경로 활성화

이 단원에서는 특정 웹 응용 프로그램 서버를 구성하여 ISA 2006을 역방향 프록시 서버로 사용하도록 세션 쿠키에 대한 루트 경로를 활성화하는 방법에 대해 설명합니다.

6.20.2.1 Apache Tomcat 6 구성

세션 쿠키가 ISA 2006과 함께 역방향 프록시 서버로 작동하도록 루트 경로를 구성하려면 server.xml의 <Connector> 요소에 다음을 추가합니다.

```
emptySessionPath="true"
```

1. Tomcat을 중지합니다.
2. 다음 위치에 있는 server.xml을 엽니다.
<CATALINA_HOME>\wconf
3. server.xml 파일에서 다음 섹션을 찾습니다.

```
<!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
<!-- See proxy documentation for more information about using this -->
<!--
<Connector port="8082"
maxThreads="150" minSpareThreads="25" maxS
pareThreads="75" enableLookups="false"
acceptCount="100" debug="0" connectionTimeout="20000"
proxyPort="80" disableUploadTimeout="true" />
```

```
-->
```

4. <!-- 및 -->를 제거하여 Connector 요소의 주석을 없앱니다.
5. 세션 쿠키가 ISA 2006과 함께 역방향 프록시 서버로 작동하도록 루트 경로를 구성하려면 server.xml의 <Connector> 요소에 다음을 추가합니다.

```
emptySessionPath="true"
```

6. 역방향 프록시 서버 수신 포트가 되도록 proxyPort의 값을 수정합니다.
7. Connector의 특성 목록에 새 proxyName 특성을 추가합니다. 값은 Tomcat에서 올바른 IP 주소로 확인할 수 있는 프록시 서버 이름이어야 합니다.
예를 들면 다음과 같습니다.

```
<!--Define a Proxied HTTP/1.1 Connector on port 8082
-->
<!-- See proxy documentation for more information about using
this -->
<Connector port="8082"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" emptySessionPath="true"
acceptCount="100" debug="0" connectionTimeout="20000"
proxyName="my_reverse_proxy_server.domain.com"
proxyPort="ReverseProxyServerPort"
disableUploadTimeout="true" />
```

8. server.xml 파일을 저장하고 닫습니다.
9. Tomcat을 다시 시작합니다.

역방향 프록시 서버에서 해당 가상 경로를 올바른 Tomcat 커넥터 포트에 매핑하는지 확인합니다. 위의 예제에서 포트는 8082입니다.

6.20.2.2 Sun Java 8.2를 구성하려면

모든 BI 플랫폼 웹 응용 프로그램의 sun-web.xml을 수정해야 합니다.

1. <SUN_WEBAPP_DOMAIN>WgeneratedWxmlWj2ee-modulesWwebappsWBOEWWEB-INF로 이동합니다.
2. sun-web.xml을 엽니다.
3. <context-root> 컨테이너 뒤에 다음을 추가합니다.

```
<session-config>
  <cookie-properties>
    <property name="cookiePath" value="/" />
  </cookie-properties>
</session-config>
<property name="reuseSessionID" value="true"/>
```

4. sun-web.xml을 저장하고 닫습니다.
5. 모든 웹 응용 프로그램에 대해 1-4단계를 반복합니다.

6.20.2.3 Oracle Application Server 10gR3을 구성하려면

모든 BI 플랫폼 웹 응용 프로그램의 배포 디렉터리에서 global-web-application.xml 또는 orion-web.xml을 수정해야 합니다.

1. <ORACLE_HOME>Wj2eeWhomeWconfigW로 이동합니다.
2. global-web-application.xml 또는 orion-web.xml을 엽니다.
3. <orion-web-app> 컨테이너에 다음 줄을 추가합니다.

```
<session-tracking cookie-path="/" />
```

4. 구성 파일을 저장하고 닫습니다.
5. Oracle Admin Console에 로그인합니다.
 - a. OC4J:home > Administration > Server Properties 로 이동합니다.
 - b. Command Line Options 아래에서 Options를 선택합니다.
 - c. Add another Row를 클릭하고 다음을 입력합니다.

```
Doracle.useSessionIDFromCookie=true
```

6. Oracle 서버를 다시 시작합니다.

6.20.2.4 WebSphere Community Edition 2.0을 구성하려면

1. WebSphere Community Edition 2.0 Admin Console을 엽니다.
2. 왼쪽 탐색 패널에서 Server(서버)를 찾아 Web Server(웹 서버)를 선택합니다.
3. 커넥터를 선택하고 편집을 클릭합니다.
4. emptySessionPath 확인란을 선택하고 Save(저장)를 클릭합니다.
5. ProxyName에 ISA 서버 이름을 입력합니다.
6. ProxyPort에 ISA 수신기 포트 번호를 입력합니다.
7. 커넥터를 중지하고 다시 시작합니다.

6.20.3 SAP BusinessObjects Live Office의 역방향 프록시 활성화

역방향 프록시에 대한 SAP BusinessObjects Live Office 웹 브라우저에서 개체 보기 기능을 활성화하려면 기본 뷰어 URL을 조정합니다. 이 작업은 중앙 관리 콘솔(CMC) 또는 Live Office 옵션을 통해 수행할 수 있습니다.

참고:

이 단원에서는 BI 실행 패드 및 BI 플랫폼 웹 서비스에 대해 역방향 프록시가 성공적으로 활성화되었다고 가정됩니다.

6.20.3.1 CMC를 사용하여 기본 뷰어 URL을 조정하려면

1. CMC에 로그인합니다.
2. 응용 프로그램 페이지로 이동하여 CMC를 클릭합니다.
3. 작업 메뉴에서 처리 확장을 선택합니다.
4. URL 필드에서 올바른 기본 뷰어 URL을 설정하고 URL 설정을 클릭합니다. 예를 들면 다음과 같습니다.

```
http://ReverseProxyServer:ReverseProxyServerPort/BOE/OpenDocument.jsp?slDType=CUID&iDo  
cID=%SI_CUID%
```

여기서 ReverseProxyServer와 ReverseProxyServerPort는 올바른 역방향 프록시 서버 이름과 해당 수신 포트를 가리킵니다.

장7 인증

7.1 BI 플랫폼의 인증 옵션

인증은 시스템에 액세스하려는 사용자의 ID를 확인하는 프로세스이고, 권한 부여는 지정된 개체에 대해 요청한 작업을 수행하는 데 필요한 권한이 사용자에게 부여되어 있는지 확인하는 프로세스입니다.

보안 플러그인을 사용하면 더 다양한 방식으로 BI 플랫폼에서 사용자를 인증하고 인증 방식을 사용자 지정할 수도 있습니다. 보안 플러그인을 통해 타사 시스템에서 해당 플랫폼 서비스로 사용자 계정과 그룹을 매핑할 수 있으므로 계정을 만들고 관리하는 작업을 손쉽게 수행할 수 있습니다. 타사 사용자 계정 또는 그룹을 기존의 BI 플랫폼 사용자 계정 또는 그룹에 매핑하거나, 외부 시스템에서 매핑되는 각 항목에 해당하는 Enterprise 사용자 계정 또는 그룹을 새로 만들 수 있습니다.

현재 릴리스에서는 다음과 같은 인증 방법을 지원합니다.

- Enterprise
- LDAP
- Windows AD
- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

BI 플랫폼은 다양하게 사용자 지정할 수 있으므로 시스템마다 인증 및 그 프로세스가 다를 수 있습니다.

관련 항목

- 333 페이지에서 [JD Edwards EnterpriseOne 인증 사용](#)"
- 345 페이지에서 [Oracle EBS 인증 사용](#)"
- 315 페이지에서 [PeopleSoft Enterprise 인증 사용](#)"
- 339 페이지에서 [Siebel 인증 사용](#)"

7.1.1 기본 인증

기본 인증은 사용자가 처음으로 시스템에 액세스하려 할 때 진행됩니다. 다음 두 작업 중 하나가 기본 인증 중에 수행됩니다.

- 단일 로그인에 구성되지 않은 경우 사용자가 자신의 사용자 이름, 암호 및 인증 형식과 같은 자격 증명을 제공합니다.
이러한 세부 정보는 사용자가 로그인 화면에서 입력합니다.
- 단일 로그인 방법이 구성된 경우에는 사용자에 대한 자격 증명이 자동으로 전파됩니다.
이러한 세부 정보는 Kerberos, SiteMinder와 같은 다른 방법을 사용하여 추출됩니다.
- 인증 유형은 중앙 관리 콘솔(CMC)의 인증 관리 영역에서 활성화하여 설정한 유형에 따라 Enterprise, LDAP, Windows AD, SAP, Oracle EBS, Siebel, JD Edwards EnterpriseOne, PeopleSoft Enterprise일 수 있습니다. 사용자의 웹 브라우저에서는 HTTP를 통해 웹 서버로 정보를 보내고 웹 서버에서는 CMS 또는 해당 플랫폼 서버로 정보를 보냅니다.

웹 응용 프로그램 서버에서는 서버 측 스크립트를 통해 사용자 정보를 전달합니다. 내부적으로 이 스크립트는 SDK와 통신하고 궁극적으로는 적절한 보안 플러그 인이 사용자 데이터베이스를 기준으로 사용자를 인증합니다.

예를 들어, 사용자가 BI 실행 패드에 로그인하여 Enterprise 인증을 지정하면 SDK를 통해 BI 플랫폼 보안 플러그 인에서 인증이 수행됩니다. 중앙 관리 서버(CMS)에서는 BusinessObjects Enterprise 보안 플러그 인을 사용하여 시스템 데이터베이스를 기준으로 사용자 이름과 암호를 확인합니다. 또는 사용자가 인증 방법을 지정하면 SDK에서 해당 보안 플러그 인을 사용하여 사용자를 인증합니다.

보안 플러그 인에서 자격 증명이 일치한다고 보고하면 CMS는 사용자에게 활성 시스템 ID를 부여하고 다음과 같은 작업이 수행됩니다.

- CMS는 사용자에 대한 Enterprise 세션을 만듭니다. 세션이 활성 상태여서 이 세션에는 시스템의 사용자 라이선스 하나가 사용됩니다.
- CMS는 로그인 토큰을 생성하고 인코딩하여 웹 응용 프로그램 서버로 보냅니다.
- 웹 응용 프로그램 서버는 메모리의 사용자의 정보를 세션 변수에 저장합니다. 활성 상태에서 이 세션은 BI 플랫폼이 사용자의 요청에 응답하는 데 필요한 정보를 저장합니다.

참고:

세션 변수에는 사용자의 암호가 포함되지 않습니다.

- 웹 응용 프로그램 서버는 클라이언트 브라우저의 쿠키에 로그인 토큰을 유지합니다. 이 로그인 토큰은 클러스터링된 CMS가 있는 경우 또는 세션 선호도를 위해 BI 실행 패드가 클러스터링된 경우처럼 장애 조치 목적으로만 사용됩니다.

참고:

로그인 토큰을 비활성화할 수는 있으나, 로그인 토큰을 비활성화하면 장애 조치가 비활성화됩니다.

7.1.2 보안 플러그 인

보안 플러그 인을 사용하면 더 다양한 방식으로 BI 플랫폼에서 사용자를 인증할 수 있고 인증 방식을 사용자 지정할 수도 있습니다. 현재 BI 플랫폼과 함께 제공되는 플러그 인은 다음과 같습니다.

- Enterprise
- LDAP
- Windows AD
- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

보안 플러그인을 통해 타사 시스템에서 BI 플랫폼으로 사용자 계정과 그룹을 매핑할 수 있으므로 계정을 만들고 관리하는 작업을 손쉽게 수행할 수 있습니다. 타사 사용자 계정 또는 그룹을 기존의 BI 플랫폼 사용자 계정 또는 그룹에 매핑하거나, 외부 시스템에서 매핑되는 각 항목에 해당하는 Enterprise 사용자 계정 또는 그룹을 새로 만들 수 있습니다.

보안 플러그 인은 타사 사용자 및 그룹 목록을 동적으로 관리합니다. 외부 그룹을 BI 플랫폼에 매핑하면 해당 그룹에 속한 모든 사용자가 BI 플랫폼에 로그인할 수 있습니다. 이후에 타사 그룹 멤버를 변경하더라도 BI 플랫폼에서 목록을 업데이트하거나 새로 고칠 필요가 없습니다. 예를 들어 LDAP 그룹을 BI 플랫폼에 매핑한 다음 새 사용자를 그룹에 추가하면, 이 새로운 사용자가 유효한 LDAP 자격 증명을 사용하여 BI 플랫폼에 처음으로 로그인할 때 보안 플러그 인에서 사용자의 별칭을 동적으로 지정합니다.

또한 보안 플러그 인을 사용하면 매핑된 사용자와 그룹이 Enterprise 계정처럼 처리되므로 일관된 방식으로 사용자와 그룹에 권한을 할당할 수 있습니다. 예를 들어, Windows AD의 일부 사용자 계정 또는 그룹과 LDAP 디렉터리 서버의 일부 사용자 계정 또는 그룹을 매핑할 수 있습니다. 그런 다음 BI 플랫폼 내에서 권한을 할당하거나 새로운 사용자 지정 그룹을 만들어야 하는 경우에는 CMC에서 모든 필요한 사항을 설정할 수 있습니다.

각 보안 플러그 인은 적절한 사용자 데이터베이스를 기준으로 사용자 자격 증명을 확인하는 인증 공급자의 역할을 합니다. BI 플랫폼에 로그인할 때 사용자는 CMC의 권한 부여 관리 영역에서 활성화 및 설정되어 있는 사용 가능한 인증 형식 중 하나를 선택합니다.

참고:

BI 플랫폼 서버 구성 요소가 UNIX에서 실행 중인 경우에는 Windows AD 보안 플러그 인이 사용자를 인증할 수 없습니다.

7.1.3 BI 플랫폼에 대한 단일 로그인

BI 플랫폼에 대한 단일 로그인은 사용자가 일단 운영 체제에 로그인하면 자격 증명을 다시 제공하지 않아도 SSO가 지원되는 응용 프로그램에 액세스할 수 있음을 의미합니다. 사용자가 로그인하면 해당 사용자에 대한 보안 컨텍스트가 만들어집니다. 이 컨텍스트는 SSO를 수행하여 사용자가 자신에 해당하는 사용자로 로그인할 수 있도록 BI 플랫폼에 전파될 수 있습니다.

익명 단일 로그인이라는 용어도 BI 플랫폼에 대한 단일 로그인을 말하지만 좀더 구체적으로 설명하면 Guest 사용자 계정에 대한 단일 로그인 기능을 말합니다. Guest 사용자 계정이 활성화되면(기본값) 누구나 BI 플랫폼에 Guest로 로그인할 수 있으며 이 시스템에 대한 액세스 권한을 갖게 됩니다.

7.1.3.1 단일 로그인 지원

단일 로그인이라는 용어는 다양한 시나리오를 기술하는 데 사용됩니다. 가장 기본적인 의미에서 단일 로그인이란 사용자가 로그인 자격 증명을 한 번만 제공하고 둘 이상의 응용 프로그램 또는 시스템에 액세스할 수 있는 기능을 말합니다. 따라서 이 기능을 사용하면 사용자는 시스템과 쉽게 상호 작용할 수 있습니다.

응용 프로그램 서버 유형 및 운영 체제에 따라 다른 인증 도구나 BI 플랫폼에서 BI 실행 패드에 대한 단일 로그인을 제공할 수 있습니다.

이러한 단일 로그인 방법은 Windows에서 Java 응용 프로그램을 사용하는 경우에 지원됩니다.

- Kerberos를 사용한 Windows AD
- SiteMinder 사용 Windows AD

이러한 단일 로그인 방법은 Windows에서 IIS를 사용하는 경우에 지원됩니다.

- Kerberos를 사용한 Windows AD
- NTLM을 사용한 Windows AD
- SiteMinder를 사용한 Windows AD

이러한 단일 로그인 방법은 플랫폼에 대해 웹 응용 프로그램 서버를 지원하는 Windows 또는 Unix에서 사용할 수 있습니다.

- SiteMinder를 사용한 LDAP
- 신뢰할 수 있는 인증
- Kerberos를 사용한 Windows AD

참고:

Kerberos를 사용한 Windows AD는 UNIX에서 Java 응용 프로그램을 사용하는 경우에 지원됩니다. 그러나 BI 플랫폼 서비스는 Windows 서버에서 실행해야 합니다.

다음 표에는 BI 실행 패드의 단일 로그인 지원 방법에 대한 설명이 나와 있습니다.

인증 모드	CMS 서버	옵션	참고
Windows AD	Windows 전용	Kerberos를 사용한 Windows AD 전용	BI 실행 패드와 CMC에 대한 Windows AD 인증은 기본적으로 제공됩니다.
LDAP	지원되는 모든 플랫폼	지원되는 LDAP 디렉터리 서버, Site-Minder 전용	BI 실행 패드 및 CMC에 대한 LDAP 인증은 기본적으로 제공됩니다. InfoView와 CMC에 대한 SSO에는 SiteMinder가 필요합니다.
Enterprise	지원되는 모든 플랫폼	신뢰할 수 있는 인증	BI 실행 패드 및 CMC에 대한 Enterprise 인증은 기본적으로 제공됩니다. InfoView와 CMC에 대한 Enterprise 인증을 사용한 SSO에는 신뢰할 수 있는 인증이 필요합니다.

- 213 페이지에서 ["BI 플랫폼에 대한 단일 로그인"](#)
- 215 페이지에서 ["데이터베이스에 대한 단일 로그인"](#)
- 215 페이지에서 ["종단 간 단일 로그인"](#)

7.1.3.2 데이터베이스에 대한 단일 로그인

사용자는 BI 플랫폼에 로그인한 후 로그인 자격 증명을 다시 제공하지 않아도 데이터베이스에 대한 단일 로그인을 통해 데이터베이스 액세스가 필요한 작업(예: 보고서 보기 및 새로 고침)을 수행할 수 있습니다. 데이터베이스에 대한 단일 로그인과 BI 플랫폼에 대한 단일 로그인을 함께 사용하면 필요한 리소스에 보다 쉽게 액세스할 수 있습니다.

7.1.3.3 종단 간 단일 로그인

종단 간 단일 로그인은 사용자가 프런트 엔드에서 BI 플랫폼에 대한 단일 로그인 액세스 권한을 갖고 백 엔드에서 데이터베이스에 대한 단일 로그인 액세스 권한을 갖는 구성을 말합니다. 따라서 사용자는 운영 체제에 로그인할 때 로그인 자격 증명을 한 번만 제공하면 BI 플랫폼에 액세스할 수 있으며 보고서 보기와 같이 데이터베이스 액세스가 필요한 작업도 수행할 수 있습니다.

BI 플랫폼에서는 Windows AD 및 Kerberos를 통해 종단 간 단일 로그인이 지원됩니다.

7.2 Enterprise 인증

7.2.1 Enterprise 인증 개요

Enterprise 인증은 BI 플랫폼의 기본 인증 방법으로, 시스템을 처음 설치하면 자동으로 활성화되며 비활성화할 수는 없습니다. 사용자 및 그룹을 추가하고 관리할 때 BI 플랫폼의 데이터베이스에 사용자 및 그룹 정보가 유지됩니다.

팁:

BI 플랫폼에 사용할 고유한 계정과 그룹을 만들려는 경우 또는 타사 디렉터리 서버에 사용자와 그룹 계층 구조를 아직 설정하지 않은 경우에는 시스템 기본값인 Enterprise 인증을 사용하십시오.

Enterprise 인증은 구성하거나 활성화할 필요가 없습니다. 하지만 조직의 보안 요구 사항을 충족하기 위해 Enterprise 인증의 설정을 수정할 수는 있습니다. Enterprise 인증의 설정은 중앙 관리 콘솔(CMC)에서 수정할 수 있습니다.

7.2.2 Enterprise 인증 설정

설정	옵션	설명
암호 제한		
	암호에 대/소문자를 혼용해야 함	이 옵션을 적용하면 대문자, 소문자, 숫자 또는 문장 부호 중 적어도 두 가지 이상을 암호에 포함시켜야 합니다.
	N개 이상의 문자를 포함해야 함	암호의 복잡한 정도를 설정할 때 그 최소 수준을 강화하면 악의적인 사용자가 유효한 사용자 암호를 쉽게 추측하지 못하도록 할 수 있습니다.
사용자 제한		
	N일마다 암호를 변경해야 함	이 옵션은 암호가 취약해지기 전에 정기적으로 바꾸도록 합니다.
	최근 N개의 암호는 다시 사용할 수 없음	이 옵션은 암호를 돌려가며 사용하지 못하도록 합니다.
	암호를 변경하려면 N분을 기다려야 함	이 옵션은 새 암호를 시스템에 입력한 후 바로 바꿀 수 없도록 합니다.
로그온 제한		
	로그온에 N번 실패하면 계정을 사용할 수 없음	이 보안 옵션은 계정이 비활성화되기 전에 사용자가 시도할 수 있는 시스템 로그온 시도 횟수를 지정합니다.
	실패한 로그온 횟수를 N분 후에 재설정	이 옵션은 로그온 시도 카운터를 재설정하는 시간 간격을 지정합니다.
	N분 후에 계정을 다시 사용할 수 있음	이 옵션은 로그온 시도를 N번 실패한 후 계정을 일시 중지하는 기간을 지정합니다.
로그온할 때 데이터 소스 자격 증명 동기화		
	로그온 시 사용자의 데이터 소스 자격 증명 활성화 및 업데이트	이 옵션은 사용자가 로그인한 후 데이터 소스 자격 증명을 활성화합니다.
신뢰할 수 있는 인증		신뢰할 수 있는 인증에 대한 설정을 제공합니다.

관련 항목

- 219 페이지에서 [신뢰할 수 있는 인증 활성화](#)

7.2.3 Enterprise 설정 변경

1. CMC의 인증 관리 영역으로 이동합니다.
2. Enterprise를 두 번 클릭합니다.
Enterprise 대화 상자가 나타납니다.
3. 설정을 변경합니다.

팁:

모든 설정을 기본값으로 되돌리려면 재설정을 클릭합니다.

4. 업데이트를 클릭하여 수정 내용을 저장합니다.

7.2.3.1 일반 암호 설정 변경

1. CMC의 인증 관리 영역으로 이동합니다.
2. Enterprise를 두 번 클릭합니다.
Enterprise 대화 상자가 나타납니다.
3. 사용할 각 암호 설정에 대한 확인란을 선택하고 필요한 경우 값을 지정합니다.
다음 표에는 구성할 수 있는 각 암호 관련 설정의 최대값과 최소값이 정리되어 있습니다.

테이블 7-1: 암호 설정

암호 설정	최소값	권장 최대값
암호에 대/소문자를 혼용해야 함	N/A	N/A
N개 이상의 문자를 포함해야 함	0자	64자
N일마다 암호를 변경해야 함	1일	100일
최근 N개의 암호는 다시 사용할 수 없음	암호 1개	암호 100개
암호를 변경하려면 N분을 기다려야 함	0분	100분

암호 설정	최소값	권장 최대값
로그온에 N번 실패하면 계정을 사용할 수 없음	1번 실패	100번 실패
실패한 로그온 횟수를 N분 후에 재설정	1분	100분
N분 후에 계정을 다시 사용할 수 있음	0분	100분

4. 업데이트를 클릭합니다.

7.2.4 신뢰할 수 있는 인증 활성화

엔터프라이즈 신뢰할 수 있는 인증은 웹 응용 프로그램 서버를 사용하여 사용자 ID를 확인하는 방식으로 단일 로그온을 수행하는 데 사용됩니다. 이 인증 방법은 중앙 관리 서버(CMS)와 BI 플랫폼 웹 응용 프로그램을 호스팅하는 웹 응용 프로그램 서버 간에 신뢰를 설정하는 것과 관련이 있습니다. 신뢰가 설정되면 시스템 대신 웹 응용 프로그램에서 사용자의 ID를 확인합니다. 신뢰할 수 있는 인증을 통해 SAML, x.509 등의 인증 방법 및 전용 인증 플러그 인이 없는 다른 방법을 지원할 수 있습니다.

사용자는 세션 중 암호를 여러 번 제공할 필요 없이 시스템에 한 번만 로그인하는 것을 선호합니다. 신뢰할 수 있는 인증은 BI 플랫폼 인증 솔루션을 타사 인증 솔루션과 통합하기 위한 Java 단일 로그인 솔루션을 제공합니다. 중앙 관리 서버(CMS)에 대한 신뢰가 설정된 응용 프로그램에서는 신뢰할 수 있는 인증을 통해 사용자가 암호를 입력하지 않고도 로그인할 수 있습니다.

신뢰할 수 있는 인증을 사용하려면 Enterprise 인증 설정을 통해 서버의 공유 암호를 구성해야 하고, 클라이언트는 BOE war 파일에 지정된 속성을 통해 구성되어 있습니다.

참고:

- 신뢰할 수 있는 인증을 사용하려면 Enterprise 사용자를 만들거나 BI 플랫폼에 로그인해야 하는 타사 사용자를 매핑해야 합니다.
- BI 실행 패드의 단일 로그온 URL은 `http://server:port/BOE/BI`입니다.

관련 항목

- 220 페이지에서 [신뢰할 수 있는 인증을 사용하도록 서버 구성](#)"
- 223 페이지에서 [웹 응용 프로그램에 대해 신뢰할 수 있는 인증 구성](#)"

7.2.4.1 신뢰할 수 있는 인증을 사용하도록 서버 구성

신뢰할 수 있는 인증을 사용하려면 그 전에 Enterprise 사용자가 만들어져 있거나 BI 플랫폼에 로그인할 타사 사용자를 매핑한 상태여야 합니다.

1. CMC에 로그인합니다.
2. 인증 관리 영역으로 이동합니다.
3. Enterprise 옵션을 클릭합니다.
Enterprise 대화 상자가 열립니다.
4. 신뢰할 수 있는 인증이 나타날 때까지 아래로 스크롤합니다.
 - a. 신뢰할 수 있는 인증 사용을 클릭합니다.
 - b. 새 공유 암호를 클릭합니다.
다음 메시지가 표시됩니다.
공유 암호 키가 생성되어 다운로드할 준비가 되었습니다.
 - c. 공유 암호 다운로드를 클릭합니다.

참고:

공유 암호는 클라이언트와 CMS가 신뢰를 설정하는 데 사용합니다. 또한 서버에 대해 신뢰할 수 있는 인증 구성을 마친 다음에 클라이언트를 구성해야 합니다.

파일 다운로드 대화 상자가 열립니다.

- d. 저장을 클릭하고 TrustedPrincipal.conf 파일을 저장할 위치를 다음 디렉터리로 지정합니다.
<INSTALLDIR>WSAP BusinessObjects Enterprise XI 4.0Wwin32_x86W
- e. 공유 암호의 유효 일수를 지정하려면 공유 암호 유효 기간 필드에 값을 입력합니다.
- f. 신뢰할 수 있는 인증 요청에 대한 제한 시간 값을 지정합니다.

참고:

제한 시간 값은 클라이언트 시계와 CMS 시계의 최대 시간 차이(밀리초)입니다. 0을 입력하면 두 시계의 시간 차이에 제한이 없는 것입니다. 반복되는 공격에 취약할 수 있으므로 이 값을 0으로 설정하지 않는 것이 좋습니다.

5. 업데이트를 클릭하여 공유 암호를 확정합니다.

참고:

신뢰할 수 있는 인증 매개 변수에 대한 수정 내용을 BI 플랫폼에서 전부 감사하지는 않습니다. 신뢰할 수 있는 인증의 정보를 모두 수동으로 백업해 두는 것이 좋습니다.

공유 암호는 클라이언트와 CMS가 신뢰를 설정하는 데 사용합니다. 또한 서버에 대해 신뢰할 수 있는 인증 구성을 마친 다음에 클라이언트를 구성해야 합니다.

7.2.5 웹 응용 프로그램에 대한 신뢰할 수 있는 인증 구성

클라이언트에 대해 신뢰할 수 있는 인증을 구성하려면 BOE war 파일에 대한 전역 속성에 액세스해서 수정하고 BI 실행 패드와 Open Document 응용 프로그램에서 고유 속성에 액세스하여 수정해야 합니다.

다음 두 가지 방법 중 하나를 사용하여 클라이언트에 공유 암호를 전달할 수 있습니다.

- 웹 세션
- TrustedPrincipal.conf 파일

공유 암호 외에 사용자 이름을 클라이언트에 전달하는 방법을 다음에서 하나 선택해야 합니다.

- 웹 세션
- 쿠키
- HTTP 헤더:
- URL 쿼리

어떤 방법을 선택하든 선택한 방법을 BOE war 파일의 Trusted.auth.user.retrieval 전역 속성에서 사용자 지정해야 합니다.

7.2.5.1 SAML 단일 로그인을 위해 신뢰할 수 있는 인증 사용

SAML(Security Assertion Markup Language)은 ID 정보를 주고 받는 데 사용되는 XML 기반 표준입니다. SAML을 사용할 경우 보안 통신을 통해 ID와 암호를 주고받을 수 있으므로, BI 플랫폼에 액세스하려는 사용자가 추가로 로그인할 필요가 없는 단일 로그인 메커니즘을 사용할 수 있습니다.

SAML 인증 사용

응용 프로그램 서버가 SAML 서비스 공급자로 사용될 경우 신뢰할 수 있는 인증을 통해 BI 플랫폼에 SAML SSO를 제공할 수 있습니다.

이를 위해서는 먼저 SAML 인증을 사용할 수 있도록 웹 응용 프로그램 서버를 구성해야 합니다.

아래의 예제에는 SAML 인증을 사용하도록 구성된 샘플 web.xml이 포함되어 있습니다.

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>InfoView</web-resource-name>
    <url-pattern>*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
```

```

<role-name>j2ee-admin</role-name>
<role-name>j2ee-guest</role-name>
<role-name>j2ee-special</role-name>
</auth-constraint>
<user-data-constraint>
  <transport-guarantee>NONE</transport-guarantee>
</user-data-constraint>
</security-constraint>
<login-config>
  <auth-method>FORM</auth-method>
  <realm-name>InfoView</realm-name>
  <form-login-config>
    <form-login-page>/logon.jsp</form-login-page>
    <form-error-page>/logon.jsp</form-error-page>
  </form-login-config>
</login-config>
<security-role>
  <description>Assigned to the SAP J2EE Engine System Administrators</description>
  <role-name>j2ee-admin</role-name>
</security-role>
<security-role>
  <description>Assigned to all users</description>
  <role-name>j2ee-guest</role-name>
</security-role>
<security-role>
  <description>Assigned to a special group of users</description>
  <role-name>j2ee-special</role-name>
</security-role>

```

구성 방법은 응용 프로그램 서버에 따라 다르므로 이에 대한 자세한 지침은 해당 응용 프로그램 서버 설명서를 참조하십시오.

신뢰할 수 있는 인증 사용

응용 프로그램 서버가 SAML 서비스 공급자로 사용되도록 구성된 경우 신뢰할 수 있는 인증을 통해 SAML SSO를 제공할 수 있습니다.

참고:

BI 플랫폼으로 사용자를 가져오거나 사용자에게 Enterprise 계정이 있어야 합니다.

SSO 설정을 위해 동적 별칭 설정이 사용됩니다. 사용자가 SAML을 통해 로그인 페이지에 처음으로 액세스하면 기존 BI 플랫폼 계정 자격 증명을 사용하여 수동으로 로그인할지 묻는 메시지가 표시됩니다. 사용자의 자격 증명에 확인되면 사용자의 SAML ID에 대한 별칭이 BI 플랫폼 계정에 설정됩니다. 시스템에서는 사용자의 ID 별칭을 기존 계정에 동적으로 일치시키기 때문에 이후에는 SSO를 통해 로그인됩니다.

참고:

이 메커니즘을 사용하려면 BOE war 파일에 대한 특정 속성인 `trusted.auth.user.namespace.enabled`를 설정해야 합니다.

7.2.5.2 웹 응용 프로그램에 대한 신뢰할 수 있는 인증 속성

다음 표에는 BOE.war의 기본 `global.properties` 파일에 포함된 신뢰할 수 있는 인증 설정이 나와 있습니다. 이러한 설정을 덮어쓰려면 `C:\WProgram Files (x86)\WSAP BusinessObjects\WSAP`

BusinessObjects Enterprise XI 4.0\warfiles\webapps\WBOE\WEB-INF\config\Wcustom에 새 파일을 만드십시오.

속성	기본값	설명
sso.enabled=true	sso.enabled=false	BI 플랫폼에 대한 단일 로그인(SSO)을 활성화하거나 비활성화합니다. 신뢰할 수 있는 인증을 설정하려면 이 속성을 true로 설정해야 합니다.
trusted.auth.shared.secret	없음	신뢰할 수 있는 인증 암호를 검색하는 데 사용되는 세션 변수 이름입니다. 웹 세션을 사용하여 공유 암호를 전달하는 경우에만 적용됩니다.
trusted.auth.user.param	없음	신뢰할 수 있는 인증의 사용자 이름을 검색하는 데 사용되는 변수를 지정합니다.
trusted.auth.user.retrieval	없음	신뢰할 수 있는 인증의 사용자 이름을 검색하는 데 사용되는 방법을 지정합니다. 다음 중 하나로 설정할 수 있습니다. <ul style="list-style-type: none"> • "REMOTE_USER" • "HTTP_HEADER" • "COOKIE" • "QUERY_STRING" • "WEB_SESSION" • "USER_PRINCIPAL" 신뢰할 수 있는 인증을 사용하지 않으려면 빈 문자열로 설정하십시오.
trusted.auth.user.namespace.enabled	trusted.auth.user.namespace.enabled=false	기존 사용자 계정에 대한 동적 별칭 바인딩을 설정하거나 해제합니다. 속성이 true로 설정되어 있는 경우, 신뢰할 수 있는 인증에서는 별칭 바인딩을 사용하여 BI 플랫폼에 대해 사용자를 인증합니다. 별칭 바인딩을 사용할 경우 응용 프로그램 서버가 SAML 서비스 공급자로 사용되므로 신뢰할 수 있는 인증을 통해 시스템에 SAML 단일 로그인을 제공할 수 있습니다. false로 설정할 경우 신뢰할 수 있는 인증에서 사용자 인증 시 이름 일치를 사용합니다.

7.2.5.3 웹 응용 프로그램에 대해 신뢰할 수 있는 인증 구성

공유 암호를 TrustedPrincipal.conf 파일에 저장하려는 경우 파일이 해당 플랫폼 디렉터리에 저장되어 있는지 확인하십시오.

플랫폼	TrustedPrincipal.conf의 위치
Windows(기본 설치 디렉터리)	<INSTALLDIR>WSAP BusinessObjects Enterprise XI 4.0\Win32_x86\
AIX	<INSTALLDIR>/sap_bobj/enterprise_xi40/aix_rs6000/
Solaris	<INSTALLDIR>/sap_bobj/enterprise_xi40/solaris_sparc/
HP_UX	<INSTALLDIR>/sap_bobj/enterprise_xi40/hpux_pa-risc/
Linux	<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x86

웹 응용 프로그램을 호스팅하는 클라이언트에 대해 신뢰할 수 있는 인증을 구성하는 데 사용되는 사용자 이름 변수를 채우는 방법에는 여러 가지가 있습니다. 이러한 사용자 이름 검색 방법을 사용하기 전에 사용자 이름이 노출되도록 웹 응용 프로그램 서버를 구성하거나 설정합니다. 자세한 내용은 <http://java.sun.com/j2ee/1.4/docs/api/javax/servlet/http/HttpServletRequest.html> 을 참조하십시오.

클라이언트에 대해 신뢰할 수 있는 인증을 구성하려면 BOE.war 파일에 대한 속성에 액세스하여 수정해야 합니다. BOE.war 파일에는 BI 실행 패드 및 OpenDocument 웹 응용 프로그램에 대한 일반 속성과 전용 속성이 포함되어 있습니다.

참고:

사용자 이름과 공유 암호를 검색하는 방법에 따라 추가 단계가 필요할 수 있습니다.

1. 웹 응용 프로그램을 호스팅하는 컴퓨터에서 BOE.war 파일에 대한 사용자 지정 폴더에 액세스합니다.

BI 플랫폼 설치와 함께 제공되는 Tomcat 웹 응용 프로그램 서버를 사용 중인 경우 다음 폴더에 직접 액세스할 수 있습니다.

C:\Program Files (x86)\WSAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom\

팁:

배포된 웹 응용 프로그램에 직접 액세스할 수 없는 웹 응용 프로그램 서버를 사용 중인 경우 제품 폴더에 있는 다음 폴더를 사용하여 BOE.war 파일을 수정할 수 있습니다.

<INSTALLDIR>WSAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\.

수정된 BOE.war 파일은 나중에 다시 배포해야 합니다.

2. 새 파일을 만듭니다.

참고:

메모장이나 다른 텍스트 편집 유틸리티를 사용하십시오.

3. 다음을 입력하여 신뢰할 수 있는 인증 속성을 지정합니다.

```
sso.enabled=true
trusted.auth.user.retrieval=Method for user ID retrieval
trusted.auth.user.param=Variable
trusted.auth.shared.secret=WEB_SESSION
```

다음 표는 사용자 이름 검색 옵션을 보여줍니다.

옵션	사용자 이름을 검색하는 방법
HTTP_HEADER	지정된 HTTP 헤더의 내용에서 사용자 이름을 검색합니다. trusted.auth.user.param 속성에 사용할 HTTP 헤더를 지정해야 합니다.
QUERY_STRING	요청 URL의 지정된 매개 변수에서 사용자 이름을 검색합니다. trusted.auth.user.param 속성에 사용할 쿼리 문자열을 지정해야 합니다.
COOKIE	지정된 쿠키에서 사용자 이름을 검색합니다. trusted.auth.user.param 속성에 사용할 쿠키를 지정해야 합니다.
WEB_SESSION	지정된 세션 변수의 내용에서 사용자 이름을 검색합니다. trusted.auth.user.param에서 사용할 웹 세션 변수를 global.properties에 지정해야 합니다.
USER_PRINCIPAL	서블릿 또는 JSP의 현재 요청에 대한 HttpServletRequest 개체의 getUserPrincipal().getName() 호출에서 사용자 이름이 검색됩니다.

참고:

- 일부 웹 응용 프로그램 서버는 웹 응용 프로그램 서버에서 환경 변수 REMOTE_USER를 true로 설정해야 합니다. true로 설정해야 하는지 여부에 대한 자세한 내용은 해당 웹 응용 프로그램 서버 설명서를 참조하십시오. 이런 경우 사용자 이름 검색 방법을 사용할 때 환경 변수가 true로 설정되어 있어야 합니다.
- USER_PRINCIPAL을 사용하여 사용자 이름을 전달하는 경우 trusted.auth.user.param을 비워 두십시오.

4. 파일을 다음 이름으로 저장합니다.

global.properties

5. 웹 응용 프로그램 서버를 다시 시작합니다.

웹 응용 프로그램 서버를 실행하는 컴퓨터에 수정된 BOE 웹 응용 프로그램을 다시 배포해야 새 속성이 적용됩니다. WDeploy를 사용하여 웹 응용 프로그램 서버에 WAR 파일을 다시 배포하십시오. WDeploy에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 웹 응용 프로그램 배포 가이드를 참조하십시오.

7.2.5.3.1 샘플 구성

7.2.5.3.1.1 TrustedPrincipal.conf 파일을 통한 공유 암호 전달

다음 샘플 구성은 사용자 JohnDoe가 BI 플랫폼에서 만들어졌다고 가정합니다.

사용자 정보는 웹 세션을 통해 저장 및 전달되고, 공유 암호는 TrustedPrincipal.conf 파일을 통해 전달됩니다. 이 파일은 C:\WProgram Files (x86)\WSAP BusinessObjects\WSAP BusinessObjects Enterprise XI 4.0\Win32_x86 디렉터리에 있는 것으로 간주됩니다. Tomcat 6의 번들 버전은 웹 응용 프로그램 서버입니다.

1. 다음 디렉터리에 액세스합니다.

```
<INSTALLDIR>WSAP BusinessObjects Enterprise XI
4.0\Wwarfiles\Wwebapps\WBOEWWEB-INF\Wconfig\WcustomW
```

2. 새 파일을 만듭니다.

참고:

메모장이나 다른 텍스트 편집 유틸리티를 사용하십시오.

3. 다음을 입력하여 신뢰할 수 있는 인증 속성을 지정합니다.

```
sso.enabled=true
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.user.param=MyUser
trusted.auth.shared.secret=
```

4. 파일을 다음 이름으로 저장합니다.

```
global.properties
```

5. 다음 파일에 액세스합니다.

```
C:\WProgram Files (x86)\WSAP BusinessObjects\WTomcat6\Wwebapps\WBOEWWEB-
INF\Wclipse\Wplugins\Wwebpath.InfoView\Wweb\Wcustom.jsp
```

6. 다음을 포함하도록 파일 내용을 수정합니다.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<%@ page language="java" contentType="text/html; charset=utf-8" %>
<%
//custom Java code
request.getSession().setAttribute("MyUser", "JohnDoe");
%>
<html>
<head>
<title>Custom Entry Point</title>
</head>
<body>
<script type="text/javascript" src="noCacheCustomResources/myScript.js"></script>
<a href="javascript:goToLogonPage()">Click this to go to the logon page of BI launch pad</a>
</body>
</html>
```

7. 다음 디렉터리에 myScript.js 파일을 만듭니다.

C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\Weclipse\plugins\webpath.InfoView\Web\noCacheCustomResources

8. myScript.js에 다음을 추가합니다.

```
function goToLogonPage() {
    window.location = "logon.jsp";
}
```

9. Tomcat을 종료합니다.

10. 다음 디렉터리에서 작업 폴더를 삭제합니다.

C:\Program Files (x86)\SAP BusinessObjects\Tomcat6

11. Tomcat을 다시 시작합니다.

신뢰할 수 있는 인증을 제대로 구성했는지 확인하려면 URL `http://[cmsname]:8080/BOE/BI/custom.jsp`를 사용하여 BI 실행 패드 응용 프로그램에 액세스하십시오. 여기서 [cmsname]은 CMS를 호스팅하는 컴퓨터의 이름입니다. 다음 링크가 표시되어야 합니다. 이 링크를 클릭하면 BI 실행 패드의 로그인 페이지로 이동합니다.

7.2.5.3.1.2 웹 세션 변수를 통한 공유 암호 전달

다음 샘플 구성은 사용자 JohnDoe가 BI 플랫폼에서 만들어졌다고 가정합니다.

사용자 정보는 웹 세션을 통해 저장 및 전달되고, 공유 암호는 웹 세션 변수를 통해 전달됩니다. 이 파일은 C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Win32_x86 디렉터리에 있는 것으로 간주됩니다. 파일을 열고 파일의 내용을 메모해야 합니다. 이 샘플 구성에서는 공유 암호가 다음과 같다고 간주합니다.

```
9ecb0778edc9f048edae0fcdde1a5db8211293486774a127ec949c1bdb98dae8e0ea388979edc65773
841c8ae5d1f675a6bf5d7c66038b6a3f1345285b55a0a7
```

Tomcat 6의 번들 버전은 웹 응용 프로그램 서버입니다.

1. 다음 디렉터리에 액세스합니다.

<INSTALLDIR>WSAP BusinessObjects Enterprise XI
4.0\Wwarfiles\Wwebapps\WBOE\WEB-INF\Wconfig\Wcustom\W

2. 새 파일을 만듭니다.

참고:

메모장이나 다른 텍스트 편집 유틸리티를 사용하십시오.

3. 다음을 입력하여 신뢰할 수 있는 인증 속성을 지정합니다.

```
sso.enabled=true
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.user.param=MyUser
trusted.auth.shared.secret=MySecret
```

4. 파일을 다음 이름으로 저장합니다.

global.properties

5. 다음 파일에 액세스합니다.

C:\Program Files (x86)\WSAP BusinessObjects\WTomcat6\Wwebapps\WBOE\WEB-INF\Wclipse\Wplugins\Wwebpath.InfoView\Wweb\Wcustom.jsp

6. 다음을 포함하도록 파일 내용을 수정합니다.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<%@ page language="java" contentType="text/html; charset=utf-8" %>
<%
//custom Java code
request.getSession().setAttribute("MySecret", "9ecb0778edcff048edae0fcdde1a5db82112934
86774a127ec949c1bdb98dae8e0ea388979edc65773841c8ae5d1f675a6bf5d7c66038b6a3f1345
285b55a0a7"
request.getSession().setAttribute("MyUser", "JohnDoe");
%>
<html>
<head>
<title>Custom Entry Point</title>
</head>
<body>
<script type="text/javascript" src="noCacheCustomResources/myScript.js"></script>
<a href="javascript:goToLogonPage()">Click this to go to the logon page of BI launch pad</a>
</body>
</html>
```

7. 다음 디렉터리에 myScript.js 파일을 만듭니다.

C:\Program Files (x86)\WSAP BusinessObjects\WTomcat6\Wwebapps\WBOE\WEB-INF\Wclipse\Wplugins\Wwebpath.InfoView\Wweb\WnoCacheCustomResources

8. myScript.js에 다음을 추가합니다.

```
function goToLogonPage() {
    window.location = "logon.jsp";
}
```

9. Tomcat을 종료합니다.

10. 다음 디렉터리에서 작업 폴더를 삭제합니다.

C:\Program Files (x86)\W SAP BusinessObjects\WTomcat6

11. Tomcat을 다시 시작합니다.

신뢰할 수 있는 인증을 제대로 구성했는지 확인하려면 URL `http://[cmsname]:8080/BOE/BI/custom.jsp`를 사용하여 BI 실행 패드 응용 프로그램에 액세스하십시오. 여기서 [cmsname]은 CMS를 호스팅하는 컴퓨터의 이름입니다. 다음 링크가 표시되어야 합니다.
이 링크를 클릭하면 BI 실행 패드의 로그인 페이지로 이동합니다.

7.2.5.3.1.3 사용자 이름을 통한 사용자 이름 전달

다음 샘플 구성은 사용자 JohnDoe가 BI 플랫폼에서 만들어졌다고 가정합니다.

사용자 정보는 사용자 이름 옵션을 통해 저장 및 전달되고, 공유 암호는 `TrustedPrincipal.conf` 파일을 통해 전달됩니다. 이 파일은 `C:\WProgram Files (x86)\WSAP BusinessObjects\WSAP BusinessObjects Enterprise XI 4.0\Win32_x86` 디렉터리에 있는 것으로 간주됩니다. Tomcat 6의 번들 버전은 웹 응용 프로그램 서버입니다.

1. Tomcat 서버를 중지합니다.

2. Tomcat의 `server.xml` 파일을 엽니다.

이 파일은 기본적으로 다음 디렉터리에 있습니다.

`C:\WProgram Files (x86)\W SAP BusinessObjects\Tomcat6\conf\W`

3. `Realm className=`의 값을 다음으로 변경합니다.

`Realm className=org.apache.catalina.realm.MemoryRealm`

4. `tomcat-users.xml` 파일을 엽니다.

이 파일은 기본적으로 다음 디렉터리에 있습니다.

`C:\WProgram Files (x86)\W SAP BusinessObjects\Tomcat6\conf\W`

5. `<tomcat-users>` 태그를 찾은 후 다음을 수정합니다.

```
<user name=JohnDoe password=password
roles=onjavauser/>
```

6. 다음 디렉터리에서 `web.xml` 파일을 엽니다.

`C:\WProgram Files (x86)\W SAP BusinessObjects\Tomcat6\webapps\WBOEW\WEB-INF\W`

7. `</web-app>` 태그 앞에 다음을 추가합니다.

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>OnJavaApplication</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>onjavauser</role-name>
  </auth-constraint>
</security-constraint>
```

```
<login-config>
  <auth-method>BASIC</auth-method>
  <realm-name>OnJava Application</realm-name>
</login-config>
```

참고:

<url-pattern></url-pattern> 매개변수에 대해 특정 페이지를 입력해야 합니다. 일반적으로 이 페이지는 BI 실행 패드 또는 다른 웹 응용 프로그램의 기본 URL이 아닙니다.

8. 다음 디렉터리에서 작업 폴더를 삭제합니다.

C:\WProgram Files (x86)\W SAP BusinessObjects\Tomcat6

9. Tomcat을 다시 시작합니다.

참고:

원격 사용자 방식을 사용하는 경우 웹 응용 프로그램 서버 구성이 동일합니다.

신뢰할 수 있는 인증을 제대로 구성했는지 확인하려면 URL `http://[cmsname]:8080/BOE/BI`를 사용하여 BI 실행 패드 응용 프로그램에 액세스하십시오. 여기서 [cmsname]은 CMS를 호스팅하는 컴퓨터의 이름입니다. 잠시 후 로그인 대화 상자가 나타납니다.

7.3 LDAP 인증

7.3.1 LDAP 인증 사용

이 단원에서는 LDAP 인증과 BI 플랫폼이 함께 작동하는 방식을 전반적으로 설명합니다. 그런 다음 LDAP 계정을 관리하고 플랫폼에 대해 구성할 수 있는 관리 도구를 소개합니다.

BI 플랫폼을 설치하면 LDAP 인증 플러그 인도 자동으로 설치되지만 기본적으로 사용되지는 않습니다. LDAP 인증을 사용하려면 먼저 각 LDAP 디렉터리가 설정되어 있는지 확인해야 합니다. LDAP에 대한 자세한 내용은 LDAP 설명서를 참조하십시오.

응용 프로그램에 종속되지 않은 공통 디렉터리인 LDAP(Lightweight Directory Access Protocol)를 사용하면 여러 응용 프로그램 사이에 정보를 공유할 수 있습니다. 개방형 표준을 기반으로 한 LDAP를 사용하면 디렉터리의 정보에 액세스하고 이를 업데이트할 수 있습니다.

LDAP는 DAP(Directory Access Protocol)를 사용하여 디렉터리 클라이언트와 디렉터리 서버 사이에 통신하는 X.500 표준을 기반으로 합니다. LDAP는 DAP보다 더 적은 리소스를 사용하고 일부 X.500 작업과 기능을 간소화하거나 생략하므로 DAP의 대안으로 사용됩니다.

LDAP 내의 디렉터리 구조에는 특정 스키마로 정렬된 항목이 있습니다. 각 항목은 DN(고유 이름) 또는 CN(공통 이름)으로 식별됩니다. 다른 공통 특성에는 OU(조직 단위 이름)와 O(조직 이름)가 있습니다. 예를 들어, 멤버 그룹이 다음과 같은 디렉터리 트리에 배치될 수 있습니다(cn=BI 플랫폼 사용자, ou=Enterprise 사용자 A, o=연구소). 자세한 내용은 LDAP 설명서를 참조하십시오.

LDAP는 응용 프로그램에 종속되지 않으므로 적절한 권한이 부여된 모든 클라이언트에서 LDAP의 디렉터리에 액세스할 수 있습니다. LDAP를 사용하면 사용자가 LDAP 인증을 통해 BI 플랫폼에 로그인하도록 설정할 수 있습니다. LDAP를 사용하면 시스템의 개체에 사용자가 액세스하려 할 때 적절한 권한을 부여하도록 할 수도 있습니다. 하나 이상의 LDAP 서버가 실행되고 있고 기존의 네트워크 환경 컴퓨터 시스템에서 LDAP를 사용하는 경우에는 Enterprise 및 Windows AD 인증과 함께 LDAP 인증을 항상 사용할 수 있습니다.

원하는 경우 BI 플랫폼에 제공되는 LDAP 보안 플러그 인에서 서버 인증 또는 상호 인증을 통해 설정된 SSL 연결을 사용하여 LDAP 서버와 통신할 수 있습니다. 서버 인증을 사용하면 서버가 신뢰되는지 확인하기 위해 BI 플랫폼에서 사용하는 보안 인증서가 LDAP 서버에 추가되고 LDAP 서버에 익명 클라이언트의 연결이 허용됩니다. 상호 인증을 사용하면 LDAP 서버와 BI 플랫폼 모두에 보안 인증서가 추가되고 LDAP 서버에서는 연결을 설정하기 전에 클라이언트 인증서도 확인해야 합니다.

BI 플랫폼에서 제공되는 LDAP 보안 플러그 인이 SSL을 통해 LDAP 서버와 통신하도록 구성할 수 있지만 이 플러그 인은 사용자의 자격 증명을 확인할 때 항상 기본 인증을 수행합니다. BI 플랫폼과 함께 LDAP 인증을 배포하려면 먼저 이러한 LDAP 형식 간의 차이점에 대해 잘 알고 있어야 합니다. 자세한 내용은 <http://www.faqs.org/rfcs/rfc2251.html>의 RFC2251을 참조하십시오.

관련 항목

- 232 페이지에서 [LDAP 인증 구성](#)"
- 243 페이지에서 [LDAP 그룹 매핑](#)"

7.3.1.1 LDAP 보안 플러그 인

LDAP 보안 플러그 인을 통해 LDAP 디렉터리 서버의 사용자 계정과 그룹을 BI 플랫폼에 매핑할 수 있으며 LDAP 인증을 지정하는 모든 로그인 요청을 시스템이 확인하도록 할 수도 있습니다. CMS에서 사용자에게 활성 BI 플랫폼 세션을 허용하기 전에 LDAP 디렉터리 서버를 기준으로 사용자를 인증하고 매핑된 LDAP 그룹을 통해 이 사용자의 멤버 자격을 확인하는 과정을 거칩니다. 사용자 목록과 그룹 멤버 구성은 시스템에서 동적으로 관리합니다. 보안을 강화하기 위해 플랫폼에서 SSL(Secure Sockets Layer) 연결을 사용하여 LDAP 디렉터리 서버와 통신하도록 지정할 수 있습니다.

BI 플랫폼용 LDAP 인증은 그룹을 매핑하고 인증, 권한 및 별칭 작성을 설정할 수 있다는 점에서 Windows AD 인증과 유사합니다. 또한, NT 또는 AD 인증의 경우와 마찬가지로 기존의 LDAP 사용자에게 대해 새로운 Enterprise 계정을 만들 수 있고, 사용자 이름이 Enterprise 사용자 이름과 일치하는 경우 기존의 사용자에게 LDAP 별칭을 할당할 수 있습니다. 또한 다음과 같은 작업을 수행할 수 있습니다.

- LDAP 디렉터리 서비스의 사용자와 그룹을 매핑할 수 있습니다.

- AD에 대해 LDAP를 매핑할 수 있습니다. AD에 대해 LDAP를 구성하는 경우 여러 가지 제한 사항을 고려해야 합니다.
- 다중 호스트 이름과 포트를 지정할 수 있습니다.
- SiteMinder를 사용하여 LDAP를 구성할 수 있습니다.

LDAP 사용자와 그룹을 매핑하면 모든 BI 플랫폼 클라이언트 도구에서 LDAP 인증이 지원됩니다. LDAP 인증을 지원하는 고유한 응용 프로그램을 직접 만들 수도 있습니다.

관련 항목

- 236 페이지에서 [LDAP 서버 또는 상호 인증에 대한 SSL 설정 구성 "](#)
- 246 페이지에서 [Windows AD에 대해 LDAP 매핑 "](#)
- 241 페이지에서 [SiteMinder에 대해 LDAP 플러그 인 구성 "](#)

7.3.2 LDAP 인증 구성

관리를 간소화하기 위해 BI 플랫폼에서는 사용자 및 그룹 계정에 LDAP 인증을 지원합니다. 사용자가 LDAP 사용자 이름과 암호를 사용하여 시스템에 로그인하려면 먼저 LDAP 계정을 BI 플랫폼에 매핑해야 합니다. LDAP 계정을 매핑할 때 새 계정을 만들 수도 있고 기존의 BI 플랫폼 계정에 연결할 수도 있습니다.

LDAP 인증을 설정하고 사용하기 전에 LDAP 디렉터리가 설정되어 있는지 확인해야 합니다. 자세한 내용은 LDAP 설명서를 참조하십시오.

LDAP 인증을 구성할 때는 다음과 같은 작업을 합니다.

- LDAP 호스트 구성
- LDAP 서버에서 SSL 사용 준비(필요한 경우)
- SiteMinder용 LDAP 플러그 인 구성(필요한 경우)

참고:

AD에 대해 LDAP를 구성하면 사용자를 매핑할 수 있지만 AD 단일 로그인 또는 데이터베이스에 대한 단일 로그인 구성할 수 없습니다. 그러나 SiteMinder 등의 LDAP 단일 로그인 방법 및 신뢰할 수 있는 인증은 계속 사용할 수 있습니다.

7.3.2.1 LDAP 호스트 구성

LDAP 호스트를 구성하기 전에 LDAP 서버를 설치하여 실행하는 것이 좋습니다.

1. CMC의 인증 관리 영역으로 이동한 다음 LDAP를 두 번 클릭합니다.

참고:

인증 관리 영역으로 이동하려면 탐색 목록에서 인증을 선택합니다.

2. LDAP 호스트 추가(호스트 이름:포트) 필드에 LDAP 호스트의 이름 및 포트 번호를 입력하고(예: "myserver:123") 추가를 클릭한 다음 확인을 클릭합니다.

팁:

장애 조치 서버로 사용할 수 있는 호스트를 추가하려면 이 단계를 반복하여 같은 서버의 LDAP 호스트를 두 개 이상 추가합니다. 호스트를 제거하려면 호스트 이름을 강조 표시하고 삭제를 클릭합니다.

3. LDAP 서버 유형 목록에서 서버 유형을 선택합니다.

참고:

LDAP를 AD로 매핑하는 경우 서버 유형으로 Microsoft Active Directory Application Server를 선택합니다.

4. LDAP 서버 특성 매핑 또는 LDAP 기본 검색 특성을 보거나 변경하려면 특성 매핑 표시를 클릭합니다.

기본적으로 지원되는 각 서버 유형의 서버 특성 매핑과 검색 특성은 이미 설정되어 있습니다.

5. 다음을 클릭합니다.

6. 기본 LDAP 고유 이름 필드에 LDAP 서버에 대한 고유 이름(예: o=SomeBase)을 입력한 후 다음을 클릭합니다.

7. LDAP 서버 자격 증명 영역에서 디렉터리에 대한 읽기 권한이 있는 사용자 계정과 관련하여 구별된 이름 및 암호를 지정합니다.

참고:

관리자 자격 증명은 필요하지 않습니다.

참고:

LDAP 서버에서 익명 바인딩을 허용하는 경우 이 영역을 비워 두면 BI 플랫폼 서버와 클라이언트가 익명 로그온을 통해 기본 호스트에 바인딩합니다.

8. LDAP 호스트에서 조회를 구성한 경우 LDAP 조회 자격 증명 영역에 인증 정보를 입력한 다음 최대 조회 홉 필드에 조회 홉 수를 입력합니다.

참고:

다음은 모두 적용되는 경우 "LDAP 조회 자격 증명" 영역을 구성해야 합니다.

- 주 호스트는 지정된 기반에서 항목에 대한 쿼리를 처리하는 다른 디렉터리 서버를 참조하도록 구성되어 있습니다.
- 참조되는 호스트는 익명 바인딩을 허용하지 않도록 구성되어 있습니다.

- 참조되는 호스트의 그룹은 BI 플랫폼에 매핑됩니다.

참고:

- 다중 호스트의 그룹을 매핑할 수 있지만 조회 자격 증명 집합은 하나만 설정할 수 있습니다. 따라서 조회 호스트가 여러 개 있는 경우에는 각 호스트에서 동일한 고유 이름과 암호를 사용하는 사용자 계정을 만들어야 합니다.
- "최대 조회 횟수"이 0으로 설정되어 있는 경우 조회가 수행되지 않습니다.

9. 다음을 클릭합니다.

10. 사용된 SSL(Secure Sockets Layer) 인증 유형을 선택한 후 다음을 클릭합니다.

선택할 수 있는 항목은 다음과 같습니다.

- 기본(SSL 없음)
- 서버 인증
- 상호 인증

11. LDAP 단일 로그인 인증 방법을 선택한 후 다음을 클릭합니다.

선택할 수 있는 항목은 다음과 같습니다.

- 기본(SSO 없음)
- SiteMinder

12. 별칭과 사용자를 BI 플랫폼 계정에 매핑하는 방식을 선택합니다.

a. 새 별칭 옵션에서 새 별칭이 Enterprise 계정에 매핑되는 방식을 선택합니다. 다음 항목 중 하나를 선택합니다.

- 추가된 각 LDAP 별칭을 같은 이름의 계정에 할당
사용자에게 같은 이름의 기존 Enterprise 계정이 있다는 것을 아는 경우 이 옵션을 사용합니다. 즉, LDAP 별칭이 기존 사용자에게 할당됩니다(자동 별칭 만들기 사용). 기존 Enterprise 계정이 없는 사용자 또는 Enterprise 및 LDAP 계정에 같은 이름이 없는 사용자는 새 사용자로 추가됩니다.
- 추가된 모든 LDAP 별칭에 대해 새 계정 만들기
각 사용자에게 대해 새 계정을 만들려는 경우 이 옵션을 사용합니다.

b. 별칭 업데이트 옵션에서 Enterprise 계정의 별칭 업데이트를 관리할 방법을 선택합니다. 다음 항목 중 하나를 선택합니다.

- 별칭을 업데이트할 때마다 새 별칭 만들기
BI 플랫폼에 매핑된 모든 LDAP 사용자에게 대해 자동으로 새 별칭을 만들려면 이 옵션을 사용합니다. BI 플랫폼 계정이 없는 사용자나 추가된 모든 LDAP 별칭에 대해 새 계정 만들기 옵션을 선택한 경우 모든 사용자에게 대해 새 LDAP 계정이 추가됩니다.
- 사용자가 로그인할 경우에만 새 별칭 만들기
매핑하는 LDAP 디렉터리에 여러 사용자가 들어 있지만 그 중 일부만 BI 플랫폼을 사용하는 경우 이 옵션을 사용합니다. 모든 사용자에게 대해 별칭과 Enterprise 계정이 자동으로 생성되지 않습니다. 대신 플랫폼에 로그인하는 사용자에게 대해서만 별칭 및 계정(필요한 경우)이 생성됩니다.

- c. 새 사용자 옵션에서 새 사용자를 만드는 방식을 지정합니다.

SAP BusinessObjects Business Intelligence 플랫폼 라이선스가 사용자 역할을 기반으로 하는 경우, 다음 새 사용자 옵션 중 하나를 선택하십시오.

- BI Viewer

새 사용자 계정이 BI Viewer 역할에 구성됩니다. BI Viewer 역할의 모든 계정에 대한 BI 플랫폼 응용 프로그램 액세스 권한이 사용권 계약에 정의됩니다. 사용자는 BI Viewer 역할용으로 정의된 응용 프로그램 워크플로에만 액세스할 수 있습니다. 액세스 권한은 일반적으로 비즈니스 인텔리전스 문서를 보는 것으로 제한됩니다. 이 역할은 일반적으로 BI 플랫폼 응용 프로그램을 통해 콘텐츠를 사용하는 사용자에게 적합합니다.

- BI Analyst: 새 사용자 계정이 BI Analyst 역할에 구성됩니다. BI Analyst 역할의 모든 계정에 대한 BI 플랫폼 응용 프로그램 액세스 권한이 사용권 계약에 정의됩니다. 사용자는 BI Analyst 역할에 대해 정의된 모든 응용 프로그램 워크플로에 액세스할 수 있습니다. 액세스 권한에는 비즈니스 인텔리전스 문서를 보고 수정하는 것이 포함됩니다. 이 역할은 일반적으로 BI 플랫폼 응용 프로그램의 콘텐츠를 만들고 수정하는 사용자에게 적합합니다.

SAP BusinessObjects Business Intelligence 플랫폼 라이선스가 사용자 역할을 기반으로 하지 않는 경우에는 다음 옵션 중 하나를 선택하십시오.

- 새 사용자를 명명된 사용자로 만들기

새 사용자 계정이 명명된 사용자 라이선스를 사용하도록 구성됩니다. 명명된 사용자 라이선스는 특정 사용자와 관련되며 이 라이선스를 사용하면 사용자 이름과 암호를 기반으로 시스템에 액세스할 수 있습니다. 이 옵션을 사용하면 명명된 사용자는 연결된 다른 사용자 수에 관계없이 시스템에 액세스할 수 있습니다. 이 옵션을 사용하여 만든 각 사용자 계정에 대한 명명된 사용자 라이선스가 있어야 합니다.

- 새 사용자를 동시 사용자로 만들기

새 사용자 계정이 동시 사용자 라이선스를 사용하도록 구성됩니다. 동시 라이선스는 동시에 SAP BusinessObjects Business Intelligence 플랫폼에 연결할 수 있는 인원 수를 지정합니다. 이 라이선스 유형은 소규모 동시 라이선스로 많은 사용자 기반을 지원할 수 있으므로 매우 유연합니다. 예를 들어 사용자가 해당 플랫폼에 액세스하는 빈도 및 시간에 따라 100개의 동시 사용자 라이선스로 250명, 500명 또는 700명의 사용자를 지원할 수 있습니다.

13. 특성 바인딩 옵션 영역에서 LDAP 플러그인의 특성 바인딩 우선 순위를 지정할 수 있습니다.

- a. 전체 이름 및 전자 메일 주소 가져오기 상자를 클릭합니다.

LDAP 계정에 사용된 전체 이름과 설명을 가져와서 사용자 개체와 함께 시스템에 저장됩니다.

- b. 다른 특성 바인딩을 기준으로 LDAP 특성 바인딩의 우선 순위 설정 옵션을 지정합니다.

참고:

이 옵션을 1로 설정하면 LDAP과 다른 플러그인(Windows AD 및 SAP)이 활성화된 경우 LDAP 특성이 우선 적용됩니다. 3으로 설정하면 다른 활성화된 플러그인의 특성이 우선 적용됩니다.

14. 마침을 클릭합니다 .

관련 항목

- 236 페이지에서 [LDAP 서버 또는 상호 인증에 대한 SSL 설정 구성 "](#)
- 241 페이지에서 [SiteMinder에 대해 LDAP 플러그인 구성 "](#)
- 90 페이지에서 [역할 기반 라이선스 "](#)

7.3.2.2 여러 LDAP 호스트 관리

LDAP 및 BI 플랫폼을 사용하여 여러 LDAP 호스트를 추가하면 시스템에서 작업이 실패하는 경우를 대비할 수 있습니다. 시스템에서는 첫 번째로 추가되는 호스트를 주 LDAP 호스트로 사용하며 후속 호스트를 장애 조치 호스트로 간주합니다.

주 LDAP 호스트와 모든 장애 조치 호스트는 정확하게 같은 방법으로 구성되어야 하며 각 LDAP 호스트는 그룹이 매핑될 모든 추가 원본 호스트를 참조해야 합니다. LDAP 호스트 및 조회 호스트에 대한 자세한 내용은 LDAP 설명서를 참조하십시오.

여러 개의 LDAP 호스트를 추가하려면 LDAP 구성 마법사를 사용하여 LDAP를 구성할 때 모든 호스트를 입력합니다(자세한 내용은 관련 내용 참조). 또는 LDAP를 이미 구성한 경우에는 중앙 관리 콘솔의 인증 관리 영역으로 이동한 다음 LDAP 탭을 클릭합니다. LDAP 서버 구성 요약 영역에서 LDAP 호스트의 이름을 클릭하여 호스트를 추가하거나 삭제할 수 있는 페이지를 엽니다.

참고:

- 주 호스트를 먼저 추가한 다음 나머지 장애 조치 호스트를 추가하십시오.
- 장애 조치 LDAP 호스트를 사용하면 최고 수준의 SSL 보안을 사용할 수 없습니다. 즉, "신뢰할 수 있는 인증 기관에서 발급한 인증서이고 인증서의 CN 특성이 서버의 DNS 호스트 이름과 일치하는 경우 서버 인증서를 수락"을 선택할 수 없습니다.

관련 항목

- 232 페이지에서 [LDAP 인증 구성](#)

7.3.2.3 LDAP 서버 또는 상호 인증에 대한 SSL 설정 구성

이 단원에서는 LDAP 서버 및 상호 인증을 사용하여 SSL을 구성하기 위한 CMC 관련 정보를 제공합니다. LDAP 호스트의 구성을 마쳤고 SSL 인증으로 다음 중 하나를 선택한 상황을 가정하여 설명합니다.

- 서버 인증
- 상호 인증

LDAP 호스트 서버에 대한 정보나 서버 구성에 대한 자세한 내용은 LDAP 공급업체 설명서를 참조하십시오.

관련 항목

- 232 페이지에서 [LDAP 호스트 구성](#)"

7.3.2.3.1 LDAP 서버 또는 상호 인증 구성

리소스	필수 작업
CA 인증서	CA 인증서를 만들려면 인증 기관이 필요합니다. 이 인증서는 이후 LDAP 서버에 추가해야 합니다. 자세한 내용은 LDAP 공급업체 설명서를 참조하십시오. 이 작업은 SSL을 사용한 서버 인증과 상호 인증 모두에 필요합니다.
서버 인증서	먼저 서버 인증서를 요청한 다음 이를 만들어야 합니다. LDAP 서버에 인증서를 추가하기 전에 이 인증서를 승인해야 합니다. 이 작업은 SSL을 사용한 서버 인증과 상호 인증 모두에 필요합니다.
cert7.db key3.db	<p>cert7.db 파일을 만들 수 있는 certutil 응용 프로그램에 액세스해야 합니다. 이 응용 프로그램은 ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_6_RTM/ 에서 다운로드할 수 있습니다. CA 인증서를 certutil이 있는 디렉터리에 복사하십시오. 다음 명령을 사용하여 cert7.db, key3.db, secmod.db 파일을 만듭니다.</p> <pre>certutil -N -d .</pre> <p>다음 명령을 사용하여 cert7.db 파일에 CA 인증서를 추가합니다.</p> <pre>certutil -A -n <CA_alias_name> -t CT -d . -I cacert.cer</pre> <p>이 세 개의 파일을 SAP BusinessObjects Business Intelligence 플랫폼을 호스팅하는 컴퓨터의 디렉터리에 저장합니다. 이 파일들은 SSL을 사용한 서버 인증과 상호 인증 모두에 필요합니다.</p>
cacerts	<p>이 파일은 BI 실행 패드와 같은 Java 응용 프로그램용 SSL을 사용한 서버 인증 또는 상호 인증에만 필요합니다. Java bin 디렉터리에 있는 keytool 파일에 액세스합니다. 다음 명령을 사용하여 cacerts 파일을 만듭니다.</p> <pre>keytool -import -v -alias <CA_alias_name> -file <CA_certificate_name> -trustcacerts -keystore</pre> <p>cacerts 파일을 cert7.db와 key3.db 파일이 있는 디렉터리에 저장합니다.</p>
클라이언트 인증서	

리소스	필수 작업
	<p>cert7.db와 .keystore 파일에 대해 별도의 클라이언트 요청을 만들어야 합니다. LDAP 플러그 인을 구성하려면 certutil을 사용하여 클라이언트 인증서 요청을 만들어야 합니다. 클라이언트 인증서 요청을 만들려면 다음 명령을 사용합니다.</p> <pre>certutil -R -s "<client_dn>" -a -o <certificate_request_name> -d .</pre> <p>참고: <client_dn>에는 "CN=<client_name>, OU=org unit, O=Companyname, L=city, ST=province, C=country와 같은 정보가 포함됩니다. 이후 이 인증서 요청은 인증 기관을 통해 인증받아야 합니다. 인증서를 검색하여 cert7.db 파일에 삽입하려면 다음 명령을 사용합니다.</p> <pre>certutil -A -n <client_name> -t Pu -d . -I <client_certificate_name></pre> <p>SSL을 사용한 Java 인증을 사용하려면 Java bin 디렉터리에 있는 keytool 유틸리티를 사용해 클라이언트 인증서 요청을 만들어야 합니다. 다음 명령을 사용하여 키 쌍을 만듭니다.</p> <pre>keytool -genkey -keystore .keystore</pre> <p>클라이언트 정보를 지정한 후 다음 명령을 통해 클라이언트 인증서 요청을 만듭니다.</p> <pre>keytool -certreq -file <certificate_request_name> -keystore .keystore</pre> <p>클라이언트 인증서 요청이 인증 기관에서 인증되면 다음 명령을 사용하여 CA 인증서를 .keystore 파일에 삽입해야 합니다.</p> <pre>keytool -import -v -alias <CA_alias_name> -file <ca_certificate_name> -trustcacerts -keystore .keystore</pre> <p>마지막으로, CA에서 클라이언트 인증서를 가져온 후 다음 명령을 통해 .keystore 파일에 삽입합니다.</p> <pre>keytool -import -v -file <client_certificate_name> -trustcacerts -keystore .keystore</pre> <p>BI 플랫폼을 호스팅하는 컴퓨터에서 cert7.db 및 cacerts가 있는 디렉터리에 .keystore 파일을 저장합니다.</p>

1. 사용 가능한 옵션에서 사용할 SSL 보안 수준을 선택합니다.

참고:

Java 응용 프로그램은 첫 번째 설정과 마지막 설정을 무시하고 신뢰할 수 있는 인증 기관에서 발급한 서버 인증서만 수락합니다.

- 서버 인증서를 항상 수락

이 옵션은 보안 수준이 가장 낮습니다. BI 플랫폼에서 LDAP 사용자 및 그룹을 인증하기 위해 LDAP 호스트와 SSL 연결을 설정하려면 먼저 LDAP 호스트에서 보안 인증서를 받아야 합니다. BI 플랫폼에서는 받은 인증서를 확인하지 않습니다.

- 신뢰할 수 있는 인증 기관에서 발급한 서버 인증서를 수락

이 옵션은 보안 수준이 중간입니다. BI 플랫폼에서 LDAP 사용자 및 그룹을 인증하기 위해 LDAP 호스트와 SSL 연결을 설정하려면 먼저 LDAP 호스트가 보낸 보안 인증서를 받아서 확인해야 합니다. 인증서 확인을 위해 시스템은 인증서 데이터베이스에서 이 인증서를 발급한 인증 기관을 찾아야 합니다.

- 신뢰할 수 있는 인증 기관에서 발급한 인증서이고 인증서의 CN 특성이 서버의 DNS 호스트 이름과 일치하는 경우 서버 인증서를 수락

이 옵션은 보안 수준이 가장 높습니다. BI 플랫폼에서 LDAP 사용자 및 그룹을 인증하기 위해 LDAP 호스트와 SSL 연결을 설정하려면 먼저 LDAP 호스트가 보낸 보안 인증서를 받아서 확인해야 합니다. 인증서 확인을 위해 BI 플랫폼은 인증서 데이터베이스에서 이 인증서를 발급한 인증 기관을 찾아야 합니다. 또한 서버 인증서의 CN 특성이 마법사의 첫 번째 단계에서 "LDAP 호스트 추가" 필드에 입력한 LDAP 호스트의 호스트 이름과 정확하게 일치하는지도 확인할 수 있어야 합니다. 예를 들어, LDAP 호스트 이름을 ABALONE.rd.crystald.net:389로 입력한 경우 인증서에 CN =ABALONE:389를 사용하면 제대로 동작하지 않습니다.

서버 보안 인증서의 호스트 이름은 주 LDAP 호스트의 이름입니다. 따라서 이 옵션을 선택하면 장애 조치 LDAP 호스트를 사용할 수 없습니다.

2. SSL 호스트 입력란에 각 컴퓨터의 호스트 이름을 입력한 다음 추가를 클릭합니다.

참고:

그리고 BI 플랫폼 배포에 SAP BusinessObjects Business Intelligence 플랫폼 SDK를 사용하는 각 컴퓨터의 호스트 이름을 추가해야 합니다. 여기에는 중앙 관리 서버를 실행하는 컴퓨터와 웹 응용 프로그램 서버를 실행하는 컴퓨터가 포함됩니다.

3. 목록에 추가한 각 SSL 호스트에 대한 SSL 설정을 지정하고 목록에 없는 각 호스트에 대해 사용할 기본 설정을 지정합니다.

참고:

기본 설정은 "기본값 사용" 확인란이 선택되어 있는 모든 호스트 또는 SSL 호스트 목록에 이름이 명시적으로 추가되지 않은 컴퓨터를 설정하는 데 사용됩니다.

기본 설정을 지정하려면

- a. SSL 목록에서 기본값을 선택합니다.
- b. 기본값 사용 확인란을 선택 취소합니다.
- c. "인증서 및 주요 데이터베이스 파일의 경로" 및 "주요 데이터베이스의 암호" 값을 입력합니다.
- d. 상호 인증에 대한 설정을 지정하는 경우 "cert7.db에 있는 클라이언트 인증서의 애칭" 필드에 값을 입력할 수도 있습니다.

다른 호스트에 대한 설정을 선택하려면 왼쪽에 있는 목록에서 이름을 선택한 다음 오른쪽에 있는 상자에 적절한 값을 입력합니다.

4. 다음을 클릭합니다.
5. 다음과 같은 선택 사항에서 LDAP 단일 로그인 인증 방법을 선택합니다.
 - 기본(SSO 없음)
 - SiteMinder
6. 새 LDAP 사용자와 별칭을 만드는 방법을 선택합니다.
7. 마침을 클릭합니다.

관련 항목

- 241 페이지에서 [SiteMinder에 대해 LDAP 플러그인 구성](#)

7.3.2.4 LDAP 구성 설정 수정

LDAP 구성 마법사를 사용하여 LDAP 인증을 구성한 다음에는 LDAP 서버 구성 요약 페이지를 사용하여 LDAP 연결 매개 변수 및 멤버 그룹을 변경할 수 있습니다.

1. CMC의 인증 관리 영역으로 이동합니다.
2. LDAP를 두 번 클릭합니다.

LDAP 인증이 구성되면 LDAP 서버 구성 요약 페이지가 나타납니다. 이 페이지에서 연결 매개 변수 영역 또는 필드를 변경할 수 있습니다. 매핑된 LDAP 멤버 그룹 영역도 수정할 수 있습니다.

3. 현재 매핑된 그룹 중에서 새 연결 설정으로 더 이상 액세스할 수 없는 그룹을 삭제한 다음 업데이트를 클릭합니다.
4. 연결 설정을 변경한 다음 업데이트를 클릭합니다.
5. 별칭 및 새 사용자 옵션을 변경한 다음 업데이트를 클릭합니다.
6. 새 LDAP 멤버 그룹을 매핑한 다음 업데이트를 클릭합니다.

7.3.2.5 SiteMinder에 대해 LDAP 플러그 인 구성

이 단원에서는 SiteMinder에서 LDAP를 사용하도록 CMC를 구성하는 방법을 설명합니다. SiteMinder는 BI 플랫폼에 대한 단일 로그인을 생성하기 위해 LDAP 보안 플러그 인과 함께 사용할 수 있는 타사 사용자 액세스 및 인증 도구입니다.

BI 플랫폼에서 SiteMinder 및 LDAP를 사용하려면 다음 두 위치에서 구성을 변경해야 합니다.

- CMC를 통한 LDAP 플러그 인
- BOE.war 파일 속성

참고:

SiteMinder 관리자가 4.x 에이전트에 대한 지원 기능을 활성화했는지 확인합니다. 이 작업은 사용 중인 SiteMinder의 지원되는 버전에 관계없이 수행해야 합니다. SiteMinder에 대한 추가 정보와 설치 방법은 SiteMinder 설명서를 참조하십시오.

관련 항목

- 232 페이지에서 [LDAP 호스트 구성](#)

7.3.2.5.1 SiteMinder로 단일 로그온을 위해 LDAP를 구성하려면

1. 다음 방법 중 하나를 사용하여 SiteMinder 설정을 구성하십시오. 화면을 엽니다.
 - LDAP 구성 마법사의 "LDAP 단일 로그온 인증 방식을 선택하십시오." 화면에서 SiteMinder를 선택합니다.
 - LDAP를 이미 구성한 상태에서 SSO를 추가할 때 사용할 수 있는 LDAP 인증 화면에서 "단일 로그온 유형" 링크를 선택합니다.
2. 정책 서버 호스트 입력란에 정책 서버의 이름을 입력하고 추가를 클릭합니다.
3. 각 정책 서버 호스트에 대해 계정, 인증 및 인증 포트 번호를 지정합니다.
4. 에이전트 이름 및 공유 암호를 입력합니다. 공유 암호를 다시 입력합니다.
5. 다음을 클릭합니다.
6. 이어서 LDAP 옵션 구성 작업을 진행합니다.

7.3.2.5.2 BOE.war 파일에서 LDAP 및 SiteMinder 활성화

LDAP 보안 플러그 인에 SiteMinder 설정을 지정하는 것 이외에 BOE.war 속성에도 SiteMinder 설정을 지정해야 합니다.

1. BI 플랫폼이 설치된 다음 디렉터리로 이동합니다.
 <INSTALLDIR>WSAP BusinessObjects Enterprise XI
 4.0\Warfiles\Webapps\BOE\WEB-INF\config\customW
2. 새 파일을 만듭니다.

참고:

메모장이나 다른 텍스트 편집 유틸리티를 사용하십시오.

3. 파일을 닫고 다음 이름으로 저장합니다.
 BIlaunchpad.properties
4. 다음 문을 입력합니다.

```
siteminder.authentication=secLDAP
siteminder.enabled=true
```

5. 파일을 닫고 다음 이름으로 저장합니다.

global.properties

참고:

파일 이름에 .txt 등의 확장자가 붙지 않도록 하십시오.

6. 같은 디렉터리에 다른 파일을 만듭니다.

7. 다음 문을 입력합니다.

```
authentication.default=LDAP
cms.default=[enter your cms name]:[Enter the CMS port number]
```

예:

```
authentication.default=LDAP
cms.default=mycms:6400
```

8. 파일을 닫고 다음 이름으로 저장합니다.

bilaunchpad.properties

웹 응용 프로그램 서버를 실행하는 컴퓨터에 수정된 BOE 웹 응용 프로그램을 다시 배포해야 새 속성이 적용됩니다. WDeploy를 사용하여 웹 응용 프로그램 서버에 WAR 파일을 다시 배포하십시오. WDeploy에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 웹 응용 프로그램 배포 가이드를 참조하십시오.

7.3.3 LDAP 그룹 매핑

LDAP 구성 마법사로 LDAP 호스트 구성을 마치고 나면 LDAP 그룹을 Enterprise 그룹에 매핑할 수 있습니다.

LDAP 그룹을 매핑하고 나면 인증 관리 영역의 LDAP 옵션을 클릭하여 이 그룹을 볼 수 있습니다. LDAP 인증이 구성되면 BI 플랫폼에 매핑된 LDAP 그룹이 "매핑된 LDAP 멤버 그룹" 영역에 표시됩니다.

LDAP 보안 플러그인을 통해 BI 플랫폼에서 인증할 Windows AD 그룹을 매핑할 수도 있습니다.

참고:

AD에 대해 LDAP를 구성한 경우 AD 그룹을 매핑하는 절차는 다음과 같습니다.

관련 항목

- 246 페이지에서 [Windows AD에 대해 LDAP 매핑](#)

7.3.3.1 BI 플랫폼을 사용하여 LDAP 그룹 매핑

1. CMC의 인증 관리 영역으로 이동합니다.

2. LDAP를 두 번 클릭합니다.

LDAP 인증이 구성되면 LDAP 요약 페이지가 나타납니다.

3. "매핑된 LDAP 멤버 그룹" 영역의 LDAP 그룹 추가(일반 이름 또는 고유 이름) 필드에서 일반 이름 또는 고유 이름을 사용하여 LDAP 그룹을 지정한 다음 추가를 클릭합니다.

이 단계를 반복하여 LDAP 그룹을 두 개 이상 추가할 수 있습니다. 그룹을 제거하려면 LDAP 그룹을 강조 표시한 다음 삭제를 클릭합니다.

4. 새 별칭 옵션을 사용하여 LDAP 별칭을 Enterprise 계정에 매핑하는 방법을 지정할 수 있습니다. 다음 중 하나를 선택합니다.

- 추가된 각 LDAP 별칭을 같은 이름의 계정에 할당

사용자에게 같은 이름의 기존 Enterprise 계정이 있다는 것을 아는 경우 이 옵션을 사용합니다. 즉, LDAP 별칭이 기존 사용자에게 할당됩니다(자동 별칭 만들기 사용). 기존 Enterprise 계정이 없는 사용자 또는 Enterprise 및 LDAP 계정에 같은 이름이 없는 사용자는 새 LDAP 사용자로 추가됩니다.

또는

- 추가된 모든 LDAP 별칭에 대해 새 계정 만들기

각 사용자에게 대해 새 계정을 만들려는 경우 이 옵션을 사용합니다.

5. 업데이트 옵션을 사용하여 모든 새 사용자에게 대해 LDAP 별칭을 자동으로 만들지 여부를 지정할 수 있습니다. 다음 중 하나를 선택합니다.

- 새 별칭을 추가하고 새 사용자 만들기

BI 플랫폼에 매핑된 모든 LDAP 사용자에게 대해 자동으로 새 별칭을 만들려면 이 옵션을 사용합니다. BI 플랫폼 계정이 없는 사용자나 "추가된 모든 LDAP 별칭에 대해 새 계정 만들기" 옵션을 선택하고 업데이트를 클릭한 경우 모든 사용자에게 대해 새 LDAP 계정이 추가됩니다.

또는

- 새 별칭을 추가하지 않고 새 사용자를 만들지 않음

매핑하는 LDAP 디렉터리에 여러 사용자가 들어 있지만 그 중 일부만 BI 플랫폼을 사용하는 경우 이 옵션을 사용합니다. 모든 사용자에게 대해 별칭과 Enterprise 계정이 자동으로 생성되지 않습니다. 대신 BI 플랫폼에 로그인하는 사용자에게 대해서만 별칭 및 계정(필요한 경우)이 생성됩니다.

6. 새 사용자 옵션을 사용하여 LDAP 계정에 매핑하기 위해 만들어진 새 Enterprise 계정의 속성을 지정할 수 있습니다.

SAP BusinessObjects Business Intelligence 플랫폼 라이선스가 사용자 역할을 기반으로 하는 경우, 다음 새 사용자 옵션 중 하나를 선택하십시오.

- BI Viewer

새 사용자 계정이 BI Viewer 역할에 구성됩니다. BI Viewer 역할의 모든 계정에 대한 BI 플랫폼 응용 프로그램 액세스 권한이 사용권 계약에 정의됩니다. 사용자는 BI Viewer 역할용으로 정의된 응용 프로그램 워크플로에만 액세스할 수 있습니다. 액세스 권한은 일반적으로 비즈니스

스 인텔리전스 문서를 보는 것으로 제한됩니다. 이 역할은 일반적으로 BI 플랫폼 응용 프로그램을 통해 콘텐츠를 사용하는 사용자에게 적합합니다.

- BI Analyst

새 사용자 계정이 BI Analyst 역할에 구성됩니다. BI Analyst 역할의 모든 계정에 대한 BI 플랫폼 응용 프로그램 액세스 권한이 사용권 계약에 정의됩니다. 사용자는 BI Analyst 역할에 대해 정의된 모든 응용 프로그램 워크플로에 액세스할 수 있습니다. 액세스 권한에는 비즈니스 인텔리전스 문서를 보고 수정하는 것이 포함됩니다. 이 역할은 일반적으로 BI 플랫폼 응용 프로그램의 콘텐츠를 만들고 수정하는 사용자에게 적합합니다.

SAP BusinessObjects Business Intelligence 플랫폼 라이선스가 사용자 역할을 기반으로 하지 않는 경우에는 다음 옵션 중 하나를 선택하십시오.

- 새 사용자를 명명된 사용자로 만들기

새 사용자 계정이 명명된 사용자 라이선스를 사용하도록 구성됩니다. 명명된 사용자 라이선스는 특정 사용자와 관련되며 이 라이선스를 사용하면 사용자 이름과 암호를 기반으로 시스템에 액세스할 수 있습니다. 이 옵션을 사용하면 명명된 사용자는 연결된 다른 사용자 수에 관계없이 시스템에 액세스할 수 있습니다. 이 옵션을 사용하여 만든 각 사용자 계정에 대한 명명된 사용자 라이선스가 있어야 합니다.

- 새 사용자를 동시 사용자로 만들기

새 사용자 계정이 동시 사용자 라이선스를 사용하도록 구성됩니다. 동시 라이선스는 BI 플랫폼에 동시에 연결할 수 있는 사용자 수를 지정합니다. 이 라이선스 유형은 소규모 동시 라이선스로 많은 사용자 기반을 지원할 수 있으므로 매우 유연합니다. 예를 들어 사용자가 해당 시스템에 액세스하는 빈도 및 시간에 따라 100개의 동시 사용자 라이선스로 250명, 500명 또는 700명의 사용자를 지원할 수 있습니다.

7. 업데이트를 클릭합니다.

관련 항목

- 90 페이지에서 [역할 기반 라이선스](#) "

7.3.3.2 BI 플랫폼을 사용하여 LDAP 그룹 매핑 해제

1. CMC의 인증 관리 영역으로 이동합니다.

2. LDAP를 두 번 클릭합니다.

LDAP 인증이 구성되면 LDAP 요약 페이지가 나타납니다.

3. "매핑된 LDAP 멤버 그룹" 영역에서 제거할 LDAP 그룹을 선택합니다.

4. 삭제를 클릭한 다음 업데이트를 클릭합니다.

이제 이 그룹의 사용자는 BI 플랫폼에 액세스할 수 없습니다.

참고:

사용자에게 Enterprise 계정의 별칭이 있는 경우는 예외입니다. 액세스를 제한하려면 사용자의 Enterprise 계정을 비활성화하거나 삭제합니다.

모든 그룹에 대해 LDAP 인증을 거부하려면 "LDAP 인증 사용" 확인란의 선택을 취소하고 업데이트를 클릭합니다.

7.3.3.3 Windows AD에 대해 LDAP 매핑

Windows AD(AD)에 대해 LDAP를 구성하는 경우 다음과 같은 제한이 있습니다.

- AD에 대해 LDAP를 구성하면 사용자를 매핑할 수 있지만 AD 단일 로그인 또는 데이터베이스에 대한 단일 로그인 구성할 수 없습니다. 그러나 SiteMinder 등의 LDAP 단일 로그인 방법 및 신뢰할 수 있는 인증은 계속 사용할 수 있습니다.
- AD의 기본 그룹에만 속하는 사용자는 로그인할 수 없습니다. 사용자는 AD에서 명시적으로 만든 다른 그룹의 멤버여야 하며 해당 그룹을 매핑해야 합니다. 이러한 그룹의 예로는 "도메인 사용자" 그룹을 들 수 있습니다.
- 매핑된 도메인 로컬 그룹의 포리스트에 다른 도메인의 사용자가 포함되어 있는 경우 해당 사용자는 로그인할 수 없습니다.
- LDAP 호스트로 지정된 DC가 아닌 도메인의 유니버설 그룹에 속하는 사용자는 로그인할 수 없습니다.
- LDAP 플러그 인을 사용하여 BI 플랫폼이 설치된 포리스트 외부의 AD 포리스트에서 사용자와 그룹을 매핑할 수 없습니다.
- AD의 도메인 사용자 그룹에서는 매핑할 수 없습니다.
- 컴퓨터 로컬 그룹은 매핑할 수 없습니다.
- 글로벌 카탈로그 도메인 컨트롤러를 사용하는 경우 AD에 대해 LDAP를 매핑할 때 추가로 고려해야 할 사항이 있습니다.

상황	고려 사항
여러 도메인에서 글로벌 카탈로그 도메인 컨트롤러를 가리키는 경우	<p>다음 그룹에서 매핑을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> • 자식 도메인의 유니버설 그룹 • 자식 도메인의 유니버설 그룹이 포함된 동일한 도메인의 그룹 • 상호 도메인의 유니버설 그룹 <p>다음 그룹에서 매핑을 수행할 수 없습니다.</p> <ul style="list-style-type: none"> • 자식 도메인의 글로벌 그룹 • 자식 도메인의 로컬 그룹 • 자식 도메인의 글로벌 그룹이 포함된 동일한 도메인의 그룹 • 상호 도메인 글로벌 그룹 <p>일반적으로 그룹이 유니버설 그룹인 경우 상호 도메인이거나 자식 도메인의 사용자를 지원합니다. 다른 그룹에 상호 도메인이거나 자식 도메인의 사용자가 포함된 경우 이를 매핑할 수 없습니다. 대상 도메인 내에서 도메인 로컬, 글로벌 및 유니버설 그룹을 매핑할 수 있습니다.</p>
유니버설 그룹의 매핑	유니버설 그룹에서 매핑을 수행하려면 글로벌 카탈로그 도메인 컨트롤러를 가리켜야 합니다. 또한 기본 포트 번호인 389 대신 포트 번호 3268을 사용해야 합니다.

- 여러 개의 도메인을 사용하지만 글로벌 카탈로그 도메인 컨트롤러를 가리키지 않는 경우에는 상호 도메인이거나 자식 도메인의 어떠한 형식의 그룹에서도 매핑할 수 없습니다. 대상으로 가리키고 있는 특정 도메인의 경우에만 모든 그룹 유형에서 매핑을 수행할 수 있습니다.

7.3.3.4 LDAP 계정 문제 해결

- LDAP 사용자 계정을 새로 만드는 경우, 계정이 BI 플랫폼에 매핑된 그룹 계정에 속하지 않으면 그룹을 매핑하거나 시스템에 이미 매핑된 그룹에 새로운 LDAP 사용자 계정을 추가합니다.
- 새 LDAP 사용자 계정을 만들 때 해당 계정이 BI 플랫폼에 매핑된 그룹 계정에 속하는 경우라면 사용자 목록을 새로 고치십시오.

관련 항목

- 232 페이지에서 [LDAP 인증 구성](#)
- 243 페이지에서 [LDAP 그룹 매핑](#)

7.4 Windows AD 인증

7.4.1 개요

7.4.1.1 Windows AD 인증 사용

이 단원에서는 Windows AD(Active Directory) 인증과 BI 플랫폼이 함께 작동하는 방식을 일반적으로 설명합니다. 다음으로 BI 플랫폼에서 AD 계정 사용 및 관리에 필요한 관리 워크플로를 소개합니다. 단원의 마지막 부분에는 문제 해결을 위한 기본적인 팁이 제공됩니다.

지원 요구 사항

BI 플랫폼에서 AD 인증을 사용하려면 다음 지원 요구 사항을 고려해야 합니다.

- 지원되는 Windows 플랫폼에 항상 CMS가 설치되어 있어야 합니다.
- Windows 2003, 2008 및 지원되는 플랫폼은 Kerberos와 NTLM 인증을 모두 지원하지만 특정 인증 방법만 사용하는 BI 플랫폼 응용 프로그램도 있습니다. 예를 들어 BI 실행 패드 및 중앙 관리 콘솔(CMC)과 같은 응용 프로그램은 Kerberos만 지원합니다.

기본적인 AD 인증 워크플로

BI 플랫폼에서 AD 인증을 사용하려면 다음과 같은 기본 워크플로를 따라야 합니다.

1. 필요한 도메인 컨트롤러 리소스를 구성합니다.
2. Windows AD 인증을 사용하도록 BI 플랫폼 호스트를 준비합니다.

3. AD 보안 플러그 인을 활성화하고 AD 그룹에서 매핑합니다.
4. 인증 방법을 선택합니다.
 - Kerberos를 사용한 Windows AD
 - NTLM을 사용한 Windows AD
5. BI 플랫폼 응용 프로그램에 대한 단일 로그인 설정합니다. 다음과 같은 방법을 통해 이 선택적 단계를 수행할 수 있습니다.
 - Vintela를 사용한 Windows AD(Kerberos)
 - SiteMinder를 사용한 Windows AD(Kerberos)

7.4.1.1.1 Windows AD 보안 플러그 인

Windows AD 보안 플러그인을 통해 Microsoft AD(Active Directory) 2003 및 2008 사용자 데이터베이스의 사용자 계정과 그룹을 BI 플랫폼에 매핑할 수 있습니다. AD 인증을 지정하는 모든 로그인 요청을 시스템에서 확인할 수 있습니다. 중앙 관리 서버(CMS)는 사용자가 AD 사용자 데이터베이스에 대해 인증받고 매핑된 AD 그룹의 소속 여부를 확인받은 후에 사용자에게 활성 BI 플랫폼 세션을 승인합니다.

Windows AD 보안 플러그 인을 통해 다음을 구성할 수 있습니다.

- NTLM을 사용한 Windows AD 인증
- Kerberos를 사용한 Windows AD 인증
- 단일 로그인을 위한 SiteMinder 사용 Windows AD 인증

Windows AD 보안 플러그 인은 기본 모드 또는 혼합 모드에서 실행되는 Microsoft Active Directory 2003 및 2008 도메인과 호환됩니다.

AD 사용자와 그룹을 매핑하고 나면 AD 인증을 통해 BI 플랫폼 클라이언트 도구에 액세스할 수 있습니다.

- Windows AD 인증은 CMS가 Windows에서 실행되는 경우에만 작동합니다. 데이터베이스에 대해 단일 로그인을 사용하려면 보고서 작성 서버도 Windows에서 실행되어야 합니다. 그렇지 않은 경우에는 다른 모든 서버와 서비스를 지원하는 모든 플랫폼에서 실행할 수 있습니다.
- BI 플랫폼용 Windows AD 플러그 인은 여러 포리스트 내부의 도메인을 지원합니다.

7.4.1.1.2 Windows AD 사용자 및 그룹 사용

BI 플랫폼은 Windows 보안 플러그 인을 통해 AD(Active Directory) 인증을 지원합니다. Windows 보안 플러그 인은 Windows 플랫폼에 제품을 설치할 때 기본으로 포함됩니다. Windows AD 인증을 지원한다는 것은 Microsoft Active Directory 2003 및 2008에서 만든 사용자와 그룹 계정을 사용하여 BI 플랫폼에서 인증할 수 있다는 의미입니다. 그러므로 시스템 관리자는 BI 플랫폼 내에서 각 사용자와 그룹을 설정하는 대신 기존 AD 계정을 매핑할 수 있습니다.

7.4.1.1.2.1 Windows AD 그룹 업데이트 예약

BI 플랫폼을 통해 관리자는 Windows AD 그룹과 사용자 별칭에 대한 업데이트를 예약할 수 있습니다. 이 기능은 Kerberos 또는 NTLM을 통한 AD 인증에 대해서만 사용할 수 있습니다. 또한 CMC에서 마지막 업데이트가 수행된 시간과 날짜를 확인할 수 있습니다.

참고:

AD 인증이 BI 플랫폼에서 작동하려면 AD 그룹과 별칭에 대한 업데이트 일정 설정 방식을 구성해야 합니다.

업데이트를 예약할 때 다음 표에 요약된 되풀이 패턴 중 하나를 선택할 수 있습니다.

되풀이 패턴	설명
매시간	업데이트가 매시간 실행됩니다. 시작할 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매일	업데이트가 매일 실행되거나 지정된 일 수 간격으로 실행됩니다. 실행할 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매주	업데이트가 매주 실행됩니다. 개체를 매주 한 번 또는 여러 번 실행할 수 있으며 실행할 시간 및 날짜를 지정하고 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월	업데이트가 매월 또는 몇 달 간격으로 실행됩니다. 업데이트 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 N일	매월 특정 날짜에 업데이트가 실행됩니다. 실행 날짜와 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 첫째 월요일	업데이트가 매월 첫 번째 월요일에 실행됩니다. 업데이트 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.

되풀이 패턴	설명
매월 마지막 날	업데이트가 매월 마지막 날 실행됩니다. 업데이트 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 N번째 주 X	업데이트가 매월 지정된 주의 지정된 요일에 실행됩니다. 업데이트 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
달력	이전에 생성된 달력에 지정한 날짜에 업데이트가 실행됩니다.

AD 그룹 업데이트 예약

BI 플랫폼은 AD(Active Directory)에서 사용자 및 그룹 정보를 가져옵니다. AD 플러그 인은 AD로 전송되는 쿼리의 양을 최소화하기 위해 그룹에 대한 정보 및 그룹 간의 관계와 사용자 소속 그룹과의 관계에 대한 정보를 캐시에 보관합니다. 특정 일정이 정의되지 않은 경우 업데이트가 실행되지 않습니다.

그룹 업데이트 새로 고침이 되풀이되는 방식을 구성하려면 CMC를 사용해야 합니다. 소속 그룹 정보를 얼마나 자주 수정할지에 맞춰 예약을 구성합니다.

AD 사용자 별칭 업데이트 예약

사용자가 AD 자격 증명을 사용하여 BI 플랫폼에 로그인할 수 있도록 Windows AD(Active Directory) 계정의 별칭을 사용자 개체로 지정할 수 있습니다. AD 계정에 대한 업데이트는 AD 플러그 인에 의해 BI 플랫폼으로 전파됩니다. AD에서 생성, 삭제 또는 비활성화된 계정은 BI 플랫폼에서도 생성, 삭제 또는 비활성화됩니다.

AD 별칭 업데이트를 예약하지 않으면 다음과 같은 경우에만 AD 별칭이 업데이트됩니다.

- 사용자가 로그인하는 경우
- 관리자가 CMC의 주문형 AD 업데이트 영역에서 지금 AD 그룹 및 별칭 업데이트 를 선택하는 경우

참고:

AD 암호는 사용자 별칭에 저장되지 않습니다.

7.4.1.1.3 Windows AD 사용 단일 로그인

Windows AD 보안 플러그 인은 단일 로그인을 지원하므로 인증된 AD 사용자는 자격 증명을 명시적으로 입력하지 않고도 BI 플랫폼에 로그인할 수 있습니다. 단일 로그인에 필요한 요구 사항은 사용자가 썸(thick) 클라이언트 또는 웹 중 어떠한 경로를 통해 BI 플랫폼에 액세스하는지에 따라 달라집니다. 두 시나리오 모두에서 보안 플러그 인은 인증 공급자로부터 사용자의 보안 컨텍스트를 얻고, 사용자가 매핑된 AD 그룹의 멤버인 경우 이 사용자에게 활성 BI 플랫폼 세션을 허용합니다.

가장 일반적인 활용 사례는 BI 실행 패드 웹 응용 프로그램에 대한 단일 로그인입니다.

데이터베이스에 대한 단일 로그인

Windows AD 플러그인은 데이터베이스에 대한 단일 로그인을 지원합니다. 적절히 인증된 AD 사용자는 BI 실행 패드 응용 프로그램에서 보고서에 액세스할 때 자신의 계정 자격 증명을 입력할 필요가 없습니다.

관련 항목

- 275 페이지에서 [SiteMinder와 함께 Windows AD 사용 "](#)
- 266 페이지에서 [Vintela 단일 로그인을 사용한 Windows AD 인증\(Kerberos\) 구성"](#)

7.4.2 AD 인증(Kerberos) 준비

7.4.2.1 Kerberos와 함께 Windows AD 인증 사용

이 단원에서는 BI 플랫폼에 Kerberos 인증을 설정하기 위해 필요한 작업을 설명합니다. 필요한 모든 사전 작업이 완료되면 Windows AD 보안 플러그인에서 Kerberos용 Windows AD 인증 옵션 구성을 진행할 수 있습니다.

권장 워크플로

Windows AD 인증을 제대로 설정하기 위해서는 다음 사전 작업을 완료해야 합니다.

- BI 플랫폼을 실행할 수 있도록 서비스 계정 설정
- Kerberos 사용 Windows AD 인증을 위한 BI 플랫폼 서버 준비
- Kerberos 사용 Windows AD 인증을 위한 웹 응용 프로그램 서버 구성

7.4.2.1.1 Kerberos 사용 AD 인증을 위한 서비스 계정 설정

Kerberos 및 Windows AD 인증을 위해 BI 플랫폼을 구성하려면 서비스 계정이 필요합니다. 도메인 계정을 새로 만들거나 기존 도메인 계정을 사용할 수 있습니다. 서비스 계정은 BI 플랫폼 서버를 실행하는 데 사용됩니다.

참고:

서비스 계정을 설정한 후에는 이 계정에 적절한 권한을 부여해야 합니다.

Windows 2003 또는 2008 도메인을 사용하는 경우 제한된 위임을 설정할 수도 있습니다.

7.4.2.1.1.1 Windows 2003 또는 2008 도메인에 서비스 계정 설정

Kerberos를 사용한 Windows AD 인증이 성공적으로 실행되도록 하려면 도메인 컨트롤러에 새 서비스 계정을 설정해야 합니다. 이 서비스 계정은 특정 Windows AD 그룹의 사용자의 BI 실행 패드에 대한 단일 로그인을 허용하기 위한 목적으로 사용됩니다. 이 작업은 AD 도메인 컨트롤러 컴퓨터에서 수행됩니다.

1. 도메인 컨트롤러에 암호를 사용하여 새 계정을 만들거나 기존 계정을 사용합니다.

자세한 지침은 <http://msdn.microsoft.com/> 을 참조하십시오.

2. keytabktpass 명령을 실행하여 Kerberos keytab 파일을 작성하여 저장합니다.

다음 표에 나열된 ktpass 매개 변수를 지정해야 합니다.

매개 변수	설명
-out	생성할 Kerberos keytab 파일 이름을 지정합니다.
-mapuser	SPN이 매핑되는 사용자 계정의 이름을 지정합니다. Server Intelligence Agent가 실행되는 계정입니다.
-pass	서비스 계정에서 사용하는 암호를 지정합니다.
-kvno	키를 만드는 데 사용되는 키 버전 번호를 지정합니다.
-ptype	보안 주체 유형을 지정합니다. 다음과 같이 지정해야 합니다. -ptype KRB5_NT_PRINCIPAL
-crypto	서비스 계정에서 사용할 암호화 유형을 지정합니다. 다음을 사용합니다. -crypto RC4-HMAC-NT

예를 들면 다음과 같습니다.

```
ktpass -out -mapuser sbo.serviceDOMAIN.COM -pass password
-kvno 255 -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

ktpass 명령의 결과는 대상 도메인 컨트롤러를 확인하고 공유 암호가 포함된 Kerberos keytab 파일이 생성되었는지 확인해야 합니다. 이 명령은 또한 보안 주체 이름을 (로컬) 서비스 계정에 매핑합니다.

3. setspn -i 명령을 실행하여 ktpass 명령이 성공적으로 실행되었는지 확인합니다.
표시 출력에는 로컬 서비스 계정에 등록된 모든 서비스 보안 주체 이름이 나열됩니다.
4. 1단계에서 만든 서비스 계정을 마우스 오른쪽 단추로 클릭하고 속성 > 위임을 선택합니다.
5. 모든 서비스에 대한 위임용으로 이 사용자 트러스트(Kerberos만)를 선택합니다.
6. 설정 내용을 저장하려면 확인을 클릭합니다.

생성한 서비스 계정은 권한을 부여하고 서버의 로컬 관리자 그룹에 추가해야 합니다.

7.4.2.1.1.2 서비스 계정에 권한 부여

Windows AD 및 Kerberos를 지원하려면 운영 체제의 일부로 작동할 수 있는 권한을 서비스 계정에 부여해야 합니다. 이 작업은 중앙 관리 서버(CMS)와 함께 SIA(Server Intelligence Agent)를 실행하는 각 컴퓨터에서 수행해야 합니다.

데이터베이스에 대한 단일 로그인에 필요한 경우, SIA에는 다음 서버가 포함되어야 합니다.

- Crystal Reports 처리 서버
- Report Application Server
- Web Intelligence 처리 서버

참고:

데이터베이스에 대한 단일 로그인이 작동하도록 하려면 서비스 계정을 위임용으로 트러스터할 수 있어야 합니다.

7.4.2.1.1.2.1 서비스 계정에 권한 부여

1. 시작 > 제어판 > 관리 도구 > 로컬 보안 정책을 클릭합니다.
2. 로컬 정책을 확장한 다음 사용자 권한 할당을 클릭합니다.
3. 운영 체제의 일부로 작동을 두 번 클릭합니다.
4. 추가를 클릭합니다.
5. 만든 서비스 계정의 이름을 입력한 다음 확인을 클릭합니다.
6. 로컬 정책 설정 확인란이 선택되어 있는지 확인하고 확인을 클릭합니다.
7. BI 플랫폼 서버를 실행하는 각 컴퓨터에서 위의 단계를 반복합니다.

참고:

운영 체제의 일부로 작동을 선택한 후에는 유효 권한을 확인하는 작업으로 마무리하는 것이 중요합니다. 일반적으로 이렇게 하려면 서버를 다시 시작해야 합니다. 서버를 다시 시작한 후에도 이 옵션이 여전히 설정되지 않으면 로컬 정책 설정이 도메인 정책 설정에 의해 무시되는 상태입니다.

7.4.2.1.1.3 서버의 로컬 관리자 그룹에 서비스 계정 추가

Kerberos를 지원하려면 다음 서비스 중 하나가 배포되어 있는 SIA를 포함하는 각 서버의 로컬 관리자 그룹에 속한 서비스 계정을 사용해야 합니다.

- CMS
- Crystal Reports 처리 서버(SSO2DB에만 필요)
- Report Application Server(SSO2DB에만 필요)
- Web Intelligence 처리 서버(SSO2DB에만 필요)

참고:

SSO2DB를 사용하는 경우에는 위임에 대해 신뢰된 서비스 계정이 필요합니다. 또한 서버에 대한 관리 권한도 있어야 합니다.

7.4.2.1.1.3.1 관리자 그룹에 계정 추가

1. 원하는 컴퓨터에서 내 컴퓨터를 마우스 오른쪽 단추로 클릭한 다음 관리를 클릭합니다.
2. 시스템 도구 > 로컬 사용자 및 그룹 > 그룹으로 이동합니다.

3. 관리자를 마우스 오른쪽 단추로 클릭한 다음 그룹에 추가를 클릭합니다.
4. 추가를 클릭하고 서비스 계정의 로그인 이름을 입력합니다.
5. 이름 확인을 클릭하여 계정을 확인합니다.
6. 확인을 클릭한 다음 확인을 다시 클릭합니다.
7. 구성해야 하는 각 BI 플랫폼 서버에 대해 이 단계를 반복합니다.

7.4.2.1.2 Kerberos 사용 Windows AD 인증을 위한 서버 준비

서비스 계정을 생성하고 Kerberos를 사용한 Windows AD 인증용으로 구성된 후에는 BI 플랫폼 배포 환경의 각 SIA를 해당 계정으로 실행해야 합니다.

7.4.2.1.2.1 서비스 계정에서 SIA 구성

Kerberos를 사용한 Windows AD 인증용으로 생성한 서비스 계정에서 사용되는 서비스를 실행하는 모든 SIA(Server Intelligence Agent)에 대해 다음 단계를 수행해야 합니다.

1. 모든 프로그램 > SAP BusinessObjects Enterprise XI 4.0 > SAP BusinessObjects Enterprise > 중앙 구성 관리자 로 이동합니다.
2. CCM에서 SIA(Server Intelligence Agent)를 마우스 오른쪽 단추로 클릭하고 중지를 선택합니다.

참고:

SIA를 중지하면 SIA에서 관리하던 모든 서비스가 중지됩니다.

3. SIA를 마우스 오른쪽 단추로 클릭한 다음 속성을 선택합니다.
4. 시스템 계정 확인란 선택을 취소합니다.
5. 서비스 계정 자격 증명(DOMAINNAME\서비스 이름)을 입력하고 확인을 클릭합니다.
6. SIA를 다시 시작합니다.
7. 필요한 경우 구성해야 할 서비스를 실행하고 있는 각 SIA에 대해 1-5단계를 반복합니다.

7.4.2.1.3 Windows AD 인증(Kerberos)을 위한 응용 프로그램 서버 준비

이 단원에서는 다음 응용 프로그램 서버에서 사용하기 위해 Kerberos를 구성하는 데 관련된 작업에 대해 설명합니다.

- Tomcat
- WebSphere
- WebLogic
- Oracle Application Server
- SAP NetWeaver 7.10

이 단원에는 다음 정보가 포함되어 있습니다.

- 특정 웹 응용 프로그램 서버별 워크플로. 응용 프로그램 서버마다 JAAS(Java 인증 및 권한 부여 서비스)를 다르게 구현하므로 이 워크플로는 반드시 필요합니다.
- 워크플로의 각 단계에 대한 자세한 절차
- Java 응용 프로그램 서버용 샘플 Krb5.ini 파일

7.4.2.1.3.1 개요

웹 응용 프로그램 서버를 위한 Kerberos 구성의 특정 프로세스는 특정 응용 프로그램 서버에 따라 조금씩 다릅니다. 하지만 일반적인 Kerberos 구성 프로세스에는 다음 단계가 포함됩니다.

- Kerberos 구성 파일 만들기
- JAAS 로그인 구성 파일 만들기

참고:

이 단계는 SAP NetWeaver 7.10 Java 응용 프로그램 서버에는 필요하지 않습니다. 하지만 LoginModule을 SAP NetWeaver 서버에 추가해야 합니다.

- Java 옵션 수정
- Java 응용 프로그램 서버 다시 시작

7.4.2.1.3.1.1 SAP NetWeaver, Tomcat, WebLogic, SAP NetWeaver 또는 Oracle용 Kerberos 구성 파일 만들기

SAP Netweaver 7.10, Tomcat 6, Oracle Application Server 또는 WebLogic을 사용할 경우 다음 단계에 따라 Kerberos 구성 파일을 만듭니다.

1. krb5.ini 파일이 없으면 이 파일을 만들어 Windows의 C:\WINNT 아래 저장합니다.

참고:

- 응용 프로그램 서버가 UNIX에 설치된 경우 다음 디렉터리를 사용해야 합니다.
Solaris: /etc/krb5/krb5.conf
Linux: /etc/krb5.conf
- 다른 위치에 이 파일을 저장할 수 있지만, 이렇게 하려면 java 옵션에서 파일의 위치를 지정해야 합니다. krb5.ini에 대한 자세한 내용은 <http://docs.sun.com/app/docs/doc/816-0219/6m6njqb94?a=view>를 참조하십시오.

2. Kerberos 구성 파일에 다음 필수 정보를 추가합니다.

```
[libdefaults]
default_realm = DOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
[domain_realm]
.domain.com = DOMAIN.COM
domain.com = DOMAIN.COM
.domain2.com = DOMAIN2.COM
domain2.com = DOMAIN2.COM
[realms]
DOMAIN.COM = {
default_domain = DOMAIN.COM
kdc = HOSTNAME.DOMAIN.COM
}
DOMAIN2.COM = {
default_domain = DOMAIN2.COM
kdc = HOSTNAME.DOMAIN2.COM
}
[capaths]
DOMAIN2.COM = {
DOMAIN.COM =
```

참고:

DOMAIN.COM은 도메인의 DNS 이름이며 FQDN 형식에 따라 대문자로 입력해야 합니다. kdc는 도메인 컨트롤러의 호스트 이름입니다. 사용자가 여러 도메인에서 로그인하는 경우 [realms] 섹션에 여러 도메인 항목을 추가할 수 있습니다. [capath]는 다른 AD 포리스트에 있는 도메인 간의 신뢰를 정의합니다. 위 예제에서 DOMAIN2.COM은 외부 포리스트의 도메인이며 DOMAIN.COM과 직접 양방향 전이 신뢰 관계입니다. 복수 도메인 구성에서는 [libdefaults] 아래의 default_realm

값이 소스 도메인일 수도 있습니다. 따라서 이러한 경우에는 AD 계정을 사용하여 인증할 사용자 수가 가장 많은 도메인을 사용하는 것이 좋습니다. 로그인 시 UPN 접미사가 제공되지 않은 경우 기본값인 default_realm이 사용됩니다. 이 값은 CMC의 기본 도메인 설정과 일치해야 합니다.

관련 항목

- 262 페이지에서 [Tomcat에서 Kerberos에 대한 Java 옵션을 수정하려면](#)

7.4.2.1.3.1.2 WebSphere에 대한 Kerberos 구성 파일 만들기

1. krb5.ini 파일이 없으면 이 파일을 만들어 Windows의 C:\WINNT 아래 저장합니다.

참고:

다른 위치에 이 파일을 저장할 수 있지만, 이렇게 하려면 java 옵션에서 파일의 위치를 지정해야 합니다.

2. Kerberos 구성 파일에 다음 필수 정보를 추가합니다.

```
[libdefaults]
default_realm = DOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
[domain_realm]
.domain.com = DOMAIN.COM
domain.com = DOMAIN.COM
.domain2.com = DOMAIN2.COM
domain2.com = DOMAIN2.COM
[realms]
DOMAIN.COM = {
default_domain = DOMAIN.COM
kdc = HOSTNAME.DOMAIN.COM
}
DOMAIN2.COM = {
default_domain = DOMAIN2.COM
kdc = HOSTNAME.DOMAIN2.COM
}
[capaths]
DOMAIN2.COM = {
DOMAIN.COM =
```

참고:

- DES 암호화를 사용하는 경우 rc4-hmac를 des-cbc-crc로 변경합니다.
- DOMAIN.COM은 도메인의 DNS 이름이며 FQDN 형식에 따라 대문자로 입력해야 합니다.
- hostname은 도메인 컨트롤러의 호스트 이름입니다.

3. 파일을 저장하고 닫습니다.

관련 항목

- 265 페이지에서 [WebSphere에서 Kerberos에 대한 Java 옵션 수정](#)"

7.4.2.1.3.1.3 여러 도메인 Krb5.ini 샘플 파일

다음은 도메인이 여러 개인 경우의 샘플 파일입니다.

```
[domain_realm]
: trust relationship: childtest4<->sbopetest3<->sbopetest<->sbopetest2
[libdefaults]
default_realm = SBOPTEST.COM
[realms]
SBOPTEST.COM = {
kdc = VANPGVMBOBJ01.sbopetest.com
}
SBOPTEST2.COM = {
kdc = VANPGVMBOBJ05.sbopetest2.com
}
SBOPTEST3.COM = {
kdc = VANPGVMBOBJ07.sbopetest3.com
}
CHILDTTEST4.SBOPTEST3.COM = {
kdc = vanpgvmbobj08.childtest4.sbopetest3.com
}
[capaths]
: for clients in sbopetest3 to login sbopetest2
SBOPTEST3.COM = {
SBOPTEST2.COM = SBOPTEST.COM
}
: for clients in childtest4 to login sbopetest2
CHILDTTEST4.SBOPTEST3.COM = {
SBOPTEST2.COM = SBOPTEST.COM
SBOPTEST2.COM = SBOPTEST3.COM
}
```

7.4.2.1.3.1.4 Tomcat 또는 WebLogic JAAS 구성 파일 만들기

1. bscLogin.conf라는 파일이 없으면 이 파일을 만들어 기본 위치인 C:\WINNT에 저장합니다.

참고:

이 파일을 다른 위치에 저장할 수 있습니다. 그러나 이렇게 하려면 java 옵션에서 파일의 위치를 지정해야 합니다.

2. JAAS bscLogin.conf 구성 파일에 다음 코드를 추가합니다.

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
```

3. 파일을 저장하고 닫습니다.

7.4.2.1.3.1.5 Oracle JAAS 로그인 구성 파일 만들기

1. jazn-data.xml 파일을 찾습니다.

참고:

이 파일의 기본 위치는 C:\WOrHome_1Wj2eeWhomeWconfig입니다. Oracle Application Server를 다른 위치에 설치한 경우 설치 관련 파일을 찾습니다.

2. 파일에서 <jazn-loginconfig> 태그 사이에 다음 내용을 추가합니다.

```
<application>
<name>com.businessobjects.security.jgss.initiate</name>
<login-modules>
<login-module>
<class>com.sun.security.auth.module.Krb5LoginModule</class>
<control-flag>required</control-flag>
</login-module>
</login-modules>
</application>
```

3. jazn-data.xml 파일을 저장하고 닫습니다.

7.4.2.1.3.1.6 WebSphere JAAS 로그인 구성 파일 만들기

1. bscLogin.conf라는 파일이 없으면 이 파일을 만들어 기본 위치인 C:\WWINNT에 저장합니다.
2. JAAS bscLogin.conf 구성 파일에 다음 코드를 추가합니다.

```
com.businessobjects.security.jgss.initiate {
com.ibm.security.auth.module.Krb5LoginModule required;
};
```

3. 파일을 저장하고 닫습니다.

7.4.2.1.3.1.7 SAP NetWeaver에 LoginModule 추가

Kerberos 및 SAP NetWeaver 7.10을 사용하려면 Tomcat 웹 응용 프로그램 서버를 사용하는 것처럼 시스템을 구성하십시오. bscLogin.conf 파일은 만들 필요가 없습니다.

이 과정을 끝내고 나면 SAP NetWeaver 7.10에서 LoginModule을 추가하고 일부 Java 설정을 업데이트해야 합니다.

com.sun.security.auth.module.Krb5LoginModule을 com.businessobjects.security.jgss.initiate에 매핑하려면 NetWeaver에 LoginModule을 수동으로 추가해야 합니다.

1. 웹 브라우저에 `http://<컴퓨터 이름>:<포트>/nwa`를 입력하여 NetWeaver Administrator를 엽니다.
2. Configuration Management > Security > Authentication > Login Modules > Edit를 클릭합니다.
3. 다음 정보를 사용하여 새 로그인 모듈을 추가합니다.

표시 이름	Krb5LoginModule
클래스 이름	com.sun.security.auth.module.Krb5LoginModule

4. 저장을 클릭합니다.
NetWeaver에서 새 모듈이 만들어집니다.
5. Components > Edit를 클릭합니다.
6. 이름이 com.businessobjects.security.jgss.initiate인 새 정책을 추가합니다.
7. Authentication Stack에서 3단계에서 만든 로그인 모듈을 추가하고 Required로 설정합니다.
8. Options for Selected Login Module에 다른 항목이 있는지 확인합니다. 있으면 이를 제거하십시오.
9. 저장을 클릭합니다.
10. NetWeaver Administrator에서 로그아웃합니다.

7.4.2.1.3.1.8 Tomcat에서 Kerberos에 대한 Java 옵션을 수정하려면

1. 시작 메뉴에서 프로그램 > Tomcat > Tomcat 구성을 선택합니다.
2. Java 탭을 클릭합니다.
3. 다음 옵션을 추가합니다.

```
-Djava.security.auth.login.config=C:\XXXX\WbscLogin.conf
-Djava.security.krb5.conf=C:\XXXX\Wkrb5.ini
```

여기서 XXXX는 파일이 저장된 위치입니다.

4. Tomcat 구성 파일을 닫습니다.
5. Tomcat을 다시 시작합니다.

7.4.2.1.3.1.9 SAP NetWeaver 7.10용 Java 옵션 수정

1. Java 구성 도구가 있는 곳으로 이동하여(기본 위치: C:\Wusr\Wsap\W<NetWeaver ID>\W<instance>\Wj2ee\Wconfigtool\W) configtool.bat를 두 번 클릭합니다.
구성 도구가 열립니다.
2. 보기 > 전문가 모드를 클릭합니다.
3. 클러스터-데이터 > 템플릿을 확장합니다.
4. NetWeaver 서버에 해당하는 인스턴스를 선택합니다(예: 인스턴스 - <시스템 ID><컴퓨터 이름>).
5. VM 매개 변수를 클릭합니다.
6. 공급업체 목록에서 SAP를 선택하고 플랫폼 목록에서 글로벌을 선택합니다.
7. 시스템을 클릭합니다.
8. 다음 사용자 지정 매개 변수 정보를 추가합니다.

java.security.krb5.conf	<krb5.ini 파일의 경로(파일 이름 포함)>
javax.security.auth.useSubjectCredsOnly	False

9. Save를 클릭합니다.
10. 구성 편집기를 클릭합니다.
11. 구성 > 보안 > 구성 > com.businessobjects.security.jgss.initiate > 보안 > 인증을 클릭합니다.
12. 편집 모드를 클릭합니다.
13. 인증 노드를 마우스 오른쪽 단추로 클릭하고 하위 노드 만들기를 선택합니다.
14. 맨 위 목록에서 값-항목을 선택합니다.
15. 다음과 같이 입력합니다.

이름	Create_security_session
값	False

16. 만들기를 클릭합니다.
17. 창을 닫습니다.
18. 구성 도구를 클릭합니다.
19. Save를 클릭합니다.

구성을 업데이트한 후에는 NetWeaver 서버를 다시 시작해야 합니다.

7.4.2.1.3.1.10 WebLogic에서 Kerberos용 Java 옵션 수정

WebLogic과 함께 Kerberos를 사용하는 경우, Java 옵션에서 Kerberos 구성 파일과 Kerberos 로그인 모듈의 지정 위치를 수정해야 합니다.

1. BI 플랫폼 응용 프로그램을 실행하는 WebLogic 도메인을 중지합니다.
2. BI 플랫폼 응용 프로그램을 실행하는 WebLogic의 도메인을 시작하는 스크립트(Windows의 경우 startWeblogic.cmd, UNIX의 경우 startWebLogic.sh)를 엽니다.
3. 파일의 Java_Options 섹션에 다음 정보를 추가합니다.

```
set JAVA_OPTIONS=-Djava.security.auth.login.config=C:/XXXX/bscLogin.conf -Djava.security.krb5.conf=C:/XXX/krb5.ini
```

여기서 XXXX는 파일이 저장된 위치입니다.

4. BI 플랫폼 응용 프로그램을 실행하는 WebLogic 도메인을 다시 시작합니다.

7.4.2.1.3.1.11 Oracle Application Server에서 Kerberos에 대한 Java 옵션 수정

Oracle Application Server에서 Kerberos를 사용하는 경우 Java 옵션을 수정하여 kerberos 구성 파일의 위치를 지정해야 합니다.

1. Oracle Application Server의 관리 콘솔에 로그인합니다.
2. BI 플랫폼 응용 프로그램을 실행하는 OC4J 인스턴스 이름을 클릭합니다.
3. 서버 속성을 선택합니다.

4. 아래쪽으로 스크롤하여 여러 VM 구성 섹션을 찾습니다.
5. 명령줄 옵션 섹션에서 Java 옵션 텍스트 필드의 끝에 `-Djava.security.krb5.conf=C:/XXXX/krb5.ini`를 추가합니다. 여기서 XXXX는 파일이 저장된 위치입니다.
6. OC4J 인스턴스를 다시 시작합니다.

7.4.2.1.3.1.12 WebSphere에서 Kerberos에 대한 Java 옵션 수정

1. WebSphere용 관리 콘솔에 로그인합니다.
IBM WebSphere 5.1의 경우 `http://servername:9090/admin`을 입력합니다. IBM WebSphere 6.0의 경우 `http://servername:9060/ibm/console`을 입력합니다.
2. 서버를 확장하고 응용 프로그램 서버를 클릭한 다음 BI 플랫폼과 함께 사용하기 위해 만든 응용 프로그램 서버의 이름을 클릭합니다.
3. JVM 페이지로 이동합니다.
WebSphere 5.1을 사용하는 경우 다음 단계에 따라 JVM 페이지로 이동합니다.
 - a. 서버 페이지에서 추가 속성 열에 프로세스 정의가 나타날 때까지 아래로 스크롤합니다.
 - b. 프로세스 정의를 클릭합니다.
 - c. 아래로 스크롤한 다음 Java Virtual Machine을 클릭합니다.
 WebSphere 6.0을 사용하는 경우에는 다음 단계에 따라 JVM 페이지로 이동합니다.
 - a. 서버 페이지에서 Java 및 프로세스 관리를 선택합니다.
 - b. 프로세스 정의를 선택합니다.
 - c. Java Virtual Machine을 선택합니다.
4. 일반 JVM 인수를 클릭한 다음 Krb5.ini의 위치와 bscLogin.conf 파일의 위치를 입력합니다.
`-Djava.security.auth.login.config=C:\XXXX\WbscLogin.conf`
`-Djava.security.krb5.conf=C:\XXXX\Wkrb5.ini`
 여기서 XXXX는 파일이 저장된 위치입니다.
5. 적용을 클릭한 다음 저장을 클릭합니다.
6. 서버를 중지했다가 다시 시작합니다.

7.4.3 AD 인증 단일 로그인

7.4.3.1 Windows AD 인증 단일 로그인 옵션

다음 두 가지 방법으로 BI 플랫폼에서 Windows AD 인증을 위한 단일 로그인을 설정할 수 있습니다.

- Vintela 단일 로그인 - 이 옵션은 Kerberos와 함께 사용하는 경우만 가능합니다.
- SiteMinder를 통한 단일 로그인 - 이 옵션은 Kerberos와 함께 사용하는 경우만 가능합니다.

참고:

가장 일반적인 단일 로그인 시나리오는 Java 응용 프로그램 서버에만 배포 가능한 BI 실행 패드 응용 프로그램 액세스를 통한 것입니다. BI 실행 패드의 단일 로그인은 Kerberos를 통해서만 가능합니다.

7.4.3.2 Windows AD 인증 단일 로그인 준비

7.4.3.2.1 Vintela 단일 로그인을 사용한 Windows AD 인증(Kerberos) 구성

다음 단원에서는 BI 플랫폼에서 Windows AD 인증 및 Vintela 단일 로그인을 사용하도록 설정하는데 필요한 작업을 설명합니다.

참고:

Windows AD 인증에 필요한 사전 설정 작업 및 특정 Vintela 단일 로그인 작업을 먼저 완료한 후 CMC에서 Windows AD 인증 옵션을 구성해야 합니다.

관련 항목

- 252 페이지에서 [Kerberos 사용 AD 인증을 위한 서비스 계정 설정](#)"
- 256 페이지에서 [Kerberos 사용 Windows AD 인증을 위한 서버 준비](#)"
- 257 페이지에서 [Windows AD 인증\(Kerberos\)을 위한 응용 프로그램 서버 준비](#) "

7.4.3.2.2 Java BI 실행 패드에 대한 Kerberos 및 단일 로그인 구성 워크플로

BI 플랫폼에서 Windows AD 인증 및 Vintela 단일 로그인을 사용할 수 있도록 설정하려면 다음 작업을 완료해야 합니다.

1. Vintela 단일 로그인에 사용할 서비스 계정을 생성하여 구성합니다.
2. 해당 서비스 계정에서 실행되도록 BI 플랫폼 배포 환경을 설정합니다.
3. Vintela 단일 로그인에 대한 BOE 일반 속성 및 BI 실행 패드 특정 속성을 구성합니다.
4. Java 응용 프로그램 서버의 헤더 크기 제한을 늘립니다.
5. Vintela 단일 로그인에 대한 인터넷 브라우저를 구성합니다.
6. Vintela 단일 로그인에 대한 제한 위임을 구성합니다(옵션).

이 작업이 모두 완료되면 CMC에서 Windows AD 인증 옵션을 구성할 수 있습니다.

7.4.3.2.3 Vintela 단일 로그인을 위한 서비스 계정 설정

Windows AD 인증을 위한 Vintela 단일 로그인을 사용하기 위해서는 도메인 컨트롤러에 새 서비스 계정을 설정해야 합니다. 이 서비스 계정은 특정 Windows AD 그룹의 사용자의 BI 실행 패드에 대한 단일 로그인을 허용하기 위한 목적으로 사용됩니다. 이 작업은 AD 도메인 컨트롤러 컴퓨터에서 수행됩니다. 아래 1-5단계는 Kerberos를 사용한 Windows AD 사용에 필요하며, 6-7단계는 Vintela 단일 로그인 설정에 필요한 절차입니다.

1. 기본 도메인 컨트롤러에 암호를 사용하여 새 서비스 계정을 생성합니다.
2. kerberos keytab 설치 명령 ktpass를 실행하여 keytab 파일을 만들고 저장합니다.

다음 표에 나열된 ktpass 매개 변수를 지정해야 합니다.

매개 변수	설명
-out	생성할 Kerberos keytab 파일의 이름을 지정합니다.

매개 변수	설명
-princ	서비스 계정에 사용할 보안 주체 이름을 지정합니다. 이 매개 변수는 SPN 형식으로 지정되어야 합니다. 참고: 서비스 계정 이름은 대/소문자를 구분합니다. SPN에는 서비스 인스턴스가 실행되는 호스트 컴퓨터 이름이 항상 포함됩니다. 팁: SPN은 등록된 포리스트 내에서 고유해야 합니다. Windows 지원 도구인 Ldp.exe를 사용하여 SPN을 검색하여 이를 확인할 수 있습니다.
-mapuser	위의 -princ가 매핑되는 사용자 계정의 이름을 지정합니다. Server Intelligence Agent가 실행되는 계정입니다.
-pass	서비스 계정에서 사용하는 암호를 지정합니다.
-kvno	키를 만드는 데 사용되는 키 버전 번호를 지정합니다.
-ptype	보안 주체 유형을 지정합니다. 다음과 같이 지정해야 합니다. -ptype KRB5_NT_PRINCIPAL
-crypto	서비스 계정에서 사용할 암호화 유형을 지정합니다. 다음을 사용합니다. -crypto RC4-HMAC-NT

예를 들면 다음과 같습니다.

```
ktpass -out keytab_filename.keytab -princ
MYSIAMYSERVER/sbo.service.DOMAIN.COM
-mapuser sbo.serviceDOMAIN.COM -pass password
-kvno 255 -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

ktpass 명령의 결과를 통해 대상 도메인 컨트롤러를 확인하고 공유 암호가 포함된 Kerberos keytab 파일이 생성되었는지 확인할 수 있습니다. 이 명령은 또한 보안 주체 이름을 (로컬) 서비스 계정에 매핑합니다.

3. setspn -i 명령을 실행하여 ktpass 명령이 성공적으로 실행되었는지 확인합니다.
표시 출력에는 로컬 서비스 계정에 등록된 모든 서비스 보안 주체 이름이 나열됩니다.
4. 1단계에서 만든 서비스 계정을 마우스 오른쪽 단추로 클릭하고 속성 > 위임을 선택합니다.
5. 모든 서비스에 대한 위임용으로 이 사용자 트러스트(Kerberos만)를 선택합니다.
6. setspn -a 명령을 사용하여 1단계에서 만든 서비스 계정에 HTTP 서비스 보안 주체 이름을 추가합니다. 서버의 서비스 보안 주체 이름, 정규화된 도메인 서버, BI 실행패드가 배포된 컴퓨터의 IP 주소를 지정합니다.

예를 들면 다음과 같습니다.

```
setspn -a HTTP/servername servicename
setspn -a HTTP/servernamedomain servicename
setspn -a HTTP/<ip address of server> servicename
```

여기에서 `servername`은 BI 실행 패드가 배포된 서버의 이름이며, `servernamedomain`은 서버의 정규화된 도메인 이름입니다.

7. `setspn -I servicename`을 실행하여 HTTP 서비스 보안 주체 이름이 서비스 계정에 추가되었는지 확인합니다.

명령으로 출력되는 결과에는 아래 예에서와 같이 등록된 모든 서비스 보안 주체 이름이 포함되어야 합니다.

```
Registered ServicePrincipalNames for
CN=bo.service,OU=boe,OU=BIP,OU=PG,DC=DOMAIN,DC=com:
HTTP/<ip address of server>
HTTP/servname.DOMAIN.com
HTTP/servname
servname/servicenameDOMAIN.com
```

서비스 계정에 필요한 모든 서비스 보안 주체 이름이 추가되었고 필수 keytab 파일이 생성되었습니다.

Vintela 단일 로그인에 작동하도록 하려면 BI 플랫폼 서버를 설정하고 BI 실행 패드 속성을 편집한 후 keytab 파일을 해당 디렉터리에 복사해야 합니다.

7.4.3.2.4 Vintela 단일 로그인을 위한 서버 준비

BI 플랫폼 서버가 배포된 컴퓨터가 기본 도메인에 추가되었으며 필요한 DNS 접미사가 추가되었는지 확인해야 합니다.

다음 작업을 수행하려면 Kerberos를 사용한 Windows AD 인증을 위해 생성한 keytab 파일이 필요합니다.

1. BI 플랫폼 서버를 호스팅하는 컴퓨터의 위치에 Kerberos keytab 파일을 복사합니다.
2. Kerberos 서비스 계정을 호스트 컴퓨터의 관리자 그룹에 추가합니다.
계정 이름은 `DOMAINNAME\서비스 이름` 형식을 따릅니다.
3. Kerberos 서비스 계정을 로컬 보안 정책 MMC의 다음 시스템 권한에 추가합니다.

시스템 권한	영향
운영 체제의 일부로 작동	인증 필요 없이 프로세스가 임의의 사용자를 가장하도록 허용합니다.
일괄 작업으로 로그인	사용자가 배치 대기열 기능을 통해 로그인하도록 합니다.
서비스로 로그인	서비스 계정이 프로세스를 서비스로 등록하도록 허용합니다.

시스템 권한	영향
프로세스 수준 토큰 바꾸기	계정이 CreateProcessAsUser() API를 호출하여 특정 서비스를 통해 다른 서비스를 시작할 수 있도록 허용합니다.

서비스 계정에서 BI 플랫폼 서버를 실행해야 합니다.

4. 모든 프로그램 > SAP BusinessObjects Enterprise XI 4.0 > SAPBusinessObjects Enterprise > 중앙 구성 관리자 로 이동합니다.
5. CCM에서 SIA(Server Intelligence Agent)를 마우스 오른쪽 단추로 클릭하고 중지를 선택합니다.
6. SIA를 마우스 오른쪽 단추로 클릭한 다음 속성을 선택합니다.
7. 시스템 계정 확인란 선택을 취소합니다.
8. 2단계의 Kerberos 계정 자격 증명(DOMAINNAME\서비스 이름)을 입력하고 확인을 클릭합니다.
9. SIA를 다시 시작합니다.

Vintela 단일 로그인 설정을 완료하려면 다음 작업을 완료해야 합니다.

- Vintela 단일 로그인을 위한 웹 응용 프로그램 서버 및 BI 실행 패드 속성을 준비합니다.
- Windows AD 인증 및 Vintela 단일 로그인을 사용하도록 Window AD 보안 플러그 인을 구성합니다.

7.4.3.2.5 BI 실행 패드 및 OpenDocument용 Vintela 단일 로그인 사용

이 절차는 BI 실행 패드 및 OpenDocument 웹 응용 프로그램 모두에 사용할 수 있습니다. Windows AD 보안 플러그 인에 대한 Vintela 설정을 지정하는 것 외에 BOE.war 속성에도 SiteMinder 설정을 지정해야 합니다.

1. 웹 응용 프로그램 서버를 호스팅하는 컴퓨터에서 BOE 웹 응용 프로그램에 대한 사용자 지정 폴더에 액세스합니다.

BI 플랫폼 설치와 함께 제공되는 Tomcat 웹 응용 프로그램 서버를 사용 중인 경우 다음 폴더에 직접 액세스할 수 있습니다.

C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom\

팁:

배포된 웹 응용 프로그램에 직접 액세스할 수 없는 웹 응용 프로그램 서버를 사용 중인 경우 제품 설치에 있는 다음 폴더를 사용하여 BOE 웹 응용 프로그램을 수정할 수 있습니다.

<INSTALLDIR>\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\

수정된 BOE 웹 응용 프로그램을 나중에 다시 배포해야 합니다.

2. 새 파일을 만듭니다.

참고:

메모장이나 기타 텍스트 편집 유틸리티를 사용하십시오.

3. 다음과 같이 입력합니다.

```
sso.enabled=true
siteminder.enabled=false
vintela.enabled=true
idm.realm=[YOUR_REALM]
idm.princ=[YOUR_PRINCIPAL]
idm.allowUnsecured=true
idm.allowNTLM=false
idm.logger.name=simple
idm.logger.props=error-log.properties
```

참고:

idm.realm과 idm.princ 매개 변수는 필수로 입력해야 하며 유효한 값을 입력해야 합니다. idm.realm의 값은 krb5.ini 파일에서 default_realm을 구성할 때 설정한 값과 같아야 합니다. 이 값은 모두 대문자여야 합니다. idm.princ 매개 변수는 Vintela 단일 로그인에 대해 생성된 서비스 계정에 사용되는 SPN입니다.

4. keytab 파일을 사용하도록 선택한 경우 키 패드 매개 변수를 추가하고 파일의 경로를 다음과 같이 지정합니다.

```
idm.keytab=C:/WIN/filename.keytab
```

Windows AD 인증 및 Vintela 로그인에 대한 제한 위임을 사용하지 않는 경우에는 다음 단계를 생략합니다.

5. 제한 위임 추가를 사용하려면

```
idm.allowS4U=true
```

6. 파일을 닫고 다음 이름으로 저장합니다.

global.properties

참고:

파일 이름에 .txt 등의 확장자가 붙지 않도록 하십시오.

7. 같은 디렉터리에 다른 파일을 만듭니다. 필요에 따라 파일을 OpenDocument.properties 또는 BI launchpad.properties로 저장합니다.
8. 다음 문을 입력합니다.

```
authentication.default=secWinAD
cms.default=[enter your cms name]:[Enter the CMS port number]
```

예:

```
authentication.default=secWinAD
cms.default=mycms:6400
```

9. 파일을 저장하고 닫습니다.
10. 웹 응용 프로그램 서버를 다시 시작합니다.

새 속성을 적용하려면 웹 응용 프로그램 서버를 실행하는 컴퓨터에 BOE 웹 응용 프로그램을 다시 배포해야 합니다. WDeploy를 사용하여 웹 응용 프로그램 서버에 BOE를 다시 배포하십시오. WDeploy

를 사용하여 웹 응용 프로그램의 배포를 취소하는 방법은 SAP BusinessObjects Business Intelligence Platform 웹 응용 프로그램 배포 가이드를 참조하십시오.

참고:

배포에서 방화벽을 사용하는 경우 필요한 모든 포트를 열어야 합니다. 그렇지 않으면 웹 응용 프로그램이 BI 플랫폼 서버에 연결할 수 없습니다.

관련 항목

- 260 페이지에서 [여러 도메인 Krb5.ini 샘플 파일](#)"
- 257 페이지에서 [Windows AD 인증\(Kerberos\)을 위한 응용 프로그램 서버 준비 "](#)

7.4.3.2.6 Tomcat용 헤더 크기 제한 늘리기

Active Directory에서는 인증 프로세스에서 사용되는 Kerberos 토큰을 만듭니다. 이 토큰은 HTTP 헤더에 저장됩니다. Java 응용 프로그램 서버에는 기본 HTTP 헤더 크기가 부여됩니다. 오류를 방지하려면 최소 기본 크기가 16384바이트 이상이어야 합니다. 배포에 따라서는 이보다 더 커야할 수도 있습니다. 자세한 내용은 Microsoft의 지원 사이트(<http://support.microsoft.com/kb/327825>)에서 크기 지정 지침을 참조하십시오.

1. Tomcat이 설치된 서버에서 server.xml 파일을 엽니다.

Windows에서 이 파일은 <TomcatINSTALLDIR>/conf에 있습니다.

- Windows에서 BI 플랫폼과 함께 설치되는 Tomcat 버전을 사용하고 기본 설치 위치를 수정하지 않은 경우

<TomcatINSTALLDIR>을 C:\Program Files (x86)\SAP BusinessObjects\Tomcat6W으로 대체합니다.

- 지원되는 다른 웹 응용 프로그램 서버를 사용하는 경우 해당 웹 응용 프로그램 서버의 설명서를 참조하여 적절한 경로를 결정합니다.

2. 구성된 포트 번호에 해당하는 <Connector ...> 태그를 찾습니다.

기본 포트인 8080을 사용하는 경우 <Connector ...> 태그에 포트=8080이 포함된 태그를 찾습니다.

예를 들면 다음과 같습니다.

```
<Connector URIEncoding="UTF-8" acceptCount="100"
connectionTimeout="20000" debug="0"
disableUploadTimeout="true" enableLookups="false"
maxSpareThreads="75" maxThreads="150"
minSpareThreads="25" port="8080" redirectPort="8443"
/>
```

3. <Connector ...> 태그 안에 다음 값을 추가합니다.

```
maxHttpHeaderSize="16384"
```


예를 들면 다음과 같습니다.

```
<Connector URIEncoding="UTF-8" acceptCount="100"
connectionTimeout="20000" debug="0"
disableUploadTimeout="true" enableLookups="false"
maxSpareThreads="75" maxThreads="150"
maxHttpHeaderSize="16384" minSpareThreads="25" port="8080" redirectPort="8443" />
```

4. server.xml 파일을 저장하고 닫습니다.
5. Tomcat을 다시 시작합니다.

참고:

다른 Java 응용 프로그램 서버에 대한 자세한 내용은 해당 Java 응용 프로그램 서버의 설명서를 참조하십시오.

7.4.3.2.7 인터넷 브라우저 구성

Kerberos 단일 로그온을 지원하려면 BI 플랫폼 클라이언트를 구성해야 합니다. 이때 클라이언트 컴퓨터에서 IE(Internet Explorer) 브라우저도 구성해야 합니다.

7.4.3.2.7.1 클라이언트 컴퓨터에서 Internet Explorer 구성

1. 클라이언트 컴퓨터에서 IE 브라우저 창을 엽니다.
2. Windows 통합 인증을 활성화합니다.
 - a. 도구 메뉴에서 인터넷 옵션을 클릭합니다.
 - b. 고급 탭을 클릭합니다.
 - c. 탭을 스크롤하여 보안을 찾은 다음 Windows 통합 인증 사용을 선택하고 적용을 클릭합니다.
3. Java 응용 프로그램 컴퓨터나 신뢰할 수 있는 사이트의 URL을 추가합니다. 사이트의 전체 도메인 이름을 입력할 수 있습니다.
 - a. 도구 메뉴에서 인터넷 옵션을 클릭합니다.
 - b. 보안 탭을 클릭합니다.
 - c. 사이트를 클릭한 다음 고급을 클릭합니다.
 - d. 사이트를 선택하거나 입력한 후 추가를 클릭합니다.
 - e. 확인을 계속 클릭하여 인터넷 옵션 대화 상자를 닫습니다.

4. 변경 내용이 적용되도록 Internet Explorer 브라우저 창을 닫았다가 다시 엽니다.
5. 각각의 BI 플랫폼 클라이언트 컴퓨터에서 이 모든 단계를 반복합니다.

7.4.3.2.7.2 클라이언트 컴퓨터에서 Firefox 구성

1. network.negotiate-auth.delegation-uris 수정
 - a. 클라이언트 컴퓨터에서 Firefox 브라우저 창을 엽니다.
 - b. URL 주소 필드에 about:config를 입력합니다. 이렇게 하면 구성 가능한 속성의 목록이 나타납니다.
 - c. network.negotiate-auth.delegation-uris를 두 번 클릭하여 속성을 편집합니다.
 - d. BI 실행 패드에 액세스하는 데 사용할 URL을 입력합니다. 예를 들어, BI 실행 패드 URL이 http://machine.domain.com:8080/BOE/BI이면 http://http://machine.domain.com을 입력해야 합니다.

참고:
URL을 둘 이상 추가하려면 각 URL을 쉼표로 구분합니다. 예: http://machine.domain.com,machine2.domain.com

 - e. 확인을 클릭합니다.
2. network.negotiate-auth.trusted-uris 수정
 - a. 클라이언트 컴퓨터에서 Firefox 브라우저 창을 엽니다.
 - b. URL 주소 필드에 about:config를 입력합니다. 이렇게 하면 구성 가능한 속성의 목록이 나타납니다.
 - c. network.negotiate-auth.trusted-uris를 두 번 클릭하여 속성을 편집합니다.
 - d. InfoView에 액세스하는 데 사용할 URL을 입력합니다. 예를 들어, BI 실행 패드 URL이 http://machine.domain.com:8080/BOE/BI이면 http://machine.domain.com을 입력해야 합니다.

참고:
URL을 둘 이상 추가하려면 각 URL을 쉼표로 구분합니다. 예: http://machine.domain.com,machine2.domain.com.

 - e. 확인을 클릭합니다.
3. 이러한 변경 내용이 적용되도록 Firefox 브라우저 창을 닫고 다시 엽니다.
4. 각각의 BI 플랫폼 클라이언트 컴퓨터에서 이 모든 단계를 반복합니다.

7.4.3.2.8 Vintela 단일 로그인에 대한 제한 위임 구성

제한 위임은 AD 인증 및 Vintela 단일 로그인에서는 옵션 사항이지만, 시스템 데이터베이스 단일 로그인이 관련된 배포 시나리오에서는 필수 항목입니다.

1. AD 도메인 컨트롤러 컴퓨터에서 Active Directory 사용자 및 컴퓨터 스냅인을 엽니다.
2. Vintela 단일 로그인에 대해 만든 서비스 계정을 마우스 오른쪽 단추로 클릭하고 속성 > 위임을 클릭합니다.
3. 지정한 서비스에 대한 위임용으로만 이 사용자 트러스트를 선택합니다.
4. Kerberos만 사용을 선택합니다.
5. 추가 > 사용자 또는 컴퓨터를 클릭합니다.
6. 서비스 계정 이름(Vintela 단일 로그인에 사용)을 입력하고 확인을 클릭합니다.
서비스 목록이 표시됩니다.
7. 다음 서비스를 선택한 후 확인을 클릭합니다.
 - HTTP 서비스
 - BI 플랫폼을 호스팅하는 컴퓨터에서 Service Intelligence Agent(SIA)를 실행하는 데 사용되는 서비스

(Vintela 단일 로그인) 계정에 위임될 수 있는 서비스 목록에 서비스가 추가됩니다.

이 수정 사항이 계정에 적용되도록 웹 응용 프로그램 속성을 수정해야 합니다. 웹 응용 프로그램 서버에 있는 BOE global.properties 파일을 엽니다. 다음 항목을 추가한 후 웹 응용 프로그램 서버를 다시 시작합니다.

```
idm.allowS4U=true
```

7.4.3.3 SiteMinder 사용

7.4.3.3.1 SiteMinder와 함께 Windows AD 사용

이 단원에서는 AD 및 SiteMinder를 사용하는 방법에 대해 설명합니다. SiteMinder는 BI 플랫폼에 대한 단일 로그인을 생성하기 위해 AD 보안 플러그 인과 함께 사용할 수 있는 타사 사용자 액세스 및 인증 도구입니다. SiteMinder를 Kerberos와 함께 사용할 수 있습니다.

Windows AD 인증이 SiteMinder에서 실행되도록 구성하기 전에 SiteMinder ID 관리 리소스가 설치되고 구성되었는지 확인하십시오. SiteMinder에 대한 추가 정보와 설치 방법은 SiteMinder 설명서를 참조하십시오.

SiteMinder를 사용한 AD 단일 로그인을 활성화하려면 다음 두 가지 작업을 수행해야 합니다.

- SiteMinder에서 단일 로그인을 위한 AD 플러그인 구성
- BOE 웹 응용 프로그램을 위한 SiteMinder 속성 구성

참고:

SiteMinder 관리자가 4.x 에이전트에 대한 지원 기능을 활성화했는지 확인합니다. 이 작업은 사용 중인 SiteMinder의 지원되는 버전에 관계없이 수행해야 합니다. SiteMinder 구성에 대한 자세한 내용은 SiteMinder 설명서를 참조하십시오.

7.4.3.3.1.1 SiteMinder를 사용한 Windows AD 인증용 BOE 속성 수정

Windows AD 보안 플러그인에 SiteMinder 설정을 지정하는 것 외에 BOE war 속성에도 SiteMinder 설정을 지정해야 합니다.

1. BI 플랫폼이 설치된 다음 디렉터리로 이동합니다.
`<INSTALLDIR>WSAP BusinessObjects Enterprise XI
 4.0\Wwarfiles\Wwebapps\WBOEWWEB-INF\Wconfig\Wcustom\W`

2. 새 파일을 만듭니다.

참고:

메모장이나 다른 텍스트 편집 유틸리티를 사용하십시오.

3. 파일을 닫고 다음 이름으로 저장합니다.

`Bllaunchpad.properties`

4. 다음 문을 입력합니다.

```
sso.enabled=true
siteminder.authentication=secWinAD
siteminder.enabled=true
```

5. 파일을 닫고 다음 이름으로 저장합니다.

`global.properties`

참고:

파일 이름에 .txt 등의 확장자가 붙지 않도록 하십시오.

6. 같은 디렉터리에 다른 파일을 만듭니다.

7. 다음 문을 입력합니다.

```
authentication.default=secWinAD
cms.default=[enter your cms name]:[Enter the CMS port number]
```

예:

```
authentication.default=LDAP
cms.default=mycms:6400
```

8. 파일을 닫고 다음 이름으로 저장합니다.

Bllaunchpad.properties

웹 응용 프로그램 서버를 실행하는 컴퓨터에 BOE.war 파일을 다시 배포해야 새 속성이 적용됩니다. WDeploy를 사용하여 웹 응용 프로그램 서버에 WAR 파일을 다시 배포하십시오. WDeploy를 사용하여 웹 응용 프로그램의 배포를 취소하는 방법은 SAP BusinessObjects Business Intelligence Platform 웹 응용 프로그램 배포 가이드를 참조하십시오.

7.4.3.3.1.2 SiteMinder 비활성화

SiteMinder를 구성하지 못하도록 하거나 CMC에서 구성 후 비활성화하려면 BI 실행 패드에 대한 웹 구성 파일을 수정하십시오.

7.4.3.3.1.2.1 Java 클라이언트에 대한 SiteMinder 비활성화

Windows AD 보안 플러그 인에 대한 SiteMinder 설정을 비활성화하는 것 외에 웹 응용 프로그램 서버의 BOE war 파일에서도 SiteMinder 설정을 비활성화해야 합니다.

1. BI 플랫폼이 설치된 다음 디렉터리로 이동합니다.

```
<INSTALLDIR>WSAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\WBOE\WEB-INF\config\customW
```

2. global.properties 파일을 엽니다.

3. siteminder.enabled를 False로 변경합니다.

```
siteminder.enabled=false
```

4. 변경 사항을 저장하고 파일을 닫습니다.

변경 내용은 웹 응용 프로그램 서버를 실행하는 컴퓨터에 BOE.war 파일을 다시 배포해야 적용됩니다. WDeploy를 사용하여 웹 응용 프로그램 서버에 WAR 파일을 다시 배포하십시오. WDeploy를 사용하여 웹 응용 프로그램의 배포를 취소하는 방법은 SAP BusinessObjects Business Intelligence 플랫폼 웹 응용 프로그램 배포 가이드를 참조하십시오.

7.4.4 AD 그룹 매핑 및 AD 인증 구성

7.4.4.1 AD 사용자와 그룹 매핑 및 Windows AD 보안 플러그 인 구성

특정 인증 유형을 사용하여 Windows AD 인증이 작동하도록 구성하려면 먼저 필요한 모든 사전 작업을 완료해야 합니다. 자세한 내용은 아래 "관련 항목" 단원을 참조하십시오.

사용되는 프로토콜에 관계없이 다음 단계를 수행하여 AD 사용자의 인증을 허용해야 합니다. 아래 절차에 소개된 1-8단계에 따라 AD 그룹을 BI 플랫폼으로 가져옵니다.

1. CMC의 인증 관리 영역으로 이동합니다.
2. Windows AD를 두 번 클릭합니다.
3. Windows Active Directory(AD) 사용 확인란을 선택합니다.
4. Windows AD 구성 요약 영역에서 AD 관리 이름 옆에 있는 링크를 클릭합니다.

참고:

Windows AD 플러그 인을 구성하기 이전에는 이 링크가 두 개의 큰따옴표로 표시됩니다. 구성을 저장한 이후에는 링크가 AD 관리 이름으로 채워집니다.

5. 활성화된 도메인 사용자 계정의 이름과 암호를 입력합니다. BI 플랫폼은 이 계정을 사용하여 AD에서 정보를 쿼리합니다.

관리 자격 증명은 다음 형식 중 하나를 사용할 수 있습니다.

- NT 이름(DomainName\UserName)
- UPN(user@DNS_domain_name)

BI 플랫폼에서는 AD의 내용을 수정, 추가, 삭제하지 않으며 정보를 읽기만 하므로 해당 권한만 필요합니다.

참고:

AD 디렉터리를 읽는 데 사용한 AD 계정이 유효하지 않게 되면 AD 인증이 계속되지 않습니다. 계정의 암호가 변경 또는 만료되었거나 계정이 비활성화된 경우 등을 예로 들 수 있습니다.

6. 기본 AD 도메인 필드에 원하는 도메인을 입력합니다.

참고:

- 기본 도메인의 그룹은 도메인 이름 접두사를 지정하지 않아도 매핑할 수 있습니다.
- 기본 AD 도메인 이름을 입력하면 기본 도메인의 사용자는 AD 인증을 통해 BI 플랫폼에 로그인할 때 AD 도메인 이름을 지정할 필요가 없습니다.

7. 매핑된 AD 멤버 그룹 영역의 AD 그룹 추가(도메인W그룹) 필드에 AD 도메인W그룹을 입력합니다.

다음 형식 중 하나를 사용하여 그룹을 매핑할 수 있습니다.

- NT 이름이라고도 하는 SAM(보안 계정 관리자) 계정 이름(DomainNameWGroupName)
- DN(cn=GroupName,, dc=DomainName, dc=com)

참고:

로컬 그룹을 매핑하려면 NT 이름 형식(WWServerNameWGroupName)만 사용하면 됩니다. AD에서는 로컬 사용자를 지원하지 않습니다. 즉, 매핑된 로컬 그룹에 속한 로컬 사용자가 BI 플랫폼에 매핑되지 않습니다. 따라서 이들은 해당 시스템에 액세스할 수 없습니다.

8. 추가를 클릭합니다.

목록에 그룹이 추가됩니다.

AD 그룹 계정을 가져온 후 AD 인증 옵션 또는 AD 그룹 업데이트를 구성하지 않으려는 경우에는 9-18단계는 생략해도 됩니다.

9. 단일 로그온을 구성하려면 선택된 인증 모드를 위한 단일 로그온 사용을 선택합니다.

참고:

이 옵션을 선택한 경우, 단일 로그온을 사용하려면 BOE 웹 응용 프로그램 일반 속성 및 BI 실행 패드 속성을 구성해야 합니다.

10. 자격 증명 동기화 영역에서 이 옵션을 선택하여 로그인할 때 AD 사용자의 데이터 소스 자격 증명을 활성화 및 업데이트합니다. 이렇게 하면 사용자의 현재 로그인 자격 증명으로 데이터 소스가 동기화됩니다.
11. 페이지의 SiteMinder 옵션 영역에서 Kerberos를 사용한 AD 인증용 단일 로그온 옵션으로 SiteMinder를 구성합니다.

참고:

단일 로그온 옵션으로 Vintela 또는 SiteMinder를 구성할 수 있지만, 두 가지를 동시에 사용할 수는 없습니다. SiteMinder 옵션을 구성하려면 서비스 사용자 이름 필드(9b 단계)에 입력된 값을 지웁니다.

- a. 사용 안 함을 클릭합니다.

Windows AD SiteMinder 구성 페이지가 나타납니다.

참고:

Windows AD 플러그 인을 구성하지 않은 경우 경고가 나타나며 계속할지 여부를 묻는 메시지가 표시됩니다. 확인을 클릭합니다.

- b. SiteMinder 단일 로그인 사용을 클릭합니다.
- c. 정책 서비스 호스트 입력란에 각 정책 서버의 이름을 입력하고 추가를 클릭합니다.
- d. 각 정책 서버 호스트에 대해 계정, 인증 및 인증 포트 번호를 지정합니다.
- e. 에이전트 이름 및 공유 암호를 입력합니다. 공유 암호를 다시 입력합니다.

참고:

SiteMinder 관리자가 4.x 에이전트에 대한 지원 기능을 활성화했는지 확인합니다. 이 작업은 사용 중인 SiteMinder의 지원되는 버전에 관계없이 수행해야 합니다. SiteMinder에 대한 추가 정보와 설치 방법은 SiteMinder 설명서를 참조하십시오.

- f. 정보를 저장하고 기본 AD 인증 페이지로 돌아가려면 업데이트를 클릭합니다.
12. AD 별칭 옵션 영역에서는 새 별칭이 BI 플랫폼에 추가되고 업데이트되는 방식을 지정합니다.
- a. 새 별칭 옵션에서 새 별칭이 Enterprise 계정에 매핑되는 방식을 선택합니다. 다음 항목 중 하나를 선택합니다.
 - 이름이 같은 기존 사용자 계정에 새 AD 별칭 할당

사용자에게 같은 이름의 기존 Enterprise 계정이 있다는 것을 아는 경우 이 옵션을 사용합니다. 즉, AD 별칭이 기존 사용자에게 할당됩니다(자동 별칭 만들기 사용). 기존 Enterprise 계정이 없는 사용자 또는 Enterprise 및 계정에 같은 이름이 없는 사용자는 새 사용자로 추가됩니다.
 - 새 AD 별칭마다 새 사용자 계정 만들기

각 사용자에게 대해 새 계정을 만들려는 경우 이 옵션을 사용합니다.
 - b. 별칭 업데이트 옵션에서 Enterprise 계정의 별칭 업데이트를 관리할 방법을 선택합니다. 다음 항목 중 하나를 선택합니다.
 - 별칭을 업데이트할 때마다 새 별칭 만들기

BI 플랫폼에 매핑된 모든 AD 사용자에게 대해 자동으로 새 별칭을 만들려면 이 옵션을 사용합니다. BI 플랫폼 계정이 없는 사용자나 "새 AD 별칭마다 새 사용자 계정 만들기" 옵션을 선택하고 업데이트를 클릭한 모든 사용자에게 대해 새 AD 계정이 추가됩니다.
 - 사용자가 로그인할 경우에만 새 별칭 만들기

매핑하는 AD 디렉터리에 여러 사용자가 들어 있지만 그 중 일부만 BI 플랫폼을 사용하는 경우 이 옵션을 사용합니다. 모든 사용자에게 대해 별칭과 Enterprise 계정이 자동으로 생성되는 것은 아닙니다. 대신 BI 플랫폼에 로그인하는 사용자에게 대해서만 별칭 및 계정(필요한 경우)이 생성됩니다.
 - c. 새 사용자 옵션에서 다음 항목 중 하나를 선택하여 새 사용자가 만들어지는 방식을 지정합니다. SAP BusinessObjects Business Intelligence 플랫폼 라이선스가 사용자 역할을 기반으로 하는 경우 다음 옵션 중 하나를 선택하십시오.
 - BI Viewer 사용자

새 사용자 계정이 BI Viewer 역할에 구성됩니다. BI Viewer 역할의 모든 계정에 대한 BI 플랫폼 응용 프로그램 액세스 권한이 사용권 계약에 정의됩니다. 사용자는 BI Viewer 역할용으로 정의된 응용 프로그램 워크플로에만 액세스할 수 있습니다. 액세스 권한은 일반적으로 비즈니스 인텔리전스 문서를 보는 것으로 제한됩니다. 이 역할은 일반적으로 BI 플랫폼 응용 프로그램을 통해 콘텐츠를 사용하는 사용자에게 적합합니다.
 - BI Analyst 사용자

새 사용자 계정이 BI Analyst 역할에 구성됩니다. BI Analyst 역할의 모든 계정에 대한 BI 플랫폼 응용 프로그램 액세스 권한이 사용권 계약에 정의됩니다. 사용자는 BI Analyst 역할에 대해 정의된 모든 응용 프로그램 워크플로에 액세스할 수 있습니다. 액세스 권한에는 비즈니스 인텔리전스 문서를 보고 수정하는 것이 포함됩니다. 이 역할은 일반적으로 BI 플랫폼 응용 프로그램의 콘텐츠를 만들고 수정하는 사용자에게 적합합니다.

SAP BusinessObjects Business Intelligence 플랫폼 라이선스가 사용자 역할을 기준으로 하지 않은 라이선스이면 다음 옵션 중 하나를 선택하십시오.

- 새 사용자를 명명된 사용자로 만들기

새 사용자 계정이 명명된 사용자 라이선스를 사용하도록 구성됩니다. 명명된 사용자 라이선스는 특정 사용자와 관련되며 이 라이선스를 사용하면 사용자 이름과 암호를 기반으로 시스템에 액세스할 수 있습니다. 이 옵션을 사용하면 명명된 사용자는 연결된 다른 사용자 수에 관계없이 시스템에 액세스할 수 있습니다. 이 옵션을 사용하여 만든 각 사용자 계정에 대한 명명된 사용자 라이선스가 있어야 합니다.

- 새 사용자를 동시 사용자로 만들기

새 사용자 계정이 동시 사용자 라이선스를 사용하도록 구성됩니다. 동시 라이선스는 BI 플랫폼에 동시에 연결할 수 있는 사용자 수를 지정합니다. 이 라이선스 유형은 소규모 동시 라이선스로 많은 사용자 기반을 지원할 수 있으므로 매우 유연합니다. 예를 들어 사용자가 해당 시스템에 액세스하는 빈도 및 시간에 따라 100개의 동시 사용자 라이선스로 250명, 500명 또는 700명의 사용자를 지원할 수 있습니다.

13. AD 별칭 업데이트를 예약할 방법을 구성하려면 AD 별칭 업데이트 예약을 클릭합니다.

- 일정 대화 상자의 개체 실행 드롭다운 목록에서 되풀이를 선택합니다.
- 필요에 따라 기타 일정 옵션과 매개 변수를 설정합니다.
- 일정을 클릭합니다.

별칭이 업데이트될 때 그룹 정보도 함께 업데이트됩니다.

14. 특성 바인딩 옵션 영역에서 AD 플러그 인의 특성 바인딩 우선 순위를 지정할 수 있습니다.

- 전체 이름 및 전자 메일 주소 가져오기 상자를 클릭합니다.

AD 계정에 사용된 전체 이름과 설명을 가져와서 BI 플랫폼에 사용자 개체와 함께 저장합니다.

- 다른 특성 바인딩을 기준으로 AD 특성 바인딩의 우선 순위 설정 옵션을 지정합니다.

참고:

이 옵션을 1로 설정하면 AD와 다른 플러그 인(LDAP 및 SAP)이 활성화된 경우 AD 특성이 우선 적용됩니다. 3으로 설정하면 다른 활성화된 플러그 인의 특성이 우선 적용됩니다.

15. AD 그룹 옵션 영역에서 AD 그룹 업데이트를 구성할 수 있습니다.

- AD 그룹 업데이트 예약을 클릭합니다.
일정 대화 상자가 나타납니다.
- 개체 실행 목록에서 되풀이를 선택합니다.
- 필요에 따라 기타 일정 옵션과 매개 변수를 설정합니다.
- 일정을 클릭합니다.

업데이트가 예약되고 지정된 일정 정보에 따라 업데이트가 실행됩니다. AD 그룹 옵션에서 AD 그룹 계정에 대해 예약된 다음 업데이트를 확인할 수 있습니다.

16. 주문형 AD 업데이트 영역의 설정을 사용하여 업데이트 대상을 지정합니다. 다음 옵션 중 하나를 선택할 수 있습니다.

- AD 그룹 지금 업데이트

AD 그룹을 업데이트하려면 이 옵션을 선택합니다. 업데이트를 클릭한 후에만 업데이트가 수행됩니다.

참고:

이 옵션은 예약된 모든 AD 그룹 업데이트에 영향을 미칩니다. 예약된 다음 AD 그룹 업데이트가 AD 그룹 옵션 아래에 나열됩니다.

- 지금 AD 그룹 및 별칭 업데이트

AD 그룹 및 사용자 별칭을 업데이트하려면 이 옵션을 선택합니다. 업데이트를 클릭한 후에만 업데이트가 수행됩니다.

참고:

이 옵션은 예약된 모든 AD 그룹 업데이트에 영향을 미칩니다. 예약된 다음 업데이트가 AD 그룹 옵션 및 AD 별칭 옵션 아래에 나열됩니다.

- 지금 AD 그룹 및 별칭 업데이트 안 함

업데이트를 클릭해도 그룹이나 사용자 별칭이 업데이트되지 않습니다.

참고:

이 옵션은 예약된 모든 그룹 또는 별칭 업데이트에 영향을 줍니다. 예약된 다음 업데이트가 AD 그룹 옵션 및 AD 별칭 옵션 아래에 나열됩니다.

17. 업데이트를 클릭합니다.

18. 확인을 클릭합니다.

관련 항목

- 251 페이지에서 [Windows AD 사용 단일 로그인](#)"
- 275 페이지에서 [SiteMinder와 함께 Windows AD 사용 "](#)
- 252 페이지에서 [Kerberos와 함께 Windows AD 인증 사용"](#)

7.4.5 Windows AD 인증 문제 해결

7.4.5.1 구성 문제 해결

Kerberos를 구성할 때 문제가 발생하면 다음 단계를 참조하십시오.

- 로깅 활성화
- Java SDK Kerberos 구성 테스트

7.4.5.1.1 로깅 활성화

1. 시작 메뉴에서 프로그램 > Tomcat > Tomcat 구성을 선택합니다.
2. Java 탭을 클릭합니다.
3. 다음 옵션을 추가합니다.

```
-Dcrystal.enterprise.trace.configuration=verbose
-sun.security.krb5.debug=true
```

다음 위치에 로그 파일이 만들어집니다.

```
C:\Documents and Settings\<user name>\W.businessobjects\Wjce_verbose.log
```

7.4.5.1.2 Java Kerberos 구성을 테스트하려면

- 다음 명령을 실행하여 Kerberos 구성을 테스트합니다. 여기서 **servact**는 CMS가 실행되는 서비스 계정과 도메인이고 **password**는 서비스 계정과 연결된 암호입니다.

```
<Install Directory>\SAP Business Objects Enterprise XI 4.0\win64_64\jdk\bin servact@TESTM03.COM Password
```

예를 들면 다음과 같습니다.

