



Руководство администратора платформы Business Intelligence

- SAP BusinessObjects Business Intelligence platform 4.0 Support Package 2

2011-05-06

© 2011 SAP AG. Все права защищены. SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign и другие упомянутые здесь продукты и услуги SAP, а также соответствующие им логотипы являются торговыми марками или зарегистрированными торговыми марками SAP AG в Германии и других странах. Business Objects и логотип Business Objects, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius и другие продукты упомянутые здесь продукты и услуги Business Objects, а также соответствующие им логотипы являются торговыми марками или зарегистрированными торговыми марками Business Objects S.A. в США и других странах. Business Objects является компанией SAP. Все другие указанные продукты и услуги являются торговыми марками соответствующих компаний. Данные, содержащиеся в этом документе, предназначены только для информационных целей. Характеристики продуктов, поставляемых в разные страны, могут изменяться. Эти материалы могут быть изменены без предварительного уведомления. Материалы предоставлены компанией SAP AG и ее дочерними компаниями ("SAP Group") исключительно в информационных целях, без представления гарантии любого вида. SAP Group не несет ответственности за ошибки или пропуски в настоящих материалах. Все гарантии по продуктам и услугам SAP Group оговариваются в специальных гарантийных документах, которые прилагаются к соответствующим продуктам и услугам, имеющим гарантию. Ничто изложенное в данном документе не должно трактоваться как предоставление дополнительных гарантий

2011-05-06

Содержание

Глава 1	Начало работы.....	17
1.1	О справке.....	17
1.1.1	Для кого предназначена данная справка?.....	17
1.1.2	Платформа SAP BusinessObjects Business Intelligence	17
1.1.3	Переменные.....	18
1.2	Начало работы.....	18
1.2.1	Основные понятия.....	19
1.2.2	Основные инструменты администрирования.....	21
1.2.3	Ключевые задачи.....	22
Глава 2	Архитектура.....	25
2.1	Обзорная информация по архитектуре.....	25
2.1.1	Обзор системы.....	26
2.1.2	Базы данных.....	27
2.1.3	Серверы.....	28
2.1.4	Серверы веб-приложений.....	29
2.1.5	Software Development Kit.....	31
2.1.6	Источники данных.....	34
2.1.7	Языковая поддержка.....	35
2.1.8	Аутентификация и единый вход.....	36
2.1.9	Интеграция SAP.....	38
2.1.10	Управление жизненным циклом (LCM).....	40
2.1.11	Интегрированное управление версиями.....	40
2.1.12	постоянные данные.....	40
2.1.13	Путь обновления.....	41
2.2	Концептуальные ярусы.....	41
2.3	Службы и серверы.....	42
2.3.1	Службы.....	44
2.3.2	Категории служб.....	52
2.3.3	Типы серверов.....	56
2.3.4	Серверы.....	59
2.4	Клиентские приложения.....	62

2.4.1	Устанавливается вместе со средствами клиента платформы SAP BusinessObjects Business Intelligence.....	63
2.4.2	Устанавливается вместе с платформой SAP BusinessObjects Business Intelligence.....	68
2.4.3	Доступно отдельно.....	69
2.4.4	Клиенты веб-приложений.....	71
2.5	Потоки информации.....	75
2.5.1	Аутентификация.....	75
2.5.2	Планирование.....	77
2.5.3	Просмотр.....	82
2.5.4	По требованию.....	84
Глава 3	Управление лицензиями.....	89
3.1	Управление лицензионными ключами.....	89
3.1.1	Просмотр сведений лицензии.....	89
3.1.2	Для добавления ключа лицензии.....	90
3.1.3	Для просмотра текущей деятельности учетной записи.....	90
3.2	Измерение показателей использования лицензий.....	90
3.2.1	Проведение аудита лицензий.....	91
Глава 4	Управление пользователями и группами.....	93
4.1	Обзор управления учетными записями.....	93
4.1.1	Управление пользователями.....	93
4.1.2	Управление группами.....	95
4.1.3	Доступные типы аутентификации	96
4.2	Управление Enterprise и общими учетными записями.....	98
4.2.1	Создание учетной записи пользователя.....	98
4.2.2	Для изменения учетной записи пользователя.....	100
4.2.3	Чтобы удалить учетную запись пользователя.....	100
4.2.4	Чтобы создать новую группу.....	101
4.2.5	Для изменения свойств группы.....	101
4.2.6	Просмотр членов групп.....	102
4.2.7	Чтобы добавить подгруппы.....	102
4.2.8	Задание принадлежности к группе.....	103
4.2.9	Удаление группы.....	103
4.2.10	Чтобы включить учетную запись Гостя.....	104
4.2.11	Добавление пользователей в группы.....	104
4.2.12	Изменение настроек пароля.....	106
4.2.13	Предоставление доступа пользователям и группам.....	107
4.2.14	Управление доступом к каталогам "Входящие" пользователей.....	108
4.2.15	Настройка параметров стартовой панели BI.....	108

4.3	Управление псевдонимами.....	112
4.3.1	Чтобы создать пользователя и добавить сторонний псевдоним.....	113
4.3.2	Для создания нового псевдонима существующего пользователя.....	113
4.3.3	Для присвоения псевдонима пользователю.....	114
4.3.4	Для удаления псевдонима.....	115
4.3.5	Для отключения псевдонима.....	115

Глава 5 Установка прав.....117

5.1	Права на платформе BI.....	117
5.1.1	Уровни доступа.....	118
5.1.2	Параметры расширенных прав.....	118
5.1.3	Наследование.....	119
5.1.4	Права для конкретных типов объектов.....	125
5.1.5	Определение эффективных прав.....	126
5.2	Управление настройками безопасности для объектов в СМС.....	127
5.2.1	Для просмотра прав принципала на объект.....	127
5.2.2	Для назначения принципалов списку управления доступом к объекту.....	128
5.2.3	Для изменения безопасности объекта для принципала.....	129
5.2.4	Настройка прав на папку верхнего уровня в платформе BI.....	129
5.2.5	Проверка настроек безопасности для принципала.....	130
5.3	Работа с уровнями доступа.....	133
5.3.1	Выбор между уровнями доступа Просмотр и Просмотр по требованию.....	135
5.3.2	Чтобы скопировать существующий уровень доступа.....	136
5.3.3	Создание уровня доступа.....	137
5.3.4	Переименование уровня доступа.....	137
5.3.5	Для удаления уровня доступа.....	137
5.3.6	Чтобы изменить права в уровне доступа.....	138
5.3.7	Трассировка связи между уровнями доступа и объектами.....	139
5.3.8	Управление уровнями доступа по сайтам.....	139
5.4	Отключение наследования.....	140
5.4.1	Отключение наследования.....	142
5.5	Использование прав передачи административных полномочий.....	142
5.5.1	Выбор параметров Изменить права пользователей на объекты.....	144
5.5.2	Права владельца.....	146
5.6	Сводка рекомендаций по управлению правами.....	146

Глава 6 Обеспечение безопасности платформы BI.....149

6.1	Обзор вопросов безопасности	149
6.2	Планирование аварийного восстановления.....	149
6.3	Общие рекомендации по обеспечению безопасности развертывания.....	150

6.4	Настройка безопасности для связанных серверов сторонних производителей.....	151
6.5	Активные доверительные отношения.....	151
6.5.1	Маркеры входа.....	152
6.5.2	Механизм билетов для распределенной безопасности.....	152
6.6	Сеансы и отслеживание сеансов.....	153
6.6.1	Отслеживание сеансов центральным сервером управления.....	154
6.7	Защита среды.....	154
6.7.1	Веб-браузер с веб-сервером.....	154
6.7.2	Веб-сервер – платформа BI.....	155
6.8	Аудит изменений параметров безопасности	155
6.9	Аудит действий через Интернет.....	155
6.9.1	Защита от попыток выполнения входа злоумышленником.....	156
6.9.2	Ограничения для пароля.....	156
6.9.3	Ограничения на вход.....	156
6.9.4	Ограничения для пользователя.....	157
6.9.5	Ограничения учетной записи гостя.....	157
6.10	Расширения обработки.....	157
6.11	Обзор безопасности данных платформы BI.....	158
6.11.1	Защищенные режимы обработки данных.....	158
6.12	Криптография в платформе BI.....	161
6.12.1	Работа с ключами кластера.....	162
6.12.2	Специалисты по шифрованию.....	164
6.12.3	Управление криптографическими ключами с помощью CMC.....	165
6.13	Настройка серверов для SSL.....	171
6.13.1	Создание файлов ключа и сертификата.....	171
6.13.2	Настройка протокола SSL.....	174
6.14	Основные сведения об обмене данными между компонентами платформы BI.....	179
6.14.1	Обзор серверов платформы BI и портов обмена данными.....	179
6.14.2	Взаимодействие между компонентами платформы BI	182
6.15	Настройка платформы BI для брандмауэров.....	190
6.15.1	Настройка системы для использования брандмауэров.....	190
6.15.2	Отладка развертывания брандмауэра.....	194
6.16	Примеры типовых сценариев развертывания брандмауэров.....	195
6.16.1	Пример: уровень приложений развернут в отдельной сети.....	196
6.16.2	Пример: толстый клиент и уровень БД отделены брандмауэром от платформы BI	198
6.17	Настройки брандмауэра для интегрированных сред.....	201
6.17.1	Рекомендации по настройке брандмауэра для интеграции SAP.....	201
6.17.2	Настройка брандмауэра для интеграции с JD Edwards EnterpriseOne.....	203
6.17.3	Конкретные рекомендации по настройке брандмауэра для Oracle EBS.....	205
6.17.4	Настройка брандмауэра для интеграции с PeopleSoft Enterprise	206
6.17.5	Настройка брандмауэра для интеграции с Siebel.....	208

6.18	Платформа BI и обратные прокси-серверы	210
6.18.1	Поддерживаемые обратные прокси-серверы	210
6.18.2	Понимание механизма развертывания веб-приложений	210
6.19	Настройка обратных прокси-серверов для веб-приложений платформы BI	211
6.19.1	Подробные инструкции по настройке обратных прокси-серверов.....	211
6.19.2	Настройка обратного прокси-сервера.....	212
6.19.3	Настройка обратного прокси-сервера Apache 2.2 для платформы BI	212
6.19.4	Настройка обратного прокси-сервера WebSEAL 6.0 для платформы BI	213
6.19.5	Настройка Microsoft ISA 2006 для платформы BI	214
6.20	Специальная настройка для платформы BI при развертывании с обратным прокси-сервером	216
6.20.1	Включение обратного прокси-сервера для веб-служб	216
6.20.2	Включение пути к корневому каталогу для файлов cookie сеанса для ISA 2006.....	218
6.20.3	Включение обратного прокси-сервера для приложения SAP BusinessObjects Live Office.....	221
Глава 7	Аутентификация.....	223
7.1	Параметры аутентификации платформы BI.....	223
7.1.1	Основная аутентификация.....	224
7.1.2	Подключаемые модули безопасности.....	225
7.1.3	Единый вход на платформу BI.....	226
7.2	Аутентификация Enterprise.....	228
7.2.1	Общая информация об аутентификации Enterprise.....	228
7.2.2	Настройки аутентификации Enterprise.....	229
7.2.3	Изменение параметров Enterprise.....	230
7.2.4	Включение доверительной аутентификации.....	232
7.2.5	Настройка доверительной аутентификации для веб-приложения.....	234
7.3	Аутентификация LDAP.....	244
7.3.1	Использование аутентификации LDAP.....	244
7.3.2	Настройка аутентификации LDAP.....	246
7.3.3	Сопоставление групп LDAP.....	257
7.4	Аутентификация Windows AD.....	262
7.4.1	Обзор.....	262
7.4.2	Подготовка для аутентификации AD (Kerberos).....	266
7.4.3	Аутентификация AD с функцией единого входа.....	277
7.4.4	Сопоставление групп AD и настройка аутентификации AD.....	288
7.4.5	Устранение неполадок с аутентификацией Windows AD.....	293
7.5	Аутентификация SAP.....	295
7.5.1	Настройка аутентификации SAP	295
7.5.2	Создание учетной записи пользователя для платформы BI.....	296
7.5.3	Подключение к системам контроля полномочий SAP.....	298
7.5.4	Настройка параметров аутентификации SAP.....	300

7.5.5	Импорт ролей SAP.....	305
7.5.6	Настройка защищенного сетевого соединения (SNC).....	310
7.5.7	Настройка единого входа в систему SAP.....	323
7.5.8	Настройка единого входа для SAP Crystal Reports и SAP Netweaver.....	327
7.6	Аутентификация PeopleSoft.....	328
7.6.1	Обзор.....	328
7.6.2	Включение аутентификации PeopleSoft Enterprise.....	328
7.6.3	Сопоставление ролей PeopleSoft в платформе BI.....	329
7.6.4	Планирование пользовательских обновлений.....	333
7.6.5	Использование моста безопасности PeopleSoft.....	335
7.7	Аутентификация JD Edwards.....	346
7.7.1	Обзор.....	346
7.7.2	Включение аутентификации JD Edwards EnterpriseOne.....	346
7.7.3	Сопоставление ролей JD Edwards EnterpriseOne в платформе BI.....	347
7.7.4	Планирование пользовательских обновлений.....	351
7.8	Аутентификация Siebel.....	353
7.8.1	Включение аутентификации Siebel.....	353
7.8.2	Сопоставление ролей платформе BI.....	353
7.8.3	Планирование пользовательских обновлений.....	357
7.9	Аутентификация Oracle EBS.....	359
7.9.1	Разрешение аутентификации Oracle EBS.....	359
7.9.2	Сопоставление ролей Oracle E-Business Suite с платформой BI.....	360
7.9.3	Неотображаемые роли	365
7.9.4	Настройка прав для назначенных групп и пользователей Oracle EBS	366
7.9.5	Настройка единого входа (SSO) для SAP Crystal Reports и Oracle EBS.....	367
Глава 8	Администрирование сервера.....	369
8.1	Администрирование сервера.....	369
8.1.1	Работа с областью управления СМС "Серверы".....	369
8.1.2	Управление серверами с помощью скриптов в Windows	373
8.1.3	Управление серверами в UNIX	373
8.1.4	Управление лицензионными ключами.....	374
8.1.5	Измерение показателей использования лицензий.....	375
8.1.6	Просмотр и изменение статуса сервера.....	377
8.1.7	Добавление, клонирование и удаление серверов.....	382
8.1.8	Кластеризация центральных серверов управления (CMS).....	385
8.1.9	Управление группами серверов.....	390
8.1.10	Оценка производительности системы.....	394
8.1.11	Конфигурация настроек серверов.....	399
8.1.12	Настройка сетевых параметров сервера.....	403
8.1.13	Управление узлами.....	412

8.1.14	Переименование компьютера в разворачивании платформы SAP BusinessObjects Business Intelligence.....	434
8.1.15	Использование 32-битных и 64-битных библиотек сторонних разработчиков с платформой SAP BusinessObjects Business Intelligence.....	435
8.1.16	Управление заполнителями сервера и узла	436
Глава 9	Управление базами данных центрального сервера управления (CMS).....	437
9.1	Управление подключением к системной базе данных центрального сервера управления.....	437
9.2	Выбор новой или существующей базы данных центрального сервера управления.....	437
9.2.1	Выбор новой или существующей базы данных CMS в Windows.....	438
9.2.2	Выбор новой или существующей базы данных центрального сервера управления в UNIX.....	438
9.3	Повторное создание базы данных системы центрального сервера управления.....	439
9.3.1	Восстановление системной базы данных CMS в ОС Windows.....	440
9.3.2	Восстановление системной базы данных CMS в ОС UNIX.....	441
9.4	Копирование данных из одной базы данных CMS в другую.....	441
9.4.1	Подготовка к копированию системной базы данных CMS.....	442
9.4.2	Копирование системной базы данных CMS в Windows.....	443
9.4.3	Для копирования данных из базы данных системы центрального сервера управления на UNIX.....	443
Глава 10	Управление серверами контейнера веб-приложений (WACS).....	445
10.1	WACS.....	445
10.1.1	Сервер контейнера веб-приложений (WACS).....	445
10.1.2	Добавление дополнительных серверов WACS в систему и их удаление.....	449
10.1.3	Добавление или удаление служб на сервере WACS.....	453
10.1.4	Настройка HTTPS/SSL.....	455
10.1.5	Поддерживаемые методы аутентификации.....	459
10.1.6	Настройка Kerberos AD для WACS	460
10.1.7	Настройка единого входа в AD Kerberos	466
10.1.8	Сервер контейнера веб-приложений (WACS) и ваша IT-среда.....	468
10.1.9	Настройка свойств веб-приложений.....	471
10.1.10	Устранение неполадок.....	472
10.1.11	Свойства WACS.....	476
Глава 11	Резервное копирование и восстановление.....	477
11.1	Резервное копирование и восстановление системы.....	477
11.1.1	Выполнение резервного копирования системы.....	478
11.1.2	Резервное копирование настроек сервера.....	479
11.1.3	Резервное копирование содержимого Business Intelligence.....	482
11.1.4	Восстановление системы.....	482

11.1.5	Восстановление утерянных или поврежденных файлов платформы SAP BusinessObjects Business Intelligence 4.0 при наличии резервной копии.....	487
11.1.6	Повторное создание платформы SAP BusinessObjects Business Intelligence при утрате файлов.....	488
11.1.7	Параметры BackupCluster и RestoreCluster.....	488
Глава 12	Управление жизненным циклом.....	493
12.1	Консоль управления жизненным циклом.....	493
12.2	Параметры системы управления версиями для консоли управления жизненным циклом.....	493
12.2.1	Параметры системы управления версиями для консоли управления жизненным циклом.....	494
12.3	Инструмент командной строки механизма BIAR.....	494
12.3.1	Использование файла свойств	497
12.3.2	Использование инструмента командной строки механизма BIAR.....	503
Глава 13	Управление приложениями.....	505
13.1	Управление приложениями с помощью CMC.....	505
13.1.1	Обзор.....	505
13.1.2	Общие настройки приложений.....	506
13.1.3	Настройки, зависящие от приложения.....	508
13.2	Управление приложениями с помощью свойств BOE.war.....	527
13.2.1	Файл BOE.war.....	527
13.3	Настройка точек входа в систему для стартовой панели BI и OpenDocument.....	535
13.3.1	Местоположения файлов стартовой панели BI и OpenDocument.....	536
13.3.2	Определение пользовательской страницы входа в систему.....	537
13.3.3	Добавление доверительной аутентификации при входе в систему.....	538
13.4	Настройка веб-интеграции BEx	539
13.4.1	Запуск сервера для веб-приложений BEx	540
13.4.2	Запуск отдельного сервера для веб-приложений BEx	541
13.4.3	Настройка параметров сервера.....	541
13.4.4	Проверка подключения к системе BW	542
13.4.5	Настройка соединения между конструктором веб-приложений BEx и платформы BI.....	542
Глава 14	Управление соединениями и юниверсами.....	545
14.1	Управление соединениями.....	545
14.1.1	Для удаления соединения юниверса.....	545
14.2	Управление Юниверсами.....	546
14.2.1	Удаление юниверсов.....	546
Глава 15	Мониторинг.....	549
15.1	О приложении мониторинга.....	549

15.2	Термины мониторинга.....	549
15.2.1	Архитектура.....	551
15.3	Поддержка кластеров для сервера мониторинга.....	554
15.4	Показатели.....	554
15.5	Свойства конфигурации.....	566
15.5.1	URL-адрес конечной точки JMX.....	569
15.6	Интеграция с другими приложениями.....	571
15.6.1	Интеграция приложения мониторинга с IBM Tivoli.....	571
15.6.2	Интеграция приложения мониторинга с SAP Solution Manager	574
15.7	Создание юниверса для базы данных Derby.....	574
15.8	Устранение неполадок.....	575
15.8.1	Панель мониторинга.....	576
15.8.2	Сигналы.....	576
15.8.3	Список наблюдений.....	576
15.8.4	Зонды.....	577
15.8.5	Показатели.....	578
15.8.6	Диаграмма.....	578
Глава 16	Аудит.....	579
16.1	Обзор.....	579
16.2	Страница "Аудит СМС".....	585
16.2.1	Состояние аудита.....	585
16.2.2	Настройка аудита событий.....	587
16.2.3	Параметры конфигурации хранилища данных аудита.....	589
16.3	События аудита.....	591
16.3.1	События и детали аудита.....	598
Глава 17	Поиск по платформе.....	619
17.1	Обзор.....	619
17.2	Архитектура.....	619
17.3	Поддержка кластеров для поиска по платформе.....	621
17.4	SDK и открытый поиск.....	622
17.4.1	Platform Search SDK.....	622
17.4.2	Open Search.....	622
17.5	Настройка свойств приложения.....	625
17.6	Типы содержимого, доступного для поиска.....	631
17.7	Предложенные запросы.....	632
17.8	Фасеты.....	633
17.9	Многоязыковая поддержка.....	634
17.10	Предложения.....	634

17.11	Объединение результатов поиска из SAP BusinessObjects Explorer.....	635
17.12	Интеграция времени поиска с SAP NetWeaver Enterprise Search.....	635
17.12.1	Создание соединителя в SAP NetWeaver Enterprise Search	636
17.12.2	Импорт роли пользователя в аутентификации SAP BusinessObjects Enterprise.....	637
17.12.3	Поиск из NetWeaver Enterprise Search.....	637
17.13	Выполнение аудита.....	638
17.14	Список сбоев индексации.....	639
17.15	Устранение неполадок.....	640

Глава 18

Глава 18	Интеграция.....	643
18.1	интеграция.....	643
18.2	Термины модуля "Интеграция".....	644
18.2.1	Приложение BI	645
18.2.2	Сайт-адресат	645
18.2.3	Локальный.....	645
18.2.4	Выполняемые локально завершенные экземпляры	645
18.2.5	Несколько сайтов-источников	645
18.2.6	Однонаправленное тиражирование	646
18.2.7	Сайт-источник	646
18.2.8	Удаленный.....	646
18.2.9	Удаленное соединение.....	646
18.2.10	Удаленное планирование.....	646
18.2.11	Тиражирование.....	647
18.2.12	Задание тиражирования.....	647
18.2.13	Список тиражирования.....	647
18.2.14	Объект тиражирования.....	647
18.2.15	Пакет тиражирования.....	647
18.2.16	Обновление тиражирования.....	648
18.2.17	Двунаправленное тиражирование.....	648
18.3	Управление правами безопасности.....	648
18.3.1	Права, необходимые на сайте-источнике.....	648
18.3.2	Права, необходимые на сайте-адресате.....	649
18.3.3	Права, характерные для интеграции.....	650
18.3.4	Тиражирование безопасности объекта.....	652
18.3.5	Тиражирование параметров безопасности с использованием уровней доступа.....	653
18.4	Параметры типов и режимов тиражирования.....	654
18.4.1	Однонаправленное тиражирование	654
18.4.2	Двунаправленное тиражирование	654
18.4.3	"Обновлять из источника" или "Обновлять из адресата".....	655
18.5	Тиражирование сторонних пользователей и групп.....	656
18.6	Тиражирование юниверсов и соединений юниверсов.....	657

18.7	Управление списками тиражирования.....	658
18.7.1	Создание списков тиражирования.....	659
18.7.2	Изменение списков тиражирования.....	661
18.8	Управление удаленными соединениями.....	662
18.8.1	Создание удаленных соединений.....	663
18.8.2	Изменение удаленных соединений.....	665
18.9	Управление заданиями тиражирования.....	666
18.9.1	Создание заданий тиражирования.....	666
18.9.2	Планирование заданий тиражирования.....	668
18.9.3	Изменение заданий тиражирования.....	669
18.9.4	Просмотр журнала после выполнения задания тиражирования.....	670
18.10	Управление очисткой объектов.....	671
18.10.1	Способ использования очистки объектов.....	671
18.10.2	Ограничения очистки объектов.....	672
18.10.3	Частота очистки объектов.....	672
18.11	Управление обнаружением и разрешением конфликтов.....	673
18.11.1	Разрешение конфликтов однонаправленного тиражирования.....	674
18.11.2	Разрешение конфликта двунаправленного тиражирования.....	675
18.12	Использование веб-служб в модуле "Интеграция".....	679
18.12.1	Переменные сеанса	679
18.12.2	Кэширование файлов	679
18.12.3	Настраиваемое развертывание	680
18.13	Удаленное планирование и экземпляры, выполняемые локально.....	681
18.13.1	Удаленное планирование.....	681
18.13.2	Экземпляры, выполняемые локально.....	683
18.13.3	Совместное использование экземпляров.....	683
18.14	Импорт и перенос тиражированного содержимого.....	684
18.14.1	Импорт тиражированного содержимого.....	684
18.14.2	Импорт тиражированного содержимого и продолжение тиражирования	685
18.14.3	Перенос содержимого из тестовой среды.....	686
18.14.4	Повторное назначение сайта-адресата.....	687
18.15	Оптимальные методы работы.....	687
18.15.1	Текущие ограничения выпуска.....	690
18.15.2	Устранение неисправностей: сообщения об ошибках.....	691
Глава 19	Дополнительные конфигурации для сред ERP.....	695
19.1	Конфигурации для интеграции с SAP NetWeaver.....	695
19.1.1	Интеграция с SAP Netweaver Business Warehouse (BW).....	695
19.2	Настройка для интеграции с JD Edwards.....	745
19.2.1	Настройка единого входа (SSO) для SAP Crystal Reports.....	745
19.2.2	Настройка протокола SSL для интеграции с JD Edwards.....	746

19.3	Настройка для интеграции с PeopleSoft Enterprise.....	747
19.3.1	Настройка единого входа (SSO) для SAP Crystal Reports и PeopleSoft Enterprise.....	747
19.3.2	Настройка соединений по протоколу SSL.....	748
19.3.3	Настройка производительности для систем PeopleSoft.....	750
19.4	Настройка для интеграции с Siebel.....	752
19.4.1	Настройка Siebel для интеграции с платформой SAP BusinessObjects Business Intelligence.....	752
19.4.2	Создание пункта меню "Crystal Reports".....	753
19.4.3	Контекстуальная зависимость.....	754
19.4.4	Настройка единого входа (SSO) для SAP Crystal Reports и Siebel.....	757
19.4.5	Настройка соединений по протоколу SSL.....	758
Глава 20	Управление журналами и их настройка.....	759
20.1	Ведение журнала трассировок компонентов.....	759
20.2	Уровни журнала трассировки.....	759
20.3	Настройка трассировки для серверов.....	760
20.3.1	Настройка уровня журнала трассировки сервера в CMC.....	761
20.3.2	Установка уровня журнала трассировки для нескольких серверов, управляемых в CMC.....	762
20.3.3	Настройка серверной трассировки с использованием файла BO_trace.ini.....	762
20.4	Настройка трассировки для веб-приложений.....	766
20.4.1	Настройка уровня журнала трассировки веб-приложения в CMC.....	767
20.4.2	Изменение параметров трассировки вручную при помощи файла BO_trace.ini.....	767
20.5	Настройка трассировки для средства управления обновлением.....	773
20.5.1	Настройка трассировки для средства управления обновлениями.....	773
Глава 21	Интеграция с SAP Solution Manager.....	775
21.1	Обзор интеграции.....	775
21.2	Контрольный список по интеграции SAP Solution Manager.....	775
21.3	Управление регистрацией System Landscape Directory.....	777
21.3.1	Регистрация платформы BI в System Landscape.....	777
21.3.2	Точки запуска SLD.....	778
21.3.3	Ведение журнала SLD-соединения	779
21.4	Управление агентами Solution Management Diagnostics.....	779
21.4.1	Обзор Solution Manager Diagnostics (SMD).....	779
21.4.2	Работа с SMD-агентами.....	780
21.4.3	Учетная запись пользователя SMAdmin.....	780
21.5	Инструментальные средства управления производительностью.....	781
21.5.1	Настройка инструментов мониторинга производительности для платформы BI.....	781
21.5.2	Настройка инструментальных средств мониторинга производительности для платформы BI.....	781
21.5.3	Настройка конфигурации производительности для веб-уровня.....	783

21.5.4	Файлы журнала настройки конфигурации	783
21.6	Трассировка с использованием SAP Passport.....	784
Глава 22	Администрирование в командной строке.....	785
22.1	Скрипты UNIX.....	785
22.1.1	Утилиты скриптов.....	785
22.1.2	Шаблоны скриптов.....	791
22.1.3	Скрипты, используемые платформой SAP BusinessObjects Business Intelligence.....	792
22.2	Скрипты Windows.....	794
22.2.1	ssm.exe.....	794
22.3	Командные строки сервера.....	797
22.3.1	Обзор командных строк.....	797
22.3.2	Стандартные параметры для всех серверов.....	798
22.3.3	Центральный сервер управления.....	799
22.3.4	Сервер обработки Crystal Reports и кэш-сервер Crystal Reports.....	803
22.3.5	Сервер обработки Dashboard Design и кэш-сервер Dashboard Design.....	804
22.3.6	Серверы заданий.....	805
22.3.7	Адаптивный сервер обработки.....	806
22.3.8	Сервер приложений отчетов.....	807
22.3.9	Сервер обработки Web Intelligence.....	809
22.3.10	Серверы репозитория входящих и исходящих файлов.....	810
22.3.11	Сервер событий.....	812
22.3.12	Сервера информационных панелей и аналитики информационных панелей	813
Глава 23	Приложение "Права".....	815
23.1	О приложении "Права".....	815
23.2	Общие права.....	815
23.3	Права для определенных типов объектов.....	818
23.3.1	Права доступа к папке.....	818
23.3.2	Категории.....	818
23.3.3	Примечания.....	819
23.3.4	Отчеты Crystal.....	820
23.3.5	Документы Web Intelligence.....	820
23.3.6	Пользователи и группы.....	822
23.3.7	Уровни доступа.....	823
23.3.8	Рабочие пространства BI.....	824
23.3.9	Права универсов (.unv).....	825
23.3.10	Права универсов (.unx).....	826
23.3.11	Уровни доступа к объектам для универсов.....	828
23.3.12	Права соединений.....	829

23.3.13	Программные приложения.....	831
Глава 24	Приложение "Свойства серверов".....	845
24.1	О приложении "Свойства серверов".....	845
24.1.1	Общие свойства сервера.....	845
24.1.2	Свойства основных служб.....	848
24.1.3	Свойства служб соединения.....	861
24.1.4	Свойства служб Crystal Reports.....	864
24.1.5	Свойства служб Analysis.....	875
24.1.6	Свойства служб объединения данных.....	876
24.1.7	Свойства служб Web Intelligence.....	877
24.1.8	Свойства служб Dashboard Design.....	888
Глава 25	Приложение "Показатели сервера".....	893
25.1	О приложении "Показатели сервера".....	893
25.1.1	Общие показатели сервера	893
25.1.2	Показатели центрального сервера управления.....	896
25.1.3	Показатели сервера соединений.....	901
25.1.4	Показатели сервера событий.....	901
25.1.5	Показатели сервера репозитория файлов.....	902
25.1.6	Показатели адаптивного сервера обработки.....	903
25.1.7	Показатели сервера контейнера веб-приложений.....	908
25.1.8	Показатели адаптивного сервера заданий.....	909
25.1.9	Показатели сервера Crystal Report.....	912
25.1.10	Показатели сервера Web Intelligence.....	915
25.1.11	Показатели сервера Dashboard Design.....	917
Глава 26	Приложение заполнителя сервера и узла.....	921
26.1	Заполнители сервера и узлов.....	921
Глава 27	Приложение выполнения аудита схемы склада данных.....	933
27.1	Обзор.....	933
27.2	Диаграмма схемы.....	933
27.3	Таблицы аудита склада данных.....	934
Приложение А	Дополнительная информация.....	945
Указатель		949

Начало работы

1.1 О справке

В данной справке приведены полезные сведения и инструкции для развертывания и настройки платформы BI. Здесь представлены процедуры выполнения стандартных задач. В каждой расширенной теме содержится основная необходимая информация и технические данные.

Для получения сведений об установке этого продукта см. *Руководство по установке платформы SAP BusinessObjects Business Intelligence*.

1.1.1 Для кого предназначена данная справка?

Данная справка описывает задачи развертывания и настройки. С данным руководством рекомендуется ознакомиться в следующих случаях:

- планирование развертывания первой системы
- настройка первой развернутой системы
- существенные изменения архитектуры имеющейся системы
- повышение производительности системы.

Справка предназначена для системных администраторов, осуществляющих настройку платформы BI и ее обслуживание. Администраторам пригодится знание операционной системы и сетевой среды, а также общие представления об управлении сервером веб-приложений и технологий работы со сценариями. При этом в данном руководстве содержится достаточная базовая и концептуальная информация, которая не зависит от уровня подготовки в области администрирования и понятно описывает все административные функции и задачи.

1.1.2 Платформа SAP BusinessObjects Business Intelligence

Платформа BI – это гибкое, масштабируемое и надежное решение, предназначенное для предоставления многофункциональных интерактивных отчетов конечному пользователю.

посредством сетевых приложений – локальных сетей, Интернета или корпоративного портала. При использовании для распространения еженедельных отчетов о продажах, предоставления клиентам персонализированных предложений услуг или интеграции критической информации в корпоративные порталы платформа BI обеспечивает ощутимые преимущества, действие которых простирается на всю организацию и за ее пределы. В качестве интегрированного пакета для составления отчетов, аналитической деятельности и предоставления информации платформа BI представляет собой решение, повышающее эффективность работы конечного пользователя и сокращающее потребность в административной деятельности.

1.1.3 Переменные

В настоящем руководстве используются перечисленные ниже переменные.

Переменная	Описание
<INSTALLDIR>	Каталог установки платформы BI. На компьютере под управлением Windows каталог по умолчанию – C:\Program Files (x86)\SAP BusinessObjects.
<PLATFORM64DIR>	Название операционной системы UNIX. Допустимы следующие значения: <ul style="list-style-type: none"> • aix_rs6000_64 • linux_x64 • solaris_sparcv9 • hpux_ia64
<SCRIPTDIR>	Каталог, где расположены скрипты администрирования платформы BI. На компьютере под управлением Windows это каталог <INSTALLDIR>\win64_x64\scripts. На компьютерах под управлением Unix это каталог <INSTALLDIR>/<PLATFORM64DIR>/scripts.

1.2 Начало работы

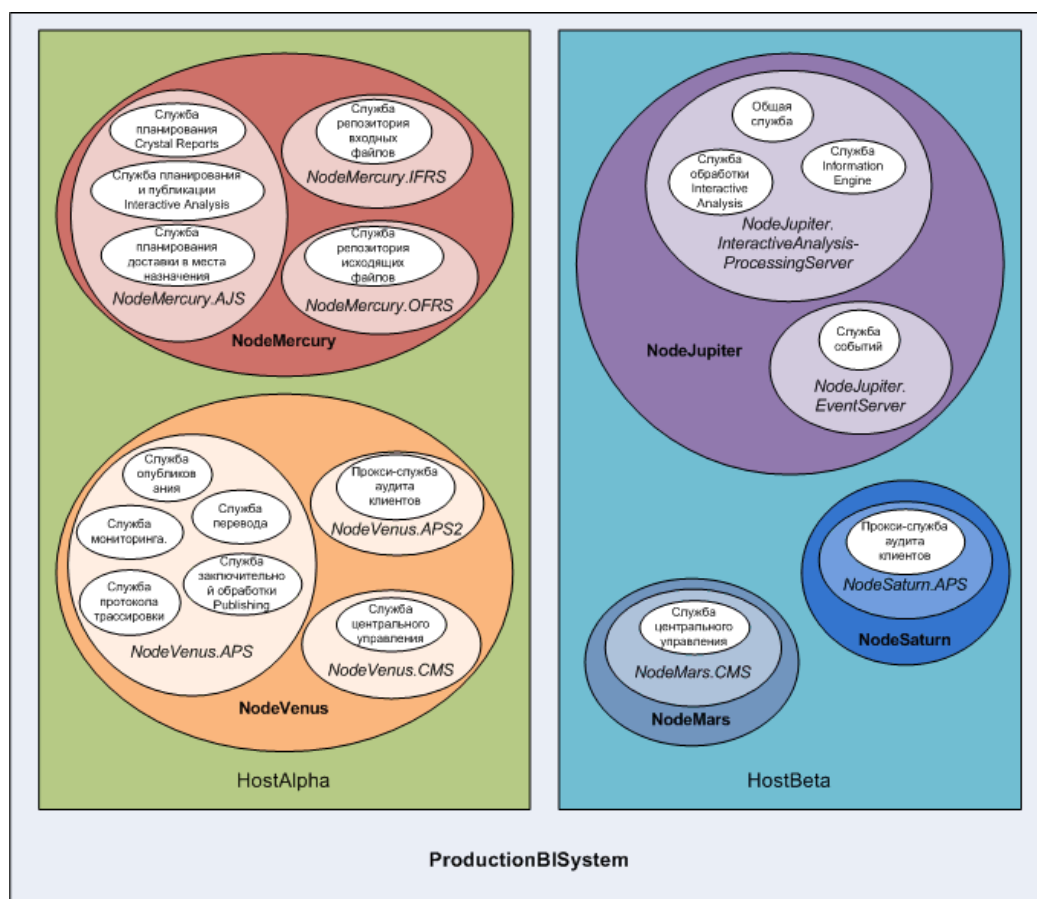
1.2.1 Основные понятия

1.2.1.1 Службы и серверы

На следующей диаграмме показана возможная установка платформы BI.

Примечание:

Узлы, серверы и службы показаны только для иллюстрации. В реальной установке число хостов, узлов, серверов и служб, а также типы серверов и служб, может отличаться.



Кластер с именем *ProductionBISystem* имеет два хоста.

- На хосте, называемом *HostAlpha*, установлена платформа BI. Для него настроены два узла:
 - *NodeMercury*: содержит адаптивный сервер заданий (*NodeMercury.AJS*) со службами для планирования и публикации отчетов, сервер репозитория входных файлов (*NodeMercury.IFRS*) со службой для хранения входных отчетов и сервер репозитория выходных файлов (*NodeMercury.OFRS*) со службой хранения выходных данных отчета.
 - *NodeVenus*: содержит адаптивный сервер обработки (*NodeVenus.APS*) со службами для функций публикации, мониторинга и перевода, адаптивный сервер обработки (*NodeVenus.APS*) со службой для аудита клиентов, а также Центральный сервер управления (*NodeVenus.CMS*) со службой для CMS.
- На хосте, называемом *HostBeta*, установлена платформа BI. Для него настроены три узла:
 - *NodeMars*: содержит Центральный сервер управления (*NodeMars.CMS*) со службой для CMS.
 - *NodeJupiter*: содержит сервер обработки Web Intelligence (*NodeJupiter.Web Intelligence*) со службой предоставления отчетности Web Intelligence и сервер событий (*NodeJupiter.EventServer*) для мониторинга файлов отчета.
 - *NodeSaturn*: содержит адаптивный сервер обработки (*NodeSaturn.APS*) со службой предоставления аудита клиентов.

В отношении платформы BI термины *сервер* и *служба* означают два типа программного обеспечения, выполняемого на компьютере с установленным программным пакетом платформы BI.

Служба – это серверная подсистема, выполняющая определенные функции. Служба выполняется в памяти сервера под идентификатором процесса родительского контейнера (сервера). Например, служба планирования и публикаций SAP BusinessObjects Web Intelligence представляет собой подсистему, выполняемую на адаптивном сервере заданий.

Термином *сервер* обозначается процесс уровня операционной системы (в некоторых системах он носит название *демон*), в котором размещаются одна или несколько служб. В качестве примера подобного сервера можно привести Центральный сервер управления (CMS) и сервер адаптивной обработки. Сервер запускается под определенной учетной записью операционной системы и обладает собственным идентификатором PID.

Узел – ряд серверов платформы BI, запускаемых на одном хосте. На одном хосте могут размещаться один или несколько узлов.

Платформу BI можно установить на один компьютер, на несколько компьютеров внутренней сети или распределить различные компоненты этого программного пакета в глобальной сети (WAN).

1.2.1.2 серверная аналитика

Серверная аналитика – это компонент Central Management Console (CMC), служащий для управления коллекцией или процессами серверов, вместе составляющих узел. Изменения в процессах серверов, сделанные в CMC, распространяются на затронутые серверы посредством

Server Intelligence Agent (SIA). SIA также используется для автоматического перезапуска или завершения работы сервера при обнаружении непредвиденного условия; он также используется центральным сервером управления (CMS) для управления узлами.

На сервере Server Intelligence Agent (SIA) архивируются данные о серверных процессах в базе данных CMS, что позволяет легко восстанавливать стандартные параметры сервера или создавать резервные экземпляры серверных процессов с такими же параметрами.

1.2.2 Основные инструменты администрирования

1.2.2.1 Central Management Console (CMC)

Central Management Console (CMC) – это веб-инструмент, с помощью которого можно выполнять задачи администрирования, включая управление пользователями, содержимым и серверами. Это также позволяет публиковать, организовывать и настраивать параметры безопасности. Поскольку CMC является веб-приложением, все вышеупомянутые административные задачи можно выполнять посредством веб-браузера на любом компьютере, который может подключиться к серверу.

Все пользователи могут входить в CMC для изменения предпочтений. Только члены группы *Администраторы* могут изменять параметры управления, если другим пользователям явно не предоставлены для этого права. В CMC также можно назначить роли, это даст некоторым пользователям права на выполнение мелких административных заданий

1.2.2.2 Central Configuration Manager (CCM)

Central Configuration Manager (CCM) – это средство устранения неполадок серверов и управления узлами, доступное в двух видах: В среде Microsoft Windows CCM позволяет управлять локальными и удаленными серверами с помощью графического пользовательского интерфейса или командной строки. В среде UNIX скрипт оболочки CCM (ccm.sh) позволяет управлять серверами из командной строки.

С помощью CCM можно создавать и настраивать узлы Server Intelligence Agent (SIA), а также запускать или останавливать работу сервера веб-приложений. В Windows с помощью данного приложения также можно изменять параметры сети (например, параметры шифрования SSL). Эти параметры применяются ко всем серверам в пределах узла.

Примечание:

В настоящее время большинство задач по управлению серверами выполняются посредством CMC, а не CCM. Сейчас CCM используется для устранения неполадок и настройки узлов.

1.2.2.3 Repository Diagnostic Tool

Repository Diagnostic Tool (RDT) может выполнять сканирование, диагностику и устранение несоответствий, которые могут возникать между системной базой данных центрального сервера управления (CMS) и файловым хранилищем серверов репозитория файлов (FRS). Можно задать предельное количество ошибок, которое будет обнаружено и исправлено средством RDT перед остановкой работы.

Средство RDT должно использоваться после восстановления системы платформы BI.

1.2.2.4 Средство управления обновлением

Средство управления обновлением (ранее мастер импорта) устанавливается как часть платформы BI и используется как вспомогательное средство для администраторов при выполнении процедур импорта пользователей, групп и папок из предыдущих версий платформы BI. Это также дает возможность импортировать и обновлять объекты, события, группы серверов, объекты репозитория и календари.

Для получения сведений об обновлении с предыдущей версии платформы BI см. *Руководство по обновлению SAP BusinessObjects Business Intelligence*.

1.2.3 Ключевые задачи

В зависимости от ситуации может потребоваться изучение конкретных разделов данной справки. Вам также могут быть доступны другие ресурсы. Для каждой из описанных ниже ситуаций есть список рекомендованных задач и разделов для изучения.

См. также

- [Планирование или выполнение первого развертывания системы](#)
- [Настройка развертывания](#)
- [Повышение производительности системы](#)
- [Central Management Console \(CMC\)](#)

1.2.3.1 Планирование или выполнение первого развертывания системы

Если планируется или выполняется первое развертывание платформы BI, рекомендуется выполнить указанные ниже задачи и ознакомиться с соответствующими разделами:

- Для ознакомления с компонентами платформы BI см. «Обзор архитектуры».
- Чтобы оценить текущие потребности и разработать наиболее подходящую архитектуру развертывания, см. *Руководство по планированию развертывания платформы SAP BusinessObjects Business Intelligence*.
- «Обмен данными между компонентами платформы BI»
- «Настройки безопасности»
- Если планируется использование средств аутентификации сторонних производителей, см. раздел «Аутентификация».
- Для получения дополнительных сведений об установке платформы BI см. *Руководство по установке платформы SAP BusinessObjects Business Intelligence*.
- После установки прочтите раздел «Обзор управления серверами»

См. также

- [Обзорная информация по архитектуре](#)
- [Основные сведения об обмене данными между компонентами платформы BI](#)
- [Обзор вопросов безопасности](#)
- [Параметры аутентификации платформы BI](#)
- [Администрирование сервера](#)

1.2.3.2 Настройка развертывания

Когда завершена установка платформы BI и требуется выполнить начальные задачи настройки (например, настройку брандмауэра и управления пользователями), рекомендуется прочесть следующие разделы:

См. также

- [Администрирование сервера](#)
- [Взаимодействие между компонентами платформы BI](#)
- [Обзор вопросов безопасности](#)
- [О приложении мониторинга](#)

1.2.3.3 Повышение производительности системы

Если требуется оценить эффективность системы и настроить ее так, чтобы максимизировать ресурсы, рекомендуется прочесть следующие разделы:

- Если требуется осуществлять наблюдение за имеющейся системой, ознакомьтесь с разделом «Мониторинг».
- Описание ежедневных задач обслуживания и процедур работы с серверами в консоли СМС см. в разделе «Сопровождение сервера».

См. также

- [О приложении мониторинга](#)
- [Администрирование сервера](#)

1.2.3.4 Работа с объектами в СМС

Если выполняется работа с объектами в СМС, прочтите следующие разделы:

- Информацию о настройке пользователей и групп в СМС см. в разделе «Обзор управления учетными записями».
- Для настройки безопасности объектов см. «Работа с правами на платформе BI»
- Для получения общих сведений о работе с объектами см. *Руководство пользователя платформы SAP BusinessObjects Business Intelligence*.

См. также

- [Обзор управления учетными записями](#)
- [Права на платформе BI](#)

Архитектура

2.1 Обзорная информация по архитектуре

В этом разделе дается общий обзор архитектуры платформы, а также системы и служебных компонентов, входящих в платформу SAP BusinessObjects Business Intelligence. Данная информация поможет администраторам понять важнейшие аспекты системы и сформировать план развертывания, управления и обслуживания системы.

Платформа SAP BusinessObjects Business Intelligence рассчитана на высокую производительность при использовании различными пользователями и в различных сценариях развертывания. Например, специализированные службы платформ обеспечивают доступ к данным по требованию и создают отчеты либо составляют расписание отчетов в зависимости от времени и событий. Можно разгрузить интенсивное планирование и обработку процессора, создав выделенные серверы для размещения конкретных служб. Архитектура спроектирована так, чтобы соответствовать требованиям практически любого варианта развертывания Business Intelligence, и обеспечивает достаточную гибкость, чтобы в ней могли работать и несколько пользователей в одном средстве, и десятки тысяч пользователей в различных средствах через различные интерфейсы.

Разработчики могут интегрировать платформу SAP BusinessObjects Business Intelligence в другие технологические системы организации, используя веб-службы и интерфейсы программирования приложений (API) Java или .NET.

Пользователи могут получать доступ, создавать, изменять отчеты и работать с ними с помощью специальных средств и приложений, включая:

- Клиенты, устанавливаемые программой установки средств клиента платформы SAP BusinessObjects Business Intelligence:
 - Web Intelligence
 - Диспетчер Business View
 - Средство преобразования отчетов
 - Средство создания универсов
 - Средство запросов веб-служб (ранее Query as a Web Service)
 - Средство дизайна информации (ранее "Дизайнер информации")
 - Средство управления переводами (ранее "Диспетчер переводов")
 - Виджеты для платформы SAP BusinessObjects Business Intelligence (ранее BI Widgets)
- Клиенты, доступные отдельно:
 - SAP Crystal Reports
 - SAP BusinessObjects Dashboard Design (ранее Xcelsius)

- SAP BusinessObjects Analysis (ранее Voyager)
- Рабочие пространства BI (ранее Dashboard Builder)

ИТ-отделы могут использовать следующие средства управления данными и системой:

- Средства просмотра отчетов
- Central Management Console (CMC)
- Диспетчер центральной конфигурации (CCM)
- Средство диагностики репозитория (RDT)
- Средство администрирования объединения данных
- Средство управления обновлением (ранее "Мастер импорта")
- Средство создания юниверсов (ранее Universe Designer)
- SAP BusinessObjects Mobile

Для обеспечения гибкости, надежности и расширяемости компоненты платформы SAP BusinessObjects Business Intelligence можно установить на один или несколько компьютеров. Можно даже установить две различные версии платформы SAP BusinessObjects Business Intelligence одновременно на один компьютер, хотя такая конфигурация рекомендуется к использованию только в рамках процесса обновления или в целях тестирования.

Серверные процессы могут быть «вертикальными» (когда на одном компьютере выполняется несколько или все серверные процессы) для снижения затрат или «горизонтальными» (когда серверные процессы распределены между двумя и более сетевыми компьютерами) для повышения производительности. Также возможен запуск нескольких избыточных версий одного и того же серверного процесса на нескольких компьютерах, таким образом обработка может продолжиться в случае, если основной процесс будет прерван ошибкой.

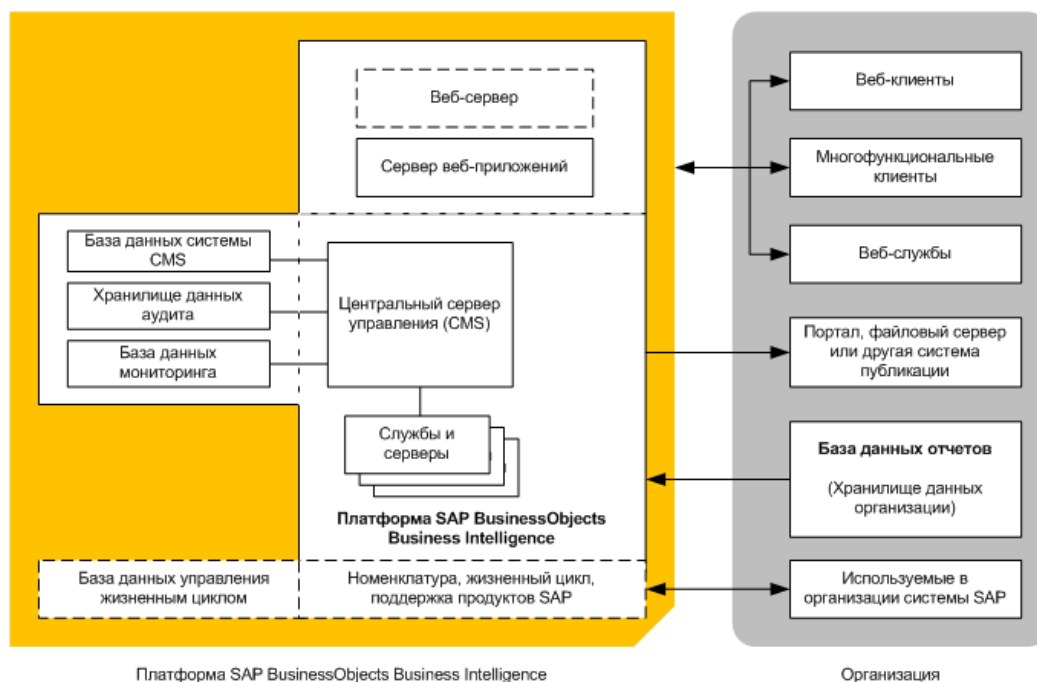
Примечание:

Хотя возможно одновременно использовать платформы Windows или платформы Unix, не рекомендуется смешивать системы для процессов сервера центрального управления (CMS).

2.1.1 Обзор системы

Платформа SAP BusinessObjects Business Intelligence предоставляет средства анализа данных и отчетности на корпоративном уровне. Можно анализировать данные из любой поддерживаемой системы баз данных (включая текстовые или многомерные системы OLAP), а отчеты BI публиковать в различных форматах в многочисленных системах публикации.

Следующая диаграмма показывает, как платформа SAP BusinessObjects Business Intelligence вписывается в инфраструктуру организации.



Платформа SAP BusinessObjects Business Intelligence предоставляет данные в базы данных организации из многих соединений, доступных только для чтения, и использует свои собственные базы данных для хранения своей конфигурации, данных аудита и других операционных сведений. Создаваемые в системе отчеты BI могут направляться в различные пункты назначения, включая файловые системы и адреса электронной почты, а также размещаться на веб-сайтах или порталах.

Платформа SAP BusinessObjects Business Intelligence – самодостаточная система, которая может быть установлена на одном компьютере (например, как небольшая среда разработки или предпроизводственных испытаний) или в группе нескольких компьютеров, на которых работают различные компоненты (к примеру, как крупномасштабная производственная среда).

2.1.2 Базы данных

В платформе SAP BusinessObjects Business Intelligence используется несколько различных баз данных.

- База данных отчетов

Используется для информации организации. Это исходные данные, используемые для анализа и отчетности в платформе SAP BusinessObjects Business Intelligence. Как правило, эти сведения хранятся в реляционной базе данных, однако они также могут находиться в текстовых файлах, документах Microsoft Office и OLAP-системах.

- База данных системы CMS

Для хранения данных платформы SAP BusinessObjects Business Intelligence, таких как сведения о пользователе, сервере, папке, документе, конфигурации, авторизации и аутентификации, используется база данных системы CMS. Она находится под управлением центрального сервера управления (CMS) и иногда называется *системным репозиторием*.

- Хранилище данных аудита

Хранилище данных аудита (ADS) используется для хранения сведений об отслеживаемых событиях, которые происходят в платформе SAP BusinessObjects Business Intelligence. Эти сведения могут быть использованы для мониторинга использования системных компонентов, активности пользователей или других аспектов ежедневных операций.

- База данных управления жизненным циклом

В базе данных управления жизненным циклом отслеживаются конфигурации и версии, связанные с установкой платформы SAP BusinessObjects Business Intelligence, а также обновления.

- База данных мониторинга

Для мониторинга используется база данных Java Derby, где хранятся сведения о системной конфигурации и компонентах, предназначенные для обеспечения поддержки SAP.

Если сервер базы данных для работы с базами данных системы CMS и хранилища данных аудита отсутствует, он может быть автоматически создан и настроен программой установки платформы SAP BusinessObjects Business Intelligence. Рекомендуется сравнить свои требования со сведениями поставщика сервера базы данных, чтобы определить, какая из поддерживаемых баз данных лучше всего отвечает требованиям организации.

2.1.3 Серверы

Платформа SAP BusinessObjects Business Intelligence состоит из коллекций серверов, выполняющихся на одном или нескольких хостах. В небольших установках (такие как тестовые системы или системы разработки) могут быть использованы сервер веб-приложений, сервер базы данных и все серверы платформы SAP BusinessObjects Business Intelligence.

В средних и крупных средах серверы могут размещаться на нескольких хостах. Например, хост сервера веб-приложений может использоваться совместно с хостом сервера платформы SAP BusinessObjects Business Intelligence. Это позволяет освободить ресурсы на хосте сервера платформы SAP BusinessObjects Business Intelligence, предоставляя ему возможность обработать больше информации, чем если бы на нем размещался еще и сервер веб-приложений.

В крупных установках несколько хостов серверов платформы SAP BusinessObjects Business Intelligence могут использоваться совместно в кластере. Например, если в организации много пользователей SAP Crystal Reports, можно создать несколько серверов обработки Crystal Reports на нескольких хостах платформы SAP BusinessObjects Business Intelligence, что обеспечивает наличие достаточных ресурсов для обработки запросов от клиентов.

Преимущества использования нескольких серверов:

- Повышение производительности

На нескольких хостах сервера платформы SAP BusinessObjects Business Intelligence обработка очереди данных отчетности ведется быстрее, чем на одном хосте сервера платформы SAP BusinessObjects Business Intelligence.

- Выравнивание нагрузки

Если нагрузка на сервер выше, чем для других серверов кластера, CMS автоматически направляет задания на сервер с максимальными ресурсами.

- Повышение доступности

При возникновении непредвиденной ситуации на сервере CMS автоматически перенаправляет задания на другие сервера до устранения неполадок с сервером.

2.1.4 Серверы веб-приложений

Сервер веб-приложений выполняет функции уровня преобразования между веб-браузером или полным приложением и платформой SAP BusinessObjects Business Intelligence. Поддерживаются серверы веб-приложений под управлением Windows, Unix и Linux.

Поддерживаются следующие серверы веб-приложений:

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

Для получения подробного списка поддерживаемых серверов веб-приложений см. *Руководство по поддерживаемым платформам* по адресу <http://service.sap.com/bosap-support>.

Если сервер веб-приложений для использования с платформой SAP BusinessObjects Business Intelligence не установлен, программа установки может установить и настроить сервер веб-приложений Tomcat 6. Рекомендуется сравнить свои требования с информацией от поставщика сервера веб-приложений, чтобы определить, какой из поддерживаемых серверов веб-приложений лучше всего отвечает требованиям организации.

Примечание:

При настройке производственной среды рекомендуется разместить сервер веб-приложений в отдельной системе. Одновременная работа платформы SAP BusinessObjects Business Intelligence и сервера веб-приложений на одном хосте в производственной среде может привести к снижению производительности.

2.1.4.1 Служба контейнера веб-приложений (WACS)

Для размещения веб-приложений платформы SAP BusinessObjects Business Intelligence требуется сервер веб-приложений.

Опытный администратор серверов веб-приложений на базе Java с расширенными потребностями в отношении администрирования может использовать для размещения веб-приложений платформы SAP BusinessObjects Business Intelligence поддерживаемый сервер веб-приложений на базе Java. Если для размещения платформы SAP BusinessObjects Business Intelligence используется поддерживаемая операционная система Windows и важна простота процесса установки сервера веб-приложений, или отсутствуют ресурсы для администрирования сервера веб-приложений на базе Java, можно при установке платформы SAP BusinessObjects Business Intelligence установить службу Web Application Container Service (WACS).

WACS представляет собой сервер платформы SAP BusinessObjects Business Intelligence, который позволяет запускать веб-приложения платформы SAP BusinessObjects Business Intelligence, такие как консоль СМС, стартовая панель BI и веб-службы, без предварительной установки сервера веб-приложений на базе Java.

Преимущества использования сервера WACS:

- Установка, обслуживание и настройка WACS требуют минимальных усилий. Он устанавливается и настраивается с помощью программы установки платформы SAP BusinessObjects Business Intelligence; для его запуска не требуются дополнительные действия.
- Благодаря WACS вам не требуются особые навыки администрирования и обслуживания серверов Java-приложений.
- WACS предоставляет интерфейс администрирования, согласованный с другими серверами платформы SAP BusinessObjects Business Intelligence.
- Как и другие серверы платформы SAP BusinessObjects Business Intelligence, WACS может устанавливаться на выделенном хосте.

Примечание:

Есть определенные ограничения в отношении использования WACS вместо выделенного Java-сервера веб-приложений:

- WACS доступен только в поддерживаемых операционных системах Windows.
- На WACS невозможно развернуть пользовательские веб-приложения, поскольку он поддерживает только веб-приложения, установленные вместе с платформой SAP BusinessObjects Business Intelligence.
- WACS не поддерживает балансировщик нагрузки Apache.

В дополнение к WACS можно использовать выделенный сервер веб-приложений. Это позволяет разместить на выделенном сервере веб-приложений пользовательские веб-приложения, при этом СМС и другие веб-приложения платформы SAP BusinessObjects Business Intelligence размещаются на WACS.

2.1.5 Software Development Kit

Пакет Software Development Kit (SDK) позволяет разработчикам включать функциональность платформы SAP BusinessObjects Business Intelligence в приложения и системы организаций.

Платформа SAP BusinessObjects Business Intelligence содержит пакеты SDK для разработки приложений на платформах Java и .NET.

Примечание:

Пакеты .NET SDK платформы SAP BusinessObjects Business Intelligence не устанавливаются по умолчанию и должны быть загружены с портала SAP Service Marketplace.

Платформой SAP BusinessObjects Business Intelligence поддерживаются следующие SDK:

- Java SDK и .NET SDK платформы SAP BusinessObjects Business Intelligence

Пакеты SDK для платформы SAP BusinessObjects Business Intelligence позволяют выполнять в приложениях такие задачи, как аутентификация, управление сеансом, работа с объектами репозитория, планирование и публикация отчетов, а также управление сервером.

Примечание:

Полный доступ ко всем функциям безопасности, управления серверами и аудита обеспечивает Java SDK.

- Пакеты Java SDK и .NET SDK для Report Application Server

Пакеты SDK Report Application Server позволяют открывать, создавать и изменять существующие отчеты Crystal Reports из приложений, включая значения параметров настройки, изменение источников данных и экспорт в другие форматы, в том числе XML, PDF, Microsoft Word и Microsoft Excel.

- Пакеты Java SDK и .NET SDK для Report Engine

Пакеты SDK для подсистемы отчетов обеспечивают взаимодействие приложений с отчетами, созданными с помощью SAP BusinessObjects Web Intelligence.

В состав пакета SDK для Report Engine входят библиотеки, которые можно использовать для создания веб-средств проектирования отчетов. Приложения, созданные с использованием этого пакета SDK, могут просматривать, создавать и изменять различные документы SAP BusinessObjects Web Intelligence. Пользователи могут изменять документы посредством добавления, удаления и изменения таких объектов, как таблицы, диаграммы, условия и фильтры.

- Пакет Platform Search SDK – это интерфейс между клиентским приложением и службой поиска по платформе. Служба поиска по платформе поддерживает общедоступный пакет SDK, входящий в состав Platform Search SDK.

Параметр запроса на поиск, отправленный через клиентское приложение на уровень SDK, преобразуется последним в XML-формат и передается в службу поиска по платформе.

- Пакеты .NET SDK и Crystal Reports Viewers Java SDK

Пакеты SDK для средств просмотра позволяют приложениям просматривать и экспортировать отчеты Crystal Reports. Доступны следующие средства просмотра:

- Средство просмотра страниц отчета DHTML. Представляет данные и позволяет выполнять детализацию, переходы между страницами, изменение масштаба, запросы, поиск, выделение, экспорт и печать.
- Средство просмотра фрагментов отчета. Это средство позволяет просматривать отдельные компоненты отчета, включая диаграммы, текст и поля.
- Библиотека тегов средства просмотра. Позволяет настраивать действия средства просмотра на страницах JSP.
- Java Consumer SDK и .NET Consumer SDK платформы SAP BusinessObjects Business Intelligence
Внедрение веб-служб, позволяющих обрабатывать запросы аутентификации и безопасности, осуществлять доступ к документам и отчетам, планирование, публикации и управление серверами.