```
C:\Program Files\SAP BusinessObjects\W
SAP Business Objects Enterprise XI 4.0\win64_64\jdk\bin\W
servact@TESTM03.COM Password
```

여전히 문제가 있으면 도메인과 서비스 사용자 이름으로 입력한 대/소문자가 Active Directory에서 설정된 것과 정확히 일치하는지 확인합니다.

7.4.5.1.3 다른 AD UPN 및 SAM 이름으로 인한 로그인 실패

사용자의 Active Directory ID가 BI 플랫폼에 성공적으로 매핑되었습니다. 하지만 사용자가 Windows AD 인증과 Kerberos를 통해 CMC나 BI 실행 패드에 DOMAINWABC123 형식으로 로그인할 수 없습니다.

이 문제는 Active Directory에서 사용자를 설정할 때 사용한 UPN 및 SAM 이름이 서로 다른 경우에 발생할 수 있습니다. 다음 예제의 경우 문제가 발생할 수 있습니다.

- UPN은 abc123@company.com이지만 SAM 이름은 DOMAINWABC123입니다.
- UPN은 jsmith@company.com이지만 SAM 이름은 DOMAINWjohnsmith입니다.

다음 두 가지 방법으로 문제를 해결할 수 있습니다.

- 사용자가 SAM 이름 대신 UPN 이름을 사용하여 로그인하도록 만듭니다.
- SAM 계정 이름과 UPN 이름이 같은지 확인합니다.

7.4.5.1.4 사전 인증 오류

이전에 로그인했던 사용자가 더 이상 성공적으로 로그인할 수 없습니다. 계정 정보를 인식할 수 없음 오류 메시지가 나타납니다. Tomcat 오류 로그에는 "사전 인증 정보가 유효하지 않습니다.(24)"라는 오류가 표시됩니다.

이는 Kerberos 사용자가 AD의 UPN을 수정하지 않았기 때문에 나타날 수 있습니다. Kerberos 사용자 데이터베이스 및 AD 정보의 비동기화를 의미할 수도 있습니다.

이 문제를 해결하려면 AD에서 사용자 암호를 재설정하십시오. 변경 사항이 제대로 전달된 것을 확인할 수 있습니다.

참고:

이 문제는 J2SE 5.0과 관련이 없습니다.

7.5 SAP 인증

7.5.1 SAP 인증 구성

이 단원에서는 SAP 환경에 대해 BI 플랫폼 인증을 구성하는 방법을 설명합니다.

SAP 인증을 통해 SAP 사용자는 BI 플랫폼에 암호를 저장하지 않고 SAP 사용자 이름과 암호를 사용하여 BI 플랫폼에 로그인할 수 있습니다. 또한 SAP 인증을 사용하면 SAP의 사용자 역할에 대한 정보를 보존하고, 플랫폼 내에서 이 역할 정보를 사용하여 관리 작업을 수행하거나 콘텐츠에 액세스하는데 필요한 권한을 부여할 수 있습니다.

SAP 인증 응용 프로그램 액세스

SAP 인증을 설치한 다음 SAP 시스템에 대한 정보를 BI 플랫폼에 제공해야 합니다. 이 웹 응용 프로그램에는 기본 BI 플랫폼 관리 도구인 중앙 관리 콘솔(CMC)을 통해 액세스할 수 있습니다. CMC의 홈 페이지에서 이 응용 프로그램에 액세스하려면 인증을 클릭합니다.

SAP 사용자 인증

보안 플러그 인을 사용하면 더 다양한 방식으로 BI 플랫폼에서 사용자를 인증하고 인증 방식을 사용자 지정할 수도 있습니다. SAP 인증 기능에는 BI 플랫폼의 중앙 관리 서버(CMS) 구성 요소에 대한 SAP 보안 플러그 인(secSAPR3.dll)이 포함되어 있습니다. 이 SAP 보안 플러그 인을 사용하면 여러 가지 이점을 얻을 수 있습니다.

- 이 보안 플러그 인은 CMS 대신 SAP 시스템에 대해 사용자 자격 증명을 확인하는 인증 공급자 역할을 합니다. 사용자가 BI 플랫폼에 직접 로그인할 때 SAP 인증을 선택하고 자신의 일반적인 SAP 사용자 이름과 암호를 입력할 수 있습니다. 또한 BI 플랫폼은 SAP 시스템에 대해 Enterprise 포털 로그인 티켓의 유효성을 검사할 수 있습니다.
- SAP에서 BI 플랫폼 사용자 그룹으로 역할을 매핑하여 계정을 손쉽게 만들 수 있고, BI 플랫폼 내에서 일관된 방식으로 사용자와 그룹에 권한을 부여하여 계정을 효율적으로 관리할 수 있습니다.
- SAP 역할 목록을 동적으로 유지 관리할 수 있습니다. 따라서 SAP 역할을 플랫폼에 일단 매핑하고 나면 해당 역할에 속한 모든 사용자가 시스템에 로그인할 수 있습니다. 이후에 SAP 역할 소속 그룹을 변경하더라도 BI 플랫폼에서 목록을 업데이트하거나 새로 고칠 필요가 없습니다.
- SAP 인증 구성 요소에는 플러그 인 구성을 위한 웹 응용 프로그램이 포함되어 있습니다. 중앙 관리 콘솔(CMC)의 인증 영역에서 이 응용 프로그램에 액세스할 수 있습니다.

7.5.2 BI 플랫폼의 사용자 계정 만들기

BI 플랫폼 시스템에는 SAP 역할 소속 그룹 목록에 액세스하고 SAP를 인증할 권한이 있는 SAP 사용자 계정이 있어야 합니다. BI 플랫폼을 SAP 시스템에 연결할 때 이 계정 자격 증명이 필요합니다. SAP 사용자 계정 만들기과 역할을 통한 권한 할당에 대한 일반적인 지침을 보려면 SAP BW 설명서를 참조하십시오.

SU01 트랜잭션을 사용하여 CRYSTAL이라는 새 SAP 사용자 계정을 만듭니다. PFCG 트랜잭션을 사용하여 CRYSTAL_ENTITLEMENT라는 새 역할을 만듭니다. 이들 이름을 사용하는 것이 좋지만 원하는 경우 다른 이름을 사용해도 됩니다. 다음 인증 개체에 대해 해당 값을 설정하여 새 역할의 인증 데이터를 변경합니다.

인증 개체	필드	값
파일 액세스를 위한 인증 (S_DATASET)	작업(ACTVT)	읽기, 쓰기(33, 34)
	실제 파일 이름(FILENAME)	*(모두를 의미함)
	ABAP 프로그램 이름(PROGRAM)	*
RFC 액세스를 위한 인증 확인 (S_RFC)	작업(ACTVT)	16
	보호할 RFC의 이름 (RFC_NAME)	BDCH, STPA, SUSO, BDL5, SUUS, SU_USER, SYST, SUNI, RFC1, SDIFRUNTIME, PRGN_J2EE, /CRYSTAL/SECURITY
	보호할 RFC 개체의 유형 (RFC_TYPE)	함수 그룹(FUGR)
사용자 마스터 유지 관리: 사용자 그룹(S_USER_GRP)	작업(ACTVT)	만들기 또는 생성 및 표시(03)
	사용자 마스터 유지 관리의 사용자 그룹(CLASS)	<p>*</p> <p>참고: 보안을 강화하기 위해 BI 플랫폼에 액세스해야 할 구성원이 포함된 사용자 그룹을 명시적으로 지정할 수도 있습니다.</p>

마지막으로 CRYSTAL 사용자를 CRYSTAL_ENTITLEMENT 역할에 추가합니다.

팁:

사용자가 시스템에 처음 로그인할 때 자신의 암호를 변경하도록 시스템 정책에서 규정하고 있는 경우 CRYSTAL 사용자 계정으로 로그인하여 암호를 다시 설정합니다.

7.5.3 SAP 권한 부여 시스템에 연결

BI 플랫폼에 역할을 가져오거나 BW 콘텐츠를 게시하려면 먼저 통합할 SAP 권한 부여 시스템에 대한 정보를 제공해야 합니다. BI 플랫폼은 역할 소속 그룹을 결정하고 SAP 사용자를 인증할 때 이 정보를 사용하여 대상 SAP 시스템에 연결합니다.

7.5.3.1 SAP 권한 부여 시스템 추가

1. CMC의 인증 관리 영역으로 이동합니다.
2. SAP 링크를 두 번 클릭합니다.

권한 부여 시스템 설정이 나타납니다.

팁:

권한 부여 시스템이 이미 논리 시스템 이름 목록에 표시되어 있으면 새로 만들기를 클릭합니다.

3. SAP 시스템의 세 글자로 된 SID(시스템 ID)를 시스템 필드에 입력합니다.
4. SAP 시스템에 로그인할 때 BI 플랫폼에서 사용해야 할 클라이언트 번호를 클라이언트 필드에 입력합니다.
BI 플랫폼은 시스템과 클라이언트 정보를 조합하여 논리 시스템 이름 목록에 항목을 추가합니다.
5. 사용 안 함 확인란이 선택되어 있지 않아야 합니다.

참고:

사용 안 함 확인란을 사용하면 BI 플랫폼에서 특정 SAP 시스템을 일시적으로 사용하지 못하도록 지정할 수 있습니다.

6. 메시지 서버를 통해 BI 플랫폼에 로그인해야 하도록 부하 분산을 설정한 경우 메시지 서버 및 로그인 그룹 필드에 적절한 내용을 입력합니다.

참고:

부하 분산을 사용하려면 BI 플랫폼 컴퓨터의 Services 파일에 적절한 항목을 만들어야 합니다. 특히, 단일 컴퓨터에 배포하지 않은 경우가 이에 해당합니다. CMS를 호스팅하는 컴퓨터, 웹 응용 프로그램 서버 및 인증 계정과 설정을 관리하는 모든 컴퓨터를 특별히 고려해야 합니다.

7. 부하 분산을 설정하지 않았거나 BI 플랫폼에서 SAP 시스템에 곧바로 로그인하도록 설정하려는 경우에는 응용 프로그램 서버 및 시스템 번호 필드에 필요한 정보를 입력합니다.
8. 사용자 이름, 암호 및 언어 필드에 BI 플랫폼이 SAP에 로그인할 때 사용할 SAP 계정의 사용자 이름, 암호, 언어 코드를 입력합니다.

참고:

이 자격 증명은 BI 플랫폼에 대해 만든 사용자 계정과 일치해야 합니다.

9. 업데이트를 클릭합니다.

권한 부여 시스템을 여러 개 추가하는 경우에는 옵션 탭을 클릭하고 BI 플랫폼에서 기본적으로 사용할 시스템(특정 SAP 시스템을 지정하지 않고 SAP 자격 증명을 사용하여 로그인을 시도하는 사용자를 인증하기 위해 접속할 시스템)을 지정합니다.

관련 항목

- 285 페이지에서 [BI 플랫폼의 사용자 계정 만들기](#)

7.5.3.2 권한 부여 시스템이 올바르게 추가되었는지 확인

1. 역할 가져오기 탭을 클릭합니다.
2. 논리 시스템 이름 목록에서 권한 부여 시스템 이름을 선택합니다.

권한 부여 시스템이 올바르게 추가되었으면 가져오도록 선택할 수 있는 역할의 목록이 사용 가능한 역할 목록에 표시됩니다.

팁:

논리 시스템 이름 목록에 역할이 표시되지 않으면 페이지에서 오류 메시지를 확인하십시오. 오류 메시지에서 문제 해결에 필요한 정보를 얻을 수 있습니다.

7.5.3.3 SAP 권한 부여 시스템에 대한 연결을 일시적으로 사용하지 않도록 설정하려면

CMC에서 BI 플랫폼과 SAP 권한 부여 시스템 간의 연결을 일시적으로 사용하지 않도록 설정할 수 있습니다. 이렇게 하면 SAP 권한 부여 시스템의 예약된 작동 중단과 같은 상황에서 BI 플랫폼의 응답 능력을 유지할 수 있습니다.

1. CMC에서 권한 부여 관리 영역으로 이동합니다.

2. SAP 링크를 두 번 클릭합니다.
3. 논리 시스템 이름 목록에서 사용하지 않도록 설정할 시스템을 선택합니다.
4. 사용 안 함 확인란을 선택합니다.
5. 업데이트를 클릭합니다.

7.5.4 SAP 인증 옵션 설정

SAP 인증에는 BI 플랫폼을 SAP 시스템과 통합할 때 지정할 수 있는 몇 가지 옵션이 포함됩니다. 다음과 같은 옵션을 지정할 수 있습니다.

- SAP 인증 사용 및 사용 안 함
- 연결 설정 지정
- 가져온 사용자를 BI 플랫폼 라이선스 모델에 연결
- SAP 시스템에 대한 단일 로그인 구성

7.5.4.1 SAP 인증 옵션 설정

1. CMC의 인증 관리 영역으로 이동합니다.
2. SAP 링크를 두 번 클릭한 다음 옵션 탭을 클릭합니다.
3. 설정을 검토하고 필요에 따라 수정합니다.

설정	설명
SAP 인증 사용	SAP 인증을 전혀 사용하지 않으려면 이 확인란의 선택을 취소합니다. 특정 SAP 시스템에 대해 SAP 인증을 비활성화하려면 권한 부여 시스템 탭에서 해당 시스템과 관련된 사용 안 함 확인란을 선택합니다.
내용 폴더 루트	이 필드에서는 BI 플랫폼이 CMC와 BI 실행 패드의 BW 폴더 구조를 복제할 원본 폴더를 지정할 수 있습니다. 기본 폴더는 /SAP/2.0이지만 다른 폴더로 변경할 수 있습니다. 이 값을 변경하려면 CMC와 Content Administration 워크벤치 모두에서 해당 값을 변경해야 합니다.
기본 시스템	이 목록에서는 BI 플랫폼이 기본적으로 사용할 SAP 권한 부여 시스템 (특정 SAP 시스템을 지정하지 않고 SAP 자격 증명을 사용하여 로그인 을 시도하는 사용자를 인증하기 위해 접속할 시스템)을 선택합니다. 참고: 기본 시스템을 지정할 경우 해당 시스템의 사용자는 Live Office 또는 Universe Designer와 같은 클라이언트 도구에서 SAP 인증을 사용하여 연결할 때 시스템 ID와 클라이언트를 입력할 필요가 없습니다. 예를 들어 SYS~100을 기본 시스템으로 설정하면 SYS~100/user1은 SAP 인증을 선택한 경우 user1로 로그인할 수 있습니다.
권한 부여 시스템 액세스 시도 실패 최대 횟수	플랫폼이 인증 요청을 완수하기 위해 SAP 시스템에 계속 접속을 시도 해야 하는 최대 횟수를 입력합니다. -1로 설정하면 BI 플랫폼이 횟수에 제한 없이 권한 부여 시스템에 접속을 시도합니다. 0으로 설정하면 BI 플랫폼은 권한 부여 시스템에 한 번만 접속을 시도합니다. 참고: 이 설정과 권한 부여 시스템 사용 안 함[초]을 같이 사용하면 SAP 권한 부여 시스템을 일시적으로 사용할 수 없을 때 BI 플랫폼이 이에 대처하는 방식을 구성할 수 있습니다. 시스템에서는 사용할 수 없게 된 SAP 시스템과의 통신을 언제 중지하고 해당 시스템과의 통신을 언제 다시 시작할 것인지 결정하는 데 이 설정을 사용합니다.
권한 부여 시스템 사용 안 함[초]	SAP 시스템에 대한 사용자 인증 시도를 다시 시작하기 전에 BI 플랫폼이 대기해야 하는 기간(초)을 입력합니다. 예를 들어 권한 부여 시스템 액세스의 최대 실패 수에 3을 입력하면 BI 플랫폼은 특정 SAP 시스템에 대해 최대 3회의 사용자 인증을 시도하고 4회째에도 실패하면 시스템에서 지정한 시간 동안 사용자 인증 시도를 멈춥니다.
시스템당 최대 동시 연결	이 필드를 사용하면 SAP 시스템에 대해 동시에 열리는 연결의 수를 지정할 수 있습니다. 예를 들어 이 필드에 2를 입력하면 BI 플랫폼은 SAP에 대해 두 개의 분리된 연결을 열어둡니다.
연결당 사용자 수	이 필드를 사용하면 각 연결마다 SAP 시스템에 허용되는 작업 수를 지정할 수 있습니다. 예를 들어 시스템당 최대 동시 연결에 2를, 연결당 사용자 수에 3을 입력한 경우 한 연결에서 로그인 수가 3개가 되면 BI 플랫폼은 해당 연결을 닫고 다시 시작합니다.

설정	설명
BI Viewer 및 BI Analyst	<p>새 사용자 계정이 BI Viewer 또는 BI Analyst 사용자 역할에 구성된 경우 이 옵션을 사용하십시오. BI Viewer 역할은 일반적으로 콘텐츠 소비자인 사용자에게 할당됩니다. 이 역할은 SAP BusinessObjects Business Intelligence 플랫폼은 사용권 계약에 규정된 대로 응용 프로그램 워크플로에 대해 제한된 액세스 권한만 갖습니다. BI Analyst 역할은 플랫폼 응용 프로그램의 콘텐츠를 만들고 수정하는 사용자를 위한 역할입니다. 이 역할에는 응용 프로그램 워크플로에 대한 액세스 권한에 제한이 없습니다.</p> <p>참고: 여기에서 선택하는 옵션은 BI 플랫폼에 설치한 사용자 라이선스의 수나 종류에 영향을 미치지 않습니다. 선택한 옵션에 해당하는 적절한 라이선스를 시스템에서 사용할 수 있어야 합니다.</p>
동시 사용자 및 명명된 사용자	<p>새 사용자 계정을 구성할 때 해당 사용자 계정에서 동시 사용자 라이선스를 사용할지 명명된 사용자 라이선스를 사용할지 지정하려면 이 옵션을 사용합니다. 동시 라이선스는 BI 플랫폼에 동시에 연결할 수 있는 사용자 수를 지정합니다. 이 유형의 라이선스는 적은 수의 동시 라이선스로 많은 사용자를 지원할 수 있으므로 유연성이 매우 높습니다. 예를 들어 사용자가 해당 시스템에 액세스하는 빈도 및 시간에 따라 100개의 동시 사용자 라이선스로 250명, 500명 또는 700명의 사용자를 지원할 수 있습니다. 명명된 사용자 라이선스는 특정 사용자와 관련되며 이 라이선스를 사용하면 사용자 이름과 암호를 기반으로 시스템에 액세스할 수 있습니다. 이 옵션을 사용하면 명명된 사용자는 연결된 다른 사용자 수에 관계없이 시스템에 액세스할 수 있습니다.</p> <p>참고: 여기에서 선택하는 옵션은 BI 플랫폼에 설치한 사용자 라이선스의 수나 종류에 영향을 미치지 않습니다. 선택한 옵션에 해당하는 적절한 라이선스를 시스템에서 사용할 수 있어야 합니다.</p>
전체 이름 및 전자 메일 주소 가져오기	SAP 인증 플러그 인에 대한 우선 순위 수준을 지정하려면 이 옵션을 선택합니다. SAP 계정에 사용된 전체 이름과 설명을 가져와서 BI 플랫폼에 사용자 개체와 함께 저장됩니다.
다른 특성 바인딩을 기준으로 SAP 특성 바인딩의 우선 순위 설정	SAP 사용자 특성(전체 이름 및 전자 메일 주소) 바인딩의 우선 순위를 지정합니다. 이 옵션을 1로 설정하면 SAP와 다른 플러그 인(Windows AD 및 LDAP)이 활성화된 경우 SAP 특성이 우선 적용됩니다. 3으로 설정하면 다른 활성화된 플러그 인의 특성이 우선 적용됩니다.

다음은 SAP 단일 로그인 서비스를 구성하는 데 사용되는 필드입니다.

설정	설명
시스템 ID	SAP 단일 로그인 서비스를 수행할 때 BI 플랫폼이 SAP 시스템에 제공하는 시스템 식별자입니다.
찾아보기	SAP 단일 로그인을 사용하기 위해 생성된 키 저장소 파일을 업로드하려면 이 단추를 사용합니다. 필드에 직접 파일에 대한 전체 경로를 입력할 수도 있습니다.
키 저장소 암호	키 저장소 파일에 액세스하기 위해 필요한 암호를 지정합니다.
개인 키 암호	키 저장소 파일에 관련된 인증서에 액세스하기 위해 필요한 암호를 지정합니다. 인증서는 SAP 시스템에 저장됩니다.
개인 키 별칭	키 저장소 파일에 액세스하기 위해 필요한 별칭을 지정합니다.

4. 업데이트를 클릭합니다.

관련 항목

- 90 페이지에서 [역할 기반 라이선스](#) "
- 285 페이지에서 [SAP 인증 구성](#) "

7.5.4.2 내용 폴더 루트 변경

1. CMC의 인증 관리 영역으로 이동합니다.
2. SAP 링크를 두 번 클릭합니다.
3. 옵션을 클릭하고 내용 폴더 루트 필드에 폴더 이름을 입력합니다.
여기에는 BI 플랫폼에서 BW 폴더 구조의 복제를 복제할 원본 폴더의 이름을 입력해야 합니다.
4. 업데이트를 클릭합니다.
5. BW Content Administration 워크벤치에서 Enterprise 시스템을 확장합니다.
6. 사용 가능한 시스템을 확장하고 BI 플랫폼을 연결할 시스템을 두 번 클릭합니다.
7. 레이아웃 탭을 클릭하고 콘텐츠 기본 폴더에 BI 플랫폼의 루트 SAP 폴더로 사용할 폴더를 입력합니다(예: /SAP/2.0/).

7.5.5 SAP 역할 가져오기

BI 플랫폼으로 SAP 역할을 가져오면 역할 구성원이 자신의 일반적인 SAP 자격 증명을 사용하여 시스템에 로그인하도록 할 수 있습니다. 또한 단일 로그인(SSO)이 활성화되어 SAP 사용자가 SAP GUI 또는 SAP Enterprise Portal에서 보고서에 액세스할 때 BI 플랫폼에 자동 로그인됩니다.

참고:

SSO를 활성화하려면 여러 가지 요구 사항을 충족해야 합니다. 예를 들어 SSO를 지원하는 드라이버와 응용 프로그램을 사용해야 하고 사용자의 서버와 웹 서버가 동일한 도메인에 있어야 하는 등의 조건이 있습니다.

가져오는 각 역할에 대해 BI 플랫폼에서 그룹이 생성됩니다. 각 그룹에는 SystemID~ClientNumber@NameOfRole 규칙에 따라 이름이 지정됩니다. 새 그룹은 CMC의 사용자 및 그룹 관리 영역에서 볼 수 있습니다. 이러한 그룹을 사용하여 BI 플랫폼 내에서 개체 보안을 정의할 수도 있습니다.

게시를 위해 BI 플랫폼을 구성하고 시스템으로 역할을 가져올 때는 다음과 같은 세 가지 주요 사용자 범주를 고려해야 합니다.

- BI 플랫폼 관리자

Enterprise 관리자는 SAP에서 콘텐츠를 게시할 수 있도록 시스템을 구성합니다. 관리자는 적절한 역할을 가져오고, 필요한 폴더를 만들고, BI 플랫폼에서 해당 역할과 폴더에 권한을 부여합니다.

- 콘텐츠 게시자

콘텐츠 게시자는 콘텐츠를 역할에 게시하는 데 필요한 권한을 갖고 있는 사용자입니다. 이 사용자 범주를 별도로 지정한 이유는 보고서를 게시하는 데 필요한 권한이 있는 사용자와 일반 역할 멤버를 구분하기 위해서입니다.

- 역할 멤버

역할 멤버는 콘텐츠 보유 역할에 속한 사용자입니다. 즉 이들 사용자는 보고서가 게시되는 대상 역할에 속합니다. 이들은 자신이 멤버로 속해 있는 역할을 대상으로 게시되는 모든 보고서에 대한 보기, 요청 시 보기 및 예약 권한을 갖습니다. 그러나 일반적인 역할 멤버는 새 콘텐츠를 게시할 수 없고 콘텐츠의 업데이트된 버전을 게시할 수도 없습니다.

콘텐츠를 처음 게시할 때는 먼저 모든 콘텐츠 게시 및 모든 콘텐츠 보유 역할을 BI 플랫폼으로 가져와야 합니다.

참고:

역할별 작업을 명확하게 구분하여 유지 관리하는 것이 좋습니다. 예를 들어 관리자 역할에서 콘텐츠를 게시할 수도 있지만 가능하면 콘텐츠 게시자 역할의 멤버만 콘텐츠를 게시할 수 있도록 하는 것이 더 좋습니다. 또한 콘텐츠 게시 역할의 기능은 콘텐츠를 게시할 수 있는 사용자를 정의하는 것으로만 국한됩니다. 따라서 콘텐츠 게시 역할에는 어떠한 콘텐츠도 포함되지 않아야 합니다. 콘텐츠 게시자의 임무는 일반 역할 멤버에게 액세스할 수 있는 콘텐츠 보유 역할에 콘텐츠를 게시하는 데서 그쳐야 합니다.

관련 항목

- 113 페이지에서 [BI 플랫폼에서 권한 작동 방식](#)"
- 123 페이지에서 [CMC에서 개체의 보안 설정 관리](#)"

7.5.5.1 SAP 역할 가져오기

1. CMC의 인증 관리 영역으로 이동합니다.
2. SAP 링크를 두 번 클릭합니다.
3. 옵션 탭에서 라이선스 계약에 따라 BI Viewer, BI Analyst, 동시 사용자 또는 명명된 사용자를 선택합니다.
여기에서 선택하는 옵션에 따라 BI 플랫폼에 설치된 사용자 라이선스의 수와 유형이 변경되지는 않습니다. 선택한 옵션에 해당하는 적절한 라이선스를 시스템에서 사용할 수 있어야 합니다.
4. 업데이트를 클릭합니다.
5. 역할 가져오기 탭의 논리 시스템 이름 목록에서 적절한 권한 부여 시스템을 선택합니다.
6. 사용 가능한 역할 영역에서 가져올 역할을 하나 이상 선택한 다음 추가를 클릭합니다.
7. 업데이트를 클릭합니다.

7.5.5.2 역할과 사용자를 올바르게 가져왔는지 확인

1. 방금 BI 플랫폼에 매핑한 역할 중 하나에 속한 SAP 사용자의 사용자 이름과 암호를 확인합니다.
2. Java BI 실행 패드의 경우 `http://webserver:portnumber/BOE/BI`로 이동합니다.
`webserver`는 웹 서버 이름으로, `portnumber`는 BI 플랫폼용으로 설정한 포트 번호로 바꾸십시오.
입력할 웹 서버의 이름, 포트 번호 또는 정확한 URL을 관리자에게 문의해야 할 수도 있습니다.
3. 인증 형식 목록에서 SAP를 선택합니다.
4. 로그인하려는 SAP 시스템 및 시스템 클라이언트를 입력합니다.
5. 매핑된 사용자의 사용자 이름과 암호를 입력합니다.
6. 로그인을 클릭합니다.
BI 실행 패드에 선택한 사용자로 로그인해야 합니다.

7.5.5.3 SAP 역할 및 사용자 업데이트

SAP 인증을 사용 가능하게 설정한 후에는 BI 플랫폼으로 가져온 매핑된 역할에 대한 정기 업데이트를 예약하고 실행해야 합니다. 그러면 SAP 역할 정보가 정확히 해당 플랫폼에 반영됩니다.

SAP 역할에 대한 업데이트를 실행하고 예약하기 위한 두 가지 옵션이 있습니다.

- **역할만 업데이트:** 이 옵션을 사용하면 BI 플랫폼으로 가져온 현재 매핑된 역할 간의 링크만 업데이트됩니다. 자주 업데이트를 실행할 것으로 예상하고 시스템 리소스 사용에 대한 우려가 있는 경우 이 옵션을 사용하는 것이 좋습니다. SAP 역할만 업데이트하면 새 사용자 계정이 만들어지지 않습니다.
- **역할 및 별칭 업데이트:** 이 옵션을 선택하면 역할 간의 링크가 업데이트될 뿐 아니라, SAP 시스템의 역할에 추가된 사용자 별칭에 대한 사용자 계정도 BI 플랫폼에 새로 만들어집니다.

참고:

SAP 인증을 사용했을 때 업데이트에 대한 사용자 별칭을 자동으로 만들도록 지정하지 않은 경우에는 새 별칭에 대해 계정이 만들어지지 않습니다.

7.5.5.3.1 SAP 역할에 대한 업데이트 예약

역할을 BI 플랫폼에 매핑한 후에는 시스템에서 이들 역할이 매핑되는 방식을 지정해야 합니다.

1. 사용자 업데이트 탭을 클릭합니다.
2. 역할만 업데이트 또는 역할 및 별칭 업데이트 섹션에서 예약을 클릭합니다.

팁:

업데이트를 즉시 실행하려면 지금 업데이트를 클릭합니다.

팁:

자주 업데이트를 수행하고 시스템 리소스에 대한 우려가 있는 경우 역할만 업데이트 옵션을 사용합니다. 역할과 별칭을 모두 업데이트하면 시간이 더 오래 걸립니다.

되풀이 대화 상자가 표시됩니다.

3. 개체 실행 풀다운 목록에서 옵션을 선택하고 표시된 필드에서 요청하는 예약 정보를 전부 입력합니다.

업데이트를 예약할 때 다음 표에 요약된 되풀이 패턴 중 하나를 선택할 수 있습니다.

되풀이 패턴	설명
매시간	업데이트가 매시간 실행됩니다. 시작할 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.

되풀이 패턴	설명
매일	업데이트가 매일 실행되거나 지정된 날짜 수마다 실행됩니다. 실행할 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매주	업데이트가 매주 실행됩니다. 개체를 매주 한 번 또는 여러 번 실행할 수 있으며 실행할 시간 및 날짜를 지정하고 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월	업데이트가 매월 또는 몇 달마다 실행됩니다. 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 N일	매월 특정 날짜에 업데이트가 실행됩니다. 실행 날짜와 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 첫째 월요일	업데이트가 매월 첫 번째 월요일에 실행됩니다. 실행할 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 마지막 날	업데이트가 매월 마지막 날 실행됩니다. 실행할 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 N번째 주 X	업데이트가 매월 지정된 주의 지정된 요일에 실행됩니다. 실행할 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
달력	이전에 생성된 달력에 지정한 날짜에 업데이트가 실행됩니다.

4. 예약 정보 입력을 마친 후 예약을 클릭합니다.

사용자 업데이트 탭에 예약된 다음 역할 업데이트 날짜가 표시됩니다.

참고:

역할만 업데이트 또는 역할 및 별칭 업데이트 섹션에서 예약된 업데이트 취소를 클릭하면 예약된 다음 업데이트를 언제든지 취소할 수 있습니다.

7.5.6 보안 네트워크 연결(SNC) 구성

이 단원에서는 BI 플랫폼에 대한 SAP 인증 설정 프로세스의 일부로 SNC를 구성하는 방법을 설명합니다.

SAP와 BI 플랫폼 시스템 간에 신뢰를 설정하려면 먼저 SNC에 대해 설정된 계정에서 SIA가 시작 및 실행되도록 구성해야 합니다. 또한 BI 플랫폼을 신뢰하도록 SAP 시스템을 구성해야 합니다. 이 가이드의 ERP 환경에 대한 보완 구성 장의 SAP 서버측 신뢰 구성 단원에 설명된 지침을 따르는 것이 좋습니다.

7.5.6.1 SAP 서버 측 트러스트 개요

이 단원에서는 SAP Web Application Servers(버전 6.20 이상) 및 BI 플랫폼 간 서버 측 트러스트를 구성하는 절차에 대해 설명합니다. 보고서 쿼리가 사용자의 컨텍스트에 의존하는 게시에서 다단계 보고서 표시를 사용할 경우 서버 측 트러스트를 설정해야 합니다.

서버 측 트러스트는 암호 없는 가장과 관련됩니다. 암호를 제공하지 않고 SAP 사용자를 가장하려면 사용자는 SAP에서 일반 사용자 이름 및 암호보다 더 안전한 방법을 사용하여 식별되어야 합니다. SAP_ALL 인증 프로파일 있는 SAP 사용자는 해당 암호를 알아야만 다른 SAP 사용자를 가장할 수 있습니다.

무료 SAP 암호화 라이브러리를 사용하여 서버 측 트러스트 활성화

무료 SAP 암호화 라이브러리를 사용하여 BI 플랫폼에 대한 서버 측 트러스트를 활성화하려면 등록된 보안 네트워크 통신(SNC) 공급자를 사용하여 인증된 자격 증명에 따라 관련 서버를 실행해야 합니다. 이러한 자격 증명은 암호 없이 가장할 수 있도록 하기 위해 SAP 내에서 구성됩니다. BI 플랫폼의 경우 이러한 SNC 자격 증명으로 보고서 표시와 관련된 서버(예: Crystal Reports 작업 서버)를 실행해야 합니다.

또한 서버 측 트러스트를 구성하기 위해 암호화 라이브러리가 필요합니다. SAP 암호화 라이브러리는 SAP 웹 사이트에서 다운로드할 수 있습니다. SAP 암호화 라이브러리는 서버 측 트러스트를 설정하는 데만 사용할 수 있습니다. Windows 및 UNIX용 암호화 라이브러리를 사용할 수 있습니다. 암호화 라이브러리에 대한 자세한 내용은 SAP 웹 사이트에서 SAP Notes 711093, 597059 및 397175를 참조하십시오.

SAP 서버 및 BI 플랫폼에는 자신의 ID를 서로에게 입증하는 인증서가 지정되어야 합니다. 각 서버는 자체의 인증서와 트러스트되는 상대방의 인증서 목록을 갖게 됩니다. SAP와 BI 플랫폼 간에 서버 측 트러스트를 구성하려면 개인 보안 환경(PSE)이라는 암호로 보호되는 인증서 집합을 만들어야 합니다. 이 문서에서는 PSE를 설정 및 유지 관리하는 방법과 PSE를 BI 플랫폼 처리 서버와 안전하게 연결하는 방법을 설명합니다.

클라이언트와 서버 SNC 비교

클라이언트 SNC에서 SNC 이름 식별자는 SU01에 있는 하나 이상의 SAP 사용자 이름으로 매핑됩니다. 로그인 요청이 전송되면 SAP 이름과 함께 SNC 이름이 SAP 시스템으로 전달되지만 암호는 전송되지 않습니다. SNC 이름이 지정한 SAP 이름으로 매핑되면 로그인이 허용됩니다. 직접 응용 프로그램 호스트 로그온에 대한 클라이언트쪽 로그온 문자열은 다음과 같이 표시됩니다.

```
ASHOST=myserver.mydomain SYSNR=37 CLIENT=066 LANG=EN USER=USER123
SNC_MODE=1 SNC_QOP=9 SNC_LIB="/usr/local/lib/libsapcrypto.so"
SNC_PARTNERNAME="p:CN=TheServer, OU=Dept., O=TheCompany, C=FR"
SNC_MYNAME="p:CN=TheUser, O=TheCompany, C=US"
```

이러한 로그인 시도가 성공하려면 SAP 사용자인 USER123이 p:CN=TheUser, O=TheCompany, C=SU01의 US로 매핑되어야 합니다. 한편, 서버 SNC에서는 SNC 이름 식별자와 SAP 사용자 이름 간에 명시적 매핑을 수행할 필요가 없습니다. 대신 사용자의 암호를 입력하지 않고 모든 사용자에 대

해 가장 로그온을 수행할 수 있도록 SNC 이름이 트랜잭션 SNC0에서 구성됩니다. 예를 들면 다음과 같습니다.

```
ASHOST=myserver.mydomain SYSNR=37 CLIENT=066 LANG=EN SNC_MODE=1
SNC_QOP=9 SNC_LIB="/usr/local/lib/libsapcrypto.so"
SNC_PARTNERNAME="p:CN=TheServer, OU=Dept., O=TheCompany, C=FR"
SNC_MYNAME="p:CN=TheUser, O=TheCompany, C=US" EXTIDTYPE=UN EXTIDDATA=USER123
```

서버 SNC 가장 로그온 또는 외부 ID를 통한 로그온은 이에 대응하는 클라이언트쪽 로그온에 비해 훨씬 강력합니다. 이러한 로그온을 통해 시스템의 모든 SAP 사용자 계정에 액세스할 수 있습니다. 기타 외부 ID 로그온 옵션에는 로그온 티켓 및 X.509 클라이언트 인증서가 있습니다.

BI 플랫폼 서버 책임

특정 BI 플랫폼 서버는 단일 로그온(SSO)을 사용하는 SAP 통합 환경에서 역할이 있습니다. 다음 표에는 이러한 서버와 해당 서버가 특정 책임 영역에 필요로 하는 SNC 유형이 나와 있습니다.

서버	SNC 유형	책임 영역
웹 응용 프로그램 서버	클라이언트	SAP 인증 역할 목록
	서버	Crystal Reports 동적 매개 변수 선택 목록 및 사용자 설정
CMS	클라이언트	암호, 티켓, 역할 소속 그룹 확인 및 사용자 목록
페이지 서버	서버	요청 시 Crystal Reports 보기
작업 서버	서버	Crystal Reports 예약
Web Intelligence 처리 서버	서버	Web Intelligence 보고서와 LOV(값 목록) 프롬프트 확인 및 예약
다차원 분석 서비스	서버	분석

참고:

웹 응용 프로그램 서버와 CMS는 클라이언트 SNC를 사용하므로 SNC 이름을 SAP 사용자 이름으로 명시적으로 매핑해야 합니다. 이는 테이블 USRACL에 대한 트랜잭션 SU01 또는 SM30 중 하나에 지정되어 있습니다.

7.5.6.2 SAP에서 서버측 트러스트 구성

다음 절차에서는 BI 플랫폼에서 사용하도록 SNC를 설정하는 방법을 설명합니다. 자세한 내용 또는 문제 해결 정보를 얻으려면 SAP 서버와 함께 제공되는 SAP 설명서를 참조하십시오.

7.5.6.2.1 서버 측 트러스트를 위해 SAP를 구성하려면

1. SAP 마켓 플레이스에서 모든 관련 플랫폼에 대한 SAP 암호화 라이브러리를 다운로드합니다.

참고:

암호화 라이브러리에 대한 자세한 내용은 SAP 웹 사이트에서 SAP 노트 711093, 597059 및 397175를 참조하십시오.

2. SAP 및 SAP가 실행되는 컴퓨터에 대한 SAP 관리자 자격 증명이 있는지와 BI 플랫폼 및 이 프로그램이 실행 중인 컴퓨터에 대한 관리자 자격 증명이 있는지 확인합니다.
3. SAP 컴퓨터에서 SAP 암호화 라이브러리 및 SAPGENPSE 도구를
<DRIVE>:WusrWsapW<SID>WSYSWexeWrunW 디렉터리(Windows)로 복사합니다.
4. SAP 암호화 라이브러리와 함께 설치된 "ticket" 파일을 찾은 후
<DRIVE>:WusrWsapW<SID>W<instance>WsecW 디렉터리(Windows)로 복사합니다.
5. 티켓이 있는 디렉터리를 가리키는 SECUDIR 환경 변수를 만듭니다.

참고:

SAP의 disp+ work 프로세스가 실행되는 사용자 계정에서 이 변수에 액세스할 수 있어야 합니다.

6. SAP GUI에서 트랜잭션 RZ10으로 이동한 후 Extended maintenance(확장 유지 관리) 모드에서 인스턴스 프로필을 변경합니다.
7. 프로필 편집 모드에서 SAP 프로필 변수에 암호화 라이브러리를 지정하고 SAP 시스템에 DN(고유 이름)을 지정합니다. 이러한 변수는 LDAP 명명 규칙을 따라야 합니다.

태그	의미	설명
CN	일반 이름	인증서 소유자의 일반 이름입니다.
OU	조직 단위	제품 그룹을 나타내는 PG와 같은 예를 들 수 있습니다.
O	조직	인증서가 발급된 조직의 이름입니다.
C	국가	조직이 있는 국가입니다.

예: R21: p:CN=R21, OU=PG, O=BOBJ, C=CA

참고:

접두사 p:는 SAP 암호화 라이브러리에 대한 것입니다. 이 접두사는 SAP 내의 DN을 참조할 때 필요하지만 STRUST에서 인증서를 검토하거나 SAPGENPSE를 사용할 때는 표시되지 않습니다.

8. 필요한 경우 SAP 시스템 대신 다음 프로필 값을 입력합니다.

프로필 변수	값
ssf/name	SAPSECULIB
ssf/ssfapi_lib	sapcrypto lib의 전체 경로
sec/libsapsecu	sapcrypto lib의 전체 경로
snc/gssapi_lib	sapcrypto lib의 전체 경로
snc/identity/as	SAP 시스템의 DN

9. SAP 인스턴스를 다시 시작합니다.
10. 시스템이 다시 실행되고 있을 때 로그인한 후 트랜잭션 STRUST로 이동합니다. 이제 이 트랜잭션에는 SNC 및 SSL에 대한 추가 항목이 있어야 합니다.
11. SNC 노드를 마우스 오른쪽 단추로 클릭하고 만들기를 클릭합니다.
RZ10에 지정한 ID가 나타납니다.
12. 확인을 클릭합니다.
13. SNC PSE에 암호를 지정하려면 잠금 아이콘을 클릭합니다.

참고:

이 암호는 잊어서는 안 됩니다. SNC PSE를 보거나 편집할 때마다 STRUST에서 이 암호를 입력하라는 메시지를 표시합니다.

14. 변경 사항을 저장합니다.

참고:

변경 내용을 저장하지 않은 경우 SNC를 활성화해도 응용 프로그램 서버가 시작되지 않습니다.

15. 트랜잭션 RZ10으로 돌아간 후 SNC 프로필 매개 변수의 나머지 부분을 추가합니다.

프로필 변수	매개 변수
snc/accept_insecure_rfc	1
snc/accept_insecure_r3int_rfc	1
snc/accept_insecure_gui	1
snc/accept_insecure_cplic	1

프로필 변수	매개 변수
snc/permit_insecure_start	1
snc/data_protection/min	1
snc/data_protection/max	3
snc/enable	1

최소 보호 수준은 인증만 (1)으로 설정되고 최대 보호 수준은 개인 정보 (3)입니다. snc/data_protection/use 값은 이 경우에 인증만 사용되도록 정의하지만 무결성 (2), 개인 정보 (3) 및 사용 가능한 최대 수준 (9)일 수도 있습니다. snc/accept_insecure_rfc, snc/accept_insecure_r3int_rfc, snc/accept_insecure_gui 및 snc/accept_insecure_cplic 값은 이전 통신 방법 및 안전하지 않을 수 있는 통신 방법이 여전히 허용되도록 하기 위해 (1)로 설정됩니다.

16. SAP 시스템을 다시 시작합니다.

이제 서버 측 트러스트를 위해 BI 플랫폼을 구성해야 합니다.

7.5.6.3 서버 측 신뢰를 위한 BI 플랫폼 구성

서버 측 신뢰를 위해 BI 플랫폼을 구성하려면 다음 절차를 수행해야 합니다. 이러한 단계는 Windows 기반이지만 SAP 도구가 명령줄 도구이므로 UNIX에서도 비슷한 단계가 적용됩니다.

1. 환경을 설정합니다.
2. 개인 보안 환경(PSE)을 생성합니다.
3. BI 플랫폼 서버를 구성합니다.
4. PSE 액세스를 구성합니다.
5. SAP 인증 SNC 설정을 구성합니다.
6. SAP 전용 서버 그룹을 설정합니다.

관련 항목

- 302 페이지에서 [환경을 설정하려면](#)"
- 302 페이지에서 [PSE를 생성하려면](#)"
- 304 페이지에서 [BI 플랫폼 서버 구성](#)"
- 304 페이지에서 [PSE 액세스를 구성하려면](#)"
- 305 페이지에서 [SAP 인증 SNC 설정을 구성하려면](#)"

- 306 페이지에서 [서버 그룹 사용](#)"

7.5.6.3.1 환경을 설정하려면

시작하기 전에 다음을 확인합니다.

- SAP 암호화 라이브러리를 다운로드한 후 BI 플랫폼 처리 서버가 실행되는 호스트에서 확장했습니다.
- SAP 암호화 라이브러리를 SNC 공급자로 사용하도록 해당 SAP 시스템을 구성했습니다.

PSE 유지 관리를 시작하려면 먼저 라이브러리, 도구 및 PSE가 저장되어 있는 환경을 설정해야 합니다.

1. SAP 암호화 라이브러리(PSE 유지 관리 도구 포함)를 BI 플랫폼이 실행되는 컴퓨터의 폴더에 복사합니다.
예: C:\Program Files\WSAPWCrypto
2. 이 폴더를 PATH 환경 변수에 추가합니다.
3. 암호화 라이브러리를 가리키는 시스템 차원의 환경 변수 SNC_LIB를 추가합니다.
예: C:\Program Files\WSAPWCrypto\Wsapcrypto.dll
4. sec라는 하위 폴더를 만듭니다.
예: C:\Program Files\WSAPWCrypto\Wsec
5. sec 폴더를 가리키는 시스템 차원의 환경 변수 SECUDIR을 추가합니다.
6. SAP 암호화 라이브러리의 ticket 파일을 sec 폴더에 복사합니다.

관련 항목

- 298 페이지에서 [SAP에서 서버측 트러스트 구성](#)"

7.5.6.3.2 PSE를 생성하려면

관련 BI 플랫폼 서버에 PSE가 있고 이 PSE가 SAP와 연결되어 있으면 SAP는 BI 플랫폼 서버를 트러스트된 엔터티로 받아 들입니다. SAP 및 BI 플랫폼 구성 요소의 공용 인증서 버전을 상호 공유하여

트러스트가 설정됩니다. 첫 번째 단계는 자체 인증서를 자동으로 생성하는 BI 플랫폼에 대한 PSE를 생성하는 것입니다.

1. 명령 프롬프트를 열고 암호화 라이브러리 폴더 내에서 `sapgenpse.exe gen_pse -v -p BOE.pse`를 실행합니다.
2. BI 플랫폼 시스템에 대해 원하는 PIN 및 DN을 선택합니다.
예: CN=MyBOE01, OU=PG, O=BOBJ, C=CA.
이제 자체 인증서가 있는 기본 PSE가 생성되었습니다.
3. 다음 명령을 사용하여 PSE의 인증서를 내보냅니다.

```
sapgenpse.exe export_own_cert -v -p BOE.pse -o MyBOECert.crt
```

4. SAP GUI에서 트랜잭션 STRUST로 이동한 후 SNC PSE를 엽니다.
이미 지정한 암호를 입력할 수 있는 대화 상자가 표시됩니다.
5. 이전에 만든 MyBOECert.crt 파일을 가져옵니다.
SAPGENPSE의 인증서는 Base64로 인코딩됩니다. 가져올 때 Base64를 선택했는지 확인합니다.
6. SAP 서버의 PSE 인증서 목록에 BI 플랫폼 인증서를 추가하려면 인증서 목록에 추가 단추를 클릭합니다.
7. BI 플랫폼의 PSE에 SAP의 인증서를 추가하려면 SAP 인증서를 두 번 클릭합니다.
8. STRUST에서 변경 내용을 저장합니다.
9. 내보내기 단추를 클릭하고 인증서에 대한 파일 이름을 제공합니다.
예: MySAPCert.crt.

참고:

Base64 형식이 그대로 적용됩니다.

10. 트랜잭션 SNC0으로 이동합니다.
11. 다음을 참조하여 새 항목을 추가합니다.
 - 시스템 ID는 임의로 지정할 수 있지만 BI 플랫폼 시스템을 반영해야 합니다.
 - SNC 이름은 2단계에서 BI 플랫폼 PSE를 만들 때 제공한 DN(앞에 p:가 붙음)입니다.
 - RFC에 대한 항목 활성화 및 종료 ID에 대한 항목 활성화 확인란을 모두 선택해야 합니다.
12. 내보낸 인증서를 BI 플랫폼 PSE에 추가하려면 명령 프롬프트에서 다음 명령을 실행합니다.

```
sapgenpse.exe maintain_pk -v -a MySAPCert.crt -p BOE.pse
```

SAP 암호화 라이브러리가 BI 플랫폼 컴퓨터에 설치됩니다. BI 플랫폼 서버를 SAP 서버로 인식하는 데 사용되는 PSE가 생성되었습니다. SAP와 BI 플랫폼 PSE 간에 인증서가 교환되었습니다. SAP는 BI 플랫폼 PSE에 대한 액세스 권한이 있는 엔터티가 RFC 호출 및 암호 없는 가장을 수행하도록 허용합니다.

관련 항목

- 304 페이지에서 [BI 플랫폼 서버 구성](#)

7.5.6.3.3 BI 플랫폼 서버 구성

BI 플랫폼에 대한 PSE를 생성한 후에 SAP 처리에 적절한 서버 구조를 구성해야 합니다. 다음 절차에서는 SAP 처리 서버에 대한 노드를 만들어 노드 수준에서 운영 체제 자격 증명을 설정할 수 있도록 합니다.

참고:

이 버전의 BI 플랫폼에서 서버는 더 이상 중앙 구성 관리자(CCM)에서 구성되지 않습니다. 대신 새 SIA(Server Intelligence Agent)가 만들어집니다.

1. CCM에서 SAP 처리 서버에 대한 새 노드를 만듭니다.
SAPProcessor와 같은 적절한 이름으로 노드의 이름을 지정합니다.
2. CMC에서 필요한 처리 서버를 새 노드에 추가한 후 새 서버를 시작합니다.

7.5.6.3.4 PSE 액세스를 구성하려면

BI 플랫폼 노드 및 서버를 구성한 후에는 SAPGENPSE 도구를 사용하여 PSE 액세스를 구성해야 합니다.

1. 명령 프롬프트에서 다음 명령을 실행합니다.

```
sapgenpse.exe seclogin -p SBOE.pse
```

참고:

PSE PIN을 입력하라는 메시지가 표시됩니다. 이 도구를 BI 플랫폼 SAP 처리 서버에 사용되는 것과 동일한 자격 증명에서 실행할 경우 사용자 이름을 지정할 필요가 없습니다.

2. SSO(단일 로그인) 링크가 설정되어 있는지 확인하려면 다음 명령을 사용하여 PSE의 내용을 나열합니다.

```
sapgenpse.exe maintain_pk -l
```

결과는 다음과 유사합니다.

```
C:\Documents and Settings\Whareskoug\Desktop\sapcrypto.x86\Wntintel>sapgenpse.exe
maintain_pk -l
maintain_pk for PSE "C:\Documents and Settings\Whareskoug\My Documents\WsnC\Wsec\Wbobjsapproc.pse"
*** Object <PKList> is of the type <PKList_OID> ***
```



```

1. -----
Version:          0 (X.509v1-1988)
SubjectName:      CN=R21Again, OU=PG, O=BOBJ, C=CA
IssuerName:       CN=R21Again, OU=PG, O=BOBJ, C=CA
SerialNumber:     00
Validity - NotBefore:  Wed Nov 28 16:23:53 2007 (071129002353Z)
                  NotAfter:  Thu Dec 31 16:00:01 2037 (380101000001Z)
Public Key Fingerprint:  851C 225D 1789 8974 21DB 9E9B 2AE8 9E9E
SubjectKey:       Algorithm RSA (OID 1.2.840.113549.1.1.1), NULL

```

C:\WDocuments and Settings\Whareskoug\Desktop\Wsapcrypto.x86\Wntintel>

seclogin 명령을 성공적으로 수행한 후에는 PSE PIN을 다시 입력하라는 메시지가 표시되지 않습니다.

참고:

PSE 액세스 문제가 발생하면 -O를 사용하여 PSE 액세스를 지정합니다. 예를 들어, 특정 도메인에 있는 특정 사용자에게 PSE 액세스 권한을 부여하려면 다음을 입력합니다.

```
sapgenpse seclogin -p SBOE.pse -O <domainWuser>
```

7.5.6.3.5 SAP 인증 SNC 설정을 구성하려면

PSE 액세스를 구성한 후에 CMC에서 SAP 인증 설정을 구성해야 합니다.

1. CMC의 인증 관리 영역으로 이동합니다.
2. SAP 링크를 두 번 클릭합니다.
권한 부여 시스템 설정이 나타납니다.
3. SAP 인증 페이지에서 SNC 설정 탭을 클릭합니다.
4. 논리 시스템 이름 목록에서 권한 부여 시스템을 선택합니다.
5. 기본 설정에서 SNC[보안 네트워크 통신] 사용을 선택합니다.
6. SNC 라이브러리 경로에 SNC 라이브러리 설정의 경로를 입력합니다.

참고:

SNC_LIB 환경 변수에 라이브러리가 이미 정의되어 있더라도 이 단계가 필요합니다.

7. 보호 품질 아래에서 보호 수준을 선택합니다.
예를 들어 인증을 선택합니다.

참고:

SAP 시스템에 구성한 보호 수준을 초과하지 않아야 합니다. 보호 수준을 사용자 지정할 수 있습니다. 보호 수준은 조직의 요구 사항과 SNC 라이브러리의 기능에 따라 결정됩니다.

8. 상호 인증 설정 아래에 SAP 시스템의 SNC 이름을 입력합니다.

SNC 이름의 형식은 SNC 라이브러리에 따라 다릅니다. SAP 암호화 라이브러리를 사용하는 경우 LDAP 명명 규칙에 따라 구별된 이름을 사용하는 것이 좋습니다. 이 이름에는 "p:"를 접두사로 추가해야 합니다.

9. BI 플랫폼 서버를 실행하는 데 사용되는 자격 증명의 SNC 이름이 Enterprise 시스템의 SNC 이름 필드에 표시되는지 확인합니다.

참고:

여러 개의 SNC 이름이 구성되어 있을 때는 이 필드가 비어 있어야 합니다.

10. SAP 시스템 및 BI 플랫폼 PSE 모두의 DN을 입력합니다.

7.5.6.3.6 서버 그룹 사용

PSE에 대한 액세스 권한이 있는 자격 증명에 따라 처리 서버(Crystal Report 또는 Web Intelligence) 서버가 실행되고 있지 않은 경우, 필수 지원 서버와 함께 이러한 서버만 포함하는 특정 서버 그룹을 만들어야 합니다. 다양한 BI 플랫폼 서버에 대한 자세한 내용과 설명은 아키텍처 장을 참조하십시오.

SAP 콘텐츠용 콘텐츠 처리 서버를 구성하는 경우 세 개의 옵션 중 하나를 선택할 수 있습니다.

1. PSE에 대한 액세스 권한이 있는 자격 증명에 따라 실행되는 모든 BI 플랫폼 서버를 비롯한 단일 SIA 유지 관리. 이는 가장 간단한 옵션으로 서버 그룹을 만들 필요가 없습니다. 불필요한 개수의 서버까지 PSE에 액세스할 수 있기 때문에 이 옵션의 보안 수준은 가장 낮습니다.
2. PSE에 대한 액세스 권한이 있는 보조 SIA를 만들어 Crystal 보고서 또는 Interactive 처리 서버에 추가합니다. 원본 SIA에서 중복된 서버를 삭제합니다. 서버 그룹을 만들 필요는 없지만 PSE에 액세스할 수 있는 서버 수가 줄어듭니다.
3. PSE에 대한 액세스 권한이 있는 SAP 전용 SIA 만들기. SIA를 Crystal 보고서 또는 Web Intelligence 처리 서버에 추가합니다. 이러한 방법을 사용하는 경우 무엇보다 중요한 점은 SAP 콘텐츠는 이러한 서버에서만 실행되어야 한다는 사실입니다. 이러한 시나리오에서는 콘텐츠를 특정 서버로 전달해야 하기 때문에 SIA를 위한 서버 그룹을 만들어야 합니다.

서버 그룹 사용 지침

서버 그룹은 SAP 콘텐츠 처리에만 사용되는 SIA를 참조해야 합니다. 또한 서버 그룹은 다음 서버도 참조해야 합니다.

- 적응 서버
- 게시 서버
- 대상 작업 서버

모든 SAP 콘텐츠, Web Intelligence 문서 및 Crystal 보고서는 매우 긴밀한 연결을 사용하여 서버 그룹과 연결되어야 합니다. 즉, 그룹에 포함된 서버에서 실행되어야 합니다. 개체 수준에서 이러한 연결이 설정되면 서버 그룹 설정은 게시뿐만 아니라 직접 일정 설정 모두의 설정으로 전파되어야 합니다.

SAP 관련 처리 서버에서 다른(비SAP) 콘텐츠가 처리되는 것을 방지하려면 원본 SIA의 모든 서버를 포함하는 다른 서버 그룹을 만들어야 합니다. 이러한 콘텐츠와 비 SAP 서버 그룹 간에 긴밀한 연결을 설정하는 것이 좋습니다.

7.5.6.4 멀티 패스 게시 구성

멀티 패스 게시 문제 해결

멀티 패스 게시 관련 문제가 발생하면, SAP용 MDA(다차원 데이터 액세스) 드라이버 또는 CR(Crystal Reports) 추적을 활성화하고 각 작업 또는 받는 사람에 대해 사용된 로그인 문자열을 확인합니다. 이러한 로그인 문자열은 다음과 유사합니다.

```
SAP: Successfully logged on to SAP server.
Logon handle: 1. Logon string: CLIENT=800 LANG=en
ASHOST="vanrdw2k107.sap.crystald.net" SYSNR=00 SNC_MODE=1 SNC_QOP=1
SNC_LIB="C:\WINDOWS\System32\Wsapcrypto.dll"
SNC_PARTNERNAME="p:CN=R21Again, OU=PG, O=BOBJ, C=CA" EXTIDDATA=HENRIKRPT3 EXTIDTYPE=UN
```

로그온 문자열에는 사용자 이름에 대해 EXTIDTYPE=UN이 있어야 하며 EXTIDDATA는 받는 사람의 SAP 사용자 이름이어야 합니다. 이 예제에서는 로그인 시도가 성공적으로 수행되었습니다.

7.5.6.5 보안 네트워크 통신과 통합하기 위한 워크플로

BI 플랫폼에서는 SAP 구성 요소 간 데이터 암호화 및 인증을 위해 보안 네트워크 통신(SNC)을 구현하는 환경을 지원합니다. SAP Cryptographic Library(또는 SNC 인터페이스를 사용하는 기타 외부 보안 제품)를 배포한 경우에는 보안 환경 내에 BI 플랫폼을 효과적으로 통합하기 위해 몇 가지 값을 추가로 설정해야 합니다.

보안 네트워크 통신을 사용하도록 플랫폼을 구성하려면 다음 작업을 수행해야 합니다.

1. 적절한 사용자 계정을 통해 시작 및 실행되도록 BI 플랫폼 서버를 구성합니다.
2. BI 플랫폼 시스템을 신뢰하도록 SAP 시스템을 구성합니다.
3. 중앙 관리 콘솔에 있는 SNC 링크에서 SNC 설정을 구성합니다.
4. BI 플랫폼으로 SAP 역할과 사용자를 가져옵니다.

관련 항목

- 292 페이지에서 [SAP 역할 가져오기](#)

- 298 페이지에서 [SAP에서 서버측 트러스트 구성](#)
- 301 페이지에서 [서버 측 신뢰를 위한 BI 플랫폼 구성](#)

7.5.6.6 중앙 관리 콘솔에서 SNC 설정 구성

SNC 설정을 구성하려면 먼저 BI 플랫폼에 새 권한 부여 시스템을 추가해야 합니다. 또한 SNC 라이브러리 파일을 알려진 디렉터리에 복사하고 이 파일을 가리키는 환경 변수 RFC_LIB를 만들어야 합니다.

1. SAP 인증 페이지에서 SNC 설정 탭을 클릭합니다.
2. 논리 시스템 이름 목록에서 권한 부여 시스템을 선택합니다.
3. 기본 설정에서 SNC[보안 네트워크 통신] 사용을 선택합니다.
4. SNC 라이브러리 경로에 SNC 라이브러리 설정의 경로를 입력합니다.

참고:

응용 프로그램 서버와 CMS는 동일한 OS 유형이어야 하며, 암호화 라이브러리에 대한 경로가 동일해야 합니다.

5. 보호 품질 아래에서 보호 수준을 선택합니다.
예를 들어 인증을 선택합니다.

참고:

보호 수준을 사용자 지정할 수 있습니다. 보호 수준은 조직의 요구 사항과 SNC 라이브러리의 기능에 따라 결정됩니다.

6. 상호 인증 설정 아래에 SAP 시스템의 SNC 이름을 입력합니다.

SNC 이름의 형식은 SNC 라이브러리에 따라 다릅니다. SAP 암호화 라이브러리를 사용하는 경우 LDAP 명명 규칙에 따라 구별된 이름을 사용하는 것이 좋습니다. 이 이름에는 "p:"를 접두사로 추가해야 합니다.

7. BI 플랫폼 서버를 실행하는 데 사용되는 자격 증명의 SNC 이름이 Enterprise 시스템의 SNC 이름 필드에 표시되는지 확인합니다.

참고:

여러 개의 SNC 이름을 구성한 시나리오에서는 이 필드가 비어 있어야 합니다.

8. 업데이트를 클릭합니다.
9. SAP 인증 페이지에서 권한 부여 시스템 탭을 클릭합니다.
10. 언어 필드 아래 SNC 이름이라는 다른 필드가 새로 추가된 것을 알 수 있습니다.
11. SAP BW 서버에 대해 구성한 SNC 이름을 SNC 이름 필드에 입력합니다. 이 필드는 선택 사항입니다. 이 이름은 BI 플랫폼을 신뢰하도록 SAP 시스템을 구성할 때 사용한 이름과 같아야 합니다.

관련 항목

- 287 페이지에서 [SAP 권한 부여 시스템에 연결](#)

7.5.6.7 권한 부여 사용자를 SNC 이름에 연결

1. SAP BW 시스템에 로그인하여 SU01 트랜잭션을 실행합니다.
사용자 유지 관리: 시작 화면이 열립니다.
2. 권한 부여 사용자로 지정된 SAP 계정의 이름을 사용자 필드에 입력한 다음 도구 모음에서 변경을 클릭합니다.
사용자 유지 관리 화면이 열립니다.
3. SNC 탭을 클릭합니다.
4. 앞서 4단계에서 입력한 SNC USER ACCOUNT를 SNC 이름 필드에 입력합니다.
5. 저장을 클릭합니다.

7.5.6.8 SNC 액세스 제어 목록에 시스템 ID 추가

1. SAP BW 시스템에 로그인하여 SNC0 트랜잭션을 실행합니다.
뷰 변경 "SNC: 시스템의 ACL(액세스 제어 목록): 개요" 화면이 열립니다.
2. 도구 모음에서 새 항목을 클릭합니다.
새 항목: 추가된 항목의 세부 정보 화면이 열립니다.
3. BI 플랫폼 컴퓨터의 이름을 시스템 ID 필드에 입력합니다.
4. SNC 사용자 이름 필드에 p:<SNC 사용자 이름>을 입력합니다. 여기서 SNC 사용자 이름은 BI 플랫폼 서버를 구성할 때 사용한 계정입니다.

참고:

SNC 공급자가 gssapi32.dll인 경우 SNC 사용자 이름을 입력할 때 대문자를 사용합니다. 사용자 계정을 지정할 때 도메인 이름을 포함해야 합니다. 예를 들면 domainWusername 같은 형식입니다.

5. RFC 항목 활성화됨 및 외부 ID 항목 활성화됨을 선택합니다.
6. 다른 모든 옵션의 선택을 취소하고 저장을 클릭합니다.

7.5.7 SAP 시스템에 대한 단일 로그인 설정

SAP 시스템에 대한 단일 로그인을 활성화하려면 키 저장소 파일과 관련 인증서를 만들어야 합니다. 이 파일과 인증서를 만들려면 keytool 명령줄 프로그램을 사용하십시오. keytool 프로그램은 기본적으로 각 플랫폼의 sdk/bin 디렉터리에 설치됩니다.

인증서는 CMC를 사용하여 SAP ABAP BW 시스템과 BI 플랫폼에 추가해야 합니다.

참고:

SAP 데이터베이스에 대한 단일 로그인을 설정하려면 먼저 SAP 인증 플러그인을 구성해야 합니다.

7.5.7.1 키 저장소 파일 생성

PKCS12Tool 프로그램을 사용하면 SAP 데이터베이스에 대한 단일 로그인 설정에 필요한 키 저장소 파일과 인증서를 생성할 수 있습니다. 다음 표에 지원되는 각 플랫폼에서의 PKCS12Tool.jar 기본 위치가 나열되어 있습니다.

플랫폼	기본 위치
Windows	<INSTALLDIR>WSAP BusinessObjects Enterprise XI 4.0\java\lib
Unix	sap_bobj/enterprise_xi40/java/lib

1. 명령 프롬프트를 시작하고 PKCS12Tool 프로그램이 있는 디렉터리로 이동합니다.
2. 키 저장소 파일을 기본 설정으로 생성하려면 다음 명령을 실행합니다.

```
java -jar PKCS12Tool.jar
```

cert.der 및 keystore.p12 파일이 동일한 디렉터리에 생성됩니다. 파일에는 다음 기본값이 포함됩니다.

매개 변수	기본값
-keystore	keystore.p12
-alias	myalias
-storepass	123456
-dname	CN=CA
-validity	365
-cert	cert.der

팁:

기본값을 무시하려면 -? 매개 변수를 사용하여 도구를 실행합니다. 다음 메시지가 표시됩니다.

```
Usage: PKCS12Tool <options>
  -keystore <filename(keystore.p12)>
  -alias <key entry alias(myalias)>
  -storepass <keystore password(123456)>
  -dname <certificate subject DN(CN=CA)>
  -validity <number of days(365)>
  -cert <filename (cert.der)>
  (No certificate is generated when importing a keystore)
  -disablefips
  -importkeystore <filename>
```

이 매개 변수를 사용하여 기본값을 무시할 수 있습니다.

7.5.7.2 공개 키 인증서 내보내기

키 저장소 파일에 대한 인증서를 만든 후 내보내야 합니다.

1. 명령 프롬프트를 시작하고 keytool 프로그램이 있는 디렉터리로 이동합니다.
2. 키 저장소 파일에 대한 키 인증서를 내보내려면 다음 명령을 사용합니다.

```
keytool -exportcert -keystore <keystore> -storetype pkcs12 -file <filename>
  -alias <alias>
```

<keystore> 부분을 키 저장소 파일의 이름으로 바꾸십시오.

<filename> 부분을 인증서 이름으로 바꾸십시오.

<alias> 부분을 키 저장소 파일을 만들 때 사용한 별칭으로 바꾸십시오.

3. 창이 뜨면 키 저장소 파일에 지정했던 암호를 입력합니다.

keytool 프로그램이 있는 디렉터리에 키 저장소 파일과 인증서가 생겼습니다.

7.5.7.3 대상 ABAP SAP 시스템에 인증서 파일 가져오기

다음 작업을 수행하려면 BI 플랫폼 배포 환경에 해당하는 키 저장소 파일과 이에 연결된 인증서가 필요합니다.

참고:

이 작업은 ABAP SAP 시스템에만 수행할 수 있습니다.

1. SAP GUI를 사용하여 SAP ABAP BW 시스템에 연결합니다.

참고:

관리 권한이 있는 사용자로 연결해야 합니다.

2. SAP GUI에서 STRUSTSSO2를 실행합니다.
시스템에서 인증서 파일을 가져올 준비가 되었습니다.
3. Certificate 탭으로 이동합니다.
4. Use Binary option 확인란이 선택되어 있어야 합니다.
5. 파일 경로 단추를 클릭하여 인증서 파일이 있는 위치를 지정합니다.
6. 녹색 확인 표시를 클릭합니다.
인증서 파일이 업로드됩니다.
7. Add to Certificate List를 클릭합니다.
인증서 파일이 Certificate List에 표시됩니다.
8. Add to ACL을 클릭하고 시스템 ID와 클라이언트를 지정합니다.
시스템 ID는 SAP BW가 BI 플랫폼 시스템을 확인할 때 사용하는 ID와 같아야 합니다.
인증서가 액세스 제어 목록(ACL)에 추가됩니다. 클라이언트가 000으로 지정되어야 합니다.
9. 설정을 저장하고 끝냅니다.
변경 내용이 SAP 시스템에 저장됩니다.

7.5.7.4 CMC에서 SAP 데이터베이스에 대한 단일 로그인 설정

다음 절차를 수행하려면 관리자 계정을 사용하여 SAP 보안 플러그 인에 액세스해야 합니다.

1. CMC의 인증 관리 영역으로 이동합니다.

2. SAP 링크를 두 번 클릭한 다음 옵션 탭을 클릭합니다.
가져온 인증서가 없는 경우에는 SAP SSO 서비스 섹션에 다음 메시지가 표시됩니다.
키 저장소 파일이 업로드되지 않았습니다.
3. 제공된 필드에 BI 플랫폼 시스템의 시스템 ID를 지정합니다.
이 값은 대상 SAP ABAP 시스템의 인증서를 가져올 때 사용한 값과 동일해야 합니다.
4. 찾아보기 단추를 클릭하여 키 저장소 파일을 지정합니다.
5. 다음 필수 세부 정보를 입력합니다.

필드	필수 정보
키 저장소 암호	키 저장소 파일에 액세스하기 위해 필요한 암호를 지정합니다. 이 암호는 키 저장소 파일을 만들 때 지정합니다.
개인 키 암호	키 저장소 파일에 관련된 인증서에 액세스하기 위해 필요한 암호를 지정합니다. 이 암호는 키 저장소 파일에 대한 인증서를 만들 때 지정합니다.
개인 키 별칭	키 저장소 파일에 액세스하기 위해 필요한 별칭을 지정합니다. 이 별칭은 키 저장소 파일을 만들 때 지정합니다.

6. 업데이트를 눌러 설정을 제출합니다.
설정이 제출되면 시스템 ID 필드 아래 다음 메시지가 표시됩니다.
키 저장소 파일이 업로드되었습니다.

7.5.7.5 적응형 처리 서버에 보안 토큰 서비스 추가

클러스터 환경에서 보안 토큰 서비스는 각 적응형 처리 서버에 개별적으로 추가됩니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 핵심 서비스를 두 번 클릭합니다.
핵심 서비스 아래 서버 목록이 표시됩니다.
3. 적응형 처리 서버를 마우스 오른쪽 단추로 클릭하고 중지를 선택합니다.
서버 상태가 중지됨으로 될 때까지 기다리십시오.
4. 적응형 처리 서버를 마우스 오른쪽 단추로 클릭하고 서비스 선택을 선택합니다.
서비스 선택 대화 상자가 표시됩니다.
5. 사용 가능한 서비스 목록에서 보안 토큰 서비스를 오른쪽의 서비스 목록으로 옮깁니다.
선택 영역에 추가 단추를 사용하여 선택을 이동합니다.
6. 확인을 클릭합니다.
7. 적응형 처리 서버를 다시 시작합니다.

7.5.8 SAP Crystal Reports 및 SAP Netweaver에 대해 SSO 구성

기본적으로, BI 플랫폼은 SAP Crystal Reports 사용자가 단일 로그인(SSO)을 사용하여 SAP 데이터에 액세스할 수 있도록 구성됩니다.

7.5.8.1 SAP Netweaver 및 SAP Crystal Reports에 대해 SSO 비활성화

1. 중앙 관리 콘솔(CMC)에서 응용 프로그램을 클릭합니다.
2. Crystal Reports 구성을 두 번 클릭합니다.
3. 단일 로그인 옵션을 클릭합니다.
4. 다음 드라이버 중 하나를 선택합니다.

드라이버	표시 이름
운영 데이터 저장소 드라이버	crdb_ods
Open SQL 드라이버	crdb_opensql
InfoSet 드라이버	crdb_infoSet
BW MDX 쿼리 드라이버	crdb_bwmdx

5. 제거를 클릭합니다.
6. 저장 후 닫기를 클릭합니다.
7. SAP Crystal Reports를 다시 시작합니다.

7.5.8.2 SAP Netweaver 및 SAP Crystal Reports에 대해 SSO 재활성화

SAP Netweaver(ABAP) 및 SAP Crystal Reports에 대해 SSO를 다시 활성화하려면 다음 단계를 수행하십시오.

1. 중앙 관리 콘솔(CMC)에서 응용 프로그램을 클릭합니다.
2. Crystal Reports 구성을 두 번 클릭합니다.
3. 단일 로그인 옵션을 클릭합니다.
4. 데이터베이스 로그인에 SSO 컨텍스트 사용에서 다음을 입력합니다.

crdb_ods	ODS 드라이버 활성화
crdb_opensql	Open SQL 드라이버 활성화
crdb_bwmdx	SAP BW MDX 쿼리 드라이버 활성화
crdb_infoset	InfoSet 드라이버 활성화

5. 추가를 클릭합니다.
6. 저장 후 닫기를 클릭합니다.
7. SAP Crystal Reports를 다시 시작합니다.

7.6 PeopleSoft 인증

7.6.1 개요

BI 플랫폼에서 PeopleSoft Enterprise 데이터를 사용하려면 프로그램에 현재의 배포 환경에 대한 정보를 제공해야 합니다. 이 정보에 따라 BI 플랫폼은 사용자가 자신의 PeopleSoft 자격 증명을 사용하여 프로그램에 로그인할 수 있도록 승인합니다.

7.6.2 PeopleSoft Enterprise 인증 사용

PeopleSoft Enterprise 정보를 BI 플랫폼에서 사용하려면 BI 플랫폼에 PeopleSoft Enterprise 시스템 인증 방법에 대한 정보가 필요합니다.

7.6.2.1 BI 플랫폼에서 PeopleSoft Enterprise 인증 사용

1. 중앙 관리 콘솔에 관리자로 로그인합니다.
2. 관리 영역에서 인증을 클릭합니다.
3. PeopleSoft Enterprise를 두 번 클릭합니다.
PeopleSoft Enterprise 페이지가 나타납니다. 옵션, 도메인, 역할, 사용자 업데이트 네 개의 탭이 있습니다.
4. 옵션 탭에서 PeopleSoft Enterprise 인증 사용 확인란을 선택합니다.
5. 새 별칭, 업데이트 옵션, 새 사용자 옵션에서 BI 플랫폼 배포 환경에 맞는 값으로 적절히 변경합니다. 시스템 탭으로 이동하기 전에 업데이트를 클릭하여 변경 내용을 저장합니다.
6. 서버 탭을 클릭합니다.
7. PeopleSoft Enterprise 시스템 사용자 영역에서 PeopleSoft Enterprise 데이터베이스에 로그인할 때 사용할 BI 플랫폼의 데이터베이스 사용자 이름과 암호를 입력합니다.
8. PeopleSoft Enterprise 도메인 영역에서 PeopleSoft Enterprise 환경에 연결할 때 사용되는 도메인 이름과 QAS 주소를 입력하고 추가를 클릭합니다.

참고:

PeopleSoft 도메인이 여러 개인 경우 액세스할 추가 도메인에 대해 이 단계를 반복하십시오. 먼저 입력한 도메인이 기본 도메인이 됩니다.

9. 업데이트를 클릭하여 변경 내용을 저장합니다.

7.6.3 PeopleSoft 역할을 BI 플랫폼에 매핑

BI 플랫폼에서는 사용자가 매핑하는 PeopleSoft 역할마다 그룹이 자동으로 만들어집니다. 매핑된 PeopleSoft 역할의 멤버를 나타내는 별칭도 생성됩니다.

만들어진 각 별칭에 대해 사용자 계정을 만들 수 있습니다.

하지만, 여러 시스템을 실행하고 사용자가 둘 이상의 시스템에 계정을 가진 경우에는 같은 이름을 가진 별칭에 각 사용자를 할당한 후 BI 플랫폼에서 계정을 만들 수 있습니다.

그렇게 하면 BI 플랫폼에서 같은 사용자에 대해 만들어지는 계정 수가 줄어듭니다.

예를 들어, PeopleSoft HR 8.3 및 PeopleSoft Financials 8.4를 실행하고 사용자 중 30명이 두 시스템에 모두 액세스할 수 있는 경우에는 이들 사용자에게 대해 30개의 계정만 만들어집니다. 같은 이름을 가진 별칭에 각 사용자를 지정하지 않으면 BI 플랫폼에서 30명의 사용자에게 대해 60개의 계정이 만들어집니다.

하지만, 여러 시스템을 실행하고 사용자 이름이 겹치는 경우에는 만들어지는 각 별칭에 대해 새 멤버 계정을 만들어야 합니다.

예를 들어, Russell Aquino(사용자 이름 "raquino")의 사용자 계정으로 PeopleSoft HR 8.3을 실행하고 Raoul Aquino(사용자 이름 "raquino")의 사용자 계정으로 PeopleSoft Financials 8.4를 실행하는 경우에는 각 사용자의 별칭에 대한 계정을 따로 만들어야 합니다. 그렇지 않으면 같은 BI 플랫폼 계정에 두 명의 사용자가 추가되는데, 이 두 사용자는 자신의 PeopleSoft 자격 증명으로 BI 플랫폼에 로그인하고 두 PeopleSoft 시스템의 데이터에 모두 액세스할 수 있게 됩니다.

7.6.3.1 BI 플랫폼에 PeopleSoft 역할 매핑

1. 중앙 관리 콘솔에 관리자로 로그인합니다.
2. 인증을 클릭합니다.
3. PeopleSoft Enterprise for PeopleTools를 두 번 클릭합니다.
4. PeopleSoft Enterprise 도메인 영역의 역할 탭에서 BI 플랫폼에 매핑할 역할과 관련된 도메인을 선택합니다.
5. 매핑할 역할을 선택하려면 다음 옵션 중 하나를 사용합니다.
 - PeopleSoft Enterprise 역할 영역의 역할 검색 상자에서 찾으려는 역할을 입력하고 BI 플랫폼에 매핑한 후 >를 클릭합니다.
 - 사용 가능한 역할 목록에서 BI 플랫폼에 매핑할 역할을 선택하고 >를 클릭합니다.

참고:

- 특정 사용자 또는 역할을 검색할 때 와일드카드 %를 사용할 수 있습니다. 예를 들어, "A"로 시작하는 모든 역할을 검색하려면 A%를 입력합니다. 검색에서는 대/소문자도 구분합니다.
 - 다른 도메인에서 역할을 매핑하려면 다른 도메인의 역할에 일치하도록 사용 가능한 도메인 목록에서 새 도메인을 선택해야 합니다.
6. BI 플랫폼과 PeopleSoft 간에 강제로 그룹과 사용자를 동기화하려면 사용자 동기화 강제 수행 확인란을 선택합니다. BI 플랫폼에서 이미 가져온 PeopleSoft 그룹을 제거하려면 사용자 동기화 강제 수행 확인란을 선택하지 않은 상태로 둡니다.
 7. 새 별칭 옵션 영역에서 다음 옵션 중 하나를 선택합니다.
 - 추가된 각 별칭을 같은 이름의 계정에 할당

둘 이상의 시스템에 계정이 있는 사용자의 계정으로 여러 PeopleSoft Enterprise 시스템을 운영하고 두 사용자가 다른 시스템에 대해 같은 사용자 이름을 가지고 있지 않은 경우 이 옵션을 선택합니다.
 - 추가된 모든 별칭에 대한 새 계정 만들기

PeopleSoft Enterprise를 하나만 운영하거나, 사용자 대다수가 시스템 중 하나에만 계정이 있거나, 사용자 이름이 둘 이상의 시스템에 있는 다른 사용자의 사용자 이름과 겹치는 경우 이 옵션을 선택합니다.

8. 업데이트 옵션 영역에서 다음 옵션 중 하나를 선택합니다.

- 새 별칭을 추가하고 새 사용자 만들기

BI 플랫폼에 매핑된 모든 사용자에게 대해 새 별칭을 만들려면 이 옵션을 선택합니다. BI 플랫폼 계정이 없는 사용자에게 대해 새 계정이 추가되거나, 추가된 모든 별칭에 대한 새 계정 만들기 옵션을 선택한 경우에는 모든 사용자에게 대해 새 계정이 추가됩니다.

- 새 별칭을 추가하지 않고 새 사용자를 만들지 않음

매핑할 역할에 사용자가 많지만 이 중 일부 사용자만 BI 플랫폼을 사용할 경우 이 옵션을 선택합니다. 플랫폼에서는 사용자에게 대해 별칭과 계정을 자동으로 만들지 않습니다. 대신 BI 플랫폼에 처음으로 로그인하는 사용자에게 대해서만 별칭 및 계정(필요한 경우)을 만듭니다. 이는 기본 옵션입니다.

9. 새 사용자 옵션 영역에서 새 사용자를 만드는 방식을 지정합니다.

SAP BusinessObjects Business Intelligence 플랫폼 라이선스가 사용자 역할을 기반으로 하는 경우 다음 옵션 중 하나를 선택하십시오.

- 새 사용자를 BI Viewer로 만들기

새 사용자 계정이 BI Viewer 역할에 구성됩니다. BI Viewer 역할의 모든 계정에 대한 BI 플랫폼 응용 프로그램 액세스 권한이 사용권 계약에 정의됩니다. 사용자는 BI Viewer 역할용으로 정의된 응용 프로그램 워크플로에만 액세스할 수 있습니다. 액세스 권한은 일반적으로 비즈니스 인텔리전스 문서를 보는 것으로 제한됩니다. 이 역할은 일반적으로 BI 플랫폼 응용 프로그램을 통해 콘텐츠를 사용하는 사용자에게 적합합니다.

- 새 사용자를 BI Analyst로 만들기 새 계정이 BI Analyst 역할에 구성됩니다. BI Analyst 역할의 모든 계정에 대한 BI 플랫폼 응용 프로그램 액세스 권한이 사용권 계약에 정의됩니다. 사용자는 BI Analyst 역할에 대해 정의된 모든 응용 프로그램 워크플로에 액세스할 수 있습니다. 액세스 권한에는 비즈니스 인텔리전스 문서를 보고 수정하는 것이 포함됩니다. 이 역할은 일반적으로 BI 플랫폼 응용 프로그램의 콘텐츠를 만들고 수정하는 사용자에게 적합합니다.

SAP BusinessObjects Business Intelligence 플랫폼 라이선스가 사용자 역할을 기반으로 하지 않는 경우에는 다음 옵션 중 하나를 선택하십시오.

- 새 사용자를 명명된 사용자로 만들기

새 사용자 계정이 명명된 사용자 라이선스를 사용하도록 구성됩니다. 명명된 사용자 라이선스는 특정 사용자와 관련되며 이 라이선스를 사용하면 사용자 이름과 암호를 기반으로 시스템에 액세스할 수 있습니다. 이 옵션을 사용하면 명명된 사용자는 연결된 다른 사용자 수에 관계없이 시스템에 액세스할 수 있습니다. 이 옵션을 사용하여 만든 각 사용자 계정에 대한 명명된 사용자 라이선스가 있어야 합니다.

- 새 사용자를 동시 사용자로 만들기

새 사용자 계정이 동시 사용자 라이선스를 사용하도록 구성됩니다. 동시 라이선스는 BI 플랫폼에 동시에 연결할 수 있는 사용자 수를 지정합니다. 이 유형의 라이선스는 소규모 동시 라이선스로 많은 사용자를 지원할 수 있으므로 매우 유연합니다. 예를 들어 사용자가 BI 플랫폼에 액세스하는 빈도 및 시간에 따라 100개의 동시 사용자 라이선스로 250명, 500명 또는 700명의 사용자를 지원할 수 있습니다.

지금 선택한 역할은 BI 플랫폼에서 그룹으로 나타납니다.

7.6.3.2 다시 매핑할 때의 고려 사항

BI 플랫폼에 이미 매핑되어 있는 역할에 사용자를 추가하는 경우 역할을 다시 매핑하여 BI 플랫폼에 사용자를 추가해야 합니다. 역할을 다시 매핑할 때 사용자를 명명된 사용자로 매핑할지 동시 사용자로 매핑할지 지정하는 옵션은 역할에 추가한 새 사용자에게만 영향을 미칩니다.

예를 들어 먼저 "새 사용자를 명명된 사용자로 만들기" 옵션을 선택하여 역할을 BI 플랫폼에 매핑합니다. 그 후에 같은 역할에 사용자를 추가하고 이 역할을 "새 사용자를 동시 사용자로 만들기" 옵션을 선택하여 다시 매핑합니다.

이 경우 해당 역할의 새 사용자만 BI 플랫폼에 동시 사용자로 매핑되고 이전에 매핑되었던 사용자는 명명된 사용자로 유지됩니다. 이는 처음에 사용자를 동시 사용자로 매핑하고 나중에 새 사용자를 명명된 사용자로 다시 매핑할 때도 동일합니다.

7.6.3.3 역할 매핑 해제

1. 중앙 관리 콘솔에 관리자로 로그인합니다.
2. 인증을 클릭합니다.
3. PeopleSoft Enterprise를 클릭합니다.
4. 역할을 클릭합니다.
5. 제거할 역할을 선택하고 < 기호를 클릭합니다.
6. 업데이트를 클릭합니다.

해당 역할의 멤버가 다른 계정이나 별칭을 갖고 있지 않다면 더 이상 BI 플랫폼에 액세스할 수 없습니다.

참고:

BI 플랫폼에 역할을 매핑하기 전에 개별 계정을 삭제하거나 역할에서 사용자를 제거하여 특정 사용자가 로그인하지 못하도록 할 수도 있습니다.

7.6.4 사용자 업데이트 예약

ERP 시스템에 대한 사용자 데이터 변경 내용이 BI 플랫폼 사용자 데이터에 반영되도록 하려면 정기적인 사용자 업데이트를 예약하면 됩니다. 업데이트를 통해 중앙 관리 콘솔(CMC)에서 구성한 매핑 설정에 따라 ERP 및 BI 플랫폼 사용자가 자동으로 동기화됩니다.

가져온 역할에 대한 업데이트를 실행하고 예약하기 위한 두 가지 옵션이 있습니다.

- **역할만 업데이트:** 이 옵션을 사용하면 BI 플랫폼으로 가져온 현재 매핑된 역할 간의 링크만 업데이트됩니다. 자주 업데이트를 실행하며 시스템 리소스 사용량에 대한 우려가 있는 경우 이 옵션을 사용하는 것이 좋습니다. 역할만 업데이트하면 새 사용자 계정이 만들어지지 않습니다.
- **역할 및 별칭 업데이트:** 이 옵션을 선택하면 역할 간의 링크가 업데이트될 뿐 아니라, EBS 시스템에 추가된 새 사용자 별칭에 대한 사용자 계정도 BI 플랫폼에 새로 만들어집니다.

참고:

인증을 사용했을 때 업데이트에 대한 사용자 별칭을 자동으로 만들도록 지정하지 않은 경우에는 새 별칭에 대해 계정이 만들어지지 않습니다.

7.6.4.1 사용자 업데이트 예약

역할을 BI 플랫폼에 매핑한 후에는 해당 역할이 시스템에서 업데이트되는 방식을 지정해야 합니다.

1. 사용자 업데이트 탭을 클릭합니다.
2. 역할만 업데이트 또는 역할 및 별칭 업데이트 섹션에서 예약을 클릭합니다.

팁:

업데이트를 즉시 실행하려면 지금 업데이트를 클릭합니다.

팁:

자주 업데이트를 수행하고 시스템 리소스에 대한 우려가 있는 경우 역할만 업데이트 옵션을 사용합니다. 역할과 별칭을 모두 업데이트하면 시간이 더 오래 걸립니다.

되풀이 대화 상자가 표시됩니다.

3. 개체 실행 목록에서 옵션을 선택하고 요청하는 예약 정보를 모두 입력합니다.

업데이트를 예약할 때 다음 표에 요약된 되풀이 패턴 중 하나를 선택할 수 있습니다.

되풀이 패턴	설명
매시간	업데이트가 매시간 실행됩니다. 시작할 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매일	업데이트가 매일 실행되거나 지정된 일 수 간격으로 실행됩니다. 실행할 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.

되풀이 패턴	설명
매주	업데이트가 매주 실행됩니다. 개체를 매주 한 번 또는 여러 번 실행할 수 있으며 실행할 시간 및 날짜를 지정하고 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월	업데이트가 매월 또는 몇 달 간격으로 실행됩니다. 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 N일	매월 특정 날짜에 업데이트가 실행됩니다. 실행 날짜와 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 첫째 월요일	업데이트가 매월 첫 번째 월요일에 실행됩니다. 업데이트 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 마지막 날	업데이트가 매월 마지막 날 실행됩니다. 업데이트 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 N번째 주 X	업데이트가 매월 지정된 주의 지정된 요일에 실행됩니다. 업데이트 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
달력	이전에 생성된 달력에 지정한 날짜에 업데이트가 실행됩니다.

4. 예약 정보 입력을 마친 후 예약을 클릭합니다.

사용자 업데이트 탭에 예약된 다음 역할 업데이트 날짜가 표시됩니다.

참고:

역할만 업데이트 또는 역할 및 별칭 업데이트 섹션에서 예약된 업데이트 취소를 클릭하면 예약된 다음 업데이트를 언제든지 취소할 수 있습니다.

7.6.5 PeopleSoft 보안 브리지 사용

BI 플랫폼의 보안 브리지 기능을 사용하면 BI 플랫폼으로 PeopleSoft EPM 보안 설정을 가져올 수 있습니다.

보안 브리지는 다음의 두 가지 모드로 작동합니다.

- 구성 모드

구성 모드에서 보안 브리지는 응답 파일을 만들 수 있는 인터페이스를 제공합니다. 이 응답 파일을 통해 실행 모드의 보안 브리지 동작을 관리합니다.

- 실행 모드

응답 파일에 정의한 매개 변수에 따라 보안 브리지는 PeopleSoft EPM에 있는 차원 테이블의 보안 설정을 BI 플랫폼의 유니버스로 가져옵니다.

7.6.5.1 보안 설정 가져오기

보안 설정을 가져오려면 다음 작업을 순서대로 수행하십시오.

- 보안 브리지에서 관리할 개체를 정의합니다.
- 응답 파일을 만듭니다.
- 보안 브리지 응용 프로그램을 실행합니다.

설정을 가져온 후의 보안 관리에 대한 자세한 내용은 보안 설정 관리 단원을 참조하십시오.

7.6.5.1.1 관리되는 개체 정의

보안 브리지를 실행하기에 앞서 이 응용 프로그램으로 관리할 개체를 결정하는 과정이 중요합니다. 보안 브리지는 하나 이상의 PeopleSoft 역할과 BI 플랫폼 그룹, 하나 이상의 유니버스를 관리합니다.

- 관리되는 PeopleSoft 역할

이는 PeopleSoft 시스템에 있는 역할입니다. 이 역할을 가진 멤버는 PeopleSoft EPM을 통해 PeopleSoft 데이터로 작업합니다. BI 플랫폼의 관리되는 유니버스에 대한 액세스 권한을 부여하거나 이 권한을 업데이트할 멤버가 포함되어 있는 역할을 선택해야 합니다.

이 역할의 멤버에 대해 정의되는 액세스 권한은 PeopleSoft EPM에서의 멤버 권한에 따라 결정됩니다. 보안 브리지는 이 보안 설정을 BI 플랫폼에 가져옵니다.

- 관리되는 BI 플랫폼 그룹

보안 브리지를 실행하면 이 프로그램은 관리되는 PeopleSoft 역할의 각 멤버마다 사용자를 BI 플랫폼에 만듭니다.

사용자가 만들어지는 그룹은 관리되는 BI 플랫폼 그룹입니다. 이 그룹의 멤버는 관리되는 유니버스에 대한 액세스 권한이 보안 브리지를 통해 유지 관리됩니다. 모든 사용자가 하나의 그룹에 만들어지기 때문에 관리되는 BI 플랫폼 그룹에서 특정 사용자를 제거하면 해당 사용자의 보안 설정이 보안 브리지에서 업데이트되지 않도록 구성할 수 있습니다.

보안 브리지를 실행하기 전에 BI 플랫폼에서 사용자를 만들 그룹을 선택해야 합니다. 지정한 그룹이 존재하지 않는 경우에는 보안 브리지가 BI 플랫폼에 이 그룹을 만듭니다.

- 관리되는 유니버스

관리되는 유니버스는 보안 브리지가 PeopleSoft EPM으로부터 가져오는 보안 설정의 대상이 되는 유니버스입니다. BI 플랫폼 시스템에 저장된 유니버스 중에서 보안 브리지로 관리할 유니버스를 선택해야 합니다. 관리되는 PeopleSoft 역할의 멤버인 동시에 관리되는 BI 플랫폼 그룹의 멤버인 사람은 PeopleSoft EPM에서 액세스할 수 없는 유니버스를 통해서 어떤 데이터에도 액세스할 수 없습니다.

7.6.5.1.2 응답 파일을 만들기

1. 보안 브리지를 설치할 때 지정한 폴더로 이동하여 Windows이면 `crpsepmsecuritybridge.bat`, UNIX이면 `crpsepmsecuritybridge.sh`를 실행합니다.

참고:

Windows에서는 기본적으로 이 위치는 `C:\Program Files\Business Objects\Business Objects 12.0 Integration Kit for PeopleSoft\Wepm`입니다.

PeopleSoft EPM의 보안 브리지 대화 상자가 나타납니다.

2. 새로 만들기를 선택하여 응답 파일을 만들거나 열기를 선택한 후 찾아보기를 클릭하여 수정할 응답 파일을 지정합니다. 파일에 사용할 언어를 선택합니다.
3. 다음을 클릭합니다.
4. PeopleSoft EPM SDK 및 BI 플랫폼 SDK의 위치를 지정합니다.

참고:

- PeopleSoft EPM SDK는 일반적으로 PeopleSoft 서버의 `<PS_HOME>\class\com.peoplesoft.epm.pf.jar`에 있습니다.
- BI 플랫폼 SDK는 일반적으로 `C:\Program Files (x86)\SAP Business Objects\WSAP Business Objects Enterprise XI 4.0\java\lib`에 있습니다.

5. 다음을 클릭합니다.

대화 상자에서 PeopleSoft 데이터베이스에 대한 연결과 드라이버 정보를 묻는 메시지가 표시됩니다.

6. 데이터베이스 목록에서 적절한 데이터베이스 유형을 선택하고 다음 필드에 정보를 입력하십시오.

필드	설명
데이터베이스	PeopleSoft 데이터베이스의 이름입니다.
호스트	데이터베이스를 호스팅하는 서버의 이름입니다.
포트 번호	서버에 액세스할 때 사용하는 포트 번호입니다.
클래스 위치	데이터베이스 드라이버에 대한 클래스 파일의 위치입니다.
사용자 이름	사용자 이름입니다.
암호	암호입니다.

7. 다음을 클릭합니다.

보안 브리지 실행 시 사용할 모든 클래스의 목록이 대화 상자에 표시됩니다. 필요한 경우 이 목록에 클래스를 추가하거나 제거할 수 있습니다.

8. 다음을 클릭합니다.

BI 플랫폼의 연결 정보를 입력할 수 있는 대화 상자가 나타납니다.

9. 다음 필드에 적절한 정보를 입력하십시오.

필드	설명
서버	중앙 관리 서버(CMS)가 있는 서버의 이름입니다.
사용자 이름	사용자 이름입니다.
암호	암호입니다.
인증	인증 형식입니다.

10. 다음을 클릭합니다.

11. BI 플랫폼 그룹을 선택하고 다음을 클릭합니다.

참고:

- 이 필드에 지정하는 그룹이 보안 브리지가 관리되는 PeopleSoft 역할의 멤버에 대한 사용자를 만드는 곳입니다.
- 존재하지 않는 그룹을 지정하면 보안 브리지가 이 그룹을 새로 만듭니다.

PeopleSoft 시스템의 역할 목록이 대화 상자에 표시됩니다.

12. 보안 브리지가 관리할 역할에 대해 가져옴 옵션을 선택하고 다음을 클릭합니다.

참고:

보안 브리지는 선택한 역할의 각 멤버마다 사용자를 관리되는 BI 플랫폼 그룹(이전 단계에서 지정한 그룹)에 만듭니다.

대화 상자에 BI 플랫폼의 유니버스가 목록으로 나타납니다.

13. 보안 브리지가 보안 설정을 가져와 전달할 유니버스를 선택하고 다음을 클릭합니다.
 14. 보안 브리지 로그 파일의 파일 이름과 이 로그 파일의 저장 위치를 지정합니다. 로그 파일은 보안 브리지가 PeopleSoft EPM에서 보안 설정을 성공적으로 가져왔는지 판단할 때 사용합니다.
 15. 다음을 클릭합니다.

대화 상자에 보안 브리지가 실행 모드에서 사용할 응답 파일의 미리 보기가 표시됩니다.

16. 저장을 클릭하고 응답 파일을 저장할 위치를 선택합니다.
 17. 다음을 클릭합니다.

보안 브리지에 대한 응답 파일이 만들어졌습니다.

18. 끝내기를 클릭합니다.

참고:

응답 파일은 직접 만들거나 수정할 수도 있는 Java 속성 파일입니다. 자세한 내용은 PeopleSoft 응답 파일 단원을 참조하십시오.

7.6.5.2 보안 설정 적용

보안 설정을 적용하려면 `crpsepmsecuritybridge.bat`(Windows의 경우) 또는 `the crpsempsecurity bridge.sh`(UNIX의 경우) 파일을 실행하고 앞서 만든 응답 파일을 인수로 사용하십시오. 예를 들어 `crpsepmsecuritybridge.bat`(Windows) 또는 `crpsempsecuritybridge.sh`(UNIX) `myresponsefile.properties`를 입력합니다.

보안 브리지 응용 프로그램이 실행됩니다. 응답 파일에 지정한 PeopleSoft 역할의 멤버에 대해 BI 플랫폼에 사용자를 만들고 PeopleSoft EPM에서 보안 설정을 관련 유니버스로 가져옵니다.

7.6.5.2.1 매핑 시 고려 사항

실행 모드 중 보안 브리지는 관리되는 PeopleSoft 역할의 각 멤버마다 사용자를 BI 플랫폼에 만듭니다.

사용자는 Enterprise 인증 별칭만 가지도록 만들어지며 BI 플랫폼에서 해당 사용자에게 임의의 암호를 할당합니다. 따라서 사용자는 관리자가 새 암호를 직접 다시 할당하거나 PeopleSoft 보안 플러그인을 통해 BI 플랫폼에 역할을 매핑하여 PeopleSoft 자격 증명으로 로그인할 수 있어야 BI 플랫폼 로그인이 가능합니다.

7.6.5.3 보안 설정 관리

적용한 보안 설정을 관리하려면 보안 브리지에 의해 관리되는 개체를 수정하면 됩니다.

7.6.5.3.1 관리되는 사용자

보안 브리지는 다음 기준에 따라 사용자를 관리합니다.

- 사용자가 관리되는 PeopleSoft 역할의 멤버인지 여부
- 사용자가 관리되는 BI 플랫폼 그룹의 멤버인지 여부

어떤 사용자가 BI 플랫폼의 유니버스를 통해 PeopleSoft 데이터에 액세스할 수 있도록 하려면 해당 사용자가 관리되는 PeopleSoft 역할 및 관리되는 BI 플랫폼 그룹 모두의 멤버여야 합니다.

- 관리되는 PeopleSoft 역할의 멤버지만 BI 플랫폼에 계정이 없는 사용자의 경우, 보안 브리지는 계정을 만들어 임의의 암호를 할당합니다. 관리자는 사용자가 BI 플랫폼에 로그인할 수 있도록 새 암호를 수동으로 다시 할당할지 아니면 역할을 PeopleSoft 보안 플러그인을 통해 BI 플랫폼에 매핑할지를 결정해야 합니다.

- 관리되는 BI 플랫폼 그룹의 멤버이면서 관리되는 PeopleSoft 역할의 멤버인 사용자의 경우, 보안 브리지는 해당 사용자에게 적용되는 보안 설정을 업데이트하여 관리되는 유니버스를 통해 적절한 데이터에 액세스할 수 있도록 합니다.

관리되는 PeopleSoft 역할의 멤버가 BI 플랫폼에 기존 계정을 갖고 있지만 관리되는 BI 플랫폼 그룹의 멤버가 아닌 경우 보안 브리지는 해당 사용자에게 적용되는 보안 설정을 업데이트하지 않습니다. 일반적으로 이러한 상황은 보안 브리지가 만든 사용자 계정을 관리되는 BI 플랫폼 그룹에서 관리자가 수동으로 제거하는 경우에만 발생합니다.

참고:

관리되는 BI 플랫폼 그룹에서 사용자를 제거하면 이 사용자들의 보안 설정을 PeopleSoft에서와는 다르게 구성할 수 있으므로 이는 효과적인 보안 관리 방법이 될 수 있습니다.

반대로 관리되는 BI 플랫폼 그룹의 멤버가 관리되는 PeopleSoft 역할의 멤버가 아닌 경우, 보안 브리지는 해당 사용자에게 관리되는 유니버스에 대한 액세스를 허용하지 않습니다. 일반적으로 이러한 상황은 보안 브리지가 이전에 BI 플랫폼에 매핑한 사용자를 PeopleSoft 관리자가 관리되는 PeopleSoft 역할에서 제거하는 경우에만 발생합니다.

참고:

관리되는 PeopleSoft 역할에서 사용자를 제거하면 해당 사용자가 PeopleSoft의 데이터에 액세스할 수 없게 되므로 이 또한 보안 관리 방법 중 하나입니다.

7.6.5.3.2 관리되는 유니버스

보안 브리지는 제한 집합을 통해 유니버스를 관리하는데, 이는 관리되는 사용자가 관리되는 유니버스를 통해 액세스할 수 있는 데이터를 제한합니다.

제한 집합은 쿼리 컨트롤, SQL 생성 등에 대한 제한을 모은 것입니다. 다음과 같이 보안 브리지는 관리되는 유니버스에 대한 행 액세스와 개체 액세스 제한을 적용/업데이트합니다.

- PeopleSoft EPM에 정의된 차원 테이블에 행 액세스 제한을 적용합니다. 이 제한은 사용자별로 적용되며 다음 설정 중 하나로 구성할 수 있습니다.
 - 사용자가 모든 데이터에 액세스할 수 있음
 - 사용자가 데이터에 액세스할 수 없음
 - 사용자가 PeopleSoft에서의 자기 행 수준 권한에 따라 데이터에 액세스할 수 있음(해당 권한은 PeopleSoft EPM에 정의된 SJT(Security Join Table)을 통해 노출됨)
- 계수 개체가 액세스하는 필드에 따라 계수 개체에 개체 액세스 제한을 적용합니다.

계수 개체가 PeopleSoft의 메트릭으로 정의된 필드에 액세스하는 경우 이 계수 개체에 대한 액세스 허용 여부는 PeopleSoft의 참조되는 메트릭에 사용자가 액세스할 수 있는지에 따라 결정됩니다. 사용자가 이 메트릭에 액세스할 수 없으면 이 계수 개체로의 액세스는 거부됩니다. 사용자가 모든 메트릭에 액세스할 수 있으면 이 계수 개체로의 액세스가 허용됩니다.

관리자는 보안 브리지가 관리하는 유니버스의 수를 제한하는 방식으로 사용자가 PeopleSoft 시스템으로부터 액세스할 수 있는 데이터를 제한할 수도 있습니다.

7.6.5.4 PeopleSoft 응답 파일

BI 플랫폼의 보안 브리지 기능은 응답 파일에 지정된 설정에 따라 작동합니다.

일반적으로 구성 모드에서 보안 브리지에 제공되는 인터페이스를 사용하여 응답 파일을 만듭니다. 하지만 이 파일은 Java 속성 파일이기 때문에 직접 만들거나 수정할 수도 있습니다.

이 부록에는 응답 파일을 직접 만들 때 이 파일에 삽입해야 하는 매개 변수에 대한 정보가 제공됩니다.

참고:

이 파일을 만들 때는 Java 속성 파일의 이스케이프 용법을 준수해야 합니다(예: ':' 기호는 'W:'로 나타냄).

7.6.5.4.1 응답 파일 매개 변수

다음 표에 응답 파일에 포함되는 매개 변수가 나와 있습니다.

매개 변수	설명
classpath	필요한 .jar 파일을 로드하기 위한 클래스 경로입니다. 경로가 여러 개인 경우 Windows와 UNIX 모두 ';' 기호로 구분해야 합니다. com.peoplesoft.epm.pf.jar 및 JDBC 드라이버 .jar 파일의 클래스 경로가 필요합니다.
db.driver.name	PeopleSoft 데이터베이스에 연결할 때 사용하는 JDBC 드라이버 이름입니다(예: com.microsoft.jdbc.sqlserver.SQLServerDriver).

매개 변수	설명
db.connect.str	PeopleSoft 데이터베이스에 연결할 때 사용하는 JDBC 연결 문자열입니다(예: jdbc:microsoft:sqlserver://vanrdpsft01:1433;DatabaseName=PRDMO).
db.user.name	PeopleSoft 데이터베이스에 로그인할 때 사용하는 사용자 이름입니다.
db.password	PeopleSoft 데이터베이스에 로그인할 때 사용하는 암호입니다.
db.password.encrypted	이 매개 변수의 값은 응답 파일의 암호 매개 변수를 암호화할지 결정합니다. True 또는 False로 설정할 수 있습니다. 값을 지정하지 않으면 False가 기본값입니다.
enterprise.cms.name	유니버스가 있는 CMS입니다.
enterprise.user.name	CMS에 로그인할 때 사용하는 사용자 이름입니다.
enterprise.password	CMS에 로그인할 때 사용하는 암호입니다.
enterprise.password.encrypted	이 매개 변수의 값은 응답 파일의 암호 매개 변수를 암호화할지 결정합니다. True 또는 False로 설정할 수 있습니다. 값을 지정하지 않으면 False가 기본값입니다.
enterprise.authMethod	CMS에 로그인할 때 사용하는 인증 방법입니다.
enterprise.role	관리되는 BI 플랫폼 그룹. 자세한 내용은 322 페이지에서 "관리되는 개체 정의" 를 참조하십시오.
enterprise.license	Peoplesoft에서 사용자를 가져올 때 사용하는 라이선스 종류를 결정합니다. "0"은 명명된 사용자 라이선스, "1"은 동시 사용자 라이선스입니다.

매개 변수	설명
peoplesoft.role.n	<p>관리되는 PeopleSoft 역할의 목록입니다. 자세한 내용은 322 페이지에서 "관리되는 개체 정의"를 참조하십시오.</p> <p>n은 정수이고 각 항목은 peoplesoft.role 접두사 속성에 들어갑니다.</p> <p>참고: n은 1부터 시작합니다.</p> <p>사용 가능한 모든 PeopleSoft 역할을 의미하려면 '*' 기호를 사용합니다. n이 1일 때에는 응답 파일에 peoplesoft.role 접두사가 있는 유일한 속성임을 의미합니다.</p>
mapped.universe.n	<p>보안 브리지가 업데이트할 유니버스의 목록입니다. 자세한 내용은 322 페이지에서 "관리되는 개체 정의"를 참조하십시오.</p> <p>n은 정수이고 각 항목은 mapped.universe 접두사의 속성에 들어갑니다.</p> <p>참고: n은 1부터 시작합니다.</p> <p>사용 가능한 모든 유니버스를 의미하려면 '*' 기호를 사용합니다. n이 1일 때에는 응답 파일에 mapped.universe 접두사가 있는 유일한 속성임을 의미합니다.</p>
log4j.appender.file.File	보안 브리지가 작성하는 로그 파일입니다.

매개 변수	설명
log4j.*	<p>log4j가 올바르게 작동하기 위해 필요한 기본 log4j 속성입니다.</p> <p>log4j.rootLogger=INFO, file, stdout</p> <p>log4j.appender.file=org.apache.log4j.Rolling File Appender</p> <p>log4j.appender.file.layout=org.apache.log4j.PatternLayout</p> <p>log4j.appender.file.MaxFileSize=5000KB</p> <p>log4j.appender.file.MaxBackupIndex=100</p> <p>log4j.appender.file.layout.ConversionPattern=%d [%-5] %c{1} - %m%n</p> <p>log4j.appender.stdout=org.apache.log4j.ConsoleAppender</p> <p>log4j.appender.stdout.layout=org.apache.log4j.PatternLayout</p> <p>log4j.appender.stdout.layout.ConversionPattern=%d [%-5] %c{1} - %m%n</p>
peoplesoft classpath	<p>PeopleSoft EPM API .jar 파일에 대한 클래스 경로입니다.</p> <p>이 매개 변수는 선택 사항입니다.</p>
enterprise.classpath	<p>BI 플랫폼 SDK .jar 파일에 대한 클래스 경로입니다.</p> <p>이 매개 변수는 선택 사항입니다.</p>

매개 변수	설명
db.driver.type	<p>PeopleSoft 데이터베이스 유형입니다. 이 매개 변수는 다음 중 하나의 값이 될 수 있습니다.</p> <p>Microsoft SQL Server 2000</p> <p>Oracle Database 10.1</p> <p>DB2 UDB 8.2 Fixpack 7</p> <p>사용자 지정</p> <p>사용자 지정은 인식되는 유형 또는 버전 외의 데이터베이스를 지정할 때 사용합니다.</p> <p>이 매개 변수는 선택 사항입니다.</p>
sql.db.class.location sql.db.host sql.db.port sql.db.database	<p>SQL Server JDBC 드라이버 .jar 파일의 위치, SQL Server 호스트 컴퓨터, SQL Server 포트 및 SQL Server 데이터베이스 이름입니다.</p> <p>이 매개 변수는 db.driver.type이 Microsoft SQL Server 2000인 경우에만 사용할 수 있습니다.</p> <p>이 매개 변수는 선택 사항입니다.</p>
oracle.db.class.location oracle.db.host oracle.db.port oracle.db.sid	<p>Oracle JDBC 드라이버 .jar 파일의 위치, Oracle 데이터베이스 호스트 컴퓨터, Oracle 데이터베이스 포트 및 Oracle 데이터베이스 SID입니다.</p> <p>이 매개 변수는 db.driver.type이 Oracle Database 10.1인 경우에만 사용할 수 있습니다.</p> <p>이 매개 변수는 선택 사항입니다.</p>
db2.db.class.location db2.db.host db2.db.port db2.db.sid	<p>DB2 JDBC 드라이버 .jar 파일의 위치, DB2 데이터베이스 호스트 컴퓨터, DB2 데이터베이스 포트 및 DB2 데이터베이스 SID입니다.</p> <p>이 매개 변수는 db.driver.type이 DB2 UDB 8.2 Fixpack 7인 경우에만 사용할 수 있습니다.</p> <p>이 매개 변수는 선택 사항입니다.</p>

매개 변수	설명
custom.db.class.location	사용자 지정 JDBC 드라이버의 위치, 이름 및 연결 문자열입니다.
custom.db.drivertype	이 매개 변수는 db.driver.type이 사용자 지정인 경우에만 사용할 수 있습니다.
custom.db.connectStr	이 매개 변수는 선택 사항입니다.

7.7 JD Edwards 인증

7.7.1 개요

BI 플랫폼에서 JD Edwards 데이터를 사용하려면 JD Edwards 배포에 대한 정보를 시스템에 입력해야 합니다. 이 정보에 따라 사용자가 자신의 JD Edwards EnterpriseOne 자격 증명을 사용하여 BI 플랫폼에 로그인할 수 있도록 BI 플랫폼에서 사용자를 인증할 수 있습니다.

7.7.2 JD Edwards EnterpriseOne 인증 사용

JD Edwards EnterpriseOne 정보를 BI 플랫폼에서 사용하려면 Enterprise에 JD Edwards EnterpriseOne 시스템 인증 방법에 대한 정보가 필요합니다.

7.7.2.1 BI 플랫폼에서 JD Edwards 인증 사용

1. 중앙 관리 콘솔에 관리자로 로그인합니다.
2. 관리 영역에서 인증을 클릭합니다.
3. JD Edwards EnterpriseOne을 두 번 클릭합니다.
JD Edwards EnterpriseOne 페이지가 나타납니다. 옵션, 서버, 역할 및 사용자 업데이트 네 개의 탭이 있습니다.
4. 옵션 탭에서 JD Edwards EnterpriseOne 인증 사용 확인란을 클릭합니다.
5. 새 별칭, 업데이트 옵션, 새 사용자 옵션에서 BI 플랫폼 배포 환경에 맞는 값으로 적절히 변경합니다. 시스템 탭으로 이동하기 전에 업데이트를 클릭하여 변경 내용을 저장합니다.
6. 서버 탭을 클릭합니다.
7. JD Edwards EnterpriseOne 시스템 사용자 영역에서 JD Edwards EnterpriseOne 데이터베이스에 로그인할 때 사용할 BI 플랫폼의 데이터베이스 사용자 이름과 암호를 입력합니다.
8. JD Edwards EnterpriseOne 도메인 영역에서 JD Edwards EnterpriseOne 환경에 연결하기 위해 사용할 이름, 호스트, 포트를 입력하고 이 환경의 이름을 입력한 후 추가를 클릭합니다.
9. 업데이트를 클릭하여 변경 내용을 저장합니다.

7.7.3 JD Edwards EnterpriseOne 역할을 BI 플랫폼에 매핑

BI 플랫폼에서는 사용자가 매핑하는 JD Edwards EnterpriseOne 역할마다 그룹이 자동으로 만들어 집니다. 매핑된 JD Edwards EnterpriseOne 역할의 멤버를 나타내는 별칭도 만들어 집니다.

만들어진 각 별칭에 대해 사용자 계정을 만들 수 있습니다.

하지만, 여러 시스템을 실행하고 사용자가 둘 이상의 시스템에 계정을 가진 경우에는 같은 이름을 가진 별칭에 각 사용자를 할당한 후 BI 플랫폼에서 계정을 만들 수 있습니다.

그렇게 하면 BI 플랫폼에서 같은 사용자에 대해 만들어지는 계정 수가 줄어듭니다.

예를 들어, JD Edwards EnterpriseOne 테스트 환경과 프로덕션 환경을 실행하고 사용자 중 30명이 두 시스템에 모두 액세스할 수 있는 경우에는 이들 사용자에 대해 30개의 계정만 만들어 집니다. 같은 이름을 가진 별칭에 각 사용자를 지정하지 않으면 BI 플랫폼에서 30명의 사용자에 대해 60개의 계정이 만들어 집니다.

하지만, 여러 시스템을 실행하고 사용자 이름이 겹치는 경우에는 만들어지는 각 별칭에 대해 새 멤버 계정을 만들어야 합니다.

예를 들어, Russell Aquino(사용자 이름 "raquino")의 사용자 계정으로 테스트 환경을 실행하고 Raoul Aquino(사용자 이름 "raquino")의 사용자 계정으로 프로덕션 환경을 실행하는 경우에는 각 사용자의 별칭에 대한 계정을 따로 만들어야 합니다. 그렇게 하지 않으면 같은 BI 플랫폼 계정에 두 명의 사용자가 추가되고, 이 두 사용자는 자신의 JD Edwards EnterpriseOne 자격 증명으로 BI 플랫폼에 로그인할 수 없게 됩니다.

7.7.3.1 JD Edwards EnterpriseOne 역할 매핑

1. 중앙 관리 콘솔에 관리자로 로그인합니다.
2. 관리 영역에서 인증을 클릭합니다.
3. JD Edwards EnterpriseOne을 두 번 클릭합니다.
4. 새 별칭 옵션 영역에서 다음 옵션 중 하나를 선택합니다.

- 추가된 각 별칭을 같은 이름의 계정에 할당

둘 이상의 시스템에 계정이 있는 사용자의 계정으로 여러 JD Edwards EnterpriseOne Enterprise 시스템을 운영하고 두 사용자가 다른 시스템에 대해 같은 사용자 이름을 가지고 있지 않은 경우 이 옵션을 선택합니다.

- 추가된 모든 별칭에 대한 새 계정 만들기

JD Edwards EnterpriseOne을 하나만 운영하거나, 사용자 대다수가 시스템 중 하나에만 계정이 있거나, 사용자 이름이 둘 이상의 시스템에 있는 다른 사용자의 사용자 이름과 겹치는 경우 이 옵션을 선택합니다.

5. 업데이트 옵션 영역에서 다음 옵션 중 하나를 선택합니다.

- 새 별칭을 추가하고 새 사용자 만들기

BI 플랫폼에 매핑된 모든 사용자에게 대해 새 별칭을 만들려면 이 옵션을 선택합니다. BI 플랫폼 계정이 없는 사용자에게 대해 새 계정이 추가되거나, 추가된 모든 별칭에 대한 새 계정 만들기 옵션을 선택한 경우에는 모든 사용자에게 대해 새 계정이 추가됩니다.

- 새 별칭을 추가하지 않고 새 사용자를 만들지 않음

매핑할 역할에 사용자가 많지만 이 중 일부 사용자만 BI 플랫폼을 사용할 경우 이 옵션을 선택합니다. 사용자에게 대해 별칭과 계정이 자동으로 생성되지 않습니다. 대신 BI 플랫폼에 처음으로 로그인하는 사용자에게 대해서만 별칭 및 계정(필요한 경우)이 생성됩니다. 이는 기본 옵션입니다.

6. 새 사용자 옵션 영역에서 새 사용자를 만드는 방식을 지정합니다.

SAP BusinessObjects Business Intelligence 플랫폼 라이선스가 사용자 역할을 기준으로 한 라이선스이면 다음 옵션 중 하나를 선택하십시오.

- 새 사용자를 BI Viewer로 만들기

새 사용자 계정이 BI Viewer 역할에 구성됩니다. BI Viewer 역할의 모든 계정에 대한 BI 플랫폼 응용 프로그램 액세스 권한이 사용권 계약에 정의됩니다. 사용자는 BI Viewer 역할용으로 정의된 응용 프로그램 워크플로에만 액세스할 수 있습니다. 액세스 권한은 일반적으로 비즈니스 인텔리전스 문서를 보는 것으로 제한됩니다. 이 역할은 일반적으로 BI 플랫폼 응용 프로그램을 통해 콘텐츠를 사용하는 사용자에게 적합합니다.

- 새 사용자를 BI Analyst로 만들기

새 사용자 계정이 BI Analyst 역할에 구성됩니다. BI Analyst 역할의 모든 계정에 대한 BI 플랫폼 응용 프로그램 액세스 권한이 사용권 계약에 정의됩니다. 사용자는 BI Analyst 역할에 대해 정의된 모든 응용 프로그램 워크플로에 액세스할 수 있습니다. 액세스 권한에는 비즈니스 인텔리전스 문서를 보고 수정하는 것이 포함됩니다. 이 역할은 일반적으로 BI 플랫폼 응용 프로그램의 콘텐츠를 만들고 수정하는 사용자에게 적합합니다.

SAP BusinessObjects Business Intelligence 플랫폼 라이선스가 사용자 역할을 기준으로 하지 않은 라이선스이면 다음 옵션 중 하나를 선택하십시오.

- 새 사용자를 명명된 사용자로 만들기

새 사용자 계정이 명명된 사용자 라이선스를 사용하도록 구성됩니다. 명명된 사용자 라이선스는 특정 사용자와 관련되며 이 라이선스를 사용하면 사용자 이름과 암호를 기반으로 시스템에 액세스할 수 있습니다. 이 옵션을 사용하면 명명된 사용자는 연결된 다른 사용자 수에 관계없이 시스템에 액세스할 수 있습니다. 이 옵션을 사용하여 만든 각 사용자 계정에 대한 명명된 사용자 라이선스가 있어야 합니다.

- 새 사용자를 동시 사용자로 만들기

새 사용자 계정이 동시 사용자 라이선스를 사용하도록 구성됩니다. 동시 라이선스는 BI 플랫폼에 동시에 연결할 수 있는 사용자 수를 지정합니다. 이 라이선스 유형은 소규모 동시 라이선스로 많은 사용자 기반을 지원할 수 있으므로 매우 유연합니다. 예를 들어 사용자가 해당 플랫폼에 액세스하는 빈도 및 시간에 따라 100개의 동시 사용자 라이선스로 250명, 500명 또는 700명의 사용자를 지원할 수 있습니다.

지금 선택한 역할은 BI 플랫폼에서 그룹으로 나타납니다.

7. 역할 탭을 클릭합니다.
8. 서버 선택에서 매핑할 역할이 포함된 JD Edwards 서버를 선택합니다.
9. 가져온 역할에서 BI 플랫폼에 매핑할 역할을 선택하고 <를 클릭합니다.
10. 업데이트를 클릭합니다.
BI 플랫폼에 역할이 매핑됩니다.

7.7.3.2 다시 매핑할 때의 고려 사항

BI 플랫폼에 이미 매핑되어 있는 역할에 사용자를 추가하는 경우 역할을 다시 매핑하여 BI 플랫폼에 사용자를 추가해야 합니다. 역할을 다시 매핑할 때 사용자를 명명된 사용자로 매핑할지 동시에 사용자로 매핑할지 지정하는 옵션은 역할에 추가한 새 사용자에게만 영향을 미칩니다.

예를 들어 먼저 "새 사용자를 명명된 사용자로 만들기" 옵션을 선택하여 역할을 BI 플랫폼에 매핑합니다. 그 후에 같은 역할에 사용자를 추가하고 이 역할을 "새 사용자를 동시에 사용자로 만들기" 옵션을 선택하여 다시 매핑합니다.

이 경우 해당 역할의 새 사용자만 BI 플랫폼에 동시에 사용자로 매핑되고 이전에 매핑되었던 사용자는 명명된 사용자로 유지됩니다. 이는 처음에 사용자를 동시에 사용자로 매핑하고 나중에 새 사용자를 명명된 사용자로 다시 매핑할 때도 동일합니다.

7.7.3.3 역할 매핑 해제

1. 중앙 관리 콘솔에 관리자로 로그인합니다.
2. 관리 영역에서 인증을 클릭합니다.
3. JD Edwards EnterpriseOne에 대한 탭을 클릭합니다.
4. 역할 영역에서 제거할 역할을 선택하고 < 기호를 클릭합니다.
5. 업데이트를 클릭합니다.

해당 역할의 멤버가 다른 계정이나 별칭을 갖고 있지 않다면 더 이상 BI 플랫폼에 액세스할 수 없습니다.

참고:

BI 플랫폼에 역할을 매핑하기 전에 개별 계정을 삭제하거나 역할에서 사용자를 제거하여 특정 사용자가 로그인하지 못하도록 할 수도 있습니다.

7.7.4 사용자 업데이트 예약

ERP 시스템에 대한 사용자 데이터 변경 내용이 BI 플랫폼 사용자 데이터에 반영되도록 하려면 정기적인 사용자 업데이트를 예약하면 됩니다. 업데이트를 통해 중앙 관리 콘솔(CMC)에서 구성한 매핑 설정에 따라 ERP 및 BI 플랫폼 사용자가 자동으로 동기화됩니다.

가져온 역할에 대한 업데이트를 실행하고 예약하기 위한 두 가지 옵션이 있습니다.

- 역할만 업데이트: 이 옵션을 사용하면 BI 플랫폼으로 가져온 현재 매핑된 역할 간의 링크만 업데이트됩니다. 자주 업데이트를 실행하며 시스템 리소스 사용량에 대한 우려가 있는 경우 이 옵션을 사용하는 것이 좋습니다. 역할만 업데이트하면 새 사용자 계정이 만들어지지 않습니다.
- 역할 및 별칭 업데이트: 이 옵션을 선택하면 역할 간의 링크가 업데이트될 뿐 아니라, EBS 시스템에 추가된 새 사용자 별칭에 대한 사용자 계정도 BI 플랫폼에 새로 만들어집니다.

참고:

인증을 사용했을 때 업데이트에 대한 사용자 별칭을 자동으로 만들도록 지정하지 않은 경우에는 새 별칭에 대해 계정이 만들어지지 않습니다.

7.7.4.1 사용자 업데이트 예약

역할을 BI 플랫폼에 매핑한 후에는 해당 역할이 시스템에서 업데이트되는 방식을 지정해야 합니다.

1. 사용자 업데이트 탭을 클릭합니다.
2. 역할만 업데이트 또는 역할 및 별칭 업데이트 섹션에서 예약을 클릭합니다.

팁:

업데이트를 즉시 실행하려면 지금 업데이트를 클릭합니다.

팁:

자주 업데이트를 수행하고 시스템 리소스에 대한 우려가 있는 경우 역할만 업데이트 옵션을 사용합니다. 역할과 별칭을 모두 업데이트하면 시간이 더 오래 걸립니다.

되풀이 대화 상자가 표시됩니다.

3. 개체 실행 목록에서 옵션을 선택하고 요청하는 예약 정보를 모두 입력합니다.

업데이트를 예약할 때 다음 표에 요약된 되풀이 패턴 중 하나를 선택할 수 있습니다.

되풀이 패턴	설명
매시간	업데이트가 매시간 실행됩니다. 시작할 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매일	업데이트가 매일 실행되거나 지정된 일 수 간격으로 실행됩니다. 실행할 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매주	업데이트가 매주 실행됩니다. 개체를 매주 한 번 또는 여러 번 실행할 수 있으며 실행할 시간 및 날짜를 지정하고 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월	업데이트가 매월 또는 몇 달 간격으로 실행됩니다. 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.

되풀이 패턴	설명
매월 N일	매월 특정 날짜에 업데이트가 실행됩니다. 실행 날짜와 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 첫째 월요일	업데이트가 매월 첫 번째 월요일에 실행됩니다. 업데이트 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 마지막 날	업데이트가 매월 마지막 날 실행됩니다. 업데이트 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 N번째 주 X	업데이트가 매월 지정된 주의 지정된 요일에 실행됩니다. 업데이트 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
달력	이전에 생성된 달력에 지정한 날짜에 업데이트가 실행됩니다.

4. 예약 정보 입력을 마친 후 예약을 클릭합니다.

사용자 업데이트 탭에 예약된 다음 역할 업데이트 날짜가 표시됩니다.

참고:

역할만 업데이트 또는 역할 및 별칭 업데이트 섹션에서 예약된 업데이트 취소를 클릭하면 예약된 다음 업데이트를 언제든지 취소할 수 있습니다.

7.8 Siebel 인증

7.8.1 Siebel 인증 사용

Siebel 정보를 BI 플랫폼에서 사용하려면 Siebel 시스템 인증 방법에 대한 정보가 필요합니다.

7.8.1.1 BI 플랫폼에서 Siebel 인증 사용

1. 중앙 관리 콘솔에 관리자로 로그인합니다.
2. 관리 영역에서 인증을 클릭합니다.
3. Siebel을 두 번 클릭합니다.
Siebel 페이지가 나타납니다. 옵션, 시스템, 책임 및 사용자 업데이트 네 개의 탭이 있습니다.
4. 옵션 탭에서 Siebel 인증 사용 확인란을 선택합니다.
5. 새 별칭, 업데이트 옵션, 새 사용자 옵션에서 BI 플랫폼 배포 환경에 맞는 값으로 적절히 변경합니다. 시스템 탭으로 이동하기 전에 업데이트를 클릭하여 변경 내용을 저장합니다.
6. 도메인 탭을 클릭합니다.
7. 연결할 Siebel 시스템의 도메인 이름을 도메인 이름 필드에 입력합니다.
8. 연결에서 그 도메인에 대한 연결 문자열을 입력합니다.
9. 사용자 이름 영역에서 Siebel 데이터베이스에 로그인할 때 사용할 BI 플랫폼의 데이터베이스 사용자 이름과 암호를 입력합니다.
10. 암호 영역에서 선택한 사용자의 암호를 입력합니다.
11. 추가를 클릭하여 현재 도메인 목록에 시스템 정보를 추가합니다.
12. 업데이트를 클릭하여 변경 내용을 저장합니다.

7.8.2 BI 플랫폼에 역할 매핑

BI 플랫폼에서는 사용자가 매핑하는 Siebel 역할마다 그룹이 자동으로 만들어집니다. 매핑된 Siebel 역할의 멤버를 나타내는 별칭도 생성됩니다.

만들어진 각 별칭에 대해 사용자 계정을 만들 수 있습니다.

하지만, 여러 시스템을 실행하고 사용자가 둘 이상의 시스템에 계정을 가진 경우에는 같은 이름을 가진 별칭에 각 사용자를 할당한 후 BI 플랫폼에서 계정을 만들 수 있습니다.

그렇게 하면 프로그램에서 같은 사용자에 대해 만들어지는 계정 수가 줄어듭니다.

예를 들어, Siebel eBusiness 테스트 환경과 프로덕션 환경을 실행하고 사용자 중 30명이 두 시스템에 모두 액세스할 수 있는 경우에는 이들 사용자에 대해 30개의 계정만 만들어집니다. 같은 이름을 가진 별칭에 각 사용자를 지정하지 않으면 BI 플랫폼에서 30명의 사용자에 대해 60개의 계정이 만들어집니다.

하지만, 여러 시스템을 실행하고 사용자 이름이 겹치는 경우에는 만들어지는 각 별칭에 대해 새 멤버 계정을 만들어야 합니다.

예를 들어, Russell Aquino(사용자 이름 "raquino")의 사용자 계정으로 테스트 환경을 실행하고 Raoul Aquino(사용자 이름 "raquino")의 사용자 계정으로 프로덕션 환경을 실행하는 경우에는 각 사용자의 별칭에 대한 계정을 따로 만들어야 합니다. 그렇게 하지 않으면 같은 계정에 두 명의 사용자가 추가되고, 이 두 사용자는 자신의 Siebel eBusiness 자격 증명으로 BI 플랫폼에 로그인할 수 없게 됩니다.

7.8.2.1 BI 플랫폼에 Siebel eBusiness 역할 매핑

1. 중앙 관리 콘솔에 관리자로 로그인합니다.
2. 인증을 클릭합니다.
3. Siebel eBusiness를 두 번 클릭합니다.
4. 새 별칭 옵션 영역에서 다음 옵션 중 하나를 선택합니다.
 - 추가된 각 별칭을 같은 이름의 계정에 할당
 둘 이상의 시스템에 계정이 있는 사용자의 계정으로 여러 Siebel eBusiness 시스템을 운영하고 두 사용자가 다른 시스템에 대해 같은 사용자 이름을 가지고 있지 않은 경우 이 옵션을 선택합니다.
 - 추가된 모든 별칭에 대한 새 계정 만들기
 Siebel eBusiness를 하나만 운영하거나, 사용자 대다수가 시스템 중 하나에만 계정이 있거나, 사용자 이름이 둘 이상의 시스템에 있는 다른 사용자의 사용자 이름과 겹치는 경우 이 옵션을 선택합니다.
5. 업데이트 옵션 영역에서 다음 옵션 중 하나를 선택합니다.
 - 새 별칭을 추가하고 새 사용자 만들기
 BI 플랫폼에 매핑된 모든 사용자에게 대해 새 별칭을 만들려면 이 옵션을 선택합니다. BI 플랫폼 계정이 없는 사용자에게 대해 새 계정이 추가되거나, 추가된 모든 별칭에 대한 새 계정 만들기 옵션을 선택한 경우에는 모든 사용자에게 대해 새 계정이 추가됩니다.
 - 새 별칭을 추가하지 않고 새 사용자를 만들지 않음
 매핑할 역할에 사용자가 많지만 이 중 일부 사용자만 BI 플랫폼을 사용할 경우 이 옵션을 선택합니다. 이 프로그램에서는 사용자에게 대해 별칭과 계정을 자동으로 만들지 않습니다. 대신 BI 플랫폼에 처음으로 로그인하는 사용자에게 대해서만 별칭 및 계정(필요한 경우)을 만듭니다. 이는 기본 옵션입니다.
6. 새 사용자 옵션 영역에서 새 사용자를 만드는 방식을 지정합니다.
 BI 플랫폼 라이선스가 사용자 역할을 기반으로 하는 경우 다음 옵션 중 하나를 선택합니다.
 - 새 사용자를 BI Viewer로 만들기
 새 사용자 계정이 BI Viewer 역할에 구성됩니다. BI Viewer 역할의 모든 계정에 대한 BI 플랫폼 응용 프로그램 액세스 권한이 사용권 계약에 정의됩니다. 사용자는 BI Viewer 역할용으로 정의된 응용 프로그램 워크플로에만 액세스할 수 있습니다. 액세스 권한은 일반적으로 비즈니스 인텔리전스 문서를 보는 것으로 제한됩니다. 이 역할은 일반적으로 BI 플랫폼 응용 프로그램을 통해 콘텐츠를 사용하는 사용자에게 적합합니다.
 - 새 사용자를 BI Analyst로 만들기

새 사용자 계정이 BI Analyst 역할에 구성됩니다. BI Analyst 역할의 모든 계정에 대한 BI 플랫폼 응용 프로그램 액세스 권한이 사용권 계약에 정의됩니다. 사용자는 BI Analyst 역할에 대해 정의된 모든 응용 프로그램 워크플로에 액세스할 수 있습니다. 액세스 권한에는 비즈니스 인텔리전스 문서를 보고 수정하는 것이 포함됩니다. 이 역할은 일반적으로 BI 플랫폼 응용 프로그램의 콘텐츠를 만들고 수정하는 사용자에게 적합합니다.

BI 플랫폼 라이선스가 사용자 역할을 기반으로 하지 않는 경우 다음 옵션 중 하나를 선택합니다.

- 새 사용자를 명명된 사용자로 만들기

새 사용자 계정이 명명된 사용자 라이선스를 사용하도록 구성됩니다. 명명된 사용자 라이선스는 특정 사용자와 관련되며 이 라이선스를 사용하면 사용자 이름과 암호를 기반으로 시스템에 액세스할 수 있습니다. 이 옵션을 사용하면 명명된 사용자는 연결된 다른 사용자 수에 관계없이 시스템에 액세스할 수 있습니다. 이 옵션을 사용하여 만든 각 사용자 계정에 대한 명명된 사용자 라이선스가 있어야 합니다.

- 새 사용자를 동시 사용자로 만들기

새 사용자 계정이 동시 사용자 라이선스를 사용하도록 구성됩니다. 동시 라이선스는 BI 플랫폼에 동시에 연결할 수 있는 사용자 수를 지정합니다. 이 유형의 라이선스는 소규모 동시 라이선스로 많은 사용자를 지원할 수 있으므로 매우 유연합니다. 예를 들어 사용자가 BI 플랫폼에 액세스하는 빈도 및 시간에 따라 100개의 동시 사용자 라이선스로 250명, 500명 또는 700명의 사용자를 지원할 수 있습니다.

7. 역할 탭을 클릭합니다.

8. 역할을 매핑할 Siebel 서버에 해당하는 도메인을 선택합니다.

9. 사용 가능한 역할에서 매핑할 역할을 선택하고 >를 클릭합니다.

참고:

역할 개수가 많은 경우에는 다음으로 시작하는 역할 검색: 필드를 사용하여 검색 범위를 좁힐 수 있습니다. 역할의 시작 문자를 입력한 후 와일드카드(%) 문자를 입력하고 검색을 클릭합니다.

10. 업데이트를 클릭합니다.

BI 플랫폼에 역할이 매핑됩니다.

7.8.2.2 다시 매핑할 때의 고려 사항

BI 플랫폼과 Siebel 간에 강제로 그룹과 사용자를 동기화하려면 사용자 동기화 강제 수행을 설정하십시오.

참고:

사용자 동기화 강제 수행을 선택하려면 먼저 새 별칭을 추가하고 새 사용자 만들기를 선택해야 합니다.

역할을 다시 매핑할 때 사용자를 명명된 사용자로 매핑할지 동시 사용자로 매핑할지 지정하는 옵션은 역할에 추가한 새 사용자에게만 영향을 미칩니다.

예를 들어 먼저 "새 사용자를 명명된 사용자로 만들기" 옵션을 선택하여 역할을 BI 플랫폼에 매핑합니다. 그 후에 같은 역할에 사용자를 추가하고 이 역할을 "새 사용자를 동시 사용자로 만들기" 옵션을 선택하여 다시 매핑합니다.

이 경우 해당 역할의 새 사용자만 BI 플랫폼에 동시 사용자로 매핑되고 이전에 매핑되었던 사용자는 명명된 사용자로 유지됩니다. 이는 처음에 사용자를 동시 사용자로 매핑하고 나중에 새 사용자를 명명된 사용자로 다시 매핑할 때도 동일합니다.

7.8.2.3 역할 매핑 해제

1. 중앙 관리 콘솔에 관리자로 로그인합니다.
2. 관리 영역에서 인증을 클릭합니다.
3. Siebel를 두 번 클릭합니다.
4. 도메인 탭에서 매핑을 해제할 역할에 해당하는 Siebel 도메인을 선택합니다.
5. 역할 탭에서 제거할 역할을 선택하고 < 기호를 클릭합니다.
6. 업데이트를 클릭합니다.

해당 책임의 멤버가 다른 계정이나 별칭을 갖고 있지 않다면 더 이상 BI 플랫폼에 액세스할 수 없습니다.

참고:

BI 플랫폼에 역할을 매핑하기 전에 개별 계정을 삭제하거나 역할에서 사용자를 제거하여 특정 사용자가 로그인하지 못하도록 할 수도 있습니다.

7.8.3 사용자 업데이트 예약

ERP 시스템에 대한 사용자 데이터 변경 내용이 BI 플랫폼 사용자 데이터에 반영되도록 하려면 정기적인 사용자 업데이트를 예약하면 됩니다. 업데이트를 통해 중앙 관리 콘솔(CMC)에서 구성한 매핑 설정에 따라 ERP 및 BI 플랫폼 사용자가 자동으로 동기화됩니다.

가져온 역할에 대한 업데이트를 실행하고 예약하기 위한 두 가지 옵션이 있습니다.

- 역할만 업데이트: 이 옵션을 사용하면 BI 플랫폼으로 가져온 현재 매핑된 역할 간의 링크만 업데이트됩니다. 자주 업데이트를 실행하며 시스템 리소스 사용량에 대한 우려가 있는 경우 이 옵션을 사용하는 것이 좋습니다. 역할만 업데이트하면 새 사용자 계정이 만들어지지 않습니다.
- 역할 및 별칭 업데이트: 이 옵션을 선택하면 역할 간의 링크가 업데이트될 뿐 아니라, EBS 시스템에 추가된 새 사용자 별칭에 대한 사용자 계정도 BI 플랫폼에 새로 만들어집니다.

참고:

인증을 사용했을 때 업데이트에 대한 사용자 별칭을 자동으로 만들도록 지정하지 않은 경우에는 새 별칭에 대해 계정이 만들어지지 않습니다.

7.8.3.1 사용자 업데이트 예약

역할을 BI 플랫폼에 매핑한 후에는 해당 역할이 시스템에서 업데이트되는 방식을 지정해야 합니다.

1. 사용자 업데이트 탭을 클릭합니다.
2. 역할만 업데이트 또는 역할 및 별칭 업데이트 섹션에서 예약을 클릭합니다.

팁:

업데이트를 즉시 실행하려면 지금 업데이트를 클릭합니다.

팁:

자주 업데이트를 수행하고 시스템 리소스에 대한 우려가 있는 경우 역할만 업데이트 옵션을 사용합니다. 역할과 별칭을 모두 업데이트하면 시간이 더 오래 걸립니다.

되풀이 대화 상자가 표시됩니다.

3. 개체 실행 목록에서 옵션을 선택하고 요청하는 예약 정보를 모두 입력합니다.

업데이트를 예약할 때 다음 표에 요약된 되풀이 패턴 중 하나를 선택할 수 있습니다.

되풀이 패턴	설명
매시간	업데이트가 매시간 실행됩니다. 시작할 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매일	업데이트가 매일 실행되거나 지정된 일 수 간격으로 실행됩니다. 실행할 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매주	업데이트가 매주 실행됩니다. 개체를 매주 한 번 또는 여러 번 실행할 수 있으며 실행할 시간 및 날짜를 지정하고 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월	업데이트가 매월 또는 몇 달 간격으로 실행됩니다. 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.

되풀이 패턴	설명
매월 N일	매월 특정 날짜에 업데이트가 실행됩니다. 실행 날짜와 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 첫째 월요일	업데이트가 매월 첫 번째 월요일에 실행됩니다. 업데이트 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 마지막 날	업데이트가 매월 마지막 날 실행됩니다. 업데이트 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 N번째 주 X	업데이트가 매월 지정된 주의 지정된 요일에 실행됩니다. 업데이트 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
달력	이전에 생성된 달력에 지정한 날짜에 업데이트가 실행됩니다.

4. 예약 정보 입력을 마친 후 예약을 클릭합니다.

사용자 업데이트 탭에 예약된 다음 역할 업데이트 날짜가 표시됩니다.

참고:

역할만 업데이트 또는 역할 및 별칭 업데이트 섹션에서 예약된 업데이트 취소를 클릭하면 예약된 다음 업데이트를 언제든지 취소할 수 있습니다.

7.9 Oracle EBS 인증

7.9.1 Oracle EBS 인증 사용

Oracle EBS 정보를 BI 플랫폼에서 사용하려면 시스템에 Oracle EBS 시스템 인증 방법에 대한 정보가 필요합니다.

7.9.1.1 Oracle E-Business Suite 인증 사용

1. 중앙 관리 콘솔에 관리자로 로그인합니다.
 2. 관리 영역에서 인증을 클릭합니다.
 3. Oracle EBS를 클릭합니다.
Oracle EBS 페이지가 나타납니다. 옵션, 시스템, 책임 및 사용자 업데이트 네 개의 탭이 있습니다.
 4. 옵션 탭에서 Oracle EBS 인증 사용 확인란을 선택합니다.
 5. 새 별칭, 업데이트 옵션, 새 사용자 옵션에서 BI 플랫폼 배포 환경에 맞는 값으로 적절히 변경합니다. 시스템 탭으로 이동하기 전에 업데이트를 클릭하여 변경 내용을 저장합니다.
 6. 시스템 탭을 클릭합니다.
 7. Oracle EBS 시스템 사용자 영역에서 Oracle E-Business Suite 데이터베이스에 로그인할 때 사용할 BI 플랫폼의 데이터베이스 사용자 이름과 암호를 입력합니다.
 8. Oracle EBS 서비스 영역에서 Oracle EBS 환경에서 사용되는 서비스 이름을 입력하고 추가를 클릭합니다.
 9. 업데이트를 클릭하여 변경 내용을 저장합니다.
- 이제 Oracle EBS 역할을 시스템으로 매핑해야 합니다.

관련 항목

- 347 페이지에서 [Oracle E-Business Suite 역할 매핑](#)

7.9.2 Oracle E-Business Suite 역할을 BI 플랫폼에 매핑

BI 플랫폼에서는 사용자가 매핑하는 Oracle E-Business Suite(EBS) 역할마다 그룹이 자동으로 만들어집니다. 매핑된 Oracle E-Business Suite 역할의 멤버를 나타내는 별칭도 생성됩니다.

만들어진 각 별칭에 대해 사용자 계정을 만들 수 있습니다. 하지만, 여러 시스템을 실행하고 사용자가 둘 이상의 시스템에 계정을 가진 경우에는 같은 이름을 가진 별칭에 각 사용자를 할당한 후 BI 플랫폼에서 계정을 만들 수 있습니다.

그렇게 하면 시스템에서 같은 사용자에 대해 만들어지는 계정 수가 줄어듭니다.

예를 들어, EBS 테스트 환경과 프로덕션 환경을 실행하고 사용자 중 30명이 두 시스템에 모두 액세스할 수 있는 경우에는 이들 사용자에 대해 30개의 계정만 만들어집니다. 같은 이름을 가진 별칭에 각 사용자를 지정하지 않으면 BI 플랫폼에서 30명의 사용자에 대해 60개의 계정이 만들어집니다.

하지만, 여러 시스템을 실행하고 사용자 이름이 겹치는 경우에는 만들어지는 각 별칭에 대해 새 멤버 계정을 만들어야 합니다.

예를 들어, Russell Aquino(사용자 이름 "raquino")의 사용자 계정으로 테스트 환경을 실행하고 Raoul Aquino(사용자 이름 "raquino")의 사용자 계정으로 프로덕션 환경을 실행하는 경우에는 각 사용자의 별칭에 대한 계정을 따로 만들어야 합니다. 그렇지 않으면, 같은 BI 플랫폼 계정에 두 명의 사용자가

추가되고, 이 두 사용자는 자신의 Oracle EBS 자격 증명으로 시스템에 로그인하고 양쪽 EBS 환경의 데이터에 모두 액세스할 수 있게 됩니다.

7.9.2.1 Oracle E-Business Suite 역할 매핑

1. 중앙 관리 콘솔에 관리자로 로그인합니다.
2. 관리 영역에서 인증을 클릭합니다.
3. Oracle EBS를 클릭합니다.

Oracle EBS 페이지에 옵션 탭이 표시됩니다.

4. 새 별칭 옵션 영역에서 다음 옵션 중 하나를 선택합니다.

- 추가된 각 Oracle EBS 별칭을 같은 이름의 계정에 할당

둘 이상의 시스템에 계정이 있는 사용자의 계정으로 여러 Oracle E-Business Suite 시스템을 운영하고 두 사용자가 다른 시스템에 대해 같은 사용자 이름을 가지고 있지 않은 경우 이 옵션을 선택합니다.

- 추가된 모든 Oracle EBS 별칭에 대한 새 계정 만들기

Oracle E-Business Suite를 하나만 운영하거나, 사용자 대다수가 시스템 중 하나에만 계정이 있거나, 사용자 이름이 둘 이상의 시스템에 있는 다른 사용자의 사용자 이름과 겹치는 경우 이 옵션을 선택합니다.

5. 업데이트 옵션 영역에서 다음 옵션 중 하나를 선택합니다.

- 새 별칭을 추가하고 새 사용자 만들기

BI 플랫폼에 매핑된 모든 사용자에게 대해 새 별칭을 만들려면 이 옵션을 선택합니다. BI 플랫폼 계정이 없는 사용자에게 대해 새 계정이 추가되거나, 추가된 모든 Oracle EBS 별칭에 대한 새 계정 만들기 옵션을 선택한 경우에는 모든 사용자에게 대해 새 계정이 추가됩니다.

- 새 별칭을 추가하지 않고 새 사용자를 만들지 않음

매핑할 역할에 사용자가 많지만 이 중 일부 사용자만 BI 플랫폼을 사용할 경우 이 옵션을 선택합니다. 플랫폼에서는 사용자에게 대해 별칭과 계정을 자동으로 만들지 않습니다. 대신 BI 플랫폼에 처음으로 로그인하는 사용자에게 대해서만 별칭 및 계정(필요한 경우)이 생성됩니다. 이는 기본 옵션입니다.

6. 새 사용자 옵션에서 새 사용자를 만드는 방식을 지정한 다음 업데이트를 클릭합니다.

SAP BusinessObjects Business Intelligence 플랫폼 라이선스가 사용자 역할을 기준으로 한 라이선스이면 다음 옵션 중 하나를 선택하십시오.

- 새 사용자를 BI Viewer로 만들기

새 사용자 계정이 BI Viewer 역할에 구성됩니다. BI Viewer 역할의 모든 계정에 대한 BI 플랫폼 응용 프로그램 액세스 권한이 사용권 계약에 정의됩니다. 사용자는 BI Viewer 역할용으로 정의된 응용 프로그램 워크플로에만 액세스할 수 있습니다. 액세스 권한은 일반적으로 비즈니스

스 인텔리전스 문서를 보는 것으로 제한됩니다. 이 역할은 일반적으로 BI 플랫폼 응용 프로그램을 통해 콘텐츠를 사용하는 사용자에게 적합합니다.

- 새 사용자를 BI Analyst로 만들기

새 사용자 계정이 BI Analyst 역할에 구성됩니다. BI Analyst 역할의 모든 계정에 대한 BI 플랫폼 응용 프로그램 액세스 권한이 사용권 계약에 정의됩니다. 사용자는 BI Analyst 역할에 대해 정의된 모든 응용 프로그램 워크플로에 액세스할 수 있습니다. 액세스 권한에는 비즈니스 인텔리전스 문서를 보고 수정하는 것이 포함됩니다. 이 역할은 일반적으로 BI 플랫폼 응용 프로그램의 콘텐츠를 만들고 수정하는 사용자에게 적합합니다.

SAP BusinessObjects Business Intelligence 플랫폼 라이선스가 사용자 역할을 기준으로 하지 않은 라이선스이면 다음 옵션 중 하나를 선택하십시오.

- 새 사용자를 명명된 사용자로 만들기

새 사용자 계정이 명명된 사용자 라이선스를 사용하도록 구성됩니다. 명명된 사용자 라이선스는 특정 사용자와 관련되며 이 라이선스를 사용하면 사용자 이름과 암호를 기반으로 시스템에 액세스할 수 있습니다. 이 옵션을 사용하면 명명된 사용자는 연결된 다른 사용자 수에 관계없이 시스템에 액세스할 수 있습니다. 이 옵션을 사용하여 만든 각 사용자 계정에 대한 명명된 사용자 라이선스가 있어야 합니다.

- 새 사용자를 동시 사용자로 만들기

새 사용자 계정이 동시 사용자 라이선스를 사용하도록 구성됩니다. 동시 라이선스는 BI 플랫폼에 동시에 연결할 수 있는 사용자 수를 지정합니다. 이 라이선스 유형은 소규모 동시 라이선스로 많은 사용자 기반을 지원할 수 있으므로 매우 유연합니다. 예를 들어 사용자가 해당 플랫폼에 액세스하는 빈도 및 시간에 따라 100개의 동시 사용자 라이선스로 250명, 500명 또는 700명의 사용자를 지원할 수 있습니다.

지금 선택한 역할은 BI 플랫폼에서 그룹으로 나타납니다.

7. 책임 탭을 클릭합니다.
8. 책임 탭에서 업데이트를 클릭한 후 Oracle EBS 사용자 계정 정보를 동기화하려면 사용자 동기화 강제 수행을 선택합니다.
9. 현재 Oracle EBS 서비스에서 매핑할 역할이 포함된 Oracle EBS 서비스를 선택합니다.
10. 매핑된 Oracle EBS 역할에서 Oracle EBS 사용자에게 대한 필터를 지정할 수 있습니다.
 - a. 사용자가 응용 프로그램 목록에서 새 역할에 대해 어떤 응용 프로그램을 사용할 수 있는지 선택합니다.
 - b. 사용자가 책임 목록에서 어떤 Oracle 응용 프로그램, 기능, 보고서 및 동시 프로그램을 실행할 수 있는지 선택합니다.
 - c. 보안 그룹의 보안 그룹에서 새 역할이 어떤 보안 그룹에 지정될지 선택합니다.
 - d. 현재 역할에서 추가 및 삭제 단추를 사용하여 역할에 대한 보안 그룹 지정을 수정합니다.
11. 업데이트를 클릭합니다.
BI 플랫폼에 역할이 매핑됩니다.

역할을 BI 플랫폼에 매핑한 후에는 해당 역할이 시스템에서 업데이트되는 방식을 지정해야 합니다.

관련 항목

- 90 페이지에서 [역할 기반 라이선스](#) "

7.9.2.1.1 Oracle EBS 역할 및 사용자 업데이트

Oracle EBS 인증을 설정한 후에는 BI 플랫폼으로 가져온 매핑된 역할에 대한 정기 업데이트를 예약하고 실행해야 합니다. 그러면 업데이트된 Oracle EBS 역할 정보가 BI 플랫폼에 정확하게 반영됩니다.

Oracle EBS 역할에 대한 업데이트를 실행하고 예약하기 위한 두 가지 옵션이 있습니다.

- **역할만 업데이트:** 이 옵션을 사용하면 BI 플랫폼으로 가져온 현재 매핑된 역할 간의 링크만 업데이트됩니다. 자주 업데이트를 실행할 것으로 예상하고 시스템 리소스 사용에 대한 우려가 있는 경우 이 옵션을 사용하는 것이 좋습니다. Oracle EBS 역할만 업데이트하면 새 사용자 계정이 만들어지지 않습니다.
- **역할 및 별칭 업데이트:** 이 옵션을 선택하면 역할 간의 링크가 업데이트될 뿐 아니라, Oracle EBS 시스템의 역할에 추가된 사용자 별칭에 대한 사용자 계정도 BI 플랫폼에 새로 만들어집니다.

참고:

Oracle EBS 인증을 사용했을 때 업데이트에 대한 사용자 별칭을 자동으로 만들도록 지정하지 않은 경우에는 새 별칭에 대해 계정이 만들어지지 않습니다.

7.9.2.1.2 Oracle EBS 역할에 대한 업데이트 예약

역할을 BI 플랫폼에 매핑한 후에는 해당 역할이 시스템에서 업데이트되는 방식을 지정해야 합니다.

1. 사용자 업데이트 탭을 클릭합니다.
2. 역할만 업데이트 또는 역할 및 별칭 업데이트 섹션에서 예약을 클릭합니다.

팁:

업데이트를 즉시 실행하려면 지금 업데이트를 클릭합니다.

팁:

자주 업데이트를 수행하고 시스템 리소스에 대한 우려가 있는 경우 역할만 업데이트 옵션을 사용합니다. 역할과 별칭을 모두 업데이트하면 시간이 더 오래 걸립니다.

되풀이 대화 상자가 표시됩니다.

3. 개체 실행 풀다운 목록에서 옵션을 선택하고 표시된 필드에서 요청하는 예약 정보를 전부 입력합니다.

업데이트를 예약할 때 다음 표에 요약된 되풀이 패턴 중 하나를 선택할 수 있습니다.

되풀이 패턴	설명
매시간	업데이트가 매시간 실행됩니다. 시작할 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매일	업데이트가 매일 실행되거나 지정된 일 수 간격으로 실행됩니다. 실행할 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매주	업데이트가 매주 실행됩니다. 한 주에 한 번 또는 여러 번 실행되도록 지정할 수 있습니다. 실행할 시간 및 날짜를 지정하고 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월	업데이트가 매월 또는 몇 달 간격으로 실행됩니다. 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 N일	매월 특정 날짜에 업데이트가 실행됩니다. 실행 날짜와 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 첫째 월요일	업데이트가 매월 첫 번째 월요일에 실행됩니다. 업데이트 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 마지막 날	업데이트가 매월 마지막 날 실행됩니다. 업데이트 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
매월 N번째 주 X	업데이트가 매월 지정된 주의 지정된 요일에 실행됩니다. 업데이트 실행 시간 및 시작 날짜와 종료 날짜를 지정할 수 있습니다.
달력	이전에 생성된 달력에 지정된 날짜에 업데이트가 실행됩니다.

4. 예약 정보 입력을 마친 후 예약을 클릭합니다.

사용자 업데이트 탭에 예약된 다음 역할 업데이트 날짜가 표시됩니다.

참고:

역할만 업데이트 또는 역할 및 별칭 업데이트 섹션에서 예약된 업데이트 취소를 클릭하면 예약된 다음 업데이트를 언제든지 취소할 수 있습니다.

7.9.3 역할 매핑 해제

특정 사용자 그룹이 BI 플랫폼에 로그인하지 못하도록 이 그룹이 속해 있는 역할의 매핑을 해제할 수 있습니다.

7.9.3.1 역할 매핑 해제

1. 중앙 관리 콘솔에 관리자로 로그인합니다.
2. 관리 영역에서 인증을 클릭합니다.
3. 역할 매핑을 해제할 ERP 시스템의 이름을 두 번 클릭합니다.
ERP 시스템 페이지에 옵션 탭이 표시됩니다.
4. 책임 또는 역할 탭을 클릭합니다.
5. 가져온 역할 영역에서 대상 역할을 선택하고 < 또는 삭제를 클릭하여 제거합니다.
6. 업데이트를 클릭합니다.

해당 역할의 멤버가 다른 계정이나 별칭을 갖고 있지 않다면 더 이상 BI 플랫폼에 액세스할 수 없습니다.

참고:

BI 플랫폼에 역할을 매핑하기 전에 개별 계정을 삭제하거나 역할에서 사용자를 제거하여 특정 사용자가 로그인하지 못하도록 할 수도 있습니다.

7.9.4 매핑된 Oracle EBS 그룹 및 사용자의 권한 사용자 지정

BI 플랫폼에 역할을 매핑할 때, 만든 그룹과 사용자에 대해 권한을 설정할 수도 있고 권한을 부여할 수도 있습니다.

7.9.4.1 관리 권한 할당

사용자가 BI 플랫폼을 유지 관리할 수 있도록 하려면 이 사용자를 기본 관리자 그룹의 멤버로 지정해야 합니다. 이 그룹의 멤버는 계정, 서버, 폴더, 개체, 설정 등 시스템의 전반적인 사항을 제어할 수 있습니다.

1. 중앙 관리 콘솔에 관리자로 로그인합니다.
2. 구성 영역에서 사용자를 클릭합니다.
3. 이름 열에서 관리자를 클릭합니다.
4. 그룹 목록을 클릭한 다음 작업 목록에서 추가를 클릭합니다.

사용 가능한 사용자/그룹 페이지가 나타납니다.

5. 사용자 목록 또는 그룹 목록 영역에서 관리 권한을 할당할 매핑된 역할을 선택합니다.
6. > 기호를 클릭하여 해당 역할을 관리자 그룹의 하위 그룹으로 만들고 확인을 클릭합니다.

해당 역할의 멤버가 BI 플랫폼에서 관리 권한을 갖게 되었습니다.

참고:

Oracle EBS에서 역할을 만들고, 적절한 사용자를 이 역할에 추가하여 이 역할을 BI 플랫폼에 매핑한 후 매핑한 역할을 기본 관리자 그룹의 하위 그룹으로 설정하여 멤버에게 역할 관리 권한을 승인할 수도 있습니다.

7.9.4.2 게시 권한 할당

시스템에 조직 내의 콘텐츠 작성자로 지정된 사용자가 있는 경우 이 사용자들에게 BI 플랫폼에 개체를 게시할 수 있는 권한을 부여할 수 있습니다.

1. 중앙 관리 콘솔에 관리자로 로그인합니다.
2. 구성 영역에서 폴더를 클릭합니다.
3. 사용자가 개체를 추가할 수 있도록 허용할 폴더로 이동합니다.
4. 관리를 클릭하고 최상위 보안을 클릭한 다음 모든 폴더를 클릭합니다.
5. 보안 주체 추가를 클릭합니다.

보안 주체 추가 페이지가 나타납니다.

6. 사용 가능한 사용자/그룹 목록에서 게시 권한을 지정할 멤버가 있는 그룹을 선택합니다.
7. > 기호를 클릭하여 이 그룹이 해당 폴더에 액세스할 수 있도록 한 후 보안 추가 및 할당을 클릭합니다.

보안 할당 페이지가 나타납니다.

8. 사용 가능한 액세스 수준에서 원하는 액세스 수준을 선택하고 > 기호를 클릭하여 액세스 수준을 명시적으로 할당합니다.
9. 부모 폴더에서 상속과 부모 그룹에서 상속 옵션이 선택되어 있으면 선택을 취소하고 적용을 클릭합니다.

10. 확인을 클릭합니다.

해당 역할의 멤버에게 지정한 폴더와 그 하위 폴더에 개체를 추가할 수 있는 권한이 부여되었습니다. 할당한 권한을 제거하려면 액세스 제거를 클릭하십시오.

7.9.5 SAP Crystal Reports 및 Oracle EBS에 대한 단일 로그인(SSO) 구성

기본적으로 BI 플랫폼은 SAP Crystal Reports 사용자가 단일 로그인(SSO)을 사용하여 Oracle EBS 데이터에 액세스할 수 있도록 구성됩니다.

7.9.5.1 Oracle EBS 및 SAP Crystal Reports에 대해 SSO 비활성화

1. 중앙 관리 콘솔(CMC)에서 응용 프로그램을 클릭합니다.
2. Crystal Reports 구성을 두 번 클릭합니다.
3. 단일 로그인 옵션을 클릭합니다.
4. crdb_oraapps를 선택합니다.
5. 제거를 클릭합니다.
6. 저장 후 닫기를 클릭합니다.
7. SAP Crystal Reports를 다시 시작합니다.

7.9.5.2 Oracle EBS 및 SAP Crystal Reports에 대해 SSO 재활성화

Oracle EBS 및 SAP Crystal Reports에 대해 SSO를 다시 활성화하려면 다음 단계를 수행하십시오.

1. 중앙 관리 콘솔(CMC)에서 응용 프로그램을 클릭합니다.
2. Crystal Reports 구성을 두 번 클릭합니다.
3. 단일 로그인 옵션을 클릭합니다.
4. 데이터베이스 로그인에 SSO 컨텍스트 사용 항목에 crdb_oraapps를 입력합니다.
5. 추가를 클릭합니다.

6. 저장 후 닫기를 클릭합니다.
7. SAP Crystal Reports를 다시 시작합니다.

장8 서버 관리

8.1 서버 관리

8.1.1 CMC의 서버 관리 영역 작업

CMC의 서버 관리 영역은 서버 관리 작업을 위한 주요 도구입니다. 여기에는 해당 배포에 있는 모든 서버 목록이 나열됩니다. 대부분의 관리 및 구성 작업은 목록에서 서버를 선택하고 관리 또는 작업 메뉴에서 명령을 선택하는 방식으로 수행할 수 있습니다.

탐색 트리 정보

서버 관리 영역의 왼쪽에 있는 탐색 트리에서는 서버 목록을 여러 가지 방식으로 표시할 수 있습니다. 탐색 트리에서 항목을 선택하면 세부 정보 창에 표시되는 정보가 변경됩니다.

탐색 트리 옵션	설명
서버 목록	배포의 모든 서버에 대한 전체 목록을 표시합니다.
서버 그룹 목록	사용할 수 있는 모든 서버 그룹의 단순 목록을 세부 정보 창에 표시합니다. 서버 그룹 설정이나 보안을 구성하려면 이 옵션을 선택합니다.
서버 그룹	서버 그룹과 각 서버 그룹 내의 서버 목록을 표시합니다. 서버 그룹을 선택하면 해당 서버 및 서버 그룹이 세부 정보 창에 계층 구조 보기로 표시됩니다.

탐색 트리 옵션	설명
노드	<p>배포의 노드 목록을 표시합니다. 노드는 CCM에서 구성합니다. 이것을 클릭하여 노드를 선택하면 해당 노드 상의 서버를 보거나 관리할 수 있습니다.</p>
서비스 범주	<p>배포에 있을 수 있는 서비스 유형의 목록을 제공합니다. 서비스 범주는 핵심 BI 플랫폼 서비스와 특정 SAP Business Objects 구성 요소에 관련된 서비스로 나뉩니다. 서비스 범주에는 다음과 같은 것이 있습니다.</p> <ul style="list-style-type: none"> • 연결 서비스 • 핵심 서비스 • Crystal Reports 서비스 • 데이터 연합 서비스 • 주기 관리 서비스 • Analysis 서비스 • Web Intelligence 서비스 • Dashboard Design 서비스 <p>탐색 목록에서 서비스 범주를 선택하여 해당 범주의 서버를 보거나 관리할 수 있습니다.</p> <p>참고: 서버는 여러 서비스 범주에 속하는 서비스를 호스트할 수 있습니다. 따라서 한 서버가 여러 서비스 범주에 표시될 수 있습니다.</p>

탐색 트리 옵션	설명
서버 상태	<p>현재 상태에 따라 서버를 표시합니다. 이는 어떤 서버가 실행 또는 중지 상태인지 확인하는 데 중요하게 사용되는 도구입니다. 예를 들어, 시스템의 성능이 저하된 경우 서버 상태 목록을 사용하여 비정상적인 상태의 서버가 있는지 여부를 신속하게 확인할 수 있습니다. 서버는 다음과 같은 상태가 될 수 있습니다.</p> <ul style="list-style-type: none"> • 중지됨 • 시작하는 중 • 초기화 중 • 실행 중 • 중지하는 중 • 시작되었지만 오류가 발생함 • 실패 • 리소스 대기 중

세부 정보 창 정보

탐색 트리에서 선택한 옵션에 따라 서버 관리 영역 오른쪽에 있는 세부 정보 창에 서버, 서버 그룹, 상태, 범주 또는 노드의 목록이 표시됩니다. 다음 표에는 서버와 관련하여 세부 정보 창에 나열되는 정보에 대한 설명이 나와 있습니다.

참고:

노드, 서버 그룹, 범주 및 상태와 관련하여 세부 정보 창에는 일반적으로 이름과 설명이 표시됩니다.

세부 정보 창 열	설명
서버 이름 또는 이름	서버의 이름을 표시합니다.
상태	<p>서버의 현재 상태를 표시합니다. 탐색 트리에서 서버 상태 목록을 사용하여 서버 상태별로 목록을 정렬할 수 있습니다. 서버는 다음과 같은 상태가 될 수 있습니다.</p> <ul style="list-style-type: none"> • 중지됨 • 시작하는 중 • 초기화 중 • 실행 중 • 중지하는 중 • 시작되었지만 오류가 발생함 • 실패 • 리소스 대기 중

세부 정보 창 열	설명
사용	서버의 활성화 또는 비활성화 여부를 표시합니다.
지난	서버가 부실로 표시되면 서버를 다시 시작해야 합니다. 예를 들어, 서버의 속성 화면에서 특정 서버 설정을 변경한 경우 변경 내용을 적용하기 위해 서버를 다시 시작해야 할 수도 있습니다.
종류	서버의 유형을 표시합니다.
호스트 이름	서버의 호스트 이름을 표시합니다.
상태	서버의 전반적인 상태를 나타냅니다.
PID	서버의 고유한 프로세스 ID 번호를 표시합니다.
설명	서버에 대한 설명을 표시합니다. 서버의 속성 페이지에서 이 설명을 변경할 수 있습니다.
수정한 날짜	서버가 마지막으로 수정되었거나 서버의 상태가 변경된 날짜를 표시합니다. 이 열은 최근에 변경된 서버의 상태를 확인하려는 경우에 매우 유용합니다.

관련 항목

- 377 페이지에서 [서버 그룹 관리](#)"
- 400 페이지에서 [노드 사용](#)"
- 362 페이지에서 [서버 상태 보기](#)"
- 363 페이지에서 [서버 시작, 중지 및 다시 시작](#)"
- 387 페이지에서 [서버 속성 변경](#)"

8.1.2 Windows에서 스크립트를 이용한 서버 관리

ccm.exe 실행 파일을 사용하면 명령줄을 통해 Windows 배포 환경에서 서버를 시작, 중지, 다시 시작, 사용 및 사용 안 할 수 있습니다.

관련 항목

- 776 페이지에서 [ccm.exe](#)"

8.1.3 UNIX에서 서버 관리

ccm.sh 실행 파일을 사용하면 명령줄을 통해 Windows 배포 환경에서 서버를 시작, 중지, 다시 시작, 사용 및 사용 안 할 수 있습니다.

관련 항목

- 767 페이지에서 [ccm.sh](#)"

8.1.4 라이선스 키 관리

이 단원에서는 BI 플랫폼 배포에 필요한 라이선스 키를 관리하는 방법에 대해 설명합니다.

관련 항목

- 359 페이지에서 [라이선스 정보 보기](#)"
- 360 페이지에서 [라이선스 키 추가](#)"
- 360 페이지에서 [현재 계정 활동을 보려면](#)"

8.1.4.1 라이선스 정보 보기

CMC의 라이선스 키 관리 영역에서는 역할(BI Viewer 및 BI Analyst)에 따라 각 키와 관련된 동시 라이선스, 명명된 라이선스 및 프로세서 라이선스 수를 확인할 수 있습니다.

1. CMC의 라이선스 키 관리 영역으로 이동합니다.
2. 라이선스 키를 선택합니다.

선택한 키와 관련된 자세한 정보가 라이선스 키 정보 영역에 나타납니다. 추가 라이선스 키를 구입하려면 SAP 영업 담당자에게 문의하십시오.

관련 항목

- 359 페이지에서 [라이선스 키 관리](#)"
- 360 페이지에서 [라이선스 키 추가](#)"
- 360 페이지에서 [현재 계정 활동을 보려면](#)"

8.1.4.2 라이선스 키 추가

평가판 제품을 업그레이드할 경우에는 새 라이선스 키 또는 정품 인증 키코드를 추가하기 전에 평가용 키를 삭제해야 합니다.

1. CMC의 라이선스 키 관리 영역으로 이동합니다.
2. 키 추가 필드에 키를 입력합니다.
3. 추가를 클릭합니다.

목록에 키가 추가됩니다.

관련 항목

- 359 페이지에서 [라이선스 정보 보기](#)"
- 360 페이지에서 [현재 계정 활동을 보려면](#)"

8.1.4.3 현재 계정 활동을 보려면

1. CMC의 설정 관리 영역으로 이동합니다.
2. 전역 시스템 메트릭 보기를 클릭합니다.

이 섹션에는 추가 작업 메트릭과 함께 현재 사용하는 라이선스 정보가 표시됩니다.

관련 항목

- 359 페이지에서 [라이선스 키 관리](#)"
- 360 페이지에서 [라이선스 키 추가](#)"
- 359 페이지에서 [라이선스 정보 보기](#)"

8.1.5 라이선스 측정

BOLMT(BusinessObjects License Measurement Tool)는 BI 플랫폼 라이선스 데이터를 수집 및 저장하는 데 사용되는 Java 명령줄 유틸리티입니다. 출력 XML 문서에는 라이선스 배포 측정값이 포함되어 있으며 이 문서는 라이선스 감사의 일부로 통합되도록 SAP GLAS(Global License Auditing Services)로 전송됩니다.

시스템 관리자는 라이선스 감사가 요청될 때마다 모든 BI 플랫폼 클러스터에 대해 BOLMT를 설치하고 실행합니다. BOLMT에서는 명명된 역할 기반 동시 사용자 라이선스에 대한 사용 측정값을 수집합니다.

관리자는 XML 문서에 대한 특정 출력 디렉터리를 지정하고 시스템 사용자를 식별하는 데 사용할 수 있는 정보를 포함하지 않도록 출력 문서를 구성할 수 있습니다.

8.1.5.1 라이선스 감사 실행

라이선스 감사를 수행하려면 관리자 권한이 필요하며 BI 플랫폼 설치의 BOLMT.jar 파일이 포함된 디렉터리에 액세스해야 합니다.

1. 명령줄 콘솔을 엽니다.
2. BI 플랫폼을 설치하는 데 필요한 Java 실행 파일이 포함된 디렉터리로 디렉터리를 변경합니다.
기본적으로 이 파일은 [INSTALLDIR]WSAP BusinessObjects Enterprise XI 4.0WjavaWlib 디렉터리에 설치됩니다.
3. BOLMT.jar를 실행합니다.
-jar BOLMT.jar [options] <outputFile>과 같은 형식으로 실행 명령을 입력합니다
아래 표에서는 사용 가능한 옵션에 대해 간략하게 설명합니다.

옵션	설명
-c --cms	중앙 관리 서버(CMS)의 이름 식별자 및 포트 번호를 지정합니다. cmsname:port number로 지정합니다. 이 설정이 지정되어 있지 않으면 기본적으로 로컬 호스트에 대한 CMS 설정이 사용됩니다.
-p --password	CMS에 연결하는 데 사용되는 관리자 계정 암호를 지정합니다.
-a --auth	사용자를 CMS에 연결하는 인증 방법을 지정합니다. 기본 방법은 secEnterprise로 지정된 Enterprise입니다.
-s --sanitize	출력 감사 문서에서 사용자를 식별하는 데 사용할 수 있는 개인 정보를 필터링하도록 지정합니다.

참고:

출력 파일은 항상 명령줄의 마지막 인수로 지정됩니다. 이 설정은 선택 사항입니다. 지정된 인수가 없는 경우 해당 출력이 콘솔의 표준 출력이 됩니다. 또한 명령줄 인수로 스크립트에 출력을 파이프할 수도 있습니다.

예제

```
C:\Program Files (x86)\WSAP
Business Objects\WSAP BusinessObjects Enterprise XI 4.0\WjavaWlib>"C:\Program Files
(x86)\WSAP Business Objects\WSAP BusinessObjects Enterprise XI 4.0\Wwin64_x64\Wsapjvm\Wbin
Wjava.exe" -jar BOLMT.jar --cms=mycms:6400 -uAdministrator
-p=7juujg --auth=secEnterprise --sanitize audit.xml
```

8.1.6 서버 상태 확인 및 변경

8.1.6.1 서버 상태 보기

서버의 상태란 서버의 현재 작업 상태를 말합니다. 서버는 실행 중, 시작하는 중, 중지하는 중, 중지됨, 실패, 초기화하는 중, 시작되었지만 오류가 발생함, 리소스 대기 중 등의 상태가 될 수 있습니다. SAP BusinessObjects Business Intelligence 플랫폼 요청에 응답하려면 서버를 실행하여 활성화해야 합니다. 비활성화된 서버는 프로세스로서 실행을 계속하지만 SAP BusinessObjects Business Intelligence 플랫폼의 다른 요청을 수락하지는 않습니다. 중지된 서버는 더 이상 프로세스로서 실행되지 않습니다.

이 단원에서는 CMC를 사용하여 서버의 상태를 수정하는 방법을 보여 줍니다.

관련 항목

- 363 페이지에서 [서버의 상태를 보려면](#)
- 363 페이지에서 [서버 시작, 중지 및 다시 시작](#)
- 367 페이지에서 [서버 활성화 및 비활성화](#)
- 366 페이지에서 [중앙 관리 서버 중지](#)
- 365 페이지에서 [서버 자동 시작](#)

8.1.6.1.1 서버의 상태를 보려면

1. CMC의 서버 관리 영역으로 이동합니다.

세부 정보 창에는 배포의 서비스 범주가 표시됩니다.

2. 지정된 서버 그룹, 노드 또는 서비스 범주의 서버 목록을 보려면 탐색 트리에서 서버 그룹, 노드 또는 범주를 클릭합니다.

세부 정보 창에는 배포된 서버 목록이 표시됩니다. 상태 열에는 목록의 각 서버에 대한 상태가 표시됩니다.

3. 현재 특정 상태에 있는 모든 서버의 목록을 보려면 탐색 트리에서 서버 상태 옵션을 확장하고 원하는 상태를 선택합니다.

선택한 상태의 서버 목록이 세부 정보 창에 표시됩니다.

참고:

이 방법은 제대로 시작되지 않았거나 갑자기 중지된 서버의 목록을 빨리 확인해야 하는 경우 특히 유용합니다.

8.1.6.2 서버 시작, 중지 및 다시 시작

서버를 시작, 중지 및 다시 시작하는 작업은 서버를 구성하거나 서버를 오프라인 상태로 만들 때 일반적으로 수행하는 작업입니다. 예를 들어 서버의 이름을 변경하려면 먼저 서버를 중지해야 합니다. 필요한 내용을 변경한 다음 서버를 다시 시작하면 변경 사항이 적용됩니다. 서버의 구성 설정을 변경했을 때 서버를 다시 시작해야 하는 경우에는 관련 메시지가 CMC에 표시됩니다.

이 단원의 나머지 부분에서는 특정한 구성 변경에 따라 서버를 먼저 중지하거나 다시 시작해야 하는 경우에 대해 설명합니다. 이러한 작업은 자주 수행하게 되므로 그 개념과 차이점을 먼저 설명하고 일반적인 절차를 참조로 설명합니다.

작업	설명
서버 중지	특정 속성과 설정을 수정하려면 먼저 SAP BusinessObjects Business Intelligence 플랫폼 서버를 중지해야 할 수도 있습니다.
서버 시작	서버를 구성하기 위해 중지한 경우, 변경 사항을 적용하고 서버에서 요청을 계속 처리하도록 하려면 서버를 시작해야 합니다.
서버 다시 시작	서버 다시 시작은 서버를 완전히 중지한 다음 다시 시작하는 작업을 결합한 것입니다. 서버 설정을 변경한 후에 서버를 다시 시작해야 하는 경우 CMC에 관련 메시지가 표시됩니다.
자동으로 서버 시작	Server Intelligence Agent를 시작할 때 서버가 자동으로 시작되도록 설정할 수 있습니다.
강제 종료	현재 처리 중인 작업을 완료한 다음 서버를 중지하는 일반적인 경우와 달리 서버를 즉시 중지합니다. 서버 중지에 실패하여 즉시 서버를 중지시킬 필요가 있을 때만 서버를 강제로 종료합니다.

팁:

서버를 중지하거나 다시 시작할 때 서버의 프로세스를 종료하여 서버를 완전히 중지합니다. 서버를 중지하기 전에 다음을 수행하는 것이 좋습니다.

- 진행 중인 작업 처리를 완료할 수 있도록 서버를 비활성화합니다.
- 대기열에 감사 이벤트가 남아 있지 않은지 확인합니다. 대기열에 남아 있는 감사 이벤트 수를 확인하려면 서버의 메트릭 화면으로 이동한 다음 대기열의 현재 감사 이벤트 수 메트릭을 확인합니다.

관련 항목

- 367 페이지에서 [서버 활성화 및 비활성화](#)

8.1.6.2.1 CMC를 사용하여 서버 시작, 중지, 다시 시작

1. CMC의 서버 관리 영역으로 이동합니다.

세부 정보 창에는 배포의 서비스 범주가 표시됩니다.

2. 특정 서버 그룹, 노드 또는 서비스 범주의 서버 목록을 보려면 탐색 창에서 그룹, 노드 또는 범주를 선택합니다.

세부 정보 창에 서버 목록이 표시됩니다.

3. 현재 특정 상태에 있는 모든 서버의 목록을 보려면 탐색 트리에서 서버 상태 옵션을 확장하고 원하는 상태를 선택합니다.

선택한 상태의 서버 목록이 세부 정보 창에 표시됩니다.

참고:

이 방법은 제대로 시작되지 않았거나 갑자기 중지된 서버의 목록을 빨리 확인해야 하는 경우 특히 유용합니다.

4. 상태를 변경할 서버를 마우스 오른쪽 단추로 클릭하고 수행해야 할 작업에 따라 서버 시작, 서버 다시 시작, 서버 중지 또는 강제 종료를 선택합니다.

관련 항목

- 362 페이지에서 [서버 상태 보기](#)"

8.1.6.2.2 CCM을 사용하여 Windows 서버 시작, 중지 또는 다시 시작

1. CCM에서 도구 모음의 서버 관리 단추를 클릭합니다.
2. 로그인하라는 메시지가 표시되면 관리 계정을 사용하여 CMS에 로그인합니다.
3. 서버 관리 대화 상자에서 시작, 중지 또는 다시 시작할 서버를 선택합니다.
4. 시작, 중지, 다시 시작 또는 강제 종료를 클릭합니다.
5. 닫기를 클릭하여 CCM으로 돌아갑니다.

8.1.6.2.3 서버 자동 시작

기본적으로 배포 환경의 서버는 Server Intelligence Agent를 시작할 때 자동으로 시작됩니다. 다음 절차에서는 이 옵션을 어떻게 설정할 수 있는지 보여 줍니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 자동으로 시작할 서버를 두 번 클릭합니다.
속성 화면이 나타납니다.
3. 일반 설정에서 Server Intelligence Agent가 시작되면 자동으로 이 서버 시작 확인란을 선택한 다음 저장 또는 저장 후 닫기를 클릭합니다.

참고:

클러스터의 모든 CMS에 대해 자동 시작 설정을 해제한 경우 시스템을 다시 시작하려면 CCM을 사용해야 합니다. CCM을 사용하여 SIA를 중지한 후 SIA를 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다. 시작 탭에서 자동 시작 설정을 예로 변경한 다음 저장을 클릭합니다. SIA를 다시 시작합니다.

8.1.6.3 중앙 관리 서버 중지

SAP BusinessObjects Business Intelligence 플랫폼 설치 환경에 활성화된 중앙 관리 서버(CMS)가 여러 개인 경우 데이터를 잃거나 시스템 기능에 영향을 주지 않으면서 CMS 하나를 종료할 수 있습니다. 중지된 서버의 작업 부하는 노드의 다른 CMS를 통해 처리됩니다. 여러 CMS를 클러스터링하면 SAP BusinessObjects Business Intelligence 플랫폼의 서비스 상태를 계속 유지하면서 각 중앙 관리 서버에 대한 유지 관리 작업을 차례로 수행할 수 있습니다.

그러나 SAP BusinessObjects Business Intelligence 플랫폼 배포에 CMS가 하나뿐인 경우 이를 종료하면 사용자가 SAP BusinessObjects Business Intelligence 플랫폼을 사용할 수 없게 되고 보고서 및 프로그램의 처리가 중단됩니다. 이 문제를 방지하기 위해 각 노드의 Server Intelligence Agent에서는 항상 적어도 하나 이상의 CMS가 실행되도록 합니다. 이 경우에도 해당 SIA를 중지하여 CMS를 중지할 수는 있지만, SIA를 중지하기 전에 CMC를 통해 처리 서버를 비활성화해야 합니다. 이렇게 하면 노드의 다른 모든 서버도 종료되므로 SAP BusinessObjects Business Intelligence 플랫폼을 종료하기 전에 처리 중이던 모든 작업을 마칠 수 있습니다.

참고:

때로는 CMS가 중지되어 CCM에서 시스템을 다시 시작해야 하는 상황이 발생할 수 있습니다. 예를 들어 SIA를 시작할 때 모든 CMS가 자동으로 시작되도록 설정하지 않은 상태에서 노드의 모든 CMS를 종료한 경우 시스템을 다시 시작하려면 CCM을 사용해야 합니다. CCM에서 SIA를 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다. 시작 탭에서 자동 시작 설정을 예로 변경한 다음 저장을 클릭합니다. SIA를 다시 시작합니다.

다른 서버를 시작하거나 중지하는 일 없이 클러스터에서 중앙 관리 서버(CMS)를 시작하고 중지할 수 있도록 시스템을 구성하려면 CMS를 별도의 노드에 배치합니다. 새 노드를 만들고 CMS를 해당 노드에 복제합니다. CMS를 고유한 자체 노드에 배치하면 다른 서버에 영향을 주지 않은 채 노드를 쉽게 종료할 수 있습니다.

관련 항목

- 400 페이지에서 [노드 사용](#)"
- 369 페이지에서 [서버 복제](#)"
- 372 페이지에서 [중앙 관리 서버 클러스터링](#)"

8.1.6.4 서버 활성화 및 비활성화

SAP BusinessObjects Business Intelligence 플랫폼 서버를 비활성화하면 해당 서버가 새 SAP BusinessObjects Business Intelligence 플랫폼 요청을 수신하거나 새 요청에 응답하지는 않지만 서버 프로세스가 실제로 중지되지는 않습니다. 이는 서버를 완전히 중지하기 전에 해당 서버에서 현재 진행 중인 요청 처리를 모두 마치도록 하려는 경우에 유용합니다.

예를 들어, 작업 서버가 실행되고 있는 컴퓨터를 다시 부팅하기 전에 먼저 이 서버를 중지시키려고 합니다. 단 해당 대기열에 있는 해결되지 않은 모든 보고서 요청을 서버에서 수행하도록 만들려고 합니다. 이렇게 하려면 우선 추가 요청을 더 이상 수락하지 않도록 작업 서버를 비활성화합니다. 그런 다음 중앙 관리 콘솔로 이동하여 서버에서 진행 중인 작업의 완료 상태를 모니터링합니다. (서버 관리 영역에서 서버를 마우스 오른쪽 단추로 클릭하고 메트릭을 선택합니다.) 현재 처리 중인 요청이 완료되면 서버를 안전하게 중지할 수 있습니다.

참고:

- 다른 서버를 활성화하거나 비활성화하려면 CMS가 실행되고 있어야 합니다.
- CMS를 활성화 또는 비활성화할 수 없습니다.

8.1.6.4.1 CMC를 사용하여 서버를 활성화 또는 비활성화하려면

1. CMC의 서버 관리 영역으로 이동합니다.
2. 상태를 변경할 서버를 마우스 오른쪽 단추로 클릭하고 수행해야 할 작업에 따라 서버 사용 또는 서버 사용 안 함을 클릭합니다.

8.1.6.4.2 CCM을 사용하여 Windows 서버를 활성화 또는 비활성화하려면

1. CCM에서 서버 관리를 클릭합니다.
2. 로그인하라는 메시지가 표시되면 BI 플랫폼에 대한 관리 권한이 있는 자격 증명을 사용하여 CMS에 로그인합니다.
3. 서버 관리 대화 상자에서 활성화 또는 비활성화하려는 서버를 선택합니다.
4. 사용 또는 사용 안 함을 클릭합니다.
5. 닫기를 클릭하여 CCM으로 돌아갑니다.

8.1.7 서버 추가, 복제 또는 삭제

8.1.7.1 서버 추가, 복제 및 삭제

별도의 새 컴퓨터에 서버 구성 요소를 설치하여 SAP BusinessObjects Business Intelligence 플랫폼에 하드웨어를 새로 추가하는 경우에는 배포된 제품에서 SAP BusinessObjects Business Intelligence 플랫폼 설치 프로그램을 실행해야 합니다. 설치 프로그램을 사용하면 사용자 지정 설치를 수행할 수 있습니다. 사용자 지정 설치 과정에서는 기존 배포의 CMS를 지정하고 로컬 컴퓨터에 설치할 구성 요소를 선택합니다. 사용자 지정 설치 옵션에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 설치 가이드를 참조하십시오.

8.1.7.1.1 서버 추가

동일한 컴퓨터에서 동일한 BI 플랫폼 서버의 여러 인스턴스를 실행할 수 있습니다. 서버를 추가하려면 다음과 같이 하십시오.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 관리 메뉴에서 새로 만들기 > 새 서버를 클릭합니다.
새 서버 만들기 대화 상자가 나타납니다.
3. 서비스 범주를 선택합니다.
4. 서비스 선택 목록에서 필요한 서비스 유형을 선택하고 다음을 클릭합니다.
5. 서버에 다른 서비스를 추가하려면 사용 가능한 추가 서비스 목록에서 서비스를 선택하고 >를 클릭합니다.

참고:

모든 서버 유형에 대해 추가 서비스를 사용할 수 있는 것은 아닙니다.

6. 원하는 다른 서비스를 추가했으면 다음을 클릭합니다.
7. BI 플랫폼 아키텍처가 여러 개의 노드로 구성된 경우에는 노드 목록에서 새 서버를 추가할 노드를 선택합니다.
8. 서버 이름 상자에 서버의 이름을 입력합니다.
시스템의 각 서버 이름은 고유한 것이어야 합니다. 기본 명명 규칙은 <NODENAME>.<servertype>입니다. 동일한 호스트 컴퓨터에 동일한 유형의 서버가 두 개 이상 있는 경우 번호가 추가됩니다.
9. 필요한 경우 설명 상자에 서버에 대한 설명을 입력합니다.
10. 새로운 중앙 관리 서버를 추가하려는 경우 이름 서버 포트 필드에 포트 번호를 입력합니다.
11. 만들기를 클릭합니다.
CMC의 서버 영역에 있는 서버 목록에 새 서버가 표시되지만 새 서버가 시작되거나 활성화되지는 않습니다.
12. 새 서버가 BI 플랫폼 요청에 응답하도록 만들려면 CMC를 사용하여 서버를 시작하고 활성화합니다.

관련 항목

- 44 페이지에서 [서비스 및 서버](#)
- 387 페이지에서 [서버 설정 구성](#)
- 397 페이지에서 [포트 번호 구성](#)
- 362 페이지에서 [서버 상태 보기](#)

8.1.7.1.2 서버 복제

기존 배포에 새 서버 인스턴스를 추가하려는 경우 기존 서버를 복제할 수 있습니다. 복제된 서버는 원래 서버의 구성 설정을 유지합니다. 배포를 확장하고 기존 서버와 같은 서버 구성 설정을 거의 대부분 사용하는 새 서버 인스턴스를 만들려는 경우 이 기능이 특히 유용할 수 있습니다.

또한 복제를 통해 노드 간에 서버를 간편하게 이동할 수 있습니다. 기존 CMS를 다른 노드로 이동하려면 이를 새 노드에 복제합니다. 복제한 CMS가 새 노드에 표시됩니다. 이렇게 복제한 CMS는 원래 CMS의 모든 구성 설정을 그대로 유지합니다.

서버를 복제할 때는 몇 가지 사항을 고려해야 합니다. 모든 설정을 복제할 필요가 없을 수도 있으므로 복제된 서버를 확인하여 필요에 맞는 지 확인하는 것이 좋습니다. 예를 들어, CMS를 동일한 컴퓨터에 복제하는 경우 원래 CMS에서 복제된 CMS로 복사된 포트 번호 설정을 변경해야 합니다.

참고:

- 서버를 복제하려면 먼저 배포 환경의 모든 컴퓨터에 동일한 버전의 SAP BusinessObjects Business Intelligence 플랫폼(및 해당하는 경우 업데이트)이 설치되어 있는지 확인해야 합니다.
- 서버는 어느 컴퓨터에서나 복제할 수 있습니다. 그러나 해당 서버에 필요한 이진 파일이 설치되어 있는 컴퓨터에만 서버를 복제할 수 있습니다.
- 서버를 복제하더라도 새 서버에 반드시 동일한 OS 자격 증명이 사용되는 것은 아닙니다. 사용자 계정은 서버를 실행하는 데 사용되는 Server Intelligence Agent에서 제어합니다.

8.1.7.1.2.1 서버 설정 자리 표시자 사용

자리 표시자는 노드에서 실행 중인 서버에서 사용하는 노드 수준 변수로, 중앙 관리 콘솔(CMC)의 전용 페이지에 나열되어 있습니다. CMC에서 서버에 나열된 서버를 두 번 클릭하면 자리 표시자의 왼쪽 탐색 창에 링크가 제공됩니다. 자리 표시자 페이지에는 선택된 서버에 대해 사용 가능한 모든 자리 표시자 이름과 관련 값이 나열됩니다. 자리 표시자에는 읽기 전용 값이 포함되고 자리 표시자 이름은 백분율 문자 %로 시작되고 끝납니다.

참고:

항상 CMC 서버 속성 페이지에서 특정 문자열로 자리 표시자 설정을 덮어쓸 수 있습니다.

예제

서버를 복제할 경우 자리 표시자가 유용합니다. 예를 들어 복수 드라이브 컴퓨터 A의 경우 SAP BusinessObjects Enterprise는 C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0에 설치되어 있습니다. 따라서 %DefaultAuditingDir% 자리 표시

자는 D:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\을 가리킵니다.

다른 컴퓨터인 컴퓨터 B에는 하나의 디스크 드라이브(드라이브 D 없음)만 있고 SAP BusinessObjects Enterprise가 C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0 에 설치되어 있습니다. 이 경우 %DefaultAuditingDir% 자리 표시자는 C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\을 가리킵니다.

컴퓨터 A에서 컴퓨터 B로 이벤트 서버를 복제하기 위해 감사 임시 디렉터리에서 자리 표시자를 사용할 경우 이 자리 표시자가 자체적으로 확인되므로 이벤트 서버가 올바르게 작동합니다. 자리 표시자를 사용하지 않을 경우 감사 임시 디렉터리 설정을 수동으로 덮어쓰지 않으면 이벤트 서버가 실패합니다.

8.1.7.1.2.2 서버 복제

1. 복제된 서버에 추가할 컴퓨터에서 CMC의 서버 관리 영역으로 이동합니다.
2. 복제할 서버를 마우스 오른쪽 단추로 클릭하고 서버 복제를 선택합니다.
복제 서버 대화 상자가 나타납니다.
3. 새 서버 이름 필드에 서버 이름을 입력하거나 기본 이름을 사용합니다.
4. 중앙 관리 서버를 복제하려는 경우 이름 서버 포트 필드에 포트 번호를 입력합니다.
5. 노드에 복제 목록에서 복제된 서버를 추가할 노드를 선택한 다음 확인을 클릭합니다.
CMC의 서버 관리 영역에 새 서버가 나타납니다.

참고:

포트 번호 설정도 복제됩니다. CMS를 복제할 때와 같은 대부분의 경우 원래 서버와 복제된 서버 간에 포트가 충돌하지 않도록 포트 번호를 변경하는 것이 좋습니다.

8.1.7.1.3 서버 삭제

1. CMC의 서버 관리 영역으로 이동합니다.
2. 삭제하려는 서버를 중지합니다.
3. 서버를 마우스 오른쪽 단추로 클릭하고 삭제를 클릭합니다.

4. 확인 메시지가 나타나면 확인을 클릭합니다.

8.1.8 중앙 관리 서버 클러스터링

8.1.8.1 중앙 관리 서버 클러스터링

구현된 SAP BusinessObjects Business Intelligence 플랫폼의 규모가 크거나 매우 중요한 경우 여러 CMS 컴퓨터를 클러스터로 함께 실행할 수 있습니다. 클러스터는 공통 CMS 시스템 데이터베이스에 대해 함께 작동하는 두 개 이상의 CMS 서버로 구성됩니다. CMS 중 하나가 실행되는 컴퓨터에서 문제가 발생하면 다른 CMS가 실행되는 컴퓨터에서 SAP BusinessObjects Business Intelligence 플랫폼 요청을 계속 처리합니다. 이러한 "고가용성" 지원 덕분에 장비에 문제가 있는 경우에도 SAP BusinessObjects Business Intelligence 플랫폼 사용자는 필요한 정보에 계속 액세스할 수 있습니다.

이 단원에서는 이미 설정을 마치고 실행 중인 운영 시스템에 새 CMS 클러스터 멤버를 추가하는 방법을 설명합니다. 기존의 클러스터에 새 CMS를 추가할 때는 새 CMS가 기존의 CMS 시스템 데이터베이스에 연결되고 기존의 CMS 컴퓨터와 처리 작업 부하를 공유하도록 지정합니다. 현재 CMS에 대한 정보는 CMC의 서버 관리 영역에서 확인할 수 있습니다.

CMS 컴퓨터를 클러스터링하기 전에 각 CMS가 운영 체제, 데이터베이스 서버, 데이터베이스 액세스 방법, 데이터베이스 드라이버 및 데이터베이스 클라이언트에 대한 세부 요구 사항(버전 수준 및 패치 수준 포함)을 충족하는 시스템에 설치되어 있는지 확인해야 합니다. 이러한 요구 사항에 대한 개요는 배포된 제품에 포함되어 있는 platforms.txt 파일을 참조하십시오.

또한, 다음과 같은 클러스터링 요구 사항을 충족시켜야 합니다.

- 최적의 성능을 얻기 위해서는 시스템 데이터베이스를 호스팅할 데이터베이스 서버로 단순한 쿼리들을 매우 빠르게 처리할 수 있는 서버를 선택해야 합니다. CMS는 시스템 데이터베이스와 자주 통신하며 많은 양의 단순한 쿼리를 전달합니다. 데이터베이스 서버에서 이러한 요청을 적시에 처리하지 못하면 SAP BusinessObjects Business Intelligence 플랫폼 성능이 크게 저하될 수 있습니다.
- 최적의 성능을 얻기 위해서는 메모리 크기와 CPU 종류가 동일한 컴퓨터에서 각 CMS 클러스터 멤버를 실행해야 합니다.
- 각 컴퓨터를 서로 비슷하게 구성해야 합니다.
 - 운영 체제 서비스 팩과 패치 버전까지 동일하게 맞추어 동일한 운영 체제를 설치합니다.

- 동일한 버전의 SAP BusinessObjects Business Intelligence 플랫폼(사용 가능한 경우 패치도 포함)을 설치합니다.
- 네이티브를 사용하든 ODBC 드라이버를 사용하든 각 CMS는 동일한 방식으로 CMS 시스템 데이터베이스에 연결되어야 합니다. 각 컴퓨터의 드라이버가 동일하고 지원되는 버전인지 확인합니다.
- 각 CMS에서 시스템 데이터베이스에 연결하는 데 지원되는 버전의 동일한 데이터베이스 클라이언트를 사용해야 합니다.
- 각 CMS에서 CMS 시스템 데이터베이스에 연결하는 데 동일한 데이터베이스 사용자 계정과 암호를 사용하는지 확인합니다. 이 계정에는 시스템 데이터베이스에 대한 작성, 삭제 및 업데이트 권한이 있어야 합니다.
- 각 CMS가 있는 노드가 동일한 운영 체제 계정으로 실행되는지 확인합니다. Windows의 경우 기본 계정은 "LocalSystem"입니다.
- 각 CMS 컴퓨터마다 일광 절약 시간 설정을 비롯하여 현재 날짜와 시간이 올바르게 설정되어 있는지 확인합니다.
- 클러스터의 모든 웹 응용 프로그램 서버에 동일한 WAR 파일이 설치되어 있어야 합니다. WAR 파일 배포에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 설치 가이드를 참조하십시오.
- 클러스터의 각 CMS가 모두 동일한 LAN에 속해 있는지 확인합니다.
- 클러스터에 CMS 클러스터 멤버가 9개 이상인 경우 각 CMS에 대한 명령줄에 `-oobthreads <numCMS>` 옵션이 포함되어야 합니다. 여기에서 `<numCMS>`는 클러스터의 CMS 서버 수입니다. 이 옵션을 사용해야 클러스터가 과부하를 처리할 수 있습니다. 서버 명령줄 구성에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드를 참조하십시오.
- 감사 기능을 사용하려면 각 CMS가 동일한 감사 데이터베이스를 사용하고 동일한 방식으로 이 데이터베이스에 연결되도록 구성해야 합니다. 감사 데이터베이스에 대한 요구 사항은 데이터베이스 서버, 클라이언트, 액세스 방법, 드라이버 및 사용자 ID의 측면에서 시스템 데이터베이스에 대한 요구 사항과 동일합니다.

팁:

기본적으로 클러스터 이름에는 설치된 첫째 CMS의 이름이 반영됩니다.

관련 항목

- 376 페이지에서 [CMS 클러스터의 이름 변경](#)

8.1.8.1.1 클러스터에 CMS 추가

새 CMS 클러스터 멤버를 추가하는 데는 여러 가지 방법이 있습니다. 다음 중 적절한 절차를 따릅니다.

- 새 컴퓨터에 CMS와 함께 새 노드를 설치할 수 있습니다.
- 이미 CMS 이진 파일과 함께 노드를 설치한 경우 CMC에서 새 CMS 서버를 추가할 수 있습니다.
- 이미 CMS 이진 파일과 함께 노드를 설치한 경우 기존 CMS 서버를 복제하여 새 CMS 서버를 추가할 수도 있습니다.

참고:

변경하기 전에 현재 CMS 시스템 데이터베이스와 입력 및 출력 파일 리포지토리의 콘텐츠를 백업하는 것이 좋습니다. 필요한 경우 데이터베이스 관리자에게 문의하십시오.

관련 항목

- 374 페이지에서 [클러스터에 새 노드 추가](#)"
- 368 페이지에서 [서버 추가](#)"
- 369 페이지에서 [서버 복제](#)"
- 469 페이지에서 [시스템 백업 및 복원](#)"

8.1.8.1.2 클러스터에 새 노드 추가

노드를 추가할 때 메시지에 따라 새 CMS를 만들거나 기존 CMS에 노드를 클러스터링할 수 있습니다.

노드를 기존 CMS에 클러스터링할 때는 설치 프로그램을 사용할 수도 있습니다. 새 CMS 클러스터 멤버를 설치할 컴퓨터에서 SAP BusinessObjects Business Intelligence 플랫폼 설치 프로그램을 실행합니다. 설치 프로그램을 사용하면 사용자 지정 설치를 수행할 수 있습니다. 사용자 지정 설치 과정에서 시스템을 확장할 기존의 CMS를 지정하고 로컬 컴퓨터에 설치하려는 구성 요소를 선택합니다. 이 경우 기존의 시스템에서 실행되는 CMS의 이름을 지정하고 로컬 컴퓨터에 새 CMS를 설치하도록 선택합니다. 그런 다음 기존의 CMS 시스템 데이터베이스에 연결하는 데 필요한 정보를 설치 프로그램에 입력합니다. 설치 프로그램이 로컬 컴퓨터에 새 CMS를 설치할 때 기존의 클러스터에 서버가 자동으로 추가됩니다.

관련 항목

- 400 페이지에서 [노드 사용](#)"

8.1.8.1.3 웹 응용 프로그램 속성 파일에 클러스터 추가

배포 환경에 CMS를 더 추가했으며 Java 응용 프로그램 서버를 사용하는 경우 웹 응용 프로그램 배포의 `WwebappsWBOEWWEB-INFWconfigWcustom` 디렉터리에 있는 `PlatformServices.properties` 파일을 수정해야 합니다.

8.1.8.1.3.1 BOE 웹 응용 프로그램에 대한 클러스터 속성 정의

1. 웹 응용 프로그램을 호스팅하는 컴퓨터에서 `BOE.war` 파일에 대한 사용자 지정 폴더에 액세스합니다.

SAP BusinessObjects Business Intelligence 플랫폼 설치 시 함께 제공되는 Tomcat 웹 응용 프로그램 서버를 사용 중인 경우 다음 폴더에 직접 액세스할 수 있습니다.

`C:\WProgram Files (x86)\WSAP BusinessObjects\Tomcat6\Wwebapps\WBOEWWEB-INF\Wconfig\Wcustom\W`

팁:

배포된 웹 응용 프로그램에 대한 직접 액세스를 지원하지 않는 웹 응용 프로그램 서버를 사용 중인 경우 설치된 제품의 다음 폴더에서 `BOE.war` 파일을 수정할 수 있습니다.

`<INSTALLDIR>\WSAP BusinessObjects Business Intelligence platform 4.0\Wwarfiles\Wwebapps\WBOEWWEB-INF\Wconfig\Wcustom\W.`

나중에 수정된 `BOE.war`를 다시 배포해야 합니다.

2. 새 파일을 만듭니다.

참고:

메모장이나 다른 텍스트 편집 유틸리티를 사용하십시오.

3. CMC 클러스터 속성을 지정합니다.

`cms.clusters` 속성 - 배포에 모든 클러스터를 지정합니다. 모든 클러스터 이름 앞에 `@` 문자를 사용하고 이를 쉼표로 구분해야 합니다. `cms.clusters=@samplecluster,@samplecluster2,@samplecluster3`을 예로 들 수 있습니다. `cms.clusters`를 사용하십시오. [클러스터 이름] 속성 - 클러스터에 포함된 모든 CMS를 지정합니다. 예를 들면 다음과 같습니다.

```
cms.clusters=@samplecluster,@samplecluster2,@samplecluster3
cms.clusters.samplecluster=cmsone:6400,cmstwo
cms.clusters.samplecluster2=cms3,cms4,cms5
cms.clusters.samplecluster3=aps05
```

참고:

각 CMS 이름은 쉼표로 구분합니다. 포트 번호는 CMS 이름과 콜론으로 구분됩니다. 포트 번호가 지정되지 않으면 6400으로 간주됩니다. 각 클러스터에 대해 이 절차를 반복합니다.

4. 파일을 다음 이름으로 저장합니다.

PlatformServices.properties

5. 응용 프로그램 서버를 다시 시작합니다.

웹 응용 프로그램 서버가 실행되는 컴퓨터에 수정된 BOE 웹 응용 프로그램을 다시 배포해야 새 속성이 적용됩니다. Wdeploy를 사용하여 웹 응용 프로그램 서버에 WAR 파일을 다시 배포하십시오. WDeploy를 사용하는 자세한 방법은 SAP BusinessObjects Business Intelligence 플랫폼 웹 응용 프로그램 배포 가이드를 참조하십시오.

8.1.8.1.4 CMS 클러스터의 이름 변경

다음 절차를 수행하면 이미 설치되어 있는 클러스터의 이름을 변경할 수 있습니다. CMS 클러스터의 이름을 변경한 후 Server Intelligence Agent는 각 SAP Business Objects 서버를 자동으로 다시 구성하여 개별 CMS가 아닌 CMS 클러스터에 등록합니다.

참고:

SAP BusinessObjects Business Intelligence 플랫폼에 속련된 관리자일 경우 더 이상 서버 명령줄에서 -ns 옵션을 사용하여 서버를 등록할 CMS를 구성할 수 없습니다. 이 구성은 이제 SIA를 통해 자동으로 처리됩니다.

8.1.8.1.4.1 Windows에서 클러스터 이름을 변경하려면

1. 이름을 변경할 클러스터의 멤버인 중앙 관리 서버가 들어 있는 노드에 대해 CCM을 사용하여 Server Intelligence Agent를 중지합니다.
2. Server Intelligence Agent를 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.
3. 속성 대화 상자에서 구성 탭을 클릭합니다.
4. 클러스터 이름을 다음으로 변경 확인란을 선택합니다.
5. 클러스터의 새 이름을 입력합니다.
6. 확인을 클릭한 다음 Server Intelligence Agent를 다시 시작합니다.

이제 CMS 클러스터 이름이 변경되었습니다. 다른 모든 CMS 클러스터 멤버에는 새 클러스터 이름이 동적으로 적용됩니다. 클러스터 멤버 전체에 변경 내용이 전파되는 데는 몇 분 정도 걸릴 수도 있습니다.

7. CMC의 서버 관리 영역으로 이동하여 모든 서버가 활성화된 상태를 유지하고 있는지 확인합니다. 필요한 경우 이름 변경으로 인해 비활성화된 서버를 다시 활성화합니다.

8.1.8.1.4.2 UNIX에서 클러스터 이름 변경

cmsdbsetup.sh 스크립트를 사용합니다. 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드의 "Unix 도구" 장을 참조하십시오.

8.1.9 서버 그룹 관리

SAP BusinessObjects Business Intelligence 플랫폼 서버를 서버 그룹으로 구성하면 여러 대의 서버를 더 쉽게 관리할 수 있습니다. 즉 서버 그룹을 관리하는 경우에는 시스템의 모든 서버에 대한 하위 집합만 확인하면 됩니다. 더 중요한 점은, 서버 그룹이 SAP BusinessObjects Business Intelligence 플랫폼을 사용자 지정하는 강력한 수단으로 활용되며 이를 통해 각기 다른 위치에 있는 사용자들이나 서로 다른 유형의 개체에 맞도록 시스템을 최적화할 수 있다는 사실입니다.

서버를 지역별로 그룹화하면 특정 지역의 사무실에서 근무하는 사용자에게 맞게 기본 처리 설정, 주기적인 일정 및 일정 대상을 쉽게 지정할 수 있습니다. 특정 서버 그룹과 개체를 연결하여 개체를 항상 동일한 서버에서 처리하도록 할 수 있습니다. 또한, 일정이 설정된 개체를 특정 서버 그룹에 연결하여 개체를 올바른 프린터, 파일 서버 등에 보낼 수 있습니다. 이와 같이 서버 그룹을 사용하면 여러 지역과 여러 시간대에 걸쳐 분포해 있는 시스템을 관리하는 데 특히 유용합니다.

서버를 유형별로 그룹화하면 각 개체에 대하여 최적화된 서버에서 적절한 개체가 처리되도록 구성할 수 있습니다. 예를 들어, 처리 서버는 게시된 보고서의 데이터가 들어 있는 데이터베이스와 자주 통신해야 합니다. 액세스해야 하는 데이터베이스 서버에 가깝게 처리 서버를 배치하면 시스템 성능이 향상되고 네트워크 트래픽이 최소화됩니다. 따라서 DB2 데이터베이스를 사용하여 실행된 보고서가 여러 개 있는 경우 DB2 데이터베이스 서버에 대해서만 보고서를 처리하는 처리 서버 그룹을 만들 수 있습니다. 그런 다음 보고서를 볼 때 항상 이 처리 서버 그룹을 사용하도록 구성하면 이러한 보고서를 볼 때의 시스템 성능을 향상시킬 수 있습니다.

서버 그룹을 만든 다음 보고서 일정 설정, 보기 또는 수정 작업에 특정 서버 그룹을 사용하도록 개체를 구성합니다. CMC의 서버 관리 영역에 있는 탐색 트리를 사용하여 서버 그룹을 봅니다. 서버 그룹 목록 옵션을 사용하면 세부 정보 창에 서버 목록이 표시됩니다. 서버 그룹 옵션을 사용하면 그룹에 포함된 서버를 볼 수 있습니다.

8.1.9.1 서버 그룹 만들기

서버 그룹을 만들려면 그룹의 이름과 설명을 지정한 다음 서버를 그룹에 추가해야 합니다.

8.1.9.1.1 서버 그룹 만들기

1. CMC의 서버 관리 영역으로 이동합니다.
2. 관리 > 새로 만들기 > 서버 그룹 만들기를 선택합니다.
서버 그룹 만들기 대화 상자가 나타납니다.
3. 이름 필드에 새 서버 그룹 이름을 입력합니다.
4. 서버 그룹에 대한 추가 정보를 포함시키려면 설명 필드에 입력합니다.
5. 확인을 클릭합니다.
6. 서버 관리 영역의 탐색 트리에서 서버 그룹을 클릭하고 새 서버 그룹을 선택합니다.
7. 작업 메뉴에서 멤버 추가를 선택합니다.
8. 이 그룹에 추가할 서버를 선택한 다음 >를 클릭합니다.

팁:

CTRL + 클릭을 사용하여 서버를 여러 개 선택할 수 있습니다.

9. 확인을 클릭합니다.

서버 관리 영역으로 돌아가면 그룹에 추가한 서버가 모두 나열됩니다. 이제 그룹의 서버에 대한 속성을 변경하고 서버 메트릭을 확인하고 상태를 변경할 수 있습니다.

관련 항목

- 362 페이지에서 [서버 상태 보기](#)"

8.1.9.2 서버 하위 그룹 작업

서버의 하위 그룹을 사용하면 서버를 더 세밀하게 구성할 수 있습니다. 하위 그룹은 다른 서버 그룹에 포함된 서버 그룹입니다.

예를 들어, 서버를 지역 및 국가별로 그룹화하면 각 지역별 그룹이 국가 그룹의 하위 그룹이 됩니다. 이러한 방식으로 서버를 구성하려면 먼저 각 지역별 그룹을 만들고 해당 서버를 이 그룹에 추가합니다. 그런 다음 각 국가별 그룹을 만들고 각 지역별 그룹을 해당 국가 그룹에 추가합니다.

하위 그룹을 설정하는 데는 두 가지 방법이 있습니다. 서버 그룹의 하위 그룹을 수정하거나 한 서버 그룹을 다른 서버 그룹의 멤버로 만들 수 있습니다. 결과는 동일하므로 어느 쪽이든 사용자에게 더 편리한 방법을 사용하면 됩니다.

8.1.9.2.1 서버 그룹에 하위 그룹 추가

1. CMC의 서버 관리 영역으로 이동합니다.
2. 탐색 트리에서 서버 그룹을 클릭하고 하위 그룹을 추가할 서버 그룹을 선택합니다.
이 그룹은 부모 그룹이 됩니다.
3. 작업 메뉴에서 멤버 추가를 선택합니다.
4. 탐색 트리에서 서버 그룹을 클릭하고 이 그룹에 추가할 서버 그룹을 선택한 다음 >를 클릭합니다.
팁:
CTRL + 클릭을 사용하여 서버 그룹을 여러 개 선택할 수 있습니다.
5. 확인을 클릭합니다.
서버 관리 영역으로 돌아가면 부모 그룹에 추가한 서버 그룹이 모두 나열됩니다.

8.1.9.2.2 서버 그룹을 다른 서버 그룹의 멤버로 만들려면

1. CMC의 서버 관리 영역으로 이동합니다.
2. 다른 그룹에 추가할 그룹을 클릭합니다.

3. 작업 메뉴에서 서버 그룹에 추가를 선택합니다.
4. 사용 가능한 서버 그룹 목록에서 해당 그룹을 추가할 다른 그룹을 선택한 다음 >를 클릭합니다.

팁:

CTRL + 클릭을 사용하여 서버 그룹을 여러 개 선택할 수 있습니다.

5. 확인을 클릭합니다.

8.1.9.3 서버의 그룹 멤버 구성 수정

서버의 그룹 멤버 구성을 수정하면 시스템에 이미 작성되어 있는 그룹 또는 하위 그룹에서 서버를 쉽게 추가하거나 제거할 수 있습니다.

예를 들어, 여러 지역별 서버 그룹이 작성되어 있는 경우를 생각해 볼 수 있습니다. 하나의 중앙 관리 서버(CMS)를 여러 지역에 사용하려고 하는 경우, CMS를 각 지역별 서버 그룹에 개별적으로 추가하는 대신 서버의 소속 그룹 링크를 클릭하여 이를 세 지역 모두에 한 번에 추가할 수 있습니다.

8.1.9.3.1 서버의 그룹 멤버 구성 수정

1. CMC의 서버 관리 영역으로 이동합니다.
2. 소속 그룹 정보를 변경할 서버를 마우스 오른쪽 단추로 클릭하고 기존 서버 그룹을 선택합니다.
세부 정보 패널의 사용 가능한 서버 그룹 목록에 서버를 추가할 수 있는 그룹이 표시됩니다. 서버 그룹의 멤버 목록에는 해당 서버가 현재 속해 있는 모든 서버 그룹이 표시됩니다.
3. 서버가 속한 그룹을 변경하려면 화살표를 사용하여 목록 간에 서버 그룹을 이동한 다음 확인을 클릭합니다.

8.1.9.4 서버 및 서버 그룹에 대한 사용자 액세스

권한을 사용하면 서버와 서버 그룹에 대한 액세스 권한을 사용자에게 부여하여 서버 시작 및 중지 같은 작업을 수행하도록 할 수 있습니다.

시스템 구성과 보안 요구 사항에 따라 서버 관리 권한을 SAP BusinessObjects Business Intelligence 플랫폼 관리자로 제한할 수도 있습니다. 그러나 이러한 서버를 사용하는 다른 사용자에게도 액세스 권한을 제공해야 할 수 있습니다. 대부분의 조직에는 서버 관리를 전담하는 IT 전문가 그룹이 있습니다. 서버 팀이 일상적인 서버 유지 관리 작업을 수행하기 위해 서버를 종료하고 시작해야 하는 경우 서버에 대한 권한을 담당자에게 부여해야 합니다. 다른 사용자에게 SAP BusinessObjects Business Intelligence 플랫폼 서버 관리 작업을 위임할 수도 있습니다. 또는 조직 내의 각기 다른 그룹이 자신의 서버 관리를 개별적으로 담당하도록 만들 수 있습니다.

8.1.9.4.1 서버 또는 서버 그룹에 대한 액세스를 허용하려면

1. CMC의 서버 관리 영역으로 이동합니다.
2. 액세스 권한을 부여할 서버 또는 서버 그룹을 마우스 오른쪽 단추로 클릭하고 사용자 보안을 선택합니다.
3. 선택된 서버 또는 서버 그룹에 대한 액세스 권한을 부여할 사용자나 그룹을 추가하려면 보안 주체 추가를 클릭합니다.
보안 주체 추가 대화 상자가 나타납니다.
4. 지정된 서버 또는 서버 그룹에 대한 액세스 권한을 부여할 사용자나 그룹을 선택한 다음 >를 클릭합니다.
5. 보안 추가 및 할당을 클릭합니다.
6. 보안 할당 화면에서 사용자 또는 그룹에 사용할 보안 설정을 선택하고 확인을 클릭합니다.
권한 할당에 대한 자세한 내용은 권한 설정 장을 참조하십시오.

8.1.9.4.2 Report Application Server에 대한 개체 권한

사용자가 RAS(Report Application Server)를 통해 웹에서 보고서를 만들거나 수정할 수 있도록 하려면 시스템에 사용 가능한 RAS Report Modification 라이선스가 있어야 합니다. 사용자에게 최소한의 개체 권한 집합도 부여해야 합니다. 보고서 개체에 대한 이러한 권한을 사용자에게 부여하면 사용자가 직접 보고서를 수정하거나 새 보고서의 데이터 소스로 사용할 보고서를 선택할 수 있습니다.

- 개체 보기(또는 필요한 경우 문서 인스턴스 보기)

- 개체 편집
- 보고서 데이터 새로 고침
- 보고서 데이터 내보내기

또한, 사용자가 새 보고서를 SAP BusinessObjects Business Intelligence 플랫폼에 다시 저장하려면 적어도 하나 이상의 폴더에 개체를 추가하는 데 필요한 권한이 사용자에게 있어야 합니다.

사용자가 복사, 일정, 인쇄 등과 같은 추가적인 보고서 작성 작업을 수행하는 데 필요한 권한을 유지하도록 하려면 먼저 적절한 액세스 수준을 할당하고 변경 사항을 업데이트하는 것이 좋습니다. 그런 다음 액세스 수준을 고급으로 변경하고 아직 부여되지 않은 필수 권한을 추가합니다. 예를 들어, 보고서 개체에 대한 요청 시 보기 권한이 이미 사용자에게 있는 경우 액세스 수준을 고급으로 변경하고 명시적인 개체 편집 권한을 추가로 부여하여 사용자가 보고서를 수정할 수 있도록 합니다.

사용자가 고급 DHTML 뷰어 및 RAS를 통해 보고서를 보는 경우, 보고서를 표시하는 데는 보기 액세스 수준으로도 충분하지만 고급 검색 기능을 실제로 사용하려면 요청 시 보기 액세스 수준이 필요합니다. 추가적인 개체 편집 권한은 필요하지 않습니다.

8.1.10 시스템 성능 평가

8.1.10.1 SAP BusinessObjects Business Intelligence 플랫폼 서버 모니터링

모니터링 응용 프로그램은 보고 및 알림을 위해 SAP BusinessObjects Business Intelligence 플랫폼 서버의 런타임 및 기록 메트릭을 캡처할 수 있는 기능을 제공합니다. 따라서 시스템 관리자가 서버가 정상적으로 작동하는지 여부와 응답 시간이 예상대로 작동하는지 여부를 식별할 수 있습니다.

관련 항목

- 537 페이지에서 [모니터링 정보](#)

8.1.10.2 서버 메트릭 분석

중앙 관리 콘솔(CMC)에서는 시스템의 여러 서버에 대한 메트릭을 확인할 수 있습니다. 이러한 메트릭에는 서버 유형별 세부 정보를 비롯하여 각 컴퓨터에 대한 일반 정보가 포함됩니다. CMC를 사용하면 시스템 메트릭을 볼 수도 있습니다. 여기에는 사용자의 제품 버전, CMS 및 현재 시스템 작업에 대한 정보가 포함됩니다.

참고:

현재 실행 중인 서버에 대한 메트릭만 확인할 수 있습니다.

8.1.10.2.1 서버 메트릭 보기

1. CMC의 서버 관리 영역으로 이동합니다.
2. 보려는 메트릭을 가진 서버를 마우스 오른쪽 단추로 클릭하고 메트릭을 선택합니다.

메트릭 탭에는 서버의 메트릭 목록이 표시됩니다.

관련 항목

- 387 페이지에서 [서버 속성 변경](#)"
- 861 페이지에서 [서버 메트릭 부록 정보](#)"

8.1.10.3 시스템 메트릭 보기

CMC의 설정 관리 영역에는 SAP BusinessObjects Business Intelligence 플랫폼 설치에 관련된 일반 정보를 제공하는 시스템 메트릭이 표시됩니다. 속성 섹션에는 제품 버전과 빌드에 대한 정보가 표시됩니다. 여기에는 CMS 데이터베이스의 데이터베이스 사용자 이름, 데이터베이스 이름 및 데이터 소스도 나열됩니다. 전역 시스템 메트릭 보기 섹션에는 현재 계정 작업이 현재 작업 및 처리된 작업에 대한 통계와 함께 나열됩니다. 클러스터 섹션에는 현재 연결된 CMS의 이름, CMS 클러스터의 이름 및 다른 클러스터 멤버의 이름이 나열됩니다.

8.1.10.3.1 시스템 메트릭 보기

1. CMC의 설정 관리 영역으로 이동합니다.
2. 속성, 전역 시스템 메트릭 보기 및 클러스터 섹션을 확장하고 그 설정을 보려면 화살표를 클릭하십시오.

8.1.10.4 서버 작업 로깅

SAP BusinessObjects Business Intelligence 플랫폼을 통해 SAP BusinessObjects Business Intelligence 플랫폼 웹 작업에 대한 특정 정보를 기록할 수 있습니다.

- 또한 각 SAP BusinessObjects Business Intelligence 플랫폼 서버는 운영 체제의 표준 시스템 로그에 메시지를 기록하도록 디자인되어 있습니다.
- Windows의 경우 SAP BusinessObjects Business Intelligence 플랫폼은 이벤트 로그 서비스에 메시지를 기록합니다. 응용 프로그램 로그의 이벤트 뷰어를 사용하여 결과를 볼 수 있습니다.
- UNIX의 경우 SAP BusinessObjects Business Intelligence 플랫폼은 사용자 응용 프로그램으로서의 syslog 데몬에 메시지를 기록합니다. 각 서버는 기록하는 모든 메시지에 서버의 이름과 PID를 추가합니다.

각 서버에서는 제품 설치 환경의 로깅 디렉터리에 어설션 메시지도 기록합니다. 이러한 파일에 기록되는 프로그램 정보는 일반적으로 SAP Business Objects 지원 담당자가 전문 디버깅 작업을 수행하는 경우에만 필요합니다. 이러한 로그 파일의 위치는 운영 체제에 따라 다릅니다.

- Windows에서는 기본 로깅 디렉터리가 <INSTALLDIR>WSAP BusinessObjects Enterprise XI 4.0WLogging입니다.
- UNIX의 경우 기본 로깅 디렉터리는 설치 제품의 <INSTALLDIR>/sap_bobj/logging 디렉터리입니다.

이러한 로그 파일은 자동으로 정리되므로 서버별로 최대 약 1MB의 데이터만 유지된다는 점에 유의해야 합니다.

참고:

SAP BusinessObjects Business Intelligence 플랫폼 서버를 호스팅하는 UNIX 컴퓨터에서 로깅 기능을 활성화하려면 정보 수준이나 더 높은 수준의 사용자 기능에 로깅되는 모든 메시지를 기록하도록 시스템 로깅을 설정 및 구성해야 합니다. 또한, 원격 로깅을 허가하도록 SYSLOGD를 구성해야 합니다.

이러한 설정 절차는 시스템마다 다릅니다. 자세한 지침은 운영 체제 설명서를 참조하십시오.

8.1.10.5 CMC에서 서버를 구성하여 게시 성능 최적화

일반적으로 다음과 같은 방법으로 게시 서버 성능을 최적화할 수 있습니다.

- CMC의 서버 영역에서 불필요한 서버를 비활성화합니다. 예를 들어, Crystal 보고서 게시만 실행할 경우 Desktop Intelligence 및 Web Intelligence 서버를 비활성화할 수 있습니다. 그러나 이 작업을 수행하기 전에 비활성화하려는 서버가 시스템의 다른 사용자에게 의해 사용되고 있지 않은지 확인합니다.
- 게시에 사용되는 작업 서버에서 최대 동시 작업을 CPU당 5개로 설정합니다. 이렇게 하려면 서버 영역에서 작업 서버를 선택하고 관리 > 속성을 클릭합니다.

적응 처리 서버에서 기록하는 세부 수준을 변경합니다.

참고:

로그 파일의 세부 수준을 높이면 서버 성능이 저하될 수 있습니다.

로그 파일의 세부 수준에 대해 권장되는 기본 설정은 오류입니다. 그러나 관리자나 게시자는 게시 작업의 진행률을 보다 쉽게 추적할 수 있도록 적응 처리 서버 로그 파일의 세부 수준을 높일 수 있습니다. 이렇게 하려면 서버 영역에서 적응 처리 서버를 선택하고 관리 > 속성을 클릭합니다. 로그 수준 목록에서 정보를 선택합니다. 정보를 선택하면 다음과 같은 세부 사항을 확인할 수 있습니다.

- 게시물이 받는 사람에게 배달되었습니다.
- 받는 사람의 배치가 정상적으로 처리되었습니다.
- 사후 처리 게시 확장이 초기화되었습니다.

적응 처리 서버에서 더 많은 작업을 처리하도록 구성합니다.

다음과 같은 방법으로 적응 처리 서버의 성능을 높일 수 있습니다.

- 여러 게시가 동시에 실행되는 경우 적응 처리 서버의 여러 인스턴스를 만듭니다. 일반적으로 3개의 동시 게시에 대해 적응 처리 서버 인스턴스를 하나씩 만드는 것이 좋습니다.
- 적응 처리 서버의 힙 크기를 늘립니다. 이렇게 하려면 관리 > 속성을 클릭하고 명령줄 매개 변수에 -Xmx1024M을 추가합니다.
- 게시 서비스와 게시 사후 처리 서비스를 적응 처리 서버의 서로 다른 인스턴스에서 실행합니다.

게시자가 감사 및 정리 기능을 사용하려는 경우 CMS에 대한 감사에서 모든 세부 정보가 기록되도록 구성합니다.

게시 볼륨이 큰 경우 게시자가 정리 기능을 사용하여 게시 작업 도중 생성된 불필요한 파일을 삭제하고 서버 공간을 절약하는 것이 좋습니다. 이렇게 하려면 게시 디자인 과정에서 게시자가 대상으로 기본 Enterprise 위치의 선택을 취소합니다.

게시에서 감사 기능이 사용되는 경우 삭제된 파일의 세부 정보도 계속 기록되도록 CMS를 구성하여 이 시나리오를 지원해야 합니다 서버 영역에서 CMS를 선택하고 관리 > 속성을 클릭합니다. 대화 상자가 나타나면 탐색 목록에서 감사 이벤트를 클릭합니다 감사가 활성화됨 및 개체가 삭제됨을 선택합니다.

대상 작업 서버에서 전자 메일 설정이 제대로 구성되어 있는지 확인합니다.

전자 메일이 대상 작업 서버에 대한 대상으로 제대로 구성되어 있지 않기 때문에 전자 메일 대상에 대한 게시가 실패할 수 있습니다. CMC의 서버 영역에서 대상 작업 서버를 두 번 클릭합니다. 속성 대화 상자의 탐색 목록에서 대상을 클릭하여 다음을 확인합니다.

- 전자 메일이 대상으로 추가되었는지 확인합니다.
- 도메인 이름, 호스트 및 포트 필드의 값이 올바른지 확인합니다.
- 받는 사람 필드에 %SI_EMAIL_ADDRESS%가 포함되어 있는지 확인합니다.

대상 작업 서버에서 처리할 수 있는 동시 작업 수를 늘립니다.

기본 BI 플랫폼 위치나 관리되지 않는 디스크 대상으로 게시해야 하며 출력 FRS로 스트라이프 디스크를 사용하는 경우 최대 동시 작업 수를 디스크 수에 5를 곱한 숫자로 설정하는 것이 좋습니다.

게시자가 Crystal 보고서의 동적 받는 사람 소스를 사용하는 경우 RAS(Report Application Server)가 올바르게 구성되어 있어야 합니다.

RAS는 동적 받는 사람 소스에 있는 받는 사람 수와 적어도 동일한 수의 데이터베이스 레코드를 읽도록 구성되어야 합니다. 예를 들어, 100,000명의 받는 사람에 대한 동적 받는 사람 소스를 처리하려면 RAS를 100,000개가 넘는 데이터베이스 레코드를 읽도록 설정해야 합니다.

이 설정을 해결하려면 CMC의 서버 영역에서 RAS를 선택한 후 관리 > 속성으로 이동합니다. 보고서 미리 보기 또는 새로 고침 시 읽을 데이터베이스 레코드의 수 필드에서 값이 올바른지 확인하거나 새 값을 입력합니다.

메모리 부족 오류 해결

고용량 게시를 실행할 때 java.lang.OutOfMemoryError: 새 원시 스레드를 만들 수 없음이라는 오류 메시지가 표시되면 적응 처리 서버 및 게시 서비스에서 스택 메모리가 부족하여 생성되는 게시 스레드 수를 처리할 수 없는 것입니다. 스택 메모리가 Java 힙 공간으로 지정된 경우 이 오류가 발생할 수 있습니다.

적응 처리 서버의 스레드 제한을 설정할 수 있습니다. CMC의 서버 영역에서 적응 처리 서버를 선택한 후 관리 > 속성으로 이동합니다. 명령줄 매개 변수 필드에서 다음 명령줄 매개 변수를 입력합니다.

-Dcom.businessobjects.publisher.threadpool.size=threadlimitnumber

threadlimitnumber를 원하는 스레드 제한으로 바꿉니다.

고용량 게시를 실행할 때 java.lang.OutOfMemoryError: Java 힙 공간이라는 오류 메시지가 표시되면 적응 처리 서버에서 힙 공간이 부족한 것입니다. CMC의 서버 영역에서 적응 처리 서버를 선택한 후

관리 > 속성으로 이동합니다. 명령줄 매개 변수 필드에서 명령줄 매개 변수 -Xmx256m의 숫자를 더 큰 숫자(예: -Xmx1024m)로 변경합니다.

참고:

메모리 부족 오류를 해결하기 위해 적응 처리 서버의 인스턴스를 더 만들어야 하는 경우도 있습니다.

8.1.11 서버 설정 구성

이 단원에서는 SAP BusinessObjects Business Intelligence 플랫폼 서버의 설정을 수정하는 데 관련된 기술적인 내용과 절차를 설명합니다.

이 단원에서 설명하는 설정의 대부분은 사용 중인 하드웨어, 소프트웨어 및 네트워크 구성에 SAP BusinessObjects Business Intelligence 플랫폼을 더욱 효율적으로 통합할 수 있도록 하기 위한 것입니다. 따라서 사용자가 선택할 설정은 고유한 요구 사항에 따라 크게 달라질 수 있습니다.

다음 두 가지 방법으로 중앙 관리 콘솔(CMC)을 통해 서버 설정을 변경할 수 있습니다.

- 서버의 속성 화면
- 서버의 공통 서비스 편집 화면

모든 변경 내용이 즉시 적용되는 것은 아니라는 점을 염두에 둘 필요가 있습니다. 설정이 즉시 변경되지 않는 경우 속성 및 공통 서비스 편집 화면에 현재 설정(빨간색 텍스트)과 필요한 설정이 모두 표시됩니다. 서버 관리 영역으로 돌아가면 서버가 지난으로 표시됩니다. 서버를 다시 시작하면 새로 지정된 설정이 사용되고 서버에서 지난 플래그가 제거됩니다.

참고:

SAP BusinessObjects Business Intelligence 플랫폼 응용 프로그램을 배포하기 위해 웹 응용 프로그램 서버를 구성하는 방법은 이 단원에서 설명하지 않습니다. 이 작업은 일반적으로 제품을 설치할 때 수행합니다. 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 설치 가이드를 참조하십시오.

관련 항목

- 397 페이지에서 [포트 번호 구성](#)"
- 387 페이지에서 [서버 속성 변경](#)"
- 429 페이지에서 [CMS 시스템 데이터베이스 다시 만들기](#)"
- 427 페이지에서 [새 CMS 데이터베이스 또는 기존 CMS 데이터베이스 선택](#)"

8.1.11.1 서버 속성 변경

1. CMC의 서버 관리 영역으로 이동합니다.
2. 설정을 변경할 서버를 두 번 클릭합니다.
속성 화면이 나타납니다.
3. 원하는 내용을 변경하고 저장 또는 저장 후 닫기를 클릭합니다.

참고:

모든 변경 내용이 즉시 적용되는 것은 아닙니다. 설정이 즉시 변경되지 않는 경우 속성 대화 상자에 현재 설정(빨간색 텍스트)과 필요한 설정이 모두 표시됩니다. 서버 관리 영역으로 돌아가면 서버가 지난으로 표시됩니다. 서버를 다시 시작하면 속성 대화 상자에서 새로 지정한 설정이 사용되고 서버에서 지난 플래그가 제거됩니다.

8.1.11.2 여러 서버에 서비스 설정 적용

여러 서버에서 호스팅되는 서비스에 같은 설정을 적용하려면 다음을 수행하십시오.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 변경하려는 설정을 사용하는 서비스를 호스팅하는 서버를 마우스 오른쪽 단추를 클릭한 다음 공통 서비스 편집을 선택합니다.
공통 서비스 편집 대화 상자에 변경하려는 설정을 갖는 선택한 모든 서버가 표시됩니다.
3. 공통 서비스 편집 대화 상자에 여러 개의 서비스가 나열될 경우 편집하려는 서비스를 선택하고 계속을 클릭합니다.
4. 원하는 내용을 변경하고 확인을 클릭합니다.

참고:

CMC의 서버 관리 영역으로 리디렉션됩니다. 서버를 다시 시작해야 할 경우 서버가 지난 상태로 표시됩니다. 서버를 다시 시작하면 새로 지정한 설정이 사용되고 서버에서 오래된 플래그가 제거됩니다.

8.1.11.3 구성 템플릿 작업

구성 템플릿을 사용하면 서버의 여러 인스턴스를 쉽게 구성할 수 있습니다. 구성 템플릿에는 추가 서버 인스턴스를 구성하는 데 사용할 수 있는 각 서비스 유형에 대한 설정 목록이 저장됩니다. 예를 들어 12개의 Web Intelligence 처리 서버를 개별적으로 구성하려는 경우 그 중 하나에 대해서만 설정을 구성하면 됩니다. 그런 다음 이렇게 구성된 서비스를 사용하여 Web Intelligence 처리 서버에 대한 구성 템플릿을 정의하고 이 템플릿을 나머지 11개의 서비스 인스턴스에 적용할 수 있습니다.

SAP BusinessObjects Business Intelligence 플랫폼 서비스의 각 유형에는 고유한 구성 템플릿이 있습니다. 예를 들어 Web Intelligence 처리 서비스 유형에 대한 구성 템플릿, 게시 서비스 유형에 대한 구성 템플릿 등이 각각 하나씩 있습니다. 구성 템플릿은 중앙 관리 콘솔(CMC)의 서버 속성에서 정의합니다.

서버가 구성 템플릿을 사용하도록 할 경우 템플릿의 값이 서버의 기존 설정을 덮어씁니다. 나중에 이 템플릿 사용을 중단하기로 결정해도 원래 설정이 복원되지 않습니다. 이후 구성 템플릿에 적용된 변경 사항은 더 이상 서버에 영향을 주지 않습니다.

구성 템플릿을 사용할 때는 다음 지침을 따르는 것이 좋습니다.

1. 서버 하나에 대해 구성 템플릿을 설정합니다.
2. 유형이 같은 모든 서버에 대해 동일한 구성을 사용하려는 경우 구성 템플릿을 설정한 서버를 포함하여 유형이 같은 모든 서버에 대해 구성 템플릿 사용을 선택합니다.
3. 나중에 이 유형의 서비스 전체에 대해 구성을 변경하려면 서비스 중 하나의 속성을 표시하고 구성 템플릿 사용 확인란의 선택을 취소합니다. 설정을 원하는 대로 변경한 다음 해당 서버에 대해 구성 템플릿 설정을 선택하고 저장을 클릭합니다. 해당 유형의 서비스가 모두 업데이트됩니다. 서버가 항상 구성 템플릿으로 설정되지 않도록 하면 해당 유형의 서버 전체에 대해 구성 설정을 실수로 변경하는 경우를 방지할 수 있습니다.

관련 항목

- 389 페이지에서 [구성 템플릿 설정](#)
- 390 페이지에서 [서버에 구성 템플릿 적용](#)

8.1.11.3.1 구성 템플릿 설정

각 서비스 유형에 대해 구성 템플릿을 설정할 수 있습니다. 한 서비스에 대해 여러 구성 템플릿을 설정할 수는 없습니다. 서버의 속성 페이지를 사용하여 해당 서버에 호스팅된 서비스 유형에 대한 구성 템플릿에서 사용할 설정을 구성할 수 있습니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 구성 템플릿을 설정할 서비스를 호스팅하는 서버를 두 번 클릭합니다.
속성 화면이 나타납니다.
3. 템플릿에 사용할 서비스 설정을 구성하고 구성 템플릿 설정 확인란을 선택한 다음 저장 또는 저장 후 닫기를 클릭합니다.

선택한 서비스 유형에 대한 구성 템플릿이 현재 서버의 설정에 따라 정의됩니다. 동일한 서비스를 호스팅하는 동일한 유형의 다른 서버에 대해 속성에서 구성 템플릿 사용 옵션을 활성화한 경우 이러한 서버가 구성 템플릿에 일치하도록 자동으로 즉시 다시 구성됩니다.

참고:

구성 템플릿의 설정을 명시적으로 정의하지 않은 경우 서비스의 기본 설정이 사용됩니다.

관련 항목

- 390 페이지에서 [서버에 구성 템플릿 적용](#)"

8.1.11.3.2 서버에 구성 템플릿 적용

구성 템플릿을 적용하려면 먼저 템플릿을 적용하려는 서버 유형에 대해 구성 템플릿 설정을 정의해야 합니다. 구성 템플릿 설정을 명시적으로 정의하지 않은 경우 서비스의 기본 설정이 사용됩니다.

참고:

구성 템플릿 사용 설정을 활성화하지 않은 서버는 구성 템플릿의 설정을 수정해도 업데이트되지 않습니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 구성 템플릿을 적용할 서비스를 호스팅하는 서버를 두 번 클릭합니다.
속성 화면이 나타납니다.
3. 구성 템플릿 사용 확인란을 선택하고 저장 또는 저장 후 단기를 클릭합니다.

참고:

새 설정을 적용하기 위해 서버를 다시 시작해야 하는 경우 서버 목록에 해당 서버가 "지난"으로 표시됩니다.

적절한 구성 템플릿이 현재 서버에 적용됩니다. 이후 구성 템플릿을 변경하면 이 구성 템플릿을 사용하는 모든 서버의 구성이 변경됩니다.

구성 템플릿 사용 선택을 취소하면 구성 템플릿을 적용했을 당시의 값으로 서버 구성이 복원되지 않습니다. 이후 구성 템플릿에 적용된 변경 사항은 구성 템플릿을 사용하고 있는 서버 구성에 영향을 주지 않습니다.

관련 항목

- 389 페이지에서 [구성 템플릿 설정](#)"

8.1.11.3.3 시스템 기본값 복원

서비스의 구성을 처음 설치할 때의 설정으로 되돌려야 할 수도 있습니다. 서버를 잘못 구성했거나 성능에 문제가 있는 경우 등을 예로 들 수 있습니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 시스템 기본값을 복원할 서비스를 호스팅하는 서버를 두 번 클릭합니다.
속성 화면이 나타납니다.
3. 시스템 기본값 복원 확인란을 선택하고 저장 또는 저장 후 닫기를 클릭합니다.
특정 서비스 유형의 기본 설정이 복원됩니다.

8.1.12 서버 네트워크 설정 구성

SAP BusinessObjects Business Intelligence 플랫폼 서버에 대한 네트워크 설정은 CMC를 통해 관리됩니다. 이러한 설정은 포트 설정 및 호스트 ID라는 두 가지 범주로 구성됩니다.

기본 설정

설치 중에 서버 호스트 ID는 자동 할당으로 설정됩니다. 그러나 각 서버에 특정 IP 주소나 호스트 이름을 할당할 수도 있습니다. 기본 CMS 포트 번호는 6400입니다. 기타 SAP BusinessObjects Business Intelligence 플랫폼 서버는 사용 가능한 포트에 동적으로 바인딩됩니다. 포트 번호는 SAP BusinessObjects Business Intelligence 플랫폼에서 자동으로 관리하지만 CMC를 사용하여 포트 번호를 지정할 수도 있습니다.

8.1.12.1 네트워크 환경 옵션

SAP BusinessObjects Business Intelligence 플랫폼은 IPv 6(Internet Protocol version 6) 및 IPv 4(Internet Protocol version 4) 네트워크 트래픽을 모두 지원합니다. 다음과 같은 환경에서 서버 및 클라이언트 구성 요소를 사용할 수 있습니다.

- IPv4 네트워크: IPv4 프로토콜로만 실행되는 모든 서버 및 클라이언트 구성 요소
- IPv6 네트워크: IPv6 프로토콜로만 실행되는 모든 서버 및 클라이언트 구성 요소
- 혼합형 IPv6/IPv4 네트워크: IPv6와 IPv4 프로토콜로 실행되는 모든 서버 및 클라이언트 구성 요소

참고:

시스템 및 네트워크 관리자만 네트워크 구성을 수행해야 합니다. SAP BusinessObjects Business Intelligence 플랫폼은 네트워크 환경을 지정할 수 있는 메커니즘을 제공하지 않습니다. CMC를 사용하여 SAP BusinessObjects Business Intelligence 플랫폼 서버에 대해 특정 IPv6 또는 IPv4 주소를 바인딩할 수 있습니다.

8.1.12.1.1 혼합형 IPv6/IPv4 환경

IPv6/IPv4 네트워크 환경에서 가능한 사항은 다음과 같습니다.

- SAP BusinessObjects Business Intelligence 플랫폼 서버에서 혼합형 IPv6/IPv4 모드를 실행할 경우 IPv6 및 IPv4 요청을 둘 다 처리할 수 있습니다.
- 클라이언트 구성 요소는 IPv6 전용 노드, IPv4 전용 노드 또는 IPv6/IPv4 노드에서 서버와 상호 운용이 가능합니다.

혼합형 모드는 다음 환경에서 특히 유용합니다.

- IPv4 전용 노드에서 IPv6 전용 노드 환경으로 전환하는 경우 모든 클라이언트 및 서버 구성 요소는 전환이 완료될 때까지 계속해서 원활하게 상호 운용됩니다. 그 다음 모든 서버에 대한 IPv4 설정을 비활성화할 수 있습니다.
- IPv6가 호환되지 않는 타사 소프트웨어도 IPv6/IPv4 노드 환경에서 정상적으로 작동합니다.

참고:

Windows 2003에서 IPv6 전용 노드를 사용하는 경우 DNS 이름이 올바르게 확인되지 않습니다. Windows 2003에서 IPv4 스택이 비활성화된 경우 IPv6/IPv4로 실행되어야 합니다.

8.1.12.2 서버 호스트 ID 옵션

호스트 ID 옵션을 각 SAP BusinessObjects Business Intelligence 플랫폼 서버의 CMC에 지정할 수 있습니다. 다음 표에서는 일반 설정 영역에서 사용할 수 있는 옵션이 요약되어 있습니다.

옵션	설명
자동 할당	모든 서버의 기본 설정입니다. 자동 할당을 선택하면 서버가 서버의 요청 포트를 컴퓨터의 첫 번째 네트워크 인터페이스로 자동 바인딩합니다. 참고: 호스트 이름 설정에 대해 자동 할당 확인란을 선택하는 것이 좋습니다. 그러나 서버가 다중 홈 컴퓨터에서 실행되는 경우나 서버가 특정 방화벽 구성과 상호 연동되어야 하는 경우 등 일부 특수한 경우에는 특정 호스트 이름이나 IP 주소를 고려해야 합니다. 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드의 멀티홈 컴퓨터 구성 및 방화벽을 사용한 작업 장을 참조하십시오.
호스트 이름	서버가 요청을 수신하는 데 사용할 네트워크 인터페이스의 호스트 이름을 지정합니다. CMS의 경우, CMS에서 이름 서버 포트와 요청한 포트를 바인딩하는 네트워크 인터페이스의 호스트 이름을 지정합니다.
IP 주소	서버가 요청을 수신하는 데 사용할 네트워크 인터페이스의 IP 주소를 지정합니다. CMS의 경우 이 설정은 CMS에서 이름 서버 포트와 요청한 포트를 바인딩하는 네트워크 인터페이스의 주소를 지정합니다. 각 서버에 대해 IPv4 및/또는 IPv6 IP 주소를 지정할 수 있는 별도의 필드가 제공됩니다.

주의:

중요: 멀티홈 컴퓨터에서 자동 할당을 지정하면 CMS가 잘못된 네트워크 인터페이스에 자동 바인딩될 수 있습니다. 이러한 문제가 발생하지 않게 하려면 호스트 컴퓨터에서 OS 도구를 사용하여 네트워크 인터페이스가 올바른 순서로 나열되는지 확인합니다. 또한 CMC에서 CMS의 호스트 이름 설정을 지정해야 합니다.

참고:

다중 홈 컴퓨터에서 작업하거나 특정 NAT 방화벽이 구성되어 있는 경우에는 호스트 이름 대신 정규화된 도메인 이름을 사용하여 호스트 이름을 지정해야 할 수도 있습니다.

관련 항목

- 394 페이지에서 [다중 홈 컴퓨터 구성](#)"
- 396 페이지에서 [다중 네트워크 인터페이스 관련 문제를 해결하려면](#)"

8.1.12.2.1 서버의 호스트 ID를 수정하려면

1. CMC의 서버 관리 영역으로 이동합니다.
2. 서버를 선택한 다음 작업 메뉴에서 서버 중지를 선택합니다.
3. 관리 메뉴에서 속성을 선택합니다.
4. 일반 설정에서 다음 옵션 중 하나를 선택합니다.

옵션	설명
자동 할당	서버는 사용 가능한 네트워크 인터페이스 중 하나에 바인딩됩니다.
호스트 이름	서버가 요청을 수신할 네트워크 인터페이스의 호스트 이름을 입력합니다.
IP 주소	서버가 요청을 수신할 네트워크 인터페이스의 IPv4 또는 IPv6 IP 주소를 제공된 필드에 입력합니다. 참고: 서버가 이중 IPv4/IPv6 노드로 작동하도록 하려면 두 필드에 유효한 IP 주소를 입력합니다.

5. 저장 또는 저장 후 닫기를 클릭합니다.
속성 탭에 표시되는 명령줄에 변경 내용이 반영됩니다.
6. 서버를 시작하고 활성화합니다.

8.1.12.3 다중 홈 컴퓨터 구성

다중 홈 컴퓨터는 다중 네트워크 주소를 가진 컴퓨터입니다. 이러한 환경은 각각 하나 이상의 IP 주소가 있는 다중 네트워크 인터페이스를 사용하거나 여러 IP 주소가 할당된 단일 네트워크 인터페이스를 사용하여 설정할 수 있습니다.

각각 하나의 IP 주소가 할당된 여러 네트워크 인터페이스를 사용하는 경우 SAP BusinessObjects Business Intelligence 플랫폼 서버를 바인딩할 네트워크 인터페이스가 맨 위에 나오도록 바인딩 순서를 변경합니다. 인터페이스에 여러 IP 주소가 있는 경우 CMC에서 호스트 이름 옵션을 사용하여 SAP BusinessObjects Business Intelligence 플랫폼 서버에 사용할 네트워크 인터페이스 카드를 지정합니다. 이를 지정하는 데 호스트 이름이나 IP 주소를 사용할 수 있습니다. 호스트 이름 설정을 구성하는 방법은 여러 NIC 문제 해결을 참조하십시오.

팁:

이 단원에서는 모든 서버를 동일한 네트워크 주소로 제한하는 방법을 보여 줍니다. 물론, 개별 서버를 서로 다른 주소에 바인딩할 수도 있습니다. 예를 들어, 파일 리포지토리 서버를 사용자의 컴퓨터에서

라우팅할 수 없는 개인 주소에 바인딩할 수도 있습니다. 이와 같은 고급 구성을 위해서는 모든 SAP BusinessObjects Business Intelligence 플랫폼 서버 구성 요소 사이에 통신을 효율적으로 라우팅하기 위한 DNS 구성이 필요합니다. 이 예제의 경우 DNS는 다른 SAP BusinessObjects Business Intelligence 플랫폼 서버에서 파일 리포지토리 서버의 개인 주소로 통신을 라우팅해야 합니다.

관련 항목

- 396 페이지에서 [다중 네트워크 인터페이스 관련 문제를 해결하려면](#)

8.1.12.3.1 네트워크 주소에 바인딩할 CMS를 구성하려면

참고:

멀티홈 컴퓨터에서는 서버를 바인딩할 인터페이스의 정규화된 도메인 이름이나 IP 주소로 호스트 ID를 설정할 수 있습니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. CMS를 두 번 클릭합니다.
3. 일반 설정에서 다음 옵션 중 하나를 선택합니다.
 - 호스트 이름
 - 서버가 바인딩할 네트워크 인터페이스의 호스트 이름을 입력합니다.
 - IP 주소
 - 서버가 바인딩할 네트워크 인터페이스의 IPv4 또는 IPv6 IP 주소를 해당 필드에 입력합니다.

참고:

서버가 이중 IPv4/IPv6 노드로 작동하도록 하려면 두 필드에 유효한 IP 주소를 입력합니다.

주의:

자동 할당을 선택하지 마십시오.

4. 요청 포트에 대해 다음 중 하나를 수행할 수 있습니다.
 - 자동 할당 옵션을 선택합니다.
 - 요청 포트 필드에 유효한 포트 번호를 입력합니다.
5. 포트 번호가 이름 서버 포트 대화 상자에 지정되어 있어야 합니다.

참고:

기본 포트 번호는 6400입니다.

8.1.12.3.2 네트워크 주소에 바인딩할 나머지 서버 구성

기본적으로 나머지 SAP BusinessObjects Business Intelligence 플랫폼 서버의 포트는 동적으로 선택됩니다. 이 정보를 동적으로 전파하는 자동 할당 설정을 해제하는 방법은 요청 수락을 위해 서버에 사용되는 포트 변경을 참조하십시오.

관련 항목

- 400 페이지에서 [요청 수락을 위해 서버에 사용되는 포트 변경](#)

8.1.12.3.3 다중 네트워크 인터페이스 관련 문제를 해결하려면

다중 홈 컴퓨터에서는 CMS가 잘못된 네트워크 인터페이스에 자동 바인딩될 수 있습니다. 이 문제를 방지하려면 컴퓨터의 OS 도구를 사용하여 호스트 컴퓨터의 네트워크 인터페이스를 올바른 순서대로 나열하거나 CMC에서 CMS의 호스트 이름 설정을 지정합니다. 기본 네트워크 인터페이스를 라우팅할 수 없는 경우 다음 절차에 따라 BI 플랫폼을 구성하여 라우팅 가능한 보조 네트워크 인터페이스에 바인딩할 수 있습니다. 이 단계는 로컬 컴퓨터에 BI 플랫폼을 설치한 직후 다른 컴퓨터에 해당 플랫폼을 설치하기 전에 수행해야 합니다.

1. CCM을 열고 네트워크 인터페이스가 여러 개인 컴퓨터의 노드에 대한 SIA를 중지합니다.
2. SIA를 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.
3. 속성 대화 상자에서 구성 탭을 클릭합니다.
4. SIA를 특정 네트워크 인터페이스에 바인딩하려면 포트 필드에 다음 중 하나를 입력합니다.
 - 대상 네트워크 인터페이스의 호스트 이름과 포트 번호이며 호스트 이름:포트 번호 형식을 사용합니다.
 - 대상 네트워크 인터페이스의 IP 주소와 포트 번호이며 IP 주소:포트 번호 형식을 사용합니다.
5. 확인을 클릭하고 시작 탭을 선택합니다.
6. 로컬 CMS 서버 목록에서 CMS를 선택하고 속성을 클릭합니다.
7. CMS를 특정 네트워크 인터페이스에 바인딩하려면 포트 필드에 다음 중 하나를 입력합니다.
 - 대상 네트워크 인터페이스의 호스트 이름과 포트 번호이며 호스트 이름:포트 번호 형식을 사용합니다.
 - 대상 네트워크 인터페이스의 IP 주소와 포트 번호이며 IP 주소:포트 번호 형식을 사용합니다.

8. 확인을 클릭하여 새 설정을 적용합니다.
9. SIA를 시작하고 서버가 시작될 때까지 기다립니다.
10. 중앙 관리 콘솔(CMC)을 실행하고 서버 관리 영역으로 이동합니다. 각 서버에 대해 11~14단계를 반복합니다.
11. 서버를 선택한 다음 작업 메뉴에서 서버 중지를 선택합니다.
12. 관리 메뉴에서 속성을 선택합니다.
13. 일반 설정에서 다음 옵션 중 하나를 선택합니다.
 - 호스트 이름: 서버가 바인딩할 네트워크 인터페이스의 호스트 이름을 입력합니다.
 - IP 주소: 서버가 바인딩할 네트워크 인터페이스의 IPv4 또는 IPv6 IP 주소를 해당 필드에 입력합니다.

참고:

서버가 이중 IPv4/IPv6 노드로 작동하도록 하려면 두 필드에 유효한 IP 주소를 입력합니다.

주의:

자동 할당을 선택하지 마십시오.

14. 저장 또는 저장 후 단기를 클릭합니다.
15. CCM으로 돌아가 SIA를 다시 시작합니다.

SIA를 통해 노드의 모든 서버가 다시 시작됩니다. 이제 컴퓨터의 모든 서버가 올바른 네트워크 인터페이스에 바인딩됩니다.

8.1.12.4 포트 번호 구성

설치 과정에서 CMS는 기본 포트 번호를 사용하도록 설정됩니다. 기본 CMS 포트 번호는 6400입니다. 이 포트는 SAP Business Objects에 예약된 포트 범위(6400-6410) 내에 있습니다. 이러한 포트를 사용한 통신은 타사 응용 프로그램과 충돌하지 않아야 합니다.

나머지 SAP BusinessObjects Business Intelligence 플랫폼 서버는 시작되어 활성화될 때 각각 1024보다 큰 가용 포트에 동적으로 바인딩되고, CMS에서 포트를 등록한 다음 이 포트에서 SAP BusinessObjects Business Intelligence 플랫폼 요청을 수신합니다. 필요한 경우 동적으로 빈 포트를 선택하는 것이 아니라 각 서버 구성 요소가 특정 포트에서 수신하도록 지정할 수도 있습니다.

CMC에서 각 서버의 속성 탭을 사용하여 포트 번호를 지정할 수 있습니다. 다음 표에는 일반 설정 영역에서 서버 유형별로 포트 사용과 관련된 옵션이 요약되어 있습니다.

설정	CMS	기타 서버
요청 포트	이름 서버 요청을 제외하고 다른 서버의 모든 요청을 받기 위해 CMS에서 사용하는 포트를 지정합니다. 이름 서버 포트와 동일한 네트워크 인터페이스를 사용합니다. 자동 할당을 선택하면 OS를 통해 할당된 포트 번호가 서버에 자동으로 사용됩니다.	서버에서 모든 요청을 수신할 포트를 지정합니다. 자동 할당을 선택하면 OS를 통해 할당된 포트 번호가 서버에 자동으로 사용됩니다.
이름 서버 포트	CMS에서 이름 서비스 요청을 수신할 SAP BusinessObjects Business Intelligence 플랫폼 포트를 지정합니다. 기본값은 6400입니다.	해당 없음

8.1.12.4.1 CMC에서 기본 MCS 포트 변경

클러스터에서 이미 실행되고 있는 CMS가 있으면 CMC를 사용하여 기본 CMS 포트 번호를 변경할 수 있습니다. 클러스터에서 실행되고 있는 CMS가 없으면 CCM(Windows) 또는 serverconfig.sh 스크립트(UNIX)를 사용하여 포트 번호를 변경해야 합니다.

참고:

CMS에서는 요청 포트 및 이름 서버 포트에 대해 동일한 네트워크 인터페이스 카드를 사용합니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 서버 목록에서 CMS를 두 번 클릭합니다.
3. 이름 서버 포트 번호를 CMS에서 수신에 사용할 포트 번호로 바꿉니다. 기본 포트는 6400입니다.
4. 저장 후 닫기를 클릭합니다.
5. CMS를 다시 시작합니다.

지정된 포트 번호를 사용하여 CMS에서 수신이 시작됩니다. 노드의 다른 서버에서 요청 포트에 대한 자동 할당 옵션이 선택되어 있으면 Server Intelligence Agent가 해당 서버에 새 설정을 동적으로 전파합니다. 모든 노드 구성원의 속성 설정에 변경 내용을 표시하는 데는 수 분이 걸릴 수 있습니다.

속성 페이지에서 선택한 설정은 서버 명령줄에 적용되고, 속성 페이지에도 표시됩니다.

8.1.12.4.2 CCM에서 기본 CMS 포트 변경(Windows)

클러스터에 액세스할 수 있는 CMS가 없어서 배포에 있는 하나 이상의 CMS에 대한 기본 CMS 포트를 수정하려는 경우, CCM을 사용하여 CMS 포트 번호를 변경해야 합니다.

1. CCM을 열고 노드에 대한 SIA를 중지합니다.
2. SIA를 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.
3. 속성 대화 상자에서 시작 탭을 클릭합니다.
4. 로컬 CMS 서버 목록에서 포트 번호를 변경하려는 CMS를 선택하고 속성을 클릭합니다.
5. CMS를 특정 포트에 바인딩하려면 포트 필드에 다음 중 하나를 입력합니다.
 - 포트 번호
 - 호스트 이름 및 포트 번호(호스트 이름:포트 번호 형식 사용)
 - IP 주소 및 포트 번호(IP 주소:포트 번호 형식 사용)
6. 확인을 클릭하여 새 설정을 적용합니다.
7. SIA를 시작하고 서버가 시작될 때까지 기다립니다.

8.1.12.4.3 CCM에서 기본 CMS 포트 변경(UNIX)

클러스터에 액세스할 수 있는 CMS가 없어서 배포에 있는 하나 이상의 CMS에 대한 기본 CMS 포트를 수정하려는 경우, `serverconfig.sh` 스크립트를 사용하여 CMS 포트 번호를 변경해야 합니다.

1. `ccm.sh` 스크립트를 사용하여 포트 번호를 변경하려는 CMS를 호스팅하는 SIA(Server Intelligence Agent)를 중지합니다.
2. `serverconfig.sh` 스크립트를 실행합니다. 기본적으로 이 스크립트는 `<InstallDir>/sap_bobj` 디렉터리에 있습니다.
3. 3 - Server Intelligence Agent 수정을 선택하고 Enter 키를 누릅니다.
4. 수정하려는 CMS를 호스팅하는 SIA를 선택하고 Enter 키를 누릅니다.
5. 4 - 서버 수정을 선택하고 Enter 키를 누릅니다.
SIA에서 현재 호스트되는 CMS 목록이 표시됩니다.
6. 수정하려는 CMS를 선택하고 Enter 키를 누릅니다.
7. CMS에 대한 새 포트 번호를 입력하고 Enter 키를 누릅니다.

8. SIA가 시작될 때 CMS가 자동으로 시작되도록 할지 여부를 지정하고 Enter 키를 누릅니다.
9. CMS에 대한 명령줄 인수를 입력하거나 현재 인수를 그대로 사용하고 Enter 키를 누릅니다.
10. ccm.sh 스크립트로 SIA를 시작한 다음 서버가 시작될 때까지 기다립니다.

8.1.12.4.4 요청 수락을 위해 서버에 사용되는 포트 변경

1. CMC의 서버 관리 영역으로 이동합니다.
2. 서버를 선택한 다음 작업 메뉴에서 서버 중지를 선택합니다.
3. 서버를 두 번 클릭합니다.
속성 화면이 나타납니다.
4. 일반 설정에서 요청 포트에 대한 자동 할당 확인란의 선택을 취소한 다음 서버의 수신에 사용할 포트 번호를 입력합니다.
5. 저장 또는 저장 후 단기를 클릭합니다.
6. 서버를 시작하고 활성화합니다.

서버가 새 포트에 바인딩되고 CMS에 등록된 다음 새 포트에서 SAP BusinessObjects Business Intelligence 플랫폼 요청을 수신하기 시작합니다.

8.1.13 노드 관리

8.1.13.1 노드 사용

노드는 동일한 호스트에서 실행되는 BI 플랫폼 서버 그룹입니다. 노드의 모든 서버는 동일한 사용자 계정으로 실행됩니다.

한 컴퓨터에 여러 개의 노드가 포함될 수 있으므로 다른 사용자 계정으로 프로세스를 실행할 수 있습니다.

한 개의 SIA(Server Intelligence Agent)가 노드에 있는 모든 서버를 관리하고 모니터링하여 이러한 서버가 올바르게 작동되도록 합니다.

참고:

모든 노드 관리 프로시저를 안전하게 수행하려면 Enterprise 인증을 통해 관리자 계정을 사용해야 합니다. 하지만, 서버 간에 SSL 통신이 사용되는 경우 노드 관리 절차를 수행하려면 SSL을 비활성화해야 합니다. 자세한 내용은 SSL을 위한 서버 구성 단원을 참조하십시오.

8.1.13.1.1 변수

여기에서는 다음 변수에 대해 설명합니다.

변수	설명
<INSTALLDIR>	BI 플랫폼이 설치된 디렉터리입니다. Windows 컴퓨터의 경우 C:\Program Files (x86)\WSAP BusinessObjects입니다.
<SCRIPTDIR>	노드 관리 스크립트가 있는 디렉터리입니다. Windows 컴퓨터의 경우 <INSTALLDIR>\WSAP BusinessObjects Business Intelligence platform 4.0\win64_x64\scripts입니다. UNIX 컴퓨터의 경우 <INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/scripts입니다.
<PLATFORM>	UNIX 운영 체제의 이름입니다. 허용되는 값은 다음과 같습니다. <ul style="list-style-type: none"> • aix_rs6000_64 • linux_x64 • solaris_sparcv9 • hpux_ia64

8.1.13.2 새 노드 추가

처음 BI 플랫폼을 설치할 때 설치 프로그램에서 노드를 만듭니다.

클러스터의 성능 향상을 위해 기존 클러스터에 새 컴퓨터를 추가하려는 경우 또는 기존 배포가 있는 다른 사용자 계정에서 서버를 실행하려는 경우 추가 서버가 필요할 수 있습니다.

새 노드를 추가할 때 중앙 구성 관리자(CCM) 또는 노드 관리 스크립트를 사용할 수 있습니다. 방화벽을 사용하는 경우 SIA(Server Intelligence Agent) 및 중앙 관리 서버(CMS)의 포트가 열려 있는지 확인합니다.

기억:

노드가 있는 컴퓨터에서만 노드를 추가할 수 있습니다.

8.1.13.2.1 기존 배포의 새 컴퓨터에 노드 추가

설치 프로그램을 사용하여 기존 배포에 새 컴퓨터를 추가하는 경우 첫 번째 노드는 컴퓨터에 자동으로 만들어집니다.

팁:

설치 중에는 펼치기를 클릭하여 기존 중앙 관리 서버를 지정하십시오.

추가 노드를 만들려면 중앙 구성 관리자 또는 스크립트를 사용하십시오.

설치에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 설치 가이드를 참조하십시오.

8.1.13.2.2 Windows에서 노드 추가

주의:

노드를 추가하기 전이나 추가한 후에는 전체 클러스터에 대한 서버 구성을 백업하십시오.

1. 중앙 구성 관리자(CCM)의 도구 모음에서 노드 추가를 클릭합니다.

2. 노드 추가 마법사에서 새 SIA(Server Intelligence Agent)의 노드 이름과 포트 번호를 입력합니다.

3. 새 노드에 서버를 만들지 여부를 선택합니다.

- 서버가 없는 노드 추가
- CMS가 있는 노드 추가
- 기본 서버가 있는 노드 추가

이 옵션은 이 컴퓨터에 설치된 서버만 만듭니다. 즉, 가능한 서버 중 일부만 포함됩니다.

4. CMS를 선택합니다.

- 배포가 실행 중인 경우 실행 중인 기존 CMS 사용을 선택하고 다음을 클릭합니다.

프롬프트가 표시되면 기존 CMS의 호스트 이름과 포트, 관리자 자격 증명, 데이터 소스 이름, 시스템 데이터베이스에 대한 자격 증명, 클러스터 키를 입력합니다.

- 배포가 중지된 경우 새 임시 CMS 시작을 선택하고 다음을 클릭합니다.

프롬프트가 표시되면 임시 CMS의 호스트 이름과 포트, 관리자 자격 증명, 데이터 소스 이름, 시스템 데이터베이스에 대한 데이터베이스 자격 증명, 클러스터 키를 입력합니다. 임시 CMS가 시작됩니다. (임시 CMS는 이 프로세스가 완료되면 중지됩니다.)

주의:

임시 CMS가 실행되는 동안에는 배포를 사용하지 않도록 하고, 기존 CMS와 임시 CMS가 서로 다른 포트를 사용하는지 확인하십시오.

5. 확인 페이지를 검토하고 완료를 클릭합니다.

CCM에서 노드를 만듭니다. 오류가 발생한 경우 로그 파일을 검토합니다.

이제 CCM을 사용하여 새 노드를 시작할 수 있습니다.

8.1.13.2.2.1 스크립트를 사용하여 Windows에서 노드 추가

주의:

노드를 추가하기 전이나 추가한 후에는 전체 클러스터에 대한 서버 구성을 백업하십시오.

Windows 컴퓨터에서는 AddNode.bat을 사용하여 노드를 추가할 수 있습니다. 자세한 내용은 노드 추가, 다시 만들기 및 삭제를 위한 스크립트 매개 변수 단원을 참조하십시오.

예제

명령 프롬프트의 제한 사항으로 인해 -connect 문자열에서 캐럿(^)을 사용하여 공백, 등호(=) 및 세미콜론을 이스케이프 처리해야 합니다.

```
<SCRIPTDIR>WAddNode.bat -name mynode2
-siaport 6415
-cms mycms:6400
-username Administrator
-password Password1
-cmsport 7400
-dbdriver mysqldatabasesubsystem
-connect "DSN^=BusinessObjects^ CMS^ 140^:UID^=username^;PWD^=Password1^;HOSTNAME^=database^;PORT^=3306"
-dbkey abc1234
```

참고:

긴 문자열에서 캐럿을 사용하지 않으려면 임시 response.bat 파일에 스크립트 이름과 모든 매개 변수를 기록한 다음 매개 변수 없이 response.bat 파일을 실행하면 됩니다.

관련 항목

- 401 페이지에서 [변수](#)
- 418 페이지에서 [노드 추가, 다시 만들기 및 삭제를 위한 스크립트 매개 변수](#)

8.1.13.2.3 UNIX에서 노드 추가

주의:

노드를 추가하기 전이나 추가한 후에는 전체 클러스터에 대한 서버 구성을 백업하십시오.

1. <INSTALLEDIR>/sap_bobj/serverconfig.sh를 실행합니다.
2. 1 - 노드 추가를 선택하고 Enter 키를 누릅니다.
3. 새 노드의 이름을 입력하고 Enter 키를 누릅니다.
4. 새 SIA의 포트 번호를 입력하고 Enter 키를 누릅니다.
5. 새 노드에 서버를 만들지 여부를 선택합니다.
 - 서버 없음
서버가 포함되지 않은 노드를 만듭니다.
 - cms
노드에 CMS만 만들고, 다른 서버는 만들지 않습니다.
 - 기본 서버
이 컴퓨터에 설치된 서버만 만듭니다. 즉, 가능한 서버 중 일부만 포함됩니다.

6. CMS를 선택합니다.

- 배포가 실행 중인 경우 기존을 선택하고 Enter 키를 누릅니다.

프롬프트가 표시되면 기존 CMS의 호스트 이름과 포트, 관리자 자격 증명, 데이터베이스 연결 정보, 시스템 데이터베이스에 대한 자격 증명 및 클러스터 키를 입력합니다.

- 배포가 중지된 경우 임시를 선택하고 Enter 키를 누릅니다.

프롬프트가 표시되면 임시 CMS의 호스트 이름과 포트, 관리자 자격 증명, 데이터베이스 연결 정보, 시스템 데이터베이스에 대한 자격 증명 및 클러스터 키를 입력합니다. 임시 CMS가 시작됩니다. (임시 CMS는 이 프로세스가 완료되면 중지됩니다.)

주의:

임시 CMS가 실행되는 동안에는 배포를 사용하지 않도록 하고, 기존 CMS와 임시 CMS가 서로 다른 포트를 사용하는지 확인하십시오.

7. 확인 페이지를 검토하고 Enter 키를 누릅니다.

CCM에서 노드를 만듭니다. 오류가 발생한 경우 로그 파일을 검토합니다.

이제 <INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>을 실행하여 새 노드를 시작할 수 있습니다.

8.1.13.2.3.1 스크립트를 사용하여 UNIX에서 노드 추가

주의:

노드를 추가하기 전이나 추가한 후에는 전체 클러스터에 대한 서버 구성을 백업하십시오.

UNIX 컴퓨터에서는 addnode.sh를 사용하여 노드를 추가할 수 있습니다. 자세한 내용은 노드 추가, 다시 만들기 및 삭제를 위한 스크립트 매개 변수 단원을 참조하십시오.

예제

```
<SCRIPTDIR>/addnode.sh -name mynode2
-siaport 6415
-cms mycms:6400
-username Administrator
-password Password1
-cmsport 7400
-dbdriver mysqldatabasesubsystem
-connect "DSN=BusinessObjects CMS 140:UID=Administrator:PWD=Password1;HOSTNAME=myDatabase;PORT=3306"
-dbkey abc1234
```

관련 항목

- 401 페이지에서 [변수](#)
- 418 페이지에서 [노드 추가, 다시 만들기 및 삭제를 위한 스크립트 매개 변수](#)

8.1.13.3 노드 다시 만들기

전체 클러스터에 대한 서버 구성을 복원한 후 또는 배포를 호스팅하는 컴퓨터에 오류가 발생했거나 손상된 파일 시스템이 있거나 이 컴퓨터가 손상된 경우, 중앙 구성 관리자(CCM) 또는 노드 관리 스크립트를 사용하여 노드를 다시 만들 수 있습니다. 다음 지침을 따르십시오.

- 설치 옵션과 노드 이름이 동일한 대체 컴퓨터에 배포를 다시 설치하는 경우에는 노드를 다시 만들 필요가 없습니다. 설치 프로그램에서 자동으로 노드를 다시 만듭니다.
- 설치 옵션과 패치 수준이 동일한 기존 배포가 있는 컴퓨터에서만 노드를 다시 만들어야 합니다.
- 배포된 어떠한 컴퓨터에도 존재하지 않는 노드만 다시 만들어야 합니다. 다른 컴퓨터에서 동일한 노드를 호스팅하지 않는지 확인합니다.
- 배포에서 노드를 서로 다른 운영 체제에서 실행할 수 있도록 허용하더라도 동일한 운영 체제를 사용하는 컴퓨터에서만 노드를 다시 만들어야 합니다.
- 방화벽을 사용하는 경우 SIA(Server Intelligence Agent) 및 중앙 관리 서버(CMS)의 포트가 열려 있는지 확인합니다.

기억:

노드가 있는 컴퓨터에서만 노드를 다시 만들 수 있습니다.

관련 항목

- 474 페이지에서 [시스템 복원](#)

8.1.13.3.1 Windows에서 노드를 다시 만들기

1. 중앙 구성 관리자(CCM)의 도구 모음에서 노드 추가를 클릭합니다.
2. 노드 추가 마법사에서 다시 만든 SIA(Server Intelligence Agent)의 노드 이름과 포트 번호를 입력합니다.

참고:

원래 노드와 다시 만든 노드의 이름이 동일해야 합니다.

3. 노드 다시 만들기를 선택하고 다음을 클릭합니다.
 - 중앙 관리 시스템(CMS)의 시스템 데이터베이스에 노드가 있는 경우 로컬 호스트에서 다시 만들어집니다.

주의:

클러스터의 호스트에 노드가 없는 경우에만 이 옵션을 사용하십시오.

- CMS의 시스템 데이터베이스에 노드가 없는 경우 기본 서버가 포함된 새 노드가 추가됩니다. 기본 서버에는 호스트에 설치된 모든 서버가 포함됩니다.

4. CMS를 선택합니다.

- CMS가 실행 중인 경우 실행 중인 기존 CMS 사용을 선택하고 다음을 클릭합니다.

프롬프트가 표시되면 기존 CMS의 호스트 이름과 포트, 관리자 자격 증명, 데이터 소스 이름, 시스템 데이터베이스에 대한 자격 증명, 클러스터 키를 입력합니다.

- CMS가 중지된 경우 새 임시 CMS 시작을 선택하고 다음을 클릭합니다.

프롬프트가 표시되면 임시 CMS의 호스트 이름과 포트, 관리자 자격 증명, 데이터 소스 이름, 시스템 데이터베이스에 대한 자격 증명, 클러스터 키를 입력합니다. 임시 CMS가 시작됩니다. (임시 CMS는 이 프로세스가 완료되면 중지됩니다.)

주의:

임시 CMS가 실행되는 동안에는 배포를 사용하지 않도록 하고, 기존 CMS와 임시 CMS가 서로 다른 포트를 사용하는지 확인하십시오.

5. 확인 페이지를 검토하고 완료를 클릭합니다.

CCM에서 노드를 다시 만들고 노드 정보를 로컬 컴퓨터에 추가합니다. 오류가 발생한 경우 로그 파일을 검토합니다.

이제 CCM을 사용하여 다시 만든 노드를 시작할 수 있습니다.

8.1.13.3.1.1 스크립트를 사용하여 Windows에서 노드 다시 만들기

Windows 컴퓨터에서는 AddNode.bat을 사용하여 노드를 다시 만들 수 있습니다. 자세한 내용은 노드 추가, 다시 만들기 및 삭제를 위한 스크립트 매개 변수 단원을 참조하십시오.

예제

명령 프롬프트의 제한 사항으로 인해 -connect 문자열에서 캐럿(^)을 사용하여 공백, 등호(=) 및 세미콜론을 이스케이프 처리해야 합니다.

```
<SCRIPTDIR>WAddNode.bat -name mynode2
-siaport 6415
-cms mycms:6400
-username Administrator
-password Password1
-cmsport 7400
-dbdriver mysqldatabasesubsystem
-connect "DSN^=BusinessObjects^ CMS^ 140^:UID^=username^;PWD^=Password1^;HOSTNAME^=database^;PORT^=3306"
-dbkey abc1234
-adopt
```

참고:

긴 문자열에서 캐럿을 사용하지 않으려면 임시 response.bat 파일에 스크립트 이름과 모든 매개 변수를 기록한 다음 매개 변수 없이 response.bat 파일을 실행하면 됩니다.

관련 항목

- 401 페이지에서 [변수](#)
- 418 페이지에서 [노드 추가, 다시 만들기 및 삭제를 위한 스크립트 매개 변수](#)

8.1.13.3.2 UNIX에서 노드 다시 만들기

1. <INSTALLDIR>/sap_bobj/serverconfig.sh를 실행합니다.
2. 1 - 노드 추가를 선택하고 Enter 키를 누릅니다.
3. 새 노드의 이름을 입력하고 Enter 키를 누릅니다.

참고:

원래 노드와 다시 만든 노드의 이름이 동일해야 합니다.

4. 새 SIA의 포트 번호를 입력하고 Enter 키를 누릅니다.
5. 노드 다시 만들기를 선택하고 Enter 키를 누릅니다.
 - 중앙 관리 서버(CMS)의 시스템 데이터베이스에 노드가 있는 경우 로컬 호스트에 노드가 다시 만들어집니다.

주의:

클러스터의 호스트에 노드가 없는 경우에만 이 옵션을 사용하십시오.

- CMS의 시스템 데이터베이스에 노드가 없는 경우 기본 서버가 포함된 새 노드가 추가됩니다. 기본 서버에는 호스트에 설치된 모든 서버가 포함됩니다.
6. CMS를 선택합니다.
 - 배포가 실행 중인 경우 기존을 선택하고 Enter 키를 누릅니다.
프롬프트가 표시되면 기존 CMS의 호스트 이름과 포트, 관리자 자격 증명, 데이터베이스 연결 정보, 시스템 데이터베이스에 대한 자격 증명 및 클러스터 키를 입력합니다.
 - 배포가 중지된 경우 임시를 선택하고 Enter 키를 누릅니다.
프롬프트가 표시되면 임시 CMS의 호스트 이름과 포트, 관리자 자격 증명, 데이터베이스 연결 정보, 시스템 데이터베이스에 대한 자격 증명 및 클러스터 키를 입력합니다. 임시 CMS가 시작됩니다. (임시 CMS는 이 프로세스가 완료되면 중지됩니다.)

주의:

임시 CMS가 실행되는 동안에는 배포를 사용하지 않도록 하고, 기존 CMS와 임시 CMS가 서로 다른 포트를 사용하는지 확인하십시오.

7. 확인 페이지를 검토하고 Enter 키를 누릅니다.

CCM에서 노드를 다시 만들고 노드 정보를 로컬 컴퓨터에 추가합니다. 오류가 발생한 경우 로그 파일을 검토합니다.

이제 <INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>을 실행하여 다시 만든 노드를 시작할 수 있습니다.

8.1.13.3.2.1 스크립트를 사용하여 UNIX에서 노드 다시 만들기

UNIX 컴퓨터에서는 addnode.sh를 사용하여 노드를 다시 만들 수 있습니다. 자세한 내용은 노드 추가, 다시 만들기 및 삭제를 위한 스크립트 매개 변수 단원을 참조하십시오.

예제

```
<SCRIPTDIR>/addnode.sh -name mynode2
-siport 6415
-cms mycms:6400
-username Administrator
-password Password1
-cmsport 7400
-dbdriver mysqldatabasesubsystem
-connect "DSN=BusinessObjects CMS 140:UID=Administrator:PWD=Password1;HOSTNAME=database:PORT=3306"
-dbkey abc1234
-adopt
```

관련 항목

- 401 페이지에서 [변수](#)"
- 418 페이지에서 [노드 추가, 다시 만들기 및 삭제를 위한 스크립트 매개 변수](#)"

8.1.13.4 노드 삭제

중앙 구성 관리자(CCM) 또는 노드 관리 스크립트를 사용하여 중지된 노드를 삭제할 수 있습니다. 다음 지침을 따르십시오.

- 노드를 삭제하면 노드에 있는 모든 서버도 영구적으로 삭제됩니다.
- 클러스터에 여러 개의 컴퓨터가 포함된 경우, 먼저 노드를 삭제한 다음 클러스터에서 컴퓨터를 제거하고 소프트웨어를 제거합니다. 노드를 삭제하기 전에 클러스터에서 컴퓨터를 제거했거나 컴퓨터에 있는 파일 시스템이 잘못 작동하는 경우, 동일한 클러스터에서 동일한 서버를 포함하는 다른 서버에 노드를 다시 만든 다음 노드를 삭제합니다.

기억:

노드가 있는 컴퓨터에서만 노드를 삭제할 수 있습니다.

관련 항목

- 406 페이지에서 [노드 다시 만들기](#)"

8.1.13.4.1 Windows에서 노드 삭제

주의:

노드를 삭제하기 전이나 삭제한 후에는 전체 클러스터에 대한 서버 구성을 백업하십시오.

1. 중앙 구성 관리자(CCM)를 실행합니다.
2. CCM에서 삭제할 노드를 중지합니다.
3. 노드를 선택하고 도구 모음에서 노드 삭제를 클릭합니다.
4. 프롬프트가 표시되면 CMS의 호스트 이름, 포트, 관리자 자격 증명 및 클러스터 키를 입력합니다.

CCM에서 노드 및 노드에 있는 모든 서버를 삭제합니다.

8.1.13.4.1.1 스크립트를 사용하여 Windows에서 노드 삭제

주의:

노드를 삭제하기 전이나 삭제한 후에는 전체 클러스터에 대한 서버 구성을 백업하십시오.

Windows 컴퓨터에서는 RemoveNode.bat을 사용하여 노드를 삭제할 수 있습니다. 자세한 내용은 노드 추가, 다시 만들기 및 삭제를 위한 스크립트 매개 변수 단원을 참조하십시오.

예제

```
<SCRIPTDIR>WRemoveNode.bat -name mynode2
-cms mycms:6400
```

```
-username Administrator
-password Password1
```

관련 항목

- 401 페이지에서 [변수](#)"
- 418 페이지에서 [노드 추가, 다시 만들기 및 삭제를 위한 스크립트 매개 변수](#)"

8.1.13.4.2 UNIX에서 노드 삭제

주의:

노드를 삭제하기 전이나 삭제한 후에는 전체 클러스터에 대한 서버 구성을 백업하십시오.

1. <INSTALLDIR>/sap_bobj/ccm.sh -stop <nodeName>을 실행하여 삭제하려는 노드를 중지합니다.
2. <INSTALLDIR>/sap_bobj/serverconfig.sh를 실행합니다.
3. 2 - 노드 삭제를 선택하고 Enter 키를 누릅니다.
4. 삭제할 노드를 선택하고 Enter 키를 누릅니다.
5. 프롬프트가 표시되면 CMS의 호스트 이름, 포트, 관리자 자격 증명 및 클러스터 키를 입력합니다. 노드 및 노드에 있는 모든 서버가 삭제됩니다.

8.1.13.4.2.1 스크립트를 사용하여 UNIX에서 노드 삭제

주의:

노드를 삭제하기 전이나 삭제한 후에는 전체 클러스터에 대한 서버 구성을 백업하십시오.

UNIX 컴퓨터에서는 removenode.sh를 사용하여 노드를 삭제할 수 있습니다. 자세한 내용은 노드 추가, 다시 만들기 및 삭제를 위한 스크립트 매개 변수 단원을 참조하십시오.

예제

```
<SCRIPTDIR>\WRemoveNode.sh -name mynode2
-cms mycms:6400
```

```
-username Administrator
-password Password1
```

관련 항목

- 401 페이지에서 [변수](#)"
- 418 페이지에서 [노드 추가, 다시 만들기 및 삭제를 위한 스크립트 매개 변수](#)"

8.1.13.5 노드 이름 바꾸기

중앙 구성 관리자(CCM)를 사용하여 노드 이름을 바꿀 수 있습니다. 노드 이름을 바꾸려면 새 이름을 사용하는 노드를 새로 만들고 서버를 원래 노드에서 새 노드로 복제한 다음 원래 노드를 삭제하십시오. 다음 지침을 따르십시오.

- 노드가 있는 컴퓨터의 이름을 바꾼 경우 노드 이름을 바꿀 필요가 없습니다. 기존 노드 이름을 계속 사용할 수 있습니다.
- 방화벽을 사용하는 경우 SIA(Server Intelligence Agent) 및 중앙 관리 서버(CMS)의 포트가 열려 있는지 확인합니다.

기억:

노드가 있는 컴퓨터에서만 노드의 이름을 바꿀 수 있습니다.

관련 항목

- 401 페이지에서 [새 노드 추가](#)"
- 369 페이지에서 [서버 복제](#)"
- 409 페이지에서 [노드 삭제](#)"

8.1.13.5.1 Windows에서 노드 이름 바꾸기

주의:

노드 이름을 바꾸기 전이나 바꾼 후에는 전체 클러스터에 대한 서버 구성을 백업하십시오.

1. 중앙 구성 관리자(CCM)를 시작합니다.
2. 중앙 구성 관리자(CCM)의 도구 모음에서 노드 추가를 클릭합니다.

3. 노드 추가 마법사에서 새 SIA(Server Intelligence Agent)에 대한 노드 이름과 포트 번호, 관리자 자격 증명, 데이터베이스 연결 정보, 시스템 데이터베이스에 대한 자격 증명 및 클러스터 키를 입력합니다.
4. 서버가 없는 노드 추가를 선택합니다.
5. 노드를 만든 후 중앙 관리 콘솔의 서버 관리 페이지에서 모든 서버를 원래 노드에서 새 노드로 복제합니다.

참고:

복제된 서버에서 이전 노드에 있는 서버와 포트가 충돌하지 않는지 확인합니다.

6. CCM에서 새 노드를 시작합니다.
7. 새 노드를 5분 동안 실행한 후 CCM을 사용하여 원래 노드를 삭제합니다.

관련 항목

- 401 페이지에서 [새 노드 추가](#)"
- 369 페이지에서 [서버 복제](#)"
- 409 페이지에서 [노드 삭제](#)"

8.1.13.5.2 UNIX에서 노드 이름 바꾸기

주의:

노드 이름을 바꾸기 전이나 바꾼 후에는 전체 클러스터에 대한 서버 구성을 백업하십시오.

1. <INSTALLDIR>/sap_bobj/serverconfig.sh를 실행합니다.
2. 1 - 노드 추가를 선택하고 Enter 키를 누릅니다.
3. 새 노드의 이름을 입력하고 Enter 키를 누릅니다.
4. 새 SIA의 포트 번호를 입력하고 Enter 키를 누릅니다.
5. 프롬프트가 표시되면 관리자 자격 증명, 데이터베이스 연결 정보, 시스템 데이터베이스에 대한 자격 증명 및 클러스터 키를 입력합니다.
6. 서버 없음을 선택하고 Enter 키를 누릅니다.
7. 노드를 만든 후 중앙 관리 콘솔의 서버 관리 페이지에서 모든 서버를 원래 노드에서 새 노드로 복제합니다.

참고:

복제된 서버에서 이전 노드에 있는 서버와 포트가 충돌하지 않는지 확인합니다.

8. <INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>을 실행하여 새 노드를 시작합니다.
9. 새 노드를 5분 동안 실행한 후 serverconfig.sh를 사용하여 원래 노드를 삭제합니다.

관련 항목

- 401 페이지에서 [새 노드 추가](#)"
- 369 페이지에서 [서버 복제](#)"
- 409 페이지에서 [노드 삭제](#)"

8.1.13.6 노드 이동

중앙 구성 관리자(CCM) 또는 노드 관리 스크립트를 사용하여 중지된 노드를 다른 클러스터로 이동할 수 있습니다. 다음 지침을 따르십시오.

- 대상 클러스터에 동일한 이름의 노드가 없는지 확인합니다.
- 소스 노드가 위치한 컴퓨터에 설치된 모든 서버 유형이 프로덕션 클러스터에도 설치되어 있는지 확인합니다.
- 운영 클러스터에 새 컴퓨터를 추가하되 테스트가 완료될 때까지는 이 컴퓨터를 사용하지 않으려는 경우, 독립 실행형 컴퓨터에 BI 플랫폼을 설치하고 컴퓨터를 테스트한 다음 노드를 운영 클러스터로 이동합니다.

기억:

노드가 있는 컴퓨터에서만 노드를 이동할 수 있습니다.

8.1.13.6.1 Windows에서 기존 노드 이동

이 예에서 이동하려는 노드는 소스 시스템에 설치되어 있습니다. 클러스터에 포함되지 않았던 컴퓨터를 대상 클러스터에 추가하려고 합니다.

주의:

노드를 이동하기 전이나 이동한 후에는 전체 클러스터에 대한 서버 구성을 백업하십시오.

1. 중앙 구성 관리자(CCM)에서 노드를 중지합니다.
2. 노드를 마우스 오른쪽 단추로 클릭하고 이동을 선택합니다.
3. 프롬프트가 표시되면 데이터 소스 이름을 선택하고 대상 CMS의 호스트 이름, 포트, 데이터베이스 연결 정보, 관리자 자격 증명 및 클러스터 키를 입력합니다.
4. CMS를 선택합니다.
 - 소스 배포가 실행 중인 경우 실행 중인 기존 CMS 사용을 선택하고 다음을 클릭합니다.

프롬프트가 표시되면 소스 시스템의 기존 CMS에 대한 호스트 이름과 포트, 관리자 자격 증명, 데이터 소스 이름, 소스 시스템 데이터베이스에 대한 자격 증명, 클러스터 키를 입력합니다.

- 소스 배포가 중지된 경우 새 임시 CMS 시작을 선택하고 다음을 클릭합니다.

프롬프트가 표시되면 소스 시스템의 임시 CMS에 대한 호스트 이름과 포트, 관리자 자격 증명, 데이터 소스 이름, 소스 시스템 데이터베이스에 대한 데이터베이스 자격 증명, 클러스터 키를 입력합니다. 임시 CMS가 시작됩니다. (임시 CMS는 이 프로세스가 완료되면 중지됩니다.)

주의:

임시 CMS가 실행되는 동안에는 배포를 사용하지 않도록 하고, 기존 CMS와 임시 CMS가 서로 다른 포트를 사용하는지 확인하십시오.

5. 확인 페이지를 검토하고 완료를 클릭합니다.

CCM에서 소스 클러스터의 노드와 동일한 서버 및 동일한 이름을 사용하는 새 노드를 대상 클러스터에 만듭니다. 노드 복사본은 소스 클러스터에 남아 있습니다. 노드에 있는 서버 구성 템플릿은 이동되지 않습니다. 오류가 발생한 경우 로그 파일을 검토합니다.

주의:

노드를 이동한 후에는 소스 클러스터를 사용하지 마십시오.

6. CCM에서 이동된 노드를 시작합니다.

8.1.13.6.1.1 스크립트를 사용하여 Windows에서 노드 이동

주의:

노드를 이동하기 전이나 이동한 후에는 전체 클러스터에 대한 서버 구성을 백업하십시오.

Windows 컴퓨터에서는 MoveNode.bat을 사용하여 노드를 이동할 수 있습니다. 자세한 내용은 노드 이동을 위한 스크립트 매개 변수 단원을 참조하십시오.

예제

명령 프롬프트의 제한 사항으로 인해 -connect 문자열에서 캐럿(^)을 사용하여 공백, 등호(=) 및 세미콜론을 이스케이프 처리해야 합니다.

```
<SCRIPTDIR>WMoveNode.bat -cms sourceMachine:6409
-username Administrator
-password Password1
-dbdriver mysql databasesubsystem
-connect "DSN^=Source^ BOEXI40^;UID^=username^;PWD^=Password1^;HOSTNAME^=database1^;PORT^=3306"
-dbkey abc1234
-destcms destinationMachine:6401
-destusername Administrator
-destpassword Password2
-destdbdriver sybasedatabasesubsystem
-destconnect "DSN^=Destin^ BOEXI40^;UID^=username^;PWD^=Password2^;"
-destdbkey def5678
```

참고:

긴 문자열에서 캐럿을 사용하지 않으려면 임시 response.bat 파일에 스크립트 이름과 모든 매개 변수를 기록한 다음 매개 변수 없이 response.bat 파일을 실행하면 됩니다.

관련 항목

- 401 페이지에서 [변수](#)
- 420 페이지에서 [노드 이동을 위한 스크립트 매개 변수](#)

8.1.13.6.2 UNIX에서 기존 노드 이동

이 예에서 이동하려는 노드는 소스 시스템에 설치되어 있습니다. 독립 실행형 클러스터에 포함되었던 컴퓨터를 대상 클러스터에 추가하려고 합니다.

주의:

노드를 이동하기 전이나 이동한 후에는 전체 클러스터에 대한 서버 구성을 백업하십시오.

1. <INSTALLDIR>/sap_bobj/ccm.sh -stop <nodeName>을 실행하여 노드를 중지합니다.
2. <INSTALLDIR>/sap_bobj/serverconfig.sh를 실행합니다.
3. 4 - 노드 이동을 선택하고 Enter 키를 누릅니다.
4. 이동할 노드를 선택하고 Enter 키를 누릅니다.
5. 프롬프트가 표시되면 시스템 데이터베이스 연결 정보를 선택하고 대상 CMS의 호스트 이름, 포트, 관리자 자격 증명 및 클러스터 키를 입력합니다.
6. CMS를 선택합니다.
 - 소스 배포가 실행 중인 경우 기존을 선택하고 Enter 키를 누릅니다.
프롬프트가 표시되면 소스 시스템의 기존 CMS에 대한 호스트 이름과 포트, 관리자 자격 증명, 데이터베이스 연결 정보, 소스 시스템 데이터베이스에 대한 자격 증명 및 클러스터 키를 입력합니다.
 - 소스 배포가 중지된 경우 임시를 선택하고 Enter 키를 누릅니다.
프롬프트가 표시되면 소스 시스템의 임시 CMS에 대한 호스트 이름과 포트, 관리자 자격 증명, 데이터베이스 연결 정보, 소스 시스템 데이터베이스에 대한 자격 증명 및 클러스터 키를 입력합니다. 임시 CMS가 시작됩니다. (임시 CMS는 이 프로세스가 완료되면 중지됩니다.)

주의:

임시 CMS가 실행되는 동안에는 배포를 사용하지 않도록 하고, 기존 CMS와 임시 CMS가 서로 다른 포트를 사용하는지 확인하십시오.

7. 확인 페이지를 검토하고 Enter 키를 누릅니다.

CCM에서 소스 클러스터의 노드와 동일한 서버 및 동일한 이름을 사용하는 새 노드를 대상 클러스터에 만듭니다. 노드 복사본은 소스 클러스터에 남아 있습니다. 노드에 있는 서버 구성 템플릿은 이동되지 않습니다. 오류가 발생한 경우 로그 파일을 검토합니다.

주의:

노드를 이동한 후에는 소스 클러스터를 사용하지 마십시오.

8. <INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>을 실행하여 이동한 노드를 시작합니다.

8.1.13.6.2.1 스크립트를 사용하여 UNIX에서 노드 이동

주의:

노드를 이동하기 전이나 이동한 후에는 전체 클러스터에 대한 서버 구성을 백업하십시오.

UNIX 컴퓨터에서는 movenode.sh 를 사용하여 노드를 이동할 수 있습니다. 자세한 내용은 노드 이동을 위한 스크립트 매개 변수 단원을 참조하십시오.

예제

```
<SCRIPTDIR>/movenode.sh -cms sourceMachine:6409
-username Administrator
-password Password1
-dbdriver mysqldatabasesubsystem
-connect "DSN=Source BOEXI40:UID=username;PWD=Password1;HOSTNAME=database1;PORT=3306"
-dbkey abc1234
-destcms destinationMachine:6401
-destusername Administrator
-destpassword Password2
-destdbdriver sybasedatabasesubsystem
-destconnect "DSN=Destin BOEXI40:UID=username;PWD=Password2;"
-destdbkey def5678
```

관련 항목

- 401 페이지에서 [변수](#)
- 420 페이지에서 [노드 이동을 위한 스크립트 매개 변수](#)

8.1.13.7 스크립트 매개 변수

8.1.13.7.1 노드 추가, 다시 만들기 및 삭제를 위한 스크립트 매개 변수

매개 변수	설명	예제
-adopt	CMS에 노드가 이미 있을 경우 노드를 다시 만듭니다.	-adopt
-cms	중앙 관리 서버(CMS)의 이름과 포트 번호입니다. 주의: -usetempcms를 사용하는 경우에는 이 매개 변수를 사용하지 마십시오. 참고: CMS가 기본 포트(6400)에서 실행 중이지 않은 경우 포트 번호를 지정해야 합니다.	-cms mycms:6409
-cmsport	<ul style="list-style-type: none"> 임시 CMS를 시작할 때 사용되는 CMS 포트입니다. 제한: -usetempcms, -dbdriver, -connect 및 -dbkey 매개 변수를 사용할 수도 있습니다. 새 CMS를 만들 때 사용되는 CMS 포트입니다. 제한: -dbdriver, -connect 및 -dbkey 매개 변수를 사용할 수도 있습니다. 	-cmsport 6401
-connect	CMS 또는 임시 CMS 시스템 데이터베이스의 연결 문자열입니다. 참고: DB2, Oracle, SQL Server 또는 Sybase 데이터베이스에 연결하는 경우에는 HOSTNAME 및 PORT 특성을 생략하십시오.	-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=password;HOST NAME=database;PORT=3306"

매개 변수	설명	예제
-dbdriver	CMS의 데이터베이스 드라이버입니다. 가능한 값: <ul style="list-style-type: none"> • db2databasesubsystem • maxdbdatabasesubsystem • mysqldatabasesubsystem • oracledatabasesubsystem • sqlserverdatabasesubsystem • sybasedatabasesubsystem 	-dbdriver mysqldatabasesubsystem
-dbkey	클러스터 키입니다.	-dbkey abc1234
-name	노드 이름입니다.	-name mynode2
-noservers	서버가 포함되지 않은 노드를 만듭니다. 참고: 추가 -createcms 매개 변수는 CMS만 포함하고 다른 서버는 포함하지 않는 노드를 만듭니다. 모든 기본 서버가 포함된 노드를 만들려면 이러한 매개 변수를 생략하십시오.	-noservers
-password	관리자 계정의 암호입니다.	-password Password1
-siaport	노드에 대한 Server Intelligence Agent 포트 번호입니다.	-siaport 6409
-username	관리자 계정의 사용자 이름입니다.	-username Administrator
-usetempcms	주의: -cms를 사용하는 경우에는 이 매개 변수를 사용하지 마십시오. 임시 CMS를 시작하여 사용합니다. 참고: 배포가 실행 중이지 않은 경우 임시 CMS를 사용하십시오.	-usetempcms

관련 항목

- 403 페이지에서 [스크립트를 사용하여 Windows에서 노드 추가](#)"
- 405 페이지에서 [스크립트를 사용하여 UNIX에서 노드 추가](#)"
- 407 페이지에서 [스크립트를 사용하여 Windows에서 노드 다시 만들기 "](#)

- 409 페이지에서 [스크립트를 사용하여 UNIX에서 노드 다시 만들기](#)"
- 410 페이지에서 [스크립트를 사용하여 Windows에서 노드 삭제](#)"
- 411 페이지에서 [스크립트를 사용하여 UNIX에서 노드 삭제](#)"

8.1.13.7.2 노드 이동을 위한 스크립트 매개 변수

매개 변수	설명	예제
-cms	<p>소스 중앙 관리 서버(CMS)의 이름입니다.</p> <p>주의: -usetempcms를 사용하는 경우에는 이 매개 변수를 사용하지 마십시오.</p> <p>참고: CMS가 기본 포트(6400)에서 실행 중이지 않은 경우 포트 번호를 지정해야 합니다.</p>	-cms sourceMachine:6409
-cmsport	<ul style="list-style-type: none"> • 임시 CMS를 시작할 때 사용되는 CMS 포트입니다. <p>제한: -usetempcms, -dbdriver, -connect 및 -dbkey 매개 변수를 사용할 수도 있습니다.</p> <ul style="list-style-type: none"> • 새 CMS를 만들 때 사용되는 CMS 포트입니다. <p>제한: -dbdriver, -connect 및 -dbkey 매개 변수를 사용할 수도 있습니다.</p>	-cmsport 6401

매개 변수	설명	예제
-connect	<p>소스 CMS 또는 임시 CMS 시스템 데이터베이스의 연결 문자열입니다.</p> <p>참고: DB2, Oracle, SQL Server 또는 Sybase 데이터베이스에 연결하는 경우에는 HOSTNAME 및 PORT 특성을 생략하십시오.</p>	<pre>-connect "DSN=Source BOEXI40;UID=username;PWD=password;HOST NAME=database;PORT=3306"</pre>
-dbdriver	<p>소스 CMS의 데이터베이스 드라이버입니다.</p> <p>가능한 값:</p> <ul style="list-style-type: none"> • db2databasesubsystem • maxdbdatabasesubsystem • mysqldatabasesubsystem • oracledatabasesubsystem • sqlserverdatabasesubsystem • sybasedatabasesubsystem 	<pre>-dbdriver mysqldatabasesubsystem</pre>
-dbkey	소스 클러스터 키입니다.	<pre>-dbkey abc1234</pre>
-destcms	<p>대상 CMS의 이름입니다.</p> <p>참고: CMS가 기본 포트(6400)에서 실행 중이지 않은 경우 포트 번호를 지정해야 합니다.</p>	<pre>-destcms destinationMachine:6401</pre>
-destconnect	<p>대상 CMS 시스템 데이터베이스의 연결 문자열입니다.</p> <p>참고: DB2, Oracle, SQL Server 또는 Sybase 데이터베이스에 연결하는 경우에는 HOSTNAME 및 PORT 특성을 생략하십시오.</p>	<pre>-destconnect "DSN=Destin BOEXI40;UID=username;PWD=password;HOST NAME=database;PORT=3306"</pre>

매개 변수	설명	예제
-destdbdriver	<p>대상 CMS의 데이터베이스 드라이버입니다.</p> <p>가능한 값:</p> <ul style="list-style-type: none"> • db2databasesubsystem • maxdbdatabasesubsystem • mysqldatabasesubsystem • oracledatabasesubsystem • sqlserverdatabasesubsystem • sybasedatabasesubsystem <p>참고: sqlserverdatabase는 Unix에서 지원되지 않습니다.</p>	-destdbdriver sybasedatabasesubsystem
-destdbkey	대상 클러스터 키입니다.	-destdbkey def5678
-destpassword	대상 CMS에 대한 관리자 계정의 암호입니다.	-destpassword Password2
-destusername	대상 CMS에 대한 관리자 계정의 사용자 이름입니다.	-destusername Administrator
-password	소스 CMS에 대한 관리자 계정의 암호입니다.	-password Password1
-username	소스 CMS에 대한 관리자 계정의 사용자 이름입니다.	-username Administrator
-usetempcms	<p>주의: -cms를 사용하는 경우에는 이 매개 변수를 사용하지 마십시오.</p> <p>임시 CMS를 시작하여 사용합니다.</p> <p>참고: 배포가 실행 중이지 않은 경우 임시 CMS를 사용하십시오.</p>	-usetempcms

관련 항목

- 415 페이지에서 [스크립트를 사용하여 Windows에서 노드 이동](#)"
- 417 페이지에서 [스크립트를 사용하여 UNIX에서 노드 이동](#)"

8.1.13.8 Windows 서버 종속성 추가

Windows 환경에서 SIA(Server Intelligence Agent)의 각 인스턴스는 이벤트 로그 및 원격 프로시저 호출(RPC) 서비스에 종속됩니다.

SIA가 올바르게 작동하지 않을 경우 두 서비스가 모두 SIA의 종속성 탭에 표시되는지 확인하십시오.

8.1.13.8.1 Windows 서버 종속성 추가

1. 중앙 구성 관리자(CCM)를 사용하여 SIA(Server Intelligence Agent)를 중지합니다.
2. SIA를 마우스 오른쪽 단추로 클릭한 다음 속성을 선택합니다.
3. 종속성 탭을 클릭합니다.
4. 추가를 클릭합니다.
종속성 추가 대화 상자에 사용 가능한 모든 종속성의 목록이 표시됩니다.
5. 종속성을 선택하고 추가를 클릭합니다.
6. 확인을 클릭합니다.
7. CCM을 사용하여 SIA를 다시 시작합니다.

8.1.13.9 노드에 대한 사용자 자격 증명 변경

운영 체제 암호가 변경된 경우 또는 다른 사용자 계정으로 노드에 있는 모든 서버를 실행하려는 경우, 중앙 구성 관리자(CCM)를 사용하여 SIA(Server Intelligence Agent)에 대한 사용자 자격 증명을 지정하거나 업데이트할 수 있습니다.

SIA에서 관리하는 모든 서버는 동일한 계정을 사용하여 실행됩니다. 시스템 계정이 아닌 다른 계정을 사용하여 서버를 실행하려면 본인의 계정이 서버 컴퓨터에 있는 로컬 관리자 그룹의 멤버인지, 프로세스 수준 토큰 바꾸기 권한을 보유하고 있는지 확인하십시오.

제한:

UNIX 컴퓨터의 경우 설치에 사용했던 것과 동일한 계정으로 SAP BI 플랫폼을 실행해야 합니다. 다른 계정을 사용하려면 다른 계정을 사용하여 배포를 다시 설치하십시오.

8.1.13.9.1 Windows에서 노드에 대한 사용자 자격 증명 변경

1. 중앙 구성 관리자(CCM)를 사용하여 SIA(Server Intelligence Agent)를 중지합니다.
2. SIA를 마우스 오른쪽 단추로 클릭한 다음 속성을 선택합니다.
3. 시스템 계정 확인란 선택을 취소합니다.
4. 사용자 이름과 암호를 입력한 다음 확인을 클릭합니다.
5. CCM을 사용하여 SIA를 다시 시작합니다.

SIA 및 서버 프로세스가 새 사용자 계정으로 로컬 컴퓨터에 로그인합니다.

8.1.14 SAP BusinessObjects Business Intelligence 플랫폼 배포에서 컴퓨터 이름 바꾸기

컴퓨터상의 모든 SAP BusinessObjects Business Intelligence 플랫폼 서버를 중지한 다음 컴퓨터의 이름을 바꾸면 언제든지 SAP BusinessObjects Business Intelligence 플랫폼 배포에서 컴퓨터의 이름을 변경할 수 있습니다. 이 컴퓨터가 클러스터에 속하는 경우, 클러스터에 속하는 모든 컴퓨터와 서버를 중지할 필요는 없고 다른 컴퓨터가 작동하고 있는 동안 중앙 관리 콘솔(CMC)에서 서버의 이름을 바꿀 수 있습니다.

이름을 바꿀 컴퓨터에 CMS 시스템 데이터베이스나 감사 데이터베이스가 있는 경우, 컴퓨터 이름을 바꾼 후 데이터베이스 연결 정보를 업데이트해야 합니다. 이들 데이터베이스 중 어느 하나에 대해 ODBC 연결을 사용 중이라면, 컴퓨터의 새 이름으로 연결을 업데이트해야 합니다. 다른 모든 데이터베이스 연결의 경우, 중앙 구성 관리자(CCM)에서 기존 데이터베이스를 선택해야 합니다.

배포 환경에서 컴퓨터의 이름을 바꾸는 경우 컴퓨터의 노드 이름을 바꿀 필요는 없습니다.

관련 항목

- 427 페이지에서 [새 CMS 데이터베이스 또는 기존 CMS 데이터베이스 선택](#)

8.1.15 SAP BusinessObjects Business Intelligence 플랫폼에서 32비트 및 64비트 타사 라이브러리 사용

SAP BusinessObjects Business Intelligence 플랫폼 서버는 32비트 및 64비트 프로세스의 조합입니다. 일부 서버에서는 추가로 32비트 및 64비트 자식 프로세스를 실행합니다. SAP BusinessObjects Business Intelligence 플랫폼 프로세스에서 올바른 버전의 타사 라이브러리(32비트 또는 64비트)를 사용하려면 SAP BusinessObjects Business Intelligence 플랫폼을 호스트하는 컴퓨터에서 버전별로 별도의 환경 변수를 설정해야 합니다. 그런 다음 32비트 및 64비트 버전의 쉘표로 구분된 환경 변수 목록을 포함하는 추가 환경 변수를 설정해야 합니다. SAP BusinessObjects Business Intelligence 플랫폼에서 프로세스가 실행되면 32비트 또는 64비트 프로세스인지에 따라 적합한 변수가 선택됩니다.

- <FIRST_ENV_VAR>= 64비트 SAP BusinessObjects Business Intelligence 플랫폼 프로세스에서 사용할 값입니다.
- <FIRST_ENV_VAR32>=32비트 프로세스에서 사용할 값입니다.
- <SECOND_ENV_VAR>=64비트 프로세스에서 사용할 값입니다.
- <SECOND_ENV_VAR32>=32비트 프로세스에서 사용할 값입니다.
- BOE_USE_32BIT_ENV_FOR=<FIRST_ENV_VAR>,<SECOND_ENV_VAR>

예를 들어 SAP BusinessObjects Business Intelligence 플랫폼을 AIX 컴퓨터와 32비트 및 64비트 Oracle 클라이언트에 설치했으며 LIBPATH 변수를 설정해야 하는 경우, 다음 변수를 설정하십시오.

- ORACLE_HOME=<64비트 버전의 Oracle 클라이언트>
- ORACLE_HOME32=<32비트 버전>
- LIBPATH=<64비트 버전>
- LIBPATH32=<32비트 버전>
- BOE_USE_32BIT_ENV_FOR=ORACLE_HOME,LIBPATH

8.1.16 서버 및 노드 자리 표시자 관리

8.1.16.1 서버 자리 표시자 보기

- CMC의 서버 관리 영역에서 서버를 마우스 오른쪽 단추로 클릭하고 자리 표시자를 선택합니다.
자리 표시자 대화 상자에는 사용자가 선택한 서버와 같은 클러스터에 있는 모든 서버의 자리 표시자 목록이 표시됩니다. 자리 표시자의 값을 변경하려면 노드에 대한 자리 표시자를 수정합니다.

관련 항목

- 885 페이지에서 [서버 및 노드 자리 표시자](#)"

8.1.16.2 노드의 자리 표시자 보기 및 편집

1. 중앙 관리 콘솔의 서버 관리 영역에서 자리 표시자를 변경할 노드를 마우스 오른쪽 단추로 클릭하고 자리 표시자를 선택합니다.
2. 자리 표시자에 대한 설정 중 어느 것이든 편집하려면 알맞은 변경 작업을 수행하고 확인을 클릭하여 계속합니다.

관련 항목

- 885 페이지에서 [서버 및 노드 자리 표시자](#)"

장9 중앙 관리 서버(CMS) 데이터베이스 관리

9.1 CMS 시스템 데이터베이스 연결 관리

예를 들어, 하드웨어 또는 소프트웨어 오류나 네트워크 문제로 인해 CMS 시스템 데이터베이스를 사용할 수 없는 경우 CMS는 리소스 대기 중 상태가 됩니다. SAP BusinessObjects Business Intelligence 플랫폼 배포 환경에 여러 개의 CMS가 있는 경우, 다른 서버에서 보내는 이후의 요청은 시스템 데이터베이스에 대한 연결이 활성화되어 있는 클러스터 내의 모든 CMS로 전달됩니다. CMS가 리소스 대기 중 상태에 있는 경우 데이터베이스 액세스가 필요하지 않은 모든 현재 요청은 계속 처리되지만, CMS 데이터베이스에 대한 액세스가 필요한 요청은 실패하게 됩니다.

기본적으로 리소스 대기 중 상태에 있는 CMS는 요청된 시스템 데이터베이스 연결 속성에 지정된 연결 횟수만큼 주기적으로 연결 재설정을 시도합니다. 적어도 하나의 데이터베이스 연결이 설정되는 즉시 CMS는 필요한 데이터를 모두 동기화하고 실행 중 상태로 전환한 다음 정상 작업을 계속합니다.

일부 경우 CMS가 데이터베이스에 대한 연결을 자동으로 재설정하지 않도록 해야 할 수 있습니다. 예를 들어, 데이터베이스 연결이 재설정되기 전에 데이터베이스 무결성을 확인해야 할 수 있습니다. 이렇게 하려면 CMS 서버의 속성 페이지에서 시스템 데이터베이스 자동 다시 연결을 선택 해제하십시오.

관련 항목

- 387 페이지에서 [서버 속성 변경](#)"

9.2 새 CMS 데이터베이스 또는 기존 CMS 데이터베이스 선택

CCM을 사용하여 노드에 대한 새 CMS 시스템 데이터베이스나 기존 데이터베이스를 지정할 수 있습니다. 일반적으로 이러한 단계를 수행해야 하는 경우는 많지 않습니다.

- 현재 CMS 시스템 데이터베이스의 암호를 변경한 경우 이러한 단계를 수행할 때 현재 데이터베이스에 연결을 끊었다가 다시 연결할 수 있습니다. 암호 입력 메시지가 표시되면 CMS에 새 암호를 입력할 수 있습니다.
- SAP BusinessObjects Business Intelligence 플랫폼에 대해 빈 데이터베이스를 선택하여 초기화하려는 경우 이러한 단계를 통해 새 데이터 소스를 선택할 수 있습니다.
- 표준 데이터베이스 관리 도구 및 절차를 사용하여 백업에서 CMS 시스템 데이터베이스를 복원하여 원래 데이터베이스 연결이 더 이상 유효하지 않게 렌더링되는 경우 복원된 데이터베이스에 CMS를 다시 연결해야 합니다. 새로 설치한 데이터베이스 서버에 원래 CMS 데이터베이스를 복원하는 경우를 예로 들 수 있습니다.

9.2.1 Windows에서 새 CMS 데이터베이스 또는 기존 데이터베이스 선택

1. CCM을 사용하여 SIA(Server Intelligence Agent)를 중지합니다.
2. SIA를 선택하고 도구 모음에서 CMS 시스템 데이터베이스 데이터 소스 지정을 클릭합니다.
3. 속성 대화 상자의 구성 탭에 있는 CMS 데이터 소스 아래에서 지정을 클릭합니다.
4. 나머지 단계는 선택한 연결 유형에 따라 달라집니다.
 - ODBC를 선택한 경우 Windows "데이터 원본 선택" 대화 상자가 열립니다. CMS 데이터베이스로 사용하려는 ODBC 데이터 소스를 선택한 다음 확인을 클릭합니다. 새 DSN을 구성하려면 새로 만들기를 클릭합니다. 필요한 경우 데이터베이스 자격 증명을 입력하고 확인을 클릭합니다.
 - 네이티브 드라이버를 선택한 경우 데이터베이스 서버 이름, 사용자의 로그인 ID 및 암호를 입력하라는 메시지가 표시됩니다. 그러한 정보를 입력한 다음 확인을 클릭합니다.

CMS 데이터베이스 설정이 완료되면 관련 메시지가 CCM에 나타납니다.

5. 속성 대화 상자에서 확인을 클릭합니다.
6. Server Intelligence Agent를 다시 시작합니다.

9.2.2 UNIX에서 새 CMS 데이터베이스 또는 기존 데이터베이스 선택

cmsdbsetup.sh 스크립트를 사용합니다. 자세한 내용은 UNIX 도구 관련 장을 참조하십시오.

1. cmsdbsetup.sh 스크립트(기본 위치: <InstallDirectory>/sap_bobj/)를 실행합니다.
2. 업데이트 작업(옵션 6)을 선택합니다.
3. 새 CMS 데이터베이스의 데이터베이스 유형을 묻는 메시지가 나타나면 해당 정보를 입력합니다.

4. 호스트 이름, 사용자 이름, 암호 등과 같은 데이터베이스 정보를 입력합니다.
CMS 데이터베이스가 새 위치를 가리키면 알림 메시지가 나타납니다.
5. SIA(Server Intelligence Agent)를 다시 작성하라는 메시지가 나타나면 CMS에서 통신에 사용할 포트 번호와 관리자 암호를 입력합니다.

참고:

비어 있는 CMS 데이터베이스를 가리키는 경우에만 이 정보를 입력하라는 메시지가 표시됩니다.

9.3 CMS 시스템 데이터베이스 다시 만들기

다음 절차에서는 현재 CMS 시스템 데이터베이스를 다시 작성(다시 초기화)하는 방법을 보여 줍니다. 이 작업을 수행하면 이미 데이터베이스에 들어 있는 데이터가 모두 소멸됩니다. 이 절차는 직접 만든 사용자 지정 웹 응용 프로그램을 디자인하고 테스트하기 위한 개발 환경에 SAP BusinessObjects Business Intelligence 플랫폼을 설치한 경우에 유용합니다. 시스템에서 CMS 시스템 데이터베이스의 데이터를 모두 삭제해야 할 때마다 개발 환경에서 이 데이터베이스를 다시 초기화할 수 있습니다.

주의:

이 워크플로에서 설명하는 단계를 수행하면 CMS 데이터베이스의 모든 데이터뿐만 아니라 보고서 및 사용자 등의 개체가 삭제됩니다. 프로덕션 배포 환경에서는 이 단계를 수행하지 마십시오.

CMS 시스템 데이터베이스를 다시 초기화하기 전에는 모든 서버 구성 설정을 백업해야 합니다. 데이터베이스를 다시 만들면 서버 구성 설정이 삭제되므로 이 정보를 복원하기 위해서는 백업이 있어야 합니다.

시스템 데이터베이스를 다시 만들 때 기존 라이선스 키는 데이터베이스에 그대로 있어야 합니다. 그러나 라이선스 키를 다시 입력해야 하는 경우에는 기본 관리자 계정으로 CMC에 로그인하십시오. 권한 부여 관리 영역으로 이동한 다음 라이선스 키 탭에서 정보를 입력합니다.

참고:

CMS 시스템 데이터베이스를 다시 초기화하면 현재 CMS 시스템 데이터베이스의 모든 데이터가 삭제됩니다. 따라서 작업을 시작하기 전에 현재 데이터베이스를 백업하는 것이 좋습니다. 필요한 경우 데이터베이스 관리자에게 문의하십시오.

관련 항목

- 471 페이지에서 [서버 설정 백업](#)

9.3.1 Windows에서 CMS 시스템 데이터베이스 다시 만들기

1. CCM을 사용하여 SIA(Server Intelligence Agent)를 중지합니다.

참고:

이 절차를 수행할 때는 원격 컴퓨터에서 CCM을 실행할 수 없습니다. 적어도 한 개 이상의 유효한 노드가 있는 컴퓨터에서 이를 실행해야 합니다.

2. SIA를 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.
3. 속성 대화 상자에서 구성 탭으로 이동한 후 지정을 클릭합니다.
4. CMS 데이터베이스 설정 대화 상자에서 현재 데이터 소스 다시 생성을 클릭합니다.

참고:

1단계에서 CCM을 실행한 컴퓨터의 서버와 개체도 모두 다시 만들어집니다.

5. 확인을 클릭하고 확인 메시지가 나타나면 예를 클릭합니다.
6. CMS 시스템 데이터베이스에 대한 암호를 지정하고 확인을 클릭합니다.
CMS 시스템 데이터베이스 설정이 완료되면 관련 메시지가 CCM에 나타납니다.
7. 확인을 클릭합니다.
CCM으로 돌아옵니다.
8. Server Intelligence Agent를 다시 시작하고 서비스를 활성화합니다.
이때 Server Intelligence Agent에서 CMS를 시작합니다. CMS는 새로 만든 빈 데이터 소스에 필요한 시스템 데이터를 씁니다.
9. 배포에 여러 대의 컴퓨터가 포함되어 있으면 다른 컴퓨터에서 노드를 다시 만들어야 합니다.

9.3.2 UNIX에서 CMS 시스템 데이터베이스 다시 만들기

cmsdbsetup.sh 스크립트를 사용합니다. 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드의 UNIX 도구 장을 참조하십시오.

1. cmsdbsetup.sh(기본 위치: <INSTALLDIR>/sap_bobj/)를 실행합니다.
2. "다시 초기화" 옵션(옵션 5)을 선택하고 선택 사항을 확인합니다.
cmsdbsetup.sh 스크립트가 CMS 시스템 데이터베이스를 다시 만드는 과정을 시작합니다.
3. CMS 시스템 데이터베이스 암호를 제공합니다.
4. 데이터베이스 작성이 완료되면 cmsdbsetup.sh 스크립트를 종료합니다.
5. 호스트 이름, 사용자 이름, 암호 등과 같은 데이터베이스 정보를 입력합니다.
CMS 데이터베이스가 새 위치를 가리키면 알림 메시지가 나타납니다.

6. SIA(Server Intelligence Agent)를 다시 작성하라는 메시지가 나타나면 CMS에서 통신에 사용할 포트 번호와 관리자 암호를 입력합니다.

참고:

비어 있는 CMS 데이터베이스를 가리키는 경우에만 이 정보를 입력하라는 메시지가 표시됩니다.

7. <INSTALLEDIR>/sap_bobj/ 디렉터리에서 다음 명령을 사용하여 노드를 시작합니다.

```
ccm.sh -start <nodename>
```

8. 서비스를 활성화하려면 다음 명령을 사용합니다.

```
ccm.sh -enable all -cms <CMSNAME:PORT> -username administrator -password <password>
```

참고:

방금 CMS 데이터베이스를 다시 만든 상태이므로 관리자 암호는 비어 있습니다.

9.4 CMS 시스템 데이터베이스 간에 데이터 복사

중앙 구성 관리자(CCM)에서는 시스템 데이터를 한 데이터베이스 서버에서 다른 데이터베이스 서버로 복사할 수 있습니다. 예를 들어, 데이터베이스를 업그레이드하거나 한 데이터베이스 유형에서 다른 유형으로 옮기려는 관계로 데이터베이스를 다른 데이터베이스로 바꾸려는 경우, 기존 데이터베이스의 콘텐츠를 새 데이터베이스로 복사한 후 서비스를 해제하면 됩니다.

대상 데이터베이스는 새 데이터를 복사하기 전에 초기화되므로 대상 데이터베이스에 포함된 기존 내용은 영구 삭제됩니다. 모든 BI 플랫폼 테이블은 영구적으로 소멸된 다음 다시 작성됩니다. 데이터가 복사된 후에는 대상 데이터베이스가 CMS의 현재 데이터베이스로 설정됩니다.

참고:

이전 버전의 BI 플랫폼에서 현재 버전으로 사용자, 그룹, 폴더 및 보고서를 가져오려면 업그레이드 관리 도구를 사용합니다. 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 업그레이드 가이드를 참조하십시오.

9.4.1 CMS 시스템 데이터베이스 복사 준비

CMS 시스템 데이터베이스를 복사하려면 먼저 모든 서버를 비활성화하고 중지하여 소스 및 대상 환경을 오프라인 상태로 만듭니다. CMS 데이터베이스를 모두 백업하고 모든 입력 및 출력 파일 리포지토리 서버에 사용되는 루트 디렉터리를 백업합니다. 필요한 경우 데이터베이스 또는 네트워크 관리자에게 문의하십시오.

소스 데이터베이스의 모든 데이터를 읽을 수 있는 권한을 가진 데이터베이스 사용자 계정과 대상 데이터베이스에 대한 작성, 삭제 및 업데이트 권한을 가진 데이터베이스 사용자 계정이 있어야 합니다. 데이터베이스를 바꾸려는 CMS 컴퓨터에서 두 데이터베이스에 모두 연결할 수 있는지 확인해야 합니다. 이러한 연결은 구성에 따라 데이터베이스 클라이언트 소프트웨어 또는 ODBC를 통해 이루어집니다.

현재 위치에서 다른 데이터베이스 서버로 CMS 데이터베이스를 복사하는 경우 현재 CMS 데이터베이스는 소스 환경입니다. 이 데이터베이스의 내용은 대상 데이터베이스에 복사되고 이 데이터베이스는 현재 CMS에 대한 활성 데이터베이스로 설정됩니다. 기존의 기본 데이터베이스에서 Microsoft SQL Server, Informix, Oracle, DB2, Sybase 같은 전용 데이터베이스 서버로 기본 CMS 데이터베이스를 옮기려는 경우 이 절차를 수행합니다. 데이터베이스를 이동하고자 하는 CMS가 실행되고 있는 컴퓨터에 관리 계정을 사용하여 로그인합니다.

참고:

- 데이터베이스 사이에서 데이터를 복사하는 경우, 대상 데이터베이스는 새 데이터를 복사하기 전에 초기화됩니다. 즉, 대상 데이터베이스에 SAP BusinessObjects Business Intelligence 플랫폼 시스템 테이블이 포함되어 있지 않은 경우에는 이러한 테이블이 작성됩니다. 대상 데이터베이스에 SAP BusinessObjects Business Intelligence 플랫폼 시스템 테이블이 포함되어 있으면 해당 테이블이 영구 삭제되고 새 시스템 테이블이 작성된 다음 소스 데이터베이스에서 새 테이블로 데이터가 복사됩니다. 데이터베이스의 다른 테이블은 영향을 받지 않습니다.
- Windows에서 CMS 시스템 데이터베이스를 MaxDB 대상 데이터베이스로 복사하는 경우 MaxDB 클라이언트의 경로가 PATH 환경 변수에 추가되었는지 확인해야 합니다 (예: ;C:\WProgram Files\Wsdb\MAXDB1\Wpgm).

9.4.2 Windows에서 CMS 시스템 데이터베이스 복사

CMS 데이터베이스의 콘텐츠를 복사하기 전에 대상 데이터베이스의 테이블을 추가 또는 삭제하거나 해당 테이블의 데이터를 추가, 삭제 또는 수정할 수 있는 권한이 있는 계정을 사용하여 대상 데이터베이스에 로그인할 수 있는지 확인해야 합니다.

1. 중앙 구성 관리자(CCM)를 열고 SIA(Server Intelligences Agent)를 중지합니다.
2. SIA를 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.
3. 구성 탭을 클릭한 후 지정을 클릭합니다.
4. 복사를 선택하고 확인을 클릭합니다.
5. 소스 CMS 데이터베이스의 데이터베이스 유형을 선택한 다음, 호스트 이름, 사용자 이름 및 암호 등 데이터베이스 정보를 지정합니다.
6. 대상 CMS 데이터베이스의 데이터베이스 유형을 선택한 다음, 해당 데이터베이스 정보(예: 호스트 이름, 사용자 이름 및 암호 등)를 지정합니다.
7. CMS 데이터베이스 복사가 끝나면 확인을 클릭합니다.

9.4.3 UNIX에 설치된 CMS에서 데이터 복사

CMS 데이터베이스의 콘텐츠를 복사하기 전에 대상 데이터베이스의 테이블을 추가 또는 삭제하거나 해당 테이블의 데이터를 추가, 삭제 또는 수정할 수 있는 권한이 있는 계정을 사용하여 대상 데이터베이스에 로그인할 수 있는지 확인해야 합니다.

참고:

UNIX의 경우에는 CMS 데이터베이스와의 ODBC 연결을 사용하는 소스 환경에서 직접 마이그레이션할 수 없습니다. 소스 CMS 데이터베이스에서 ODBC를 사용하는 경우에는 지원되는 네이티브 드라이버로 시스템을 먼저 업그레이드해야 합니다.

1. 다음 명령을 입력하여 CMS를 중지합니다.
`./ccm.sh -stop <nodename>`
 2. `cmsdbsetup.sh`(기본 위치: `<InstallDirectory>/sap_bobj/`)를 실행합니다.
 3. 복사 옵션(옵션 4)을 선택하고 선택 사항을 확인합니다.
 4. 소스 CMS 데이터베이스의 데이터베이스 유형을 선택한 다음, 해당 데이터베이스 정보(예: 호스트 이름, 사용자 이름 및 암호 등)를 지정합니다.
 5. 대상 CMS 데이터베이스의 데이터베이스 유형을 선택한 다음, 해당 데이터베이스 정보(예: 호스트 이름, 사용자 이름 및 암호 등)를 지정합니다.
- CMS 데이터베이스가 대상 데이터베이스로 복사됩니다. 복사가 완료되면 메시지가 표시됩니다.

장10 웹 응용 프로그램 컨테이너 서버(WACS) 관리

10.1 WACS

10.1.1 웹 응용 프로그램 컨테이너 서버(WACS)

웹 응용 프로그램 컨테이너 서버(WACS)는 BI 플랫폼 웹 응용 프로그램을 호스팅하기 위한 플랫폼을 제공합니다. 예를 들어, 중앙 관리 콘솔(CMC)을 WACS에서 호스팅할 수 있습니다.

WACS는 이전에 응용 프로그램 서버를 구성하고 웹 응용 프로그램을 배포하는 데 요구되었던 수많은 워크플로를 제거하고 간소화되고 일관성 있는 관리 인터페이스를 제공하여 시스템 관리 작업을 간소화합니다.

웹 응용 프로그램은 WACS에 자동으로 배포됩니다. WACS는 BI 플랫폼이나 외부 웹 응용 프로그램의 수동 또는 WDeploy 배포를 지원하지 않습니다.

10.1.1.1 WACS 필요 여부

SAP Business Objects 웹 응용 프로그램을 호스팅하는 데 Java 응용 프로그램 서버를 사용하지 않으려는 경우 이러한 웹 응용 프로그램을 WACS에서 호스팅할 수 있습니다.

지원되는 Java 응용 프로그램 서버를 사용하여 SAP BusinessObjects Business Intelligence 플랫폼 웹 응용 프로그램을 배포하거나 UNIX 시스템에 SAP BusinessObjects Business Intelligence 플랫폼을 설치하는 경우에는 WACS를 설치하여 사용할 필요가 없습니다.

10.1.1.2 WACS를 사용할 때의 장점

WACS를 사용하여 CMC를 호스팅하는 방법에는 몇 가지 장점이 있습니다.

- 설치, 유지 관리 및 구성에 필요한 작업이 최소화됩니다.
- 호스팅되는 모든 응용 프로그램이 WACS에 사전 배포되므로 추가 단계를 수동으로 실행할 필요가 없습니다.
- WACS는 SAP의 지원을 받습니다.
- Java 응용 프로그램 서버 관리 및 유지 관리 기술이 없어도 됩니다.
- 다른 SAP BusinessObjects Business Intelligence 플랫폼 서버와 일관성 있는 관리 인터페이스가 제공됩니다.

10.1.1.3 일반 작업

작업	설명	항목
WACS에서 호스팅되는 웹 응용 프로그램 또는 웹 서비스의 성능을 향상시킬 수 있는 방법	여러 대의 컴퓨터에 WACS를 설치하면 웹 응용 프로그램 또는 웹 서비스의 성능을 향상시킬 수 있습니다.	<ul style="list-style-type: none"> 438 페이지에서 "추가 WACS를 배포에 추가 또는 제거" 441 페이지에서 "웹 응용 프로그램 컨테이너 서버 복제"
web-tier의 가용성을 향상시키는 방법	배포 환경에서 WACS를 추가로 만들면 특정 서버에서 하드웨어 또는 소프트웨어 실패가 발생하는 경우에도 다른 서버에서 계속해서 요청을 처리할 수 있습니다.	438 페이지에서 "추가 WACS를 배포에 추가 또는 제거"
잘못 구성된 CMC로부터 간편하게 복구할 수 있는 환경을 만드는 방법	중지된 보조 WACS를 만들고 이 WACS를 사용하여 구성 템플릿을 정의합니다. 기본 WACS가 잘못 구성된 경우 첫 번째 서버를 구성할 때까지 보조 WACS를 사용하거나 첫 번째 서버에 구성 템플릿을 적용합니다.	438 페이지에서 "추가 WACS를 배포에 추가 또는 제거"
클라이언트와 WACS 사이의 통신 보안을 강화하는 방법	WACS에서 HTTPS를 구성합니다.	<ul style="list-style-type: none"> 443 페이지에서 "HTTPS/SSL 구성" 461 페이지에서 "방화벽과 함께 WACS 사용"
배포 환경에서 WACS와 기타 Business Objects 서버 사이의 통신 보안을 강화하는 방법	배포 환경에서 WACS와 기타 SAP BusinessObjects Business Intelligence 플랫폼 서버 사이에 SSL 통신을 구성합니다.	<ul style="list-style-type: none"> 161 페이지에서 "SSL에 대해 서버 구성" 461 페이지에서 "방화벽과 함께 WACS 사용"
HTTPS 및 역방향 프록시를 통해 WACS를 사용하는 방법	두 개의 WACS를 만들고 두 서버를 HTTPS로 구성하는 경우 HTTPS 및 역방향 프록시를 통해 WACS를 사용할 수 있습니다. 내부 네트워크의 통신에는 첫 번째 WACS를 사용하고 역방향 프록시를 통한 외부 네트워크 통신에는 다른 WACS를 사용합니다.	461 페이지에서 "역방향 프록시로 HTTPS를 지원하도록 WACS를 구성하려면"
IT 환경에 맞게 WACS를 사용하는 방법	WACS는 기존 웹 서버, 하드웨어 부하 분산, 역방향 프록시 및 방화벽을 사용하는 IT 환경에 배포할 수 있습니다.	<ul style="list-style-type: none"> 459 페이지에서 "WACS를 다른 웹 서버로 사용" 459 페이지에서 "WACS를 부하 분산으로 사용" 460 페이지에서 "WACS를 역방향 프록시로 사용" 461 페이지에서 "방화벽과 함께 WACS 사용"

작업	설명	항목
부하 분산을 사용하는 배포 환경에서 WACS를 이용하는 방법	하드웨어 부하 분산을 사용하는 배포 환경에서 WACS를 이용할 수 있습니다. WACS 자체는 부하 분산으로 사용할 수 없습니다.	459 페이지에서 "WACS를 부하 분산으로 사용"
역방향 프록시를 사용하는 배포 환경에서 WACS를 이용하는 방법	역방향 프록시를 사용하는 배포 환경에서 WACS를 이용할 수 있습니다. WACS 자체는 역방향 프록시로 사용할 수 없습니다.	460 페이지에서 "WACS를 역방향 프록시로 사용"
내 WACS 서버에서 문제를 해결하는 방법	WACS 성능이 떨어지는 이유 및 원인을 파악해야 하는 경우 로그 파일과 시스템 메트릭을 확인할 수 있습니다.	<ul style="list-style-type: none"> 463 페이지에서 "WACS에서 추적 구성" 463 페이지에서 "서버 메트릭 보기"
특정 포트에서 어떤 페이지도 표시되지 않는 경우 해결 방법	<p>WACS에 연결할 수 없는 데는 여러 가지 이유가 있습니다. 다음을 확인합니다.</p> <ul style="list-style-type: none"> WACS에 대해 지정한 HTTP, HTTP through proxy 및 HTTPS 포트를 다른 응용 프로그램에서 사용하고 있는지 확인합니다. WACS에 할당된 메모리가 충분한지 확인합니다. WACS에서 허용하는 동시 요청 수가 충분한지 확인합니다. 필요한 경우 WACS에 대한 값을 시스템 기본값으로 복원합니다. 	<ul style="list-style-type: none"> 465 페이지에서 "HTTP 포트 충돌을 해결하려면" 466 페이지에서 "메모리 설정 변경" 466 페이지에서 "동시 요청 수 변경" 467 페이지에서 "시스템 기본값 복원"
WACS에서 호스팅되는 웹 응용 프로그램의 속성을 구성할 수 있는 방법	웹 응용 프로그램의 속성을 구성하는 절차는 특정 속성 및 웹 응용 프로그램에 따라 다릅니다. 자세한 내용은 이 장의 웹 응용 프로그램 속성 구성 단원을 참조하십시오.	462 페이지에서 "웹 응용 프로그램 속성 구성"
WACS 속성 목록을 찾는 방법	이 가이드의 서버 속성 부록에 WACS 속성 목록이 나와 있습니다.	824 페이지에서 "핵심 서비스 속성"

10.1.2 추가 WACS를 배포에 추가 또는 제거

추가 WACS를 배포에 추가하면 여러 가지 이점이 있습니다.

- 잘못 구성된 서버에서 신속한 복구 가능
- 서버 가용성 향상
- 부하 분산 성능 향상
- 전반적인 성능 향상

다음과 같은 세 가지 방식으로 추가 WACS를 배포에 추가할 수 있습니다.

- 컴퓨터에 WACS 설치
- 새 WACS 만들기
- WACS 복제

참고:

높은 리소스 사용량을 야기할 수 있으므로 동일한 컴퓨터에서 한 번에 하나의 WACS만 실행하는 것이 좋습니다. 그러나 동일한 컴퓨터에서 WACS를 하나 이상 배포할 수 있으며 이중 하나를 실행하여 WACS가 잘못 구성된 경우 복원할 수 있습니다.

10.1.2.1 WACS 설치

별도의 컴퓨터에 WACS를 설치하면 배포 성능은 물론 부하 분산 성능 및 서버 가용성이 향상됩니다. 배포 시 별도의 컴퓨터에 두 개 이상의 WACS를 설치하는 경우 하드웨어나 소프트웨어 오류가 발생한다고 해도 다른 WACS가 계속해서 서비스를 제공하므로 웹 응용 프로그램과 웹 서비스의 가용성에 문제가 생기는 일은 없습니다.

웹 응용 프로그램 컨테이너 서버는 BI 플랫폼 설치 프로그램을 사용하여 설치할 수 있습니다. 다음 두 가지 방법으로 WACS를 설치할 수 있습니다.

- 전체 설치에서는 Java 웹 응용 프로그램 선택 화면에서 웹 응용 프로그램 컨테이너 서버를 설치하고 이 서버에 웹 응용 프로그램과 서비스를 자동으로 배포합니다.를 선택합니다.

새 설치에서 Java 응용 프로그램을 선택한 경우 WACS가 설치되지 않습니다.

- 사용자 지정 설치/확장 설치의 기능 선택 화면에서 서버 > 플랫폼 서비스를 확장하고 웹 응용 프로그램 컨테이너 서버를 선택하여 WACS를 설치하도록 선택할 수 있습니다.

WACS를 설치하는 경우 설치 프로그램에서 <NODE>.WebApplicationContainerServer라는 이름의 서버를 자동으로 만들며 이때 <NODE>는 노드 이름입니다. BI 플랫폼 웹 응용 프로그램 및 웹 서비스가 해당 서버에 배포됩니다. CMC를 배포하고 구성하기 위해 사용자가 직접 수행해야 하는 내용은 없습니다. 이제 시스템을 사용할 수 있습니다.

WACS를 설치하는 경우 설치 프로그램에서 WACS에 대한 HTTP 포트 번호를 묻는 메시지를 표시합니다. 사용하지 않는 포트 번호를 지정해야 합니다. 기본 포트 번호는 6405입니다. 사용자가 방화벽 외부에서 WACS에 연결하도록 허용하려면 방화벽에서 서버의 HTTP 포트를 열어 두어야 합니다.

WACS는 Windows 운영 체제에서만 지원됩니다.

참고:

WACS에서 호스팅하는 웹 응용 프로그램은 WACS를 설치할 때 또는 WACS나 WACS에서 호스팅되는 웹 응용 프로그램에 업데이트 또는 핫픽스를 적용할 때 자동으로 배포됩니다. 웹 응용 프로그램이 배포되려면 몇 분이 걸립니다. 웹 응용 프로그램 배포가 끝나기 전에는 WACS가 초기화 중 상태입니다. 사용자는 웹 응용 프로그램이 완전히 배포될 때까지 WACS에서 호스팅하는 웹 응용 프로그램에 액세스할 수 없습니다. 최초 배포가 완료될 때까지 서버를 중지하지 마십시오. 중앙 구성 관리자(CCM)를 통해 WACS의 서버 상태를 확인할 수 있습니다.

이러한 지연은 WACS를 설치하거나 업데이트를 적용한 후 WACS를 처음 시작할 때만 발생합니다. 이후에 WACS를 다시 시작할 때는 이러한 지연이 없습니다.

웹 응용 프로그램을 WACS 서버에 수동으로 배포할 수는 없습니다. WDeploy를 사용하여 웹 응용 프로그램을 WACS에 배포할 수 없습니다.

10.1.2.2 새 웹 응용 프로그램 컨테이너 서버 추가

참고:

높은 리소스 사용량을 야기할 수 있으므로 동일한 컴퓨터에서 한 번에 하나의 WACS만 실행하는 것이 좋습니다. 그러나 동일한 컴퓨터에서 WACS를 하나 이상 배포할 수 있으며 이중 하나를 실행하여 WACS가 잘못 구성된 경우 복원할 수 있습니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 관리 > 새로 만들기 > 새 서버를 선택합니다.
새 서버 만들기 화면이 나타납니다.
3. 서비스 범주 목록에서 핵심 서비스를 선택합니다.
4. 서비스 선택 목록에서 WACS에서 호스팅할 서비스를 선택하고 다음을 클릭합니다.
 - WACS에서 CMC, BI 실행 패드 또는 OpenDocument와 같은 웹 응용 프로그램을 호스팅하도록 하려면 BOE 웹 응용 프로그램 서비스를 선택합니다.
 - WACS에서 Live Office 또는 QaaWS(Query as a Web Service)와 같은 웹 서비스를 호스팅하도록 하려면 웹 서비스 SDK 및 QaaWS를 선택합니다.
 - WACS에서 비즈니스 프로세스 BI 웹 서비스를 호스팅하도록 하려면 비즈니스 프로세스 BI 웹 서비스를 선택합니다.
 - WACS에서 서버 추적을 지원하도록 하려면 TraceLog 서비스를 선택합니다.
5. 다음 새 서버 만들기 화면에서 WACS에서 호스팅할 추가 서비스를 선택하고 다음을 클릭합니다.

6. 다음 새 서버 만들기 화면에서 다음을 클릭합니다.
7. 다음 서버 만들기 화면에서 서버를 추가할 노드를 선택하고 서버 이름 및 서버에 대한 설명을 입력한 후 만들기를 클릭합니다.

참고:

WACS가 설치되어 있는 노드만 노드 목록에 나타납니다.

8. 서버 화면에서 새로 만든 WACS를 두 번 클릭합니다.
속성 화면이 나타납니다.
9. 시스템을 다시 시작할 때 WACS가 자동으로 시작되지 않도록 하려면 일반 설정 창에서 Server Intelligence Agent가 시작되면 자동으로 이 서버 시작 확인란의 선택이 취소되었는지 확인합니다.
10. 저장 후 단기를 클릭합니다.
새 WACS가 만들어졌습니다. 기본 설정 및 속성이 해당 서버에 적용됩니다.

10.1.2.3 웹 응용 프로그램 컨테이너 서버 복제

새 WACS를 배포에 추가하는 다른 방법으로 WACS를 같은 컴퓨터 또는 다른 컴퓨터로 복제하는 방법이 있습니다. 새 WACS를 추가하면 기본 설정으로 서버가 만들어지지만 WACS를 복제하면 원본 WACS의 설정이 새 WACS에 적용됩니다.

서버는 WACS가 이미 설치되어 있는 컴퓨터에만 복제할 수 있습니다.

참고:

높은 리소스 사용량을 야기할 수 있으므로 동일한 컴퓨터에서 한 번에 하나의 WACS만 실행하는 것이 좋습니다. 그러나 동일한 컴퓨터에서 WACS를 하나 이상 배포할 수 있으며 이중 하나를 실행하여 WACS가 잘못 구성된 경우 복원할 수 있습니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 복제할 WACS를 선택하고 복제 서버를 마우스 오른쪽 단추로 클릭하고 선택합니다.
복제 서버 화면에 WACS를 복제할 수 있는 배포 환경의 노드 목록이 표시됩니다. WACS가 설치되어 있는 노드만 노드에 복제 목록에 나타납니다.
3. 복제 서버 화면에서 새 서버 이름을 입력하고 서버를 복제할 노드를 선택하고 확인을 클릭합니다.
새 WACS가 만들어졌습니다. 새 서버에는 원본 복제 서버와 동일한 서비스가 포함되어 있습니다. 대상 서버에서 호스팅하는 대상 서버와 서비스에는 복제 원본 서버와 동일한 설정이 포함되며 단, 서버 이름은 예외입니다.

참고:

WACS를 동일한 컴퓨터에 복제한 경우 복제에 사용된 WACS와 포트 충돌이 발생할 수 있습니다. 충돌이 발생하는 경우 새로 복제된 WACS 인스턴스에서 포트 번호를 변경해야 합니다.

관련 항목

- 465 페이지에서 [HTTP 포트 충돌을 해결하려면](#)

10.1.2.4 배포 환경에서 WACS 삭제

서버에서 현재 CMC 서비스를 제공하지 않는 경우에만 WACS를 삭제할 수 있습니다. 배포에서 WACS를 삭제하려면 다른 WACS 또는 Java 응용 프로그램 서버에서 CMC에 로그인해야 합니다. 현재 CMC 서비스를 제공하고 있는 WACS는 삭제할 수 없습니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 서버를 마우스 오른쪽 단추로 클릭하고 서버 중지를 클릭하여 삭제할 서버를 중지합니다.
3. 서버를 마우스 오른쪽 단추로 클릭하고 삭제를 클릭합니다.
4. 확인 메시지가 나타나면 확인을 클릭합니다.

10.1.3 WACS에 서비스 추가 또는 제거

10.1.3.1 WACS에 웹 응용 프로그램 또는 웹 서비스 추가

WACS에 추가 BI 플랫폼 웹 응용 프로그램 또는 웹 서비스를 추가하려면 WACS를 중지해야 합니다. 따라서 WACS를 중지하고 다른 WACS에 서비스를 추가하는 동안 BOE 웹 응용 프로그램 서비스를 제공하는 적어도 하나의 CMC가 배포 환경의 WACS에서 추가로 호스팅되고 있어야 합니다.

WACS에 서비스를 추가하면 서버가 다시 시작될 때 서비스가 자동으로 WACS에 배포됩니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 서비스를 추가할 WACS를 두 번 클릭하고 추가하려는 서비스가 아직 없는지 서버 속성을 확인합니다.
3. 서버 화면으로 돌아가려면 취소를 클릭합니다.
4. 서버를 마우스 오른쪽 단추로 클릭한 다음 서버 중지를 클릭하여 서버를 중지합니다.

현재 CMC 서비스를 제공하고 있는 WACS를 중지하는 경우 경고 메시지가 나타납니다. 배포 환경의 다른 WACS에서 추가로 실행 중인 BOE 웹 응용 프로그램 서비스가 하나 이상일 경우에만 진행하십시오. 이러한 조건에 맞는 경우 확인을 클릭하고 다른 WACS에 로그인한 다음 이 절차를 처음부터 다시 시작합니다.

5. 서버를 마우스 오른쪽 단추로 클릭하고 서비스 선택을 선택합니다.
서비스 선택 화면이 나타납니다.
6. 서버에 추가할 서비스를 선택하고 >를 클릭하여 서비스를 서버에 추가한 다음 확인을 클릭합니다.
7. 서버를 마우스 오른쪽 단추로 클릭한 다음 서버 시작을 클릭하여 WACS를 시작합니다.
서비스가 WACS에 추가됩니다. 서비스에 대한 기본 설정 및 속성이 적용됩니다.

10.1.3.2 WACS에서 웹 응용 프로그램 또는 웹 서비스 제거

WACS에서 웹 응용 프로그램 또는 웹 서비스를 제거하려면 다른 WACS 또는 Java 응용 프로그램 서버에서 CMC에 로그인해야 합니다. 현재 CMC 서비스를 제공하고 있는 WACS는 중지할 수 없습니다.

WACS에서 마지막 서비스를 삭제할 수 없습니다. 따라서 WACS에서 웹 서비스를 제거하는 경우 서버에서 적어도 하나의 다른 서비스를 호스팅 중이어야 합니다.

WACS에서 마지막 서비스를 제거하려면 WACS 자체를 삭제합니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 웹 서비스를 제거할 WACS를 두 번 클릭하고 제거하려는 서비스가 있는지 서버 속성을 확인합니다.
3. 서버 화면으로 돌아가려면 취소를 클릭합니다.
4. 서버를 마우스 오른쪽 단추로 클릭한 다음 서버 중지를 클릭하여 WACS를 중지합니다.
현재 CMC 서비스를 제공하고 있는 WACS를 중지하는 경우 경고 메시지가 나타납니다. 배포 환경의 다른 WACS에서 추가로 실행 중인 BOE 웹 응용 프로그램 서비스가 하나 이상일 경우에만 진행하십시오. 이러한 조건에 맞는 경우 확인을 클릭하고 다른 WACS에 로그인한 다음 이 절차를 처음부터 다시 시작합니다.
5. WACS를 마우스 오른쪽 단추로 클릭하고 서비스 선택을 선택합니다.
서비스 선택 화면이 나타납니다.
6. 제거할 서비스를 선택하고 <를 클릭한 다음 확인을 클릭합니다.
7. 서버를 마우스 오른쪽 단추로 클릭한 다음 서버 시작을 클릭하여 WACS를 시작합니다.
서비스가 WACS에서 제거됩니다.

10.1.4 HTTPS/SSL 구성

SAP BusinessObjects Business Intelligence 플랫폼 배포 환경에서 클라이언트와 WACS 간의 모든 네트워크 통신에 SSL(Secure Sockets Layer) 프로토콜과 HTTP를 사용할 수 있습니다. SSL/HTTPS는 네트워크 트래픽을 암호화하고 보안을 강화합니다.

SSL에는 두 가지 유형이 있습니다.

- 배포 환경에서 WACS 및 기타 SAP BusinessObjects Business Intelligence 플랫폼 서버를 포함한 SAP BusinessObjects Business Intelligence 플랫폼 서버 간에 사용되는 SSL. 이를 CorbaSSL이라고 합니다. 배포 환경에서 SAP BusinessObjects Business Intelligence 플랫폼 서버 간에 SSL을 사용하는 방법은 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드의 방화벽을 사용한 작업 장에서 SAP BusinessObjects Business Intelligence 플랫폼 구성 요소 사이의 통신 이해 단원을 참조하십시오.
- WACS와 통신하는 클라이언트(예: 브라우저) 사이에 사용되는 HTTP over SSL

참고:

프록시 또는 역방향 프록시가 있는 배포 환경에 WACS를 배포하는 경우 SSL을 사용하여 배포 환경의 네트워크 통신 보안을 강화하려면 WACS를 두 개 만들어야 합니다. 자세한 내용은 WACS를 역방향 프록시로 사용을 참조하십시오.

WACS에서 HTTPS/SSL을 구성하려면 다음 단계를 수행해야 합니다.

- 인증서와 개인 키가 들어 있는 PKCS12 인증서 저장소 또는 JKS keystore를 생성하거나 가져옵니다. Microsoft 인터넷 정보 서비스(IIS) 및 MMC(Microsoft Management Console)를 사용하여 PKCS12 파일을 생성하거나 openssl 또는 Java keytool 명령줄 도구를 사용하여 keystore 파일을 생성할 수 있습니다.
- 특정 클라이언트만 WACS에 연결하려는 경우에는 인증서 신뢰 목록 파일을 생성해야 합니다.
- 인증서 저장소와 인증서 신뢰 목록 파일이 있는 경우(필요한 경우) 파일을 WACS 컴퓨터에 복사합니다.
- WACS에서 HTTPS를 구성합니다.

관련 항목

- 169 페이지에서 [BI 플랫폼 구성 요소 간의 통신 이해](#)
- 460 페이지에서 [WACS를 역방향 프록시로 사용](#)

10.1.4.1 PKCS12 인증서 파일 저장소를 생성하려면

다양한 방법과 도구를 사용하여 PKCS12 인증서 파일 저장소 또는 Java keystores를 생성할 수 있습니다. 사용 가능 여부와 익숙한 정도에 따라 다른 방법을 사용할 수 있습니다.

다음 예에서는 Microsoft IIS(인터넷 정보 서비스)와 MMC(Microsoft Management Console)를 사용하여 PKCS12 파일을 생성하는 방법을 보여 줍니다.

1. WACS를 호스팅하는 컴퓨터에 관리자로 로그인합니다.
2. IIS에서 인증 기관의 인증서를 요청합니다. 자세한 내용은 IIS 도움말 문서를 참조하십시오.
3. 시작 > 실행을 클릭하고 mmc.exe를 입력한 다음 확인을 클릭하여 MMC를 시작합니다.
4. MMC에 인증서 스냅인을 추가합니다.
 - a. 파일 메뉴에서 스냅인 추가/제거를 클릭합니다.
 - b. 추가를 클릭합니다.
 - c. 독립 실행형 스냅인 추가 대화 상자에서 인증서를 선택하고 추가를 클릭합니다.
 - d. 컴퓨터 계정을 선택하고 다음을 클릭합니다.
 - e. 로컬 컴퓨터를 선택하고 마침을 클릭합니다.
 - f. 닫기를 클릭하고 확인을 클릭합니다.
 인증서 스냅인이 MMC에 추가됩니다.
5. MMC에서 인증서를 확장하고 사용할 인증서를 선택합니다.
6. 작업 메뉴에서 모든 작업 > 내보내기를 선택합니다.
인증서 내보내기 마법사가 시작됩니다.
7. 다음을 클릭합니다.
8. 예, 개인 키를 내보냅니다.를 선택하고 다음을 클릭합니다.
9. 개인 정보 교환 - PKCS #12(.PFX)를 선택하고 다음을 클릭합니다.
10. 인증서를 만들 때 사용한 암호를 입력하고 다음을 클릭합니다. WACS에 대한 HTTPS를 구성할 때 개인 키 액세스 암호 필드에 이 암호를 지정해야 합니다.
PKCS12 인증서 파일 저장소가 만들어집니다.

10.1.4.2 인증서 신뢰 목록을 생성하려면

1. WACS를 호스팅하는 컴퓨터에 관리자로 로그인합니다.
2. MMC(Microsoft Management Console)를 시작합니다.
3. 인터넷 정보 서비스 스냅인을 추가합니다.
 - a. 파일 메뉴에서 스냅인 추가/제거를 선택하고 추가를 클릭합니다.
 - b. In the 독립 실행형 스냅인 추가 대화 상자에서 인터넷 정보 서비스(IIS) 관리자를 선택하고 추가를 클릭합니다.
 - c. 닫기를 클릭하고 확인을 클릭합니다.
IIS 스냅인이 MMC에 추가됩니다.

4. MMC의 왼쪽 창에서 인증서 신뢰 목록을 만들 웹 사이트를 찾습니다.
5. 웹 사이트를 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.
6. 디렉터리 보안 탭을 클릭하고 보안 통신에서 편집을 클릭합니다.
7. 인증서 신뢰 목록 사용을 선택하고 새로 만들기를 클릭합니다.
인증서 신뢰 목록 마법사가 시작됩니다.
8. 다음을 클릭합니다.
9. 저장소에서 추가 또는 파일에서 추가를 클릭하고 인증서 신뢰 목록에 추가할 인증서를 선택한 후 확인, 다음을 차례로 클릭합니다.
10. 인증서 신뢰 목록에 대한 설명을 입력하고 다음을 클릭합니다
11. 마침을 클릭한 다음 확인을 클릭합니다.
인증서 신뢰 목록이 현재 CTL 필드에 표시됩니다.
12. 인증서 신뢰 목록을 선택하고 편집을 클릭합니다.
인증서 신뢰 목록 마법사가 시작됩니다.
13. 다음을 클릭합니다.
14. 현재 CTL 인증서 목록에서 신뢰 목록을 선택하고 인증서 보기를 클릭합니다.
15. 세부 정보 탭을 클릭하고 파일에 복사를 클릭합니다.
인증서 내보내기 마법사가 시작됩니다.
16. 다음을 클릭합니다.
17. 예, 개인 키를 내보냅니다.를 선택하고 다음을 클릭합니다.
18. 개인 정보 교환 - PKCS #12(.PFX)를 선택하고 다음을 클릭합니다.
19. 인증서를 만들 때 사용한 암호를 입력하고 다음을 클릭합니다. WACS에 대한 HTTPS를 구성할 때 인증서 신뢰 목록 개인 키 액세스 암호 필드에 이 암호를 지정해야 합니다.

10.1.4.3 HTTPS/SSL 구성

WACS에서 HTTPS/SSL을 구성하려면 먼저 PKCS12 파일 또는 JKS keystore를 만들고 해당 파일을 WACS가 호스팅되고 있는 컴퓨터로 복사하거나 이동해야 합니다.

1. MMC의 서버 관리 영역으로 이동합니다.
2. HTTPS를 사용하려는 서버인 WACS를 두 번 클릭합니다.
속성 화면이 나타납니다.
3. HTTPS 구성 섹션에서 HTTPS 사용 확인란을 선택합니다.
4. 호스트 이름 또는 IP 주소에 바인딩 필드에 인증서를 발행하고 WACS에서 바인딩할 IP 주소를 지정합니다.
지정한 IP 주소를 통해 HTTPS 서비스가 제공됩니다.

5. HTTPS 포트 필드에 WACS에서 HTTPS 서비스를 제공할 포트 번호를 지정합니다. 해당 포트는 사용 중이 아닌 포트여야 합니다. 사용자가 방화벽 외부에서 WACS에 연결되도록 허용하려면 해당 포트가 방화벽에서 열려 있어야 합니다.
6. 프록시로 SSL을 구성하는 경우 프록시 호스트 이름 및 프록시 포트 필드에 프록시 서버의 호스트 이름과 포트를 지정합니다.
7. 프로토콜 목록에서 프로토콜을 선택합니다. 다음과 같은 옵션을 사용할 수 있습니다.
 - SSL

SSL은 Secure Sockets Layer 프로토콜로 네트워크 트래픽을 암호화하기 위한 프로토콜입니다.
 - TLS

TLS은 Transport Layer Security 프로토콜로 새롭게 개선된 프로토콜입니다. SSL과 TLS의 차이점은 거의 없으나 TLS가 보다 강력한 암호화 알고리즘을 제공합니다.
8. 인증서 저장소 유형 필드에 인증서의 파일 형식을 지정합니다. 다음과 같은 옵션을 사용할 수 있습니다.
 - PKCS12

Microsoft 도구로 작업하는 것이 더 편한 경우 PKCS12를 선택합니다.
 - JKS

Java 도구로 작업하는 것이 더 편한 경우 JKS를 선택합니다.
9. 인증서 저장소 파일 위치 필드에 인증서 파일 저장소 또는 Java keystore 파일을 복사하거나 이동할 경로를 지정합니다.
10. 개인 키 액세스 암호 필드에 암호를 지정합니다.

PKCS12 인증서 저장소 및 JKS keystore에는 무단 액세스로부터 보호하기 위해 암호로 보호되는 개인 키가 들어 있습니다. 개인 키에 액세스할 수 있는 암호를 지정해야 WACS에서 개인 키에 액세스할 수 있습니다.
11. 인증서 파일 저장소 또는 keystore를 사용하는 것이 좋습니다. 이 경우 저장소에 한 개의 인증서만 있거나 사용할 인증서가 저장소 목록에서 첫 번째 항목으로 있어야 합니다. 한편 하나 이상의 인증서를 포함하고 사용할 인증서가 파일 저장소의 첫 번째 항목이 아닌 경우 인증서 파일 저장소 또는 keystore를 사용하려면 인증서 별칭 필드에 인증서에 대한 별칭을 지정해야 합니다.
12. WACS가 특정 클라이언트로부터 HTTPS 요청만 허용하도록 하려면 클라이언트 인증을 사용합니다.

클라이언트 인증은 사용자를 인증하는 것이 아니며 WACS에서 특정 클라이언트에 대한 HTTPS 요청만 서비스하도록 합니다.

 - a. 클라이언트 인증 사용을 선택합니다.
 - b. 인증서 신뢰 목록 파일 위치에서 신뢰 목록 파일이 들어 있는 PCKS12 파일 또는 JKS keystore의 위치를 지정합니다.

참고:
인증서 신뢰 목록 유형은 인증서 저장소 유형과 같아야 합니다.

 - c. 인증서 신뢰 목록 개인 키 액세스 암호 필드에 인증서 신뢰 목록 파일에 있는 개인 키에 대한 액세스를 보호할 암호를 입력합니다.

참고:

클라이언트 인증을 사용하고 브라우저 또는 웹 서비스 사용자가 인증되지 않은 경우 HTTPS 연결은 거부됩니다.

13. 저장 후 닫기를 클릭합니다.
14. 메트릭 화면으로 이동하여 HTTPS 커넥터가 WACS 커넥터 실행 목록에 나타나는지 확인합니다. HTTPS가 나타나지 않는 경우 HTTPS 커넥터가 올바르게 구성되었는지 확인합니다.

10.1.5 지원되는 인증 방법

WACS에서는 다음과 같은 인증 방법을 지원합니다.

- Enterprise
- LDAP
- AD Kerberos

다음 인증 방법은 WACS에서 지원되지 않습니다.

- NT
- AD NTLM
- 단일 로그인 사용 LDAP

10.1.6 WACS에 대해 AD Kerberos 구성

WACS에 대해 AD Kerberos 인증을 구성하려면 우선 컴퓨터가 AD를 지원하도록 구성해야 합니다. 이를 위해 다음 단계를 수행해야 합니다.

- Windows AD 보안 플러그 인을 활성화합니다.
- 사용자와 그룹을 매핑합니다.
- 서비스 계정을 설정합니다.
- 제한된 위임을 설정합니다.
- WACS용 Windows AD 플러그 인에서 Kerberos 인증을 활성화합니다.
- 구성 파일을 만듭니다.

WACS를 호스팅하는 컴퓨터에서 AD Kerberos 인증을 사용하도록 설정한 후에는 중앙 관리 콘솔(CMC)을 통해 추가 구성 단계를 수행해야 합니다.

관련 항목

- 249 페이지에서 [Windows AD 사용자 및 그룹 사용](#)"
- 249 페이지에서 [Windows AD 보안 플러그 인](#)"
- 252 페이지에서 [Kerberos 사용 AD 인증을 위한 서비스 계정 설정](#)"
- 256 페이지에서 [Kerberos 사용 Windows AD 인증을 위한 서버 준비](#)"
- 449 페이지에서 [WACS용 Windows AD 플러그 인에서 Kerberos 인증 활성화](#)"
- 450 페이지에서 [구성 파일 만들기](#)"
- 453 페이지에서 [AD Kerberos를 사용하도록 WACS 구성](#)"
- 456 페이지에서 [AD Kerberos 단일 로그인 구성](#) "

10.1.6.1 WACS용 Windows AD 플러그 인에서 Kerberos 인증 활성화

Kerberos를 지원하기 위해서는 Kerberos 인증을 사용하도록 CMC에서 Windows AD 보안 플러그 인을 구성해야 합니다. 다음과 같은 작업이 필요합니다.

- Windows AD 인증이 활성화되어 있는지 확인합니다.
- AD 관리자 계정을 입력합니다.

참고:

이 계정에는 Active Directory에 대한 읽기 권한만이 필요하며 다른 권한은 필요하지 않습니다.

-
- 서비스 계정에 대한 SPN(서비스 사용자 이름)을 입력합니다.

10.1.6.1.1 필수 요건

Kerberos를 위한 Windows AD 보안 플러그 인을 구성하려면 먼저 다음 작업을 수행해야 합니다.

- 252 페이지에서 ["Kerberos 사용 AD 인증을 위한 서비스 계정 설정"](#)
- 254 페이지에서 ["서비스 계정에 권한 부여"](#)
- 256 페이지에서 ["Kerberos 사용 Windows AD 인증을 위한 서버 준비"](#)
- "Mapping Windows AD accounts"

10.1.6.1.2 Kerberos용 Windows AD 보안 플러그 인 구성

1. CMC의 인증 관리 영역으로 이동합니다.
2. Windows AD를 두 번 클릭합니다.
3. Windows Active Directory 인증 사용 확인란이 선택되어 있는지 확인합니다.
4. 인증 옵션에서 Kerberos 인증 사용을 선택합니다.
5. 서비스 사용자 이름 필드에서 서비스 계정의 계정과 도메인을 입력하거나 서비스 계정에 대한 SPN 매핑을 입력합니다.

이때 다음 형식을 사용합니다. 여기서 svcacct는 앞서 만든 서비스 계정 또는 SPN의 이름이고 DNS.COM은 대문자로 표시한 정규화된 도메인입니다. 예를 들어, 서비스 계정은 svcacct@DNS.COM이고 SPN은 BOBJCentralMS/some_name@DOMAIN.COM일 수 있습니다.

참고:

- 기본 도메인이 아닌 다른 도메인의 사용자가 로그인할 수 있도록 허용하려면 앞서 매핑한 SPN을 제공해야 합니다.
- 서비스 계정은 대/소문자를 구분합니다. 여기서 입력하는 계정의 대/소문자는 Active Directory 도메인에서 설정된 것과 일치해야 합니다.
- 이 이름은 SAP BusinessObjects Business Intelligence 플랫폼 서버를 실행하는 데 사용할 계정 또는 이 계정에 매핑할 SPN과 같아야 합니다.

관련 항목

- 456 페이지에서 [AD Kerberos 단일 로그인 구성](#) "

10.1.6.2 구성 파일 만들기

응용 프로그램 서버에서 Kerberos를 구성하는 일반적인 과정에는 다음 단계가 포함됩니다.

- Kerberos 구성 파일 만들기
- JAAS 로그인 구성 파일 만들기

참고:

- 기본 Active Directory 도메인은 대문자 DNS 형식이어야 합니다.
- MIT Kerberos for Windows를 다운로드하여 설치할 필요가 없습니다. 또한 서비스 계정에 키 탭이 더 이상 필요하지 않습니다.

10.1.6.2.1 Kerberos 구성 파일을 만들려면

다음 단계에 따라 Kerberos 구성 파일을 만듭니다.

1. krb5.ini 파일이 없으면 이 파일을 만들어 Windows의 C:\WINNT 아래 저장합니다.

참고:

이 파일을 다른 위치에 저장할 수 있습니다. 그러나 이러한 경우 CMC를 통해 WACS 서버의 속성 페이지에서 Krb5.ini 파일 위치 필드에 해당 위치를 지정해야 합니다.

2. Kerberos 구성 파일에 다음 필수 정보를 추가합니다.

```
[libdefaults]
default_realm = DOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
[domain_realm]
.domain.com = DOMAIN.COM
domain.com = DOMAIN.COM
.domain2.com = DOMAIN2.COM
domain2.com = DOMAIN2.COM
[realms]
DOMAIN.COM = {
default_domain = DOMAIN.COM
kdc = HOSTNAME.DOMAIN.COM
}
DOMAIN2.COM = {
default_domain = DOMAIN2.COM
kdc = HOSTNAME.DOMAIN2.COM
}
[capaths]
DOMAIN2.COM = {
DOMAIN.COM =
```

참고:

- DNS.COM은 도메인의 DNS 이름입니다. 이 이름은 FQDN 형식에 맞춰 대문자로 입력해야 합니다.
- kdc는 도메인 컨트롤러의 호스트 이름입니다.
- 사용자가 여러 도메인에서 로그인하는 경우 [realms] 섹션에 여러 도메인 항목을 추가할 수 있습니다. 여러 도메인 항목이 포함된 샘플 파일을 보려면 452 페이지에서 ["샘플 Krb5.ini 파일"](#)을 참조하십시오.
- 여러 도메인 구성에서는 [libdefaults] 아래의 default_realm 값이 원하는 도메인일 수도 있습니다. 따라서 이러한 경우에는 AD 계정을 사용하여 인증할 사용자 수가 가장 많은 도메인을 사용하는 것이 좋습니다.

10.1.6.2.2 JAAS 로그인 구성 파일을 만들려면

1. bscLogin.conf라는 파일이 없으면 이 파일을 만들어 기본 위치인 C:\WINNT에 저장합니다.

참고:

이 파일을 다른 위치에 저장할 수 있습니다. 그러나 이러한 경우 CMC를 통해 WACS 서버의 속성 페이지에서 bscLogin.conf 파일 위치 필드에 해당 위치를 지정해야 합니다.

2. JAAS bscLogin.conf 구성 파일에 다음 코드를 추가합니다.

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
```

3. 파일을 저장하고 닫습니다.

10.1.6.2.3 샘플 Krb5.ini 파일

여러 도메인 Krb5.ini 샘플 파일

다음은 도메인이 여러 개인 경우의 샘플 파일입니다.

```
[domain_realm]
.domain03.com = DOMAIN03.COM
domain03.com = DOMAIN03.com
.child1.domain03.com = CHILD1.DOMAIN03.COM
child1.domain03.com = CHILD1.DOMAIN03.com
.child2.domain03.com = CHILD2.DOMAIN03.COM
child2.domain03.com = CHILD2.DOMAIN03.com
.domain04.com = DOMAIN04.COM
domain04.com = DOMAIN04.com
[libdefaults]
default_realm = DOMAIN03.COM
dns_lookup_kdc = true
dns_lookup_realm = true
[realms]
DOMAIN03.COM = {
admin_server = testvmw2k07
kdc = testvmw2k07
default_domain = domain03.com
}
CHILD1.DOMAIN03.COM = {
admin_server = testvmw2k08
kdc = testvmw2k08
default_domain = child1.domain03.com
}
CHILD2.DOMAIN03.COM = {
admin_server = testvmw2k09
```

```
kdc = testvmw2k09
default_domain = child2.domain03.com
}
DOMAIN04.COM = {
admin_server = testvmw2k011
kdc = testvmw2k011
default_domain = domain04.com
}
```

단일 도메인 Krb5.ini 샘플 파일

도메인이 하나만 포함된 krb5.ini 샘플 파일은 다음과 같습니다.

```
[libdefaults]
default_realm = ABCD.MFROOT.ORG
dns_lookup_kdc = true
dns_lookup_realm = true
[realms]
ABCD.MFROOT.ORG = {
kdc = ABCDIR20.ABCD.MFROOT.ORG
kdc = ABCDIR21.ABCD.MFROOT.ORG
kdc = ABCDIR22.ABCD.MFROOT.ORG
kdc = ABCDIR23.ABCD.MFROOT.ORG
default_domain = ABCD.MFROOT.ORG
}
```

10.1.6.3 AD Kerberos를 사용하도록 WACS 구성

WACS를 호스팅하는 컴퓨터에서 AD Kerberos 인증을 사용하도록 구성한 후에는 중앙 관리 콘솔(CMC)을 통해 WACS 자체를 구성해야 합니다.