Примечание:

Компоненты JavaServer Faces платформы SAP BusinessObjects Business Intelligence отсутствуют.

Комбинации пакетов SDK обеспечивают использование широкого диапазона функциональных возможностей BI в приложениях. Например, с помощью этих SDK было создано веб-приложение стартовой панели BI, входящее в состав платформы SAP BusinessObjects Business Intelligence.

Для получения сведений о пакетах SDK для платформы SAP BusinessObjects Business Intelligence см. руководство *SAP BusinessObjects Business Intelligence Platform SDK Developer Guide*, руководство *Report Application Server Java SDK Developer Guide*, руководство *Report Application Server Java SDK Developer Guide* и руководство *Viewers Java SDK Developer Guide*, доступные по адресу <http://service.sap.com/bosap-support>.

2.1.5.1 SDK потребителей веб-служб Java и .NET

Пакеты Web Services Java SDK и .NET Consumer SDK платформы SAP BusinessObjects Business Intelligence позволяют создавать распределенные приложения веб-служб, использующие все функциональные преимущества платформы SAP BusinessObjects Business Intelligence.

Веб-службы состоят из программных компонентов, которые можно удаленно вызывать с помощью протокола SOAP. SOAP – это протокол для обмена информацией, не зависящий от определенной платформы, объектной модели или языка программирования.

Веб-службы платформы SAP BusinessObjects Business Intelligence включают функциональные возможности в следующих областях:

- Сеанс
Управление аутентификацией и пользователями
- Платформа BI

Предоставляет такие расширенные функции платформы, как планирование, поиск, администрирование пользователей и групп, а также службы администрирования сервера.

- Report Engine

Отображает SAP BusinessObjects Business Intelligence Solution и Crystal Reports в формате HTML, PDF, Excel и XML.

- Запрос

Создание специальных запросов на основе семантического уровня юниверса.

Веб-службы платформы SAP BusinessObjects Business Intelligence используют такие стандарты, как XML, SOAP, AXIS 2.0 и WSDL. Платформа соответствует спецификациям веб-служб WS-Interoperability Basic Profile 1.0

Примечание:

В настоящее время приложения веб-служб поддерживаются в следующих конфигурациях распределителя нагрузки:

1. Постоянство IP-адреса источника.
2. Постоянство порта назначения и IP-адреса источника (доступно только в коммутаторах Cisco Content Services Switch).
3. Постоянное использование SSL.

Примечание:

В некоторых веб-браузерах постоянное использование SSL может приводить к проблемам безопасности и надежности. При помощи администратора сети проверьте, подходит ли организации постоянное использование SSL.

2.1.5.2 Средство запросов веб-служб

Средство запросов веб-служб – это приложение-мастер, которое позволяет выполнять запросы к веб-службе и интегрируется в веб-приложения. Запросы можно сохранять в каталоге стандартных запросов, которыми при необходимости могут пользоваться создатели приложений.

Как правило, содержимое BI привязано к определенному пользовательскому интерфейсу средств BI. Средство запросов веб-служб меняет ситуацию, предоставляя возможность доступа к содержимому BI любому пользовательскому интерфейсу, который может обрабатывать веб-службы.

Средство запросов веб-служб, как и другие веб-службы, поддерживается любым приложением Microsoft Windows. Средство запросов веб-служб построено на базе спецификаций веб-служб W3C SOAP, WSDL и XML. Этот инструмент состоит из двух главных компонентов:

- Серверный компонент

На серверном компоненте (входит в состав платформы SAP BusinessObjects Business Intelligence) хранится каталог средства запросов веб-служб и размещаются опубликованные веб-службы.

- Клиентское средство

Это средство позволяет бизнес-пользователям создавать и публиковать свои запросы в форме веб-службы на сервере. Средство клиента можно установить на несколько компьютеров, где будет реализован совместный доступ к одному каталогу средства запросов веб-служб, хранящемуся на сервере. Средство клиента обменивается данными с серверными компонентами через веб-службы.

Средство запросов веб-служб позволяет использовать веб-запросы в составе ряда клиентских решений, в том числе следующих:

- Microsoft Office, Excel и InfoPath.
- SAP NetWeaver
- OpenOffice
- Приложения управления бизнес-правилами и -процессами
- Платформы Enterprise Service Bus

2.1.6 Источники данных

2.1.6.1 Юниверсы

При доступе к данным, их обработке и организации юниверс позволяет абстрагироваться от сложности данных посредством использования бизнес-лексики вместо языка данных. Этот бизнес-язык хранится в файле юниверса в виде объектов. В Web Intelligence и Crystal Reports юниверсы используются для того, чтобы упростить для пользователя процесс создания, необходимый для выполнения простых и сложных запросов и анализа пользователями.

Юниверсы являются основным компонентом платформы SAP BusinessObjects Business Intelligence. Все объекты юниверса и соединения защищены и хранятся в центральной репозитории сервера соединений. Для доступа к системе и создания юниверсов средствам создания юниверсов требуется выполнить вход в платформу SAP BusinessObjects Business Intelligence. Доступом к юниверсам и безопасностью на уровне необработанных исходных данных можно управлять на уровне групп и отдельных пользователей в среде проектирования.

Семантический уровень позволяет SAP BusinessObjects Web Intelligence доставлять документы, используя несколько синхронизированных поставщиков данных, включая источники данных OLAP и CWM.

2.1.6.2 Объекты Business View

Средство Business Views упрощает создание отчетов и взаимодействие, абстрагируя сложность данных для разработчиков отчетов. Business Views помогает разделить подключения к данным, доступ к данным, бизнес-элементы и управление доступом.

Средство Business Views может использоваться только с приложением Crystal Reports и предназначено для упрощения доступа к данным и обеспечения безопасности при просмотре, необходимой для создания отчетов Crystal. Business Views поддерживает использование в одном представлении комбинации из нескольких источников данных. В платформе SAP BusinessObjects Business Intelligence полностью поддерживается Business Views.

В состав платформы SAP BusinessObjects Business Intelligence входит ряд специальных предварительно настроенных служб управления платформой, которые предназначены для таких задач, как управление паролями, показатели серверов и управление доступом пользователей к децентрализованным функциям управления.

2.1.7 Языковая поддержка

Продукты платформы SAP BusinessObjects Business Intelligence переведены на многие языки и поддерживают данные на еще большем количестве языков.

Интерфейс продукта доступен на следующих языках:

- чешский
- китайский (упрощенное письмо)
- китайский традиционный
- датский
- голландский
- английский
- финский
- французский
- немецкий
- итальянский
- японский
- корейский
- норвежский (букмол)
- польский
- португальский
- русский
- испанский

- шведский
- тайский

В дополнение к поддержке данных на любых доступных в интерфейсе языках, также поддерживаются следующие наборы символов:

- греческий
- малайский
- иврит
- арабский
- румынский
- вьетнамский
- венгерский
- турецкий
- хинди

2.1.8 Аутентификация и единый вход

Управление безопасностью системы осуществляется при помощи центрального сервера управления (CMS), подключаемых модулей безопасности, а также средств аутентификации сторонних производителей, таких как SiteMinder или Kerberos. Эти компоненты выполняют аутентификацию пользователей и авторизацию их доступа к платформе SAP BusinessObjects Business Intelligence, ее папкам и другим объектам.

Доступны следующие подключаемые модули безопасности сторонних производителей для аутентификации пользователей при едином входе:

- Enterprise (по умолчанию), включая поддержку доверительной аутентификации для сторонней аутентификации.
- LDAP
- Windows Active Directory (AD)

При использовании ERP-системы функция единого входа используется для аутентификации пользователей при входе в ERP-систему, что позволяет вести отчетность по данным ERP. Поддерживается единый вход с аутентификацией для следующих ERP-систем:

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

2.1.8.1 Подключаемые модули безопасности

Подключаемые модули безопасности автоматизируют создание учетных записей и управление ими, позволяя сопоставлять учетные записи пользователей и группы из систем сторонних производителей с платформой SAP BusinessObjects Business Intelligence. Учетные записи и группы из систем сторонних производителей можно сопоставлять существующим учетным записям и группам BusinessObjects Enterprise. Кроме того, можно создавать учетные записи пользователей и группы Enterprise, которые соответствуют каждой из сопоставленных записей внешней системы.

Подключаемые модули безопасности автоматически управляют списками пользователей и групп в системах сторонних производителей. Таким образом, после сопоставления группы Lightweight Directory Access Protocol (LDAP) или Windows Active Directory (AD) с платформой SAP BusinessObjects Business Intelligence все пользователи, относящиеся к этой группе, могут входить в платформу SAP BusinessObjects Business Intelligence. Последующие изменения в членстве в группах сторонних разработчиков распространяются автоматически.

Платформа SAP BusinessObjects Business Intelligence также поддерживает следующие подключаемые модули безопасности:

- Подключаемый модуль безопасности Enterprise

Центральный сервер управления (CMS) ведет обработку таких данных безопасности, как учетные записи пользователей, участие в группах и права доступа к объектам, которые определяют полномочия пользователей и групп. Этот функционал называется аутентификацией Enterprise.

Аутентификация Enterprise всегда включена. Ее нельзя отключить. Аутентификация по умолчанию (Enterprise) используется в том случае, если нужно создать отдельные учетные записи и группы для платформы SAP BusinessObjects Business Intelligence или не создана иерархия пользователей и групп на сервере LDAP либо Windows AD.

Доверительная аутентификация является компонентом аутентификации Enterprise, который интегрируется с решениями единого входа сторонних разработчиков, включая службу аутентификации и авторизации Java (JAAS). Доверительная аутентификация может использоваться для приложений, которые имеют доверительные отношения с сервером центрального управления, чтобы позволить пользователям входить в систему без ввода пароля.

- Подключаемый модуль безопасности LDAP
- Windows AD

Примечание:

Хотя пользователь может настраивать с помощью CMS аутентификацию Windows AD для платформы SAP BusinessObjects Business Intelligence и пользовательских приложений, CMS и стартовая панель BI непосредственно не поддерживают аутентификацию Windows AD с NTLM. Единственными методами аутентификации, поддерживаемыми CMS и стартовой

панелью BI, являются аутентификация Windows AD с Kerberos, LDAP, Enterprise, а также доверительная аутентификация.

2.1.8.2 Интеграция планирования ресурсов предприятия (ERP)

Приложение для планирования ресурсов предприятия (ERP) поддерживает важные функции процессов организации, собирая в режиме реального времени информацию, связанную с повседневными операциями. Платформа SAP BusinessObjects Business Intelligence поддерживает возможности единого входа и составления отчетности для следующих ERP-систем:

- SAP ERP и Business Warehouse (BW)

Примечание:

До использования соединений с OLAP Data Access (ODA), приложения SAP BusinessObjects Analysis (ранее Voyager) или BW должен быть установлен графический интерфейс пользователя SAP.

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

Примечание:

- Поддержка SAP ERP и BW установлена по умолчанию. Чтобы отказаться от поддержки SAP ERP и BW, следует отключить поддержку интеграции при помощи варианта установки Пользовательская / расширенная.
- Поддержка Siebel Enterprise, Oracle E-Business Suite, JD Edwards EnterpriseOne или PeopleSoft не устанавливается по умолчанию. Для выбора и установки интеграции с ERP-системами, отличными от систем SAP, воспользуйтесь вариантом установки «Пользовательская / расширенная».

Для получения подробных сведений о конкретных версиях, поддерживаемых платформой SAP BusinessObjects Business Intelligence, см. документ *Supported Platforms Guide*, доступном по адресу service.sap.com/bosap-support.

Для получения подробных сведений о настройке интеграции ERP см. *Руководство администратора платформы SAP BusinessObjects Business Intelligence*.

2.1.9 Интеграция SAP

Платформа SAP BusinessObjects Business Intelligence интегрируется с существующей инфраструктурой SAP с помощью следующих средств SAP:

- SAP System Landscape Directory (SLD)

Каталог System Landscape Directory в SAP NetWeaver является центральным источником сведений System Landscape, которые соответствуют управлению жизненным циклом. При предоставлении папки, в которой будет собрана информация о всех устанавливаемых программных продуктах, доступных в SAP, и автоматически обновив данные о уже установленных в ландшафте системах, получится основа для поддержки средств планирования заданий жизненного цикла программного обеспечения в системном ландшафте.

Программа установки платформы SAP BusinessObjects Business Intelligence регистрирует имена поставщиков и продуктов, а также их версии с помощью SLD наряду с именами, версиями и расположением внешних компонентов и серверов.

- SAP Solution Manager

SAP Solution Manager – это платформа, которая предоставляет интегрированные инструменты, содержимое и методики для внедрения, поддержки, эксплуатации и отслеживания решений SAP и сторонних производителей в масштабе организации.

Программное обеспечение сторонних разработчиков, обладающее сертификатом на интеграцию с SAP, вносится в центральный репозиторий и автоматически передается в SAP System Landscape Directories (SLD). Клиенты SAP могут легко определить, какие версии интеграции сторонних продуктов были сертифицированы SAP в рамках своей системной среды SAP. Эта служба обеспечивает дополнительную информацию о продуктах сторонних производителей помимо интерактивных каталогов SAP для этих продуктов.

Клиентам SAP бесплатно доступна система SAP Solution Manager, которая обеспечивает прямой доступ к службе поддержки SAP и сведениям о пути обновления продуктов SAP. Для получения дополнительных сведений о SLD см. раздел «Регистрация платформы SAP BusinessObjects Business Intelligence в System Landscape» в *Руководстве администратора платформы SAP BusinessObjects Business Intelligence*.

- Транспорт CTS (CTS+)

Система изменения и транспорта (CTS) помогает организовать проекты разработки в ABAP Workbench и в Customizing, а затем переместить изменения между системами SAP в системном ландшафте. Так же, как и объекты ABAP, в ландшафте можно перемещать объекты Java (J2EE, JEE) и характерные для SAP технологии, не являющиеся технологиями ABAP (такие, как Web Dynpro Java или SAP NetWeaver Portal).

- Мониторинг с использованием CA Wily Introscope

CA Wily Introscope – это продукт для управления веб-приложениями, который дает возможность мониторинга и определения проблем производительности, возникающих в производимых модулях SAP на основе Java, включая видимость в пользовательских приложениях Java и подключение к серверным системам. Это позволяет изолировать слабые места производительности в модулях NetWeaver, включая индивидуальные сервлеты, JSP, EJB, JCO, классы, методы и т.п. Она предлагает производительный мониторинг в реальном времени, непрерывную видимость транзакции, исторические данные для анализа или планирования объема, изменяемые информационные панели, автоматизированные пороговые предупреждения и открытую архитектуру для распространения мониторинга вне сред NetWeaver.

2.1.10 Управление жизненным циклом (LCM)

Управление жизненным циклом (LCM) – это набор процессов, связанных с управлением сведениями о продукте для установки. Здесь устанавливаются процедуры управления установкой платформы SAP BusinessObjects Business Intelligence для сред разработки, тестирования, производства или обслуживания.

Диспетчер жизненного цикла платформы SAP BusinessObjects Business Intelligence представляет собой веб-средство, позволяющее перемещать объекты BI из одной системы в другую, не затрагивая зависимости этих объектов. Помимо этого он делает возможным управление различными версиями, зависимостями, а также возврат в предыдущее состояние объекта, перемещенного на уровень выше.

Средство LCM является подключаемым модулем платформы SAP BusinessObjects Business Intelligence. Объект BI можно передать из одной системы в другую только в том случае, если в исходной и целевой системах установлены одинаковые версии приложения.

Подробнее см. *Руководство пользователя консоли управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence 4.0.*

2.1.11 Интегрированное управление версиями

Для файлов платформы SAP BusinessObjects Business Intelligence в системе сервера теперь поддерживается управление версиями. Программа установки выполнит установку и настройку вспомогательной версии системы контроля версий либо можно ввести сведения вручную для использования существующей системы контроля версий вспомогательной версии или ClearCase.

Система управления версиями позволяет хранить и восстанавливать различные версии конфигурации и других файлов, то есть система всегда может быть возвращена в известное состояние на любой момент времени в прошлом.

2.1.12 постоянные данные

Термин "постоянные данные" относится к любому количеству информации, достаточно важному, чтобы быть перемещенным во время обновления системы. Например, центральный сервер управления (CMS) хранит сведения о конфигурации в базе данных CMS, а не в реестре Windows и не в файле конфигурации.

Постоянные данные всех продуктов платформы SAP BusinessObjects Business Intelligence хранятся в системной базе данных CMC. Это позволяет легко переносить сведения о конфигурации и данных в новую версию при обновлении.

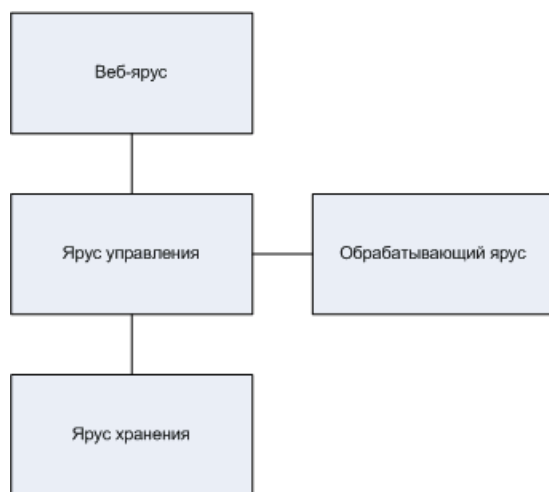
2.1.13 Путь обновления

Существует возможность обновления предыдущей версии платформы SAP BusinessObjects Business Intelligence, однако требуется установить платформу SAP BusinessObjects Business Intelligence 4.0, а затем с помощью средства управления обновлением перенести настройки и данные из существующей системы.

Для получения сведений об обновлении предыдущей версии см. *Руководство по обновлению платформы SAP BusinessObjects Business Intelligence*.

2.2 Концептуальные ярусы

Платформу SAP BusinessObjects Business Intelligence можно представить как последовательность концептуальных ярусов:



- Веб-ярус

Веб-ярус содержит веб-приложения, развернутые на сервере приложений Java. Конечным пользователям веб-приложения предоставляют функции платформы SAP BusinessObjects Business Intelligence через веб-браузер. К примерам веб-приложений относятся веб-интерфейс администрирования консоли CMC и стартовая панель BI.

Веб-ярус включает также веб-службы. Программным средствам веб-службы предоставляют через сервер веб-приложений такие функции платформы SAP BusinessObjects Business Intelligence, как аутентификация сеанса, управление правами пользователей, планирование, поиск, администрирование, составление отчетов и управление запросами. Например, Live Office – это продукт, который использует веб-службы для интеграции отчетности платформы SAP BusinessObjects Business Intelligence в продукты Microsoft Office.

- Ярус управления

Ярус управления координирует и контролирует все компоненты, составляющие платформу SAP BusinessObjects Business Intelligence. Он состоит из центрального сервера управления (CMS) и сервера событий. CMS предоставляет данные безопасности и конфигурации, отправляет служебные запросы серверам, управляет аудитом и ведет системную базу данных CMS. Сервер событий управляет относящимися к файлам событиями, которые возникают в ярусе хранения.

- Обрабатывающий ярус

На ярусе обработки анализируются данные и составляются отчеты. Это единственный ярус, который обращается к базам данных, содержащим данные отчетов.

- Ярус хранения

Ярус хранения предназначен для обработки файлов, таких как документы и отчеты.

Сервер репозитория входных файлов управляет файлами, содержащими данные, которые используются в отчетах. Эти файлы могут иметь следующие расширения: .rpt, .car, .exe, .bat, .js, .xls, .doc, .ppt, .rtf, .txt, .pdf, .wid, .rep, .unv.

Сервер репозитория выходных файлов управляет отчетами, созданными системой. Этим отчетам соответствуют файлы со следующими расширениями: .rpt, .csv, .xls, .doc, .rtf, .txt, .pdf, .wid, .rep.

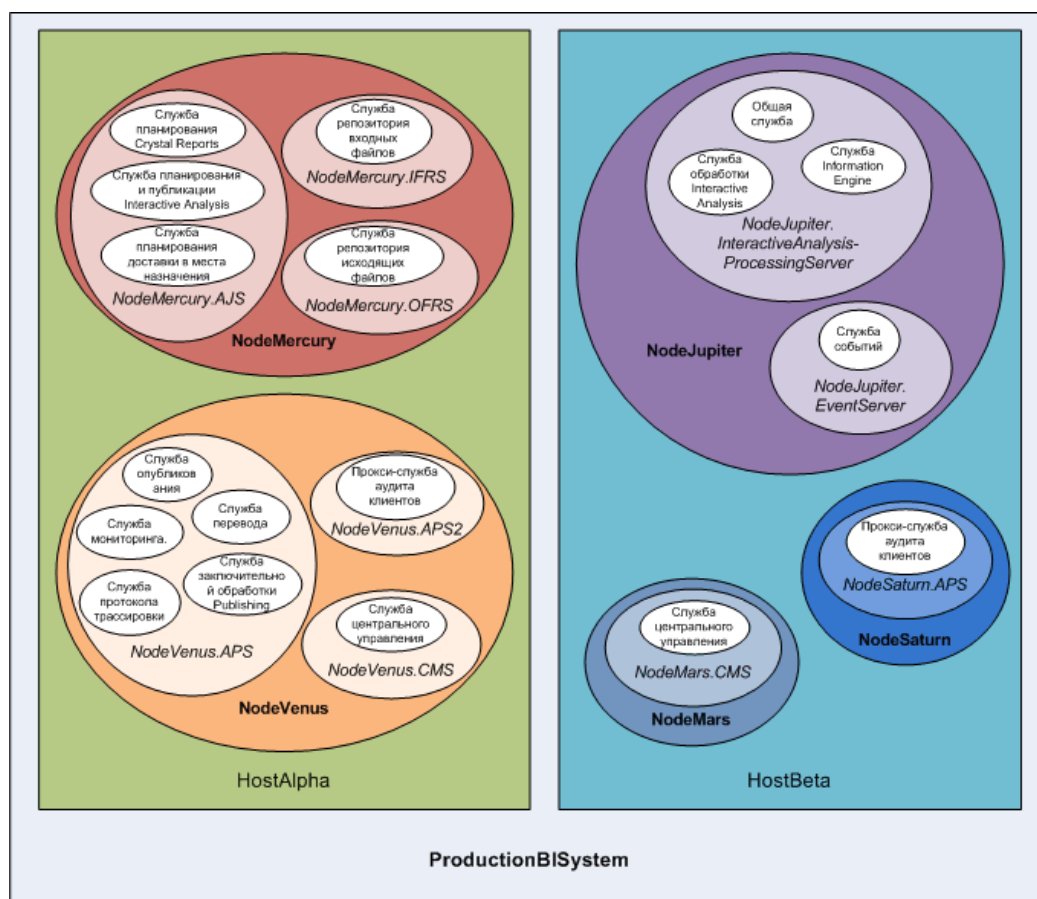
Ярус хранения также обрабатывает кэширование отчетов для экономии системных ресурсов при обращении пользователей к отчетам.

2.3 Службы и серверы

На следующей диаграмме показана возможная установка платформы BI.

Примечание:

Узлы, серверы и службы показаны только для иллюстрации. В реальной установке число хостов, узлов, серверов и служб, а также типы серверов и служб, может отличаться.



Кластер с именем *ProductionBISystem* имеет два хоста.

- На хосте, называемом *HostAlpha*, установлена платформа BI. Для него настроены два узла:
 - *NodeMercury*: содержит адаптивный сервер заданий (*NodeMercury.AJS*) со службами для планирования и публикации отчетов, сервер репозитория входных файлов (*NodeMercury.IFRS*) со службой для хранения входных отчетов и сервер репозитория выходных файлов (*NodeMercury.OFRS*) со службой хранения выходных данных отчета.
 - *NodeVenus*: содержит адаптивный сервер обработки (*NodeVenus.APS*) со службами для функций публикации, мониторинга и перевода, адаптивный сервер обработки (*NodeVenus.APS*) со службой для аудита клиентов, а также Центральный сервер управления (*NodeVenus.CMS*) со службой для CMS.
- На хосте, называемом *HostBeta*, установлена платформа BI. Для него настроены три узла:
 - *NodeMars*: содержит Центральный сервер управления (*NodeMars.CMS*) со службой для CMS.
 - *NodeJupiter*: содержит сервер обработки Web Intelligence (*NodeJupiter.Web Intelligence*) со службой предоставления отчетности Web Intelligence и сервер событий (*NodeJupiter.EventServer*) для мониторинга файлов отчета.
 - *NodeSaturn*: содержит адаптивный сервер обработки (*NodeSaturn.APS*) со службой предоставления аудита клиентов.

В отношении платформы BI термины *сервер* и *служба* означают два типа программного обеспечения, выполняемого на компьютере с установленным программным пакетом платформы BI.

Служба – это серверная подсистема, выполняющая определенные функции. Служба выполняется в памяти сервера под идентификатором процесса родительского контейнера (сервера). Например, служба планирования и публикаций SAP BusinessObjects Web Intelligence представляет собой подсистему, выполняемую на адаптивном сервере заданий.

Термином *сервер* обозначается процесс уровня операционной системы (в некоторых системах он носит название *демон*), в котором размещаются одна или несколько служб. В качестве примера подобного сервера можно привести Центральный сервер управления (CMS) и сервер адаптивной обработки. Сервер запускается под определенной учетной записью операционной системы и обладает собственным идентификатором PID.

Узел – ряд серверов платформы BI, запускаемых на одном хосте. На одном хосте могут размещаться один или несколько узлов.

Платформу BI можно установить на один компьютер, на несколько компьютеров внутренней сети или распределить различные компоненты этого программного пакета в глобальной сети (WAN).

2.3.1 Службы

В следующей ниже таблице описаны все службы.

Таблица 2-1: Службы

Служба	Категория службы	Тип сервера	Описание службы
Служба адаптивного соединения	Службы соединения	Адаптивный сервер обработки	Предоставляет службы подключений (заменяет сервер подключений).
Служба планирования обновления аутентификации	Корневые службы	Адаптивный сервер заданий	Обеспечивает синхронизацию обновлений подключаемых модулей безопасности сторонних разработчиков.

Служба	Категория службы	Тип сервера	Описание службы
Служба веб-приложений ВЕх	Службы соединения	Адаптивный сервер обработки	Обеспечивает интеграцию веб-приложений SAP Business Warehouse (BW) Business Explorer (ВЕх) и стартовой панели BI.
Служба веб-приложения ВОЕ	Корневые службы	Сервер контейнера веб-приложений	Предоставляет веб-приложения для WACS: включает СМС, стартовую панель BI и OpenDocument.
Служба Business Process BI	Корневые службы	Сервер контейнера веб-приложений	Предоставляет веб-службы BI бизнес-процесса для WACS: позволяет встраивать технологию BI в веб-приложения. Служба BI бизнес-процесса исключена.
Служба центрального управления	Корневые службы	Центральный сервер управления	Обеспечивает управление сеансами, пользователями и серверами, а также управление безопасностью (авторизацией и аутентификацией). Для работы кластера в нем должна быть доступна по меньшей мере одна служба центрального управления.
Прокси-служба аудита клиента	Корневые службы	Адаптивный сервер обработки	Осуществляет сбор событий аудита, отправляемых с клиента, и направляет их на сервер CMS.

Служба	Категория службы	Тип сервера	Описание службы
Служба обработки Crystal Reports 2011	Службы Crystal Reports	Сервер обработки Crystal Reports	Принимает и обрабатывает отчеты Crystal Reports 2011; может объединять данные разных отчетов, что сокращает число обращений к базе данных.
Служба планирования Crystal Reports 2011	Службы Crystal Reports	Адаптивный сервер заданий	Выполняет запланированные прежние задания Crystal Reports и публикует результаты в заданном местоположении.
Служба просмотра и изменения Crystal Reports 2011	Службы Crystal Reports	RAS	Сервер приложений отчетов (RAS).
Служба кэша Crystal Reports	Службы Crystal Reports	Кэш-сервер Crystal Reports	Ограничивает число обращений к базе данных из отчетов Crystal и ускоряет создание отчетов посредством управления кэшем отчетов.
Служба обработки Crystal Reports	Службы Crystal Reports	Сервер обработки Crystal Reports	Принимает и обрабатывает отчеты Crystal; может объединять данные для разных отчетов, что сокращает число обращений к базе данных.
Служба планирования Crystal Reports	Службы Crystal Reports	Адаптивный сервер заданий	Выполняет запланированные новые задания Crystal Reports и публикует результаты в заданном местоположении.
Служба доступа к пользовательским данным	Службы соединения	Адаптивный сервер обработки	Обеспечивает динамическое подключение к источникам данных, для которого не требуется сервер подключений.

Служба	Категория службы	Тип сервера	Описание службы
Служба аналитики информационных панелей	Корневые службы	Сервер аналитики информационных панелей	Поддерживает рабочее пространство BI и функциональность модулей для анализа данных.
Служба кэширования Dashboard Design	Службы Dashboard Design	Кэш-сервер Dashboard Design	Ограничивает число обращений к базе данных из отчетов Dashboard Design и ускоряет создание отчетов посредством управления кэшем отчетов.
Служба обработки Dashboard Design	Службы Dashboard Design	Сервер обработки Dashboard Design	Принимает и обрабатывает отчеты Dashboard Design; может объединять данные разных отчетов, что сокращает число обращений к базе данных.
Служба информационных панелей	Корневые службы	Сервер информационных панелей	поддержка рабочего пространства BI
Служба объединения данных	Службы объединения данных	Адаптивный сервер обработки	Служба объединения данных.
Служба планирования доставки в места назначения	Корневые службы	Адаптивный сервер заданий	Выполняет запланированные задания и публикует результаты в заданное местоположение, такое как файловая система, FTP-ресурс, адрес электронной почты или папка входящей почты пользователя.
Служба восстановления документов	Службы Web Intelligence	Сервер адаптивной обработки	Автоматическое сохранение и восстановление документа Web Intelligence.

Служба	Категория службы	Тип сервера	Описание службы
Служба DSL Bridge	Службы Web Intelligence	Адаптивный сервер обработки	Поддержка сеанса двойного семантического слоя (DSL).
Служба событий	Корневые службы	Сервер событий	Отслеживает события файлов на сервере репозитория файлов (FRS) и при необходимости запускает выполнение отчетов.
Служба доступа к данным Excel	Службы соединения	Адаптивный сервер обработки	Поддерживает в качестве источников данных файлы Excel, загруженные в платформу SAP BusinessObjects Business Intelligence.
Служба Information Engine	Службы Web Intelligence	Сервер обработки Web Intelligence	Служба, необходимая для обработки документов Web Intelligence.
Служба хранилища входящих файлов	Корневые службы	Сервер репозитория входящих файлов	Осуществляет ведение объектов опубликованных отчетов и программ, которые могут использоваться для создания новых отчетов, при получении входного файла.
Общая служба Web Intelligence	Службы Web Intelligence	Сервер обработки Web Intelligence	Поддерживает обработку документов Web Intelligence.
Основная служба Web Intelligence	Службы Web Intelligence	Сервер обработки Web Intelligence	Поддерживает обработку документов Web Intelligence.
Служба мониторинга Web Intelligence	Службы Web Intelligence	Сервер адаптивной обработки	Осуществляет мониторинг серверов Web Intelligence.
Служба обработки Web Intelligence	Службы Web Intelligence	Сервер обработки Web Intelligence	Принимает и обрабатывает документы Web Intelligence.