10.1.6.3.1 AD Kerberos용 WACS를 구성하려면

1. CMC의 서버 관리 영역으로 이동합니다.
2. AD를 구성할 WACS를 두 번 클릭합니다.
속성 화면이 나타납니다.
3. Krb5.ini 파일 위치 필드에 krb5.ini 구성 파일의 경로를 지정합니다.
4. bscLogin.conf 파일 위치 필드에 bscLogin.conf 구성 파일의 경로를 지정합니다.
5. 저장 후 단기를 클릭합니다.
6. WACS를 다시 시작합니다.

10.1.6.4 Kerberos 문제 해결

Kerberos를 구성할 때 문제가 발생하면 다음 단계를 참조하십시오.

- 로깅 활성화
- Kerberos 구성 테스트

10.1.6.4.1 Kerberos 로깅 활성화

1. 중앙 구성 관리자(CCM)를 시작하고 서버 관리를 클릭합니다.
2. 로그인 자격 증명을 지정합니다.
3. 서버 관리 화면에서 WACS를 중지합니다.
4. Web Tier 구성을 클릭합니다.

참고:

Web Tier 구성 아이콘은 WACS가 중지된 경우에만 활성화됩니다.

Web Tier 구성 화면이 나타납니다.

5. 명령줄 매개 변수 아래에서 다음 텍스트를 매개 변수 끝에 복사합니다.

```
-Dcrystal.enterprise.trace.configuration=verbose  
-Djcsi.kerberos.debug=true
```

6. 확인을 클릭합니다.
7. 서버 관리 화면에서 WACS를 시작합니다.

10.1.6.4.2 Kerberos 구성을 테스트하려면

- 다음 명령을 실행하여 Kerberos 구성을 테스트합니다. 여기서 servact는 CMS가 실행되는 서비스 계정과 도메인이고 password는 서비스 계정과 연결된 암호입니다.

```
<Install Directory>WBusiness ObjectsWjvasdkWbinWkinit.exe servact@TESTM03.COM Password
```

예를 들면 다음과 같습니다.

```
C:\Program Files\Business Objects\Wjvasdk\bin\Wkinit.exe servact@TESTM03.COM Password
```

여전히 문제가 있으면 도메인과 서비스 사용자 이름으로 입력한 대/소문자가 Active Directory에서 설정된 것과 정확히 일치하는지 확인합니다.

10.1.6.4.3 매핑된 AD 사용자가 WACS에서 BusinessObjects Enterprise에 로그인할 수 없는 경우

사용자가 SAP BusinessObjects Enterprise에 매핑되었더라도 다음 두 가지 문제가 발생할 수 있습니다.

10.1.6.4.3.1 다른 AD UPN 및 SAM 이름으로 인한 로그인 실패

사용자의 Active Directory ID가 SAP BusinessObjects Enterprise에 성공적으로 매핑되었습니다. 그러나 DOMAINWABC123과 같은 형식으로 AD 인증과 Kerberos를 사용하여 CMC에 로그인할 수 없습니다.

이 문제는 Active Directory에서 사용자를 설정할 때 사용한 UPN 및 SAM 이름이 서로 다른 경우에 발생할 수 있습니다. 예를 들어, 두 이름의 대/소문자가 다르거나 기타 부분이 다를 수 있습니다. 다음은 문제가 발생할 수 있는 두 가지 예입니다.

- UPN은 abc123@company.com이지만 SAM 이름은 DOMAINWABC123입니다.
- UPN은 jsmith@company.com이지만 SAM 이름은 DOMAINWjohnsmith입니다.

다음 두 가지 방법으로 문제를 해결할 수 있습니다.

- 사용자가 SAM 이름 대신 UPN 이름을 사용하여 로그인하도록 만듭니다.
- SAM 계정 이름과 UPN 이름이 같은지 확인합니다.

10.1.6.4.3.2 사전 인증 오류

이전에 로그인했던 사용자가 더 이상 성공적으로 로그인할 수 없습니다. 계정 정보를 인식할 수 없음 오류 메시지가 나타납니다. WACS 로그에는 "사전 인증 정보가 유효하지 않습니다.(24)"라는 오류가 표시됩니다.

이는 Kerberos 사용자가 AD의 UPN을 수정하지 않았기 때문에 나타날 수 있습니다. Kerberos 사용자 데이터베이스 및 AD 정보의 비동기화를 의미할 수도 있습니다.

이 문제를 해결하려면 AD에서 사용자 암호를 재설정하십시오. 이렇게 하면 변경 내용이 올바르게 전파됩니다.

10.1.7 AD Kerberos 단일 로그인 구성

BI 실행 패드 또는 웹 서비스 SDK 및 QaaWS에 대해 AD Kerberos 단일 로그인을 구성하는 경우 AD Kerberos 인증을 위해 WACS와 WACS를 호스팅하는 컴퓨터를 모두 구성해야 합니다. 자세한 내용은 448 페이지에서 ["WACS에 대해 AD Kerberos 구성"](#)을 참조하십시오.

참고:

역방향 프록시 환경에서 단일 로그인을 사용하려는 경우 먼저 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드의 SAP BusinessObjects Business Intelligence 플랫폼 보안 장을 읽어 보십시오.

10.1.7.1 컴퓨터에서 AD Kerberos 단일 로그인 구성

웹 서비스 SDK 및 QaaWS에 대해 AD Kerberos 단일 로그인을 구성하려면 먼저 WACS를 호스팅하는 컴퓨터를 구성해야 합니다.

- 274 페이지에서 ["Vintela 단일 로그인에 대한 제한 위임 구성"](#)

- "To create an SPN for your web application server"
- "To reset the service account password"
- "To create and place a keytab file"
- 457 페이지에서 ["다중 SPN 설정"](#)
- 457 페이지에서 ["WACS의 헤더 크기 제한 늘리기"](#)

다음 단원에서는 이러한 각 단계를 수행하는 방법을 설명합니다.

10.1.7.1.1 다중 SPN 설정

다중 SPN 사용은 지원되지 않습니다.

10.1.7.1.2 WACS의 헤더 크기 제한 늘리기

Active Directory에서는 인증 프로세스에서 사용되는 Kerberos 토큰을 만듭니다. 이 토큰은 HTTP 헤더에 저장됩니다. WACS에 설정된 기본 HTTP 헤더 크기는 대부분의 사용자에게 충분합니다. 이 헤더 크기를 구성할 수 있습니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. HTTP 헤더 크기를 변경할 WACS를 두 번 클릭합니다.
속성 화면이 나타납니다.
3. HTTP 구성, 프로시를 통한 HTTP 구성 또는 HTTPS 구성 섹션 아래의 최대 HTTP 헤더 크기(바이트) 필드에 값을 지정합니다.
4. 저장 후 단기를 클릭합니다.
5. 서버를 다시 시작합니다.

10.1.7.2 WACS에서 AD Kerberos 단일 로그인 구성

AD Kerberos 단일 로그인을 사용하도록 웹 응용 프로그램 컨테이너 서버를 구성할 수 있습니다. AD Kerberos 단일 로그인은 지원되고 AD NTLM은 지원되지 않습니다.

WACS를 구성하기 전에 WACS를 호스팅하는 컴퓨터에 대해 AD Kerberos 단일 로그인을 구성해야 합니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 구성할 WACS를 두 번 클릭합니다.
속성 화면이 나타납니다.
3. Kerberos Active Directory 단일 로그인 사용을 선택합니다.
4. 기본 AD 도메인, 서비스 사용자 이름 및 Keytab 파일 속성의 값을 지정하고 저장 후 닫기를 클릭합니다.
5. WACS를 다시 시작합니다.

이제 AD Kerberos 단일 로그인을 사용할 준비가 되었습니다.

10.1.7.3 데이터베이스에 대한 Kerberos 및 single sign-on 구성

다음과 같은 요구 사항을 모두 충족하는 배포를 위해 데이터베이스에 대한 single sign-on이 지원됩니다.

- SAP BusinessObjects Business Intelligence 플랫폼은 WACS에 배포됩니다.
- WACS가 Kerberos를 사용하여 AD로 구성되어 있어야 합니다.
- single sign-on을 필요로 하는 데이터베이스는 SQL 서버나 Oracle이 지원되는 버전이어야 합니다.
- 데이터베이스에 액세스해야 하는 그룹 또는 사용자는 SQL 서버나 Oracle 내에서 권한을 부여받아야 합니다.
- CMC의 AD 인증 페이지에 있는 캐시 보안 컨텍스트 확인란을 선택합니다. 데이터베이스에 대해 single sign-on을 사용하려면 이 확인란을 선택해야 합니다.

데이터베이스에 대한 single sign-on을 지원하려면 마지막으로 krb5.ini 파일을 수정해야 합니다.

참고:

관련 지침에서 데이터베이스에 대한 single sign-on 구성 방법이 설명됩니다. 데이터베이스에 대한 종단 간 single sign-on을 구성하려면 Vintela single sign-on에 필요한 구성 단계도 수행해야 합니다. 자세한 내용은 456 페이지에서 ["AD Kerberos 단일 로그인 구성"](#)을 참조하십시오.

10.1.7.3.1 데이터베이스에 대한 single sign-on 활성화

1. SAP BusinessObjects Business Intelligence 플랫폼에 사용 중인 krb5.ini 파일을 엽니다.
이 파일의 기본 위치는 웹 응용 프로그램 서버에 있는 WINNT 디렉터리입니다.
2. 파일에서 [libdefaults] 섹션으로 이동합니다.
3. 해당 파일의 [realms] 섹션을 시작하기 전에 다음 문자열을 입력합니다.

```
forwardable = true
```

4. 파일을 저장하고 닫습니다.
5. WACS를 다시 시작합니다.

10.1.8 WACS 및 IT 환경

이 단원에서는 복잡한 환경에서 WACS를 구성하는 방법에 대해 설명합니다.

10.1.8.1 WACS를 다른 웹 서버로 사용

WACS(웹 응용 프로그램 컨테이너 서버)가 설치된 경우 WACS를 다른 추가 구성 작업을 수행하지 않고 응용 프로그램 서버 및 웹 서버로 사용할 수 있습니다. IIS(인터넷 정보 서비스) 및 Apache와 같은 지원되는 웹 서버를 구성하여 URL을 WACS 서버로 전달할 수 있습니다.

참고:

ISAPI 필터를 사용한 IIS로부터 WACS로 요청 전달은 지원되지 않습니다.

WACS는 웹 서버가 정적 콘텐츠를 호스팅하고 WACS가 동적 콘텐츠를 호스팅하는 배포 시나리오는 지원하지 않습니다. 정적 및 동적 콘텐츠는 항상 WACS에 상주해야 합니다.

10.1.8.2 WACS를 부하 분산으로 사용

배포 환경에서 WACS를 부하 분산으로 사용하려면 부하 분산에서 IP 라우팅 또는 능동적 쿠키를 사용하도록 구성해야 합니다. 즉 특정 WACS에서 사용자 세션이 설정되면 같은 사용자의 모든 후속 요청이 동일한 WACS로 전송됩니다.

WACS는 수동적 쿠키를 사용하는 하드웨어 부하 분산으로는 지원되지 않습니다.

하드웨어 부하 분산에서 SSL 암호화 HTTPS 요청을 WACS로 전달하면 사용자는 WACS에서 HTTPS를 구성하고 WACS마다 SSL 인증서를 설치해야 합니다.

하드웨어 부하 분산에서 HTTPS 트래픽을 해독하여 해독된 HTTP 요청을 WACS로 전달하면 WACS에서 추가 구성이 필요 없습니다.

관련 항목

- 443 페이지에서 [HTTPS/SSL 구성](#)

10.1.8.3 WACS를 역방향 프록시로 사용

배포 환경에서 WACS를 정방향 또는 역방향 프록시 서버로 사용할 수 있습니다. WACS 자체를 프록시 서버로 사용할 수는 없습니다.

10.1.8.3.1 역방향 프록시로 HTTP를 지원하도록 WACS 구성

배포 환경에서 WACS를 역방향 프록시로 사용하려면 방화벽 내부(예: 보안 네트워크) 통신에는 HTTP 포트를, 방화벽 외부(예: 인터넷) 통신에는 HTTP through Proxy 포트를 사용하도록 WACS를 구성합니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 구성할 WACS를 두 번 클릭합니다.
속성 화면이 나타납니다.
3. 프록시를 통한 HTTP 구성 섹션에서 다음을 수행합니다.
 - a. 프록시를 통한 HTTP 사용을 선택합니다.

- b. 프록시를 통한 통신에 사용할 WACS의 HTTP 포트를 지정합니다.
 - c. 프록시 서버의 프록시 호스트 이름 및 프록시 포트를 지정합니다.
4. 저장 후 단기를 클릭합니다.

10.1.8.3.2 역방향 프록시로 HTTPS를 지원하도록 WACS를 구성하려면

일부 부하 분산 및 역방향 프록시 서버는 HTTPS 트래픽을 해독한 다음 이를 응용 프로그램 서버로 전달하도록 구성할 수 있습니다. 이 경우 WACS에서 HTTP나 HTTP through Proxy를 사용하도록 구성할 수 있습니다.

부하 분산이나 역방향 프록시에서 HTTPS 트래픽을 전달하고 HTTPS를 역방향 프록시로 구성하려는 경우 두 개의 WACS를 만든 후 이중 하나는 역방향 프록시를 통한 외부 트래픽을 위한 HTTPS로 구성하고 다른 하나는 내부 네트워크의 클라이언트와 HTTPS를 통해 통신하도록 구성할 수 있습니다.

10.1.8.4 방화벽과 함께 WACS 사용

방화벽이 있는 IT 환경에 WACS를 배포하는 것이 지원됩니다.

기본적으로 WACS는 WACS가 설치된 컴퓨터에서 모든 IP 주소에 바인딩됩니다. 클라이언트와 WACS 사이에 방화벽을 사용할 계획인 경우 HTTP 또는 프록시를 통한 HTTP에 대해 WACS가 특정 IP 주소로 바인딩되도록 해야 합니다. 이렇게 하려면 모든 IP 주소에 바인딩의 선택을 취소한 다음 바인딩할 호스트 이름 또는 IP 주소를 지정합니다.

배포 환경에서 WACS 서버와 다른 SAP BusinessObjects Business Intelligence 플랫폼 서버 간에 방화벽을 사용하려는 경우 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드의 SAP BusinessObjects Business Intelligence 플랫폼 구성 요소 사이의 통신 이해 단원을 참조하십시오.

관련 항목

- 169 페이지에서 [BI 플랫폼 구성 요소 간의 통신 이해](#)

10.1.8.5 다중 홈 컴퓨터에서 WACS 구성

다중 홈 컴퓨터는 다중 네트워크 주소를 가진 컴퓨터입니다. 기본적으로 웹 응용 프로그램 컨테이너 서버 인스턴스는 자신의 HTTP 포트를 모든 IP 주소로 바인딩합니다. WACS를 특정 NIC(네트워크 인터페이스 카드)로 바인딩하는 경우, 예를 들어, WACS의 HTTP 포트를 특정 NIC로 바인딩하고 요청 포트를 다른 NIC로 바인딩하는 경우 다음을 수행합니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 구성할 WACS를 두 번 클릭합니다.
속성 화면이 나타납니다.
3. 웹 응용 프로그램 컨테이너 서비스 창의 프록시를 통해 HTTP 구성 섹션에서 모든 IP 주소에 바인딩의 선택을 취소하고 WACS를 바인딩할 IP 주소를 입력합니다.
4. HTTPS 구성 섹션에서 모든 IP 주소에 바인딩의 선택을 취소하고 WACS를 바인딩할 IP 주소나 호스트 이름을 입력합니다.
5. 일반 설정에서 자동 할당의 선택을 해제한 다음 배포에서 WACS와 기타 BI 플랫폼 서버 간의 통신에 사용되는 NIC의 호스트 이름이나 IP 주소를 지정합니다.
6. 저장 후 닫기를 클릭합니다.
7. WACS를 다시 시작합니다.

10.1.9 웹 응용 프로그램 속성 구성

WACS에서 호스팅되는 웹 응용 프로그램의 속성은 다음과 같은 방법으로 구성할 수 있습니다.

- 자주 변경되는 속성은 WACS의 구성 가능한 서비스 속성으로 표시됩니다. 이러한 속성을 편집하려면 중앙 관리 콘솔(CMC)에서 WACS의 속성 페이지를 열고 해당 속성에 대한 값을 수정한 다음 저장을 클릭합니다.
- WACS에서 호스팅되는 웹 응용 프로그램의 세션 제한 시간을 수정하려면 먼저 CMC에서 구성할 수 있는 속성이 웹 응용 프로그램에 있는지 확인합니다.

CMC에서 구성할 수 있는 속성이 웹 응용 프로그램에 있는 경우 웹 응용 프로그램의 web_xml.ino 파일을 수정합니다. 이 파일은 <WebAppName>_web_xml.ino입니다. 여기서 <WebAppName>은 웹 응용 프로그램의 이름이며, <EnterpriseDirectory>/java/pjs/services/<WebAppName> 디렉터리에서 찾을 수 있습니다.

CMC에서 구성할 수 있는 속성이 웹 응용 프로그램에 없는 경우 웹 응용 프로그램의 web.xml 파일을 수정합니다. 이 파일은 <EnterpriseDirectory>/warfile/webapps/<WebAppName>에 있습니다. 여기서 <WebAppName>은 웹 응용 프로그램의 이름입니다.

- CMC에서 WACS의 속성 화면에 표시되는 속성 또는 세션 제한 시간 이외의 다른 속성을 수정하려면 웹 응용 프로그램의 .properties 파일을 수정합니다. 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드의 BOE.war 속성을 통해 응용 프로그램 관리 단원을 참조하십시오.

참고:

- <EnterpriseDirectory>/java/pjs/container/work/<ServerFriendlyName> 디렉터리에 있는 web.xml, web_xml.ino 또는 .properties 파일은 WACS가 시작되거나 다시 시작될 때마다 변경 내용이 덮어쓰여지므로 수정하지 마십시오.
- WACS의 속성을 수정한 후에는 WACS를 항상 다시 시작해야 합니다.

관련 항목

- 387 페이지에서 ["서버 속성 변경"](#)
- 514 페이지에서 ["BOE war 파일"](#)

10.1.10 문제 해결

10.1.10.1 WACS에서 추적 구성

WACS에서 추적을 구성하려면 743 페이지에서 ["구성 요소에서 추적 로깅"](#)을 참조하십시오.

10.1.10.2 서버 메트릭 보기

중앙 관리 콘솔(CMC)에서 WACS의 서버 메트릭을 볼 수 있습니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. WACS를 마우스 오른쪽 단추로 클릭하고 메트릭을 클릭합니다.

관련 항목

- 875 페이지에서 [웹 응용 프로그램 컨테이너 서버 메트릭](#)"

10.1.10.3 WACS의 상태 보기

WACS의 상태를 보려면 CMC의 서버 영역으로 이동합니다. 서버 목록에는 목록의 각 서버에 대한 상태를 표시하는 상태 열이 포함되어 있습니다.

WACS에는 시작되었지만 오류가 발생함이라는 새로운 서버 상태가 포함되어 있습니다. 이 상태에 있는 WACS는 실행되고 있지만 잘못 구성된 HTTP, HTTP through Proxy 또는 HTTPS 커넥터를 하나 이상 포함하고 있는 것입니다.

WACS 상태가 시작되었지만 오류가 발생함인 경우 메트릭 페이지로 이동하여 실행 중인 WACS 커넥터 목록 메트릭을 확인합니다. 활성화된 커넥터가 이 목록에 나타나지 않는 경우 커넥터가 제대로 구성되지 않은 것입니다.

10.1.10.4 포트 충돌 해결

특정 포트를 통해 CMC에 액세스를 시도할 때 어떤 페이지도 표시되지 않을 경우 WACS에 대해 지정한 HTTP, HTTP through Proxy 또는 HTTPS 포트를 다른 응용 프로그램에서 사용하고 있지 않은지 확인하십시오.

WACS에서 포트 충돌이 있는지 여부를 확인하는 방법에는 두 가지가 있습니다. 배포 환경에 WACS가 두 개 이상 있는 경우 CMC에 로그인하고 실행 중인 WACS 커넥터와 WACS 시작 오류 메트릭을 확인합니다. HTTP, HTTP through Proxy 또는 HTTP 커넥터가 실행 중인 WACS 커넥터 목록에 나타나지 않는 경우 이러한 커넥터는 포트 충돌로 인해 시작할 수 없습니다.

배포 환경에 하나의 WACS만 있거나 WACS를 통해 CMC에 액세스할 수 없는 경우 netstat 같은 유틸리티를 사용하여 다른 응용 프로그램에서 WACS 포트를 사용하는지 확인합니다.

10.1.10.4.1 HTTP 포트 충돌을 해결하려면

1. 중앙 구성 관리자(CCM)를 시작하고 서버 관리 아이콘을 클릭합니다.
2. 로그인 자격 증명을 지정합니다.
3. 서버 관리 화면에서 WACS를 중지합니다.
4. Web Tier 구성 아이콘을 클릭합니다.

참고:

Web Tier 구성 아이콘은 WACS가 중지된 경우에만 활성화됩니다.

Web Tier 구성 화면이 나타납니다.

5. HTTP 포트 필드에 웹 응용 프로그램 컨테이너 서버에서 사용할 HTTP 포트를 지정하고 확인을 클릭합니다.
6. 서버 관리 화면에서 WACS를 시작합니다.

10.1.10.4.2 HTTP through Proxy 또는 HTTPS 포트 충돌을 해결하려면

HTTP through Proxy 또는 HTTPS 포트를 통해 WACS에 액세스할 수 없지만 HTTP 포트를 통해 여전히 중앙 관리 콘솔(CMC)에 연결할 수 있는 경우 CMC에서 사용하는 포트 번호를 변경합니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 구성할 WACS를 중지하려면 서버를 마우스 오른쪽 단추로 클릭하고 서버 중지를 클릭합니다.
3. 구성할 WACS를 두 번 클릭합니다.
속성 화면이 나타납니다.
4. 프록시를 통한 HTTP 구성 섹션에서 새로운 HTTP 포트를 지정합니다.
5. HTTPS 포트를 변경하려면 HTTPS 구성 섹션에서 HTTPS 포트 필드에 새 값을 입력합니다.
6. 저장 후 닫기를 클릭합니다.
7. WACS를 시작하려면 서버를 마우스 오른쪽 단추로 클릭하고 서버 시작을 클릭합니다.

10.1.10.5 메모리 설정 변경

WACS의 서버 성능을 향상시키기 위해 CCM(중앙 구성 관리자)을 통해 서버에 할당된 메모리의 양을 변경할 수 있습니다.

1. CCM을 시작하고 서버 관리 아이콘을 클릭합니다.
2. CMC에 대한 로그인 자격 증명을 지정합니다.
3. 서버 관리 화면에서 WACS를 중지합니다.
4. Web Tier 구성 아이콘을 클릭합니다.

참고:

Web Tier 구성 아이콘은 WACS가 중지된 경우에만 활성화됩니다.

Web Tier 구성 화면이 나타납니다.

5. 명령줄 매개 변수에서 명령줄을 편집하여 새 메모리 값을 지정합니다.
 - a. -Xmx 옵션을 찾습니다. 이 옵션은 일반적으로 지정된 값을 포함합니다.
예를 들어, -Xmx1g은 서버에 1기가바이트의 메모리를 할당합니다.
 - b. 매개 변수의 새 값을 지정합니다.
 - 메가바이트로 값을 지정하려면 m을 사용합니다. 예를 들어, -Xmx640m은 WACS에 640메가바이트의 메모리를 할당합니다.
 - 기가바이트로 값을 지정하려면 g를 사용합니다. 예를 들어, -Xmx2g는 WACS에 2기가바이트의 메모리를 할당합니다.
 - c. 확인을 클릭합니다.
6. 서버 관리 화면에서 WACS를 시작합니다.

10.1.10.6 동시 요청 수 변경

WACS에서 처리할 수 있는 동시 HTTP 요청 수의 기본값은 150개로 구성됩니다. 대부분의 배포 시나리오에 이 값을 사용할 수 있습니다. WACS의 성능을 향상시키기 위해 최대 동시 HTTP 요청 수를 늘릴 수 있습니다. 동시 요청 수를 늘리면 성능이 향상되지만 이 값을 너무 높게 설정하면 오히려 성능이 저하될 수 있습니다. 하드웨어, 소프트웨어 및 IT 요구 사항에 맞게 설정하는 것이 바람직합니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 구성할 WACS를 중지하려면 서버를 마우스 오른쪽 단추로 클릭하고 서버 중지를 클릭합니다.

3. 구성할 WACS를 두 번 클릭합니다.
속성 화면이 나타납니다.
4. 동시성 설정(커넥터마다)의 최대 동시 요청Requests 필드에 원하는 동시 요청 수를 입력하고 저장 후 단기를 클릭합니다.
5. WACS를 시작하려면 서버를 마우스 오른쪽 단추로 클릭하고 서버 시작을 클릭합니다.

10.1.10.7 시스템 기본값 복원

WACS를 잘못 구성한 경우 중앙 구성 관리자(CCM)를 통해 시스템 기본값을 복원할 수 있습니다.

1. CCM을 시작하고 서버 관리 아이콘을 클릭합니다.
2. 로그인 자격 증명을 지정합니다.
3. 서버 관리 화면에서 WACS를 중지합니다.
4. Web Tier 구성 아이콘을 클릭합니다.

참고:

Web Tier 구성 아이콘은 WACS가 중지된 경우에만 활성화됩니다.

Web Tier 구성 화면이 나타납니다.

5. 시스템 기본값 복원을 클릭합니다.
6. 필요한 경우 사용 가능한 HTTP 포트를 지정하고 확인을 클릭합니다.
7. 서버 관리 화면에서 WACS를 시작합니다.

10.1.10.8 사용자가 HTTP를 통해 WACS에 연결할 수 없도록 하려면

상황에 따라 로컬 컴퓨터의 사용자만 HTTP 또는 HTTPS를 통해 WACS에 연결되도록 허용하려는 경우가 있습니다. 예를 들어, HTTP 포트를 닫을 수 없는 경우에도 WACS와 동일한 컴퓨터에 있는 클라이언트의 HTTP 요청만 처리하도록 WACS를 구성하려는 경우입니다. 즉 WACS와 동일한 컴퓨터의 브라우저를 통해 WACS에서 유지 관리 또는 구성 작업을 수행하고 다른 사용자는 서버에 액세스할 수 없도록 할 수 있습니다.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 수정할 WACS를 두 번 클릭합니다.
속성 화면이 나타납니다.
3. 웹 응용 프로그램 컨테이너 서비스 섹션에서 모든 IP 주소에 바인딩 확인란을 취소합니다.

4. 호스트 이름 또는 IP 주소에 바인딩 필드에 127.0.0.1을 입력하고 확인을 클릭합니다.
5. WACS를 시작하려면 서버를 마우스 오른쪽 단추로 클릭하고 서버 시작을 클릭합니다.
이러한 방식으로 구성된 WACS는 로컬 컴퓨터로부터의 연결만 허용합니다.

10.1.11 WACS 속성

WACS에서 구성할 수 있는 일반, HTTP, 프록시를 통한 HTTP 및 HTTPS 구성 속성의 전체 목록은 서버 속성 부록의 핵심 서버 설정 단원을 참조하십시오.

관련 항목

- 824 페이지에서 [핵심 서비스 속성](#)

장11 백업 및 복원

11.1 시스템 백업 및 복원

이 장에서는 SAP BusinessObjects Business Intelligence 플랫폼 시스템 및 데이터 파일의 백업을 수행하는 권장 절차 및 데이터 손실 또는 하드웨어 오류로부터 복구하는 절차를 설명합니다. 계획을 실행하려면 숙련된 BusinessObjects 전문가, 시스템 관리자 및 데이터베이스 관리자여야 합니다.

백업 및 복구 프로세스는 모든 환경 즉, 개발, 테스트 및 프로덕션에서 비슷합니다. 따라서 이 장에서는 특정 환경을 언급하지 않습니다. 모든 환경을 백업하는 것이 좋습니다.

백업 및 복구 계획은 자연 재해 또는 재난으로 인해 시스템 장애가 발생할 경우에 대비한 예방 조치로 구성됩니다. 이 계획은 업무에 중요한 기능을 유지 관리하거나 신속하게 다시 시작할 수 있도록 일상적인 작업에 미치는 재난의 영향을 최소화하기 위한 것입니다.

하드웨어 오류, 소프트웨어 오류 또는 잘못 구성된 서버 설정으로부터 시스템을 보호하려면 중앙 관리 서버(CMS) 시스템 데이터베이스, 입력 및 출력 파일 리포지토리의 콘텐츠 및 SAP BusinessObjects Business Intelligence 플랫폼이 설치된 컴퓨터의 파일 시스템을 정기적으로 백업하는 것이 좋습니다.

또한 SAP BusinessObjects Business Intelligence 플랫폼 4.0용 주기 관리 콘솔을 사용하여 콘텐츠를 Business Intelligence 아카이브(LCMBIAR) 파일에 내보내 보고서, 사용자, 권한 등의 비즈니스 인텔리전스 콘텐츠도 정기적으로 백업하는 것이 좋습니다. 콘텐츠가 손상되었거나 누락된 경우 전체 CMS 데이터베이스 또는 파일 리포지토리를 복원하지 않고도 나중에 해당 콘텐츠를 복원할 수 있습니다. SAP BusinessObjects Business Intelligence 플랫폼 4.0용 주기 관리 콘솔 사용에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 4.0용 주기 관리 콘솔 사용자 가이드를 참조하십시오. SAP BusinessObjects Business Intelligence 플랫폼 4.0용 주기 관리 콘솔과 함께 Subversion을 사용하고 있는 경우, SAP BusinessObjects Business Intelligence 플랫폼 4.0용 주기 관리 콘솔 사용자 가이드의 Subversion 파일 백업 장에서 Subversion 리포지토리 백업에 대한 정보를 참조하십시오.

이 장의 나머지 부분에서는 CMS 시스템 데이터베이스, 파일 리포지토리 또는 파일 시스템이 손실 또는 손상된 경우 시스템을 백업 및 복원하는 방법에 대해 설명합니다. 또한 CMS가 잘못 구성된 경우 CMS를 복구하는 방법도 설명합니다. 이 경우에는 SAP BusinessObjects Business Intelligence 플랫폼 4.0용 주기 관리 콘솔을 사용하여 서버 설정 또는 비즈니스 인텔리전스 콘텐츠를 복원할 수 없습니다.

참고:

SAP BusinessObjects Business Intelligence 플랫폼 시스템을 백업한 다음 복원하면 시스템 복사본이 만들어집니다.

11.1.1 시스템 백업 수행

다음 요소는 정기적으로 백업하는 것이 좋습니다.

- 중앙 관리 서버(CMS) 시스템 데이터베이스

CMS 시스템 데이터베이스는 자주 백업하는 것이 중요합니다. CMS 시스템 데이터베이스를 제대로 백업하지 않을 경우 환경을 복원할 수 없습니다. CMS 시스템 데이터베이스를 백업하려면 먼저 시스템을 중지해야 합니다. CMS 시스템 데이터베이스 백업은 데이터베이스 공급업체의 데이터베이스 백업 도구를 사용하여 수행해야 합니다.

백업 프로세스의 첫 번째 단계로 CMS 데이터베이스를 백업해야 합니다. 이 작업을 시작하고 나서 파일 리포지토리 서버 백업을 시작할 수 있습니다.

- 입력 및 출력 파일 리포지토리 서버

백업의 무결성을 유지하려면 CMS 시스템 데이터베이스에 추가하여 파일 리포지토리 서버(FRS)의 콘텐츠를 백업하는 것이 좋습니다. 파일 리포지토리 백업은 입력 및 출력 파일 리포지토리 서버의 파일 저장 디렉터리 속성에 지정된 폴더에 있는 모든 파일을 백업하는 것입니다. 파일 리포지토리를 백업하려면 먼저 시스템을 중지해야 합니다. 백업은 파일 시스템 백업 도구를 사용하여 수행해야 합니다.

CMS 시스템 데이터베이스, 파일 리포지토리 및 파일 시스템을 백업하는 빈도는 조직의 비즈니스 요구에 따라 다릅니다.

BI 플랫폼 시스템을 중단하고 콜드 백업을 수행하도록 선택할 수 있습니다. 이 경우, 데이터베이스가 정적인 상태를 유지하고 변경되는 데이터로 인해 백업의 질이 저하될 가능성이 최소화됩니다.

가장 좋은 방법은 다음 요소도 백업하는 것입니다.

- 감사 데이터베이스
- 감사 임시 파일
- 사용자 지정 응용 프로그램

사용자 지정 응용 프로그램과 사용자 지정 사항은 수정될 때마다 백업해야 합니다.

- 데이터베이스 연결

11.1.2 서버 설정 백업

잘못 구성된 서버 설정으로부터 시스템을 보호하려면 정기적으로 서버 설정을 BIAR 파일에 백업하는 것이 좋습니다. 서버 백업을 활성화하면 CMS 시스템 데이터베이스, 파일 리포지토리 또는 비즈니스 인텔리전스 콘텐츠를 복원하지 않고도 설정을 복원할 수 있습니다.

시스템의 토폴로지를 변경할 때마다 반드시 서버 설정을 백업해야 합니다. 노드 만들기, 이름 바꾸기, 이동 및 삭제와 서버 만들기 또는 삭제가 이에 포함됩니다. 서버 설정을 백업한 후에 설정을 변경하고, 변경 내용이 만족스러운지 확인한 후 다시 서버 설정을 백업하는 것이 좋습니다.

중앙 구성 관리자(CCM)나 스크립트를 사용하여 BI 플랫폼 서버 설정을 BIAR 파일에 백업한 다음, 파일을 다른 컴퓨터에 따로 저장합니다. 설정을 수정할 때마다 서버 설정을 백업하는 것이 좋습니다.

참고:

SSL이 활성화된 배포에서 서버 설정을 백업 또는 복원하는 경우 먼저 CCM을 통해 SSL을 비활성화한 다음 백업 또는 백업이 완료되면 SSL을 다시 활성화해야 합니다.

Windows의 경우, BackupCluster.bat 스크립트는 <INSTALLDIR>WSAP BusinessObjects Business Intelligence platform 4.0\Win64_x64\scripts 디렉터리에 있습니다.

UNIX에서 backupcluster.sh 스크립트는 /<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform64>/scripts 디렉터리에 있습니다.

관련 항목

- 164 페이지에서 [SSL 프로토콜 구성](#)

11.1.2.1 Windows에서 CCM을 사용하여 서버 설정 백업

이 절차는 전체 클러스터에 대한 서버 설정을 백업하기 위한 것입니다. 개별 서버에 대한 설정을 백업할 수는 없습니다.

참고:

임시 CMS를 사용 중인 경우 로컬 CMS가 있는 컴퓨터에서 CCM을 시작해야 합니다.

1. CCM을 시작하고 도구 모음에서 서버 구성 백업을 클릭합니다.
서버 구성 백업 마법사가 나타납니다.

2. 다음을 클릭하여 마법사를 시작합니다.
3. 기존의 CMS를 사용하여 서버 구성 설정을 백업하거나 임시 CMS를 만들지 여부를 지정합니다.
 - 작동 중인 시스템에서 서버 설정을 백업하려면 실행 중인 기존 CMS 사용을 선택하고 다음을 클릭합니다.
 - 작동 중이지 않은 시스템에서 서버 설정을 백업하려면 새 임시 CMS 시작을 선택하고 다음을 클릭합니다.
4. 임시 CMS를 사용 중인 경우 실행할 CMS용 포트 번호를 선택하고 데이터베이스 연결 정보를 지정합니다.
 시스템을 백업 또는 복원하는 동안 사용자들이 시스템에 액세스할 위험을 최소화하려면 기존 CMS에서 사용하는 포트 번호와는 다른 포트 번호를 지정합니다.
5. 메시지가 표시되면 시스템과 관리 권한이 있는 계정의 사용자 이름 및 암호를 지정하여 CMS에 로그인하고 계속하려면 다음을 클릭합니다.
6. 서버 구성 설정을 백업할 BIAR 파일의 위치와 이름을 지정하고 계속하려면 다음을 클릭합니다.
 확인 화면에 사용자가 입력한 정보가 표시됩니다.
7. 확인 화면에 표시되는 정보가 올바른지 확인하고 계속하려면 마침을 클릭합니다.
 CCM은 전체 클러스터에 대한 서버 구성 설정을 사용자가 지정하는 BIAR 파일에 백업합니다. 자세한 백업 절차가 로그 파일에 기록되고, 로그 파일의 이름과 경로는 대화 상자에 표시됩니다.
8. 백업 작업이 실패한 경우 로그 파일에서 원인을 확인하십시오.
9. 확인을 클릭하여 마법사를 닫습니다.

11.1.2.2 UNIX에서 서버 설정 백업

UNIX 컴퓨터에서 배포의 서버 설정을 BIAR 파일에 백업하려면 `serverconfig.sh` 스크립트를 사용하십시오.

1. 5 - 서버 구성 백업을 선택하고 Enter 키를 누릅니다.
2. 기존 CMS를 사용하여 서버 구성 설정을 백업할지 아니면 임시 CMS를 만들지 여부를 지정합니다.
 - 실행 중인 시스템의 서버 설정을 백업하려면 기존을 선택하고 Enter 키를 누릅니다.
 - 실행 중이지 않은 시스템의 서버 설정을 백업하거나 서버 설정을 복원하려면 임시를 선택하고 Enter 키를 누릅니다.
3. 임시 CMS를 사용하여 서버 설정을 백업하는 경우, 다음 몇 개의 화면에서 실행할 임시 CMS에 대한 포트 번호 및 CMS 시스템 데이터베이스에 대한 연결 정보를 선택합니다.
 시스템을 백업 또는 복원하는 동안 사용자가 시스템에 액세스하는 위험을 최소화하려면 기존 CMS에서 사용하는 포트 번호가 아닌 다른 포트 번호를 지정합니다.
4. 메시지가 표시되면 시스템 및 관리 권한이 있는 계정의 사용자 이름과 암호를 지정한 다음 Enter 키를 눌러 CMS에 로그인합니다.
5. 메시지가 표시되면 서버 구성 설정을 백업할 BIAR 파일의 위치와 이름을 지정하고 Enter 키를 누릅니다.

요약 화면에 제공한 정보가 표시됩니다.

6. 화면에 표시된 정보가 올바른지 확인한 다음 계속하려면 Enter 키를 누릅니다.
serverconfig.sh 스크립트가 전체 클러스터에 대한 서버 구성 설정을 지정한 BIAR 파일에 백업합니다. 자세한 백업 절차는 로그 파일에 기록되어 있습니다. 로그 파일의 이름과 경로는 화면에 표시됩니다.
7. 백업 작업이 실패한 경우 로그 파일에서 원인을 확인하십시오.

11.1.2.3 스크립트로 서버 설정 백업

backupcluster.bat 스크립트(Windows) 또는 BackupCluster.sh 스크립트(UNIX)를 실행하여 배포의 서버 설정을 백업할 수 있습니다.

Windows의 경우, BackupCluster.bat 파일은 <INSTALLDIR>WSAP BusinessObjects Business Intelligence platform 4.0Wwin64_x64Wscripts 디렉터리에 있습니다.

UNIX 컴퓨터의 경우 backupcluster.sh 파일은 /<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform64>/scripts 디렉터리에 있습니다.

스크립트에 사용된 매개 변수에 대한 자세한 내용은 480 페이지에서 ["BackupCluster 및 RestoreCluster 매개 변수"](#)를 참조하십시오.

11.1.3 비즈니스 인텔리전스 콘텐츠 백업

SAP BusinessObjects Business Intelligence 플랫폼 4.0용 주기 관리 콘솔을 사용하여 비즈니스 인텔리전스 콘텐츠(예: 보고서, 사용자와 그룹, 유니버스)를 정기적으로 백업하는 것이 좋습니다. 최신 콘텐츠 백업이 있으면 전체 시스템 또는 시스템 설정을 복원할 필요 없이 Business Intelligence를 복원할 수 있습니다.

SAP BusinessObjects Business Intelligence 플랫폼 4.0용 주기 관리 콘솔 사용에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 4.0용 주기 관리 콘솔 사용자 가이드를 참조하십시오.

SAP BusinessObjects Business Intelligence 플랫폼 4.0용 주기 관리 콘솔과 함께 Subversion을 사용하고 있는 경우, SAP BusinessObjects Business Intelligence 플랫폼 4.0용 주기 관리 콘솔 사용자 가이드의 Subversion 파일 백업 장에서 Subversion 리포지토리 백업에 대한 정보를 참조하십시오.

11.1.4 시스템 복원

시스템 복원을 위해 수행하는 단계는 손실되거나 손상된 구성 요소가 중앙 관리 서버(CMS) 시스템 데이터베이스인지, 입력 및 출력 파일 리포지토리인지, SAP BusinessObjects Business Intelligence 플랫폼이 설치된 컴퓨터의 파일 시스템인지 여부와 이러한 구성 요소의 사용 가능한 백업이 있는지 여부에 따라 달라집니다.

- CMS 시스템 데이터베이스가 손상되었거나 손실되었는데 시스템 데이터베이스와 파일 리포지토리의 사용 가능한 백업이 있다면 474 페이지에서 ["백업이 있는 SAP BusinessObjects Business Intelligence 플랫폼 시스템 복원"](#)의 내용을 참조하십시오.
- CMS 시스템 데이터베이스가 손상되었거나 손실되었고 데이터베이스와 파일 리포지토리의 사용 가능한 백업이 없지만 비즈니스 인텔리전스 콘텐츠를 BIAR 파일에 백업했다면 475 페이지에서 ["백업이 없는 SAP BusinessObjects Business Intelligence 플랫폼 시스템 다시 만들기"](#)의 내용을 참조하십시오.
- 파일 리포지토리가 손상되었거나 손실되었는데 CMS 시스템 데이터베이스와 파일 리포지토리의 백업이 있다면 474 페이지에서 ["백업이 있는 SAP BusinessObjects Business Intelligence 플랫폼 시스템 복원"](#)의 내용을 참조하십시오.
- 파일 리포지토리가 손상되었거나 손실되었고 CMS 시스템 데이터베이스와 파일 리포지토리의 사용 가능한 백업이 없지만 콘텐츠를 BIAR 파일에 백업했다면 475 페이지에서 ["백업이 없는 SAP BusinessObjects Business Intelligence 플랫폼 시스템 다시 만들기"](#)의 내용을 참조하십시오.
- 서버가 잘못 구성되어 전체 시스템을 이전 상태로 롤백하려고 하는데 CMS 시스템 데이터베이스와 파일 리포지토리의 백업이 있다면 474 페이지에서 ["백업이 있는 SAP BusinessObjects Business Intelligence 플랫폼 시스템 복원"](#)의 내용을 참조하십시오.

CMS 시스템 데이터베이스 또는 파일 리포지토리를 복원하기 전에 다음을 수행해야 합니다.

1. SAP BusinessObjects Business Intelligence 플랫폼의 작동을 중지합니다.
2. 현재 CMS 시스템 데이터베이스, 파일 리포지토리를 백업합니다.

참고:

CMS 시스템 데이터베이스와 파일 리포지토리의 백업이 없으며 서버 구성 설정을 BIAR 파일에 백업하지 않고 파일 리포지토리만 LCMBIAR에 백업한 경우에는 시스템을 복원할 수 없습니다.

관련 항목

- 22 페이지에서 [리포지토리 진단 도구](#)

11.1.4.1 백업이 있는 SAP BusinessObjects Business Intelligence 플랫폼 시스템 복원

이 워크플로우는 다음과 같은 백업이 있다고 가정합니다.

- CMS 시스템 데이터베이스의 사용 가능한 백업
- 파일 리포지토리의 사용 가능한 백업

CMS 시스템 데이터베이스 또는 파일 리포지토리 서버가 손실되거나 손상된 경우, CMS 시스템 데이터베이스 및 파일 리포지토리를 현재 백업에서 복원하십시오.

참고:

CMS 시스템 데이터베이스 또는 파일 리포지토리를 현재 백업에서 복원할 때 같은 백업에서 데이터베이스와 파일 리포지토리를 둘 다 복원해야 합니다. 둘 중 하나만 복원할 경우 CMS와 파일 리포지토리 간에 불일치가 발생합니다. 데이터베이스 공급업체의 백업 및 복원 도구를 사용하여 CMS 시스템 데이터베이스를 복원하십시오. 파일 리포지토리 복원은 입력 및 출력 파일 리포지토리 서버의 파일 저장 디렉터리 속성에 지정된 폴더에 있는 백업 파일에서 복원하는 것입니다. 복원은 파일 시스템 백업 및 복원 도구를 사용하여 수행해야 합니다.

CMS 시스템 데이터베이스 또는 파일 리포지토리를 복원할 때 BI 플랫폼이 설치된 컴퓨터의 파일 시스템을 복원할 필요는 없습니다.

1. 사용 가능한 백업에서 CMS 시스템 데이터베이스를 복원합니다.
2. 사용 가능한 백업에서 파일 리포지토리를 복원합니다.

참고:

작동 중단 시간을 최소화하기 위해 두 구성 요소를 동시에 복원할 수 있습니다.

시스템 콘텐츠, 사용자 및 서버 설정을 비롯한 BI 플랫폼 시스템이 백업 당시와 동일한 상태로 복원됩니다.

복원이 완료되면 다음을 수행하십시오.

1. 리포지토리 진단 도구(RDT)를 실행하여 CMS 시스템 데이터베이스와 파일 리포지토리 간에 불일치가 없는지 확인합니다. 리포지토리 진단 도구 사용에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 리포지토리 진단 도구 사용자 가이드를 참조하십시오.
2. BI 플랫폼을 시작하고 시스템에 제대로 작동하는지 확인합니다.

시스템을 가능한 한 빨리 다시 온라인 상태로 만드는 것이 어느 정도 중요하냐에 따라 BI 플랫폼을 먼저 시작한 다음 RDT를 실행하거나 RDT를 먼저 실행한 다음 BI 플랫폼을 시작할 수 있습니다. RDT에서 발견된 불일치 사항은 RDT를 완료해야 해결됩니다.

11.1.4.2 백업이 없는 SAP BusinessObjects Business Intelligence 플랫폼 시스템 다시 만들기

CMS 시스템 데이터베이스 또는 파일 리포지토리가 손실되거나 손상되었는데 백업이 없는 경우, 시스템을 다시 만들 수 있습니다. 단, 시스템의 서버 설정은 BIAR 파일에 백업되어 있고 비즈니스 인텔리전스 콘텐츠는 LCMBIAR 파일에 백업되어 있어야 합니다.

1. 중앙 구성 관리자(CCM)에서 CMS 시스템 데이터베이스를 다시 만듭니다.
그러면 기존 콘텐츠가 모두 지워진 기본 상태로 CMS 시스템 데이터베이스가 다시 만들어집니다.
2. 중앙 구성 관리자(CCM) 또는 RestoreCluster 스크립트를 사용하여 BIAR 파일에서 서버 설정을 복원합니다.
3. LifeCycle Manager를 사용하여 LCMBIAR 파일에서 비즈니스 인텔리전스 콘텐츠를 복원합니다.
LifeCycle Manager 사용에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 4.0용 주기 관리 콘솔 사용자 가이드를 참조하십시오.

관련 항목

- 429 페이지에서 [CMS 시스템 데이터베이스 다시 만들기](#)
- 476 페이지에서 [서버 설정 복원](#)

11.1.4.3 서버 설정 복원

BIAR 파일에서 시스템의 서버 설정을 복원해야 하는 경우 중앙 구성 관리자(CCM) 또는 RestoreCluster 스크립트를 사용하여 서버 설정을 복원할 수 있습니다. BIAR 파일에서 서버 콘텐츠를 복원해도 보고서, 사용자와 그룹 또는 보안 설정과 같은 비즈니스 인텔리전스 콘텐츠에는 영향을 미치지 않습니다.

참고:

- 서버 설정을 복원할 때는 전체 클러스터에 대한 설정 복원만 지원됩니다. 클러스터에 있는 서버 중 일부의 설정만 복원하는 것은 불가능합니다.
- SSL이 사용되는 배포 환경에서 서버 설정을 백업하거나 복원할 경우, 우선 CCM을 통해 SSL의 사용 설정을 해제한 후 백업 또는 복원이 완료되면 SSL을 다시 사용해야 합니다.

관련 항목

- 164 페이지에서 [SSL 프로토콜 구성](#)

11.1.4.3.1 Windows에서 CCM으로 서버 설정 복원

중앙 구성 관리자(CCM)를 사용하여 서버 설정을 복원할 수 있습니다. 서버 설정을 복원한 후에는 시스템의 클러스터에 있는 모든 컴퓨터에서 시스템 노드를 다시 만들어야 합니다.

1. 각 노드의 Server Intelligence Agent를 중지하여 서버 구성 설정을 복원할 클러스터 내에 있는 모든 컴퓨터의 모든 노드를 중지합니다.
2. CMS가 있는 컴퓨터에서 CCM을 시작합니다.
3. 도구 모음에서 서버 구성 복원을 클릭합니다.
서버 구성 복원 마법사가 나타납니다.
4. 다음을 클릭하여 마법사를 시작합니다.
5. 메시지가 표시되면 임시로 사용할 중앙 관리 서버(CMS)를 위한 포트 번호와 CMS 시스템 데이터 베이스에 연결하기 위한 정보를 입력하고 계속하려면 다음을 클릭합니다.
6. 메시지가 표시되면 CMS 이름과 관리 권한이 있는 계정의 사용자 이름 및 암호를 입력하여 CMS에 로그인하고 계속하려면 다음을 클릭합니다.
7. 복원할 서버 구성 설정이 포함된 BIAR 파일의 위치와 이름을 지정하고 계속하려면 다음을 클릭합니다.
사용자가 입력한 정보를 표시하는 요약 화면이 나타납니다.
8. 계속하려면 마침을 클릭합니다.
BIAR 파일에 지정된 값으로 기존 서버 설정을 덮어쓸 것이라는 경고 메시지입니다. 이 절차를 진행하면 현재 서버 설정을 잃게 됩니다.
9. 서버 구성 설정을 복원하려면 예를 클릭합니다.
CCM이 BIAR 파일에서 전체 클러스터에 대한 서버 구성 설정을 복원합니다. 자세한 절차가 로그 파일에 기록됩니다. 로그 파일의 이름과 경로는 대화 상자에 표시됩니다.
10. 복원 작업에 실패한 경우 로그 파일을 검토하여 이유를 확인합니다.
11. 확인을 클릭하여 마법사를 닫습니다.

BIAR 파일의 서버 설정이 시스템에서 복원됩니다. 복원 전에 시스템에 없었던 BIAR 파일에 있는 존재하는 모든 노드와 서버가 만들어집니다. 시스템에는 있지만 BIAR 파일에는 없는 모든 노드와 서버가 삭제됩니다.

클러스터에 대한 서버 설정을 복원한 후에는 시스템의 노드를 클러스터에 있는 모든 컴퓨터에서 다시 만들어야 합니다.

관련 항목

- 406 페이지에서 [노드 다시 만들기](#)

11.1.4.3.2 UNIX에서 CCM으로 서버 설정 복원

UNIX 컴퓨터에서 배포의 서버 설정을 BIAR 파일에서 복원하려면 `serverconfig.sh` 스크립트를 사용하십시오.

1. 6 - 서버 구성 복원을 선택하고 Enter 키를 누릅니다.
2. 사용할 임시 중앙 관리 서버(CMS)에 대한 포트 번호를 입력하고 Enter 키를 누릅니다.
3. 다음 몇 개의 화면에서 CMS 시스템 데이터베이스에 대한 연결 정보를 지정합니다.
4. 메시지가 표시되면 시스템 및 관리 권한이 있는 계정의 사용자 이름과 암호를 지정한 다음 Enter 키를 눌러 CMS에 로그인합니다.
5. 메시지가 표시되면 서버 구성 설정을 복원할 BIAR 파일의 위치와 이름을 지정하고 Enter 키를 누릅니다.
요약 화면에 제공한 정보가 표시됩니다.
6. 화면에 표시된 정보가 올바른지 확인한 다음 계속하려면 ...를 누릅니다.
`serverconfig.sh` 스크립트가 전체 클러스터에 대한 서버 구성 설정을 지정한 BIAR 파일에서 복원합니다. 자세한 복원 절차는 로그 파일에 기록되어 있습니다. 로그 파일의 이름과 경로는 화면에 표시됩니다.
7. 복원 작업이 실패한 경우 로그 파일에서 원인을 확인하십시오.

11.1.4.3.3 스크립트로 서버 설정 복원

원하는 경우 `RestoreCluster.bat` 스크립트(Windows) 또는 `restorecluster.sh` 스크립트(UNIX)를 실행하여 배포의 서버 설정을 복원할 수 있습니다.

Windows의 경우 `RestoreCluster.bat` 파일은 `<INSTALLEDIR>WSAP BusinessObjects Business Intelligence platform 4.0Win64_x64Wscripts` 디렉터리에 있습니다.

UNIX의 경우 `restorecluster.sh` 파일은 `/<INSTALLEDIR>/sap_bobj/enterprise_xi40/<platform64>/scripts` 디렉터리에 있습니다.

스크립트에 사용된 매개 변수에 대한 자세한 내용은 480 페이지에서 ["BackupCluster 및 RestoreCluster 매개 변수"](#)를 참조하십시오.

11.1.4.4 비즈니스 인텔리전스 콘텐츠 복원

비즈니스 인텔리전스 콘텐츠를 LCMBIAR 파일로 백업한 경우 SAP BusinessObjects Business Intelligence 플랫폼 4.0용 주기 관리 콘솔을 사용하여 전체 시스템을 복원하지 않고도 콘텐츠를 복원할 수 있습니다. 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 4.0용 주기 관리 콘솔 사용자 가이드를 참조하십시오.

11.1.5 백업이 있는 경우 손실 또는 손상된 SAP BusinessObjects Business Intelligence 플랫폼 파일 복원

CMS 시스템 데이터베이스 및 파일 리포지토리가 정상적으로 작동하지만 SAP BusinessObjects Business Intelligence 플랫폼 구성 파일이 손실되었거나 손상되었고 사용 가능한 파일 백업이 있는 경우, 백업에서 파일 시스템을 복원하십시오. 파일 시스템을 복원할 때 시스템의 CMS 시스템 데이터베이스와 파일 리포지토리를 복원해야 합니다.

11.1.6 파일이 손실된 경우 SAP BusinessObjects Business Intelligence 플랫폼 시스템 다시 만들기

이 절차는 다음과 같은 백업이 있다고 가정합니다.

- CMS 시스템 데이터베이스의 백업
- 파일 리포지토리 서버 콘텐츠의 백업

SAP BusinessObjects Business Intelligence 플랫폼이 설치된 컴퓨터의 파일 시스템이 손실되었거나 손상되었는데 사용 가능한 파일 시스템 백업이 없는 경우, 같은 컴퓨터 또는 다른 컴퓨터에 SAP BusinessObjects Business Intelligence 플랫폼을 다시 설치하여 이 시스템을 복구할 수 있습니다.

1. 원래 설치와 동일한 옵션으로 SAP BusinessObjects Business Intelligence 플랫폼을 새로 설치합니다. 새 설치에 있는 노드 수는 원래 설치의 노드 수와 같아야 하며, 노드 이름은 원래 설치의 노드 이름과 같아야 합니다. SAP BusinessObjects Business Intelligence 플랫폼은 원래 설치와

동일한 폴더에 설치해야 합니다. SAP BusinessObjects Business Intelligence 플랫폼을 설치할 때 기존 CMS 시스템 데이터베이스를 데이터베이스로 지정합니다.

참고:

설치 중에 기존 CMS 시스템 데이터베이스를 선택할 때, CMS 리포지토리 데이터베이스 구성 화면에서 기존 데이터베이스 재설정 확인란이 선택 취소되어 있는지 확인해야 합니다. 이 확인란을 선택한 상태로 두면 기존 데이터베이스의 모든 콘텐츠가 삭제됩니다.

2. 사용 가능한 백업에서 파일 리포지토리를 복원합니다.

11.1.7 BackupCluster 및 RestoreCluster 매개 변수

다음 표에는 BackupCluster 스크립트와 함께 사용되는 명령줄 매개 변수가 설명되어 있습니다.

테이블 11-1: BackupCluster 매개 변수

이름	설명	예제
-backup	복원할 시스템 서버 설정을 백업할 BIAR 파일의 이름과 경로입니다.	-backup "C:\Users\Administrator\Desktop\my.biar"
-cms	시스템의 중앙 관리 서버가 있는 컴퓨터의 호스트 이름입니다. CMS가 기본 포트(6400)가 아닌 다른 포트에서 실행 중인 경우 포트 번호도 지정해야 합니다.	-cms mycms:6400
-username	관리자 계정의 사용자 이름입니다.	-username Administrator
-password	관리자 계정의 암호입니다.	-password Password1

다음 표에는 RestoreCluster 스크립트와 함께 사용되는 명령줄 매개 변수가 설명되어 있습니다.

테이블 11-2: RestoreCluster 매개 변수

이름	설명	예제
-restore	복원할 서버 구성 파일이 포함된 BIAR 파일의 이름과 경로입니다.	-restore "C:\Users\Administrator\Desktop\my.biar"

이름	설명	예제
-username	관리자 계정의 사용자 이름입니다.	-username Administrator
-password	관리자 계정의 암호입니다.	-password Password1
-displaycontents	BIAR 파일에 포함된 노드 및 서버 목록을 표시합니다.	-displaycontents "C:\Users\Administrator\Desktop\my.biar"

참고:

서버 설정을 복원하기 전에 BIAR 파일의 콘텐츠를 표시하려면 RestoreCluster 스크립트를 -display contents 매개 변수와 함께 실행하는 것이 좋습니다.

실행 중이지 않은 시스템의 서버 설정을 백업하거나 서버 설정을 복원하는 경우 필수 매개 변수는 다음과 같습니다.

테이블 11-3: 임시 CMS를 사용할 경우에 사용되는 매개 변수

이름	설명	예제
-usetempcms	지정된 작업을 위한 임시 CMS를 만듭니다. 작업이 완료되면 임시 CMS가 중지됩니다.	-usetempcms
-cmsport	임시 CMS의 포트 번호입니다.	-cmsport 6400
-dbdriver	CMS 시스템 데이터베이스의 데이터베이스 드라이버입니다. 사용할 수 있는 값은 다음과 같습니다. <ul style="list-style-type: none"> • db2databasesubsystem • maxdbdatabasesubsystem • mysqldatabasesubsystem • oracledatabasesubsystem • sqlserverdatabasesubsystem • sybasedatabasesubsystem 	-dbdriver sqlserverdatabasesubsystem

이름	설명	예제
-connect	<p>CMS 시스템 데이터베이스 연결 문자열입니다.</p> <p>참고:</p> <p>명령 프롬프트의 제한 사항으로 인해 -connect 문자열에서 캐럿(^)을 사용하여 공백, 등호(=) 및 세미콜론을 이스케이프 처리해야 합니다.</p> <p>긴 문자열에서 캐럿을 사용하지 않으려면 임시 response.bat 파일에 스크립트 이름과 모든 매개 변수를 기록한 다음 매개 변수 없이 response.bat 파일을 실행하면 됩니다.</p>	<pre>-connect "DSN^=BusinessObjects^ CMS^ 140^;UID^=user name^;PWD^=Pass word1^;HOST NAME^=database^;PORT^=3306"</pre>
-dbkey	클러스터 키입니다.	-dbkey abc1234

예제

다음 예제는 기존 CMS를 사용하여 서버 설정을 BIAR 파일에 백업하는 방법을 보여 줍니다.

```
-backup "C:\Users\Administrator\Desktop\my.biar"
-cms mycms:6400
-username Administrator
-password Password1
```

예제

다음 예제는 BIAR 파일의 콘텐츠를 표시하는 방법을 보여 줍니다.

```
-displaycontents "C:\Users\Administrator\Desktop\mybiar.biar"
```

예제

다음 예제는 BIAR 파일의 설정을 복원하는 방법을 보여 줍니다. 서버 설정을 복원하는 경우 항상 임시 CMS를 사용해야 합니다.

```
-restore "C:\Users\Administrator\Desktop\my.biar"
-cms mycms:6400
-username Administrator
-password Password1
-usetempcms
-cmsport 6400
-dbdriver sqlserverdatabasesubsystem
-connect "DSN^=BusinessObjects^ CMS^ 140^;UID^=username^;PWD^=Password1^;HOSTNAME^=database^;PORT^=3306"
-dbkey abc1234
```

장12 수명 주기 관리

12.1 주기 관리 콘솔

SAP BusinessObjects Business Intelligence 플랫폼 4.0용 주기 관리 콘솔은 BI 리소스의 종속성에 영향을 주지 않고 시스템 간에 BI 리소스를 이동할 수 있는 웹 기반 도구입니다. 또한 이 도구를 사용하면 여러 버전의 BI 리소스 및 BI 리소스의 종속성을 관리할 수 있으며 승격된 리소스를 되돌려서 대상 시스템을 이전 상태로 복원할 수도 있습니다.

주기 관리 콘솔 도구는 SAP BusinessObjects Business Intelligence 플랫폼 응용 프로그램용 플러그인입니다. 소스 시스템과 대상 시스템에 동일한 버전의 SAP BusinessObjects Business Intelligence 플랫폼 응용 프로그램이 설치된 경우에만 시스템 간에 BI 리소스의 수준을 올릴 수 있습니다.

SAP BusinessObjects는 버전 번호가 동일한 두 SAP BusinessObjects Business Intelligence 플랫폼 배포에서 개체를 가져올 수 있도록 다음 도구를 제공합니다.

- 주기 관리 콘솔

주기 관리 콘솔 사용에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 4.0용 주기 관리 콘솔 사용자 가이드를 참조하십시오.

- BIAR 명령줄 도구

BIAR 명령줄 도구 사용에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 4.0용 주기 관리 콘솔 사용자 가이드를 참조하십시오.

12.2 주기 관리 콘솔용 버전 관리 시스템

12.2.1 주기 관리 콘솔용 버전 관리 시스템

- 주기 관리 콘솔 Subversion이 SAP BusinessObjects Business Intelligence 플랫폼과 함께 설치되는 경우 구성 설정이 자동으로 수행됩니다.
- 그러나 이미 설치된 주기 관리 콘솔 Subversion을 구성하려는 경우 주기 관리 콘솔 도구 관리 옵션의 VMS 설정 페이지에 적절한 값을 입력합니다.

다음 그림은 VMS 설정 페이지에서 지정할 수 있는 값을 보여 줍니다.

버전 관리 시스템 SubVersion ▼

SubVersion 설정

☒ 기본 VMS로 사용

서버 이름 localhost

서버 포트 3690

사용자 이름 LCM

암호 ●●●

설치 경로 D:\Program Files (x86)\SAP Business

리포지토리 이름 svn_repository

작업 영역 디렉터리 D:\checkout

- SAP BusinessObjects Business Intelligence 플랫폼을 설치한 다음 주기 관리 Subversion을 설치하는 경우,

참고:

Subversion 서비스가 실행 중이며 리포지토리가 만들어졌는지 확인합니다.

1. 주기 관리 콘솔 도구 관리 옵션의 VMS 설정 페이지에 적절한 값을 입력합니다.
2. SIA를 다시 시작합니다.

12.3 BIAR 엔진 명령줄 도구

BIAR 엔진 명령줄 도구는 관리자와 위임된 관리자가 개발, 품질 보증 및 운영 SAP BusinessObjects Business Intelligence 플랫폼 환경 간에 콘텐츠의 수준을 올리는 데 유용합니다. 이 도구는 스크립트를 사용하여 자동으로 개체를 가져오거나 내보냅니다.

BIAR 엔진 명령줄 도구는 SAP BusinessObjects Business Intelligence 플랫폼 4.0 시스템 간의 개체 마이그레이션만 지원합니다. 이 도구를 통해서 BusinessObjects, Crystal Enterprise 또는 이전 버전의 SAP BusinessObjects Business Intelligence 플랫폼에서 개체를 가져올 수 없습니다. 이전 버전의 콘텐츠를 가져오려면 SAP BusinessObjects Business Intelligence 플랫폼 업그레이드 관리 도구를 사용해야 합니다.

BIAR 엔진 명령줄 도구의 파일 이름은 biarengine.jar입니다. Windows 환경의 경우 이 파일은 <InstallDir>\SAP BusinessObjects Enterprise XI 4.0\Wjava\lib에 있습니다. UNIX 환경의 경우 이 파일은 <InstallDir>/sap_bobj/java/lib/에 있습니다.

참고:

- 이 도구를 사용하려면 Java Runtime Environment를 설치해야 합니다. 지원되는 JRE 목록은 지원 웹 사이트에서 온라인으로 제공하는 SAP BusinessObjects Business Intelligence 플랫폼 supported platform document 가이드를 참조하십시오.
- BIAR 엔진 명령줄 도구를 사용하려면 콘텐츠를 가져오거나 내보내려는 환경에 대한 관리자 계정 자격 증명이 있어야 합니다. 또한 위임된 관리자 계정도 사용할 수 있습니다.
- BIAR 엔진 명령줄 도구를 사용하여 SAP BusinessObjects Business Intelligence 플랫폼 업그레이드 관리 도구에서 생성한 BIAR 파일을 가져오는 것은 지원되지 않습니다.

BIAR 엔진 명령줄 도구를 사용하여 가져올 수 있는 개체의 유형은 다음과 같습니다.

분석 연결	Web Intelligence 문서
분석 작업 영역	LDAP 사용자
알 수 없는 문서	값 목록(LOV)
분석 개체	개체 패키지
BI 모델러 개체	오버로드
BI 작업 영역	PDF
비즈니스 뷰	PowerPoint 프레젠테이션
달력	프로필
범주	프로그램 개체
클라이언트 작업	프롬프트 그룹
사용자 지정 역할	게시
Dashboard Design 문서	Query as a Web Service
토론	보고서
Encyclopedia	보고서 인스턴스
Enterprise 사용자 그룹	서식 있는 텍스트 형식 문서
Enterprise 사용자	서버 그룹
이벤트	바로 가기
Excel 스프레드시트	텍스트 파일
Flash 파일	유니버스
폴더	WinAD 사용자
전체 클라이언트 추가 기능	Word 문서
전체 클라이언트 템플릿	XcelsiusDMTTemplates
하이퍼링크	

관계 가져오기

BIAR 엔진 명령줄 도구는 두 개체를 함께 가져오는 경우나 개체 중 하나가 이미 대상 시스템에 있는 경우에만 가져온 개체 간의 관계를 그대로 유지합니다. 예를 들어 유니버스를 사용하는 Web Intelligence 보고서가 있을 때, 유니버스는 가져오지 않고 보고서만 가져오는 경우 이 둘 사이의 관계는 끊어집니다. 따라서 보고서가 대상 시스템에서 실행되지 않습니다.

사용자 및 그룹 가져오기

그룹과 사용자를 SAP BusinessObjects Business Intelligence 플랫폼 시스템으로 가져오는 경우 그룹이 이미 대상 시스템에 있으면 BIAR 파일에서 내보낸 소속 그룹이 대상에 있는 소속 그룹을 덮어씁니다.

니다. 즉, BIAR 파일 그룹에 포함되지 않은 사용자가 대상 시스템의 그룹에 있더라도 해당 사용자는 가져오기를 마친 후 그룹에 포함되지 않습니다.

권한 가져오기

사용자/그룹을 개체와 함께 내보내거나 사용자/그룹이 이미 대상에 있는 경우에만 BIAR 엔진 명령줄 도구를 사용하여 개체에 대한 권한을 가져올 수 있습니다.

개체 및 사용자 또는 그룹이 이미 대상 시스템에 있는 경우 해당 개체 및 사용자에게 대해 가져온 권한이 대상 시스템에 있는 기존 권한을 덮어씁니다.

그러나 개체가 이미 대상에 있고 사용자/그룹이 대상에서 해당 개체에 대해 지정된 권한을 갖고 있더라도 BIAR 파일을 사용할 때 이 사용자/그룹에 대해 아무런 개체 관련 권한을 지정하지 않으면 사용자/그룹의 기존 권한이 제거되지 않습니다.

즉, 대상 개체에 대해 설정된 권한을 덮어쓸 수는 있어도 제거할 수는 없습니다.

여러 BIAR 파일 사용

BIAR 엔진 명령줄 도구를 사용하여 콘텐츠를 내보내면 해당 콘텐츠가 BIAR 파일에 배치됩니다. BIAR 파일의 위치와 이름은 `exportBiarLocation` 매개 변수를 통해 결정됩니다. BIAR 파일 하나에 저장할 수 있는 정보의 양보다 많은 콘텐츠를 내보낼 경우에는 정보가 분할되어 여러 개의 BIAR 파일에 저장됩니다. 이들 파일에는 사용자가 지정한 이름이 사용되고 각 파일 이름 끝에 번호가 추가됩니다.

예를 들어 `exportBiarLocation = C:\Archive.biar`을 설정하고 BIAR 파일 하나에 포함할 수 있는 것보다 많은 콘텐츠를 내보내면 `Archive.biar`, `Archive1.biar`, `Archive2.biar` 등의 파일이 만들어집니다. 이러한 파일은 C: 디렉터리에 생깁니다.

참고:

여러 개의 BIAR 파일에 저장되어 있는 콘텐츠를 가져오려면 모든 BIAR 파일이 동일한 디렉터리에 있어야 합니다.

12.3.1 속성 파일 사용

BIAR 엔진 명령줄 도구의 속성 파일에는 BIAR에서 수행할 작업과 연결할 SAP BusinessObjects Business Intelligence 플랫폼 시스템 등을 알려주는 매개 변수가 포함되어 있어야 합니다.

이 파일의 확장명은 `.properties`여야 합니다. 예를 들면 `Myproperties.properties` 같은 형식입니다.

속성 파일에 포함될 수 있는 매개 변수는 다음과 같습니다.

매개 변수	허용되는 값	설명	예제
Action	exportXML, importXML	이 도구를 사용하여 BIAR 파일에서 SAP BusinessObjects Business Intelligence 플랫폼 시스템으로 콘텐츠를 가져올지 아니면 배포에서 BIAR 파일로 콘텐츠를 내보낼지 여부를 지정합니다. 필수 항목입니다.	Action=exportXML
exportBiarLocation	자유 형식의 텍스트입니다. .biar 확장명을 포함해야 합니다.	내보낸 BIAR 파일을 저장할 위치를 지정합니다. action=exportXML인 경우 필수 항목입니다.	exportBiarLocation=C:/BiarExportFile.biar
importBiarLocation	자유 형식의 텍스트입니다. .biar 확장명을 포함해야 합니다.	가져올 BIAR 파일이 있는 위치를 지정합니다. 콘텐츠가 너무 커서 BIAR 파일 하나의 용량을 초과하는 경우 BIAR 파일이 여러 개로 분할됩니다. 분할된 BIAR 파일 중 아무거나 열 수는 있지만 분할된 모든 파일은 동일한 디렉터리에 있어야 합니다. action=importXML인 경우 필수 항목입니다.	importBiarLocation=C:/BiarImportFile.biar
userName	자유 형식의 텍스트입니다.	중앙 관리 서버(CMS)에 연결하기 위해 이 도구에서 사용해야 할 관리 계정의 사용자 이름입니다. 이는 위임된 관리자 계정의 사용자 이름이 될 수 있습니다. 필수 항목입니다.	userName=Administrator

매개 변수	허용되는 값	설명	예제
password	자유 형식의 텍스트입니다.	관리 계정의 암호입니다. 필수 항목입니다.	password=password
authentication	secEnterprise, secWinAd, secLdap	도구에서 사용하는 인증 유형입니다. 선택 항목입니다. 인증 형 식을 지정하지 않은 경우 기본값은 secEnterprise 입니다.	authentication=secEnter prise
CMS	자유 형식의 텍스트입니 다.	연결하려는 CMS의 이름 입니다. 필수 항목입니다.	CMS=mycms:6400
exportDependencies	True, False	개체의 모든 종속 항목을 가져올지 여부를 지정합 니다. 선택된 개체와 관련 된 모든 개체를 가져오게 될 수 있으므로 이 옵션을 사용할 때는 특히 주의해 야 합니다. BIAR 파일의 크기가 매우 커질 수 있기 때문입니다. 선택 항목입니다. 값을 지 정하지 않은 경우 기본값 은 False입니다. action=exportXML인 경 우에만 사용합니다.	exportDependen cies=false

매개 변수	허용되는 값	설명	예제
includeSecurity	True, False	<p>선택한 개체 및 사용자와 관련된 보안을 내보내거나 가져올지 여부를 지정합니다. 보안을 유지하려면 콘텐츠를 내보내고 가져올 때는 반드시 includeSecurity를 True로 설정해야 합니다.</p> <p>참고: 액세스 수준을 사용하는 경우 이러한 개체를 명시적으로 내보내야 합니다.</p> <p>선택 항목입니다. 이 매개 변수의 값을 지정하지 않은 경우 기본값은 True입니다.</p>	includeSecurity=false
exportQuery	자유 형식의 텍스트입니다. CMS 쿼리 언어 형식을 사용해야 합니다.	<p>내보낼 개체를 수집하기 위해 도구에서 실행해야 할 쿼리를 지정합니다.</p> <p>속성 파일 하나에 사용할 수 있는 쿼리 수에는 제한이 없지만 쿼리 이름은 exportQuery1, exportQuery2 등과 같은 방식으로 지정해야 합니다.</p> <p>action=exportXML인 경우 필수 항목입니다.</p>	<pre>exportQuery=select * from ci_Infoobjects where si_name = 'Xtreme Employees' and si_kind = 'Webi'</pre>
exportQueriesTotal	양의 정수입니다.	<p>도구에서 실행할 내보내기 쿼리의 수를 지정합니다. 내보내기 쿼리 수가 x개이고 그 모두를 실행하려면 이 매개 변수를 x로 설정해야 합니다.</p> <p>선택 항목입니다. 이 매개 변수의 값을 지정하지 않은 경우 기본값은 1입니다.</p> <p>action=exportXML인 경우에만 사용됩니다.</p>	exportQueriesTotal=5

참고:

주석 처리해야 할 줄이 있으면 # 문자를 사용합니다. 예를 들면 다음과 같습니다.

```
action=importXML
#exportLocation=C:/mybiar.biar
importLocation=C:/mybiar.biar
```

다음은 BIAR 파일에서 콘텐츠를 가져오는 속성 파일의 예입니다.

```
#This file imports a biar, note this line is a comment
importBiarLocation=C:/CR.biar
action=importXML
userName=Administrator
password=
CMS=mycms:6400
authentication=secEnterprise
```

다음은 Xtreme Employees라는 Web Intelligence 보고서를 BIAR 파일로 내보내는 속성 파일의 예입니다.

```
#This file exports a single report
# Remember to include indexed properties with your query!
# The more indexed properties, the better!
exportBiarLocation=C:/CR.biar
action=importXML
userName=Administrator
password=
CMS=mycms:6400
authentication=secEnterprise
exportDependencies=false
exportQuery= select * from ci_Infoobjects where si_name = 'Xtreme Employees' and si_kind = 'Webi'
```

12.3.2 BIAR 엔진 명령줄 도구 사용

1. 명령줄 창을 열고 biarengine.jar이 있는 디렉터리로 이동합니다.

예를 들면 <InstallDir>WSAP BusinessObjects Enterprise XI4.0\JavaWLib 디렉터리로 이동합니다.

2. biarengine.jar을 실행합니다.

예를 들어 java -jar biarengine.jar <속성 파일>을 실행합니다.

BIAR 엔진 명령줄 도구는 속성 파일의 action 매개 변수에 따라 SAP BusinessObjects Business Intelligence 플랫폼 배포에서 BIAR 파일로 콘텐츠를 내보내거나 BIAR 파일에서 SAP BusinessObjects Business Intelligence 플랫폼 배포로 콘텐츠를 가져옵니다.

장13 응용 프로그램 관리

13.1 CMC를 통한 응용 프로그램 관리

13.1.1 개요

CMC의 응용 프로그램 관리 영역에서는 별도의 프로그래밍 작업 없이도 CMC나 BI 실행 패드 같은 웹 응용 프로그램의 모양과 기능을 변경할 수 있습니다. 사용자, 그룹 및 관리자에게 연결된 권한을 변경하여 각각의 응용 프로그램 액세스 권한을 수정할 수도 있습니다.

이 단원에서는 여러 가지 설정을 관리하는 방법에 대한 상황에 맞는 정보, 절차 및 지침을 제공합니다. 다음 응용 프로그램에는 CMC를 통해 수정할 수 있는 설정이 있습니다.

- Analysis, OLAP용 에디션
- 경고
- BI 실행 패드
- BI 작업 영역
- 중앙 관리 콘솔
- Crystal Reports
- Dashboard Design
- 토론
- 정보 디자이너
- Web Intelligence
- LifeCycle Manager
- 모니터링
- 문서 열기
- 플랫폼 검색
- 보고서 변환 도구

- SAP BusinessObjects Mobile
- 번역 관리 도구
- 유니버스 디자인 도구
- 업그레이드 관리 도구
- VisualDiff 응용 프로그램
- 웹 서비스
- SAP BusinessObjects Business Intelligence 플랫폼용 위젯

13.1.2 응용 프로그램의 일반 설정

13.1.2.1 응용 프로그램에 대한 사용자 권한 설정

권한을 사용하면 응용 프로그램의 특정 기능에 대한 사용자 액세스를 제어할 수 있습니다. CMC의 응용 프로그램 영역을 통해 응용 프로그램에 대한 액세스 제어 목록에 사용자를 할당하고, 사용자가 보유한 권한을 확인하며, 응용 프로그램에 대해 사용자가 갖고 있는 권한을 수정할 수 있습니다. 권한 관리에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드를 참조하십시오.

13.1.2.2 CMC에서 웹 응용 프로그램 추적 로그 수준 설정

기본적으로, CMC의 웹 응용 프로그램에 대한 추적 로그 수준은 지정되지 않음으로 설정됩니다. CMC에서 다음 응용 프로그램에 대한 추적 로그 설정을 사용할 수 있습니다.

- 중앙 관리 콘솔
- BI 실행 패드
- Open Document
- 웹 서비스

다른 웹 응용 프로그램을 모두 추적하려면 해당 BO_trace 파일을 구성하기 위한 수동 방법을 사용하십시오.

1. CMC의 응용 프로그램 관리 영역으로 이동합니다.
응용 프로그램 대화 상자가 표시됩니다.
 2. 응용 프로그램을 마우스 오른쪽 단추로 클릭하고 추적 로그 설정을 선택합니다.
추적 로그 설정 대화 상자가 나타납니다.
 3. 로그 수준 목록에서 원하는 설정을 선택합니다.
 4. 저장 후 닫기를 클릭하여 추적 로그 수준을 제출합니다.
- 새 추적 로그 수준은 다음에 웹 응용 프로그램에 로그인한 후에 적용됩니다.

관련 항목

- 743 페이지에서 [추적 로그 수준](#)

13.1.2.2.1 추적 로그 수준

다음 표에는 BI 플랫폼 구성 요소에서 사용 가능한 추적 로그 수준이 나와 있습니다.

수준	설명
지정되지 않음	추적 로그 수준은 다른 메커니즘(보통 .ini 파일)을 통해 지정됩니다.
없음	추적 로그 수준이 없음으로 설정되어 있을 때는 지정된 중요도 수준 미만으로 추적을 선택적으로 억제할 수 있는 필터가 비활성화됩니다. 참고: 추적 로그 수준이 없음이라고 해서 추적 기능이 해제되는 것은 아닙니다. 시스템 리소스는 계속 모니터링되고 실패한 어설션과 같이 드물게 발생하는 중요 이벤트에 대해 추적이 로그됩니다.
낮음	경고 메시지와 대부분의 상태 메시지를 무시한 상태에서 오류 메시지를 로그할 수 있도록 추적 로그 필터가 설정됩니다. 하지만, 시작 및 종료 요청 메시지뿐 아니라 구성 요소 시작, 시스템 종료에 대해서도 매우 중요한 상태 메시지가 로그로 기록됩니다. 참고: 디버깅할 목적이라면 이 수준으로 설정하지 않는 것이 좋습니다.
중간	추적 로그 필터는 로그 출력에 오류, 경고 및 대부분의 상태 메시지를 포함하도록 설정됩니다. 중요도가 최소이거나 세부 정보 표시 수준이 높은 상태 메시지는 필터링됩니다. 디버깅할 목적이라면 이 수준은 세부 정보를 표시하기에 충분치 않습니다.
높음	이 필터로는 어떤 메시지도 제외되지 않습니다. 디버깅할 목적이라면 이 수준으로 설정하는 것이 좋습니다. 참고: 높음 추적 로그 수준 설정으로 시스템 리소스에 영향을 미칠 수 있습니다. 파일 시스템의 저장 공간뿐 아니라 CPU 사용량을 증가시켰을 가능성이 있습니다.

13.1.3 응용 프로그램 관련 설정

13.1.3.1 CMC 응용 프로그램 설정 관리

13.1.3.1.1 인증 및 프로그램 개체

리포지토리에 프로그램 개체를 추가할 때 잠재적 보안 위험이 있을 수 있습니다. 프로그램 개체를 실행하는 데 사용되는 계정의 파일 권한 수준에 따라 프로그램에서 수정할 수 있는 파일의 내용이 결정됩니다.

사용자가 실행할 수 있는 프로그램 개체의 형식을 제어할 수 있고 프로그램 개체를 실행하는 데 필요한 자격 증명을 구성할 수 있습니다.

프로그램 개체 형식 활성화 또는 비활성화

보안을 위한 첫 번째 단계는 사용 가능한 프로그램 개체의 유형을 지정하는 것입니다.

모든 플랫폼에서의 인증

CMC의 폴더 관리 영역에서 프로그램 실행에 사용되는 계정의 자격 증명을 지정해야 합니다. 이 기능을 사용하면 프로그램에 대해 특정 사용자 계정을 설정하고 이 계정에 적절한 권한을 할당해서 프로그램 개체가 이 계정에서 실행되도록 할 수 있습니다.

또는 BI 플랫폼에 프로그램 개체를 추가하는 사용자는 자신의 자격 증명을 프로그램 개체에 할당하여 프로그램이 시스템에 액세스하도록 할 수 있습니다. 이 경우 프로그램은 이 사용자 계정을 통해 실행되며 프로그램의 권한은 사용자의 권한으로 제한됩니다. 프로그램 개체에 대한 사용자 계정을 지정하지 않으면 일반적으로 로컬 권한은 있지만 네트워크를 통한 권한은 부여되지 않은 기본 시스템 계정을 사용하여 프로그램 개체가 실행됩니다.

참고:

기본적으로 프로그램 개체에 일정을 설정할 때 자격 증명을 지정하지 않으면 작업에 실패합니다. 기본 자격 증명을 제공하려면 응용 프로그램 관리 영역에서 CMC를 선택합니다. 작업 메뉴에서 프로그램 개체 권한을 클릭합니다. 다음 운영 체제 자격 증명을 사용하여 일정을 설정합니다.를 클릭하고 기본 사용자 이름 및 암호를 입력합니다.

Java 프로그램에 대한 인증

BI 플랫폼을 사용하면 모든 프로그램 개체에 대한 보안을 설정할 수 있습니다. Java 프로그램의 경우 BI 플랫폼에서는 안전하지 않은 코드에 대한 Java 기본값과 일치하는 기본 설정이 있는 Java 정책 파일을 사용합니다. JDK(Java Development Kit)에서 제공되는 Java 정책 도구를 사용하면 사용자의 필요에 맞게 Java 정책 파일을 수정할 수 있습니다.

Java 정책 도구에는 두 가지 코드 베이스 항목이 있습니다. BI 플랫폼 Java SDK를 가리키는 첫 번째 항목을 사용하면 모든 BI 플랫폼 JAR 파일에 대한 모든 권한을 프로그램 개체에 부여할 수 있습니다. 두 번째 코드 베이스 항목은 모든 로컬 파일에 적용됩니다. 이 항목에서는 안전하지 않은 코드에 대한 Java 기본값과 동일한 보안 설정을 보안되지 않은 코드에 사용합니다.

참고:

- Java 정책 설정은 동일한 컴퓨터에서 실행되는 모든 프로그램 작업 서버에 공통으로 적용됩니다.

- 기본적으로 Java 정책 파일은 BI 플랫폼 설치 루트 디렉터리의 Java SDK 디렉터리에 설치됩니다. 예를 들어 Windows에서의 일반적인 위치는 C:\WProgram Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Wconf\Wcrystal-program.policy입니다.

13.1.3.1.1.1 프로그램 개체 유형 활성화 또는 비활성화

1. 응용 프로그램 영역에서 중앙 관리 콘솔을 선택합니다.
2. 작업 > 프로그램 개체 권한을 클릭합니다.
프로그램 개체 권한 대화 상자가 나타납니다.
3. 사용자에게 허용할 권한 영역에서 사용자가 실행할 수 있도록 할 프로그램 개체의 종류를 선택합니다.
스크립트/이진 파일 실행 또는 Java 프로그램 실행을 선택할 수 있습니다.
Java 프로그램 실행을 선택한 경우에는 가상 사용 확인란을 선택하거나 취소할 수 있습니다. 이 옵션을 선택하면 BI 플랫폼에 로그인할 때 사용하는 토큰이 Java 프로그램에 제공됩니다.
4. 저장 후 단기를 클릭합니다.

13.1.3.1.2 시스템에 처리 확장 등록

참고:

이 기능은 Web Intelligence 문서에는 적용되지 않습니다.

특정 개체에 처리 확장을 적용하려면 먼저 관련 예약 또는 보기 요청을 처리할 각 컴퓨터에서 코드 라이브러리를 사용할 수 있도록 해야 합니다. BI 플랫폼을 설치하면 각 작업 서버, 처리 서버 및 RAS(Report Application Server)에 처리 확장을 위한 기본 디렉터리가 생성됩니다. 처리 확장을 각 서버의 기본 디렉터리에 복사하는 것이 좋습니다. Windows에서 기본 디렉터리는 C:\WProgram Files\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\Wwin32_x86\WProcessExt입니다. UNIX에서는 sap_bobj/ProcessExt입니다.

팁:

처리 확장 파일은 공유할 수 있습니다.

확장에서 구현한 기능에 따라 라이브러리를 다음 컴퓨터에 복사합니다.

- 처리 확장에서 예약 요청만 차단하는 경우 적응형 작업 서버로 실행되는 각 컴퓨터에 라이브러리를 복사합니다.
- 처리 확장에서 보기 요청만 차단하는 경우 Crystal Reports 처리 서버 또는 RAS로 실행되는 각 컴퓨터에 라이브러리를 복사합니다.
- 처리 확장이 예약 요청과 보기 요청을 차단하는 경우 적응형 작업 서버, Crystal Reports 처리 서버 또는 RAS로 실행되는 각 컴퓨터에 라이브러리를 복사합니다.

참고:

특정 서버 그룹에 대한 일정/보기 요청에만 처리 확장이 필요한 경우 해당 그룹의 각 처리 서버에만 라이브러리를 복사하면 됩니다.

관련 항목

- 500 페이지에서 [여러 서버 사이에서 처리 확장 공유](#)"

13.1.3.1.2.1 시스템에 처리 확장 등록

1. CMC의 응용 프로그램 관리 영역으로 이동합니다.
2. 중앙 관리 콘솔을 선택합니다.
3. 작업 > 처리 확장을 클릭합니다.
처리 확장: CMC 대화 상자가 나타납니다.
4. 이름 필드에 처리 확장의 표시 이름을 입력합니다.
5. 위치 필드에 처리 확장의 파일 이름을 모든 추가 경로 정보와 함께 입력합니다.
 - 처리 확장을 각 컴퓨터의 기본 디렉터리에 복사한 경우 파일 확장명 없이 파일 이름만 입력합니다.
 - 처리 확장을 기본 디렉터리 아래의 하위 폴더에 복사한 경우 하위 폴더/파일 이름 형식으로 위치를 입력합니다.
6. 설명 필드를 사용하여 처리 확장에 대한 정보를 추가합니다.
7. 추가를 클릭합니다.

팁:

처리 확장을 삭제하려면 기존 확장 목록에서 확장을 선택하고 삭제를 클릭합니다. 이 처리 확장을 기반으로 한 이후의 모든 작업이 실패하게 되므로 이를 기반으로 어떠한 작업도 되풀이되지 않도록 해야 합니다.

8. 저장 후 단기를 클릭합니다.
처리 확장이 CMC에 등록됩니다.

이제 이 처리 확장을 선택하여 해당 논리를 특정 개체에 적용할 수 있습니다.

13.1.3.1.2.2 여러 서버 사이에서 처리 확장 공유

참고:

BI 플랫폼에서 만들어진 Web Intelligence 문서나 보고서에서는 이 기능을 사용할 수 없습니다.

적응형 작업 서버, Crystal Reports 처리 서버 및 RAS마다 기본 처리 확장 디렉터리를 재정의하면 모든 처리 확장을 한 곳에 배치할 수 있습니다. 먼저 모든 서버에서 액세스할 수 있는 네트워크 드라이브의 공유 디렉터리에 처리 확장을 복사합니다. 각 서버 컴퓨터에서 네트워크 드라이브를 매핑(또는 마운팅)합니다.

참고:

Windows의 경우 매핑된 드라이브를 사용하려면 컴퓨터를 다시 부팅해야 합니다.

Windows와 UNIX 모두에서 서버를 실행하는 경우에는 모든 처리 확장의 .dll 및 .so 버전을 공유 디렉터리에 복사해야 합니다. 또한 공유 네트워크 드라이브는 Samba 또는 다른 파일 공유 시스템을 통해 Windows와 UNIX 컴퓨터에 모두 표시되어야 합니다.

마지막으로 각 서버의 명령줄을 변경하여 기본 처리 확장 디렉터리를 수정합니다. 명령줄에 `-report_ProcessExtPath` 절대 경로를 추가하면 됩니다. 여기에서 절대 경로는 서버가 실행되는 운영 체제에 적합한 경로 규칙을 사용하여 새 폴더의 경로로 바꿉니다(예: `M:\WcodeWextensions`, `/home/shared/code/extensions` 등).

기본 처리 확장 디렉터리를 수정하려면 CMC를 사용하여 서버를 중지합니다. 그런 다음 서버의 속성을 열고 명령줄을 수정합니다. 필요한 사항을 모두 수정한 다음 서버를 다시 시작합니다.

13.1.3.2 토론 설정 관리

BI 플랫폼에 포함된 CMC의 응용 프로그램 영역에서는 시스템 수준의 토론 스레드 설정을 지정할 수 있습니다.

토론 응용 프로그램의 경우 다음을 포함한 여러 가지 방법으로 토론 스레드를 관리하고 상호 작용할 수 있습니다.

- 지정된 검색 조건에 따라 토론 스레드 검색
- 토론 스레드 검색 결과 정렬
- 토론 스레드 삭제

참고:

토론 응용 프로그램에는 사용자 권한 설정을 사용할 수 없습니다. 그러나 개별 보고서에 대한 권한을 설정할 수는 있습니다.

13.1.3.2.1 토론 스레드 검색

기본적으로 토론 페이지에는 모든 토론 스레드의 제목이 표시됩니다. 루트 수준의 스레드만 표시되며 토론 스레드의 목록 페이지 사이를 이동하려면 이전 및 다음 단추를 사용합니다. 특정 스레드를 검색하거나 스레드 그룹을 검색할 수도 있습니다.

1. CMC의 응용 프로그램 영역으로 이동하여 토론을 선택합니다.
2. 관리 > 속성을 클릭합니다.
메모 관리 대화 상자가 열립니다.
3. 필드 이름 목록에서 옵션을 선택합니다.

옵션	설명
스레드 제목	스레드 제목을 기준으로 검색합니다.
만든 날짜	만든 날짜를 기준으로 검색합니다.
마지막으로 수정한 날짜	마지막 수정한 날짜를 기준으로 검색합니다.
만든 이	만든 이를 기준으로 검색합니다.

4. 두 번째 목록에서 검색 조건을 상세하게 설정합니다.

참고:

검색에서는 대/소문자를 구분하지 않습니다.

- 스레드 제목이나 만든 이를 기준으로 검색하는 경우 두 번째 필드에서 다음 옵션을 선택합니다.

옵션	설명
같음	스레드 제목 또는 만든 이 이름이 세 번째 필드에 입력한 텍스트와 정확히 일치하는 토론 스레드를 검색합니다.
같지 않음	스레드 제목 또는 만든 이 이름이 세 번째 필드에 입력한 텍스트와 정확히 일치하지 않는 토론 스레드를 검색합니다.
포함	스레드 제목 또는 만든 이의 이름에 검색 텍스트 문자열이 포함된 토론 스레드를 검색합니다.
포함하지 않음	스레드 제목에 텍스트 문자열이 포함되지 않은 토론 스레드를 검색합니다.

- 만든 날짜 또는 마지막으로 수정한 날짜를 선택하는 경우 다음 옵션 중 하나를 선택한 후 검색 날짜를 지정하십시오.

옵션	설명
이전	검색 날짜 이전에 만들거나 수정한 토론 스레드를 검색합니다.
이후	검색 날짜 이후에 만들거나 수정한 토론 스레드를 검색합니다.
사이에 있음	두 검색 날짜 사이에 만들거나 수정한 토론 스레드를 검색합니다.

5. 검색을 더 구체적으로 정의하려면 셋째 텍스트 필드를 사용합니다.
 - 처음 두 필드에서 텍스트를 기반으로 한 검색을 선택한 경우 텍스트 문자열을 입력합니다.
 - 날짜 기반 검색을 선택한 경우에는 해당 필드에 한 개 이상의 날짜를 입력합니다.
6. 검색을 클릭합니다.

13.1.3.2.2 토론 스레드 검색 결과 정렬

토론 스레드를 검색할 때 검색 결과를 표시할 방식을 선택할 수 있습니다. 예를 들어 검색 결과를 사전 오름차순으로 정렬할 수 있고 한 페이지에 표시할 결과 수를 선택할 수 있습니다.

1. CMC의 응용 프로그램 영역으로 이동하여 토론을 선택합니다.
2. 관리 > 속성을 클릭합니다.
메모 관리 대화 상자가 열립니다.
3. 정렬 기준 목록에서 정렬 옵션을 선택합니다.

옵션	설명
스레드 제목	토론 스레드의 제목을 기준으로 정렬합니다.
만든 날짜	토론 스레드를 만든 날짜를 기준으로 정렬합니다.
마지막으로 수정한 날짜	토론 스레드를 마지막으로 수정한 날짜를 기준으로 정렬합니다.
만든 이	특정 토론 스레드를 만든 이를 기준으로 정렬합니다.

4. 두 번째 목록에서 레코드를 오름차순으로 표시할지 또는 내림차순으로 표시할지 선택합니다.
5. 셋째 텍스트 필드에는 각 페이지에 표시할 토론 스레드 결과의 수를 입력합니다.
기본적으로 페이지당 10개의 결과가 표시됩니다.
6. 검색을 클릭합니다.

13.1.3.2.3 토론 스레드 삭제

BI 플랫폼에 포함된 CMC의 응용 프로그램 영역에서 토론 스레드를 삭제할 수 있습니다.

1. CMC의 응용 프로그램 영역으로 이동하여 토론을 선택합니다.
2. 관리 > 속성을 클릭합니다.
메모 관리 대화 상자가 열립니다.
3. 결과 목록에서 삭제하려는 토론 스레드를 검색한 다음 선택합니다.
4. 삭제를 클릭합니다.

13.1.3.3 BI 실행 패드 설정 관리

BI 플랫폼에 포함된 CMC의 응용 프로그램 영역에서 관리 > 속성으로 이동하여 BI 실행 패드의 표시 옵션을 변경할 수 있습니다.

BI 실행 패드에 대해 사용자 또는 그룹에 다음과 같은 권한을 부여할 수 있습니다.

- 기본 설정 변경
- 폴더 구성
- 검색
- 개체 형식별로 개체 목록 필터링
- 즐겨찾기 폴더 보기

예를 들어 표준 명명 규칙을 사용하여 사용자의 폴더를 만든 경우 사용자가 자신의 폴더를 구성할 수 없도록 관련 권한을 거부할 수도 있습니다.

참고:

기본적으로 모든 사용자는 이러한 기능에 액세스할 수 있습니다.

13.1.3.3.1 BI 실행 패드의 표시 설정 변경

1. CMC의 응용 프로그램 영역으로 이동하여 BI 실행 패드를 선택합니다.
2. 관리 > 속성을 클릭합니다.
BI 실행 패드 속성 대화 상자가 열립니다.
3. BI 실행 패드 사용자를 위해 토론을 사용하려면 토론 사용을 선택합니다.
4. 예약을 위해 필터 기능을 사용하려면 예약 페이지에서 "필터" 표시 탭을 선택합니다.
이 설정은 사용자가 Crystal 보고서를 예약할 때 레코드 또는 그룹 선택 수식을 입력할 수 있을지 여부를 조정합니다.
5. 저장 후 닫기를 클릭합니다.

13.1.3.4 Web Intelligence 설정 관리

Web Intelligence 응용 프로그램에 대한 속성을 설정하여 Web Intelligence 문서 액세스와 관련하여 사용자에게 제공되는 기능을 제어할 수 있습니다.

13.1.3.4.1 Web Intelligence의 표시 설정 수정

1. CMC의 응용 프로그램 영역으로 이동하여 Web Intelligence를 선택합니다.
2. 관리 > 속성을 클릭합니다.
표시 옵션이 있는 속성 대화 상자가 열립니다.
3. 다음 표시 옵션 중 필요한 항목을 정의합니다.

옵션	설명
차원 및 세부 정보	이 영역에 있는 옵션은 추가된 데이터가 보고서에 표시되는 방식을 정의하는 데 사용합니다. 글꼴 스타일, 텍스트 색 및 배경색을 변경할 수 있습니다. 변경 내용이 셀 미리 보기에 자동으로 표시됩니다. 마치면 확인을 클릭합니다.
변화하는 값(숫자 측정값)	이 영역에 있는 옵션은 페이지 머리글을 수정하고 서식 지정하는 데 사용합니다. 글꼴 스타일, 텍스트 색 및 배경색을 변경할 수 있습니다. 변경 내용이 셀 미리 보기에 자동으로 표시됩니다. 마치면 확인을 클릭합니다.
포함된 이미지 속성	포함된 이미지의 최대 크기를 입력합니다.
빠른 표시 모드 속성	최대 세로 레코드 수, 최대 가로 레코드 수, 페이지의 최소 너비, 페이지의 최소 높이, 오른쪽 안쪽 여백 값 및 아래쪽 안쪽 여백 값을 해당 필드에 입력합니다.

4. 저장 후 단기를 클릭합니다.

참고:

선택 내용을 기본 표시 변수로 되돌리려면 원래대로를 클릭합니다.

13.1.3.5 경고 설정 관리

BI 플랫폼에 포함된 CMC의 응용 프로그램 영역에서는 시스템 수준의 경고 설정을 지정할 수 있습니다.

경고 응용 프로그램의 경우 다음과 같은 방법으로 시스템 사용자가 경고에 액세스하는 방식을 제어하고 정의할 수 있습니다.

- 경고 가입자용 내 경고 폴더 사용
- 전자 메일을 통해 전송된 경고 메시지 사용 및 서식 지정
- 시스템의 경고 수 제한 설정
- 경고 메시지 만료 기간 설정

관련 항목

- 494 페이지에서 [응용 프로그램에 대한 사용자 권한 설정](#)
- 505 페이지에서 [경고 설정 관리](#)

13.1.3.5.1 경고 대상 속성 수정

1. CMC의 응용 프로그램 영역으로 이동하여 경고 응용 프로그램을 선택합니다.
2. 관리 > 속성을 클릭합니다.
경고 대화 상자가 열리면서 기본 대상 속성이 표시됩니다.
3. 적절한 옵션을 설정합니다.

옵션	설명
내 경고 사용	경고 가입자가 알림을 받도록 허용하려면 BI 실행 패드의 내 경고 섹션에서 이 옵션을 선택합니다.
전자 메일 사용	경고 가입자가 전자 메일을 통해 알림을 받도록 허용하려면 이 옵션을 선택합니다. 이 옵션을 선택하면 경고에 대한 전역 전자 메일 설정이 표시됩니다.

참고:

위 대상 옵션 중 하나 이상을 지정해야 합니다.

전자 메일 사용을 선택한 경우 다음과 같은 전역 설정을 수정할 수 있습니다.

옵션	설명
보낸 사람	경고 알림을 전송하는 전자 메일 주소를 지정합니다. 가입자는 지정된 발신인으로부터 경고 전자 메일을 받게 됩니다. 시스템이 인식할 수 있는 유효한 전자 메일 주소를 사용하는 것이 좋습니다.
받는 사람	경고 가입자의 전자 메일 주소를 지정합니다. 팁: 이 설정에는 %SI_EMAIL_ADDRESS% 자리 표시자를 유지하는 것이 좋습니다. 특정 전자 메일 주소 또는 받는 사람을 지정하면 기본적으로 모든 시스템 경고가 지정된 전자 메일 주소로 전송됩니다.
참조	전자 메일을 통해 전송된 경고를 함께 받을 사람을 지정합니다.
제목	시스템 경고가 포함된 전자 메일의 기본 제목 머리글을 지정합니다.

옵션	설명
메시지	시스템 경고가 포함된 전자 메일의 기본 메시지를 지정합니다.
첨부 파일 추가	시스템 경고가 포함된 전자 메일에 첨부 파일을 기본으로 포함하려면 이 옵션을 선택합니다. 이 옵션은 트리거된 경고와 연관 있는 Crystal Reports를 기본적으로 포함하려는 경우에 주로 사용됩니다.
파일 이름	첨부 파일 추가 옵션을 선택한 경우 자동 생성 또는 특정 이름 중 하나를 선택하여 전자 메일에서 첨부 파일의 이름이 결정되는 방식을 지정합니다.

4. 저장 후 닫기를 클릭합니다.

관련 항목

- 494 페이지에서 [응용 프로그램에 대한 사용자 권한 설정](#)"
- 505 페이지에서 [경고 설정 관리](#)"

13.1.3.5.2 경고 기본 속성 수정

1. CMC의 응용 프로그램 영역으로 이동하여 경고 응용 프로그램을 선택합니다.
2. 관리 > 속성 > 기본 설정을 클릭합니다.
3. 다음 속성에 적절한 값을 설정합니다.

옵션	설명
만료 기간	시스템에서 경고 메시지가 삭제되기까지의 기간을 지정합니다.
최대 경고 메시지 수	시스템이 지원하는 경고 메시지의 최대 수를 지정합니다. 임계값에 도달하면 가장 오래된 메시지부터 시작하여 경고 메시지의 20%가 자동으로 제거됩니다.

4. 저장 후 닫기를 클릭합니다.

관련 항목

- 123 페이지에서 [CMC에서 개체의 보안 설정 관리](#)"
- 505 페이지에서 [경고 설정 관리](#)"

13.1.3.6 위젯 설정 관리

SAP BusinessObjects용 위젯은 사용자가 BI 플랫폼의 비즈니스 인텔리전스 콘텐츠와 SAP NetWeaver Application Server의 Web Dynpro 응용 프로그램에 손쉽게 액세스할 수 있도록 바탕 화면에 미니 응용 프로그램을 추가할 수 있게 해주는 데스크톱 응용 프로그램입니다.

CMC의 "응용 프로그램" 영역에서는 바탕 화면에 위젯을 만들어 사용하기 위한 사용자 액세스뿐 아니라, 바탕 화면의 위젯 응용 프로그램 내에서 BI 플랫폼 리포지토리를 검색하는 기능도 제어할 수 있습니다.

사용자나 그룹에게 다음과 같은 능력을 부여할 수 있습니다.

- 위젯 사용
- 위젯에서 만든 개체 편집
- 액세스 개체에 대한 사용자 권한 수정

참고:

기본적으로 모든 일반 사용자는 이러한 기능에 액세스할 수 있습니다.

관련 항목

- 123 페이지에서 [CMC에서 개체의 보안 설정 관리](#)

13.1.3.7 SAP BusinessObjects Explorer 설정 관리

CMC의 응용 프로그램 영역에서 해당 보안 권한을 설정하면 SAP BusinessObjects Explorer와 관련하여 사용자가 액세스할 수 있는 기능을 정의할 수 있습니다.

관련 항목

- 123 페이지에서 [CMC에서 개체의 보안 설정 관리](#)

13.1.3.7.1 SAP BusinessObjects Explorer 응용 프로그램 속성 수정

1. CMC의 응용 프로그램 영역으로 이동합니다.
2. 관리 > 속성을 클릭합니다.
SAP BusinessObjects Explorer 속성 대화 상자가 나타납니다.
3. 다음 SAP BusinessObjects Explorer 설정 중 필요한 항목을 정의합니다.
 - 기본 인덱스 폴더 위치
 - 스레드 수
 - 체크알피 유효성
4. 저장 후 닫기를 클릭합니다.

13.1.3.8 플랫폼 검색 설정 관리

BI 플랫폼에 포함된 CMC의 응용 프로그램 영역에서는 시스템 수준의 플랫폼 검색 응용 프로그램 설정을 지정할 수 있습니다.

관련 항목

- 617 페이지에서 [인덱싱 오류 목록](#)
- 604 페이지에서 [응용 프로그램 속성 구성](#)

13.1.3.8.1 응용 프로그램 속성 구성

플랫폼 검색 응용 프로그램 속성을 구성하려면 다음 단계를 완료하십시오.

1. CMC의 응용 프로그램 영역으로 이동합니다.

2. 플랫폼 검색 응용 프로그램을 선택합니다.
3. 관리 > 속성을 클릭합니다. 플랫폼 검색 응용 프로그램 속성 대화 상자가 나타납니다.
4. 원하는 플랫폼 검색 설정을 구성합니다.

다음 표에 구성 속성에 대한 설명이 나와 있습니다.

옵션	설명
검색 통계	<p>플랫폼 검색은 다음과 같은 검색 통계를 제공합니다.</p> <ul style="list-style-type: none"> 인덱싱 상태: 인덱싱 프로세스 상태를 표시합니다. 인덱싱된 문서 수: 인덱싱된 문서 수를 표시합니다. 마지막 인덱싱 타임스탬프: 문서가 마지막으로 인덱싱된 타임스탬프를 표시합니다.
인덱싱 중지/시작	<p>연속 크롤링에서 예약된 크롤링으로 전환하려는 경우 또는 유지 관리를 위해 인덱싱 시작 또는 중지 옵션을 사용하여 인덱싱 프로세스를 시작 또는 중지할 수 있습니다.</p> <p>인덱싱을 중지하려면 인덱싱 중지를 클릭한 다음 확인 대화 상자에서 확인을 클릭합니다.</p>
인덱스 로캘	<p>인덱스 로캘을 다른 언어로 변경하면 플랫폼 검색에서 문서를 선택한 언어로 다시 인덱싱합니다.</p> <p>브라질어, 중국어, 체코어, 덴마크어, 네덜란드어, 영어, 핀란드어, 프랑스어, 독일어, 이탈리아어, 일본어, 한국어, 노르웨이어(북말), 폴란드어, 포르투갈어, 러시아어, 스페인어, 스웨덴어 및 태국어 중 한 가지 언어로 인덱싱 로캘을 설정합니다.</p> <p>참고: 기본적으로, 영어가 인덱스 로캘로 선택되어 있습니다.</p>

옵션	설명
크롤링 빈도	<p>다음 옵션을 사용하여 전체 BI 플랫폼 리포지토리를 인덱싱할 수 있습니다.</p> <ul style="list-style-type: none"> • 연속 크롤링: 이 옵션을 선택한 경우, 개체를 추가, 수정 또는 삭제할 때마다 리포지토리를 인덱싱할 때 인덱싱이 연속으로 이루어집니다. 또한 최신 SAP BusinessObjects Business Intelligence 플랫폼 콘텐츠를 보거나 사용할 수 있습니다. 기본적으로 연속 크롤링이 설정되어 있으며 연속 크롤링은 수행하는 작업에 따라 지속적으로 BI 플랫폼 리포지토리를 업데이트합니다. 연속 크롤링은 사용자 개입 없이 작동하므로 문서 인덱싱에 걸리는 시간이 단축됩니다. • 예약된 크롤링: 이 옵션을 선택한 경우, 인덱싱은 예약 옵션에서 설정한 예약을 기준으로 이루어집니다. <p>개체 예약에 대한 자세한 내용은 BI 플랫폼 CMC 온라인 도움말에서 플랫폼 검색의 개체 예약 단원을 참조하십시오.</p> <p>참고:</p> <ul style="list-style-type: none"> • 크롤링 예약을 선택하고 되풀이를 지금 이외의 다른 옵션으로 설정하면 플랫폼 검색에 문서를 다음으로 인덱싱하기로 예약한 날짜 및 타임스탬프가 표시됩니다. • 크롤링 예약을 선택한 경우에는 인덱싱 시작 단추가 활성화되며 인덱싱 중지 단추는 비활성화됩니다. • 예약이 완료되면 인덱싱 중지 단추를 사용할 수 없습니다.

옵션	설명
인덱스 위치	<p>인덱싱된 문서는 다음 위치의 공유 폴더에 저장됩니다.</p> <ul style="list-style-type: none"> • 마스터 인덱스 위치(인덱스, 맞춤법 검사기): 마스터 및 맞춤법 검사기는 이 위치에 저장됩니다. 검색 워크플로 중, 최초 검색 항목들은 마스터 인덱스를 사용하여 검색되고 맞춤법 검사기 인덱스는 제안 사항을 검색하는 데 사용됩니다. 클러스터된 BOE 배포에서 이 위치는 클러스터의 모든 노드에서 액세스 가능한 공유 파일 시스템에 있어야 합니다. • 영구 데이터 위치(컨텐츠 저장소): 콘텐츠 저장소가 이 위치에 놓입니다. 콘텐츠 저장소는 마스터 인덱스 위치에서 만들어지고 이 위치와 동기화된 상태로 남습니다. 콘텐츠 저장소는 패킷을 생성하고 마스터 인덱스 위치에서 생성된 최초 검색 항목을 처리하는 데 사용됩니다. 클러스터된 BI 플랫폼 배포에서 콘텐츠 저장소는 각 노드마다 생성됩니다. <p>영구 데이터 위치는 콘텐츠 저장소 폴더를 포함하고 있으므로 클러스터된 환경의 영향을 받는 유일한 인덱스 위치입니다. 검색 서비스가 하나만 있는 컴퓨터에는 콘텐츠 저장소 위치가 하나만 있습니다. 예: {boj.enterprise.home}\data\PlatformSearchData\workspace\Server\ContentStores</p> <p>그러나 클러스터된 환경에 여러 검색 서비스가 있는 경우 각 검색 서비스에는 하나의 콘텐츠 저장소 위치가 있습니다. 예를 들어, 실행 중인 서버 인스턴스가 두 개일 경우 콘텐츠 저장소 위치는 다음과 같습니다.</p> <ol style="list-style-type: none"> a. {boj.enterprise.home}\data\PlatformSearchData\workspace\Server\ContentStores b. {boj.enterprise.home}\data\PlatformSearchData\workspace\Server1\ContentStores <ul style="list-style-type: none"> • 비영구 데이터 위치(임시 서로게이트 파일, 델타 인덱스): 델타 인덱스가 마스터 인덱스와 병합되기 전에 이 위치에 임시로 만들어져 저장됩니다. 이 위치에서 인덱싱된 문서는 마스터 인덱스와 병합되면 삭제됩니다. 또한, 이 위치에서 서로게이트 파일(추출기의 출력 파일)이 만들어지고 이 파일이 델타 인덱스로 변환될 때까지 임시로 저장됩니다. <p>참고:</p> <ul style="list-style-type: none"> • 모든 인덱스 위치는 공유 위치여야 합니다. • 인덱스 위치를 수정하려면 인덱싱 중지를 클릭해야 합니다. • 인덱스 위치를 수정하는 경우 콘텐츠를 새 위치에 복사해야 하며, 그렇지 않으면 기존 인덱스 정보가 손실됩니다.

옵션	설명
인덱싱 수준	<p>다음과 같은 방법으로 인덱싱 수준을 설정하여 검색 콘텐츠를 조정할 수 있습니다.</p> <ul style="list-style-type: none"> 플랫폼 메타데이터: 문서 제목, 키워드, 설명 등의 플랫폼 메타데이터 정보에 대해서만 인덱스가 만들어집니다. 플랫폼 및 문서 메타데이터: 이 인덱스에는 플랫폼 메타데이터와 문서 메타데이터가 포함됩니다. 문서 메타데이터에는 만든 날짜, 수정한 날짜 및 작성자 이름이 포함됩니다. 전체 콘텐츠: 이 인덱스에는 플랫폼 메타데이터, 문서 메타데이터 및 다음과 같은 기타 콘텐츠가 포함됩니다. <ul style="list-style-type: none"> 문서의 실제 콘텐츠 프롬프트 및 LOV의 콘텐츠 차트, 그래프 및 레이블 <p>참고: 인덱싱 수준을 수정하면 전체 BI 플랫폼 리포지토리를 새로 고치기 위해 인덱싱이 초기화됩니다.</p>
콘텐츠 형식	<p>인덱싱을 위해 다음 콘텐츠 형식을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> Microsoft Word Microsoft Excel Microsoft PowerPoint 텍스트 Adobe Acrobat 서식 있는 텍스트 Crystal Reports 유니버스 Web Intelligence
인덱스 재작성	<p>이 옵션을 이용해 인덱싱된 기존 콘텐츠를 모두 삭제하고 처음부터 전체 문서를 다시 인덱싱합니다.</p> <p>인덱싱 상태에 상관없이 인덱스 재작성 옵션을 선택할 수 있습니다. 하지만, 인덱싱이 중지되는 경우 인덱스 재작성 옵션이 작용하지 않으므로 인덱스 재작성을 선택하고 플랫폼 검색 응용 프로그램을 저장하고 닫습니다.</p> <p>인덱싱이 중지되어 인덱스 재작성을 선택하고 플랫폼 검색 응용 프로그램을 저장하고 닫은 다음 구성 페이지를 다시 열고 인덱싱 시작을 클릭하면, 저장된 재작성 인덱스가 전체 문서를 자동으로 다시 인덱싱합니다.</p> <p>플랫폼 검색에서 문서를 다시 인덱싱하지 않으려는 경우에는 인덱스 재작성을 선택 취소한 후 인덱싱 시작 단추를 클릭해야 합니다.</p>

옵션	설명
인덱싱에서 제외된 문서	<p>인덱싱에서 제외된 문서 옵션은 문서를 인덱싱에서 제외합니다. 예를 들어, Report Application Server 리소스가 오버로드되지 않도록 크기가 너무 큰 Crystal 보고서를 검색 대상에 포함되지 않도록 할 수 있습니다. 또는 수백 개의 사용자 설정 보고서가 포함된 게시를 인덱싱에서 제외되도록 할 수 있습니다.</p> <p>특정 문서를 제외하여 이 문서가 플랫폼 검색으로 검색되지 않도록 할 수 있습니다. 단, 문서를 이 그룹에 넣기 전에 문서가 이미 인덱싱된 경우에는 계속 검색이 가능합니다. 인덱싱에서 제외된 문서 그룹의 문서를 검색하지 못하게 하려면 인덱스를 다시 작성해야 합니다.</p> <p>기본적으로 관리자 계정은 인덱싱에서 제외된 문서에 대한 전체 권한을 갖고 있습니다. 다음 권한이 있는 다른 사용자는 인덱싱에서 제외된 문서 그룹에 문서를 추가만 할 수 있습니다.</p> <ul style="list-style-type: none"> • 범주에 대한 권한 보기 및 편집 • 문서 직접 편집

5. 저장 후 닫기를 클릭합니다.

참고:

사용자가 인덱스 재작성 옵션을 선택하지 않고 인덱싱 수준을 변경하거나 추출기를 선택 또는 선택 취소하는 경우에는 기존 인덱스를 삭제하지 않고 처음부터 인덱스가 증분 업데이트됩니다.

13.2 BOE.war 속성을 통한 응용 프로그램 관리

13.2.1 BOE war 파일

BI 플랫폼 웹 응용 프로그램에 대한 설정을 수정하기 위해 BOE.war 파일에 대한 기본 속성을 덮어쓸 수 있습니다. 이 파일은 웹 응용 프로그램 서버를 호스팅하는 컴퓨터에 배포됩니다. 파일 배포 방법에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 웹 응용 프로그램 배포 가이드를 참조하십시오.

BOE.war 파일에 포함된 속성은 기본 로그인 동작, 기본 인증 방법, 단일 로그인 설정을 위한 지정을 관리합니다. 사용자가 지정할 수 있는 속성의 유형은 두 가지입니다.

- 전역 속성 - 전역 속성은 BOE.war 파일에 포함된 모든 웹 응용 프로그램에 영향을 미칩니다.
- 응용 프로그램별 속성 - 특정 웹 응용 프로그램에만 영향을 주는 속성 설정입니다.

기본 속성을 수정하려면 사용자 지정 구성 디렉터리를 사용하여 전역 속성 또는 응용 프로그램별 속성에 대한 새 설정을 저장합니다. 기본적으로, 디렉터리의 위치는 C:\WProgram Files (x86)\WSAP BusinessObjects\WSAP BusinessObjects Enterprise XI 4.0\Wwarfiles\Wwebapps\WBOEWWEB-INF\Wconfig\Wcustom입니다.

config\Wdefault 디렉터리에서 속성을 수정하지 마십시오.

참고:

BI 플랫폼과 함께 제공되는 일부 웹 응용 프로그램 서버(예: Tomcat 버전)에서는 BOE.war에 직접 액세스할 수 있습니다. 이 경우 WAR 파일의 배포를 취소하지 않고 사용자 지정 설정을 직접 설정할 수 있습니다. 배포된 웹 응용 프로그램에 직접 액세스할 수 없을 때는 파일 배포를 취소하고 사용자 지정된 다음 다시 배포해야 합니다. 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 웹 응용 프로그램 배포 가이드를 참조하십시오.

13.2.1.1 전역 BOE.war 속성

다음 표에는 BOE.war용 기본 global.properties 파일에 포함된 설정이 표시됩니다. 설정을 덮어쓰려면 C:\WProgram Files (x86)\WSAP BusinessObjects\WSAP BusinessObjects Enterprise XI 4.0\Wwarfiles\Wwebapps\WBOEWWEB-INF\Wconfig\Wcustom에 새 파일을 만듭니다.

설정	기본값	설명
persistentcookies.enabled	persistentcookies.enabled=true	웹 응용 프로그램 로그인 페이지에서 영구적인 쿠키를 사용하거나 사용하지 않습니다.
siteminder.authentication	siteminder.authentication=secLDAP	SiteMinder에서 사용할 인증 방법을 지정합니다. 옵션은 secLDAP와 secwinAD만 가능합니다.
siteminder.enabled	siteminder.enabled=false	SiteMinder에서 인증을 사용하거나 사용하지 않습니다.
sso.enabled	sso.enabled=false	BI 플랫폼에서 단일 로그인(SSO)을 사용하거나 사용하지 않습니다.

설정	기본값	설명
sso.sap.primary	sso.sap.primary=false	SAP SSO를 응용 프로그램의 기본 단일 로그인 메커니즘으로 사용하려는 경우 true로 설정합니다. SAP 및 SiteMinder SSO를 모두 사용하는 경우에만 적용됩니다.
tree.pagesize	tree.pagesize=100	웹 응용 프로그램 탐색 창에 표시할 수 있는 항목의 최대 개수를 지정합니다.
trusted.auth.shared.secret	없음	신뢰할 수 있는 인증을 위한 암호를 검색하는 데 사용되는 세션 변수 이름을 지정합니다. 웹 세션을 사용하여 공유 암호를 전달하는 경우에만 적용됩니다.
trusted.auth.user.param	없음	신뢰할 수 있는 인증을 위한 사용자 이름을 검색하는 데 사용되는 변수를 지정합니다. 다음 중 하나로 설정 가능합니다. <ul style="list-style-type: none"> • Header • URL Parameter • Cookie • Session
trusted.auth.user.retrieval	없음	신뢰할 수 있는 인증을 위한 사용자 이름을 검색하는 방법을 지정합니다. 다음 중 하나로 설정 가능합니다. <ul style="list-style-type: none"> • "REMOTE_USER" • "HTTP_HEADER" • "COOKIE" • "QUERY_STRING" • "WEB_SESSION" • "USER_PRINCIPAL" 신뢰할 수 있는 인증을 사용하지 않으려면 비어 있음으로 설정합니다.

설정	기본값	설명
trusted.auth.user.namespace.enabled	trusted.auth.user.namespace.enabled=false	기존 사용자 계정에 대한 별칭의 동적 바인딩을 사용하거나 사용하지 않습니다. 속성이 true로 설정된 경우 신뢰할 수 있는 인증은 별칭 바인딩을 사용하여 BI 플랫폼에서 사용자를 인증합니다. 응용 프로그램 서버는 별칭 바인딩을 이용해 SAML 서비스 공급자 역할을 할 수 있으므로, 신뢰할 수 있는 인증을 통해 시스템에 SAML SSO를 제공할 수 있습니다. false로 설정된 경우, 신뢰할 수 있는 인증에서는 일치하는 이름을 사용하여 사용자를 인증합니다.
vintela.enabled	vintela.enabled=false idm.realm=YOUR_REALM idm.princ=YOUR_PRINCIPAL idm.allowUnsecured=true idm.allowNTLM=false idm.logger.name=simple idm.logger.props=error-log.properties	Windows AD 인증을 위한 Vintela 설정을 사용하거나 사용 안 하도록 설정하는데 사용됩니다.
pinger.showWarningDialog.cmc	pinger.showWarningDialog.cmc=true	현재 세션이 CMC에서 곧 만료될 것임을 나타내는 메시지와 함께 경고 대화 상자를 표시할지 여부를 지정합니다.
pinger.showWarningDialog.bilaunchpad	pinger.showWarningDialog.bilaunchpad=true	현재 세션이 BI 실행 패드에서 곧 만료될 것임을 나타내는 메시지와 함께 경고 대화 상자를 표시할지 여부를 지정합니다.
pinger.warningPeriod.pingIncrementsInSeconds	pinger.warningPeriod.pingIncrementsInSeconds=15	세션 만료 경고 메시지가 표시되는 동안 웹 서버 요청을 얼마나 자주 보내야 할지 지정합니다. 이는 응용 프로그램 간 경고 대화 상자의 동기화를 위해 중요한 설정입니다.
pinger.warningPeriod.lengthInMinutes	pinger.warningPeriod.lengthInMinutes=5	세션 만료 이전에 경고를 표시할 기간을 지정합니다.

설정	기본값	설명
logoff.on.websession.expiry	logoff.on.websession.expiry=true	웹 세션이 만료될 때 모든 응용 프로그램 세션이 로그오프되는지 여부를 지정합니다.
pinger.enabled	pinger.enabled=true	세션 만료 경고 메시징 메커니즘을 사용하거나 사용하지 않습니다.
system.com.sap.bip.jcomanager.destinations.maxsize	system.com.sap.bip.jcomanager.destinations.maxsize=1000	캐시된 Java 연결의 최대 개수를 지정합니다.

13.2.1.2 BI 실행 패드 속성

다음 표에는 BOE.war 파일용 기본 bilaunchpad.properties 파일에 포함된 설정이 표시됩니다. 설정을 덮어쓰려면 C:\WProgram Files (x86)\WSAP BusinessObjects\WSAP BusinessObjects Enterprise XI 4.0\Wwarfiles\Wwebapps\WBOE\WEB-INF\Wconfig\Wcustom에 새 파일을 만듭니다.

설정	설명
app.name	응용 프로그램의 표시 이름을 지정합니다. 웹 응용 프로그램 제목 페이지와 로그인 화면에 이름이 나타납니다. 기본값: app.name=BI launch pad
app.name.greeting	기본값: app.name.greeting=BusinessObjects
app.name.short	응용 프로그램의 표시 이름을 지정합니다. 웹 응용 프로그램 제목 페이지와 로그인 화면에 이름이 나타납니다. 기본값: app.name.short=BI launch pad
app.url.name	/ 문자 뒤에 응용 프로그램의 URL 이름을 지정합니다. 기본값: app.url.name=/BI

설정	설명																		
authentication.default	<p>사용자를 응용 프로그램에 인증하는 데 사용되는 기본 인증 방법을 지정합니다. 이 설정에 대해 다음 중 하나를 사용할 수 있습니다.</p> <table> <tr> <th>인증</th><th>설정 값</th></tr> <tr> <td>Enterprise</td><td>secEnterprise</td></tr> <tr> <td>LDAP</td><td>secLDAP</td></tr> <tr> <td>Windows AD</td><td>secWinAD</td></tr> <tr> <td>SAP</td><td>secSAPR3</td></tr> <tr> <td>PeopleSoft</td><td>secpseenterprise</td></tr> <tr> <td>JD Edwards</td><td>secPSE1</td></tr> <tr> <td>Siebel</td><td>secSiebel7</td></tr> <tr> <td>Oracles EBS</td><td>secOraApps</td></tr> </table> <p>기본값: authentication.default=secEnterprise</p>	인증	설정 값	Enterprise	secEnterprise	LDAP	secLDAP	Windows AD	secWinAD	SAP	secSAPR3	PeopleSoft	secpseenterprise	JD Edwards	secPSE1	Siebel	secSiebel7	Oracles EBS	secOraApps
인증	설정 값																		
Enterprise	secEnterprise																		
LDAP	secLDAP																		
Windows AD	secWinAD																		
SAP	secSAPR3																		
PeopleSoft	secpseenterprise																		
JD Edwards	secPSE1																		
Siebel	secSiebel7																		
Oracles EBS	secOraApps																		
authentication.visible	BI 실행 패드에 로그인하는 사용자에게 인증 방법을 보고 변경할 수 있는 옵션을 부여할지 여부를 지정합니다. 기본값: authentication.visible=false																		
cms.default	기본 CMS 이름을 지정합니다. 기본값: cms.default=[name of host machine]																		
cms.visible	BI 실행 패드에 로그인하는 사용자에게 CMS 이름을 보고 변경할 수 있는 옵션을 부여할지 여부를 지정합니다. 기본값: cms.visible=true																		
dialogue.prompt.enabled	대화 상자의 입력 페이지에서 다른 위치를 탐색할 때 사용자에게 메시지를 표시해야 할지 여부를 지정합니다. 기본값: dialogue.prompt.enabled=false																		
logontoken.enabled	사용자가 BI 실행 패드에 로그인한 후 해당 세션용 토큰 만들기를 사용할지 여부를 지정합니다. 토큰은 쿠키에 저장됩니다. 기본값: logontoken.enabled=false																		
SMTPFrom	개체를 대상에 예약할 때 보낸 사람 필드를 사용하거나 사용하지 않습니다. 기본값: SMTPFrom=true																		

설정	설명
url.exit	BI 실행 패드 세션을 종료한 후 사용자를 리디렉션할 URL을 지정합니다. 외부 확인 프로세스를 통해 응용 프로그램에 로그인한 사용자에게만 이 설정이 적용됩니다.
disable.locale.preference	사용자가 BI 실행 패드에 대한 로컬 기본 설정을 보고 수정할 수 있거나 없도록 설정합니다. 기본값: disable.locale.preference=false
extlogon.allow.logoff	BI 실행 패드 세션을 닫은 후 사용자 세션에서 자동으로 로그오프할 수 있거나 없도록 설정합니다. 사용자가 BI 실행 패드에서 로그오프할 때 사용자 세션이 자동으로 종료되지 않도록 하려면 False로 설정합니다. 기본값: extlogon.allow.logoff=true

13.2.1.3 OpenDocument 속성

다음 표에는 BOE.war 파일용 기본 opendocument.properties 파일에 포함된 설정이 표시됩니다. 설정을 덮어쓰려면 C:\WProgram Files (x86)\WSAP BusinessObjects\WSAP BusinessObjects Enterprise XI 4.0\Wwarfiles\Wwebapps\WBOE\WEB-INF\Wconfig\Wcustom에 새 파일을 만듭니다.

설정	설명																		
app.name	응용 프로그램의 표시 이름을 지정합니다. 웹 응용 프로그램 제목 페이지와 로그인 화면에 이름이 나타납니다. 기본값: app.name=SAP BusinessObjects OpenDocument																		
app.name.short	응용 프로그램의 표시 이름을 지정합니다. 웹 응용 프로그램 제목 페이지와 로그인 화면에 이름이 나타납니다. 기본값: app.name.short=OpenDocument																		
authentication.default	<p>사용자를 응용 프로그램에 인증하는 데 사용되는 기본 인증 방법을 지정합니다. 이 설정에 대해 다음 중 하나를 사용할 수 있습니다.</p> <table border="1"> <thead> <tr> <th>인증</th><th>설정 값</th></tr> </thead> <tbody> <tr> <td>Enterprise</td><td>secEnterprise</td></tr> <tr> <td>LDAP</td><td>secLDAP</td></tr> <tr> <td>Windows AD</td><td>secWinAD</td></tr> <tr> <td>SAP</td><td>secSAPR3</td></tr> <tr> <td>PeopleSoft</td><td>secpcenterprise</td></tr> <tr> <td>JD Edwards</td><td>secPSE1</td></tr> <tr> <td>Siebel</td><td>secSiebel7</td></tr> <tr> <td>Oracles EBS</td><td>secOraApps</td></tr> </tbody> </table> <p>기본값: authentication.default=secEnterprise</p>	인증	설정 값	Enterprise	secEnterprise	LDAP	secLDAP	Windows AD	secWinAD	SAP	secSAPR3	PeopleSoft	secpcenterprise	JD Edwards	secPSE1	Siebel	secSiebel7	Oracles EBS	secOraApps
인증	설정 값																		
Enterprise	secEnterprise																		
LDAP	secLDAP																		
Windows AD	secWinAD																		
SAP	secSAPR3																		
PeopleSoft	secpcenterprise																		
JD Edwards	secPSE1																		
Siebel	secSiebel7																		
Oracles EBS	secOraApps																		
authentication.visible	OpenDocument에 로그인하는 사용자에게 인증 방법을 보고 변경할 수 있는 옵션을 부여할지 여부를 지정합니다. 기본값: authentication.visible=false																		
cms.default	기본 CMS 이름을 지정합니다. 기본값: cms.default=[name of host machine]																		
cms.visible	OpenDocument에 로그인하는 사용자에게 CMS 이름을 보고 변경할 수 있는 옵션을 부여할지 여부를 지정합니다. 기본값: cms.visible=true																		
logontoken.enabled	사용자가 OpenDocument에 로그인한 후 해당 세션용 토큰 만들기를 사용할지 여부를 지정합니다. 토큰은 쿠키에 저장됩니다. 기본값: logontoken.enabled=false																		
extlogon.allow.logoff	OpenDocument 세션을 닫은 후 사용자 세션에서 자동으로 로그오프할 수 있거나 없도록 설정합니다. 사용자가 OpenDocument에서 로그오프할 때 사용자 세션이 자동으로 종료되지 않도록 하려면 False로 설정합니다. 기본값: extlogon.allow.logoff=true																		

13.2.1.4 CMC 속성

다음 표에는 BOE.war용 기본 cmc.properties 파일에 포함된 설정이 표시됩니다. 설정을 덮어쓰려면 C:\WProgram Files (x86)\WSAP BusinessObjects\WSAP BusinessObjects Enterprise XI 4.0\Wwarfiles\Wwebapps\WBOE\WEB-INF\Wconfig\Wcustom에 새 파일을 만듭니다.

설정	설명																		
app.url.name	"/" 문자 뒤에 응용 프로그램의 URL 이름을 지정합니다. 기본값: app.url.name=/CMC																		
authentication.default	<p>사용자를 응용 프로그램에 인증하는 데 사용되는 기본 인증 방법을 지정합니다. 이 설정에 대해 다음 중 하나를 사용할 수 있습니다.</p> <table> <tr> <th>인증</th><th>설정 값</th></tr> <tr> <td>Enterprise</td><td>secEnterprise</td></tr> <tr> <td>LDAP</td><td>secLDAP</td></tr> <tr> <td>Windows AD</td><td>secWinAD</td></tr> <tr> <td>SAP</td><td>secSAPR3</td></tr> <tr> <td>PeopleSoft</td><td>secpsenterprise</td></tr> <tr> <td>JD Edwards</td><td>secPSE1</td></tr> <tr> <td>Siebel</td><td>secSiebel7</td></tr> <tr> <td>Oracles EBS</td><td>secOraApps</td></tr> </table> <p>기본값: authentication.default=secEnterprise</p>	인증	설정 값	Enterprise	secEnterprise	LDAP	secLDAP	Windows AD	secWinAD	SAP	secSAPR3	PeopleSoft	secpsenterprise	JD Edwards	secPSE1	Siebel	secSiebel7	Oracles EBS	secOraApps
인증	설정 값																		
Enterprise	secEnterprise																		
LDAP	secLDAP																		
Windows AD	secWinAD																		
SAP	secSAPR3																		
PeopleSoft	secpsenterprise																		
JD Edwards	secPSE1																		
Siebel	secSiebel7																		
Oracles EBS	secOraApps																		
authentication.visible	CMC에 로그인하는 사용자에게 인증 방법을 보고 변경할 수 있는 옵션을 부여할지 여부를 지정합니다. 기본값: authentication.visible=false																		
cms.default	기본 CMS 이름을 지정합니다. 기본값: cms.default=[name of host machine]																		

설정	설명
cms.visible	CMC에 로그인하는 사용자가 CMS 이름을 보고 변경할 수 있는 옵션이 있는지 여부를 지정합니다. 기본값: cms.visible=true
dialogue.prompt.enabled	대화 상자의 입력 페이지에서 다른 위치를 탐색할 때 사용자에게 메시지를 표시해야 할지 여부를 지정합니다. 기본값: dialogue.prompt.enabled=false
logontoken.enabled	사용자가 CMC에 로그인한 후 해당 세션용 토큰 만들기를 사용할지 여부를 지정합니다. 토큰은 쿠키에 저장됩니다. 기본값: logontoken.enabled=false

13.3 BI 실행 패드 및 OpenDocument 로그인 진입점 사용자 지정

BI 실행 패드 및 OpenDocument 웹 응용 프로그램용 로그인 페이지를 사용자 지정할 수 있습니다. 예를 들어, 회사 로고 또는 회사 스타일 시트를 사용하도록 로그인 페이지를 사용자 지정하거나, 신뢰할 수 있는 인증을 사용하는 사용자 지정 로그인 페이지를 만들 수 있습니다.

로그인 페이지를 사용자 지정하려면 BOE.war 웹 응용 프로그램의 BI 실행 패드 및 OpenDocument 웹 응용 프로그램 영역에 저장된 custom.jsp 파일을 수정한 다음, BI 플랫폼 시스템에 BOE.war 웹 응용 프로그램을 다시 배포합니다. 사용자는 고유의 URL을 탐색하여 사용자 지정 로그인 진입점에 액세스합니다.

이런 예제를 실습하려면 BI 플랫폼 웹 응용 프로그램 배포 방법에 익숙해야 합니다. 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 웹 응용 프로그램 배포 가이드를 참조하십시오.

13.3.1 BI 실행 패드 및 OpenDocument 파일 위치

BI 실행 패드 및 OpenDocument 웹 응용 프로그램은 BOE.war 웹 보관 파일 내에 패키징됩니다. BOE.war 보관 파일의 위치는 BOE.properties 파일에 정의됩니다.

Windows 시스템에서는 다음 위치에서 BOE.properties 파일을 찾을 수 있습니다.

- <BOE_INSTALL_DIR>\WSAP BusinessObjects Enterprise XI 4.0\wdeploy\conf\apps\BOE.properties

UNIX 시스템에서는 다음 위치에서 BOE.properties 파일을 찾을 수 있습니다.

- <BOE_INSTALL_DIR>/sap_bobj/enterprise_xi40/wdeploy/conf/apps/BOE.properties

아래의 표는 BI 실행 패드 및 OpenDocument 응용 프로그램 모두의 BOE.war 웹 보관 파일 내에 있는 공통 파일의 위치를 정의한 것입니다.

테이블13-2: BI 실행 패드 파일 위치

참고:

BI 실행 패드 웹 응용 프로그램은 InfoView의 새로운 이름입니다.

파일 형식	위치
사용자 지정 로그인 스크립트	WEB-INFWeclipseWpluginsWwebpath.InfoViewWwebWcustom.jsp
추가 파일용 디렉터리	WEB-INFWeclipseWpluginsWwebpath.InfoViewWwebWnoCacheCustomResources
사용자 지정 로그인 URL	http://<servername>:<port>/BOE/BI/custom.jsp

테이블13-3: OpenDocument 파일 위치

파일 형식	위치
사용자 지정 로그인 스크립트	WEB-INFWeclipseWpluginsWwebpath.OpenDocumentWwebWopendocWcustom.jsp
추가 파일용 디렉터리	WEB-INFWeclipseWpluginsWwebpath.OpenDocumentWwebWnoCacheCustomResources
사용자 지정 로그인 URL	http://<servername>:<port>/BOE/OpenDocument/opendoc/custom.jsp

13.3.2 사용자 지정 로그인 페이지 정의

BI 플랫폼 로그인 페이지에 대한 진입점을 사용자 지정할 수 있습니다. 예를 들어, 회사 로고를 표시하고 회사 스타일 시트를 사용하는 사용자 지정 로그인 페이지를 만들 수 있습니다.

custom.jsp 파일을 편집하여 사용자의 로그인 환경을 사용자 지정하고 noCacheCustomResources 폴더에 지원 파일을 넣습니다.

이 예에서는 사용자를 기본 로그인 페이지로 리디렉션하는 사용자 지정 로그인 페이지를 만드는 방법을 보여줍니다.

1. 사용자 지정 로그인 코드를 포함한 파일을 만들고 이 파일을 noCacheCustomResources 폴더에 custom.js로 저장합니다.

이 예에서는 사용자를 기본 로그인 페이지인 logon.jsp로 리디렉션하는 함수를 정의합니다.

```
function load() {window.location = "logon.jsp";}
```

2. custom.jsp 파일을 편집하여 로그인 페이지를 사용자 지정합니다.

이 예에서는 시작 메시지와 custom.js 파일에 정의된 load 메서드를 호출하는 하이퍼링크를 표시합니다.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">

<%@ page language="java" contentType="text/html; charset=utf-8"%>
<html>
<head> <title>Welcome</title>
</head>
<body>
<script type="text/javascript" src="noCacheCustomResources/custom.js"></script>
<p>Welcome to ABC corporation.</p>
<a href="javascript:load()">Enter</a>
</body>
</html>
```

3. BOE.war 웹 응용 프로그램을 다시 배포하고 웹 서버를 다시 시작합니다.

13.3.3 로그인 시 신뢰할 수 있는 인증 추가

신뢰할 수 있는 인증을 사용하려면 custom.jsp 파일에서 신뢰할 수 있는 사용자를 세션 특성으로 설정하고 global.properties 파일의 복사본에서 인증 설정을 수정합니다. global.properties 파일의 사용자 지정 복사본 값은 기본값을 덮어씁니다.

1. custom.jsp 파일을 편집하여 신뢰할 수 있는 사용자를 정의하는 세션 특성을 설정합니다.

```
request.getSession().setAttribute("TrustedUserAttribute", "TrustedUser");
```

2. WEB-INFWconfigWdefaultWglobal.properties를 WEB-INFWconfigWcustomWglobal.properties로 복사하여 global.properties 파일의 사용자 지정 복사본을 만듭니다.
3. 단일 로그인(SSO)을 사용하도록 WEB-INFWconfigWcustomWglobal.properties를 수정합니다.

```
sso.enabled=true
```

4. 신뢰할 수 있는 사용자 세션 변수를 포함한 신뢰할 수 있는 인증 매개 변수와 공유 암호를 설정하도록 WEB-INFWconfigWcustomWglobal.properties를 수정합니다.

"..."를 시스템의 공유 암호로 바꿉니다.

```
trusted.auth.user.param=TrustedUserAttribute
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.shared.secret="..."
```

5. 웹 응용 프로그램을 다시 배포하고 웹 서버를 다시 시작합니다.

관련 항목

- 219 페이지에서 [신뢰할 수 있는 인증 활성화](#)

13.4 BEx 웹 통합 구성

BEx 웹 응용 프로그램은 SAP NetWeaver Business Warehouse(BW)의 Business Explorer(BEx)에서 제공하는 웹 기반 응용 프로그램으로, 웹에서 데이터 분석, 보고 및 분석 응용 프로그램에 사용됩니다.

Business Explorer는 SAP NetWeaver Business Intelligence 제품군에 속하며, 전략적 분석 및 의사 결정 지원을 위해 유연한 보고 및 분석 도구를 제공합니다. 이러한 도구에는 쿼리, 보고 및 분석 기능이 있습니다. 액세스 권한이 있는 직원이라면 웹 및 Microsoft Excel을 통해 다양한 상세 수준에서 그리고 여러 관점에서 과거 또는 현재 데이터를 평가할 수 있습니다.

사용자는 SAP NetWeaver Portal 또는 BI 실행 패드를 통해 데이터에 액세스합니다. BEx 웹 응용 프로그램의 작성자는 BEx Web Application Designer의 BI 실행 패드에서 직접 웹 응용 프로그램을 실행할 수 있습니다.

BI 플랫폼에서 BEx 웹 응용 프로그램을 통합하려면 다음 구성 단계를 수행하십시오.

1. 중앙 관리 콘솔(CMC)에서 BEx 웹 응용 프로그램용 서버를 설정합니다.
BEx 웹 응용 프로그램에 대해 일반 또는 표준 서버를 사용할 수 있습니다.

팁:

다른 여러 서비스에서 보통 일반 서버를 사용하므로 BEx 웹 응용 프로그램에 대해 독립 실행형 서버를 설정하는 것이 좋습니다.

2. 서버 설정을 구성합니다.
3. BW 시스템에 대한 연결을 확인합니다.
4. 작성자가 BEx Web Application Designer의 BI 실행 패드에서 직접 BEx 웹 응용 프로그램을 실행하도록 하려면 BW 시스템의 연결된 포털 테이블(RSPOR_T_PORTAL)에 관련 설정을 해야 합니다.

BI 플랫폼 서버를 구성한 후에는 BI 실행 패드에서 BEx 웹 응용 프로그램을 열 수 있습니다. 또한 여기에 있는 데이터를 탐색하고 BEx 웹 응용 프로그램을 웹 브라우저의 즐겨찾기에 책갈피로 저장할 수 있습니다.

제한:

이 통합의 경우 SAP NetWeaver Java 스택이 필요하지 않으므로 다음과 같은 제한 사항이 적용됩니다.

- 정보 브로드캐스팅이 지원되지 않습니다.
- 포털 및 SAP NetWeaver의 Knowledge Management가 필요하지 않으므로, BEx 웹 응용 프로그램에서 문서 통합 및 포털 모티브 사용이 지원되지 않습니다.
- 보고서 웹 항목은 지원되지 않습니다. 서식이 지정된 보고서 작성을 위해서는 SAP Crystal Reports를 사용할 것을 권장합니다.
- BEx 웹 응용 프로그램의 인쇄 버전을 만들기 위해 SAP Business Explorer용 익스포트 라이브러리가 사용됩니다. Adobe Document Services(ADS)는 사용할 수 없습니다.
- BI 플랫폼에 통합된 BEx 웹 응용 프로그램에는 BW 마스터 시스템에 저장된 데이터 소스만 포함될 수 있습니다. 시스템 관리에서 BusinessObjects Business Intelligence 플랫폼에서 BW 마스터 시스템으로 구성할 시스템을 정의하십시오.
- BI 플랫폼과 SAP NetWeaver BW 시스템 간 단일 로그인은 사용할 수 없습니다. 각 BI 플랫폼 세션마다 BEx 웹 응용 프로그램 사용자가 해당 BW 마스터 시스템에 로그인해야 합니다.
- BEx 웹 응용 프로그램에 대한 보고서-보고서 인터페이스가 지원되지 않습니다. 해당 명령이 실행되지 않습니다.

BEx 웹 응용 프로그램의 기능에 대한 자세한 내용은 SAP Help Portal(<http://help.sap.com>)에서 SAP NetWeaver 7.0 (2004s) > SAP NetWeaver Library > SAP NetWeaver By Key Capability > Information Integration by Key Capability > Business Intelligence > BI Suite: Business Explorer > BEx Web > Analysis & Reporting: BEx Web Applications를 참조하십시오.

BI 실행 패드에서 BEx 웹 응용 프로그램을 액세스 및 저장하는 방법에 대한 자세한 내용은 <http://help.sap.com>의 BI 실행 패드 사용자 가이드를 참조하십시오.

관련 항목

- 527 페이지에서 [BEx 웹 응용 프로그램용 서버 시작](#) "
- 528 페이지에서 [BEx 웹 응용 프로그램에 대해 표준 서버 시작](#) "
- 528 페이지에서 [서버 설정 구성](#) "
- 529 페이지에서 [BW 시스템에 대한 연결 확인](#) "
- 529 페이지에서 [BEx Web Application Designer 및 BI 플랫폼 간 연결 구성](#) "

13.4.1 BEx 웹 응용 프로그램용 서버 시작

1. 중앙 관리 콘솔(CMC)에 로그인합니다.
2. 서버를 선택합니다.
3. 서비스 범주 노드를 확장하고 Analysis Services를 선택합니다.
4. 적응형 처리 서버를 선택한 다음 상황에 맞는 메뉴에서 서비스 선택을 선택합니다.
5. 사용 가능한 서비스 목록에서 BExWebApplicationsService를 선택한 다음 AdaptiveProcessingServerServices 목록으로 이동합니다.

6. 상황에 맞는 메뉴를 사용하여 BEx 웹 응용 프로그램 서비스를 활성화하고 시작합니다.

13.4.2 BEx 웹 응용 프로그램에 대해 표준 서버 시작

1. 중앙 관리 콘솔(CMC)에 로그인합니다.
2. 서버를 선택합니다.
3. 서비스 범주 노드를 확장하고 Analysis Services를 선택합니다.
4. 적응형 처리 서버를 선택한 다음 상황에 맞는 메뉴에서 복제 서버를 선택합니다.
5. 서버 이름(예: AdaptiveProcessingServer)을 입력한 다음 노드에 복제 상자에서 필요한 서버를 선택합니다.
6. 복제된 서버를 선택한 다음 상황에 맞는 메뉴에서 서비스 선택을 선택합니다.
7. 사용 가능한 서비스 목록에서 BExWebApplicationsService를 선택한 다음 AdaptiveProcessingServerServices 목록으로 이동합니다.
8. 상황에 맞는 메뉴를 사용하여 BEx 웹 응용 프로그램 서비스를 활성화하고 시작합니다.

13.4.3 서버 설정 구성

1. 중앙 관리 콘솔(CMC)에 로그인합니다.
2. 서버를 선택합니다.
3. 서비스 범주 노드를 확장하고 Analysis Services를 선택합니다.
4. BEx 웹 응용 프로그램 서비스를 선택하고 상황에 맞는 메뉴에서 등록정보를 선택합니다.
5. BEx 웹 응용 프로그램 서비스 영역의 BEx 웹 응용 프로그램 서비스 구성에서 다음과 같이 설정합니다.
 - a. 클라이언트 세션의 최대 개수를 선택하고 필요 시 변경합니다.
 - b. SAP BW 마스터 시스템에 BI 플랫폼에서 생성한 BW 시스템의 OLAP 연결 이름을 입력합니다. 기본 이름은 SAP_BW입니다.
 - c. RFC 연결 구성(트랜잭션 코드 sm59)에 BW 시스템에 입력한 JCo 서버 RFC 대상의 이름을 입력합니다.
 - d. RFC 연결 구성(트랜잭션 코드 sm59)에 BW 시스템에 정의한 JCo 서버 게이트웨이 호스트의 이름을 입력합니다.
 - e. RFC 연결 구성(트랜잭션 코드 sm59)에 BW 시스템에 정의한 JCo 서버 게이트웨이 서비스의 이름을 입력합니다.
 - f. JCo 서버 연결 개수를 선택하고 필요 시 변경합니다.

6. 저장 후 닫기를 선택합니다.
7. BEx 웹 응용 프로그램 서비스를 선택하고 상황에 맞는 메뉴에서 서버 다시 시작을 선택합니다.
선택한 설정을 적용하려면 서버를 다시 시작해야 합니다.

참고:

서버를 다시 시작하기 전에 ABAP 시스템에 RFC 대상이 생성되어 있어야 합니다.

관련 항목

- 530 페이지에서 [ABAP 시스템에 RFC 대상 생성](#)"

13.4.4 BW 시스템에 대한 연결 확인

1. 중앙 관리 콘솔(CMC)에 로그인합니다.
2. OLAP 연결을 선택합니다.
3. BW 시스템에 연결이 설정되었는지 확인합니다. 설정되지 않은 경우 설정합니다. 연결의 기본 이름은 SAP_BW입니다. 다른 이름을 입력할 수도 있습니다.
4. 인증에서 미리 정의됨을 선택하고 사용자 및 암호에 필요한 값을 입력하십시오.

참고:

이 사용자 계정은 BEx Web Application Designer, BW 시스템 및 BI 플랫폼을 통합하는 데 사용할 수 있는 JCo 서버 RFC 대상에 필요합니다.

팁:

연결의 보안을 유지하기 위해 관리자만 액세스 권한을 갖도록 합니다.

- a. 이와 같이 설정하려면 위해 BW 시스템에 연결(기본 이름 SAP_BW)을 마우스 오른쪽 단추로 클릭한 다음 사용자 보안을 선택합니다.
- b. 필요한 보안을 설정하고 가능하면 관리자에게만 액세스 권한을 부여합니다.

13.4.5 BEx Web Application Designer 및 BI 플랫폼 간 연결 구성

작성자가 BEx Web Application Designer의 BI 실행 패드에서 직접 BEx 웹 응용 프로그램을 실행하도록 하려면 BW 시스템의 연결된 포털 테이블(RSPOR_T_PORTAL)에서 관련 설정을 해야 합니다.

1. BW 시스템에서 트랜잭션 SM30(테이블 뷰 유지보수)을 호출합니다.
2. 테이블/뷰 아래에서 RSPOR_T_PORTAL을 입력합니다.

3. 유지보수를 선택합니다.
4. 새 항목을 만들려면 신규 엔트리를 선택합니다.
5. 다음을 설정합니다.
 - a. BW 시스템 및 BI 플랫폼을 통합하려면 SM59 트랜잭션을 통해 RFC 대상을 만들어야 합니다. 대상 아래에 이 RFC 대상을 입력합니다.
 - b. 표준 포털을 선택합니다. 이렇게 하면 웹 응용 프로그램 디자이너의 웹 응용 프로그램이 항상 BI 플랫폼에서 호출됩니다.
 - c. URL 접두부에 프로토콜, 호스트 이름 및 포트를 포함하여 BI 플랫폼 웹 응용 프로그램 컨테이너 서버(WACS)의 URL을 입력합니다(예: http://<wacs><도메인>:<포트>).
 - d. 플랫폼에서 BOE를 선택합니다.
 - e. SAP 비즈니스 탐색기의 익스포트 라이브러리를 활성화하여 PDF, PostScript 및 PCL 파일을 BEx 웹 응용 프로그램에서 내보낼 수 있도록 하려면 SAP 익스포트 라이브러리(PDF) 사용을 선택합니다.
6. 항목을 저장합니다.

관련 항목

- 530 페이지에서 [ABAP 시스템에 RFC 대상 생성](#)

13.4.5.1 ABAP 시스템에 RFC 대상 생성

BW 시스템과 BI 플랫폼을 통합하려면 RFC 대상이 필요합니다. 이 RFC 대상을 통해 BW 시스템과 BI 플랫폼이 서로 통신할 수 있습니다.

1. RFC 연결 구성(트랜잭션 코드 SM59)을 호출합니다.
2. 만들기를 선택합니다.
3. 다음과 같이 RFC 대상을 설정합니다.
 - a. RFC 대상의 이름을 입력합니다.
 - b. 연결 유형으로 TCP/IP 연결용 T를 선택합니다.
 - c. 설명을 입력합니다.
RFC 대상의 설명은 각 언어 별로 입력할 수 있습니다.
 - d. 기술 설정 아래에서 활성화 유형으로 등록된 서버 프로그램을 선택합니다.
 - e. 기술 설정 아래에 프로그램 ID를 입력합니다.
프로그램 ID는 BI 플랫폼 서버에서 BW 시스템의 대상을 만들 때 지정한 프로그램 ID(JCo Server RFC 대상)와 동일해야 합니다.
 - f. 게이트웨이 옵션 아래의 기술 설정에서 BI 플랫폼이 BW 시스템과 통신할 때 사용하는 게이트웨이 호스트 및 게이트웨이 서비스를 입력합니다.
4. 로그인 및 보안 탭 페이지에서 SAP 로그인 티켓 발신 옵션을 활성화합니다.
5. 항목을 저장합니다.

관련 항목

- 528 페이지에서 [서버 설정 구성](#)"

장14 연결 및 유니버스 관리

14.1 연결 관리

연결은 하나 이상의 SAP BusinessObjects 응용 프로그램이 어떤 방식으로 관계형 또는 OLAP 데이터베이스에 액세스할 수 있는지 정의하는 명명된 매개 변수 집합입니다. 서버 이름, 데이터베이스, 사용자 이름 및 암호와 같은 연결 세부 정보는 Connections 폴더의 BI 플랫폼 리포지토리에 안전하게 저장할 수 있습니다.

디자이너들은 연결을 바탕으로 유니버스를 정의합니다. 쿼리, 분석 및 보고 응용 프로그램 사용자는 데이터베이스의 기본 데이터 구조에 대한 지식 없이도 유니버스를 통해 데이터베이스에 액세스할 수 있습니다.

사용자는 다음 응용 프로그램을 사용하여 연결을 만들 수 있습니다.

- 유니버스 디자인 도구. 연결은 리포지토리에 저장됩니다.
- 정보 디자인 도구. 로컬에서 연결을 만든 다음 리포지토리에 게시하거나, 리포지토리에서 직접 연결을 만들고 편집할 수 있습니다.

참고:

OLAP 데이터 소스 연결 관리 방법에 대한 자세한 내용은 SAP BusinessObjects Analysis, OLAP용 에디션 관리자 가이드를 참조하십시오.

사용자가 연결을 만들고 편집하고 삭제할 수 있는 권한을 부여합니다.

유니버스 연결에 대한 사용자 액세스를 허용하고, 유니버스 및 연결을 사용하는 문서를 사용자가 만들거나 보도록 허용합니다.

관련 항목

- 123 페이지에서 [CMC에서 개체의 보안 설정 관리](#)"
- 808 페이지에서 [연결 권한](#)"

14.1.1 유니버스 연결 삭제

팁:

유니버스 디자인 도구와 정보 디자인 도구에서 연결을 삭제하는 것도 가능합니다.

1. 연결 영역에 있는 목록에서 유니버스 연결을 선택합니다.
2. 관리 > 삭제를 클릭합니다.

14.2 유니버스 관리

유니버스는 비즈니스 사용자가 쉬운 언어로 회사 데이터를 분석하고 보고할 수 있도록 구성된 메타데이터 개체 컬렉션입니다. 이러한 개체로는 차원, 계수, 계층 구조, 특성, 미리 정의된 계산, 함수, 쿼리 등이 있습니다. 메타데이터 개체 계층은 관계형 데이터베이스 스키마 또는 OLAP 큐브에 작성되므로 개체가 데이터베이스 구조에 직접 매핑됩니다. 유니버스에는 데이터 소스에 대한 연결이 포함되므로 쿼리 및 분석 도구 사용자는 데이터베이스의 기본 데이터 구조에 대해 알 필요 없이 유니버스에 연결하여 쿼리를 실행하고 유니버스의 개체를 사용하여 보고서를 만들 수 있습니다.

다음 도구로 유니버스를 만들 수 있습니다.

- 유니버스 디자인 도구. 이 도구로 만든 유니버스는 .unv 확장자로 구별할 수 있으므로 .unv 유니버스라고 합니다. .unv 유니버스는 보안 연결에서 정의되고 리포지토리 Universes 폴더에 저장됩니다.
- 정보 디자인 도구. 이 도구로 만든 유니버스는 새 의미 계층을 바탕으로 합니다. 이런 유니버스는 .unx 확장자로 구별되므로 .unx 유니버스라고 합니다. .unx 유니버스는 로컬에서 작성되어 리포지토리 Universes 폴더에 게시됩니다. 디자이너는 정보 디자인 도구 보안 편집기를 사용하여 개체 수준 보안을 정의할 수 있습니다.

사용자가 유니버스에서 보안을 디자인할 뿐 아니라, 유니버스를 만들고 편집하고 삭제할 수 있도록 해주는 응용 프로그램 권한과 유니버스 권한을 부여합니다.

사용자가 유니버스를 사용하는 문서를 만들고 볼 수 있도록 유니버스 권한을 부여합니다.

관련 항목

- 123 페이지에서 [CMC에서 개체의 보안 설정 관리](#)"
- 815 페이지에서 [유니버스 디자인 도구 권한](#)"
- 804 페이지에서 [유니버스\(.unv\) 권한](#)"
- 815 페이지에서 [정보 디자인 도구 권한](#)"
- 805 페이지에서 [유니버스\(.unx\) 권한](#)"

14.2.1 유니버스 삭제

팁:

정보 디자인 도구에서 유니버스를 삭제하는 것도 가능합니다.

1. CMC의 유니버스 영역에 있는 목록에서 유니버스를 선택합니다.
2. 관리 > 삭제를 클릭합니다.
3. 확인 메시지가 나타나면 확인을 클릭합니다.

장15 모니터링

15.1 모니터링 정보

모니터링은 SAP BusinessObjects Business Intelligence 플랫폼 4.0의 새 응용 프로그램이며, 보고 및 알림을 위해 SAP BusinessObjects Business Intelligence 플랫폼 4.0 서버의 런타임 및 기록 메트릭을 캡처할 수 있는 기능을 제공합니다. 따라서 시스템 관리자가 응용 프로그램이 정상적으로 작동하는지 여부와 응답 시간이 예상대로 작동하는지 여부를 식별할 수 있습니다. 모니터링 응용 프로그램에서 제공하는 주요 비즈니스 메트릭을 통해 SAP BusinessObjects Business Intelligence 플랫폼 4.0의 상태를 보다 잘 파악할 수 있습니다.

모니터링의 기능은 다음과 같습니다.

- 각 서버의 성능 확인: 이 기능은 각 서버의 상태를 신호등으로 나타내는 감시를 통해 가능합니다. 시스템 관리자는 이러한 감시에 대한 임계값을 설정하고 해당 임계값이 위반될 때 경고를 받을 수 있습니다. 이는 실패 또는 중지가 예상되는 경우 사전 예방 조치를 취하는 데 유용합니다.
- 중요한 시스템 핵심 성과 지표(KPI) 보기: 작업 및 리소스 모니터링에 유용합니다. 이러한 KPI는 모니터링 응용 프로그램의 대시보드 페이지에 표시됩니다.
- 시스템 가용성 및 응답 시간 확인: 프로브를 통해 워크플로우를 시뮬레이션하여 배포된 Enterprise 서버 및 서비스가 예상대로 작동하는지 확인할 수 있습니다. 시스템 관리자는 주기적인 간격으로 이러한 프로브의 왕복 시간을 분석하여 시스템 사용 패턴을 평가할 수 있습니다.
- CMS에 대한 최고 부하 및 최고 사용 기간 분석: 시스템 관리자가 라이선스 또는 시스템 리소스를 추가로 확보해야 할지 여부를 결정하는 데 유용합니다.
- 다른 엔터프라이즈 응용 프로그램과 통합: SAP BusinessObjects Business Intelligence 플랫폼 4.0 모니터링 응용 프로그램을 다른 엔터프라이즈 응용 프로그램(예: SAP Solution Manager 및 IBM Tivoli Monitoring)과 통합할 수 있습니다.

15.2 모니터링 용어

다음은 모니터링 응용 프로그램과 관련된 용어입니다.

대시보드

대시보드 페이지에는 시스템 관리자가 모든 서버의 성능을 모니터링하는 데 사용할 수 있는 중앙화된 뷰가 제공됩니다. 또한 시스템 KPI에 대한 실시간 정보, 최근 경고, 감시 및 감시 상태 기반 그래프가 제공됩니다.

감시

감시는 SAP BusinessObjects Business Intelligence 플랫폼 환경 내 서버 및 워크플로의 실시간 상태 및 기록 추세를 제공합니다. 사용자는 임계값 및 경고를 감시에 연결할 수 있습니다. 프로브, 서버, SAPOSCOL 또는 파생 메트릭의 데이터를 사용하여 감시를 만들 수 있습니다.

파생 메트릭

파생 메트릭을 사용하면 사용자의 요구 사항을 바탕으로 메트릭을 만든 다음 이 메트릭을 사용하여 감시를 만들 수 있는 유연성이 있습니다. 둘 이상의 기존 메트릭을 한 수학적식에 조합하여 파생 메트릭을 만들 수 있습니다.

KPI

핵심 성과 지표(KPI)는 SAP BusinessObjects Business Intelligence 플랫폼 배포의 표준 메트릭입니다. 일정 및 로그인 세션에 대한 정보를 제공합니다. 예를 들어 실행 작업의 수가 많을수록 서버 성능이 좋다는 것을 나타내고, 보류 작업의 수가 많을수록 성능이 저조하고 시스템 부하가 높다는 것을 나타냅니다.

프로브

프로브는 여러 서비스를 모니터링하고 SAP BusinessObjects Business Intelligence 플랫폼 구성 요소의 다양한 기능을 시뮬레이션합니다. 시스템 관리자는 지정한 간격에 실행되도록 프로브를 예약하여 SAP BusinessObjects Business Intelligence 플랫폼 4.0에서 제공하는 주요 서비스의 가용성과 성능을 추적할 수 있습니다. 이 데이터는 용량 계획에도 사용될 수 있습니다.

신호등

신호등은 지정한 시간에 감시 상태를 나타냅니다. 감시 상태를 나타내는 데는 녹색, 황색 및 빨간색이 사용됩니다. 하나의 감시에 두 개 또는 세 개의 상태를 설정할 수 있습니다.

트렌딩 그래프

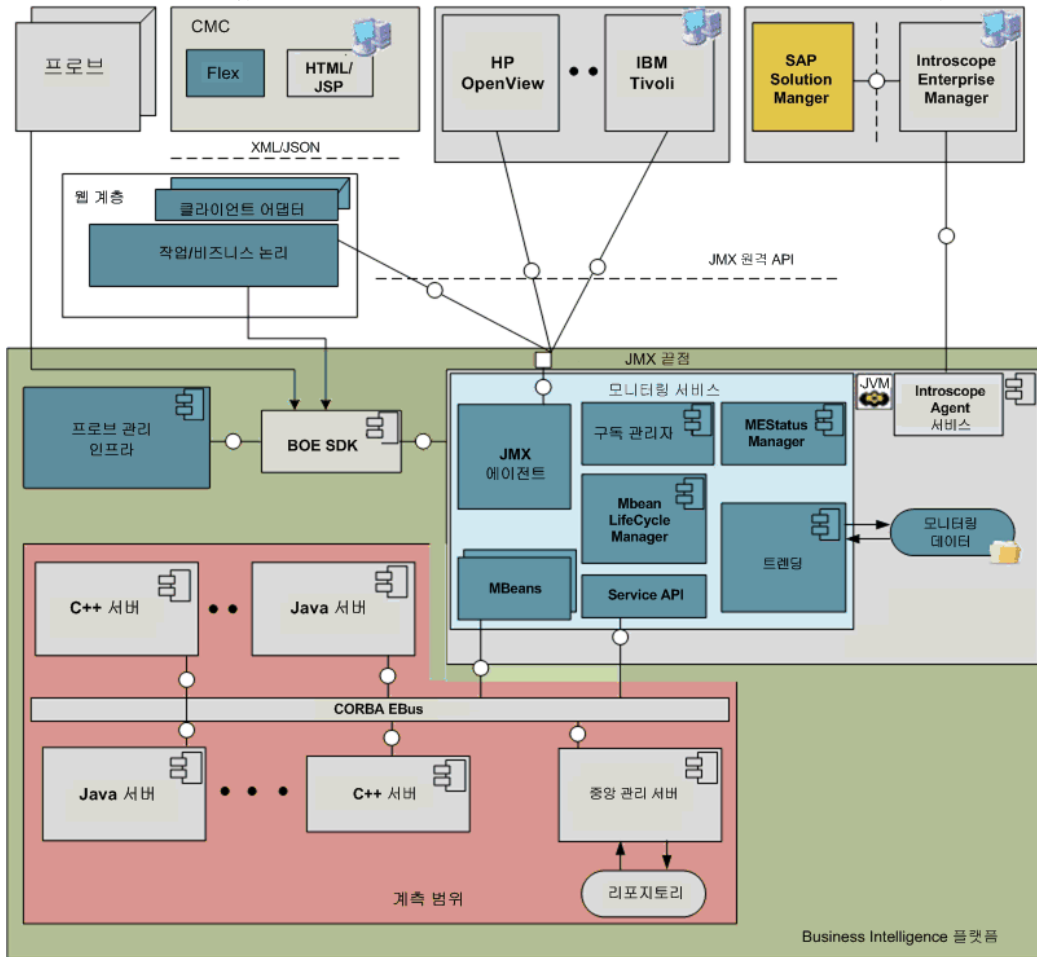
트렌딩 그래프는 프로브 및 서버가 생성한 기록 메트릭 데이터를 그래픽으로 나타낸 것입니다. 시스템 관리자는 이 그래프를 통해 다른 시간 간격별로 시스템을 모니터링하고 시스템 사용 패턴을 평가할 수 있습니다.

경고

경고는 감시에 적용되는 여러 메트릭에 대해 설정된 사용자 정의 임계값이 위반될 때 모니터링 응용 프로그램에서 생성하는 알림입니다. "대시보드" 페이지에서 전자 메일 또는 뷰를 통해 경고를 받도록 선택할 수 있습니다.

15.2.1 아키텍처

이 단원에서는 모니터링 아키텍처에 대한 높은 수준의 개요를 제공하며 구성 요소의 역할에 대해 간략히 설명합니다. 다음은 모니터링 아키텍처를 그래픽으로 나타낸 것입니다.



다음은 아키텍처의 고급 구성 요소입니다.

- PJS(Platform Java Server)
- JMX(Java Management Extensions) 에이전트/서버
- MBeans
- JMX 클라이언트
- 관리 콘솔
- 트렌딩 데이터베이스

모니터링 서비스는 Platform Java Server에서 호스팅됩니다. 응용 프로그램은 JMX 기술을 기반으로 합니다.

Monitoring Platform Java Service는 모니터링 응용 프로그램에서 사용 가능한 핵심 서비스를 제공합니다. Monitoring Platform Java Service에서 제공하는 서비스는 다음과 같습니다.

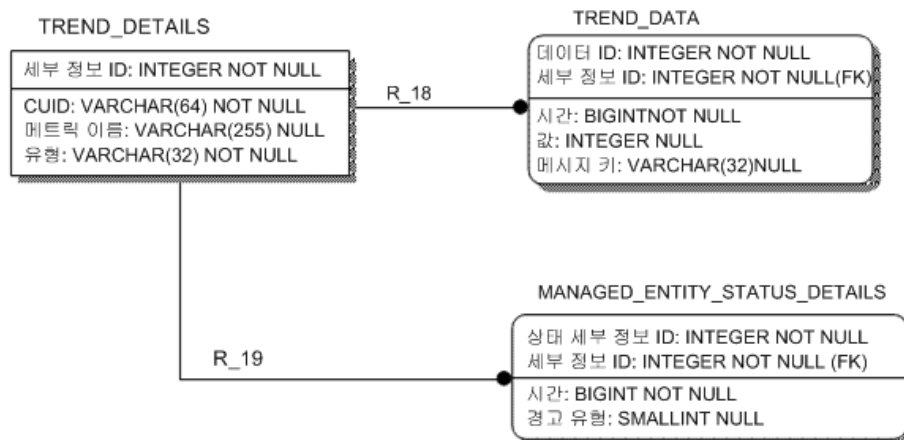
- JMX 에이전트 서비스를 제공합니다.
- SAP BusinessObjects 서버에 대해 동적으로 MBean을 만듭니다.
- MBean에 대한 주기 관리를 제공합니다.
- 새 프로브를 등록할 수 있는 메커니즘을 제공합니다.
- 사용자가 서버 메트릭을 사용하여 복합 임계값 조건을 만들 수 있도록 합니다.
- 임계값 알람 메커니즘을 제공하고 경고를 보냅니다.
- 기록 데이터를 저장하여 트렌딩 함수를 제공합니다.

적응형 작업 서버에서 호스팅되는 프로브 예약 서비스는 프로브 실행 및 예약을 관리합니다. 따라서 프로브를 실행하려면 적응형 작업 서버가 실행 중이어야 합니다.

모니터링 응용 프로그램은 JMX RMI(Remote Method Invocation) URL 끝점도 제공합니다. 다른 엔터프라이즈 응용 프로그램(예: SAP Solution Manager 및 IBM Tivoli Monitoring)은 모니터링 응용 프로그램에 연결하고 JMX 원격 API를 사용하여 SAP BusinessObjects 메트릭에 액세스할 수 있습니다. 모니터링 응용 프로그램은 전용 Derby 데이터베이스를 사용하여 트렌딩용으로 기록 데이터를 저장합니다. 트렌딩 데이터베이스 스키마에 대한 자세한 내용은 540 페이지에서 ["트렌딩 DB 스키마"](#)를 참조하십시오.

15.2.1.1 트렌딩 DB 스키마

다음 트렌딩 데이터베이스 다이어그램과 표 설명에서는 메트릭, 프로브 및 감시 데이터가 기록되는 테이블과 이러한 테이블의 관계를 보여 줍니다.



테이블15-1: TREND_DETAILS

이 테이블에는 관리되는 엔터티, 프로브 및 감시에 대한 정보가 기록됩니다. CUID 및 메트릭 이름을 예로 들 수 있습니다.

열 이름	설명	기본 키
DetailsId		자동으로 생성됨
CUID (64)	InfoObject의 CUID 또는 비InfoObject의 고유 ID	NULL이 아님
MetricName	메트릭의 이름	NULL이 아님
Type (32)	가입 또는 메트릭 유형	NULL이 아님

테이블15-2: TREND_DATA

이 테이블에는 메트릭, 감시 및 프로브의 트렌딩 데이터가 기록됩니다. 메트릭 값 및 시간을 예로 들 수 있습니다.

열 이름	설명	기본 키
DataId		자동으로 생성됨
DetailsId		외래 키
Time	데이터가 수집된 시간	NULL이 아님
Value	메트릭/가입 값	아니오

테이블15-3: MANAGED_ENTITY_STATUS_DETAILS

이 테이블에는 가입 위반에 대한 정보와 경고 전달 정보가 기록됩니다. 위반 시간 및 경고 전달 시간을 예로 들 수 있습니다.

열 이름	설명	기본 키
StatusDetailsId		자동으로 생성됨
DetailsId		외래 키
Time	데이터가 수집된 시간	NULL이 아님
AlertType	가입 알림 전달 유형(예: 전자 메일)	아니오

15.3 모니터링 서버에 대한 클러스터 지원

모니터링 응용 프로그램은 클러스터를 지원합니다. 클러스터 지원은 간단한 방식으로 장애 조치 지원을 구현하여 제공합니다.

클러스터 지원을 사용하면 지정된 시간에 하나의 서비스만 활성화되며 다른 모든 서비스는 비활성화됩니다. 예를 들어, 클러스터된 환경에 s1과 s2라는 두 개의 모니터링 서비스가 있을 경우 두 서비스 중 하나만 사용 가능한 상태여야 합니다. s1과 s2가 활성화를 시도하면, 두 서비스 중 하나만 성공하고 다른 서비스는 비활성화됩니다.

비활성 서비스의 경우 주기적(1분 간격)으로 활성 서비스로 사용할 수 있는지 확인하여 활성 서비스를 사용할 수 없게 될 경우 비활성 서비스가 즉시 활성 서비스로 전환됩니다.

참고:

적응형 처리 서버(APS)의 손상, 다시 시작 또는 성능 저하를 피하기 위해 별개의 APS 인스턴스에 모니터링 서비스를 호스트하는 것이 좋습니다.

15.4 메트릭

감시를 만드는 데 여러 가지 메트릭을 사용할 수 있습니다. 이러한 메트릭은 다음과 같습니다.

- 프로브 메트릭
- 서버 메트릭
- 호스트 메트릭
- 파생 메트릭

기본 프로브가 실행되면 execution time 및 passed 메트릭이 생성됩니다. 이러한 메트릭을 가상 메트릭이라고 합니다.

다음 표에는 SAP BusinessObjects Business Intelligence 플랫폼 4.0 서버 메트릭이 나열되어 있습니다.

서버	메트릭
적응형 처리 서버	<ul style="list-style-type: none"> 감사 이벤트 수신 대기열에 있는 이벤트의 AuditingMetrics.number 사용 가능한 프로세서 사용 중인 서버 스레드 CPU 사용률 큐브 개수 CvomServerImpl.debugClassID DataFederatorService.activeConnectorsConnectionsCount DataFederatorService.activeConnectorsCount DataFederatorService.activeQueriesCount DataFederatorService.activeThreadsCount DataFederatorService.analyzingQueriesCount DataFederatorService.connectionsCount DataFederatorService.diskUsedSize DataFederatorService.executingQueriesCount DataFederatorService.failedQueriesCount DataFederatorService.memoryUsedSize DataFederatorService.metadataCacheSize DataFederatorService.optimizingQueriesCount DataFederatorService.outputDataTransfer DataFederatorService.outputRowsCount DataFederatorService.queriesConsumingMemoryCount DataFederatorService.queries UsingDiskCount DataFederatorService.sourceInputDataTransfer DataFederatorService.sourceInputRowsCount DataFederatorService.waitingQueriesCount 서비스 시작 이후 실패한 추출 시도 횟수 사용 가능한 메모리 JVM 교착 상태 스레드 카운터 JVM 잠금 컨텐션 수 최대 메모리 전체 GC 수 GC 동안 페이지 오류 수 GC 동안 중단된 시스템 비율 쿼리 개수 서버 사용 상태 서버 실행 중 상태 세션 개수 서비스 시작 이후 성공한 추출 시도 횟수 전송 레이어의 스레드 전체 메모리 전송 레이어 스레드 풀 크기

서버	메트릭
중앙 관리 서버	<ul style="list-style-type: none"> • 감사 스레드 사용률 • 시작 이후 평균 커밋 응답 시간(밀리초) • 시작 이후 평균 쿼리 응답 시간(밀리초) • 사용 중인 서버 스레드 • CPU • 완료된 작업 • 현재 사용된 시스템 데이터베이스 연결 • 디스크 크기(GB) • 설정된 시스템 데이터베이스 연결 • 기존의 동시 사용자 계정 • 기존의 명명된 사용자 계정 • 작업 실패 • 시작 이후 가장 긴 커밋 응답 시간(밀리초) • 시작 이후 가장 긴 쿼리 응답 시간(밀리초) • 시작 이후 커밋 수 • CMS 시스템 캐시의 개체 수 • CMS 시스템 DB의 개체 수 • 시작 이후 쿼리 수 • 모든 사용자가 설정한 세션 수 • 동시 사용자가 설정한 세션 수 • 명명된 사용자가 설정한 세션 수 • 서버에 설정된 세션 수 • 시작 이후 사용자 로그인 수 • PID • 시작 이후 사용자 세션 최대 수 • 보류 중인 작업 • 보류 중인 시스템 데이터베이스 요청 • RAM(MB) • 실행 중인 작업 • 서버 사용 상태 • 서버 보류 중 상태 • 사용한 디스크 공간(GB) • 대기 중인 작업 • 감사 데이터베이스 마지막 업데이트 날짜 • 감사 스레드 마지막 폴링 주기 기간(초) • CMS 감사자 • 동시 사용자 라이선스 • 감사 데이터베이스 연결 설정 • 대기열의 현재 감사 이벤트 수 • 명명된 사용자 라이선스
연결 서버	

서버	메트릭
	<ul style="list-style-type: none"> • 사용 중인 서버 스레드 • CPU • 디스크 크기 • PID • RAM • 서버 사용 상태 • 서버 실행 중 상태 • 사용한 디스크 공간
연결 서버 32	<ul style="list-style-type: none"> • 사용 중인 서버 스레드 • CPU • 디스크 크기 • PID • RAM • 서버 사용 상태 • 서버 실행 중 상태 • 사용한 디스크 공간
Crystal Reports 2010 처리 서버	<ul style="list-style-type: none"> • 사용 중인 서버 스레드 • CPU • 페이지 및 캐시 서버를 통한 Crystal Reports 서비스 • 디스크 크기(GB) • PID • RAM(MB) • 서버 사용 상태 • 서버 실행 중 상태 • 사용한 디스크 공간
Crystal Reports 2010 Report Application Server	<ul style="list-style-type: none"> • 사용 중인 서버 스레드 • CPU • Report Application Server를 통한 Crystal Reports 서비스 • 디스크 크기(GB) • PID • RAM(MB) • 서버 사용 상태 • 서버 실행 중 상태 • 사용한 디스크 공간 • 대기열의 현재 감사 이벤트 수 • 현재 에이전트 스레드 수 • 현재 문서 수 • 총 에이전트 스레드 수 • 총 문서 수

서버	메트릭
Crystal Reports 캐시 서버	<ul style="list-style-type: none"> • 사용 중인 서버 스레드 • CPU • 디스크 크기(GB) • PID • RAM(MB) • 서버 사용 상태 • 서버 실행 중 상태 • 사용한 디스크 공간
Crystal Reports 처리 서버	<ul style="list-style-type: none"> • 사용 중인 서버 스레드 • CPU • CrystalReportsservicethroughPageandCacheServer executiontime • 디스크 크기(GB) • PID • RAM(MB) • 서버 사용 상태 • 서버 실행 중 상태 • 사용한 디스크 공간(GB)
대시보드 분석 서버	<ul style="list-style-type: none"> • 사용 중인 서버 스레드 • CPU • 디스크 크기 • PID • RAM • 서버 사용 상태 • 서버 실행 중 상태 • 사용한 디스크 공간
대시보드 서버	<ul style="list-style-type: none"> • 사용 중인 서버 스레드 • CPU • 디스크 크기 • PID • RAM • 서버 사용 상태 • 서버 실행 중 상태 • 사용한 디스크 공간 • 대기열 N Pseudoloc의 현재 감사 이벤트 수

서버	메트릭
이벤트 서버	<ul style="list-style-type: none"> • 사용 중인 서버 스레드 • CPU • 디스크 크기(GB) • 모니터링한 파일 • PID • RAM(MB) • 서버 사용 상태 • 서버 실행 중 상태 • 사용한 디스크 공간(GB) • 대기열 N Pseudoloc의 현재 감사 이벤트 수
입력 파일 리포지토리	<ul style="list-style-type: none"> • 활성 연결 • 활성 파일 • 루트 디렉터리의 사용 가능한 디스크 공간(%) • 루트 디렉터리의 사용 가능한 디스크 공간(GB) • 사용 중인 서버 스레드 • CPU • 보낸 데이터(MB) • 작성한 데이터(MB) • 디스크 크기(GB) • 루트 디렉터리의 빈 디스크 공간(GB) • PID • RAM(MB) • 서버 사용 상태 • 서버 실행 중 상태 • 루트 디렉터리의 전체 디스크 공간(GB) • 사용한 디스크 공간(GB)

서버	메트릭
출력 파일 리포지토리	<ul style="list-style-type: none"> • 활성 연결 • 활성 파일 • 루트 디렉터리의 사용 가능한 디스크 공간(%) • 루트 디렉터리의 사용 가능한 디스크 공간(GB) • 사용 중인 서버 스레드 • CPU • 보낸 데이터(MB) • 작성한 데이터(MB) • 디스크 크기(GB) • 루트 디렉터리의 빈 디스크 공간(GB) • PID • RAM(MB) • 서버 사용 상태 • 서버 실행 중 상태 • 루트 디렉터리의 전체 디스크 공간(GB) • 사용한 디스크 공간(GB)
PM 리포지토리 서버	<ul style="list-style-type: none"> • 사용 중인 서버 스레드 • CPU • 디스크 크기 • PID • RAM • 서버 사용 상태 • 서버 실행 중 상태 • 사용한 디스크 공간
웹 응용 프로그램 컨테이너 서버	<ul style="list-style-type: none"> • 서버 사용 상태 • 서버 실행 중 상태

서버	메트릭
Web Intelligence 처리 서버	<ul style="list-style-type: none"> • 사용 중인 서버 스레드 • CPU 사용량(%) • CPU • 캐시 높은 표시 수 • 캐시 크기(KB) • 현재 활성 세션 수 • 현재 클라이언트 호출 수 • 현재 세션 수 • 현재 작업 수 • 디스크 크기(GB) • 메모리 높은 임계값 수 • 메모리 수준 • 메모리 최대 임계값 수 • 문서 교체 수 • 문서 제한 시간 수 • 문서 수 • 교체된 문서 수 • 사용자 수 • PID • RAM(MB) • 서버 사용 상태 • 서버 실행 중 상태 • 총 CPU 시간(초) • 총 클라이언트 호출 수 • 총 세션 수 • 총 작업 수 • 사용한 디스크 공간(GB) • 가상 메모리 크기(MB) • WebI 메모리(MB) • WebI 서버(제한 시간) • 대기열 N Pseudoloc의 현재 감사 이벤트 수
Xcelsius 데이터 캐시 서버	<ul style="list-style-type: none"> • 사용 중인 서버 스레드 • CPU • 디스크 크기 • PID • RAM • 서버 사용 상태 • 서버 실행 중 상태 • 사용한 디스크 공간
Xcelsius 데이터 처리 서버	

서버	메트릭
	<ul style="list-style-type: none"> • 사용 중인 서버 스레드 • CPU • 디스크 크기 • PID • RAM • 서버 사용 상태 • 서버 실행 중 상태 • 사용한 디스크 공간

참고:

새 서버를 추가하거나 기존 서버를 시작할 때 메트릭 페이지에 메트릭이 표시되지 않는 경우, 메트릭 페이지에 메트릭이 표시될 때까지 약 10분간 기다리십시오.

15.5 구성 속성

이 단원에서는 모니터링 응용 프로그램 속성과 이러한 속성을 편집하는 방법에 대해 설명합니다.

모니터링 응용 프로그램의 구성 속성을 보려면

1. CMC의 응용 프로그램 영역으로 이동합니다.
2. 모니터링을 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다. 그러면 모니터링 응용 프로그램 속성 창이 나타납니다. 다음 표에 구성 속성에 대한 설명이 나와 있습니다.

섹션	필드	설명
	모니터링 응용 프로그램 활성화	모니터링 기능을 활성화하려면 이 옵션을 선택합니다. 이 옵션의 선택을 해제하면 프로브를 제외한 모든 모니터링 기능이 비활성화됩니다. 프로브 트렌딩도 비활성화됩니다.
	기본 JMX 에이전트 끝점 URL(IIOP)	이 URL에는 IIOP 프로토콜을 사용하는 JMX 에이전트 끝점 URL이 포함되어 있습니다. 모니터링을 활성화한 다음 서버를 다시 시작하면 이 URL이 자동으로 생성됩니다. 모니터링 서비스의 기본 프로토콜입니다. 이 URL은 읽기 전용 필드입니다.

섹션	필드	설명
RMI	JMX에 RMI 프로토콜 사용	기본적으로 이 옵션은 비활성화되어 있습니다. 이 옵션을 활성화할 경우 RMI 포트 번호를 제공해야 합니다. 이 포트는 RMI 레지스트리 항목과 RMI 커넥터 포트에 사용됩니다. 서비스에 이 포트를 사용할 수 있어야 합니다. 그렇지 않으면 서비스가 시작되지 않습니다. RMI 포트 번호를 제공한 후에는 서버를 다시 시작합니다. 서버를 다시 시작하면 RMI JMX 에이전트 끝점 URL이 생성됩니다. 이 속성은 RMI 프로토콜을 사용하는 JMX 에이전트 끝점 URL이 포함된 읽기 전용 속성입니다. 이 URL을 사용하여 다른 클라이언트에서 모니터링에 연결할 수 있습니다.
호스트 메트릭	호스트 메트릭 사용	기본적으로 이 옵션은 비활성화되어 있습니다. 이 옵션을 활성화할 경우 SAPOSCOL 이진 설치 경로를 제공해야 합니다. 호스트 메트릭을 활성화하려면 SAPOSCOL을 설치해야 합니다. SAPOSCOL 설치 방법은 553 페이지에서 "SAPOSCOL 설치" 를 참조하십시오.

섹션	필드	설명
기타 설정	메트릭 새로 고침 간격(초)	지정할 수 있는 최소 간격은 15초입니다. 이 간격에 따라 다음 사항이 제어됩니다. <ul style="list-style-type: none"> 감시에 대한 가입 계산: 여기에 지정된 시간 간격에 따라 주의 및 위험 규칙이 지속적으로 계산됩니다. 감시 상태 계산: 감시의 이벤트 설정이 주의 또는 위험 규칙이 true로 평가될 때마다 감시 상태 변경 옵션과 함께 선택된 경우 메트릭 새로 고침 기간에 지정된 시간 간격에 따라 감시 상태가 지속적으로 계산됩니다. 트렌딩 기간: 여기에 지정된 시간 간격에 따라 그래프의 기록 모드가 항상 지속적으로 트렌딩됩니다.
	데이터베이스 크기가 다음을 초과하면 기존 데이터 삭제 (MB)	데이터베이스가 지정된 크기를 초과하면 트렌딩 데이터베이스의 데이터가 정리됩니다. 데이터베이스에 대해 30% 버퍼가 만들어집니다. 예를 들어, 이 옵션을 100MB로 설정한 상태에서 검사 시 데이터베이스가 100MB를 초과하면 데이터베이스가 70MB까지 지워집니다.
	모니터링 UI 자동 새로 고침 간격(초)	이 간격은 모니터링 사용자 인터페이스(대시보드, 감시 목록 및 프로브 포함)에서 자동 새로 고침에 사용됩니다. 최소 간격은 15초입니다. 기본적으로 15초로 설정된 자동 새로 고침은 그래프의 라이브 모드에서 시간 간격에 영향을 끼치지 않습니다.
	매일 다음 시간에 데이터베이스 정리 작업 실행	지정한 시간에 데이터베이스 정리 작업이 시작됩니다. 데이터베이스가 지정한 최대 크기를 초과하면 데이터베이스가 정리됩니다.
	다음 간격으로 트렌딩 데이터베이스 백업	기본적으로 이 옵션은 비활성화되어 있습니다. 이 옵션을 활성화할 경우 트렌딩 데이터베이스 백업 작업이 지정된 시간에 시작됩니다.
	트렌딩 데이터베이스 백업 디렉터리	기본적으로 이 위치는 지정되어 있지 않습니다. 위치를 지정할 수 있습니다. 단, 상대 경로가 아닌 절대 경로를 제공하십시오. 공유 위치의 경우 공유 위치에 대한 액세스 권한이 부여되어야 합니다.
	데이터베이스 백업 작업 실행	이 옵션을 클릭하면 데이터베이스 백업 작업이 시작됩니다. 이 옵션을 선택하기 전에 데이터베이스 백업 디렉터리 위치를 지정하십시오.
	트렌딩 데이터베이스 위치	

섹션	필드	설명
		기본적으로 트렌딩 데이터베이스 위치는 BOE_Install_DirWSAP Business ObjectsWSAP BusinessObjects Enterprise XI 4.0/Data/TrendingDB입니다. 다른 위치를 지정할 수도 있습니다. 단, 상대 경로가 아닌 절대 경로를 제공하십시오. 클러스터 환경의 경우 위치가 공유될 수 있으며 공유 위치에 대한 액세스 권한이 부여되어야 합니다.

3. 저장을 클릭합니다.

참고:

모니터링 응용 프로그램 활성화 및 비활성화를 제외하고 이러한 속성을 변경하는 경우 적응형 처리 서버에서 호스팅되는 모니터링 서비스를 다시 시작해야 합니다.

SAPOSCOL 설치

SAPOSCOL을 설치하려면 다음 단계를 수행하십시오.

1. SAP Marketplace(<http://service.sap.com>)에서 SAPHOSTAGENT710_XX.SAR을 다운로드합니다.
2. SAPHOSTAGENT710_XX.SAR 명령을 실행하여 SAPHOSTAGENT710_XX.SAR을 추출합니다.
3. saphostexec.exe -install 명령을 실행하여 saphostexec를 설치합니다. saphostexec가 서비스로 설치되면 SAPOSCOL이 시작됩니다.
4. saposcol -s 명령을 실행하여 SAPOSCOL 상태를 확인합니다.

15.5.1 JMX 끝점 URL

모니터링 응용 프로그램은 다른 클라이언트가 JMX 원격 API를 사용하여 연결할 때 필요한 JMX 끝점 URL을 제공합니다. 기본적으로 JMX 연결은 IIOP(Internet Inter-Orb Protocol) 또는 CORBA(Common Object Request Broker Architecture) 전송을 통해 제공됩니다. 이 연결 URL은 모니터링 응용 프로그램의 속성 페이지에 표시됩니다. IIOP를 통해 연결할 수 있으면 방화벽에 대해 걱정할 필요가 없으며 포트를 제공하지 않아도 됩니다. 기본적으로 CORBA 포트를 사용할 수 있습니다. 연결하려면 JMX 클라이언트 측에서 다음 표에 나열된 jar 파일이 필요합니다.

Jar 파일
activation-1.1.jar
axiom-api-1.2.5.jar
axiom-impl-1.2.5.jar
axis2-adb-1.3.jar
axis2-kernel-1.3.jar
cecore.jar
celib.jar
cesession.jar
commons-logging-1.1.jar
corbaidl.jar
ebus405.jar
log4j.jar
logging.jar
monitoring-plugins.jar
monitoring-sdk.jar
stax-api-1.0.1.jar
wsdl4j-1.6.2.jar
wstx-asl-3.2.1.jar
XmlSchema-1.3.2.jar
TraceLog.jar
ceaspect.jar
aspectjrt.jar

기본 RMI 포트를 통해 연결할 수도 있습니다. RMI 포트를 통해 연결하는 방법에 대한 자세한 내용은 550 페이지에서 ["구성 속성"](#)을 참조하십시오.

15.6 다른 응용 프로그램과 통합

SAP Solution Manager 및 IBM Tivoli Monitoring 등의 Enterprise 솔루션은 JMX 끝점 URL을 통해 연결하여 JMX 클라이언트와 같은 모니터링 응용 프로그램과 통합됩니다. 통합 후 클라이언트의 사용자 인터페이스에서 SAP BusinessObjects 메트릭을 볼 수 있습니다.

15.6.1 IBM Tivoli와 모니터링 응용 프로그램 통합

모니터링 응용 프로그램을 IBM Tivoli와 통합하려면 IBM Tivoli Monitoring 에이전트를 만들어 설치하고 구성해야 합니다. IBM Tivoli Monitoring 에이전트를 만들려면 다음 단계를 수행하십시오.

1. IBM Tivoli Monitoring 에이전트 작성기 버전 6.2.1 소프트웨어를 설치합니다.
2. 새 에이전트를 만듭니다. 새 에이전트를 만드는 방법은 IBM Tivoli Monitoring Agent 사용자 안내서를 참조하십시오.
3. 데이터 모니터링 유형 정의 단계에서는 Monitoring Data Categories(모니터링 데이터 범주) 영역에서 Data from a server(서버의 데이터)를 선택하고 Data Sources(데이터 원본) 영역에서 JMX를 선택합니다.
4. 다음을 클릭합니다.
5. JMX Information(JMX 정보) 창에서 Browse(찾아보기)를 클릭하여 MBean 서버에 있는 모든 JMX MBean을 확인합니다.

참고:

브라우저를 처음 실행하는 경우 새 연결을 추가해야 합니다.

6. JMX(Java Management Extensions) 브라우저 창에서 Connection Name(연결 이름) 옆에 있는 + 를 클릭하여 새 연결을 추가합니다.
7. MBean Server Connection Wizard(MBean 서버 연결 마법사) 창에서 Standard JMX Connections(JSR-160)(표준 JMX 연결(JSR-160))을 선택합니다.
8. 연결 속성 창에 다음 정보를 입력합니다.

필드	설명
Connection Name(연결 이름)	JSR-160 호환 서버입니다.
User ID(사용자 ID)	SAP BusinessObjects Enterprise에 로그인하는 데 사용되는 사용자 이름입니다.
Password(비밀번호)	SAP BusinessObjects Enterprise에 로그인하는 데 사용되는 암호입니다.
Service URL(서비스 URL)	JMX 끝점 URL을 제공합니다.

9. Finish(완료)을 클릭합니다.
10. MBean Key Properties(MBean 키 특성) 영역에서 Domain(도메인) 및 Type(유형)을 선택합니다.

그러면 아래의 텍스트 필드에 모든 MBean이 나타납니다.

11. 특성이 나열되도록 MBean을 한 번에 하나씩, 도메인이 서버인 모든 MBean을 선택합니다. 동일한 유형의 MBean이 여러 개 표시될 경우 키 특성을 선택합니다. 예를 들어, 실행 중인 서버의 인스턴스가 두 개일 경우 각 인스턴스의 PID가 키 특성일 수 있습니다.
12. 서버를 선택하고 JMX Agent-Wide Options(JMX 에이전트 차원의 옵션) 창에서 JMX 특성 그룹에 대한 옵션을 선택합니다.
13. Data Source Definition(데이터 원본 정의) 창에서 추가한 에이전트를 선택하고 Add to Selected(선택된 항목에 추가)를 클릭합니다. 그러면 에이전트를 만드는 과정의 처음으로 돌아가므로 모니터링할 다른 서버를 추가하려면 위 단계를 반복해야 합니다.
14. 에이전트를 만든 후에는 에이전트를 설치해야 합니다. 에이전트를 설치하는 방법은 IBM Tivoli Monitoring Agent 사용자 안내서, 그림 번호 154를 참조하십시오. 이 단원에서는 로컬에서 에이전트를 설치하는 방법과 설치 가능한 에이전트 솔루션을 만드는 방법도 설명합니다.

참고:

에이전트 작성기를 사용하여 SAP BusinessObjects Business Intelligence 플랫폼용 에이전트를 만드는 경우 동일한 시스템에 SAP BusinessObjects Business Intelligence 플랫폼 4.0이 설치되어 있어야 합니다. 하지만 설치 관리자 파일을 사용하여 이미 만들어진 에이전트를 설치하는 경우 구성 시 JMX 끝점과 함께 시스템 세부 정보를 제공할 수 있으므로 BOE 모니터링이 설치되어 있지 않아도 됩니다.

설치된 에이전트를 구성하려면 다음 단계를 수행하십시오.

1. TEMS 모드로 Manage Tivoli Enterprise Monitoring Services(Tivoli Enterprise Monitoring 서비스 관리)를 엽니다. 그러면 설치된 에이전트가 표시됩니다.
2. 에이전트 템플릿을 마우스 오른쪽 단추로 클릭하고 기본값을 사용하여 구성을 선택합니다.
3. 인스턴스 이름을 선택합니다.

두 가지 다른 프로토콜(RMI 및 BOEIIOP)을 사용하여 에이전트를 구성할 수 있습니다.

RMI 프로토콜을 사용하려면

- 다음을 클릭합니다. Java 매개 변수는 변경하지 마십시오.
- 사용자 ID, 암호 및 서비스 URL 등 JMX 자격 증명 값을 입력합니다. 자세한 내용은 관련 항목의 속성 구성을 참조하십시오.
- 확인을 클릭합니다.

BOEIIOP 프로토콜을 사용하려면

- bcm.jar 및 cryptojFIPS.jar 파일을 %InstallDir%\WSAP BusinessObjects\WSAP BusinessObjects Enterprise XI 4.0\java\lib에서 사용 중인 시스템의 폴더로 복사합니다.
- 다음 표에 나열된 jar 파일을 다른 폴더에 복사합니다.
- Java 매개 변수의 JVM 인수를 -Djmx.remote.protocol.provider.pkgs = com.businessobjects.sdk.monitoring 및 -Djmx.boeiiop.bcm.dir=< bcm.jar 파일과 cryptojFIPS.jar 파일을 복사한 폴더 위치>로 설정합니다.
- 다음을 선택합니다.
- 사용자 ID, 암호 및 서비스 URL 등 JMX 자격 증명 값을 입력합니다. 자세한 내용은 관련 항목의 속성 구성을 참조하십시오.
- <Jar Directories(Jar 디렉터리)> 값을 표에 제공된 jar 파일 목록을 복사한 폴더의 위치로 설정합니다.
- 확인을 클릭합니다.

Jar 파일
activation-1.1.jar
axiom-api-1.2.5.jar
axiom-impl-1.2.5.jar
axis2-adb-1.3.jar
axis2-kernel-1.3.jar
cecore.jar
celib.jar
cesession.jar
commons-logging-1.1.jar
corbaidl.jar
ebus405.jar
log4j.jar
logging.jar
monitoring-plugins.jar
monitoring-sdk.jar
stax-api-1.0.1.jar
wsdl4j-1.6.2.jar
wstx-asl-3.2.1.jar
XmlSchema-1.3.2.jar
TraceLog.jar
ceaspect.jar
aspectjrt.jar

4. Tivoli Enterprise 모니터링 서비스 관리 창에서 에이전트를 마우스 오른쪽 단추로 클릭하고 시작을 선택합니다.
5. IBM Tivoli Enterprise Portal Desktop/Browser Client(IBM Tivoli Enterprise Portal 데스크톱/브라우저 클라이언트)를 엽니다. 그러면 Navigator(탐색기) 창에 단추가 나타납니다.
6. 검색기 단추를 클릭합니다.

에이전트가 Navigator(탐색기)에 추가됩니다.

관련 항목

- 550 페이지에서 [구성 속성](#)

15.6.2 SAP Solution Manager와 모니터링 응용 프로그램 통합

모니터링 응용 프로그램을 SAP Solution Manager와 통합하려면 시스템에 [Wily Introscope](#)가 설치되어 실행 중이어야 하며, SAP Solution Manager를 Introscope 워크스테이션에 대해 구성해야 합니다. SAP BusinessObjects Business Intelligence 플랫폼 4.0을 설치하는 동안 다음 단계를 수행합니다.

1. Introscope Enterprise Manager에 대한 연결 구성 단계에서 호스트 이름과 포트 세부 정보를 제공합니다. Introscope Agent는 SAP BusinessObjects Business Intelligence 플랫폼 4.0이 설치될 때 C:\Program Files (x86)\SAP Business Objects\SAP Business Objects Enterprise XI 4.0\java\Wiley에 설치됩니다.
2. Introscope 워크스테이션을 시작하고 New Investigator를 클릭합니다. 구성된 에이전트의 JMX 섹션에서 SAP BusinessObjects 서버 메트릭 및 프로브 가상 메트릭을 볼 수 있습니다.

참고:

CMC > 서버 > 서버 노드 > 자리 표시자를 선택하여 IS(Introscope) 에이전트를 구성할 수 있습니다. IS Enterprise Manager 호스트 및 포트 또한 여기에서 IS 에이전트에 구성되어 모니터링 응용 프로그램과 통신합니다. 자세한 내용은 SAP BOE CMC 도움말 가이드의 관리 서버를 참조하십시오.

IS에서 JMX 메트릭을 사용하려면 IS 에이전트 서비스 및 모니터링 서비스가 AdaptiveProcessingServer 인스턴스에서 사용할 수 있는지 확인합니다.

IS 계측을 활성화하면 코드 계측이 자동으로 활성화됩니다.

15.7 Derby 데이터베이스용 유니버스 만들기

Derby 데이터베이스용 유니버스는 Derby 데이터베이스에서 쿼리를 실행하여 보고서를 만들고 데이터 분석을 실행하기 위해 만듭니다. 유니버스 만들기에 대한 자세한 내용은 SAP BOE Universe Designer 가이드를 참조하십시오.

참고:

Derby 데이터베이스용 유니버스는 해당 데이터베이스의 백업 작업을 실행한 후에 만듭니다. 데이터베이스 백업 작업에 대한 자세한 내용은 관련 항목의 속성 구성을 참조하십시오.

1. 유니버스 디자인 도구 마법사를 실행하여 Derby 데이터베이스용 유니버스를 만듭니다.
마법사를 사용한 유니버스 작성에 대한 자세한 내용은 SAP BOE Universe Designer 가이드의 빠른 디자인 마법사 사용을 참조하십시오.
Apache 및 Generic의 두 가지 데이터베이스 연결을 사용하여 유니버스를 만들 수 있습니다.

2. Apache 연결을 선택한 경우 다음과 같이 진행합니다.
 - a. JDBC 드라이버를 클릭합니다.
 - b. INSTALL_DIR\WSAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer\jdbc 위치에서 derby.sbo 파일을 선택합니다.
 - c. 클래스 경로 <ClassPath> <Path>W...W...Wderby.jar</Path></ClassPath>를 추가합니다.
클래스 경로를 추가하기 전에 Apache 웹 사이트에서 최신 derby.jar 파일(버전 10.5.x)을 다운로드합니다.
 - d. 새 Apache 데이터베이스 연결을 만들려면 서버 필드에 Derby 데이터베이스 폴더 위치를 입력합니다.
데이터베이스가 C:\WDerby에 있으면 C:\WDerby;create=false를 입력합니다.
3. Generic 연결을 선택한 경우 다음과 같이 진행합니다.
 - a. Generic JDBC를 선택합니다.
 - b. INSTALL_DIR\WSAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer\jdbc 위치에서 jdbc.sbo 파일을 선택합니다.
 - c. 클래스 경로 <ClassPath> <Path>W...W...Wderby.jar</Path></ClassPath> 및 JDBC 클래스 세부 정보 <Parameter Name="JDBC Class">org.apache.derby.jdbc.EmbeddedDriver</Parameter>를 추가합니다.
 - d. Generic 데이터베이스 연결을 새로 만드는 경우 URL 필드에 jdbc:derby:C:\WDerby;create=false를 입력합니다.

관련 항목

- 550 페이지에서 [구성 속성](#)"

15.8 문제 해결

이 단원에서는 모니터링 응용 프로그램을 사용하면서 발생할 수 있는 다양한 문제에 대한 단계별 솔루션을 제공합니다.

15.8.1 대시보드

CMC 페이지에 모니터링 링크가 표시되지 않습니다.

- 사용자에게 적절한 액세스 권한이 있는지 확인합니다.

- 사용자가 모니터링 사용자 그룹이나 관리자 그룹 또는 이러한 그룹의 멤버인 다른 그룹에 추가되었는지 확인합니다.

모니터링 대시보드에 핵심 성과 지표(KPI)가 표시되지 않습니다

- CMS 서버 속성 > 메트릭을 선택하여 필요한 메트릭이 표시되는지 확인합니다.
- 중앙 관리 서버가 예상대로 응답하는지 확인합니다.

모니터링 응용 프로그램을 실행할 수 없습니다.

최신 Flash Player(10.5.x)를 다운로드하여 설치합니다.

15.8.2 경고

경고 페이지에서 경고를 수신할 수 없습니다.

- 알림 설정에서 경고 알림 사용이 선택되어 있는지 확인합니다.
- 경고를 수신할 수 있는 적절한 액세스 권한이 있는지 확인합니다.
- 모니터링 대시보드에 최근 경고가 표시되는지 확인합니다
- SMTP 서버가 작동 중인지 확인합니다.
- 전자 메일 경고를 수신하도록 설정된 전자 메일 ID가 적합한지 확인합니다.
- AdaptiveJobServer 인스턴스가 사용 가능한지 확인합니다.
- AdaptiveJobServer 인스턴스 대상의 SMTP 설정을 확인합니다.

참고:

SMTP가 예상대로 작동 중일 경우 테스트용으로 설정한 전자 메일 ID로 CR 문서를 보낼 수 있습니다.

15.8.3 감시 목록

감시용 기록 데이터를 수신할 수 없습니다.

- 모니터링 응용 프로그램의 속성 페이지에서 폴링 간격을 확인합니다.
- 로깅 폴더에서 추적 파일을 확인합니다.
- CMC 응용 프로그램 페이지에 트래킹 데이터베이스 위치가 지정되어 있는지 확인합니다. 클러스터 환경의 경우 사용자에게 공유 위치에 액세스할 수 있는 권한이 있는지 확인합니다. 자세한 내용은 관련 항목의 속성 구성을 참조하십시오.
- 서버와 클라이언트의 시스템 시간이 특정 시간대에서 동일한지 확인합니다.

동기화된 라이브 데이터를 검색하는 중 오류가 발생했습니다

AdaptiveProcessingServer 인스턴스가 실행 중인지 확인합니다.

감시 목록 탭이 비활성화되어 있습니다.

- 메트릭이 지정된 서버가 실행 중인지 확인합니다.
- 메트릭 목록 페이지의 해당 메트릭이 라이브 모드 및 기록 모드에서 정보를 표시하는지 확인합니다.
- 모니터링 서비스 로그에서 오류 메시지를 확인합니다.
- jconsole에 메트릭이 표시되는지 확인합니다

관련 항목

- 550 페이지에서 [구성 속성](#)"

15.8.4 프로브

프로브를 예약할 수 없습니다.

- AdaptiveJobServer 인스턴스가 실행 중인지 확인합니다.
- Crystal 보고서 및 Web Intelligence 문서에 사용되는 보고서 CUID가 적합한지 확인합니다.
- 사용자가 적절한 권한을 가지고 있는지 아니면 관리자 그룹의 멤버인지 확인합니다.
- 해당 프로브에 사용되는 Crystal Reports 또는 Web Intelligence 문서에 대해 열기, 새로 고침, 내 보내기를 수행할 수 있는 적절한 권한이 사용자에게 있는지 확인합니다.

프로브 일정 상태가 보류 중입니다.

- ProbeSchedulingService 인스턴스가 설치되었는지 확인합니다.
- AdaptiveJobServer 인스턴스가 실행 중인지 확인합니다.

데이터베이스에서 추세 데이터를 검색하는 중 오류가 발생했습니다

AdaptiveProcessingServer 인스턴스가 실행 중인지 확인합니다.

probeRun.bat이 성공적으로 실행되지 않습니다.

- java_home이 설정되어 있는지 확인합니다.
- 명령 프롬프트에 올바른 매개 변수를 입력했는지 확인합니다

참고:

명령 프롬프트에 probeRun.bat -help를 입력하여 모든 매개 변수가 적합한지 확인합니다.

15.8.5 메트릭

호스트 메트릭이 나열되지 않습니다.

- SAPOSCOL이 실행 중인지 확인합니다.
- 모니터링 응용 프로그램의 속성 페이지에서 호스트 메트릭 사용 옵션이 선택되어 있는지 확인합니다.
- AdaptiveProcessingServer 인스턴스를 다시 시작하여 변경 내용을 적용합니다.
- SAPOSCOL 이진 설치 경로가 적합한지 확인합니다.

JMX 클라이언트를 검색하는 중 오류가 발생했습니다.

AdaptiveProcessingServer 인스턴스가 실행 중인지 확인합니다.

메트릭 페이지에서 SAPOSCOL 메트릭 값이 0입니다.

- SAPOSCOL이 실행 중인지 확인합니다.
- SAPOSCOL이 설치된 호스트에서 다음을 수행합니다.
 1. `saposcol -s`를 실행하여 상태를 확인합니다
 2. `saposcol -m`을 실행하여 SAPOSCOL에서 수집한 데이터의 스냅샷을 가져옵니다.

15.8.6 그래프

그래프에 표시되는 라이브 모드와 기록 모드의 시간이 서로 다릅니다.

서버와 클라이언트의 시스템 시간이 특정 시간대에서 동일한지 확인합니다.

클러스터 시나리오의 기록 모드에서 그래프 데이터가 표시되지 않습니다.

모든 AdaptiveProcessingServer 인스턴스가 동일한 Derby 데이터베이스 위치를 가리키는지 확인합니다.

장16 감사

16.1 개요

감사를 사용하면 서버 및 응용 프로그램의 중요한 이벤트에 대한 레코드를 관리할 수 있으므로, 액세스 대상 정보, 정보 액세스 방식과 변경 과정, 해당 작업을 수행 중인 사용자 등을 파악할 수 있습니다. 이 정보는 감사 데이터 저장소(ADS)라는 데이터베이스에 기록됩니다. 데이터가 ADS에 기록된 후에는 요구 사항에 맞춰 사용자 지정 보고서를 디자인할 수 있습니다. [SAP Developer Network](#)에서 샘플 유니버스와 보고서를 찾을 수 있습니다.

이번 장에서 말하는 감사자는 특정 이벤트에 대한 정보를 기록하거나 저장하는 역할을 맡은 시스템이며, 감사 대상은 감사 가능한 이벤트가 수행되는 모든 시스템입니다. 상황에 따라서는 한 시스템이 두 가지 기능을 모두 수행할 수 있습니다.

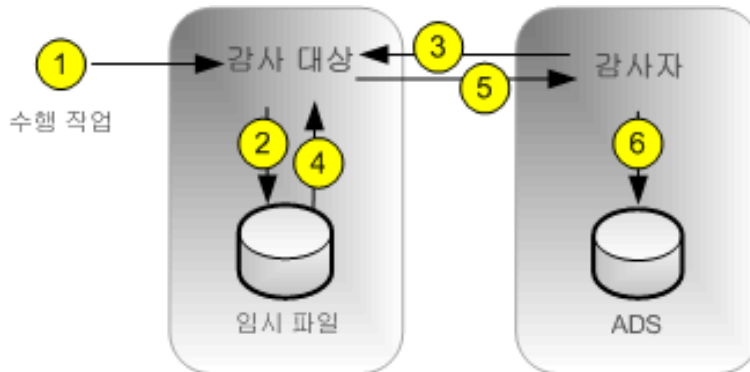
감사 기능 작동 방식

중앙 관리 서버(CMS)는 시스템 감사자 역할을 하고, 감사 가능한 이벤트를 트리거하는 각 서버 또는 응용 프로그램은 감사 대상이 됩니다. 감사 대상인 이벤트가 트리거되면 감사 대상이 레코드를 생성하고 이를 로컬 임시 파일로 저장합니다. CMS는 정기적으로 감사 대상과 통신하여 이런 레코드를 요청하고 ADS에 데이터를 작성합니다.

또한 CMS는 다른 컴퓨터에서 발생하는 감사 이벤트의 동기화를 제어합니다. 각 감사 대상은 감사 이벤트를 기록할 때 타임스탬프를 함께 제공합니다. 서로 다른 여러 서버에서 발생하는 이벤트의 타임스탬프를 일치시키기 위하여 CMS는 시스템 시간을 감사 대상에 주기적으로 브로드캐스트합니다. 그러면 감사 대상은 이 시간을 내부 클럭과 비교합니다. 시간에 차이가 있을 경우 이후의 감사 이벤트를 위해 기록되는 시간을 수정합니다.

감사 대상의 유형에 따라 시스템에서 다음 워크플로 중 하나를 사용하여 이벤트를 기록합니다.

서버 감사

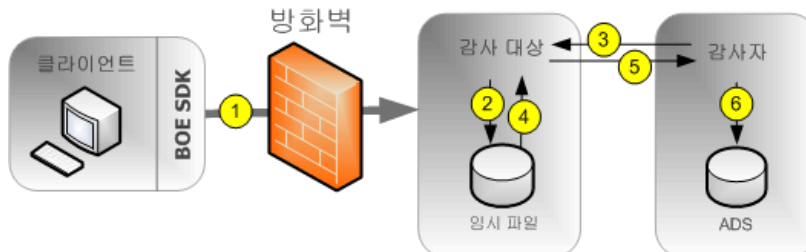


참고: 감사자와 감사 대상이 같은 CMS 서버에 함께 존재할 수도 있습니다.

1. 감사 가능한 이벤트가 서버를 통해 수행됩니다.
2. 감사 대상이 임시 파일에 이벤트를 기록합니다.
3. 감사자가 감사 대상을 폴링하고 감사 이벤트의 배치를 요청합니다.
4. 감사 대상이 임시 파일에서 이벤트를 검색합니다.
5. 감사 대상이 감사자에게 이벤트를 전송합니다.
6. 감사자가 ADS에 이벤트를 기록하고 감사 대상에게 임시 파일에서 이벤트를 삭제하도록 지시합니다.

CORBA를 통해 연결되는 클라이언트에 대한 클라이언트 로그온 감사

SAP BusinessObjects Web Intelligence와 같은 응용 프로그램이 여기에 포함됩니다.



참고: 감사자와 감사 대상이 같은 CMS 서버에 함께 존재할 수도 있습니다.

1. 클라이언트가 감사 대상의 역할을 하는 CMS에 연결합니다. 클라이언트에서 해당 IP 주소와 컴퓨터 이름을 제공하면 감사 대상이 이를 확인합니다.

참고:

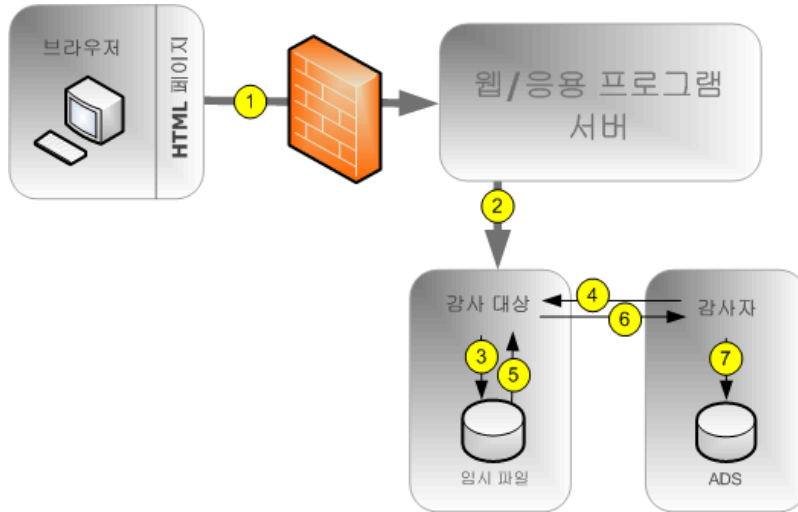
클라이언트와 CMS 사이의 방화벽에 포트가 열려 있어야 합니다. 방화벽에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드의 보안 장에서 확인할 수 있습니다.

2. 감사 대상이 임시 파일에 이벤트를 기록합니다.
3. 감사자가 감사 대상을 폴링하고 감사 이벤트의 배치를 요청합니다.
4. 감사 대상이 임시 파일에서 이벤트를 검색합니다.
5. 감사 대상이 감사자에게 이벤트를 전송합니다.

6. 감사자가 ADS에 이벤트를 기록하고 감사 대상에게 임시 파일에서 이벤트를 삭제하도록 지시합니다.

HTTP를 통해 연결되는 클라이언트에 대한 클라이언트 로그인 감사

여기에는 BI 실행 패드, 중앙 관리 콘솔, SAP BusinessObjects Web Intelligence 등과 같은 온라인 응용 프로그램이 포함됩니다.

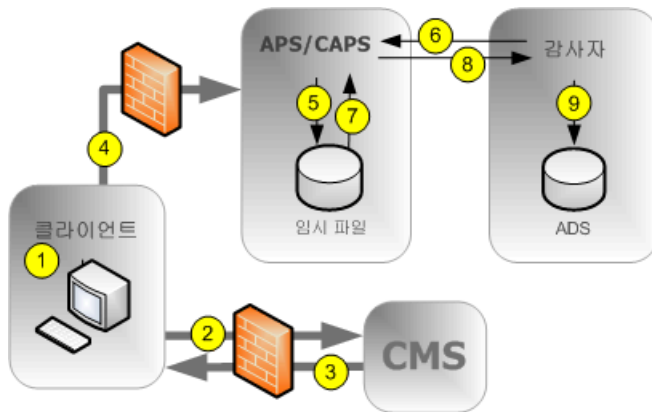


참고: 감사자와 감사 대상이 같은 CMS 서버에 함께 존재할 수도 있습니다.

1. 브라우저가 웹 응용 프로그램 서버에 연결되고 로그인 데이터가 웹 응용 프로그램 서버에 제출됩니다.
2. BI 플랫폼 SDK에서 로그인 요청을 브라우저 컴퓨터의 IP 주소 및 이름과 함께 감사 대상(CMS)에 제출합니다.
3. 감사 대상이 임시 파일에 이벤트를 기록합니다.
4. 감사자가 감사 대상을 폴링하고 감사 이벤트의 배치를 요청합니다.
5. 감사 대상이 임시 파일에서 이벤트를 검색합니다.
6. 감사 대상이 감사자에게 이벤트를 보냅니다.
7. 감사자가 ADS에 이벤트를 기록하고 감사 대상에게 임시 파일에서 이벤트를 삭제하도록 지시합니다.

CORBA를 통해 연결되는 클라이언트에 대한 비로그온 감사

이 워크플로는 CORBA를 통해 연결할 때 발생하는 SAP BusinessObjects Web Intelligence 이벤트를 감사하는 데 적용됩니다.



1. 감사 대상이 될 수 있는 작업을 사용자가 수행합니다.
2. 클라이언트에서 CMS에 연결하여 해당 작업을 감사하도록 구성되어 있는지 확인합니다.
3. 작업을 감사하도록 설정되어 있는 경우 CMS는 이 정보를 클라이언트로 전달합니다.
4. 클라이언트에서 이벤트 정보를 클라이언트 감사 프록시 서비스(CAPS)로 보냅니다. 이 서비스는 적응형 처리 서버에서 호스팅됩니다.

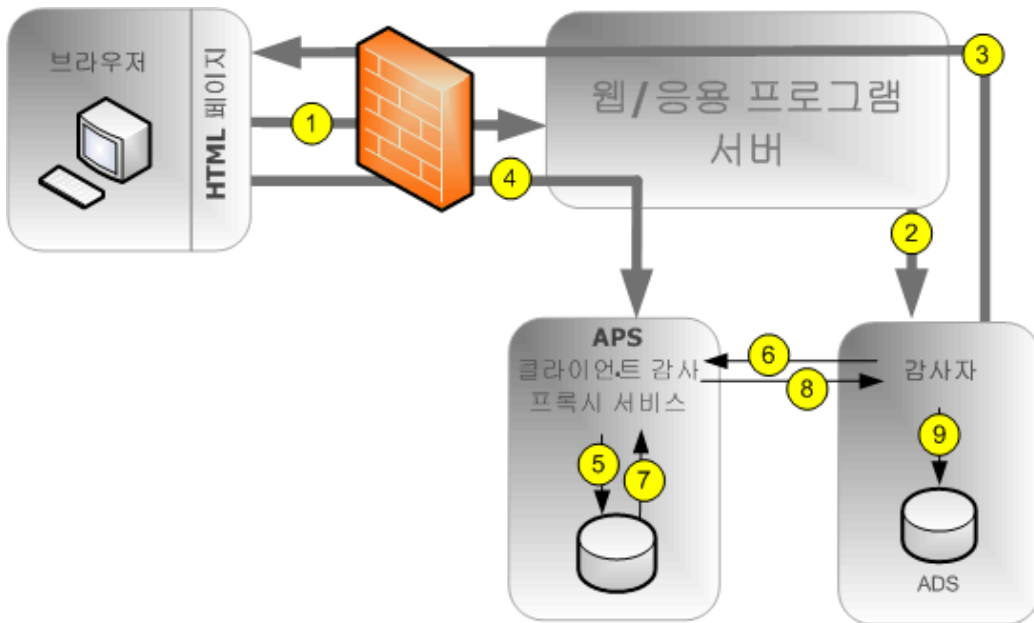
참고:

각 클라이언트와 CAPS를 호스팅하는 모든 적응형 처리 서버 사이 및 각 클라이언트와 CMS 사이의 방화벽 포트를 열어 두어야 합니다. 방화벽에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드의 보안 장에서 확인할 수 있습니다.

5. CAPS가 임시 파일에 이벤트를 기록합니다.
6. 감사자가 CAPS를 폴링하고 감사 이벤트 배치를 요청합니다.
7. CAPS가 임시 파일에서 이벤트를 검색합니다.
8. CAPS가 감사자에게 이벤트 정보를 보냅니다.
9. 감사자가 ADS에 이벤트를 기록하고 CAPS에 임시 파일에서 이벤트를 삭제하도록 지시합니다.

HTTP를 통해 연결되는 클라이언트에 대한 비로그인 감사

이 워크플로는 HTTP를 통해 연결할 때 발생하는 SAP BusinessObjects Web Intelligence 이벤트 (로그온 이벤트 제외)를 감사하는 데 적용됩니다.



참고: 감사자와 감사 대상이 같은 CMS 서버에 함께 존재할 수도 있습니다.

1. 감사 대상이 될 수도 있는 이벤트를 사용자가 시작합니다. 클라이언트 응용 프로그램이 웹 응용 프로그램 서버에 연결됩니다.
2. 웹 응용 프로그램이 해당 이벤트가 감사 대상으로 구성되어 있는지 여부를 확인합니다.

참고:

그림에는 연결을 시도하는 감사자 CMS가 나와 있지만 클러스터에 있는 임의의 CMS에 연결하여 이 정보를 얻을 수 있습니다.

3. CMS가 감사 구성 정보를 웹 응용 프로그램 서버에 반환하면 웹 응용 프로그램 서버에서는 이 정보를 다시 클라이언트 응용 프로그램으로 전달합니다.
4. 이벤트가 감사 대상으로 구성되어 있으면 클라이언트에서 이벤트 정보를 웹 응용 프로그램 서버로 보내고, 웹 응용 프로그램 서버는 그 정보를 적응형 처리 서버(APS)에 호스팅되어 있는 클라이언트 감사 프록시 서비스(CPAS)로 전달합니다.
5. CAPS가 임시 파일에 이벤트를 기록합니다.
6. 감사자가 CAPS를 폴링하고 감사 이벤트의 배치를 요청합니다.
7. CAPS가 임시 파일에서 이벤트를 검색합니다.
8. CAPS가 감사자에게 이벤트 정보를 보냅니다.
9. 감사자가 ADS에 이벤트를 기록하고 CAPS에 임시 파일에서 이벤트를 삭제하도록 지시합니다.

감사를 지원하는 클라이언트

감사를 지원하는 클라이언트 응용 프로그램은 다음과 같습니다.

- 중앙 관리 콘솔(CMC)
- BI 실행 패드
- Open Document
- 분석
- Live Office 웹 서비스 공급자
- Web Intelligence Desktop

참고:

위에 나열된 감사 이벤트를 수집하기 위해서는 적어도 하나의 CAPS 인스턴스가 실행 중이어야 합니다.

위에 나열된 클라이언트는 이벤트를 직접 생성하지는 않지만 클라이언트 응용 프로그램 작업의 결과로 서버에서 수행된 일부 조치를 감사할 수는 있습니다.

감사 일관성

감사를 제대로 설치, 구성 및 보안하고 있고 모든 클라이언트 응용 프로그램의 올바른 버전을 사용하고 있는 대부분의 상황에서는 감사를 통해 모든 지정된 시스템 이벤트가 올바르게 일관되게 기록됩니다. 그러나 일부 시스템과 환경 조건은 감사에 부정적인 영향을 줄 수도 있음을 염두에 두어야 합니다.

이벤트가 발생하는 시각과 감사자 데이터베이스에 이벤트가 최종적으로 전송되는 시각 사이에는 항상 시간차가 있습니다. CMS나 감사 데이터베이스를 사용할 수 없거나 네트워크 연결 손실과 같은 상황에서는 이런 지연이 증가할 수 있습니다.

시스템 관리자는 불완전한 감사 레코드의 원인이 될 수 있는 다음과 같은 상황을 방지하기 위해 노력해야 합니다.

- 감사 데이터를 저장하는 드라이브가 최대 용량에 이르지 않도록 해야 합니다. 감사 데이터베이스와 감사 대상 임시 파일 저장에 사용할 수 있는 디스크 공간이 충분한지 확인해야 합니다.
- 모든 감사 이벤트를 전송하기 전에 감사 대상 서버가 네트워크에서 잘못 제거되지 않도록 해야 합니다. 네트워크에서 서버를 제거할 때는 감사 이벤트가 감사 데이터베이스에 게시될 수 있도록 충분한 시간 여유를 두어야 합니다.
- 감사 대상 임시 파일이 삭제 또는 수정되지 않도록 해야 합니다.
- 하드웨어 또는 디스크 오류가 발생하지 않도록 해야 합니다.
- 감사 대상 또는 감사자 호스트 컴퓨터가 물리적으로 손상되지 않도록 해야 합니다.

경우에 따라서는 감사 이벤트가 CMS 감사자에 도달하지 못하는 상황도 발생할 수 있습니다. 다음과 같은 경우를 예로 들 수 있습니다.

- 사용자가 이전 버전의 클라이언트를 사용하고 있을 수 있습니다.
- 올바르게 구성하지 않은 방화벽으로 인해 감사 정보의 전송이 차단될 수 있습니다.

참고:

- 클라이언트 응용 프로그램에 의해 생성된 이벤트에는 클라이언트 측, 즉 시스템의 신뢰할 수 있는 영역 외부에서 제출된 정보가 들어 있습니다. 따라서 어떤 조건에서는 이 정보가 시스템 서버에서 기록된 정보로 볼 수 없는 경우도 있습니다. 이 서버가 신뢰할 수 있는 영역 외부에 있으므로, BI 작업 영역 캐시 서버에서 생성된 이벤트가 이 정보에 포함될 수도 있습니다.
- 배포에서 서버를 제거하려면 먼저 해당 서버를 비활성화하되 임시 파일의 이벤트가 모두 감사 데이터베이스로 전송될 때까지 서버가 네트워크에 연결된 채 계속 실행되도록 해야 합니다. 서버의 대기열의 현재 감사 이벤트 수 메트릭은 전송 대기 중인 감사 이벤트 수를 표시하고, 이 수가 0에 이르면 서버를 중지할 수 있습니다. 임시 파일의 위치는 해당 노드의 자리 표시자에 정의됩니다. 자리 표시자에 대한 자세한 내용은 서버 관리 장을 참조하십시오.
- 클라이언트 감사를 사용하려면 클라이언트 감사 프로시 서비스를 위한 전용 적응형 처리 서버를 만드는 것이 좋습니다. 그러면 최상의 시스템 성능을 얻을 수 있을 것입니다. 시스템의 내결함성을 높이기 위해 둘 이상의 APS에서 CAPS를 실행하는 방법을 고려해볼 수도 있습니다.

관련 링크

885 페이지에서 ["서버 및 노드 자리 표시자"](#)

16.2 CMC 감사 페이지

CMC의 감사 페이지에는 다음과 같은 영역이 있습니다.

- 감사 상태 요약
- 이벤트 설정
- 이벤트 세부 정보 설정
- 구성

16.2.1 감사 상태

감사 상태에는 감사 구성을 최적화하는 데 도움이 되고 감사 데이터의 무결성에 영향을 줄 수 있는 문제를 경고하는 메트릭 집합이 표시됩니다. 상태 요약은 중앙 관리 콘솔의 감사 페이지 맨 위에 있습니다.

다음 상황에서는 요약에 경고도 표시됩니다.

- 감사 데이터 저장소(ADS) 데이터베이스에 연결할 수 없는 경우
- 실행 중이거나 활성화된 클라이언트 감사 프록시 서비스가 없어 클라이언트 이벤트를 수집할 수 없는 경우
- 감사 대상에게 검색하지 못한 이벤트가 있는 경우(해당 서버가 표시됨) 이는 보통 서버가 올바르게 중지 또는 종료되지 않았으며 임시 파일에 아직 이벤트가 있음을 나타냅니다.

감사 상태 메트릭

메트릭	세부 정보
ADS 마지막 업데이트 날짜	CMS가 감사 이벤트에 대해 감사 대상을 마지막으로 폴링하기 시작한 날짜와 시간입니다.
감사 스레드 사용률	<p>CMS 감사자가 감사 대상으로부터 데이터를 수집하는 데 걸리는 폴링 주기의 백분율로, 나머지는 폴링 간의 휴지 시간입니다.</p> <p>이 비율이 100%에 도달하면 수치가 노란색으로 표시되는데, 이는 다음 폴링이 시작되려고 할 때 감사자가 여전히 감사 대상으로부터 데이터를 수집하고 있음을 의미합니다. 이로 인해 이벤트가 ADS에 연결되는 것이 지연될 수 있습니다.</p> <p>이런 일이 자주 또는 계속 발생하는 경우, ADS 데이터베이스가 더 높은 속도로(예: 더 빠른 네트워크 연결 또는 더 강력한 데이터베이스 하드웨어) 데이터를 수신하도록 배포를 업데이트하거나 시스템에서 추적하는 감사 이벤트 수를 줄이는 것이 좋습니다.</p>
마지막 폴링 주기 기간	<p>마지막 폴링 주기의 기간(초)입니다. 이전 폴링 주기 중 이벤트 데이터가 ADS에 연결되기까지 걸린 최대 지연 시간을 나타냅니다.</p> <ul style="list-style-type: none"> 이 수치가 20분(1,200초) 미만인 경우 녹색 배경에 나타납니다. 20분에서 2시간(7,200초) 사이인 경우에는 노란색 배경에 나타납니다. 2시간을 초과하는 경우에는 빨간색 배경에 나타납니다. <p>이 상태가 지속되고 지연이 너무 길다고 생각하는 경우, ADS 데이터베이스가 더 높은 속도로(예: 더 빠른 네트워크 연결 또는 더 강력한 데이터베이스 하드웨어) 데이터를 수신하도록 배포를 업데이트하거나 시스템에서 추적하는 감사 이벤트 수를 줄이는 것이 좋습니다.</p>
CMS 감사자	현재 감사자 역할을 하는 CMS의 이름입니다.
ADS 데이터베이스 연결 이름	CMS 감사자가 감사 데이터 저장소(ADS)에 연결하기 위해 현재 사용 중인 데이터베이스 연결의 이름입니다. SQL 서버의 경우 이는 ODBC 연결의 이름이 될 것입니다. 다른 데이터베이스 유형의 경우 이는 데이터베이스 이름 뒤에 서버 이름 및 연결 포트가 이어진 형태입니다.
ADS 데이터베이스 사용자 이름	CMS 감사자가 ADS 데이터베이스에 로그인하기 위해 사용 중인 사용자 이름입니다.

16.2.2 감사 이벤트 구성

CMC 감사 페이지를 이용해 감사를 활성화하고 전체 시스템에서 어떤 이벤트를 감사할지 선택할 수 있습니다.

특정 이벤트 또는 이벤트 세부 정보에 관심이 없는 경우 이를 선택하지 않은 상태로 두면 시스템 성능을 높일 수 있습니다.

참고:

BI 플랫폼을 설치할 때 ADS 연결을 구성하지 않기로 한 경우, 데이터베이스에 대한 연결을 설정한 후 감사 이벤트를 구성해야 합니다. 감사 데이터 저장소 구성 설정을 참조하십시오.

16.2.2.1 감사 이벤트 구성

1. 중앙 관리 콘솔에서 감사 탭을 선택합니다.
감사 페이지가 나타납니다.
2. 이벤트 설정 슬라이더를 원하는 수준으로 설정합니다.
다음 표에는 슬라이더의 4가지 다른 설정과 각 수준에서 캡처된 이벤트가 나와 있습니다.

감사 수준	캡처된 이벤트
해제	없음
최소	<ul style="list-style-type: none"> 로그온 로그아웃 권한 수정 사용자 지정 액세스 수준이 수정됨 감사 수정
기본값	<p>최소 이벤트와 다음이 포함됩니다.</p> <ul style="list-style-type: none"> 뷰 새로 고침 프롬프트 만들기 삭제 수정 저장 검색 편집 실행 배달
전체	<p>최소 및 기본값 이벤트와 다음이 포함됩니다.</p> <ul style="list-style-type: none"> 검색 트리거 범위 밖으로 드릴 페이지를 가져옴 LCM 구성 롤백 VMS 추가 VMS 검색 VMS 체크인 VMS 체크아웃 VMS 내보내기 VMS 잠금 VMS 잠금 해제 큐브 연결 MDAS 세션
사용자 지정	이벤트의 사용자 지정 집합을 선택합니다.

3. 사용자 지정을 선택한 경우 이벤트 설정 슬라이더 아래의 목록에서 캡처할 이벤트를 클릭합니다.
4. 이벤트 세부 정보 설정에서 이벤트와 함께 기록할 옵션 세부 정보를 클릭합니다. 세부 정보를 적게 기록하면 시스템 성능이 향상됩니다.

세부 정보	설명
쿼리	이 옵션을 설정하면 데이터베이스를 쿼리하는 모든 이벤트에 대해 쿼리 이벤트 세부 정보(세부 정보 ID 25)가 기록됩니다.
폴더 경로 세부 정보	이 옵션을 설정하면 다음 세부 정보가 캡처됩니다. <ul style="list-style-type: none"> 개체 폴더 경로(세부 정보 ID 71) 최상위 폴더 이름(세부 정보 ID 72) 컨테이너 폴더 경로(세부 정보 ID 64)
권한 세부 정보	이 옵션을 설정하면 다음 세부 정보가 캡처됩니다. <ul style="list-style-type: none"> 권한이 추가됨(세부 정보 ID 55) 권한이 제거됨(세부 정보 ID 56) 권한이 수정됨(세부 정보 ID 57)
사용자 그룹 세부 정보	이 옵션을 설정하면 다음 세부 정보가 캡처됩니다. <ul style="list-style-type: none"> 사용자 그룹 이름(세부 정보 ID 16) 사용자 그룹 ID(세부 정보 ID 15)
속성 값 세부 정보	이 옵션을 설정하면 개체 속성이 업데이트될 때 속성 값 이벤트 세부 정보(세부 정보 ID 29)가 캡처됩니다. CMC, BI 실행 패드 또는 SharePoint 이벤트에 대해서만 속성 값 이벤트 세부 정보가 생성됩니다.

5. 저장을 클릭합니다.

참고:

클라이언트 감사의 경우, 변경한 후 시스템에서 새 이벤트에 대한 데이터를 기록하기 시작하기까지 최대 2분이 걸릴 수 있습니다. 시스템에 변경 내용을 구현할 때 이 정도의 지연 시간을 고려해야 합니다.

16.2.3 감사 데이터 저장소 구성 설정

BI 플랫폼을 설치할 때 감사 데이터베이스를 설치하지 않기로 선택했거나 데이터베이스 위치 또는 설정을 변경하려는 경우, 다음 절차에 따라 ADS에 대한 연결을 구성할 수 있습니다.

또한 여기서 감사 이벤트가 데이터베이스에 보존되는 기간을 구성할 수도 있습니다.

이전 버전의 BI 플랫폼에서 업그레이드를 수행하고 Business Objects Metadata Manager(BOMM) 버전 3.x를 설치한 경우에는 ADS가 BOMM과 같은 데이터베이스 또는 테이블 공간을 사용하도록 구성하는 것이 좋습니다.

참고:

기존의 DB2 9.7 Workgroup을 감사 데이터베이스로 사용 중인 경우에는 데이터베이스 계정의 페이지 크기가 8kB 이상이 되도록 구성되어 있는지 확인하십시오.

16.2.3.1 감사 데이터 저장소 데이터베이스 설정 구성

1. 중앙 관리 콘솔에서 감사 탭을 선택합니다.
감사 페이지가 나타납니다.
2. 구성 머리글에서 ADS 데이터베이스 유형을 클릭합니다.
지원되는 데이터베이스 유형 목록이 나타납니다.
3. 감사 데이터를 위해 설치한 데이터베이스 유형을 선택합니다.
4. 연결 이름에서 감사 데이터베이스를 위해 구성된 연결의 이름을 입력합니다. SQL 데이터베이스의 경우 이 이름이 ODBC 이름이 되고, 다른 데이터베이스들은 모두 <서버 호스트 이름>,<포트>,<데이터베이스 이름>의 형식을 취합니다.
 - a. Windows 인증으로 Microsoft SQL 데이터베이스를 사용하는 경우 Windows 인증 옵션을 사용합니다.
5. 사용자 이름 및 암호 필드에는 데이터베이스에 로그인할 때 감사자 CMS에서 사용할 사용자 이름과 암호를 입력합니다.
6. 다음보다 오래된 이벤트 삭제(일) 필드에는 데이터베이스에 정보를 남길 일수를 입력합니다. (최소 값 1, 최대 값 109,500)

주의:

여기서 설정한 일수보다 오래된 데이터는 ADS에서 영구 삭제되며 복구할 수 없습니다. 장기적으로 레코드를 유지 관리하려는 경우 레코드를 주기적으로 보관 데이터베이스로 이동하는 방안을 고려해 볼 수 있습니다.

7. 데이터베이스 연결이 끊기는 경우, CMS 감사자를 데이터베이스에 수동으로 다시 연결하려면 ADS 자동 다시 연결 옵션을 선택 취소합니다.

참고:

이 옵션을 선택 취소하지 않으면 연결이 끊긴 경우 ADS에 대한 연결을 수동으로 다시 설정해야 합니다. CMS를 다시 시작하거나 ADS 자동 다시 연결을 활성화하면 됩니다. 이벤트가 기록되고 ADS를 다시 연결할 때까지 임시 파일에 저장된 상태로 남습니다.

8. 저장을 클릭합니다.
9. CMS를 다시 시작합니다.

16.3 감사 이벤트

다음 표에는 멤버 시스템의 모든 감사 이벤트 및 이러한 이벤트 각각에 대한 설명이 나와 있습니다. 이벤트를 만드는 서비스 유형 목록도 함께 제시됩니다.

이벤트	설명 및 이벤트 유형을 생성하는 서버/클라이언트
감사 수정	시스템의 감사 설정이 수정되었습니다. <ul style="list-style-type: none"> • 중앙 관리 서비스
만들기	새 개체가 시스템에 추가되었습니다. <ul style="list-style-type: none"> • Web Intelligence 처리 서비스 • Crystal Reports 보기 및 수정 서비스 • 중앙 관리 서비스 • Web Intelligence • 주기 관리
큐브 연결	OLAP 큐브 연결 작업이 수행되었습니다. <ul style="list-style-type: none"> • 다차원 분석 서비스
사용자 지정 액세스 수준이 수정됨	권한 정보가 수정되었습니다. <ul style="list-style-type: none"> • 중앙 관리 서비스
삭제	개체가 시스템에서 제거되었습니다. <ul style="list-style-type: none"> • 중앙 관리 서비스 • 주기 관리 서비스
배달	개체가 대상에 전송/배달되었습니다. <ul style="list-style-type: none"> • 대상 배달 예약 서비스 • Crystal Reports 예약 서비스 • Crystal Reports for Enterprise 예약 서비스 • Web Intelligence 게시 및 예약 서비스 • 중앙 관리 서비스 • 프로그램 예약 서비스
범위 밖으로 드릴	Web Intelligence 문서의 사용자가 보고서의 미리 로드된 데이터 범위 밖의 세 부 수준으로 드릴했습니다. <ul style="list-style-type: none"> • Web Intelligence • Web Intelligence 처리 서비스
편집	개체의 내용이 편집되었습니다. <ul style="list-style-type: none"> • Web Intelligence 처리 서비스 • 대시보드 서비스 • Web Intelligence

이벤트	설명 및 이벤트 유형을 생성하는 서버/클라이언트
LCM 구성	주기 관리 콘솔(LCM)의 구성 세부 정보가 변경되었습니다. <ul style="list-style-type: none"> • 주기 관리
로그온	사용자가 시스템에 로그인합니다. <ul style="list-style-type: none"> • 중앙 관리 서비스
로그아웃	사용자가 시스템에서 로그아웃합니다. <ul style="list-style-type: none"> • 중앙 관리 서비스
수정	개체의 파일 속성이 변경되었습니다. <ul style="list-style-type: none"> • Web Intelligence • 주기 관리 • 중앙 관리 서비스
MDAS 세션	다차원 분석 서비스 작업이 수행되었습니다. <ul style="list-style-type: none"> • 다차원 분석 서비스
페이지 검색	SAP BusinessObjects Web Intelligence 클라이언트가 리포지토리에서 추가 정보를 검색합니다. <ul style="list-style-type: none"> • Web Intelligence 처리 서비스
프롬프트	개체 프롬프트에 정보가 입력되었습니다. <ul style="list-style-type: none"> • Dashboard Design 캐시 서비스 • Live Office • Crystal Reports 예약 서비스 • Crystal Reports for Enterprise • Crystal Reports 캐시 서비스 • Web Intelligence 처리 서비스 • Web Intelligence
새로 고침	사용자의 요청으로 데이터베이스에서 개체의 데이터가 업데이트되었습니다. <ul style="list-style-type: none"> • Dashboard Design 캐시 서비스 • Live Office • Crystal Reports for Enterprise 예약 서비스 • Crystal Reports 캐시 서비스 • Crystal Reports 예약 서비스 • Web Intelligence 처리 서비스 • Web Intelligence
검색	개체가 리포지토리에서 검색되었습니다. <ul style="list-style-type: none"> • 중앙 관리 서비스
권한 수정	사용자, 그룹 또는 개체에 대한 보안 정보가 변경되었습니다. <ul style="list-style-type: none"> • 중앙 관리 서비스

이벤트	설명 및 이벤트 유형을 생성하는 서버/클라이언트
롤백	LifeCycle Manager를 사용하여 개체를 이전 버전으로 되돌립니다. <ul style="list-style-type: none"> 주기 관리
실행	작업이 실행되었습니다. <ul style="list-style-type: none"> 주기 관리 예약 서비스 대상 배달 예약 서비스 복제 서비스 Crystal Reports 예약 서비스 Crystal Reports for Enterprise 예약 서비스 Web Intelligence 예약 및 캐시 서비스 캐시 예약 서비스 프로그램 예약 서비스 주기 관리
저장	업데이트 또는 변경 후 개체가 저장되었습니다. <ul style="list-style-type: none"> Crystal Reports Enterprise 예약 서비스 Crystal Reports 캐시 서비스 다차원 분석 서비스 주기 관리 서비스 Web Intelligence 처리 서비스 Crystal Reports 보기 및 수정 서비스 Crystal Reports 예약 서비스
검색	검색이 수행되었습니다. <ul style="list-style-type: none"> 검색 서비스
트리거	파일 이벤트가 트리거되었습니다. <ul style="list-style-type: none"> 이벤트 서비스 중앙 관리 서비스
보기	개체를 확인했습니다. <ul style="list-style-type: none"> Web Intelligence Web Intelligence 처리 서비스 중앙 관리 콘솔 BI 실행 패드 Dashboard Design 캐시 서비스 Crystal Reports 캐시 서비스 Crystal Reports 보기 및 수정 서비스 대시보드 서비스 문서 열기
VMS 추가	개체가 LCM 버전 관리 시스템에 추가되었습니다. <ul style="list-style-type: none"> 주기 관리

이벤트	설명 및 이벤트 유형을 생성하는 서버/클라이언트
VMS 체크인	개체가 LCM 버전 관리 시스템에 체크인되었습니다. • 주기 관리
VMS 체크아웃	개체가 LCM 버전 관리 시스템에서 체크아웃되었습니다. • 주기 관리
VMS 내보내기	VMS에서 리소스를 내보냈습니다. • 주기 관리
VMS 잠금	VMS의 리소스가 잠금 상태입니다. • 주기 관리
VMS 잠금 해제	VMS의 리소스가 잠금 해제 상태입니다. • 주기 관리
VMS 검색	개체가 LCM 버전 관리 시스템에서 검색되었습니다. • 주기 관리

서비스 유형별 이벤트

서비스 유형	생성된 이벤트 유형
BI 실행 패드	보기
중앙 관리 서비스	<ul style="list-style-type: none"> • 감사 수정 • 만들기 • 사용자 지정 액세스 수준이 수정됨 • 삭제 • 배달 • 로그인 • 로그아웃 • 수정 • 검색 • 권한 수정 • 트리거
중앙 관리 콘솔	보기
Crystal Reports 캐시 서비스	<ul style="list-style-type: none"> • 프롬프트 • 새로 고침 • 저장 • 보기

서비스 유형	생성된 이벤트 유형
Crystal Reports for Enterprise 예약 서비스	<ul style="list-style-type: none"> • 배달 • 프롬프트 • 새로 고침 • 실행 • 저장
Crystal Reports 예약 서비스	<ul style="list-style-type: none"> • 배달 • 프롬프트 • 새로 고침 • 실행 • 저장
Crystal Reports 보기 및 수정 서비스	<ul style="list-style-type: none"> • 만들기 • 저장 • 보기
Dashboard Design 캐시 서비스	<ul style="list-style-type: none"> • 프롬프트 • 새로 고침 • 보기
대시보드 서비스	<ul style="list-style-type: none"> • 편집 • 보기
대상 배달 예약 서비스	<ul style="list-style-type: none"> • 배달 • 실행
이벤트 서비스	트리거
LCM 예약 서비스	실행
LCM 서비스	<ul style="list-style-type: none"> • 만들기 • 삭제 • LCM 콘솔 구성 • 수정 • 롤백 • 실행 • 저장 • 버전 • VMS 추가 • VMS 체크인 • VMS 체크아웃 • VMS 잠금 • VMS 잠금 해제

서비스 유형	생성된 이벤트 유형
Live Office	<ul style="list-style-type: none"> 프롬프트 새로 고침
다차원 분석 서비스	<ul style="list-style-type: none"> MDAS 큐브 연결 MDAS 세션 저장
문서 열기	보기
프로그램 예약 서비스	<ul style="list-style-type: none"> 배달 실행
게시 예약 서비스	실행
복제 서비스	실행
검색 서비스	검색
Web Intelligence	<ul style="list-style-type: none"> 만들기 범위 밖으로 드릴 편집 수정 프롬프트 새로 고침 저장 보기
Web Intelligence 처리 서비스	<ul style="list-style-type: none"> 만들기 범위 밖으로 드릴 편집 페이지 검색 프롬프트 새로 고침 저장 보기
Web Intelligence 예약 및 게시 서비스	<ul style="list-style-type: none"> 배달 실행

이벤트 속성 및 세부 정보

BI 플랫폼에서 기록하는 각 이벤트에는 일련의 이벤트 속성 및 세부 정보가 포함되어 있습니다.

이벤트 속성은 항상 이벤트와 함께 생성되지만 일부의 경우에는 정보가 특정 이벤트에 해당하지 않을 경우 값을 갖지 않을 수 있습니다. ADS에서 이벤트 속성은 이벤트를 저장하는 테이블에 포함되어 있으므로 보고서를 만들 때 이벤트를 정렬 또는 그룹화하는 데 사용할 수 있습니다.

이벤트 세부 정보는 이벤트 속성에 포함되지 않은 이벤트에 대한 추가 정보를 기록합니다. 이벤트 세부 정보가 특정 이벤트와 관련이 없을 경우 해당 이벤트 세부 정보는 생성되지 않습니다. 공통 이벤트 세부 정보는 관련된 모든 이벤트 유형에 대해 생성될 수 있습니다. 추가 이벤트 세부 정보는 특정 이벤트 유형에 대해 생성됩니다. 예를 들어, 프롬프트 이벤트는 이벤트 세부 정보에 프롬프트에 대해 입력한 값을 기록하지만, 다른 이벤트 유형은 프롬프트 값 이벤트 세부 정보를 생성하지 않습니다. ADS에서 세부 정보는 부모 이벤트에 연결되는 별도의 테이블에 저장됩니다.

다국어 데이터(예: 개체 또는 폴더 이름)는 감사자 CMS의 로캘에 해당하는 기본 언어로 기록됩니다.

16.3.1 감사 이벤트 및 세부 정보

다음 단원에서는 모든 이벤트 유형을 소개하고, 이어서 속성 설명 및 이러한 이벤트에만 해당하는 이벤트 세부 정보에 대해 설명합니다. 단원 앞쪽에는 모든 이벤트 유형에 공통적으로 사용되는 속성 및 세부 정보가 나열됩니다.

참고:

일부 클라이언트 프로그램의 경우 고유한 이벤트가 없어 공통 이벤트와 플랫폼 이벤트에 의존하여 작업 관련 정보를 캡처합니다.

16.3.1.1 전역 이벤트 속성 및 세부 정보

다음 표에는 모든 이벤트에 대해 기록되는 속성 및 이벤트 세부 정보가 나와 있습니다.

이벤트 속성	설명
Event_ID	고유한 이벤트 식별자입니다.
Client_Type_ID	이벤트를 수행한 응용 프로그램 유형에 대한 식별자입니다.
Service_Type_ID	이벤트를 트리거한 서비스 또는 응용 프로그램의 ID를 표시합니다.
Start_Time	이벤트가 시작된 날짜 및 시간(GMT)입니다.
Duration	이벤트 기간(밀리초)입니다.
Session_ID	이벤트가 트리거된 세션의 ID입니다.
Event_Type_ID	이벤트 유형입니다(예: 보기 이벤트의 경우 1002).

이벤트 속성	설명
Status_ID	작업 성공 여부를 기록합니다("0" = 성공, "1" = 실패). 일부 이벤트의 경우 추가 상태 유형이 있습니다. 이에 대해서는 해당 이벤트에 대한 설명에 자세히 설명되어 있습니다.
Object_ID	영향을 받는 개체의 CUID입니다(해당하는 경우). 트리거 이벤트를 위한 경고 이벤트의 CUID입니다. 참고: CMS 리포지토리에 저장되지 않은 모든 개체의 ID는 0입니다. CMS 데이터베이스에 아직 저장되지 않은 문서 또는 클라이언트 컴퓨터 로컬에 저장된 문서 등이 이러한 개체에 해당합니다. 이러한 개체는 Object_Name 속성으로 구별해야 합니다.
User_ID	이벤트를 수행한 사용자의 CUID입니다.
User_Name	이벤트를 수행한 사용자의 사용자 이름입니다.
Object_Name	영향을 받는 개체의 이름입니다(해당하는 경우). 트리거 이벤트를 위한 경고 이벤트의 이름입니다.
Object_Type_ID	개체 유형(예: 문서, 폴더 등)의 CUID입니다.
Object_Folder_Path	CMS 리포지토리에서 영향을 받는 개체가 있는 위치에 대한 전체 폴더 경로입니다 (예: Sales/North America/East Coast).
Folder_ID	개체가 저장되어 있는 폴더의 CUID입니다.
Top_Folder_Name	영향을 받는 개체가 저장되어 있는 최상위 폴더의 이름입니다. 예를 들어 개체가 Sales/North America/East Coast에 있다면 값은 Sales입니다.
Top_Folder_ID	영향을 받는 개체가 있는 최상위 폴더의 CUID입니다. 예를 들어 개체가 Sales/North America/East Coast에 있다면 값은 Sales 폴더의 CUID입니다.
Cluster ID	이벤트를 기록한 CMS 클러스터의 CUID입니다.
Action_ID	단일 사용자 작업으로 시작된 일련의 이벤트를 함께 묶는 데 사용할 수 있는 고유 식별자입니다.

이벤트 세부 정보	ID	설명
오류	1	작업이 실패할 경우에만 기록됩니다. 시도할 때 발생하는 오류 메시지의 텍스트입니다.
요소 ID	2	컨테이너 개체(예: Live Office 문서 또는 비즈니스 대시보드)에 있는 개체의 이름입니다.
요소 이름	3	컨테이너 개체(예: Live Office 문서 또는 비즈니스 대시보드)에 있는 개체에 대해 생성된 ID입니다.
요소 유형 ID	5	보고 있거나 수정 중인 컨테이너 개체에 있는 개체의 유형입니다. 해당하는 경우에만 생성됩니다.

이벤트 세부 정보	ID	설명
상위 문서 ID	12	<ul style="list-style-type: none"> 문서 인스턴스의 경우 상위 문서의 CUID입니다. 상위 문서의 경우 자체 CUID입니다.
유니버스 ID	13	문서 또는 개체에서 사용하는 유니버스의 CUID입니다. 유니버스가 둘 이상인 경우 각 유니버스마다 이벤트 세부 정보가 생성됩니다.
유니버스 이름	14	문서 또는 개체에서 사용하는 유니버스의 이름입니다. 유니버스가 둘 이상인 경우 각 유니버스마다 이벤트 세부 정보가 생성됩니다.
사용자 그룹 이름	15	작업을 수행하는 사용자가 속해 있는 사용자 그룹 이름입니다. 사용자가 여러 그룹에 속해 있을 경우 각 그룹마다 이벤트 세부 정보가 생성됩니다.
사용자 그룹 ID	16	작업을 수행하는 사용자가 속해 있는 사용자 그룹 ID입니다. 사용자가 여러 그룹에 속해 있을 경우 각 그룹마다 이벤트 세부 정보가 생성됩니다.

16.3.1.2 공통 이벤트

다음 이벤트 유형은 모든 SAP BusinessObjects XI 구성 요소에 공통입니다.

보기

사용자가 문서/개체를 보았습니다.

- 이벤트 유형 ID: 1002

이벤트 세부 정보	ID	설명
크기	17	이벤트의 영향을 받는 개체의 크기(바이트)입니다.
컨테이너 ID	32	개체가 있는 컨테이너 개체(예: 대시보드)의 CUID입니다(해당하는 경우).
컨테이너 유형	33	개체 컨테이너의 응용 프로그램 유형입니다(해당하는 경우).

새로 고침

데이터베이스에서 개체가 새로 고쳐졌습니다.

- 이벤트 유형 ID: 1003

이벤트 세부 정보	ID	설명
크기	17	이벤트의 영향을 받는 개체의 크기(바이트)입니다. 참고: 요청 시 보기 Crystal Reports의 경우 0으로 설정됩니다.
행 수	63	데이터베이스 서버에서 반환된 레코드 수입니다. 참고: 요청 시 보기 Crystal Reports의 경우 0으로 설정됩니다.
쿼리	25	데이터를 새로 고칠 때 사용한 SQL 쿼리를 기록합니다(선택적, CMC에 설정됨).
유니버스 개체 이름	31	문서 또는 개체에서 사용하는 유니버스의 이름입니다. 문서 또는 개체에서 액세스하는 각 유니버스마다 이벤트 세부 정보가 생성됩니다.
문서 범위	36	게시 설정에 있는 지정된 문서 범위에 대한 정보를 기록합니다(예: 국가=미국, 역할=관리자). 게시 워크플로에만 적용할 수 있습니다.
게시 인스턴스 ID	37	해당 게시 인스턴스의 ID입니다. 게시 워크플로에만 적용할 수 있습니다.
Live Office 개체 유형	10701	Live Office 문서(예: Crystal 보고서)에서 새로 고쳐지는 개체의 유형을 식별합니다. 이 속성은 Live Office 문서에 대해서만 생성됩니다.

프롬프트

프롬프트에 대한 값을 입력했습니다.

- 이벤트 유형 ID: 1004

이벤트 세부 정보	ID	설명
프롬프트 이름	26	프롬프트에 할당된 이름입니다(예: 날짜). 문서 또는 개체의 각 프롬프트에 대해 별도의 세부 정보가 생성되며, 이러한 세부 정보는 그룹화됩니다.
프롬프트 값	27	프롬프트에 입력한 값입니다. 입력한 값마다 별도의 세부 정보가 생성됩니다. 이러한 세부 정보는 함께 그룹화되어 다시 프롬프트 이름과 관련됩니다.
문서 범위	36	지정된 문서 범위에 대한 정보입니다(예: 국가=미국, 역할=관리자).
게시 인스턴스 ID	37	해당 게시 인스턴스의 ID입니다. 게시 워크플로에만 적용됩니다.
설계 시 이름	90	설계 당시 Xcelsius 문서의 이름입니다. 이 속성은 Xcelsius 새로 고침 또는 프롬프트를 포함하는 Xcelsius 또는 Live Office 문서에 대해서만 생성됩니다.
Live Office 개체 유형	10701	Live Office 문서(예: Crystal 보고서)에서 새로 고쳐지는 개체의 유형을 식별합니다. 이 속성은 포함된 개체가 프롬프트를 포함하는 Live Office 문서에 대해서만 생성됩니다.

만들기

사용자가 개체를 만들었습니다.

- 이벤트 유형 ID: 1005

이벤트 세부 정보	ID	설명
크기	17	이벤트의 영향을 받는 개체의 크기(바이트)입니다.
덮어쓰기	21	새 문서 또는 개체이거나 문서 또는 개체가 기존 개체를 덮어쓰는 경우에 기록됩니다(0= 새 문서 또는 개체, 1= 기존 문서 또는 개체 덮어쓰기).
열 때 새로 고침	23	열 때 문서 또는 개체가 자동으로 새로 고쳐지는 경우에 기록됩니다(0= 새로 고치지 않음, 1= 열 때 새로 고침). 해당하는 경우에만 생성됩니다.
설명	24	문서 또는 개체의 설명 필드에 정보를 기록합니다.

삭제

사용자가 개체를 삭제했습니다.

- 이벤트 유형 ID: 1006

수정

사용자가 개체의 파일 속성을 수정했습니다.

- 이벤트 유형 ID: 1007

이벤트 세부 정보	ID	설명
속성 이름	28	수정된 속성의 이름입니다. 수정된 각 속성마다 이벤트 세부 정보가 생성됩니다.
속성 값	29	문서 또는 개체의 수정된 속성의 새 값입니다. 수정된 각 속성마다 이벤트 세부 정보가 생성됩니다.

저장

문서 또는 개체를 기존 형식 또는 다른 형식으로 CMS 리포지토리에 로컬 또는 원격으로 저장하거나 내보냅니다.

- 이벤트 유형 ID: 1008
- 상태:
 - "0"은 개체가 성공적으로 로컬에 저장되었음을 나타냅니다.
 - "1"은 저장 시도가 실패했음을 나타냅니다.
 - "2"는 개체가 성공적으로 리포지토리에 내보내졌거나 저장되었음을 나타냅니다.
 - "3"은 개체가 성공적으로 새 형식으로 내보내졌거나 저장되었음을 나타냅니다.

이벤트 세부 정보	ID	설명
크기	17	저장했거나 내보낸 개체의 크기(바이트)입니다.
파일 이름	18	문서 또는 개체를 저장할 때 사용한 전체 이름입니다. 클라이언트 응용 프로그램에서 파일을 로컬에 저장한 경우 이름도 파일 경로에 포함됩니다.
덮어쓰기	21	새 문서 또는 개체이거나 문서 또는 개체가 기존 파일을 덮어쓰는 경우에 기록됩니다. 0= 새 문서 또는 개체, 1= 기존 문서 또는 개체 덮어쓰기
형식	22	저장했거나 내보낸 문서의 형식을 지정합니다. 이 형식은 일반적인 세 자 파일 확장명(예: Microsoft Word 파일의 경우 ".doc", 또는 Adobe PDF 파일의 경우 ".pdf")으로 표시됩니다.
열 때 새로 고침	23	열 때 문서 또는 개체가 자동으로 새로 고쳐지는 경우에 기록됩니다("0"= 새로 고치지 않음, "1"= 열 때 새로 고침). 해당하는 경우에만 기록됩니다.

검색

검색이 수행되었습니다.

- 이벤트 유형 ID: 1009

이벤트 세부 정보	ID	설명
키워드	19	수행된 검색의 키워드입니다.
범주	20	검색에 사용된 범주입니다(해당하는 경우).
행 수	63	검색을 통해 반환되는 행 수입니다.

편집

사용자가 개체의 내용을 편집했습니다.

- 이벤트 유형 ID: 1010

이벤트 세부 정보	ID	설명
크기	17	이벤트의 영향을 받는 개체의 크기(바이트)입니다.
쿼리	25	편집 시 SQL 쿼리를 수정한 경우 새 쿼리가 기록됩니다. 이 설정은 선택적 설정이며 CMC 감사 페이지에서 선택할 수 있습니다.
유니버스 개체 이름	31	문서 또는 개체에서 사용하는 유니버스의 이름입니다. 문서 또는 개체에서 액세스하는 각 유니버스마다 별도의 세부 정보가 생성됩니다.
컨테이너 ID	32	개체를 사용하는 컨테이너(예: 대시보드)의 CUID입니다(해당하는 경우).
컨테이너 유형	34	개체 컨테이너의 응용 프로그램 유형입니다(해당하는 경우).
컨테이너 폴더 경로	64	개체 컨테이너의 폴더 경로입니다(해당하는 경우).

실행

작업이 실행되었습니다.

- 이벤트 유형 ID: 1011
- 상태:
 - "0"은 작업이 성공했음을 나타냅니다.
 - "1"은 작업이 실패했음을 나타냅니다.
 - "2"는 작업이 실패했지만 다시 시도할 것임을 나타냅니다.
 - "3"은 작업이 취소되었음을 나타냅니다.

이벤트 세부 정보	ID	설명
크기	17	실행된 문서의 크기(바이트)입니다.
문서 범위	36	지정된 문서 범위에 대한 정보입니다(예: 국가=미국, 역할=관리자).

배달

개체가 배달되었습니다.

- 이벤트 유형 ID: 1012

이벤트 세부 정보	ID	설명
크기	17	배달된 개체의 크기(바이트)입니다.
대상 유형	35	문서 또는 개체 인스턴스의 대상입니다. 예를 들면 전자 메일, FTP, 관리되지 않는 디스크, 받은 파일함, 프린터 등이 있습니다.
문서 범위	36	지정된 문서 범위에 대한 정보입니다(예: 국가=미국, 역할=관리자).
게시 인스턴스 ID	37	문서 또는 개체 인스턴스의 CUID입니다.
도메인	38	전자 메일을 통해 배포된 문서/개체의 SMTP 서버 도메인 이름을 기록합니다(해당하는 경우).
호스트 이름	39	전자 메일 또는 FTP를 통해 배포된 문서/개체의 SMTP 또는 FTP 호스트의 이름을 기록합니다(해당하는 경우).
포트	40	전자 메일 또는 FTP를 통해 배포된 문서/개체의 SMTP 또는 FTP 서버 도메인 포트를 기록합니다(해당하는 경우).
보낸 사람 주소	41	전자 메일을 통해 배포된 문서/개체의 보낸 사람 주소를 기록합니다(해당하는 경우).
받는 사람 주소	42	전자 메일을 통해 배포된 문서/개체의 받는 사람 주소를 기록합니다(해당하는 경우). 받는 사람, 참조 또는 숨은 참조 필드에 주소를 포함할지 여부도 지정합니다. 지정된 받는 사람마다 이벤트 세부 정보가 생성됩니다.
파일 이름	18	전자 메일 또는 FTP를 통해 배포되었거나 Business Objects 배포에 포함되지 않은 디스크에 직접 기록된 문서/개체의 파일 이름을 기록합니다.
계정 이름	45	다음 중 하나를 기록합니다. <ul style="list-style-type: none"> • 받은 파일함으로 배달되는 개체의 경우, BusinessObjects 사용자 계정 이름 목록 • FTP로 배달되는 개체의 경우, FTP 계정 이름 • 관리되지 않는 디스크로 배달되는 개체의 경우, 사용된 로그인 계정 이름 • SMTP로 배달되는 개체의 경우, SMTP 서버에 사용된 로그인 계정

이벤트 세부 정보	ID	설명
프린터 이름	46	문서 또는 개체를 배달한 프린터의 이름입니다(해당하는 경우).
인쇄 매수	47	문서 또는 개체의 인쇄 매수입니다(해당하는 경우).
받는 사람 이름	48	문서 또는 개체 받는 사람의 사용자 이름입니다. 지정된 받는 사람마다 이벤트 세부 정보가 생성됩니다.
경고 이벤트 ID	92	경고 이벤트의 CUID입니다. 이 속성은 이벤트가 경고에 의해 프롬프트된 경우에만 생성됩니다.
경고 이벤트 이름	93	경고 이벤트의 이름입니다. 이 속성은 이벤트가 경고에 의해 프롬프트된 경우에만 생성됩니다.
배달 유형	35	배달이 시작된 방식을 나타냅니다. <ul style="list-style-type: none"> "0"은 예약되었음을 나타냅니다. "1"은 대상에 전송되었음을 나타냅니다. "2"는 게시되었음을 나타냅니다. "3"은 경고가 트리거되었음을 나타냅니다.

검색

개체가 CMS에서 검색되었습니다.

- 이벤트 유형 ID: 1013

로그온

사용자가 로그인합니다.

- 이벤트 유형 ID: 1014
- 상태:
 - "0"은 동시 사용자 라이선스 로그온이 성공했음을 나타냅니다.
 - "1"은 로그인 시도가 실패했음을 나타냅니다.
 - "2"는 명명된 사용자 라이선스 로그온이 성공했음을 나타냅니다.
 - "3"은 비사용자(시스템) 로그인이 성공했음을 나타냅니다.

이벤트 세부 정보	ID	설명
동시 사용자 수	50	이벤트가 트리거된 당시 시스템에 있던 사용자의 수입니다.
클라이언트에서 보고한 호스트 이름	51	클라이언트에서 보고한 클라이언트의 호스트 이름입니다.
서버에서 확인된 호스트 이름	52	서버에서 확인된 클라이언트의 호스트 이름입니다. 클라이언트 호스트 이름을 확인할 수 없는 경우 값이 기록되지 않습니다.
클라이언트에서 보고한 IP 주소	53	클라이언트에서 보고한 클라이언트의 IP 주소입니다.
서버에서 확인된 IP 주소	54	서버에서 확인된 클라이언트의 IP 주소입니다. 클라이언트 IP를 확인할 수 없는 경우 값이 기록되지 않습니다.

로그아웃

사용자가 로그오프합니다.

- 이벤트 유형 ID: 1015

이벤트 세부 정보	ID	설명
동시 사용자 수	50	이벤트가 트리거된 당시 시스템에 있던 동시 사용자의 수입니다.

트리거

파일 이벤트가 트리거되었습니다.

- 이벤트 유형 ID: 10016

이벤트 세부 정보	ID	설명
파일 이름	17	이벤트를 모니터링 및 트리거하는 파일의 이름입니다.

16.3.1.3 플랫폼 이벤트

다음 이벤트는 BI 플랫폼 플랫폼에서만 발생합니다.

권한 수정

개체에 대한 하나 이상의 권한이 수정되었습니다.

- 이벤트 유형 ID: 10003

이벤트 세부 정보	ID	설명
권한 추가	55	추가된 권한의 종류, 새 권한의 범위(대상 개체) 및 권한이 적용된 개체 유형입니다. 이 정보의 구조는 added right=Export; new value=Granted; scope=Current object; applicable object type=all object types와 같이 구성됩니다.
권한 제거	56	제거된 권한의 종류, 새 권한의 범위(대상 개체) 및 권한이 적용된 개체 유형입니다. 이 정보의 구조는 removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types와 같이 구성됩니다.
권한 수정	57	수정된 권한의 종류, 새 권한의 범위(대상 개체) 및 권한이 적용된 개체 유형입니다. 이 정보의 구조는 modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types와 같이 구성됩니다.

사용자 지정 액세스 수준 수정

사용자 지정 액세스 수준이 수정되었습니다.

- 이벤트 유형 ID: 10004

이벤트 세부 정보	ID	설명
권한 추가	55	추가된 권한의 종류, 새 권한의 범위(대상 개체) 및 권한이 적용된 개체 유형입니다. 이 정보의 구조는 added right=Export; new value=Granted; scope=Current object; applicable object type=all object types와 같이 구성됩니다.
권한 제거	56	제거된 권한의 종류, 새 권한의 범위(대상 개체) 및 권한이 적용된 개체 유형입니다. 이 정보의 구조는 removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types와 같이 구성됩니다.
권한 수정	57	수정된 권한의 종류, 새 권한의 범위(대상 개체) 및 권한이 적용된 개체 유형입니다. 이 정보의 구조는 modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types와 같이 구성됩니다.

감사 수정

시스템의 감사 설정이 변경되었습니다.

- 이벤트 유형 ID: 10006

이벤트 세부 정보	ID	설명
이벤트 유형 ID	58	활성화 또는 비활성화된 감사 이벤트 유형의 ID를 기록합니다. 한 번에 여러 개의 이벤트 유형이 활성화되거나 비활성화되면 각 이벤트 유형별로 이벤트 세부 정보가 작성됩니다.
작업	59	활성화 또는 비활성화된 감사 이벤트를 기록합니다.
새 감사 수준	60	세부 정보의 감사 수준이 변경되면 새 수준 설정을 기록합니다(해제, 최소, 기본값 등).
기존 감사 수준	61	세부 정보의 감사 수준이 변경되면 이전 수준 설정을 기록합니다(해제, 최소, 기본값 등).
감사 옵션	62	선택적 세부 정보가 활성화 또는 비활성화되면 수정된 세부 정보와 활성화, 비활성화 여부를 기록합니다. 한 번에 여러 개의 세부 정보가 활성화되거나 비활성화되면 각 수정된 세부 정보별로 세부 정보 레코드가 만들어집니다.
ADS 연결	70	감사 데이터 저장소에 대한 연결이 변경되면 DBType=Oracle,DB Name=MyADS,Username=USR1,Password="*****",SSO=off,DBReconnect=on과 같은 형식을 사용하여 새 연결 설정을 기록합니다. 변경된 세부 정보만 기록됩니다. 예를 들어 사용자 이름만 업데이트된 경우 Username="new"만 기록됩니다. 참고: 데이터베이스에서 암호 정보는 항상 * 기호로 표시됩니다.
자동 삭제 간격	105	이 세부 정보에는 감사 CMC 페이지의 다음보다 오래된 이벤트 삭제 필드 변경 내용이 기록됩니다. 감사 정보를 며칠 동안 ADS에 유지할지를 관리하는 항목입니다.

16.3.1.4 SAP BusinessObjects Web Intelligence 이벤트

다음은 SAP BusinessObjects Web Intelligence 구성 요소에만 해당되는 이벤트입니다.

범위 밖으로 드릴

사용자가 보고서 범위 밖으로 드릴했습니다.

- 이벤트 유형 ID: 10201

이벤트 세부 정보	ID	설명
개체 인스턴스	11	이벤트가 예약된 업데이트로 인한 것인지 아니면 개체를 보는 사용자로 인한 것인지 기록합니다("0"은 개체를 보는 사용자, "1"은 개체의 예약된 새로 고침).
행 수	63	데이터베이스 서버에서 반환된 행의 수입니다.
쿼리	25	데이터를 새로 고칠 때 사용한 쿼리를 기록합니다(선택적, CMC에 설정).
유니버스 개체 이름	31	문서에서 사용하는 유니버스의 이름입니다. 문서가 액세스하는 유니버스별로 인스턴스가 기록됩니다.
유니버스 개체 ID	32	문서에서 사용하는 유니버스의 CUID입니다. 문서가 액세스하는 유니버스별로 인스턴스가 기록됩니다.

페이지 검색

Web Intelligence 문서 페이지가 검색됩니다.

- 이벤트 유형 ID: 10202

16.3.1.5 SAP BusinessObjects Analysis, OLAP용 에디션 이벤트

MDAS 세션

MDAS 세션 작업이 수행되었습니다.

- 이벤트 유형 ID: 10300
- 상태:
 - "0" = 새 세션이 시작되었습니다.
 - "1" = 새 세션을 시작하지 못했습니다.
 - "2" = 기존 세션이 종료되었습니다.

MDAS 큐브 연결

큐브 연결 작업이 수행되었습니다.

- 이벤트 유형 ID: 10301
- 상태:
 - "0" = 새 연결이 시작되었습니다.
 - "1" = 새 연결을 시작하지 못했습니다.
 - "2" = 기존 연결이 종료되었습니다.

이벤트 세부 정보	ID	설명
연결 ID	94	연결의 고유 ID입니다.
연결 이름	95	연결의 이름입니다.
공급자 유형	96	큐브에 대한 공급자의 유형입니다.
큐브 이름	97	사용되는 큐브의 전체 이름입니다.

16.3.1.6 SAP BusinessObjects 주기 관리 콘솔 이벤트

다음 이벤트는 SAP BusinessObjects용 주기 관리 구성 요소에만 있습니다.

SAP BusinessObjects 주기 관리 콘솔 공통 세부 정보

모든 주기 관리 이벤트에는 다음과 같은 추가 이벤트 세부 정보가 있습니다.

이벤트 세부 정보	ID	설명
요소 클러스터	6	주기 관리 콘솔이 다른 클러스터에 있는 개체에 대해 작업을 수행할 때 관련된 클러스터의 CUID입니다. 각 관련 클러스터에 대한 이벤트 세부 정보가 만들어집니다.
요소 주식	7	개체에 대한 추가 정보입니다.
기본 요소	8	요소가 기본 요소이면 이 세부 정보는 "1"로 설정되고 종속 요소이면 "0"으로 설정됩니다.
요소 상태	9	작업 요소에 오류가 발생하면 이 세부 정보는 "1"로 그렇지 않으면 "0"으로 설정됩니다.
작업	10	추가, 삭제, 수정과 같은 수행되는 작업의 종류를 나타냅니다

SAP BusinessObjects 주기 관리 콘솔 구성

주기 관리 구성이 변경되었습니다.

- 이벤트 유형 ID: 10900

이벤트 세부 정보	ID	설명
구성	100	사용자가 주기 관리 콘솔 구성을 봅니다. 구성에는 쉼표로 구분되는 값의 쌍이 표시됩니다(예: rollback settings=enabled, port=900).
구성 전	101	개체의 주기 관리 콘솔 설정이 수정되면 이전 구성 설정을 기록합니다. 구성과 동일한 형식을 사용합니다.
구성 후	102	개체의 주기 관리 콘솔 설정이 수정되면 새 구성 설정을 기록합니다. 구성과 동일한 형식을 사용합니다.
VMS 유형	10900	버전 관리 시스템의 유형입니다.

롤백

개체가 이전의 버전 관리 시스템(VMS) 버전으로 롤백되었습니다.

- 이벤트 유형 ID: 10901

VMS 추가

VMS에 리소스가 추가되었습니다.

- 이벤트 유형 ID: 10902

이벤트 세부 정보	ID	설명
버전	104	버전 관리 시스템에 문서의 버전 번호를 기록합니다.

VMS 검색

VMS에서 리소스가 검색되었습니다.

- 이벤트 유형 ID: 10903

이벤트 세부 정보	ID	설명
삭제된 개체 복원	103	검색된 개체가 시스템에서 삭제되었는지 나타냅니다. "0"은 개체가 삭제되지 않았음을 "1"은 삭제되었음을 나타냅니다.
버전	104	VMS에 문서의 버전 번호를 기록합니다.

VMS 체크인

VMS에 리소스가 체크인되었습니다.

- 이벤트 유형 ID: 10904

이벤트 세부 정보	ID	설명
버전	104	VMS에 문서의 버전 번호를 기록합니다.

VMS 체크아웃

VMS에서 리소스가 체크아웃되었습니다.

- 이벤트 유형 ID: 10905

이벤트 세부 정보	ID	설명
버전	104	VMS에 문서의 버전 번호를 기록합니다.

VMS 내보내기

VMS에서 리소스를 내보냈습니다.

- 이벤트 유형 ID: 10906

이벤트 세부 정보	ID	설명
버전	104	VMS에 문서의 버전 번호를 기록합니다.

VMS 잠금

VMS의 리소스가 잠겨 사용자는 이를 편집할 수 없습니다.

- 이벤트 유형 ID: 10907

이벤트 세부 정보	ID	설명
버전	104	VMS에 문서의 버전 번호를 기록합니다.
잠금 사람	10901	이 작업을 수행한 사용자의 이름입니다.

VMS 잠금 해제

VMS의 리소스가 잠금 해제되어 편집 가능합니다.

- 이벤트 유형 ID: 10908

이벤트 세부 정보	ID	설명
버전	104	VMS에 문서의 버전 번호를 기록합니다.
잠금을 해제한 사람	10901	이 작업을 수행한 사용자의 이름입니다.

장17 플랫폼 검색

17.1 개요

플랫폼 검색을 사용하면 SAP BusinessObjects Business Intelligence 플랫폼 리포지토리 내에서 콘텐츠를 검색할 수 있습니다. 플랫폼 검색은 검색 결과를 범주별로 그룹화하고 연관성에 따라 순위를 지정하여 검색 결과를 구체화합니다. 또한 클라이언트 응용 프로그램 및 플랫폼 검색 간에 인터페이스로 동작하는 공용 SDK를 지원합니다.

이 SAP BusinessObjects Business Intelligence 플랫폼 버전에서는 다음 기능을 통해 플랫폼 검색이 향상되었습니다.

- SAP BusinessObjects Business Intelligence 플랫폼 및 탐색기 콘텐츠 모두 검색
- 기존 문서를 찾을 수 없는 경우 문서를 만들기 위한 쿼리 제안
- 연속 인덱싱과 일정 기반 인덱싱 모두 지원
- 클러스터된 환경에서 인덱싱 지원
- 인덱싱 수준 설정 및 수정
- 고급 검색 구성 옵션 제공
- 다국어 검색 및 인덱싱 지원
- 고급 검색 구문 제공
- 메타데이터, 콘텐츠 및 동적 패킷 지원
- 시스템 부하에 따라 자동 복구 지원

참고:

이전 버전에서 새 버전으로 마이그레이션 하는 경우 인덱스는 마이그레이션되지 않습니다.

17.2 아키텍처

이 단원에서는 플랫폼 검색 아키텍처에 대한 개요를 제공하고 각 구성 요소의 역할에 대해 간략히 설명합니다. 플랫폼 검색은 인덱싱 및 검색에 사용되는 다양한 구성 요소를 내부적으로 호스팅하는 적

응형 처리 서버에서 호스팅됩니다. 또한 인덱스 유형에 따라, 즉 일정 기반 또는 연속적으로 인덱싱을 수행합니다.

플랫폼 검색에는 두 개의 기본 프로세스인 인덱싱과 검색 프로세스가 포함됩니다. 또한 자체 자동 복구 메커니즘도 있습니다.

인덱싱

인덱싱은 다음 작업을 순차적으로 처리하는 연속적인 프로세스입니다.

1. 크롤링: 크롤링은 CMS 리포지토리를 폴링하여 게시, 수정 또는 삭제된 개체를 식별하는 메커니즘으로, 두 가지 방법, 즉 연속 크롤링 및 예약된 크롤링을 통해 수행할 수 있습니다.

연속 크롤링 및 예약된 크롤링에 대한 자세한 내용은 관련 항목의 응용 프로그램 속성 구성 항목을 참조하십시오.

2. 추출: 추출은 문서 유형에 따라 추출기를 호출하는 메커니즘입니다. 리포지토리에서 사용 가능한 모든 문서 종류에는 전용 추출기가 있습니다. 새 문서 종류를 검색할 수 있도록 새 추출기 플러그인을 정의할 수도 있으며, 많은 양의 레코드를 포함하는 큰 문서에서 콘텐츠를 추출할 수 있도록 이러한 추출기를 각각 확장할 수도 있습니다.

다음과 같은 추출기가 지원됩니다.

- 메타데이터 추출기
- Crystal 보고서 추출기
- Web Intelligence 추출기
- 유니버스 추출기
- 타사 추출기(MS Office 2003, 2007 및 PDF 문서)

검색 가능한 문서 유형에 대한 자세한 내용은 관련 항목에서 검색 가능한 콘텐츠 유형 항목을 참조하십시오.

3. 인덱싱: 인덱싱은 Apache Lucene Engine이라는 타사 라이브러리를 통해 추출된 모든 콘텐츠를 인덱싱하는 메커니즘입니다. 인덱싱에 걸리는 시간은 시스템에 있는 개체 수, 문서의 크기 및 유형에 따라 다릅니다.

검색 인덱스는 파일의 지정된 위치에 저장되며, 인덱싱되는 문서의 검색 가능한 모든 콘텐츠를 포함합니다.

인덱싱을 성공적으로 실행하려면 다음 서버가 실행 중이고 사용 가능해야 합니다.

- IFRS(InputFileRepositoryServer)
- OFRS(OutputFileRepositoryServer)
- CMS(CentralManagementServer)
- APS(AdaptiveProcessingServer)

개체 유형을 Web Intelligence 또는 Crystal 보고서로 선택한 경우 해당 Web Intelligence 처리 서버 또는 Crystal Reports 응용 프로그램 서버가 실행 중이고 선택한 각 개체 유형에 대해 사용 가능해야 합니다.

4. 콘텐츠 저장소: 콘텐츠 저장소에는 ID, CUID, 이름, 종류, 주 인덱스에서 추출된 인스턴스 등의 정보가 읽기 쉬운 형식으로 포함됩니다. 이를 통해 검색 프로세스를 빠르게 처리할 수 있습니다.

검색

사용자가 BI 실행 패드 또는 플랫폼 검색 SDK를 사용하는 다른 응용 프로그램에서 키워드를 검색하는 경우 마스터 인덱스에서 이러한 검색어를 검사합니다. 사용자의 보기 권한을 기반으로 검색 엔진은 사용자가 액세스 권한이 있는 문서만 표시합니다.

자동 복구

플랫폼 검색에는 자체적인 자동 복구 메커니즘이 있습니다. 플랫폼 검색에서는 지속적으로 검색 서비스 메모리 사용을 모니터링하고 메모리 사용이 임계값을 초과하면 자동으로 인덱싱을 중지합니다. 또한 메모리 사용이 적절한 한계까지 줄어든 후 자동으로 인덱싱을 시작합니다. 그러나 사용자는 이 프로세스가 진행되는 동안 계속 검색을 수행할 수 있지만 특정 기간 동안에는 인덱싱할 수 없습니다. 플랫폼 검색에서는 기본적으로 문서 유형에 따라 한 시점에 인덱싱할 수 있는 문서 개수를 구성합니다. 인덱싱은 CPU 및 메모리 등 시스템 리소스에 따라 시작됩니다.

관련 항목

- 604 페이지에서 [응용 프로그램 속성 구성](#)"
- 609 페이지에서 [검색 가능한 콘텐츠 유형](#)"

17.3 플랫폼 검색의 클러스터 지원

플랫폼 검색은 클러스터된 환경의 여러 노드로 부하를 분산할 수 있습니다. 클러스터된 환경의 배포에서는 시스템 리소스가 최적화되므로 서버 성능이 향상됩니다.

플랫폼 검색은 검색 및 인덱싱 기능에 대해 수평적 클러스터링과 수직적 클러스터링을 지원합니다. 클러스터된 환경을 사용할 경우 검색 프로세스와 인덱스 프로세스의 성능이 최적화됩니다.

부하 분산

플랫폼 검색은 인덱싱과 검색의 부하 분산을 지원합니다.

클러스터된 환경에서는 부하 분산을 위해 여러 노드에서 인덱싱 및 검색 요청을 실행할 수 있습니다. 각 노드는 독립적으로 작동하여 콘텐츠를 인덱싱하고 델타 인덱스를 만듭니다. 그러나 클러스터의 노드 하나만 마스터 인덱스의 역할을 수행하고 델타 인덱스를 마스터 인덱스로 병합합니다. 모든 노드는 마스터 인덱스에 액세스할 수 있습니다. 따라서 동시 검색 요청이 가능합니다.

장애 조치

기술적인 오류나 유지 관리 관련 작업으로 인해 클러스터 내의 특정 노드를 사용할 수 없게 되면 다른 노드에서 자동으로 인덱싱 및 검색 요청을 처리합니다. 장애 조치 메커니즘을 통해 사용자는 검색을 계속할 수 있으며 인덱싱 작업이 중단되지 않습니다.

17.4 SDK 및 Open Search

플랫폼 검색은 SDK 및 Open Search를 둘 다 지원합니다.

17.4.1 플랫폼 검색 SDK

플랫폼 검색 SDK는 클라이언트 응용 프로그램과 플랫폼 검색 서비스를 연계하는 인터페이스입니다. 이 키트는 공개되어 사용자가 쉽게 검색 서비스를 사용자 지정하여 응용 프로그램과 통합할 수 있게 되었습니다.

검색 요청 매개 변수가 클라이언트 응용 프로그램을 통해 SDK 계층으로 전송되면 SDK 계층은 요청 매개 변수를 XML 인코딩 형식으로 변환하여 플랫폼 검색 서비스로 전달합니다.

플랫폼 검색 API에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence platform Java API Reference를 참조하십시오.

17.4.2 Open Search

플랫폼 검색은 OpenSearch 표준을 지원하므로, 클라이언트 응용 프로그램이 OpenSearch 표준 또는 형식을 사용하여 플랫폼 검색과 통신할 수 있습니다. OpenSearch는 SAP BusinessObjects Business Intelligence 플랫폼 제품군에 기본적으로 설치되지 않으므로, 사용자는 SAP BusinessObjects Business Intelligence 플랫폼용으로 사용되거나 WDeploy 도구를 사용하는 Tomcat과 같은 응용 프로그램 서버에 OpenSearch를 별개의 WAR 파일(opensearch.war)로 수동 배포해야 합니다. 설치 프로그램에서는 이 파일을 {BOE_INSTALL_DIR}\warfiles\OpenSearch 디렉터리로 복사합니다.

참고:

- 클라이언트 프로그램은 OpenSearch 표준에 따라 플랫폼 검색과 통신해야 합니다.
- SAP BusinessObjects Business Intelligence 플랫폼을 설치하면 기본적으로 Tomcat 응용 프로그램 서버가 설치됩니다.

17.4.2.1 OpenSearch 배포

SAP BusinessObjects Business Intelligence 플랫폼 환경에 OpenSearch를 배포하려면 다음 단계를 수행하십시오.

1. {설치 디렉터리}/SAP BusinessObjects Enterprise 4.0\warfiles\ 위치로 이동합니다.
2. OpenSearch 폴더를 {INSTALLDIR}\Tomcat6\Webapps로 복사합니다.
3. 아래에 설명된 대로 OpenSearch\WEB-INF\config.properties 파일에서 구성 매개 변수를 변경합니다.
 - CMS: CMS 이름과 포트 번호(예: <CMS 이름>:<포트 번호>)
 - OpenDocURL: OpenDocument 응용 프로그램의 URL(http://<tomcathost>:<connector port>/BOE/OpenDocument/opendoc/openDocument.jsp 등)
 - Proxy.rpurl: 역방향 프록시를 사용할 경우 역방향 프록시 서버 이름
 - Proxy.opendoc.rpurl: 역방향 프록시를 사용할 경우 OpenDoc 역방향 프록시 서버 이름
4. Tomcat 응용 프로그램 서버를 다시 시작하여 OpenSearch를 배포합니다.

17.4.2.2 WDeploy를 사용하여 OpenSearch 배포

WDeploy를 사용하여 OpenSearch를 배포하려면 다음 단계를 수행하십시오.

참고:

Windows 및 UNIX의 경우 명령은 각각 wdeploy.bat < parameters> 및 wdeploy.sh <parameters>로 언급됩니다.

1. 설치 디렉터리, 인스턴스 이름, 관리 포트, 관리 사용자 이름 및 관리자 암호와 같은 필수적인 웹 응용 프로그램 서버 매개 변수와 함께 <BOE_Install_Dir>\<Enterprise_DIR>\wdeploy\conf에 있는 config.<app server server> 파일을 업데이트합니다.
2. 아래에 설명된 대로 OpenSearch\WEB-INF\config.properties 파일에서 구성 매개 변수를 변경합니다.
 - CMS: CMS 이름과 포트 번호(예: <CMS 이름>:<포트 번호>)
 - OpenDocURL: OpenDocument 응용 프로그램의 URL(예: http://<응용 프로그램 서버 호스트>:<connectorport>/BOE/OpenDocument/opendoc/openDocument.jsp)
 - Proxy.rpurl: 역방향 프록시를 사용할 경우 역방향 프록시 서버 이름
 - Proxy.opendoc.rpurl: 역방향 프록시를 사용할 경우 OpenDoc 역방향 프록시 서버 이름.
3. <BOE_Install_Dir>\<Enterprise_DIR>\wdeploy 위치에서 wdeploy.bat <WEB_APPLICATION_SERVER> -Dapp_source_dir=<LOCATION_OF_OpenSearch_Webapp> -DAPP=OpenSearch deploy 명령을 실행합니다.

예를 들어, 다음 명령은 WebSphere 7 웹 응용 프로그램 서버에 OpenSearch를 배포합니다.

```
wdeploy.bat websphere7 -Dapp_source_tree=<BOE_Install_Dir>\<Enterprise_DIR>\warfiles" -DAPP=OpenSearch deploy
```

4. 응용 프로그램 서버를 다시 시작합니다.

17.4.2.3 OpenSearch용 역방향 프록시 구성

역방향 프록시 서버 뒤에 위치한 웹 응용 프로그램 서버에 SAP BusinessObjects Business Intelligence 플랫폼 웹 응용 프로그램을 배포하려면 들어오는 URL 요청을 올바른 WAR 파일에 매핑하도록 역방향 프록시 서버를 구성하십시오.

참고:

Apache 2.2 역방향 프록시 서버를 예제로 사용하여 구성 단계를 설명합니다.

OpenSearch용 Apache 2.2 역방향 프록시 서버 구성

1. 역방향 프록시를 설정한 다음 OpenSearch의 WEB-INF\wconfig.properties 파일에서 매개 변수를 변경합니다.
2. 다음 컨텍스트 매개 변수를 설정한 다음 값을 적절하게 변경합니다.
 - proxy.rpurl: OpenSearch용 역방향 프록시 URL(http://machineIPAddress/RP/OpenSearch/ 등)
 - proxy.opendoc.rpurl: Open Doc용 역방향 프록시 URL(http://machineIPAddress/RP/BOE/ 등)
3. Apache 역방향 프록시 설치 폴더 아래에 있는 httpd.conf 파일을 다음 설정으로 업데이트합니다.
 - ProxyPass /RP/BOE/OpenDocument/ http://<Tomcat host>:<Connector Port>/BOE/OpenDocument/
 - ProxyPass /RP/OpenSearchRP/ http://<Tomcat host>:<Connector Port>/OpenSearch/
 - ProxyPassReverseCookiePath /BOE /RP/BOE
 - ProxyPassReverseCookiePath /OpenSearchRP /RP/OpenSearchRP
4. Apache 2.2 역방향 프록시 서버를 다시 시작합니다.

17.5 응용 프로그램 속성 구성

플랫폼 검색 응용 프로그램 속성을 구성하려면 다음 단계를 완료하십시오.

1. CMC의 응용 프로그램 영역으로 이동합니다.
2. 플랫폼 검색 응용 프로그램을 선택합니다.
3. 관리 > 속성을 클릭합니다. 플랫폼 검색 응용 프로그램 속성 대화 상자가 나타납니다.
4. 원하는 플랫폼 검색 설정을 구성합니다.

다음 표에 구성 속성에 대한 설명이 나와 있습니다.

옵션	설명
검색 통계	<p>플랫폼 검색은 다음과 같은 검색 통계를 제공합니다.</p> <ul style="list-style-type: none"> • 인덱싱 상태: 인덱싱 프로세스 상태를 표시합니다. • 인덱싱된 문서 수: 인덱싱된 문서 수를 표시합니다. • 마지막 인덱싱 타임스탬프: 문서가 마지막으로 인덱싱된 타임스탬프를 표시합니다.
인덱싱 중지/시작	<p>연속 크롤링에서 예약된 크롤링으로 전환하려는 경우 또는 유지 관리를 위해 인덱싱 시작 또는 중지 옵션을 사용하여 인덱싱 프로세스를 시작 또는 중지할 수 있습니다.</p> <p>인덱싱을 중지하려면 인덱싱 중지를 클릭한 다음 확인 대화 상자에서 확인을 클릭합니다.</p>
인덱스 로캘	<p>인덱스 로캘을 다른 언어로 변경하면 플랫폼 검색에서 문서를 선택한 언어로 다시 인덱싱합니다.</p> <p>브라질어, 중국어, 체코어, 덴마크어, 네덜란드어, 영어, 핀란드어, 프랑스어, 독일어, 이탈리아어, 일본어, 한국어, 노르웨이어(북말), 폴란드어, 포르투갈어, 러시아어, 스페인어, 스웨덴어 및 태국어 중 한 가지 언어로 인덱싱 로캘을 설정합니다.</p> <p>참고: 기본적으로, 영어가 인덱스 로캘로 선택되어 있습니다.</p>

옵션	설명
크롤링 빈도	<p>다음 옵션을 사용하여 전체 BI 플랫폼 리포지토리를 인덱싱할 수 있습니다.</p> <ul style="list-style-type: none"> 연속 크롤링: 이 옵션을 선택한 경우, 개체를 추가, 수정 또는 삭제할 때마다 리포지토리를 인덱싱할 때 인덱싱이 연속으로 이루어집니다. 또한 최신 SAP BusinessObjects Business Intelligence 플랫폼 콘텐츠를 보거나 사용할 수 있습니다. 기본적으로 연속 크롤링이 설정되어 있으며 연속 크롤링은 수행하는 작업에 따라 지속적으로 BI 플랫폼 리포지토리를 업데이트합니다. 연속 크롤링은 사용자 개입 없이 작동하므로 문서 인덱싱에 걸리는 시간이 단축됩니다. 예약된 크롤링: 이 옵션을 선택한 경우, 인덱싱은 예약 옵션에서 설정한 예약을 기준으로 이루어집니다. <p>개체 예약에 대한 자세한 내용은 BI 플랫폼 CMC 온라인 도움말에서 플랫폼 검색의 개체 예약 단원을 참조하십시오.</p> <p>참고:</p> <ul style="list-style-type: none"> 크롤링 예약을 선택하고 되풀이를 지금 이외의 다른 옵션으로 설정하면 플랫폼 검색에 문서를 다음으로 인덱싱하기로 예약한 날짜 및 타임스탬프가 표시됩니다. 크롤링 예약을 선택한 경우에는 인덱싱 시작 단추가 활성화되며 인덱싱 중지 단추는 비활성화됩니다. 예약이 완료되면 인덱싱 중지 단추를 사용할 수 없습니다.

옵션	설명
인덱스 위치	<p>인덱싱된 문서는 다음 위치의 공유 폴더에 저장됩니다.</p> <ul style="list-style-type: none"> • 마스터 인덱스 위치(인덱스, 맞춤법 검사기): 마스터 및 맞춤법 검사기는 이 위치에 저장됩니다. 검색 워크플로 중, 최초 검색 항목들은 마스터 인덱스를 사용하여 검색되고 맞춤법 검사기 인덱스는 제안 사항을 검색하는 데 사용됩니다. 클러스터된 BOE 배포에서 이 위치는 클러스터의 모든 노드에서 액세스 가능한 공유 파일 시스템에 있어야 합니다. • 영구 데이터 위치(컨텐츠 저장소): 콘텐츠 저장소가 이 위치에 놓입니다. 콘텐츠 저장소는 마스터 인덱스 위치에서 만들어지고 이 위치와 동기화된 상태로 남습니다. 콘텐츠 저장소는 패킷을 생성하고 마스터 인덱스 위치에서 생성된 최초 검색 항목을 처리하는 데 사용됩니다. 클러스터된 BI 플랫폼 배포에서 콘텐츠 저장소는 각 노드마다 생성됩니다. <p>영구 데이터 위치는 콘텐츠 저장소 폴더를 포함하고 있으므로 클러스터된 환경의 영향을 받는 유일한 인덱스 위치입니다. 검색 서비스가 하나만 있는 컴퓨터에는 콘텐츠 저장소 위치가 하나만 있습니다. 예: {bobj.enterprise.home}\Wdata\WPlatformSearchData\Wworkspace\WServer\WContentStores</p> <p>그러나 클러스터된 환경에 여러 검색 서비스가 있는 경우 각 검색 서비스에는 하나의 콘텐츠 저장소 위치가 있습니다. 예를 들어, 실행 중인 서버 인스턴스가 두 개일 경우 콘텐츠 저장소 위치는 다음과 같습니다.</p> <ol style="list-style-type: none"> a. {bobj.enterprise.home}\Wdata\WPlatformSearchData\Wworkspace\WServer\WContentStores b. {bobj.enterprise.home}\Wdata\WPlatformSearchData\Wworkspace\WServer1\WContentStores <ul style="list-style-type: none"> • 비영구 데이터 위치(임시 서로게이트 파일, 델타 인덱스): 델타 인덱스가 마스터 인덱스와 병합되기 전에 이 위치에 임시로 만들어져 저장됩니다. 이 위치에서 인덱싱된 문서는 마스터 인덱스와 병합되면 삭제됩니다. 또한, 이 위치에서 서로게이트 파일(추출기의 출력 파일)이 만들어지고 이 파일이 델타 인덱스로 변환될 때까지 임시로 저장됩니다. <p>참고:</p> <ul style="list-style-type: none"> • 모든 인덱스 위치는 공유 위치여야 합니다. • 인덱스 위치를 수정하려면 인덱싱 중지를 클릭해야 합니다. • 인덱스 위치를 수정하는 경우 콘텐츠를 새 위치에 복사해야 하며, 그렇지 않으면 기존 인덱스 정보가 손실됩니다.

옵션	설명
인덱싱 수준	<p>다음과 같은 방법으로 인덱싱 수준을 설정하여 검색 콘텐츠를 조정할 수 있습니다.</p> <ul style="list-style-type: none"> • 플랫폼 메타데이터: 문서 제목, 키워드, 설명 등의 플랫폼 메타데이터 정보에 대해서만 인덱스가 만들어집니다. • 플랫폼 및 문서 메타데이터: 이 인덱스에는 플랫폼 메타데이터와 문서 메타데이터가 포함됩니다. 문서 메타데이터에는 만든 날짜, 수정한 날짜 및 작성자 이름이 포함됩니다. • 전체 콘텐츠: 이 인덱스에는 플랫폼 메타데이터, 문서 메타데이터 및 다음과 같은 기타 콘텐츠가 포함됩니다. <ul style="list-style-type: none"> • 문서의 실제 콘텐츠 • 프롬프트 및 LOV의 콘텐츠 • 차트, 그래프 및 레이블 <p>참고: 인덱싱 수준을 수정하면 전체 BI 플랫폼 리포지토리를 새로 고치기 위해 인덱싱이 초기화됩니다.</p>
콘텐츠 형식	<p>인덱싱을 위해 다음 콘텐츠 형식을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • Microsoft Word • Microsoft Excel • Microsoft PowerPoint • 텍스트 • Adobe Acrobat • 서식 있는 텍스트 • Crystal Reports • 유니버스 • Web Intelligence
인덱스 재작성	<p>이 옵션을 이용해 인덱싱된 기존 콘텐츠를 모두 삭제하고 처음부터 전체 문서를 다시 인덱싱합니다.</p> <p>인덱싱 상태에 상관없이 인덱스 재작성 옵션을 선택할 수 있습니다. 하지만, 인덱싱이 중지되는 경우 인덱스 재작성 옵션이 작용하지 않으므로 인덱스 재작성을 선택하고 플랫폼 검색 응용 프로그램을 저장하고 닫습니다.</p> <p>인덱싱이 중지되어 인덱스 재작성을 선택하고 플랫폼 검색 응용 프로그램을 저장하고 닫은 다음 구성 페이지를 다시 열고 인덱싱 시작을 클릭하면, 저장된 재작성 인덱스가 전체 문서를 자동으로 다시 인덱싱합니다.</p> <p>플랫폼 검색에서 문서를 다시 인덱싱하지 않으려는 경우에는 인덱스 재작성을 선택 취소한 후 인덱싱 시작 단추를 클릭해야 합니다.</p>

옵션	설명
인덱싱에서 제외된 문서	<p>인덱싱에서 제외된 문서 옵션은 문서를 인덱싱에서 제외합니다. 예를 들어, Report Application Server 리소스가 오버로드되지 않도록 크기가 너무 큰 Crystal 보고서를 검색 대상에 포함되지 않도록 할 수 있습니다. 또는 수백 개의 사용자 설정 보고서가 포함된 게시를 인덱싱에서 제외되도록 할 수 있습니다.</p> <p>특정 문서를 제외하여 이 문서가 플랫폼 검색으로 검색되지 않도록 할 수 있습니다. 단, 문서를 이 그룹에 넣기 전에 문서가 이미 인덱싱된 경우에는 계속 검색이 가능합니다. 인덱싱에서 제외된 문서 그룹의 문서를 검색하지 못하게 하려면 인덱스를 다시 작성해야 합니다.</p> <p>기본적으로 관리자 계정은 인덱싱에서 제외된 문서에 대한 전체 권한을 갖고 있습니다. 다음 권한이 있는 다른 사용자는 인덱싱에서 제외된 문서 그룹에 문서를 추가만 할 수 있습니다.</p> <ul style="list-style-type: none"> • 범주에 대한 권한 보기 및 편집 • 문서 직접 편집

5. 저장 후 단기를 클릭합니다.

참고:

사용자가 인덱스 재작성 옵션을 선택하지 않고 인덱싱 수준을 변경하거나 추출기를 선택 또는 선택 취소하는 경우에는 기존 인덱스를 삭제하지 않고 처음부터 인덱스가 증분 업데이트됩니다.

17.6 검색 가능한 콘텐츠 유형

SAP BusinessObjects Business Intelligence 플랫폼에 게시된 콘텐츠는 플랫폼 검색을 통해 검색할 수 있습니다. 다음 표에는 해당하는 인덱싱된 콘텐츠와 함께 개체 유형이 나와 있습니다.

개체 유형	인덱싱된 콘텐츠
Crystal Reports(2008 및 2011)	제목, 설명, 수식 선택, 저장된 데이터, 모든 섹션의 텍스트 필드, 매개 변수 값 및 하위 보고서

개체 유형	인덱싱된 콘텐츠
Web Intelligence 문서	제목, 설명, 보고서에 사용된 유니버스 필터 이름, 저장된 데이터, 보고서에 로컬로 정의된 필터 조건의 상수, 보고서에 사용된 유니버스 계수 이름, 보고서에 사용된 유니버스 개체 이름, 레코드 집합의 데이터 및 셀의 정적 텍스트
Microsoft Excel 문서(2003 및 2007)	문서 속성(제목, 주제, 작성자, 회사, 범주, 키워드 및 주식)의 요약 페이지에 있는 비어 있지 않은 모든 셀 및 필드의 데이터, 문서 머리글과 바닥글에 있는 텍스트 등 계산 또는 수식을 사용하는 셀의 경우 평가 후 값을 검색할 수 있습니다. 숫자 또는 날짜/시간 값의 경우 원시 데이터는 검색 가능합니다.
Microsoft Word 문서(2003 및 2007)	모든 단락 및 표에 있는 텍스트, 문서 속성(제목, 주제, 작성자, 회사, 범주, 키워드, 주식)의 요약 페이지에 있는 필드, 문서 머리글과 바닥글에 있는 텍스트 및 숫자 텍스트
RTF, PDF, PPT 및 TXT 파일	이러한 파일에 있는 모든 텍스트는 검색 가능합니다.
LCMJob, 유니버스, AFDashboard 페이지, Dashboard Design, ObjectPackage, 웹 서비스 쿼리(QaaWS), 프로파일, 토론, InformationDesigner, SAP BusinessObjects Business Intelligence 플랫폼용 위젯, MDAnalysis, 게시, Flash, 분석 및 하이퍼링크	메타데이터 콘텐츠를 검색할 수 있습니다.
이벤트	사용자 지정 이벤트, 시스템 이벤트, Crystal Reports 이벤트 및 모니터링 이벤트 등 모든 이벤트를 검색할 수 있습니다. 이벤트가 소스와 연결된 경우 플랫폼 검색에서는 소스를 이벤트와 함께 표시합니다. 참고: 플랫폼 검색에서는 Crystal Reports for Enterprise의 이벤트를 지원합니다.

참고:

타사 문서(MS Office 2003 및 2007, PDF 문서)에 지원되는 최대 크기는 15MB입니다.

17.7 제안된 쿼리

플랫폼 검색을 사용하는 경우 사용자는 특정 개체를 찾지 않고 특정 질문에 대한 답을 찾으려고 할 수 있습니다. 이러한 질문에 대한 답은 SAP BusinessObjects Business Intelligence 플랫폼 리포지토리에서 제공하는 보고서에 있을 수도 있고 그렇지 않을 수도 있습니다.

플랫폼 검색에서는 유니버스와 SAP BusinessObjects Business Intelligence 플랫폼 리포지토리에 있는 기존 보고서의 구조를 분석하고 이 정보를 사용자가 입력한 검색 요청과 비교하여 사용자가 질문에 대한 답을 찾는 데 도움이 될 만한 새로운 SAP BusinessObjects Web Intelligence 쿼리를 제안합니다.

플랫폼 검색에서는 모든 유니버스에 있는 단어의 차원, 계수, 조건 및 필터 값을 일치시켜 잠재 보고서를 만듭니다.

플랫폼 검색은 유니버스 또는 기존 SAP BusinessObjects Web Intelligence 문서에 대한 다음 정보에서 일치 항목을 찾습니다.

- 검색 입력의 단어와 일치하는 유니버스의 계수.
계수가 검색어 중 하나와 일치하면 결과로 나타나는 SAP BusinessObjects Web intelligence 문서에 해당 계수가 사용됩니다.
- 검색 입력의 단어와 일치하는 유니버스의 차원 이름.
차원 이름이 검색 용어 중 하나와 일치하면 Web Intelligence 문서 결과가 이 차원에 대한 정보로 분할됩니다.
- 문서에 표시되는 데이터에 초점을 맞추기 위해 쿼리 필터를 사용할 수 있습니다. 이러한 쿼리 필터는 검색 입력을 분석하여 생성됩니다.
 - 유니버스의 이름 조건이 검색 용어 중 하나와 일치하면 해당 조건이 필터로 사용됩니다.
 - 이름이 검색어와 일치하는 필드 값이 기존 SAP BusinessObjects Web Intelligence 문서에 있으면 일치하는 값이 들어 있는 기록 보고서의 차원을 통해 필터가 만들어집니다. 이때 조건 연산자로 "같음"이 사용됩니다.

플랫폼 검색을 통해 충분한 수의 일치 항목을 찾아 결과 문서에 두 개의 결과 필드와 한 개의 필터가 포함되면 쿼리를 실행할 준비가 끝난 것으로 간주됩니다. 이 경우 사용자는 완성된 보고서를 클릭하여 볼 수 있습니다.

유니버스와 문서 간 일치하는 항목의 수가 충분하지 않은 경우 쿼리를 편집한 후 실행할 수 있습니다.

입력된 검색어와 일치하는 유니버스가 여러 개이거나 차원 이름 및 필터 값과 같이 서로 다른 두 개의 일치 항목에 동일한 단어가 나타나는 경우 플랫폼 검색에서 여러 개의 쿼리를 제안합니다.

17.8 패킷

플랫폼 검색은 검색 결과를 유사한 개체 유형의 패킷 또는 범주별로 그룹화하고, 검색어에 대해 반환된 결과 중에서 범주의 수 순서로 검색 결과의 순위를 지정하여 검색 결과를 구체화합니다. 패킷을 통해 정확한 결과로 이동할 수 있습니다.

플랫폼 검색은 InfoObject 메타데이터, 문서 메타데이터 및 문서 콘텐츠에서 패킷을 생성하며, 지정된 쿼리와 일치하는 문서가 세 개 이상인 패킷만 표시합니다. 패킷은 검색 쿼리와 일치하는 문서에 따라 동적으로 표시되며, 문서 수를 기준으로 정렬됩니다.

SAP BusinessObjects Business Intelligence 플랫폼 문서는 다음의 일반 패킷 또는 범주별로 그룹화됩니다.

- 개인 또는 공용(예: HR, 회사 및 재무): BI 플랫폼 문서 범주를 기반으로 합니다.
- 문서 유형: Web Intelligence, Crystal Report, Microsoft Word(2003 및 2007), Microsoft Excel 문서(2003 및 2007) 및 Xcelsius 등의 문서 유형을 기반으로 합니다.
- 유니버스 및 연결: 콘텐츠 소스를 기반으로 합니다.
- 날짜: 마지막으로 새로 고친 날짜(연도, 분기 및 월)가 포함됩니다.
- 시간: 마지막으로 새로 고친 시간(예: 24시간, 지난 주)이 포함됩니다.
- 작성자: 문서를 만든 사용자의 이름입니다.

17.9 다국어 지원

플랫폼 검색은 콘텐츠를 인덱싱하고, 검색 결과를 검색한 다음 제안 사항을 원하는 언어로 표시하는 다국어 지원을 지원합니다. 결과는 클라이언트에 설정된 로캘에 상관없이 CMC 응용 프로그램의 인덱스 로캘에 설정된 언어로 검색됩니다. 플랫폼 검색은 메타데이터, 문서 속성 및 보고서 콘텐츠를 인덱싱합니다.

인덱싱 프로세스는 구성 페이지에 지정된 로캘에 해당하는 분석기를 사용합니다. 이때 항상 한 개의 언어만 인덱싱에 사용됩니다.

최상의 검색 결과를 얻기 위해서는 인덱싱과 검색을 수행할 때 동일한 로캘을 사용해야 합니다. 기본적으로 영어가 인덱스 로캘로 설정되어 있으므로, 플랫폼 검색에서 인덱싱과 검색 시 영어가 사용됩니다. 로캘을 변경하면 새 구성을 저장할 때 선택한 옵션을 기준으로 인덱스가 다시 초기화되거나 다시 작성됩니다. 이후에 문서를 인덱싱하면 새 언어 설정이 사용됩니다.

CMC 응용 프로그램에서 로캘을 다른 언어로 변경(예: 영어에서 독일어로 변경)할 경우, 기존 모든 문서에 대해 독일어 분석기를 사용하여 전체 인덱스가 증분 방식으로 업데이트됩니다.

로캘을 다른 언어로 재설정(예: 영어에서 독일어로 재설정)한 다음 인덱스 재작성을 선택하면 현재 인덱스가 삭제되고 새 인덱스가 독일어로 작성됩니다.

17.10 제안

플랫폼 검색은 철자가 잘못된 검색 쿼리에 대한 제안을 제공합니다. 원래 검색 쿼리로는 일치하는 결과를 찾을 수 없는 경우 플랫폼 검색이 인덱싱된 콘텐츠를 기준으로 가장 가능성이 높은 단어를 제안합니다.

제안은 하이퍼링크가 있는 키워드로 표시됩니다. 하이퍼링크를 클릭하면 원본 쿼리와 일치하는 키워드를 포함하는 문서 목록이 표시됩니다. 이러한 제안 사항은 다양한 객관적 요소에 따라 알고리즘적으로 결정됩니다.

원래 요청과 일치하는 단어가 여러 개일 경우, 플랫폼 검색은 CMC 응용 프로그램에 인덱스 로캘로 설정된 언어로 상위 세 개의 항목을 제안합니다.

참고:

플랫폼 검색에서 제안 사항을 생성하지 않는 경우는 다음과 같습니다.

- 검색 쿼리가 세 자 미만인 경우
- 유형: Crystal 보고서와 같이 특성을 사용하는 검색
- 유니버스 메타데이터 및 콘텐츠
- 멀티바이트 언어(예: 중국어, 일본어, 한국어)

17.11 SAP BusinessObjects Explorer의 검색 결과 연함

플랫폼 검색에서는 SAP BusinessObjects Explorer의 검색 요청 및 표면 정보 공간을 SAP BusinessObjects Business Intelligence 플랫폼 콘텐츠와 연함합니다.

SAP BusinessObjects Explorer의 검색 결과는 메타데이터 범주별로 그룹화됩니다. 지원되는 InfoSpace의 패킷에는 유형, 위치 및 새로 고침 시간이 있습니다.

SAP BusinessObjects Explorer에서는 검색 쿼리의 각 검색 용어에 대해 플랫폼 검색으로 용어 빈도를 보냅니다. 플랫폼 검색에서는 용어 빈도의 제공된 합계를 사용하여 관련성을 계산합니다. 결과 값은 각 정보 공간에 점수로 할당됩니다. 그러면 결과가 점수별로 정렬되어 클라이언트로 전송됩니다.

17.12 SAP NetWeaver Enterprise Search를 이용한 검색 시간 통합

SAP NetWeaver Enterprise Search 7.20 이상에서는 OpenSearch(RSS 및 ATOM)를 바탕으로 검색 서비스를 사용할 수 있습니다. 원격 검색 서비스 공급자 시스템으로 검색 요청을 위임할 수 있습니다. 이 경우, OpenSearch는 서비스 공급자이고, NetWeaver Enterprise Search는 검색 결과에 대한 소비자이며, SAP BusinessObjects Platform Search는 검색 서비스 공급자입니다.

사용자가 검색 요청을 전송하면 SAP NetWeaver Enterprise Search가 검색 요청을 OpenSearch 공급자로 직접 전달합니다. 공급자는 검색 요청에 대해 회신하고 SAP NetWeaver Enterprise Search로 다시 회신을 보냅니다. 그러면 다른 검색 개체 커넥터에서 수신한 결과가 검색 결과로 통합되어 사용자 인터페이스에 표시됩니다.

SAP NetWeaver Enterprise Search와 Platform Search를 통합하려면 다음 단계를 수행해야 합니다.

1. SAP NetWeaver Enterprise Search에서 커넥터를 만듭니다.
2. SAP BusinessObjects Business Intelligence 플랫폼 인증 섹션의 사용자 역할을 가져옵니다.

17.12.1 SAP NetWeaver Enterprise Search에서 커넥터 만들기

OpenSearch 유형의 검색 개체 커넥터를 사용하여 OpenSearch를 통해 사용할 수 있는 검색 기능을 제공하는 외부 검색 공급자를 통합할 수 있습니다.

SAP NetWeaver Enterprise Search에서 커넥터를 만들려면 다음 필수 구성 요소가 필요합니다.

1. OpenSearch 설명 서비스 URL.
2. OpenSearch 설명 서비스는 RSS 또는 ATOM 형식으로만 지원되어야 합니다.

SAP NetWeaver Enterprise Search에서 커넥터를 만들려면 다음 단계를 수행하십시오.

1. Administration Cockpit을 실행하고 만들기를 선택합니다.
2. OpenSearch를 검색 개체 커넥터 유형으로 선택합니다.
3. Next를 선택합니다.
4. OpenSearch 공급자의 OpenSearch 설명 서비스 URL을 입력합니다.
5. 다음 인증 설정 중 하나를 선택하여 설명 서비스 URL을 시작합니다.
 - 인증 없음: 아무런 인증도 이루어지지 않습니다.
 - SAP 인증 어설션 티켓: 이 사용자는 SSO를 통한 인증에 사용됩니다.
 - 사용자/암호: 미리 정의된 사용자가 인증에 사용됩니다.
6. OpenSearch URL 설정에서 검색 URL 시작을 선택합니다.

그러면 적당한 검색 서비스에 대해 OpenSearch 설명 서비스의 유효성이 검사됩니다. 검색 URL 템플릿과 관련 설명에 대한 값이 자동으로 입력됩니다.

7. 다음 인증 설정 중 하나를 선택하여 커넥터를 설치합니다.
 - 인증 없음: 아무런 인증도 이루어지지 않습니다.
 - SAP 인증 어설션 티켓: 이 사용자는 SSO를 통한 인증에 사용됩니다.
 - 사용자/암호: 미리 정의된 사용자가 인증에 사용됩니다.
8. Next를 선택합니다.
요약 대화 상자가 나타나 이 검색 개체 커넥터에 대해 입력된 값을 표시합니다.
9. 설정을 수정하려면 이전을 선택하고 입력된 데이터를 전부 삭제하려면 취소를 선택합니다.
10. 마침을 선택하여 설정을 저장합니다.

17.12.2 SAP BusinessObjects Enterprise 인증의 사용자 역할 가져오기

SAP BusinessObjects Business Intelligence 플랫폼 인증에서 사용자 역할을 가져오려면 다음 단계를 수행하십시오.

참고:

관리자는 사용자 세부 정보, 시스템 정보 및 응용 프로그램 호스트 정보와 사용자 자격 증명이 있어야 합니다.

1. CMC의 인증 영역으로 이동합니다.
2. SAP를 선택합니다.
3. 권한 부여 시스템 탭에서 다음을 지정합니다.
 - 시스템
 - 클라이언트
 - 응용 프로그램 서버
 - 시스템 번호
 - 사용자 이름
 - 암호
 - 언어
4. 업데이트를 선택합니다.
5. 역할 가져오기 탭을 클릭하고 사용자 역할을 가져옵니다.
6. 업데이트를 선택합니다.
7. CMC에서 관리 > 사용자 보안을 선택하여 알맞은 사용자 권한을 할당합니다.

17.12.3 NetWeaver Enterprise Search에서 검색

SAP NetWeaver Enterprise Search에서 결과를 검색하려면 다음 단계를 수행합니다.

1. SAP NetWeaver Enterprise Search 응용 프로그램에 로그인합니다.
2. 고급 검색을 선택합니다.
3. 플랫폼 검색용으로 만들어진 커넥터를 선택합니다.
4. 키워드를 검색합니다.

키워드에 일치되는 부분이 있는 경우 키워드에 대해 통합된 결과에 플랫폼 검색의 결과가 포함됩니다.

17.13 감사

플랫폼 검색 서비스를 사용하는 클라이언트 응용 프로그램으로부터 전송된 검색 요청과 검색 응답의 모든 이벤트는 감사됩니다. 플랫폼 검색의 경우 감사는 서비스 수준에서 구현됩니다.

플랫폼 검색에 대해서는 하나의 이벤트 ID 1009가 있으며 플랫폼 검색 관련 이벤트 세부 정보로는 다음과 같은 네 개 항목이 있습니다.

- 키워드 검색(ID: 19)
- 검색 결과 수(ID: 63)
- 페킷 검색(ID: 20)
- 검색 예외(ID: 1)

위 이벤트 세부 정보와 별도로, BI 플랫폼 모듈에서는 감사에 대해 몇 가지 표준 이벤트 세부 정보(예: sessionCuid 및 userCuid)가 지원됩니다.

플랫폼 검색에서의 감사 작동 방식이 아래에 예와 함께 설명되어 있습니다.

"Sales"와 같은 키워드를 검색하는 경우 총 검색 결과 수는 다섯 개일 수 있습니다. 이 경우 다음과 같은 이벤트가 감사됩니다.

- 이벤트 ID 1009
- sales 값이 포함된 이벤트 세부 정보 ID 19
- 5 값이 포함된 이벤트 세부 정보 ID 63
- 세션 CUID
- 사용자 CUID
- 성공을 의미하는 0 값이 포함된 상태
- 시작 시간
- 기간
- 개체

- 서비스 측 감사이므로 0 값이 포함된 ID

패킷이 생성되고 패킷을 하나 이상 선택하면 다음과 같은 이벤트가 감사됩니다.

- 이벤트 ID 1009
- sales 값이 포함된 이벤트 세부 정보 ID 19
- 5 값이 포함된 이벤트 세부 정보 ID 63
- 폼표로 구분된 패킷 문자열이 포함된 이벤트 세부 정보 ID 20
- 세션 CUID
- 사용자 CUID
- 성공을 의미하는 0 값이 포함된 상태
- 시작 시간
- 기간
- 서비스 측 감사이므로 0 값이 포함된 개체 ID

잘못된 항목(예: "*"a")으로 인해 검색 예외가 발생할 경우 다음과 같은 이벤트 세부 정보가 감사됩니다.

- 이벤트 ID 1009
- sales 값이 포함된 이벤트 세부 정보 ID 19
- 0 값이 포함된 이벤트 세부 정보 ID 63
- 예외 메시지가 포함된 이벤트 세부 정보 ID 1
- 세션 CUID
- 사용자 CUID
- 실패를 의미하는 1 값이 포함된 상태
- 시작 시간
- 기간
- 서비스 측 감사이므로 0 값이 포함된 개체 ID

17.14 인덱싱 오류 목록

인덱싱 오류 목록에는 인덱싱하지 못한 문서 목록이 표시됩니다. 플랫폼 검색에서는 인덱싱할 문서에 대해 세 차례 인덱싱을 시도합니다. 문서를 인덱싱하지 못한 경우 인덱싱 오류 목록에 이 문서가 표시됩니다.

인덱싱 실패 목록을 보려면 다음 단계를 수행합니다.

1. CMC의 응용 프로그램 영역으로 이동합니다.
2. 플랫폼 검색 응용 프로그램을 선택합니다.
3. 작업 > 인덱싱 오류 목록을 클릭합니다.

다음과 같은 세부 정보가 포함된 문서 목록을 표시하는 플랫폼 검색 응용 프로그램 대화 상자가 나타납니다.

- 제목: 인덱싱하지 못한 문서의 제목이 표시됩니다.
- 유형: 문서 유형(Crystal Report 및 Web Intelligence)의 이름과 문서 위치가 표시됩니다.
- 오류 유형: 문서의 인덱스 오류에 대한 오류 코드 및 원인이 표시됩니다. 추가 정보 하이퍼링크를 클릭하면 오류 원인의 스택 추적에 대한 자세한 내용을 확인할 수 있습니다.
- 마지막 시도 시간: 문서를 인덱싱하려는 마지막 시도의 타임스탬프가 표시됩니다.

17.15 문제 해결

이 단원에서는 플랫폼 검색에서 검색 결과를 가져오는 동안 발생할 수 있는 다양한 문제에 대한 단계별 솔루션을 제공합니다.

키워드가 포함된 새로 추가된 문서에서 검색 결과를 가져올 수 없음

- 플랫폼 검색에서 제출된 문서의 문서 유형을 지원하는지 확인합니다. 문서 유형이 지원되지 않는 경우 문서가 인덱싱되지 않습니다.

지원되는 문서 유형에 대한 자세한 내용은 아래 나열된 관련 항목에서 검색 가능한 콘텐츠 유형 항목을 참조하십시오.

- 크롤링 빈도에 선택된 옵션을 확인합니다. 크롤링 빈도가 연속 크롤링으로 설정된 경우 문서가 즉시 선택되어 인덱싱됩니다. 크롤링 빈도가 예약된 크롤링으로 설정된 경우 예약된 기간에만 인덱싱이 실행됩니다.

크롤링 빈도에 대한 자세한 내용은 아래 나열된 관련 항목에서 응용 프로그램 속성 구성 항목을 참조하십시오.

- 문서가 성공적으로 인덱싱되었는지 인덱싱 오류 목록을 확인합니다. 문서가 목록에 표시되는 경우 문서를 수정하고 다시 제출하여 플랫폼 검색에서 이 문서를 인덱싱에 사용하도록 해야 합니다.

참고:

필드를 추가하거나 삭제하고 다시 저장하여 문서를 수정할 수 있습니다. 이렇게 하면 SAP BusinessObjects Business Intelligence 플랫폼 리포지토리에서 문서의 타임스탬프가 업데이트되어 문서가 다시 인덱싱됩니다.

인덱싱에 실패한 문서에 대한 자세한 내용은 아래의 관련 항목에서 인덱싱 오류 목록 항목을 참조하십시오.

- 인덱싱 실패에 대한 정보가 들어 있는 적응형 처리 서버의 추적 로그를 확인합니다.
 1. 파일 시스템에서 .gif 확장명의 APS 추적 로그가 있는 {BOE 설치 디렉터리}\WloggingW으로 이동합니다.
 2. 추적 로그 파일을 열어 인덱싱 대상인 문서의 SL_ID를 검색합니다.

참고:

문서 SL_ID는 문서 속성에서 찾을 수 있습니다.

Crystal Report 문서를 검색 결과로 가져올 수 없음

플랫폼 검색에서는 버전 2008 및 2011의 Crystal Report 콘텐츠만 인덱싱합니다. Crystal Reports for Enterprise의 콘텐츠는 인덱싱하지 않습니다.

그러나 Crystal Reports for Enterprise의 경우 문서 속성의 부분인 제목, 설명 및 키워드 등 문서의 메타데이터를 검색할 수 있습니다.

문서에 인덱싱 가능한 콘텐츠가 들어 있는 경우에는 위에서 설명한 키워드가 포함된 새로 추가된 문서에서 검색 결과를 가져올 수 없음 단원에 나열된 것과 같은 프로세스를 따라야 합니다.

BI 실행 패드의 제품 로컬로 설정된 언어 세트에서 검색 결과를 가져올 수 없음

플랫폼 검색에서는 CMC에서 설정한 인덱스 로컬에 따라 SAP BusinessObjects Business Intelligence 플랫폼 리포지토리의 콘텐츠를 검색하고 인덱싱합니다. BI 실행 패드에 설정된 제품 로컬이 CMC에서 설정한 로컬과 다른 경우 플랫폼 검색에서는 결과를 가져오지 않습니다.

인덱스 로컬 구성에 대한 자세한 내용은 아래의 관련 항목에서 응용 프로그램 속성 구성을 참조하십시오.

SAP BusinessObjects Explorer InfoSpaces를 검색 결과로 가져올 수 없음

SAP BusinessObjects Explorer 서버가 중지되거나 비활성화되는지 확인합니다. 플랫폼 검색용 서버를 사용하여 SAP BusinessObjects Explorer에서 검색 결과를 가져옵니다.

SAP NetWeaver Enterprise 검색에서 SAP BusinessObjects Business Intelligence 플랫폼 리포지토리의 결과를 가져올 수 없음

- 플랫폼 검색에서 문제의 원인이 플랫폼 검색 및 SAP NetWeaver Enterprise Search 통합으로 인한 것인지 알아보기 위해 BI 실행 패드를 사용하여 검색 결과를 가져오는지 확인합니다.
- OpenSearch가 웹 응용 프로그램 서버에 올바르게 배포되어 있는지 확인합니다. OpenSearch 배포의 유효성 검사를 위한 구체적인 단계는 사용 중인 웹 응용 프로그램 서버의 유형에 따라 다릅니다.
- SAP NetWeaver Enterprise Search 구성에서 커넥터가 올바르게 만들어지거나 구성되는지 확인합니다. SAP NetWeaver Enterprise Search가 플랫폼 검색의 결과를 연합하는 데 알맞은 커넥터를 사용해야 합니다.
- 각각 SAP NetWeaver Enterprise Search와 SAP BusinessObjects Enterprise를 실행 중인 컴퓨터 간에 통신이 올바르게 이루어지는지 확인합니다. 분산 환경에서 네트워크 문제가 발생한 경우, SAP NetWeaver Enterprise Search에서 결과를 연합하지 못할 수 있습니다.
- SAP NetWeaver Enterprise Search 사용자가 적절한 권한을 가지고 SAP BusinessObjects Business Intelligence 플랫폼에 추가되는지 확인합니다. 사용자 권한의 유효성을 검사하려면 CMC의 인증 영역으로 이동하고 SAP를 선택합니다.

관련 항목

- 617 페이지에서 [인덱싱 오류 목록](#)"
- 604 페이지에서 [응용 프로그램 속성 구성](#)"
- 609 페이지에서 [검색 가능한 콘텐츠 유형](#)"

장18 연합

18.1 연합

연합은 글로벌 환경에서 여러 곳에 배포된 SAP BusinessObjects Business Intelligence 플랫폼을 사용하여 작업하는 사이트 간 복제 도구입니다.

특정 BI 플랫폼 배포 환경에서 콘텐츠를 만들어 관리하고 이를 되풀이 일정에 따라 지리적으로 멀리 떨어져 있는 다른 BI 플랫폼 배포 환경에 복제할 수 있습니다. 사용자는 단방향 복제 및 양방향 복제 작업을 모두 수행할 수 있습니다.

연합 기능을 사용하면 다음과 같은 이점이 있습니다.

- 네트워크 트래픽을 줄일 수 있습니다.
- 한 곳에서 콘텐츠를 만들고 관리할 수 있습니다.
- 최종 사용자에게 향상된 성능을 제공할 수 있습니다.

연합 기능을 사용하여 콘텐츠를 복제할 때 얻을 수 있는 이점은 다음과 같습니다.

- 여러 배포를 간단히 관리할 수 있습니다.
- 글로벌 조직의 여러 사무실에 일관된 권한 정책을 적용할 수 있습니다.
- 정보를 더 신속하게 얻을 수 있고 데이터가 있는 원격지에서 보고서를 처리할 수 있습니다.
- 로컬 및 분산 데이터를 더 신속하게 검색하여 시간을 절약할 수 있습니다.
- 사용자 지정 코드를 작성하지 않고도 여러 배포의 콘텐츠를 동기화할 수 있습니다.

연합을 통해 보안 모델, 수명 주기, 테스트 및 배포 시간을 분리할 뿐만 아니라 비즈니스 소유자와 관리자도 구분할 수 있습니다. 예를 들어 판매 응용 프로그램 관리자가 인사 응용 프로그램을 변경하지 못하도록 제한하는 관리 기능을 위임할 수 있습니다.

다음 표에서 설명하고 있는 것과 같이 연합을 사용하여 복제할 수 있는 개체에는 여러 가지가 있습니다.

범주	복제할 수 있는 개체 유형	추가 참고 사항
비즈니스 뷰	비즈니스 뷰 관리자, DataConnection, LOV, 데이터 기반 등	개별 수준은 아니더라도 모든 개체가 지원됩니다.
보고서	Crystal 보고서, Web Intelligence, Dashboard Design	Full Client 추가 기능 및 템플릿이 지원됩니다.
타사 개체	Excel, PDF, PowerPoint, Flash, Word, 텍스트, 서식 있는 텍스트 및 Shockwave Flash 파일	
사용자	사용자, 그룹, 받은 파일함, 즐겨찾기 및 개인 범주	
Business Intelligence 플랫폼	폴더, 이벤트, 범주, 달력, 액세스 수준, 하이퍼링크, 바로 가기, 프로그램, 프로필, 개체 패키지, Agnostic	
유니버스	유니버스, 연결 및 유니버스 오버로드	

다음은 조직에서 연합을 어떻게 사용할 수 있는지 보여 주는 두 가지 예제 시나리오입니다.

시나리오 1: 소매(중앙 집중식 디자인)

ACME 상점에서 단방향 복제 방법을 사용하여 다른 상점으로 월별 매출 보고서를 보내려고 합니다. 원본 사이트의 관리자가 보고서를 만들면 각 대상 사이트의 관리자가 이 보고서를 복제하고 해당 상점의 데이터베이스를 기반으로 보고서를 실행합니다.

팁:

로컬 버전의 인스턴스를 다시 원본 사이트로 보내 각 개체의 복제된 정보를 유지 관리할 수 있습니다. 예를 들어 적절한 로고, 데이터베이스 연결 정보 등을 적용할 수 있습니다.

시나리오 2: 원격 일정(분산 액세스)

데이터가 원본 사이트에 있습니다. 보류 중인 복제 작업을 실행하기 위해 해당 작업이 원본 사이트로 보내집니다. 완료된 복제 작업을 볼 수 있도록 해당 작업이 다시 대상 사이트로 보내집니다. 예를 들어 대상 사이트에서는 보고서의 데이터를 사용할 수 없지만 완성된 보고서를 대상 사이트로 다시 보내기 전에 원본 사이트에서 보고서를 실행하도록 구성할 수 있습니다.

18.2 연합 용어

다음 용어 목록에서는 개념 이해와 실무에 도움이 되도록 연합과 관련된 단어와 구를 소개합니다.

18.2.1 BI 응용 프로그램

특정 목적이나 대상을 갖고 서로 연관된 Business Intelligence(BI) 콘텐츠로 이루어진 논리적 그룹입니다. BI 응용 프로그램은 개체가 아닙니다. BI 플랫폼 배포 하나에서 여러 BI 응용 프로그램을 호스팅할 수 있고, 각 응용 프로그램은 개별 보안 모델, 수명 주기, 테스트 및 배포 일정을 비롯하여 개별 비즈니스 소유자와 관리자를 가질 수 있습니다.

18.2.2 대상 사이트

원본 사이트에서 복제된 BI 플랫폼 콘텐츠를 가져오는 BI 플랫폼 시스템입니다.

18.2.3 로컬

사용자나 관리자가 연결되어 있는 로컬 시스템입니다. 예를 들어 대상 사이트의 관리자는 대상 사이트에 대해 로컬로 간주됩니다.

18.2.4 로컬에서 실행되는 완료된 인스턴스

대상 사이트에서 처리된 후 원본 사이트로 다시 보내지는 인스턴스입니다.

18.2.5 다중 원본 사이트

여러 사이트를 원본 사이트로 사용할 수 있습니다. 예를 들어, 대부분의 개발 센터에는 일반적으로 여러 개의 원본 사이트가 있습니다. 그러나 복제당 원본 사이트는 하나씩만 존재할 수 있습니다.

18.2.6 단방향 복제

개체가 한 방향으로만, 즉 원본 사이트에서 대상 사이트로만 복제됩니다. 대상 사이트의 업데이트는 대상 사이트에 남습니다.

18.2.7 원본 사이트

컨텐츠가 처음 만들어진 BI 플랫폼 시스템입니다.

18.2.8 원격

사용자에게 로컬이 아닌 시스템입니다. 예를 들어 대상 사이트의 사용자와 관리자에게는 원본 사이트가 원격인 것으로 간주됩니다.

18.2.9 원격 연결

사용자 이름과 암호, CMS 이름, 웹 서비스 URI 및 정리 옵션을 비롯하여 BI 플랫폼 배포 환경에 연결하는 데 사용되는 정보가 들어 있는 개체입니다.

18.2.10 원격 일정 설정

대상 사이트에서 원본 사이트로 전달되는 일정 요청입니다. 대상 사이트의 보고서를 원격으로 예약할 수 있습니다. 이 경우 보고서 인스턴스를 처리하기 위해 해당 인스턴스가 원본 사이트로 다시 보내집니다. 그런 다음 완료된 인스턴스가 대상 사이트로 반환됩니다.

18.2.11 복제

특정 BI 플랫폼 시스템에서 다른 시스템으로 콘텐츠를 복사하는 과정입니다.

18.2.12 복제 작업

복제 일정, 복제할 콘텐츠, 콘텐츠를 복제할 때 수행해야 할 모든 특별한 작업에 대한 정보가 들어 있는 개체입니다.

18.2.13 복제 목록

복제할 개체의 목록입니다. 복제 목록에서는 BI 플랫폼 배포 환경에서 함께 복제할 사용자, 그룹, 보고서 등의 다른 콘텐츠를 참조합니다.

18.2.14 복제 개체

원본 사이트에서 대상 사이트로 복제되는 개체입니다. 대상 사이트의 모든 복제된 개체에는 복제 아이콘이 표시됩니다. 충돌이 발생한 개체에는 충돌 아이콘이 표시됩니다.

18.2.15 복제 패키지

전송 과정에서 만들어지는 복제 패키지에는 복제 작업의 개체가 포함됩니다. 여기에는 빠르게 변하는 환경이나 초기 복제의 경우에서처럼 복제 목록에 정의된 모든 개체가 포함될 수 있습니다. 또는 복제 작업의 일정에 비해 개체가 자주 변경되지 않는 경우에서처럼 복제 목록의 하위 집합이 포함될 수도 있습니다. 복제 패키지는 BIAR(BI 응용 프로그램 리소스) 파일로 구현됩니다.

18.2.16 복제 새로 고침

마지막으로 수정한 버전과 상관없이 복제 목록의 모든 개체가 새로 고쳐집니다.

18.2.17 양방향 복제

단방향 복제와 동일하게 작동하지만 양방향 복제에서는 변경 내용이 두 방향으로 모두 전달된다는 차이가 있습니다. 원본 사이트의 업데이트 내용이 각 대상 사이트로 복제됩니다. 대상 사이트의 업데이트 내용과 새 개체가 원본 사이트로 전달됩니다.

18.3 보안 권한 관리

연합에서는 개별 배포 간에 콘텐츠를 복제하고 다른 관리자와 공동으로 작업해야 하므로 연합을 사용하기 전에 보안 관련 내용을 이해해야 합니다.

연합을 사용하려면 개별 배포 환경의 관리자가 서로 협력해야 합니다. 관리자는 콘텐츠를 복제한 후 콘텐츠를 변경할 수 있습니다.

일부 작업의 경우 원본 및 대상 배포 환경에 대해 특정 권한을 가지고 있어야 완료할 수 있습니다.

- 원본 사이트에 필요한 권한
- 대상 사이트에 필요한 권한
- 연합 관련 개체에 필요한 권한
- 연합 시나리오

팁:

연합을 사용하기 전에 이 장의 내용을 먼저 읽는 것이 좋습니다.

18.3.1 원본 사이트에 필요한 권한

이 단원에서는 원본 사이트에 대한 작업 및 원본 사이트에 연결하려는 사용자 계정에 필요한 권한에 대해 설명합니다. 이 계정은 대상 사이트의 원격 연결 개체에 입력하는 계정입니다.

작업	설명	필요한 권한
단방향 복제	원본 사이트에서 대상 사이트로만 복제를 수행합니다. 참고: 보기와 복제 권한은 종속성에 따라 자동으로 복제되는 개체를 비롯하여 복제하려는 모든 개체에 대해 필요합니다.	<ul style="list-style-type: none"> • 복제하려는 모든 개체에 대한 보기 및 복제 권한 • 복제 목록에 대한 보기 권한
양방향 복제	원본 사이트에서 대상 사이트로 복제를 수행하고 대상 사이트에서 원본 사이트로 복제를 수행합니다.	<ul style="list-style-type: none"> • 복제하려는 모든 개체에 대한 보기 및 복제 권한 • 복제 목록에 대한 보기 권한 • 암호 변경 사항을 복제하려는 사용자 개체에 대한 권한 수정 권한
일정	대상 사이트에서 원본 사이트에 대한 원격 예약을 허용합니다.	<ul style="list-style-type: none"> • 원격으로 일정을 예약하려는 모든 개체에 대한 일정 권한

관련 항목

- 627 페이지에서 [대상 사이트에 필요한 권한](#)

18.3.2 대상 사이트에 필요한 권한

이 단원에서는 대상 사이트에 적용한 작업과 복제 작업을 실행하는 사용자 계정에 필요한 권한에 대해 설명합니다. 이 계정은 복제 작업을 만든 사용자의 계정입니다.

참고:

예약 가능한 다른 개체와 마찬가지로 다른 사람 대신 복제 작업을 예약할 수 있습니다.

작업	설명	필요한 권한
모든 개체	단방향인지 아니면 양방향인지에 관계없이 개체를 복제합니다.	<ul style="list-style-type: none"> 모든 개체에 대한 보기, 추가, 편집 및 권한 수정 권한 모든 사용자 개체에 대한 사용자 암호 수정 권한
첫 번째 복제	복제 작업을 처음 실행할 때는 대상 사이트에 아직 아무 개체도 없습니다. 따라서 복제 작업을 실행하는 사용자 계정에 콘텐츠를 추가할 모든 최상위 폴더 및 기본 개체에 대해 권한이 있어야 합니다.	<ul style="list-style-type: none"> 최상위 폴더 및 기본 개체 전체에 대한 보기, 추가, 편집 및 권한 수정 권한

관련 항목

- 627 페이지에서 [원본 사이트에 필요한 권한](#)

18.3.3 연합 관련 권한

이 단원에서는 연합과 관련된 시나리오에 대해 자세히 설명합니다.

작업	설명	필요한 권한
개체 정리	개체 정리는 대상 사이트의 개체를 삭제합니다.	<ul style="list-style-type: none"> 복제 작업이 실행 중인 계정은 삭제 가능성이 있는 모든 개체에 대해 삭제 권한을 가지고 있어야 합니다.
특정 개체의 정리 비활성화	<p>원본 사이트의 특정 개체를 복제한 경우 원본 사이트의 개체를 삭제하더라도 대상 사이트에서는 해당 개체를 유지하고자 할 수도 있습니다. 권한을 통해 이러한 개체를 보존할 수 있습니다. 예를 들어 원본 사이트의 사용자에게 종속되지 않은 개체를 대상 사이트의 사용자가 사용하려는 경우 이 옵션을 선택합니다.</p> <p>예를 들어 복제된 유니버스가 있고 대상 사이트의 사용자가 고유한 로컬 보고서를 만드는 데 이 유니버스를 사용한 경우 원본 사이트에서 해당 유니버스가 삭제되더라도 대상 사이트에서는 이를 유지하고자 할 수 있습니다.</p>	<ul style="list-style-type: none"> 유지하려는 개체에 대해 복제 작업을 실행하는 데 사용되는 사용자 계정의 삭제 권한을 거부합니다.
원본 사이트에서 수정 작업 없이 양방향 복제 사용	<p>경우에 따라서는 양방향 복제를 선택하되 대상 사이트의 변경 내용과 상관없이 원본 사이트의 일부 개체가 수정되지 않도록 하고자 할 수 있습니다. 개체의 특수성으로 인해 원본 사이트의 사용자만 개체를 변경할 수 있도록 해야 하는 경우나 원격 예약을 활성화하되 변경 내용이 다시 전파되지 않도록 하려는 경우 등이 있습니다.</p> <p>참고: 원격 예약의 경우 원격 예약 관련 개체만 처리하는 작업을 만들 수 있습니다. 그러나 이 경우에도 보고서, 보고서가 들어 있는 폴더, 해당 폴더의 부모 폴더를 비롯한 상위 개체는 여전히 복제됩니다. 대상 사이트의 모든 변경 내용은 원본 사이트로 복제되고, 원본 사이트의 모든 변경 내용은 대상 사이트로 복제됩니다.</p>	<ul style="list-style-type: none"> 원격 연결 개체의 연결에 사용되는 사용자 계정의 편집 권한을 거부합니다.

18.3.4 개체에 대한 보안 복제

개체에 대한 보안 권한을 유지하려면 개체와 해당 사용자 또는 그룹을 동시에 복제해야 합니다. 아니면 해당 사용자나 그룹이 복제 대상 사이트에 이미 있어야 하고 각 사이트에서 동일한 고유 식별자(CUID)를 갖고 있어야 합니다.

개체만 복제하고 사용자나 그룹을 복제하지 않거나 복제 대상 사이트에 사용자나 그룹이 없으면 관련 권한이 삭제됩니다.

예제

개체 A에 대한 권한이 그룹 A와 그룹 B에 할당되어 있는데, 그룹 A에는 보기 권한이, 그룹 B에는 보기 거부 권한이 있는 경우를 가정합니다. 복제 작업을 통해 그룹 A와 개체 A만 복제하는 경우 대상 사이트에서 개체 A에는 연결된 그룹 A에 대한 보기 권한만 포함됩니다.

개체를 복제할 때 개체에 대한 명시적 권한이 있는 모든 그룹을 복제하지 않으면 보안 위험이 발생할 수 있습니다. 위 예제에서는 그러한 잠재적 위험을 잘 보여 줍니다. 사용자 A가 그룹 A와 그룹 B 모두에 속한 경우 이 사용자에게는 원본 사이트에서 개체 A를 보는 데 필요한 권한이 없습니다. 그러나 사용자 A는 두 그룹에 모두 속해 있으므로 대상 사이트로 복제됩니다. 이때 그룹 B는 복제되지 않았으므로 사용자 A는 원본 사이트에서 개체 A를 볼 수 없음에도 불구하고 대상 사이트에서는 개체 A를 볼 수 있는 권한을 갖습니다.

복제 작업에 포함되지 않은 다른 개체 또는 아직 대상 사이트에 없는 개체를 참조하는 개체가 로그 파일에 표시됩니다. 로그 파일에는 개체가 복제되지 않은 개체를 참조했으며 해당 참조를 삭제한 것으로 표시됩니다.

특정 사용자 또는 그룹에 대한 개체의 보안은 원본 사이트에서 대상 사이트로만 복제됩니다. 대상 사이트에서 복제된 개체에 대한 보안을 설정할 수는 있지만 해당 설정이 원본 사이트로 복제되지 않습니다.

18.3.5 액세스 수준을 사용하여 보안 복제

권한은 유지할 액세스 수준을 사용하여 정의되어야 합니다. 개체, 사용자나 그룹, 액세스 수준을 동시에 복제해야 합니다. 아니면 복제하려는 대상 사이트에 이들 항목이 이미 있어야 합니다.

복제 작업에 포함되지 않았거나 아직 대상 사이트에 없는 사용자 또는 그룹에 명시적으로 권한을 할당하는 개체가 해당 로그 파일에 표시됩니다. 이 로그 파일에는 복제되지 않은 권한이 개체에 할당되었으며 해당 권한이 삭제된 것으로 표시됩니다.

가져온 개체에 대해 사용되는 액세스 수준을 자동으로 복제하도록 선택할 수도 있습니다. 이 옵션은 복제 목록에서 사용할 수 있습니다.

참고:

기본 액세스 수준은 복제되지 않지만 참조는 계속 유지됩니다.

18.4 복제 유형 및 모드 옵션

복제 유형과 복제 모드를 어떻게 선택하느냐에 따라 다음 네 가지 복제 작업 옵션 중 하나를 만들 수 있습니다.

- 단방향 복제
- 양방향 복제
- 원본에서 새로 고침
- 대상에서 새로 고침

18.4.1 단방향 복제

단방향 복제를 사용하면 원본 사이트에서 대상 사이트로 한 방향으로만 콘텐츠를 복제할 수 있습니다. 복제 목록에 있는 원본 사이트의 개체에 대한 모든 변경 내용은 대상 사이트로 전달됩니다. 그러나 대상 사이트의 개체에 대한 변경 내용은 원본 사이트로 다시 전달되지 않습니다.

단방향 복제는 중앙의 단일 BI 플랫폼 배포 환경에서 개체를 만들고 수정하고 관리하는 경우에 가장 적합합니다. 다른 배포 환경에서는 중앙 배포 환경의 콘텐츠를 사용합니다.

단방향 복제를 만들려면 다음 옵션을 선택합니다.

- 복제 유형 = 단방향 복제
- 복제 모드 = 일반 복제

18.4.2 양방향 복제

양방향 복제를 사용하면 원본 사이트와 대상 사이트 사이에서 양방향으로 콘텐츠를 복제할 수 있습니다. 원본 사이트 개체의 모든 변경 내용이 대상 사이트에 복제되고, 대상 사이트의 모든 변경 내용이 원본 사이트에 복제됩니다.

참고:

원격 일정 설정을 수행하고 로컬에서 실행된 인스턴스를 다시 원본 사이트로 복제하려면 양방향 복제 모드를 선택해야 합니다.

여러 BI 플랫폼 배포 환경에서 콘텐츠를 만들고 수정하고 관리하며 두 위치 모두에서 콘텐츠를 사용하는 경우에는 양방향 복제를 사용하는 것이 가장 효율적입니다. 이렇게 하면 배포를 동기화할 수도 있습니다.

양방향 복제를 만들려면 다음 옵션을 선택합니다.

- 복제 유형 = 양방향 복제
- 복제 모드 = 일반 복제

관련 항목

- 656 페이지에서 [원격 일정 설정 및 로컬에서 실행되는 인스턴스](#)"

18.4.3 원본에서 새로 고침 또는 대상에서 새로 고침

단방향 또는 양방향 복제 모드로 콘텐츠를 복제하면 복제 목록에 있는 개체가 대상 사이트로 복제됩니다. 그러나 복제 작업을 실행할 때마다 모든 개체를 복제할 수는 없습니다.

연합에는 복제 작업을 더 빨리 마치는 데 도움이 되도록 설계한 최적화 엔진이 있습니다. 여기서는 개체의 버전과 타임스탬프를 함께 사용하여 마지막 복제 이후 개체가 수정되었는지 여부를 확인합니다. 이 확인 작업은 복제 목록에서 특별히 선택한 개체와 종속성 확인을 진행하는 동안 복제된 모든 개체에 대해 수행됩니다.

그러나 경우에 따라서는 최적화 엔진에서 개체를 발견하지 못하여 개체가 복제되지 않을 수도 있습니다. 이러한 경우 원본에서 새로 고침과 대상에서 새로 고침을 사용하여 타임스탬프와 상관없이 복제 작업을 적용하여 콘텐츠 및 해당 종속성을 복제할 수 있습니다.

"원본에서 새로 고침"은 원본 사이트의 콘텐츠를 대상 사이트로 보내는 작업만 수행하고, "대상에서 새로 고침"은 대상 사이트의 콘텐츠를 원본 사이트로 보내는 작업만 수행합니다.

예제

다음 세 가지 예제에서는 최적화 과정에서 특정 개체가 누락되었을 때 원본에서 새로 고침과 대상에서 새로 고침을 사용하는 시나리오를 보여 줍니다.

시나리오 1: 다른 개체가 포함된 개체를 복제하려는 영역에 추가합니다.

폴더 A를 원본 사이트에서 대상 사이트로 복제했습니다. 이제 이 폴더는 두 사이트에 모두 존재합니다. 보고서 B가 들어 있는 폴더 B를 사용자가 원본 사이트의 폴더 A로 이동하거나 복사합니다. 다음 번 복제 과정에서 폴더 B의 타임스탬프가 변경되었음을 연합을 통해 확인하고 이를 대상 사이트로 복제합니다. 그러나 보고서 B의 타임스탬프는 변경되지 않은 상태입니다. 따라서 일반적인 단방향 또는 양방향 복제 작업에서는 보고서 B가 누락됩니다.

폴더 B의 콘텐츠를 제대로 복제하려면 원본에서 새로 고침을 복제 작업에 한 차례 사용해야 합니다. 그런 다음 일반적인 단방향 또는 양방향 복제 작업을 수행하면 이 개체가 올바르게 복제됩니다. 이 예제와는 반대되는 상황에서 대상 사이트에 폴더 B를 이동했거나 복사한 경우에는 대상에서 새로 고침을 사용합니다.

시나리오 2: 주기 관리자나 BIAR 명령줄을 사용하여 새 개체를 추가합니다.

주기 관리자나 BIAR 명령줄을 사용하여 복제하려는 영역에 개체를 추가하는 경우에는 일반적인 단방향 또는 양방향 복제 작업을 통해 해당 개체를 선택하지 못할 수 있습니다. 주기 관리자나 BIAR 명령줄을 사용할 때 원본 시스템과 대상 시스템의 내부 클록이 동기화되지 않았을 때 이러한 문제가 발생할 수 있습니다.

참고:

원본 사이트에서 복제하려는 영역으로 새 개체를 가져온 다음에는 원본에서 새로 고침 복제 작업을 실행하는 것이 좋습니다. 대상 사이트에서 복제하려는 영역으로 새 개체를 가져온 다음에는 대상에서 새로 고침 복제 작업을 실행하는 것이 좋습니다.

시나리오 3: 예약된 복제 시간 사이에 일어날 수 있는 상황입니다.

복제하려는 영역에 개체를 추가해야 하지만 예약된 다음 번 복제 시간까지 기다릴 수 없는 경우 원본에서 새로 고침 및 대상에서 새로 고침 복제 작업을 사용할 수 있습니다. 개체가 추가된 영역을 선택하면 콘텐츠를 신속하게 복제할 수 있습니다.

참고:

- 복제 목록이 큰 경우 이 작업을 수행하는 데 많은 비용이 들 수 있으므로 이 시나리오는 자주 사용하지 않는 것이 좋습니다. 예를 들어, 원본에서 새로 고침이나 대상에서 새로 고침 모드를 사용하여 매시간 실행되는 복제 작업을 만들 필요는 없습니다. 이러한 모드는 지금 실행하거나 비정기 일정으로 사용해야 합니다.
- 충돌 해결을 사용할 수 없는 경우도 있습니다. 예를 들어, 원본에서 새로 고침을 사용하면 대상 사이트에서 실행 옵션이 차단되고, 대상에서 새로 고침을 사용하면 원본 사이트에서 실행 옵션이 차단됩니다.

18.5 타사 사용자 및 그룹 복제

연합에서 타사 사용자와 그룹을 복제할 수 있습니다. 특히 AD(Active Directory) 및 LDAP 사용자와 그룹이 여기에 해당합니다.

팁:

이러한 유형의 사용자와 그룹을 복제하거나 즐겨찾기 폴더 또는 받은 파일함 같은 해당 개인 콘텐츠를 복제하려면 이 단원의 내용을 참조하십시오.

사용자 및 그룹 매핑

1. 연합에서 사용자와 그룹을 올바르게 복제할 수 있도록 원본 사이트의 사용자와 그룹을 매핑해야 합니다.

2. 그런 다음 매핑된 사용자와 그룹을 대상 사이트로 복제합니다.

참고:

대상 사이트에서 그룹과 사용자를 개별적으로 매핑하지 마십시오. 그렇게 하면 그룹과 사용자가 대상 및 원본 사이트에서 서로 다른 고유 식별자(CUID)를 갖게 되므로 연합에서 사용자나 그룹을 일치시킬 수 없게 됩니다.

예제

관리자가 원본 사이트와 대상 사이트에서 사용자 A가 포함된 그룹 A를 매핑합니다. 그룹 A와 사용자 A 모두 원본 및 대상 사이트에서 서로 다른 고유 식별자를 갖게 됩니다. 복제 과정에서 연합을 통해 이들을 일치시킬 수 없으므로 별칭이 충돌하여 그룹 A나 사용자 A가 복제되지 않습니다.

참고:

- 타사 사용자 및 그룹을 복제하려면 먼저 AD 또는 LDAP 인증을 사용하도록 대상 사이트를 설정해야 합니다. 여기에 더해 AD 또는 LDAP를 사용하도록 대상 사이트를 구성하여 디렉터리 서버나 도메인 컨트롤러와 통신할 수 있도록 해야 합니다.
- AD 또는 LDAP 그룹을 처음 복제한 후에는 AD/LDAP 그룹 그래프를 새로 고쳐야 해당 그룹의 사용자가 로그인할 수 있습니다. 이 작업은 대략 15분마다 자동으로 수행됩니다. AD/LDAP 그룹 그래프를 수동으로 새로 고치려면 CMC의 인증 페이지로 이동하고 Windows AD 또는 LDAP를 두 번 클릭한 다음 업데이트를 클릭합니다.
- 타사 그룹을 복제할 때는 특히 주의해야 합니다. 디렉터리 서버의 그룹에 새 사용자를 추가하는 경우 이 사용자는 두 사이트 모두에 로그인할 수 있습니다. AD 또는 LDAP 인증의 이러한 보안 문제는 연합과는 관계가 없습니다.

대상 및 원본 사이트에 개별적으로 로그인하거나 CMC 인증 페이지의 업데이트 단추를 사용하여 두 사이트 모두에서 소속 그룹을 업데이트하면 두 사이트 모두에 사용자 계정이 만들어집니다. 이들 계정은 고유 ID가 서로 다르므로 연합에서 이러한 사용자 계정을 올바르게 복제할 수 없게 됩니다.

참고:

사이트 중 하나에 계정을 만든 다음 다른 사이트에 복제해야 합니다.

18.6 유니버스 및 유니버스 연결 복제

연합에서 BI 플랫폼 배포 간에 유니버스를 복제하는 경우 먼저 계획을 세워야 합니다. 기본 유니버스 연결 없이는 유니버스 개체가 작동할 수 없습니다.

유니버스 연결 개체에는 보고서 작성 데이터베이스에 필요한 정보가 들어 있습니다. 제대로 작동하려면 유니버스 연결 개체에 올바른 정보가 포함되고 이러한 개체를 통해 데이터베이스 연결이 설정되어야 합니다.

참고:

양방향 복제를 사용하는 경우 해당 유니버스 연결을 제외한 채로 원본 사이트에서 대상 사이트로 유니버스를 복제하면 이후 복제에서 원본 사이트의 유니버스와 원본 사이트의 유니버스 연결 간의 관계를 덮어쓰거나 제거할 수 있습니다. 이러한 문제가 발생하지 않게 하려면 항상 유니버스와 함께 유니버스 연결을 복제해야 합니다.

종속된 유니버스 연결이 유니버스와 함께 복제되도록 하려면 유니버스를 포함하는 복제 목록을 만들거나 수정할 때 항상 다음 옵션을 선택하십시오.

- 선택한 유니버스에 사용되는 연결 포함
- 선택한 유니버스에 필요한 유니버스 포함

참고:

유니버스와 해당 유니버스 연결의 관계가 덮어쓰지거나 제거된 경우 Universe Designer를 열고 파일 > 매개 변수 아래에서 연결 정보를 수정합니다.

다음 두 예제에서는 유니버스와 관련 유니버스 연결을 복제하는 과정을 보여 줍니다.

예제

유니버스와 유니버스 연결을 복제할 때는 원본 사이트의 연결 환경이 대상 사이트의 연결 환경과 일치하는지 확인해야 합니다.

예를 들어 유니버스 연결에 TestODBC라는 ODBC 연결이 사용되는 경우, 대상 환경에도 올바르게 구성된 TestODBC라는 ODBC 연결이 있어야 합니다. ODBC 연결은 동일한 데이터베이스나 서로 다른 데이터베이스로 확인될 수 있습니다. 이 연결을 사용하는 유니버스에 연결 문제가 발생하지 않게 하려면 데이터베이스의 스키마가 동일해야 합니다.

예제

대상 사이트의 복제된 유니버스에 원본 사이트의 유니버스와 다른 데이터베이스가 사용되도록 하려면 유니버스 연결을 복제하되 대상 사이트의 연결 정보가 원하는 데이터베이스를 가리키도록 설정하십시오.

예를 들어 원본 사이트의 유니버스 연결에 DatabaseA를 가리키는 Test라는 ODBC 연결이 사용되는 경우 대상 사이트에도 DatabaseB를 가리키는 Test라는 ODBC 연결이 사용되도록 하십시오.

18.7 복제 목록 관리

복제 목록에는 BI 플랫폼 배포에서 함께 복제할 수 있는 사용자, 그룹, 보고서 등의 콘텐츠가 포함됩니다. 복제 목록은 CMC를 통해 액세스할 수 있습니다.

다음 표에는 복제할 수 있는 콘텐츠 유형이 설명되어 있습니다.

범주	지원되는 개체
리포지토리 개체	비즈니스 뷰, 데이터 연결, LOV, 데이터 기반 등을 포함하는 개체입니다. 참고: 개별 수준은 아니더라도 모든 개체가 지원됩니다.
보고서	Crystal 보고서, Web Intelligence 문서, Xcelsius 개체 참고: Full Client 추가 기능 및 템플릿이 지원됩니다.
타사 개체	Excel, PDF, PowerPoint, Flash, Word, 텍스트 파일, 서식 있는 텍스트 파일, Shockwave Flash 파일
사용자	사용자, 그룹, 받은 파일함, 즐겨찾기, 개인 범주
Business Intelligence 플랫폼	폴더, 이벤트, 범주, 달력, 사용자 지정 역할, 하이퍼링크, 바로 가기, 프로그램, 프로필, 개체 패키지, 알 수 없음
유니버스	유니버스, 연결, 유니버스 오버로드

[참고:](#)

다음 개체를 원본 사이트에서 만든 다음 대상 사이트에 복제해야 합니다. 이러한 개체를 대상 사이트에서 만든 다음 원본 사이트로 복제하면 원본 사이트에서 개체가 제대로 작동하지 않을 수 있습니다.

- 비즈니스 뷰
- 비즈니스 요소
- 데이터 기반
- 데이터 연결
- 값 목록
- 유니버스 오버로드

18.7.1 복제 목록 만들기

복제 목록은 CMC의 복제 목록 영역에 있습니다. 만든 폴더 및 하위 폴더에서 복제 목록을 구성할 수 있습니다.

18.7.1.1 복제 목록 폴더 만들기

1. CMC의 복제 목록 영역으로 이동합니다.
2. 복제 목록을 클릭합니다.
3. 관리 > 새로 만들기 > 폴더를 클릭합니다.
폴더 만들기 대화 상자가 나타납니다.
4. 폴더 이름을 입력하고 확인을 클릭합니다.
그러면 이 폴더에서 복제 목록을 만들 수 있습니다.

18.7.1.2 복제 목록 만들기

1. CMC의 복제 목록 영역으로 이동합니다.
2. 새 복제 목록을 저장할 폴더를 선택합니다.
3. 관리 > 새로 만들기 > 새 복제 목록을 클릭합니다.
새 복제 목록 대화 상자가 나타납니다.
4. 복제 목록에 대한 제목과 설명을 입력합니다.
5. 고급 옵션을 설정하려면 복제 목록 속성 링크를 클릭합니다.
그러면 원본 사이트에서 대상 사이트로 자동 복제될 종속성을 지정할 수 있습니다.
6. 다음 표의 설명을 참조하여 필요한 옵션을 선택합니다.

종속성 개체 옵션	정의
선택한 사용자에게 대한 개인 폴더 포함	선택한 사용자의 개인 폴더와 그 콘텐츠를 복제합니다.
선택한 사용자에게 대한 개인 범주 포함	선택한 사용자의 개인 범주를 복제합니다.
선택한 보고서에 대한 유니버스 포함	선택한 보고서 개체가 종속된 모든 유니버스를 복제합니다.
선택한 사용자 그룹의 멤버 포함	선택한 그룹에 속한 사용자를 복제합니다.
선택한 유니버스에 필요한 유니버스 포함	다른 유니버스에 종속된 모든 유니버스를 복제합니다.
선택한 사용자에게 대한 받은 파일함 포함	선택한 사용자의 받은 파일함과 그 콘텐츠를 복제합니다.

종속성 개체 옵션	정의
선택한 유니버스에 대한 사용자 그룹 포함	유니버스의 오버로드와 관련된 사용자 그룹을 복제합니다.
선택한 개체에 설정된 액세스 수준 포함	선택한 개체 하나에라도 사용된 모든 액세스 수준을 복제합니다.
선택한 범주에 대한 문서 포함	Word, Excel 및 PDF를 비롯하여 선택한 범주에 포함된 모든 문서를 복제합니다.
선택한 Flash 개체에 대해 지원되는 종속성 포함	Flash 개체가 종속된 모든 Crystal 보고서, 하이퍼링크, Web Intelligence 문서 또는 유니버스를 복제합니다.
선택한 사용자 및 사용자 그룹에 대한 프로필 포함	선택한 사용자나 그룹과 관련된 모든 프로필을 복제합니다.
선택한 유니버스에 사용된 연결 포함	선택한 개체에 사용된 모든 유니버스 연결 개체를 복제합니다.

참고:

BI 플랫폼의 일부 개체는 다른 개체에 종속되어 있습니다. 예를 들어 Web Intelligence 문서는 구조, 콘텐츠 등이 기본 유니버스에 종속됩니다. Web Intelligence 문서를 복제할 때 이 보고서에 사용되는 유니버스를 선택하지 않으면, 해당 유니버스가 아직 대상 사이트에 복제되지 않은 경우 대상 사이트에서 복제가 수행되지 않습니다. 단, 선택한 보고서에 대한 유니버스 포함을 활성화한 경우 보고서가 종속된 유니버스가 연합에서 자동으로 복제됩니다.

7. 다음을 클릭합니다.

8. 복제 목록에 추가할 개체를 하나 이상 선택합니다.

- 화살표 단추를 사용하여 사용 가능한 개체 폴더에서 개체를 추가하거나 제거합니다.
- 모두 복제: 리포지토리 개체를 클릭하여 보고서 이미지와 함수를 비롯한 모든 비즈니스 뷰, 비즈니스 요소, 데이터 기반, 데이터 연결, 값 목록 및 리포지토리 개체를 복제할 수도 있습니다.

참고:

사용 가능한 개체 폴더에 있는 최상위 폴더는 복제할 수 없습니다.

9. 저장 후 단기를 클릭합니다.

18.7.2 복제 목록 수정

복제 목록을 만든 후에는 해당 속성이나 개체를 수정할 수 있습니다.

18.7.2.1 복제 목록의 속성 수정

1. CMC의 복제 목록 영역으로 이동합니다.
2. 수정할 복제 목록을 선택합니다.
3. 관리 > 속성을 클릭합니다.
일반 속성 대화 상자가 나타납니다.
4. 제목과 설명을 수정합니다. 일반 속성 대화 상자를 열어 둔 상태에서 복제 목록의 다른 영역을 수정할 수도 있습니다.
5. 종속성 옵션을 수정하려면 탐색 목록에서 복제 목록 속성을 클릭합니다.
6. 저장 후 닫기를 클릭합니다.

관련 항목

- 636 페이지에서 [복제 목록 만들기](#)

18.7.2.2 복제 목록의 개체 수정

1. CMC의 복제 목록 영역으로 이동합니다.
2. 복제 목록을 선택합니다.
3. 작업 > 복제 목록 관리를 클릭합니다.
복제 목록에 포함된 개체 목록과 함께 복제 목록 관리 대화 상자가 나타납니다.
4. 원하는 대로 개체를 추가하거나 제거합니다.
5. 저장 후 닫기를 클릭합니다.

관련 항목

- 636 페이지에서 [복제 목록 만들기](#)

18.8 원격 연결 관리

원격 연결 개체에는 원격 BI 플랫폼 배포 환경에 연결하는 데 필요한 정보가 들어 있습니다.

참고:

원격 연결 개체는 대상 사이트 BI 플랫폼 배포에서 만들어지며, 원격 연결은 원본 사이트에서 설정됩니다.

CMC의 연합 영역에서 원격 연결을 확인할 수 있습니다.

18.8.1 원격 연결 만들기

연합에서 원격 연결을 설정하면 원격 BI 플랫폼 배포 환경에 연결됩니다. 복제할 콘텐츠가 있는 원본 사이트에 대한 연결을 설정하려면 먼저 대상 사이트에서 원격 연결을 만들어야 합니다.

폴더 및 하위 폴더를 만들어 원격 연결을 구성할 수 있습니다.

18.8.1.1 원격 연결 폴더 만들기

1. CMC의 연합 영역으로 이동합니다.
2. 원격 연결을 클릭합니다.
3. 관리 > 새로 만들기 > 폴더를 클릭합니다.
폴더 만들기 대화 상자가 나타납니다.
4. 폴더 이름을 입력하고 확인을 클릭합니다.
그러면 이 폴더에서 원격 연결을 만들 수 있습니다.

18.8.1.2 원격 연결 만들기

원격 BI 플랫폼 배포 환경에 연결하려면 연합에서 원격 연결을 만들어야 합니다.

1. CMC의 연합 영역으로 이동합니다.
2. 원격 연결을 클릭합니다.
3. 관리 > 새로 만들기 > 새 원격 연결을 클릭합니다.
새 원격 시스템 연결 대화 상자가 나타납니다.
4. 제목을 입력하고 필요에 따라 설명과 관련 필드를 입력합니다.

참고:

설명과 정리 개체의 수를 다음으로 제한을 제외한 모든 필드는 필수입니다.

필드	설명
제목	원격 연결 개체의 이름입니다.
설명	원격 연결 개체에 대한 설명입니다. (옵션)
원격 시스템 웹 서비스 URI	Java 응용 프로그램 서버에 자동으로 배포되는 연합 웹 서비스의 URL입니다. 원본 사이트인지 대상 사이트인지 또는 다른 배포 환경인지 여부에 관계없이 BI 플랫폼에서 모든 연합 웹 서비스를 사용할 수 있습니다. 이때 사용할 형식은 <code>http://application_yourserver_machine_name:port/dswsbobje</code> 입니다. 예를 들면 <code>http://mymachine.mydomain.com:8080/dswsbobje</code> 와 같이 사용할 수 있습니다.
원격 시스템 CMS	연합 웹 서비스를 통해 액세스할 수 있도록 연결할 CMS의 이름입니다. 이는 원본 사이트의 CMS로 처리됩니다. 형식은 <code>CMS_이름:포트</code> (예: <code>mymachine:6400</code>)입니다. 참고: 기본 포트인 6400을 사용하는 경우 포트 지정은 옵션입니다.
사용자 이름	원본 사이트에 연결하는 데 사용할 사용자 이름입니다. 참고: 사용하려는 사용자 이름은 원본 사이트 배포의 복제 목록에 대해 보기 권한을 가져야 합니다.
암호	원본 사이트에 연결하는 데 사용할 사용자 계정의 암호입니다.
인증	원본 사이트에 연결하는 데 사용할 계정 인증의 유형입니다. Enterprise, AD 또는 LDAP 중에서 선택할 수 있습니다.

필드	설명
정리 간격(시간)	이 원격 연결 개체를 사용하는 복제 작업을 통해 개체 정리를 수행할 간격입니다. 여기에는 양의 정수만 입력해야 합니다. 값은 시간 단위입니다. 기본값은 24입니다.
정리 개체의 수를 다음으로 제한	복제 작업을 통해 정리할 개체의 수입니다. (옵션)

5. 확인을 클릭합니다.

관련 항목

- 647 페이지에서 [개체 정리 관리](#)"

18.8.2 원격 연결 수정

원격 연결을 만든 후에는 해당 속성과 보안 옵션을 수정할 수 있습니다.

원격 연결 수정

1. CMC의 연합 영역으로 이동합니다.
2. 원격 연결을 클릭합니다.
3. 수정할 원격 연결을 두 번 클릭합니다.

원격 연결 속성 대화 상자가 나타납니다. 다음 속성을 수정할 수 있습니다.



- 제목
- 설명
- 원격 시스템 웹 서비스 URI
- 원격 시스템 CMS
- 사용자 이름
- 암호
- 인증
- 정리 간격(시간)
- 정리 개체의 수를 다음으로 제한

4. 변경 사항을 지정합니다.
5. 저장 후 단기를 클릭합니다.

18.9 복제 작업 관리

복제 작업은 일정에 따라 실행되는 개체 유형이며, 연합에서 두 BI 플랫폼 배포 간에 콘텐츠를 복제하는 데 사용됩니다.

참고:

대상 사이트의 복제된 개체에는  과 같은 복제 아이콘이 플래그로 설정됩니다. 충돌이 발생하면 개체에  과 같은 충돌 아이콘이 플래그로 설정됩니다.

CMC의 연합 영역에 있는 원격 연결 폴더에서 복제 작업 목록을 확인할 수 있습니다.

18.9.1 복제 작업 만들기

연합에서 두 BI 플랫폼 배포 간에 콘텐츠를 복제하려면 복제 작업이 필요합니다. 각 복제 작업에는 원격 연결과 복제 목록이 하나씩만 연결되어야 합니다.

18.9.1.1 복제 작업 만들기

1. CMC의 연합 영역으로 이동합니다.
2. 원격 연결을 클릭합니다.
3. 새 복제 작업을 포함할 원격 연결을 선택합니다.

주의:

마법사를 사용하여 작업을 계속하려면 CMC에서 원격 연결 URI의 웹 서비스에 연결할 수 있어야 합니다.

4. 관리 > 새로 만들기 > 새 복제 작업을 클릭합니다.
새 복제 작업 대화 상자가 열립니다.
5. 복제 작업에 대한 제목과 설명을 입력합니다.
6. 다음을 클릭합니다.
원본 사이트에서 사용 가능한 복제 목록이 나타납니다.
7. 복제 작업에 사용할 복제 목록을 선택합니다.
8. 다음을 클릭합니다.
9. 다음 표의 설명을 참조하여 구성 옵션을 선택합니다.

옵션	설명
대상에서 개체 정리 허용	원본 사이트에서 원래 개체를 제거한 경우 대상 사이트의 모든 복제된 개체를 복제 작업에서 삭제할 수 있도록 합니다. 참고: 종속성에 따라 복제했거나 복제 목록에서 선택한 개체는 개체 정리에 서 삭제되지 않습니다.
단방향 복제	원본 사이트에서 대상 사이트로만 개체를 복제하도록 지정합니다. 복 제 후 원본 사이트의 개체를 변경하면 변경 내용이 대상 사이트로 복제 되지만 대상 사이트에서 수행한 변경 내용은 원본 사이트로 다시 복제 되지 않습니다.
양방향 복제	개체를 두 방향으로 모두 복제하도록 지정합니다. 즉, 개체를 원본 사 이트에서 대상 사이트로 복제하고 대상 사이트에서 원본 사이트로도 복제합니다. 복제 후에 한 사이트에서 이 개체를 변경하면 그 내용이 자동으로 다른 사이트에 복제됩니다.
원본 사이트 먼저 적용	원본 사이트의 개체와 대상 사이트의 복제된 버전 사이에 충돌이 발견 된 경우 원본 사이트의 개체가 우선 적용되도록 지정합니다.
자동 충돌 해결 사용 안 함	충돌이 감지되더라도 이를 해결하기 위한 어떠한 조치도 취하지 않도 록 지정합니다.
대상 사이트 먼저 적용(양 방향 복제에서만 사용 가 능)	원본 사이트의 개체와 대상 사이트의 복제된 버전 사이에 충돌이 발견 된 경우 대상 사이트의 개체가 우선 적용되도록 지정합니다.
일반 복제	일반적인 방식으로 복제 작업을 수행하도록 지정합니다.
원본에서 새로 고침	컨텐츠 변경 여부에 관계없이 원본 사이트에서 대상 사이트로 모든 컨 텐츠를 복제합니다. 복제 목록 일부 또는 전체를 복제할 수 있습니다.
대상에서 새로 고침(양방 향 복제에서만 사용 가능)	컨텐츠 변경 여부에 관계없이 대상 사이트에서 원본 사이트로 모든 컨 텐츠를 복제합니다. 복제 목록 일부 또는 전체를 복제할 수 있습니다.
모든 개체 복제(양방향 복 제에서만 사용 가능)	전체 복제 목록을 복제합니다. 참고: 이는 가장 완전한 옵션이지만 수행하는 데 시간이 가장 오래 걸립니다.
원격 일정 복제(양방향 복 제에서만 사용 가능)	보류 중인 원격 인스턴스를 대상 사이트에서 원본 사이트로 복제하고 완료된 인스턴스를 원본 사이트에서 대상 사이트로 복제합니다.
문서 템플릿 복제	인스턴스가 아닌 모든 개체(로컬에서 실행되는 개체나 원격 일정 설정 과 관련하여 선택한 보고서)를 복제합니다. 여기에는 사용자, 그룹, 폴 더, 보고서 등이 포함됩니다.
로컬에서 실행되는 완료 된 인스턴스 복제	완료된 인스턴스를 대상 사이트에서 원본 사이트로만 복제합니다.

10. 확인을 클릭합니다.

관련 항목

- 647 페이지에서 [개체 정리 관리](#)"
- 649 페이지에서 [충돌 감지 및 해결 관리](#)"
- 656 페이지에서 [원격 일정 설정 및 로컬에서 실행되는 인스턴스](#)"

18.9.2 복제 작업 예약

복제 작업을 만든 후에는 이 작업을 한 번만 실행하거나 정기적으로 실행하도록 예약할 수 있습니다. 원본 사이트 하나에서 대상 사이트 하나에 대해 여러 개의 복제 작업을 예약할 수도 있습니다.

참고:

대상 사이트 하나에서 여러 개의 복제 작업을 예약하더라도 한 번에 한 개의 복제 작업만 원본 사이트에 연결할 수 있습니다. 연결을 시도하는 다른 모든 복제 작업은 보류 중 상태로 전환되고 원본 사이트에 자동으로 연결할 수 있게 될 때까지 보류 중 상태로 유지됩니다.

18.9.2.1 복제 작업 예약

1. CMC의 연합 영역으로 이동합니다.
2. 예약할 복제 작업을 선택합니다.
3. 작업 > 일정을 클릭합니다.
4. 원하는 예약 옵션을 선택합니다.

18.9.3 복제 작업 수정

연합에서 복제 작업을 만든 후에는 해당 속성을 수정할 수 있습니다.

18.9.3.1 복제 작업 수정

1. CMC의 연합 영역으로 이동합니다.
2. 원격 연결 폴더를 클릭합니다.
3. 수정하려는 복제 작업이 포함된 원격 연결 개체를 선택합니다.
4. 수정할 복제 작업을 선택합니다.
5. 관리 > 개체 속성 관리를 클릭합니다.
6. 속성, 일정, 기록, 복제 목록 및 사용자 보안을 확인하고 필요에 따라 편집합니다.

섹션	설명
속성	복제 작업의 이름, 설명 및 기타 일반적인 속성과 옵션을 수정합니다.
일정	되풀이되는 일정에 따라 복제 작업을 실행하도록 설정합니다.
기록	복제 작업의 모든 인스턴스를 보고 관리합니다.
복제 목록	선택된 복제 목록을 변경합니다.
사용자 보안	복제 작업에 대한 권한을 설정합니다.

18.9.4 복제 작업 후 로그 보기

복제 작업을 실행할 때마다 연합에서 로그 파일이 자동으로 생성됩니다. 이 로그 파일은 대상 사이트에 저장됩니다. 로그 파일에서는 XML 1.1 표준을 사용하며 XML 1.1을 지원하는 웹 브라우저가 필요합니다.

복제 로그 보기

1. CMC의 연합 영역으로 이동합니다.
2. 모든 복제 작업을 클릭합니다.
3. 목록에서 복제 작업을 선택합니다.
4. 속성을 클릭합니다.
복제 작업 속성 페이지가 열립니다.

5. 기록을 클릭합니다.
6. 성공한 복제 작업을 보려면 로그 파일의 인스턴스 시간을 클릭하고, 실패한 복제 작업의 로그 파일을 보려면 실패 상태를 클릭합니다.
7. 로그 파일을 보려는 인스턴스를 선택합니다.
로그 파일이 XML 형식으로 생성되고, 이때 정보를 HTML 페이지로 표시하기 위해 XSL 양식이 사용됩니다.
적용 작업 서버가 포함되어 있는 Server Intelligence Agent를 실행하는 컴퓨터에서 XML 로그에 액세스할 수 있습니다. 로그 파일의 위치는 다음과 같습니다.
 - Windows:<InstallDir>WSAP BusinessObjects XI 4.0Wlogging
 - Unix:<InstallDir>/sap_bobj/logging

18.10 개체 정리 관리

연합에서는 복제 프로세스의 수명 주기 동안 계속 개체 정리를 수행하여 원본 사이트에서 삭제한 모든 개체가 각 대상 사이트에서도 삭제되도록 해야 합니다.

개체 정리에는 원격 연결과 복제 작업이라는 두 가지 요소가 관여합니다. 원격 연결 개체는 일반적인 정리 옵션을 정의하고, 복제 작업은 적절한 간격을 두고 정리 작업을 수행합니다.

18.10.1 개체 정리 사용 방법

동일한 원격 연결을 사용하는 개별 복제 작업은 개체 정리 과정에서 함께 수행됩니다. 즉, 복제 작업에서 해당 복제 목록에 포함된 개체를 정리할 뿐만 아니라 동일한 원격 연결을 사용하는 다른 복제 목록 내의 개체도 정리합니다. 원격 연결은 복제 작업의 상위가 동일한 원격 연결 개체인 경우에만 동일한 것으로 간주됩니다.

예제

복제 작업 A와 B에서 개체 A와 개체 B를 복제하고, 이 두 작업은 모두 동일한 원본 사이트에서 복제를 수행하며 동일한 원격 연결을 사용한다고 가정합니다. 원본 사이트에서 개체 B를 삭제하면 복제 작업 A는 개체 B가 삭제되었는지 확인합니다. 복제 작업 B는 개체를 복제하는 작업이지만 개체 B도 대상 사이트에서 제거됩니다. 복제 작업 B를 실행할 때 개체 정리를 수행할 필요가 없습니다.

참고:

개체 정리 과정에서는 대상 사이트의 개체만 삭제됩니다. 복제의 일부인 개체를 원본 사이트에서 제거하면 해당 개체가 대상 사이트에서 제거됩니다. 그러나 대상 사이트에서 제거한 개체는 개체를 정리할 때 원본 사이트에서 제거되지 않으며, 이는 복제 작업을 양방향 복제 모드로 수행하는 경우에도 마찬가지입니다.

복제 목록에서 삭제되거나 제거된 개체는 대상 사이트에서 삭제되지 않습니다. 복제 목록에 지정된 개체를 올바르게 제거하려면 해당 개체를 대상 사이트와 원본 사이트에서 모두 삭제해야 합니다. 종속 관계에 따라 복제 대상에 함께 포함되었던 개체는 삭제되지 않습니다.

18.10.2 개체 정리 제한

원격 연결 개체에서 복제 작업을 통해 한 번에 정리할 개체의 수를 정의할 수 있습니다. 연합을 사용하면 정리 작업이 어디에서 끝났는지 자동으로 추적할 수 있습니다. 따라서 다음 번에 복제 작업을 실행할 때 해당 지점부터 정리 작업을 다시 시작할 수 있습니다.

팁:

복제 작업을 더 빠르게 완료하려면 정리할 개체의 수를 제한하면 됩니다.

예제

복제 작업 A와 B에서 개체 A와 개체 B를 복제하고, 두 개체를 모두 동일한 원본 사이트에서 복제하며 두 복제 작업에 모두 동일한 원격 연결을 사용한다고 가정합니다.

개체 제한을 1로 설정한 경우 원본 사이트에서 개체 B를 삭제하면 다음 번에 복제 작업 A를 실행할 때 개체 A의 삭제 여부만 확인됩니다. 이와 같이 개체 B의 삭제 여부가 확인되지 않으므로 이 개체는 삭제되지 않습니다.

다시 복제 작업 B를 실행하면 복제 작업 A가 끝난 지점에서 개체 정리가 시작됩니다. 이번에는 개체 B의 삭제 여부를 확인하고 이 개체를 대상 사이트에서 제거합니다. 이 옵션은 원격 연결 개체의 정리 개체의 수를 다음으로 제한: 속성에서 설정할 수 있습니다.

참고:

이 옵션을 선택하지 않으면 해당 원격 연결을 사용하는 모든 복제 작업에서 정리 대상에 포함될 수 있는 모든 개체가 확인됩니다.

18.10.3 개체 정리 간격

원격 연결 정리 간격 필드에서 복제 작업을 통한 개체 정리 간격을 설정할 수 있습니다.

참고:

이 필드에는 개체 정리를 수행하는 각 처리 작업 사이에 몇 시간이나 대기할지 나타내는 값을 양의 정수로 입력해야 합니다.

예제

복제 작업 A와 B에서 개체 A와 개체 B를 복제하고, 두 개체를 모두 동일한 원본 사이트에서 복제하며 두 복제 작업에 모두 동일한 원격 연결을 사용한다고 가정합니다.

개체 B가 원본 사이트에서 삭제되고 다음 조건이 모두 참일 경우, 복제 작업은 개체 A가 삭제되었는지 확인합니다.

- 개체 제한은 1입니다.
- 정리 간격은 150시간입니다.
- 복제 작업 A가 다음에 실행됩니다.

개체 제한이 1로 설정되어 있으므로 개체 B는 대상 사이트에서 확인 또는 삭제되지 않습니다.

다음 번 정리 작업은 복제 작업 A를 통해 처음 검사를 수행한 후 150시간이 지나야 시작됩니다. 150시간이 지나기 전에는 복제 작업 A와 B를 여러 번 실행해도 개체 정리가 실행되지 않습니다. 150시간이 지나면 다음 복제 작업이 실행되고 정리가 시도됩니다. 그런 다음 원본 사이트에서 개체 B가 삭제되었는지 확인하고 대상 사이트에서 삭제합니다.

옵션 활성화 및 비활성화

각 복제 작업이 개체 정리에 관여할 수 있습니다. 복제 작업에 대해 대상에서 개체 정리 허용 옵션을 사용하여 개체 정리 실행 여부를 지정할 수 있습니다. 경우에 따라 복제 작업의 우선 순위가 높으면 개체 정리에 관여하지 않도록 하여 작업을 최대한 빠르게 실행할 수도 있습니다. 개체 정리를 비활성화하면 됩니다.

관련 항목

- 648 페이지에서 [개체 정리 제한](#)"

18.11 충돌 감지 및 해결 관리

연합을 사용할 때 원본 사이트와 대상 사이트 모두에서 개체의 속성이 변경되면 충돌이 발생할 수 있습니다. 충돌 여부를 검사할 때는 개체의 최상위 속성과 중첩된 속성을 모두 확인합니다. 예를 들어,

보고서 또는 보고서 이름이 원본 사이트와 대상 사이트에서 모두 수정되는 경우 충돌이 발생할 수 있습니다.

경우에 따라서는 충돌이 발생하지 않을 수 있습니다. 예를 들어, 원본 사이트에서 보고서 이름을 수정하고 대상 사이트에서 복제된 버전의 설명을 수정하는 경우 변경 내용이 함께 병합되고 충돌이 발생하지 않습니다.

18.11.1 단방향 복제 충돌 해결

단방향 복제에서는 다음과 같은 두 가지 방법 중 하나로 충돌을 해결할 수 있습니다.

원본 사이트 먼저 적용

단방향 복제 과정에서 충돌이 발생하면 원본 사이트의 개체가 우선권을 갖습니다. 대상 사이트의 개체에 대한 모든 변경 내용을 무시하고 원본 사이트의 정보로 이를 덮어씁니다. 예를 들어 보고서가 원본 사이트와 대상 사이트에서 모두 수정되는 경우 다음 복제 작업을 수행하면 원본 사이트가 대상 사이트 수정 내용을 덮어쓰게 됩니다.

참고:

이 경우 충돌이 자동으로 해결되므로 충돌이 로그 파일에 기록되지 않고 충돌 개체 목록에도 표시되지 않습니다.

자동 충돌 해결 사용 안 함

자동 충돌 해결 사용 안 함을 선택한 경우 충돌이 발생하면 충돌이 해결되지 않습니다. 이 경우 로그 파일이 생성되지도 않고 충돌 개체 목록에 표시되지도 않습니다.

관리자는 충돌을 일으킨 모든 복제된 개체의 목록을 CMC의 연합 영역에서 확인할 수 있습니다. 충돌을 일으킨 개체는 원본 사이트에 연결하는 데 사용한 원격 연결별로 나누어 그룹화됩니다. 이 목록에 액세스하려면 CMC의 연합 영역에 있는 복제 오류 폴더로 이동하여 원하는 원격 연결을 선택합니다. 대상 사이트의 모든 복제된 개체에는 복제 아이콘이 표시됩니다. 충돌이 발생한 개체에는 충돌 아이콘이 표시됩니다. 속성 페이지에는 경고 메시지도 나타납니다.

참고:

- 원격 연결을 사용하는 복제 작업이 완료되면 이 목록이 업데이트됩니다. 이 목록에는 특정 원격 연결을 사용하는 모든 복제 작업에 대해 충돌을 일으킨 모든 개체가 포함됩니다.
- CMC와 복제 작업 인스턴스에 액세스할 수 있는 사용자는 누구든지 로그 파일 디렉터리에 저장된 XML 로그를 볼 수 있습니다. 대상 사이트 개체의 아이콘에 충돌을 나타내는 플래그가 설정됩니다. 처리 과정에서 충돌 로그가 생성됩니다.

압둘이 원본 사이트에서 보고서 A를 수정합니다. 마리아가 대상 사이트에서 복제된 버전을 수정합니다. 보고서가 양쪽 사이트 모두에서 변경되었으므로 다음 번에 복제 작업을 실행하면 해당 보고서와 관련하여 충돌이 발생하고 충돌이 해결되지는 않습니다.

대상 사이트의 보고서가 그대로 유지되고 원본 사이트의 보고서에 대한 변경 내용이 대상 사이트로 복제되지 않습니다. 충돌을 해결하기 전까지는 후속 복제 작업이 같은 방식으로 진행됩니다. 충돌을 직접 해결하기 전까지는 원본 사이트의 어떠한 변경 내용도 복제되지 않습니다.

참고:

이 경우 전체 개체가 복제되지 않습니다. 충돌하지 않았을 수 있는 다른 변경 내용도 가져오지 않습니다.

충돌을 직접 해결하는 데는 세 가지 방법이 있습니다.

1. 충돌을 일으킨 개체만 복제하는 복제 작업을 만듭니다. 여기에는 동일한 원격 연결 개체와 복제 목록을 사용해야 합니다.

원본 사이트의 변경 내용을 유지하려면 복제 작업을 만듭니다. 그런 다음 복제 모드를 원본에서 새로 고침으로 설정하고 자동 충돌 해결을 원본 사이트 먼저 적용으로 설정합니다.

대상 사이트의 변경 내용을 유지하려면 복제 유형을 양방향 복제로, 복제 모드를 대상에서 새로 고침으로, 자동 충돌 해결을 대상 사이트 먼저 적용으로 설정하여 복제 작업을 만듭니다.

참고:

복제 목록 중 충돌을 일으킨 개체만 선택하려면 복제 모드를 원본에서 새로 고침이나 대상에서 새로 고침으로 설정합니다. 이렇게 하면 다른 개체는 복제되지 않습니다. 그런 다음 복제 작업을 실행할 일정을 설정하면 지정된 내용에 따라 선택한 개체가 복제되고 충돌이 해결됩니다.

2. 충돌을 일으킨 개체만 복제하는 복제 작업을 만듭니다. 여기에는 동일한 원격 연결 개체를 사용해야 합니다. 그러나 첫 번째 방법과 달리 이번에는 원본 사이트에 새 복제 목록을 만들 수 있습니다. 충돌을 일으킨 개체만 사용하여 새 복제 목록을 만들고 이 복제 목록을 사용할 새 복제 작업을 만듭니다.

원본 사이트의 변경 내용을 유지하려면 자동 충돌 해결을 원본 사이트 먼저 적용으로 설정합니다.

대상 사이트의 변경 내용을 유지하려면 자동 충돌 해결을 대상 사이트 먼저 적용으로 설정하고 복제 유형을 양방향 복제로 설정합니다.

3. 단방향 복제 작업의 경우 대상 사이트의 개체만 삭제할 수도 있습니다. 다음 번에 복제 작업을 실행하면 원본 사이트에서 대상 사이트로 개체가 복제됩니다.

참고:

개체를 삭제할 때는 종속된 다른 개체가 함께 제거되거나 작동을 멈추거나 보안이 약화될 수 있으므로 주의해야 합니다. 가능하면 첫째 방법이나 둘째 방법을 사용하는 것이 좋습니다.

18.11.2 양방향 복제 충돌 해결

양방향 복제 충돌이 발생한 경우에는 다음과 같은 세 가지 방법 중 하나로 충돌을 감지할 수 있습니다.

- 원본 사이트 먼저 적용
- 대상 사이트 먼저 적용
- 자동 충돌 해결 사용 안 함

원본 사이트 먼저 적용

충돌이 발생하면 원본 사이트가 우선권을 갖고 대상 사이트의 모든 변경 내용을 덮어씁니다.

예제

릴리가 보고서의 이름을 보고서 A로 수정하고 말릭이 대상 사이트에서 복제된 버전의 이름을 보고서 B로 수정한 경우 다음 번 복제 작업을 실행하면 대상 사이트의 복제된 버전 이름이 보고서 A로 바뀝니다.

이 경우 충돌이 로그 파일에 기록되지 않고 충돌 개체 목록에도 표시되지 않습니다. 원본 사이트에서 사용자가 지정한 대로 충돌이 해결되었기 때문입니다.

대상 사이트 먼저 적용

충돌이 발생하면 대상 사이트의 변경 내용을 유지하고 원본 사이트에 변경 내용을 덮어씁니다.

예제

카말이 보고서의 이름을 보고서 A로 수정하고 피터가 대상 사이트에서 복제된 버전의 이름을 보고서 B로 수정한 경우 복제 작업을 실행하면 충돌이 감지됩니다. 이 상황에서 대상 사이트의 보고서 이름이 보고서 B로 계속 유지됩니다.

양방향 복제에서는 변경 내용이 원본 사이트로도 다시 전달됩니다. 이 예제에서는 원본 사이트가 업데이트되고 보고서 이름이 보고서 B로 변경됩니다. 이 경우 충돌이 로그 파일에 기록되지 않고 충돌 개체 목록에 표시되지도 않습니다. 이는 사용자가 지정한 대로 충돌이 해결되었기 때문입니다.

자동 충돌 해결 사용 안 함

자동 충돌 해결 사용 안 함을 선택한 경우에는 충돌이 해결되지 않습니다. 이 충돌은 관리자가 볼 수 있도록 로그 파일에 기록되고, 관리자는 충돌을 직접 해결해야 합니다.

참고:

- 충돌이 발생했음을 나타내는 플래그가 개체의 아이콘에 설정됩니다.
- 양방향 복제에서는 변경 내용이 원본 및 대상 사이트 모두에 복제되지만 대상 사이트의 버전에만 충돌 아이콘이 표시됩니다.

참고:

CMC와 복제 작업 인스턴스에 액세스할 수 있는 사용자는 누구든지 로그 파일 디렉터리에 출력된 XML 로그를 볼 수 있습니다. 대상 사이트 개체의 아이콘에 충돌을 나타내는 플래그가 설정됩니다. 처리 과정에서 충돌 로그가 생성됩니다.

관리자는 충돌을 일으킨 모든 복제된 개체의 목록을 CMC의 연합 영역에서 확인할 수 있습니다. 충돌을 일으킨 개체는 원본 사이트에 연결하는 데 사용한 원격 연결별로 나누어 그룹화됩니다. 이러한 목록에 액세스하려면 CMC > 연합 > 복제 오류 > 원격 연결로 이동합니다.

참고:

원격 연결을 사용하는 복제 작업이 완료되면 이 목록이 업데이트됩니다. 이 목록에는 특정 원격 연결을 사용하는 모든 복제 작업에 대해 충돌을 일으킨 모든 개체가 포함됩니다. 대상 사이트의 모든 복제된 개체에는 복제 아이콘이 표시됩니다. 충돌이 발생한 개체에는 충돌 아이콘이 표시됩니다.

예제

미가엘이 원본 사이트에서 보고서 A를 수정합니다. 다민이 대상 사이트에서 복제된 버전을 수정합니다. 보고서가 양쪽 사이트 모두에서 변경되었으므로 다음 번에 복제 작업을 실행하면 해당 보고서와 관련하여 충돌이 발생하고 충돌이 해결되지 않습니다.

대상 사이트의 보고서가 그대로 유지되고 원본 사이트의 보고서에 대한 변경 내용이 대상 사이트로 복제되지 않습니다. 충돌을 해결하기 전까지는 이후의 복제 작업이 같은 방식으로 진행됩니다. 관리자나 위임된 관리자가 충돌을 직접 해결하지 않는 한 원본 사이트의 어떠한 변경 내용도 복제되지 않습니다.

참고:

- 이 경우 전체 개체가 복제되지 않습니다. 충돌하지 않은 다른 변경 내용은 복제되지 않습니다.
- CMC와 복제 작업 인스턴스에 액세스할 수 있는 사용자는 누구든지 로그 파일 디렉터리에 출력된 XML 로그를 볼 수 있습니다. 대상 사이트 개체의 아이콘에 충돌을 나타내는 플래그가 설정됩니다. 처리 과정에서 충돌 로그가 생성됩니다.

관리자는 충돌을 일으킨 모든 복제된 개체의 목록을 CMC의 연합 영역에서 확인할 수 있습니다. 충돌을 일으킨 개체는 원본 사이트에 연결하는 데 사용한 원격 연결별로 나누어 그룹화됩니다. 이러한 목록에 액세스하려면 CMC > 연합 > 복제 오류 > 원격 연결로 이동합니다.

참고:

원격 연결을 사용하는 복제 작업이 완료되면 이 목록이 업데이트됩니다. 이 목록에는 특정 원격 연결을 사용하는 모든 복제 작업에 대해 충돌을 일으킨 모든 개체가 포함됩니다. 대상 사이트의 모든 복제된 개체에는 복제 아이콘이 표시됩니다. 충돌이 발생한 개체에는 충돌 아이콘이 표시됩니다.

충돌을 직접 해결하는 데는 세 가지 방법이 있습니다.

1. 충돌을 일으킨 개체만 복제하는 복제 작업을 만듭니다. 여기에는 동일한 원격 연결 개체와 복제 목록을 사용해야 합니다.

원본 사이트의 변경 내용을 유지하려면 복제 작업을 만듭니다. 그런 다음 복제 모드를 원본에서 새로 고침으로 설정하고 자동 충돌 해결을 원본 사이트 먼저 적용으로 설정합니다.

대상 사이트의 변경 내용을 유지하려면 복제 유형을 양방향 복제로, 복제 모드를 대상에서 새로 고침으로, 자동 충돌 해결을 대상 사이트 먼저 적용으로 설정하여 복제 작업을 만듭니다.

참고:

복제 목록 중 충돌을 일으킨 개체만 선택하려면 복제 모드를 원본에서 새로 고침이나 대상에서 새로 고침으로 설정합니다. 이렇게 하면 다른 개체는 복제되지 않습니다. 그런 다음 복제 작업을 실행할 일정을 설정하면 지정된 내용에 따라 선택한 개체가 복제되고 충돌이 해결됩니다.

2. 충돌을 일으킨 개체만 복제하는 복제 작업을 만듭니다. 여기에는 동일한 원격 연결 개체를 사용해야 합니다. 그러나 첫 번째 방법과 달리 이번에는 원본 사이트에 새 복제 목록을 만들 수 있습니다. 충돌을 일으킨 개체만 사용하여 새 복제 목록을 만들고 이 복제 목록을 사용할 새 복제 작업을 만듭니다.

원본 사이트의 변경 내용을 유지하려면 자동 충돌 해결을 원본 사이트 먼저 적용으로 설정합니다.

대상 사이트의 변경 내용을 유지하려면 자동 충돌 해결을 대상 사이트 먼저 적용으로 설정하고 복제 유형을 양방향 복제로 설정합니다.

3. 사이트에서 검색하지 않을 개체를 삭제합니다.

참고:

개체를 삭제할 때는 종속된 다른 개체가 함께 제거되거나 작동을 멈추거나 보안이 약화될 수 있으므로 주의해야 합니다. 가능하면 첫째 방법이나 둘째 방법을 사용하는 것이 좋습니다.

대상 사이트의 변경 내용을 유지하려면 원본 사이트의 개체를 삭제합니다. 다음 번에 복제 작업을 실행하면 대상 사이트에서 원본 사이트로 개체가 복제됩니다.

참고:

원본 사이트의 복사본을 삭제할 때는 주의해야 합니다. 복사본이 다시 복제되기 전에 해당 개체를 복제하는 다른 대상 사이트에서 자체적으로 복제 작업을 실행할 수 있기 때문입니다. 이 경우 다른 대상 사이트에서 해당 복사본이 삭제되므로 복사본을 반환하여 복원하기 전까지는 그 복사본을 사용할 수 없게 됩니다.

원본 사이트의 변경 내용을 유지하려면 대상 사이트에서 개체를 삭제하면 됩니다.

18.12 연합에 웹 서비스 사용

연합에서 원본 및 대상 사이트 사이에 개체와 그 변경 내용을 보내는 데는 웹 서비스가 사용됩니다. 연합과 관련된 웹 서비스는 BI 플랫폼 설치 환경에 자동으로 설치 및 배포됩니다. 그러나 기능을 향상시키기 위해 웹 서비스의 속성을 수정하거나 배포를 사용자 지정할 수도 있습니다. 이번 단원에서는 그 방법을 설명합니다.

팁:

파일 관리 및 기능을 향상시키려면 연합에 파일 캐싱을 사용할 수 있도록 설정합니다.

18.12.1 세션 변수

한 번의 복제 작업으로 많은 콘텐츠 파일을 전송하려는 경우에는 연합 웹 서비스의 세션 제한 시간을 늘리면 됩니다.

이 속성은 dsws.properties 파일에서 지정할 수 있습니다.

<응용 프로그램 서버 설치 디렉터리>WdswsbobjeWWeb-INFWebclasses

예를 들면 다음과 같습니다.

C:\WProgram Files\WSAP BusinessObjects\WTomcat6\Wwebapps\Wdswsbobje\WEB-INF\Webclasses

세션 변수를 활성화하려면 다음과 같이 입력합니다.