Служба	Категория службы	Тип сервера	Описание службы
Служба планирования Web Intelligence	Службы Web Intelligence	Адаптивный сервер заданий	Обеспечивает поддержку запланированных заданий Web Intelligence.
Служба ClearCase управления жизненным циклом	Службы управления жизненным циклом	Адаптивный сервер обработки	Обеспечивает поддержку ClearCase для управления жизненным циклом.
Служба планирования управления жизненным циклом	Службы управления жизненным циклом	Адаптивный сервер заданий	Выполняет запланированные задания управления жизненным циклом.
Служба управления жизненным циклом	Службы управления жизненным циклом	Адаптивный сервер обработки	Корневая служба управления жизненным циклом.
Служба мониторинга	Корневые службы	Адаптивный сервер обработки	Обеспечивает функции мониторинга.
Служба многомерного анализа	Службы Analysis Services	Сервер адаптивной обработки	Обеспечивает доступ к многомерным OLAP-данным; преобразует необработанные данные в формат XML, который можно затем перенести в кросс-таблицы и диаграммы в Excel, PDF, или Analysis (ранее Voyager).
Служба прямого соединения	Службы соединения	Сервер соединений	Предоставляет службы прямого соединения для 64-битных архитектур.
Служба прямого соединения (32-битная)	Службы соединения	Сервер соединений	Предоставляет службы прямого соединения для 32-битных архитектур.
Служба хранилища выходных файлов	Корневые службы	Сервер репозитория выходных файлов	Осуществляет сбор готовых документов.

Служба	Категория службы	Тип сервера	Описание службы
Служба планирования поиска по платформе	Корневые службы	Адаптивный сервер заданий	Выполняет запланированный поиск для индексации всего содержимого в репозитории CMS.
Служба поиска по платформе	Корневые службы	Адаптивный сервер обработки	Обеспечивает функциональность поиска для платформы BI.
Служба планирования зонда	Корневые службы	Адаптивный сервер заданий	Предоставляет запланированные задания зонда и публикует результаты в заданном выходном местоположении.
Служба планирования программ	Корневые службы	Адаптивный сервер заданий	Выполняет программы, запланированные для выполнения в заданное время.
Служба планирования публикаций	Корневые службы	Адаптивный сервер заданий	Выполняет запланированные задания публикации и публикует результаты в заданном выходном местоположении.
Служба заключительной обработки публикаций	Корневые службы	Адаптивный сервер обработки	Выполняет действия над отчетами после их завершения, например отправку отчета в конкретное выходное местоположение.

Служба	Категория службы	Тип сервера	Описание службы
Служба публикации	Корневые службы	Адаптивный сервер обработки	Осуществляет координацию со службой заключительной обработки публикаций и целевой службой заданий для публикации отчетов в заданном выходном местоположении, например файловой системе, FTP-ресурсе, электронной почте или ящике входящих сообщений пользователя.
Служба Rebean	Службы Web Intelligence	Сервер адаптивной обработки	Пакет SDK, используемый приложениями Web Intelligence и Explorer.
Служба тиражирования	Корневые службы	Адаптивный сервер заданий	Выполняет запланированные задания объединения для репликации содержимого между объединенными узлами.
Служба планирования запросов безопасности	Корневые службы	Адаптивный сервер заданий	Выполняет запланированные задания запросов безопасности
Служба маркера безопасности	Корневые службы	Адаптивный сервер обработки	Поддержка единого входа для SAP
Служба единого входа	Корневые службы	Центральный сервер управления	Поддержка единого входа для Active Directory. Это вспомогательная служба. Она автоматически добавляется в службу центрального управления.
Служба протокола трассировки	Корневые службы	Любой сервер	Поддержка трассировки, протокола и обслуживания

Служба	Категория службы	Тип сервера	Описание службы
Служба преобразований	Корневые службы	Адаптивный сервер обработки	Переводит объекты InfoObject с входными данными из клиента диспетчера переводов.
Служба планирования Visual Difference	Службы управления жизненным циклом	Адаптивный сервер заданий	Выполняет запланированные задания Visual Difference (управление жизненным циклом) и публикует результаты в заданном выходном местоположении.
Служба Visual Difference	Службы управления жизненным циклом	Адаптивный сервер обработки	Определяет, являются ли документы визуально идентичными для перевода документа на уровень выше и управления жизненным циклом.
Служба визуализации	Службы Web Intelligence	Сервер адаптивной обработки	Служба Common Visualization Object Model, используемая приложением Web Intelligence.
Пакет SDK для веб-служб и QaaWS	Корневые службы	Сервер контейнера веб-приложений	Веб-службы на WACS.

Примечание:

В будущих пакетах дополнений платформы SAP BusinessObjects Business Intelligence могут быть добавлены новые типы служб или серверов.

2.3.2 Категории служб

В следующей ниже таблице перечислены все серверы в порядке по категории служб. Описание каждой из служб см. в разделе *Службы*.

Примечание:

В будущих пакетах дополнений платформы SAP BusinessObjects Business Intelligence могут быть добавлены новые типы служб или серверов.

Таблица 2-2: Службы в порядке по категории службы

Категория службы	Служба	Тип сервера
Службы Analysis Services	Веб-служба приложений BEx	Адаптивный сервер обработки
Службы Analysis Services	Служба многомерного анализа	Адаптивный сервер обработки
Службы соединения	Служба адаптивного соединения	Адаптивный сервер обработки
Службы соединения	Служба доступа к пользовательским данным	Адаптивный сервер обработки
Службы соединения	Служба доступа к данным Excel	Адаптивный сервер обработки
Службы соединения	Служба прямого соединения	Сервер соединений
Службы соединения	Служба прямого соединения (32-битная)	Сервер соединений
Корневые службы	Служба планирования обновления аутентификации	Адаптивный сервер заданий
Корневые службы	Служба веб-приложения BOE	Сервер контейнера веб-приложений
Корневые службы	Служба Business Process BI	Сервер контейнера веб-приложений
Корневые службы	Служба центрального управления	Центральный сервер управления
Корневые службы	Прокси-служба аудита клиента	Адаптивный сервер обработки
Корневые службы	Служба аналитики информационных панелей	Сервер аналитики информационных панелей
Корневые службы	Служба информационных панелей	Сервер информационных панелей
Корневые службы	Служба планирования доставки в места назначения	Адаптивный сервер заданий
Корневые службы	Служба событий	Сервер событий

Категория службы	Служба	Тип сервера
Корневые службы	Служба хранилища входящих файлов	Сервер репозитория входящих файлов
Корневые службы	Служба мониторинга	Адаптивный сервер обработки
Корневые службы	Служба хранилища выходных файлов	Сервер репозитория выходных файлов
Корневые службы	Служба планирования поиска по платформе	Адаптивный сервер заданий
Корневые службы	Служба поиска по платформе	Адаптивный сервер обработки
Корневые службы	Служба планирования зонда	Адаптивный сервер заданий
Корневые службы	Служба планирования программ	Адаптивный сервер заданий
Корневые службы	Служба планирования публикаций	Адаптивный сервер заданий
Корневые службы	Служба заключительной обработки публикаций	Адаптивный сервер обработки
Корневые службы	Служба публикации	Адаптивный сервер обработки
Корневые службы	Служба тиражирования	Адаптивный сервер заданий
Корневые службы	Служба планирования запросов безопасности	Адаптивный сервер заданий
Корневые службы	Служба маркера безопасности	Адаптивный сервер обработки
Корневые службы	Служба единого входа	Центральный сервер управления
Корневые службы	Служба протокола трассировки	Любой сервер
Корневые службы	Служба преобразований	Адаптивный сервер обработки
Корневые службы	Пакет SDK для веб-служб и QaaWS	Сервер контейнера веб-приложений
Службы Crystal Reports	Служба обработки Crystal Reports 2011	Сервер обработки Crystal Reports
Службы Crystal Reports	Служба планирования Crystal Reports 2011	Адаптивный сервер заданий

Категория службы	Служба	Тип сервера
Службы Crystal Reports	Служба просмотра и изменения Crystal Reports 2011	RAS
Службы Crystal Reports	Служба кэша Crystal Reports	Кэш-сервер Crystal Reports
Службы Crystal Reports	Служба обработки Crystal Reports	Сервер обработки Crystal Reports
Службы Crystal Reports	Служба планирования Crystal Reports	Адаптивный сервер заданий
Службы Dashboard Design	Служба кэширования Dashboard Design	Кэш-сервер Dashboard Design
Службы Dashboard Design	Служба обработки Dashboard Design	Сервер обработки Dashboard Design
Службы объединения данных	Служба объединения данных	Адаптивный сервер обработки
Службы управления жизненным циклом	служба ClearCase управления жизненным циклом;	Адаптивный сервер обработки
Службы управления жизненным циклом	Служба планирования управления жизненным циклом	Адаптивный сервер заданий
Службы управления жизненным циклом	Служба управления жизненным циклом	Адаптивный сервер обработки
Службы управления жизненным циклом	Служба планирования Visual Difference	Адаптивный сервер заданий
Службы управления жизненным циклом	Служба Visual Difference	Адаптивный сервер обработки
Службы Web Intelligence	Служба восстановления документов	Адаптивный сервер обработки
Службы Web Intelligence	Служба DSL Bridge	Адаптивный сервер обработки
Службы Web Intelligence	Служба Information Engine	Сервер обработки Web Intelligence
Службы Web Intelligence	Служба мониторинга Web Intelligence	Сервер адаптивной обработки
Службы Web Intelligence	Служба Rebean	Адаптивный сервер обработки
Службы Web Intelligence	Служба визуализации	Адаптивный сервер обработки
Службы Web Intelligence	Общая служба Web Intelligence	Сервер обработки Web Intelligence

Категория службы	Служба	Тип сервера
Службы Web Intelligence	Основная служба Web Intelligence	Сервер обработки Web Intelligence
Службы Web Intelligence	Служба обработки Web Intelligence	Сервер обработки Web Intelligence
Службы Web Intelligence	Служба планирования Web Intelligence	Адаптивный сервер заданий

2.3.3 Типы серверов

В следующей ниже таблице перечисляются все серверы в порядке по типу сервера. Описание каждой из служб см. в разделе *Службы*.

Таблица 2-3: Серверы, упорядочены по типу сервера

Тип сервера	Служба	Категория службы
Адаптивный сервер заданий	Служба планирования обновления аутентификации	Корневые службы
Адаптивный сервер заданий	Служба планирования Crystal Reports 2011	Службы Crystal Reports
Адаптивный сервер заданий	Служба планирования Crystal Reports	Службы Crystal Reports
Адаптивный сервер заданий	Служба планирования доставки в места назначения	Корневые службы
Адаптивный сервер заданий	Служба планирования управления жизненным циклом	Службы управления жизненным циклом
Адаптивный сервер заданий	Служба планирования поиска по платформе	Корневые службы
Адаптивный сервер заданий	Служба планирования зонда	Корневые службы
Адаптивный сервер заданий	Служба планирования программ	Корневые службы
Адаптивный сервер заданий	Служба планирования публикаций	Корневые службы

Тип сервера	Служба	Категория службы
Адаптивный сервер заданий	Служба тиражирования	Корневые службы
Адаптивный сервер заданий	Служба планирования запросов безопасности	Корневые службы
Адаптивный сервер заданий	Служба планирования Visual Difference	Службы управления жизненным циклом
Адаптивный сервер заданий	Служба планирования Web Intelligence	Службы Web Intelligence
Адаптивный сервер обработки	Служба адаптивного соединения	Службы соединения
Адаптивный сервер обработки	Веб-служба приложений BEx	Службы Analysis Services
Адаптивный сервер обработки	Прокси-служба аудита клиента	Корневые службы
Адаптивный сервер обработки	Служба доступа к пользовательским данным	Службы соединения
Адаптивный сервер обработки	Служба объединения данных	Службы объединения данных
Адаптивный сервер обработки	Служба восстановления документов	Службы Web Intelligence
Адаптивный сервер обработки	Служба DSL Bridge	Службы Web Intelligence
Адаптивный сервер обработки	Служба доступа к данным Excel	Службы соединения
Адаптивный сервер обработки	Служба мониторинга Web Intelligence	Службы Web Intelligence
Адаптивный сервер обработки	Служба ClearCase управления жизненным циклом	Службы управления жизненным циклом
Адаптивный сервер обработки	Служба консоли управления жизненным циклом	Службы управления жизненным циклом
Адаптивный сервер обработки	Служба мониторинга	Корневые службы
Адаптивный сервер обработки	Служба многомерного анализа	Службы Analysis Services
Адаптивный сервер обработки	Служба поиска по платформе	Корневые службы
Адаптивный сервер обработки	Служба заключительной обработки публикаций	Корневые службы

Тип сервера	Служба	Категория службы
Адаптивный сервер обработки	Служба публикации	Корневые службы
Адаптивный сервер обработки	Служба Rebean	Службы Web Intelligence
Адаптивный сервер обработки	Служба маркера безопасности	Корневые службы
Адаптивный сервер обработки	Служба преобразований	Корневые службы
Адаптивный сервер обработки	Служба Visual Difference	Службы управления жизненным циклом
Адаптивный сервер обработки	Служба визуализации	Службы Web Intelligence
ЛЮБОЙ СЕРВЕР	Служба протокола трассировки	Корневые службы
Центральный сервер управления	Служба центрального управления	Корневые службы
Центральный сервер управления	Служба единого входа	Корневые службы
Сервер соединений	Служба прямого соединения	Службы соединения
Сервер соединений	Служба прямого соединения (32-битная)	Службы соединения
Кэш-сервер Crystal Reports	Служба кэша Crystal Reports	Службы Crystal Reports
Сервер обработки Crystal Reports	Служба обработки Crystal Reports 2011	Службы Crystal Reports
Сервер обработки Crystal Reports	Служба обработки Crystal Reports	Службы Crystal Reports
Сервер аналитики информационных панелей	Служба аналитики информационных панелей	Корневые службы
Кэш-сервер Dashboard Design	Служба кэширования Dashboard Design	Службы Dashboard Design
Сервер обработки Dashboard Design	Служба обработки Dashboard Design	Службы Dashboard Design
Сервер информационных панелей	Служба информационных панелей	Корневые службы
Сервер событий	Служба событий	Корневые службы
Сервер репозитория входящих файлов	Служба хранилища входящих файлов	Корневые службы

Тип сервера	Служба	Категория службы
Сервер репозитория выходных файлов	Служба хранилища выходных файлов	Корневые службы
RAS	Служба просмотра и изменения Crystal Reports 2011	Службы Crystal Reports
Сервер контейнера веб-приложений	Служба веб-приложения BOE	Корневые службы
Сервер контейнера веб-приложений	Служба Business Process BI	Корневые службы
Сервер контейнера веб-приложений	Пакет SDK для веб-служб и QaaWS	Корневые службы
Сервер обработки Web Intelligence	Служба Information Engine	Службы Web Intelligence
Сервер обработки Web Intelligence	Общая служба Web Intelligence	Службы Web Intelligence
Сервер обработки Web Intelligence	Основная служба Web Intelligence	Службы Web Intelligence
Сервер обработки Web Intelligence	Служба обработки Web Intelligence	Службы Web Intelligence

2.3.4 Серверы

Серверы представляют собой наборы служб, выполняемых на хосте под управлением Server Intelligence Agent (SIA). Тип сервера определяется выполняемыми на нем службами. Серверы могут создаваться в Central Management Console (CMC). В следующей ниже таблице перечисляются различные типы серверов, которые могут быть созданы в CMC.

Сервер	Описание
Адаптивный сервер заданий	<p>Общий сервер, на котором осуществляется обработка запланированных заданий. При добавлении сервера заданий в платформу SAP BusinessObjects Business Intelligence можно настроить на сервере заданий обработку отчетов, документов, программ или публикаций, а также отправку результатов в различные места назначения.</p>
Адаптивный сервер обработки	<p>Общий сервер, на котором находятся службы, отвечающие за обработку запросов из различных источников.</p> <p>Примечание:</p> <p>Программа установки устанавливает один адаптивный сервер обработки в системе хоста. В зависимости от установленных функций на этом адаптивном сервере обработки может размещаться большое количество служб, например служба мониторинга, служба управления жизненным циклом, служба многомерного анализа (MDAS), служба публикации и другие.</p> <p>При установке производственной среды не следует использовать адаптивный сервер обработки по умолчанию. Вместо этого настоятельно рекомендуется по завершении процесса установки выполнить масштабирование системы для определения следующего:</p> <ul style="list-style-type: none"> • Тип и количество служб адаптивного сервера обработки. • Распределение служб по нескольким адаптивным серверам обработки. • Оптимальное количество адаптивных серверов обработки. Наличие нескольких серверов обеспечивает дублирование функций, повышенную производительность, а также более высокую надежность. • Распределение адаптивных серверов обработки по нескольким узлам. <p>Создайте новые экземпляры адаптивных серверов обработки в соответствии с условиями процесса масштабирования.</p> <p>Например, если в результате процесса масштабирования предполагается создание по одному адаптивному серверу обработки для каждой категории служб, это может обусловить создание восьми адаптивных серверов обработки. По одному для каждой из следующих категорий служб: службы Analysis Services, службы соединений, основные службы, службы Crystal Reports, службы Dashboard Design, службы объединения данных, службы управления жизненным циклом и службы Web Intelligence.</p>
Центральный сервер управления (CMS)	

Сервер	Описание
	Обслуживает базу данных о платформе SAP BusinessObjects Business Intelligence (в системной базе данных CMS) и проверяемых действиях пользователя (в хранилище данных аудита). Сервер CMS управляет всеми службами платформы. Сервер CMS также управляет доступом к системным файлам, где хранятся документы, а также сведения о пользователях, группах пользователей, уровнях безопасности (включая аутентификацию и авторизацию), а также содержимое.
Сервер соединений	Обеспечивает доступ базы данных к исходным данными. Поддерживает реляционные базы данных, а также OLAP и другие форматы. Сервер соединений отвечает за обработку соединений и взаимодействие с различными источниками данных, а также предоставление клиентам типичного набора функций.
Кэш-сервер Crystal Reports	Перехватывает запросы на отчет, отправленные клиентами на сервер страниц. Если кэш-сервер не может выполнить запрос с использованием кэшированной страницы отчета, он передает запрос серверу обработки Crystal Reports, который создает отчет и возвращает результаты. После этого кэш-сервер кэширует страницу отчета для возможного использования в будущем.
Сервер обработки Crystal Reports	Отвечает на запросы страниц путем обработки отчетов и создания страниц в формате инкапсулированной страницы (EPF). Основное преимущество формата EPF заключается в поддержке доступа к страницам по требованию, поэтому вместо возврата всего отчета передается запрошенная страница. Это повышает производительность системы и снижает потребление трафика для больших отчетов.
Сервер аналитики информационных панелей	Процесс сервера, используемый компонентом рабочего пространства BI для создания и работы с корпоративным и личным модулем рабочего пространства BI.
Сервер информационных панелей	Используется компонентом рабочих пространств BI для создания и работы с корпоративными и личными информационными панелями. Рабочие пространства BI предлагают возможности управления информационными панелями, чтобы помочь организациям отслеживать и понимать свои бизнес-операции
Кэш-сервер Dashboard Design	Перехватывает запросы на отчет, отправленные клиентами на сервер информационных панелей. Если кэш-сервер не может обработать запрос с использованием кэшированной страницы отчета, он передает запрос серверу информационных панелей, который создает отчет и возвращает результаты. После этого кэш-сервер кэширует страницу отчета для возможного использования в будущем.

Сервер	Описание
Сервер обработки Dashboard Design	Отвечает на запросы Dashboard Design путем обработки отчетов и создания страниц в формате инкапсулированной страницы (EPF). Основное преимущество формата EPF заключается в поддержке доступа к страницам по требованию, поэтому вместо возврата всего отчета передается запрошенная страница. Это повышает производительность системы и снижает потребление трафика для больших отчетов.
Сервер событий	Проверяет наличие в системе событий, которые могут инициировать выполнение отчета. После настройки события-инициатора сервер событий отслеживает соответствующее условие и уведомляет CMS о событии на базе файла. Затем CMS запускает все задания, которые связаны с событием.
Сервер репозитория файлов	Отвечают за создание объектов файловой системы, таких, как экспортируемые отчеты и импортируемые файлы в сторонних форматах. На сервере репозитория входящих файлов хранятся объекты отчетов и программ, которые были опубликованы в системе администраторами и конечными пользователями. На сервере репозитория исходящих файлов хранятся все экземпляры отчетов, созданные на сервере заданий.
Сервер обработки Web Intelligence	Обрабатывает документы SAP BusinessObjects Web Intelligence.
Сервер приложений отчетов	Предоставляет возможность прямого составления отчетов, благодаря чему пользователи могут создавать и изменять отчеты Crystal посредством пакета (SDK) SAP Crystal Reports Server Embedded.

2.4 Клиентские приложения

Взаимодействие с платформой SAP BusinessObjects Business Intelligence осуществляется с помощью приложений для настольных систем двух разных типов:

- Приложения для рабочих станций

Эти приложения должны быть установлены в поддерживаемой операционной системе Microsoft Windows и иметь возможность обрабатывать данные и создавать отчеты в локальной системе.

Примечание:

Программа установки платформы SAP BusinessObjects Business Intelligence в настоящее время не устанавливает приложения для настольных систем. Для установки настольных приложений на сервере воспользуйтесь автономной программой установки средств клиента платформы SAP BusinessObjects Business Intelligence.

Клиенты настольных систем позволяют переносить обработку некоторых отчетов BI на отдельные клиентские компьютеры. Большинство приложений для настольных систем обращается к данным организации через драйверы, установленные на компьютере, а обмен данными с разворачиванием платформы SAP BusinessObjects Business Intelligence осуществляется с использованием архитектуры CORBA или CORBA с шифрованием SSL.

Примеры приложений этого типа: Crystal Reports и Live Office.

Примечание:

Хотя Live Office является полнофункциональным приложением, обмен данными с веб-службами платформы SAP BusinessObjects Business Intelligence в нем ведется по протоколу HTTP.

- Веб-приложения

Эти приложения размещаются на сервере веб-приложений, и доступ к ним осуществляется через веб-браузеры операционных систем Windows, Macintosh, Unix и Linux.

Такой подход позволяет обеспечить доступ к Business Intelligence (BI) большим группам пользователей без необходимости разворачивания ПО на рабочих станциях. Обмен данными осуществляется по протоколу HTTP с шифрованием SSL или без него (HTTPS).

Примеры приложений этого типа: стартовая панель BI, SAP BusinessObjects Web Intelligence, Central Management Console (CMC) и средства просмотра отчетов.

2.4.1 Устанавливается вместе со средствами клиента платформы SAP BusinessObjects Business Intelligence

2.4.1.1 Web Intelligence Desktop

Web Intelligence Desktop – это средство специального анализа и составления отчетов для пользователей с доступом или без доступа к платформе SAP BusinessObjects Business Intelligence.

Это позволяет им обращаться к данным из реляционных источников, OLAP, электронных таблиц или текстовых файлов, а также комбинировать такие данные с использованием привычных бизнес-терминов в графическом интерфейсе. Рабочие процессы позволяют анализировать очень широкие или узкие вопросы, а также ставить уточняющие вопросы на любом этапе рабочего процесса анализа.

Пользователи Web Intelligence Desktop могут продолжать работать с файлами документов Web Intelligence (.wid) даже тогда, когда не могут подключиться к центральному серверу управления (CMS).

2.4.1.2 Диспетчер Business View

Диспетчер Business View позволяет пользователям создавать объекты семантического уровня, упрощающие сложность основной базы данных.

Диспетчер Business View может создавать соединения данных, соединения динамических данных, основания данных, бизнес-элементы, бизнес-представления, а также реляционные представления. Это также дает возможность задать подробные параметры безопасности уровня столбца и строки для объектов в отчете.

Разработчики могут создавать подключения к нескольким источникам данных, объединить таблицы, создать псевдонимы полей и поля вычислений, а затем использовать получившуюся упрощенную структуру в качестве Business View. Создатели отчетов и пользователи могут затем использовать бизнес-представление как основу для своих отчетов, им не придется создавать собственные запросы напрямую из данных.

2.4.1.3 Средство преобразования отчетов

Средство преобразования отчетов преобразует отчеты в формат Web Intelligence и публикует их на центральном сервере управления (CMS).

Отчеты можно получить из папок CMS *Общие*, *Избранное* или *Входящие*. После преобразования отчеты публикуются в папку, в которой находится исходный отчет Web Intelligence, или в любую другую. Это средство преобразует не все функции и отчеты Web Intelligence. Уровень преобразования зависит от свойств и позиций исходного отчета. Некоторые свойства защищают отчет от преобразования. Другие свойства могут изменяться, переустанавливаться или удаляться с помощью средства.

Кроме того, средство преобразования отчетов позволяет выполнять аудит преобразованных отчетов. Это помогает выявлять отчеты, которые не удается полностью преобразовать с помощью средства преобразования отчетов, а также узнать причину этого.

2.4.1.4 Средство создания юниверсов

Средство создания юниверсов (ранее Universe Designer) позволяет разработчикам данных объединять данные из нескольких источников в семантический уровень, скрывающий сложность базы данных от конечных пользователей. Он позволяет абстрагироваться от сложности данных

путем использования деловой лексики вместо технической для организации данных и доступа к ним, а также для управления данными.

Средство создания юниверсов предоставляет графический интерфейс, с помощью которого можно выбирать и просматривать таблицы базы данных. Таблицы базы данных представлены в виде названий таблиц в схеме диаграммы. Этот интерфейс может быть использован разработчиками для управления таблицами, создания объединений, связывающих таблицы, создания псевдонимов таблиц, контекстов и циклов решения в схеме.

Юниверсы также можно создать из других источников метаданных. Средство создания юниверсов используется для создания юниверса на конечном этапе создания.

2.4.1.5 Средство запросов веб-служб

Средство запросов веб-служб (ранее Query as a Web Service) позволяет использовать запросы BI в пользовательских веб-приложениях. Пользователи создают запросы из соединения юниверса и публикуют их в виде веб-службы; таким образом, их можно встроить в веб-приложение.

Средство запросов веб-служб предоставляет новые клиентские решения для бизнеса. Например, это позволяет SAP BusinessObjects Dashboard Design (ранее Xcelsius) объединять разнообразные источники несопоставимых данных в достоверном представлении BI.

Средство запросов веб-служб работает с широким диапазоном решений клиентской стороны и средств, например:

- Microsoft Office, Excel и InfoPath.
- SAP NetWeaver
- OpenOffice
- Приложения управления бизнес-правилами и процессами
- Службы Enterprise

2.4.1.6 Средство дизайна информации

Средство дизайна информации (ранее дизайнер информации) – это среда для проектирования метаданных SAP BusinessObjects, позволяющая разработчику извлекать и определять метаданные из реляционных и OLAP-источников, а также управлять ими при создании и развертывании юниверсов SAP BusinessObjects.

2.4.1.7 Средство управления переводами

Платформа SAP BusinessObjects Business Intelligence обеспечивает поддержку многоязычных документов и юниверсов. Документ на нескольких языках содержит локализованные версии запросов на метаданные юниверса и документы. Пользователь может создавать отчеты, например, из одного юниверса в выбранные языки.

Средство управления переводами (ранее "Диспетчер переводов") определяет юниверсы на нескольких языках и управляет переводом юниверсов, их документов и запросов на ввод Web Intelligence.

Средство управления переводами

- Переводит документы юниверса или SAP BusinessObjects Web Intelligence для многоязычной аудитории.
- Определяет части языка метаданных документа и правильный перевод. Создает внешний формат XLIFF и импортирует XLIFF-файлы для получения переведенной информации.
- Указывает структуру переводимого документа юниверса или SAP BusinessObjects Web Intelligence.
- Позволяет переводить метаданные посредством пользовательского интерфейса или с помощью внешнего средства перевода, импортируя и экспортируя файлы XLIFF.
- Создает многоязычные документы.

2.4.1.8 Средство администрирования объединения данных

Средство администрирования объединения данных (ранее Data Federator) – это полнофункциональное клиентское приложение, обеспечивающее использование удобных функций управления службой объединения данных.

Тесная интеграция службы объединения данных с платформой SAP BusinessObjects Business Intelligence позволяет работать с юниверсами с несколькими источниками за счет распределения запросов между разрозненными источниками данных. Такая интеграция позволяет объединять данные с помощью единого основания данных.

Средство администрирования объединения данных позволяет оптимизировать запросы на объединение данных и точно настроить подсистему запросов на объединение данных для обеспечения максимально возможной производительности.

Средство администрирования объединения данных используется для выполнения следующих задач.

- Проверка SQL-запросов.

- Визуализация планов оптимизации, в которых подробно описывается распределение объединенных запросов для каждого источника.
- Сбор «статистики» и установка системных параметров для точной настройки служб объединения данных и обеспечения максимально возможной производительности.
- Управление свойствами, определяющими порядок выполнения запросов в каждом источнике данных на уровне коннектора.
- Отслеживание выполнения SQL-запросов.
- Просмотр журнала выполненных запросов.

2.4.1.9 Виджеты для платформы SAP BusinessObjects Business Intelligence

Виджеты обеспечивают несложный и быстрый доступ к часто используемым функциям и предоставляют визуальные сведения на рабочем столе. Виджеты для платформы SAP BusinessObjects Business Intelligence (ранее BI Widgets) позволяют организации обеспечить доступ к существующему содержимому BI в платформе SAP BusinessObjects Business Intelligence. Можно также добавить на сервер приложений SAP NetWeaver приложения Web Dynpro, зарегистрированные как XBCML-виджеты, в качестве виджетов настольных систем. (Альтернатива: Можно также добавить в качестве виджетов настольных систем приложения Web Dynpro, зарегистрированные в качестве XBCML-виджетов на сервере приложений SAP NetWeaver)

Для отображения XBCML-виджетов на пользовательском настольном компьютере используется клиент SAP Web Dynpro Flex Client. Клиент SAP Web Dynpro Flex Client основан на Adobe Flex и используется для визуализации виджетов. Для получения сведений о настройке приложений Web Dynpro см. раздел *Включение виджетов на сервере приложений SAP NetWeaver* в *Объекты виджетов для руководства пользователя SAP BusinessObjects*.

Примечание:

Поддержка XBCML-виджетов в клиенте SAP Web Dynpro Flex Client реализована с версии 7.0 EhP2 SP3. Поддержка очереди в Flex Client ограничена проблемами Flex Client, обнаруженными в XBCML-виджетах в этих указанных версиях.

С помощью виджетов для платформы SAP BusinessObjects Business Intelligence можно искать и просматривать существующее содержимое, такое как документы Web Intelligence, модели Dashboard Design и приложения Web Dynpro, а также копировать информацию на рабочий стол для удобства работы с ней.

Использование содержимого в виде виджета дает возможность применять следующие функции платформы виджетов:

- Управляемые пользователем размер и положение
- Автоматическое обновление
- Дополнительная настройка в качестве верхнего окна приложения
- Полная безопасность платформы SAP BusinessObjects Business Intelligence (только части отчетов Web Intelligence и модели дизайнера информационных панелей)

- Сохранение режима отображения
- Сохранение состояния контекста данных (только для частей отчета Web Intelligence)
- Ссылки Web Intelligence OpenDocument на подробные отчеты (только документы Web Intelligence)
- Табличные представления (только модели Dashboard Design)

2.4.2 Устанавливается вместе с платформой SAP BusinessObjects Business Intelligence

2.4.2.1 Central Configuration Manager (CCM)

Central Configuration Manager (CCM) – это средство устранения неполадок серверов и управления узлами, доступное в двух видах: В среде Microsoft Windows CCM позволяет управлять локальными и удаленными серверами с помощью графического пользовательского интерфейса или командной строки. В среде UNIX скрипт оболочки CCM (ccm.sh) позволяет управлять серверами из командной строки.

С помощью CCM можно создавать и настраивать узлы Server Intelligence Agent (SIA), а также запускать или останавливать работу сервера веб-приложений. В Windows с помощью данного приложения также можно изменять параметры сети (например, параметры шифрования SSL). Эти параметры применяются ко всем серверам в пределах узла.

Примечание:

В настоящее время большинство задач по управлению серверами выполняются посредством CMC, а не CCM. Сейчас CCM используется для устранения неполадок и настройки узлов.

2.4.2.2 Средство управления обновлением

Средство управления обновлением (ранее мастер импорта) устанавливается как часть платформы BI и используется как вспомогательное средство для администраторов при выполнении процедур импорта пользователей, групп и папок из предыдущих версий платформы BI. Это также дает возможность импортировать и обновлять объекты, события, группы серверов, объекты репозитория и календари.

Для получения сведений об обновлении с предыдущей версии платформы BI см. *Руководство по обновлению SAP BusinessObjects Business Intelligence*.

2.4.2.3 Repository Diagnostic Tool

Repository Diagnostic Tool (RDT) может выполнять сканирование, диагностику и устранение несоответствий, которые могут возникать между системной базой данных центрального сервера управления (CMS) и файловым хранилищем серверов репозитория файлов (FRS).

Оно также может сообщать о статусе исправления и завершенных действиях. После первого выполнения горячего резервного копирования следует использовать RDT для определения синхронизации между файловой системой и базой данных. Также можно использовать его после восстановления и перед запуском служб платформы SAP BusinessObjects Business Intelligence. Пользователь может устанавливать предельное количество ошибок, которые RDT находит и исправляет перед тем, как остановить работу.

2.4.3 Доступно отдельно

2.4.3.1 SAP BusinessObjects Analysis, выпуск для Microsoft Office

SAP BusinessObjects Analysis, выпуск для Microsoft Office, – это альтернатива бизнес-класса для решения Business Explorer (BEx), с помощью которой бизнес-аналитики могут исследовать многомерные данные OLAP.

Аналитики могут быстро получать ответы на ключевые бизнес-вопросы и обмениваться результатами и рабочими пространствами с другими пользователями в формате *анализа*.

SAP BusinessObjects Analysis, выпуск для Microsoft Office, дает аналитикам следующие возможности:

- Мониторинг трендов, отклонений и подробных данных, хранящихся в финансовых системах, без помощи администратора базы данных.
- Получение эффективных ответов на бизнес-вопросы при просмотре крупных или небольших наборов многомерных данных.
- Доступ ко всему диапазону источников OLAP-данных, доступных в организации, и распространение результатов посредством понятного и наглядного интерфейса.
- Доступ к различным OLAP-источникам в одном анализе для получения комплексной картины бизнеса и информации о возможном взаимовлиянии направлений.
- Выявление, анализ, сравнение и прогнозирование критичных бизнес-факторов.
- Использование комплексного диапазона вычислений, связанных с бизнесом и временем.

2.4.3.2 SAP Crystal Reports

Программное обеспечение SAP Crystal Reports позволяет пользователям разрабатывать интерактивные отчеты по источнику данных.

2.4.3.3 SAP BusinessObjects Dashboard Design

SAP BusinessObjects Dashboard Design (ранее Xcelsius) представляет собой средство для визуализации данных и создания динамических интерактивных информационных панелей. Данные и формулы импортируются или вводятся напрямую во встроенную таблицу Microsoft Excel. Flash-интерфейс предоставляет основу, которая отображает разнообразные аналитики и информационные панели.

Доступно динамическое обновление данных из платформы SAP BusinessObjects Business Intelligence, а также их экспорт в различные стандартные форматы, например PowerPoint, PDF или Flash, в которых их смогут просмотреть потребители данных.

2.4.3.4 SAP BusinessObjects Explorer

SAP BusinessObjects Explorer – это приложение, использующее мощные возможности поиска данных и позволяющее быстро и точно получать ответы на поставленные бизнес-вопросы на основе корпоративных данных.

При установке SAP BusinessObjects Explorer в Central Configuration Manager (CCM) и Central Management Console (CMC) платформы SAP BusinessObjects Business Intelligence добавляются следующие серверы:

- Основной сервер Explorer: осуществляет управление всеми серверами Explorer.
- Сервер индексации Explorer: управляет индексированием данных и метаданных в информационных пространствах и предоставляет необходимые для этого средства.
- Поисковый сервер Explorer: обрабатывает поисковые запросы и возвращает результаты поиска.
- Исследовательский сервер Explorer: обеспечивает функцию исследования информационных пространств и управляет этим процессом, поддерживает функции анализа, включая поиск данных, фильтрацию и агрегирование.

2.4.4 Клиенты веб-приложений

Клиенты веб-приложений находятся на сервере веб-приложений, доступ к ним осуществляется на клиентском компьютере с использованием веб-браузера. Веб-приложения автоматически развертываются при установке платформы SAP BusinessObjects Business Intelligence.

Веб-приложения легко доступны пользователям через интернет-браузер, а обмен данными можно зашифровать с помощью SSL, если планируется разрешить пользователям доступ извне корпоративной сети.

Веб-приложения Java также можно перенастроить или развернуть после первичной установки с помощью связанного средства командной строки WDeploy, позволяющего двумя способами развертывать веб-приложения на сервере веб-приложений:

1. Автономный режим

Все ресурсы веб-приложения разворачиваются на сервере веб-приложений, который обслуживает динамическое и статическое содержимое. Данное упорядочивание подходит для небольших установок.

2. Режим разделения

Статическое содержимое веб-приложения (HTML, изображения, CSS) развертывается на выделенный веб-сервер, в то время как динамическое содержимое (JSP) развертывается на сервер веб-приложения. Это упорядочивание подходит для более крупных установок, для которых освобождение сервера веб-приложений от обслуживания статического веб-содержимого станет преимуществом.

Для получения дополнительных сведений о WDeploy см. *Руководство по развертыванию веб-приложений платформы SAP BusinessObjects Business Intelligence*.

2.4.4.1 Central Management Console (CMC)

Central Management Console (CMC) – это веб-инструмент, с помощью которого можно выполнять задачи администрирования, включая управление пользователями, содержимым и серверами. Это также позволяет публиковать, организовывать и настраивать параметры безопасности. Поскольку CMC является веб-приложением, все вышеупомянутые административные задачи можно выполнять посредством веб-браузера на любом компьютере, который может подключиться к серверу.

Все пользователи могут входить в CMC для изменения предпочтений. Только члены группы *Администраторы* могут изменять параметры управления, если другим пользователям явно не

предоставлены для этого права. В СМС также можно назначить роли, это даст некоторым пользователям права на выполнение мелких административных заданий

2.4.4.2 стартовая панель BI

Стартовая панель BI (ранее InfoView) представляет собой веб-интерфейс, используемый конечными пользователями для просмотра, планирования и отслеживания опубликованных отчетов BI. Стартовая панель BI может получать доступ к любым типам бизнес-логики, взаимодействовать с ними и экспортировать их. Это могут быть отчеты, аналитики, информационные панели, карты балльных оценок и схемы стратегий.

Стартовая панель BI позволяет осуществлять:

- Просмотр и поиск в каталоге Business Intelligence.
- Доступ к содержимому Business Intelligence (создание, редактирование и просмотр).
- Планирование и публикация содержимого Business Intelligence.

2.4.4.3 Рабочие пространства BI

Рабочие пространства BI (ранее Dashboard Builder) позволяют отслеживать бизнес-операции и производительность с использованием модулей (шаблонов для данных) и рабочих пространств BI (просматривая данные в одном или нескольких модулях). Модули и рабочие пространства BI предоставляют данные, необходимые для настройки бизнес-правил при изменении условий. Это позволяет отслеживать и анализировать ключевые бизнес-данные посредством управления рабочими пространствами BI и модулями. Это также обеспечивает поддержку группового принятия решений и анализа посредством возможностей интегрированного сотрудничества и рабочих процессов. В рабочих пространствах BI доступны следующие функции:

- Обзор с использованием вкладок
- Создание страницы: "Управление рабочими пространствами и модулями BI"
- Средство построения приложения с помощью мыши
- Связывание содержимого между модулями для детализированного анализа данных

Примечание:

Для использования функций рабочих пространств BI необходимо приобрести лицензию платформы SAP BusinessObjects Business Intelligence, в рамках которой предусматривается использование рабочих пространств BI.

2.4.4.4 Средства просмотра отчетов

Средства просмотра отчетов поддерживают различные платформы и различные браузеры, и попадают в одну из двух категорий:

- Клиентские средства просмотра (средство просмотра Active X, средство просмотра Java)

Клиентские средства просмотра отчетов загружаются и устанавливаются в браузер клиента. Когда пользователь запрашивает отчет, сервер приложений обрабатывает запрос и получает страницы отчета из платформы SAP BusinessObjects Business Intelligence. Затем сервер веб-приложений передает страницы отчета клиентскому средству просмотра, которое обрабатывает страницы отчета и отображает их в браузере.

- Средства просмотра отчетов, не требующие дополнительного ПО (средство просмотра DHTML)

Средства просмотра отчетов, не требующие дополнительного ПО, находятся на сервере веб-приложений. Когда пользователь запрашивает отчет, сервер веб-приложений получает страницы отчета из платформы SAP BusinessObjects Business Intelligence и создает страницы DHTML, которые отображаются в веб-браузере.

Все запросы на отчеты от средства просмотра отчетов и страницы текущих отчетов, отображаемые в интернет-браузере.

Для получения дополнительных сведений о конкретных функциях или поддержке платформ в каждом из средств просмотра отчета см. *Руководство пользователя по стартовой панели BI*, руководство *Report Application Server .NET SDK Developer Guide* или *Руководство разработчика средств просмотра Java*.

2.4.4.5 SAP BusinessObjects Web Intelligence

SAP BusinessObjects Web Intelligence – это инструментальное средство на базе веб-интерфейса для работы с запросами, отчетами, а также для проведения анализа реляционных источников данных посредством одного продукта на базе веб-интерфейса.

Это позволяет пользователям создавать отчеты, выполнять специальные запросы, анализировать данные и форматировать отчеты, используя интерфейс перетаскивания. Благодаря Web Intelligence сложность источников данных нижнего уровня остается незамеченной для пользователя.

Отчеты можно публиковать на поддерживаемом веб-портале или в приложениях Microsoft Office с помощью SAP BusinessObjects Live Office.

2.4.4.6 SAP BusinessObjects Analysis, выпуск OLAP

Приложение SAP BusinessObjects Analysis, выпуск для OLAP, (ранее Voyager) представляет собой инструмент интерактивной аналитической обработки (OLAP) в стартовой панели BI и предназначено для работы с многомерными данными. Также можно комбинировать информацию из разных источников данных OLAP в одном рабочем пространстве. К поддерживаемым поставщикам OLAP относятся SAP BW и службы Microsoft Analysis Services.

Набор функций Analysis OLAP сочетает элементы SAP Crystal Reports (прямой доступ к данным OLAP-кубов для составления отчетов о производстве) и решения SAP BusinessObjects Web Intelligence (создание разовой аналитической отчетности по юниверсам из источников данных OLAP). Обеспечивает набор бизнес-вычислений и подсчета времени, а также содержит такие функции, как регуляторы времени, которые позволяют упростить анализ данных OLAP до предела.

Примечание:

Веб-приложение Analysis, выпуск для OLAP, доступно только как веб-приложение Java. Соответствующее приложение для платформы .NET отсутствует.

2.4.4.7 SAP BusinessObjects Mobile

SAP BusinessObjects Mobile дает пользователям возможность осуществлять удаленный доступ к отчетам Business Intelligence (BI), показателям и данным в реальном времени, доступным на клиентских компьютерах, с помощью беспроводных устройств. Содержимое оптимизировано для мобильных устройств, таким образом можно с легкостью использовать знакомые отчеты, переходить по ним и анализировать их без дополнительного обучения.

Благодаря SAP BusinessObjects Mobile специалисты, работающие с информацией, и администраторы будут всегда иметь самые свежие данные и смогут использовать их при принятии решений. Торговый персонал и персонал по обслуживанию на месте продажи может предоставить нужного покупателя, продукт и сведения о порядке работы где и когда необходимо.

SAP BusinessObjects Mobile поддерживает широкий диапазон мобильных устройств, таких как BlackBerry, Windows Mobile и Symbian.

Для получения дополнительных сведений об установке, настройке и развертывании мобильных продуктов см. *Руководстве по установке и развертыванию SAP BusinessObjects Mobile*. Для получения сведений об использовании SAP BusinessObjects Mobile см. *Руководство по использованию SAP BusinessObjects Mobile*.

2.5 Потоки информации

При выполнении задач в платформе SAP BusinessObjects Business Intelligence (например, входа в систему, внесения отчета в расписание или просмотра отчета) информация передается по системе, и происходит взаимодействие между серверами. В следующем разделе изложены принципы выполнения некоторых процессов в системе платформы SAP BusinessObjects Business Intelligence.

2.5.1 Аутентификация

2.5.1.1 Вход в платформу SAP BusinessObjects Business Intelligence

Данный рабочий процесс описывает вход пользователя в платформу SAP BusinessObjects Business Intelligence из веб-браузера.

1. Браузер направляет запрос на вход в систему через веб-сервер на сервер веб-приложений.
2. Сервер веб-приложений определяет, что целью данного запроса является вход в систему. Сервер веб-приложений направляет имя пользователя, пароль и данные о типе аутентификации на указанный CMS для выполнения аутентификации.
3. CMS проверяет имя пользователя и пароль по соответствующей базе данных (в данном случае используется аутентификация Enterprise и выполняется аутентификация учетных данных пользователя по базе данных системы CMS).
4. После подтверждения CMS создает сеанс для пользователя в памяти.
5. CMS направляет ответ на сервер веб-приложений с информацией о том, что подтверждение выполнено успешно. Сервер веб-приложений создает маркер входа для сеанса пользователя в памяти. Для оставшейся части данного сеанса сервер веб-приложений использует маркер входа для подтверждения пользователя на CMS.
6. Сервер веб-приложений генерирует HTML-страницу для отправки клиенту. Сервер веб-приложений отправляет ответ обратно на компьютер пользователя, где он сохраняется в веб-клиенте.

2.5.1.2 Запуск узла SIA

Можно настроить автоматический запуск узла Server Intelligence Agent (SIA) с помощью основной операционной системы или запускать его вручную с помощью Central Configuration Manager (CCM).

Узел SIA извлекает информацию об управляемых серверах с сервера Central Management Server (CMS). Если SIA использует локальный CMS, который не запущен, SIA запускает CMS. Если SIA использует удаленный CMS, предпринимается попытка соединения с CMS.

После запуска SIA выполняются следующие события.

1. SIA проверяет кэш в поисках CMS.
 - a. Если SIA настроен для запуска CMS, и CMS не запущен, SIA запускает CMS и устанавливает соединение с ним.
 - b. Если SIA настроен для использования запущенного CMS (локального или удаленного), он пытается подключиться к первому CMS в своем кэше. Если CMS в данный момент недоступен, SIA пытается подключиться к следующему CMS в кэше. Если нет доступных кэшированных CMS, SIA ожидает, пока станет доступным какой-нибудь из них.
2. CMS подтверждает идентификационную информацию SIA, чтобы гарантировать его допустимость.
3. После успешного подключения к CMS SIA запрашивает список серверов для управления. SIA не сохраняет информацию о серверах, которыми управляет. Информация о конфигурации, которая определяет, каким сервером управляет SIA, хранится в базе данных системы CMS и извлекается из CMS при запуске SIA.
4. CMS запрашивает в базе данных системы CMS список серверов, управляемых SIA. Кроме того, извлекается конфигурация для каждого сервера.
5. CMS возвращает агенту SIA список серверов и их конфигурацию.
6. SIA запускает каждый сервер, для которого настроен автоматический запуск, с соответствующей конфигурацией и отслеживает его состояние. Каждый сервер, запускаемый SIA, сконфигурирован для использования того же CMS, который используется SIA. Серверы, не настроенные для автоматического запуска с SIA, не будут запущены.

2.5.1.3 Отключение SIA

Можно настроить автоматическое отключение узла Server Intelligence Agent (SIA) с помощью основной операционной системы или отключать его вручную с помощью Central Configuration Manager (CCM).

При отключении SIA выполняются следующие шаги.

1. CMS дает SIA команду на завершение работы.
2. SIA сообщает CMS о своем отключении.
 - a. Если SIA отключается в результате завершения работы основной операционной системы, SIA запрашивает остановку серверов. Серверы, которые не завершают работу в течение 25 секунд, останавливаются принудительно.

- b. Если SIA отключается вручную, он ожидает завершения управляемыми серверами существующих заданий. Управляемые серверы не будут принимать никаких новых заданий. После завершения всех заданий серверы выключаются. После остановки всех серверов SIA также завершает работу.

Примечание:

При принудительном завершении работы SIA дает команду на немедленное выключение всех серверов.

2.5.2 Планирование

2.5.2.1 Планирование отчета SAP Crystal

Этот рабочий процесс описывает процесс планирования пользователем отчета SAP Crystal, который должен выполняться в последующем.

1. Веб-клиент направляет на сервер веб-приложений URL-запрос на внесение в расписание – как правило, посредством веб-сервера.
2. Сервер веб-приложений интерпретирует URL-запрос и определяет, что это – запрос на внесение в расписание. Сервер веб-приложений направляет данные о запланированном времени, значения учетных данных для входа в базу данных, значения параметров, информацию о месте назначения и формате на указанный CMS.
3. CMS определяет наличие у пользователя прав на планирование объекта. При наличии у пользователя достаточных прав CMS добавляет новую запись в базу данных системы CMS. CMS также добавляет экземпляр в список отложенных расписаний.

2.5.2.2 Планирование выполнения отчета SAP Crystal в настоящий момент

Данный рабочий процесс описывает процесс планирования пользователем немедленного запуска отчета SAP Crystal.

1. Пользователь вносит отчет в расписание, и данный отчет направляется на сервер веб-приложений.
2. Сервер веб-приложений передает запрос центральному серверу управления (CMS).
3. CMS определяет, есть ли у пользователя права на добавление данного отчета в расписание.
4. При наличии у пользователя соответствующих прав CMS назначает системной базе данных CMS выполнение запроса на добавление объекта в расписание.

5. В запланированное время CMS находит доступный сервер заданий Crystal Reports, используя значение «Максимальное количество заданий», заданное для каждого сервера заданий Crystal Reports.
6. CMS направляет на сервер заданий Crystal Reports информацию о задании.
7. Сервер заданий Crystal Reports определяет расположение сервера репозитория входных файлов (FRS), на котором размещается данный отчет. Затем сервер обработки Crystal Reports запрашивает шаблон отчета у сервера репозитория входящих файлов.
8. Сервер репозитория входящих файлов обращается к шаблону отчета и направляет его на сервер обработки Crystal Reports.
9. Шаблон отчета помещается во временный каталог на сервере обработки Crystal Reports.
10. Сервер обработки Crystal Reports запускает дочерний процесс (JobServerChild.exe) для координации выполнения отчета.
11. JobServerChild.exe запускает библиотеку ProcReport.dll и передает ей все экземпляры, полученные от сервера обработки Crystal Reports. ProcReport.dll обращается к Crpe32.dll.
12. Отчет создается, когда Crpe32.dll завершает следующие задания:
 - открытие отчета;
 - подключение к производственной базе данных;
 - обработку отчета;
 - создание и сохранение экземпляра отчета;
 - возвращение отчета JobServerChild.exe.
13. Сервер обработки Crystal Reports периодически обновляет на CMS информацию о состоянии выполнения задания. На этом этапе информация о состоянии указывает на выполнение обработки отчета.
14. JobServerChild.exe загружает экземпляр отчета на сервер репозитория исходящих файлов.
15. Сервер репозитория исходящих файлов уведомляет JobServerChild.exe об успешном сохранении отчета.
16. JobServerChild.exe уведомляет сервер обработки Crystal Reports о завершении процесса создания отчета.
17. Сервер заданий для отчета обновляет на CMS информацию о состоянии выполнения задания. JobServerChild.exe удаляет себя из памяти.
18. CMS обновляет статус задания в собственной памяти, а затем записывает сведения об экземпляре объекта в базу данных системы CMS.

2.5.2.3 Выполнение запланированного отчета SAP Crystal

Этот рабочий процесс описывает процесс выполнения запланированного отчета SAP Crystal в заданное время.

1. Центральный сервер управления (CMS) проверяет базу данных системы CMS на наличие отчетов SAP Crystal, выполнение которых запланировано на это время.
2. В запланированное время CMS находит доступный сервер заданий Crystal Reports, используя значение «Максимально разрешенное число заданий», заданное для каждого сервера заданий

Crystal Reports. CMS направляет на сервер обработки Crystal Reports информацию о задании. Информация, которую CMS направляет на сервер обработки Crystal Reports: идентификатор отчета, его формат, назначение, информация для входа в систему, параметры и формулы выбора.

3. Сервер обработки Crystal Reports обращается к серверу репозитория входящих файлов (FRS) для получения шаблона отчета согласно запрошенному идентификатору отчета.
4. Сервер обработки Crystal Reports запускает процесс JobChildserver.
5. Дочерний процесс (JobChildserver) запускает библиотеку ProcReport.dll после получения шаблона от сервера репозитория входящих файлов через инфраструктуру Enterprise. ProcReport.dll содержит все параметры, переданные от CMS на сервер обработки Crystal Reports.
6. ProcReport.dll запускает библиотеку Crpe32.dll, выполняющую обработку отчета согласно всем переданным параметрам.
7. Еще во время обработки записи извлекаются с сервера базы данных, как определено в отчете.
8. Сервер обработки Crystal Reports периодически обновляет на CMS информацию о состоянии выполнения задания. На этом этапе информация о состоянии указывает на выполнение обработки.
9. После компилирования в память сервера заданий Crystal Reports отчет необходимо импортировать в другой формат, такой как Portable Document Format (PDF). При экспорте в PDF используется PDF .dll.
10. Отчет с сохраненными данными также необходимо передать в местоположение по умолчанию. Затем он будет направлен на сервер репозитория исходящих файлов (FRS).
11. По завершении процесса сервер обработки Crystal Reports обновляет информацию о состоянии выполнения задания на CMS. На этом этапе информация о состоянии указывает на то, что задание выполнено успешно.
12. CMS обновляет статус задания в собственной памяти, а затем записывает сведения об экземпляре объекта в базу данных системы CMS.

2.5.2.4 Планирование документа SAP BusinessObjects Web Intelligence

Данный рабочий процесс описывает процесс планирования пользователем запуска документа SAP BusinessObjects Web Intelligence в будущем.

1. Пользователь задает расписание для документа, и на веб-сервер направляется запрос. Веб-сервер передает запрос на добавление документа в расписание на сервер веб-приложений.
2. Сервер веб-приложений направляет запрос на добавление документа в расписание на CMS.
3. CMS определяет, есть ли у пользователя права на добавление данного документа в расписание.
4. На CMS создается экземпляр документа SAP BusinessObjects Web Intelligence, содержащий всю информацию, связанную с расписанием.
5. При наличии прав для планирования документа пользователь задает различные параметры планирования.

6. CMS фиксирует запланированный запрос объекта в системной базе данных.

2.5.2.5 Выполняется запланированный документ SAP BusinessObjects Web Intelligence, выпуск для OLAP

Данный рабочий процесс описывает процесс выполнения запланированного документа SAP BusinessObjects Web Intelligence в заданное время.

1. Сервер центрального управления (CMS) проверяет системную базу данных CMS на наличие запланированных к выполнению заданий SAP BusinessObjects Web Intelligence.
2. Когда наступает указанное в расписании время, CMS направляет запрос в расписании и всю информацию о запросе на адаптивный сервер заданий, на котором размещается служба планирования и публикаций SAP BusinessObjects Web Intelligence.
3. Адаптивный сервер заданий (служба планирования и публикаций Web Intelligence) обращается к доступному серверу обработки Web Intelligence. Доступность сервера определяется по значению "Максимально разрешенное число заданий", заданному для каждого сервера обработки SAP BusinessObjects Web Intelligence.
4. Сервер обработки SAP BusinessObjects Web Intelligence обращается к серверу репозитория входных файлов (FRS), где размещается документ и файл слоя метаданных юниверса, на котором основан этот документ. Сервер обработки SAP BusinessObjects Web Intelligence запрашивает данный документ у сервера репозитория входных файлов. Сервер репозитория входных файлов обращается к документу SAP BusinessObjects Web Intelligence и к файлу юниверса, на котором он основан, и направляет их на сервер обработки SAP BusinessObjects Web Intelligence.
5. Документ SAP BusinessObjects Web Intelligence размещается во временном каталоге сервера обработки SAP BusinessObjects Web Intelligence. Сервер обработки SAP BusinessObjects Web Intelligence открывает документ в памяти. Библиотека QT.dll генерирует SQL из юниверса, на котором основан документ. Сервер соединений (компонент сервера обработки SAP BusinessObjects Web Intelligence) подключается к базе данных. Данные запроса передаются через библиотеку QT.dll на Document Engine, где происходит обработка документа. Новый экземпляр создан успешно.
6. Сервер обработки SAP BusinessObjects Web Intelligence загружает экземпляр документа на сервер репозитория выходных файлов.
7. Сервер обработки SAP BusinessObjects Web Intelligence уведомляет сервер адаптивных заданий (службу планирования и публикаций SAP BusinessObjects Web Intelligence), что создание документа завершено. Если документ запланирован в определенное место назначения (файловую систему, FTP, SMTP или папку "Входящие"), адаптивный сервер заданий извлекает обработанный документ с сервера репозитория исходящих файлов и доставляет в указанное место назначения. Предположим, что для текущего примера этого не требуется.
8. Адаптивный сервер заданий (служба планирования и публикаций Web Intelligence) обновляет на CMS информацию о состоянии выполнения задания.
9. CMS обновляет статус задания в собственной памяти, а затем записывает сведения об экземпляре объекта в базу данных системы CMS.

2.5.2.6 Планирование объекта

Данный рабочий процесс описывает процесс планирования пользователем запускаемого объекта.

1. Пользователь вносит в расписание объект, и на веб-сервер направляется запрос.
2. Веб-сервер передает запрос на внесение в расписание на сервер веб-приложений.
3. Сервер веб-приложений передает запрос центральному серверу управления (CMS).
4. CMS определяет, есть ли у пользователя права на добавление данного объекта в расписание.
5. При наличии у пользователя соответствующих прав CMS отправляет запланированный запрос объекта в базу данных системы CMS.
6. В запланированное время CMS обращается к доступному серверу выполнения программы, используя значение "Максимально разрешенное число заданий", заданное для каждого сервера выполнения программы.
7. CMS направляет на сервер выполнения программы информацию о задании.
8. Сервер выполнения программы обращается к серверу репозитория входящих файлов с запросом на объект программы.
9. Сервер репозитория входящих файлов возвращает объект программы на сервер выполнения программы.
10. Сервер выполнения программы запускает внесенный в расписание объект.
11. Сервер выполнения программы периодически обновляет на CMS информацию о состоянии выполнения задания. На этом этапе информация о состоянии указывает на то, что программа выполняет обработку.
12. Сервер выполнения программы направляет файл журнала на сервер репозитория исходящих файлов.
13. Сервер репозитория исходящих файлов уведомляет сервер выполнения программы о том, что объект внесен в расписание, отправляя файл журнала объекта.
14. Сервер выполнения программы обновляет на CMS информацию о состоянии выполнения задания.
15. CMS обновляет статус задания в собственной памяти, а затем записывает сведения об экземпляре объекта в базу данных системы CMS.

2.5.2.7 Планирование немедленного запуска объекта

Данный рабочий процесс описывает процесс планирования немедленного запуска объекта пользователем.

1. Пользователь вносит в расписание объект, и на веб-сервер направляется запрос.
2. Веб-сервер передает запрос на внесение в расписание на сервер веб-приложений.
3. Сервер веб-приложений передает запрос центральному серверу управления (CMS).

4. CMS определяет, есть ли у пользователя права на добавление данного объекта в расписание.
5. При наличии у пользователя соответствующих прав CMS отправляет запланированный запрос объекта в базе данных системы CMS.
6. В запланированное время CMS обращается к доступному серверу выполнения программы, используя значение «"Максимально разрешенное число заданий"», заданное для каждого сервера выполнения программы.
7. CMS направляет на сервер выполнения программы информацию о задании.
8. Сервер выполнения программы обращается к серверу репозитория входящих файлов с запросом на объект программы.
9. Сервер репозитория входящих файлов возвращает объект программы на сервер выполнения программы.
10. Сервер выполнения программы запускает внесенный в расписание объект.
11. Сервер выполнения программы периодически обновляет на CMS информацию о состоянии выполнения задания. На этом этапе информация о состоянии указывает на то, что программа выполняет обработку.
12. Сервер выполнения программы направляет файл журнала на сервер репозитория исходящих файлов.
13. Сервер репозитория исходящих файлов уведомляет сервер выполнения программы о том, что объект внесен в расписание, отправляя файл журнала объекта.
14. Сервер выполнения программы обновляет на CMS информацию о состоянии выполнения задания.
15. CMS обновляет статус задания в собственной памяти, а затем записывает сведения об экземпляре объекта в базу данных системы CMS.

2.5.3 Просмотр

2.5.3.1 Просмотр отчета SAP Crystal

Этот рабочий процесс описывает процесс запроса пользователем страницы отчета SAP Crystal, если отчет еще не существует на кэш-сервере.

1. Пользователь направляет запрос на просмотр на сервер веб-приложений через веб-сервер.
2. Сервер веб-приложений определяет, что данный запрос является запросом на просмотр страницы отчета. Сервер веб-приложений запрашивает у CMS информацию о наличии у пользователя достаточных прав на просмотр отчета.
3. CMS определяет, есть ли у пользователя права на просмотр данного отчета.
4. CMS направляет на сервер веб-приложений подтверждение наличия у пользователя прав на просмотр отчета.