```
session.timeout = x
```

여기서 x는 원하는 시간입니다. 이 x는 초 단위 값입니다. 지정되지 않은 경우 기본값은 1200초(20분)입니다.

18.12.2 파일 캐싱

파일 캐싱을 사용하면 웹 서비스에서 파일을 메모리에 버퍼링하지 않고도 매우 큰 첨부 파일을 처리할 수 있습니다. 이를 활성화하지 않은 상태에서 매우 큰 파일을 전송하면 Java Virtual Machine의 메모리가 모두 소모되어 복제가 실패할 수 있습니다.

참고:

반면에 파일 캐싱을 사용하면 웹 서비스에서 작업을 처리하는 데 메모리 대신 파일을 사용하게 되므로 성능이 저하될 수 있습니다. 큰 규모의 전송은 파일로 처리하고 작은 크기의 전송은 메모리에서 처리하도록 두 옵션을 조합하여 사용할 수 있습니다.

파일 캐싱을 활성화하려면 다음 위치에 있는 Axis2.xml 파일을 수정하십시오.

<응용 프로그램 서버 설치 디렉터리>WdswsbobjeWWeb-InfWconf

예:

C:\Program Files\SAP BusinessObjects\Tomcat6\Webapps\Wdswsbobje\WEB-INF\conf

다음과 같이 입력합니다.

```
<parameter name="cacheAttachments" locked="false">true</parameter>
```

```
<parameter name="attachmentDIR" locked="false">temp directory</parameter>
```

```
<parameter name="sizeThreshold" locked="false">4000</parameter>
```

참고:

임계값 크기는 바이트 단위입니다.

18.12.3 사용자 지정 배포

연합 웹 서비스가 자동으로 배포되어 federator, biplatform 및 session 서비스를 활성화해야 할 수도 있습니다. 연합이나 기타 웹 서비스를 비활성화하려면 해당 웹 서비스의 service.xml 파일을 수정합니다.

BI 플랫폼 웹 서비스 위치:

<응용 프로그램 서버 설치 디렉터리>WdswsbobjeWWEB-INFWservices

예:

C:\WProgram Files\WSAP BusinessObjects\WTomcat6\Wwebapps\WdswsbobjeWWEB-INFWservices

웹 서비스를 비활성화하려면

- service.xml 파일의 서비스 이름 태그에 activate 속성을 추가하고 false로 설정합니다.
- Java 응용 프로그램 서버를 다시 시작합니다.

예를 들어, 연합을 비활성화하려면 다음과 같이 하십시오.

services.xml 파일이 다음 위치에 있습니다.

C:\WProgram Files\WBusiness Objects\WTomcat55\Wwebapps\WdswsbobjeWWEB-INFWservices\Wfederator\WMETA-INF

다음과 같은 서비스 이름을

<service name="Federator">

다음과 같이 변경합니다.

<service name="Federator" activate="false">

18.13 원격 일정 설정 및 로컬에서 실행되는 인스턴스

이 단원에서는 원격 일정 설정, 로컬에서 실행되는 인스턴스 및 인스턴스 공유에 대해 자세히 설명합니다. 이러한 기능을 사용하면 데이터가 있는 위치에서 보고서를 실행할 수 있고 완료된 인스턴스를 적절한 위치로 보낼 수 있습니다.

18.13.1 원격 일정 설정

연합을 사용하면 대상 사이트에 보고서 일정을 설정하고 이를 원본 사이트에서 처리할 수 있습니다. 완료된 인스턴스는 대상 사이트로 반환됩니다.

원격 예약 기능을 사용하려면 일반적인 방법으로 보고서를 예약하고 원본 사이트에서 실행 옵션을 설정합니다. 이 옵션을 설정하려면 예약 > 예약 서버 그룹 > 원본 사이트에서 실행을 클릭합니다. 예약된 인스턴스는 생성된 후 보류 중 단계에 배치됩니다.

원격 일정 설정 과정에서 대상 사이트에 제출한 정보는 무시되고 보고서 인스턴스가 보류 중 상태로 남습니다.

보고서를 관리하는 다음 번 복제 작업에서 원격 일정 설정이 가능하도록 지정하면 이 복제 작업에서는 인스턴스를 처리할 수 있도록 원본 사이트로 복사합니다. 인스턴스는 스케줄러에서 처리하기 전까지 보류 중 상태로 남습니다. 이때 인스턴스를 보냈던 복제 작업에서는 이전에 완료된 모든 인스턴스 및 개체 변경 내용을 모두 반환합니다.

원본 사이트에서 처리를 마친 인스턴스는 완료 상태로 이전됩니다. 보고서를 관리하는 다음 번 복제 작업에서 원격 일정 설정이 사용 가능할 경우 이 복제 작업에서는 완료된 인스턴스를 사용하여 대상 사이트의 복사본을 업데이트합니다. 업데이트를 마치면 대상 사이트에서 인스턴스가 완료됩니다.

참고:

완료된 인스턴스 하나를 반환하려면 복제 작업을 두 번 실행해야 합니다.

예제

1. 톰이 원격 일정 설정과 관련하여 보고서 A를 예약합니다.
2. 보고서 A가 대상 사이트에 만들어지고 보류 중 상태가 됩니다.
3. 복제 작업 A가 실행됩니다. 우선 이전에 완료된 인스턴스를 포함한 원본 사이트의 변경 내용이 대상 사이트에 복제됩니다. 그런 다음 대상 사이트에서 원본 사이트로 복제해야 할 변경 내용을 비롯하여 보류 중 상태인 인스턴스를 원본 사이트로 복사합니다.
4. 원본 사이트의 스케줄러가 보류 중 상태인 인스턴스를 선택한 다음 이를 처리할 수 있도록 적절한 작업 서버로 보냅니다. 원본 사이트에서 인스턴스가 처리되고 완료 상태로 배치됩니다.
5. 복제 작업 A가 다시 실행됩니다. 이 복제 작업을 통해 원본 사이트에서 대상 사이트로 콘텐츠를 복제할 때 완료된 인스턴스 보고서 A가 선택되고 변경 내용이 대상 사이트의 버전에 적용됩니다.
6. 이 작업이 끝나면 대상의 버전이 완성됩니다.

원격 일정 설정은 양방향 복제 작업에서 원격 일정 복제를 활성화한 경우에만 가능합니다. 이 옵션은 복제 작업 속성 페이지의 복제 필터 영역에 있습니다. 예약된 작업을 복제 목록의 다른 개체보다 자주 원격으로 복제해야 하는 경우도 있습니다. 이렇게 하려면 복제 작업 두 개를 만듭니다. 그 중 한 작업은 원격 일정 설정을 전달하도록 복제 작업에 대해 원격 일정 복제를 활성화합니다. 다른 한 작업은 문서 템플릿 복제 또는 모든 개체 복제(필터 없음)을 활성화합니다.

참고:

원격 예약을 사용하면 완료된 인스턴스와 실패한 인스턴스가 원본 및 대상 사이트에 모두 표시됩니다.

대상 사이트의 사용자가 원격 일정 설정이 가능하도록 보고서의 일정을 설정한 경우, 원본 사이트에 사용자가 없으면 원본 사이트에서 인스턴스가 실패합니다. 실패한 인스턴스의 소유자는 원본 사이트에 연결하는 데 사용한 원격 연결 개체의 사용자 계정이 됩니다.

복제 작업을 원격 예약 전용으로 구성할 수도 있지만 항상 보고서 인스턴스의 상위 개체가 복제됩니다. 즉, 복제 사이에 변경된 내용이 있으면 실제 보고서, 보고서 폴더 순으로 복제됩니다. 대상 사이트의 이러한 변경 내용이 원본 사이트로 복제되지 않도록 하려면 보안 권한을 사용하여 복제할 변경 내용을 제어할 수 있습니다.

관련 항목

- 626 페이지에서 [보안 권한 관리](#)"

18.13.2 로컬에서 실행되는 인스턴스

로컬에서 실행되는 인스턴스는 대상 사이트의 보고서에서 처리된 보고서의 인스턴스입니다. 연합을 사용하면 대상 사이트의 완료된 인스턴스를 원본 사이트로 복제할 수 있습니다.

복제 작업을 통해 완료된 인스턴스와 실패한 인스턴스를 대상 사이트에서 원본 사이트로 복제하려면 복제 작업 속성 > 복제 필터 > 로컬에서 실행되는 완료된 인스턴스 복제를 클릭합니다.

복제 작업을 통해 로컬에서 실행되는 인스턴스만 복제해야 하는 경우도 있습니다. 이렇게 하려면 로컬에서 실행되는 완료된 인스턴스 복제를 활성화합니다.

참고:

복제 작업에 대해 로컬에서 실행되는 인스턴스를 활성화하면 완료된 인스턴스와 실패한 인스턴스가 모두 원본 사이트로 복제됩니다. 즉, 원본 사이트와 대상 사이트에 모두 복사본이 저장됩니다.

보류 중인 인스턴스는 복제되지 않습니다.

로컬에서 실행되는 인스턴스의 소유자가 원본 사이트에 없으면 원격 연결 개체의 연결에 사용되는 사용자 계정이 소유자가 됩니다.

18.13.3 인스턴스 공유

원격 일정 설정과 로컬에서 실행되는 인스턴스를 복제 작업에 사용하는 경우 동일한 보고서를 복제하는 여러 대상 사이트가 원본 사이트 하나에 연결되어 있으면 인스턴스 공유가 발생할 수 있습니다.

예제

원본 사이트에 보고서 A가 있고 대상 사이트 A와 B에서 이 보고서를 복제하는 경우를 가정합니다. 두 대상 사이트에서 모두 인스턴스가 공유됩니다.

- 복제 작업에서 원격 일정 복제 및/또는 로컬에서 실행되는 완료된 인스턴스 복제를 사용합니다. 위와 동일한 복제 작업을 사용하여 보고서 A를 복제합니다.
- 대상 사이트에서 보고서 A가 원본 사이트에서 실행 및/또는 로컬에서 실행되도록 예약합니다.

대상 사이트 A와 B에서 모두 보고서 A를 복제하는 경우 각 복제 작업에서 원격 일정을 복제하거나 로컬에서 실행되는 인스턴스를 복제하면 대상 사이트 A에서 처리한 모든 인스턴스 및/또는 대상 사이트 A 대신 원본 사이트에서 처리한 모든 인스턴스가 대상 사이트 B와 공유됩니다.

마찬가지로, 대상 사이트 B에서 처리한 모든 인스턴스 및/또는 원본 사이트에서 처리한 모든 인스턴스도 대상 사이트 A와 공유됩니다. 최종적으로 원본 사이트와 대상 사이트 A 및 B가 모두 동일한 인스턴스 집합을 갖게 됩니다.

인스턴스 공유는 많은 점에서 바람직한 상태입니다. 예를 들어, 다른 사이트의 사용자가 이웃 배포의 정보에 액세스해야 할 수도 있습니다. 이 경우 로컬 사이트의 사용자가 인스턴스를 볼 수 없도록 하기 위해 적절한 보안 권한을 설정해야 합니다. 예를 들어, 사용자 자신이 소유한 인스턴스만 볼 수 있도록 보고서 개체에 권한을 적용할 수 있습니다.

참고:

모든 개체는 BI 플랫폼 보안 규칙을 따릅니다. 사용자와 그룹이 자신이 소유한 인스턴스만 볼 수 있도록 권한을 설정하여 각자에게 허용되는 인스턴스만 볼 수 있게 하는 것이 좋습니다. 예를 들어, 사용자 자신이 소유한 인스턴스만 볼 수 있도록 보고서 개체에 권한을 적용할 수 있습니다.

관련 항목

- 626 페이지에서 [보안 권한 관리](#)"

18.14 복제된 콘텐츠 가져오기 및 승격

경우에 따라 BI 플랫폼 시스템 간에 복제된 콘텐츠를 가져오거나 수준을 올릴 수 있습니다. 이 단원에서는 연합의 이와 같은 기능을 설명합니다.

18.14.1 복제된 콘텐츠 가져오기

LifeCycle Manager를 사용하여 BI 플랫폼 배포 환경 간에 콘텐츠를 가져오는 경우, 가져오는 복제된 개체에 연결된 정보 중 복제에 해당되는 정보는 가져오지 않습니다. 따라서 가져온 개체는 복제된 적이 없는 것처럼 작동합니다. 이는 대상 사이트의 복제된 개체에 해당하는 내용입니다. 구체적인 예는 다음 시나리오에서 설명합니다.

예제

BI 플랫폼 A가 연합 프로세스의 대상 사이트라고 가정합니다. LifeCycle Manager를 사용하여 시스템 A에 있는 복제된 보고서인 보고서 A를 시스템 A에서 BI 플랫폼 B로 가져옵니다.

결과: 보고서 A가 BI 플랫폼 B에 복사되지만 복제된 정보가 전혀 포함되지 않습니다. 따라서 보고서 A에 더 이상 복제 아이콘이 표시되지 않습니다. 개체가 BI 플랫폼 A에서 충돌했다라도 시스템 B에서는 충돌을 일으키지 않습니다. 본질적으로 이 개체는 시스템 B에서 처음 만든 개체처럼 취급됩니다.

참고:

CUID는 주기 관리자에서 선택한 가져오기 옵션에 따라 동일할 수도 동일하지 않을 수도 있습니다.

18.14.2 복제된 콘텐츠를 가져온 후 복제 진행

복제된 콘텐츠를 가져온 후 가져온 개체를 연합 프로세스에 포함할 수 있습니다. 이때 가져온 개체가 있는 시스템을 원본 사이트로 취급할 수도 있고 대상 사이트로 취급할 수도 있습니다. 이 시스템을 원본 사이트로 취급하려면 일반적인 방법으로 연합을 계속 진행합니다.

이 시스템을 대상 사이트로 취급하고 원본 사이트에서 가져온 개체를 복제하려면 다음 지침에 따라야 합니다.

- 주기 관리자를 사용할 때 개체의 CUID를 그대로 유지해야 합니다.
- 첫 복제 작업의 충돌 해결 방법을 원본 사이트에서 실행이나 대상 사이트에서 실행으로 설정해야 합니다.

팁:

주기 관리자를 사용하여 대상 사이트 간에 개체를 가져오는 대신 연합만 사용하여 개체를 복제하는 것이 더 효율적이며 권장되는 방법입니다.

예제

BI 플랫폼 시스템 A에서 보고서 A를 만들었고, 시스템 X에서 연합을 사용하여 시스템 A의 보고서 A를 시스템 X로 복제했습니다. 그런 다음 LifeCycle Manager에서 시스템 X의 보고서 A를 시스템 Y로 가져왔습니다.

계획: 시스템 Y에서 시스템 A에 대한 연합을 설정하고 보고서 A를 복제의 일부로 유지하려고 합니다. 시스템 Y는 대상이고 시스템 A는 원본입니다.

작업: 시스템 X에서 시스템 Y로 보고서 A를 가져올 때 보고서 A의 CUID를 그대로 유지해야 합니다. 복제 작업을 처음 실행하면 보고서 A를 복제하려 시도하지만 개체가 이미 시스템 Y에 있으므로 복제 시 충돌이 발생합니다. 사용할 버전을 지정하려면 충돌 해결 모드를 원본 사이트에서 실행이나 대상 사이트에서 실행으로 설정해야 합니다.

참고:

이 예제의 경우 주기 관리자를 사용하여 대상 사이트 간에 개체를 가져오는 대신 연합만 사용하여 개체를 복제하는 것이 좋습니다. 보고서 A가 시스템 A에서 시스템 Y로 복제됩니다. 주기 관리자를 사용하여 시스템 X에서 시스템 Y로 가져올 필요는 없습니다.

18.14.3 테스트 환경의 콘텐츠 수준 올리기

어떤 조직에서든 테스트는 작업물을 프로덕션 환경에 배치하기 전에 수행하는 것이 일반적입니다. 프로덕션 컴퓨터에 연합을 설정하기 전에 개발 또는 테스트 환경의 BI 플랫폼 시스템 사이에서 연합을 테스트하는 것이 일반적입니다. 테스트 환경에서 원본 사이트, 대상 사이트 및 콘텐츠를 만든 후 다음과 같은 단계에 따라 이 설정을 프로덕션 컴퓨터로 승격할 수 있습니다.

1. 주기 관리자를 사용하여 테스트 환경의 원본 사이트에서 원본 사이트로 사용할 프로덕션 컴퓨터로 콘텐츠를 승격합니다.

참고:

주기 관리자를 사용할 때는 복제 목록 개체를 선택할 수 없습니다.

2. 프로덕션 환경의 원본 사이트에서 복제 목록을 만들고 원하는 콘텐츠를 포함합니다.
3. 다음 두 옵션 중 하나를 선택합니다.
 - A) 대상 사이트로 사용할 프로덕션 환경의 프로덕션 시스템에서 원격 연결 개체와 적절한 복제 작업을 만듭니다.
 - B) 주기 관리자를 사용하여 개발/QA 환경의 대상 사이트에서 대상 사이트로 사용할 프로덕션 컴퓨터로 원격 연결 및 복제 작업을 가져옵니다. 그런 다음 원본 사이트로 사용할 프로덕션 환경의 시스템을 가리키도록 가져온 원격 연결을 편집합니다.

18.14.4 대상 사이트 다시 가리키기

현재, 개체가 원본 사이트에서 복제되어 새로운 시스템을 가리키도록 원격 연결 개체가 편집되면 다른 BI 플랫폼으로부터 복제할 수 없고 항상 원본 사이트로부터 복제해야 합니다. 원격 연결 개체가 아닌 다른 BI 플랫폼 시스템에서 복제된 적이 있는 개체를 다시 복제하려고 시도하면 복제에 실패합니다. 다른 원본 사이트에서 개체를 복제하려면 대상 사이트에서 해당 개체를 먼저 삭제해야 합니다.

참고:

복제된 개체를 복사하고 나면 복사본의 CUID가 변경되고 어떠한 복제 관련 정보도 복사본에 포함되지 않습니다.

18.15 모범 사례

연합을 사용하여 복제 작업 성능을 최적화할 수 있습니다.

단일 복제 작업에 개체 수가 아주 많은 경우, 몇 가지 추가 단계를 통해 작업을 성공적으로 실행할 수 있습니다. 일반적으로 각 복제 작업을 통해 복제할 수 있는 개체 수는 최대 32,000개까지입니다. 그러나 배포에 따라서는 복제 크기를 더 작거나 더 크게 구성해야 할 수도 있습니다.

1) 전용 웹 서비스 공급자 확보

연합에서 복제된 콘텐츠는 웹 서비스를 사용하여 전달됩니다. 기본 설정에 따라 BI 플랫폼을 설치한 경우 모든 웹 서비스에 동일한 웹 서비스 공급자가 사용됩니다. 규모가 큰 복제 작업의 경우 웹 서비스 공급자를 오랜 시간 점유하게 되므로 해당 공급자가 서비스하는 응용 프로그램 뿐만 아니라 다른 웹 서비스 요청에 대해서도 응답 속도가 느려질 수 있습니다.

많은 개체를 한꺼번에 복제하거나 여러 개의 복제 작업을 연속으로 실행하려는 경우에는 자체 웹 서비스 공급자를 사용하는 고유한 Java 응용 프로그램 서버에 연합 웹 서비스를 배포하는 방법도 고려해 볼 수 있습니다.

이 작업을 수행하려면 BI 플랫폼 설치 관리자를 사용하여 웹 서비스를 설치합니다. Java 응용 프로그램 서버는 이미 실행되고 있는 상태여야 합니다. 그렇지 않은 경우 전체 웹 계층 구성 요소 옵션을 설치하여 웹 서비스 및 Tomcat을 설치합니다.

참고:

- 기존 CMS의 정보를 입력해야 합니다(예: 호스트 이름, 포트, 관리자 암호).
- 원격 연결의 URI 필드에 이 새로운 웹 서비스 공급자의 URI를 사용해야 합니다.

2) Java 응용 프로그램 서버의 사용 가능한 메모리 늘리기

복제 작업 하나에서 여러 개의 개체를 복제하거나 응용 프로그램 서버를 다른 응용 프로그램과 공유하는 경우 Java 응용 프로그램 서버에서 사용 가능한 메모리의 양을 늘려야 합니다.

BI 플랫폼과 Tomcat을 배포한 경우 기본적으로 사용할 수 있는 메모리는 1GB입니다. Tomcat에 사용할 수 있는 메모리의 양을 늘리려면

Windows의 경우

1. 시작 > 프로그램 > Tomcat > Tomcat 구성을 클릭합니다.
2. Java를 선택합니다.
3. Java 옵션 상자에서 -Xmx1024M을 찾습니다.
4. -Xmx1024M을 원하는 크기로 늘립니다.

예제

메모리를 2GB로 늘리려면 -Xmx2048M을 입력합니다.

Unix의 경우

1. <BOE_Install_Dir>/setup/에서 텍스트 편집기를 사용하여 env.sh를 엽니다. -Xmx1024m 매개 변수를 원하는 크기로 늘립니다.
2. 다음 줄을 찾습니다.

```
# if [ -d "$BOBJEDIR"/tomcat ]; then
# set the JAVA_OPTS for Tomcat
JAVA_OPTS="-Dboj.enterprise.home=${BOBJEDIR}enterprise120
-Djava.awt.headless=true"

if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" =
"SunOS" -o "$SOFTWARE" = "Linux" -o "$SOFTWARE" = "HP-UX" ];
then
  JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m"
fi
export JAVA_OPTS
# fi
```

3. -Xmx1024m 매개 변수를 원하는 크기로 늘립니다.

예제

메모리를 2GB로 늘리려면 -Xmx2048m을 입력합니다.

팁:

다른 Java 응용 프로그램 서버에서 사용 가능한 메모리를 늘리는 방법은 해당 Java 응용 프로그램 서버의 설명서를 참조하십시오.

3) 작성되는 BIAR 파일의 크기 줄이기

연합에서는 웹 서비스를 사용하여 원본 사이트와 대상 사이트 사이에 콘텐츠를 복제합니다. 개체는 더 효율적인 전송을 위해 BIAR 파일로 함께 그룹화되고 압축됩니다.

복제할 개체 수가 많은 경우에는 생성되는 BIAR 파일의 크기를 줄이도록 Java 응용 프로그램 서버를 구성하는 것이 좋습니다. 연합에서는 개체를 여러 개의 작은 BIAR 파일에 걸쳐 패키지화하고 압축하므로 개체를 그 수에 상관없이 복제할 수 있습니다.

생성되는 BIAR 파일의 크기를 줄이려면 Java 응용 프로그램 서버에 다음과 같은 Java 매개 변수를 추가합니다.

```
Dbobj.biar.suggestSplit
and
Dbobj.biar.forceSplit
```

bobj.biar.suggestSplit을 사용하면 BIAR 파일의 적절한 크기가 제안되고 가능한 한 그 크기에 맞추려 시도합니다. 제안되는 새 값은 90MB입니다.

bobj.biar.forceSplit을 사용하면 지정된 크기로 BIAR 파일의 크기가 제한됩니다. 제안되는 새 값은 100MB입니다.

참고:

응용 프로그램 서버의 메모리가 부족하여 최대 힙 크기를 더 이상 늘릴 수 없는 경우가 아니라면 기본 BIAR 파일 크기를 변경할 필요가 없습니다.

Tomcat Windows의 경우

1. Tomcat 구성 도구를 열려면 시작 > 모든 프로그램 > Tomcat > Tomcat 구성을 클릭합니다.
2. Java를 선택합니다.

3. Java 옵션 상자의 끝부분에 다음 행을 추가합니다.

```
-Dbobj.biar.suggestSplit=90
-Dbobj.biar.forceSplit=100
```

Tomcat Unix/Linux의 경우

1. 텍스트 편집기로 env.sh를 엽니다. 이 파일은 <BOE 설치 디렉터리>/setup/에 있습니다.
2. 다음 행을 찾습니다.

```
# if [ -d "$BOBJEDIR"/tomcat ]; then
# set the JAVA_OPTS for tomcat
JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120 -Djava.awt.headless=true"

if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" = "SunOS" -o "$SOFTWARE" = "Linux" -o "$SOFTWARE" = "HP-UX" ]; then
  JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m"
fi
export JAVA_OPTS
# fi
```

원하는 BIAR 파일 크기 매개 변수를 추가합니다.

예: JAVA_OPTS="\$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m -Dbobj.biar.suggestSplit=90 -Dbobj.biar.forceSplit=100"

다른 Java 응용 프로그램 서버의 경우 Java 시스템 속성을 추가하는 방법은 해당 설명서를 참조하십시오.

4) 소켓 제한 시간 늘리기

복제 작업의 실행은 적응 작업 서버에서 담당합니다. 적응 작업 서버에서는 복제 작업을 실행하는 동안 원본 사이트에 대한 연결을 설정합니다. 원본 사이트에서 받을 정보의 양이 많은 경우 적응 작업 서버에서 정보를 받는 데 사용하는 소켓이 제한 시간을 초과하지 않도록 해야 합니다.

기본값은 90분입니다. 필요한 경우 소켓 제한 시간을 늘릴 수 있습니다.

적응 작업 서버의 소켓 제한 시간을 늘리려면

1. 중앙 관리 콘솔(CMC)을 엽니다.
2. 서버 섹션을 찾아 적응 작업 서버를 선택합니다.
3. 속성을 클릭합니다.
4. 다음 행 끝에 명령줄 매개 변수를 추가합니다.
 - Windows: -javaArgs Xmx1000m,Xincgc,server,Dbobj.federation.WSTimeout=<timeout in minutes>
 - Unix: -javaArgs Xmx512m,Dbobj.federation.WSTimeout=<timeout in minutes>

관련 항목

- 666 페이지에서 [오류 메시지 문제 해결](#)
- 654 페이지에서 [연함에 웹 서비스 사용](#)
- 664 페이지에서 [현재 릴리스 제한 사항](#)

18.15.1 현재 릴리스 제한 사항

연합은 유연한 도구이지만 프로덕션 상황에서는 몇 가지 제한 사항으로 인해 성능이 저하될 수 있습니다. 이 단원에서는 연합 작업을 최적화하기 위해 수정할 수 있는 항목을 중점적으로 설명합니다.

- 최대 개체 수

복제 작업을 수행할 때마다 BI 플랫폼 배포 환경 간에 개체가 복제됩니다. 복제 작업 한 번으로 복제할 개체의 수는 최대 100,000개를 넘지 않는 것이 좋습니다. 개체 수가 100,000개를 초과해도 복제 작업을 실행할 수는 있지만 연합 기능에서는 개체 복제를 최대 100,000개까지만 지원합니다.

- 권한

연합에서는 권한이 원본 사이트에서 대상 사이트로만 복제됩니다. 두 배포에 모두 공통으로 필요한 사용자 권한은 원본 사이트에 설정한 후 양방향 복제를 사용하여 대상 사이트로 복제하는 것이 좋습니다. 특정 사이트의 사용자 권한은 해당 사용자가 있는 사이트의 BI 플랫폼 배포 환경에서 일반적인 방법으로 관리됩니다.

- 비즈니스 뷰 및 관련 개체

BI 플랫폼에서는 비즈니스 뷰, 비즈니스 요소, 데이터 기반, 데이터 연결 및 값 목록(LOV)을 저장할 수 있습니다. 이러한 개체는 Crystal Reports의 기능을 강화하는 데 사용됩니다.

이러한 개체를 대상 사이트에서 처음 만든 다음 양방향 복제를 사용하여 원본 사이트로 복제하면 기능이 제대로 작동하지 않고 Crystal Reports에 해당 데이터가 표시되지 않을 수 있습니다.

비즈니스 뷰, 비즈니스 요소, 데이터 기반, 데이터 연결 및 LOV는 원본 사이트에 만든 다음 대상 사이트로 복제하는 것이 좋습니다. 대상 사이트나 원본 사이트(권한이 허용하는 경우)에서 개체를 업데이트하면 변경 내용이 다른 사이트로 적절하게 복제됩니다.

- 유니버스 오버로드

BI 플랫폼에서는 유니버스 오버로드를 저장할 수 있습니다. 대상 사이트에서 유니버스 오버로드를 만든 다음 양방향 복제를 사용하여 원본 사이트로 복제하면 기능이 제대로 작동하지 않을 수 있습니다.

이 문제를 해결하려면 유니버스 오버로드를 원본 사이트에서 먼저 만들어 대상 사이트로 복제해야 합니다. 그런 다음 원본 사이트에서 유니버스 오버로드에 대한 보안을 설정한 후 이를 대상 사이트로 복제합니다.

- 개체 정리

개체 정리를 수행하면 다른 사이트에서 삭제한 개체가 삭제됩니다. 현재 개체 정리는 원본 사이트에서 대상 사이트에 대해서만 수행할 수 있습니다.

- 연합 로그 파일

연합 로그 파일은 XML 1.1 표준을 사용하는 XML 파일에 기록됩니다. 브라우저를 사용하여 로그 파일을 보려면 브라우저에서 XML 1.1을 지원해야 합니다.

관련 항목

- 647 페이지에서 [개체 정리 관리](#)

18.15.2 오류 메시지 문제 해결

이 단원에서는 연합을 사용할 때 간혹 발생할 수 있는 오류 메시지를 설명합니다. 이러한 메시지는 복제 작업 로그에 기록되거나 보고서의 기능 영역에 표시됩니다.

1) 잘못된 GUID

오류 예제: ERROR 2008-01-10T00:31:08.234Z 개체 번호 1285의 속성 SI_PARENT_CUID에 있는 GUID ASXOOFyvy0FJnRcD0dZNTZg0I(가) 유효하지 않습니다.

이 오류는 부모를 복제 대상에 포함하지 않은 채 개체를 복제하려는 경우 그 부모가 대상 사이트에 없을 때 발생합니다. 예를 들어, 개체가 포함된 폴더는 제외한 채 개체만 복제하려는 경우가 여기에 해당합니다. 개체를 복제하려는 계정에 부모 개체에 대한 충분한 권한이 없어서 부모 개체가 복제되지 않을 수도 있습니다.

2) 원본 사이트에서 Crystal 보고서에 데이터가 표시되지 않음

이 오류는 대상 사이트에서 처음 만든 다음 원본 사이트로 복제한 비즈니스 뷰, 비즈니스 요소, 데이터 기반, 데이터 연결 또는 LOV(값 목록)를 Crystal 보고서에서 사용하는 경우에 발생합니다.

3) 유니버스 오버로드가 올바르게 적용되지 않음

이 오류는 대상 사이트에서 만들어 원본 사이트로 복제한 유니버스 오버로드가 포함된 유니버스를 보고서에 사용하는 경우에 발생합니다.

4) Java 메모리 부족

오류 예제: java.lang.OutOfMemoryError.

이 오류는 Java 응용 프로그램 서버에서 복제 작업을 처리하는 동안 메모리가 부족하게 되었을 때 발생할 수 있습니다. 복제 작업이 너무 크거나 Java 응용 프로그램 서버에 메모리가 충분하지 않기 때문일 수 있습니다.

연합 웹 서비스를 전용 컴퓨터로 옮겨 Java 응용 프로그램 서버의 사용 가능한 메모리를 늘리거나 한번의 복제 작업에서 복제되는 개체의 양을 줄여 보십시오.

5) 소켓 제한 시간

오류 예제: 원본 사이트와 통신하는 도중 오류가 발생했습니다. 읽기 시간이 초과되었습니다.

원본 사이트에서 대상 사이트의 적응 작업 서버로 정보를 보내는 데 할당된 제한 시간보다 더 오랜 시간이 걸립니다. 적응 작업 서버의 소켓 제한 시간을 늘리거나 복제 작업에서 복제되는 개체의 수를 줄여 보십시오.

6) 쿼리 제한

오류 예제: 대상 사이트에서 SDK 오류가 발생했습니다. 올바른 쿼리가 아닙니다. (FWB 00025) 쿼리 문자열이 쿼리 길이 제한보다 큼니다.

이 오류는 너무 많은 개체를 한꺼번에 복제하려고 하여 CMS에서 처리할 수 있는 크기에 비해 너무 큰 쿼리를 연합에서 제출하는 경우에 발생할 수 있습니다. 원본 사이트의 개체가 대상 사이트로 커밋됩니다. 그러나 원본 사이트로 커밋해야 할 변경 내용은 커밋되지 않습니다. 충돌은 지정한 대로 해결되지만 개체에 대한 수동 해결 충돌 플래그는 설정되지 않습니다. 대상 사이트로 커밋한 개체는 계속하여 올바르게 작동합니다.

이 문제를 해결하려면 한 번의 복제 작업에서 복제되는 개체의 수를 줄여야 합니다.

7) 복제 작업 시간 초과

오류 예제: 지정된 시간 간격 내에서 개체의 일정을 설정할 수 없습니다.

이 메시지는 다른 복제 작업이 완료되기를 기다리는 동안 복제 작업의 제한 시간이 경과한 경우에 나타날 수 있습니다. 이 오류는 여러 개의 복제 작업을 동일한 원본 사이트에 한꺼번에 연결해 둔 경우에 발생할 수 있습니다. 실패한 복제 작업은 다음 번 예약 시간에 다시 실행을 시도합니다.

이 문제를 해결하려면 실패한 복제 작업이 다른 시간에 실행되도록 예약하여 동일한 원본 사이트에 연결되는 다른 복제 작업과 충돌하지 않도록 합니다.

8) 복제 제한

오류 예제: 대상 사이트에서 SDK 오류가 발생했습니다. 데이터베이스 액세스 오류입니다. 내부 쿼리 프로세서 오류: 쿼리 최적화 과정에서 쿼리 프로세서의 스택 공간이 부족해졌습니다. ExecWithDeadlockHandling에서 쿼리를 실행하는 동안 오류가 발생했습니다.

이 메시지는 한 번에 복제할 수 있는 지원되는 개체 수를 초과한 경우에 나타날 수 있습니다. 이 문제를 해결하려면 복제 작업에서 복제할 개체 수를 줄인 다음 작업을 다시 실행해 봅니다.

9) 개체 삭제

오류 예제: 보안 권한을 확인하는 동안 오류가 발생했습니다. 또는 개체를 압축하는 동안 오류가 발생했습니다.

복제 패키지에서 개체가 삭제된 경우 이 메시지가 나타날 수 있습니다. 연합에서 권한을 확인하고 개체를 패키지하기 전에 복제가 필요한 개체를 쿼리하는 경우 이러한 문제가 발생할 수 있습니다.

10) 적응 처리 서버

오류 예제: 작업 처리 서버에서 오류가 발생했습니다.

연합에서 클래스를 너무 많이 로드하여 복제 작업을 처리할 메모리가 부족한 경우 이 오류가 발생할 수 있습니다.

이 문제를 해결하려면 다음 단계를 모두 수행해야 합니다.

1. 적응 처리 서버의 명령줄 인수에 `-javaArgs "XX:MaxPermSize=256m"` 줄을 추가합니다.
2. 연합을 위해 연결하는 Java 응용 프로그램 서버에 다음 매개 변수를 추가하여 사용하는 BIAR 파일의 크기를 줄입니다.
 - `-Dbobj.biar.suggestSplit=100m`
 - `-Dbobj.biar.forceSplit=100m`

11) 개체 관리자 공간

오류 예제: 밀어넣기 패키지를 빌드할 수 없습니다. 입력/출력 예외가 발생했습니다: "장치에 남아 있는 공간이 없습니다."

연합에서 사용하는 임시 디렉터리에 디스크 공간이 부족한 경우 이 오류가 발생합니다. 이 문제를 해결하려면 임시 디렉터리에 추가 공간을 확보하거나 다른 위치를 임시 디렉터리로 사용합니다.

원본 사이트의 임시 디렉터리를 다른 위치로 지정하려면 Java 응용 프로그램 서버의 구성 파일에 -Dbobj.tmp.dir=<TempDir> 줄을 추가합니다.

대상 사이트의 임시 디렉터리를 다른 위치로 지정하려면 적응 처리 서버의 명령줄 인수에 -javaArgs -Dbobj.tmp.dir=<TempDir> 줄을 추가합니다.

위 예제에서 <TempDir>은 사용할 임시 디렉터리의 위치입니다.

12) 유니버스 오류

오류 예제: processDPCommands API를 호출하는 동안 내부 오류가 발생했습니다.

복제된 유니버스에서 유니버스 간 연결 관계가 잘못되거나 누락된 경우 이 오류가 발생합니다. 이 문제를 해결하려면 원본에서 새로 고침 옵션을 선택하고 복제 작업을 시작한 다음 유니버스 연결이 복제되는지 확인합니다.

또는 Universe Designer에서 유니버스를 열고 유니버스의 연결을 편집한 다음 유니버스를 다시 커밋합니다.

관련 항목

- 662 페이지에서 [모범 사례](#)"
- 664 페이지에서 [현재 릴리스 제한 사항](#)"

장19 ERP 환경에 대한 보완 구성

19.1 SAP NetWeaver 통합 구성

19.1.1 SAP NetWeaver Business Warehouse(BW)와 통합

19.1.1.1 개요

이 단원에서는 SAP NetWeaver Business Warehouse에서 BI 플랫폼으로의 보고서 게시를 설정 및 관리하도록 BW를 구성하는 방법을 설명합니다.

이 단원을 시작하기 전에 CMC에서 SAP 인증 플러그 인 구성을 완료했는지 확인하십시오.

관련 항목

- 285 페이지에서 [SAP 인증 구성](#) "

19.1.1.1.1 BI 플랫폼의 폴더 및 보안 설정

BI 플랫폼에서 권한 부여 시스템을 정의하면 시스템에서 SAP 시스템에 맞는 논리적 폴더 구조를 만듭니다. 역할을 가져오고 BI 플랫폼에 콘텐츠를 게시하면 해당 폴더가 만들어집니다. 관리자 권한이 있는 경우 이러한 폴더를 만들 필요가 없습니다. SAP 인증 플러그인 구성 시 권한 부여 시스템을 정의하고 역할을 CMC로 가져온 후 BI 플랫폼에 콘텐츠를 게시하면 폴더가 만들어집니다.

참고:

BI 플랫폼 관리자는 다음 폴더에 대해 올바른 권한을 할당해야 합니다.

- SAP 최상위 폴더
 - Everyone 그룹이 SAP 최상위 폴더에 대해 제한된 액세스 권한을 갖는지 확인합니다.
- 시스템 ID 폴더
 - CMC에서 보안 주체 게시자에게 다음 권한을 지정합니다.
 - 폴더에 개체 추가
 - 개체 보기
 - 개체 편집
 - 개체에 대한 사용자의 권한 수정
 - 개체 삭제

팁:

권한을 보다 쉽게 관리하려면 이러한 권한이 포함된 사용자 지정된 게시자 액세스 수준을 만든 후 관련 시스템 ID 폴더에서 보안 주체 게시자에 이 액세스 수준을 부여할 수 있습니다.

관련 항목

- 128 페이지에서 [액세스 수준 작업](#)"
- 113 페이지에서 [BI 플랫폼에서 권한 작동 방식](#)"

19.1.1.1.2 기본 폴더 보안 패턴 이해

SAP에서 BI 플랫폼에 콘텐츠를 게시하면 시스템은 나머지 역할, 폴더 및 보고서에 대한 계층 구조를 자동으로 만듭니다. 즉, BI 플랫폼은 Crystal 보고서를 시스템 ID와 클라이언트 번호에 따라 명명된 폴더와 역할 이름에 따라 명명된 폴더로 구성합니다.

아래 그림은 한 BW 시스템의 두 역할을 게시할 때 BI 플랫폼에서 콘텐츠가 구성되는 방식을 보여 줍니다.

- 권한 부여 시스템을 정의하면 BI 플랫폼에서는 최상위 폴더 SAP, 2.0과 시스템(SID) 폴더가 만들어집니다.
- 역할이 BW에서 게시되면 필요에 따라 역할 폴더(BI 플랫폼에 그룹으로 가져옴)가 만들어집니다.
- 또한 콘텐츠가 게시되는 각 역할마다 콘텐츠 폴더를 만듭니다.
- 각 보고서 개체에 대해 보안이 설정되므로 사용자는 해당 역할에 속하는 보고서만 볼 수 있습니다.

관리자는 다양한 역할의 구성원에게 권한을 지정합니다. 이를 위해 콘텐츠 관리 워크벤치에서 다음 권한이 지정되어야 합니다.

콘텐츠 폴더

BI 플랫폼은 CMC에서 정의된 권한 부여 시스템에 추가된 각 역할에 대한 그룹을 가져옵니다.

콘텐츠 보유 역할의 모든 구성원에게 적절한 기본 권한을 부여하려면 콘텐츠 관리 워크벤치에서 BI 플랫폼에 정의된 각 권한 부여 시스템에 대한 적절한 권한을 부여합니다.

1. 콘텐츠 관리 워크벤치에서 Enterprise 시스템을 확장한 후 사용 가능한 시스템을 확장합니다.
2. 원하는 시스템을 두 번 클릭합니다.
3. 레이아웃탭을 클릭합니다.
4. 리포트의 기본 보안 정책을 보기로 설정합니다.
5. 역할 폴더의 기본 보안 정책을 요청 시 보기로 설정합니다.
6. 확인을 클릭합니다.

BI 플랫폼의 모든 콘텐츠 역할, 즉 콘텐츠가 게시된 역할에 이러한 설정이 반영됩니다. 이러한 역할의 구성원은 다른 역할에 게시된 보고서의 예약된 인스턴스를 볼 수 있으며 해당 구성원이 속하는 역할에 게시된 보고서를 새로 고칠 수 있습니다.

참고:

역할별 작업을 명확하게 구분하여 유지 관리하는 것이 좋습니다. 예를 들어, 관리자 역할에서 콘텐츠를 게시할 수도 있지만 가능하면 게시자 역할의 구성원만 콘텐츠를 게시할 수 있도록 하는 것이 더 좋습니다. 또한 게시 역할의 기능은 콘텐츠를 게시할 수 있는 사용자를 정의하는 것으로만 국한됩니다. 따라서 게시 역할에는 어떠한 콘텐츠도 포함되지 않아야 합니다. 게시자의 임무는 일반적인 역할 구성원이 액세스할 수 있는 콘텐츠 보유 역할에 대해 콘텐츠를 게시하는 데서 그쳐야 합니다.

19.1.1.2 BW 게시자 구성

BW 게시자를 사용하여 개별적으로 또는 일괄로 BW에서 BI 플랫폼으로 Crystal 보고서(.rpt 파일)를 게시할 수 있습니다.

Windows에서는 다음 두 가지 방법 중 하나로 BW 게시자를 구성할 수 있습니다.

- BI 플랫폼 컴퓨터에서 서비스를 사용하여 BW 게시자를 시작합니다. BW 게시자 서비스는 필요에 따라 BW 게시자의 인스턴스를 시작합니다.

- 로컬 SAP 게이트웨이를 통해 BW 게시자를 시작하여 BW 게시자 인스턴스를 만듭니다.

각 구성의 장단점을 고려한 후 사이트 요구에 맞는 구성 방법을 선택해야 합니다. BI 플랫폼에서 BW 게시자를 구성하고 나면 콘텐츠 관리 워크벤치에서 게시를 구성해야 합니다.

19.1.1.3 BW 게시자를 서비스로 구성

이 단원에서는 BW 게시자를 서비스로 사용하여 BW의 보고서를 BI 플랫폼에 게시할 수 있도록 설정하는 방법을 설명합니다. 다음 절차를 수행하십시오.

19.1.1.3.1 BW 게시자 설치 배포

이 단원에서는 BW 게시자 서비스의 배포에 대한 내용과 다른 BI 플랫폼 구성 요소에서 BW 게시자를 분리하는 방법을 설명합니다.

BW 게시자 서비스를 같은 BI 플랫폼 시스템에 포함된 별도의 두 컴퓨터에 설치하는 방식으로 BW의 게시 부하를 분산할 수 있습니다.

BI 플랫폼 컴퓨터에 BW 게시자를 설치할 때 각 게시자가 동일한 프로그램 ID와 SAP 게이트웨이 호스트 및 게이트웨이 서비스를 사용하도록 구성합니다. 프로그램 ID를 사용하는 RFC 대상을 만들면 BW에서는 BI 플랫폼 컴퓨터 간에 게시 부하를 분산시킵니다. 또한 한 BW 게시자를 사용할 수 없게 되면 나머지 BW 게시자를 계속 사용할 수 있습니다.

여러 BW 응용 프로그램 서버를 포함하는 구성에서는 시스템 중복성 수준을 높일 수 있습니다. 각 BW 응용 프로그램 서버가 SAP 게이트웨이를 실행하도록 구성합니다. 또한 각 서버별로 BI 플랫폼 컴퓨터에 별도의 BW 게시자 서비스를 설치합니다. 각 BW 게시자 서비스가 별도의 BW 응용 프로그램 서버의 게이트웨이 호스트 및 게이트웨이 서비스를 사용하도록 구성합니다. 이 구성에서는 BW 게시자나 응용 프로그램 서버에 오류가 발생해도 BW에서 계속 게시할 수 있습니다.

다른 BI 플랫폼 구성 요소에서 BW 게시자를 분리하려면 독립 실행형 SAP 게이트웨이를 사용하여 BW를 설치합니다.

이 경우 BW 게시자가 있는 동일한 컴퓨터에 로컬 SAP 게이트웨이를 설치해야 합니다. 또한 BW 게시자에서 BI 플랫폼 SDK(소프트웨어 개발 키트) 및 Crystal Reports 인쇄 엔진에 액세스할 수 있어야 합니다. 따라서 전용 컴퓨터에 BW 게시자 및 로컬 SAP 게이트웨이를 설치할 경우 SIA 서버도 설치해야 합니다.

19.1.1.3.2 BW 게시자 시작: UNIX

BW 게시자 스크립트를 실행하여 게시 요청을 처리할 게시자 인스턴스를 만듭니다. 하나의 게시자 인스턴스를 시작할 것을 권장합니다.

BW 게시자가 시작되면 BI 플랫폼 설치 프로그램을 실행할 때 지정한 SAP 게이트웨이 서비스와 연결됩니다.

19.1.1.3.3 BW 게시자 시작: Windows

Windows에서 중앙 구성 관리자(CCM)를 사용하여 BW 게시자 서비스를 시작합니다. BW 게시자 서비스를 시작하면 BW 시스템의 게시 요청을 처리하기 위한 게시자 인스턴스가 만들어집니다. 게시 요청의 볼륨이 증가하면 BW 게시자는 자동으로 요구에 맞게 추가 게시자를 생성합니다.

BW 게시자가 시작되면 BI 플랫폼 설치 프로그램을 실행할 때 지정한 SAP 게이트웨이 서비스와 연결됩니다.

19.1.1.3.4 BW 게시자 서비스의 대상 구성

BW 게시자를 사용하도록 설정하려면 BW 서버의 RFC 대상이 BW 게시자 서비스와 통신하도록 구성해야 합니다. BW 클러스터가 있는 경우 각 서버에서 RFC 대상을 구성하고, 모든 경우에 BW의 중앙 인스턴스를 게이트웨이 호스트로 사용합니다.

BW에서 여러 BI 플랫폼 배포 환경에 게시하려는 경우 BI 플랫폼 시스템마다 BW 게시자 서비스에 대한 별도의 RFC 대상을 만듭니다. 각 대상에 대해 고유한 프로그램 ID를 사용해야 하지만 게이트웨이 호스트와 게이트웨이 서비스는 동일해야 합니다.

19.1.1.3.5 로컬 SAP 게이트웨이로 BW 게시자 구성

참고:

BI 플랫폼이 UNIX에 설치되어 있는 경우에는 이 구성을 사용하지 마십시오. UNIX에서 이 방법을 사용하면 예측할 수 없는 시스템 동작이 발생할 수 있습니다.

BW에 있는 보고서를 BI 플랫폼에 게시할 수 있도록 설정하려면 로컬 SAP 게이트웨이를 사용하여 다음 절차를 수행하십시오.

- 674 페이지에서 ["로컬 SAP 게이트웨이 설치"](#)
- 674 페이지에서 ["BW 게시자의 대상 구성"](#)

19.1.1.3.6 로컬 SAP 게이트웨이 설치

로컬 SAP 게이트웨이는 BW 게시자를 설치한 컴퓨터에 설치되어야 합니다. SAP BASIS 관리자가 이러한 SAP 게이트웨이 중 하나를 설치하는 것이 좋습니다.

로컬 SAP 게이트웨이 설치에 대한 최신 지침을 보려면 SAP 제공 CD에 포함되어 있는 SAP 설치 지침을 참조하십시오.

BI 플랫폼에 대해 검증된 환경의 상세 목록은 제품과 함께 제공된 platforms_EN.txt 파일을 참조하십시오. 이 파일에는 응용 프로그램 서버, 운영 체제, SAP 구성 요소 등에 대한 특정 버전 및 서비스 팩 요구 사항이 나와 있습니다.

SAP 게이트웨이를 설치한 후에 regedit를 사용하여 TMP 및 TEMP 레지스트리 항목이 HKEY_CURRENT_USER\Environment 하위 키 아래에 있는지 확인합니다. 두 레지스트리 항목은 유효한 절대 디렉터리 경로인 동일한 문자열 값을 포함해야 합니다. 항목 값에 %USERPROFILE% 변수가 포함되어 있으면 절대 디렉터리 경로로 바꾸십시오. 일반적으로 두 레지스트리 항목은 C:\WINDOWS\TEMP로 설정되어 있습니다.

19.1.1.4 BW 게시자의 대상 구성

BW 게시자를 사용하도록 설정하려면 로컬 SAP 게이트웨이 및 BW 게시자를 설치한 컴퓨터의 위치를 BW에 제공하도록 RFC 대상을 구성해야 합니다.

19.1.1.5 콘텐츠 관리 워크벤치에서 게시 구성

SAP 인증을 설정하고 BW 게시자를 구성한 경우 이 단원에 대략적으로 설명되어 있는 기능을 수행하여 게시를 사용 가능하게 설정하십시오. 지침에 따라 다음을 수행할 수 있습니다.

- 콘텐츠 관리 워크벤치의 각 사용자에게 인증을 설정합니다.
- 콘텐츠가 게시되는 BI 플랫폼 배포 환경에 대한 연결을 설정합니다.
- 각 BI 플랫폼 배포 환경에 게시할 수 있는 역할을 정의합니다.
- BW의 콘텐츠를 BI 플랫폼에 게시합니다.

19.1.1.6 콘텐츠 관리 워크벤치에 액세스할 수 있는 사용자

콘텐츠 관리 워크벤치에 액세스할 수 있는 사용자 유형은 다음과 같습니다.

- 콘텐츠 보유 역할에 속하며 보고서를 볼 수 있는 콘텐츠 소비자. 이 사용자 유형은 보고서 조회만 가능합니다.
- BW에서 보고서를 조회, 게시, 수정 및 필요에 따라 삭제할 수 있는 BI 플랫폼 콘텐츠 게시자
- 콘텐츠 관리 워크벤치 내에서 모든 작업을 수행할 수 있는 BI 플랫폼 관리자. 이러한 작업에는 BI 플랫폼 시스템 정의, 보고서 게시 및 보고서 유지 관리 수행이 포함됩니다.

19.1.1.7 BW에서 지정된 콘텐츠 게시자에 대한 역할 만들기

BI 플랫폼과 통합되도록 BW를 구성할 때 현재 역할 구조가 특정 BW 사용자를 콘텐츠 게시자나 시스템 관리자로 빠르게 지정할 수 있는지 여부를 평가합니다.

만든 새 역할에 의미를 적절히 설명하는 레이블을 지정하는 것을 권장합니다. 의미를 적절히 설명하는 역할의 예에는 BOE_CONTENT_PUBLISHERS 및 BOE_SYSTEM_ADMINISTRATORS가 있습니다.

팁:

BI 플랫폼에서 관리자에게 전체 시스템 관리 권한 또는 해당 권한의 일부를 할당할 수 있습니다.

BI 플랫폼에서 이러한 새 역할이나 기존 역할이 부여되는 권한을 수정하려면 먼저 SAP 인증을 설정하고 역할을 가져와야 합니다. 그런 후 중앙 관리 콘솔을 통해 가져온 각 역할의 권한을 수정할 수 있습니다.

19.1.1.8 콘텐츠 관리 워크벤치에 대한 액세스 구성

콘텐츠 관리 워크벤치에 액세스할 수 있는 각 사용자 유형에 대해 BW에서 적절한 권한 집합을 적용해야 합니다. 이러한 권한은 다음 표에 나와 있습니다.

테이블 19-1: 관리 사용자의 권한

인증 개체	필드	값
S_RFC S_TCODE	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/CE_SYNCH, SH3A, SUNI
	ACTVT	실행(16)
	TCD	/CRYSTAL/RPTADMIN, RSCR_MAINT_PUBLISH
S_TABU_CLI	CLIIDMAINT	X

인증 개체	필드	값
S_TABU_DIS	ACTVT	변경, 표시(02, 03)
	DICBERCLS	&NC&
	JOBACTION	DELE, RELE
	JOBGROUP	' '
S_RS_ADMWB	ACTVT	실행(16)
	RSADMWBOBJ	WORKBENCH
	ACTVT	새로 만들기, 변경, 표시, 삭제 (01, 02, 03, 06)
ZCNTADMJOB	ACTVT	새로 만들기, 삭제(01, 06)
ZCNTADM RPT	ACTVT	표시, 삭제, 활성화, 유지 관리, 확인(03, 06, 07, 23, 39)

테이블 19-2: 콘텐츠 게시자의 권한

인증 개체	필드	값
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/CE_SYNCH, SH3A, SUNI
	ACTVT	실행(16)
	TCD	/CRYSTAL/RPTADMIN

인증 개체	필드	값
S_BTCH_JOB	JOBACTION	DELE, RELE
	JOBGROUP	' '
	ACTVT	실행(16)
	RSADMWBOBJ	WORKBENCH
ZCNTADMCES	ACTVT	표시(03)
ZCNTADMJOB	ACTVT	(새로 만들기, 삭제) 01, 06
ZCNTADMRPT	ACTVT	표시, 활성화, 유지 관리, 확인 (03, 07, 23, 39) 삭제(옵션)(06) 편집(옵션)(02)

BW 콘텐츠 관리 워크벤치에서 보고서를 삭제할 수 있는 권한을 콘텐츠 게시자에게 부여하는 것은 선택 사항입니다. 그러나 BW에서 보고서를 삭제하면 BI 플랫폼에서도 보고서가 삭제됩니다. 게시자가 BI 플랫폼에서 보고서를 삭제할 수 있는 충분한 권한이 없으면 오류가 발생합니다.

콘텐츠 소비자의 권한

인증 개체	필드	값
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SH3A, SUNI
	ACTVT	실행(16)
	TCD	/CRYSTAL/RPTADMIN

인증 개체	필드	값
S_RS_ADMWB	ACTVT	실행(16)
	RSADMWBOBJ	WORKBENCH
	ACTVT	표시(03)

19.1.1.9 BI 플랫폼 시스템 정의

보고서를 게시하려는 각 BI 플랫폼 시스템에 대해 콘텐츠 관리 워크벤치 내에서 시스템 정의를 만들어야 합니다.

19.1.1.9.1 BI 플랫폼 시스템 추가

1. 트랜잭션 /crystal/rptadmin을 실행하여 콘텐츠 관리 워크벤치에 액세스합니다.
2. 작업 창에서 Enterprise 시스템을 선택합니다.
3. 새 시스템 추가를 두 번 클릭합니다.
4. 시스템 탭에서 다음 값을 입력합니다.
 - 별칭 필드에 의미를 설명하는 이름을 입력합니다. 공백이나 특수 문자는 Enterprise 포털 구성 시 별칭 이름이 사용될 때 특수하게 취급되어야 하므로 사용하지 마십시오.
 - BI 플랫폼 CMS가 실행되는 컴퓨터의 이름을 입력합니다. 기본 포트가 아닌 다른 포트에서 수신 대기하도록 CMS를 구성한 경우 CMSNAME:PORT를 입력합니다.
 - BI 플랫폼 시스템에 명시적으로 할당되지 않은 역할에서 이 시스템에 보고서를 게시하려면 기본 시스템을 선택합니다. 하나의 BI 플랫폼 시스템만 기본 시스템이 될 수 있습니다.

사용 가능한 모든 시스템 목록에서 기본 시스템에는 녹색 확인 표시가 붙어 있습니다.
5. 저장을 클릭합니다.

6. RFC 대상 탭에서 이 BI 플랫폼 시스템과 관련된 각 RFC 대상을 추가합니다. 대상을 추가하려면 행 삽입 단추를 클릭합니다. 표시되는 목록에서 RFC 대상의 이름을 두 번 클릭합니다.

참고:

BI 플랫폼 시스템에는 시스템 중복성을 추가하기 위해 여러 대상이 있을 수 있습니다.

7. 다음으로, 대상을 테스트합니다. 이름 왼쪽의 회색 상자를 클릭하여 방금 추가한 대상을 선택합니다.
8. CE 정의 확인을 클릭합니다.

이 테스트는 BW가 지정한 BW 게시자에 연결할 수 있는지와 Crystal 권한 부여 사용자 계정을 사용하여 이 BI 플랫폼 시스템에 로그인할 수 있는지 확인합니다.

9. HTTP 탭에서 다음 값을 입력합니다.

- 프로토콜

BI 플랫폼에 연결되어 있는 웹 서버가 https를 사용하도록 구성되어 있지 않다면 http를 입력합니다.

- 웹 서버 호스트 및 포트

BI 실행 패드를 호스팅하는 웹 서버의 정규화된 도메인 이름이나 IP 주소를 입력합니다. Java 응용 프로그램 서버를 사용하는 설치의 경우 포트 번호를 포함시킵니다. 예를 들면 다음과 같습니다.

```
boserver01.businessobjects.com:8080
```

- 경로

다음과 같이 입력합니다.

```
SAP
```

이 경로는 기본적으로 BI 플랫폼 웹 콘텐츠의 sap 하위 폴더를 참조할 때 웹 서버가 사용하는 가상 경로입니다. BI 플랫폼 웹 콘텐츠 파일의 웹 환경 및 위치를 사용자 지정한 경우에만 다른 값을 제공합니다.

이 항목 맨 앞이나 끝에 슬래시를 입력하지 마십시오.

- 뷰어 응용 프로그램

뷰어 응용 프로그램의 이름을 입력합니다. InfoView의 Java 버전을 사용하는 BI 플랫폼의 기본 뷰어를 사용하도록 reportview.do를 입력합니다. 기본 ASP.NET 구성을 사용하여 Windows에 BI 플랫폼을 설치한 경우, 기본 브라우저를 사용하도록 report/report_view.aspx를 입력합니다.

10. 언어 탭에서 이 BI 플랫폼 시스템에 게시할 보고서의 언어를 선택합니다.
11. 역할 탭을 사용하여 이 BI 플랫폼 시스템에 연결할 콘텐츠 보유 역할을 추가합니다.
12. 행 삽입 단추를 클릭합니다.

이 BI 플랫폼 시스템에 추가할 수 있는 사용 가능한 역할 목록이 표시됩니다.

참고:

각 역할은 하나의 BI 플랫폼 시스템에만 게시할 수 있습니다. 이 BI 플랫폼에 추가하려는 역할이 목록에 표시되지 않으면 취소를 클릭하여 역할 탭으로 돌아갑니다. 그런 후 역할 다시 할당을 클릭합니다.

13. 이 BI 플랫폼 시스템에 게시할 역할을 선택한 후 확인 단추를 클릭합니다.
14. 다음으로 이 BI 플랫폼 시스템에 게시된 콘텐츠의 기본 보안 설정을 지정합니다. 레이아웃 탭을 클릭하고 보고서 및 역할 폴더에 기본적으로 사용되는 보안 설정을 선택합니다.

참고:

- 해당 시스템에 게시된 각 역할에 대한 폴더가 BI 플랫폼에 자동으로 만들어집니다. 이 폴더에는 해당 역할 아래에 게시된 보고서에 대한 바로 가기가 포함되어 있습니다.
 - 일단 BI 플랫폼 시스템을 구성하면 여기에서 기본 보안 수준을 변경해도 게시된 역할 폴더나 보고서의 보안 수준에는 영향을 주지 않습니다. BI 플랫폼에 게시된 모든 역할 및 콘텐츠의 기본 보안 수준을 변경하려면 BI 플랫폼에서 역할 폴더 및 바로 가기를 삭제합니다. 이렇게 해도 실제 보고서는 삭제되지 않습니다. 그런 후 여기에서 보안 설정을 변경하고 역할 및 보고서를 다시 게시합니다.
15. 맨 아래의 확인 단추를 클릭하여 설정을 저장하고 콘텐츠 관리 워크벤치에서 BI 플랫폼 시스템을 만듭니다.

이제 BW에 있는 보고서를 BI 플랫폼에 게시할 수 있습니다.

19.1.1.10 콘텐츠 관리 워크벤치를 사용하여 보고서 게시

BW에 보고서를 저장한 후에는 콘텐츠 관리 워크벤치를 사용하여 보고서를 게시할 수 있습니다. 콘텐츠 관리 워크벤치를 사용하여 개별 보고서를 게시하거나 특정 역할에 저장된 모든 보고서를 게시할 수 있습니다. Crystal 콘텐츠 게시자에 부여된 권한이 있는 사용자만 콘텐츠 관리 워크벤치를 사용하여 보고서를 게시하고 유지 관리할 수 있습니다.

관련 항목

- 702 페이지에서 [권한 만들기 및 적용](#)

19.1.1.11 역할 또는 보고서 게시

1. /crystal/rptadmin 트랜잭션을 실행하여 콘텐츠 관리 워크벤치에 액세스합니다.

2. 작업 창에서 리포트 게시를 선택합니다.
3. BW 시스템에 저장된 콘텐츠를 찾으려면 게시할 리포트 및 역할 선택을 두 번 클릭합니다.

사용 가능한 역할 및 보고서를 필터링할 수 있는 대화 상자가 표시됩니다.

4. 시스템 목록에서 BI 플랫폼 시스템 또는 표시하려는 콘텐츠가 포함되어 있는 시스템을 선택합니다.

참고:

시스템 목록에는 이 BW 시스템에 정의되어 있는 사용 가능한 모든 시스템이 포함되어 있습니다.

5. 다음으로 결과를 필터링하여 표시되는 보고서 및 역할의 수를 제한합니다. 다음 옵션을 사용합니다.

- 오브젝트 버전

"A: active"를 선택하면 게시될 수 있는 모든 보고서가 표시됩니다. 빈 옵션을 선택하면 모든 보고서가 표시됩니다. 나머지 옵션은 SAP 예약어입니다.

- 오브젝트 상태

"ACT Active, executable"을 선택하면 게시된 보고서만 표시됩니다. "INA Inactive, not executable"을 선택하면 게시되지 않은 보고서만 표시됩니다. 이 필드를 비워 두면 모든 보고서가 표시됩니다. 나머지 옵션은 SAP 예약어입니다.

- 역할 필터

이 상자에 텍스트를 입력하면 여기에 입력한 텍스트와 일치하는 역할만 표시됩니다. 와일드카드 문자로 *를 사용합니다. 예를 들어, 문자 d로 시작하는 모든 역할을 표시하려면 "d*"를 입력합니다.

- 리포트 내역




이 상자에 텍스트를 입력하면 해당 설명이 여기에 입력한 텍스트와 일치하는 보고서만 표시됩니다. 임의의 수의 문자를 나타내는 와일드카드 문자로 *를 사용합니다. 0개 또는 1개의 문자를 나타내는 와일드카드 문자로 +를 사용합니다. 예를 들어, 설명에 단어 revenue가 들어 있는 모든 보고서를 표시하려면 *revenue*를 입력합니다.

6. 확인을 클릭합니다.

조건과 일치하는 보고서 목록이 오른쪽 창에 표시됩니다.

보고서는 시스템 > 해당 시스템의 역할 > 역할에 저장된 보고서 등과 같은 계층으로 정렬됩니다.

계층의 각 항목에는 빨간색, 노란색 또는 녹색 점과 같은 레이블이 붙습니다. 계층에서 상위에 있는 항목은 포함하는 항목의 상태를 나타내며, 최상위 계층에는 포함 항목 중 가장 적게 사용된 상태의 레이블이 적용됩니다. 예를 들어, 역할 중 한 보고서의 상태가 노란색(활성)이지만 나머지 보고서가 모두 녹색(게시됨)이면 역할이 노란색(활성)으로 표시됩니다.

-  녹색: 항목이 완전히 게시되었음을 나타냅니다. 항목이 BI 플랫폼 시스템 또는 역할이면 해당 항목의 모든 보고서가 게시됩니다.
-  노란색: 항목이 활성 상태이지만 게시되지 않았습니다. 항목이 보고서인 경우에는 게시할 수 있습니다. 항목이 역할이거나 BI 플랫폼 시스템이면 모든 콘텐츠가 활성 상태이고 해당 역할이나 시스템에 포함된 하나 이상의 항목이 게시되지 않은 것입니다.
-  빨간색: 항목이 SAP 콘텐츠이며 콘텐츠 관리 워크벤치를 사용하여 게시할 수 없습니다. 콘텐츠는 BW Administration 워크벤치를 사용하여 활성화되어야만 게시할 수 있습니다.

7. 게시하려는 보고서를 선택합니다.

역할의 모든 보고서를 게시하려면 해당 역할을 선택합니다. BI 플랫폼 시스템에 모든 역할을 게시하려면 해당 시스템을 선택합니다.

참고:

역할이나 시스템을 선택하면 해당 역할이나 시스템에 포함되어 있는 모든 보고서가 선택됩니다. 선택한 항목을 취소하려면 역할 또는 시스템 확인란을 선택 취소한 후 새로 고침을 클릭합니다.

8. 게시를 클릭합니다.

참고:

백그라운드에서 게시된 보고서는 시스템 리소스가 사용 가능해질 때 처리됩니다. 이 옵션을 사용하려면 게시 대신 백그라운드를 클릭합니다.

9. 새로 고침을 클릭하여 콘텐츠 관리 워크벤치에서 BI 플랫폼 시스템, 역할 및 보고서의 상태 표시를 업데이트합니다.

팁:

보고서를 보려면 해당 보고서를 마우스 오른쪽 단추로 클릭하고 보기를 선택합니다. 보고서에 사용되는 쿼리를 확인하려면 보고서를 마우스 오른쪽 단추로 클릭하고 사용된 질의를 선택합니다.

참고:

보고서를 BI 플랫폼에 게시한 후에 게시한 보고서를 덮어쓰려면 덮어쓰기를 클릭합니다.

관련 항목

- 683 페이지에서 [백그라운드 게시 예약](#)

19.1.1.12 백그라운드 게시 예약

보고서를 즉시 또는 예약된 작업으로 백그라운드에서 게시하면 시스템 리소스가 보존됩니다. 시스템 응답력 향상을 위해 백그라운드에서 보고서를 게시할 것을 권장합니다.

보고서를 주기적으로 예약된 작업으로 게시하면 BW와 BI 플랫폼 시스템 간에 보고서 정보가 동기화됩니다. 모든 보고서 또는 이러한 보고서가 포함된 역할을 예약할 것을 권장합니다. 보고서 유지보수 작업의 상태 업데이트 옵션을 사용하여 역할 및 보고서를 수동으로 동기화할 수도 있습니다.

19.1.1.13 게시된 보고서에 대한 시스템 정보 업데이트

BW 게시자는 여기에 입력된 SAP 시스템 정보를 사용하여 게시된 보고서의 데이터 소스를 업데이트합니다. 부하 분산 구성을 원할 경우 로컬 BW 응용 프로그램 서버나 중앙 BW 인스턴스를 사용하도록 선택할 수 있습니다.

19.1.1.14 보고서 유지 관리

보고서 유지 관리 작업에는 BI 플랫폼과 BW 간에 보고서 관련 정보를 동기화하는 작업(상태 업데이트), 불필요한 보고서를 삭제하는 작업(보고서 삭제) 및 이전 버전의 BI 플랫폼에서 마이그레이션한 보고서를 업데이트하는 작업(마이그레이션 이후)이 포함됩니다.

19.1.1.14.1 보고서 상태 업데이트

BI 플랫폼 시스템에서 게시된 보고서를 변경하는 경우(예: 보고서가 게시된 역할 변경) BI 플랫폼과 BW를 동기화할 때까지 변경 내용이 BW에 반영되지 않습니다. BI 플랫폼과 BW를 주기적으로 동기화하도록 게시 작업의 일정을 설정하거나(683 페이지에서 ["백그라운드 게시 예약"](#) 참조) 보고서 유지 관리 도구를 사용하여 보고서 상태를 수동으로 업데이트할 수 있습니다.

19.1.1.14.2 리포트 삭제

컨텐츠 관리 워크벤치를 사용하여 BW에서 게시된 보고서를 삭제하면 BI 플랫폼에서도 해당 보고서가 삭제됩니다. BW와 BI 플랫폼 시스템 둘 다에서 보고서를 삭제하는 데 필요한 권한이 부여된 사용자만 보고서를 제거할 수 있습니다.

참고:

사용자에게 BW에서 보고서를 삭제할 권한이 있지만 해당 보고서가 게시된 BI 플랫폼 시스템에서 보고서를 삭제할 권한이 없으면 오류가 발생할 수 있습니다.

19.1.1.15 SAP http 요청 핸들러 구성

BW에서 보고서가 표시되게 설정하려면 컨텐츠 관리 워크벤치의 일부로 포함된 http 요청 핸들러를 사용하도록 BW를 구성해야 합니다. 그런 다음 BW 사용자가 SAP GUI에서 Crystal Report를 열면 BW는 웹을 통해 보기 요청을 적절히 전송할 수 있습니다.

트랜잭션 SICF를 사용하여 BW 시스템에서 활성 상태인 가상 호스트 및 서비스의 목록에 액세스합니다. default_host 계층 구조에서 BW 아래에 ce_url이라는 노드를 만든 후 처리기 목록에 /CRYSTAL/CL_BW_HTTP_HANDLER를 추가합니다. 이 서비스를 만든 후에 수동으로 활성화해야 할 수 있습니다.

19.1.1.16 SAP 데이터 처리 구성

19.1.1.16.1 SAP의 배치 모드로 예약된 보고서 처리

Windows 설치의 경우 SAP의 배치 모드를 사용하여 BI 플랫폼에서 예약된 보고서를 실행할 수 있습니다. InfoSet 및 Open SQL 드라이버는 특정 환경 변수가 1로 설정되어 있을 때 SAP의 배치 모드나 백그라운드 모드를 사용하여 보고서를 실행할 수 있습니다. 관련 환경 변수는 다음과 같습니다.

- CRYSTAL_INFOSET_FORCE_BATCH_MODE(InfoSet 드라이버용)
- CRYSTAL_OPENSQLE_FORCE_BATCH_MODE(Open SQL 드라이버용)

그러나 BI 플랫폼의 분산 설치를 수행한 경우에만 이 기능을 사용할 것을 권장합니다. 이러한 환경 변수를 1로 설정하면 드라이버는 실제로 보고서를 실행 중인 보고서 구성 요소에 관계없이, SAP의 배치 모드를 사용하여 보고서를 실행합니다. 따라서 이러한 환경 변수를 BI 플랫폼 서버 조합이 실행되는 컴퓨터의 시스템 환경 변수로 만들 경우 드라이버는 모든 보고서를 배치 모드로 실행합니다(Crystal Reports 처리 서버 및 Report Application Server의 주문형 보고서 요청 포함).

드라이버가 예약된 보고서만 배치 모드로 실행하게 하려면(예: 보고서 작업 서버에 의해 실행되는 보고서) BI 플랫폼 서버 조합이 실행되는 컴퓨터에서 시스템 환경 변수를 설정하지 마십시오. 대신 다음 단계에 따라 각 보고서 작업 서버에 맞게 환경 변수를 사용자 지정합니다.

참고:

BI 플랫폼에서 보고서 일정을 설정하는 SAP 사용자는 SAP에서 추가 권한이 필요할 수 있습니다.

관련 항목

- 725 페이지에서 [배치 모드에서 Open SQL 쿼리를 사용하여 보고서 일정 설정](#)"

19.1.1.16.2 예약된 보고서를 SAP의 배치 모드에서 처리하려면

1. 메모장과 같은 텍스트 편집기에서 다음 내용을 사용하여 배치 스크립트(.bat 파일)를 만듭니다.

```
@echo off
set CRYSTAL_INFOSET_FORCE_BATCH_MODE=1
set CRYSTAL_OPENSQLE_FORCE_BATCH_MODE=1
%*
```

이 스크립트는 환경 변수를 1로 설정한 후 명령줄에서 스크립트에 전달된 모든 매개 변수를 실행합니다.

2. 이 파일 이름을 jobserver_batchmode.bat로 지정하여 각 보고서 작업 서버 시스템의 폴더에 저장합니다.
3. BI 플랫폼 프로그램 그룹에서 중앙 구성 관리자(CCM)를 시작합니다.
4. Crystal Report 작업 서버를 마우스 오른쪽 단추로 클릭한 후 바로 가기 메뉴에서 중지를 클릭합니다.
5. Crystal Report 작업 서버를 마우스 오른쪽 단추로 클릭한 후 바로 가기 메뉴에서 속성을 클릭합니다.
6. 속성 탭에서 명령 필드를 찾습니다.

이 필드의 명령은 보고서 작업 서버의 시작 명령입니다. 예를 들어 다음과 같은 명령이 표시될 수 있습니다(한 줄로 표시).

```
"WWSERVER01WC$WProgram FilesWSAO Business ObjectsWSAP BusinessObjects EnterpriseWwin32_x86WJobServer.exe" -service -name SERVER01.report -ns SERVER01 -objectType BusinessObjects Enterprise.Report -lib procReport -restart
```

7. 보고서 작업 서버 컴퓨터에 저장한 jobserver_batchmode.bat 파일의 전체 경로를 기본 명령 앞에 입력합니다.

이 예에서 배치 파일은 SERVER01 컴퓨터에 다음으로 저장됩니다.

```
C:\Crystal Scripts\Wjobserver_batchmode.bat
```

따라서 보고서 작업 서버에 대한 새 시작 명령은 다음과 같습니다.

```
"WWSERVER01WC$WCrystal Scripts\Wjobserver_batchmode.bat" "WWSERVER01WC$WProgram FilesWSAO Business ObjectsWSAP BusinessObjects Enterprise 12.0Wwin32_x86WJobServer.exe" -service -name SERVER01.report -ns SERVER01 -objectType BusinessObjects Enterprise.Report -lib procReport -restart
```

이 새 시작 명령은 먼저 배치 파일을 시작합니다. 그러면 배치 파일은 보고서 작업 서버에 대한 원래 시작 명령을 실행하기 전에 필요한 환경 변수를 설정합니다. 그 결과 보고서 작업 서버에서 사용할 수 있는 환경 변수가 주문형 보고서 작업을 담당하는 서버(Crystal Reports 처리 서버 및 Report Application Server)에서 사용할 수 있는 환경 변수와 다르게 지정됩니다.

8. CCM에서 명령 필드를 변경한 후에는 확인을 클릭합니다.
9. Crystal Report 작업 서버를 마우스 오른쪽 단추로 클릭한 후 바로 가기 메뉴에서 시작을 클릭합니다.

참고:

보고서 작업 서버가 시작되지 않으면 새 시작 명령이 올바른지 확인합니다.

10. CCM 도구 모음에서 서버 사용/사용 안 함을 클릭하고 BI 플랫폼 관리자 자격 증명으로 로그인한 후 보고서 작업 서버가 사용 가능하게 설정되어 있는지 확인합니다.

19.1.1.17 SAP 전송 구성

19.1.1.17.1 개요

BI 플랫폼에는 Open SQL 연결 전송, 인포세트 연결 전송, 행 수준 보안 정의 전송, 클러스터 정의 전송, 콘텐츠 관리 워크벤치, BW 쿼리 매개 변수 사용자 설정 전송, MDX 전송, ODS 전송의 8가지 전송이 포함되어 있습니다.

전송에는 유니 코드 호환 전송과 ANSI 전송의 두 가지가 있습니다. 6.20 이상의 BASIS 시스템을 실행하는 경우 유니코드 호환 전송을 사용하고 6.20 이전의 BASIS 시스템을 실행하는 경우에는 ANSI 전송을 사용합니다. 제품 배포 미디어의 WCollateralsWAdd-OnsWSAPWTransportsW 디렉터리에 설치된 전송이 모두 있습니다.

참고:

가능한 설치 충돌을 확인할 때 SAP 시스템에 개체 이름이 없는지 확인합니다. 개체는 기본적으로 /crystal/ 네임스페이스를 사용하므로 이 네임스페이스를 직접 만들 필요는 없습니다. /crystal/ 네임스페이스를 수동으로 만들 경우 액세스할 수 없는 라이선스 복구 키가 요구됩니다.

19.1.1.17.2 전송 구성

BI 플랫폼의 데이터 액세스 또는 BW 게시자 구성 요소를 설정하려면 해당 전송을 SAP 시스템으로 가져와야 합니다. 이러한 구성 요소는 SAP 시스템과 통신할 때 이러한 전송 파일의 콘텐츠를 사용합니다.

SAP 시스템에 필요한 설치 및 구성 절차는 변경 및 전송 시스템에 익숙하고 SAP 시스템에 대해 관리 권한이 있는 BASIS 전문가가 수행해야 합니다. 전송 파일을 가져오는 정확한 절차는 실행 중인 BASIS 버전에 따라 다릅니다. 특정 절차 세부 사항을 보려면 SAP 설명서를 참조하십시오.

데이터 액세스 구성 요소를 처음 배포할 때 모든 사용자는 기본적으로 모든 SAP 테이블에 액세스할 수 있습니다. 사용자가 액세스할 수 있는 SAP 데이터를 안전하게 보호하려면 보안 정의 편집기를 사용하십시오.

전송을 가져온 후에는 해당 사용자 액세스 수준을 구성해야 합니다. 필요한 권한을 만든 후 Crystal 보고서를 디자인하거나 실행하거나 일정을 설정할 SAP 사용자에게 프로필이나 역할을 통해 해당 권한을 적용합니다.

관련 항목

- 702 페이지에서 [권한 만들기 및 적용](#)

19.1.1.17.2.1 전송 유형

전송에는 유니 코드 호환 전송과 ANSI 전송의 두 가지가 있습니다. 6.20 이상의 BASIS 시스템을 실행하는 경우 유니코드 호환 전송을 사용하고 6.20 이전의 BASIS 시스템을 실행하는 경우에는 ANSI 전송을 사용합니다. 설치된 전송은 모두 제품 배포 미디어의 Collaterals\WAdd-Ons\WAPWTransports 디렉터리에 있습니다. transports.txt 파일에는 유니코드 호환 및 ANSI 전송 파일이 나열됩니다.

각 전송 유형에 대한 설명은 다음과 같습니다.

- Open SQL 연결 전송

Open SQL 연결 전송을 사용하여 Open SQL 드라이버를 SAP 시스템에 연결하고 관련 보고서를 작성할 수 있습니다.

- 행 수준 보안 정의 전송

이 전송은 Open SQL 연결 전송의 /crystal/auth 테이블에 대한 그래픽 인터페이스로 작동하는 보안 정의 편집기 도구를 제공합니다.

- 클러스터 정의 전송

이 전송은 클러스터 정의 도구를 제공합니다. 이 도구를 사용하여 ABAP 데이터 클러스터 정의에 대한 메타데이터 리포지토리를 작성할 수 있습니다. 이러한 정의는 Open SQL 드라이버가 이러한 데이터 클러스터에 대해 보고서를 작성하는 데 필요한 정보를 제공합니다.

참고:

ABAP 데이터 클러스터는 클러스터 테이블과 다릅니다. 클러스터 테이블은 DDIC에 이미 정의되어 있습니다.

- InfoSet 연결 전송

InfoSet 연결 전송을 사용하여 InfoSet 드라이버는 InfoSet 및 SAP 쿼리에 액세스할 수 있습니다.

- Content Administration 워크벤치 전송

이 전송은 BW 시스템에 대한 콘텐츠 관리 기능을 제공합니다. 이 전송은 UNICODE 호환 전송으로만 사용할 수 있습니다.

- BW 쿼리 매개 변수 사용자 설정 전송

이 전송은 BW 쿼리를 기반으로 하는 보고서에서 사용자 설정된 매개 변수 및 기본 매개 변수 값을 사용할 수 있도록 지원합니다.

19.1.1.17.2.2 충돌 검사

전송 파일의 콘텐츠는 파일을 가져올 때 SAP Business Objects 네임스페이스에 자동으로 등록됩니다. SAP Business Objects 네임스페이스는 최신 버전의 R/3 및 mySAP ERP에서 이 용도로 예약되어 있습니다. 그러나 인증 개체, 인증 클래스 및 레거시 개체와 같은 일부 개체의 개체 이름에 적절한 접두사가 포함되어 있지 않을 수 있습니다. 전송 파일을 가져오기 전에 이러한 개체 유형에 충돌이 없는지 확인할 것을 권장합니다.

함수 그룹, 함수 모듈 또는 기타 개체가 SAP 시스템에 이미 존재할 경우 BI 플랫폼 전송 파일을 가져오기 전에 네임스페이스를 확인해야 합니다. 사용 중인 SAP 버전에 대한 절차를 보려면 SAP 설명서를 참조하십시오.

19.1.1.17.2.3 전송 파일 가져오기

제품 배포 매체의 WCollateralsWAdd-OnsWSAPWTransportsW 디렉터리에 있는 transports_EN.txt 파일을 검토하십시오. 이 텍스트 파일에는 각 전송을 구성하는 파일의 정확한 이름이 표시됩니다. transports 디렉터리 아래의 cofiles 및 data 디렉터리는 SAP 서버의 .../trans/cofiles 및 .../trans/data 디렉터리에 해당합니다.

행 수준 보안 정의나 클러스터 정의 전송을 가져오기 전에 Open SQL 연결 전송을 가져와야 합니다. 다른 전송은 순서에 상관없이 가져올 수 있습니다.

참고:

- CD에서 서버로 파일을 복사한 후에는 모든 파일을 쓸 수 있는지 확인한 다음 전송을 가져옵니다. 가져올 파일이 읽기 전용이면 가져올 수 없습니다.
- 전송이 이진 파일이므로 UNIX 시스템의 경우 파일 손상을 피하기 위해 FTP를 통해 이진 모드로 파일을 추가해야 합니다. 또한 Unix 서버에 대한 쓰기 권한이 있어야 합니다.

19.1.1.17.2.4 전송

19.1.1.17.2.4.1 Open SQL 연결 전송

Open SQL 연결 전송을 사용하여 드라이버는 SAP 시스템에 연결하고 관련 보고서를 작성할 수 있습니다.

개체	형식	설명
/CRYSTAL/BC	패키지	개발 클래스
/CRYSTAL/OPENSQ	함수 그룹	Open SQL 함수
/CRYSTAL/OS QL_AUTH_FORMS	프로그램	도우미 프로그램
/CRYSTAL/OSQL_EXECUTE	프로그램	도우미 프로그램
/CRYSTAL/OSQL_TYPEPOOL PROG	프로그램	도우미 프로그램
/CRYSTAL/OSQL_TYPE POOLS	프로그램	도우미 프로그램
/CRYSTAL/OSQL_UTILS	프로그램	도우미 프로그램
ZSSI	인증 개체 클래스	보고서 인증 개체
ZSEGREPORT	인증 개체	보고서 인증 개체
/CRYSTAL/OSQL_CLU_AC TKEY_ENTRY	테이블	클러스터 메타데이터

개체	형식	설명
/CRYSTAL/OS QL_FCN_PARAM	테이블	함수 메타데이터
/CRYSTAL/OS QL_FCN_PARAM_FIELD	테이블	함수 메타데이터
/CRYSTAL/OSQL_FIELD_ENTRY	테이블	테이블 메타데이터
/CRYSTAL/OSQL_OBJECT_ENTRY	테이블	테이블 메타데이터
/CRYSTAL/OS QL_RLS_CHK_ENTRY	테이블	RLS 메타데이터
/CRYSTAL/OS QL_RLS_FCN_ENTRY	테이블	RLS 메타데이터
/CRYSTAL/OS QL_RLS_VAL_ENTRY	테이블	RLS 메타데이터
ZCLUSTDATA	테이블	클러스터 메타데이터
ZCLUSTID	테이블	클러스터 메타데이터
ZCLUSTKEY	테이블	클러스터 메타데이터
ZCLUSTKEY2	테이블	클러스터 메타데이터
/CRYSTAL/AUTHCHK	테이블	RLS 메타데이터
/CRYSTAL/AUTHFCN	테이블	RLS 메타데이터
/CRYSTAL/AUTHKEY	테이블	RLS 메타데이터

개체	형식	설명
/CRYSTAL/AUTHOBJ	테이블	RLS 메타데이터
/CRYSTAL/AUTHREF	테이블	RLS 메타데이터
ZSSAUTHCHK	테이블	이전 RLS 메타데이터
ZSSAUTHOBJ	테이블	이전 RLS 메타데이터
ZSSAUTHKEY	테이블	이전 RLS 메타데이터
ZSSAUTHREF	테이블	이전 RLS 메타데이터
ZSSAUTH FCN	테이블	이전 RLS 메타데이터

19.1.1.17.2.4.2 InfoSet 연결 전송

InfoSet 연결 전송을 사용하여 InfoSet 드라이버는 InfoSet에 액세스할 수 있습니다. 이 전송은 R/3 4.6c 이상과 호환됩니다. SAP R/3 4.6a 또는 이전 버전을 실행하는 경우 이 전송을 가져오지 마십시오.

개체	형식	설명
/CRYSTAL/BC	패키지	개발 클래스
/CRYSTAL/FLAT	함수 그룹	InfoSet 래퍼 함수
/CRYSTAL/QUERY_BATCH	프로그램	배치 모드 실행

개체	형식	설명
/CRYSTAL/QUERY_BATCH_STREAM	프로그램	배치 모드 실행 스트리밍

19.1.1.17.2.4.3 행 수준 보안 정의 전송

이 전송은 Open SQL 연결 전송의 /crystal/auth 테이블에 대한 그래픽 인터페이스로 작동하는 보안 정의 편집기 도구를 제공합니다.

개체	형식	설명
/CRYSTAL/BC	패키지	개발 클래스
/CRYSTAL/TABMNT	함수 그룹	함수 제한에 대한 테이블 유지 관리 보기의 함수 그룹
/CRYSTAL/RLSDEF	프로그램	주 프로그램
/CRYSTAL/RLS_INCLUDE1	프로그램	모듈 정의를 포함하는 포함 프로그램
/CRYSTAL/RLS_INCLUDE2	프로그램	서브루틴 정의를 포함하는 포함 프로그램
TDDAT [/CRYSTAL/AUTH-FCN]	테이블 내용	테이블 유지 관리 정의
TVDIR [/CRYSTAL/AUTH-FCN]	테이블 내용	테이블 유지 관리 정의

개체	형식	설명
/CRYSTAL/AUTHFCNS	전송 및 유지 관리 개체의 정의	테이블 유지 관리 정의
/CRYSTAL/RLS	트랜잭션	주 프로그램 트랜잭션
/CRYSTAL/RLSFCN	트랜잭션	주 프로그램에 의해 내부적으로 호출되는 도우미 트랜잭션

19.1.1.17.2.4.4 클러스터 정의 전송

이 전송은 클러스터 정의 도구를 제공합니다. 이 도구를 사용하여 ABAP 데이터 클러스터 정의에 대한 메타데이터 리포지토리를 작성할 수 있습니다. 이러한 정의는 Open SQL 드라이버가 이러한 데이터 클러스터에 대해 보고서를 작성하는 데 필요한 정보를 제공합니다.

참고:

ABAP 데이터 클러스터는 클러스터 테이블과 다릅니다. 클러스터 테이블은 DDIC에 이미 정의되어 있습니다.

개체	형식	설명
ZCIMPRBG	프로그램	주 프로그램
ZCRBGTOP	프로그램	포함 프로그램
ZCDD	트랜잭션	주 프로그램 트랜잭션

19.1.1.17.2.4.5 Content Administration 워크벤치

이 전송은 BW 시스템에 대한 콘텐츠 관리 기능을 제공합니다. 이 전송은 UNICODE 호환 전송으로만 사용할 수 있습니다.

개체	형식	설명
/CRYSTAL/BC	패키지	개발 클래스
/CRYSTAL/CL_BW_HTTP_HANDLER	클래스	다중 CE 인식 HTTP 요청 처리기
/CRYSTAL/OBJECT_STATUS_DOM	도메인	보고서 작업
/CRYSTAL/OBJ_POLICY_DOM	도메인	CE 개체 보안
/CRYSTAL/OBJECT_STATUS	데이터 요소	보고서 작업
/CRYSTAL/OBJ_POLICY	데이터 요소	CE 개체 보안
/CRYSTAL/CE_SYNCH	함수 그룹	게시자 스텝
/CRYSTAL/CA_MSG	메시지 클래스	상태 메시지
/CRYSTAL/CE_SYNCH_FORMS	프로그램	프로그램 구성 요소
/CRYSTAL/CONTENT_ADMIN	프로그램	프로그램 구성 요소
/CRYSTAL/CONTENT_ADMIN_CLASS_D	프로그램	프로그램 구성 요소

개체	형식	설명
/CRYSTAL/CONTENT_ADMIN_CLASS_I	프로그램	프로그램 구성 요소
/CRYSTAL/CONTENT_ADMIN_CTREE	프로그램	프로그램 구성 요소
/CRYSTAL/CONTENT_ADMIN_FORMS	프로그램	프로그램 구성 요소
/CRYSTAL/CONTENT_ADMIN_MODULES	프로그램	프로그램 구성 요소
/CRYSTAL/CONTENT_ADMIN_PAIS	프로그램	프로그램 구성 요소
/CRYSTAL/CONTENT_ADMIN_PBOS	프로그램	프로그램 구성 요소
/CRYSTAL/CONTENT_ADMIN_TAB_FRM	프로그램	프로그램 구성 요소
/CRYSTAL/CONTENT_ADMIN_TOP	프로그램	프로그램 구성 요소
/CRYSTAL/PUBLISH_WORKER	프로그램	프로그램 구성 요소
/CRYSTAL/PUBLISH_WORKER_DISP	프로그램	프로그램 구성 요소
/CRYSTAL/PUBLISH_WORKER_DISP_I	프로그램	프로그램 구성 요소
/CRYSTAL/PUBLISH_WORKER_FORMS	프로그램	프로그램 구성 요소

개체	형식	설명
/CRYSTAL/PUBLISH_WORKER_PROC	프로그램	프로그램 구성 요소
/CRYSTAL/PUBLISH_WORKER_PROC_I	프로그램	프로그램 구성 요소
/CRYSTAL/PUBLISH_WORKER_SCREEN	프로그램	프로그램 구성 요소
/CRYSTAL/CA_DEST	테이블	응용 프로그램 상태
/CRYSTAL/CA_JOB	테이블	응용 프로그램 상태
/CRYSTAL/CA_JOB2	테이블	응용 프로그램 상태
/CRYSTAL/CA_LANG	테이블	응용 프로그램 상태
/CRYSTAL/CA_PARM	테이블	응용 프로그램 상태
/CRYSTAL/CA_ROLE	테이블	응용 프로그램 상태
/CRYSTAL/CA_SYST	테이블	응용 프로그램 상태
/CRYSTAL/MENU_TREE_ITEMS	구조	응용 프로그램 상태
/CRYSTAL/REPORT_ID	테이블	응용 프로그램 상태
/CRYSTAL/RPTADMIN	트랜잭션	주 프로그램 트랜잭션
/CRYSTAL/EDIT_REPORT	프로그램	보고서 편집용 래퍼
/CRYSTAL/EDIT_REPORT	함수 그룹	보고서 편집용 함수

개체	형식	설명
ZSSI	인증 개체 클래스	Crystal 인증
ZCNTADMCES	인증 개체	CE 작업
ZCNTADM RPT	인증 개체	보고서 작업
ZCNTADMJOB	인증 개체	백그라운드 작업

19.1.1.17.2.4.6 ODS 연결 전송

이 전송을 사용하여 ODS 쿼리 드라이버는 ODS 데이터에 액세스할 수 있습니다. 이 전송은 BW 3.0B 패치 27 이상 및 BW 3.1C 패치 21 이상과 호환됩니다.

개체	형식	설명
/CRYSTAL/BC	패키지	개발 클래스
/CRYSTAL/ODS_REPORT	함수 그룹	ODS 함수

19.1.1.17.2.4.7 BW 쿼리 매개 변수 사용자 설정 전송

이 전송은 BW 쿼리를 기반으로 하는 보고서에서 사용자 설정된 매개 변수 및 기본 매개 변수 값을 사용할 수 있도록 지원합니다.

개체	형식	설명
/CRYSTAL/BC	패키지	개발 클래스
/CRYSTAL/PERS_VAR	구조	변수 정의
/CRYSTAL/PERS_VALUE	구조	값 정의
/CRYSTAL/PERS	함수 그룹	사용자 설정 함수

19.1.1.17.2.4.8 BW MDX 연결 전송

이 전송을 사용하여 MDX 쿼리 드라이버는 BW 큐브 및 쿼리에 액세스할 수 있습니다. 이 전송은 BW 3.0B 패치 27 이상 및 BW 3.1C 패치 21 이상과 호환됩니다.

개체	형식	설명
/CRYSTAL/BC	패키지	개발 클래스
/CRYSTAL/MDX	함수 그룹	MDX 함수
/CRYSTAL/MDX_STREAM_LAYOUT	테이블 정의	데이터 집합 구조
/CRYSTAL/CX_BAPI_ERROR	클래스	예외

개체	형식	설명
/CRYSTAL/CX_METADATA_ERROR	클래스	예외
/CRYSTAL/CX_MISSING_STREAMINFO	클래스	예외
/CRYSTAL/CX_NO_MORE_CELLS	클래스	예외
/CRYSTAL/CX_NO_MORE_MEMBERS	클래스	예외
/CRYSTAL/CX_NO_MORE_PROPERTIES	클래스	예외
/CRYSTAL/CX_SAVE_SESSION_STATE	클래스	예외
/CRYSTAL/MDX_APPEND_DATA	클래스	데이터 집합 프로세서
/CRYSTAL/MDX_READER_BASE	클래스	데이터 집합 프로세서
/CRYSTAL/MDX_READ_DIMENSIONS	클래스	데이터 집합 프로세서
/CRYSTAL/MDX_READ_MEASURES	클래스	데이터 집합 프로세서
/CRYSTAL/MDX_READ_PROPERTIES	클래스	데이터 집합 프로세서

개체	형식	설명
/CRYSTAL/MDX_AXIS_LEVELS	테이블 형식	메타데이터 구조
/CRYSTAL/MDX_PROPERTY_KEYS	테이블 형식	메타데이터 구조
/CRYSTAL/MDX_PROPERTY_VALUES	테이블 형식	메타데이터 구조
/CRYSTAL/MDX_STREAM_LAYOUT_TAB	테이블 형식	메타데이터 구조

19.1.1.18 인증 개요

이 단원에서는 통합 SAP 환경에서 일반 BI 플랫폼 작업을 수행할 때 사용자 경험과 테스트 환경에 필요한 SAP 인증 목록을 제공합니다. 개별 구현에 따라 추가 인증 개체 또는 필드가 필요할 수도 있습니다.

각 인증 개체에서 인증을 만들고 해당 필드 값을 정의해야 합니다. 그런 후 SAP 사용자의 프로필(또는 역할)에 해당 인증을 적용합니다. 다음 단원에서는 필요한 인증에 대해 설명하고 필수 필드 값을 제공합니다. 사용 중인 SAP 버전에 맞는 절차 세부 정보를 보려면 SAP 설명서를 참조하십시오.

참고:

- 이 부록의 정보는 참조용으로만 제공됩니다.
- ZSEGREPORT 인증 개체는 Open SQL 쿼리 지원에 필요한 SAP용 BusinessObjects XI Integration 전송 파일을 가져올 때 설치되는 ZSSI 개체 클래스에 속합니다.

19.1.1.18.1 권한 만들기 및 적용

각 사용자가 SAP용 Desktop Intelligence Integration을 사용하여 정보에 액세스하는 데 필요한 권한을 만들고 적용해야 합니다. 권한을 만들고 구성하고 적용하는 정확한 절차는 설치한 SAP 버전에 따라 다릅니다. 이 단원에서는 SAP Netweaver ABAP 환경에서 통합된 BI 플랫폼을 사용하여 일반 작업을 수행할 때 사용 환경과 테스트 환경에 따라 필요한 SAP 인증 목록을 제공합니다. 개별 구현에 따라 추가 인증 개체 또는 필드가 필요할 수도 있습니다.

관련 항목

- 675 페이지에서 [컨텐츠 관리 워크벤치에서 게시 구성](#)"

19.1.1.19 BW의 작업

이 단원에서는 BW의 다양한 작업 목록을 소개합니다.

19.1.1.19.1 Crystal Reports에서 수행하는 작업

19.1.1.19.1.1 BW 역할의 쿼리에서 새 보고서 만들기

인증 개체	필드	값
S_USER_AGR	ACT_GROUP	USER_ROLE*
	ACTVT	01, 02, 06
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	RS_PERS_BOD
	ACTVT	16
S_CTS_ADMI	CTS_ADMFCT	TABL
S_RS_COMP	RSINFOAREA	INFO_AREA**
	RSINFOCUBE	INFO_CUBE**
	RSZCOMPTP	REP
	RSZCOMPID	COMP_ID**
S_RS_COMP1	RSZCOMPID	COMP_ID**
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER*
	ACTVT	16

* USER_ROLE은 사용자가 속하는 역할의 이름을 나타냅니다. 이 필드에 여러 값을 입력할 수 있습니다.

** QUERY_OWNER는 쿼리의 소유자 이름을 나타냅니다. 이름을 지정할 경우 해당 소유자의 쿼리에 대해서만 보고할 수 있습니다. 임의 소유자의 쿼리에 대해 보고하려면 *를 입력합니다.

** INFO_AREA, INFO_CUBE 또는 COMP_ID의 경우 *를 입력하여 임의 값을 나타냅니다. 특정 값을 지정할 경우 이러한 정보 영역, 큐브 및 구성 요소 ID가 들어 있는 쿼리에 대해서만 보고할 수 있습니다.

19.1.1.19.1.2 BW 역할의 기존 보고서 열기

인증 개체	필드	값
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SUSO, SUNI, RSCR, SH3A, RFC1, RZX0, RZX2, RS_PERS_BOD, /CRYSTAL/PERS, RSOB
	ACTVT	16
S_RS_COMP	RSINFOAREA	INFO_AREA**
	RSINFOCUBE	INFO_CUBE**
	RSZCOMPTP	REP
	RSZCOMPID	COMP_ID**
S_RS_COMP1	RSZCOMPID	COMP_ID**
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER*
	ACTVT	16

** QUERY_OWNER는 보고서를 만들고 있는 쿼리의 소유자 이름을 나타냅니다. 쿼리 소유자의 이름을 입력할 경우 이 소유자의 쿼리에 대해서만 보고할 수 있습니다. 임의의 쿼리 소유자를 나타내려면 *를 입력합니다.

** INFO_AREA, INFO_CUBE 또는 COMP_ID의 경우 *를 입력하여 임의 값을 나타냅니다. 특정 값을 지정할 경우 이러한 정보 영역, 큐브 및 구성 요소 ID가 들어 있는 쿼리에 대해서만 보고할 수 있습니다.

19.1.1.19.1.3 보고서 미리 보기 또는 새로 고침

인증 개체	필드	값
S_RS_COMP	RSINFOAREA	INFO_AREA**
	RSINFOCUBE	INFO_CUBE**
	RSZCOMPTP	REP
	RSZCOMPID	COMP_ID**
S_RS_COMP1	RSZCOMPID	COMP_ID**
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER*
	ACTVT	16

** QUERY_OWNER는 보고서를 만들고 있는 쿼리의 소유자 이름을 나타냅니다. 쿼리 소유자의 이름을 입력할 경우 이 소유자의 쿼리에 대해서만 보고할 수 있습니다. 임의의 쿼리 소유자를 나타내려면 *를 입력합니다.

** INFO_AREA, INFO_CUBE 또는 COMP_ID의 경우 *를 입력하여 임의 값을 나타냅니다. 특정 값을 지정할 경우 이러한 정보 영역, 큐브 및 구성 요소 ID가 들어 있는 쿼리에 대해서만 보고할 수 있습니다.

19.1.1.19.1.4 데이터베이스 확인(보고서의 테이블 정의 새로 고침)

인증 개체	필드	값
S_RS_COMP	RSINFOAREA	INFO_AREA**
	RSINFOCUBE	INFO_CUBE**
	RSZCOMPTP	REP
	RSZCOMPID	COMP_ID**
S_RS_COMP1	RSZCOMPID	COMP_ID**
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER*
	ACTVT	16

** QUERY_OWNER는 보고서를 만들고 있는 쿼리의 소유자 이름을 나타냅니다. 쿼리 소유자의 이름을 입력할 경우 이 소유자의 쿼리에 대해서만 보고할 수 있습니다. 임의의 쿼리 소유자를 나타내려면 *를 입력합니다.

** INFO_AREA, INFO_CUBE 또는 COMP_ID의 경우 *를 입력하여 임의 값을 나타냅니다. 특정 값을 지정할 경우 이러한 정보 영역, 큐브 및 구성 요소 ID가 들어 있는 쿼리에 대해서만 보고할 수 있습니다.

19.1.1.19.1.5 데이터 소스의 위치 설정

인증 개체	필드	값
S_RS_COMP	RSINFOAREA	INFO_AREA**
	RSINFOCUBE	INFO_CUBE**
	RSZCOMPTTP	REP
	RSZCOMPID	COMP_ID**
S_RS_COMP1	RSZCOMPID	COMP_ID**
	RSZCOMPTTP	REP
	RSZOWNER	QUERY_OWNER*
	ACTVT	16

** QUERY_OWNER는 보고서를 만들고 있는 쿼리의 소유자 이름을 나타냅니다. 쿼리 소유자의 이름을 입력할 경우 이 소유자의 쿼리에 대해서만 보고할 수 있습니다. 임의의 쿼리 소유자를 나타내려면 *를 입력합니다.

** INFO_AREA, INFO_CUBE 또는 COMP_ID의 경우 *를 입력하여 임의 값을 나타냅니다. 특정 값을 지정할 경우 이러한 정보 영역, 큐브 및 구성 요소 ID가 들어 있는 쿼리에 대해서만 보고할 수 있습니다.

19.1.1.19.1.6 보고서를 BW 역할에 저장

인증 개체	필드	값
S_USER_AGR	ACT_GROUP	USER_ROLE *
	ACTVT	01, 02, 06
S_CTS_ADMI	CTS_ADMFCT	TABL

* USER_ROLE은 사용자가 속하는 역할의 이름을 나타냅니다. 이 필드에 여러 값을 입력할 수 있습니다.

19.1.1.19.1.7 보고서를 BW에 저장하는 동안 번역 준비

인증 개체	필드	값
S_USER_AGR	ACT_GROUP	USER_ROLE *
	ACTVT	01
S_CTS_ADMI	CTS_ADMFCT	TABL

* USER_ROLE은 사용자가 속하는 역할의 이름을 나타냅니다. 이 필드에 여러 값을 입력할 수 있습니다.

19.1.1.19.1.8 보고서를 저장하는 동시에 BI 플랫폼에 게시

인증 개체	필드	값
S_USER_AGR	ACT_GROUP	USER_ROLE *
	ACTVT	01
S_CTS_ADMI	CTS_ADMFCT	TABL
S_RS_COMP	RSINFOAREA	INFO_AREA ***
	RSINFOCUBE	INFO_CUBE ***
	RSZCOMPTP	REP
	RSZCOMPID	COMP_ID ***
S_RS_COMP1	RSZCOMPID	COMP_ID ***
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER **
	ACTVT	16

* USER_ROLE은 사용자가 속하는 역할의 이름을 나타냅니다. 이 필드에 여러 값을 입력할 수 있습니다.

** QUERY_OWNER는 보고서를 만들고 있는 쿼리의 소유자 이름을 나타냅니다. 쿼리 소유자의 이름을 입력할 경우 이 소유자의 쿼리에 대해서만 보고할 수 있습니다. 임의의 쿼리 소유자를 나타내려면 *를 입력합니다.

*** INFO_AREA, INFO_CUBE 또는 COMP_ID의 경우 *를 입력하여 임의 값을 나타냅니다. 특정 값을 지정할 경우 이러한 정보 영역, 큐브 및 구성 요소 ID가 들어 있는 쿼리에 대해서만 보고할 수 있습니다.

19.1.1.19.1.9 BEx Query Designer 시작

인증 개체	필드	값
S_RS_COMP	RSINFOAREA	INFO_AREA**
	RSINFOCUBE	INFO_CUBE**
	RSZCOMPTP	REP
	RSZCOMPID	COMP_ID**
S_RS_COMP1	RSZCOMPID	COMP_ID**
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER*
	ACTVT	16
S_CTS_ADMI	CST_ADMFCT	TABL

** QUERY_OWNER는 보고서를 만들고 있는 쿼리의 소유자 이름을 나타냅니다. 쿼리 소유자의 이름을 입력할 경우 이 소유자의 쿼리에 대해서만 보고할 수 있습니다. 임의의 쿼리 소유자를 나타내려면 *를 입력합니다.

** INFO_AREA, INFO_CUBE 또는 COMP_ID의 경우 *를 입력하여 임의 값을 나타냅니다. 특정 값을 지정할 경우 이러한 정보 영역, 큐브 및 구성 요소 ID가 들어 있는 쿼리에 대해서만 보고할 수 있습니다.

19.1.1.19.2 BI 실행 패드에서 수행하는 작업

19.1.1.19.2.1 SAP 자격 증명을 사용하여 BI 플랫폼에 로그인

인증 개체	필드	값
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM

19.1.1.19.2.2 요청 시 SAP BW 보고서 보기

인증 개체	필드	값
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB, SUNI
	ACTVT	16
S_RS_COMP	RSINFOAREA	INFO_AREA**
	RSINFOCUBE	INFO_CUBE**
	RSZCOMPTP	REP
	RSZCOMPID	COMP_ID**

인증 개체	필드	값
S_RS_COMP1	RSZCOMPID	COMP_ID**
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER*
	ACTVT	16
S_RS_ODSO	RSINFOAREA	INFO_AREA**
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

** QUERY_OWNER는 보고서를 만들고 있는 쿼리의 소유자 이름을 나타냅니다. 쿼리 소유자의 이름을 입력할 경우 이 소유자의 쿼리에 대해서만 보고할 수 있습니다. 임의의 쿼리 소유자를 나타내려면 *를 입력합니다.

** INFO_AREA, INFO_CUBE 또는 COMP_ID의 경우 *를 입력하여 임의 값을 나타냅니다. 특정 값을 지정할 경우 이러한 정보 영역, 큐브 및 구성 요소 ID가 들어 있는 쿼리에 대해서만 보고할 수 있습니다.

19.1.1.19.2.3 뷰어에서 보고서 새로 고침

인증 개체	필드	값
S_RS_COMP	RSINFOAREA	INFO_AREA**
	RSINFOCUBE	INFO_CUBE**
	RSZCOMPTP	REP
	RSZCOMPID	COMP_ID**
S_RS_COMP1	RSZCOMPID	COMP_ID**
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER*
	ACTVT	16
S_RS_ODSO	RSINFOAREA	INFO_AREA**
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

** QUERY_OWNER는 보고서를 만들고 있는 쿼리의 소유자 이름을 나타냅니다. 쿼리 소유자의 이름을 입력할 경우 이 소유자의 쿼리에 대해서만 보고할 수 있습니다. 임의의 쿼리 소유자를 나타내려면 *를 입력합니다.

** INFO_AREA, INFO_CUBE 또는 COMP_ID의 경우 *를 입력하여 임의 값을 나타냅니다. 특정 값을 지정할 경우 이러한 정보 영역, 큐브 및 구성 요소 ID가 들어 있는 쿼리에 대해서만 보고할 수 있습니다.

19.1.1.19.2.4 보고서 일정 설정

인증 개체	필드	값
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB, SUNI
	ACTVT	16
S_RS_COMP	RSINFOAREA	INFO_AREA**
	RSINFOCUBE	INFO_CUBE**
	RSZCOMPTP	REP
	RSZCOMPID	COMP_ID**
S_RS_COMP1	RSZCOMPID	COMP_ID**
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER*
	ACTVT	16
S_RS_ODSO	RSINFOAREA	INFO_AREA**
	RSODSOBJ	OCRM_OLVM
	RSODSPART	DATA
	ACTVT	03

** QUERY_OWNER는 보고서를 만들고 있는 쿼리의 소유자 이름을 나타냅니다. 쿼리 소유자의 이름을 입력할 경우 이 소유자의 쿼리에 대해서만 보고할 수 있습니다. 임의의 쿼리 소유자를 나타내려면 *를 입력합니다.

** INFO_AREA, INFO_CUBE 또는 COMP_ID의 경우 *를 입력하여 임의 값을 나타냅니다. 특정 값을 지정할 경우 이러한 정보 영역, 큐브 및 구성 요소 ID가 들어 있는 쿼리에 대해서만 보고할 수 있습니다.

19.1.1.19.2.5 보고서 매개 변수의 동적 선택 목록 읽기

인증 개체	필드	값
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB
	ACTVT	16

19.1.1.19.3 SAP NetWeaver(ABAP)에서 수행하는 작업

19.1.1.19.3.1 Crystal Reports에서 Open SQL 드라이버를 사용하여 수행하는 작업

이 단원에서는 Crystal Reports에서 Open SQL 드라이버를 사용하여 수행하는 SAP Netweaver(ABAP)의 다양한 작업 목록을 소개합니다.

19.1.1.19.3.2 SAP 서버에 로그인

인증 개체	필드	값
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQ
	ACTVT	16

19.1.1.19.3.3 새 보고서 만들기

인증 개체	필드	값
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQ
	ACTVT	16
ZSEGREPORT	ACTVT	01

19.1.1.19.3.4 기존 보고서 열기 또는 미리 보기

인증 개체	필드	값
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQ
	ACTVT	16
ZSEGREPORT	ACTVT	02

19.1.1.19.3.5 데이터베이스 확인(보고서의 테이블 정의 새로 고침)

인증 개체	필드	값
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM
ZSEGREPORT	ACTVT	02

인증 개체	필드	값
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQ
	ACTVT	16

19.1.1.19.3.6 데이터 소스의 위치 설정

인증 개체	필드	값
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQ
	ACTVT	16

19.1.1.19.4 Crystal Reports에서 InfoSet 드라이버 및 InfoSet 보고 기능을 통해 수행하는 작업

19.1.1.19.4.1 SAP 서버에 로그인

인증 개체	필드	값
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

19.1.1.19.4.2 SAP Netweaver(ABAP)의 InfoSet에서 새 보고서 만들기

인증 개체	필드	값
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/FLAT, SKBW, AQRC
	ACTVT	16
S_CTS_ADMI	CTS_ADMFCT	TABL

참고:

또한 데이터 행을 보기 위한 충분한 권한을 추가합니다. P_ORIG 또는 P_APAP를 예로 들 수 있습니다.

관련 항목

- 721 페이지에서 [데이터 소스의 위치 설정](#)

19.1.1.19.4.3 데이터베이스 확인(보고서의 테이블 정의 새로 고침)

인증 개체	필드	값
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM

19.1.1.19.4.4 데이터 소스의 위치 설정

인증 개체	필드	값
P_ABAP	REPID	AQTGSYSTGENERATESY, SAPDBPNP
	COARS	2

19.1.1.19.5 Crystal Reports에서 InfoSet 드라이버 및 ABAP 쿼리 보고 기능을 통해 수행하는 작업

19.1.1.19.5.1 SAP 서버에 로그인

인증 개체	필드	값
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

19.1.1.19.5.2 SAP Netweaver의 ABAP 쿼리에서 새 보고서 만들기

인증 개체	필드	값
P_ABAP	REPID	AQTG02=====P6, SAPDBPNP
	COARS	2
S_ADML_FCD	S_ADML_FCD	STOR, STOM
S_TABU_DIS	ACTVT	03
	GROUP	테이블 그룹의 이름

19.1.1.19.5.3 데이터베이스 확인

인증 개체	필드	값
S_ADML_FCD	S_ADML_FCD	STOR, STOM
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16

19.1.1.19.5.4 데이터 소스의 위치 설정

인증 개체	필드	값
P_ABAP	REPID	AQTG02=====P6, SAPDBPNP
	COARS	2
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16
S_TABU_DIS	ACTVT	03
	GROUP	테이블 그룹의 이름

19.1.1.19.6 BI 플랫폼 작업

19.1.1.19.6.1 대화 모드에서 Open SQL 쿼리를 사용하여 보고서 일정 설정

인증 개체	필드	값
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPENSQ
	ACTVT	16
ZSEGREPORT	ACTVT	02

참고:
CLASS 값은 비어 있습니다.

19.1.1.19.6.2 배치 모드에서 Open SQL 쿼리를 사용하여 보고서 일정 설정

인증 개체	필드	값
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPENSQ, SH3A
	ACTVT	16
S_BTCH_JOB	JOBGROUP	' '
	JOBACTION	RELE
ZSEGREPORT	ACTVT	02
S_BTCH_ADM	BTCADMIN	Y

참고:
CLASS 값은 비어 있습니다.

19.1.1.19.6.3 Crystal 권한 부여 시스템

인증 개체	필드	값
파일 액세스를 위한 인증 (S_DATASET)	작업(ACTVT)	읽기, 쓰기(33, 34)
	실제 파일 이름(FILENAME)	*(모두를 의미함)
	ABAP 프로그램 이름(PRO-GRAM)	*
RFC 액세스를 위한 인증 확인 (S_RFC)	작업(ACTVT)	16
	보호할 RFC의 이름 (RFC_NAME)	BDCH, STPA, SUSO, SUUS, SU_USER, SYST, SUNI, PRGN_J2EE, /CRYSTAL/SE- CURITY
	보호할 RFC 개체의 유형 (RFC_TYPE)	함수 그룹(FUGR)
사용자 마스터 유지 관리: 사용 자 그룹(S_USER_GRP)	작업(ACTVT)	만들기 또는 생성 및 표시(03)
	사용자 마스터 유지 관리의 사 용자 그룹(CLASS)	<p>*</p> <p>참고: 보안을 강화하기 위해 BI 플랫 폼에 액세스해야 할 구성원이 포함된 사용자 그룹을 명시적으 로 지정할 수도 있습니다.</p>

19.2 JD Edwards 통합 구성

19.2.1 SAP Crystal Reports에 대해 단일 로그인(SSO) 구성

기본적으로 BI 플랫폼은 SAP Crystal Reports 사용자가 단일 로그인(SSO)을 사용하여 JD Edwards EnterpriseOne 데이터에 액세스할 수 있도록 구성됩니다.

19.2.1.1 JD Edwards 및 SAP Crystal Reports에 대해 SSO 비활성화

1. 중앙 관리 콘솔(CMC)에서 응용 프로그램을 클릭합니다.
2. Crystal Reports 구성을 두 번 클릭합니다.
3. 단일 로그인 옵션을 클릭합니다.
4. crdb_pseone을 선택합니다.
5. 제거를 클릭합니다.
6. 저장 후 닫기를 클릭합니다.
7. SAP Crystal Reports를 다시 시작합니다.

19.2.1.2 JD Edwards 및 SAP Crystal Reports에 대해 SSO 활성화

JD Edwards 및 SAP Crystal Reports에 대해 SSO를 비활성화했는데 다시 활성화하려는 경우 다음을 수행하십시오.

1. 중앙 관리 콘솔(CMC)에서 응용 프로그램을 클릭합니다.
2. Crystal Reports 구성을 두 번 클릭합니다.
3. 단일 로그인 옵션을 클릭합니다.
4. 데이터베이스 로그인에 SSO 컨텍스트 사용 아래에 crdb_pseone을 입력합니다.
5. 추가를 클릭합니다.
6. 저장 후 닫기를 클릭합니다.
7. Crystal Reports 서버를 다시 시작합니다.

19.2.2 JD Edwards 통합을 위한 Secure Sockets Layer 구성

BI 플랫폼 및 JD Edwards EnterpriseOne 배포 환경에서는 클라이언트와 서버 간의 모든 네트워크 통신에 SSL(Secure Sockets Layer) 프로토콜을 사용할 수 있습니다.

BI 플랫폼에서 JD Edwards EnterpriseOne 데이터를 사용하려면 SSL 구성 일부를 변경해야 합니다. 다른 BI 플랫폼 서버 및 클라이언트에 대한 SSL 구성과 마찬가지로, BI 플랫폼 배포 환경에서 컴퓨터로 액세스할 수 있는 (동일한 디렉터리 아래의) 안전한 위치에 다음 키 파일과 인증서 파일을 저장합니다.

- 신뢰할 수 있는 인증서 파일(cacert.der)
- 생성된 서버 인증서 파일(servercert.der)
- 서버 키 파일(server.key)
- 암호 파일(passphrase.txt)

19.2.2.1 SSL과 JD Edwards EnterpriseOne 데이터 연결 사용

참고:

다음 절차에 설명된 모든 값은 대/소문자를 구분합니다.

- 다음 레지스트리 키 아래에 두 개의 레지스트리 값을 구성합니다.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Business
Objects\Suite 12.0\Integration Kit for
PeopleSoft EnterpriseOne\QRYWInstances\Wnoname]
"CommunicationProtocol"="ssl"
"SSL Configuration File"="C:\Program
Files\Business Objects\BusinessObjects XI 13.0\Wsslconf.properties"
```

이 변경 내용을 적용하려면 BI 플랫폼 보고 서비스(예: Crystal Reports 작업 서버)를 다시 시작해야 합니다.

19.2.2.2 SSL 구성 속성 파일

sslconf.properties 속성 파일에는 BI 플랫폼에서 사용하는 필수 인증서 및 키에 대한 모든 정보가 포함되어 있습니다. 예를 들면 다음과 같습니다.

```
[default]
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

sslconf.properties 파일은 BI 플랫폼 설치 폴더에 있어야 합니다. 기본적으로 설치 폴더는 C:\WProgram Files\Business Objects\BusinessObjects 13.0입니다.

19.3 PeopleSoft Enterprise 통합 구성

19.3.1 SAP Crystal Reports 및 PeopleSoft Enterprise에 대한 단일 로그인 (SSO) 구성

기본적으로, BI 플랫폼은 SAP Crystal Reports 사용자가 단일 로그인(SSO)을 사용하여 PeopleSoft Enterprise 데이터에 액세스할 수 있도록 구성됩니다.

19.3.1.1 PeopleSoft Enterprise 및 SAP Crystal Reports에 대한 SSO 비활성화

1. 중앙 관리 콘솔(CMC)에서 응용 프로그램을 클릭합니다.
2. Crystal Reports 구성을 두 번 클릭합니다.
3. 단일 로그인 옵션을 클릭합니다.
4. crdb_psenterprise를 선택합니다.
5. 제거를 클릭합니다.

6. 저장 후 단기를 클릭합니다.
7. SAP Crystal Reports를 다시 시작합니다.

19.3.1.2 PeopleSoft Enterprise 및 SAP Crystal Reports에 대한 SSO 활성화

PeopleSoft Enterprise 및 SAP Crystal Reports용 SSO를 비활성화했는데 이를 다시 활성화하려는 경우.

1. 중앙 관리 콘솔(CMC)에서 응용 프로그램을 클릭합니다.
2. Crystal Reports 구성을 두 번 클릭합니다.
3. 단일 로그인 옵션을 클릭합니다.
4. 데이터베이스 로그인에 SSO 컨텍스트 사용...에서 crdb_psenterprise를 입력합니다.
5. 추가를 클릭합니다.
6. 저장 후 단기를 클릭합니다.
7. SAP Crystal Reports를 다시 시작합니다.

19.3.2 Secure Sockets Layer 통신 구성

BI 플랫폼 배포 환경에서 클라이언트와 서버 사이의 모든 네트워크 통신에 SSL(Secure Sockets Layer) 프로토콜을 사용할 수 있습니다.

다른 BI 플랫폼 서버 및 클라이언트에 대한 SSL 구성과 마찬가지로, BI 플랫폼 배포 환경에서 컴퓨터로 액세스할 수 있는 (동일한 디렉터리 아래의) 안전한 위치에 다음 키 파일과 인증서 파일을 저장합니다.

- 신뢰할 수 있는 인증서 파일(cacert.der)
- 생성된 서버 인증서 파일(servercert.der)
- 서버 키 파일(server.key)
- 암호 파일(passphrase.txt)

19.3.2.1 SSL 구성 속성 파일

sslconf.properties 속성 파일에는 SAP BI 플랫폼 구성 요소에서 사용하는 필수 인증서 및 키에 대한 모든 정보가 포함되어 있습니다. 예를 들면 다음과 같습니다.

```
[default]
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

sslconf.properties 파일은 BI 플랫폼 제품 설치 폴더에 있어야 합니다. 기본적으로 설치 폴더는 C:\WProgram Files\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\입니다.

19.3.2.2 SSL에서 PeopleSoft Query Server 사용

참고:

다음 절차에서 설명하는 모든 값은 대/소문자를 구분합니다.

- 예를 들어, 모든 쿼리 서버에 대한 레지스트리 키에서 두 개의 레지스트리 값을 구성합니다.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Business
Objects\Suite 12.0\Integration Kit for
PeopleSoft\QRY\Instances\Wnoname]
"CommunicationProtocol"="ssl"
"SSL Configuration File"="C:\WProgram
Files\Business Objects\BusinessObjects 12.0 Integration Kit for
PeopleSoft\sslconf.properties"
```

이런 변경 내용을 적용하려면 BusinessObjects 보고 서버(예: Crystal Reports Job Server)를 다시 시작해야 합니다.

19.3.2.3 SSL에서 보안 브리지 사용

참고:

다음 절차에서 설명하는 모든 값은 대/소문자를 구분합니다.

- .bat 파일에 다음 인수를 추가하여 crpsepmsecuritybridge.bat을 실행합니다.

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir="d:\Wssl"
-DtrustedCert=cacert.der
-DsslCert=servercert.der
```

```
-DsslKey=server.key
-Dpassphrase=passphrase.txt
```

java.exe 바로 뒤 그리고 -jar 인수를 추가하기 전에 .bat 파일의 올바른 위치에 인수가 추가되는 지 확인하십시오. 예를 들면 다음과 같습니다.

```
@ECHO OFF
SETLOCAL
SET PATH=%PATH%;C:\Program Files\Business
Objects\BusinessObjects Enterprise 12.0\win32_x86\;C:\Program
Files\Business Objects\BusinessObjects 12.0 Integration Kit for
PeopleSoft\Wwepm;
"C:\Program Files\Business Objects\Wjvasdk\bin\java.exe" -Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir="C:\test" -DtrustedCert=cacert.der
-DsslCert=servercert.der -DsslKey=server.key
-Dpassphrase=passphrase.txt -jar "C:\Program Files\Business
Objects\BusinessObjects 12.0 Integration Kit for
PeopleSoft\Wwepm\Wcrpsepmsecuritybridge.jar" %1 "language"
"C:\Program Files\Business
Objects\WwLanguagePacks.xml\WLanguagePacks.xml"
```

다음 표에는 이러한 예에 해당하는 설명이 나열되어 있습니다.

DcertDir=d:\Wssl	모든 인증서와 키를 저장할 디렉터리입니다.
DtrustedCert=cacert.der	신뢰할 수 있는 인증서 파일입니다. 두 개 이상 지정할 경우 세미콜론으로 구분합니다.
DsslCert=clientcert.der	SDK에서 사용하는 인증서입니다.
DsslKey=client.key	SDK 인증서의 개인 키입니다.
Dpassphrase=passphrase.txt	개인 키의 암호를 저장하는 파일입니다.

19.3.3 PeopleSoft 시스템용 성능 조정

PeopleSoft 쿼리에 대한 보고서를 만들 때 최적의 성능을 보장하려면 Crystal Reports 및 BI 플랫폼에서 쿼리가 실행되는 방법을 이해하는 것이 중요합니다.

PeopleSoft 쿼리를 기반으로 하는 보고서를 새로 고치거나 실행할 때마다 PeopleSoft 서버로 연결됩니다.

- PeopleSoft Enterprise(PeopleTools 8.46 이상) 환경에서는 PeopleSoft Analytic Server로 연결됩니다.

- PeopleSoft Enterprise(PeopleTools 8.21-8.45) 환경에서는 PeopleSoft Application Server로 연결됩니다.

19.3.3.1 권장 사항

최적의 배포에서는 보고서 요청 처리만 담당하는 하나 이상의 PeopleSoft Analytic 또는 Application Server가 설치됩니다. 이들 각 서버에서 최소 및 최대 인스턴스에 대한 설정은 한 번에 처리할 수 있는 보고서 요청 수를 제어합니다. 이 설정의 장점은 다음과 같습니다.

- PeopleSoft 서버에서 보고서 요청과 다른 트랜잭션 요청 사이에 충돌이 없습니다.
- 트랜잭션 요청을 처리하는 서버를 사용 안하는 것으로 설정할 필요 없이 보고서 요청을 처리하는 서버에서 유지 관리 작업을 수행할 수 있습니다.

동일한 PeopleSoft Analytic 또는 Application Server에서 보고서 및 트랜잭션 요청을 모두 처리하는 환경에서는 한 번에 둘 이상의 보고서를 실행하지 않도록 BI 플랫폼을 구성해야 합니다. 그렇지 않으면 모든 PSANALYTICSRV 또는 PSAPPSRV 프로세스가 보고서 실행에 사용되는 경우 사용자는 어떤 트랜잭션 요청도 할 수 없게 됩니다.

참고:

- 예약된 보고서 작업 및 요청 시 보고서 보기 수를 제한하는 자세한 방법은 BusinessObjects Business Intelligence 플랫폼 관리자 가이드에서 "서버 관리 및 구성"을 참조하십시오.
- 동시에 서버에 액세스를 시도할 수 있는 Crystal Reports 사용자의 수를 제한하도록 시스템을 구성할 수 없습니다.

성능 문제가 발생하는 경우 Psadmin 구성 도구를 사용하여 요청이 대기열에 있는지 여부를 확인합니다. 또한, PeopleSoft Analytic 또는 Application Server 컴퓨터의 시스템 리소스를 모니터링합니다. 실제 메모리 부족 때문에 가상 메모리가 사용되고 있는 경우에는 처리 속도가 느려질 수도 있습니다.

19.3.3.2 PeopleSoft 서버

PeopleSoft Analytic Server에서 보고서를 새로 고치거나 실행하는 프로세스는 PSANALYTICSRV 프로세스입니다. PeopleSoft Application Server에서 보고서를 새로 고치거나 실행하는 프로세스는 PSAPPSRV 프로세스입니다. 사용 가능한 PSANALYTICSRV 또는 PSAPPSRV 프로세스의 수에 따라 동시에 실행할 수 있는 보고서 수가 결정됩니다.

일반적인 PeopleSoft Analytic 또는 Application Server 구성 파일에는 다음 정보가 포함됩니다.

```
Min Instances=3
Max Instances=5
```

이 예에서는 최대 5개의 프로세스까지 늘릴 수 있는 기능으로 언제든지 최소 3개의 PSANALYTICSRV 또는 PSAPPSRV 프로세스를 사용할 수 있습니다. 이렇게 설정한다고 해서 항상 5개의 보고서를 동시에 실행할 수 있다는 의미는 아니며, 이들 프로세스를 사용하여 시스템의 다른 작업을 처리할 수도 있습니다. 요청을 처리하기 위해 사용 가능한 PSANALYTICSRV 또는 PSAPPSRV 프로세스가 없는 경우에는 프로세스를 사용할 수 있을 때까지 요청이 대기열 처리됩니다.

참고:

일반적으로 PeopleSoft Application Server용 구성 파일에는 사용 가능한 프로세스에 대해 대기열 처리된 요청의 대기 시간을 지정하는 Service Timeout 매개 변수도 포함됩니다. 매개 변수에 대해 지정되는 시간 내에 어떤 프로세스도 사용할 수 없게 되는 경우에는 요청 시간이 초과됩니다.

19.4 Siebel 통합 구성

19.4.1 SAP BusinessObjects Business Intelligence 플랫폼과 통합하도록 Siebel 구성

BI 플랫폼 통합은 Crystal Reports에 대한 링크를 제공하여 BusinessObjects Business Intelligence Suite 콘텐츠를 Siebel 응용 프로그램에 포함할 수 있습니다. 새 메뉴 항목을 설치하고 구성한 후, 사용자는 이 메뉴 항목을 이용해 Siebel 응용 프로그램 내에서 InfoView를 시작할 수 있습니다.

기본적으로, C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\Siebel\Siebel Files\ 폴더에 필수 파일이 설치됩니다.

참고:

하위 폴더인 Siebel 7.7과 Siebel 8.0에는 Siebel 버전 7.7 및 8.0에서 사용하기 위한 다른 파일이 들어 있습니다.

19.4.1.1 BI 플랫폼 Siebel 통합 프로젝트 가져오기

1. Siebel 도구를 시작합니다.
2. 도구 > 아카이브에서 가져오기를 클릭합니다.
3. 보관 파일에 대한 메시지가 표시되면 통합 제품 설치의 Siebel Files 폴더를 찾아봅니다.
기본적으로, <install directory>WSAP BusinessObjects Enterprise XI 4.0WSamplesWsiebelWSiebel FilesW 폴더입니다.
4. 해당 하위 폴더(Siebel 7.7 또는 Siebel 8.0)로 이동하여 BusinessObjectsEnterprise.sif 파일을 선택합니다.
가져오기 마법사가 나타납니다.
5. 리포지토리에 정의를 포함한 보관 파일의 개체 정의 병합을 클릭합니다.
6. 마법사 화면을 계속 진행하여 통합 프로젝트 가져오기를 마칩니다.
통합 프로젝트가 리포지토리에 추가됩니다.
7. SAP Businessobjects Integration 프로젝트를 잠급니다.

19.4.2 Crystal Reports 메뉴 항목 만들기

1. Siebel Tools에서 메뉴 프로젝트를 잠급니다.
2. 개체 탐색기에서 메뉴 항목 개체를 선택합니다.
참고:
개체 탐색기에 메뉴 개체가 나타나지 않는 경우, Siebel Tools에서 보기 > 옵션을 클릭한 다음 개체 탐색기 탭을 클릭하고 메뉴 개체를 선택합니다.
3. 메뉴 목록에서 일반 웹 메뉴를 선택합니다.
4. 메뉴 항목 목록 머리글을 클릭합니다.
5. 편집 > 새 레코드를 클릭합니다.
6. 새 메뉴 항목을 적절히 정의합니다. 다음은 권장 값입니다.
 - 이름: 뷰 - Crystal Reports
 - 캡션: Crystal Reports
 - 명령: Crystal Reports
 - 설명: SAP BusinessObjects 통합 보고서 메뉴
 - 비활성: False
7. 위치 번호를 사용하여 보기 메뉴에서 메뉴 항목의 위치를 선택합니다.
위치 번호를 보다 쉽게 선택하려면 메뉴 항목을 위치별로 정렬합니다.
8. 이제 로컬 레코드를 추가하여 캡션을 적절히 지역화할 수 있습니다.

이제 Siebel 응용 프로그램을 다시 컴파일합니다. 737 페이지에서 ["Siebel 응용 프로그램 다시 컴파일"](#)을 참조하십시오.

19.4.2.1 Siebel 응용 프로그램 다시 컴파일

BI 플랫폼을 설치하고 Siebel 메뉴 항목을 통해 사용자가 이 프로그램의 명령을 사용할 수 있도록 한 경우, 일반적인 절차를 수행한 후 Siebel 응용 프로그램을 다시 컴파일해야 합니다. 자세한 내용은 Siebel Bookshelf를 참조하십시오.

Siebel 응용 프로그램을 다시 컴파일했다면 JavaScript 파일을 다시 생성하십시오. Siebel 7.7 이상에서는 재컴파일 프로세스의 일부로 JavaScript 파일을 자동으로 다시 생성할 수 있습니다.

Siebel 리포지토리 컴파일에 필요한 단계는 Siebel Tools 워크스테이션에서 수행되므로 생성된 JavaScript를 Siebel Tools 워크스테이션에서 Siebel Server로 배포해야 합니다. 일반적으로 Siebel이 설치된 위치에 따라 생성된 JavaScript 파일을 다음 위치에서 찾을 수 있습니다.

C:\Wsea77\tools\WPUBLIC\WENUWsrf1096416329_444

예제 폴더 이름 srf1096416329_444는 Siebel Tools에서 생성한 이름으로, 결과 리포지토리 파일에 고유하게 적용됩니다.

JavaScript 파일은 Siebel이 설치된 위치에 따라 Siebel Server의 다음 위치에 배포되어야 합니다.

C:\Wsea77\WSWEApp\WPUBLIC\WENUWsrf1096416329_444

폴더 이름은 Siebel Tools에서 생성한 대로 유지하십시오.

또한 서비스를 허용하도록 Siebel Server 컴퓨터에서 Siebel 구성 파일을 업데이트해야 합니다. Siebel Server 컴퓨터에서 해당 구성 파일을 찾으십시오. 예를 들어 Siebel Call Center의 영어 버전을 실행 중인 경우, uagent.cfg를 사용하십시오. Siebel 7.7의 경우 기본적으로 이 파일은 C:\Wsea77\wsiebsrvr\Wbin\WENUWuagent.cfg에 있습니다.

그런 다음 구성 파일의 SWE 섹션 끝에 다음 줄을 추가하십시오.

ClientBusinessServiceNUMBER = BusinessObjects Integration Service

ClientBusinessService 번호는 순차적입니다. SWE 섹션에 다른 ClientBusinessServices가 없는 경우 NUMBER를 0으로 설정하십시오. 그렇지 않은 경우 NUMBER를 다음으로 높은 값으로 설정하십시오.

Siebel 8.x 이상의 경우:

1. Siebel Tools에 로그인한 다음 개체 탐색기에서 Siebel Universal Agent 응용 프로그램 개체를 찾습니다.
2. 응용 프로그램 개체를 확장하여 Application User Prop 개체를 표시합니다.
3. 선언할 각 비즈니스마다 새 레코드를 만듭니다. 이때 각각에 대한 이름 및 값 속성은 다음과 같이 설정합니다.
 - 이름 = ClientBusinessServiceX

- 값 = BusinessObjects Integration

이제 가져온 Siebel 명령을 호출하는 Crystal Reports 메뉴 항목을 만들 수 있습니다.

19.4.3 Contextual Awareness

Contextual Awareness는 현재 작업과 관련된 보고서를 사용자에게 표시하는 기능입니다. 이 경우 Siebel Client 응용 프로그램에서 직접 Crystal Reports에 액세스하는 사용자에게 Siebel 데이터를 통합하도록 설계된 보고서가 자동으로 표시됩니다.

19.4.3.1 Contextual Awareness 구성

컨텍스트 민감성에 대해 구성하기 전에 다음을 완료했는지 확인합니다.

- Siebel 통합 제품 설치
 - BI 플랫폼과 통합할 수 있도록 Siebel 구성
1. BI 플랫폼의 중앙 관리 콘솔(CMC)을 엽니다.
 2. 인증을 클릭합니다.
 3. Siebel을 두 번 클릭합니다.
Siebel 매핑 인터페이스가 나타납니다.
 4. 도메인을 클릭합니다.
도메인 매핑 인터페이스가 나타납니다.
 5. 사용할 Siebel 서버에 해당하는 도메인 이름을 메모합니다.
 6. Siebel 매핑 인터페이스를 닫습니다.
 7. BI 실행 패드를 엽니다.
 8. CMC의 Siebel 도메인과 동일한 이름의 새 폴더를 PublicFoldersWSiebel에 만듭니다.
 9. Siebel 정보를 통합하도록 설계된 보고서를 이 폴더에 배치합니다.

19.4.3.2 Contextual Awareness URL 지정

1. 응용 프로그램의 JavaScript 파일을 다시 생성했으면 BI 플랫폼 설치의 Siebel Files 폴더(기본 위치: C:\Program Files\Business Objects\SAP BusinessObjects Enterprise XI\Siebel Files\W)로 이동합니다.
2. BusinessObjectsEnterpriseServer.html 파일을 복사합니다. 그런 다음 genbscript 프로그램이 새 JavaScript 파일을 생성한 공용 폴더를 찾아 BusinessObjectsEnterpriseServer.html의 복사본을 해당 언어 하위 폴더에 배치합니다.
예를 들어 응용 프로그램의 JavaScript 파일을 Siebel 서버의 c:\Wsea752\WSWEApp\WPUBLIC\WENU 폴더에 생성한 경우, BusinessObjectsEnterpriseServer.html 파일을 c:\Wsea752\WSWEApp\WPUBLIC\WENU 폴더로 복사합니다.
3. 메모장 같은 텍스트 편집기에서 공용 폴더의 BusinessObjectsEnterpriseServer.html 파일을 열어 다음 줄을 찾습니다.

```
Var userDomain = "SIEB78"
```

```
var destAddr = "http://<SAP BusinessObjects server>:8080/BOE/BI/logon/siebelStart.do"
```

참고:

- userDomain 또는 destAddr 변수를 수정한 경우 브라우저의 캐시된 웹 페이지를 지워 브라우저가 올바른 대상 주소를 가리키도록 해야 합니다.
- userDomain은 대/소문자를 구분합니다.