5. Сервер веб-приложений направляет на кэш-сервер Crystal Reports запрос для получения требуемой страницы отчета.
6. Кэш-сервер Crystal Reports определяет наличие запрошенного файла в каталоге кэша.
7. Запрошенный файл EPF отсутствует в каталоге кэша.
8. Кэш-сервер Crystal Reports направляет запрос на сервер страниц Crystal Reports.
9. Сервер страниц Crystal Reports запрашивает соответствующий экземпляр отчета на сервере репозитория выходных файлов (FRS).
10. Сервер репозитория исходящих файлов направляет запрошенный экземпляр отчета на сервер страниц Crystal Reports.
11. Сервер страниц Crystal Reports открывает данный экземпляр отчета и проверяет отчет на наличие в нем данных.
12. Сервер страниц Crystal Reports определяет, что отчет содержит данные, и создает файл для запрошенной страницы отчета, не подключаясь к производственной базе данных.
13. Сервер страниц Crystal Reports направляет файл EPF на кэш-сервер Crystal Reports.
14. Кэш-сервер Crystal Reports записывает файл EPF в каталог кэша.
15. Кэш-сервер Crystal Reports направляет запрашиваемую страницу на сервер веб-приложений.
16. Сервер веб-приложений направляет файл на веб-сервер.
17. Веб-сервер направляет запрошенную страницу в средство просмотра отчетов.

2.5.3.2 Просмотр кэшированного отчета SAP Crystal

Этот рабочий процесс описывает процесс запроса пользователем страницы отчета SAP Crystal, если отчет уже существует в кэш-сервере.

1. Веб-клиент направляет запрос на просмотр в URL-адресе на сервер веб-приложений.
2. Сервер веб-приложений интерпретирует данный запрос и определяет, что это запрос на просмотр первой страницы выбранного экземпляра отчета. Сервер веб-приложений отправляет запрос серверу CMS, чтобы убедиться в наличии у пользователя прав на просмотр объекта.
3. CMS проверяет права пользователя по базе данных системы CMS.
4. CMS направляет на сервер веб-приложений подтверждение наличия у пользователя прав на просмотр данного экземпляра.
5. Сервер веб-приложений направляет на кэш-сервер Crystal Reports запрос первой страницы экземпляра отчета. Кэш-сервер Crystal Reports проверяет наличие данной страницы. Если данная страница существует, кэш-сервер Crystal Reports возвращает ее на сервер веб-приложений.
6. Сервер веб-приложений отправляет страницу веб-клиенту, в котором эта страница подготавливается к просмотру и отображается.

2.5.3.3 Просмотр рабочего пространства SAP Analysis, выпуск для OLAP

Этот рабочий процесс описывает процесс запроса пользователем рабочего пространства SAP Analysis (ранее Voyager).

1. Веб-клиент направляет через веб-сервер на сервер веб-приложений запрос на просмотр нового рабочего пространства. Веб-клиент обращается к серверу веб-приложений с помощью технологии DHTML AJAX (асинхронный JavaScript и XML). С помощью технологии AJAX можно выполнить частичное обновление страницы, поэтому для каждого нового запроса не придется отображать новую страницу.
2. Сервер веб-приложений преобразует запрос и направляет его в CMS, чтобы определить наличие у пользователя прав на просмотр или создание нового рабочего пространства.
3. CMS извлекает учетные данные пользователя из базы данных системы CMS.
4. Если пользователь обладает правами на просмотр или создание рабочего пространства, CMS подтверждает это для сервера веб-приложений. Одновременно данный сервер направляет список доступных серверов многомерного анализа MDAS.
5. Сервер веб-приложений выбирает сервер MDAS из списка доступных серверов и направляет в службу запрос CORBA, чтобы найти соответствующие серверы OLAP для создания нового рабочего пространства или обновления существующего.
6. Серверу MDAS необходимо обратиться к серверу репозитория входных файлов (FRS) для извлечения соответствующего документа рабочего пространства, содержащего информацию об основной базе данных OLAP, и о сохраненном с ее помощью изначальном запросе OLAP. Сервер репозитория входных файлов извлекает соответствующее рабочее пространство Advanced Analyzer из основного каталога и направляет его обратно на MDAS.
7. Сервер MDAS открывает рабочее пространство, формулирует запрос и направляет его на сервер базы данных OLAP. Сервер MDAS должен обладать соответствующим клиентом базы данных OLAP, настроенным в соответствии с источником данных OLAP. Требуется преобразование запроса веб-клиента в соответствующий запрос OLAP. Сервер базы данных OLAP возвращает результат запроса на сервер MDAS.
8. Сервер MDAS на основании запроса на создание, просмотр, печать или экспорт предварительно визуализирует результат, что позволяет Java WAS быстрее завершить визуализацию. Сервер MDAS направляет пакеты XML с подготовленным к просмотру результатом обратно на сервер веб-приложений.
9. Сервер веб-приложений отображает рабочее пространство и направляет форматированную страницу или ее определенную часть на веб-клиент через веб-сервер. Веб-клиент отображает обновленную или новую запрошенную страницу. Это решение не требует загрузки дополнительных компонентов Java или ActiveX.

2.5.4 По требованию

2.5.4.1 Просмотр отчета SAP Crystal по требованию

Этот рабочий процесс описывает процесс пользователя, запрашивающего страницу отчета SAP Crystal по требованию.

1. Веб-клиент направляет на сервер веб-приложений URL-запрос на просмотр по требованию – как правило, посредством веб-сервера.
2. Сервер веб-приложений интерпретирует запрошенную страницу и значения, отправленные в URL-запросе и определяет, что это запрос на просмотре первой страницы выбранного объекта отчета.
3. Сервер веб-приложений отправляет запрос серверу CMS, чтобы убедиться в наличии у пользователя прав на просмотр объекта. CMS проверяет права пользователя по базе данных системы CMS.
4. CMS направляет на сервер веб-приложений подтверждение наличия у пользователя прав на просмотр объекта.
5. Сервер веб-приложений направляет на кэш-сервер Crystal Reports запрос первой страницы объекта отчета.
6. Кэш-сервер Crystal Reports проверяет наличие данной страницы. Если отчет не соответствует требованиям общего доступа к отчету по требованию (в заданное время для другого запроса по требованию, а также входа в базу данных или параметров), то кэш-сервер Crystal Reports направляет на сервер обработки Crystal Reports запрос на создание страницы.
7. Сервер обработки Crystal Reports запрашивает объект отчета у сервера репозитория входящих файлов. Сервер репозитория входящих файлов направляет копию объекта на сервер обработки Crystal Reports. Сервер обработки Crystal Reports открывает отчет в собственной памяти и проверяет его на наличие данных.
8. Если в объекте отчета отсутствуют данные, серверу обработки Crystal Reports необходимо подключиться к базе данных для запроса данных.
9. Сервер обработки Crystal Reports направляет страницу на кэш-сервер Crystal Reports. Кэш-сервер Crystal Reports сохраняет копию страницы в его каталоге кэша, ожидая новые запросы на просмотр.
10. Кэш-сервер Crystal Reports направляет страницу на сервер веб-приложений.
11. Сервер веб-приложений направляет страницу .erf на веб-сервер. Веб-сервер отправляет страницу на компьютер пользователя, где она подготавливается к просмотру в средстве просмотра веб-клиента.

2.5.4.2 Просмотр документа SAP BusinessObjects Web Intelligence по запросу

Данный рабочий процесс описывает процесс просмотра пользователем документа SAP BusinessObjects Web Intelligence по запросу.

1. Веб-браузер направляет запрос на просмотр на сервер веб-приложений через веб-сервер.
2. Сервер веб-приложений определяет, что это запрос документа Web Intelligence, и отправляет его в CMS, чтобы определить наличие у пользователя соответствующих прав на просмотр документа.
3. CMS направляет на сервер веб-приложений подтверждение наличия у пользователя прав на просмотр документа.
4. Сервер веб-приложений направляет на сервер обработки Web Intelligence запрос на документ.
5. Сервер обработки Web Intelligence запрашивает у сервера репозитория входящих файлов (FRS) данный документ и файл юниверса, на котором он основан. Файл юниверса содержит информацию о слое метаданных, включая данные по защите на уровне строк и столбцов.
6. Сервер репозитория входящих файлов направляет на сервер обработки Web Intelligence копию документа и файл юниверса, на котором основан запрашиваемый документ.
7. Web Intelligence Report Engine открывает документ в памяти.
8. Подсистема отчетов Web Intelligence использует компонент QT (inproc) и сервер соединений (inproc). Компонент QT генерирует/подтверждает/повторно генерирует SQL и подключается к базе данных для выполнения запроса. Сервер подключения использует SQL для получения данных из базы данных для системы отчетов, в которой документ обрабатывается.
9. Сервер обработки Web Intelligence направляет запрошенную страницу документа в пригодном для просмотра формате на сервер веб-приложений. Сервер веб-приложений направляет данную страницу на веб-сервер. Сервер веб-приложений направляет данную страницу на компьютер пользователя, где она выводится на экран в веб-браузере.

2.5.4.3 Просмотр отчета SAP Crystal по требованию, если формат просмотра по умолчанию – Web Java

Этот рабочий процесс описывает процесс пользователя, просматривающего отчет SAP Crystal, если форматом просмотра по умолчанию является Web Java.

1. Веб-клиент направляет запрос на просмотр по требованию через веб-сервер на сервер веб-приложений.
2. Сервер веб-приложений интерпретирует запрошенную страницу и значения, отправленные в URL-запросе и определяет, что это запрос на просмотре первой страницы выбранного объекта отчета.
3. Сервер веб-приложений отправляет запрос серверу CMS, чтобы убедиться в наличии у пользователя прав на просмотр объекта. CMS проверяет права пользователя по базе данных системы CMS.
4. CMS направляет на сервер веб-приложений подтверждение наличия у пользователя прав на просмотр объекта.
5. Сервер веб-приложений направляет на кэш-сервер Crystal Reports запрос первой страницы объекта отчета.
6. Кэш-сервер Crystal Reports проверяет наличие данной страницы. Если отчет не соответствует требованиям общего доступа к отчету по требованию (в заданное время для другого запроса

по требованию, а также входа в базу данных или параметров), то кэш-сервер Crystal Reports направляет на сервер обработки Crystal Reports запрос на создание страницы.

7. Сервер обработки Crystal Reports запрашивает объект отчета у сервера репозитория входящих файлов. Сервер репозитория входящих файлов направляет копию объекта на сервер обработки Crystal Reports. Сервер обработки Crystal Reports открывает отчет в собственной памяти и проверяет его на наличие данных.
8. Если в объекте отчета отсутствуют данные, серверу обработки Crystal Reports необходимо подключиться к базе данных для запроса данных.
9. Сервер обработки Crystal Reports направляет страницу .erf на кэш-сервер Crystal Reports. Кэш-сервер Crystal Reports сохраняет копию страницы .erf в каталоге кэша для новых запросов на просмотр. На этом этапе страница .erf также может быть сгенерирована и направлена на кэш-сервер Crystal Reports. Страница .erf (навигационное дерево отчета на панели слева) генерируется вместе с первой страницей отчета и при группировке отчета. Каждый отчет содержит только одну страницу .erf, которая, тем не менее, может иметь значительный размер.
10. Кэш-сервер Crystal Reports направляет страницу .erf на сервер веб-приложений.
11. Сервер веб-приложений направляет страницу .erf на веб-сервер. Веб-сервер отправляет страницу .erf на компьютер пользователя, где она отображается в средстве просмотра в веб-клиенте.

Управление лицензиями

3.1 Управление лицензионными ключами

В этом разделе описывается управление лицензионными ключами для развертывания платформы BI.

См. также

- [Просмотр сведений лицензии](#)
- [Для добавления ключа лицензии](#)
- [Для просмотра текущей деятельности учетной записи](#)

3.1.1 Просмотр сведений лицензии

В области управления СМС **Ключи лицензий** указывается количество лицензий на основе ролей (BI Viewer и BI Analyst), лицензий для одновременно работающих пользователей, лицензий для именованных пользователей и лицензий на процессор, связанное с каждым ключом.

1. Перейдите в область управления **Ключи лицензий** в СМС.
2. Выберите ключ лицензии.

Детальная информация, связанная с данным ключом, появится в области **Сведения о лицензионных ключах**. Для приобретения дополнительных ключей лицензий обращайтесь к торговому представителю SAP.

См. также

- [Управление лицензионными ключами](#)
- [Для добавления ключа лицензии](#)
- [Для просмотра текущей деятельности учетной записи](#)

3.1.2 Для добавления ключа лицензии

Если вы переходите к коммерческой версии от демо-версии, убедитесь в том, что вы удалили ключ демонстрационной версии, чтобы добавить новые ключи лицензий или коды активации продукта.

1. Перейдите в область управления **Ключи лицензий** в СМС.
2. Введите ключ в поле **Добавить ключ**.
3. Щелкните **Добавить**.

Ключ добавится в список.

См. также

- [Просмотр сведений лицензии](#)
- [Для просмотра текущей деятельности учетной записи](#)

3.1.3 Для просмотра текущей деятельности учетной записи

1. Перейдите в область управления СМС **Параметры**.
2. Нажмите кнопку **Просмотреть глобальные системные показатели**.

Здесь отображается текущее использование лицензий, вместе с дополнительными показателями работы.

См. также

- [Управление лицензионными ключами](#)
- [Для добавления ключа лицензии](#)
- [Просмотр сведений лицензии](#)

3.2 Измерение показателей использования лицензий

Инструмент измерения лицензий BusinessObjects (BOLMT) – это программа командной строки на базе Java, используемая для сбора и хранения данных о лицензиях платформы BI. Выходной документ XML содержит результаты измерения показателей использования лицензий и

направляется в службу глобального аудита лицензий SAP (GLAS) для включения в отчет об аудите лицензий.

Системный администратор устанавливает и запускает BOLMT для каждого кластера платформы BI при поступлении запроса на аудит лицензий. Программа BOLMT измеряет показатели использования лицензий, получаемых для ролей, лицензий для именованных пользователей и лицензий для одновременно работающих пользователей.

Администратор может указать конкретный выходной каталог для документа XML и настроить выходной документ так, чтобы в него не включались сведения, которые позволяли бы идентифицировать пользователей системы.

3.2.1 Проведение аудита лицензий

Для выполнения аудита лицензий необходимо иметь права администратора и возможность доступа к каталогу, содержащему файл `BOLMT.jar` в установленной платформе BI.

1. Откройте консоль командной строки.
2. Перейдите в каталог, содержащий исполняемые файлы Java для установленной платформы BI

По умолчанию требуемый файл устанавливается в следующем каталоге: `[INSTALLDIR]\SAP BusinessObjects Enterprise XI 4.0\java\lib`

3. Выполните файл `BOLMT.jar`.

Команда для выполнения файла вводится в следующем формате: `-jar BOLMT.jar [параметры] <выходной файл>`

Допустимые параметры описываются в следующей таблице:

Действие	Описание
-c --cms	Идентификационное имя и номер порта для центрального сервера управления (CMS). Используется формат <i>имя_CMS:номер_порта</i> . Если этот параметр не задан, по умолчанию используются настройки CMS для локального хоста.
-p --password	Пароль учетной записи администратора, используемый для подключения к CMS.
-a--auth	Метод аутентификации, используемый при подключении пользователя к CMS. По умолчанию используется метод Enterprise, задаваемый в виде <i>secEnterprise</i> .
-s--sanitize	Этот параметр задает исключение из выходного документа аудита любых личных сведений, которые позволяли бы идентифицировать пользователей.

Примечание:

Спецификация выходного файла всегда является последним аргументом командной строки. Это необязательный параметр. Если аргумент не указан, выходные данные направляются в стандартный поток вывода консоли. Можно также перенаправить вывод в скрипт как аргумент командной строки.

Пример:

```
C:\Program Files (x86)\SAP
Business Objects\SAP BusinessObjects Enterprise XI 4.0\java\lib>"C:\Program Files
(x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin
\java.exe" -jar BOLMT.jar --cms=mycms:6400 -uAdministrator
-p=7juujg --auth=secEnterprise --sanitize audit.xml
```

Управление пользователями и группами

4.1 Обзор управления учетными записями

Управление учетными записями может рассматриваться как совокупность заданий, связанных с созданием, отображением, изменением и организацией информации о пользователях и группах. Область управления «Пользователи и группы» консоли Central Management Console (CMC) представляет собой единый центр для выполнения этих заданий.

После того как учетные записи пользователей и групп созданы, можно добавить объекты и указать права на них. Когда пользователи выполняют вход в систему, они могут просмотреть объекты, используя стартовую панель BI или пользовательское веб-приложение.

4.1.1 Управление пользователями

В области управления «Пользователи и группы» можно указать всю информацию, необходимую для доступа пользователей к платформе BI. Также вы можете просмотреть две учетные записи, созданные по умолчанию и находящиеся в таблице «Учетные записи пользователей по умолчанию».

Таблица 4-1: Учетные записи пользователей по умолчанию

Имя учетной записи	Описание
Администратор	Этот пользователь принадлежит к группам Администраторы и Все . Администратор может выполнять все задачи во всех приложениях платформы BI (например, CMC, CCM, мастер публикаций и стартовая панель BI).
Гость	Данный пользователь принадлежит к группе Все . Эта учетная запись доступна по умолчанию, и ей в системе не назначается пароль. Если назначить этой записи пароль, будет нарушен принцип единого входа стартовой панели BI.

Имя учетной записи	Описание
SMAAdmin	Это учетная запись только для чтения, используемая SAP Solution Manager для доступа к компонентам платформы BI.

4.1.1.1 Лицензирование на основе ролей

В схеме лицензирования на основе ролей пользователей имеется две роли, которые могут быть назначены пользователям платформы BI:

- BI Analyst
- BI Viewer

Каждой роли присвоены определенные уровни доступа к приложениям платформы BI. Уровень доступа для роли пользователя не может быть изменен. Роли пользователя применяются к новым учетным записям пользователей, созданным в платформе BI, или к существующим учетным записям пользователей, импортированным из служб каталогов сторонних производителей, например Windows AD или LDAP.

Примечание:

Роли пользователей не следует путать с принадлежностью к группе. При назначении пользователю одной из двух доступных ролей ему автоматически назначаются предопределенные права для приложений. Чтобы связать пользователя с определенными уровнями доступа групп, требуется добавить этого пользователя в соответствующую группу.

Выберите **Лицензионный ключ** в СМС для получения дополнительных сведений о схеме лицензирования или о правах доступа для каждой роли пользователя обратитесь к заведующему учетными записями SAP Business Objects.

4.1.1.1.1 Роль BI Analyst

Роль BI Analyst разработана для пользователей, создающих содержимое в системе платформы BI. Роль BI Analyst следует назначать пользователям, редактирующим или создающим отчеты, разрабатывающим юниверсы и управляющим ими, а также выполняющим любые административные задачи в СМС.

4.1.1.1.2 Роль BI Viewer

Роль BI Viewer предназначена в основном для потребителей содержимого. Эти пользователи только просматривают отчеты, не изменяя содержимого.

Система предотвращает создание содержимого, изменение отчетов и выполнение общих административных задач в системе пользователями, назначенными роли BI Viewer. Роль BI Viewer не должна назначаться пользователям, которым необходимо:

- Создавать отчеты
- Обновлять или изменять отчеты
- Выполнять административные задачи с использованием СМС

Примечание:

Пользователи с ролью BI Viewer не имеют доступа к СМС.

4.1.2 Управление группами

Группы – это совокупности пользователей, которым назначены одинаковые привилегии; однако вы можете создавать группы, основываясь на отделе, роли или местоположении. Группы позволяют вам изменять права пользователей централизованно (в группе), вместо того, чтобы изменять права для каждой учетной записи пользователя. Кроме того, можно присвоить группе или нескольким группам права на объекты.

В области «Пользователи и группы» вы можете создать группы, которые предоставляют большому количеству людей доступ к отчету или папке. Это позволит вам выполнить изменения всего один раз, вместо того, чтобы изменять отдельно учетную запись каждого пользователя. Также вы можете просмотреть несколько учетных записей групп, представленных в системе по умолчанию и хранящихся в таблице «Учетные записи групп по умолчанию».

Для просмотра доступных групп в СМС, нажмите **Список групп** на панели Дерево. В качестве альтернативы, можно нажать **Иерархия групп** для отображения иерархического списка всех доступных групп.

Таблица 4-2: Учетные записи групп по умолчанию

Имя учетной записи	Описание
Администраторы	Члены этой группы могут выполнять все задачи во всех приложениях платформы BI (СМС, ССМ, мастер публикаций и стартовая панель BI). По умолчанию, группа Администраторы содержит только пользователей-администраторов.
Все	Каждый пользователь является членом группы Все .
Дизайнер группы QaaWS	Члены этой группы имеют доступ к средству Query as a Web Service.

Имя учетной записи	Описание
Пользователи средства преобразования отчетов	Члены этой группы имеют доступ к средству преобразования отчетов.
Переводчики	Элементы этой группы имеют доступ к приложению "Диспетчер переводов".
Пользователи Universe Designer	Пользователи, принадлежащие к данной группе, имеют доступ к папке Universe Designer и папке Соединения . Они могут контролировать права доступа к приложению Universe Designer. Вы должны добавить пользователей в эту группу, если это необходимо. По умолчанию в этой группе пользователей нет.

См. также

- [Права на платформе BI](#)
- [Предоставление доступа пользователям и группам](#)

4.1.3 Доступные типы аутентификации

Перед настройкой учетных записей и групп пользователей платформы BI необходимо решить, какой тип аутентификации использовать. В таблице «Типы аутентификации» представлены параметры типов аутентификации, доступных для вас в зависимости от инструментов безопасности, используемых вашей организацией.

Таблица 4-3: Типы аутентификации

Тип аутентификации	Описание
Enterprise	Аутентификация по умолчанию (Enterprise) используется в том случае, если нужно создать отдельные учетные записи и группы для использования в платформе BI или если еще не создана иерархия пользователей и групп на сервере каталогов LDAP или сервере Windows AD.

Тип аутентификации	Описание
LDAP	Если используется сервер каталогов LDAP, можно использовать существующие учетные записи пользователей и групп для входа в платформу BI. После сопоставления учетных записей LDAP в платформе BI пользователи смогут входить в платформу BI, используя имя пользователя и пароль LDAP. Это устраняет необходимость повторного создания пользователей и групп в платформе BI.
Windows AD	Можно использовать существующие учетные записи пользователей и группы Windows AD в платформе BI. После сопоставления учетных записей AD в платформе BI пользователи смогут входить в платформу BI, используя имя пользователя и пароль AD. Это устраняет необходимость повторного создания пользователей и групп в платформе BI.
SAP	Существующие роли SAP можно отображать в учетных записях платформы BI. После отображения ролей SAP пользователи могут входить в приложения платформы BI с их учетными данными SAP. Это устраняет необходимость повторного создания пользователей и групп в платформе BI.
Oracle EBS	Можно сопоставить существующие роли Oracle EBS с учетными записями в платформе BI. После сопоставления ролей Oracle EBS пользователи смогут входить в приложения платформы BI со своими учетными данными Oracle EBS. Это устраняет необходимость повторного создания пользователей и групп в платформе BI.
Siebel	Можно сопоставить существующие роли Siebel с учетными записями в платформе BI. После сопоставления ролей Siebel пользователи смогут входить в приложения платформы BI со своими учетными данными Siebel. Это устраняет необходимость повторного создания пользователей и групп в платформе BI.

Тип аутентификации	Описание
PeopleSoft Enterprise	Можно сопоставить существующие роли PeopleSoft с учетными записями в платформе BI. После сопоставления ролей PeopleSoft пользователи смогут входить в приложения платформы BI со своими учетными данными PeopleSoft. Это устраняет необходимость повторного создания пользователей и групп в платформе BI.
JD Edwards EnterpriseOne	Можно сопоставить существующие роли JD Edwards с учетными записями в платформе BI. После сопоставления ролей JD Edwards пользователи смогут входить в приложения платформы BI со своими учетными данными JD Edwards. Это устраняет необходимость повторного создания пользователей и групп в платформе BI.

4.2 Управление Enterprise и общими учетными записями

Поскольку аутентификация Enterprise является методом аутентификации, принятым по умолчанию для платформы BI, она автоматически включается при первоначальной установке системы. При добавлении пользователей и групп и управлении пользователями и группами платформа BI хранит сведения о пользователях и группах в базе данных.

Примечание:

Когда пользователи завершают веб-сеанс в платформе BI, перейдя на страницу, не имеющую отношения к платформе, или закрыв веб-браузер, их сеанс Enterprise не завершается, а лицензия сохраняется. Сеанс Enterprise завершится примерно через 24 часа. Для завершения сеанса Enterprise и освобождения лицензии для других пользователей необходимо выйти из платформы BI.

4.2.1 Создание учетной записи пользователя

При создании нового пользователя обязательно укажите его свойства и принадлежность к группе или группам.

1. Перейдите в область управления «Пользователи и группы» консоли СМС.
2. Выберите **Управление > Создать > Новый пользователь**.

Появится диалоговое окно «Новый пользователь».

3. Чтобы создать пользователя Enterprise:

- a. Щелкните **Enterprise** в списке **Тип аутентификации**.
- b. Введите имя учетной записи, полное имя пользователя, адрес его электронной почты, прочую информацию описательного характера.

Совет:

Используйте область описания для ввода дополнительной информации о пользователе или учетной записи.

- c. Укажите настройки пароля и данные о нем.

4. Чтобы создать пользователя для входа в систему с другим типом аутентификации, выберите соответствующий параметр из списка **Тип аутентификации** и введите имя учетной записи.

5. Задайте способ определения учетной записи пользователя в соответствии с параметрами, указанными в лицензионном соглашении платформы SAP BusinessObjects Business Intelligence. Если лицензионное соглашение основано на ролях пользователя, выберите один из следующих параметров:

- **BI Viewer** : доступ к приложениям платформы BI для всех учетных записей роли BI Viewer определяется в лицензионном соглашении. Пользователи ограничены доступом к рабочим процессам приложений, которые определены для роли BI Viewer. Права доступа обычно ограничены просмотром документов Business Intelligence. Эта роль обычно подходит для пользователей, которые используют контент через приложения платформы.
- **BI Analyst** : доступ к приложениям платформы BI для всех учетных записей роли BI Analyst определяется в лицензионном соглашении. Пользователи могут обращаться ко всем рабочим процессам приложений, которые определены для роли BI Analyst. Права доступа включают просмотр и изменение документов Business Intelligence. Эта роль обычно подходит для пользователей, которые создают и изменяют контент для приложений платформы.

Если лицензионное соглашение не основано на ролях пользователя, укажите тип подключения к учетной записи пользователя.

- Выберите **Конкурентный пользователь**, если пользователь использует лицензионное соглашение, дающее право на подключение в конкурентном режиме.
- Выберите **Именованный пользователь**, если пользователь использует собственную лицензию для доступа. Лицензии зарегистрированного пользователя удобны для людей, которым необходим доступ к платформе BI независимо от числа других подключенных пользователей в данный момент.

6. Нажмите кнопку **Создать и закрыть**.

Пользователь будет зарегистрирован в системе и автоматически добавлен в группу "Все". Для пользователя автоматически создается папка "Входящие" и псевдоним Enterprise. Теперь можно добавлять пользователя в группы или назначать ему права.

См. также

- [Права на платформе BI](#)
- [Лицензирование на основе ролей](#)

4.2.2 Для изменения учетной записи пользователя

Используйте эту процедуру для изменения свойств пользователя или элемента группы.

Примечание:

Внесенные изменения отразятся на пользователе при следующем входе в систему.

1. Перейдите в область управления «Пользователи и группы» консоли СМС.
2. Выберите пользователя, свойства которого хотите изменить.
3. Выберите команду **Управление > Свойства**.

Откроется диалоговое окно «Свойства» для этого пользователя.

4. Изменить свойства пользователя.

В дополнение ко всем доступным при первом создании учетной записи параметрам, теперь вы можете отключить учетную запись, установив флажок **Учетная запись отключена**.

Примечание:

Любые проведенные изменения учетной записи отразятся на пользователе только при следующем входе в систему.

5. Нажмите кнопку **Сохранить и закрыть**.

См. также

- [Для создания нового псевдонима существующего пользователя](#)

4.2.3 Чтобы удалить учетную запись пользователя

Следуйте данной инструкции, чтобы удалить учетную запись пользователя. Может появиться сообщение об ошибке, если пользователь входит в систему после удаления его учетной записи. При удалении учетной записи пользователя удаляются также папка "Избранное", личные категории и папка "Входящие" этого пользователя.

Если вы думаете, что пользователю потребуется доступ к учетной записи в будущем, то вместо удаления учетной записи установите флажок в ячейке **Учетная запись отключена** в диалоговом окне «Свойства» для выбранного пользователя.

Примечание:

Удаление учетной записи не обязательно лишает пользователя возможности войти в платформу BI снова. Если учетная запись пользователя также существует в сторонней системе и принадлежит сторонней группе, для которой установлено соответствие в платформе BI, пользователь все равно сможет войти в систему.

1. Перейдите в область управления «Пользователи и группы» консоли СМС.
2. Выберите пользователя, которого нужно удалить.
3. Выберите **Управление > Удалить**.

Появится диалоговое окно с запросом на подтверждение удаления.

4. Нажмите кнопку **ОК**.
Учетная запись пользователя будет удалена.

См. также

- [Для изменения учетной записи пользователя](#)
- [Чтобы удалить учетную запись пользователя](#)
- [Для отключения псевдонима](#)

4.2.4 Чтобы создать новую группу

1. Перейдите в область управления «Пользователи и группы» консоли СМС.
2. Выберите **Управление > Создать > Новая группа**.
Появится диалоговое окно «Создать новую группу пользователей».
3. Введите имя и описание группы.
4. Нажмите кнопку **ОК**.

После создания группы можно добавить в нее пользователей или подгруппы, а также задать для нее принадлежность к группе, чтобы она стала подгруппой. Поскольку подгруппы представляют собой дополнительные уровни организационной структуры, они используются при назначении прав объекта для осуществления контроля над доступом пользователей к содержанию платформы VI.

4.2.5 Для изменения свойств группы

Вы можете изменить свойства группы, изменив любую из этих настроек.

Примечание:

Изменение группы отразится на принадлежащих ей пользователях при их следующем входе в систему.

1. В области управления СМС «Пользователи и группы» выберите группу.
2. Выберите команду **Управление > Свойства**.
Отобразится диалоговое окно «Свойства».

3. Измените свойства группы.

Для открытия различных диалоговых окон переходите по ссылкам в списке навигации и изменяйте различные свойства.

- Если требуется изменить заголовок или описание группы, нажмите кнопку **Свойства**.
- Если требуется изменить права принципалов на доступ к данной группе, нажмите кнопку **Безопасность пользователей**.
- Если требуется изменить значения профилей для членов группы, нажмите кнопку **Значения профиля**.
- Если требуется добавить эту группу в другую группу в качестве подгруппы, нажмите кнопку **Член**.

4. Щелкните **Сохранить**.

4.2.6 Просмотр членов групп

Эту процедуру можно использовать для просмотра пользователей, принадлежащих определенной группе.

1. Перейдите в область управления «Пользователи и группы» консоли СМС.
2. Раскройте список **Иерархия групп** на панели **Дерево**.
3. Выберите группу на панели **Дерево**.

Примечание:

Если в группе содержится большое число пользователей или группа отображена в стороннем каталоге, вывод списка может занять несколько минут.

Отображается список пользователей, принадлежащих группе.

4.2.7 Чтобы добавить подгруппы

В группу можно добавить другие группы. При этом добавляемые группы становятся подгруппами.

Примечание:

Процедура добавления подгрупп имеет сходство с процедурой выбора состава группы.