19.4.3.3 Contextual Awareness 확인

1. 수정된 일반 웹 메뉴를 사용하는 Siebel 응용 프로그램에 로그인합니다.
2. 원하는 화면으로 이동한 다음 보기 메뉴를 클릭합니다.
새 Crystal Reports 메뉴 항목이 메뉴에 표시됩니다.
3. Crystal Reports 메뉴 항목을 클릭합니다.
BI 플랫폼에서 연결할 사용자 이름과 암호를 요청하는 BI 실행 패드 창이 열립니다. 이는 세션 시간 제한 이전에 처음으로 로그인한 경우에만 필요합니다. HTML 및 Siebel 인증에 구성된 도메인 이름은 이미 채워져 있어야 합니다.

참고:

이 단계는 해당 시점까지의 설치를 확인하는 데만 사용됩니다. Siebel 권한을 BI 플랫폼에 매핑할 때까지는 Siebel 인증을 사용하여 BI 플랫폼에 로그인할 수 없습니다.

19.4.3.4 BI 플랫폼에 폴더 추가

Siebel에 대한 BI 플랫폼 통합 시 Contextual Awareness 기능을 모두 사용할 수 있으려면 일부 폴더를 BI 실행 패드에 추가해야 합니다.

기능이 작동하려면 컨텍스트 폴더가 Root DirWSiebelWDomain Name 구조로 되어 있어야 합니다. Domain Name 하위 폴더에 저장되고 특정 Business Objects 비즈니스 구성 요소와 연결되도록 Siebel 시스템에서 구성된 보고서만 Contextual Awareness 기능의 일부로 표시됩니다. 여기서 사용된 Domain Name은 인증 구성에서 Siebel에 대해 구성된 도메인 이름과 동일해야 하며, Siebel 측 BusinessObjectsEnterpriseServer.html 파일에 구성된 값과 동일해야 합니다.

참고:

이 단원의 단계를 완료하려면 Siebel Tools가 필요합니다.

19.4.4 SAP Crystal Reports 및 Siebel에 대해 단일 로그인(SSO) 구성

기본적으로 BI 플랫폼은 SAP Crystal Reports 사용자가 단일 로그인(SSO)을 사용하여 Siebel 데이터에 액세스할 수 있도록 구성됩니다.

19.4.4.1 Siebel 및 Crystal Reports용 SSO 비활성화

1. 중앙 관리 콘솔(CMC)에서 응용 프로그램을 클릭합니다.
2. Crystal Reports 구성을 두 번 클릭합니다.
3. 단일 로그인 옵션을 클릭합니다.
4. crdb_siebel을 선택합니다.
5. 제거를 클릭합니다.
6. 저장 후 단기를 클릭합니다.
7. SAP Crystal Reports를 다시 시작합니다.

19.4.4.2 Siebel 및 SAP Crystal Reports용 SSO 활성화

Siebel 및 SAP Crystal Reports용 SSO를 비활성되어있고 이를 다시 활성화하려는 경우 다음 작업을 수행합니다.

1. 중앙 관리 콘솔(CMC)에서 응용 프로그램을 클릭합니다.
2. Crystal Reports 구성을 두 번 클릭합니다.
3. 단일 로그인 옵션을 클릭합니다.
4. 데이터베이스 로그인에 SSO 컨텍스트 사용에서 crdb_siebel을 입력합니다.
5. 추가를 클릭합니다.
6. 저장 후 닫기를 클릭합니다.
7. SAP Crystal Reports 서버를 다시 시작합니다.

19.4.5 Secure Socket Layer 통신을 위한 구성

Siebel 및 BI 플랫폼 배포 환경에서 클라이언트와 서버 사이의 모든 네트워크 통신에 SSL(Secure Sockets Layer) 프로토콜을 사용할 수 있습니다.

다른 BI 플랫폼 서버 및 클라이언트에 대한 SSL 구성과 마찬가지로, Siebel 배포 환경에서 컴퓨터로 액세스할 수 있는 안전한 디렉터리에 다음 키 파일과 인증서 파일을 저장합니다.

- 신뢰할 수 있는 인증서 파일(cacert.der)
- 생성된 서버 인증서 파일(servercert.der)
- 서버 키 파일(server.key)
- 암호 파일(passphrase.txt)

SSL 구성 속성 파일

속성 파일인 sslconf.properties에는 필수 인증서에 대한 모든 정보와 Siebel용 BusinessObjects XI Integration 구성 요소에서 사용하는 키가 들어 있습니다. 예를 들면, 다음과 같습니다.

```
businessobjects.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

기본적으로, sslconf.properties 파일은 BI 플랫폼 제품이 설치되어 있는 C:\WProgram Files\WBusiness Objects\WSAP BusinessObjects Enterprise XI\W 폴더에 두어야 합니다.

장20 로그 관리 및 구성

20.1 구성 요소에서 추적 로깅

추적 기능을 통해 시스템 관리자와 지원 담당자는 BI 플랫폼 구성 요소(서버 및 웹 응용 프로그램)의 성능과 대상 구성 요소에서 발생하는 활동을 보고할 수 있습니다.

BI 플랫폼 서버에서 생성된 시스템 수준 메시지가 추적되어 로그 파일에 기록됩니다. 시스템 관리자는 이 로그 파일을 사용하여 디버깅을 위해 성능을 모니터링할 수 있습니다. 추적은 모니터링되는 구성 요소 작업 중에 발생하는 이벤트 레코드입니다. 한쪽의 심각한 예외에서 다른 쪽의 단순 상태 메시지에 이르는 범위의 이벤트가 추적됩니다.

추적 로그

추적 메시지는 일반 로그 파일(.glf) 확장명으로 저장된 로그 파일에 수집됩니다. 구성 요소에 대한 추적 로그 수준을 설정할 때 로그 파일로 보낼 정보의 유형과 상세 수준을 결정하십시오. 추적 로그 수준은 지정된 수준에 도달하지 않은 추적을 표시하지 않는 필터입니다. 표시되지 않는 추적은 출력 로그 파일에 기록되지 않습니다. 구성 요소에 대한 추적 로그를 모니터링하면 증가한 작업량을 처리할 수 있도록 구성 요소의 현재 인스턴스 또는 구성을 변경해야 할지 여부 또는 부하 증가가 성능에 큰 영향을 미치지 않는지 여부를 확인할 수 있습니다.

20.2 추적 로그 수준

다음 표에는 BI 플랫폼 구성 요소에서 사용 가능한 추적 로그 수준이 나와 있습니다.

수준	설명
지정되지 않음	추적 로그 수준은 다른 메커니즘(보통 .ini 파일)을 통해 지정됩니다.
없음	추적 로그 수준이 없음으로 설정되어 있을 때는 지정된 중요도 수준 미만으로 추적을 선택적으로 억제할 수 있는 필터가 비활성화됩니다. 참고: 추적 로그 수준이 없음이라고 해서 추적 기능이 해제되는 것은 아닙니다. 시스템 리소스는 계속 모니터링되고 실패한 어설션과 같이 드물게 발생하는 중요 이벤트에 대해 추적이 로그됩니다.
낮음	경고 메시지와 대부분의 상태 메시지를 무시한 상태에서 오류 메시지를 로그할 수 있도록 추적 로그 필터가 설정됩니다. 하지만, 시작 및 종료 요청 메시지뿐 아니라 구성 요소 시작, 시스템 종료에 대해서도 매우 중요한 상태 메시지가 로그로 기록됩니다. 참고: 디버깅할 목적이라면 이 수준으로 설정하지 않는 것이 좋습니다.
중간	추적 로그 필터는 로그 출력에 오류, 경고 및 대부분의 상태 메시지를 포함하도록 설정됩니다. 중요도가 최소이거나 세부 정보 표시 수준이 높은 상태 메시지는 필터링됩니다. 디버깅할 목적이라면 이 수준은 세부 정보를 표시하기에 충분치 않습니다.
높음	이 필터로는 어떤 메시지도 제외되지 않습니다. 디버깅할 목적이라면 이 수준으로 설정하는 것이 좋습니다. 참고: 높음 추적 로그 수준 설정으로 시스템 리소스에 영향을 미칠 수 있습니다. 파일 시스템의 저장 공간뿐 아니라 CPU 사용량을 증가시켰을 가능성이 있습니다.

20.3 서버에 대한 추적 구성

모니터링되는 BI 플랫폼 서버에 대한 추적은 특정 로그 파일(.glf)에 기록되며 로깅 폴더 또는 디렉터리에 저장됩니다. Windows 플랫폼의 경우 Logging 디렉터리의 기본 위치는 Program Files <INSTALLDIR>WSAP BusinessObjects Enterprise XI 4.0\logging입니다. Unix의 경우 이 디렉터리는 <INSTALLDIR>/sap_bobj/logging입니다.

참고:

.glf 파일 이름은 간단한 식별자, 서버 이름 및 번호 참조 조합(예: aps_mysia.AdaptiveProcessingServer_trace.000012.glf) 형식으로 되어 있습니다. 로그 파일 크기가 1MB 임계값에 도달하면 모니터링되는 서버에 대해 새 추적 로그 파일이 만들어집니다.

관리자가 특정 서버 또는 서버 컬렉션에 대한 추적 로그 수준을 설정하여 로그 파일에 수집된 추적의 심각도와 중요도를 조정할 수 있습니다. 추적 로그 수준은 다음과 같은 권장 방법을 통해 수정할 수 있습니다.

- 중앙 관리 콘솔(CMC)에서 특정 서버 또는 서버 그룹에 대한 추적 로그 서비스를 사용합니다.
- BO_trace.ini 파일에서 추적 로그 수준 및 기타 설정을 수동으로 변경합니다.

특정 서버에 대한 추적 로그 수준만 수정하려는 경우 CMC에서 추적 로그 서비스를 사용하는 것이 좋습니다. 다른 추적 매개 변수를 수정하려면 BO_trace.ini 파일을 재구성해야 합니다.

20.3.1 CMC에서 서버 추적 로그 수준 설정

다른 추적 설정에 영향을 주지 않으면서 서버의 추적 로그 수준을 조정할 수 있습니다. 다음 지침에 따라 추적 로그 수준을 조정하십시오.

1. CMC의 서버 관리 영역으로 이동합니다.
2. 수정하려는 추적 로그 수준이 있는 서버에 액세스합니다.
 - a. 서버 범주를 클릭하여 특정 서버 범주의 서버에 액세스합니다.
 - b. 탐색 창에서 서버 목록을 클릭하여 전체 서버 목록에 액세스합니다.
3. 서버를 마우스 오른쪽 단추로 클릭하고 속성을 클릭합니다.
속성 대화 상자가 표시됩니다.
4. 추적 로그 서비스 영역의 로그 수준 목록에서 원하는 설정을 선택합니다.
5. 저장 후 단기를 클릭하여 수정된 추적 로그 수준을 제출합니다.

잠시 후 새 추적 로그 수준이 적용됩니다.

로그 파일에 대해 다른 디렉터리를 지정하려면 명령줄 매개 변수 영역에서 -loggingPath 매개 변수를 대상 디렉터리 경로와 함께 사용하십시오. 이 수정 사항은 서버가 다시 시작되어야 적용됩니다.

관련 항목

- 743 페이지에서 [추적 로그 수준](#)

20.3.2 CMC에서 관리되는 여러 서버에 대한 추적 로그 수준 설정

1. CMC의 서버 관리 영역으로 이동합니다.
사용 가능한 서비스 범주가 서버 페이지에 표시됩니다.

2. 재설정하려는 추적 로그 수준을 가진 서버에 액세스합니다.
 - a. 서버 범주를 클릭하여 특정 서버 범주의 서버에 액세스합니다.
 - b. 탐색 작업창에서 서버 목록을 클릭하여 전체 서버 목록에 액세스합니다.
3. 서버를 선택합니다.
여러 서버를 선택하려면 Ctrl 키를 누른 상태에서 선택합니다.
4. 마우스 오른쪽 단추를 클릭한 다음 공통 서비스 편집을 선택합니다.
공통 서비스 편집 화면이 표시됩니다.
5. 추적 로그 서비스 영역의 로그 수준 목록에서 원하는 설정을 선택합니다.
6. 확인을 클릭하여 수정된 추적 로그 수준을 제출합니다.

잠시 후 새 추적 로그 수준이 적용됩니다.

로그 파일에 대해 다른 디렉토리를 지정하려면 명령줄 매개 변수 영역에서 -loggingPath 매개 변수를 대상 디렉터리 경로와 함께 사용하십시오. 이 수정 사항은 서버가 다시 시작되어야 적용됩니다.

관련 항목

- 743 페이지에서 [추적 로그 수준](#)

20.3.3 BO_trace.ini 파일을 통해 서버 추적 구성

BO_trace.ini 파일은 1분마다 읽혀지고 기본적으로 추적을 해제하도록 구성되어 있습니다. BO_trace.ini 파일을 사용하여 추적을 활성화하고 구성하려면 다음 단계를 수행하십시오.

1. BO_trace.ini 파일을 엽니다.
 - Windows의 경우 기본 위치는 <INSTALLDIR>WSAP BusinessObjects Enterprise XI 4.0WconfW입니다.
 - UNIX의 경우 기본 위치는 <INSTALLDIR>/sap_bobj/enterprise_xi40/conf/입니다.
2. Trace Syntax and Setting 섹션에서 필요한 줄의 주석을 없앱니다.
3. 필요에 따라 서버 추적 매개 변수를 수정합니다.
아래 표에는 서버 추적을 구성하는 데 사용되는 일반적인 매개 변수가 나열되어 있습니다.

매개 변수	가능한 값	설명
active	false, true	true로 설정한 경우, importance 매개 변수에 설정된 임계값을 만족하는 추적 메시지가 추적됩니다. false로 설정한 경우, "중요도" 수준을 바탕으로 추적 메시지가 추적되지 않습니다. 기본값은 false입니다.
importance	'<<', '<=', '==', '>=', '>>', xs, s, m, l, xl 참고: importance = xs 또는 importance = <<는 importance = xl 또는 importance = >>가 최소인 상태에서 사용 가능한 가장 자세한 옵션입니다.	추적 메시지의 임계값을 지정합니다. 임계값을 초과하는 모든 메시지가 추적됩니다. 기본값은 m(보통)입니다.
alert	false, true	true로 설정한 경우, severity 매개 변수에 설정된 임계값을 만족하는 추적 메시지가 추적됩니다. false로 설정한 경우, "심각도" 수준을 바탕으로 추적 메시지가 추적되지 않습니다. 기본값은 true입니다.
severity	' ', 'W', 'E', 'A', success, warning, error, assert	메시지를 추적하는 데 기준이 될 심각도 임계값을 지정합니다. 기본값은 'E'입니다.
size	가능한 값은 1000 이상의 정수입니다.	새 추적 로그 파일이 작성되기 전에 한 추적 로그 파일에 포함될 메시지 수를 지정합니다. 기본값은 100000입니다.
keep_num	가능한 값은 1000 이상의 정수입니다.	유지할 로그 수를 지정합니다.

매개 변수	가능한 값	설명
administrator	문자열 또는 정수	출력 로그 파일에서 사용할 주석을 지정합니다. 예를 들면 다음과 같습니다. administrator = "hello" 이 문자열은 로그 파일에 삽입됩니다.
log_dir		출력 로그 파일 디렉터리를 지정합니다. 기본적으로 로그 파일은 Logging 폴더에 저장됩니다.
always_close	on, off	추적이 로그 파일에 기록된 후 로그 파일을 닫을지 여부를 지정합니다. 기본값은 off입니다.

4. BO_trace.ini 파일을 저장하고 닫습니다.

수정된 설정은 모든 서버가 다시 시작되어야 적용됩니다.

예제

```
active=false;
severity='E';
importance='==';
size=1000000;
keep_num=437;
```

20.3.3.1 서버별 추적 구성

BO_trace.ini 파일은 BI 플랫폼 서버에 대한 추적 매개 변수를 지정하는 데 사용됩니다. 이 설정은 관리되는 서버 전체에 적용됩니다. 관리자는 BO_trace.ini 파일로 특정 서버에 대한 추적 매개 변수를 설정할 수 있습니다.

1. BO_trace.ini 파일을 엽니다.

- Windows의 경우 기본 위치는 <INSTALLDIR>WSAP BusinessObjects Enterprise XI 4.0WconfW입니다.
- UNIX의 경우 기본 위치는 <INSTALLDIR>/sap_bobj/enterprise_xi40/conf/입니다.

2. Trace Syntax and Setting 섹션에서 필요한 줄의 주석을 없앱니다.

3. 특정 서버에 대한 추적 설정을 지정하려면 아래 예제에 표시된 것과 같이 IF 문을 사용합니다.

```
if (process == "aps_MySIA.ProcessingServer")
{
    active = true;
    importance = '<<' ;
```

```

alert = true;
severity = 'I';
keep_num = 487;
size = 100 * 1000;
}

```

4. BO_trace.ini 파일을 저장하고 닫습니다.

잠시 후 수정된 설정이 구현됩니다. 특정 서버에 대한 CMC에 지정된 추적 로그 수준이 새 설정으로 바뀝니다.

20.4 웹 응용 프로그램에 대한 추적 구성

모니터링되는 BI 플랫폼 웹 응용 프로그램에 대한 추적은 특정 로그 파일(.glf)에 기록되며 웹 응용 프로그램을 호스팅하는 컴퓨터의 폴더에 저장됩니다. 추적 로그 파일은 기본적으로 \$userHome/SBOP Webapp_\$application_\$IPaddress_\$port/ 디렉터리에 있습니다.

관리자가 특정 웹 응용 프로그램 또는 웹 응용 프로그램 컬렉션에 대한 추적 로그 수준을 설정하여 로그 파일에 수집된 추적의 심각도와 중요도를 조정할 수 있습니다. 추적 로그 수준은 다음과 같은 권장 방법을 통해 수정할 수 있습니다.

- 중앙 관리 콘솔(CMC)에서 추적 로그 응용 프로그램 설정을 사용합니다.
- BO_trace.ini 파일에서 추적 로그 수준 및 기타 추적 설정을 수동으로 재구성합니다. 이 파일은 BOE 및 dswebobj WAR 파일과 함께 웹 응용 프로그램 서버에 배포됩니다.

BOE 웹 응용 프로그램에 대한 추적 로그 수준만 수정하려면 CMC 옵션을 사용하는 것이 좋습니다. 추적 매개 변수를 모두 수정하려면 BO_trace.ini 파일을 재구성해야 합니다.

참고:

BO_trace.ini 파일을 재구성하려면 먼저 Wdeploy 도구를 사용하여 웹 응용 프로그램 서버에서 기존 웹 응용 프로그램의 배포를 취소해야 합니다. BO_trace.ini 파일을 재구성한 후에는 웹 응용 프로그램 서버에 웹 응용 프로그램과 함께 다시 배포해야 합니다. WDeploy를 사용하여 웹 응용 프로그램을 준비, 배포 및 배포 취소하는 방법은 SAP BusinessObjects Business Intelligence 플랫폼 웹 응용 프로그램 배포 가이드를 참조하십시오.

20.4.1 CMC에서 웹 응용 프로그램 추적 로그 수준 설정

기본적으로, CMC의 웹 응용 프로그램에 대한 추적 로그 수준은 지정되지 않음으로 설정됩니다. CMC에서 다음 응용 프로그램에 대한 추적 로그 설정을 사용할 수 있습니다.

- 중앙 관리 콘솔
- BI 실행 패드
- Open Document
- 웹 서비스

다른 웹 응용 프로그램을 모두 추적하려면 해당 BO_trace 파일을 구성하기 위한 수동 방법을 사용하십시오.

1. CMC의 응용 프로그램 관리 영역으로 이동합니다.
응용 프로그램 대화 상자가 표시됩니다.
2. 응용 프로그램을 마우스 오른쪽 단추로 클릭하고 추적 로그 설정을 선택합니다.
추적 로그 설정 대화 상자가 나타납니다.
3. 로그 수준 목록에서 원하는 설정을 선택합니다.
4. 저장 후 단기를 클릭하여 추적 로그 수준을 제출합니다.

새 추적 로그 수준은 다음에 웹 응용 프로그램에 로그인한 후에 적용됩니다.

관련 항목

- 743 페이지에서 [추적 로그 수준](#)

20.4.2 BO_trace.ini 파일을 통해 수동으로 추적 설정 수정

BO_trace.ini 파일은 BOE 및 dswebobj WAR 파일과 함께 웹 응용 프로그램 서버에 배포됩니다. 그러나 웹 응용 프로그램 서버에서 항상 액세스할 수 있는 것이 아닙니다. 다음과 같은 준비 단계를 수행해야 합니다. 영향을 받은 웹 응용 프로그램의 배포를 웹 응용 프로그램 서버에서 취소해야 합니다.

1. Wdeploy를 사용하여 웹 응용 프로그램 서버에서 웹 응용 프로그램의 배포를 취소합니다. WDeploy를 사용하여 웹 응용 프로그램의 배포를 취소하는 방법은 SAP BusinessObjects Business Intelligence 플랫폼 웹 응용 프로그램 배포 가이드를 참조하십시오.

참고:

BI 플랫폼 설치와 함께 제공되는 Tomcat 웹 응용 프로그램 서버를 사용 중인 경우 다음 디렉터리에서 BO_trace.ini 파일에 액세스할 수 있습니다. 웹 응용 프로그램의 배포를 취소하고 파일을 직접 수정할 필요는 없습니다.

- BOE.war 파일에 대한 추적 구성 파일은 <INSTALLDIR>WTomcat6WwebappsWBOEWWEB-INFWTraceLog에 있습니다.
- dswebobj.war 파일에 대한 추적 구성 파일은 <INSTALLDIR>WTomcat6WwebappsWdswebobjWWEB-INFWconf에 있습니다.

번들 Tomcat 웹 응용 프로그램 서버를 사용하는 경우에는 3단계로 건너뜁니다.

2. BOE 또는 dswebobj WAR 파일용 BO_trace.ini 파일의 사전 배포 버전에 액세스합니다.

- BOE.war 파일용 구성 파일의 사전 배포 버전은 기본적으로 <INSTALLDIR>WSAP BusinessObjects Enterprise XI 4.0\warfiles\Wwebapps\WBOE\WEB-INF\WTraceLog 디렉터리에 있습니다.
 - dswsbobje.war 파일용 구성 파일의 사전 배포 버전은 기본적으로 <INSTALLDIR>W SAP BusinessObjects Enterprise XI 4.0\warfiles\Wwebapps\Wdswsbobje\WEB-INF\Wconf 디렉터리에 있습니다.
3. BO_trace.ini 파일을 엽니다.
- Windows의 경우 기본 위치는 <INSTALLDIR>WSAP BusinessObjects Enterprise 12.0\logging\WlogConfig입니다.
 - UNIX의 경우 기본 위치는 <INSTALLDIR>/sap_bobj/enterprise_xi40/conf/입니다.
4. Trace Syntax and Setting 섹션에서 필요한 줄의 주석을 없앱니다.
5. 필요에 따라 서버 추적 매개 변수를 수정합니다.
- 아래 표에는 서버 추적을 구성하는 데 사용할 수 있는 모든 매개 변수가 나열되어 있습니다.

매개 변수	가능한 값	설명
active	false, true	true로 설정하면 현재 프로세스 또는 서버에 대한 추적이 활성화됩니다. 기본값은 false입니다.
importance	'<<', '<=', '==', '>=', '>>', xs, s, m, l, xl 참고: importance = xs가 가장 세부적인 옵션이고, importance = xl이 가장 대략적인 옵션입니다.	추적 메시지의 임계값을 지정합니다. 임계값을 초과하는 모든 메시지가 추적됩니다. 기본값은 m(보통)입니다.
alert	false, true	심각한 시스템 이벤트에 대한 추적을 자동으로 실행하도록 지정합니다. 기본값은 true입니다.
severity	' ', 'W', 'E', 'A', success, warning, error, assert	메시지를 추적하는 데 기준이 될 심각도 임계값을 지정합니다. 기본값은 'E'입니다.
size	가능한 값은 1000 이상의 정수입니다.	새 추적 로그 파일이 작성되기 전에 한 추적 로그 파일에 포함될 메시지 수를 지정합니다. 기본값은 100000입니다.
keep	false, true	새 파일이 작성된 후 이전 로그 파일을 유지할지 여부를 지정합니다. 기본값은 false입니다.

매개 변수	가능한 값	설명
administrator	문자열 또는 정수	출력 로그 파일에서 사용할 주석을 지정합니다. 예를 들면 다음과 같습니다. administrator = "hello" 이 문자열은 로그 파일에 삽입됩니다.
log_dir		출력 로그 파일 디렉터리를 지정합니다. 기본적으로 로그 파일은 Logging 폴더에 저장됩니다.
always_close	on, off	추적이 로그 파일에 기록된 후 로그 파일을 닫을지 여부를 지정합니다. 기본값은 off입니다.

```
active=false;
severity='E';
importance='==';
size=1000000;
keep=false;
```

6. BO_trace.ini 파일을 저장하고 닫습니다.
7. Wdeploy를 사용하여 웹 응용 프로그램 서버를 호스팅하는 컴퓨터에 WAR 파일을 배포합니다.
웹 응용 프로그램에 처음으로 로그인하면 수정된 추적 설정이 적용됩니다.

20.4.2.1 특정 웹 응용 프로그램에 대한 추적 구성

BO_trace.ini 파일은 BI 플랫폼 웹 응용 프로그램에 대한 추적 매개 변수를 지정하는 데 사용됩니다. 이 설정은 배포된 WAR 파일과 관련된 모든 응용 프로그램에 적용됩니다. 관리자는 BO_trace.ini 파일로 특정 웹 응용 프로그램에 대한 추적 매개 변수를 설정할 수도 있습니다.

아래 표는 현재 BI 플랫폼 릴리스의 웹 응용 프로그램 및 관련 WAR 파일을 보여 줍니다.

웹 응용 프로그램	WAR 파일	사전 배포 위치
중앙 관리 콘솔	BOE.war	<INSTALLDIR>WSAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\WBOE\WEB-INF\WTraceLog
BI 실행 패드	BOE.war	<INSTALLDIR>WSAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\WBOE\WEB-INF\WTraceLog
Open Document	BOE.war	<INSTALLDIR>WSAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\WBOE\WEB-INF\WTraceLog
웹 서비스	dswsbobje.war	<INSTALLDIR>W SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\Wdswsbobje\WEB-INF\Wconf

1. Wdeploy를 사용하여 웹 응용 프로그램 서버에서 웹 응용 프로그램의 배포를 취소합니다. WDeploy를 사용하여 웹 응용 프로그램의 배포를 취소하는 방법은 SAP BusinessObjects Business Intelligence 플랫폼 웹 응용 프로그램 배포 가이드를 참조하십시오.

참고:

BI 플랫폼 설치와 함께 제공되는 Tomcat 웹 응용 프로그램 서버를 사용 중인 경우 다음 디렉터리에서 BO_trace.ini 파일에 액세스할 수 있습니다. 웹 응용 프로그램의 배포를 취소할 필요는 없습니다. 파일을 직접 수정할 수 있습니다.

- BOE.war 파일에 대한 추적 구성 파일은 <INSTALLDIR>WTomcat6\webapps\WBOE\WEB-INF\WTraceLog에 있습니다.
- dswsbobje.war 파일에 대한 추적 구성 파일은 <INSTALLDIR>WTomcat6\webapps\Wdswsbobje\WEB-INF\Wconf에 있습니다.

번들 Tomcat 웹 응용 프로그램 서버를 사용하는 경우에는 3단계로 건너뛵니다.

2. BOE 또는 dswsbobje WAR 파일용 BO_trace.ini 파일의 사전 배포 버전에 액세스합니다.
 - BOE.war 파일용 구성 파일의 사전 배포 버전은 기본적으로 <INSTALLDIR>WSAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\WBOE\WEB-INF\WTraceLog 디렉터리에 있습니다.
 - dswsbobje.war 파일용 구성 파일의 사전 배포 버전은 기본적으로 <INSTALLDIR>W SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\Wdswsbobje\WEB-INF\Wconf 디렉터리에 있습니다.
3. BO_trace.ini 파일을 엽니다.
4. Trace Syntax and Setting 섹션에서 필요한 줄의 주석을 없앱니다.
5. 특정 웹 응용 프로그램에 대한 추적 설정을 지정하려면 아래 예제에 표시된 것과 같이 IF 문을 사용합니다.

```
if (device_name == "Webapp_opendocument_trace")
{
  active = true;
  importance = '<<';
  alert = true;
  severity = '';
  keep_num = 332;
  size = 100 * 1000;
}
```

아래 표는 웹 응용 프로그램 추적을 구성하는 데 사용할 수 있는 모든 매개 변수를 보여 줍니다.

매개 변수	가능한 값	설명
active	false, true	true로 설정하면 현재 프로세스 또는 서버에 대한 추적이 활성화됩니다. 기본값은 false입니다.
importance	'<<', '<=', '==', '>=', '>>', xs, s, m, l, xl 참고: importance = xs가 가장 세부적인 옵션이고, importance = xl이 가장 대략적인 옵션입니다.	추적 메시지의 임계값을 지정합니다. 임계값을 초과하는 모든 메시지가 추적됩니다. 기본값은 m(보통)입니다.
alert	false, true	심각한 시스템 이벤트에 대한 추적을 자동으로 실행하도록 지정합니다. 기본값은 true입니다.
severity	' ', 'W', 'E', 'A', success, warning, error, assert	메시지를 추적하는 데 기준이 될 심각도 임계값을 지정합니다. 기본값은 'E'입니다.
size	가능한 값은 1000 이상의 정수입니다.	새 추적 로그 파일이 작성되기 전에 한 추적 로그 파일에 포함될 메시지 수를 지정합니다. 기본값은 100000입니다.
keep	false, true	새 파일이 작성된 후 이전 로그 파일을 유지할지 여부를 지정합니다. 기본값은 false입니다.
administrator	문자열 또는 정수	출력 로그 파일에서 사용할 주석을 지정합니다. 예를 들면 다음과 같습니다. administrator = "hello" 이 문자열은 로그 파일에 삽입됩니다.
log_dir		출력 로그 파일 디렉터리를 지정합니다. 기본적으로 로그 파일은 Logging 폴더에 저장됩니다.
always_close	on, off	추적이 로그 파일에 기록된 후 로그 파일을 닫을지 여부를 지정합니다. 기본값은 off입니다.

6. BO_trace.ini 파일을 저장하고 닫습니다.

7. Wdeploy를 사용하여 웹 응용 프로그램 서버를 호스팅하는 컴퓨터에 WAR 파일을 배포합니다.

20.5 업그레이드 관리 도구에 대한 추적 구성

업그레이드 관리 도구에 대한 추적은 BO_trace.ini 구성 파일을 통해 수행됩니다.

Windows의 경우 기본 위치는 <INSTALLDIR>WSAP BusinessObjects Enterprise XI 4.0WconfW입니다.

UNIX의 경우 기본 위치는 <INSTALLDIR>/sap_bobj/enterprise_xi40/conf/입니다.

참고:

다른 BI 플랫폼 구성 요소와 달리, 업그레이드 관리 도구에 대한 추적 구성은 CMC를 통해 수행할 수 없습니다.

20.5.1 업그레이드 관리 도구에 대한 추적 구성

1. BO_trace.ini 파일을 엽니다.
 - Windows의 경우 기본 위치는 <INSTALLDIR>WSAP BusinessObjects Enterprise XI 4.0WconfW입니다.
 - UNIX의 경우 기본 위치는 <INSTALLDIR>/sap_bobj/enterprise_xi40/conf/입니다.
2. Trace Syntax and Setting 섹션에서 필요한 줄의 주석을 없앱니다.
3. 특정 서버에 대한 추적 설정을 지정하려면 아래 예제에 표시된 것과 같이 IF 문을 사용합니다.

```
if (process == "upgrademanagementtool")
{
  active = true;
  importance = '<<';
  alert = true;
  severity = '';
  keep = false;
  size = 100 * 1000;
}
```

팁:

추적 설정을 업그레이드 관리 도구에 적용하려면 프로세스를 upgrademanagementtool로 지정해야 합니다.

4. BO_trace.ini 파일을 저장하고 닫습니다.

잠시 후 수정된 설정이 구현됩니다.

장21 SAP Solution Manager에 통합

21.1 통합 개요

SAP Solution Manager로 통합할 수 있도록 BI 플랫폼에 지원 기능이 추가되었습니다. 다음 SAP Solution Manager 구성 요소를 사용하여 BI 플랫폼 배포를 위한 지원을 제공할 수 있습니다.

- Solution Landscape Directory
- SMD(Solution Manager Diagnostics)
- CA Wily의 Introscope
- SAP Passport

참고:

SAP BusinessObjects용 SAP 지원 포털에 액세스하려면 <https://websmp205.sap-ag.de/bosap-support>로 이동합니다.

21.2 SAP Solution Manager 통합 검사 목록

다음 표는 SAP Solution Manager를 사용하여 BI 플랫폼에 대한 지원을 제공하는 데 필요한 구성 요소를 요약한 것입니다.

SAP Solution Manager 지원	BI 플랫폼에 필수
SLD 등록	<ul style="list-style-type: none"> BI 플랫폼 서버의 등록을 사용하려면 SAPHOSTAGENT를 설치해야 합니다. 참고: SAPHOSTAGENT가 이미 설치되어 있는 경우 BI 플랫폼 설치 관리자는 서버를 자동으로 등록합니다. 백 엔드 서버에 대해 보고하는 데이터 공급자용 connect.key 파일을 만들어야 합니다. (선택사항) WebSphere 6.1 또는 7에서 SLD를 등록하려면 각각의 WebSphere 웹 응용 프로그램 서버에 SLDREG 등록 도구를 설치해야 합니다. 자세한 내용은 SAP Note 1482727을 참조하십시오. (선택사항) SAP NetWeaver 7.2에서 SLD를 등록하려면 모든 NetWeaver 호스트에 SLDREG를 설치합니다. 자세한 내용은 SAP Note 1018839를 참조하십시오.
SMD 통합	<ul style="list-style-type: none"> SMD Agent(DIAGNOSTICS.AGENT)를 다운로드하여 BI 플랫폼 서버의 모든 호스트에 설치해야 합니다. BI 플랫폼에서 SAdmin 사용자 계정을 사용해야 합니다.
성능 계측	<ul style="list-style-type: none"> Enterprise Manager에 연결하려면 Intro-scope Agent를 구성해야 합니다. BI 플랫폼 설치 관리자 또는 CMC 노드 자리 표시자를 사용하여 연결을 구성합니다. SMD Agent를 설치해야 합니다. SMD Agent에 연결하도록 BI 플랫폼을 구성해야 합니다. BI 플랫폼 설치 관리자 또는 CMC 노드 자리 표시자를 사용하여 연결을 구성합니다.
SAP Passport	<ul style="list-style-type: none"> SAP Passport 클라이언트 도구를 다운로드하여 설치해야 합니다.

21.3 System Landscape Directory 등록 관리

21.3.1 시스템 랜드스케이프에 BI 플랫폼 등록

SLD(System Landscape Directory)는 소프트웨어 수명 주기 관리와 관련된 시스템 랜드스케이프 정보의 중앙 리포지토리입니다. SLD에는 시스템 랜드스케이프, 즉 현재 설치되어 있는 시스템 및 소프트웨어 구성 요소에 대한 설명이 포함됩니다. SLD 데이터 공급자는 SLD 서버에 시스템을 등록하고 정보를 최신 상태로 유지합니다. 관리 및 비즈니스 응용 프로그램은 SLD에 저장된 정보에 액세스하여 공동 작업 컴퓨팅 환경에서 작업을 수행합니다.

SLD-DS(System Landscape Directory-Data Supplier)는 BI 플랫폼 서버를 SLS 서버에 등록하는 역할을 하는 응용 프로그램입니다. 플랫폼을 설치할 때마다 다음 구성 요소에 대해 보고하기 위해 특정 데이터 공급자가 제공됩니다.

- BI 플랫폼 서버
- WebSphere 웹 응용 프로그램 서버에 호스트된 웹 응용 프로그램과 서비스

참고:

SAP NetWeaver에는 호스트된 웹 응용 프로그램 및 서비스뿐 아니라, NetWeaver 응용 프로그램 서버도 등록하는 SLD-DS 공급자가 기본 제공됩니다. 이 SLD-DS는 SAP NetWeaver 환경 내에 통합된 BI 플랫폼 배포에 적절합니다.

BI 플랫폼 서버에 대해 보고하는 SLD-DS는 SLDREG 프로그램을 설치하고 구성해야 합니다.

SAPHOSTAGENT 도구를 설치할 때 SLDREG 프로그램이 설치됩니다. SAPHOSTAGENT에 액세스하여 설치하는 자세한 방법은 SAP BusinessObjects Business Intelligence 플랫폼 설치 가이드의 준비 단원을 참조하십시오. SLDREG가 설치된 후 connect.key 파일을 만들어 SLD 서버에 연결할 수 있게 해야 합니다.

WebSphere를 위한 특정 데이터 공급자를 구성하는 자세한 방법은 SAP 웹 응용 프로그램 배포 가이드를 참조하십시오.

BI 플랫폼 설치 중에 BI 플랫폼 등록에 필요한 정보가 구성 파일에 저장됩니다. 이 파일에는 SLD DS가 BI 플랫폼 데이터베이스에 연결하기 위해 사용하는 정보가 포함됩니다.

21.3.1.1 SLD 데이터 공급자에 알맞은 키 파일 만들기

BI 플랫폼

SLD 데이터 공급자용 connect.key 파일을 만들기 전에 SAPHOSTAGENT를 다운로드하여 설치해야 합니다. 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 설치 가이드의 준비 단원을 참조하십시오.

참고:

BI 플랫폼 서버에 대해 보고하는 데이터 공급자로 SLD 등록에 connect.key 파일이 필요합니다.

1. 명령줄 콘솔을 엽니다.
2. 기본 SAPHOSTAGENT 설치 경로를 탐색합니다.
 - Windows: Program Files\WSAP\Whostctrl\Wexe
 - Unix: /usr/sap/hostctrl/exe
3. 다음 명령을 실행합니다.


```
sldreg -configure connect.key
```
4. 다음 구성 세부 정보를 입력합니다.
 - 사용자 이름
 - 암호
 - 호스트
 - 포트 번호
 - HTTP를 사용하려면 지정

sldreg 도구가 connect.key 파일을 만듭니다. 이 파일은 SLD 서버에 정보를 제공할 때 데이터 공급자에서 자동으로 사용됩니다.

21.3.2 SLD 등록이 트리거되는 시기

다음 시나리오에서 BI 플랫폼 백 엔드 서버에 대해 보고하는 데이터 공급자가 SLD 등록 프로세스를 호출합니다.

- BI 플랫폼 배포 시 서버 노드가 다시 시작됩니다.
- 배포에 새 서버 또는 노드가 추가됩니다.
- 서버 또는 노드가 삭제됩니다.

참고:

서버 또는 노드가 삭제되면 SLD 등록 프로세스에서 SLD 서버의 콘텐츠를 수정하지 않습니다.

WebSphere SLD 등록을 위한 데이터 공급자는 수동으로 호출하거나 지정된 간격(예: 24시간마다)으로 실행하도록 설정할 수 있습니다. 이 데이터 공급자의 구성에 대한 자세한 내용은 SAP Note 482727을 참조하십시오.

21.3.3 SLD 연결 로깅

데이터 공급자 구성 파일

SLD 등록에 사용되는 구성 파일은 BI 플랫폼 배포용으로 만들어집니다. `sldparserconfig.properties` 파일은 `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/` 디렉터리에 있습니다.

SLD 연결 로깅

BI 플랫폼 배포 시 SLD 서버와 데이터 공급자 간의 연결은 `sldreg` 도구 및 `connect.key` 파일을 통해 제어됩니다.

참고:

로그 파일 이름은 `sldparserconfig.properties` 파일의 속성으로 지정됩니다.

BI 플랫폼 백 엔드 서버에 대해 보고하는 SLD 데이터 공급자의 로그 파일은 있는 기본 위치는 `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/bobjsldds.log`에 있습니다. 데이터 공급자가 실행될 때마다 파일을 덮어씁니다.

`sldreg`에 대한 로그 파일이 있는 기본 위치는 `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/log`입니다. `sldreg` 로그 파일 이름은 수정할 수 없고 그 형식은 `sldrg_<Timestamp>.log`와 같습니다.

데이터 공급자가 `sldreg`를 호출할 때마다 새 로그 파일이 만들어집니다.

21.4 Solution Manager Diagnostics Agent 관리

21.4.1 SMD(Solution Manager Diagnostics) 개요

SAP Solution Manager의 SMD(Solution Manager Diagnostics) 구성 요소는 전체 시스템 랜즈스케이프를 중앙에서 분석하고 모니터링하기 위한 모든 기능을 제공합니다. SMD Agent가 설치되어 있는 경우 SMD 서버가 BI 플랫폼을 모니터링할 수 있습니다. SMD Agent(DIAGNOSTICS.AGENT)는 근본 원인 분석에 사용할 수 있는 SMD에 대한 정보를 수집합니다. 수집한 후 SMD 서버로 보내는 정보에는 백 엔드 서버 구성과 서버 로그 파일의 위치가 포함됩니다.

21.4.2 SMD 에이전트 작업

BI 플랫폼에서는 SMD Agent를 설치하지 않습니다. DIAGNOSTICS.AGENT 에이전트는 <http://service.sap.com/swdc>에서 다운로드할 수 있습니다.

에이전트 설치 및 구성에 관한 정보는 <http://service.sap.com/diagnostics>에서 확인할 수 있습니다.

SMD Agent 작업 지침

다음은 SMD 에이전트를 사용하여 BI 플랫폼을 모니터링하기 위한 지침으로 제공됩니다.

- 모니터링하는 시스템 및 에이전트의 설치 순서는 중요하지 않습니다. BI 플랫폼을 설치 및 배포하기 전이나 후에 SMD Agent 설치를 선택할 수 있습니다.
- SMD Agent를 설치할 때, 호스트 이름과 수신 포트를 기록하십시오. 이 정보는 BI 플랫폼을 모니터링하는 시스템으로 구성하는 데 중요합니다. 모니터링하는 시스템 전에 에이전트를 설치한 경우, BI 플랫폼 설치 설정 중 구성 정보를 제공할 수 있습니다. 사용자 배포 환경의 중앙 관리 콘솔에 있는 노드의 자리 표시자를 통해 나중에 이 정보를 제공할 수도 있습니다.
- 백 엔드 서버가 분산 시스템에 배포되는 경우, 백 엔드 서버를 호스트하는 컴퓨터마다 SMD Agent를 설치해야 합니다.
- 비 Java 서버의 성능 계측에는 SMD Agent가 필요합니다.
- SMD 서버가 CMS에 액세스할 수 있도록 하려면 SMAAdmin 사용자 계정을 활성화해야 합니다.

21.4.3 SMAAdmin 사용자 계정

모든 BI 플랫폼 배포에는 SMD 통합을 촉진하기 위해 만들어진 사용자 계정이 있습니다. SMD 서버에서는 이 읽기 전용 계정을 사용하여 CMS에 로그인하고 서버 구성 및 배포에 대한 기타 정보를 수집합니다.

SMAAdmin 계정은 기본적으로 비활성화 상태입니다.

21.4.3.1 SMAAdmin 계정 활성화

1. CMC의 사용자 및 그룹 관리 영역에서 사용자 목록을 선택합니다.
사용자 목록이 표시됩니다.
2. SMAdmin 사용자 계정을 찾습니다.
3. 관리 > 속성을 클릭합니다.
속성 대화 상자가 나타납니다.
4. 계정 사용 안 함 확인란의 선택을 취소합니다.
5. 저장 후 단기를 클릭합니다.

21.5 성능 계측 관리

21.5.1 BI 플랫폼용 성능 계측

BI 플랫폼 성능 계측 측정을 위한 SAP Solution Manager의 일부로서 CA Wily Introscope를 사용할 수 있습니다. 플랫폼을 설치할 때 배포를 위해 다음 리소스가 제공됩니다.

- Introscope 에이전트: Introscope 에이전트는 BI 플랫폼 Java 백 엔드 서버에서 성능 메트릭을 수집합니다. 에이전트는 주변 컴퓨팅 환경에서도 정보를 수집합니다. 그런 다음 이런 메트릭을 Enterprise Manager에 보고합니다.
- 계측 프로세스를 용이하게 하기 위해 제공되는 파일입니다. 한 파일 집합은 비 Java 서버의 계측을 위해 제공되고, 다른 파일 집합은 Java 서버의 계측을 위해 제공됩니다, SAP Solution Manager 쪽에 EM(Enterprise Manager) 구성 요소가 필요합니다. EM은 응용 프로그램 환경에서 수집된 모든 Introscope 성능 데이터 및 메트릭을 위한 중앙 리포지토리의 역할을 합니다. EM은 성능 데이터를 처리하고 사용자가 이를 프로덕션 모니터링 및 진단에 사용할 수 있게 합니다.

21.5.2 BI 플랫폼용 성능 계측 설정

BI 플랫폼 백 엔드 서버에서 실행 중인 워크플로에 대한 성능 계측을 설정하는 방법에는 두 가지가 있습니다.

1. 설치 중에 BI 플랫폼에 대한 설정을 하는 방법. SMD Agent에 대한 호스트 이름과 수신 포트를 알아야 합니다. 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 설치 가이드를 참조하십시오. 이 옵션을 선택하면 모니터링한 시스템 배포를 마친 후 계측이 기본적으로 실행됩니다.
2. BI 플랫폼 설치 후, 중앙 관리 콘솔(CMC)의 노드 속성에 있는 자리 표시자를 통해 SMD Agent에 대한 구성 정보를 제공할 수 있습니다.

참고:

비Java 서버에서 워크플로를 계측하려면 SMD Agent(DIAGNOSTICS.AGENT)가 설치되어 있어야 합니다.

관련 항목

- 762 페이지에서 [SMD 에이전트 작업](#)"

21.5.2.1 계측을 위한 노드 구성

BI 플랫폼 설치 설정 중 SMD Agent 및 Enterprise Manager에 대한 구성 정보를 제공하지 않은 경우에는 다음 지시에 따르십시오.

1. CMC의 서버 영역으로 이동합니다.
2. 탐색 창에서 노드를 클릭합니다.
사용 가능한 모든 노드가 표시됩니다.
3. 계측을 수행할 노드를 마우스 오른쪽 단추로 클릭하고 자리 표시자를 선택합니다.
자리 표시자 대화 상자가 표시됩니다.
4. 다음 자리 표시자에 대한 값을 수정합니다.

자리 표시자	설명
%IntroscopeAgentEnable-Instrumentation%	Java 서버에서 계측을 사용하거나 사용하지 않습니다. 설치 설정 중 Enterprise Manager에 대한 구성 세부 정보를 제공한 경우 사용으로 설정됩니다. 계측을 사용하려면 true로 설정합니다.
%IntroscopeAgentEnterpriseManagerHost%	Enterprise Manager가 설치되어 있는 컴퓨터의 호스트 이름입니다.
%IntroscopeAgentEnterpriseManagerPort%	Enterprise Manager가 사용하는 수신 포트입니다.
%IntroscopeAgentEnterpriseManagerTransport%	Enterprise Manager가 사용하는 통신 프로토콜입니다. 지원되는 프로토콜에는 TCP, SSL, HTTP Tunnel 및 HTTPS가 포함됩니다.

자리 표시자	설명
%NCSInstrumentLevelThreshold%	비 Java 서버의 계측 수준을 설정하는 데 사용됩니다. 계측을 해제하려면 0으로 설정합니다. 계측을 활성화하려면 0을 초과하는 값으로 설정합니다.
%SMDAgentHost%	SMD Agent(DIAGNOSTICS.AGENT)가 설치되어 있는 컴퓨터의 호스트 이름입니다.
%SMDAgentPort%	SMD 에이전트에서 사용하는 수신 포트입니다.

5. 저장 후 닫기를 클릭합니다.

6. 노드를 다시 시작합니다.

노드가 다시 시작된 후, 제공되는 새 값은 병합된 모든 서버로 전파됩니다.

21.5.3 Web Tier를 위한 성능 계측

BI 플랫폼에는 Web Tier 구성 요소를 위한 계측 데이터가 포함되지 않습니다.

21.5.4 계측 로그 파일

BI 플랫폼 배포가 계측을 실행하도록 구성된 후, 메시지가 특정 위치에 로그됩니다. 로그 파일 확인은 계측 상태를 확인하는 한 가지 방법입니다.

Java 백 엔드 서버에서 계측하는 경우, 로그 파일은 <INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/wily/logs 폴더에 위치합니다. 각각의 Java 프로세스에 대해 별도의 .log 파일이 만들어 집니다. 이 폴더에는 계측을 위해 로드된 메서드를 지정하는 AutoProbe.log 파일도 포함됩니다.

비 Java 백 엔드 서버에서 계측하는 경우, 로그 파일의 위치는 <INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/logging/ 디렉터리입니다. Unix에서는 이 파일이 <sap_bobj>WloggingW 디렉터리에 있습니다. 비 Java 서버에 대한 계측 관련 로그 파일은 .trc 파일로 저장됩니다.

웹 응용 프로그램 서버에서 계측하는 경우, 로그 파일의 위치는 <INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/wily/webapp/logs 디렉터리입니다. 이 폴더에는 Introscope.log와 Autoprobe.log 라는 두 가지 유형의 로그 파일이 생성됩니다.

21.6 SAP Passport로 추적

추적 메커니즘은 BI 플랫폼 구성 요소(예: 서버 및 웹 응용 프로그램)를 추적하는 것 이외에도 특정 작업의 추적을 지원할 수 있습니다. 중단 간 추적 분석은 단일 트랜잭션의 성능을 분석합니다. 특정 작업에 대한 추적 정보를 모두 통합하면 SAP 지원 담당자가 다른 작업과 관련된 정보를 추적할 필요 없이 모든 추적 데이터를 확인할 수 있습니다.

SAP Passport

BI 플랫폼의 중단 간 추적을 지원하는 메커니즘은 SAP Passport라는 도구입니다. SAP Passport 클라이언트 도구는 특정 워크플로우에 대한 모든 HTTP 요청에 고유 식별자를 주입합니다. 그러면 이 식별자가 워크플로우에 사용되는 모든 서버에 전달됩니다. SAP 지원 담당자는 이 고유 식별자를 사용하여 워크플로우에 대한 중단 간 추적을 함께 수집할 수 있습니다.

참고:

추적 로그 수준이 SAP Passport 클라이언트 도구(SAPIEPlugin.exe)에 지정된 수준보다 높은 경우 CMC와 BO_trace.ini 구성 파일에 지정된 추적 로그 수준이 사용됩니다.

백 엔드 서버, 웹 응용 프로그램 및 웹 서비스에 대한 로그에서 Passport를 찾을 수 있습니다.

SAP Passport 클라이언트 도구는 BI 플랫폼의 일부로 설치되지 않습니다. 이 도구에 액세스하여 다운로드하려면 <http://service.sap.com/swdc>로 이동합니다.

장22 명령줄 관리

22.1 UNIX 스크립트

이 단원에서는 SAP BusinessObjects Business Intelligence 플랫폼의 UNIX 배포 버전에 포함되어 있는 각 관리 도구 및 스크립트에 대해 자세히 설명합니다. 이 단원의 내용은 주로 참조를 위한 것입니다. 이 가이드에서는 개념 및 구성 절차를 보다 자세하게 설명합니다.

SAP BusinessObjects Business Intelligence 플랫폼의 UNIX 배포 버전에는 Windows 버전의 중앙 구성 관리자(CCM)를 통해 사용할 수 있는 모든 구성 옵션을 제공하는 여러 가지 스크립트가 포함되어 있습니다. UNIX용 옵션을 제공하거나 사용자가 직접 스크립트를 작성하는 데 템플릿으로 사용할 수 있는 여러 가지 다른 스크립트도 포함되어 있습니다. 또한 SAP BusinessObjects Business Intelligence 플랫폼에서 사용하는 몇 가지 보조 스크립트도 있습니다. 여기에서는 각 스크립트와 해당 명령줄 옵션에 대해 설명합니다.

22.1.1 스크립트 유틸리티

이 단원에서는 UNIX에서 SAP BusinessObjects Business Intelligence 플랫폼을 사용하는 데 도움이 되는 관리 스크립트에 대해 설명합니다. 이 도움말의 나머지 부분에서는 이러한 스크립트를 사용하여 수행할 수 있는 각 작업에 대한 개념을 설명합니다. 이 참조 단원에서는 주요 명령줄 옵션과 해당 인수를 제공합니다.

22.1.1.1 ccm.sh

ccm.sh 스크립트는 설치 환경의 <SCRIPTDIR> 디렉터리에 설치됩니다. 이 스크립트는 CCM의 명령줄 버전을 제공합니다. 이 단원에서는 명령줄 옵션 및 몇 가지 예제를 보여줍니다.

참고:

- 대괄호([]) 안의 인수는 선택 요소입니다.
- Server Intelligence Agent의 정규화된 이름을 모르는 경우 ccm.config 파일에서 Command 속성을 찾아 -name 옵션 뒤에 나오는 값을 사용합니다.
- ccm.sh 스크립트는 SAP BusinessObjects Business Intelligence 플랫폼 설치를 수행한 사용자만 실행할 수 있습니다.
- 기타 인증 정보로 표시된 인수는 두 번째 표에 나와 있습니다.

CCM 옵션	유효한 인수	설명
-help	해당 없음	명령줄 도움말을 표시합니다.
-start	all 또는 sianame	각 Server Intelligence Agent를 프로세스로 시작합니다. all 옵션을 사용하면 다른 클러스터에 속하는 노드를 비롯하여, 컴퓨터에 있는 모든 노드가 시작됩니다.
-stop	all 또는 sianame	해당 프로세스 ID를 종료하여 각 Server Intelligence Agent를 중지합니다. all 옵션을 사용하면 다른 클러스터에 속하는 노드를 비롯하여, 컴퓨터에 있는 모든 노드가 시작됩니다.
-restart	all 또는 sianame	해당 프로세스 ID를 종료하여 각 Server Intelligence Agent를 중지한 다음 각 SIA를 시작합니다. all 옵션을 사용하면 다른 클러스터에 속하는 노드를 비롯하여, 컴퓨터에 있는 모든 노드가 시작됩니다.
-managedstart	<fully qualified server name>[기타 인증 정보]	서버를 시작합니다.

CCM 옵션	유효한 인수	설명
-managedstop	<fully qualified server name>[기타 인증 정보]	서버를 중지합니다.
-managedrestart	<fully qualified server name>[기타 인증 정보]	서버를 중지했다가 다시 시작합니다.
-managedforceterminate	<fully qualified server name>[기타 인증 정보]	현재 처리 중인 요청을 완료하지 않은 채 서버를 즉시 중지합니다.
-enable	<fully qualified server name>[기타 인증 정보]	시작된 서버를 활성화하여 시스템에 등록하고 적절한 포트에서 수신을 시작하도록 합니다. 정규화된 형식의 서버 이름을 사용합니다.
-disable	<fully qualified server name>[기타 인증 정보]	서버를 비활성화하여 BusinessObjects Business Intelligence 플랫폼 요청에 대한 응답을 중지하도록 합니다. 프로세스로 시작된 서버의 상태는 계속 유지합니다. 정규화된 형식의 서버 이름을 사용합니다.
-display	[기타 인증 정보]	서버 이름, 호스트 이름, 프로세스 ID, 설명, 서버가 실행 중인지 여부 및 서버의 활성화 여부를 비롯한 클러스터에 있는 모든 서버의 현재 상태를 보고합니다.

다음 표에는 [기타 인증 정보]로 표시된 인수를 구성하는 옵션에 대한 설명이 나와 있습니다.

참고:

보안 개선을 위해 Enterprise 인증을 사용하는 계정의 자격 증명을 항상 제공해야 합니다. 다른 유형의 인증은 지원되지 않습니다.

인증 옵션	유효한 인수	설명
-cms	cmsname:port#	로그온하려는 CMS를 지정합니다. 이 값을 지정하지 않으면 CCM이 로컬 컴퓨터의 기본 포트(6400)로 기본 설정됩니다.
-username	username	BusinessObjects Business Intelligence 플랫폼에 대한 관리 권한을 부여하는 계정을 지정합니다. 이 값을 지정하지 않으면 기본 Administrator 계정이 사용됩니다.
-password	password	해당 암호를 지정합니다. 이 값을 지정하지 않으면 빈 암호가 사용됩니다. 참고: -password 인수를 지정하려면 -username 인수도 지정해야 합니다.

CCM은 ccm.config 파일의 시작 문자열과 기타 구성 값을 읽습니다.

관련 항목

- 771 페이지에서 [ccm.config](#)"

22.1.1.1.1 예

다음 두 명령은 모든 SAP BusinessObjects Business Intelligence 플랫폼 서버를 시작하여 활성화합니다. 중앙 관리 서버(CMS)는 로컬 컴퓨터의 기본 포트(6400)에서 시작됩니다.

```
ccm.sh -start all
ccm.sh -enable all
```

다음 두 명령은 모든 SAP BusinessObjects Business Intelligence Platform 서버를 시작하여 활성화합니다. CMS는 기본 포트 대신 포트 6701에서 시작됩니다.

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701
```

다음 두 명령은 SysAdmin이라는 지정된 관리 계정을 사용하여 모든 SAP BusinessObjects Business Intelligence 플랫폼 서버를 시작하고 활성화합니다.

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

다음 명령은 지정된 관리 계정을 사용하여 로그인한 다음 두 번째 컴퓨터에서 실행 중인 적응형 작업 서버를 비활성화합니다.

```
ccm.sh -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

22.1.1.1.2 ccm.config

이 구성 파일은 사용자가 해당 명령을 실행할 때 CCM에 사용되는 시작 문자열과 기타 값을 정의합니다. 이 파일은 CCM 자체 및 기타 SAP BusinessObjects Business Intelligence 플랫폼 스크립트 유틸리티를 통해 관리됩니다. 이 파일은 일반적으로 Server Intelligence Agent의 명령줄을 수정해야 하는 경우에만 편집합니다.

관련 항목

- 779 페이지에서 [명령줄 개요](#)

22.1.1.2 cmsdbsetup.sh

cmsdbsetup.sh 스크립트는 설치 환경의 sap_bobj 디렉터리에 설치되며, 다음과 같은 작업을 수행할 수 있는 텍스트 기반의 프로그램을 제공합니다.

- CMS 시스템 데이터베이스 구성
- CMS 시스템 데이터베이스 다시 초기화
- 다른 데이터 소스에서 데이터 복사
- 클러스터 키 변경
- 클러스터 이름 변경

참고:

이 스크립트를 실행하기 전에 현재 CMS 시스템 데이터베이스와 입력 및 출력 파일 리포지토리의 콘텐츠를 백업하십시오. 자세한 내용은 시스템 백업 및 복원을 참조하십시오. 또한 CMS 클러스터 및 CMS 데이터베이스 구성에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드의 서버 유지 관리 장에서 중앙 관리 서버 클러스터링을 확인하십시오.

스크립트에서 SIA(Server Intelligence Agent)의 이름을 묻습니다. SIA의 이름을 확인하려면 SIA의 Command 속성을 살펴 봅니다. SIA의 현재 이름은 -nodename 옵션 뒤에 나옵니다.

관련 항목

- 372 페이지에서 [중앙 관리 서버 클러스터링](#)"
- 469 페이지에서 [시스템 백업 및 복원](#)"

22.1.1.3 configpatch.sh

configpatch.sh 스크립트는 설치 환경의 sap_bobj/enterprise/generic 디렉터리에 설치됩니다. configpatch.sh 스크립트는 시스템 구성 값의 업데이트가 필요한 패치를 설치하는 경우에 사용됩니다. 패치를 설치한 후 적절한 .cf 파일 이름을 인수로 사용하여 configpatch.sh를 실행합니다. BusinessObjects Business Intelligence 플랫폼 패치에 들어 있는 readme.txt 파일에는 configpatch.sh를 실행할 시기와 사용할 .cf 파일의 이름이 나와 있습니다.

22.1.1.4 serverconfig.sh

serverconfig.sh 스크립트는 설치 환경의 sap_bobj 디렉터리에 설치되며, 다음과 같은 작업을 수행할 수 있는 텍스트 기반의 프로그램을 제공합니다.

- 노드 추가
- 노드 삭제
- 노드 수정
- 노드 이동
- 서버 구성 백업
- 서버 구성 복원
- 노드 나열

22.1.1.4.1 UNIX에서 노드 추가/삭제/수정/표시

1. 설치 환경의 <SCRIPTDIR> 디렉터리로 이동합니다.
2. 다음 명령을 실행합니다.

```
./serverconfig.sh
```

스크립트에서 다음과 같이 옵션 목록을 표시합니다.

- 1 - Server Intelligence Agent 추가
 - 2 - Server Intelligence Agent 삭제
 - 3 - Server Intelligence Agent 수정
 - 4 - config 파일에 있는 모든 Server Intelligence Agent 나열
3. 수행하려는 작업의 번호를 입력합니다.
 4. 서버를 추가, 삭제 또는 수정하는 경우 필요한 추가 정보를 스크립트에 제공합니다.

팁:

이 스크립트를 실행하면 CMS의 이름을 입력하라는 메시지가 표시됩니다. 기본적으로 CMS 이름은 hostname.cms입니다. 즉 MACHINE01이라는 컴퓨터에 설치된 CMS의 기본 이름은 MACHINE01.cms입니다. 이 스크립트에 호스트 이름을 입력하여 CMS(또는 임의의 다른 서버)의 이름을 확인하고, ccm.config의 내용을 표시하고, 서버의 시작 문자열을 조회할 수도 있습니다. 서버의 현재 이름은 -name 옵션 뒤에 표시됩니다.

22.1.2 스크립트 템플릿

다음 스크립트는 주로 사용자가 직접 자동화 스크립트를 만드는 데 기반으로 사용할 수 있는 템플릿으로 사용됩니다.

22.1.2.1 startservers

startservers 스크립트는 설치 환경의 <SCRIPTDIR> 디렉터리에 설치됩니다. 이 스크립트는 사용자 고유의 스크립트에 대한 템플릿으로 사용할 수 있습니다. 이 스크립트는 일련의 CCM 명령을 실행하여 SAP BusinessObjects Business Intelligence 플랫폼 서버를 시작하는 스크립트를 직접 설정하는 방법을 보여 주는 예제를 제공합니다. 서버에 사용할 CCM 명령을 작성하는 데 대한 자세한 내용은 767 페이지에서 ["ccm.sh"](#)를 참조하십시오.

22.1.2.2 stopservers

stopservers 스크립트는 설치 환경의 <SCRIPTDIR> 디렉터리에 설치됩니다. 이 스크립트는 사용자 고유의 스크립트에 대한 템플릿으로 사용할 수 있습니다. 이 스크립트는 일련의 CCM 명령을 실행하여 SAP BusinessObjects Business Intelligence 플랫폼 서버를 중지하는 스크립트를 직접 설정하는 방법을 보여 주는 예제를 제공합니다. 서버에 사용할 CCM 명령을 작성하는 데 대한 자세한 내용은 767 페이지에서 ["ccm.sh"](#)를 참조하십시오.

22.1.3 SAP BusinessObjects Business Intelligence 플랫폼에서 사용하는 스크립트

이러한 보조 스크립트는 일반적으로 주요 SAP BusinessObjects Business Intelligence 플랫폼 스크립트 유틸리티를 실행할 때 백그라운드로 실행됩니다. 즉 이 스크립트는 사용자가 직접 실행할 필요가 없습니다.

22.1.3.1 bobjrestart.sh

이 스크립트는 SAP BusinessObjects Business Intelligence 플랫폼 서버 구성 요소를 시작할 때 CCM을 통해 내부적으로 실행됩니다. 정상적인 종료 코드를 반환하지 않고 서버 프로세스가 갑자기

종료되면 이 스크립트가 새 서버 프로세스를 종료 시점에서 자동으로 다시 시작합니다. 이 스크립트는 직접 실행하지 마십시오.

22.1.3.2 env.sh

env.sh 스크립트는 설치 환경의 sap_bobj/setup 디렉터리에 설치됩니다. 이 스크립트는 다른 일부 스크립트에 필요한 SAP BusinessObjects Business Intelligence 플랫폼 환경 변수를 설정합니다. SAP BusinessObjects Business Intelligence 플랫폼 스크립트에서는 필요에 따라 env.sh를 실행합니다. UNIX에서 SAP BusinessObjects Business Intelligence 플랫폼을 설치하는 경우 시작 시 이 스크립트를 참조하도록 Java 응용 프로그램 서버를 구성해야 합니다. 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 설치 가이드를 참조하십시오.

22.1.3.3 env-locale.sh

env-locale.sh 스크립트는 서로 다른 인코딩 형식(예: UTF8, EUC 또는 Shift-JIS) 사이에 스크립트 언어 문자열을 변환하는 데 사용됩니다. 이 스크립트는 필요에 따라 env.sh에 의해 실행됩니다.

22.1.3.4 initlaunch.sh

initlaunch.sh 스크립트는 env.sh를 실행하여 SAP BusinessObjects Business Intelligence 플랫폼 환경 변수를 설정한 다음 사용자가 스크립트에 명령줄 인수로 추가한 명령을 실행합니다. 이 스크립트는 주로 SAP Business Objects에서 디버깅 도구로 사용하기 위한 것입니다.

22.1.3.5 setup.sh

setup.sh 스크립트는 설치 환경의 루트 디렉터리에 설치됩니다. 이 스크립트는 SAP BusinessObjects Business Intelligence 플랫폼 설치 환경을 설정하는 데 사용할 수 있는 텍스트 기반의 프로그램을 제공합니다. 이 스크립트는 SAP BusinessObjects Business Intelligence 플랫폼을 설치할 때 자동으로 실행됩니다. 이 스크립트에서는 SAP BusinessObjects Business Intelligence 플랫폼을 처음 설치하는 데 필요한 정보를 입력하라는 메시지를 표시합니다.

SAP BusinessObjects Business Intelligence 플랫폼을 설치할 때 설치 스크립트의 메시지에 따라 작업하는 방법은 SAP BusinessObjects Business Intelligence 플랫폼 설치 가이드를 참조하십시오.

22.1.3.6 setupinit.sh

setupinit.sh 스크립트는 시스템 설치를 수행할 때 설치 환경의 /sap_bobj/init 디렉터리에 설치됩니다. 이 스크립트는 자동 시작을 위해 실행 제어 스크립트를 사용자의 rc# 디렉터리에 복사합니다. 시스템 설치를 실행하면 setup.sh 스크립트가 완료된 다음 이 스크립트를 실행하라는 메시지가 표시됩니다.

참고:

이 스크립트를 실행하려면 루트 권한이 있어야 합니다.

22.2 Windows 스크립트

이 단원에서는 SAP BusinessObjects Business Intelligence 플랫폼의 Windows 배포 버전에 포함되어 있는 각 관리 도구 및 스크립트에 대해 자세히 설명합니다. 이 단원의 내용은 주로 참조를 위한 것입니다. 이 가이드에서는 개념 및 구성 절차를 보다 자세하게 설명합니다.

SAP BusinessObjects Business Intelligence 플랫폼의 Windows 배포에는 중앙 구성 관리자(CCM)의 Windows 버전이 포함됩니다. GUI와의 상호 작용 외에도, 서버 관리를 위한 옵션으로 명령줄에서 CCM 실행 파일을 실행하도록 선택할 수 있습니다.

22.2.1 ccm.exe

ccm.exe 실행 파일은 설치 환경의 <INSTALLDIR>WSAP BusinessObjects Business Intelligence 플랫폼 4.0\win64_x64 디렉터리에 설치됩니다. 명령줄에서 직접 실행 파일을 실행하여 특정 작업을 수행할 수 있습니다. 이 단원에서는 명령줄 옵션 및 몇 가지 예제를 보여줍니다.

참고:

- SIA(Server Intelligence Agent)와 중앙 관리 서버(CMS)를 실행한 후 ccm.exe의 명령줄 옵션을 사용하여 개별 서버와 상호 작용해야 합니다.
- 대괄호([]) 안의 인수는 선택 요소입니다.
- 기타 인증 정보로 표시된 인수는 두 번째 표에 나와 있습니다.

CCM 옵션	유효한 인수	설명
-help	해당 없음	명령줄 도움말을 표시합니다.
-managedstart	all 또는 <fully qualified server name>[기타 인증 정보]	서버를 시작합니다.
-managedstop	all 또는 <fully qualified server name>[기타 인증 정보]	서버를 중지합니다.
-managedrestart	all 또는 <fully qualified server name>[기타 인증 정보]	서버를 중지했다가 다시 시작합니다.
-managedforceterminate	all 또는 <fully qualified server name>[기타 인증 정보]	현재 처리 중인 요청을 완료하지 않은 채 서버를 즉시 중지합니다.
-enable	all 또는 <fully qualified server name>[기타 인증 정보]	시작된 서버를 활성화하여 시스템에 등록하고 적절한 포트에서 수신을 시작하도록 합니다.
-disable	all 또는 <fully qualified server name>[기타 인증 정보]	서버를 비활성화하여 BusinessObjects Business Intelligence Platform 요청에 대한 응답을 중지하도록 합니다. 프로세스로 시작된 서버의 상태는 계속 유지합니다.

CCM 옵션	유효한 인수	설명
-display	[기타 인증 정보]	서버 이름, 호스트 이름, 프로세스 ID, 설명, 서버가 실행 중인지 여부 및 서버의 활성화 여부를 비롯한 클러스터에 있는 모든 서버의 현재 상태를 보고합니다.

다음 표에는 [기타 인증 정보]로 표시된 인수를 구성하는 옵션에 대한 설명이 나와 있습니다.

참고:

Enterprise 인증을 사용하는 계정의 자격 증명을 항상 제공해야 합니다.

인증 옵션	유효한 인수	설명
-cms	cmsname:port#	로그온하려는 CMS를 지정합니다. 이 값을 지정하지 않으면 CCM이 로컬 컴퓨터의 기본 포트(6400)로 기본 설정됩니다.
-username	username	SAP BusinessObjects Business Intelligence 플랫폼에 대한 관리 권한을 부여하는 계정을 지정합니다. 이 값을 지정하지 않으면 기본 Administrator 계정이 사용됩니다.
-password	password	해당 암호를 지정합니다. 이 값을 지정하지 않으면 빈 암호가 사용됩니다. 참고: -password 인수를 지정하려면 -username 인수도 지정해야 합니다.
-authentication	인증 형식	인증 형식을 지정합니다. secEnterprise만 지원됩니다.

CCM은 ccm.config 파일의 시작 문자열과 기타 구성 값을 읽습니다.

관련 항목

- 771 페이지에서 [ccm.config](#)"

22.2.1.1 예

다음 예에서는 SIA(Server Intelligence Agent)와 중앙 관리 서버(CMS)가 시작되어 실행 중이라고 가정합니다. ccm.exe의 명령줄 옵션을 사용하여 개별 서버와 상호 작용하기 전에, 다음 Windows 명령을 사용하여 SIA 서비스를 시작할 수 있습니다.

```
net start "Server Intelligence Agent (MACHINE01)"
```

net stop "Server Intelligence Agent (MACHINE01)"를 사용하여 SIA를 중지할 수도 있습니다.

이 명령을 실행하면 모든 SAP BusinessObjects Business Intelligence 플랫폼 서버가 시작됩니다.

```
ccm.exe -managedstart all
```

다음 명령은 적응형 작업 서버를 시작합니다. CMS는 기본 포트 대신 포트 6701에서 시작됩니다.

```
ccm.exe -managedstart MACHINE01.AdaptiveJobServer -cms MACHINE01:6701
```

다음 명령은 SysAdmin이라는 이름으로 지정된 관리 계정으로 적응형 작업 서버를 사용합니다.

```
ccm.exe -enable MACHINE01.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

다음 명령은 지정된 관리 계정을 사용하여 로그인한 다음 두 번째 컴퓨터에서 실행 중인 적응형 작업 서버를 비활성화합니다.

```
ccm.exe -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

22.3 서버 명령줄

22.3.1 명령줄 개요

이 단원에는 각 SAP BusinessObjects Business Intelligence 플랫폼 서버의 동작을 제어하는 명령줄 옵션이 나열되어 있습니다.

중앙 관리 콘솔(CMC)을 통해 서버를 시작하거나 구성하면 일반적인 옵션 및 값 집합이 포함된 기본 명령줄을 사용하여 서버를 시작되거나 다시 시작할 수 있습니다. 대부분의 경우 기본 명령줄은 직접 수정할 필요가 없습니다. 또한, CCM의 여러 가지 서버 구성 화면을 통해 대부분의 공통 설정을 조작할 수 있습니다. 이 단원에서 제공하는 각 서버별 지원 명령줄 옵션의 전체 목록은 참조를 위한 것입니다. SAP BusinessObjects Business Intelligence 플랫폼의 동작을 추가로 사용자 지정해야 하는 경우에는 각 서버의 명령줄을 직접 수정할 수 있습니다.

이 단원에서 대괄호([]) 안에 있는 값은 선택 사항입니다.

참고:

다음 표에는 지원되는 명령줄 옵션이 나열되어 있습니다. SAP BusinessObjects Business Intelligence 플랫폼 서버에서는 이러한 표에 나열되지 않은 다양한 내부 옵션을 사용합니다. 이런 내부 옵션을 수정하면 안 됩니다.

22.3.1.1 서버의 명령줄을 보거나 수정하려면

1. 중앙 관리 콘솔(CMC)을 사용하여 서버를 중지합니다.
2. 서버를 마우스 오른쪽 단추로 클릭하고 속성을 클릭합니다.
3. 속성 화면에서 서버에 대한 명령줄을 수정한 다음 저장 후 닫기를 클릭합니다.
4. 서버를 시작합니다.

22.3.2 모든 서버의 표준 옵션

별도로 표시하지 않은 경우 다음 명령줄 옵션은 모든 SAP BusinessObjects Business Intelligence 플랫폼 서버에 적용됩니다. 각 유형의 서버별 옵션에 대한 내용은 이 단원의 나머지 부분을 참조하십시오.

옵션	유효한 인수	동작
-requestPort	port	<p>서버가 수신 대기하는 포트를 지정합니다. 서버는 이 포트를 CMS에 등록합니다. 값이 지정되지 않은 경우 서버에서는 사용되지 않는 임의의 포트(> 1024)를 선택합니다.</p> <p>참고: 이 포트는 여러 서버에서 각기 다른 목적으로 사용됩니다. 이 값을 변경하기 전에 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드에서 기본 서버 포트 번호 변경에 대한 단원을 참조하십시오.</p>
-loggingPath	absolute path	로그 파일을 만들 경로를 지정합니다.

22.3.2.1 UNIX 신호 처리

UNIX의 경우 SAP BusinessObjects Business Intelligence 플랫폼 데몬은 다음과 같은 신호를 처리합니다.

- SIGTERM - 서버를 정상적으로 종료합니다(종료 코드 = 0).
- SIGSEGV, SIGBUS, SIGSYS, SIGFPE 및 SIGILL - 서버를 신속하게 종료합니다(종료 코드 = 1).

22.3.3 중앙 관리 서버

이 단원에서는 CMS에 관련된 명령줄 옵션을 설명합니다. Windows의 경우 기본 서버 경로는 <INSTALLDIR>WBBusinessObjects Enterprise XI 4.0\win64_x64\WCMS.exe입니다.

UNIX의 경우 기본 서버 경로는 <INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_cmsd입니다.

옵션	유효한 인수	동작
-threads	number	CMS에서 초기화하여 사용할 작업 스레드의 수를 지정합니다. 12에서 150 사이의 값을 지정할 수 있고, 기본값은 50으로 설정되어 있습니다.
-reinitializedb		CMS가 시스템 데이터베이스를 삭제하고 기본 시스템 개체만 사용하여 다시 만듭니다. 시스템 데이터베이스가 다시 만들어지면 데이터베이스에 있는 기존 데이터는 전부 손실됩니다.
-quit		-reinitializedb 옵션을 처리한 후 CMS가 종료됩니다.
-receiverPool	number	클라이언트 요청을 받기 위해 CMS에서 만드는 스레드의 수를 지정합니다. 클라이언트는 다른 Business Objects 서버, 보고서 게시 마법사, Crystal Reports 또는 사용자가 만든 사용자 지정 클라이언트 응용 프로그램일 수 있습니다. 기본값은 5입니다. 많은 수의 클라이언트와 연결되는 사용자 지정 응용 프로그램을 만드는 경우가 아니면 일반적으로 이 값을 늘릴 필요가 없습니다.

옵션	유효한 인수	동작
-maxobjectsincache	number	CMS에서 메모리 캐시에 저장하는 개체의 최대 개수를 지정합니다. 개체의 수를 늘리면 필요한 데이터베이스 호출 수가 줄어들고 CMS 성능이 크게 향상됩니다. 그러나 메모리에 너무 많은 개체를 넣으면 CMS에서 쿼리를 처리하는 데 필요한 메모리가 부족해질 수도 있습니다. 상한값은 100000입니다.
-ndbqthreads	number	데이터베이스에 요청을 보내는 CMS 작업자 스레드의 수를 지정합니다. 각 스레드마다 데이터베이스에 연결되므로 데이터베이스 용량을 초과하지 않도록 주의해야 합니다. 대부분의 경우 최대값을 20으로 설정합니다.
-oobthreads	number	클러스터에 CMS 클러스터 멤버가 9개 이상 포함된 경우 각 CMS에 대한 명령줄에 이 옵션이 포함되어야 합니다. 클러스터의 CMS 서비스 수를 지정합니다. 이 옵션을 사용해야 클러스터가 과부하를 견딜 수 있습니다.
-AuditeeTimeSyncInterval	minutes	시간 동기화 이벤트가 발생하는 간격을 지정합니다. -AuditeeTimeSyncInterval에서 지정한 간격에 따라 CMS의 시스템 시간이 감사 대상 서버에 브로드캐스팅됩니다. 감사되는 서버는 내부 시계를 CMS 시간과 비교한 다음 이후의 모든 감사 레코드에 적용되는 타임스탬프를 조정하여 이러한 레코드의 시간이 CMS 시간과 동기화되도록 만듭니다. 기본 간격은 60분입니다. 최대값은 1일(1440분)입니다. 최소값은 15분입니다. 간격을 0으로 설정하면 시간 동기화가 해제됩니다.

관련 항목

- 780 페이지에서 [모든 서버의 표준 옵션](#)"

22.3.4 Crystal Reports 처리 서버 및 Crystal Reports 캐시 서버

Crystal Reports 처리 서버와 Crystal Reports 캐시 서버는 명령줄에서 매우 유사한 방식으로 제어됩니다. 서버를 처리 서버로 시작할지, 캐시 서버로 시작할지 또는 두 서버 모두의 역할로 시작할지를 명령줄 옵션에서 지정합니다. 한 서버 유형에만 적용되는 옵션은 아래에 표시되어 있습니다.

Windows에서 이 두 서버의 기본 경로는 다음과 같습니다.

- <INSTALLDIR>WSAP BusinessObjects Business Intelligence platform 4.0
Wwin64_x64Wcacheserver.exe
- <INSTALLDIR>WBusinessObjects Business Intelligence platform XI
4.0Wwin64_x64Wpageserver.exe

UNIX에서 이 두 서버의 기본 경로는 다음과 같습니다.

- <INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/boe_cachesd.
- <INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/boe_procd.

옵션	유효한 인수	동작
-cache		캐시 서버 기능을 활성화합니다.
-deleteCache		서버를 시작하고 중지할 때마다 캐시 디렉터리를 삭제합니다.
-report_ProcessExtPath	absolutepath	처리 확장을 위한 기본 디렉터리를 지정합니다. 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드를 참조하십시오.

관련 항목

- 780 페이지에서 [모든 서버의 표준 옵션](#)"

22.3.5 Dashboard Design 처리 서버와 Dashboard Design 캐시 서버

Dashboard Design 처리 서버와 Dashboard Design 캐시 서버는 명령줄에서 매우 유사한 방식으로 제어됩니다. 서버를 처리 서버로 시작할지, 캐시 서버로 시작할지 또는 두 서버 모두의 역할로 시작할지를 명령줄 옵션에서 지정합니다. 한 서버 유형에만 적용되는 옵션은 아래에 표시되어 있습니다.

Windows에서 이 두 서버의 기본 경로는 다음과 같습니다.

- <INSTALLDIR>WSAP BusinessObjectsWSAP BusinessObjects Business Intelligence platform 4.0\Win64_x64\xccache.exe
- <INSTALLDIR>WSAP BusinessObjectsWSAP BusinessObjects Business Intelligence platform 4.0\Win64_x64\xcproc.exe

UNIX에서 이 두 서버의 기본 경로는 다음과 같습니다.

- <INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>_64/boe_xccached.
- <INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>_64/xcprocd.

옵션	유효한 인수	동작
-cache		캐시 서버 기능을 활성화합니다.
-dir	absolutepath	캐시 서버의 캐시 디렉터리 및 처리 서버의 임시 디렉터리를 지정합니다. 작성되는 디렉터리는 absolutepath/cache 및 absolutepath/temp입니다.
-deleteCache		서버를 시작하고 중지할 때마다 캐시 디렉터리를 삭제합니다.
-psdir	absolutepath	처리 서버의 임시 디렉터리를 지정합니다. 이 옵션은 -dir보다 우선합니다.
-refresh	minutes	캐시된 페이지를 분 단위로 지정한 시간 동안 공유합니다.

옵션	유효한 인수	동작
-auditMaxEventsPerFile	number	캐시 서버에서 감사 로그 파일에 기록되는 감사 동작의 최대 수를 지정합니다. 기본값은 500입니다. 레코드의 최대 수를 초과하면 서버에서 새로운 로그 파일을 엽니다.

관련 항목

- 780 페이지에서 [모든 서버의 표준 옵션](#)"

22.3.6 작업 서버

이 단원에서는 적응형 작업 서버에만 해당하는 명령줄 옵션에 대해 설명합니다.

Windows의 경우 기본 서버 경로는 <INSTALLDIR>WSAP BusinessObjects Business Intelligence platform 4.0Wwin64_x64WJobServer.exe입니다.

UNIX의 경우 기본 서버 경로는 <INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/boe_reportjobsd입니다.

옵션	유효한 인수	동작
-dir	absolutepath	작업 서버의 데이터 디렉터리를 지정합니다.
-maxJobs	number	서버에서 처리할 수 있는 동시 작업의 최대 수를 설정합니다. 기본값은 5입니다.

옵션	유효한 인수	동작
-requestJSChildPorts	lowerbound-upperbound	방화벽 환경에서 하위 프로세스가 사용할 포트의 범위를 지정합니다. 예를 들어, 6800-6805를 설정하면 하위 프로세스가 여섯 개의 포트만 사용하도록 제한됩니다. 참고: 이 옵션을 적용하려면 -requestPort 설정도 함께 지정해야 합니다.
-report_ProcessExtPath	absolutepath	처리 확장을 위한 기본 디렉터리를 지정합니다. 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드를 참조하십시오.

관련 항목

- 780 페이지에서 [모든 서버의 표준 옵션](#)"

22.3.7 적응형 처리 서버

적응형 처리 서버에서는 SAP JVM(SAP Java Virtual Machine)용으로 정의된 매개 변수를 사용합니다. 자세한 내용은 SAP JVM 설명서를 참조하십시오.

22.3.8 Report Application Server

이 단원에서는 Report Application Server에 관련된 명령줄 옵션을 설명합니다.

Windows의 경우 기본 서버 경로는 <INSTALLDIR>WSAP BusinessObjects Business Intelligence platform 4.0Wwin32_x86Wcrystalras.exe입니다.

UNIX의 경우 기본 서버 경로는 <INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/ras/boe_crystalrasd입니다.

옵션	유효한 인수	동작
-ipport	port	SAP BusinessObjects Business Intelligence 플랫폼 외부에서 독립 실행형 모드로 실행될 때 TCP/IP 요청을 받기 위한 포트 번호를 지정합니다.
-report_ProcessExtPath	absolutepath	처리 확장을 위한 기본 디렉터리를 지정합니다. 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드를 참조하십시오.

옵션	유효한 인수	동작
-ProcessAffinityMask	mask	<p>RAS가 다중 프로세서 컴퓨터에서 실행되는 경우 정확히 어떠한 CPU를 사용할지를 마스크를 사용하여 지정합니다.</p> <p>마스크는 0xffffffff 형식입니다. 여기서 각 f는 프로세서를 나타내고, 프로세서의 목록은 오른쪽에서 왼쪽으로 읽습니다. 즉, 마지막 f가 첫째 프로세서를 나타냅니다. 각 f를 0(CPU 사용이 허용되지 않음) 또는 1(CPU 사용이 허용됨)로 대체합니다.</p> <p>예를 들어, 4개의 프로세서를 가진 컴퓨터에서 RAS가 실행되고 있는 경우, 세 번째 및 네 번째 프로세서를 사용하려면 마스크 0x1100을 사용합니다. 두 번째 및 세 번째 프로세서를 사용하려면 0x0110을 사용합니다.</p> <p>참고:</p> <ul style="list-style-type: none"> RAS는 이 문자열에서 첫 번째 허용한 프로세서부터 시작하여 라이선스에서 지정한 최대 개수까지 프로세서를 사용합니다. 두 개의 프로세서에 대한 라이선스가 있는 경우 0x1110의 결과는 0x0110의 경우와 동일합니다. 마스크의 기본값은 -1이며, 이는 0x1111을 지정한 것과 같습니다.

관련 항목

- 780 페이지에서 [모든 서버의 표준 옵션](#)

22.3.9 Web Intelligence 처리 서버

이 단원에서는 Web Intelligence 처리 서버에만 사용되는 명령줄 옵션을 설명합니다.

Windows의 경우 기본 서버 경로는 <INSTALLDIR>WSAP BusinessObjects Business Intelligence platform 4.0\win64_x64\WIReportServer.exe입니다.

UNIX의 경우 기본 서버 경로는 <INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/WIReport Server입니다.

옵션	유효한 인수	동작
-ConnectionTimeout Minutes	minutes	서버 제한 시간이 종료되기 전에 대기하는 분 수를 지정합니다.
-MaxConnections	number	서버에서 한 번에 허용되는 동시 연결의 최대 수를 지정합니다.
-DocExpressEnable		Web Intelligence 문서를 볼 때 문서를 캐싱합니다.
-DocExpressRealTime CachingEnable		Web Intelligence 문서를 실시간으로 캐싱합니다.
-DocExpressCache DurationMinutes	minutes	캐시에 내용이 저장되는 분 단위 시간을 지정합니다.
-DocExpressMaxCache SizeKB	kilobytes	문서 캐시의 크기를 지정합니다.
-EnableListOfValues Cache		값 목록을 사용자 세션별로 캐싱합니다.
-ListOfValuesBatchSize	number	값 목록 배치별로 반환할 수 있는 값의 최대 수를 지정합니다.

옵션	유효한 인수	동작
-UniverseMaxCacheSize	number	캐싱할 유니버스의 수를 지정합니다.
-WIDMaxCacheSize	number	캐시에 저장할 수 있는 Web Intelligence 문서의 최대 수를 지정합니다.

관련 항목

- 780 페이지에서 [모든 서버의 표준 옵션](#)"

22.3.10 입력 및 출력 파일 리포지토리 서버

이 단원에서는 입력 및 출력 파일 리포지토리 서버에 관련된 명령줄 옵션을 설명합니다.

Windows의 경우 기본 서버 경로는 <INSTALLDIR>WSAP BusinessObjects Business Intelligence platform 4.0\win64_x64\filesrv.exe입니다.

UNIX에서 이 두 서버를 제공하는 프로그램의 기본 경로는 다음과 같습니다.

- <INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_inputfilesd.
- <INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_outputfilesd.

옵션	유효한 인수	동작
-rootDir	absolutepath	<p>서버에서 관리하는 여러 하위 폴더와 파일에 대한 루트 디렉터리를 설정합니다. 파일 리포지토리 서버의 파일을 나타내는 데 사용되는 파일 경로는 이 루트 디렉터리를 기준으로 해석됩니다.</p> <p>참고: 모든 입력 파일 리포지토리 서버와 모든 출력 파일 리포지토리 서버는 각각 동일한 루트 디렉터리를 공유해야 합니다. 그렇지 않으면 인스턴스에 일관성이 없는 문제가 발생할 수 있습니다. 또한, 입력 루트 디렉터리는 출력 루트 디렉터리와 같지 않아야 합니다. RAID 배열 또는 대체 하드웨어 솔루션을 사용하여 루트 디렉터리를 복제하는 것이 좋습니다.</p>
-tempDir	absolutepath	<p>파일을 전송하기 위해 FRS가 사용하는 임시 디렉터리의 위치를 설정합니다. FRS 임시 디렉터리의 위치를 제어하려는 경우 또는 FRS가 생성한 기본 임시 디렉터리 이름의 길이가 파일 시스템 경로 제한을 초과하여 FRS를 시작할 수 없는 경우 이 명령줄 옵션을 사용합니다.</p> <p>참고: 이 옵션에 기존 디렉터리를 지정하지 마십시오. 지정한 디렉터리는 FRS를 시작할 때 비워지고 FRS를 종료할 때 제거됩니다. 기존 디렉터리를 사용하면 해당 디렉터리가 비워지고 제거됩니다.</p>
-maxidle	minutes	<p>유틸 세션을 정리하기 전에 대기할 시간을 분 단위로 지정합니다.</p>

관련 항목

- 780 페이지에서 [모든 서버의 표준 옵션](#)"

22.3.11 이벤트 서버

이 단원에서는 이벤트 서버에 관련된 명령줄 옵션을 설명합니다.

Windows의 경우 기본 서버 경로는 <INSTALLDIR>WSAP BusinessObjects Business Intelligence platform 4.0Wwin64_x64WEvtServer.exe입니다.

UNIX의 경우 기본 서버 경로는 <INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_eventsd입니다.

옵션	유효한 인수	동작
-poll	seconds	서버가 파일 이벤트를 확인하는 시간 간격을 초 단위로 지정합니다.
-cleanup	minutes	서버가 수신기 프록시를 정리하는 시간 간격을 분 단위로 지정합니다. 이 값은 두 번의 정리를 수행하는 데 걸리는 시간을 나타냅니다. 예를 들어, 이 값을 10으로 지정하면 프록시가 5분마다 정리됩니다.

관련 항목

- 780 페이지에서 [모든 서버의 표준 옵션](#)"

22.3.12 대시보드 및 대시보드 분석 서버

대시보드 및 대시보드 분석 서버에는 명령줄 관리를 위한 명령줄 전용 매개 변수가 없습니다.

장23 권한 부록

23.1 권한 부록 소개

이 권한 부록에서는 BI 플랫폼 시스템의 다양한 개체에 대해 설정할 수 있는 대부분의 권한 목록과 설명을 제공합니다. 또한, 개체를 대상으로 작업을 수행하기 위해 둘 이상의 권한이 필요할 경우에 어떤 권한이 추가로 필요한지 설명하고, 어떤 개체에 대해 그러한 권한이 있어야 하는지 설명합니다. 이 권한에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드의 권한 설정 장을 참조하십시오.

23.2 일반 권한

이 단원에서 설명하는 권한은 여러 개체 유형에 적용됩니다.

참고:

- 이러한 권한 대부분에는 그에 상응하는 소유자 권한이 있습니다. 소유자 권한은 권한 적용 여부를 확인하려는 개체의 소유자에게만 적용되는 권한입니다.
- 다음 권한은 예약 가능한 개체에만 적용됩니다.
 - 문서 실행 일정 설정 권한
 - 다른 사용자 대신 일정 설정 권한
 - 대상에 보내도록 일정 설정 권한
 - 문서 인스턴스 보기 권한
 - 인스턴스 삭제 권한
 - 문서 인스턴스 일시 중지 및 다시 시작 권한
 - 인스턴스 일정 변경 권한

권한	설명
개체 보기	개체와 그 속성을 볼 수 있도록 합니다. 개체에 대해 이 권한이 없으면 BI 플랫폼 시스템에서 개체가 숨겨집니다. 이 권한은 모든 작업에 필요한 기본 권한입니다.
폴더에 개체 추가	개체를 폴더에 추가할 수 있도록 합니다. 이 권한은 받은 파일함, 즐겨찾기 폴더 또는 개체 패키지와 같이 폴더처럼 동작하는 개체에도 적용됩니다.
개체 편집	개체 콘텐츠 및 개체와 폴더의 속성을 편집할 수 있도록 합니다.
개체에 대한 사용자 권한 수정	개체에 대한 보안 설정을 수정할 수 있도록 합니다.
개체에 대한 사용자 권한을 안전하게 수정합니다.	자신이 이미 개체에 대해 갖고 있는 권한이나 액세스 수준을 다른 사용자에게 부여할 수 있도록 합니다. 이를 위해서는 사용자와 개체 자체에 대해 이 권한이 있어야 합니다. 이 권한에 대한 자세한 내용은 SAP BusinessObjects Business Intelligence 플랫폼 관리자 가이드의 권한 설정 장을 참조하십시오.
작업을 처리할 서버 그룹 정의	개체를 처리할 때 사용할 서버 그룹을 지정할 수 있도록 합니다. 이 권한은 처리 서버를 지정할 수 있는 개체에만 적용됩니다. 서버 그룹을 지정하려면 개체에 대한 개체 편집 권한도 있어야 합니다.
개체 삭제	개체와 더불어 그 인스턴스를 삭제할 수 있도록 합니다.
다른 폴더에 개체 복사	CMS의 다른 폴더에 개체의 복사본을 만들 수 있도록 합니다. 이를 위해서는 대상 폴더에 대한 폴더에 개체 추가 권한도 있어야 합니다. 참고: 개체를 복사하는 경우 개체에 대한 명시적 보안은 복사되지 않습니다. 새 개체에는 대상 폴더의 보안 설정이 상속되지만 명시적 보안을 다시 설정해야 합니다.
내용 복제	연합 배포에서 다른 시스템으로 개체를 복제할 수 있도록 합니다.
문서 실행 일정 설정	개체를 예약할 수 있도록 합니다.
다른 사용자 대신 일정 설정	다른 사용자나 그룹에 대해 개체를 예약할 수 있도록 합니다. 개체를 예약한 대상 사용자나 그룹은 개체 인스턴스의 소유자가 됩니다. 다른 사용자나 그룹에 대해 개체를 예약하려면 다음 권한도 있어야 합니다. <ul style="list-style-type: none"> • 사용자나 그룹에 대한 권한 • 개체에 대한 문서 실행 일정 설정 권한

권한	설명
대상에 보내도록 일정 설정	<p>다음과 같은 작업을 수행할 수 있도록 합니다.</p> <ul style="list-style-type: none"> 기본 Enterprise 위치가 아닌 다른 대상에 보내도록 개체 예약 일정이 지정된 기본 대상 수정 <p>대상에 보내도록 개체를 예약하려면 다음 권한도 있어야 합니다.</p> <ul style="list-style-type: none"> 예약하려는 개체에 대한 문서 실행 일정 설정 권한 받는 사람의 받은 파일함에 대한 폴더에 개체 추가 권한(받은 파일함을 대상으로 예약하려는 경우) 예약하려는 개체에 대한 다른 폴더에 개체 복사 권한(복사본을 바로 가기 대신 받은 파일함 대상으로 보내려는 경우)
문서 인스턴스 보기	개체 인스턴스를 볼 수 있도록 합니다. 이 권한은 개체 인스턴스에 대해 수행하는 모든 작업에 필요한 기본 권한입니다.
인스턴스 삭제	개체 인스턴스만 삭제할 수 있도록 합니다. 개체 삭제 권한이 있으면 인스턴스를 삭제하는 데 이 권한이 필요하지 않습니다.
문서 인스턴스 일시 중지 및 다시 시작	실행 중인 개체 인스턴스를 일시 중지하거나 다시 시작할 수 있도록 합니다.
인스턴스 일정 변경	개체 인스턴스를 다시 예약할 수 있도록 합니다.

관련 항목

- 140 페이지에서 [소유자 권한](#)"
- 138 페이지에서 [개체에 대한 사용자 권한 수정 옵션 선택](#)"

23.3 특정 개체 유형에 대한 권한

23.3.1 폴더 권한

권한을 더 쉽게 관리하려면 폴더에 대한 권한을 설정하고 폴더에 포함된 각 항목이 폴더의 보안 설정을 상속하도록 하는 것이 좋습니다. 폴더 권한에는 다음과 같은 권한이 포함됩니다.

- 폴더 개체에 적용되는 일반 권한
- Crystal 보고서에 대한 보고서 데이터 인쇄 권한과 같이 폴더의 콘텐츠에 적용하기 위한 유형별 권한

관련 항목

- 120 페이지에서 [유형별 권한](#)

23.3.2 범주

이 단원에서 설명하는 권한은 공용 및 개인 범주의 컨텍스트에서 특정 의미를 갖는 권한입니다.

참고:

범주에 속하는 개체는 범주에 설정된 권한을 상속하지 않습니다.

권한	설명
폴더에 개체 추가	범주 내에 새 범주를 만들 수 있도록 합니다. 범주에 개체를 추가하는 데는 이 권한이 필요하지 않습니다.
개체 편집	<p>다음과 같은 작업을 수행할 수 있도록 합니다.</p> <ul style="list-style-type: none"> • 범주 속성 수정 • 범주를 다른 범주 아래로 이동하여 하위 범주로 만들기 • 범주에 개체 추가 • 범주에서 개체 제거 <p>범주를 다른 범주 아래로 이동하여 하위 범주로 만들려면 다음 권한도 있어야 합니다.</p> <ul style="list-style-type: none"> • 원래 범주에 대한 개체 삭제 권한 • 대상 범주에 대한 폴더에 개체 추가 권한
개체 삭제	범주를 삭제할 수 있도록 합니다.

23.3.3 메모

메모를 사용하면 토론 응용 프로그램을 사용하는 다른 개체에 대한 설명을 달 수 있습니다. 메모는 토론 스레드에서 함께 연결됩니다. 이러한 토론 스레드는 토론 대상인 개체의 자식 개체로 간주됩니다. 개체 수준이나 폴더 수준에서 권한을 설정하여 토론 스레드의 사용을 제어할 수 있습니다.

이 단원에서 설명하는 권한은 메모에만 적용됩니다.

권한	설명
토론 스레드 허용	<p>이 권한이 있으면 다음과 같은 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> 토론 스레드 시작 및 응답 토론 스레드에 대한 메모 보기 게시된 메모 수정 또는 삭제

23.3.4 Crystal 보고서

이 단원에서 설명하는 권한은 Crystal 보고서에만 적용됩니다.

참고:

이러한 권한은 Crystal 보고서가 BI 플랫폼 환경에 있을 때만 적용됩니다. Crystal 보고서를 로컬 디스크로 다운로드하면 이러한 권한이 적용되지 않습니다. 이와 같이 권한이 무효화되는 경우를 방지하려면 Crystal 보고서에 대해 개체와 연결된 파일 다운로드 권한을 거부하면 됩니다.

권한	설명
보고서 데이터 인쇄	보고서를 인쇄할 수 있도록 합니다.
보고서 데이터 새로 고침	보고서 데이터를 새로 고칠 수 있도록 합니다.
보고서 데이터 내보내기	Crystal Reports 뷰어를 사용하여 온라인으로 보고서를 보고 있을 때 보고서 데이터를 임의의 형식으로 내보낼 수 있도록 합니다. 보고서 데이터를 RPT 형식으로 내보내려면 개체와 연결된 파일 다운로드 권한도 있어야 합니다.
개체와 연결된 파일 다운로드	이 권한이 있으면 다음과 같은 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> • 보고서를 RPT 형식으로 내보내기 • Crystal Reports Designer에서 보고서 열기 • 외부 대상에 대해 RPT 형식으로 보고서 예약

23.3.5 Web Intelligence 문서

이 단원에서 설명하는 권한은 Web Intelligence 문서에만 적용됩니다.

권한	설명
값 목록 사용	값 목록을 사용할 수 있도록 합니다.
보고서 데이터 내보내기	문서 데이터를 Excel, PDF 및 CSV 형식으로 내보낼 수 있도록 합니다. 이 권한이 없는 경우 문서 데이터를 내보내려면 CSV로 저장, Excel로 저장 또는 PDF로 저장 권한이 있어야 합니다. 이러한 권한을 사용하면 문서를 지정된 형식으로만 내보낼 수 있습니다.
쿼리 스크립트 - 보기 사용(SQL, MDX...)	쿼리 스크립트(SQL 및 MDX)를 볼 수 있도록 합니다.
보고서 데이터 새로 고침	문서 데이터를 새로 고칠 수 있도록 합니다.
쿼리 편집	문서의 쿼리를 편집할 수 있도록 합니다.

권한	설명
값 목록 새로 고침	프롬프트를 만들거나 문서를 볼 때 프롬프트의 값 목록을 새로 고칠 수 있도록 합니다. 이를 위해서는 문서에 대한 값 목록 사용 권한도 있어야 합니다.
CSV로 저장	문서를 CSV 파일로만 내보낼 수 있도록 합니다. 이미 문서에 대한 보고서 데이터 내보내기 권한이 있으면 이 권한이 필요하지 않습니다.
Excel로 저장	문서를 Excel 파일로만 내보낼 수 있도록 합니다. 이미 문서에 대한 보고서 데이터 내보내기 권한이 있으면 이 권한이 필요하지 않습니다.
PDF로 저장	문서를 PDF 파일로만 내보낼 수 있도록 합니다. 이미 문서에 대한 보고서 데이터 내보내기 권한이 있으면 이 권한이 필요하지 않습니다.
보내기	스케줄러 또는 BI 플랫폼 받은 파일함으로 문서를 보내거나 전자 메일에서 하이퍼링크로 보낼 수 있습니다. Web Intelligence Desktop 사용자는 이 권한을 통해 전자 메일 첨부 파일로 문서를 보낼 수도 있습니다.

23.3.6 사용자 및 그룹

BI 플랫폼 환경에서 다른 개체에 대한 권한을 설정할 때와 마찬가지로 사용자와 그룹에 대한 권한을 설정할 수 있습니다. 이 단원에서 설명하는 권한은 사용자 및 그룹 개체에만 적용되는 유형별 권한이거나 사용자 및 그룹의 컨텍스트에서 특정 의미를 갖는 일반 권한입니다.

참고:

- 사용자와 하위 그룹은 소속 그룹에서 권한을 상속할 수 있습니다.
- 사용자 계정의 작성자는 계정의 소유자로 간주됩니다. 그러나 사용자 계정을 만들고 난 후에는 계정을 실제로 사용하게 될 사용자도 계정의 소유자로 간주됩니다.

권한	설명
개체 편집	<p>다음과 같은 작업을 수행할 수 있도록 합니다.</p> <ul style="list-style-type: none"> • 사용자나 그룹의 속성 편집 • 소속 그룹 관리 <p>사용자나 그룹을 다른 그룹에 추가하려면 사용자나 그룹과 대상 그룹에 대해 이 권한이 있어야 합니다.</p>
사용자 암호 변경	<p>다음과 같은 작업을 수행할 수 있도록 합니다.</p> <ul style="list-style-type: none"> • 자신의 사용자 계정 암호를 변경합니다. 이를 위해서는 사용자 계정에 대한 개체 편집 권한도 있어야 합니다. • 다른 사람의 사용자 계정 암호를 변경합니다. 이를 위해서는 사용자 계정에 대한 개체 편집 권한과 개체에 대한 사용자 권한 수정 권한도 있어야 합니다. <p>참고:</p> <ul style="list-style-type: none"> • 다음과 같은 사용자 암호 설정에는 이 권한이 적용되지 않습니다. <ul style="list-style-type: none"> • 암호가 만료되지 않음 • 다음 로그인할 때 반드시 암호 변경 • 암호 변경할 수 없음 • Business Objects 유니버스에 대한 데이터 소스 자격 증명에는 이 권한이 적용되지 않습니다.
게시에 가입	<p>사용자를 게시에 받는 사람으로 추가할 수 있도록 합니다.</p>
다른 사용자 대신 일정 설정	<p>사용자 대신 개체를 예약하여 사용자가 개체 인스턴스의 소유자가 될 수 있도록 합니다. 이를 위해서는 개체에 대한 다른 사용자 대신 일정 설정 권한도 있어야 합니다.</p>

23.3.7 액세스 수준

이 단원에서 설명하는 권한은 액세스 수준에만 적용됩니다.

권한	설명
보안 할당에 대한 액세스 수준 사용	개체의 액세스 제어 목록에 사용자를 추가할 때 액세스 수준을 지정할 수 있도록 합니다. 이를 위해서는 사용자 및 개체와 관련하여 개체에 대한 사용자 권한 수정 권한이나 개체에 대한 사용자 권한을 안전하게 수정합니다. 권한도 있어야 합니다. 개체에 대한 사용자 권한을 안전하게 수정합니다. 권한이 부여된 경우 개체에 대해 자신에게도 동일한 액세스 수준을 부여해야 합니다.

관련 항목

- 138 페이지에서 [개체에 대한 사용자 권한 수정 옵션 선택](#)"

23.3.8 BI 작업 영역

이 단원에서 설명하는 권한은 BI 작업 영역의 컨텍스트에서 특정 사용자 작업을 제어하는 일반 권한입니다.

권한	설명
폴더에 개체 추가	BI 작업 영역에 메뉴를 추가할 수 있도록 합니다. 그러나 이 권한으로는 BI 작업 영역에 모듈이나 기타 개체를 추가할 수 없습니다. BI 작업 영역에 메뉴를 추가하려면 BI 작업 영역 편집 권한도 있어야 합니다.
개체 편집	이 권한이 있으면 다음과 같은 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> BI 작업 영역 속성과 콘텐츠를 편집합니다. BI 작업 영역 메뉴를 편집합니다. BI 작업 영역을 삭제합니다.

모듈 권한 및 BI 작업 영역

모듈은 BI 작업 영역에 표시하고 싶은 데이터를 삽입할 수 있는 템플릿입니다. BI 작업 영역은 하나 이상의 모듈로 구성됩니다.

리포지토리에 모듈을 어떻게 추가하는가에 따라 보안 설정이 영향을 받습니다. 리포지토리에 모듈을 독립적인 개체로 추가하면 모듈 자체에 대한 일반 권한을 설정할 수 있습니다. 이러한 권한은 모듈을 BI 작업 영역에 사용할 때 적용됩니다.

23.3.9 유니버스(.unv) 권한

이 단원에서 설명하는 권한은 유니버스 디자인 도구 또는 .unv 유니버스로 만든 유니버스에 적용됩니다. 나열된 권한은 유니버스에만 적용되는 유형별 권한이거나 유니버스의 컨텍스트에서 특정 의미를 갖는 일반 권한입니다.

참고:

유니버스 권한은 유니버스 디자인 도구 응용 프로그램에서 CMS를 통해 유니버스를 가져오는 경우에만 적용됩니다. 유니버스를 로컬 디스크에 저장하는 경우에는 이러한 권한이 적용되지 않습니다.

권한	설명
폴더에 개체 추가	유니버스에 제한 집합이나 개체를 추가할 수 있도록 합니다. 이를 위해서는 액세스 제한 편집 권한도 있어야 합니다.
개체 보기	유니버스에 액세스하고 볼 수 있도록 합니다.
개체 편집	이 권한이 있으면 다음과 같은 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> CMC나 유니버스 디자인 도구에서 유니버스를 편집합니다. 유니버스 잠금 또는 잠금 해제 유니버스의 잠금을 해제하려면 유니버스 잠금 해제 권한도 있어야 합니다.
개체 삭제	유니버스를 삭제할 수 있도록 합니다.
개체 변환	변환 관리 도구를 사용하여 변환된 유니버스 개체 이름을 저장할 수 있도록 합니다. 참고: 개체 변환 권한이 명시적으로 정의되지 않는 한 개체 편집 권한을 명시적으로 부여하면 변환 내용을 저장할 수도 있습니다.
새 값 목록	이 권한이 있으면 다음과 같은 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> 개체에 새 값 목록 연결 기존의 값 목록 편집 참고: 이 권한이 계단식 값 목록의 작성 여부에 영향을 주지는 않습니다.

권한	설명
유니버스 인쇄	유니버스를 인쇄할 수 있도록 합니다.
테이블 또는 개체 값 표시	유니버스의 테이블 또는 개체와 관련된 값을 볼 수 있도록 합니다.
액세스 제한 편집	유니버스에 대한 액세스 제한(오버로드)을 편집할 수 있도록 합니다.
유니버스 잠금 해제	다음과 같은 작업을 수행할 수 있도록 합니다. <ul style="list-style-type: none"> • 다른 사용자가 잠근 유니버스의 잠금 해제 • CMS에서 유니버스 내보내기 유니버스의 잠금을 해제하려면 개체 편집 권한도 있어야 합니다.
데이터 액세스	유니버스에서 데이터를 검색하고 유니버스를 기반으로 문서를 새로 고칠 수 있도록 합니다. 이를 위해서는 유니버스 디자인 도구 응용 프로그램, 문서 및 유니버스 연결에 대해 이 권한이 있어야 합니다.
유니버스 기반 쿼리 만들기 및 편집	문서를 만들고 유니버스를 기반으로 하는 쿼리를 편집할 수 있도록 합니다.

23.3.10 유니버스(.unx) 권한

이 단원에서 설명하는 권한은 정보 디자인 도구 또는 .unx 유니버스로 만든 유니버스에 적용됩니다. 나열된 권한은 유니버스에만 적용되는 유형별 권한이거나 유니버스의 컨텍스트에서 특정 의미를 갖는 일반 권한입니다.

참고:

유니버스 권한은 리포지토리에 게시된 유니버스에만 적용됩니다. 유니버스를 로컬 폴더에 저장하는 경우에는 이러한 권한이 적용되지 않습니다.

권한	설명
개체 보기	유니버스에 액세스하고 볼 수 있도록 합니다.
개체 편집	유니버스를 다시 게시할 수 있도록 합니다.
개체 삭제	유니버스를 삭제할 수 있도록 합니다.
유니버스 검색	정보 디자인 도구에서 게시된 유니버스를 검색하고 기본 리소스(비즈니스 계층 및 데이터 기반)를 편집할 수 있도록 합니다. 참고: 정보 디자인 도구 응용 프로그램 권한인 유니버스 검색 권한도 있어야 합니다.
보안 프로필 편집	정보 디자인 도구 보안 편집기에서 유니버스에 대한 보안 프로필을 삽입, 편집 및 삭제할 수 있도록 합니다. 참고: 보안 프로필을 보거나 보안 프로필 집계 옵션을 변경하는 데는 이 권한이 필요하지 않습니다.
보안 프로필 할당	정보 디자인 도구 보안 편집기에서 사용자와 그룹에 대한 보안 프로필을 할당 및 할당 취소할 수 있도록 합니다.
데이터 액세스	유니버스에서 데이터를 검색하고 유니버스를 기반으로 문서를 새로 고칠 수 있도록 합니다. 정보 디자인 도구에서 이 권한이 있으면 쿼리 패널에서 결과 집합을 미리 볼 수 있습니다.
이 유니버스에 기반한 쿼리 만들기 및 편집	유니버스를 기반으로 하는 쿼리를 만들고 편집할 수 있도록 합니다. 정보 디자인 도구에서 이 권한이 있으면 쿼리 패널을 열고 유니버스에 대한 쿼리를 실행할 수 있습니다.
모든 사용자에게 대해 저장	모든 사용자에게 대한 유니버스를 저장할 수 있도록 합니다. 참고: 정보 디자인 도구 응용 프로그램 권한인 모든 사용자에게 대해 저장 권한도 있어야 합니다.

23.3.11 유니버스 개체 액세스 수준

디자이너가 유니버스 디자인 도구를 사용하여 유니버스를 만들거나 정보 디자인 도구를 사용하여 비즈니스 계층을 만들 때, 개체 액세스 수준을 유니버스의 모든 개체에 할당합니다. 개체 액세스 수준은 다음과 같습니다.

- 공용(기본)
- 제어
- 제한
- 기밀
- 개인

유니버스가 리포지토리에 게시된 후, 응용 프로그램에서 할당된 개체 액세스 수준을 바탕으로 유니버스 개체에 대한 액세스 권한을 부여할 수 있습니다. 예를 들어, Everyone 그룹에 공용 액세스 권한을 부여할 수 있습니다. 따라서 Everyone 그룹의 사용자는 공용으로 지정된 유니버스에 있는 개체를 볼 수 있습니다.

각각의 개체 액세스 수준은 앞 단계의 설정보다 많은 개체 액세스 권한을 부여합니다. 공용이 가장 낮은 수준입니다. 공용 액세스 권한이 부여된 사용자는 공용으로 지정된 개체만 볼 수 있다. 제어 액세스 권한이 부여된 사용자는 공용 및 제어로 지정된 개체를 볼 수 있다. 개인은 최고 수준의 설정으로, 사용자가 모든 개체 액세스 수준, 즉 유니버스 내의 모든 개체에 액세스할 수 있도록 허용합니다.

참고:

- 개체 액세스 수준 보안 설정은 유니버스가 상속하는 다른 모든 보안 설정보다 우선권이 높습니다.
- .unix 유니버스의 경우, 보안 프로필에서 정의된 개체 보안과 함께 개체 액세스 수준 보안 설정이 고려됩니다. 보안 프로필에 대한 자세한 내용은 정보 디자인 도구 사용자 가이드를 참조하십시오.

관련 항목

- 807 페이지에서 [유니버스 개체 액세스 수준 지정](#) "

23.3.11.1 유니버스 개체 액세스 수준 지정

유니버스 개체 액세스 수준 보안을 설정하려면 유니버스에 대한 개체에 대한 사용자 권한 수정 권한이 있어야 합니다.

1. CMS의 유니버스 영역에서 유니버스를 선택합니다.
2. 작업 > 유니버스 보안을 클릭합니다.
3. 사용자 또는 그룹에 대한 유니버스 보안 대화 상자의 개체 수준 보안 목록에서 개체 액세스 수준을 선택합니다.

23.3.12 연결 권한

이 단원에서 설명하는 권한은 유니버스 연결에 적용되는 유형별 권한이거나 유니버스 연결의 컨텍스트에서 특정 의미를 갖는 일반 권한입니다. 이런 권한은 리포지토리에 게시되는 연결에 적용됩니다.

관계 연결 권한

권한	설명
개체 보기	연결을 볼 수 있도록 합니다.
개체 편집	연결 매개 변수를 편집할 수 있도록 합니다.
개체 삭제	연결을 삭제할 수 있도록 합니다.
다른 폴더에 개체 복사	한 폴더에서 다른 폴더로 연결을 복사할 수 있도록 합니다.
데이터 액세스	연결에 지정된 데이터베이스에서 콘텐츠를 검색할 수 있도록 합니다. 정보 디자인 도구에서 이 권한을 이용해 연결 및 데이터 기반 편집기에서 테이블 데이터를 찾아볼 수 있습니다. 쿼리 패널에서 결과 집합을 미리 볼 수도 있습니다.
저장 프로시저의 연결 사용	유니버스 연결에 지정된 데이터베이스에서 저장 프로시저를 사용할 수 있도록 합니다. 참고: 이 권한은 .unv 유니버스에만 적용됩니다.

OLAP 연결 권한

권한	설명
개체 보기	연결을 볼 수 있도록 합니다.
개체 편집	정보 디자인 도구 연결 편집기에서 연결 매개 변수를 편집할 수 있도록 합니다.
개체 삭제	연결을 삭제할 수 있도록 합니다.
다른 폴더에 개체 복사	한 폴더에서 다른 폴더로 연결을 복사할 수 있도록 합니다.

23.3.13 응용 프로그램

23.3.13.1 CMC

이 단원에서 설명하는 권한은 CMC에만 적용됩니다.

권한	설명
CMC에 로그인하여 이 개체를 CMC에 표시합니다.	CMC에 로그인할 수 있도록 합니다.
인스턴스 관리자에 대한 액세스 허용	인스턴스 관리자에 액세스할 수 있도록 합니다.
관계 쿼리에 대한 액세스 허용	CMC에서 관계 쿼리를 실행할 수 있도록 합니다.
보안 쿼리에 대한 액세스 허용	CMC에서 보안 쿼리를 실행할 수 있도록 합니다.

23.3.13.2 BI 실행 패드

이 단원에서 설명하는 권한은 BI 실행 패드에만 적용됩니다.

권한	설명
구성	다음과 같은 작업을 수행할 수 있도록 합니다. <ul style="list-style-type: none"> • 개체 이동 및 복사 • 즐겨찾기 폴더에 개체 추가 • 개체의 바로 가기 만들기
Business Objects 받은 파일함으로 보내기	개체를 BI 받은 파일함 수신자에게 보낼 수 있습니다.
전자 메일 대상으로 보내기	개체를 BI 받은 파일함 수신자에게 보낼 수 있습니다.
파일 위치로 보내기	파일 위치에 개체를 저장할 수 있습니다.
FTP 위치로 보내기	FTP 위치에 개체를 저장할 수 있습니다.

23.3.13.3 BI 작업 영역

이 단원에서 설명하는 권한은 BI 작업 영역에만 적용됩니다.

권한	설명
BI 작업 영역 만들기	사용자가 새 BI 작업 영역을 만들고 기존 BI 작업 영역을 편집할 수 있습니다.
개체 편집	사용자가 새 모듈을 만들고 기존 모듈을 편집할 수 있습니다.
BI 작업 영역 편집	사용자가 기존 BI 작업 영역을 편집할 수 있습니다. 사용자가 새 BI 작업 영역을 만들 수 없습니다.

23.3.13.4 Web Intelligence

이 단원에서 설명하는 권한은 SAP BusinessObjects Web Intelligence(데스크탑 인터페이스 포함)에만 적용되며 해당 응용 프로그램의 뷰어 및 쿼리 패널에 영향을 미칩니다.

권한	설명
데이터 - 데이터 추적 사용	변경된 데이터 추적을 허용합니다.
데이터 - 변경된 데이터의 서식 사용	변경된 데이터에 대한 서식 선택을 허용합니다.
데스크탑 인터페이스 - Web Intelligence Desktop 사용	데스크탑 인터페이스를 사용할 수 있도록 합니다.
데스크탑 인터페이스 - 로컬 데이터 공급자 사용	데스크탑 인터페이스에서 개인 데이터 공급자를 사용할 수 있도록 합니다.
데스크탑 인터페이스 - 문서 내 보내기	데스크탑 인터페이스에서 CMS로 문서 내보내기를 허용합니다.
데스크탑 인터페이스 - 문서 가져오기	데스크탑 인터페이스의 CMS에서 문서 가져오기를 허용합니다.
데스크탑 인터페이스 - BI 실행 패드에서 설치	BI 실행 패드에서 데스크탑 인터페이스 다운로드를 허용합니다.
데스크탑 인터페이스 - 문서 인쇄	데스크탑 인터페이스에서 문서 인쇄를 허용합니다.
데스크탑 인터페이스 - 문서 보안 제거	데스크탑 인터페이스에서 문서 보안 제거를 허용합니다.
데스크탑 인터페이스 - 모든 사용자에게 대해 문서 저장	데스크탑 인터페이스에서 문서를 모든 사용자에게 대해 저장할 수 있도록 허용합니다.
데스크탑 인터페이스 - 문서를 로컬에 저장	데스크탑 인터페이스의 로컬 디스크에 문서를 저장할 수 있도록 합니다.
데스크탑 인터페이스 - 메일로 보내기	데스크탑 인터페이스에서 문서를 전자 메일로 보낼 수 있도록 합니다.
데스크탑 인터페이스 - 로컬 데이터 공급자 사용	데스크탑 인터페이스에서 개인 데이터 공급자를 사용할 수 있도록 합니다.
문서 - 열 때 자동 새로 고침 사용 안 함	문서를 열 때 문서를 자동으로 새로 고치지 않도록 합니다.

권한	설명
문서 - 자동 저장 사용	(관리자가 CMC에서 자동 저장을 활성화하는 경우) 문서 자동 저장을 허용합니다.
문서 - 만들기 사용	새 문서 만들기를 허용합니다.
문서 - 게시 및 콘텐츠 관리 사용	CMS에 문서를 게시할 수 있도록 허용합니다.
대화형: 보고 - 경고 만들기 및 편집	대화형 뷰어에서 경고 만들기 및 편집을 허용합니다.
인터페이스 - RIA(Rich Internet Application) 사용	RIA(Rich Internet Application) 보기 및 편집 인터페이스(이전 릴리스에서는 Java 보고서 패널) 사용을 허용합니다.
인터페이스 - 웹 보기 인터페이스 사용	웹 보기 인터페이스(이전 릴리스에서는 DHTML 뷰어) 사용을 허용합니다.
인터페이스 - 웹 쿼리 패널 사용	웹 쿼리 패널(이전 릴리스에서는 쿼리 - HTML) 사용을 허용합니다.
일반 - '내 기본 설정' 편집	BI 실행 패드에서 기본 설정을 편집할 수 있도록 허용합니다.
일반 - 마우스 오른쪽 단추를 클릭하면 나타나는 메뉴 사용	마우스 오른쪽 단추를 클릭하면 나타나는 메뉴 사용을 허용합니다.
왼쪽 창 - 문서 요약 사용	왼쪽 창에서 문서 요약 표시를 허용합니다.
왼쪽 창 - 문서 구조 및 필터 사용	왼쪽 창에서 문서 구조 및 필터 표시를 허용합니다.
쿼리 스크립트 - 편집 사용(SQL, MDX...)	쿼리 스크립트(SQL 및 MDX) 편집을 허용합니다.
쿼리 스크립트 - 보기 사용(SQL, MDX...)	쿼리 스크립트(SQL 및 MDX) 보기를 허용합니다.
보고 - 나누기 만들기 및 편집	나누기 만들기 및 편집을 허용합니다.
보고 - 조건부 서식 규칙 만들기 및 편집	조건부 서식 규칙 만들기 및 편집을 허용합니다.
보고 - 미리 정의된 계산 만들기 및 편집	미리 정의된 계산 만들기 및 편집을 허용합니다.
보고 - 입력 컨트롤 만들기 및 편집	입력 컨트롤 만들기 및 편집을 허용합니다.

권한	설명
보고 - 보고서 필터 만들기/편집 및 입력 컨트롤 사용	보고서 필터 및 입력 컨트롤 만들기 및 편집을 허용합니다. (사용하지 않을 때는 왼쪽 창에 입력 컨트롤 창이 표시되지 않음)
보고 - 정렬 만들기 및 편집	정렬 만들기 및 편집을 허용합니다.
보고 - 수식 및 변수 만들기	수식 및 변수 만들기를 허용합니다.
보고 - 서식 사용	보고서 서식 편집을 허용합니다. 이 권한이 거부되는 경우에는 사용자가 디자인 및 데이터 모드를 사용할 수 없어야 합니다(비활성화).
보고 - 병합된 차원 사용	보고서와 데이터 관리자에서 병합된 차원을 사용한 데이터 동기화를 허용합니다.
보고 - 보고서, 테이블, 차트 및 셀 삽입/제거	보고서, 테이블, 차트 및 셀의 삽입과 제거를 허용합니다. 중복 워크플로(복사/붙여넣기)도 규정합니다.

23.3.13.5 전략 작성기

전략 작성기는 Performance Management와 관련된 도구입니다. 이 단원에서 설명하는 권한은 전략 작성기에만 적용되며 Performance Manager의 목표 관리나 전략 작성기의 특정 기능에 영향을 줄 수 있습니다.

권한	설명
목표 만들기, 수정 또는 삭제	Performance Manager에서 목표를 추가, 편집 또는 제거할 수 있도록 합니다.
목표 보기	목표가 포함된 분석에서 목표를 볼 수 있도록 합니다.
목표 관리 액세스	Performance Manager의 목표 관리 페이지에서 목표를 볼 수 있도록 합니다.
목표 게시	Performance Manager에서 목표를 게시할 수 있도록 합니다.

권한	설명
전략 작성기 액세스	Performance Manager에서 전략 작성기 도구에 액세스할 수 있도록 합니다.
역할 만들기, 수정 또는 삭제	전략 작성기에서 특정 사용자를 대상으로 목표나 메트릭을 게시하는데 사용되는 역할을 관리할 수 있도록 합니다.
전략 만들기, 수정 또는 삭제	전략 작성기에서 목표와 메트릭을 게시하고 역할을 연결하는 전략을 만들 수 있도록 합니다.

23.3.13.6 유니버스 디자인 도구 권한

이 단원에서 설명하는 권한은 유니버스 디자인 도구 응용 프로그램에 적용됩니다.

권한	설명
유니버스 무결성 검사	유니버스 무결성을 검사할 수 있도록 합니다.
구조 창 새로 고침	구조 창을 새로 고칠 수 있도록 합니다.
테이블 탐색기 사용	테이블 탐색기를 사용하여 데이터베이스 데이터를 볼 수 있도록 합니다.
유니버스 제약 조건 적용	가져온 유니버스의 사용자에게 미리 정의된 유니버스 제약 조건을 적용할 수 있도록 합니다.
유니버스 연결	두 개의 유니버스를 연결하고 구성 요소를 공유할 수 있도록 합니다.
연결 만들기, 수정 또는 삭제	리포지토리에 저장된 유니버스 연결이나 개인 또는 공유 연결로 저장된 유니버스를 만들고, 수정하고, 삭제할 수 있도록 합니다.

23.3.13.7 정보 디자인 도구 권한

이 단원에서 설명하는 권한은 정보 디자인 도구 응용 프로그램에 적용됩니다.

권한	설명
보안 프로필 관리	보안 편집기를 열 수 있도록 합니다. 참고: 보안 프로필 작업을 하려면 유니버스에서 부여된 권한이 필요합니다.
프로젝트 공유	로컬 프로젝트를 공유하고 프로젝트 동기화 보기를 열어 공유 프로젝트를 로컬 프로젝트와 동기화할 수 있도록 합니다.
연결 만들기, 수정 또는 삭제	다음과 같은 작업을 수행할 수 있도록 합니다. <ul style="list-style-type: none"> • Published Resources 보기에서 보안 연결 만들기 및 삭제 • 연결 편집기에서 연결 편집 • 리포지토리에 연결 게시
유니버스 게시	리포지토리에 유니버스를 게시할 수 있도록 합니다.
유니버스 검색	편집할 로컬 프로젝트로 게시된 유니버스를 검색하여 가져올 수 있도록 합니다.
모든 사용자에게 대해 저장	유니버스를 검색할 때 모든 사용자에게 대해 저장 옵션을 사용할 수 있도록 합니다.
통계 계산	통계를 계산하고 게시할 테이블과 열을 선택할 수 있도록 합니다.

23.3.13.8 SAP BusinessObjects Business Intelligence 플랫폼용 위젯

이 단원에서 설명하는 권한은 SAP BusinessObjects Business Intelligence 플랫폼 응용 프로그램용 위젯에만 적용됩니다.

권한	설명
탐색기 사용	사용자는 문서 목록 탐색기를 사용하여 연결된 모든 BI 플랫폼 서버에 있는 콘텐츠를 찾아볼 수 있습니다.
경고 받은 파일함 사용	(사용 안 하는 항목) 경고 받은 파일함을 사용할 수 있도록 합니다.
검색 사용	사용자는 콘텐츠 검색을 사용하여 연결된 모든 BI 플랫폼 리포지토리를 한 번에 검색할 수 있습니다.

23.3.13.9 경고

이 단원에서 설명하는 권한은 경고 응용 프로그램에만 적용됩니다.

권한	설명
"경고 트리거"	<p>경고 이벤트를 트리거할 수 있습니다.</p> <p>문서에 대한 경고를 트리거하려면 다음 권한이 필요합니다.</p> <ul style="list-style-type: none"> • 문서에 대한 보기 및 예약 권한 • 해당 이벤트에 대한 보기 및 트리거 권한
"개체에 가입"	<p>경고 이벤트에 가입할 수 있습니다.</p> <p>이벤트에 가입하려면 다음 권한이 필요합니다.</p> <ul style="list-style-type: none"> • 해당 이벤트에 대한 보기 권한 • 사용자 자신의 계정에 대한 가입 권한 <p>문서에서 경고에 가입하려면 다음 권한이 필요합니다.</p> <ul style="list-style-type: none"> • 문서에 대한 보기 권한 • 문서에 대한 인스턴스 보기 권한 • 해당 이벤트에 대한 보기 권한 • 사용자 자신의 계정에 대한 가입 권한

23.3.13.10 탐색기

이 단원에서 설명하는 권한은 Explorer에만 적용됩니다.

권한	설명
Explorer에 로그인하여 CMC에서 이 개체 보기	Explorer에 로그인합니다. 이 권한이 있어야 Explorer에서 다른 작업을 수행할 수 있습니다.
정보 공간 탐색	정보 공간을 탐색합니다. 이 작업을 수행하려면 Explorer에 로그인하여 CMC에서 이 개체 보기 권한도 있어야 합니다.
정보 공간 탐색: 책갈피/전자 메일로 내보내기	책갈피를 설정하고 전자 메일로 보냅니다. 이 작업을 수행하려면 다음과 같은 권한도 있어야 합니다. <ul style="list-style-type: none"> • Explorer에 로그인하여 CMC에서 이 개체 보기 • 정보 공간 탐색
정보 공간 탐색: CSV로 내보내기	탐색 결과를 CSV 또는 Excel 파일로 내보냅니다. 이 작업을 수행하려면 다음과 같은 권한도 있어야 합니다. <ul style="list-style-type: none"> • Explorer에 로그인하여 CMC에서 이 개체 보기 • 정보 공간 탐색
정보 공간 탐색: 이미지로 내보내기	탐색 결과를 이미지로 내보냅니다. 이 작업을 수행하려면 다음과 같은 권한도 있어야 합니다. <ul style="list-style-type: none"> • Explorer에 로그인하여 CMC에서 이 개체 보기 • 정보 공간 탐색
정보 공간 탐색: Web Intelligence로 내보내기	탐색 결과를 쿼리로 내보냅니다. 이 작업을 수행하려면 다음과 같은 권한도 있어야 합니다. <ul style="list-style-type: none"> • Explorer에 로그인하여 CMC에서 이 개체 보기 • 정보 공간 탐색
정보 공간 관리	공간 관리 메뉴에 액세스하고 관련 작업을 수행합니다. 이 작업을 수행하려면 Explorer에 로그인하여 CMC에서 이 개체 보기 권한도 있어야 합니다.

권한	설명
정보 공간 관리: 새 공간 만들기	<p>새 정보 공간을 만듭니다.</p> <p>이 작업을 수행하려면 다음과 같은 권한도 있어야 합니다.</p> <ul style="list-style-type: none"> • Explorer에 로그인하여 CMC에서 이 개체 보기 • 정보 공간 관리
정보 공간 관리: 공간 수정	<p>정보 공간을 수정하거나 삭제합니다.</p> <p>이 작업을 수행하려면 다음과 같은 권한도 있어야 합니다.</p> <ul style="list-style-type: none"> • Explorer에 로그인하여 CMC에서 이 개체 보기 • 정보 공간 관리
정보 공간 관리: 인덱싱 예약	<p>정보 공간 데이터의 인덱싱을 예약합니다.</p> <p>이 작업을 수행하려면 다음과 같은 권한도 있어야 합니다.</p> <ul style="list-style-type: none"> • Explorer에 로그인하여 CMC에서 이 개체 보기 • 정보 공간 관리
정보 공간 관리: 인덱싱 시작	<p>정보 공간 데이터의 인덱싱을 실행합니다.</p> <p>이 작업을 수행하려면 다음과 같은 권한도 있어야 합니다.</p> <ul style="list-style-type: none"> • Explorer에 로그인하여 CMC에서 이 개체 보기 • 정보 공간 관리

23.3.13.11 SAP BusinessObjects Mobile

이 단원에서 설명하는 권한은 SAP BusinessObjects Mobile 응용 프로그램에만 적용됩니다.

권한	설명
SAP BusinessObjects Mobile 응용 프로그램 로그인	Mobile 응용 프로그램을 통해 BI 플랫폼에 로그인하여 문서를 볼 수 있는 액세스 권한을 부여합니다.
문서 경고 구독	<p>문서/되풀이 경고 구독을 위한 액세스 권한을 부여합니다.</p> <p>참고:</p> <ul style="list-style-type: none"> 이전에 "문서 경고 구독" 권한을 부여 받았지만 현재 거부되는 경우에도 구독한 경고가 계속해서 수신됩니다. 경고를 수신하지 않으려면 명시적으로 경고 구독을 해지해야 합니다. 일정에 대한 문서 경고(또는 되풀이 인스턴스)를 구독하려면 사용자에게 중앙 관리 콘솔(CMC)의 "이벤트"에 있는 "시스템 이벤트" 폴더에 대해 "모든 권한" 보안 액세스 권한이 있어야 합니다.
장치의 로컬 저장소에 문서 저장	<p>Mobile 장치에 문서를 저장할 수 있는 액세스 권한을 부여합니다.</p> <p>참고:</p> <p>"장치에 로컬로 문서 저장" 권한을 부여 받은 상태에서 장치에 문서를 저장한 경우 저장 권한이 박탈되더라도 해당 문서는 장치에 계속 남아 있습니다. 하지만, 이런 문서는 동기화 프로세스 중 동기화되지 않습니다.</p>
장치에서 전자 메일로 문서 보내기	전자 메일을 통해 보고서를 보낼 수 있는 액세스 권한을 부여합니다.

자세한 내용은 SAP BusinessObjects Mobile 설치 및 배포 가이드를 참조하십시오.

장24 서버 속성 부록

24.1 서버 속성 부록에 대한 정보

이 서버 속성 부록에는 각 BI 플랫폼 서버에 설정할 수 있는 속성 및 이에 대한 설명이 나와 있습니다.

24.1.1 일반 서버 속성

이 단원에서 설명하는 서버 속성은 모든 서버 유형에 적용됩니다.

테이블24-1: 요청 포트 속성

속성	설명	기본값
서버 이름	서버 이름입니다.	기본값은 서버가 있는 노드의 이름과 서버의 이름을 합친 것입니다.
ID, CUID	서버의 짧은 ID와 클러스터에 고유한 ID입니다. 읽기 전용입니다.	이 값들은 자동으로 생성됩니다.
노드	서버가 위치한 노드의 이름입니다.	이 값은 설치 중에 지정됩니다.
설명	서버에 대한 설명	기본값은 서버의 이름입니다.
명령줄 매개 변수	서버의 명령줄 매개 변수입니다.	기본값은 서버 유형에 따라 달라집니다.

속성	설명	기본값
포트 요청	<p>서버가 요청을 수신하는 포트를 지정합니다. 방화벽이 있는 환경의 경우 서버가 방화벽에서 개방된 포트의 요청만 수신하도록 설정할 수 있습니다. 서버에 대한 포트를 지정하는 경우 다른 프로세스에서 이미 그 포트를 사용하고 있지 않은지 확인합니다.</p> <p>참고: 자동 할당을 선택하면 서버가 동적으로 할당된 포트에 바인딩됩니다. 이는 서버가 다시 시작될 때마다 임의의 포트 번호가 서버에 할당된다는 의미입니다.</p>	기본적으로 자동 할당은 TRUE로 설정되어 있으며 요청한 포트는 비어 있습니다.
자동 할당	서버가 다시 시작될 때마다 서버를 동적으로 할당된 포트에 바인딩할지 여부를 지정합니다. 서버를 특정 포트에 바인딩하려면 자동 할당을 FALSE로 설정하고 유효한 요청한 포트를 지정합니다.	기본값은 TRUE입니다.

테이블24-2: 자동 시작 속성

속성	설명	기본값
Server Intelligence Agent가 시작되면 자동으로 이 서버 시작	<p>SIA(Server Intelligence Agent)가 시작 또는 다시 시작될 때 서버를 자동으로 시작할지 여부를 지정합니다.</p> <p>이 값이 FALSE로 설정되어 있는 경우 SIA가 시작 또는 다시 시작되면 서버가 중지된 채로 있게 됩니다.</p>	기본값은 TRUE입니다.

테이블24-3: 호스트 식별자 속성

속성	설명	기본값
자동 할당	서버를 자동으로 할당되는 네트워크 인터페이스에 바인딩할지 여부를 지정합니다. FALSE로 설정된 경우 서버는 특정 네트워크 인터페이스에 바인딩됩니다. TRUE로 설정한 경우 서버는 첫 번째로 사용 가능한 IP 주소에 대한 요청을 수락합니다. 멀티홈 컴퓨터에서는 이 값을 FALSE로 설정하고 유효한 호스트 이름 또는 IP 주소를 제공하여 바인딩할 특정 네트워크 인터페이스를 지정할 수 있습니다.	기본값은 TRUE입니다.

속성	설명	기본값
호스트 이름	서버가 바인딩되는 네트워크 인터페이스의 호스트 이름입니다. 호스트 이름이 지정되어 있는 경우 서버는 이 호스트 이름과 연결된 모든 IP 주소에 대한 요청을 수락합니다.	기본적으로 자동 할당은 TRUE로 설정되어 있으며 호스트 이름은 비어 있습니다.
IP 주소	서버가 바인딩하는 네트워크 인터페이스의 IP 주소입니다. IPv4 및 IPv6 프로토콜이 모두 지원됩니다. IP 주소가 지정된 경우 서버는 IP 주소에 대한 요청만 수락합니다.	기본적으로 자동 할당은 TRUE로 설정되어 있으며 IP 주소는 비어 있습니다.

테이블24-4: 구성 템플릿 속성

속성	설명	기본값
구성 템플릿 사용	구성 템플릿을 사용할지 여부를 지정합니다.	기본값은 FALSE입니다.
시스템 기본값 복원	이 서버에 대한 원래 기본 설정의 복원 여부를 지정합니다.	기본값은 FALSE입니다.
구성 템플릿 설정	현재 서비스 설정을 동일한 유형의 모든 서비스에 대한 구성 템플릿으로 사용할지 여부를 지정합니다. TRUE로 설정할 경우 구성 템플릿 사용으로 지정된 동일한 유형의 모든 서비스는 즉시 현재 서비스의 설정을 사용하도록 다시 구성됩니다.	기본값은 FALSE입니다.

테이블24-5: TraceLog 서비스 속성

속성	설명	기본값
로그 수준	<p>기록할 최소 메시지 심각도를 지정하고 서버 로그 파일에 기록할 정보의 양을 결정합니다.</p> <p>가능한 로그 임계값 수준은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 지정되지 않음 • 없음 • 낮음 • 중간 • 높음 	기본값은 지정되지 않음입니다.

관련 항목

- 388 페이지에서 [구성 템플릿 작업](#)"
- 743 페이지에서 [추적 로그 수준](#)"

24.1.2 핵심 서비스 속성

핵심 서비스 범주에는 다음 서버가 포함됩니다.

- 적응 작업 서버
- 적응 처리 서버
- 중앙 관리 서버
- 대시보드 서버
- 대시보드 분석 서버
- 이벤트 서버
- 입력 파일 리포지토리 서버
- 출력 파일 리포지토리 서버
- 웹 응용 프로그램 컨테이너 서버

적응형 작업 서버 속성

테이블 24-6: 일반 속성

속성	설명	기본값
임시 디렉터리	필요한 경우 임시 파일을 만드는 디렉터리를 지정합니다. 이 디렉터리의 디스크 공간이 충분하지 않은 경우 성능 문제가 발생할 수 있습니다. 성능을 더욱 높이려면 이 디렉터리가 로컬 디스크에 있어야 합니다. 참고: 변경된 내용을 적용하려면 서버를 다시 시작해야 합니다.	%DefaultDataDir%

적응형 작업 서버는 다양한 서비스를 호스트할 수 있습니다. 각 서비스에는 다음 속성이 있습니다.

테이블24-7: 서비스 속성

속성	설명	기본값
최대 동시 작업	<p>서버에서 동시에 실행할 수 있도록 허용하는 독립적인 프로세스(자식 프로세스) 수를 지정합니다. 사용자의 보고서 작성 환경에 맞게 최대 작업 수를 조정할 수 있습니다.</p> <p>대부분의 경우에는 보고서를 작성할 때 기본 설정을 사용할 수 있습니다. 보고서 작성 환경에 가장 적합한 설정은 해당되는 하드웨어 구성, 데이터베이스 소프트웨어, 보고서 요구 사항에 따라 달라집니다.</p>	기본값은 5입니다.
최대 자식 요청 수	다시 시작하기 전 자식에서 처리할 작업 수를 지정합니다.	기본값은 100입니다.

적응형 처리 서버 속성

테이블24-8: 일반 속성

속성	설명	기본값
서비스 시작 제한 시간(초)	<p>서비스가 시작될 때까지 서버가 대기하는 제한 시간(초)을 지정합니다.</p> <p>서비스가 지정된 시간 내에 시작하지 못하는 데는 다음과 같은 두 가지 이유가 있을 수 있습니다.</p> <ul style="list-style-type: none"> • 데이터베이스와 같이 필요한 리소스를 찾을 수 없거나 서비스에서 포트 충돌이 발생하여 시스템에서 오류가 발생했습니다. • 시스템 속도가 너무 느려 지정된 시간 내에 서비스를 시작할 수 없습니다. <p>이유를 알아보려면 서버 로그 파일을 확인하십시오. 지정된 시간 내에 서비스를 시작할 수 없는 경우 이 값을 늘려 보십시오.</p>	기본값은 1200초입니다.

중앙 관리 서버 속성

참고:

이러한 서버 속성을 수정한 경우 변경 내용을 적용하려면 서버를 다시 시작해야 합니다.

테이블24-9: 중앙 관리 서비스 속성

속성	설명	기본값
이름 서버 포트	CMS에서 최초 이름 서비스 요청을 수신할 포트를 지정합니다.	기본값은 6400입니다.
요청된 시스템 데이터베이스 연결	CMS에서 설정할 수 있는 CMS 시스템 데이터베이스 연결 수를 지정합니다. 요청된 데이터베이스 연결을 전부 서버에서 설정할 수 없는 경우, 동시에 처리할 수 있는 요청 수가 감소하므로 CMS가 계속 작동하지만 성능은 낮습니다. CMS는 요청된 수의 연결이 설정될 때까지는 계속 연결을 추가로 설정합니다. CMS의 설정된 시스템 데이터베이스 연결 메트릭은 현재 설정된 연결 수를 보여줍니다.	기본값은 14입니다.
시스템 데이터베이스 자동 다시 연결	서비스가 중단될 경우 CMS가 자동으로 CMS 데이터베이스에 대한 연결을 다시 설정할지 여부를 지정합니다. 이 값이 FALSE로 설정되어 있으면 작업을 다시 시작하기 전에 CMS 데이터베이스의 무결성을 검사할 수 있습니다. 따라서 데이터베이스 연결을 다시 설정하려면 CMS를 다시 시작해야 합니다.	기본값은 TRUE입니다.

테이블24-10: 단일 로그인 서비스 속성

속성	설명	기본값
단일 로그인 만료(초)	만료되기 전까지 데이터 소스에 대한 SSO 연결이 유효한 시간(초)을 지정합니다. 이 설정은 데이터 소스에 대한 Windows AD SSO에 대해 구성된 보고서를 실행 중인 AD 사용자에게 적용됩니다.	기본값은 86400초입니다.

이벤트 서버 속성

테이블24-11: 이벤트 서비스 속성

속성	설명	기본값
정리 간격(분)	정리 유틸리티가 실행되는 간격(분)을 지정합니다.	기본값은 20분입니다.
이벤트 폴 간격(초)	이벤트를 트리거하는 파일에 대해 서버가 폴링하는 간격(초)을 지정합니다.	기본값은 10초입니다. 허용되는 값 범위는 1 ~ 1200초입니다.

입력 파일 리포지토리 서버 속성

테이블24-12: Input Filestore 서비스 속성

속성	설명	기본값
최대 파일 액세스 재 시도 횟수	서버가 파일에 액세스를 시도하는 횟수를 지정합니다.	기본값은 1입니다.
최대 유휴 시간(분)	비활성 연결을 닫기 전에 서버가 대기하는 시간을 지정합니다. 값을 너무 낮게 설정하면 사용자의 요청이 중간에 중단될 수 있습니다. 반대로 이 값을 너무 높게 설정하면 처리 시간과 디스크 공간 같은 시스템 리소스의 사용이 과도하게 늘어날 수 있습니다.	기본값은 10분입니다.
임시 디렉터리	필요한 경우 임시 파일을 만드는 디렉터리를 지정합니다. 참고: 이 디렉터리의 디스크 공간이 충분하지 않은 경우 성능 문제가 발생할 수 있습니다. 더 나은 성능을 위해, 임시 디렉터리는 파일 저장 디렉터리와 같은 파일 시스템에 있는 것이 좋습니다.	%DefaultInputFRS Dir/temp%
파일 저장소 디렉터리	파일 리포지토리 개체를 저장할 디렉터리를 지정합니다. 참고: 이 디렉터리의 디스크 공간이 충분하지 않은 경우 성능 문제가 발생할 수 있습니다.	%DefaultInputFRS Dir/%

출력 파일 리포지토리 서버 속성

테이블24-13: Output Filestore 서비스 속성

속성	설명	기본값
최대 파일 액세스 재 시도 횟수	서버가 파일에 액세스를 시도하는 횟수를 지정합니다.	기본값은 1입니다.
최대 유휴 시간(분)	비활성 연결을 닫기 전에 서버가 대기하는 시간을 지정합니다. 값을 너무 낮게 설정하면 사용자의 요청이 중간에 중단될 수 있습니다. 반대로 이 값을 너무 높게 설정하면 처리 시간과 디스크 공간 같은 시스템 리소스의 사용이 과도하게 늘어날 수 있습니다.	기본값은 10분입니다.

속성	설명	기본값
임시 디렉터리	필요한 경우 임시 파일을 만드는 디렉터리를 지정합니다. 참고: 이 디렉터리의 디스크 공간이 충분하지 않은 경우 성능 문제가 발생할 수 있습니다.	%DefaultOutputFRS Dir/temp%
파일 저장소 디렉터리	파일 리포지토리 개체를 저장할 디렉터리를 지정합니다. 참고: 이 디렉터리의 디스크 공간이 충분하지 않은 경우 성능 문제가 발생할 수 있습니다.	%DefaultOutputFRS Dir/%

웹 응용 프로그램 컨테이너 서버 속성

테이블24-14: 일반 속성

속성	설명	기본값
서비스 시작 제한 시간(초)	WACS에서 호스팅된 서비스가 시작되기를 기다릴 제한 시간입니다. 제한 시간이 경과되면 아직 시작되지 않은 서비스는 WACS에서 제공되지 않습니다. 컴퓨터 속도가 느린 경우 더 큰 값을 지정할 수 있습니다. 너무 작은 값을 지정한 경우 제한 시간이 지날 때까지 WACS가 시작되지 않으면 중앙 구성 관리자(CCM)를 통해 WACS의 기본 설정을 복원해야 합니다.	기본값은 600초입니다.

테이블24-15: BOE 웹 응용 프로그램 서비스 속성

속성 유형	설명	기본값
인증 형식	<p>BI 실행 패드에 로그인하는 사용자를 인증하는 데 사용되는 인증 형식입니다.</p> <p>사용할 수 있는 값은 다음과 같습니다.</p> <ul style="list-style-type: none"> • AD Kerberos • AD Kerberos SSO • Enterprise • LDAP 	기본값은 Enterprise입니다.
기본 AD 도메인	<p>기본 Active Directory 도메인을 사용하면 로그인할 때 도메인을 입력할 필요가 없습니다. 예를 들어 기본 도메인이 mydo-main으로 설정된 경우 사용자가 user라는 사용자 이름으로 로그인하면 Active Directory 로그인 인증 기관에서 user@mydo-main.com을 인증하려고 합니다.</p>	기본적으로 이 값은 비어 있습니다.
서비스 사용자 이름	<p>SPN(서비스 사용자 이름)은 클라이언트에서 서비스의 인스턴스를 고유하게 식별하는 데 사용됩니다. Kerberos 인증 서비스에서는 SPN을 사용하여 서비스를 인증합니다.</p>	기본적으로 이 값은 비어 있습니다.
Keytab 파일	<p>keytab 파일에 대한 전체 경로입니다. Keytab 파일을 사용하면 웹 응용 프로그램 컴퓨터에서 사용자 계정의 암호를 노출하지 않고 Kerberos 필터를 구성할 수 있습니다.</p>	기본적으로 이 값은 비어 있습니다.

테이블24-16: 웹 서비스 SDK 및 QaaWS 속성

속성	설명	기본값
Kerberos Active Directory 단일 로그인 사용	<p>웹 서비스 SDK 및 QaaWS에 대해 Kerberos AD 단일 로그인을 사용할지 여부입니다.</p>	기본값은 FALSE입니다.

속성	설명	기본값
기본 AD 도메인	기본 Active Directory 도메인을 사용하면 로그인할 때 도메인을 입력할 필요가 없습니다.	기본적으로 이 값은 비어 있습니다.
서비스 사용자 이름	SPN(서비스 사용자 이름)은 클라이언트에서 서비스의 인스턴스를 고유하게 식별하는 데 사용됩니다. Kerberos 인증 서비스에서는 SPN을 사용하여 서비스를 인증합니다.	기본적으로 이 값은 비어 있습니다.
Keytab 파일	keytab 파일에 대한 전체 경로입니다. Keytab 파일을 사용하면 웹 응용 프로그램 컴퓨터에서 사용자 계정의 암호를 노출하지 않고 Kerberos 필터를 구성할 수 있습니다.	기본적으로 이 값은 비어 있습니다.

테이블24-17: HTTP 구성 속성

속성	설명	기본값
모든 IP 주소에 바인딩	모든 네트워크 인터페이스에 바인딩할지 여부입니다. 서버에 NIC가 두 개 이상 있고 특정 네트워크 인터페이스에 바인딩하려는 경우 이 속성의 선택을 취소합니다.	기본값은 True입니다.
호스트 이름 또는 IP 주소에 바인딩	HTTP 서비스가 제공되는 네트워크 인터페이스(IP 주소 또는 호스트 이름)를 지정합니다. 모든 IP 주소에 바인딩의 선택을 취소한 경우에만 값을 지정할 수 있습니다.	기본값은 localhost입니다.
HTTP 포트	HTTP 서비스가 제공되는 포트입니다.	기본값은 6405입니다. 허용되는 값 범위는 1 ~ 65535입니다.
최대 HTTP 머리글 크기	요청 및 응답 HTTP 헤더의 최대 허용 크기(바이트)입니다.	기본값은 32768입니다.

테이블24-18: 프록시를 통한 HTTP 구성 속성

속성	설명	기본값
프록시를 통한 HTTP 사용	WACS에서 HTTP through Proxy 커넥터를 사용할지 여부입니다. 이 옵션은 일반적으로 역방향 프록시가 사용된 배포 환경에서 선택됩니다.	기본값은 FALSE입니다.
모든 IP 주소에 바인딩	프록시 포트를 통한 HTTP를 모든 네트워크 인터페이스에 바인딩할지 여부입니다.	기본값은 True입니다.
호스트 이름 또는 IP 주소에 바인딩	프록시를 통한 HTTP 서비스가 제공되는 네트워크 인터페이스 (IP 주소 또는 호스트 이름)를 지정합니다. 모든 IP 주소에 바인딩의 선택을 취소한 경우에만 값을 지정할 수 있습니다.	기본값은 localhost입니다.
HTTP 포트	역방향 프록시 배포 환경에서 HTTP 서비스가 제공되는 포트입니다. 프록시를 통한 HTTP 사용을 선택한 경우에만 값을 지정할 수 있습니다.	기본값은 6406입니다. 허용되는 값 범위는 1 ~ 65535입니다.
프록시 호스트 이름	프록시 서버의 IPv4 주소, IPv6 주소, 호스트 이름 또는 정규화된 도메인 이름입니다. 프록시를 통한 HTTP 사용을 선택한 경우에만 값을 지정할 수 있습니다.	기본적으로 이 값은 비어 있습니다.
프록시 포트	정방향 또는 역방향 프록시 서버의 포트입니다. 프록시를 통한 HTTP 사용을 선택한 경우에만 값을 지정할 수 있습니다.	기본적으로 이 값은 0입니다. 허용되는 값 범위는 1 ~ 65535입니다.
최대 HTTP 머리글 크기	요청 및 응답 HTTP 헤더의 최대 허용 크기(바이트)입니다.	기본값은 32768입니다.

테이블24-19: HTTPS 구성 속성

속성	설명	기본값
HTTPS 사용	HTTPS/SSL 통신을 사용할지 여부입니다.	기본값은 FALSE입니다.

속성	설명	기본값
호스트 이름 또는 IP 주소에 바인딩	HTTPS 서비스가 제공되는 네트워크 인터페이스(IP 주소 또는 호스트 이름)를 지정합니다. HTTPS 사용을 선택한 경우에만 값을 지정할 수 있습니다.	기본값은 localhost입니다.
HTTPS 포트	HTTPS 서비스가 제공되는 포트입니다. HTTPS 사용을 선택한 경우에만 값을 지정할 수 있습니다.	기본값은 443입니다. 허용되는 값 범위는 1 ~ 65535입니다.
프록시 호스트 이름	프록시 서버의 IPv4 주소, IPv6 주소, 호스트 이름 또는 정규화된 도메인 이름입니다. HTTPS 사용을 선택한 경우에만 값을 지정할 수 있습니다.	기본적으로 이 값은 비어 있습니다.
프록시 포트	정방향 또는 역방향 프록시 서버의 포트입니다. HTTPS 사용을 선택한 경우에만 값을 지정할 수 있습니다.	기본적으로 이 값은 0입니다. 허용되는 값 범위는 1 ~ 65535입니다.
프로토콜	사용할 암호화 프로토콜입니다. HTTPS 사용을 선택한 경우에만 값을 지정할 수 있습니다.	기본값은 TLS입니다. 허용되는 값은 TLS 또는 SSL입니다.
인증서 저장소 유형	인증서 및 개인 키가 들어 있는 인증서 저장소의 유형입니다. 대부분의 경우 이 값은 PKCS12입니다. HTTPS 사용을 선택한 경우에만 값을 지정할 수 있습니다.	기본값은 PKCS12입니다. 허용되는 값은 PKCS12 또는 JKS입니다.
인증서 저장소 파일 위치	인증서에 대한 전체 경로입니다. HTTPS 사용을 선택한 경우에만 값을 지정할 수 있습니다.	기본적으로 이 값은 비어 있습니다.
개인 키 액세스 암호	PKCS12 인증서 저장소 및 JKS keystore에는 무단 액세스나 도용으로부터 보호하기 위해 암호로 보호되는 개인 키가 들어 있습니다. 인증서 저장소를 생성할 때 지정한 암호를 여기에 입력해야 WACS에서 인증서 저장소의 개인 키에 액세스할 수 있습니다. HTTPS 사용을 선택한 경우에만 값을 지정할 수 있습니다.	기본적으로 이 값은 비어 있습니다.

속성	설명	기본값
인증서 별칭	인증서 저장소 안에 있는 인증서의 별칭입니다. 지정하지 않으면 저장소에 인증서가 두 개 이상 있을 때 첫 번째 인증서가 사용됩니다. 대부분의 경우에는 값을 지정할 필요가 없습니다. HTTPS 사용을 선택한 경우에만 값을 지정할 수 있습니다.	기본적으로 이 값은 비어 있습니다.
클라이언트 인증 사용	클라이언트 인증을 사용하는 경우 인증서 신뢰 목록 파일에 저장된 키를 보유한 클라이언트만 WACS 서비스를 얻을 수 있습니다. 다른 클라이언트는 거부됩니다. HTTPS 사용을 선택한 경우에만 클라이언트 인증을 사용할 수 있습니다.	기본값은 FALSE입니다.
인증서 신뢰 목록 파일 위치	인증서 신뢰 목록 파일에 대한 전체 경로입니다. HTTPS 사용 및 클라이언트 인증 사용을 선택한 경우에만 값을 지정할 수 있습니다.	기본적으로 이 값은 비어 있습니다.
인증서 신뢰 목록 개인 키 액세스 암호	인증서 신뢰 목록 파일의 개인 키에 대한 액세스를 보호하는 암호입니다. HTTPS 사용 및 클라이언트 인증 사용을 선택한 경우에만 값을 지정할 수 있습니다.	기본적으로 이 값은 비어 있습니다.
최대 HTTP 머리글 크기	요청 및 응답 HTTP 헤더의 최대 허용 크기(바이트)입니다.	기본값은 32768입니다.

테이블24-20: 동시성 설정(커넥터마다)

속성	설명	기본값
최대 동시 요청 수	각 커넥터(HTTP, HTTP through Proxy 또는 HTTPS)에서 한 번에 처리할 수 있는 동시 HTTP 또는 HTTPS 요청의 개수입니다.	기본값은 150입니다. 허용되는 값 범위는 1 ~ 1000입니다.

테이블24-21: Active Directory 구성 설정

속성	설명	기본값
Krb5.ini 파일 위치	Kerberos 구성 속성을 저장하는 krb5.ini 파일의 전체 경로입니다.	기본적으로 이 값은 비어 있습니다.
bscLogin.conf 파일 위치	bscLogin.conf 파일의 전체 경로입니다.	기본적으로 이 값은 비어 있습니다.

24.1.3 연결 서비스 속성

연결 서비스 범주에는 다음 서비스가 포함됩니다.

- 네이티브 연결 서비스(독립 실행형 서버에 호스트됨)
- 네이티브 연결 서비스(32비트 독립 실행형 서버에 호스트됨)
- 적응형 연결 서비스(APS에 호스트됨)

모든 서비스에서 구성 설정이 동일하게 공유됩니다.

테이블24-22: 서비스 작업 속성

속성	설명	기본값
기억: 다음과 같은 서비스 작업 속성을 변경한 후에는 서버를 다시 시작하지 않아도 됩니다.		
연결 풀링	연결 풀을 사용하거나 사용하지 않도록 설정합니다. 가능한 값은 다음과 같습니다. <ul style="list-style-type: none"> • 사용 - 제한 시간 있음 • 사용 - 제한 시간 없음 • 사용 안 함 참고: 연결 풀은 서버 성능을 높이기 위해 연결을 재사용 가능한 상태로 유지하는 캐싱 기능입니다.	사용 - 제한 시간 있음

속성	설명	기본값
연결 풀 제한 시간	<p>풀에서 연결 최대 유휴 시간을 지정합니다(분).</p> <p>참고: 이 속성은 cs.cfg 파일의 Max Pool Time 매개 변수와 동일합니다. 풀을 사용하지 않도록 설정하는 동작은 Max Pool Time을 0으로 설정하는 동작과 같습니다. 제한 시간 없이 풀을 사용하도록 설정하는 작업은 Max Pool Time을 -1로 설정하는 동작과 같습니다. 자세한 내용은 데이터 액세스 가이드를 참조하십시오.</p>	60
임시 개체 유휴 제한 시간	서버에서 사용되지 않는 임시 개체를 보관하는 시간을 지정합니다(분). 개체가 나중에 제거되고 해당 리소스가 다시 사용됩니다.	60
임시 개체 타이머 간격	작업 검사 간 시간을 지정합니다(분). 서버에서 정기적으로 제거할 후보 개체를 검색합니다.	5
HTTP 청크 사용	<p>HTTP 청크를 사용하거나 사용하지 않도록 설정합니다.</p> <p>참고: HTTP 청크는 3계층 배포에만 해당하는 사항이며, 대용량 문서를 반입할 때 응답이 많을수록 왕복 시간이 짧아지므로 문서 열기/새로 고침 성능에 영향을 미칩니다. HTTP 청크를 사용하지 않도록 설정하는 동작은 HTTP 청크 크기를 0으로 설정하는 동작과 같습니다.</p>	사용
HTTP 청크 크기	서버에서 내보낸 HTTP 응답 크기(KB)를 지정합니다.	64

테이블24-23: 낮은 수준 추적 속성

속성	설명	기본값
<p>기억: 다음과 같은 낮은 수준 추적 속성을 변경한 후에는 서버를 다시 시작하지 않아도 됩니다.</p>		

속성	설명	기본값
작업 추적 사용	연결 서버 작업의 추적을 사용하도록 설정합니다. 참고: 이때 로그 수준 속성이 높음으로 설정되어야 합니다.	사용 안 함
미들웨어 추적 사용	모든 미들웨어의 추적을 사용하도록 설정합니다. 특정 미들웨어를 추적하려면 cs.cfg 파일을 구성하고 서버를 다시 시작해야 합니다. 참고: 이때 로그 수준 속성이 높음으로 설정되어야 합니다.	사용 안 함

테이블24-24: 활성 데이터 소스 속성

속성	설명	기본값
주의: 다음과 같은 활성 데이터 소스 속성을 변경하고 나면 서버를 다시 시작해야 합니다.		
데이터 소스 활성화	연결할 데이터 소스를 선택할 수 있습니다. 이 속성은 드라이버의 필터로 작동합니다. 사용할 드라이버를 로드하려면 활성 데이터 소스를 지정합니다. 주의: 기본 서버 동작은 사용 가능한 드라이버를 모두 로드하는 것입니다. 이 설정을 사용하여 서버를 특수화할 수 있으며, 이는 네트워크에 여러 개의 CORBA 서버를 배포해야 할 경우 특히 유용합니다. 기억: 선택한 데이터 소스의 드라이버만 로드되며, 그 이외의 드라이버는 모두 무시됩니다. 데이터 소스를 선택하지 않으면 서버에서 사용 가능한 모든 드라이버를 로드합니다. 참고: 서버 메트릭에서 선택한 데이터 소스가 활성화되었는지 확인하십시오. 네트워크 계층 및 데이터 소스는 연결 서비스 메트릭에 표시됩니다.	선택 안 함

속성	설명	기본값
네트워크 계층	<p>연결에 사용되는 네트워크 계층을 지정합니다.</p> <p>참고: 지역화되지 않은 이름만 허용됩니다. 사용 가능한 네트워크 계층 목록은 connectionserver-install-dir\WconnectionServer 디렉터리에 있는 driver.cfg 파일에 있습니다.</p>	<ul style="list-style-type: none"> 원시 CORBA 서버용 ODBC 적응형 CORBA 서버용 JDBC
데이터베이스	<p>연결에 사용되는 데이터베이스를 지정합니다.</p> <p>참고: 지역화되지 않은 이름만 허용됩니다. 데이터베이스 이름은 순수 ASCII 문자열일 경우 정규식이 될 수 있습니다. 패턴에서 GNU regexp 구문이 사용됩니다. * 패턴을 사용하여 모든 문자를 일치시킵니다. 예를 들어 MS SQL Server.*\$ 식은 모든 MS SQL Server 데이터베이스가 사용되었음을 나타냅니다. 정규식에 대한 자세한 내용은 PERL 웹 사이트 (http://www.perl.com/doc/manual/html/pod/perlre.html#Regular_Expressions)를 참조하십시오.</p>	이 필드는 데이터베이스 이름을 입력해야 채워집니다.

관련 항목

- 821 페이지에서 [일반 서버 속성](#)

24.1.4 Crystal Reports 서비스 속성

Crystal Reports 서비스 범주에는 다음 서버가 포함됩니다.

- Crystal Reports 캐시 서버
- Crystal Reports 처리 서버
- Crystal Reports 2011 Report Application Server 속성
- Crystal Reports 2011 처리 서버

Crystal Reports 캐시 서버 속성

Crystal Reports 캐시 서버와 Crystal Reports 처리 서버에 적용되는 모든 속성은 동일한 값으로 설정되어야 합니다. 예를 들어, 캐시 서버에서 뷰어를 새로 고칠 경우 항상 현재 데이터 표시 설정을 TRUE로 설정한 경우 처리 서버에서도 동일한 속성을 TRUE로 설정해야 합니다.

참고:

이러한 서버 속성을 수정한 경우 변경 내용을 적용하려면 서버를 다시 시작해야 합니다.

테이블24-25: Crystal Reports 캐시 서비스 속성

속성	설명	기본값
뷰어를 새로 고칠 경우 항상 현재 데이터 표시	<p>사용자가 보고서를 명시적으로 새로 고칠 때 기존의 캐시된 페이지를 모두 무시하고 데이터베이스에서 새 데이터를 직접 가져올지 여부를 지정합니다.</p> <p>참고: 이 속성은 보고서 개체 자체에 설정할 수 있으며 보고서마다 다르게 설정할 수도 있습니다. 보고서 개체에 지정된 값은 서버 설정보다 우선적으로 적용됩니다. 보고서 개체에 값을 지정하려면 CMC에서 보고서를 선택하고 기본 설정 > 서버 그룹 보기를 클릭합니다.</p>	기본값은 True입니다.
클라이언트 간에 보고서 데이터 공유	<p>여러 클라이언트에서 보고서 데이터를 공유할지 여부를 지정합니다.</p> <p>참고: 이 속성은 보고서 개체 자체에 설정할 수 있으며 보고서마다 다르게 설정할 수도 있습니다. 보고서 개체에 지정된 값은 서버 설정보다 우선적으로 적용됩니다.</p>	기본값은 True입니다.
유틸리티 연결 제한 시간 (분)	Crystal Reports 캐시 서버가 유틸리티 연결 요청을 대기하는 시간(분)을 지정합니다. 대개는 기본값을 수정하지 않아도 됩니다.	기본값은 20분입니다.
보안 캐시 제한 시간 (분)	서버가 CMS 쿼리 전에 요청을 처리하기 위해 캐시된 로그인 자격 증명, 보고서 매개 변수 및 데이터 연결 정보를 사용하는 시간(분)을 지정합니다.	기본값은 20분입니다.

속성	설명	기본값
클라이언트에 전달되는 가장 오래된 주문형 데이터(초)	<p>서버가 주문형 보고서의 요청에 따라 캐시된 데이터를 사용하는 시간(초)을 지정합니다. 과거의 요청에 따라 이전에 생성한 데이터를 사용하여 처리할 수 있는 요청이 서버에 전달된 경우 데이터가 생성된 이후 경과된 시간이 여기에 설정된 값보다 작으면 서버에서는 현재의 요청을 처리할 때 해당 데이터를 재사용합니다. 이와 같이 데이터를 재사용하면 여러 사용자가 동일한 정보를 필요로 하는 경우에 시스템 성능을 크게 높일 수 있습니다. 이 값을 설정할 때는 사용자에게 최신 데이터를 제공하는 것이 어느 정도로 중요한지 고려해야 합니다. 중요한 데이터는 자주 변경될 수 있으므로 모든 사용자에게 최신 데이터를 제공하는 것이 매우 중요한 경우에는 이 값을 0으로 설정하여 데이터가 이와 같이 재사용되지 않도록 해야 할 수도 있습니다.</p> <p>참고: 이 속성은 보고서 개체 자체에 설정할 수 있으며 보고서마다 다르게 설정할 수도 있습니다. 보고서 개체에 지정된 값은 서버 설정보다 우선적으로 적용됩니다.</p>	기본값은 0초입니다.
최대 캐시 크기(KB)	보고서를 캐시하는 데 사용되는 하드 디스크 공간(KB)의 크기를 지정합니다. 서버에서 많은 보고서나 특별히 복잡한 보고서를 처리해야 하는 경우에는 캐시 크기를 늘려야 할 수 있습니다.	기본값은 256000KB입니다.
캐시 파일 디렉터리	캐시 파일 디렉터리의 위치를 지정합니다.	%DefaultDataDir%/CrystalReportsCachingServer/temp
Java VM 인수	JVM에 제공할 수 있는 명령줄 인수를 지정합니다.	기본 값은 비어 있습니다.

Crystal Reports 처리 서버 속성

Crystal Reports 캐시 서버와 Crystal Reports 처리 서버에 적용되는 모든 속성은 동일한 값으로 설정되어야 합니다. 예를 들어, 캐시 서버에서 뷰어를 새로 고칠 경우 항상 현재 데이터 표시 설정을 TRUE로 설정한 경우 처리 서버에서도 동일한 속성을 TRUE로 설정해야 합니다.

참고:

이러한 서버 속성을 수정한 경우 변경 내용을 적용하려면 서버를 다시 시작해야 합니다.

테이블24-26: Crystal Reports 처리 서비스 속성

속성	설명	기본값
유틸 작업 제한 시간 (분)	Crystal Reports 처리 서버가 지정된 작업에 대한 여러 요청 사이에 대기하는 시간(분)을 지정합니다.	기본값은 60분입니다.
자식당 최대 수명 작업	각 자식 프로세스의 수명당 관리할 수 있는 최대 작업 수를 지정합니다.	기본값은 1000입니다.
뷰어를 새로 고칠 경우 항상 현재 데이터 표시	<p>사용자가 보고서를 명시적으로 새로 고칠 때 기존의 캐시된 페이지를 모두 무시하고 데이터베이스에서 새 데이터를 직접 가져올지 여부를 지정합니다. 여러 클라이언트에서 보고서 데이터를 공유할지 여부를 지정합니다.</p> <p>참고: 이 속성은 보고서 개체 자체에 설정할 수 있으며 보고서마다 다르게 설정할 수도 있습니다. 보고서 개체에 지정된 값은 서버 설정보다 우선적으로 적용됩니다. 보고서 개체에 값을 지정하려면 CMC에서 보고서를 선택하고 기본 설정 > 서버 그룹 보기를 클릭합니다.</p>	기본값은 True입니다.
클라이언트 간에 보고서 데이터 공유	<p>여러 클라이언트에서 보고서 데이터를 공유할지 여부를 지정합니다. 여러 클라이언트에서 보고서 데이터를 공유할지 여부를 지정합니다.</p> <p>참고: 이 속성은 보고서 개체 자체에 설정할 수 있으며 보고서마다 다르게 설정할 수도 있습니다. 보고서 개체에 지정된 값은 서버 설정보다 우선적으로 적용됩니다.</p>	기본값은 True입니다.
유틸 연결 제한 시간 (분)	Crystal Reports 처리 서버가 유틸 연결 요청을 대기하는 시간(분)을 지정합니다. 대개는 기본값을 수정하지 않아도 됩니다.	기본값은 20분입니다.
최대 동시 작업(자동의 경우 0)	Crystal Reports 처리 서버에서 동시에 실행할 수 있는 독립적인 작업의 최대 개수를 지정합니다. 이 속성의 값을 0으로 설정하면 서버가 실행되고 있는 컴퓨터의 CPU와 메모리에 따라 적절한 값이 적용됩니다.	기본값은 0입니다.

속성	설명	기본값
클라이언트에 전달되는 가장 오래된 주문형 데이터(초)	<p>서버가 주문형 보고서의 요청에 따라 캐시된 데이터를 사용하는 시간(초)을 지정합니다. 과거의 요청에 따라 이전에 생성한 데이터를 사용하여 처리할 수 있는 요청이 서버에 전달된 경우 데이터가 생성된 이후 경과된 시간이 여기에 설정된 값보다 작으면 서버에서는 현재의 요청을 처리할 때 해당 데이터를 재사용합니다. 이와 같이 데이터를 재사용하면 여러 사용자가 동일한 정보를 필요로 하는 경우에 시스템 성능을 크게 높일 수 있습니다. 이 값을 설정할 때는 사용자에게 최신 데이터를 제공하는 것이 어느 정도로 중요한지 고려해야 합니다. 중요한 데이터는 자주 변경될 수 있으므로 모든 사용자에게 최신 데이터를 제공하는 것이 매우 중요한 경우에는 이 값을 0으로 설정하여 데이터가 이와 같이 재사용되지 않도록 해야 할 수도 있습니다.</p> <p>참고: 이 속성은 보고서 개체 자체에 설정할 수 있으며 보고서마다 다르게 설정할 수도 있습니다. 보고서 개체에 지정된 값은 서버 설정보다 우선적으로 적용됩니다.</p>	기본값은 0입니다.
미리 시작한 자식의 최대 수	서버에서 허용하는 미리 시작된 자식 프로세스의 최대 개수를 지정합니다. 이 값이 너무 낮을 경우 서버는 요청을 받은 후에 자식 프로세스를 만들게 되므로 대기 시간이 생길 수 있습니다. 이 값이 너무 높을 경우 유휴 자식 프로세스로 인해 시스템 리소스가 불필요하게 낭비될 수 있습니다.	기본값은 자식 1개입니다.
임시 디렉터리	<p>필요한 경우 임시 파일을 만드는 디렉터리를 지정합니다.</p> <p>참고: 이 디렉터리의 디스크 공간이 충분하지 않은 경우 성능 문제가 발생할 수 있습니다.</p>	%DefaultDataDir%/CrystalReportsProcessingServer/temp
Java 클래스 경로	서버에 필요한 Java 클래스의 이름 및 경로입니다.	%CommonJavaLibDir%/procCR.jar
Java 하위 VM 인수	서버에서 만든 자식 프로세스에 제공되는 명령줄 인수를 지정합니다.	Dbusinessobjects.connectivity.directory=%EnterpriseDir%/dataAccess/connectionServer,Xmx512m,XX:MaxPermSize=128m

테이블24-27: 단일 로그인(SSO) 서비스 속성

속성	설명	기본값
단일 로그인 만료(초)	SSO 연결이 유효한 시간(초)을 지정합니다.	기본값은 86400초입니다.

Crystal Reports 2011 Report Application Server 속성

참고:

이러한 속성을 수정한 경우 변경 내용을 적용하려면 서버를 다시 시작해야 합니다.

테이블24-28: Crystal Reports 2011 보기 및 수정 서비스 속성

속성	설명	기본값
보고서 작업을 닫을 때까지 보고서 작업을 데이터베이스에 연결된 상태로 유지	프로세스가 실행될 때까지 보고서 작업을 데이터베이스에 연결된 상태로 유지할지 여부를 지정합니다.	기본값은 FALSE입니다.
찾을 데이터 크기(레코드)	특정 필드의 값을 탐색할 때 데이터베이스에서 반환되는 고유한 레코드의 수를 지정합니다. 먼저 클라이언트의 캐시에서 데이터를 가져온 다음 해당되는 경우 서버의 캐시에서도 데이터를 가져옵니다. 어떠한 캐시에도 데이터가 없으면 데이터베이스에서 데이터를 검색합니다.	기본값은 레코드 100개입니다.
유틸 연결 제한 시간(분)	Report Application Server(RAS)가 유틸 클라이언트의 요청을 대기하는 시간(분)을 지정합니다. 값을 너무 낮게 설정하면 사용자의 요청이 중간에 중단될 수 있고 너무 높게 설정하면 서버의 확장성에 영향을 미칠 수 있습니다. 예를 들어, ReportClientDocument 개체를 명시적으로 닫지 않으면 유틸 작업이 닫힐 때까지 서버가 불필요하게 대기할 수 있습니다.	기본값은 30분입니다.
배치 크기(레코드)	각 데이터 전송 중에 데이터베이스에서 반환되는 결과 집합의 행 수를 지정합니다. 예를 들어, 레코드 500개를 요청하고 배치 크기 속성이 레코드 100개로 설정된 경우 데이터는 100개 행으로 구성된 개별 배치 5개로 반환됩니다. RAS 성능을 개선하려면 네트워크 환경, 데이터베이스 및 요청 유형을 파악하여 적절한 배치 크기를 설정해야 합니다.	기본값은 레코드 100개입니다.

속성	설명	기본값
보고서 미리 보기 또는 새로 고침 시 읽을 데이터베이스 레코드의 수(무제한의 경우 -1)	<p>보고서를 미리 보거나 새로 고칠 때 읽을 데이터베이스 레코드의 수를 지정합니다. 이 설정은 사용자가 쿼리 또는 보고서를 실행할 때 서버가 데이터베이스에서 가져오는 레코드 수를 제한합니다. 이 설정은 사용자가 지나치게 큰 레코드 집합을 반환하는 주문형 보고서를 실행하지 못하도록 하려는 경우에 유용합니다.</p> <p>이와 같은 방식으로 보고서 일정을 설정하면 사용자들이 원하는 보고서를 더 빨리 제공하면서도 이러한 대형 쿼리로 인한 데이터베이스의 작업 부하를 줄일 수 있습니다.</p>	기본값은 레코드 20000개입니다.
최대 동시 보고서 작업 수(무제한의 경우 0)	RAS에서 동시에 실행할 수 있는 독립적인 작업의 최대 개수를 지정합니다.	기본값은 작업 75개입니다.
클라이언트에 전달되는 가장 오래된 주문형 데이터(분)	주문형 보고서가 캐시된 보고서 데이터를 사용하는 시간(분)을 지정합니다.	기본값은 20분입니다.
임시 디렉터리	<p>필요한 경우 임시 파일을 만드는 디렉터리를 지정합니다.</p> <p>참고: 이 디렉터리의 디스크 공간이 충분하지 않은 경우 성능 문제가 발생할 수 있습니다.</p>	%DefaultDataDir%/CrystalReportsRasServer/temp

테이블24-29: 단일 로그인(SSO) 서비스 속성

속성	설명	기본값
단일 로그인 만료(초)	SSO 연결이 유효한 시간(초)을 지정합니다.	기본값은 86400초입니다.

Crystal Reports 2011 처리 서버 속성

참고:

이러한 속성을 수정한 경우 변경 내용을 적용하려면 서버를 다시 시작해야 합니다.

테이블24-30: Crystal Reports 2011 처리 서비스 속성

속성	설명	기본값
유틸 작업 제한 시간 (분)	Crystal Reports 처리 서버가 지정된 작업에 대한 여러 요청 사이에 대기하는 시간(분)을 지정합니다.	기본값은 60분입니다.
자식당 최대 수명 작업	각 자식 프로세스의 수명당 관리할 수 있는 최대 작업 수를 지정합니다.	기본값은 1000입니다.
뷰어를 새로 고칠 경우 항상 현재 데이터 표시	<p>사용자가 보고서를 명시적으로 새로 고칠 때 기존의 캐시된 페이지를 모두 무시하고 데이터베이스에서 새 데이터를 직접 가져올지 여부를 지정합니다. 여러 클라이언트에서 보고서 데이터를 공유할지 여부를 지정합니다.</p> <p>참고: 이 속성은 보고서 개체 자체에 설정할 수 있으며 보고서마다 다르게 설정할 수도 있습니다. 보고서 개체에 지정된 값은 서버 설정보다 우선적으로 적용됩니다. 보고서 개체에 값을 지정하려면 CMC에서 보고서를 선택하고 기본 설정 > 서버 그룹 보기를 클릭합니다.</p>	기본값은 True입니다.
클라이언트 간에 보고서 데이터 공유	<p>여러 클라이언트에서 보고서 데이터를 공유할지 여부를 지정합니다. 여러 클라이언트에서 보고서 데이터를 공유할지 여부를 지정합니다.</p> <p>참고: 이 속성은 보고서 개체 자체에 설정할 수 있으며 보고서마다 다르게 설정할 수도 있습니다. 보고서 개체에 지정된 값은 서버 설정보다 우선적으로 적용됩니다.</p>	기본값은 True입니다.
유틸 연결 제한 시간 (분)	Crystal Reports 처리 서버가 유틸 연결 요청을 대기하는 시간(분)을 지정합니다. 대개는 기본값을 수정하지 않아도 됩니다.	기본값은 20분입니다.
최대 동시 작업(자동의 경우 0)	Crystal Reports 처리 서버에서 동시에 실행할 수 있는 독립적인 작업의 최대 개수를 지정합니다. 이 속성의 값을 0으로 설정하면 서버가 실행되고 있는 컴퓨터의 CPU와 메모리에 따라 적절한 값이 적용됩니다.	기본값은 0입니다.

속성	설명	기본값
클라이언트에 전달되는 가장 오래된 주문형 데이터(초)	<p>서버가 주문형 보고서의 요청에 따라 캐시된 데이터를 사용하는 시간(초)을 지정합니다. 과거의 요청에 따라 이전에 생성한 데이터를 사용하여 처리할 수 있는 요청이 서버에 전달된 경우 데이터가 생성된 이후 경과된 시간이 여기에 설정된 값보다 작으면 서버에서는 현재의 요청을 처리할 때 해당 데이터를 재사용합니다. 이와 같이 데이터를 재사용하면 여러 사용자가 동일한 정보를 필요로 하는 경우에 시스템 성능을 크게 높일 수 있습니다. 이 값을 설정할 때는 사용자에게 최신 데이터를 제공하는 것이 어느 정도로 중요한지 고려해야 합니다. 중요한 데이터는 자주 변경될 수 있으므로 모든 사용자에게 최신 데이터를 제공하는 것이 매우 중요한 경우에는 이 값을 0으로 설정하여 데이터가 이와 같이 재사용되지 않도록 해야 할 수도 있습니다.</p> <p>참고: 이 속성은 보고서 개체 자체에 설정할 수 있으며 보고서마다 다르게 설정할 수도 있습니다. 보고서 개체에 지정된 값은 서버 설정보다 우선적으로 적용됩니다.</p>	기본값은 0입니다.
미리 시작한 자식의 최대 수	서버에서 허용하는 미리 시작된 자식 프로세스의 최대 개수를 지정합니다. 이 값이 너무 낮을 경우 서버는 요청을 받은 후에 자식 프로세스를 만들게 되므로 대기 시간이 생길 수 있습니다. 이 값이 너무 높을 경우 유휴 자식 프로세스로 인해 시스템 리소스가 불필요하게 낭비될 수 있습니다.	기본값은 자식 1개입니다.
임시 디렉터리	<p>필요한 경우 임시 파일을 만드는 디렉터리를 지정합니다.</p> <p>참고: 이 디렉터리의 디스크 공간이 충분하지 않은 경우 성능 문제가 발생할 수 있습니다.</p>	%DefaultDataDir%/CrystalReportsProcessingServer/temp
보고서 작업을 닫을 때까지 보고서 작업을 데이터베이스에 연결된 상태로 유지	작업을 닫을 때까지 보고서 작업을 데이터베이스에 연결된 상태로 유지할지 여부를 지정합니다.	기본값은 FALSE입니다.

속성	설명	기본값
미리 보기 또는 새로 고침 시 데이터베이스 레코드 읽기	<p>보고서를 미리 보거나 새로 고칠 때 읽을 데이터베이스 레코드의 수를 지정합니다. 이 설정은 사용자가 쿼리 또는 보고서를 실행할 때 서버가 데이터베이스에서 가져오는 레코드 수를 제한합니다. 이 설정은 사용자가 지나치게 큰 레코드 집합을 반환하는 주문형 보고서를 실행하지 못하도록 하려는 경우에 유용합니다.</p> <p>이와 같은 방식으로 보고서 일정을 설정하면 사용자들이 원하는 보고서를 더 빨리 제공하면서도 이러한 대형 쿼리로 인한 데이터베이스의 작업 부하를 줄일 수 있습니다.</p>	기본값은 20000입니다.

테이블24-31: 단일 로그인(SSO) 서비스 속성

속성	설명	기본값
단일 로그인 만료(초)	SSO 연결이 유효한 시간(초)을 지정합니다.	기본값은 86400초입니다.

24.1.5 분석 서비스 속성

분석 서비스 범주에는 적응형 처리 서버가 포함됩니다.

테이블24-32: 다차원 분석 서비스 속성

속성	설명	기본값
최대 클라이언트 세션 수	서버에서 동시에 열 수 있는 최대 MDAS 세션 수를 지정합니다. 열려 있는 세션의 수가 이 값에 도달한 경우 MDAS 세션을 시작하려고 하면 서버를 사용할 수 없음이라는 오류 메시지가 표시됩니다. 사용자 요구 사항 및 사용 가능한 하드웨어에 맞게 MDAS 성능을 최적화하기 위해 이 값을 변경할 수 있지만, 값을 늘리면 MDAS와 데이터베이스에서 모두 성능 문제가 발생할 수 있습니다. 기본값인 세션 15개는 보수적으로 설정한 값입니다. 사용자 쿼리가 적은 설치 환경의 경우 이 값을 크게 늘릴 수 있지만 사용자 쿼리가 많은 설치에서는 이 값을 낮게 설정해야 합니다.	기본값은 15로 설정되어 있습니다. 유효한 범위는 1~100입니다.
쿼리에 의해 반환되는 최대 셀 수	단일 쿼리에서 사용자에게 반환되는 셀 수를 지정합니다. 사용자가 극히 많은 수의 셀을 반환하여 대량의 메모리를 사용하는 쿼리를 실행하지 못하게 방지합니다. 사용자의 쿼리가 이 셀 한계를 초과하는 경우 오류 메시지가 표시됩니다.	기본값은 100,000개의 셀입니다.
필터링 시 반환되는 최대 멤버 수	멤버를 기준으로 필터링 시 검색되는 멤버 수를 지정합니다. 검색된 멤버 중 매우 많은 수의 멤버가 대량의 메모리를 사용할 수 있습니다.	기본값은 3,000개의 멤버입니다.

테이블24-33: BEx 웹 응용 프로그램 서비스 속성

속성	설명	기본값
최대 클라이언트 세션 수	서비스에서 허용되는 클라이언트 세션의 최대 개수입니다.	기본값은 세션 15개입니다.
SAP BW 마스터 시스템	BI 플랫폼에서 만든 BW 시스템에 대한 OLAP 연결의 이름입니다.	기본값은 SAP_BW입니다.
JCo 서버 RFC 대상	BW 시스템에 입력한 JCo 서버 RFS 대상의 이름입니다.	기본적으로 이 값은 비어 있습니다.
JCo 서버 게이트웨이 호스트	BW 시스템에서 정의한 JCo 서버 게이트웨이 호스트의 이름입니다.	기본적으로 이 값은 비어 있습니다.
JCo 서버 게이트웨이 서비스	BW 시스템에서 정의한 JCo 서버 게이트웨이 호스트의 이름입니다.	기본적으로 이 값은 비어 있습니다.

속성	설명	기본값
JCo 서버 연결 수	서비스에 대해 ABAP에서 Java로의 호출을 처리하는 데 사용할 수 있는 자동 생성 프로그램 수를 지정합니다.	기본값은 연결 3개입니다.

24.1.6 데이터 연합 서비스 속성

데이터 연합 서비스 범주에는 적응형 처리 서버가 포함됩니다.

테이블24-34: 데이터 연합 서비스 속성

속성	설명	기본값
최대 연결	서버에서 허용하는 최대 연결 수를 지정합니다.	기본값은 32767입니다.
실행 풀 크기	특정한 순간에 병렬 실행 가능한 최대 쿼리 수를 지정합니다.	기본값은 10입니다.
연결 비활성 제한 시간	비활성 연결이 닫힌 후의 시간(초)을 지정합니다.	기본값은 1080초입니다.
문 비활성 제한 시간	비활성 쿼리 문이 닫힌 후의 시간(초)을 지정합니다.	기본값은 60초입니다.

24.1.7 Web Intelligence 서비스 속성

Web Intelligence 서비스 범주에는 다음 서버가 포함됩니다.

- 적응형 처리 서버
- Web Intelligence 처리 서버

적응형 처리 서버 설정

테이블24-35: Web Intelligence APS 모니터링 서비스

속성	설명	기본값입니다.
모니터링 사용	해당 서비스에 모니터링을 사용할지 여부를 지정합니다.	기본값은 TRUE입니다.
모니터링 스레드 루프 지연(초)	서비스에서 클라이언트에 대한 ping 수행 시도 간의 시간(초)을 지정합니다.	기본값은 300초입니다.
모니터링한 리소스 기본 정리 제한 시간(초)	서비스가 클라이언트 세션 정리를 수행하기 전에 비활성 클라이언트를 기다리는 시간(초)을 지정합니다.	기본값은 1200초입니다.
모니터링한 리소스 기본 바꾸기 제한 시간(초)	서비스가 클라이언트 세션을 하드 디스크로 교체하기 전에 비활성 클라이언트를 기다리는 시간(초)을 지정합니다. 모니터링한 리소스 기본 정리 제한 시간 속성 값보다 낮은 값을 지정하는 것이 좋습니다.	기본값은 600초입니다.

테이블24-36: 시각화 서비스 속성

속성	설명	기본값
시각화 엔진 정리 제한 시간(초)	서비스가 클라이언트 세션 정리를 수행하기 전에 비활성 클라이언트를 기다리는 시간(초)을 지정합니다.	기본값은 1200초입니다.
시각화 엔진 교체 제한 시간(초)	서비스가 클라이언트 세션을 하드 디스크로 교체하기 전에 비활성 클라이언트를 기다리는 시간(초)을 지정합니다. 시각화 엔진 정리 제한 시간(초) 속성 값보다 낮은 값을 지정하는 것이 좋습니다.	기본값은 600초입니다.

Web Intelligence 처리 서버 속성

Web Intelligence 처리 서버 속성은 다음과 같은 서비스로 나뉩니다.

- Information Engine
- Web Intelligence Core
- Web Intelligence Processing
- Web Intelligence Common

임계값 설정은 별도의 표에 정리되어 있습니다.

테이블24-37: Information Engine Service 설정

속성	설명	기본값
값 목록 캐시 사용	Web Intelligence 처리 서버에서 값 목록에 대해 캐싱을 사용할지 여부를 지정합니다.	기본값은 TRUE입니다.
값 목록 배치 크기(항목)	각 값 목록 배치의 최대 항목 수 (또는 값)를 지정합니다.	기본값은 배치당 항목 1000개입니다.
최대 사용자 지정 정렬 크기(항목)	사용자 지정 정렬에 포함되는 최대 항목 수를 지정합니다.	기본값은 사용자 지정 정렬당 항목 100개입니다.
유니버스 캐시 최대 크기(유니버스)	Web Intelligence 처리 서버에서 캐싱할 유니버스의 수를 지정합니다.	기본값은 유니버스 20개입니다.
최대 값 목록 크기(항목)	각 값 목록에 대해 최대 항목 수 (또는 값)를 지정합니다.	기본값은 값 목록당 항목 50000개입니다.

테이블24-38: Web Intelligence 핵심 서비스 설정

속성	설명	기본값
재활용 전 제한 시간(초)	처리된 총 문서 수가 재활용 전 최대 문서 수 속성에서 지정된 값을 초과할 경우 SIA(Server Intelligence Agent)가 서버를 중단하고 다시 시작할 때까지 서버가 유휴 상태인 시간(초)을 지정합니다.	기본값은 1200초입니다.
유휴 문서 제한 시간(초)	지정한 시간(초)이 지나면 Web Intelligence 처리 서버 세션이 교체됩니다. 이 시간 안에 클라이언트가 요청을 생성하지 않으면 활성 세션을 위한 리소스 확보를 위해 이 세션이 하드 디스크로 교체됩니다.	기본값은 300초입니다. 유효한 범위는 100~1000초입니다.
서버 폴링 간격(초)	지정한 시간(분)이 지나면 서버가 새 스레드 요청에 대해 폴링합니다. 서버가 폴링 단계에 있을 때는 사용되지 않는 문서 교체와 같은 정리 작업을 수행하여 서버 메모리가 상위 메모리 임계값 미만이 되도록 유지합니다.	기본값은 120초입니다.

속성	설명	기본값
사용자당 최대 문서 수	특정 시간에 사용자와 연결될 수 있는 활성 세션(Web Intelligence 문서)의 최대 개수를 지정합니다. 기본값이 5일 경우 사용자는 한 번에 최대 5개의 활성 세션을 사용할 수 있습니다.	기본값은 5입니다. 유효한 범위는 1~20입니다.
재활용 전 최대 문서 수	서버의 재활용을 고려하기 전에 처리할 수 있는 Web Intelligence 문서 수를 지정합니다. 처리한 문서 수가 이 값에 도달하고 서버가 유휴 상태가 되면 서버는 종료되고 SIA(Server Intelligence Agent)에서 서버의 새 인스턴스를 시작합니다. 그러나 서버의 새 인스턴스가 시작될 때까지 시간 지연이 나타납니다. 이 시간 지연은 재활용 전 제한 시간 속성으로 정의됩니다.	기본값은 문서 50개입니다.
문서 맵 최대 크기 오류 허용	최대 연결 수 속성을 제한할지 여부를 지정합니다. 이 속성을 사용하면 최대 연결 수 속성에 설정된 값을 서버에서 인식합니다. 설정하지 않으면 속성이 무시됩니다.	기본값은 TRUE입니다.
유휴 연결 제한 시간(분)	서버가 유휴 연결 요청을 대기하는 시간(분)을 지정합니다. 값을 너무 낮게 설정하면 요청이 중간에 중단될 수 있습니다. 반면에 값을 너무 높게 설정하면 유휴 요청이 중단될 때까지 대기하는 동안 새로운 요청이 대기열에 머무르게 됩니다.	기본값은 20분입니다.

속성	설명	기본값
최대 연결 수	<p>한 번에 열 수 있는 동시 세션의 최대 개수를 지정합니다. 이것은 근사치입니다. 이 설정은 교체된 비활성 세션이나 세션 수 분석을 위해 만들어진 세션을 계산에 포함하지 않습니다. 이 제한에 도달했으며 다른 서버에서도 요청을 처리할 수 없는 경우 사용자에게 오류 메시지가 전달됩니다.</p> <p>참고: 서버에서 이 속성을 인식할 수 있도록 문서 맵 최대 크기 오류 허용 속성을 사용해야 합니다.</p>	기본값은 세션 50개입니다. 유효한 범위는 5~65535입니다.
메모리 분석 사용	<p>메모리 분석을 사용할지 여부를 지정합니다. 이 속성을 사용할 경우 다음 속성이 활성화되어 서버에서 인식됩니다.</p> <ul style="list-style-type: none"> • 메모리 최대 임계값 • 메모리 상위 임계값 • 메모리 하위 임계값 <p>서버의 프로세스 메모리가 메모리 상위 임계값을 초과할 경우 문서를 저장하는 작업만 허용됩니다. 프로세스 메모리가 메모리 최대 임계값을 초과할 경우 모든 작업이 중단되어 실패합니다.</p>	기본값은 TRUE입니다.
메모리 최대 임계값(MB)	메모리 사용량의 최대 임계값을 지정합니다.	기본값은 6000MB입니다.
메모리 상위 임계값(MB)	메모리 사용량의 상위 임계값을 지정합니다.	기본값은 4500MB입니다.
메모리 하위 임계값(MB)	메모리 사용량의 하위 임계값을 지정합니다.	기본값은 3500MB입니다.
PJS 서비스 모니터링 사용	적응형 처리 서버에서 호스팅되는 PJS 서비스에서 서버 모니터링을 사용합니다.	기본값은 TRUE입니다.

속성	설명	기본값
PJS 서비스 핑 실패 시 재시도 횟수	PJS 서비스에 접속할 수 없다고 판단하기 전에 수행되는 서버의 PJS 서비스 접속 시도 횟수를 지정합니다.	기본값은 3번입니다.
PJS 서비스 모니터링 스레드 기간	PJS 서비스에 접속 시도 사이의 지연 기간을 지정합니다.	기본값은 300초입니다.

테이블24-39: Web Intelligence 처리 서비스 설정

속성	설명	기본값
HTTP URL 사용 허용	서버가 원격으로 저장되는 파일에 액세스할 수 있는지 여부를 지정합니다.	기본값은 TRUE입니다.
프록시 값	네트워크의 프록시 서버 주소를 지정합니다. 네트워크에 프록시 서버가 있고 원격으로 저장되는 파일에 액세스하려는 경우에만 값을 지정해야 합니다.	기본 값은 비어 있습니다.

테이블24-40: Web Intelligence 공통 서비스 설정

속성	설명	기본값
캐시 제한 시간(분)	지정한 시간(분)이 지나면 문서 캐시의 내용이 지워집니다. 제한 시간은 각 문서에 마지막으로 액세스한 날짜에 따라 결정됩니다.	기본값은 4370분입니다.
문서 캐시 정리 간격(분)	최대 문서 캐시 크기, 최대 문서 캐시 감소 공간, 캐시의 최대 문서에 대해 문서 캐시를 검사하고 확인하는 간격(분)을 지정합니다.	기본값은 120분입니다.
캐시 공유 사용 안 함	캐시 공유를 사용하지 않을지 여부를 지정합니다. 캐시 공유 기능은 기본적으로 사용됩니다. 즉, 모든 Web Intelligence 처리 서버 인스턴스는 동일한 캐시를 공유합니다. 그러나 Web Intelligence 처리 서버의 인스턴스당 캐시 1개를 사용하려는 경우에는 이 속성을 사용해야 합니다.	기본값은 FALSE입니다.

속성	설명	기본값
문서 캐시 사용	문서 캐시를 사용할지 여부를 지정합니다. 이 속성이 사용되는 경우 예약된 Web Intelligence 문서로 캐시를 미리 로드할 수 있습니다.	기본값은 TRUE입니다.
실시간 캐시 사용	실시간 캐시를 사용할지 여부를 지정합니다. 이 속성이 사용되는 경우 캐시를 동적으로 로드할 수 있습니다. 그러므로 Web Intelligence 문서가 표시되면 Web Intelligence 처리 서버는 이 문서를 캐싱합니다. 서버는 이러한 문서가 예약 작업으로 실행될 때도 문서를 캐싱합니다. 그러나 이 경우 문서에서 사전 캐시 기능이 사용되어야 합니다.	기본값은 TRUE입니다.
최대 문서 캐시 크기(KB)	문서 캐시의 최대 크기를 지정합니다. 제한에 도달하면 최대 문서 캐시 감소 공간 속성에 따라 문서 캐시가 지워집니다.	기본값은 1000000KB입니다.
최대 문서 캐시 감소 공간	새 작업과 결과를 캐시에 저장할 수 있도록 비워지는 캐시의 백분율을 지정합니다. 마지막으로 액세스한 시간이 가장 오래된 문서가 제거됩니다.	기본값은 70%입니다.
최대 문자 스트림 크기(MB)	Web Intelligence 클라이언트에 전송되는 최대 문자 스트림 크기를 지정합니다. 참고: 최대 문자 스트림 크기 속성을 초과할 경우 Web Intelligence 문서를 만들지 않고 클라이언트에 오류 메시지를 전달합니다.	기본값은 5MB입니다. 유효한 범위는 1~65535MB입니다.
이진 스트림 최대 크기(MB)	Web Intelligence 클라이언트에 전송되는 이진 스트림의 최대 크기(MB)를 지정합니다. 참고: 이진 스트림 최대 크기 속성을 초과할 경우 Web Intelligence 문서를 만들지 않고 클라이언트에 오류 메시지를 전달합니다.	기본값은 50MB입니다. 유효한 범위는 1~65535MB입니다.

속성	설명	기본값
캐시의 최대 문서	<p>캐시에 최대 저장할 수 있는 Web Intelligence 문서 수입니다. 캐시에 있는 문서 수가 이 수보다 많아서는 안 됩니다. 즉, 총 캐시 크기가 최대 문서 캐시 감소 공간(MB) 설정에 지정된 값보다 커서는 안 됩니다.</p> <p>참고: 시스템 성능을 높이려면 실시간 캐시 사용이 선택된 경우 이 값을 0으로 설정하십시오. 실시간 캐시 사용을 선택하지 않은 경우에는 이 값을 입력해야 합니다.</p>	기본값은 0입니다. 유효한 범위는 문서 0~65535개입니다.
이미지 디렉터리	이미지 디렉터리의 위치를 지정합니다.	기본 값은 비어 있습니다.
출력 캐시 디렉터리	캐시의 위치를 지정합니다.	기본 값은 비어 있습니다.

테이블24-41: 일반 속성

속성	설명	기본값
단일 로그인 만료(초)	SSO 연결이 유효한 시간(초)을 지정합니다.	기본값은 86400초입니다.

관련 항목

- 855 페이지에서 [Web Intelligence 서버 메모리 임계값 설정](#) "

24.1.7.1 Web Intelligence 서버 메모리 임계값 설정

다음 단원에서는 메모리 최대 임계값, 메모리 상위 임계값 또는 메모리 하위 임계값에 도달한 경우 Web Intelligence 서버에서 수행하는 동작에 대해 설명합니다.

메모리 최대 임계값

메모리 최대 임계값 제한에 도달하면 모든 현재 작업이 중단됩니다.

메모리 상위 임계값

이 메모리 상위 임계값에 도달하면 리소스를 확보하고 서버를 보호하기 위해 다음 서버 작업이 실행됩니다.

- 서버는 새 연결과 메모리를 사용하는 다른 모든 스레드가 시작되지 않도록 제한합니다. Web Intelligence 문서를 저장하는 옵션만이 허용됩니다. 메모리 할당이 필요한 작업을 요청하는 사용자에게 서버 사용 중 메시지가 전달되고 보류 중인 모든 변경 내용을 저장해야 한다고 알립니다.
- 서버는 충분한 리소스를 확보하기 위해 시스템 정리 기능을 설정하여 할당된 메모리 크기가 서버 상위 임계값 속성에 설정된 제한보다 적어지도록 합니다.
- 서버는 읽기 전용 문서 삭제를 시도합니다.
- 시스템 정리를 통해 메모리 여유 공간을 충분히 확보하지 못한 경우 서버는 보기 모드에 있는 문서를 닫기 시작합니다. 서버는 문서를 닫을 때 LIFO 프로토콜을 따르므로 가장 나중에 활성화된 문서가 메모리에서 먼저 제거됩니다. 서버는 안전한 수준에 도달할 때까지 문서를 계속 닫습니다. 안전한 수준을 산출하는 공식은 메모리 상위 임계값 - (20%*(메모리 상위 임계값))입니다. 예를 들어, 메모리 상위 임계값 속성이 4500MB로 설정되어 있을 경우 안전한 수준은 다음과 같습니다.

$$4500\text{MB} - .20 \times 4500\text{MB} = 3600\text{MB}$$

- 보기 모드에 있는 문서를 닫은 후에도 메모리 여유 공간을 충분히 확보하지 못한 경우 서버는 편집 모드에 있는 문서를 포함하여 열려 있는 나머지 모든 문서를 닫기 시작합니다. 서버는 문서를 닫을 때 LIFO 프로토콜을 따르므로 가장 나중에 활성화된 문서가 메모리에서 먼저 제거됩니다. 서버는 안전한 수준에 도달할 때까지 문서를 계속 닫습니다. 안전한 수준을 산출하는 공식은 메모리 상위 임계값 - (20%*(메모리 상위 임계값))입니다. 예를 들어, 메모리 상위 임계값 속성이 4500MB로 설정되어 있을 경우 안전한 수준은 다음과 같습니다.

$$4500\text{MB} - .20 \times 4500\text{MB} = 3600\text{MB}$$

메모리 하위 임계값

메모리 하위 임계값에 도달하면 서버는 비활성 문서 위치를 하드 디스크로 교체하여 활성화된 문서에 대해 메모리 공간을 할당합니다.

24.1.8 Dashboard Design 서비스 속성

Dashboard Design 캐시 서버 속성

테이블24-42: Dashboard Design 캐시 서비스 속성

속성	설명	기본값
최대 캐시 크기(KB)	쿼리를 캐시하는 데 사용되는 하드 디스크 공간(KB)의 크기를 지정합니다. 서버에서 많은 쿼리나 매우 복잡한 쿼리를 처리해야 하는 경우에는 캐시 크기를 늘려야 할 수 있습니다.	기본값은 256000KB입니다.
유휴 연결 제한 시간(분)	Dashboard Design 캐시 서버가 유휴 연결 요청을 대기하는 시간(분)을 지정합니다. 대개는 기본값을 수정하지 않아도 됩니다.	기본값은 15분입니다.
클라이언트 간에 데이터 공유	여러 클라이언트 간에 보고서 데이터를 공유할지 여부를 지정합니다.	기본값은 TRUE입니다.

속성	설명	기본값
클라이언트에 전달되는 가장 오래된 주문형 데이터(초)	<p>서버에서 주문형 쿼리의 요청에 맞게 캐시된 데이터를 사용하는 시간(초)을 지정합니다. 서버에서 이전의 요청을 충족하기 위해 생성했던 데이터를 그대로 사용하여 충족할 수 있는 요청을 받은 경우 이 데이터가 생성된 이후 경과된 시간이 여기에 설정한 값보다 작으면 서버에서 이후의 요청을 충족하는 데 이 데이터를 다시 사용합니다. 이러한 방식으로 데이터를 다시 사용하면 여러 사용자가 동일한 정보를 필요로 하는 경우에 시스템 성능을 크게 향상시킬 수 있습니다. 이 값을 설정할 때는 사용자에게 최신 데이터를 제공하는 것이 어느 정도로 중요한지 고려해야 합니다. 모든 사용자에게 최신 데이터를 제공하는 것이 매우 중요한 경우에는(중요한 변경이 자주 발생함) 이 값을 0으로 설정하여 데이터가 이와 같이 재사용되지 않도록 해야 할 수도 있습니다.</p> <p>참고: 이 속성은 보고서 개체 자체에 설정할 수 있습니다. 보고서 개체에 지정된 값은 서버 설정보다 우선적으로 적용됩니다.</p>	기본값은 0초입니다.
보안 캐시 제한 시간(분)	서버가 CMS 쿼리 전에 요청을 처리하기 위해 캐시된 로그인 자격 증명, 쿼리 속성 및 데이터 연결 정보를 사용하는 시간(분)을 지정합니다.	기본값은 20분입니다.
Java VM 인수	JVM에 제공할 수 있는 명령줄 인수를 지정합니다.	

Dashboard Design 처리 서버 속성

테이블24-43: Dashboard Design 처리 서비스 속성

속성	설명	기본값
최대 동시 작업	서버에서 동시에 실행할 수 있는 독립적인 작업의 최대 개수를 지정합니다. 이 속성의 값을 0으로 설정하면 서버가 실행되고 있는 컴퓨터의 CPU와 메모리에 따라 적절한 값이 적용됩니다.	기본값은 0입니다.
자식당 최대 수명 작업	각 자식 프로세스의 수명당 관리할 수 있는 최대 작업 수를 지정합니다.	기본값은 1000입니다.
미리 시작한 자식의 최대 수	서버에서 허용하는 미리 시작된 자식 프로세스의 최대 개수를 지정합니다. 이 값이 너무 낮을 경우 서버는 요청을 받은 후에 자식 프로세스를 만들게 되므로 대기 시간이 생길 수 있습니다. 이 값이 너무 높을 경우 유틸 자식 프로세스에 의해 시스템 리소스가 불필요하게 낭비될 수 있습니다.	기본값은 1입니다.
유틸 연결 제한 시간(분)	서버가 유틸 연결 요청을 대기하는 시간(분)을 지정합니다. 대개는 기본값을 수정하지 않아도 됩니다.	기본값은 20분입니다.
유틸 작업 제한 시간(분)	서버가 지정된 작업에 대한 여러 요청 사이에 대기하는 시간(분)을 지정합니다.	기본값은 15분입니다.
Java 하위 VM 인수	서버에서 만든 자식 프로세스에 제공되는 명령줄 인수를 지정합니다.	

테이블24-44: 단일 로그인(SSO) 서비스 속성

속성	설명	기본값
단일 로그인 만료(초)	SSO 연결이 유효한 시간(초)을 지정합니다.	기본값은 86400초입니다.

장25 서버 메트릭 부록

25.1 서버 메트릭 부록 정보

이 부록에서는 달리 명시하지 않는 한, 서버라는 용어는 BI 플랫폼이 설치되어 있거나 작동 중인 컴퓨터가 아닌 BI 플랫폼 서버를 지칭합니다.

작동하고 있지 않은 서버에서는 서버 메트릭을 사용할 수 없습니다.

관련 항목

- 382 페이지에서 [서버 메트릭 분석](#)

25.1.1 공통 서버 메트릭

다음 메트릭은 지정된 서버가 실행 중인 컴퓨터에 대한 것입니다.

테이블25-1: 컴퓨터 관련 메트릭

메트릭	설명
컴퓨터 이름	서버가 실행 중인 컴퓨터의 호스트 이름입니다.
운영 체제	서버가 실행 중인 컴퓨터의 운영 체제입니다.
CPU 유형	서버가 실행 중인 컴퓨터의 CPU(중앙 처리 장치) 유형입니다. 이 메트릭은 적응형 처리 서버 또는 웹 응용 프로그램 컨테이너 서버(WACS)에서 사용할 수 없습니다.

메트릭	설명
CPU	서버에서 사용 가능한 CPU 수입니다. 멀티 코어 하드웨어의 경우 이 메트릭은 실제 프로세서 수가 아닌, 논리적 CPU 수를 나타낼 수 있습니다. 이 메트릭은 적응형 처리 서버 또는 웹 응용 프로그램 컨테이너 서버(WACS)에서 사용할 수 없습니다.
RAM(MB)	서버가 실행 중인 컴퓨터에서 사용 가능한 메모리의 양(MB)입니다. 이 메트릭은 적응형 처리 서버 또는 웹 응용 프로그램 컨테이너 서버(WACS)에서 사용할 수 없습니다.
현지 시간	현지 시간입니다.
디스크 크기(GB)	BI 플랫폼이 설치되어 있는 디스크의 크기(GB)입니다. 이 메트릭은 적응형 처리 서버 또는 웹 응용 프로그램 컨테이너 서버(WACS)에서 사용할 수 없습니다.
사용된 디스크 공간(GB)	BI 플랫폼이 설치되어 있는 디스크의 사용된 공간(GB)입니다. 여기에는 BI 플랫폼에서 사용하는 공간뿐만 아니라, 컴퓨터의 다른 프로그램에서 사용하는 디스크 공간도 포함됩니다. 이 메트릭은 적응형 처리 서버 또는 웹 응용 프로그램 컨테이너 서버(WACS)에서 사용할 수 없습니다.

다음 메트릭은 지정된 SAP BusinessObjects 서버를 설명합니다.

테이블25-2: 서버 관련 메트릭

메트릭	설명
이름 서버	해당 서버가 주소를 게시할 CMS 서버의 이름 및 포트 번호입니다.
등록된 이름	서버의 내부 이름입니다. CMC의 서버 화면에 나타나는 이름이 아닙니다.
버전	서버의 버전입니다.
시작 시간	서버가 최근에 시작된 시간입니다.
PID	서버의 고유한 프로세스 ID 번호입니다. 서버가 실행 중인 컴퓨터의 운영 체제에서 PID를 생성합니다. PID는 특정 서버를 식별하는 데 사용됩니다.
호스트 이름	서버에서 현재 사용하고 있는 호스트 이름의 쉼표로 구분된 목록입니다.

메트릭	설명
호스트 IP 주소	서버가 요청을 수신하는 데 사용하는 IP 주소의 범례로 구분된 목록입니다.
포트 요청	서버가 다른 서버의 요청을 수신하는 데 사용하는 포트입니다. 서버가 둘 이상의 IP 주소에서 요청을 수신하는 경우, 서버에 대한 요청 포트는 항상 동일합니다. 다른 프로세스에서 이 요청 포트를 사용할 경우 서버가 시작되지 않습니다. 다른 프로세스에서 이 포트를 사용하지 않도록 하십시오.
사용 중인 서버 스레드	현재 요청을 처리하고 있는 서버 스레드 수입니다. 이 숫자가 서버의 최대 스레드 풀 크기와 같으면 시스템에서 추가 요청을 동시에 처리할 수 없고 사용 중인 스레드가 사용 가능하게 될 때까지 새 요청이 대기해야 함을 나타냅니다.

테이블25-3: 감사 메트릭

메트릭	설명
대기열의 현재 감사 이벤트 수	<p>감사 대상이 기록되었으나 아직 CMS 감사자가 가져오지 않은 감사 이벤트 수입니다. 이 값이 무제한으로 증가한다면 감사가 올바르게 설정되어 있지 않거나, 시스템 로드량이 많아 감사자가 가져올 수 있는 것보다 빠르게 감사 이벤트가 생성되는 것일 수 있습니다.</p> <p>참고: 서버를 중지 중인 경우 먼저 서버를 비활성화하고 이 메트릭이 0이 될 때까지 대기해야 합니다. 그렇지 않으면 감사 이벤트가 대기열에 계속 남아 있지만 서버를 다시 시작하고 CMS가 이들 이벤트에 대해 폴링할 때까지 감사 데이터 저장소에 연결하지 못합니다.</p>

테이블25-4: 로깅 서비스 메트릭

메트릭	설명
로깅 디렉터리	서버에 대한 로그 파일은 이 위치에 있습니다.

25.1.2 중앙 관리 서버 메트릭

다음 표는 중앙 관리 서버(CMS)의 메트릭 화면에 나타나는 서버 메트릭에 대한 설명입니다.

테이블25-5: 중앙 관리 서버 메트릭

메트릭	설명
감사 데이터베이스 연결 설정	CMS가 감사 데이터베이스에 정상적으로 연결되었는지 여부를 나타냅니다. 값 1은 연결되어 있음을 나타냅니다. 값 0은 감사 데이터베이스에 연결되어 있지 않음을 나타냅니다. CMS가 감사자인 경우 이 값은 1이어야 합니다. 이 값이 0인 경우, 감사 데이터베이스에 대한 연결을 설정할 수 없는 이유를 조사합니다.
CMS 감사자	중앙 관리 서버(CMS)가 감사자로 작동하고 있는지 여부를 나타냅니다. 값 1은 CMS가 감사자로 실행되고 있음을 나타냅니다. 값 0은 CMS가 감사자로 실행되고 있지 않음을 나타냅니다.
감사 데이터베이스 연결 이름	감사 데이터베이스 연결의 이름입니다. 반드시 감사 데이터베이스 자체의 이름일 필요는 없습니다. 이 메트릭이 비어 있는 경우 이는 감사 데이터베이스에 대한 연결을 설정할 수 없음을 나타냅니다.
감사 데이터베이스 사용자 이름	감사 데이터베이스에 연결하는 데 사용되는 사용자 계정의 이름입니다.
감사 데이터베이스 마지막 업데이트 날짜	감사 대상으로부터 이벤트를 가져오기 위해 CMS가 성공적으로 시작된 최근 날짜 및 시간입니다. CMS가 감사자인 경우, 이 메트릭은 메트릭 페이지가 로드되는 시간과 가까운 시간을 표시해야 합니다. 마스터 페이지가 로드되기 전 이 값이 2시간을 초과하는 경우, 이는 감사가 올바르게 작동하지 않음을 나타낼 수 있습니다.

메트릭	설명
감사 스레드 마지막 폴링 주기 기간(초)	<p>마지막 폴링 주기의 기간(초)으로, 이전 폴링 주기 중 이벤트 데이터가 감사 데이터베이스에 연결되기까지 걸린 최대 지연 시간을 나타냅니다.</p> <ul style="list-style-type: none"> 값이 20분 미만이라면 상태가 양호한 시스템을 나타냅니다. 값이 20분에서 2시간 사이라면 사용 중인 시스템을 나타냅니다. 값이 2시간을 초과한다면 매우 많이 사용 중인 시스템을 나타냅니다. 이 상태에서 너무 오래 지연될 경우 보다 빠른 속도로 데이터를 수신하도록 모든 감사 데이터베이스에 대한 배포를 업데이트하거나, 시스템에서 추적하는 감사 이벤트 수를 줄이십시오.
감사 스레드 사용률	<p>CMS 감사자가 감사 대상으로부터 데이터를 수집하는 데 걸리는 폴링 주기의 백분율입니다. 나머지는 폴링 간 휴지 시간입니다.</p> <p>이 값이 100%에 도달하면 다음 폴링이 시작되려고 할 때 감사자가 여전히 감사 대상으로부터 데이터를 수집하고 있는 것입니다. 이로 인해 이벤트가 감사 데이터베이스에 연결되는 것이 지연될 수 있습니다. 스레드 사용률이 자주 100%에 도달하고 며칠 동안 이 상태가 유지되는 경우, 감사 데이터베이스가 보다 빠른 속도로 데이터를 수신하도록 배포를 업데이트하거나, 시스템에서 추적하는 감사 이벤트 수를 줄이십시오.</p>
클러스터 CMS 서버	클러스터 내에서 작동 중인 중앙 관리 서버의 호스트 이름과 포트 번호를 세미콜론으로 구분하여 표시한 목록입니다.
동시 사용자가 설정한 세션 수	동시 라이선스를 사용하는 사용자의 총 세션 수입니다.
명명된 사용자가 설정한 세션 수	명명된 라이선스를 사용하는 사용자의 총 세션 수입니다.
시작 이후 사용자 세션 최대 수	CMS가 시작된 이후로 처리된 최대 동시 사용자 세션 수입니다.
서버에 설정된 세션 수	BI 플랫폼 서버에서 CMS를 통해 만들어진 동시 세션 수입니다. 이 값이 250을 초과할 경우 추가 CMS를 만드십시오.

메트릭	설명
모든 사용자가 설정한 세션 수	메트릭 화면이 로드될 때 CMS에서 처리하는 동시 사용자 세션 수입니다. 이 값이 클수록 해당 시스템을 사용 중인 사용자 수도 많아집니다. 이 값이 250을 초과할 경우 추가 CMS를 만드십시오.
실패한 작업	서버가 시작된 이후로 CMS에서 실패한 총 작업 수입니다.
보류 중인 작업	보류 중인 현재 작업 수입니다.
실행 중인 작업	실행 중인 현재 작업 수입니다. 여기에는 예약되어 있지만 아직 예약 시간이 되지 않아 실행 준비가 되어 있지 않은 작업이 포함됩니다.
완료된 작업	서버가 시작된 이후로 CMS에서 완료된 총 작업 수입니다.
대기 중인 작업	CMS에서 대기 중인 현재 작업 수입니다. 여기에는 사용 가능한 리소스를 예약하고 대기하는 작업이 포함됩니다.
동시 사용자 라이선스	키 코드에 지정된 동시 사용자 라이선스 수입니다.
명명된 사용자 라이선스	키 코드에 지정된 명명된 사용자 라이선스 수입니다.
빌드 날짜	CMS의 빌드 날짜입니다.
시스템 데이터베이스 연결 이름	CMS 시스템 데이터베이스 연결의 이름입니다. 반드시 CMS 시스템 데이터베이스 자체의 이름일 필요는 없습니다.
시스템 데이터베이스 서버 이름	CMS 시스템 데이터베이스가 실행 중인 서버의 이름입니다. 반드시 CMS 시스템 데이터베이스 자체의 이름일 필요는 없습니다.
시스템 데이터베이스 사용자 이름	CMS 시스템 데이터베이스에 연결하는 데 사용되는 사용자 계정의 이름입니다.
데이터 소스 이름	CMS 시스템 데이터베이스 연결의 이름입니다.
빌드 번호	CMS의 빌드 번호입니다. 이 번호를 통해 설치한 BI 플랫폼의 버전을 식별할 수 있습니다.
제품 버전	CMS의 제품 버전입니다.
리소스 버전	CMS의 리소스 버전입니다.
시작 이후 평균 커밋 응답 시간(밀리초)	서버가 시작된 이후로 CMS에서 커밋 작업을 수행하는 데 걸린 평균 시간(밀리초)입니다. 응답 시간이 1000밀리초를 초과할 경우 CMS 또는 CMS 시스템 데이터베이스를 조정해야 합니다.

메트릭	설명
시작 이후 평균 쿼리 응답 시간(밀리초)	서버가 시작된 이후로 CMS에서 쿼리 작업을 수행하는 데 걸린 평균 시간(밀리초)입니다. 응답 시간이 1000밀리초를 초과할 경우 CMS 또는 CMS 시스템 데이터베이스를 조정해야 합니다.
시작 이후 가장 긴 커밋 응답 시간(밀리초)	서버가 시작된 이후로 CMS에서 커밋 작업을 수행하는 데 걸린 가장 긴 시간(밀리초)입니다. 응답 시간이 10000밀리초를 초과할 경우 CMS 또는 CMS 시스템 데이터베이스를 조정해야 합니다.
시작 이후 가장 긴 쿼리 응답 시간(밀리초)	서버가 시작된 이후로 CMS에서 쿼리 작업을 수행하는 데 걸린 가장 긴 시간(밀리초)입니다. 응답 시간이 10000밀리초를 초과할 경우 CMS 또는 CMS 시스템 데이터베이스를 조정해야 합니다.
시작 이후 커밋 수	서버가 시작된 이후로 발생한 CMS 시스템 데이터베이스에 대한 커밋 수입니다.
시작 이후 쿼리 수	서버가 시작된 이후로 발생한 총 데이터베이스 쿼리 수입니다. 값이 클수록 활동량이나 로드량이 많은 시스템을 나타냅니다.
시작 이후 사용자 로그인 수	서버가 시작된 이후로 발생한 사용자 로그인 수입니다. 값이 클수록 활동량이나 로드량이 많은 시스템을 나타냅니다.
설정된 시스템 데이터베이스 연결	CMS에서 설정할 수 있는 CMS 시스템 데이터베이스에 대한 연결 수입니다. 데이터베이스 연결이 끊길 경우 CMS에서 연결을 복원하기 위해 시도합니다. 설정된 데이터베이스 연결 수가 일관되게 속성 화면의 시스템 데이터베이스 연결 요청 속성에 지정된 시스템 데이터베이스 연결 수보다 적을 경우, CMS에서 추가 연결을 확보할 수 없으며 시스템이 최적으로 작동하는 상태가 아님을 나타내는 것일 수 있습니다. 잠재적 해결책은 CMS용으로 더 많은 데이터베이스 연결이 가능하도록 데이터베이스 서버를 구성하는 것입니다.
현재 사용된 시스템 데이터베이스 연결	CMS에서 현재 사용하고 있는 CMS 시스템 데이터베이스에 대한 연결 수입니다. 현재 사용하고 있는 연결 수가 설정된 시스템 데이터베이스 연결 수보다 작거나 같을 수 있습니다. 설정된 연결 수와 사용된 연결 수가 일정 시간 동안 동일하다면 이는 병목 현상을 나타내는 것일 수 있습니다. 속성 화면의 시스템 데이터베이스 연결 요청 속성의 값을 늘리면 CMS의 성능이 향상될 수 있습니다. CMS 시스템 데이터베이스를 조정해도 성능이 향상될 수 있습니다.

메트릭	설명
보류 중인 시스템 데이터베이스 요청	사용 가능한 연결을 대기하고 있는 CMS 시스템 데이터베이스의 요청 수입니다. 이 값이 높을 경우, 시스템 데이터베이스 연결 요청 속성의 값을 늘려 보십시오. CMS 시스템 데이터베이스를 조정해도 성능이 향상될 수 있습니다.
CMS 시스템 캐시의 개체 수	현재 CMS 시스템 캐시에 있는 총 개체 수입니다.
CMS 시스템 DB의 개체 수	현재 CMS 시스템 데이터베이스에 있는 총 개체 수입니다.
기존의 동시 사용자 계정	클러스터에서 동시 라이선스를 사용하는 총 기존 사용자 수입니다.
기존의 명명된 사용자 계정	클러스터에서 명명된 라이선스를 사용하는 총 기존 사용자 수입니다.

25.1.3 연결 서버 메트릭

다음 메트릭은 연결 서버에만 해당됩니다.

테이블25-6: 연결 서비스 메트릭

메트릭	설명
데이터 소스	<p>속성 페이지에서 활성화된 데이터 소스가 테이블에 나열됩니다. 각각의 네트워크 계층과 데이터베이스 쌍에 대해 다음 정보를 표시합니다.</p> <ul style="list-style-type: none"> 상태(로드됨 또는 실패!): 드라이버의 현재 상태 사용 가능한 연결: 사용할 수 있는 풀 연결 수 작업(CORBA): 처리 중인 작업 수(2계층 배포) 작업(HTTP): 처리 중인 작업 수(Web Tier 배포) <p>참고: 연결 풀에 대한 자세한 내용은 데이터 액세스 가이드를 참조하십시오.</p>

25.1.4 이벤트 서버 메트릭

다음 표는 이벤트 서버의 메트릭 화면에 나타나는 서버 메트릭에 대한 설명입니다.

테이블25-7: 이벤트 서비스 메트릭

메트릭	설명
모니터링한 파일 목록	이벤트 서버에서 모니터링 중인 파일이 나열된 표. 파일 이름 옆에는 파일의 이름 및 경로가 표시됩니다. 마지막으로 알린 시간 옆에는 서버에서 폴을 수행하고 해당 파일이 있음을 확인한 마지막 타임스탬프가 표시됩니다.
모니터링한 파일	이벤트 서버에서 모니터링하는 총 파일 수입입니다.

25.1.5 파일 리포지토리 서버 메트릭

다음 표는 입력 및 출력 파일 리포지토리 서버의 메트릭 화면에 나타나는 서버 메트릭에 대한 설명입니다.

테이블25-8: Filestore 서비스 메트릭

메트릭	설명
활성 파일	현재 액세스하고 있는 파일 리포지토리 서버의 파일 수입입니다.
작성한 데이터(MB)	서버의 파일에 작성한 총 MB 수입입니다.
보낸 데이터(MB)	서버의 파일에서 읽은 총 MB 수입입니다.
활성 파일 목록	현재 액세스하고 있는 파일 리포지토리 서버의 파일이 표시된 표입니다.
활성 연결	클라이언트와 다른 서버 간의 총 활성 연결 수입입니다.

메트릭	설명
루트 디렉터리의 사용 가능한 디스크 공간(GB)	서버 실행 파일이 포함된 디스크의 총 여유 공간(GB)입니다.
루트 디렉터리의 빈 디스크 공간(GB)	서버 실행 파일이 포함된 디스크의 비어 있는 총 공간(GB)입니다.
루트 디렉터리의 전체 디스크 공간(GB)	서버 실행 파일이 포함된 디스크의 총 디스크 공간(GB)입니다.
루트 디렉터리의 사용 가능한 디스크 공간(%)	서버 실행 파일이 포함된 디스크에서 사용 가능한 디스크 공간(%)입니다.

25.1.6 적응형 처리 서버 메트릭

다음 표에서는 적응형 처리 서버에 대한 메트릭 화면에 나타나는 서버 메트릭에 대해 설명합니다.

테이블 25-9: 적응형 처리 서버 메트릭

메트릭	설명
전송 레이어의 스레드	전송 레이어의 모든 스레드 풀에 있는 전체 스레드 수.
전송 레이어 스레드 풀 크기	전체 공유 전송 레이어 스레드 수. 적응형 처리 서버의 호스트된 서비스에서 이런 스레드를 사용할 수 있습니다.
사용 가능한 프로세서	서버가 작동 중인 Java Virtual Machine(JVM)에서 사용할 수 있는 프로세서 수.
최대 메모리(MB)	Java Virtual Machine이 사용하려고 시도할 최대 메모리의 양(MB).
사용 가능한 메모리(MB)	새 개체를 할당하기 위해 JVM에서 사용할 수 있는 메모리의 양(MB).
전체 메모리(MB)	Java Virtual Machine에 있는 전체 메모리의 양(MB). 호스트 환경에 따라 이 값은 시간이 지나면서 바뀔 수 있습니다.

메트릭	설명
CPU 사용률(마지막 5분)	이전 5분 동안 서버에서 사용한 총 CPU 시간의 백분율입니다. 예를 들어, 단일 스레드에서 4CPU 시스템의 한 CPU 전체를 사용하는 경우 사용률은 25%입니다. JVM에 할당된 모든 프로세서가 고려 대상입니다. 값이 80%보다 크다면 CPU 병목 현상을 나타내는 것일 수 있습니다.
CPU 사용률(마지막 15분)	이전 15분 동안 서버에서 사용한 총 CPU 시간의 백분율입니다. 예를 들어, 단일 스레드에서 4CPU 시스템의 한 CPU 전체를 사용하는 경우 사용률은 25%입니다. JVM에 할당된 모든 프로세서가 고려 대상입니다. 값이 70%보다 크다면 병목 현상을 나타내는 것일 수 있습니다.
GC 동안 중단된 시스템 비율(마지막 5분)	마지막 5분 동안 GC(가비지 수집) 실행 중 중단된 시스템의 백분율입니다. 이 상태에서 모든 APS 서비스는 가상 컴퓨터가 단독 액세스가 필요한 가비지 수집의 중요한 단계를 수행하는 동안 실행되지 못합니다. 일반적으로 낮은 한 자릿수 값은 로드 중이라 하더라도 정상적인 동작입니다. 시간이 경과하면서 두 자릿수 값이 될 경우 이는 낮은 처리량 문제일 수 있으므로 조사해야 합니다.
GC 동안 중단된 시스템 비율(마지막 15분)	마지막 15분 동안 GC(가비지 수집) 실행 중 중단된 시스템의 백분율입니다. 이 상태에서는 Java Virtual Machine에서 실행 중인 모든 응용 프로그램 코드가 실행되지 않도록 하면서, Virtual Machine에서 배타적 액세스가 필요한 중요한 단계의 가비지 수집이 수행됩니다. 일반적으로 낮은 한 자릿수 값은 로드 중이라 하더라도 정상적인 동작입니다. 시간이 경과하면서 두 자릿수 값이 될 경우 이는 낮은 처리량 문제일 수 있으므로 조사해야 합니다.
GC 동안 페이지 오류 수(마지막 5분)	이전 5분 동안 가비지 수집을 실행하는 중 발생한 페이지 오류 수. 0보다 큰 값은 시스템에 대한 로드가 많거나 메모리 부족을 나타냅니다.
GC 동안 페이지 오류 수(마지막 15분)	마지막 15분 동안 가비지 수집을 실행하는 중 발생한 페이지 오류 수. 0보다 큰 값은 시스템에 대한 로드가 많거나 메모리 부족을 나타냅니다.
전체 GC 수	서버가 시작된 이후로 발생한 전체 가비지 수집 횟수입니다. 이 값이 급격히 증가할 경우 시스템 메모리가 부족한 것일 수 있습니다.

메트릭	설명
JVM 잠금 컨텐션 수	액세스를 기다리고 있는 스레드를 포함하는 동기화된 개체 수입니다. 0보다 큰 값은 스레드가 다시 실행되지 않음을 나타냅니다. 문제의 원인에 대한 자세한 정보를 확인하려면 스레드 덤프를 시작하십시오.
JVM 디버그 정보	상태, 포트, 연결된 클라이언트(있는 경우)를 비롯한 SAP Java Virtual Machine에 대한 디버그 정보입니다.
JVM 버전 정보	SAP Java Virtual Machine에 대한 버전 정보입니다.
JVM 교착 상태 스레드 카운터	교착 상태인 스레드 수입니다. 0보다 큰 값은 스레드가 다시 실행되지 않음을 나타냅니다. 문제의 원인에 대한 자세한 정보를 확인하려면 스레드 덤프를 시작하십시오.
JVM 추적 플래그	JVM에 대해 현재 설정된 추적 플래그입니다. 이 플래그는 JVM의 추적 수준을 나타냅니다.
서비스	서버에서 호스트하는 서비스를 나열한 쉼표로 구분된 목록.

테이블25-10: DSLBridge 서비스 메트릭

메트릭	설명
DSLServiceMetrics.queryCount	클라이언트와 서비스 사이에서 열려 있는 데이터 요청 수.
DSLServiceMetrics.activeConnectionCount	클라이언트와 서비스 사이에서 현재 열려 있는 연결 수.
DSLServiceMetrics.activeSessionCount	클라이언트와 서비스 사이에서 현재 열려 있는 세션 수.
DSLServiceMetrics.activeOLAPConnection Count	OLAP 클라이언트와 서비스 사이에서 현재 열려 있는 연결 수.

테이블25-11: 클라이언트 감사 프록시 서비스 메트릭

메트릭	설명
감사 이벤트 수신	서비스가 시작된 후로 수신한 클라이언트 감사 이벤트 수. 이 메트릭을 사용하여 클라이언트 감사가 올바르게 구성되었는지 확인할 수 있습니다. 0보다 큰 값은 이 클라이언트 감사 서비스를 통해 클라이언트에서 감사 이벤트가 성공적으로 라우트되고 있음을 나타냅니다.

테이블25-12: 플랫폼 검색 서비스 메트릭

메트릭	설명
서비스 시작 이후 성공한 추출 시도 횟수	플랫폼 검색 서비스가 시작된 후 성공적인 문서 추출 시도 횟수
서비스 시작 이후 성공한 추출 시도 횟수	플랫폼 검색 서비스가 시작된 후 성공적인 문서 추출 시도 횟수
마지막 콘텐츠 저장소 생성 타임스탬프	마지막 콘텐츠 저장소가 생성된 날짜 및 시간
서비스 시작 이후 실패한 추출 시도 횟수	플랫폼 검색 서비스가 시작된 후 실패한 문서 추출 시도 횟수
사용 가능한 서비스	서비스가 사용 가능한 경우 TRUE. 그렇지 않은 경우 FALSE
실행 중인 인덱싱	인덱싱이 실행 중인 경우 TRUE. 그렇지 않은 경우 FALSE
인덱싱된 문서 수	서비스 시작 후 인덱싱된 문서 수

테이블25-13: 다차원 분석 서비스 메트릭

메트릭	설명
세션 개수	MDAS 클라이언트에서 서버까지의 현재 연결 수
큐브 개수	시간이 제한되지 않은 연결에 데이터를 공급하는데 사용 중인 데이터 소스 개수
쿼리 개수	MDS 클라이언트와 서버 사이에서 열려 있는 데이터 요청 수

테이블25-14: 데이터 연합 서비스 메트릭

메트릭	설명
실행 중인 쿼리 수	메모리 사용 여부에 관계 없이 실행 중인 총 쿼리 수
연결 수	데이터 연합 쿼리 엔진에 대한 총 사용자 연결 수
데이터 소스에서 전송된 전체 바이트	데이터 소스에서 읽어 온 데이터의 양(바이트)
데이터 소스에서 전송된 총 레코드 수	데이터 소스에서 읽어 온 총 행 수
쿼리 실행에서 작성된 전체 바이트	쿼리 출력으로 생성된 데이터의 양(바이트)
쿼리 실행에 의해 작성된 총 레코드 수	쿼리 출력으로 생성된 총 행 수
메모리 사용 중인 쿼리 수	메모리를 사용하는 실행 중인 총 쿼리 수
쿼리 실행에 의해 사용된 메모리의 전체 바이트	실행 중인 쿼리에서 현재 사용하고 있는 메모리의 양(바이트)
쿼리 실행에 의해 사용된 디스크의 전체 바이트	실행 중인 쿼리에서 현재 사용하고 있는 디스크의 양(바이트)
디스크 사용 중인 쿼리 수	디스크를 사용하는 실행 중인 총 쿼리 수
리소스 대기 중인 쿼리 수	현재 실행 대기하고 있는 실행 중인 총 쿼리 수
활성 스레드 수	요청 실행에 사용된 총 활성 스레드 수
메타데이터 캐시에 의해 사용된 메모리의 전체 바이트	메타데이터, 통계 및 커넥터 구성에 사용된 메모리 양(바이트)
실패한 쿼리 수	실패한 총 쿼리 수(예외가 발생함)
쿼리 분석 단계의 쿼리 수	분석 단계에서 현재 실행 중인 총 쿼리 수
쿼리 최적화 단계의 쿼리 수	최적화 단계에서 현재 실행 중인 총 쿼리 수
쿼리 실행 단계의 쿼리 수	실행 단계에서 현재 실행 중인 총 쿼리 수
로드된 커넥터 수	서비스에서 로드된 총 커넥터 수
로드된 커넥터에 대한 활성 연결 수	서비스에서 로드된 커넥터에 대한 총 활성 연결 수
데이터 연합 서비스를 사용할 수 있습니다.	서비스가 사용 가능한 경우 TRUE. 그렇지 않은 경우 FALSE.

25.1.7 웹 응용 프로그램 컨테이너 서버 메트릭

다음 표는 웹 응용 프로그램 컨테이너 서버의 메트릭 화면에 나타나는 서버 메트릭에 대한 설명입니다.

참고:

웹 응용 프로그램 컨테이너 서버 메트릭에는 적응형 처리 서버 메트릭 섹션에 설명된 모든 메트릭도 포함됩니다.

테이블25-15: 웹 응용 프로그램 컨테이너 서버 메트릭

메트릭	설명
실행 중인 WACS 커넥터 목록	서버에서 실행 중인 모든 커넥터 목록입니다. 커넥터(HTTP, HTTPS 및 프록시를 통한 HTTP)가 모두 표시되지 않는다면 이는 연결이 활성화되지 않았거나 시작 중 실패했음을 나타냅니다.
시작 시 WACS 커넥터 실패	오류가 발생한 커넥터가 있는지 여부입니다. True이면 하나 이상의 커넥터가 시작하지 못한 것입니다. false이면 모든 커넥터가 정상적으로 실행되고 있는 것입니다. 하나 이상의 커넥터가 시작하지 못했을 때 서버를 작동하지 마십시오. 모든 커넥터가 올바르게 시작되도록 하려면 서버의 문제를 해결해야 합니다.

관련 항목

- 870 페이지에서 [적응형 처리 서버 메트릭](#)

25.1.8 적응형 작업 서버 메트릭

테이블25-16: 작업 서버 메트릭

메트릭	설명
받은 작업 요청	서버에서 실행하기로 되어 있었던 작업 수.
동시 작업	서버에서 현재 실행 중인 작업 수. 이 수가 클 경우 서버는 사용 중입니다.
최대 작업	서버에서 동시에 실행된 최대 동시 작업 수. 서버를 다시 시작할 때까지는 절대 이 수가 줄어들지 않습니다.
실패한 작업 작성	서버에서 실패한 작업 수.
임시 디렉터리	임시 파일을 만들 디렉터리. 이 디렉터리는 해당 서버에 대한 속성 화면에서 지정할 수 있습니다. 이 디렉터리의 디스크 공간이 충분하지 않은 경우 문제가 발생할 수 있습니다.
파일 시스템 대상 기본 설정 유효	서버에서 해당 서버에 대한 대상 화면에 지정된 파일 시스템 대상으로 문서를 보낼 수 있는 경우 TRUE. 그렇지 않은 경우 FALSE.
FTP 대상 기본 설정 유효	서버에서 해당 서버에 대한 대상 화면에 지정된 FTP 서버 대상으로 문서를 보낼 수 있는 경우 TRUE. 그렇지 않은 경우 FALSE.
받은 파일함 대상 기본 설정 유효	서버에서 해당 서버에 대한 대상 화면에 지정된 받은 파일함 대상으로 개체를 보낼 수 있는 경우 TRUE. 그렇지 않은 경우 FALSE.
전자 메일 대상 기본 설정 유효	서버에서 해당 서버에 대한 대상 화면에 지정된 전자 메일 대상으로 개체를 보낼 수 있는 경우 TRUE. 그렇지 않은 경우 FALSE.
예약 서비스	서버에서 실행 중인 서비스가 표시되는 표
자식	서버에서 실행 중인 자식 프로세스가 표시되는 표

다음 표에서는 서버에서 실행 중인 각 예약 서비스에 대한 메트릭을 설명합니다.

테이블25-17: 예약 서비스 메트릭

메트릭	설명
예약 서비스	서비스의 이름
받은 작업 요청	서비스에서 실행하기로 되어 있었던 작업 수.

메트릭	설명
동시 작업	서비스에서 현재 실행 중인 동시 작업 수. 이 수가 클 경우 서비스는 사용 중입니다.
최대 작업	서버에서 동시에 실행된 최대 동시 작업 수.
허용되는 최대 동시 작업	서비스에서 동시에 실행할 수 있도록 허용하는 독립적인 프로세스(하위 프로세스) 수. 이 디렉터리는 해당 서버에 대한 속성 화면에서 지정할 수 있습니다.
실패한 작업 작성	서비스에서 실패한 작업 수.

다음 표에서는 서버에서 실행 중인 각 자식 프로세스에 대한 메트릭을 설명합니다.

테이블25-18: 하위 메트릭

메트릭	설명
예약 서비스	자식 프로세스의 이름
PID	하위 프로세스의 식별자.
받은 작업 요청	하위 프로세스에서 실행하기로 되어 있었던 작업 수.
동시 작업	하위 프로세스에서 현재 실행 중인 동시 작업 수. 보통 이 값은 1이어야 합니다.
최대 작업	하위 프로세스에서 동시에 실행된 최대 동시 작업 수.
허용된 최대 작업 수	하위 프로세스에서 허용되는 동시 작업 수.
통신 오류	상위 적응형 작업 서버에서 발생한 통신 오류 수. 이 수가 클 경우 하위 프로세스가 다시 시작됩니다.
초기화 중	하위 프로세스가 초기화 중인 경우 TRUE. 그렇지 않은 경우 FALSE.
종료	하위 프로세스가 종료 중인 경우 TRUE. 그렇지 않은 경우 FALSE.

25.1.9 Crystal Report Server 메트릭

다음 표에서는 Crystal Reports 처리 및 Crystal Reports 2011 처리 서버에 대한 메트릭 화면에 나타나는 서버 메트릭에 대해 설명합니다.

테이블25-19: Crystal Reports 처리 서버 메트릭

메트릭	설명
열려 있는 작업	서버에서 현재 실행 중인 작업 목록을 보여주는 표입니다. 이 표에는 문서의 ID와 이름, 작업을 실행 중인 사용자 이름, 마지막으로 문서에 액세스한 날짜, 작업 실행 시간이 포함됩니다.
처리된 요청 수	서버가 시작된 후 처리한 총 요청 수
열려 있는 작업 수	서버와 서버의 하위 프로세스에서 현재 처리 중인 작업 수
개체 유형	서버에서 주로 다루는 InfoObject의 유형. 이 메트릭에 대한 값은 바뀌지 않습니다.
평균 처리 시간(밀리초)	서버가 마지막으로 수신한 500개의 요청을 처리하는 데 쓴 평균 시간(밀리초). 이 수가 계속 높고 증가하고 있는 경우, 다른 컴퓨터에서 서버를 추가로 만드는 방안을 고려하십시오.
최대 처리 시간(밀리초)	서버가 마지막 500개의 요청 중 하나를 처리하는 데 쓴 최대 시간(밀리초). 이 수가 계속 높고 증가하고 있는 경우, 다른 컴퓨터에서 서버를 추가로 만드는 방안을 고려하십시오.
최소 처리 시간(밀리초)	서버가 마지막 500개의 요청 중 하나를 처리하는 데 쓴 최소 시간(밀리초). 이 수가 계속 높고 증가하고 있는 경우, 다른 컴퓨터에서 서버를 추가로 만드는 방안을 고려하십시오.
대기열에 있는 요청 수	처리 대기 중이거나 처리 중인 요청 수. 이 수가 계속 높고 증가하고 있는 경우, 다른 컴퓨터에서 서버를 추가로 만드는 방안을 고려하십시오.
ObjectDllName	서버용 처리 플러그 인의 이름입니다. 이 메트릭의 값은 바뀌지 않습니다.

메트릭	설명
열려 있는 연결 수	서버와 클라이언트 간에 현재 열려 있는 연결 수
요청 실패율	서버가 마지막으로 수신한 500개의 요청 중 처리에 실패한 요청의 비율
전송된 데이터(KB)	서버 시작 후 클라이언트로 전송된 총 데이터 양(KB)
실패한 요청 수	서버 시작 후 서버에서 완료할 수 없는 요청 수
MaxChildProcesses	서버에서 허용하는 동시 자식 프로세스의 최대 수

다음 표에서는 Crystal Reports 캐시 서버에 대한 메트릭 화면에 나타나는 서버 메트릭에 대해 설명합니다.

테이블25-20: Crystal Reports 캐시 서버 메트릭

메트릭	설명
캐시 적중률(%)	마지막 500개의 요청에 대해 캐시된 데이터로 사용된 요청의 비율
연결된 처리 서버 수	배포되어 있는 Crystal Reports 처리 서버의 목록을 보여주는 표입니다. 이 표에는 서버의 이름과 해당 서버에서 현재 열려 있는 연결 수가 나타납니다.
처리된 요청 수	서버가 시작된 후 처리한 총 요청 수
개체 유형	서버에서 주로 다루는 InfoObject의 유형 이 메트릭에 대한 값은 바뀌지 않습니다.
평균 처리 시간(밀리초)	서버가 마지막으로 수신한 500개의 요청을 처리하는 데 쓴 평균 시간(밀리초). 이 수가 계속 높고 증가하고 있는 경우, 다른 컴퓨터에서 서버를 추가로 만드는 방안을 고려하십시오.
최대 처리 시간(밀리초)	서버가 마지막 500개의 요청 중 하나를 처리하는 데 쓴 최대 시간(밀리초). 이 수가 계속 높고 증가하고 있는 경우, 다른 컴퓨터에서 서버를 추가로 만드는 방안을 고려하십시오.
최소 처리 시간(밀리초)	서버가 마지막 500개의 요청 중 하나를 처리하는 데 쓴 최소 시간(밀리초). 이 수가 계속 높고 증가하고 있는 경우, 다른 컴퓨터에서 서버를 추가로 만드는 방안을 고려하십시오.
대기열에 있는 요청 수	처리 대기 중이거나 처리 중인 요청 수. 이 수가 계속 높고 증가하고 있는 경우, 다른 컴퓨터에서 서버를 추가로 만드는 방안을 고려하십시오.

메트릭	설명
ObjectDllName	서버용 처리 플러그 인의 이름입니다. 이 메트릭의 값은 바뀌지 않습니다.
캐시 크기	서버에서 현재 캐시 중인 디스크 상의 데이터 양(KB)
열려 있는 연결 수	서버와 클라이언트 간에 현재 열려 있는 연결 수
전송된 데이터(KB)	서버 시작 후 클라이언트로 전송된 총 데이터 양(KB)

다음 표에서는 Crystal Reports 2011 Report Application Server에 대한 메트릭 화면에 나타나는 서버 메트릭에 대해 설명합니다.

테이블25-21: Crystal Reports 2011 Report Application Server 메트릭

메트릭	설명
metric_currentdoccount	서버에서 현재 처리 중인 문서 수
metric_totaldoccount	서버가 시작된 후 서버에서 처리된 문서 수
metric_currentagentthreadcount	서버에서 현재 처리 중인 스레드 수
metric_totalagentthreadcount	서버가 시작된 후 서버에서 처리된 스레드 수

25.1.10 Web Intelligence 서버 메트릭

테이블25-22: Web Intelligence 처리 서비스 메트릭

메트릭	설명
캐시 크기(KB)	캐시에 현재 저장되어 있는 양(KB)
캐시에 있는 오래된 문서 수	서버가 시작된 이후로 너무 오래되어 캐시에서 삭제한 문서 수
캐시 높은 표시 수	서버가 시작된 이후로 캐시가 서버에서 허용되는 최대 크기에 도달한 횟수
CPU 사용량(%)	서버가 시작된 이후로 서버에서 소비한 총 CPU 시간(백분율)

메트릭	설명
총 CPU 시간(초)	서버가 시작된 이후로 서버에서 소비한 총 CPU 시간(초)
메모리 높은 임계값 수	서버가 시작된 이후로 서버에서 높은 메모리 임계값에 도달한 횟수
메모리 최대 임계값 수	서버가 시작된 이후로 서버에서 최대 메모리 임계값에 도달한 횟수
가상 메모리 크기(MB)	서버에 할당된 전체 메모리의 양(MB)
현재 클라이언트 호출 수	서버에서 현재 처리 중인 CORBA 호출 수
현재 작업 수	서버에서 현재 실행 중인 작업 수
총 클라이언트 호출 수	서버가 시작된 이후로 수신한 전체 CORBA 호출 수
총 작업 수	서버가 시작된 이후로 서버에서 실행된 전체 작업 수
유희 시간(초)	서버가 클라이언트에서 수신한 마지막 요청 이후로 경과한 시간(초)
현재 활성 세션 수	현재 클라이언트의 요청을 허용할 수 있는 세션 수
문서 수	서버에서 현재 열려 있는 문서 수
현재 세션 수	서버에서 만들어진 현재 세션 수
문서 교체 수	정리 스레드에서 바꾸기 요청을 예약한 문서 수
교체된 문서 수	바꾸기 요청으로 바꾼 문서 수
세션 제한 시간 수	서버가 시작된 이후로 제한 시간이 지난 세션 수
총 세션 수	서버가 시작된 이후로 서버에서 만들어진 세션 수
사용자 수	서버에 연결된 총 사용자 수

25.1.11 Dashboard Design 서버 메트릭

테이블25-23: Dashboard Design 처리 서버 메트릭

메트릭	설명
열려 있는 작업	서버에서 현재 실행 중인 작업 목록을 보여주는 표입니다. 이 표에는 문서의 ID와 이름, 작업을 실행 중인 사용자 이름, 마지막으로 문서에 액세스한 날짜, 작업 실행 시간이 포함됩니다.
처리된 요청 수	서버가 시작된 후 처리한 총 요청 수
열려 있는 작업 수	서버와 서버의 하위 프로세스에서 현재 처리 중인 작업 수
개체 유형	서버에서 주로 다루는 InfoObject의 유형 이 메트릭에 대한 값은 바뀌지 않습니다.
평균 처리 시간(밀리초)	서버가 마지막으로 수신한 500개의 요청을 처리하는데 쓴 평균 시간(밀리초). 이 수가 계속 높고 증가하고 있는 경우, 다른 컴퓨터에서 서버를 추가로 만드는 방안을 고려하십시오.
최대 처리 시간(밀리초)	서버가 마지막 500개의 요청 중 하나를 처리하는데 쓴 최대 시간(밀리초). 이 수가 계속 높고 증가하고 있는 경우, 다른 컴퓨터에서 서버를 추가로 만드는 방안을 고려하십시오.
최소 처리 시간(밀리초)	서버가 마지막 500개의 요청 중 하나를 처리하는데 쓴 최소 시간(밀리초). 이 수가 계속 높고 증가하고 있는 경우, 다른 컴퓨터에서 서버를 추가로 만드는 방안을 고려하십시오.
대기열에 있는 요청 수	처리 대기 중이거나 처리 중인 요청 수. 이 수가 계속 높고 증가하고 있는 경우, 다른 컴퓨터에서 서버를 추가로 만드는 방안을 고려하십시오.
ObjectDllName	서버용 처리 플러그 인의 이름입니다. 이 메트릭의 값은 바뀌지 않습니다.
열려 있는 연결 수	서버와 클라이언트 간에 현재 열려 있는 연결 수
요청 실패율	서버가 마지막으로 수신한 500개의 요청 중 처리에 실패한 요청의 비율
전송된 데이터(KB)	서버 시작 후 클라이언트로 전송된 총 데이터 양(KB)
실패한 요청 수	서버 시작 후 서버에서 완료할 수 없는 요청 수

메트릭	설명
MaxChildProcesses	서버에서 허용하는 동시 자식 프로세스의 최대 수

테이블25-24: 캐시 서버 메트릭

메트릭	설명
캐시 적중률(%)	마지막 500개의 요청에 대해 캐시된 데이터로 사용된 요청의 비율
연결된 처리 서버 수	배포되어 있는 Dashboard Design 처리 서버의 목록을 보여주는 표입니다. 이 표에는 서버의 이름과 해당 서버에서 현재 열려 있는 연결 수가 나타납니다.
처리된 요청 수	서버가 시작된 후 처리한 총 요청 수
개체 유형	서버에서 주로 다루는 InfoObject의 유형 이 메트릭에 대한 값은 바뀌지 않습니다.
평균 처리 시간(밀리초)	서버가 마지막으로 수신한 500개의 요청을 처리하는 데 쓴 평균 시간(밀리초). 이 수가 계속 높고 증가하고 있는 경우, 다른 컴퓨터에서 서버를 추가로 만드는 방안을 고려하십시오.
최대 처리 시간(밀리초)	서버가 마지막 500개의 요청 중 하나를 처리하는 데 쓴 최대 시간(밀리초). 이 수가 계속 높고 증가하고 있는 경우, 다른 컴퓨터에서 서버를 추가로 만드는 방안을 고려하십시오.
최소 처리 시간(밀리초)	서버가 마지막 500개의 요청 중 하나를 처리하는 데 쓴 최소 시간(밀리초). 이 수가 계속 높고 증가하고 있는 경우, 다른 컴퓨터에서 서버를 추가로 만드는 방안을 고려하십시오.
대기열에 있는 요청 수	처리 대기 중이거나 처리 중인 요청 수. 이 수가 계속 높고 증가하고 있는 경우, 다른 컴퓨터에서 서버를 추가로 만드는 방안을 고려하십시오.
ObjectDllName	서버용 처리 플러그 인의 이름입니다. 이 메트릭의 값은 바뀌지 않습니다.
캐시 크기(KB)	서버에서 현재 캐시 중인 디스크 상의 데이터 양(KB)
열려 있는 연결 수	현재 열려 있는 클라이언트에 대한 연결 수
전송된 데이터(KB)	서버 시작 후 클라이언트로 전송된 총 데이터 양(KB)

장26 서버 및 노드 자리 표시자 부록

26.1 서버 및 노드 자리 표시자

이런 자리 표시자들은 같은 노드에 있는 모든 서버에 적용됩니다(%SERVER_FRIENDLY_NAME% 및 %SERVER_NAME% 제외).

테이블26-1: 자리 표시자

자리 표시자	설명	기본값
%AAANALYTICS_EXE%	대시보드 분석 서버용 실행 파일의 이름입니다.	Windows: AAAnalytics.exe. UNIX: AAAnalytics
%AADASHBOARD_EXE%	대시보드 서버용 실행 파일의 이름입니다.	Windows: AADashboard.exe. UNIX: AADashboard
%AuditingDatabaseConnection%	CMS에서 사용하는 감사 데이터베이스 연결.	이 값은 설치 중에 지정됩니다.
%AuditingDatabaseDriver%	감사 데이터베이스에 연결하는 데 사용되는 데이터베이스 드라이버의 유형입니다.	Windows에서 기본값은 sqlserverauditdbss입니다.
%BINDIR%	BI 플랫폼 64비트 이진 파일이 있는 폴더입니다.	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/win64_x64. UNIX: <INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/
%BINDIR32%	BI 플랫폼 32비트 이진 파일이 있는 폴더입니다.	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/win32_x86. UNIX: <INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/

자리 표시자	설명	기본값
%CACHESERVER_EXE%	Crystal Reports 캐시 서버용 실행 파일의 이름입니다.	Windows: crcache.exe UNIX: boe_crcached
%CMS_EXE%	중앙 관리 서버용 실행 파일의 이름입니다.	Windows: cms.exe UNIX: boe_cmsd
%CONNECTIONSERVER32_EXE%	32비트 연결 서버용 실행 파일의 이름입니다.	Windows: ConnectionServer32.exe UNIX: ConnectionServer32
%CONNECTIONSERVER_DIR%	연결 서버의 루트 폴더입니다.	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/dataAccess/connectionServer. UNIX: <INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>
%CONNECTIONSERVER_EXE%	64비트 연결 서버용 실행 파일의 이름입니다.	Windows: ConnectionServer.exe UNIX: ConnectionServer
%CR2011_BINDIR%	Crystal Reports 2011 서버 이진 파일이 있는 디렉터리입니다.	Windows: <INSTALLDIR>/SAP BusinessObjectsEnterprise XI 4.0/win32_x86
%CR2011_DefaultWorkingDir%	Crystal Reports 2011 서버용 기본 작업 디렉터리입니다.	Windows: <INSTALLDIR>/SAP BusinessObjectsEnterprise XI 4.0/win32_x86
%CRYSTALRAS_EXE%	Report Application Server용 실행 파일의 이름입니다.	Windows: crystalras.exe UNIX: boe_crystalrasd
%CR_ODBCINI%	.odbc.ini 파일의 이름 및 경로입니다.	UNIX: <INSTALLDIR>/bobje/odbc.ini Windows에서 이것은 빈 문자열입니다.
%CommonJavaBundlesDir%	공유 OSGI 번들이 있는 폴더입니다.	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/java/bundles. UNIX: <INSTALLDIR>/sap_bobj/enterprise_xi40/java/bundles
%CommonJavaLibDir%	공통 Java 라이브러리가 있는 폴더입니다.	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/java/lib. UNIX: <INSTALLDIR>/sap_bobje/enterprise_xi40/java/lib

자리 표시자	설명	기본값
%DLLEXT%	.dll 또는 .so 파일의 기본 확장명입니다.	Windows: .dl UNIX: .so
%DLLPATH%	BI 플랫폼이 설치되어 있는 컴퓨터의 환경 변수 이름으로, 인터프리터가 실행 파일을 검색할 디렉터리를 지정합니다.	Windows: Path UNIX: LD_LIBRARY_PATH
%DLLPATH32%	Solaris 32비트 시스템에서 BI 플랫폼이 설치되어 있는 컴퓨터의 환경 변수 이름으로, 인터프리터가 실행 파일을 검색할 디렉터리를 지정합니다.	Solaris 컴퓨터에서는 LD_LIBRARY_PATH_32입니다. 이 자리 표시자는 다른 운영 체제에서는 빈 문자열입니다.
%DLLPATH64%	Solaris 64비트 시스템에서 BI 플랫폼이 설치되어 있는 컴퓨터의 환경 변수 이름으로, 인터프리터가 실행 파일을 검색할 디렉터리를 지정합니다.	Solaris 컴퓨터에서는 LD_LIBRARY_PATH_64입니다. 이 자리 표시자는 다른 운영 체제에서는 빈 문자열입니다.
%DLLPREFIX%	.dll 또는 .so 파일의 기본 접두사입니다.	UNIX: lib. 이 자리 표시자는 Windows 컴퓨터에서는 빈 문자열입니다.
%DLLPRELOAD%	플랫폼의 LD_PRELOAD 환경 변수 이름입니다.	UNIX: LD_PRELOAD. 이 자리 표시자는 Windows 컴퓨터에서는 빈 문자열입니다.
%DLLPRELOAD32%	32비트 AIX 시스템에서 LD_PRELOAD 환경 변수의 이름입니다.	AIX: LDR_PRELOAD. 이 자리 표시자는 다른 컴퓨터에서는 빈 문자열입니다.
%DLLPRELOAD64%	64비트 AIX 시스템에서 LD_PRELOAD 환경 변수의 이름입니다.	AIX: LDR_PRELOAD64. 이 자리 표시자는 다른 컴퓨터에서는 빈 문자열입니다.
%DP%	경로 구분 기호입니다.	Windows: ;, UNIX: :
%DefaultAuditingDir%	감사 임시 파일을 기록할 디렉터리입니다. 최적의 성능을 위해 이 위치는 서버의 로컬 드라이브에 있어야 합니다.	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/Auditing. UNIX: <INSTALLDIR>/sap_bobj/data/Auditing/

자리 표시자	설명	기본값
%DefaultDataDir%	작업 서버에서 사용하는 임시 디렉터리입니다.	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/Data. UNIX: <INSTALLDIR>/sap_bobj/data/
%DefaultInputFRSDir%	입력 파일 리포지토리 서버의 루트 폴더입니다.	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/FileStore/Input. UNIX: <INSTALLDIR>/sap_bobj/data/frsinput
%DefaultLoggingDir%	로그 파일이 저장된 위치입니다.	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/logging. UNIX: <INSTALLDIR>/sap_bobj/logging
%DefaultOutputFRSDir%	출력 파일 리포지토리 서버의 루트 폴더입니다.	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/FileStore/Output. UNIX: <INSTALLDIR>/sap_bobj/data/frsoutput
%DefaultWorkingDir%	64비트 서버용 작업 디렉터리	Windows: <INSTALLDIR>/SAP BusinessObjectsEnterprise XI 4.0/win64_x64 UNIX: <INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>
%DefaultWorkingDir32%	32비트 서버용 작업 디렉터리	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/win32_x86 UNIX: <INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>
%EPM_LD_PRELOAD_ONCE%	플랫폼의 LD_PRELOAD_ONCE 환경 변수 이름입니다.	\$LD_PRELOAD_ONCE\$
%EVENTSERVER_EXE%	이벤트 서버용 실행 파일의 이름입니다.	Windows: EventServer.exe, UNIX: boe_eventsd
%EXEEXT%	실행 파일의 기본 확장명입니다.	Windows: .exe. 이 위치 표시자는 UNIX에서 사용할 수 없습니다.

자리 표시자	설명	기본값
%EXEPATH%	BI 플랫폼이 설치되어 있는 컴퓨터의 환경 변수 이름으로, 인터프리터가 실행 파일을 검색할 디렉터리를 지정합니다.	Windows: Path UNIX: PATH
%EnterpriseDir%	64비트 BI 플랫폼이 설치된 위치입니다.	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/. UNIX: <INSTALLDIR>/sap_bobj/enterprise_xi40
%EnterpriseDir32%	32비트 BI 플랫폼이 설치된 위치입니다.	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/. UNIX: <INSTALLDIR>/sap_bobj/enterprise_xi40
%ExternalJavaLibDir%	외부 즉, 타사 Java 라이브러리가 있는 폴더입니다.	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/java/lib/external. UNIX: <INSTALLDIR>/sap_bobje/enterprise_xi40/java/lib/external
%FILESERVER_EXE%	파일 서버용 실행 파일의 이름입니다.	Windows: filesrv.exe UNIX: boe_filesrv
%HOARD_PATH%	Memory Manager의 위치입니다.	기본적으로 이 위치는 비어 있습니다.
%HOARD_PRELOAD%	Memory Manager를 미리 로드할지 여부를 지정합니다.	기본적으로 이 위치는 비어 있습니다.
%INSTALLROOTDIR%	64비트 BI 플랫폼이 설치된 폴더입니다.	이 값은 설치 중에 지정됩니다.
%INSTALLROOTDIR32%	32비트 BI 플랫폼이 설치된 폴더입니다.	이 값은 설치 중에 지정됩니다.
%IntroscopeAgentEnableInstrumentation%	Introscope Agent Enterprise Manager를 사용하는 Java 서버에 대한 계측이 활성화되었는지 여부를 나타냅니다.	BI 플랫폼을 설치할 때 Introscope Agent Enterprise Manager의 사용 여부에 따라 TRUE 또는 FALSE 값이 될 수 있습니다.
%IntroscopeAgentEnterpriseManagerHost%	계측 데이터가 전송되는 Introscope Agent Enterprise Manager 호스트 이름입니다.	이 값은 설치 중에 지정됩니다.

자리 표시자	설명	기본값
%IntroscopeAgentEnterpriseManagerPort%	계측 데이터가 전송되는 Introscope Agent Enterprise Manager 포트입니다.	이 값은 설치 중에 지정됩니다.
%IntroscopeAgentEnterpriseManagerTransport%	계측 데이터를 Introscope Agent Enterprise Manager로 전송할 때 사용되는 전송입니다. 허용되는 값은 다음과 같습니다. <ul style="list-style-type: none"> • TCP • HTTP • HTTPS • SSL 	TCP
%IntroscopeAgentEnterpriseManagerTransportHTTP%	HTTP를 통해 계측 데이터를 Introscope Agent Enterprise Manager로 전송할 때 사용되는 클래스입니다.	com.wily.isengard.postofficehub.link.net.HttpTunnelingSocketFactory
%IntroscopeAgentEnterpriseManagerTransportHTTPS%	HTTPS를 통해 계측 데이터를 Introscope Agent Enterprise Manager로 전송할 때 사용되는 클래스입니다.	com.wily.isengard.postofficehub.link.net.HttpTunnelingSocketFactory
%IntroscopeAgentEnterpriseManagerTransportSSL%	SSL을 통해 계측 데이터를 Introscope Agent Enterprise Manager로 전송할 때 사용되는 클래스입니다.	com.wily.isengard.postofficehub.link.net.SSLSocketFactory
%IntroscopeAgentEnterpriseManagerTransportTCP%	TCP를 통해 계측 데이터를 Introscope Agent Enterprise Manager로 전송할 때 사용되는 클래스입니다.	com.wily.isengard.postofficehub.link.net.DefaultSocketFactory
%IntroscopeDir%	Introscope Agent Enterprise Manager가 설치된 폴더입니다.	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/java/wily. UNIX: <INSTALLDIR>/sap_bobje/enterprise_xi40/java/wily
%JAVAW_EXE%	콘솔 창이 없는 Java Virtual Machine의 실행 파일 이름입니다.	Windows: javaw.exe UNIX: java
%JAVA_EXE%	Java Virtual Machine의 실행 파일 이름입니다.	Windows: java.exe UNIX: java
%JOBSERVERCHILD_EXE%	적응형 작업 서버 하위용 실행 파일의 이름입니다.	Windows: JobServerChild.exe UNIX: boe_jobcd

자리 표시자	설명	기본값
%JOBSEVER_EXE%	적응형 작업 서버용 실행 파일의 이름입니다.	Windows: JobServer.exe UNIX: boe_jobsd
%JdkBinDir%	JDK 이진 파일이 있는 폴더입니다.	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/win64_x64/sapjvm/bin. UNIX: <INSTALLDIR>/sap_bobje/<PLATFORM>/sapjvm/bin
%JreBinDir%	JRE 이진 파일이 있는 폴더입니다.	Windows: <INSTALLDIR>/javask/bin UNIX: <INSTALLDIR>/sap_bobje/<PLATFORM>/sapjvm/jre/bin
%JVM_ARCH_ENVIRONMENT%	컴퓨터가 32비트 또는 64비트 JVM에서 작동 중인지 여부를 나타냅니다.	32비트 UNIX 컴퓨터의 경우 기본값은 -d32입니다. 64비트 컴퓨터의 경우 기본값은 -d64입니다. Windows 컴퓨터에서 이것은 빈 문자열입니다.
%JVM_HEADLESS_MODE%	JVM이 헤드리스 모드로 작동하는지 여부를 지정하는 명령줄 인수입니다.	Windows: -Djava.awt.headless=false, UNIX: -Djava.awt.headless=true
%JVM_HEAP_DUMP_ON_OUT_OF_MEMORY_ERROR%	메모리 부족 오류 발생 시 JVM에서 수행하는 작업을 지정하는 명령줄 매개 변수입니다.	"-XX:+ HeapDumpOnOutOfMemoryError" "-XX:HeapDumpPath=%DefaultLoggingDir%" "-XX:+ ExitVMOnOutOfMemoryError"
%JVM_SHARED_MEMORY_SEGMENT%	JVM 확장을 사용하고 JVM의 인스턴스 번호를 설정하는 명령줄 매개 변수입니다.	기본적으로 이 위치 표시자는 비어 있습니다.
%LANGUAGEPACKSDIR%	배포의 언어 팩이 설치되는 폴더입니다.	Windows 및 UNIX: <INSTALLDIR>
%LANGUAGEPACKSDIR32%	32비트 시스템에서 배치의 언어 팩이 설치된 폴더입니다.	Windows 및 UNIX: <INSTALLDIR>
%LSTDir%	LST 구성 파일이 저장된 폴더입니다.	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/conf/lst. UNIX: <INSTALLDIR>/sap_bobj/enterprise_xi40/conf/lst

자리 표시자	설명	기본값
%MDAS_JVM_OS_STACK_SIZE%	다차원 분석 서비스에 대한 JVM 스택 크기를 지정합니다.	기본적으로 이 위치 표시자는 비어 있습니다.
%NCSInstrumentLevelThreshold%	NCS 라이브러리용 추적 로깅의 임계값 수준입니다.	이 값은 설치 중에 결정됩니다.
%PAGESERVER_EXE%	Crystal Reports 2011 처리 서버용 실행 파일의 이름입니다.	Windows: crproc.exe UNIX: boe_crprocd.bin
%PJSContainerDir%	APS Container JARS가 있는 폴더입니다.	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/java/pjs/container. UNIX: <INSTALLDIR>/sap_bobj/enterprise_xi140/java/pjs/container
%PJSServicesDir%	APS Service JARS가 있는 폴더입니다.	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/java/pjs/services. UNIX: <INSTALLDIR>/sap_bobj/enterprise_xi140/java/pjs/services
%Platform%	BI 플랫폼이 실행 중인 컴퓨터의 운영 체제입니다.	BI 플랫폼이 실행 중인 컴퓨터의 운영 체제입니다.
%Platform32%	32비트 BI 플랫폼이 실행 중인 컴퓨터의 운영 체제입니다.	BI 플랫폼이 실행 중인 컴퓨터의 운영 체제입니다.
%RasBinDir%	Report Application Server의 루트 폴더입니다.	Windows: <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/win32_x86 UNIX: <INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/ras
%SERVER_FRIENDLY_NAME%	서버의 전체 이름입니다.	서버의 전체 이름입니다.
%SERVER_NAME%	서버의 전체 이름입니다.	서버의 전체 이름입니다.
%SMDAgentHost%	계측 데이터가 전송되는 SMD Agent 호스트 이름입니다.	이 값은 설치 중에 지정됩니다.
%SMDAgentPort%	계측 데이터가 전송되는 SMD Agent 포트입니다.	이 값은 설치 중에 지정됩니다.

자리 표시자	설명	기본값
%TRACE_CONFIGFILE_INI%	BO_Trace.ini 파일의 이름 및 경로입니다.	Windows: <INSTALLEDIR>/SAP BusinessObjects Business Intelligence platform 4.0/logging/logConfig/BO_Trace.ini. UNIX: <INSTALLEDIR>/sap_bobj/enterprise_xi140/conf/BO-trace.ini
%WEBI_LD_PRELOAD%	플랫폼의 LD_PRELOAD 환경 변수 이름입니다.	\$LD_PRELOAD\$
%WEBISERVER_EXE%	Web Intelligence 처리 서버용 실행 파일의 이름입니다.	Windows: wireportserver.exe UNIX: WIReportServer
%WEBI_LD_PRELOAD_ONCE%	플랫폼의 LD_PRELOAD_ONCE 환경 변수 이름입니다.	\$LD_PRELOAD_ONCE\$
%XCCACHE_EXE%	Dashboard Design 캐시 서버용 실행 파일의 이름입니다.	Windows: xccache.exe UNIX: boe_xccached
%XCPROC_EXE%	Dashboard Design 처리 서버용 실행 파일의 이름입니다.	Windows: xcproc.exe UNIX: boe_xcprocd

참고:

다음 자리 표시자는 노드 수준에서 편집할 수 있습니다. 설명과 기본값은 위 표에서 찾을 수 있습니다. 이 목록에 표시되지 않는 자리 표시자는 읽기 전용입니다.

- %DefaultAuditingDir%
- %DefaultDataDir%
- %DefaultLoggingDir%
- %IntroscopeAgentEnableInstrumentation%
- %IntroscopeAgentEnterpriseManagerHost%
- %IntroscopeAgentEnterpriseManagerPort%
- %IntroscopeAgentEnterpriseManagerTransport%
- %NCSInstrumentLevelThreshold%
- %SMDAgentHost%
- %SMDAgentPort%

관련 항목

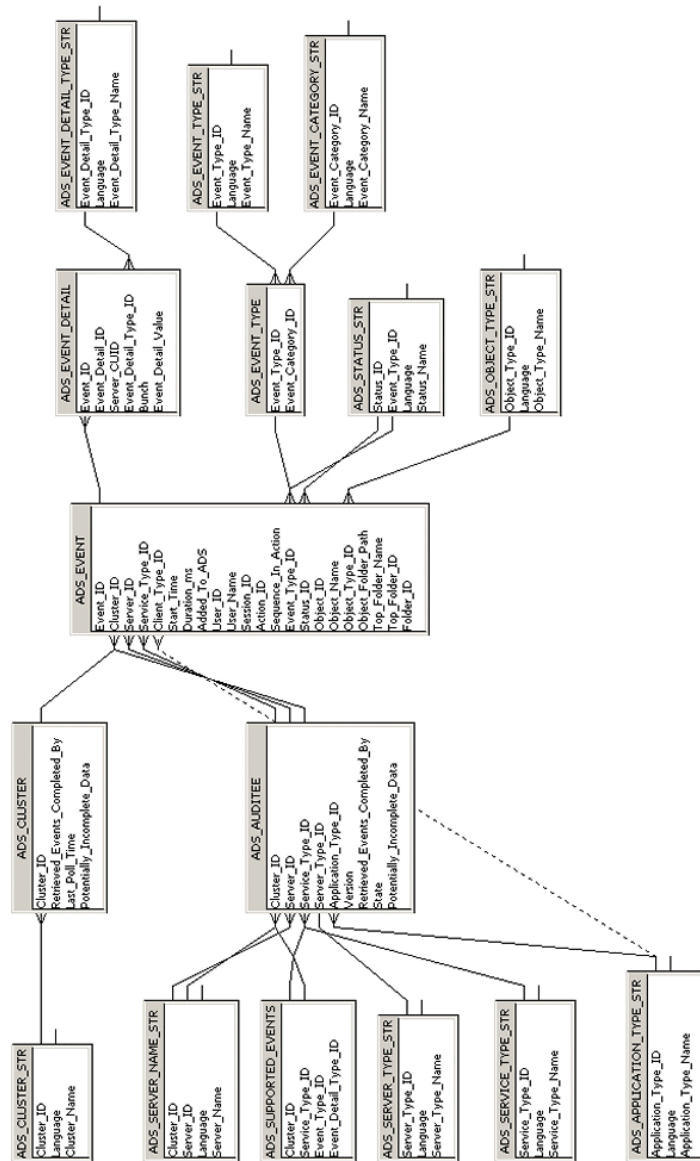
- 426 페이지에서 [노드의 자리 표시자 보기 및 편집](#)

장27 감사 데이터 저장소 스키마 부록

27.1 개요

이 부록은 감사 데이터 저장소 테이블에 액세스하거나 이 테이블을 통해 보고서를 작성하게 될 보고서 디자이너를 위한 자료입니다. 다음 그림과 표의 설명을 통해 감사 데이터가 기록되는 위치와 테이블 간의 관계를 알 수 있습니다.

27.2 스키마 다이어그램



27.3 감사 데이터 저장소 테이블

ADS_EVENT 테이블

이 테이블은 스키마 내의 다른 테이블에 대한 중앙 연결 지점인 각 이벤트의 기본 속성을 기록합니다.

열 이름	필드 형식	키	설명
Event_ID	문자(64)	기본 키	이벤트에 대해 생성된 고유 ID입니다.
Cluster_ID	문자(64)	ADS_Auditee 테이블의 외래 키	감사 대상 클러스터의 GUID입니다. 여러 클러스터에서 동일한 ADS를 사용할 수 있기 때문에 이 속성이 기록됩니다.
Server_ID	문자(64)	ADS_Auditee 테이블의 외래 키	이벤트를 트리거한 서버의 CUID입니다.
Service_Type_ID	문자(64)	ADS_Auditee 테이블의 외래 키	<ul style="list-style-type: none"> 이벤트를 트리거한 서비스 유형의 CUID입니다. 서버의 서비스는 해당 서비스 유형 CUID를 기록합니다. 클라이언트 응용 프로그램(BI 실행 패드 또는 Web Intelligence 등)은 해당 응용 프로그램 유형 CUID를 기록합니다.
Client_Type_ID	문자(64)	ADS_Application_Type 테이블의 외래 키	세션을 설정한 클라이언트의 클라이언트 유형 ID를 기록합니다.
Start_Time	날짜/시간	해당 없음	이벤트 작업이 시작된 날짜 및 시간(밀리초)입니다.
Duration_ms	정수	해당 없음	작업 기간(밀리초)입니다.
Added_to_ADS	날짜/시간	해당 없음	ADS에서 이벤트가 기록된 날짜 및 시간입니다.
User_ID	문자(64)	해당 없음	작업을 수행한 사용자의 CUID입니다.
User_Name	문자(255)	해당 없음	작업을 수행한 사용자의 ID와 관련된 이름입니다. 감사자 CMS의 기본 언어로 기록됩니다.
Session_ID	문자(64)	해당 없음	이벤트가 트리거된 세션의 GUID입니다. 연결된 세션이 없으면 필드는 Null입니다.
Action_ID	문자(64)	해당 없음	이벤트를 트리거한 사용자 작업의 ID입니다. 단일 사용자 작업의 결과로 발생하는 이벤트를 그룹화하는 데 사용됩니다.
Sequence_In_Action	정수	해당 없음	다중 서버(또는 클라이언트 및 다중 서버) 이벤트의 경우, 이벤트를 트리거한 시퀀스 내의 서버 또는 클라이언트 응용 프로그램입니다. 모든 일정 설정 워크플로에서 시퀀스 ID는 항상 0입니다.
Event_Type_ID	정수	ADS_Event_type 테이블의 외래 키	이벤트의 유형입니다(예: 보기 또는 저장).

열 이름	필드 형식	키	설명
Status_ID	정수	ADS_Status_Str 테이블의 외래 키	작업 상태입니다(예: "0" = 성공, "1" = 실패).
Object_ID	문자(64)	해당 없음	작업이 수행된 개체의 CUID입니다.
Object_Name	문자(255)	해당 없음	작업이 수행된 개체의 이름입니다. 감사자 CMS의 기본 언어로 기록됩니다.
Object_Type_ID	문자(64)	ADS_Object_Type_Str 테이블의 외래 키	작업이 수행된 개체 유형의 CUID입니다.
Object_Folder_Path	문자(255)	해당 없음	작업이 수행된 개체의 전체 폴더 경로(예: Country/Region/City)입니다. 감사자 CMS의 기본 언어로 기록됩니다. 폴더 경로를 확인할 수 없는 경우 이 값은 Null로 설정됩니다.
Folder_ID	문자(64)	해당 없음	작업이 수행된 개체에 대한 폴더의 CUID입니다.
Top_Folder_Name	문자(255)	해당 없음	개체 최상위 폴더의 이름입니다. 예를 들어 개체가 Country/Region/City에 있다면 Country가 기록됩니다.
Top_Folder_ID	문자(64)	해당 없음	개체가 있는 최상위 폴더의 CUID입니다. 예를 들어 개체가 Country/Region/City에 있다면 값은 Country 폴더의 CUID가 기록됩니다.

ADS_EVENT_DETAIL 테이블

이 테이블은 이벤트 세부 정보 속성을 기록합니다.

열 이름	형식	키	설명
Event_Detail_ID	정수	기본 키	이벤트 세부 정보에 대한 GUID입니다.
Event_ID	문자(64)	ADS_Event 테이블의 외래 키	상위 이벤트 GUID입니다.
Event_Detail_Type_ID	정수	ADS_Event_Detail_Str의 외래 키	이벤트 세부 정보의 유형입니다.

열 이름	형식	키	설명
Bunch	정수	해당 없음	<p>세부 정보가 계열의 일부일 경우 이들을 함께 연결하는 데 사용됩니다.</p> <p>예를 들어 보고서에 State 및 Country에 대한 프롬프트가 있는 경우, Country 프롬프트에는 "USA", State 프롬프트에는 "California" 및 "Nevada"를 입력할 수 있습니다. 그러면 두 개의 묶음으로 구성된 이벤트 세부 정보가 생성됩니다. Bunch 1은 다음으로 구성됩니다.</p> <ul style="list-style-type: none"> 프롬프트 이름: Country 프롬프트 값: USA <p>Bunch 2는 다음으로 구성됩니다.</p> <ul style="list-style-type: none"> 프롬프트 이름: State 프롬프트 값: California 프롬프트 값: Nevada
Event_Detail_Value	문자(긴 텍스트)	해당 없음	이벤트 세부 정보의 값입니다.

ADS_AUDITEE 테이블

이 테이블은 배포에 포함된 모든 감사 대상 서버에 대한 속성 정보를 기록합니다.

열 이름	형식	키	설명
Cluster_ID	문자(64)	기본 키	감사 대상이 속해 있는 클러스터의 GUID입니다.
Server_ID	문자(64)	<ul style="list-style-type: none"> 기본 키 ADS_Server_Name_STR 	이벤트를 트리거한 서버의 CUID입니다. 이벤트가 클라이언트에서 트리거된 경우 이벤트를 처리한 적응형 처리 서버의 CUID가 기록됩니다.
Service_Type_ID	문자(64)	<ul style="list-style-type: none"> 기본 키 ADS_Service_Type_Str ADS_Supported_Events 	이벤트를 트리거한 서비스의 서비스 유형 CUID입니다. 클라이언트에서 트리거된 이벤트의 경우 응용 프로그램 유형 CUID가 기록됩니다.
Server_Type_ID	문자(64)	ADS_Server_Type_Str	이벤트를 트리거한 서버의 서버 유형 CUID입니다.

열 이름	형식	키	설명
Application_Type_ID	문자(64)	ADS_Application_Type_Str	이벤트를 트리거한 클라이언트의 응용 프로그램 유형 CUID입니다. 서버 이벤트의 경우 서비스 유형의 ID가 기록됩니다.
Version	문자(64)	해당 없음	기록될 당시 이벤트를 트리거한 서버 또는 클라이언트의 버전입니다.
Retrieved_Events_Completed_By	날짜/시간	해당 없음	감사자 CMS가 임시 파일이 있는지 확인하기 위해 감사 대상을 마지막으로 폴링한 시간입니다. 이는 이 날짜/시간에 도달하기 이전에 완료된 해당 감사 대상의 모든 이벤트가 ADS에 있음을 나타냅니다.
State	정수	해당 없음	감사 대상의 상태(실행 중, 실행 중이지 않음, 삭제됨)입니다.
Potentially_Incomplete_Data	정수	해당 없음	해당 감사 대상에 ADS로 전송되지 않은 이벤트가 있는지 여부를 표시합니다.

ADS_SERVER_NAME_STR 테이블

이 테이블은 서버 이름에 대한 다국어 사전을 제공합니다. 값은 서버의 이름이 바뀔 때 업데이트됩니다.

열 이름	형식	키	설명
Cluster_ID	문자(64)	기본 키	서버가 속해 있는 클러스터의 GUID입니다.
Server_ID	문자(64)	기본 키	서버의 CUID입니다.
Language	문자(10)	기본 키	서버 이름 언어에 대한 코드입니다(예: EN 또는 DE).
Server_Name	문자(255)	해당 없음	서버 이름입니다.

ADS_SERVICE_TYPE_STR 테이블

이 테이블은 서버 유형 이름에 대한 다국어 사전을 제공합니다.

열 이름	형식	키	설명
Service_Type_ID	문자(64)	기본 키	서비스의 서비스 유형 또는 서비스 범주 CUID입니다.

열 이름	형식	키	설명
Language	문자(10)	기본 키	서버 유형 이름이 기록된 언어에 대한 코드입니다(예: EN 또는 DE).
Service_Type_Name	문자(255)	해당 없음	서비스 유형 이름입니다.

ADS_APPLICATION_TYPE_STR 테이블

이 테이블은 클라이언트 응용 프로그램 유형 이름에 대한 다국어 사전을 제공합니다.

열 이름	형식	키	설명
Application_Type_ID	문자(64)	기본 키	응용 프로그램의 응용 프로그램 유형 CUID입니다.
Language	문자(10)	기본 키	응용 프로그램 유형이 기록된 언어에 대한 코드입니다(예: EN 또는 DE).
Application_Type_Name	문자(255)	해당 없음	응용 프로그램 유형의 텍스트 이름입니다(예: Crystal Reports 또는 Web Intelligence).

ADS_SUPPORTED_EVENTS 테이블

이 테이블은 지원되는 이벤트 목록 및 서버 또는 클라이언트 응용 프로그램의 유형별 관련 이벤트 세부 정보를 기록합니다.

열 이름	형식	키	설명
Cluster_ID	문자(64)	기본 키	서버가 속해 있는 클러스터 GUID입니다.
Service_Type_ID	문자(64)	기본 키	이벤트를 트리거한 서비스의 서비스 유형 CUID입니다. 클라이언트 응용 프로그램에서 이벤트를 트리거한 경우 응용 프로그램 유형 CUID가 기록됩니다.
Event_Type_ID	정수	ADS_Event_Type의 외래 키	기록된 이벤트의 유형에 대한 ID입니다(예: 저장 ID).
Event_Detail_Type_ID	정수	ADS_EVENT_DETAIL_TYPE_STR	해당 이벤트에 대해 캡처된 이벤트 세부 정보의 유형을 식별하는 CUID입니다(예: 파일 경로).

ADS_CLUSTER 테이블

이 테이블은 감사 대상이 포함되어 있는 클러스터에 대한 정보를 기록합니다.

열 이름	형식	키	설명
Cluster_ID	문자(64)	<ul style="list-style-type: none"> 기본 키 ADS_Cluster_Str 	클러스터의 GUID입니다.
Retrieved_Events_Completed_By	날짜/시간	해당 없음	해당 클러스터에 대한 데이터베이스의 감사 정보가 얼마나 최신 상태인지를 표시합니다. 지정된 시점에서 현재 실행 중인 모든 감사 대상 서버에 대해 가장 이전에 검색된 감사 타임스탬프가 기록됩니다. 이는 이 날짜 이전에 완료된 모든 이벤트가 ADS에 있음을 나타냅니다.
Last_Poll_Time	날짜/시간	해당 없음	감사자 CMS가 이 클러스터에 있는 감사 대상을 마지막으로 폴링한 시간입니다.
Potentially_Incomplete_Data	정수	해당 없음	클러스터 내에 미완료된 감사 정보가 있을 수 있음을 나타냅니다. "0" = 모든 서버에서 데이터를 정상적으로 전송했습니다. "1" = 클러스터 내의 실행 중인 서버 또는 실행 중이지 않은 서버 중 적어도 하나의 서버에 미완료 데이터 플래그가 설정되어 있습니다. 즉, 한 개의 감사 대상에 ADS로 전송되지 않은 이벤트가 있습니다.

ADS_CLUSTER_STR 테이블

이 테이블은 배포 내에 있는 여러 클러스터의 참조 레코드를 제공합니다.

열 이름	형식	키	설명
Cluster_ID	문자(64)	기본 키	클러스터 고유 ID입니다.
Language	문자(10)	해당 없음	클러스터 언어 설정에 대한 코드입니다 (예: EN 또는 DE).
Cluster_Name	문자(255)	해당 없음	클러스터 이름입니다.

ADS_EVENT_TYPE 테이블

이 테이블은 이벤트의 여러 범주에 대한 참조 레코드를 제공합니다.

열 이름	형식	키	설명
Event_Type_ID	정수	복합 • 기본 키 • ADS_Event_Type_Str	이벤트 유형에 대한 고유 식별자입니다.
Event_Catagory_ID	정수	ADS_Event_Category_Str 테이블	이벤트의 범주입니다 (예: 공통, Web Intelligence 또는 Life-Cycle Management).

ADS_EVENT_TYPE_STR 테이블

이 테이블은 이벤트 유형 이름에 대한 다국어 사전을 제공합니다.

열 이름	형식	키	설명
Event_Category_ID	정수	기본 키	이벤트의 이벤트 유형 ID입니다.
Language	문자(10)	기본 키	이벤트 범주 이름이 기록된 언어에 대한 코드입니다(예: EN 또는 DE).
Event_Type_Name	문자(255)	해당 없음	이벤트 유형의 텍스트 이름입니다(예: 보기 또는 로그인).

ADS_EVENT_CATEGORY_STR 테이블

이 테이블은 이벤트 범주 이름에 대한 다국어 사전을 제공합니다.

열 이름	형식	키	설명
Event_Type_ID	정수	기본 키	이벤트 범주 ID입니다.
Language	문자(10)	기본 키	이벤트 범주 이름이 기록된 언어에 대한 코드입니다(예: EN 또는 DE).
Event_Category_Name	문자(255)	해당 없음	이벤트 범주 이름입니다.

ADS_EVENT_DETAIL_TYPE_STR 테이블

이 테이블은 이벤트 세부 정보 유형 이름에 대한 다국어 사전을 제공합니다.

열 이름	형식	키	설명
Event_Detail_ID	정수	기본 키	이벤트 세부 정보의 이벤트 세부 정보 유형 ID입니다.
Language	문자(10)	기본 키	이벤트 세부 정보 이름이 기록된 언어에 대한 코드입니다(예: EN 또는 DE).

열 이름	형식	키	설명
Event_Detail_Type_Name	문자(255)	해당 없음	이벤트 세부 정보 유형의 이름입니다.

ADS_OBJECT_TYPE_STR 테이블

이 테이블은 이벤트 개체 이름에 대한 다국어 사전을 제공합니다.

열 이름	형식	키	설명
Object_Type_ID	문자(64)	기본 키	개체의 개체 유형 CUID입니다.
Language	문자(10)	기본 키	개체 유형 이름이 기록된 언어에 대한 코드입니다(예: EN 또는 DE).
Object_Type_Name	문자(255)	해당 없음	개체 유형의 이름입니다.

ADS_STATUS_STR 테이블

이 테이블은 이벤트 상태 이름에 대한 다국어 사전을 제공합니다.

열 이름	형식	키	설명
Status_ID	정수	기본 키	작업 상태를 나타내는 숫자입니다.
Event_Type_ID	정수	기본 키	이벤트의 이벤트 유형 ID입니다 (예: 보기 이벤트의 경우 1002).
Language	문자(10)	기본 키	이벤트 상태가 기록된 언어에 대한 코드입니다 (예: EN 또는 DE).
Status_Name	문자(255)	해당 없음	이벤트 상태에 대한 텍스트 설명입니다(예: 성공 또는 실패).

ADS_EVENT_DELETES

이 테이블을 사용하거나 보고하지 마십시오. 내부 시스템용으로, 이후 릴리스에서 제거될 수 있습니다.

부록A 추가 정보

정보 리소스	위치
SAP BusinessObjects 제품 정보	http://www.sap.com
SAP Help Portal	<p>http://help.sap.com/businessobjects/의 SAP BusinessObjects Overview 사이트 패널에서 All Products를 클릭하십시오.</p> <p>전체 SAP BusinessObjects 제품 및 배포에 대한 내용이 담긴 최신 문서를 SAP Help Portal에서 이용할 수 있습니다. PDF 버전 또는 설치 가능한 HTML 라이브러리를 다운로드할 수 있습니다.</p> <p>특정 가이드는 SAP Service Marketplace에 저장되어 있으므로 SAP Help Portal에서 이용할 수 없습니다. 이러한 가이드는 SAP Service Marketplace에 대한 링크와 함께 Help Portal에 나열되어 있습니다. 유지 관리 계약을 체결한 고객은 이 사이트에 액세스하도록 허용된 사용자 ID를 가지고 있습니다. ID를 얻으려면 고객 지원 담당자에게 문의하십시오.</p>
SAP Service Marketplace	<p>http://service.sap.com/bosap-support > Documentation</p> <ul style="list-style-type: none"> • 설치 가이드: https://service.sap.com/bosap-instguides • 릴리스 노트: http://service.sap.com/releasenotes <p>SAP Service Marketplace에는 설치 가이드, 업그레이드 및 마이그레이션 가이드, 배포 가이드, 릴리스 노트 및 지원되는 플랫폼 설명서가 저장되어 있습니다. 유지 관리 계약을 체결한 고객에게는 이 사이트에 액세스하도록 허용된 사용자 ID가 제공됩니다. ID를 얻으려면 고객 지원 담당자에게 문의하십시오. SAP Help Portal에서 SAP Service Marketplace로 리디렉션된 경우, 왼쪽의 탐색 창에 있는 메뉴를 사용하여 액세스하려는 문서가 있는 범주를 찾을 수 있습니다.</p>
Docupedia	<p>https://cw.sdn.sap.com/cw/community/docupedia</p> <p>Docupedia는 추가 문서 자료, 협력적 문서 작성 환경 및 대화형 피드백 채널을 제공합니다.</p>
개발자 리소스	<p>https://bos.sdn.sap.com/</p> <p>https://www.sdn.sap.com/irj/sdn/businessobjects-sdclibrary</p>

정보 리소스	위치
SAP Community Network의 SAP BusinessObjects 문서	https://www.sdn.sap.com/irj/boc/businessobjects-articles 이 문서의 이전 명칭은 기술 문서입니다.
노트	https://service.sap.com/notes 이 노트의 이전 명칭은 지식 기반 문서입니다.
SAP Community Network의 포럼	https://www.sdn.sap.com/irj/scn/forums
교육	http://www.sap.com/services/education 강의실에서 진행되는 일반적인 학습 과정에서 특정한 대상을 위한 온라인 학습에 이르기까지 고객이 원하는 학습 내용과 스타일에 맞는 교육 과정 패키지를 제공할 수 있습니다.
온라인 고객 지원	http://service.sap.com/bosap-support SAP Support Portal에는 고객 지원 프로그램 및 서비스에 대한 정보가 포함되어 있습니다. 이 포털에는 또한 다양한 기술 정보 및 다운로드에 대한 링크가 있습니다. 유지 관리 계약을 체결한 고객에게는 이 사이트에 액세스하도록 허용된 사용자 ID가 제공됩니다. ID를 얻으려면 고객 지원 담당자에게 문의하십시오.
컨설팅	http://www.sap.com/services/bysubject/businessobjectsconsulting 고객은 초기 분석 단계에서부터 배포 프로젝트 납품에 이르기까지 Business Objects 컨설턴트의 도움을 받을 수 있습니다. 관계형 및 다차원 데이터베이스, 연결, 데이터베이스 설계 도구 및 사용자 지정된 임베딩 기술과 같은 주제에서 전문 지식을 얻을 수 있습니다.

인덱스

기호

.NET SDK(소프트웨어 개발 키트) 33

A

Analysis, OLAP 에디션 71

B

BackupCluster.bat 473

backupcluster.sh 473

BEx 웹 응용 프로그램 526

BExWebApplicationsService 527

BI Widgets

SAP BusinessObjects Business
Intelligence 플랫폼용 위젯 참
조 64

BI 실행 패드 69

관리 503

구성 104

권한 810

그룹 기본 설정 106

로그온 104, 105

로그온 사용자 지정 523

액세스 제어 494

BI 작업 영역 69

BI 작업 영역, 권한 803, 811

BI 플랫폼

기본 인증 프로세스 212

보안 권장 사항 142

서버 간 통신 169

역방향 프록시 서버와 함께 배포
198, 199

역할 가져오기 293

역할 매핑 340

웹 응용 프로그램 컨테이너 서버
(WACS) 435

재해 복구 계획 141

최상위 폴더, 권한 125

BI 플랫폼 백업

서버 설정 471

BI 플랫폼 복원

서버 설정 477

BI 플랫폼 서버

Kerberos 및 브라우저 구성 257

방화벽용으로 hosts 파일 구성 181

BIAR 명령줄 도구 483

BIAR 엔진 명령줄 도구 485, 487, 491

BOE war 파일 104, 105

BOLMT 87, 361

Business Process BI 서비스

웹 응용 프로그램 컨테이너 서버에
추가 442

웹 응용 프로그램 컨테이너 서버에
서 제거 443

BW

BI 플랫폼과 통합 669

보기 활성화 685

BW 게시자

UNIX에서 구성 672

구성 요소 배포 672

서비스로 구성 672

BW 게시자 서비스 672

RFC 대상 만들기 673

구성 672

시작 673

C

CA Wily Introscope 40

cacert.der 162

cakey.pem 162

CCM

UNIX용 768, 770

Windows용 777, 779

노드 400

다시 만들기 406

사용자 자격 증명, 변경 423,
424

삭제 410

이동 414

이름 바꾸기 412

추가 402

서버 삭제 371

서버 시작, 중지 및 다시 시작 363,
365

서버 추가 369

서버 활성화 및 비활성화 367, 368

ccm.config 771

ccm.exe 777, 779

ccm.sh 768, 770

서버 설정 복원 478

Clearcase 41

CMC

Windows 서버 종속성, 추가 423

권한 810

서버 관리 355

서버 복제 370, 371

서버 삭제 371

서버 시작, 중지 및 다시 시작 363,
365

CMC (계속됨)

서버 활성화 및 비활성화 367

암호화 키 157

액세스 제어 494

CMS 285, 315, 542

구성 397, 398, 399, 427, 428,
429, 430

기본 포트 397, 398, 399

다른 서버 활성화 및 비활성화
367, 368

멀티홈 컴퓨터 문제 해결 397

메트릭 383

명령줄 옵션 781

문제 해결 366

분산 보안 144

세션 변수 145

인증 212

추적 146

속성 824

시작 366

이름 서버 397, 398, 399

인증 212

중지 366

클러스터 이름 변경 376

클러스터링 372, 375

새 클러스터 멤버 설치 374

요구 사항 372

클러스터에 추가 373

CMS 시스템 데이터베이스 427, 428,
476

다시 만들기 429, 430

백업 470

복사 431, 432, 433

복원 474, 475, 476

삭제 429, 430

선택 427, 428

암호 변경 427

CMS 시스템 데이터베이스 초기화
429, 430

cmsdbsetup.sh 771

Contextual Awareness 738

구성 738, 740

Crystal Reports

SAP Crystal Reports 참조 67

Crystal Reports 2010 Report

Application Server 542

Crystal Reports 2010 처리 서버 542

Crystal Reports Viewer SDK 33

Crystal Reports 처리 서버 542, 784

명령줄 옵션 784

Crystal Reports 캐시 서버 542

Crystal 보고서
권한 799
CTS 전송(CTS+) 40
custom.jsp 524

D

Dashboard Builder 69
Dashboard Design 처리 서버 785
명령줄 옵션 785

E

env.sh 775
ERP(Enterprise Resource Planning)
39
Explorer 613
SAP BusinessObjects Explorer
참조 68
권한 818

F

FIPS 호환 모드
FIPS(Federal Information
Processing Standard) 150
UNIX 설정 152
Windows 설정 151
Windows 해제 152
보안 설정 150

G

Guest 계정
비활성화 100
GWSETUP 674

H

hosts 파일, NAT 방화벽에 대해 구성
181
HTML 쿼리 패널, 액세스 권한 504
HTTP 145, 212
HTTPS
웹 응용 프로그램 컨테이너 서버
(WACS) 구성 444, 446, 461

I

InfoSet 연결 전송 689
InfoView 69
initlaunch.sh 776
INSTALLDIR 18
Introscope 558

IPv6
CMC 391
CMC에서 주소 설정 394
옵션 391
ISA 2006
Oracle 10gR3에 대해 구성 206
Sun Java 8.2에 대해 구성 206
Tomcat 5.5에 대해 구성 206
WebSphere CE 2.0에 대해 구성
206
iView
보기 활성화 685

J

JAAS, 구성 파일 260, 261, 452
Java SDK(소프트웨어 개발 키트) 33
Java 응용 프로그램 서버, Kerberos
257
Java, Kerberos 264, 265
JD Edwards EnterpriseOne 39
JD Edwards EnterpriseOne 통합
방화벽 구성 191
JMX MBean 555
JMX 원격 API 553
JMX(Java Management Extensions)
539

K

Kerberos 257, 450
Java InfoView용 단일 로그인 266
Java용 single sign-on 458, 459
Krb5.ini 260, 452
구성 파일 258, 259, 451
문제 해결 283, 454
및 NetWeaver SSO 262
Kerberos 구성 257
KPI(핵심 성과 지표) 537
Krb5.ini 260, 452

L

LDAP
SSL(Secure Sockets Layer) 230
Windows AD에 대해 매핑 246
계정 230
문제 해결 247
그룹
매핑 243
단일 로그인 구성 241
보안 플러그 인 231
인증 230
구성 232
인증 플러그 인 231

LDAP (계속됨)
호스트
구성 233, 237
여러 개 관리 236
LDAP(Lightweight Directory Access
Protocol)LDAP 참조 230
Live Office
역방향 프록시 서버에 대한 구성
203
logon.csp 212

M

MBeans 539
Mobile
권한 819
Monitoring 에이전트 555

N

NetWeaver Enterprise Search에서
검색 616
NWES를 이용한 검색 시간 통합 614

O

ODBC
CMS 데이터베이스
연결 431
Open SQL 연결 689
Open SQL 연결 전송 689
OpenDocument
로그온 사용자 지정 523
OpenSearch 602
OpenSearch 구성 602
Oracle
JAAS 261
Java 옵션 264
Kerberos 258
Oracle E-Business Suite 39
역할을 정보 플랫폼 서비스에 매핑
346
Oracle E-Business Suite 통합
방화벽 구성 193
Oracle EBS
별칭 업데이트 349
역할 업데이트 349

P

PeopleSoft Analytic Server 734
PeopleSoft Enterprise 39
PeopleSoft Enterprise 통합
방화벽 구성 194

PeopleSoft EPM 보안 브리지
응답 파일 323
PeopleSoft 응답 파일 328
매개 변수 328
Platform Java Server 539
PLATFORM64DIR 18
PlatformServices.properties 375
PM 리포지토리 서버 542
PSANALYTIC 프로세스 734
PSAPPSRV 프로세스 734
PSE
서버 측 트러스트 297
액세스 구성 304

Q

Query as a Web Service
웹 서비스 쿼리 도구 참조 62

R

Report Application Server
명령줄 옵션 787
필수 개체 권한 381
Report Application Server SDK 33
restart.sh 774
RestoreCluster.bat 478
restorecluster.sh 478
RFC 대상 673
BW 게시자 서비스용 673
로컬 SAP 게이트웨이 675
RMI 프로토콜 550
RMI(Remote Method Invocation)
539

S

SAML
SSO 221
SAP
방화벽 구성 190
별칭 업데이트 295
역할 업데이트 295
통합 40
SAP BusinessObjects Analysis,
Microsoft Office용 에디션 66
SAP BusinessObjects Business
Intelligence 플랫폼
백업 및 복원 470
아키텍처 다이어그램 28
SAP BusinessObjects Business
Intelligence 플랫폼 SDK 33
SAP BusinessObjects Business
Intelligence 플랫폼 백업 469, 470
서버 설정 472

SAP BusinessObjects Business
Intelligence 플랫폼 복원 469
CMS 시스템 데이터베이스 474
서버 설정 476, 478
파일 시스템 474, 479
SAP BusinessObjects Business
Intelligence 플랫폼 서버
Kerberos 및 브라우저 구성 450
SAP BusinessObjects Business
Intelligence 플랫폼 소비자 SDK
33
SAP BusinessObjects Business
Intelligence 플랫폼용 위젯 64
SAP BusinessObjects Dashboard
Design 67
SAP BusinessObjects Enterprise
권한 113
추적 743
SAP BusinessObjects Enterprise 백
업
서버 설정 473
SAP BusinessObjects Enterprise 복
원
CMS 시스템 데이터베이스 475
SAP BusinessObjects Enterprise 서
버 554
SAP BusinessObjects Explorer 68,
508
설정 관리 508
응용 프로그램 속성 509
SAP BusinessObjects Mobile 71
SAP BusinessObjects SDK 149
SAP BusinessObjects Web
Intelligence 71
SAP Crystal Reports 67
SAP ERP 39
SAP Passport 766
SAP Solution Manager 40
SLD 759
SMD 761
개요 757
SAP 게이트웨이 307
구성 요소 배포 672
로컬을 사용하여 게시 674
및 SNC 307
설치 674
SAP 비즈니스 탐색기 526
SAP 인증 285
CMC 옵션 289
SAPGENPSE 304
SCRIPTDIR 18
SDK
소프트웨어 개발 키트 참조 33
웹 서비스 SDK 34
플랫폼 검색 602
Secure Sockets Layer, 구성 741

Server Intelligence Agent 21
Windows 서버 종속성, 추가 423
노드 400, 402, 406, 409, 412
다시 만들기 406, 407, 408,
409, 410, 411, 418
사용자 자격 증명, 변경 423,
424
삭제 410, 411, 418
새 컴퓨터, 추가 402
이동 414, 415, 416, 417, 420
이름 바꾸기 412, 413
추가 402, 403, 404, 405, 418
자동 서버 시작 366
serverconfig.sh 772, 773
노드
다시 만들기 408
삭제 411
이동 416
이름 바꾸기 413
추가 404
setup.sh 776
SI_AVAILABILITY_PROPERTY 542
SIA(Server Intelligence Agent)
시작 워크플로 73
종료 워크플로 74
Siebel Enterprise 39
Siebel 통합
Crystal Reports 메뉴 항목, 만들
기 736
Siebel 응용 프로그램 다시 컴파일
737
방화벽 구성 196
통합 프로젝트 735
single sign-on
Kerberos 458, 459
SiteMinder
BOE war 구성 242
LDAP 플러그 인 구성 241
LDAP를 사용하여 단일 로그인 설
정 241, 275
Windows AD 275
문제 해결 242
오류 242
SLD(System Landscape Directory)
connect.key 파일 759
SMAdmin 계정 762
SMD 761
SMD 에이전트 762
SNC
보안 네트워크 통신 참조 297
Solution Manager 537
SMAdmin 계정 762
SPN 유틸리티 253
SSL 161, 164, 166
sslconfig.exe 166
번역 관리 도구 167

SSL(계속됨)
 보고서 변환 도구 168
 서버 구성 161, 164, 166
 씹(thick) 클라이언트 166
 웹 응용 프로그램 컨테이너 서버
 (WACS) 구성 444, 446
 인증서 162
 키 162
 SSL(Secure Socket Layer)
 구성 729, 731
 SSL(Secure Sockets Layer) 146,
 161, 164, 166, 230
 및 LDAP 230
 및 부하 분산 144
 sslc.cnf 161
 sslc.exe 161
 SSLSSL(Secure Sockets Layer) 참
 조 230
 startservers 774
 stopservers 774
 Subversion 41
 syslog 384
 System Landscape Directory(SLD)
 40
 등록 759
 등록 확인 761
 트리거 760

T

Tomcat
 JAAS 260
 Kerberos 258

U

Universe Designer
 유니버스 디자인 도구 참조 62
 UNIX
 syslog 384
 UNIX 스크립트, 개요 767

V

Vintela 266
 WebLogic 고려 사항 270
 Voyager 71
 SAP BusinessObjects Analysis
 참조 66

W

WACS(웹 응용 프로그램 컨테이너 서
 버)
 JAAS 파일 452

WACS(웹 응용 프로그램 컨테이너 서
 버) (계속됨)
 Kerberos 구성 파일 451
 다른 웹 서버로 사용 459
 방화벽 461
 부하 분산 460
 서버 오류 463
 속성 468
 일반 작업 436
 WAR 파일
 BI 플랫폼 웹 응용 프로그램 198,
 199
 BOE 199, 514, 515, 518, 520
 BOE war 파일
 BI 실행 패드 속성 518
 CMC 속성 522
 OpenDocument 속성 520
 전역 속성 515
 dswsbobje 199
 OpenDocument 266
 WDeploy 68
 WDeploy를 사용하여 OpenSearch
 603
 Web Intelligence 504, 786
 HTML 쿼리 액세스 권한 504
 권한 812
 응용 프로그램 권한 504
 처리 서버 790
 Web Intelligence Desktop 61
 Web Intelligence 문서
 권한 800
 Web Intelligence 처리 서버 19, 44,
 542
 WebLogic
 JAAS 구성 파일 260
 Java 옵션 264
 Kerberos 258
 WebSphere
 JAAS 261
 Java 옵션 265
 Kerberos 259
 Windows
 서버 종속성, 추가 423
 이벤트 로그 384
 Windows AD
 Kerberos 구성
 응용 프로그램 서버 257
 Kerberos 활성화 449, 450
 LDAP 매핑 246
 Vintela 270
 계정 매핑 250
 계정 및 그룹 250
 업데이트 일정 설정 250
 그룹 매핑 250
 단일 로그인 267, 270
 보안 플러그 인 249

Windows AD (계속됨)
 서비스 계정 267
 인증 248
 Windows 스크립트, 개요 776

X

Xcelsius 데이터 처리 서버 542
 Xcelsius 데이터 캐시 서버 542
 Xcelsius. SAP BusinessObjects
 Dashboard Design 참조 67

Y

가상 메트릭 542
 가져오기 마법사
 업그레이드 관리 도구 참조 23, 66
 감사
 CMC 페이지 569
 Web Intelligence 이벤트 592
 감사 데이터 저장소
 스키마 다이어그램 895
 스키마 테이블 896
 공통 이벤트 581
 구성 569
 데이터베이스 연결 설정 573
 메트릭 569
 분석기 이벤트 593
 상태 요약 569
 아키텍처 563
 웹 작업 147
 이벤트
 구성 571
 데이터베이스 보존 573
 목록 575
 속성 및 세부 정보 575
 이벤트 세부 정보 581, 590, 592,
 593, 594
 이벤트 세부 정보 ID 581, 590,
 592, 593, 594
 이벤트 속성 581, 592, 593, 594
 이벤트 유형
 MDAS 세션 593
 MDAS 큐브 연결 593
 VMS 검색 594
 VMS 내보내기 594
 VMS 잠금 594
 VMS 잠금 해제 594
 VMS 체크아웃 594
 VMS 체크인 594
 VMS 추가 594
 감사 수정 590
 검색 581
 권한 수정 590
 로그아웃 581
 로그인 581

- 감사 (계속됨)
 - 이벤트 유형 (계속됨)
 - 롤백 594
 - 만들기 581
 - 배달 581
 - 범위 밖으로 드릴 592
 - 보기 581
 - 사용자 지정 액세스 수준 수정 590
 - 삭제 581
 - 수정 581
 - 실행 581
 - 저장 581
 - 트리거 581
 - 페이지 검색 592
 - 편집 581
 - 프롬프트 581
 - 이벤트 유형 ID 581, 590, 592, 593, 594
 - 정보 흐름 563
 - 주기 관리 콘솔 이벤트 594
 - 플랫폼 이벤트 590
- 감사 구성, 감사 참조 569
- 감사 데이터베이스 470
- 감사 로그 파일 470
- 감시 537
- 개요 599
- 개인 보안 환경
 - PSE 참조 297
- 개체
 - 권한 670, 795
 - 보기 123
 - 설정 124
- 개체 충돌
 - 단방향 복제 649, 650
 - 양방향 복제 649, 651
- 검색 501, 599
 - 토론 스레드 501
- 검색 가능한 콘텐츠 유형 609
- 게시
 - 관리 권장 사항 385
 - 다중 BI 플랫폼 시스템 679
 - 배치 모드로 보고서 685
 - 백그라운드에서 683
 - 백그라운드에서 예약 683
 - 설정 675
 - 역할 또는 시스템의 보고서 681
 - 역할 정의, BW에서 676
 - 역할을 사용하여 여러 보고서 681
- 게시 권한 할당 352
- 경고 505
 - 관리 505
 - 권한 817
 - 기본 속성 507
 - 대상 속성 506
 - 설정 관리 505
- 계정
 - 관리 89, 94
 - 정보 플랫폼 서비스 285
- 계층 765
 - 개요 763
 - 로깅 765
 - 비 Java 서버 763
 - 웹 계층 765
 - 자리 표시자 764
 - 확인 765
- 계층 42
 - 고급 권한 114, 122, 125
 - 공유 라이브러리, 처리 확장 149
- 관계 쿼리
 - 액세스 수준 134
- 관리
 - BI 실행 패드 494
 - CMC 494
 - 권한 137
 - 권한 할당 351
 - 그룹 103
 - 받은 파일함 104
 - 사용자 103
 - 서버 및 서버 그룹 380, 381
 - 위임 137
 - 응용 프로그램 494
- 관리되는 개체 322
 - BusinessObjects Enterprise 그룹 322, 326
 - PeopleSoft 역할 322, 326
 - 유니버스 322, 327
- 구성 550
 - Apache 2.2 200
 - CMS 데이터베이스 427, 428
 - CMS 시스템 데이터베이스 429, 430
 - CMS 클러스터 376
 - ISA 2006 202
 - Secure Sockets Layer 741
 - WebSEAL 6.0 201
- 구성 템플릿 389
 - 노드 372
 - 다중 서버 388
 - 방화벽 179
 - 신뢰할 수 있는 인증 220
 - 역방향 프록시 서버 199, 200
 - 응용 프로그램 계층 387
 - 인텔리전스 계층 387
 - 처리 계층 387
 - 클러스터 372
- 구성 모드 321
- 구성 요소 689, 695
 - 클러스터 정의 도구 689, 695
- 구성 템플릿 388
 - 설정 389
 - 시스템 기본값 복원 391
- 구성 템플릿 (계속됨)
 - 적용 390
 - 최상의 방법 388
- 국제화 37
- 권한 113, 351, 795
 - BI 실행 패드 494, 810
 - BI 작업 영역 803, 811
 - CMC 494, 810
 - Crystal 보고서 799
 - Explorer 818
 - Mobile 819
 - Report Application Server 381
 - Web Intelligence 812
 - Web Intelligence 문서 800
- 게시 권한 352
- 경고 817
- 고급 권한 114, 125
- 관리 123, 137, 140
- 관리 권한 351
- 권한
 - 복제 626, 627, 628, 629, 630
- 권한 무시 118
- 권한의 범위 120
- 그룹 103, 801
- 메모 799
- 받은 파일함 104
- 범위 제한 120
- 범주 798
- 보기 123
- 보기와 요청 시 보기 130
- 보안 관리 626, 627, 628, 629, 630
- 보안 주체에 할당 124
- 보안 쿼리 126, 127
- 사용자 103, 801
- 상속 115
 - 그룹 116
 - 무시 135
 - 폴더 117
- 서버 380, 381
- 서버 그룹 380, 381
- 소유자 권한 140
- 액세스 수준 114, 802
 - 관계 쿼리 134
 - 복제 134
 - 사이트 간 관리 134
 - 작업 128
 - 포함된 권한 수정 133
- 위젯 816
- 유니버스 디자인 도구 815
- 유니버스 연결 808
- 유니버스(.unv) 804
- 유니버스(.unx) 805
- 유형별 권한 121
- 유효한 권한 122
- 응용 프로그램 494

권한 (계속됨)
 일반 795
 전략 작성기 814
 정보 디자인 도구 816
 최상위 폴더 125
 폴더 797
 권한 범위 120
 권한 부여 시스템 287
 권한 탐색기 123
 그룹 293
 BI 실행 패드 기본 설정 106
 관리 91
 권한 801
 권한 무시 118
 상속 116
 상속 무시 135
 최상위 폴더 125
 권한 할당 124
 권한 확인 126, 127
 기본값 91
 만들기 97
 매핑 316, 334, 340, 346
 보기
 권한 123
 멤버 98
 사용자 추가 100
 삭제 99
 소속 그룹 지정 99
 수정 97
 암호화 담당자 156
 액세스 허용 103
 하위 그룹 추가 98
 기본 네트워크 인터페이스 396
 기본 보안 패턴 670
 기본 설정
 서버 391
 포트 397, 398, 399
 기본 인증 212
 기본이 아닌 네트워크 인터페이스 396

L

네트워크 인터페이스
 다중 문제 해결 396
 네트워크 인터페이스 문제 해결 397
 네트워크 주소 변환
 구성, 서버 hosts 파일 181
 네트워크 환경
 IPv4
 이중 IPv4/IPv6 노드 392
 IPv6 392
 노드 19, 44, 400
 CMC 355
 다시 만들기 418
 AddNode.bat 407
 addnode.sh 409

노드 (계속됨)
 다시 만들기 (계속됨)
 CCM 406
 RemoveNode.bat 410
 removenode.sh 411
 serverconfig.sh 408
 시나리오 406
 삭제 409, 418
 CCM 410
 serverconfig.sh 411
 이동 414, 420
 CCM 414
 MoveNode.bat 415
 movenode.sh 417
 serverconfig.sh 416
 이름 바꾸기 412
 CCM 412
 serverconfig.sh 413
 추가 402, 418
 AddNode.bat 403
 addnode.sh 405
 CCM 402
 CMS 373
 serverconfig.sh 404
 새 컴퓨터 402
 클러스터에 추가 374
 클러스터링 372
 노드 관리 스크립트, 위치 401
 노드 자리 표시자 885
 녹색 확인 표시, 기본 시스템에 대한 679

U

다국어 지원 612
 다이어그램, 아키텍처 28
 다중 홈 컴퓨터 394
 웹 응용 프로그램 컨테이너 서버 (WACS) 462
 단방향 복제 631
 단일 로그인 38, 214, 275, 285
 BI 플랫폼 214
 Kerberos 266
 데이터베이스 215
 문제 해결 242
 서비스 계정 267
 설정
 LDAP 241
 SiteMinder 241, 275
 Windows AD 251
 역할 가져오기 293
 익명 214
 인증
 Windows AD 251
 중단 간 215

단일 로그인, JD Edwards에 대한 구성 728
 단일 로그인, Oracle EBS에 대해 구성 353
 단일 로그인, PeopleSoft에 대해 구성 730
 단일 로그인, SAP Netweaver에 대해 구성 314
 단일 로그인, Siebel에 대해 구성 740
 대상 사이트
 액세스 수준 134
 대시보드 537
 대시보드 분석 서버 542, 824
 명령줄 옵션 794
 대시보드 서버 542, 824
 명령줄 옵션 794
 데몬, 신호 처리 781
 데스크톱 클라이언트 60
 데이터
 라이브 130
 영구 42
 저장 130
 데이터 보안
 FIPS 호환 모드 150
 개요 150
 기본 데이터 처리 모드 150
 암호화 153
 암호화 키 153
 이전 버전과의 호환성 150
 이중 키 암호화 150
 클러스터 키 153
 데이터 소스 연결 533
 데이터 액세스
 설치 개요 688
 데이터 연합 관리 도구 64
 데이터베이스 29
 CMS 초기화 429, 430
 CMS에 대해 선택 427, 428
 단일 로그인 액세스 215
 뷰 36
 유니버스 36
 동적 연결 라이브러리, 처리 확장 149
 디렉터리 서버 231
 LDAP 정보 230
 보안 플러그 인 231

R

라이브 데이터 130
 라이선스 감사 87, 361
 프로시저 87, 361
 라이선스 키 86, 360
 CMS 데이터베이스 마이그레이션 431
 개요 85, 359
 구입 85, 359

- 라이선스 키 (계속됨)
 - 보기 85, 359
 - 추가 86, 360
 - 측정 방법 87, 361
- 레지스트리 키 242
- 로그온
 - BI 실행 패드 105
 - 불법 시도 방지 148
 - 사용자 지정 523
 - 워크플로 72
- 로그온 사용자 지정
 - BI 실행 패드 523
 - OpenDocument 523
- 로그온 수, 로그온 토큰 144
- 로그온 토큰 144
 - 분산 보안 144
 - 세션 추적 145
 - 인증 212
- 로그 384, 765
 - 서버 작업 384
 - 웹 작업 147
- 리포지토리 진단 도구 23, 66
- 리포트
 - 삭제 685
- - 만들기
 - 그룹 97
 - 사용자 계정 94
 - 서버 하위 그룹 379
 - 액세스 수준 131
 - 매핑된 사용자, 별칭 관리 108
 - 멀티홈 컴퓨터 395
 - 메모, 권한 799
 - 메모리 설정
 - 웹 응용 프로그램 컨테이너 서버 (WACS)에서 변경 466
 - 메트릭 540
 - 보기 383
 - 명령줄 옵션 780, 790, 793, 794
 - CMS 781
 - Report Application Server 787
 - SSL 161
 - 대시보드 분석 서버 794
 - 대시보드 서버 794
 - 모든 서버 780
 - 이벤트 서버 793
 - 입력 및 출력 파일 리포지토리 서버 791
 - 적응형 작업 서버 786
 - 처리 서버 784, 785
 - 캐시 서버 784, 785
 - 모니터링 537
 - 모니터링 데이터 범주 555
 - 모니터링 서버 542
- 모니터링 서비스 550
- 문제 해결 618
 - Kerberos 454
 - Kerberos 설정 283
 - LDAP 계정 247
 - 단일 로그온 242
 - 오류 메시지 666
 - 웹 응용 프로그램 컨테이너 서버 (WACS) 463
- ▢
 - 받은 파일함
 - 액세스 제어 104
 - 방화벽 147
 - WACS(웹 응용 프로그램 컨테이너 서버) 461
 - 구성 179
 - JD Edwards EnterpriseOne 통합 191
 - Oracle E-Business 통합 193
 - PeopleSoft Enterprise 통합 194
 - SAP 통합 190
 - Siebel 통합 196
 - 구성 시나리오 184
 - 디버깅 183, 184
 - 서버 통신, 및 169
 - 이름으로 서버 등록 400
 - 배포
 - BW 게시자 구성 요소 672
 - 버전 제어 41
 - 번역 관리 도구 63
 - SSL 167
 - 범주 106
 - 권한 798
 - 변수
 - UNIX 운영 체제 18
 - 노드 관리 스크립트 401
 - 설치 디렉터리 18, 401
 - 스크립트 디렉터리 18
 - 별칭
 - 관리 108
 - 만들기 109
 - 기존 사용자 109
 - 새 사용자 108
 - 비활성화 111
 - 사용자에 할당 110
 - 삭제 110
 - 보고서
 - 게시 681
 - 배치 모드로 685
 - 데이터 소스 업데이트 684
 - 보고서 개체
 - 권한 799
 - 만들기/수정 권한 381
- 보고서 변환 도구 61
 - SSL 168
- 보고서 뷰어 70
- 보고서 엔진 SDK 33
- 보고서 유지 관리 684
- 보고서 정보 동기화 683, 684
- 보기
 - CMS 클러스터 세부 정보 383
 - 보안 주체에 대한 권한 123
 - 시스템 메트릭 383
 - 웹 응용 프로그램 컨테이너 서버 (WACS) 메트릭 463
 - 현재 메트릭 383
- 보안 38, 321, 351, 670
 - BI 플랫폼 670
 - Guest 계정 제한 149
 - 관리 123
 - 권한 사용자 지정 351
 - 기본 패턴 670
 - 로그온 제한 148
 - 방화벽 147
 - 분산 144
 - 불법 로그온 시도 방지 148
 - 사용자 제한 149
 - 설정 가져오기 322
 - 설정 관리 326
 - 세션 추적 145
 - 암호 제한 148
 - 웹 브라우저에서 웹 서버로 146
 - 웹 서버 146
 - 웹 작업 감사 147
 - 유니버스 개체 807
 - 적용 325
 - 제한 사항 149
 - 처리 확장 149
 - 최상위 폴더 125
 - 쿼리 126, 127
 - 폴더 수준 670
 - 플러그 인 38, 213
 - 환경 보호 146
 - 활성 신뢰 관계 143
- 보안 네트워크 통신
 - BusinessObjects Enterprise 서버 297
 - CMC 설정 305
 - PSE 생성 302
 - SAP 구성 298
 - SAP 암호화 라이브러리 297
 - 멀티 패스 게시 307
 - 서버 구성 304
 - 서버 그룹 306
 - 워크플로 301
 - 클라이언트와 서버 비교 297
 - 환경 설정 302
- 보안 네트워크 통신(SNC), 통합
 - SNC에 대해 구성 307

보안 정의 편집기
전송 689, 694

보안 주체
고급 권한 할당 125
권한 보기 123
권한 할당 124
권한 확인 126, 127
권한, 최상위 폴더 125
보안 플러그 인 213, 285
LDAP 인증 231
Windows AD 인증 249

복사
액세스 수준 131
복원 476
시스템 기본값 391, 467

복제
개체 621
서버 370, 371
웹 응용 프로그램 컨테이너 서버
(WACS) 441
타사 사용자 및 그룹 633

복제 목록
관리 638
만들기 636, 637
수정 639
종속성 옵션 636, 637
지원되는 개체 635

복제 작업
구성 옵션 643
만들기 643
보기 643
수정 646
일정 645
부하 분산 144

CMS 추가 373
WACS(웹 응용 프로그램 컨테이너
서버) 460
및 분산 보안 144
클러스터링 372

분석 66
분의 수, 로그인 토큰 144
뷰 36
브라우저 기반 클라이언트 60
비즈니스 뷰 관리자 61
비활성화

Guest 계정 100
별칭 111
서버 367



사용자
고급 권한 할당 125
권한 801
권한 보기 123
권한 할당 124

사용자 (계속됨)
권한 확인 126, 127
권한, 최상위 폴더 125
매핑 316, 334, 340, 346
액세스 허용 103

사용자 계정
관리 89, 94
기본값 89
만들기 94
삭제 96
수정 96

사용자 별칭 110
만들기 109
기존 사용자 109
새 사용자 108
비활성화 111
삭제 110
할당 110

사용자 자격 증명, 노트에 대해 변경
423, 424

사이트
권한 관리 626, 627, 628, 629,
630
액세스 수준 134
삭제 429, 430

CMS 시스템 데이터베이스 429,
430
그룹 99
별칭 110
사용자 계정 96
서버 371
액세스 수준 132
웹 응용 프로그램 컨테이너 서버
(WACS) 442
유니버스 535
유니버스 연결 534

상속 115
권한 무시 118
그룹 116
무시 135
제한 120
폴더 117

상태, 서버 상태 보기 및 변경 362,
363
새로 고침 모드 옵션, 연합 631, 632
서버 30

BEx 웹 응용 프로그램 서비스 속
성
JCo 서버 RFC 대상 846
JCo 서버 게이트웨이 서비스
846
JCo 서버 게이트웨이 호스트
846
JCo 서버 연결 수 846
SAP BW 마스터 시스템 846
클라이언트 세션의 최대 수 846

서버 (계속됨)

bscLogin.conf 파일 위치 824
Crystal Reports Server 속성
Java VM 인수 837
Java 클래스 경로 837
Java 하위 VM 인수 837
단일 로그인(SSO) 만료 837
미리 보기 또는 새로 고침 시
데이터베이스 레코드 읽기
837
미리 시작한 자식의 최대 수
837

배치 크기 837
보고서 미리 보기 또는 새로 고
침 시 읽을 데이터베이스 레
코드의 수 837

보고서 작업을 닫을 때까지 보
고서 작업을 데이터베이스
에 연결된 상태로 유지 837
보안 캐시 제한 시간 837
뷰어를 새로 고칠 경우 항상 현
재 데이터 표시 837

유틸 연결 제한 시간 837
유틸 작업 제한 시간 837
임시 디렉터리 837
자식당 최대 수명 작업 837
찾을 데이터 크기 837
최대 동시 보고서 작업 수 837
최대 캐시 크기 837
캐시 파일 디렉터리 837
클라이언트 간에 보고서 데이
터 공유 837
클라이언트에 전달되는 가장
오래된 주문형 데이터 837

Dashboard Design 서버 속성
Java VM 인수 856
Java 하위 VM 인수 856
미리 보기 또는 새로 고침 시
데이터베이스 레코드 읽기
856
미리 시작한 자식의 최대 수
856

보고서 작업을 닫을 때까지 보
고서 작업을 데이터베이스
에 연결된 상태로 유지 856
보안 캐시 제한 시간(분) 856
유틸 연결 제한 시간 856
유틸 연결 제한 시간(분) 856
유틸 작업 제한 시간 856
자식당 최대 수명 작업 856
최대 동시 작업 856
최대 캐시 크기(KB) 856
클라이언트 간에 데이터 공유
856

서버 (계속됨)

Dashboard Design 서버 속성 (계속됨)
 클라이언트에 전달되는 가장 오래된 주문형 데이터(초) 856
 File Store 디렉터리 824
 HTTP 포트 824
 HTTPS 사용 824
 HTTPS 포트 824
 IP 주소 설정 394
 IPv6 주소 394
 Krb5.ini 파일 위치 824
 UNIX 신호 처리 781
 Web Intelligence 서버 설정
 메모리 상위 임계값 855
 메모리 최대 임계값 855
 메모리 하위 임계값 855
 Web Intelligence 서비스 속성
 HTTP URL 사용 허용 848
 PJS 서비스 Ping 실패 시 재시도 횟수 848
 PJS 서비스 모니터링 사용 848
 PJS 서비스 모니터링 스레드 기간 848
 값 목록 배치 크기 848
 값 목록 배치 크기(항목) 848
 값 목록 캐시 사용 848
 단일 로그인 만료 848
 메모리 분석 사용 848
 메모리 상위 임계값 848
 메모리 최대 임계값 848
 메모리 하위 임계값 848
 모니터링 사용 848
 모니터링 스레드 루프 지연(초) 848
 모니터링한 리소스 기본 바꾸기 제한 시간(초) 848
 모니터링한 리소스 기본 정리 제한 시간(초) 848
 문서 맵 최대 크기 오류 허용 848
 문서 캐시 사용 848
 문서 캐시 정리 간격 848
 사용자당 최대 문서 수 848
 서버 폴링 간격 848
 시각화 엔진 교체 제한 시간(초) 848
 시각화 엔진 정리 제한 시간(초) 848
 실시간 캐시 사용 848
 유니버스 캐시 최대 크기 848
 유틸 문서 제한 시간 848
 유틸 연결 제한 시간 848
 이미지 디렉터리 848
 이진 스트림 최대 크기 848

서버 (계속됨)

Web Intelligence 서비스 속성 (계속됨)
 재활용 전 제한 시간 848
 재활용 전 최대 문서 수 848
 최대 값 목록 크기 848
 최대 문서 캐시 감소 공간 848
 최대 문서 캐시 크기 848
 최대 문자 스트림 크기 848
 최대 사용자 지정 정렬 크기 848
 최대 연결 수 848
 출력 캐시 디렉터리 848
 캐시 공유 사용 안 함 848
 캐시 제한 시간 848
 캐시의 최대 문서 848
 프록시 값 848
 개인 키 액세스 암호 824
 구성 387
 구성 템플릿 388
 설정 389
 적용 390
 그룹 멤버 구성 수정 380
 그룹화 377
 기본 설정 391
 노드 19, 44
 다시 시작 363, 365
 다차원 분석 서비스 속성
 쿼리에 의해 반환되는 최대 셀 수 846
 클라이언트 세션의 최대 수 846
 필터링 시 반환되는 최대 멤버 수 846
 단일 로그인 만료 824
 데이터 연합 서비스 속성
 문 비활성 제한 시간 848
 실행 폴 크기 848
 연결 비활성 제한 시간 848
 최대 연결 848
 로그 수준 824
 명령줄 780
 모니터링 에이전트 URL 824
 모든 IP 주소에 바인딩 824
 목록 355
 변경 362
 상태 362, 363
 복제 370, 371
 비활성화 367, 368
 삭제 371
 상태 355, 362
 서버의 상태 보기 363
 서비스 계정 설정 253
 서비스 계정에 권한 부여 254, 255
 서비스 계정을 사용하도록 서버 구성 256
 서비스 시작 제한 시간 824

서버 (계속됨)

서비스와 비교 19, 44
 성능 설정 388
 속성 388
 시각화 엔진 교체 제한 시간(초) 824
 시각화 엔진 정리 제한 시간(초) 824
 시스템 데이터베이스 자동 다시 연결 824
 시작 363, 365, 366
 자동 363, 365
 액세스 380, 381
 연결 서버 속성
 HTTP 청크 사용 834
 HTTP 청크 크기 834
 네트워크 계층 834
 데이터 소스 활성화 834
 데이터베이스 834
 미들웨어 추적 사용 834
 연결 풀 제한 시간 834
 연결 풀링 834
 임시 개체 유틸 제한 시간 834
 임시 개체 타이머 간격 834
 작업 추적 사용 834
 요청된 시스템 데이터베이스 연결 824
 유틸 연결 제한 시간 824
 유틸 임시 개체 제한 시간 824
 이름 서버 포트 824
 이름으로 등록 400
 이벤트 폴 간격 824
 인증서 별칭 824
 인증서 신뢰 목록 개인 키 액세스 암호 824
 인증서 신뢰 목록 파일 위치 824
 인증서 저장 유형 824
 인증서 저장 파일 위치 824
 일반 서버 속성
 SIA가 시작되면 자동으로 이 서버 시작 821
 구성 템플릿 사용 821
 구성 템플릿 설정 821
 로그 수준 821
 시스템 기본값 복원 821
 요청 포트 821
 자동 할당 821
 호스트 식별자 821
 임시 디렉터리 824
 자리 표시자 370
 작업 로깅 384
 작업, 로깅 384
 정리 간격 824
 중지 363, 365
 최대 HTTP 머리글 크기 824
 최대 동시 요청 수 824

서버 (계속됨)

최대 동시 작업 824
 최대 시도 824
 최대 유휴 시간 824
 최대 자식 요청 수 824
 최대 파일 액세스 재시도 횟수 824
 추가 369
 클라이언트 인증 사용 824
 탐색 트리 355
 통신 169
 포트 824
 포트 오프셋 824
 표준 명령줄 옵션 780
 프로토콜 824
 프록시 포트 824
 프록시 호스트 이름 824
 프록시를 통한 HTTP 사용 824
 핵심 서비스 속성
 bscLogin.conf 파일 위치 824
 File Store 디렉터리 824
 HTTP 포트 824
 HTTPS 사용 824
 HTTPS 포트 824
 Krb5.ini 파일 위치 824
 개인 키 액세스 암호 824
 단일 로그인 만료 824
 로그 수준 824
 모니터링 에이전트 URL 824
 모든 IP 주소에 바인딩 824
 서비스 시작 제한 시간 824
 시작화 엔진 교체 제한 시간(초)
 824
 시작화 엔진 정리 제한 시간(초)
 824
 시스템 데이터베이스 자동 다
 시 연결 824
 요청된 시스템 데이터베이스
 연결 824
 유휴 연결 제한 시간 824
 유휴 임시 개체 제한 시간 824
 이름 서버 포트 824
 이벤트 폴 간격 824
 인증서 별칭 824
 인증서 신뢰 목록 개인 키 액세
 스 암호 824
 인증서 신뢰 목록 파일 위치
 824
 인증서 저장 유형 824
 인증서 저장 파일 위치 824
 임시 디렉터리 824
 정리 간격 824
 최대 HTTP 머릿글 크기 824
 최대 동시 요청 수 824
 최대 동시 작업 824
 최대 시도 824
 최대 유휴 시간 824

서버 (계속됨)

핵심 서비스 속성 (계속됨)
 최대 자식 요청 수 824
 최대 파일 액세스 재시도 횟수
 824
 클라이언트 인증 사용 824
 포트 824
 포트 오프셋 824
 프로토콜 824
 프록시 포트 824
 프록시 호스트 이름 824
 프록시를 통한 HTTP 사용 824
 호스트 이름 또는 IP 주소에 바
 인딩 824
 호스트 ID 옵션 393
 호스트 이름 394
 호스트 이름 또는 IP 주소에 바인
 딩 824
 활성화 367, 368
 서버 그룹
 노드 355
 만들기 378
 서버의 하위 그룹 377, 379
 액세스 380, 381
 하위 그룹 379
 서버 다시 시작 363, 365
 서버 메트릭 861
 Crystal Reports Server 메트릭
 MaxChildProcesses 878
 ObjectDllName 878
 개체 유형 878
 대기열에 있는 요청 수 878
 실패한 요청 수 878
 열려 있는 연결 수 878
 열려 있는 작업 878
 요청 실패율 878
 전송된 데이터(KB) 878
 처리된 요청 878
 최대 처리 시간(밀리초) 878
 최소 처리 시간(밀리초) 878
 캐시 적중률(%) 878
 캐시 크기 878
 평균 처리 시간(밀리초) 878
 현재 열려 있는 보고서 작업 878
 현재 열려 있는 연결 878
 Dashboard Design 서버 메트릭
 MaxChildProcesses 882
 ObjectDllName 882
 개체 유형 882
 대기열에 있는 요청 수 882
 실패한 요청 수 882
 열려 있는 연결 수 882
 열려 있는 작업 882
 열려 있는 작업 수 882
 요청 실패율 882
 전송된 데이터(KB) 882

서버 메트릭 (계속됨)

Dashboard Design 서버 메트릭 (계속됨)
 처리된 요청 수 882
 최대 처리 시간(밀리초) 882
 최소 처리 시간(밀리초) 882
 캐시 적중률(%) 882
 캐시 크기(KB) 882
 평균 처리 시간(밀리초) 882
 Web Intelligence 서버 메트릭
 CPU 사용량(%) 880
 가상 메모리 크기(MB) 880
 교체된 문서 수 880
 메모리 높은 임계값 수 880
 메모리 최대 임계값 수 880
 문서 교체 수 880
 문서 수 880
 사용자 수 880
 세션 제한 시간 수 880
 유휴 시간(초) 880
 총 CPU 시간(초) 880
 총 세션 수 880
 총 작업 수 880
 총 클라이언트 호출 수 880
 캐시 높은 표시 수 880
 캐시 크기(KB) 880
 캐시에 있는 오래된 문서 수 880
 현재 세션 수 880
 현재 작업 수 880
 현재 클라이언트 호출 수 880
 현재 활성 세션 수 880
 보기 383
 연결 서버 메트릭
 데이터 소스 868
 웹 응용 프로그램 컨테이너 서버 메트릭
 시작할 때 실패한 WACS 커넥터 875
 실행 중인 WACS 커넥터 목록 875
 이벤트 서버 메트릭
 모니터링한 파일 869
 모니터링한 파일 목록 869
 적응형 작업 서버 메트릭
 FTP 대상 기본 설정 유효 875
 PID 875
 동시 작업 수 875
 받은 작업 요청 875
 받은 파일함 대상 기본 설정 유효 875
 실패한 작업 작성 875
 예약 서비스 875
 임시 디렉터리 875
 자식 875
 전자 메일 대상 기본 설정 유효 875
 종료 875
 초기화 875
 최대 작업 875
 통신 오류 875
 파일 시스템 대상 기본 설정 유효 875
 허용되는 최대 동시 작업 875

서버 메트릭 (계속됨)	서버 메트릭 (계속됨)	서버 메트릭 (계속됨)
적응형 작업 서버 메트릭 (계속됨)	적응형 처리 서버 메트릭 (계속됨)	파일 리포지토리 서버 메트릭 (계속됨)
허용된 최대 작업 수 875	쿼리 실행에 의해 사용된 메모리의 전체 바이트 870	루트 디렉터리의 사용 가능한 디스크 공간(%) 869
적응형 처리 서버 메트릭	870	869
CPU 사용률(마지막 15분) 870	쿼리 실행에 의해 작성된 총 레코드 수 870	루트 디렉터리의 사용 가능한 디스크 공간 (GB) 869
CPU 사용률(마지막 5분) 870	쿼리 실행에서 작성된 전체 바이트 870	루트 디렉터리의 전체 디스크 공간(GB) 869
DSLServiceMetrics.activeConnectionCount 870	쿼리 최적화 단계의 쿼리 수 870	보낸 데이터(MB) 869
DSLServiceMetrics.activeOLAPConnectionsCount 870	큐브 개수 870	작성한 데이터(MB) 869
DSLServiceMetrics.activeSessionCount 870	중요 관리 서비스 메트릭	활성 연결 869
DSLServiceMetrics.queryCount 870	감사자 864	활성 파일 869
GC 동안 중단된 시스템 비율(마지막 15분) 870	CMS 시스템 DB의 개체 수 864	활성 파일 목록 869
GC 동안 중단된 시스템 비율(마지막 5분) 870	데이터베이스 마지막 업데이트 날짜 864	서버 메트릭 정보
GC 동안 페이지 오류 수(마지막 15분) 870	데이터베이스 사용자 이름 864	대기열의 현재 감사 이벤트 수 861
GC 동안 페이지 오류 수(마지막 5분) 870	데이터베이스 연결 설정 864	공통 메트릭
JVM 교착 상태 스레드 카운터 870	감사 데이터베이스 연결 이름 864	CPU 861
JVM 디버그 정보 870	감사 스레드 마지막 폴링 주기 기간(초) 864	CPU 유형 861
JVM 버전 정보 870	감사 스레드 사용률 864	PID 861
JVM 잠금 컨텐션 수 870	기존의 동시 사용자 계정 864	RAM(MB) 861
JVM 추적 플래그 870	기존의 명명된 사용자 계정 864	등록된 이름 861
감사 이벤트 수신 870	대기 중인 작업 864	디스크 크기(GB) 861
데이터 소스에서 전송된 전체 바이트 870	데이터베이스 소스 이름 864	로깅 디렉터리 861
데이터 소스에서 전송된 총 레코드 수 870	동시 사용자 라이선스 864	버전 861
데이터 연합 서비스를 사용할 수 있습니까? 870	동시 사용자가 설정한 세션 수 864	사용 중인 서버 스레드 861
디스크 사용 중인 쿼리 수 870	리소스 버전 864	사용된 디스크 공간(GB) 861
로드된 커넥터 수 870	명명된 사용자 라이선스 864	요청 포트 861
로드된 커넥터에 대한 활성 연결 수 870	명명된 사용자가 설정한 세션 수 864	운영 체제 861
리소스 대기 중인 쿼리 수 870	모든 사용자가 설정한 세션 수 864	이름 서버 861
마지막 인덱스 업데이트 타임스탬프 870	보류 중인 시스템 데이터베이스 요청 864	컴퓨터 이름 861
마지막 콘텐츠 저장소 생성 타임스탬프 870	보류 중인 작업 864	현재 시간 861
메모리 사용 중인 쿼리 수 870	빌드 날짜 864	호스트 IP 주소 861
메타데이터 캐시에 의해 사용된 메모리의 바이트 870	빌드 번호 864	호스트 이름 861
사용 가능한 메모리(MB) 870	서버에 설정된 세션 수 864	상태 355
사용 가능한 서비스 870	설정된 시스템 데이터베이스 연결 864	배경 설정
사용 가능한 프로세서 870	시스템 데이터베이스 사용자 이름 864	ccm.sh
서비스 870	시스템 데이터베이스 서버 이름 864	서버 설정 백업 472
서비스 시작 이후 성공한 추출 시도 횟수 870	시스템 데이터베이스 연결 이름 864	백업 471, 472, 473
서비스 시작 이후 실패한 추출 시도 횟수 870	시작 이후 가장 긴 커밋 응답 시간(밀리초) 864	복원 476, 477, 478
세션 개수 870	시작 이후 가장 긴 쿼리 응답 시간(밀리초) 864	구성 821
실패한 쿼리 수 870	시작 이후 로그인 수 864	서버 유형 54, 57
실행 중인 인덱싱 870	시작 이후 사용자 세션 최대 수 864	서버 자리 표시자 885
실행 중인 쿼리 수 870	시작 이후 커밋 수 864	서버 중속성
연결 수 870	시작 이후 쿼리 수 864	원격 프로시저 호출 423
인덱싱된 문서 수 870	시작 이후 평균 커밋 응답 시간(밀리초) 864	이벤트 로그 423
전송 레이아웃 스레드 풀 크기 870	시작 이후 평균 쿼리 응답 시간(밀리초) 864	구성 템플릿 388
전송 레이아웃의 스레드 870	실패한 작업 864	서버와 비교 19, 44
전체 GC 수 870	실행 중인 작업 864	서비스 계정
전체 메모리(MB) 870	완료된 작업 864	서버 구성 256
최대 메모리(MB) 870	제품 버전 864	설정 253
쿼리 개수 870	클러스터 CMS 서버 864	설정 253
쿼리 분석 단계의 쿼리 수 870	현재 사용된 시스템 데이터베이스 연결 864	서비스 계정 권한 254
쿼리 실행 단계의 쿼리 수 870	파일 리포지토리 서버 메트릭	루트 디렉터리의 빈 디스크 공간(GB) 869
쿼리 실행에 의해 사용된 디스크의 전체 바이트 870	루트 디렉터리의 빈 디스크 공간(GB) 869	

서비스 범주 51, 355
 신호도, SSL(Secure Sockets Layer)
 144
 설정
 BI 실행 패드 503
 경고 505
 최상위 폴더 권한 125
 토론 500
 설치
 Windows에서 SAP 게이트웨이
 674
 기본 보안 수준 670
 설치 디렉터리, 위치 401
 성능 537
 부하 분산 144
 클러스터 372
 성능 권장 사항 733
 세션 145
 추적 145
 세션 변수 145
 인증 212
 소유자 권한 140
 소켓 제한 시간 662
 소프트웨어 개발 키트(SDK)
 Crystal Reports Viewer SDK 33
 Report Application Server SDK
 33
 SAP BusinessObjects Business
 Intelligence 플랫폼 SDK 33
 SAP BusinessObjects Business
 Intelligence 플랫폼 소비자
 SDK 33
 보고서 엔진 SDK 33
 수명 주기 관리
 BIAR 엔진 명령줄 도구 487
 스크립트 매개 변수, 노드
 다시 만들기 418
 삭제 418
 이동 420
 추가 418
 스크립트, UNIX 767
 스크립트, Windows 776
 시스템 계정 285
 시스템 메트릭, 보기 383
 웹 응용 프로그램 컨테이너 서버
 (WACS) 463
 신뢰 전송 144
 신뢰, 활성 신뢰 관계 143
 신뢰할 수 있는 인증 219, 525
 SAML 221
 사용자 이름 229
 샘플 구성 226
 속성 222
 신호 처리 781
 신호등 537
 실행 모드 321

○

아키텍처 27, 539
 플랫폼 검색 599
 아키텍처 다이어그램 28
 알람 539
 알람 전달 540
 암호 427, 428
 변경 102
 CMS 데이터베이스 427
 옵션 102, 218
 제한 사항 148
 암호화 담당자 156
 멤버 추가 156
 암호화 키 153
 CMC 157
 개체 목록 159
 상태 158
 새로 만들기 159
 손상됨으로 표시 159
 해지 160
 액세스 113
 BI 실행 패드 494
 CMC 494
 HTML 쿼리 패널 504
 그룹 103
 받은 파일함 104
 사용자 103
 서버 380, 381
 서버 그룹 380, 381
 유니버스 연결 533
 응용 프로그램 494
 액세스 수준 114, 122, 137
 RAS 381
 개체와의 관계 134
 관리 137
 권한 802
 권한 수정 133
 만들기 131
 미리 정의 128
 보기 123
 보기와 요청 시 보기 130
 보안 주체에 할당 124
 복사 131
 사이트 간 관리 134
 삭제 132
 이름 바꾸기 132
 작업, 필요한 권한 128
 액세스 제어 목록
 보기 123
 보안 주체 추가 124
 양방향 복제 631
 언어 37
 업그레이드 42
 업그레이드 관리 도구 23, 66
 에이전트 작성기 555

역방향 프록시 구성 604
 역방향 프록시 서버
 Apache 2.2 구성 200
 BI 플랫폼과 함께 구성 199, 200
 BI 플랫폼과 함께 배포 198, 199
 ISA 2006 구성 202
 Live Office 209
 Tomcat 204
 WebSEAL 6.0 구성 201
 뷰어 URL 209
 세션 쿠키 206
 웹 서비스 204, 205
 웹 응용 프로그램 컨테이너 서버
 (WACS)와 함께 배포 460
 웹 응용 프로그램 컨테이너 서버
 (WACS)와 함께 사용 461
 지원됨 198
 특수 구성 203
 역할 316, 334, 340, 346, 676
 가져오기 293
 관리용으로 만들기 676
 권한 할당 351
 다시 매핑 342
 매핑 293, 316, 319, 334, 336,
 340, 346
 매핑 해제 319, 350
 역할 매핑 293, 316, 334, 340, 346
 역할 매핑 해제 319, 350
 연결 558
 연결 서버 542
 연결 서버 32 542
 연합 621
 개체 정리 647, 648, 649
 단방향 복제 631, 632
 대상 사이트 다시 가리키기 659,
 661
 대상에서 새로 고침 631, 632
 대용량 개체 복제 662
 로그 보기 646
 로컬로 인스턴스 실행 656, 658
 모범 사례 662
 문제 해결 666
 보안 관리 626, 627, 628, 629,
 630
 복제 모드 631, 632
 복제 목록 635
 관리 638
 만들기 636, 637
 폴더 636, 637
 복제 작업 643
 만들기 643
 수정 645, 646
 일정 645
 복제된 콘텐츠 가져오기 및 수준
 올리기 661

연합 (계속됨)

- 복제된 콘텐츠 가져오기 및 승격 659, 660
- 성능 향상 665
- 액세스 수준 134
- 양방향 복제 631, 632
- 용어 622
- 원격 연결 640
 - 만들기 640, 641
 - 수정 642
- 원격 예약 656, 658
- 원본에서 새로 고침 631, 632
- 웹 서비스 654, 655
- 장점 621
- 충돌 관리 649, 650, 651
- 타사 사용자 및 그룹, 복제 633

영구 데이터 42

요구 사항

- 클러스터링 372

워크플로 72

- Analysis 작업 영역 표시 81
- Crystal 보고서 실행 76
- Crystal 보고서 예약 74, 75
- SIA 시작 73
- SIA 종료 74
- 고급 권한, 할당 125
- 권한 보기 123
- 대상으로 인스턴스 전송 78
- 사용자 로그인 72
- 액세스 제어 목록, 보안 주체 할당 124
- 예약된 Web Intelligence 문서 76, 77
- 예약된 개체 78
- 요청 시 Crystal 보고서 보기 82
- 요청 시 Web Intelligence 보고서 표시 82
- 웹 Java로 Crystal 보고서 보기 83
- 최상위 폴더 권한 설정 125
- 캐시되지 않은 Crystal 보고서 보기 79
- 캐시된 Crystal 보고서 보기 80

원격 연결

- 만들기 640, 641
- 보기 640
- 보안 642
- 수정 642
- 폴더 만들기 640

원격 예약 656, 658

원격 프로시저 호출 423

원본 사이트

- 액세스 수준 134

웹 서버

- 보안 146

웹 서비스 34

- 사용자 지정 배포 654, 655

웹 서비스 (계속됨)

- 세션 변수 654
- 역방향 프록시 서버에 대한 구성 203, 204, 205
- 웹 서비스 쿼리 도구 35
- 웹 응용 프로그램 컨테이너 서버에 추가 442
- 웹 응용 프로그램 컨테이너 서버에서 제거 443
- 파일 캐싱 654, 655
- 웹 서비스 쿼리 도구 35, 62
- 웹 응용 프로그램 서버 31
- 소프트웨어 개발 키트(SDK) 33
- 인증 212
- 웹 응용 프로그램 컨테이너 서버 (WACS) 32, 542, 824
- AD Kerberos 453
- CMC 서비스 435
- HTTPS 444, 446, 461
- SSL 444, 446
- 개요 435
- 다중 홈 컴퓨터 462
- 메모리 설정 변경 466
- 메트릭 875
- 문제 해결 463
- 복제 441
- 삭제 442
- 새 서버 만들기 440
- 설치 439
- 시스템 기본값 복원 467
- 시스템 메트릭 463
- 웹 서비스 제거 443
- 웹 서비스 추가 442
- 제거 439
- 추가 439
- 커넥터 435
- 포트 충돌 해결 464, 465
- 프록시 서버로 사용 460
- 프록시 서버와 함께 사용 460, 461

웹 클라이언트 60

위반 시간 540

위임된 관리 137

위젯

- 권한 816
- 설정 관리 508
- 유니버스 36
- 관리 534
- 권한(.unv) 804
- 권한(.unx) 805
- 복제 634

유니버스 개체 보안 807

유니버스 디자인 도구 62

유니버스 디자인 도구, 권한 815

유니버스 연결

- 관리 534
- 권한 808

유니버스 연결 (계속됨)

- 복제 634
- 삭제 534
- 유형별 권한 121
- BI 실행 패드 810
- CMC 810
- Crystal 보고서 799
- Web Intelligence 812
- Web Intelligence 문서 800
- 경고 817
- 그룹 801
- 메모 799
- 범주 798
- 사용자 801
- 액세스 수준 802
- 위젯 816
- 유니버스 디자인 도구 815
- 유니버스 연결 808
- 유니버스(.unv) 804
- 유니버스(.unx) 805
- 전략 작성기 814
- 정보 디자인 도구 816
- 폴더 797
- 유효한 권한 122
- 응답 시간 537
- 응답 파일 323
- 만들기 323
- 적용 325
- 응용 프로그램 493
- 속성 509, 604
- 플랫폼 검색 509, 604
- 응용 프로그램 계층 387
- 응용 프로그램 관리 493
- BOE war 파일 514
- 토론 스레드, 삭제 503
- 이름 바꾸기, 액세스 수준 132
- 이벤트 로그 384, 423
- 이벤트 서버 542, 824
- 명령줄 옵션 793
- 익명 단일 로그인 214
- 인덱싱 599
- 인덱싱 오류 목록 617
- 인스턴스 공유 656, 658
- 인증 38
- BI 플랫폼 내 권한 670
- LDAP 230, 231
- SAP 데이터 액세스용 703
- WACS(웹 응용 프로그램 컨테이너 서버) 448
- Windows AD 248
- 기본 212
- 보안 플러그 인 213
- 신뢰할 수 있는 인증 219
- 엔터프라이즈 216
- 유형 92
- 적용 703

인증 (계속됨)
 정보 플랫폼 서비스용 285
 콘텐츠 관리 워크벤치 676
 인증서 신뢰 목록 445
 인증서 파일 162, 444
 인코딩, 로그인 토큰 144
 인텔리전스 계층 387
 입력 파일 리포지토리 19, 44, 542, 824

ㅈ

자동 시작 서버 366
 자리 표시자 885
 계층 764
 재해 복구 계획 141
 저장된 데이터 130
 적응 처리 서버 19, 44, 542, 824
 적응형 작업 서버 19, 44, 824, 875
 명령줄 옵션 786
 소켓 제한 시간 662
 전략 작성기, 권한 814
 전송 689, 690
 Content Administration 워크벤치 696
 InfoSet 연결 689, 693
 Open SQL 연결 691
 가져오기 690
 개요 687
 개체 687
 매개 변수 사용자 설정 689, 699
 보안 정의 편집기 689
 충돌 검사 690
 클러스터 정의 689, 695
 테이블 687
 프로그램 687
 함수 그룹 687
 행 수준 보안 정의 694
 전역 시스템 메트릭 383
 정보 디자인 도구 63
 정보 디자인 도구, 권한 816
 정보 플랫폼 서비스
 게시 권한 352
 계정 만들기 285
 관리 권한 351
 역할 매핑 316, 334, 346
 제안 613
 제한 149
 Guest 계정 149
 권한의 범위 120
 로그온 148
 사용자 149
 암호 148
 중단 간 단일 로그인 215
 중단 간 추적 766

주기 관리 콘솔
 BIAR 명령줄 도구 483
 BIAR 엔진 명령줄 도구 485, 491
 주기 관리(LCM) 41
 중앙 관리 서버 19, 44
 중앙 관리 서버CMS 참조 285
 중앙 관리 콘솔(CMC) 22, 69
 중앙 구성 관리자(CCM) 22, 65
 지역화 37

ㅊ

처리 계층 387
 처리 서버
 Web Intelligence 790
 명령줄 옵션 784, 785
 처리 확장 149
 공유 500
 등록 498
 최상위
 폴더, 권한 125
 추가 372
 CMS 373
 그룹에 사용자 추가 100
 서버 369
 클러스터 멤버 372
 하위 그룹 98
 추적 743
 서버 744
 .ini 파일 구성 746
 종단 간 766
 추적 로그
 수준 495, 743
 추적 로그 수준
 CMC 서버 설정 745
 추적, 세션 145
 출력 파일 리포지토리 19, 44, 542, 824

ㅋ

캐시 서버 784, 785
 콘텐츠 관리 워크벤치 679
 BI 플랫폼 시스템 추가 679
 백그라운드에서 보고서 게시 683
 보고서 게시 681
 보고서 게시의 개요 675
 보고서 삭제 685
 보고서 정보 동기화 683, 684
 보고서의 데이터 소스 업데이트 684
 사용자 액세스 수준 정의 676
 인증 적용 676
 쿠키 145
 로그온 토큰 144
 세션 추적 145

쿼리
 보안 126, 127
 클라이언트
 Data Federator:데이터 연합 관리 도구 참조 64
 SAP BusinessObjects Analysis, Microsoft Office용 에디션 66
 SAP BusinessObjects Business Intelligence 플랫폼용 위젯 64
 SAP BusinessObjects Dashboard Design 67
 SAP Crystal Reports 67
 Web Intelligence Desktop 61
 데스크톱 60
 데이터 연합 관리 도구 64
 번역 관리 도구 63
 보고서 변환 도구 61
 비즈니스 뷰 관리자 61
 웹 60
 웹 서비스 쿼리 도구 62
 유니버스 디자인 도구 62
 정보 디자이너:정보 디자인 도구 참조 63
 정보 디자인 도구 63
 클라이언트, 데스크톱
 리포지토리 진단 도구 23, 66
 업그레이드 관리 도구 23, 66
 중앙 구성 관리자(CCM) 22, 65
 클라이언트, 브라우저 기반 68
 Analysis, OLAP 에디션 71
 BI 실행 패드 69
 BI 작업 영역 69
 SAP BusinessObjects Mobile 71
 SAP BusinessObjects Web Intelligence 71
 보고서 뷰어 70
 중앙 관리 콘솔(CMC) 22, 69
 클러스터 372, 374
 CMS 추가 373
 노드 372
 세부 정보 보기 383
 이름 변경 376
 클러스터 정의 도구 689, 695
 클러스터 정의 전송 689, 695
 클러스터 지원 542, 601
 클러스터 키 153
 dbinfo 파일 153
 UNIX에서 재설정 155
 Windows에서 재설정 154
 개요 153
 키 파일 162

ㅌ

타사 그룹, 복제 633
 타사 보안 플러그 인 213

타사 사용자, 복제 633
탐색 트리
 서버 355

토론

 설정 관리 500

토론 스레드 501

 검색 501

 검색 결과 정렬 502

 검색 취소 501

통계, 웹 작업 감사 147

통신 212

 BI 플랫폼 서버 간 169

 브라우저와 웹 응용 프로그램 서버
 간 212

통합

 SAP 40

 SNC 307

트렌딩 그래프 537

트렌딩 데이터베이스 539

특성, 로그온 토큰 144

특정 권한

 BI 작업 영역 803, 811

티켓 144

 로그온 토큰 144

 분산 보안 144

ㅍ

파일 리포지토리 서버 19, 44, 824

 명령줄 옵션 791

 백업 470

 복원 474, 475

파일 시스템

 백업 470

 복원 479

패킷 612

포트 번호

 변경 397, 398, 399

 웹 응용 프로그램 컨테이너 서버
 (WACS) 464

 충돌 465

폴더

 개체 권한

 상속 117

 권한 797

폴더 상속 117

 권한 무시 118

프로그램 개체

 인증 497

 활성화, 비활성화 497, 498

프로브 537, 540

프로필 매개 변수 307

플랫폼 검색 509, 604

플러그 인,

 보안 38

플러그 인, 보안 213

ㅎ

하위 그룹, 추가 98

행 수준 보안, 처리 확장 149

현재 계정 보기 86, 360

호스트

 LDAP 구성 233, 237

확장, 처리 149

활성 신뢰 관계 143

활성화

 서버 367, 368