1. В области управления «Пользователи и группы» консоли СМС выберите группу, которую нужно добавить в другую группу в качестве подгруппы.
2. Выберите **Действия > Присоединиться к группе**.
Будет открыто диалоговое окно «Присоединиться к группе».
3. Переместите группу, в которую нужно добавить первую группу, из списка **Доступные группы** в список **Группы-места назначения**.
4. Нажмите кнопку **ОК**.

См. также

- [Задание принадлежности к группе](#)

4.2.8 Задание принадлежности к группе

Группу можно сделать членом другой группы. В этом случае ставшая членом группа называется подгруппой. Группа, в которую была добавлена подгруппа, называется родительской группой. Подгруппа наследует права родительской группы.

1. В области управления «Пользователи и группы» консоли СМС выберите группу, которую нужно добавить в другую группу.
2. Выберите **Действия > Участник**.
Появится диалоговое окно «Член».
3. Нажмите кнопку **Присоединиться к группе**.
Появится диалоговое окно «Присоединиться к группе».
4. Переместите группу, в которую нужно добавить первую группу, из списка **Доступные группы** в список **Группы-места назначения**.
Любые права, связанные с родительской группой, будут унаследованы новой созданной группой.
5. Нажмите кнопку **ОК**.
Вы вернетесь в диалоговое окно «Член», а в списке родительских групп отобразится данная родительская группа.

4.2.9 Удаление группы

Если группа больше не требуется, ее можно удалить. Удаление групп по умолчанию (Администратор и Все) невозможно.

Примечание:

- Изменения будут применять к пользователям, принадлежащим удаленной группе, при следующем входе в систему.
- Пользователи, принадлежащие удаленной группе, теряют все права, наследуемые от группы.

Для удаления сторонней группы аутентификации, такой как группа пользователей Windows AD, используйте область управления «Аутентификация» на консоли СМС.

1. Перейдите в область управления «Пользователи и группы» консоли СМС.
2. Выберите группу, которую необходимо удалить.

3. Выберите **Управление > Удалить**.

Появится диалоговое окно с запросом на подтверждение удаления.

4. Нажмите кнопку **ОК**.

Группа удалена.

4.2.10 Чтобы включить учетную запись Гостя

По умолчанию учетная запись гостя отключена, чтобы никто не мог войти в платформу BI при помощи этой учетной записи. Данная настройка по умолчанию также отключает функцию анонимного единого входа в платформу BI, так что пользователи не смогут получить доступ к стартовой панели BI, не предоставив действительные имя пользователя и пароль.

Выполните это действие, если хотите включить учетную запись гостя, чтобы пользователям не требовались собственные учетные записи для доступа к стартовой панели BI.

1. Перейдите в область управления «Пользователи и группы» консоли СМС.

2. Щелкните **Список пользователей** на панели **Навигация**.

3. Выберите **Гость**.

4. Выберите команду **Управление > Свойства**.

Отобразится диалоговое окно «Свойства».

5. Снимите флажок в ячейке **Учетная запись отключена**.

6. Нажмите кнопку **Сохранить и закрыть**.

4.2.11 Добавление пользователей в группы

Существует несколько методов добавления пользователей в группы:

- Выберите группу, а затем выберите **Действия > Добавить участников в группу**.
- Выберите пользователя, а затем выберите **Действия > Участник**.
- Выберите пользователя, а затем выберите **Действия > Присоединиться к группе**.

Далее указано, как добавить пользователей в группы с помощью этих методов.

См. также

- [Задание принадлежности к группе](#)

4.2.11.1 Чтобы добавить пользователя в одну или несколько групп

1. Перейдите в область управления «Пользователи и группы» консоли СМС.
2. Выберите пользователя, которого нужно добавить в группу.
3. Выберите **Действия > Присоединиться к группе**.

Примечание:

Все пользователи платформы ВІ в системе являются частью группы "Все".

Будет открыто диалоговое окно «Присоединиться к группе».

4. Переместите группу, в которую нужно добавить пользователя, из списка **Доступные группы** в список **Группы-места назначения**.

Совет:

Используйте сочетание клавиши **SHIFT +** и щелчок мышью или **CTRL +** и щелчок мышью для выбора нескольких групп.

5. Нажмите кнопку **ОК**.

4.2.11.2 Чтобы добавить одного или нескольких пользователей в группу

1. В области управления «Пользователи и группы» в СМС выберите группу.
2. Выберите **Действия > Добавить участников в группу**.
Появится диалоговое окно «Добавление».
3. Щелкните **Список пользователей**.
Список **Доступные пользователи/группы** будет обновлен, и в нем отобразятся все учетные записи пользователей в системе.
4. Переместите пользователя, которого нужно добавить в группу, из списка **Доступные пользователи/группы** в список **Выбранные пользователи/группы**.

Совет:

- Для выбора нескольких пользователей используйте клавишу **SHIFT +** и щелчок кнопки **мышы**, или же клавишу **CTRL +** и щелчок кнопки **мышы**.
 - Чтобы найти какого-либо пользователя, используйте поле поиска.
 - Если в системе много пользователей, используйте для перехода по списку пользователей кнопки "Назад" и "Далее".
5. Нажмите кнопку **ОК**.

4.2.12 Изменение настроек пароля

В СМС можно изменить настройки пароля для конкретного пользователя или для всех пользователей системы. Различные ограничения, приведенные ниже, применимы только к учетным записям Enterprise, т. е. эти ограничения не применимы к учетным записям, для которых создано соответствие в базе данных внешнего пользователя (LDAP или Windows AD). Обычно, тем не менее, внешняя система позволяет задать те же ограничения для внешних учетных записей.

4.2.12.1 Чтобы изменить настройки пароля пользователя

1. Перейдите в область управления «Пользователи и группы» консоли СМС.
2. Выберите пользователя, настройки пароля которого нужно изменить.
3. Выберите команду **Управление > Свойства**.
Отобразится диалоговое окно «Свойства».
4. Установите или снимите флажок в поле, связанном с параметром пароля, который нужно изменить.
Доступны следующие варианты:
 - **Пароль не ограничен по сроку действия**
 - **Пользователю следует изменить пароль при следующем входе в систему**
 - **Пользователь не может изменить пароль**
5. Нажмите кнопку **Сохранить и закрыть**.

4.2.12.2 Чтобы изменить общие настройки пароля

1. Перейдите в область управления СМС «Аутентификация».
2. Дважды щелкните **Enterprise**.
Появится диалоговое окно «Enterprise».
3. Установите флажок в ячейке каждой необходимой настройки пароля и введите значение при необходимости.
В следующей таблице указаны минимальные и максимальные значения для каждой настройки.

Таблица 4-4: Настройки пароля

Настройка пароля	Минимум	Рекомендованный максимум
Принудительно устанавливать пароли с символами в разных регистрах	Н/Д	Н/Д
Должен содержать не менее N символов	0 символов	64 символа
Должен изменять пароль каждые N дн.:	1 день	100 дней
Не может повторно использовать N последних паролей:	1 пароль	100 паролей
Должен ждать N мин для изменения пароля:	0 минут	100 минут
Отключать учетную запись после N неудачных попыток входа:	1 неудачная попытка	100 неудачных попыток
Сбрасывать счетчик неудачных попыток через N мин:	1 минута	100 минут
Повторно включать учетную запись через N мин:	0 минут	100 минут

4. Нажмите кнопку **Обновить**.

4.2.13 Предоставление доступа пользователям и группам

Пользователям и группам можно предоставить административный доступ к другим пользователям и группам. В права администратора входит просмотр, редактирование и удаление объектов; просмотр и удаление экземпляров объектов; а также приостановка экземпляров объектов. Например, в целях обнаружения и устранения неполадок или обслуживания системы, может быть необходимо предоставить отделу ИТ доступ к редактированию и удалению объектов.

См. также

- [Для назначения принципалов списку управления доступом к объекту](#)

4.2.14 Управление доступом к каталогам "Входящие" пользователей

При добавлении пользователя в системе автоматически создается каталог "Входящие" для пользователя. Каталог "Входящие" присваивается имя пользователя. По умолчанию права доступа к каталогу "Входящие" пользователя есть только у пользователя и администратора.

См. также

- [Планирование немедленного запуска объекта](#)
- [Управление настройками безопасности для объектов в СМС](#)

4.2.15 Настройка параметров стартовой панели BI

Администраторы могут устанавливать, какими способами пользователи осуществляют доступ к приложениям стартовой панели BI. С помощью настройки свойств в файле BOE.war можно указать, какая информация будет отображаться на экране входа пользователя в систему. СМС можно также использовать для установки предпочтений стартовой панели BI для конкретных групп.

4.2.15.1 Настройка экрана входа в систему стартовой панели BI

По умолчанию на экране входа в систему стартовой панели BI содержится запрос на ввод имени пользователя и пароля. Можно также настроить приглашение пользователей на ввод имени CMS и типа аутентификации. Чтобы изменить этот параметр, потребуется изменить свойства стартовой панели BI для файла BOE.war.

4.2.15.1.1 Настройка экрана входа в систему стартовой панели BI

Чтобы изменить параметры по умолчанию стартовой панели BI, необходимо задать пользовательские свойства стартовой панели BI для файла BOE.war. Развертывание этого файла выполняется на компьютере, на котором установлен сервер веб-приложений.

1. Перейдите в следующий каталог в папке установки платформы BI:

```
<INSTALLDIR>\SAP BusinessObjects Enterprise XI  
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\
```

Примечание:

Если используется версия Tomcat, установленная с платформой BI, то можно осуществлять доступ к следующему каталогу: C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom

- Если используется другой поддерживаемый сервер веб-приложений, обратитесь к документации по серверу веб-приложений, чтобы узнать путь.

2. Создайте новый файл.

Примечание:

Воспользуйтесь программой "Блокнот" или любым другим текстовым редактором.

3. Сохраните файл под следующим именем:

Bllaunchpad.properties

4. Чтобы включить в экран входа в систему стартовой панели BI параметры аутентификации, добавьте следующее:

```
authentication.visible=true
```

5. Чтобы изменить тип аутентификации по умолчанию, добавьте следующее:

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

Замените <authentication> любым из следующих вариантов

Тип аутентификации	значение <authentication>
Enterprise	secEnterprise
LDAP	secLDAP
Windows AD	secWinAD
SAP	secSAPR3

6. Чтобы запросить у пользователя имя CMC на экране входа в систему стартовой панели BI:

```
cms.visible=true
```

7. Сохраните и закройте файл.

8. Перезапустите сервер веб-приложений.

При помощи Wdeploy повторно разверните файл BOE.war на сервере веб-приложений. Для получения дополнительной информации об использовании WDeploy см. *Руководство по развертыванию веб-приложений платформы SAP BusinessObjects Business Intelligence*

4.2.15.2 Настройка предпочтительных параметров стартовой панели BI для групп

Администраторы могут задавать параметры стартовой панели BI для конкретных групп пользователей. Эти параметры используются как предпочтительные параметры по умолчанию стартовой панели BI для всех пользователей в группе.

Примечание:

Если пользователем были определены собственные параметры, никакие настройки, определенные администратором, не отражаются на их представлении стартовой панели BI. Пользователи всегда могут переключиться с собственных параметров на параметры, определенные администратором, и использовать обновленные настройки.

По умолчанию ни для одной группы пользователей не заданы параметры стартовой панели BI. Администраторы могут задавать параметры для следующих элементов:

- Вкладка "Домашняя страница"
- Документы – начальное местоположение
- Папки
- Категории
- Число объектов на страницу
- Столбцы, отображаемые на вкладке «Документ»
- Способ вывода документов на стартовой панели BI – на вкладках или в новом окне

4.2.15.2.1 Задание параметров стартовой панели BI для группы

1. Перейдите в область управления «Пользователи и группы» консоли CMC.
2. Выберите группу из списка групп.
3. Выберите **Действия > Предпочтения стартовой панели BI**
Будет открыто диалоговое окно «Предпочтения стартовой панели BI».
4. Снимите флажок **Предпочтения не определены**.
5. Чтобы задать начальное представление пользователя:
 - Чтобы вывести вкладку Домашняя страница при первом входе пользователя в систему, щелкните вкладку **Домашняя страница** и выберите один из следующих параметров:

Действие	Описание
Домашняя страница по умолчанию	Служит для вывода вкладки Домашняя страница по умолчанию при использовании платформы BI.
Выбор домашней страницы	<p>Выводит определенный веб-сайт как вкладку домашней страницы.</p> <p>Нажмите кнопку Обзор домашней страницы. В окне «Выбор пользовательской домашней страницы» выберите объект репозитория и нажмите кнопку Открыть.</p> <p>Примечание: Можно выбирать только объект, который уже был добавлен в репозиторий.</p>

- Чтобы вывести вкладку Документы при первом входе пользователя, выберите **Документы** и задайте выдвижную панель и узел, открываемые по умолчанию. Можно выбрать из следующих возможностей:

Выдвижная панель	Параметры узла
Мои документы	<p>Выберите одну из следующих возможностей для вывода на вкладке Документы:</p> <ul style="list-style-type: none"> Мое избранное Личные категории Мои входящие
Папки	<p>Выберите одну из следующих возможностей:</p> <ul style="list-style-type: none"> Общие папки: используется для вывода общих папок на вкладке Документы Выберите общую папку <p>Щелкните Выбор папки, чтобы выбрать конкретную общую папку для вывода на вкладке Документы</p>
Категории	<p>Выберите одну из следующих возможностей:</p> <ul style="list-style-type: none"> Корпоративные категории: используется для вывода корпоративных категорий на вкладке Документы Выберите корпоративную категорию <p>Щелкните Выбор, чтобы выбрать конкретную корпоративную категорию для вывода на вкладке Документы.</p>

Например, если требуется, чтобы при первом входе открывалась выдвижная панель папки "Входящие" BI пользователя **Мои документы**, выберите **Мои документы** и щелкните **Мои входящие**.

6. В разделе «Выберите столбцы для отображения на вкладке "Документы"» выберите итоговую информацию, которую следует выводить для каждого объекта на панели пользователя Список:
- **Тип**
 - **Дата последнего запуска**
 - **Экземпляры**
 - **Описание**
 - **Автор**
 - **Создано**
 - **Расположение (категории)**
 - **Получено (входящие)**
 - **Отправлено (входящие)**
7. В области «Установка расположения просмотра документов» выберите способ просмотра документов пользователями.
- Пользователи имеют возможность открытия документов для просмотра в новых вкладках на стартовой панели BI или в новых окнах веб-браузера.
8. В поле **Установка максимального числа элементов на странице** задайте максимальное число объектов, отображаемых на странице при просмотре списков объектов.
9. Нажмите кнопку **Сохранить и закрыть**.

Заданные параметры будут использоваться по умолчанию для пользователей в группе, выбранной на шаге 2. Однако, у пользователей будет возможность создания своих собственных предпочтений стартовой панели BI при наличии у них права на задание собственных параметров. Если требуется, чтобы пользователи не могли изменять предпочтительные параметры, не следует предоставлять им право на задание параметров.

4.3 Управление псевдонимами

Если для пользователя создано несколько учетных записей в платформе BI, можно связать учетные записи с использованием функции "Назначить псевдоним". Это необходимо при наличии у пользователя сторонней учетной записи, назначенной системе Enterprise, и учетной записи Enterprise.

При назначении псевдонима пользователь может выполнять вход с использованием как стороннего имени пользователя и пароля, так и имени пользователя и пароля Enterprise. Таким образом, псевдоним позволяет пользователю входить в систему с использованием нескольких типов аутентификации.

На консоли СМС информация о псевдониме отображается в нижней части диалогового окна «Свойства» для пользователя. У пользователя может быть любая комбинация псевдонимов Enterprise, LDAP и Windows AD.

4.3.1 Чтобы создать пользователя и добавить сторонний псевдоним

При создании пользователя и выборе типа аутентификации, отличного от Enterprise, система создает нового пользователя в платформе BI и сторонний псевдоним для этого пользователя.

Примечание:

Для того чтобы система создала сторонний псевдоним, должны выполняться следующие критерии:

- Необходимо предварительно включить в СМС инструмент аутентификации.
 - Формат имени учетной записи должен соответствовать формату, требуемому для типа аутентификации.
 - Учетная запись пользователя должна существовать в стороннем инструменте аутентификации и должна принадлежать к группе, для которой уже создано соответствие в платформе BI.
1. Перейдите в область управления «Пользователи и группы» консоли СМС.
 2. Выберите **Управление > Создать > Новый пользователь**.
Появится диалоговое окно «Новый пользователь».
 3. Выберите тип аутентификации для пользователя, например Windows AD.
 4. Введите имя сторонней учетной записи для пользователя, например bsmith.
 5. Выберите тип соединения для пользователя.
 6. Нажмите кнопку **Создать и закрыть**.

Пользователь добавляется в платформу BI и ему присваивается псевдоним для выбранного типа аутентификации, например, secWindowsAD:ENTERPRISE:bsmith. При необходимости можно добавлять и снова присваивать псевдонимы пользователям.

4.3.2 Для создания нового псевдонима существующего пользователя

Псевдонимы можно создавать для существующих пользователей платформы BI. Этот псевдоним может быть псевдонимом Enterprise или псевдонимом стороннего инструмента аутентификации.

Примечание:

Для того чтобы система создала сторонний псевдоним, должны выполняться следующие критерии:

- Необходимо предварительно включить в СМС инструмент аутентификации.
- Формат имени учетной записи должен соответствовать формату, требуемому для типа аутентификации.
- Учетная запись пользователя должна существовать в стороннем инструменте аутентификации и должна принадлежать к группе, для которой создано соответствие в платформе BI.

1. Перейдите в область управления «Пользователи и группы» консоли СМС.
2. Выберите пользователя, которому будет присвоен псевдоним.
3. Выберите команду **Управление > Свойства**.
Отобразится диалоговое окно «Свойства».
4. Нажмите кнопку **Новый псевдоним**.
5. Выберите тип аутентификации.
6. Введите имя учетной записи пользователя.
7. Нажмите кнопку **Обновить**.

Псевдоним пользователя создан. При просмотре этого пользователя в СМС отображается, по крайней мере, два псевдонима – текущий и вновь созданный.

8. Нажмите **Сохранить и закрыть** для выхода из диалогового окна «Свойства».

4.3.3 Для присвоения псевдонима пользователю

При назначении псевдонима пользователю вы перемещаете сторонний псевдоним другого пользователя к пользователю, данные которого вы просматриваете. Вы не можете назначить или переприсвоить псевдонимы Enterprise.

Примечание:

Если пользователь имеет только один псевдоним, и вы присвоили его другому пользователю, система удалит учетную запись пользователя, а также его папки "Избранное", "Входящие" и категории.

1. Перейдите в область управления «Пользователи и группы» консоли СМС.
2. Выберите пользователя, которому вы хотите назначить псевдоним.
3. Выберите команду **Управление > Свойства**.
Отобразится диалоговое окно «Свойства».
4. Нажмите **Назначить псевдоним**.
5. Введите учетную запись пользователя, которому хотите назначить псевдоним, и нажмите **Найти**.
6. Переместите псевдоним, который хотите назначить, из списка **Доступные псевдонимы** в список **Псевдонимы для добавления к Имя пользователя**.

В данном случае *Имя пользователя* представляет собой имя пользователя, которому вы присваиваете псевдоним.

Совет:

Для выбора нескольких псевдонимов используйте клавишу **SHIFT +** и щелчок кнопки мыши, или же клавишу **CTRL +** и щелчок кнопки мыши.

7. Нажмите кнопку **ОК**.

4.3.4 Для удаления псевдонима

Когда вы удаляете псевдоним, он удаляется из системы. Если у пользователя имеется только один псевдоним, и вы его удаляете, система автоматически удалит учетную запись пользователя и его папки "Избранное", "Входящие" и категории.

Примечание:

Удаление псевдонима пользователя не обязательно приведет к тому, что пользователь не сможет выполнить вход в платформу BI снова. Если учетная запись пользователя до сих пор существует в сторонней системе и принадлежит группе, отображенной в платформе BI, система будет разрешать этому пользователю выполнять вход. Будет ли система создавать нового пользователя или присваивать псевдоним существующему, зависит от того, какие параметры обновления вы выбрали в инструменте аутентификации в области управления СМС «Аутентификация».

1. Перейдите в область управления «Пользователи и группы» консоли СМС.
2. Выберите пользователя, псевдоним которого требуется удалить.
3. Выберите команду **Управление > Свойства**.
Отобразится диалоговое окно «Свойства».
4. Нажмите кнопку **Удалить псевдоним** рядом с псевдонимом, который хотите удалить.
5. При запросе подтверждения нажмите кнопку **ОК**.
Псевдоним удален.
6. Нажмите кнопку **Сохранить и закрыть** для выхода из диалогового окна «Свойства».

4.3.5 Для отключения псевдонима

Можно запретить пользователю выполнять вход в платформу BI, используя метод частичной аутентификации, который заключается в отключении псевдонима пользователя, связанного с этим методом. Чтобы запретить пользователю вход в платформу BI, отключите все псевдонимы для этого пользователя.

Примечание:

Удаление пользователя из системы не обязательно обеспечивает недоступность повторного выполнения входа для этого пользователя в платформу BI. Если учетная запись пользователя до сих пор существует в сторонней системе и принадлежит группе, отображенной в платформе BI, система будет разрешать этому пользователю выполнять вход. Чтобы убедиться в том, что пользователь больше не сможет использовать ни один из своих псевдонимов для входа в платформу, лучше отключить псевдоним.

1. Перейдите в область управления «Пользователи и группы» консоли СМС.
2. Выберите пользователя, псевдоним которого хотите отключить.

3. Выберите команду **Управление > Свойства**.

Отобразится диалоговое окно «Свойства».

4. Снимите флажок **Активизировано** у псевдонима, который необходимо отключить.

Повторите этот шаг для каждого из псевдонимов, которые необходимо отключить.

5. Нажмите кнопку **Сохранить и закрыть**.

Теперь пользователь больше не сможет войти в систему, используя метод аутентификации, который был отключен.

См. также

- [Для удаления псевдонима](#)

Установка прав

5.1 Права на платформе BI

Права – это основные организационные единицы, которые контролируют пользовательский доступ к объектам, приложениям, серверам и другим компонентам платформы BI. Они играют важную роль в защите системы, указывая индивидуальные действия, которые пользователь может выполнять над объектами. Кроме того, что права контролируют доступ к содержимому платформы BI, они позволяют осуществлять управление пользователями и группами на уровне различных подразделений и обеспечивают ИТ-персоналу административный доступ к серверам и группам серверов.

Важно отметить, что лучше назначать права объектам (например, отчетам) и папкам, чем «принципалам» (пользователям или группам), имеющим к ним доступ. Например, чтобы предоставить менеджеру доступ к конкретной папке, в области «Папки» вы должны добавить менеджера в «список контроля доступа» (список владельцев учетных записей, которые имеют доступ к объекту) для этой папки. Вы не можете просто предоставить менеджеру доступ к папке, настроив его права в области «Пользователи и группы». Настройки прав в области «Пользователи и группы» используются для предоставления другим владельцам учетных записей (например, администраторам) доступа к менеджеру как объекту системы. В этом случае сами владельцы учетных записей выступают в роли объектов для владельцев учетных записей с правами более высокого уровня, управляющих ими.

Каждое право на объект может быть предоставлено, отменено или не задействовано. Модель защиты платформы BI построена таким образом, что если право не указано, это значит, что оно не предоставлено. К тому же, если в результате настроек получилось, что одно и то же право предоставлено и отменено, право не предоставляется. Модель «на основе запретов» позволяет обеспечить, чтобы пользователь или группа не могли автоматически получить права, которые явно не назначены.

Но есть важное исключение из этого правила. Если право установлено только на дочерний объект и противоречит правам, унаследованным от родительского объекта, права дочернего объекта доминируют над родительским. Это правило применяется и к пользователям, которые являются членами групп. Если пользователю предоставлено право, которое отменено для всей группы, право сохраняется за пользователем и доминирует над унаследованными от группы правами.

См. также

- [Переопределение прав](#)

5.1.1 Уровни доступа

«Уровни доступа» – это группы полномочий, которые часто необходимы пользователям. С их помощью администраторы могут быстро и единообразно определять общие уровни безопасности, а не индивидуальные права по отдельности.

Платформа BI поставляется с несколькими уже настроенными уровнями доступа. Заданные уровни доступа основаны на модели расширения прав, которая начинается с уровня **Просмотр** и заканчивается уровнем **Полное управление**, каждый уровень доступа включает в себя права предыдущего уровня.

Однако можно также создавать и настраивать свои собственные уровни доступа; это поможет значительно сократить административные и эксплуатационные затраты, связанные с безопасностью. Рассмотрим ситуацию, в которой администратор должен создать две группы: менеджеры по продажам и продавцы. Обе группы нуждаются в доступе к пяти отчетам платформы BI, но менеджерам по продажам потребуется больше прав, чем продавцам. Заранее определенные в системе уровни доступа не соответствуют требованиям ни одной из групп. Вместо добавления групп в каждый отчет как владельцев учетных записей и изменения их прав в пяти различных местах, администратор может создать два новых уровня доступа: "Менеджеры по продажам" и "Продавцы". Затем администратор может добавить обе группы владельцев учетных записей к отчетам и назначить требуемые уровни доступа. Когда права потребуются изменить, администратор может изменить уровни доступа. Так как уровни доступа применены к обеим группам, работающим с пятью отчетами, права на работу с отчетами, которые имеются у этих групп, автоматически обновляются.

См. также

- [Работа с уровнями доступа](#)


5.1.2 Параметры расширенных прав

Для предоставления возможности полного управления безопасностью объекта в СМС можно установить «Расширенные права». Эти расширенные права повышают гибкость настройки, поскольку позволяют детально определять безопасность объектов.

Используйте параметры расширенных прав, например, если необходимо настроить права принципала для определенного объекта или набора объектов. Более того, используйте расширенные права для явного запрета любого права пользователя или группы, которое будет запрещено изменять в будущем при изменении уровней безопасности составов групп или папки.

В следующей таблице приводятся сводные сведения о параметрах, используемых при настройке расширенных прав.

Таблица 5-1: Параметры прав

Значок	Параметр прав	Описание
	Предоставлено	Право предоставлено принципалу.
	Запрещено	Право запрещено для принципала.
	Не задано	Право не определено для принципала. По умолчанию, если для прав установлено значение Не задано , то права запрещены.
	Применить к объекту	Право применяется к объекту. Этот параметр становится доступен при выборе Предоставлено или Запрещено .
	Применить к подобъекту	Право применяется к подобъектам. Этот параметр становится доступен при выборе Предоставлено или Запрещено .

См. также

- [Права для конкретных типов объектов](#)

5.1.3 Наследование

Права на объект устанавливаются для принципала в целях управления доступом к объекту; однако устанавливать явное значение каждого возможного права для каждого принципала на каждый объект непрактично. Возьмем для примера систему с 100 прав, 1000 пользователей и 10000 объектов: чтобы установить явное право на каждый объект, CMS потребовалось бы хранить миллиарды прав в своей памяти и, что более важно, администратору пришлось бы устанавливать каждое право вручную.

Шаблоны наследования помогают этого избежать. Благодаря наследованию, права пользователей на объекты системы проистекают из сочетания их членства в различных группах и подгруппах и из объектов, которые имеют унаследовали права от родительских папок и подпапок. Эти пользователи могут наследовать права, так как являются членами группы; подгруппы могут наследовать права от родительских групп; и пользователи, и группы могут наследовать права от родительских папок.

По умолчанию пользователи или группы, которые имеют права на папку, унаследуют те же права на любой объект, который в последствии будет опубликован в эту папку. Следовательно, лучшей стратегией является установка соответствующих прав для пользователей и групп сначала на уровне папки, а потом публиковать в эту папку объекты.

Платформа BI распознает два типа наследования: наследование группы и наследование папки.

5.1.3.1 наследование групп

Наследование группы позволяет принципалу наследовать права на основе принадлежности группе. Наследование группы особенно необходимо при организации всех пользователей в группы, которые соответствуют текущим соглашениям о безопасности, принятым в организации.

В «первом примере наследования группы» можно увидеть принципы работы наследования группы. Красная группа является группой, вложенной в синюю группу, поэтому она наследует права синей группы. В этом случае она наследует право 1 как предоставленное и остальные права как неопределенные. Каждый член красной группы наследует эти права. Кроме того, все остальные права, которые настроены во вложенной группе, наследуются ее элементами. В этом примере зеленый пользователь является членом красной группы, поэтому он наследует право 1 как предоставленное, права 2, 3, 4 и 6 как неопределенные и право 5 как запрещенное.

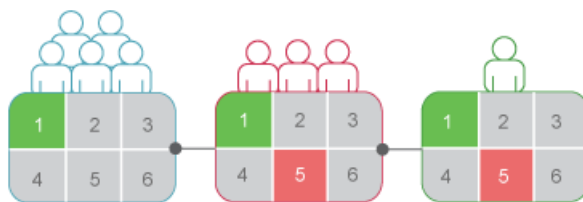


Рис. 5-1: Пример наследования группы 1

Если наследование группы включено для пользователя, который принадлежит нескольким группам, права всех родительских групп учитываются во время проверки системой учетных данных. Право запрещено пользователю, если оно явно запрещено в любой родительской группе или полностью не определено; поэтому пользователю предоставляются только те права, которые назначены в одной или нескольких группах (явно или с помощью уровней доступа) и явно не запрещены.

Во «втором примере наследования группы» зеленый пользователь является членом двух неродственных групп. От синей группы он наследует права 1 и 5 как предоставленные и остальные права как неопределенные; однако, поскольку зеленый пользователь также принадлежит красной группе и в красной группе явно запрещено право 5, наследование зеленым пользователем права 5 от синей группы отменяется.

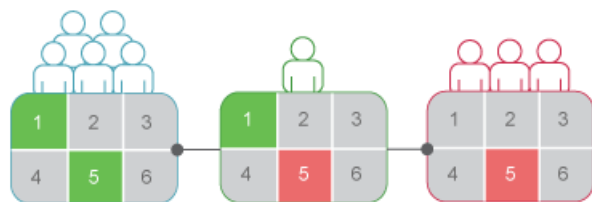


Рис. 5-2: Пример наследования группы 2

См. также

- [Переопределение прав](#)

5.1.3.2 Наследование папок

Наследование папок позволяет владельцам учетных записей наследовать права, которые были присвоены им для работы с папкой родительского объекта. Наследование папки используется при организации содержимого платформы BI в иерархии папки, отображающей соглашения текущей безопасности организации. Например, представьте, что вы создали папку под названием "Отчеты о продажах", а персоналу отдела продаж в группе "Продажи" предоставили доступ **Просмотр по требованию** к этой папке. По умолчанию, каждый пользователь, имеющий права на работу с папкой "Отчеты о продажах", унаследует те же самые права и на отчеты, которые вы впоследствии будете добавлять в эту папку. Поэтому, группа "Продажи" будет иметь права доступа **Просмотр по требованию** на все отчеты, а права на объект вам потребуется установить всего лишь один раз, на уровне папки.

В «Примере наследования папок» права на работу с папкой могут быть установлены для "Красной группы". Права 1 и 5 были предоставлены, а остальные не были указаны. Если наследование папок включено, члены "Красной группы" будут иметь права на уровне объекта, идентичные правам группы на уровне папки. Права 1 и 5 будут унаследованы, а остальные останутся неиспользованными.

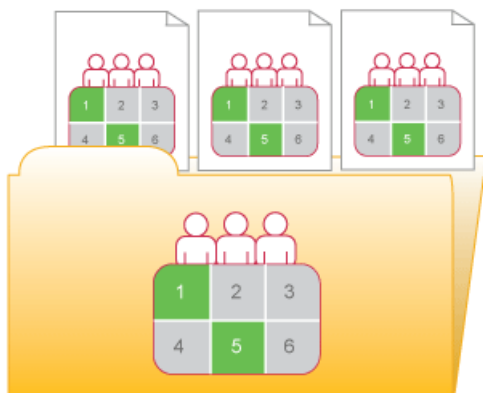


Рис. 5-3: Пример наследования папок

См. также

- [Переопределение прав](#)

5.1.3.3 Переопределение прав

«Переопределение прав» – это поведение прав, в котором права, установленные на дочерние объекты, имеют приоритет над правами родительского объекта. Переопределение прав возникает при следующих обстоятельствах:

- Обычно права, установленные на дочерние объекты, доминируют над соответствующими правами, установленными на родительские объекты.
- Обычно права, установленные на подгруппы или на элементы групп, преобладают над соответствующими правами групп.

Вам не нужно блокировать наследование для установки настраиваемых прав на объект. Дочерний объект наследует настройки прав родительского объекта и содержит права, которые явно установлены на дочерний объект. Кроме того, любые изменения настроек прав родительского объекта применяются и к дочернему.

«Пример переопределения прав» иллюстрирует, как переопределение прав работает на родительских и дочерних объектах. Для пользователя Blue отменено право редактирования содержимого папки; настройки прав на папку наследуются вложенной папкой. Однако администратор предоставляет пользователю Blue право **Редактирования** документов во вложенной папке. Право на **Редактирование** документа, которое получил пользователь Blue, доминирует над унаследованными правами, назначенными папке и вложенной папке.

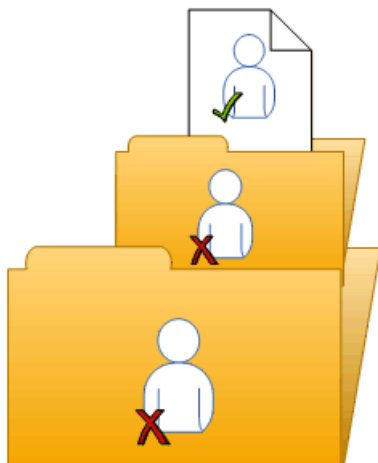


Рис. 5-4: Пример переопределения прав 1

«Пример переопределения прав 2» иллюстрирует, как переопределение прав работает с членами и группами. Для группы Blue отменено право редактирования папки; подгруппа Blue унаследовала эту настройку. Однако администратор предоставляет пользователю Blue, который является членом группы Blue и подгруппы Blue, права на **Редактирование** содержимого папки. Права на **Редактирование**, которые получил пользователь Blue, доминируют над унаследованными правами, назначенными группе и подгруппе Blue.

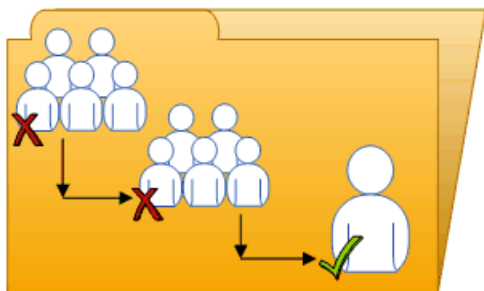


Рис. 5-5: Пример переопределения прав 2

«Комплексное переопределение прав» иллюстрирует ситуацию, в которой переопределение прав менее очевидно. Пользователь Purple является членом подгрупп 1A и 2A, которые соответственно принадлежат группам 1 и 2. Группы 1 и 2 имеют права Редактирования папки. Подгруппа 1A унаследовала права на **Редактирование** от группы 1, но администратор отменил права на **Редактирование** 2A. Эти настройки прав на 2A преобладают над настройками группы 2 благодаря переопределению прав. Однако пользователь Purple наследует противоречащие настройки прав из 1A от 2A. 1A и 2A не имеют между собой родительской и дочерней связи, поэтому переопределение прав не возникает; таким образом, настройки прав одной подгруппы не преобладают над настройками прав другой подгруппы, так как они имеют одинаковый статус. В конечном итоге права на **редактирование** для пользователя Purple отменяются согласно модели, основанной на «отмене» прав на платформе BI.

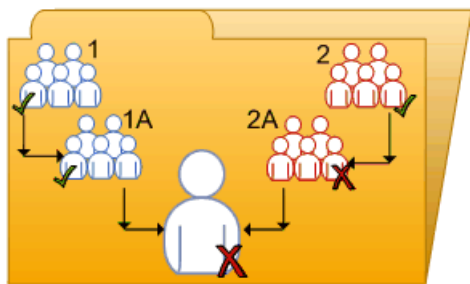


Рис. 5-6: Комплексное переопределение прав

Переопределение прав позволяет вам выполнять дополнительные корректировки настроек прав на дочерние объекты, без отмены всех унаследованных настроек. Представьте себе ситуацию, в которой менеджер по продажам нужно просмотреть конфиденциальные отчеты в папке "Конфиденциально". Менеджер по продажам является элементом группы "Продажи", для которой доступ к папке и ее содержимому отменен. Администратор предоставляет менеджеру права на **Просмотр** содержимого папки "Конфиденциально", но отмена доступа для группы "Продажи" действует. В этом случае права на **Просмотр**, предоставленные менеджеру по продажам, преобладают над отменой доступа, которую менеджер унаследовал благодаря принадлежности к группе "Продажи".

5.1.3.4 Область действия прав

«Область действия прав» относится к возможности ограничения пространства наследования прав. Для определения области действия прав необходимо решить, применяется ли право к объекту, подобъекту или к обоим компонентам. По умолчанию область действия прав распространяется и на объекты, и на подобъекты.

Область действия прав может использоваться для защиты личного содержимого в совместно используемых местоположениях. Представьте ситуацию, в которой финансовый отдел имеет совместно используемую папку "Требования затрат", в которой содержатся "Личные требования затрат" по каждому из сотрудников. Сотрудники хотят просматривать папку "Требования затрат" и добавлять туда объекты, но также они хотят защищать содержимое папок "Личные требования затрат". Администратор предоставляет всем сотрудникам права на **Просмотр** и **Добавление** записей в папку "Требования затрат", и ограничивает область действия этих прав только до папки "Требования затрат". Это означает, что права на **Просмотр** и **Добавление** не применимы к подобъектам папки "Требования затрат". Затем администратор предоставляет сотрудникам права на **Просмотр** и **Добавление** в их личные папки – "Личные требования затрат".

Области действия прав также могут сокращать эффективные права делегированного администратора. Например, делегированный администратор может иметь права **Редактирование** и **Защищенное изменение прав** по отношению к папке, но область действия этих прав ограничивается только этой папкой и не применима к ее подобъектам. Делегированный администратор не может предоставить другому пользователю права на один из подобъектов папки.

5.1.4 Права для конкретных типов объектов

«Права для конкретных типов объектов» – это права, которые влияют только на конкретные типы объектов, такие как отчеты Crystal, папки или уровни доступа. Права для конкретных объектов могут быть следующими:

- Общие права для типа объектов

Эти права идентичны общим глобальным правам (например, право добавлять, удалять или редактировать объект), но их устанавливают для конкретных типов объектов для переопределения настроек общих глобальных прав.

- Специальные права для типа объектов

Эти права доступны только для конкретных типов объектов. Например, право экспортировать данные отчета доступно для отчетов Crystal, но не для документов Word.

Диаграмма «Пример прав для конкретных типов объектов» иллюстрирует работу этих прав. Здесь право 3 представляет право на редактирование объекта. Группе Blue отказано в праве **редактировать** права в папке верхнего уровня, но ей предоставлено право **редактировать** отчеты Crystal в папке и подпапке. Такие права на **Редактирование** относятся только к отчетам Crystal и переопределяют настройки прав на общем глобальном уровне. В результате члены группы Blue имеют права на **Редактирование** отчетов Crystal, но не XLF-файла в подпапке.

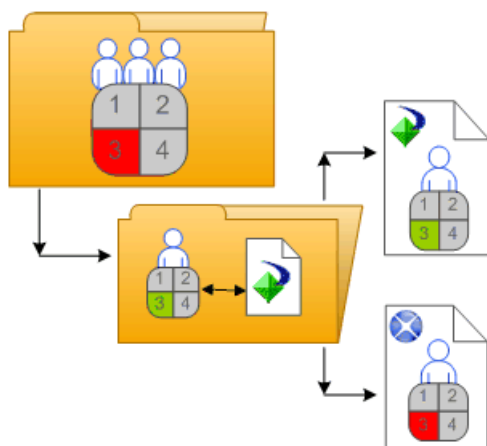


Рис. 5-7: Пример прав для конкретных типов объектов

Права для конкретных типов объектов полезны, потому что позволяют вам ограничивать права принципалов на основе типов объектов. Рассмотрим ситуацию, когда администратор хочет, чтобы сотрудники могли добавлять объекты в папку, но не могли создавать подпапки. Администратор предоставляет право на **Добавление** на общем глобальном уровне для папки, затем отзывает право на **Добавление** для типа объектов папки.

Права подразделяются на следующие коллекции на основе типов объектов, к которым они применяются:

- **Общие**

Эти права влияют на все объекты.

- **Содержимое**

Эти права делятся в зависимости от типа содержимого объектов. Примерами типов объектов являются отчеты Crystal и Adobe Acrobat PDF.

- **Приложение**

Эти права делятся в зависимости от того, на какое приложение платформы BI они влияют. Примерами приложений являются СМС и стартовая панель BI.

- **Система**

Эти права делятся в зависимости от того, на какой корневой компонент системы они влияют. Примерами корневых компонентов системы являются Календари, События, Пользователи и Группы.

Права для конкретных типов объектов находятся в коллекциях **Содержимое**, **Приложение** и **Система**. В каждой коллекции они далее подразделяются на категории по типам объектов.

5.1.5 Определение эффективных прав

При установке прав на объект помните о следующем:

- На каждом уровне доступа некоторые права предоставляются, некоторые отменяются, а некоторые остаются незадействованными. Когда пользователю предоставляется несколько уровней доступа, система группирует эффективные права и отменяет незадействованные по умолчанию.
- Когда вы назначаете владельцу учетной записи несколько уровней доступа к объекту, создается комбинация прав для каждого уровня доступа. Пользователю в группе «Несколько уровней доступа» назначено два уровня доступа. Один уровень предоставляет ему права под номерами 3 и 4, а другой – только права 3. Эффективными правами для пользователя будут права 3 и 4.

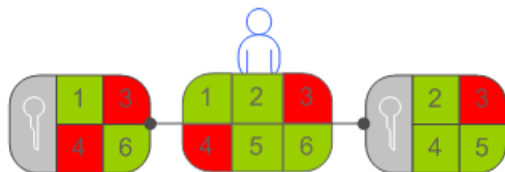


Рис. 5-8: Несколько уровней доступа

- В целях настройки прав владельца учетной записи на объект расширенные права можно комбинировать с уровнями доступа. Например, если какие-либо расширенные права на объект

и уровень доступа к нему назначены владельцу учетной записи, и расширенные права противоречат какому-либо праву этого уровня, расширенные права будут доминировать над данным правом уровня доступа.

Расширенные права могут переопределять соответствующие им права на уровнях доступа только когда они настроены у одного объекта для одного и того же владельца. Например, на общем глобальном уровне расширенные права на добавление будут доминировать над общими правами на добавление в уровне доступа, а над зависимым от типа правами на добавление не будут.

Однако, расширенные права не всегда доминируют над уровнем доступа. Например, владельцу учетной записи отказано в правах на **Редактирование** родительского объекта. При работе с дочерним объектом пользователю назначается уровень доступа, который предоставляет ему право **Редактирование**. В конечном итоге право **Редактирование**, предоставленное владельцу учетной записи для работы с дочерним объектом, сохраняется за ним, так как права, установленные по отношению к дочернему объекту, доминируют над правами на родительский объект.

- Такой принцип делает возможным доминирование прав, установленных на дочерний объект, над правами, унаследованными от родительского объекта.

5.2 Управление настройками безопасности для объектов в СМС

Можно управлять настройками безопасности большинства объектов в СМС, используя параметры безопасности в меню **Управление**. Эти параметры позволяют внести принципалов в список контроля доступа к объекту, просматривать права принципала, изменять права принципала в отношении объекта.

Сведения об управлении безопасностью изменяются в соответствии с требованиями безопасности и типом объекта, для которого вы устанавливаете права. Однако в целом последовательность выполнения операций для следующих задач одинаковая:

- Просмотр прав принципала в отношении объекта.
- Внесение принципала в список контроля доступа к объекту и указание, какие права и уровни доступа имеются у принципала.
- Настройка прав в папке верхнего уровня в платформе BI.

5.2.1 Для просмотра прав принципала на объект

Как правило, необходимо выполнить следующие действия, чтобы просмотреть права принципала на объект.

1. Выберите объект, настройки безопасности которого нужно просмотреть.
2. Выберите **Управление > Безопасность пользователя**.

Появится диалоговое окно «Безопасность пользователя» и отобразится список контроля доступа для объекта.

3. Выберите принципала в списке контроля доступа и нажмите кнопку **Просмотр безопасности**

Запустится «Просмотр полномочий» и отобразит список действующих прав принципала на объект. В дополнение к этому «Просмотр полномочий» позволяет сделать следующее:

- Перейдите к другому принципалу, чьи права требуется просмотреть.
- Отфильтровать отображаемые права в соответствии со следующими критериями:
 - назначенные права
 - предоставленные права
 - неназначенные права
 - с уровня доступа
 - тип объекта
 - имя права
- Отсортировать список прав, отображаемых по возрастанию или убыванию, в соответствии со следующими критериями:
 - коллекция
 - тип
 - имя права
 - статус права (предоставленное, отозванное или не указанное)

В дополнение к этому, можно щелкнуть одну из ссылок в колонке «Источник», чтобы отобразился источник наследованных прав.

5.2.2 Для назначения принципалов списку управления доступом к объекту

В списке управления доступом объекта содержится список пользователей, имеющих права доступа к данному объекту. По сути, вы назначаете принципала, имеющего доступ к списку управления доступом объекта и указываете набор прав, которыми он будет обладать по отношению к объекту.

1. Выберите объект, к которому будет добавлен принципал.

2. Выберите **Управление > Безопасность пользователя**.

Появится диалоговое окно «Безопасность пользователя» со списком управления доступом объекта.

3. Нажмите кнопку **Добавить принципалов**.

Появится диалоговое окно «Добавить принципалов».

4. Переместите пользователей и группы, которые будут добавлены в качестве принципалов, из списка **Доступные пользователи/группы** в список **Выбранные пользователи/группы**.

5. Щелкните **Добавить и назначить безопасность**.

6. Выберите уровни доступа, присваиваемые принципалу.

7. Разрешите или запретите использование наследования прав папки или группы.

При необходимости права можно изменять на гранулярном уровне, который имеют более высокий приоритет по сравнению с определенными правами на уровне доступа.

См. также

- [Для изменения безопасности объекта для принципала](#)

5.2.3 Для изменения безопасности объекта для принципала

Обычно рекомендуется использовать уровни доступа для предоставления прав принципалам. Однако иногда требуется переопределить конкретные права уровня доступа. Расширенные права позволяют вам задавать устанавливать права для принципала поверх уровней доступа, которые принципал уже имеет. Как правило, необходимо выполнить следующие действия, чтобы предоставить расширенные права на объект принципалу.

1. Необходимо внести принципала в список контроля доступа к объекту.
2. После того, как принципал был добавлен, перейдите к пункту **Управление > Безопасность пользователя**, чтобы отобразился список контроля доступа для объекта.
3. Выберите принципала в списке контроля доступа и щелкните **Назначить безопасность**.
Появляется диалоговое окно «Назначить безопасность».
4. Выберите вкладку **Дополнительно**.
5. Щелкните **Добавить/Удалить права**.
6. Измените права для принципала.

Все доступные права описаны в *Приложении "Права"*.

См. также

- [Для назначения принципалов списку управления доступом к объекту](#)

5.2.4 Настройка прав на папку верхнего уровня в платформе BI

Эту последовательность действий нужно выполнить, чтобы настроить права для папки верхнего уровня в платформе BI.

Примечание:

В данном выпуске принципалам необходимы права на **Просмотр** папки контейнера, чтобы перемещаться по этой папке и просматривать расположенные в ней объекты. Это означает, что принципалам необходимы права на **Просмотр** объектов, находящихся в папках верхнего уровня.

Для ограничения прав принципала на **Просмотр** можно предоставить принципалу права на **Просмотр** определенной папки и настроить область действия прав только на эту папку.

1. Перейдите в область СМС, в которой расположена папка верхнего уровня, для которой требуется настроить права.
2. Выберите **Управление > Безопасность верхнего уровня > Все Объекты**.
Здесь параметр *Объекты* обозначает содержимое папки верхнего уровня. Если появляется запрос на подтверждение, щелкните **ОК**.
Появится диалоговое окно «Безопасность пользователя», в котором отображается список контроля доступа к папке верхнего уровня.
3. Внесите принципала в список контроля доступа к папке верхнего уровня.
4. При необходимости назначьте принципалу дополнительные права.

См. также

- [Для назначения принципалов списку управления доступом к объекту](#)
- [Для изменения безопасности объекта для принципала](#)

5.2.5 Проверка настроек безопасности для принципала

В некоторых случаях вам необходимо знать объекты, доступ к которым был предоставлен принципалу или отозван у него. Чтобы сделать это, можно воспользоваться запросом безопасности. Запросы безопасности позволяют определить, на какие объекты принципал имеет определенные права, и управлять правами пользователей. Для каждого запроса безопасности необходимо предоставить следующую информацию:

- **Принципал запроса**
Укажите пользователя или группу, для которых необходимо выполнить запрос безопасности. Для каждого запроса безопасности можно указать только одного принципала.
- **Полномочия для запроса**
Укажите право или права, для проверки которых выполняется запрос безопасности, статус этих прав и тип объектов, для которого установлены эти права. Например, можно выполнить запрос безопасности для всех отчетов, которые может обновлять принципал, или для всех отчетов, которые принципал не может экспортировать.
- **Контекст запроса**
Укажите области СМС, по которым запрос безопасности будет выполнять поиск. Для каждой области можно выбрать, включать или не включать в запрос безопасности подобъекты. В запрос безопасности можно включить максимум четыре области.

При выполнении запроса безопасности результаты отображаются в области «Результаты запроса» на панели Дерево под заголовком **Запросы безопасности**. Если требуется уточнить запрос безопасности, можно выполнить повторный запрос по результатам первого запроса.

Запросы безопасности полезны, так как позволяют увидеть объекты, на которые принципал имеет определенные права, а также увидеть местоположения этих объектов, если требуется изменить права. Рассмотрим ситуацию, в которой сотрудник отдела продаж повышается в должности до позиции менеджера по продажам. Менеджер по продажам должен иметь право на **Запланировать** по отношению к отчетам Crystal, по отношению к которым он до этого имел только право на **Просмотр**, и эти отчеты находятся в разных папках. В таком случае администратор выполняет запрос безопасности для права менеджера по продажам на просмотр отчетов Crystal во всех папках и включает в запрос подобъекты. После выполнения запроса безопасности администратор может видеть все отчеты Crystal, по отношению к которым менеджер по продажам имеет право на **Просмотр**, в области «Результаты запроса». Поскольку панель Сведения отображает местоположение каждого отчета Crystal, администратор может перейти к каждому отчету и изменить права менеджера по продажам по отношению к ним.

5.2.5.1 Для выполнения запроса безопасности

1. В области «Пользователи и группы» на панели Детали выберите пользователя или группу, для которой требуется запустить запрос безопасности.
2. Выберите меню **Управление > Инструменты > Создать запрос безопасности**.

Создать запрос по безопасности: Nina

Принципал запроса

Этот запрос выполнит поиск объектов для следующего принципала:

Nina

Полномочия для запроса

Этот запрос выполнит поиск объектов, для которых указанный выше принципал обладает всеми следующими полномочиями:

☐ Не передается запрос по полномочиям

Коллекция	Тип	Имя права		
Общее	Общее	Добавить объекты в каталог	✓	<input type="button" value="x"/>
Общее	Общее	Добавить объекты в папки, принадлежащие пользователям	✓	<input type="button" value="x"/>

Контекст запроса

Этот запрос выполнит поиск объектов только в следующих разделах данной СМС:

☒ Папки

(Все) ☒ Запросить подобъект

☐ Папки

(Все) ☐ Запросить подобъект

Появится диалоговое окно «Создать запрос безопасности».

3. Убедитесь, что владелец учетной записи в области **Запрос владельца учетной записи** указан правильно.

Если вы решили запустить запрос безопасности для другого владельца учетной записей, можно нажать **Обзор** и выбрать другого принципала. В диалоговом окне «Обзор запросов владельцев учетных записей» разверните **Список пользователей** или **Список групп** для

выбора владельца учетной записи, или поиска по имени. По окончании нажмите кнопку **ОК** для возврата в диалоговое окно «Создать запрос безопасности».

4. В области «Полномочия для запроса» укажите права и статус каждого права, в отношении которого будет выполняться запрос.
 - Если требуется выполнить запрос конкретных прав, которые принципал имеет на доступ к объектам, нажмите кнопку **Обзор**, задайте статус каждого права, в отношении которого будет выполняться запрос безопасности, и нажмите кнопку **ОК**.

Совет:

Можно удалить из запроса отдельные права, нажав кнопку "Удалить" справа, или удалить все права из запроса, нажав кнопку "Удалить" в строке заголовка.

- Если нужно выполнить общий запрос безопасности, установите флажок **Не передается запрос по полномочиям**.

При этом платформа BI выполняет общий запрос безопасности для всех объектов, имеющих принципалов в списках управления доступом, независимо от полномочий принципала на доступ к объекту.

5. В области «содержание запроса» укажите области СМС, которые хотите запросить.
 - a. Установите флажок рядом с элементом списка.
 - b. В списке выберите область СМС, к которой будет относиться запрос.

Если требуется запросить более конкретное местоположение в области (например, конкретную папку в меню "Папки"), нажмите кнопку **Обзор** для открытия диалогового окна «Обзор контекста запросов». На панели Сведения выберите папку, к которой будет относиться запрос, и нажмите кнопку **ОК**. Когда вы вернетесь в диалоговое окно **Запрос безопасности**, указанная папка появится в поле под списком.
 - c. Выберите **Запросить подобъект**.
 - d. Повторите шаги для каждой области СМС, которую хотите запросить.

Примечание:

Запрос может включать максимум 4 области.

6. Нажмите кнопку **ОК**.

Запрос безопасности запускается, и вы попадаете в область «Результаты запроса».
7. Для просмотра результатов запроса на панели Дерево разверните **Запросы безопасности** и нажмите на результат запроса.

Совет:

Результаты запроса перечислены согласно именам владельцев учетных записей.

Результаты запроса отображаются на панели Детали.

Область «Результаты запроса» запоминает все результаты запроса безопасности на время сеанса пользователя до его выхода из системы. Если требуется выполнить запрос повторно, но с новыми параметрами, выберите **Действия > Редактировать запрос**. Можно также повторно выполнить тот же самый запрос, выбрав его и нажав **Действия > Повторно выполнить запрос**. Если требуется сохранить результаты запроса безопасности, выберите **Действия > Экспорт**, чтобы экспортировать результаты запроса защиты в файл CSV.

5.3 Работа с уровнями доступа

Над уровнями доступа может выполнять следующие действия:

- Копировать существующий уровень доступа, изменять копию, переименовывать ее и сохранять как новый уровень доступа.
- Создавать, переименовывать и удалять уровни доступа.
- Изменять права в уровне доступа.
- Отслеживать взаимосвязи между уровнями доступа и другими объектами системы.
- Тиражировать уровни доступа и управлять уровнями доступа по сайтам.
- Используйте один из predefined уровней доступа в платформе BI, чтобы быстро и единообразно установить права для многих принципалов.

В следующей таблице приведены права, которые содержит каждый predefined уровень доступа.

Таблица 5-2: Предопределенные уровни доступа

Уровень доступа	Описание	Задействованные права
Просмотр	Если это право задано на уровне папок, принципал может просматривать папку, объекты в папке и экземпляры каждого объекта. Если это право задано на уровне объекта, принципал может просматривать объект, его журнал и экземпляры.	<ul style="list-style-type: none"> • Просмотр объектов • Просмотр экземпляров документа

Уровень доступа	Описание	Задействованные права
Запланировать	Принципал может создавать экземпляры, планируя запуск объекта в соответствии с указанным источником данных один раз или периодически. Принципал может просматривать, удалять и приостанавливать расписание экземпляров, которыми владеет. Принципалы могут также составлять расписание для различных форматов и адресатов, настраивать параметры и информацию о подключении к базе данных, выбирать серверы для обработки заданий, добавлять содержимое в папку, а также копировать объект или папку.	Права уровня доступа Просмотр , плюс: <ul style="list-style-type: none"> • Составить расписание для запуска документа • Определить серверные группы для обработки задач • Копировать объекты в другой каталог • Расписание по адресатам • Печать данных отчета • Экспортировать данные отчета • Изменить объекты, которыми владеет данный пользователь • Удалить экземпляры, которыми владеет пользователь • Установить паузу и возобновить экземпляры документов, которыми владеет данный пользователь
Просмотр по требованию	Принципал может получать обновленные данные из источника данных по запросу.	Права уровня доступа Запланировать , плюс: <ul style="list-style-type: none"> • Обновить данные отчета
Полное управление	Принципал может осуществлять полное управление объектом.	Все доступные права, включая: <ul style="list-style-type: none"> • Добавить объекты в каталог • Изменить объекты • Изменение прав пользователей в отношении объектов • Удалить объекты • Удалить экземпляры

В следующей таблице приведены права, необходимые для решения определенных задач, связанных с уровнями доступа.

Задача, связанная с уровнем доступа	Необходимые права
Создать уровень доступа	<ul style="list-style-type: none"> Права на Добавление для папки верхнего уровня Уровней доступа
Просмотр конкретных прав в уровне доступа	<ul style="list-style-type: none"> Права на Просмотр для уровня доступа.
Назначить принципалу уровень доступа к объекту	<ul style="list-style-type: none"> Права на Просмотр для уровня доступа. Право на Использовать уровень доступа для назначения защиты для уровня доступа Права на Изменить права для объекта или право Изменить права в безопасном режиме для объекта и принципала <p>Примечание: Пользователи, которые обладают правом Изменить права в безопасном режиме и хотят назначить уровень доступа для принципала, должны иметь тот же уровень доступа, назначенный для себя.</p>
Изменить уровень доступа	<ul style="list-style-type: none"> Права на Просмотр и Редактирование для уровня доступа
Удалить уровень доступа	<ul style="list-style-type: none"> Права на Просмотр и Удаление для уровня доступа
Клонировать уровень доступа	<ul style="list-style-type: none"> Права на Просмотр для уровня доступа. Права на Копирование для уровня доступа Права на Добавление для папки верхнего уровня Уровней доступа

5.3.1 Выбор между уровнями доступа **Просмотр** и **Просмотр по требованию**

При работе с отчетами в Интернете одним из важных принимаемых решений будет выбор между использованием оперативных и сохраненных данных. Однако независимо от сделанного выбора платформа BI отображает первую страницу как можно быстрее, чтобы можно было видеть отчет, пока обрабатываются другие данные. В данном разделе объясняется разница между двумя предопределенными уровнями доступа, которые можно использовать для принятия решения.

Уровень доступа **Просмотр по требованию**

Работа с отчетами по требованию предоставляет пользователям доступ к оперативным данным, непосредственно с сервера баз данных. Используйте оперативные данные, чтобы пользователи имели доступ к самым актуальным, с точностью до секунды, из постоянно меняющихся данных. Например, если менеджер крупной оптовой базы необходимо отслеживать товары,

поставляемые на регулярной основе, то получение оперативных данных в отчетах – это то, что им нужно.

Однако перед тем, как предоставить оперативные данные для всех отчетов, подумайте, стоит ли позволять всем пользователям постоянно обращаться к серверу баз данных. Если данные меняются не очень быстро и часто, то все эти запросы в базу данных будут просто увеличивать сетевой трафик и потреблять ресурсы сервера. В таких случаях можно запланировать отчеты на периодические повторы, чтобы пользователи могли видеть последние данные (экземпляры отчета), не обращаясь слишком часто к серверу баз данных.

Пользователи должны иметь доступ на **Просмотр по требованию**, чтобы обновлять отчеты через базу данных.

Уровень доступа Просмотр

Чтобы сократить потребление сетевого трафика и уменьшить количество запросов на серверы баз данных, можно запланировать отчеты на обработку в конкретное время. После обработки отчета пользователи могут при необходимости просматривать экземпляр отчета, не обращаясь лишний раз к базе данных.

Экземпляры отчета полезны, когда вы имеете дело с данными, которые не обновляются постоянно. Когда пользователи перемещаются по экземплярам отчета и переходят вниз по иерархии для просмотра сведений о столбцах или диаграммах, они не обращаются напрямую к серверу баз данных, а получают доступ к сохраненным данным. Следовательно, отчеты с сохраненными данными не только минимизируют передачу данных в сети, но и уменьшают нагрузку сервера баз данных.

Например, если база данных о продажах обновляется один раз в день, можно по такому же графику обрабатывать отчет. В таком случае сотрудники отдела продаж будут всегда иметь доступ к текущим данным, не обращаясь к базе данных каждый раз, когда открывают отчет.

Для отображения экземпляров отчета пользователи должны иметь доступ только на **Просмотр**.

5.3.2 Чтобы скопировать существующий уровень доступа

Это лучший способ создать уровень доступа, который незначительно отличается от одного из существующих уровней доступа.

1. Перейдите в область «Уровни доступа».
2. На панели Сведения выберите уровень доступа.

Совет:

Выберите уровень доступа, который содержит права, схожие с теми, которые нужны для вашего уровня доступа.

3. Выберите **Организовать > Копировать**.

Копия выбранного уровня доступа появится на панели Сведения.

5.3.3 Создание уровня доступа

Ниже описывается оптимальный способ создания уровня доступа, который будет в значительной степени отличаться от существующих уровней доступа.

1. Перейдите в область «Уровни доступа».
2. Выберите **Управление > Создать > Создать уровень доступа**.
Появится диалоговое окно «Создать новый уровень доступа».
3. Введите заголовок и описание нового уровня доступа и нажмите кнопку **ОК**.
Откроется область «Уровни доступа», а новый уровень доступа появится на панели **Сведения**.

5.3.4 Переименование уровня доступа

1. В области «Уровни доступа» на панели **Сведения** выберите уровень доступа, который необходимо переименовать.
2. Выберите команду **Управление > Свойства**.
Отобразится диалоговое окно «Свойства».
3. В поле **Заголовок** введите новое имя уровня доступа, затем нажмите кнопку **Сохранить и закрыть**.
После этого будет выполнен возврат в область «Уровни доступа».

5.3.5 Для удаления уровня доступа

1. В области «Уровни доступа» на панели **Детали** выберите уровень доступа, который требуется удалить.
2. Выберите **Управление > Удалить уровень доступа**.

Примечание:

Предварительно определенные уровни доступа удалить нельзя.

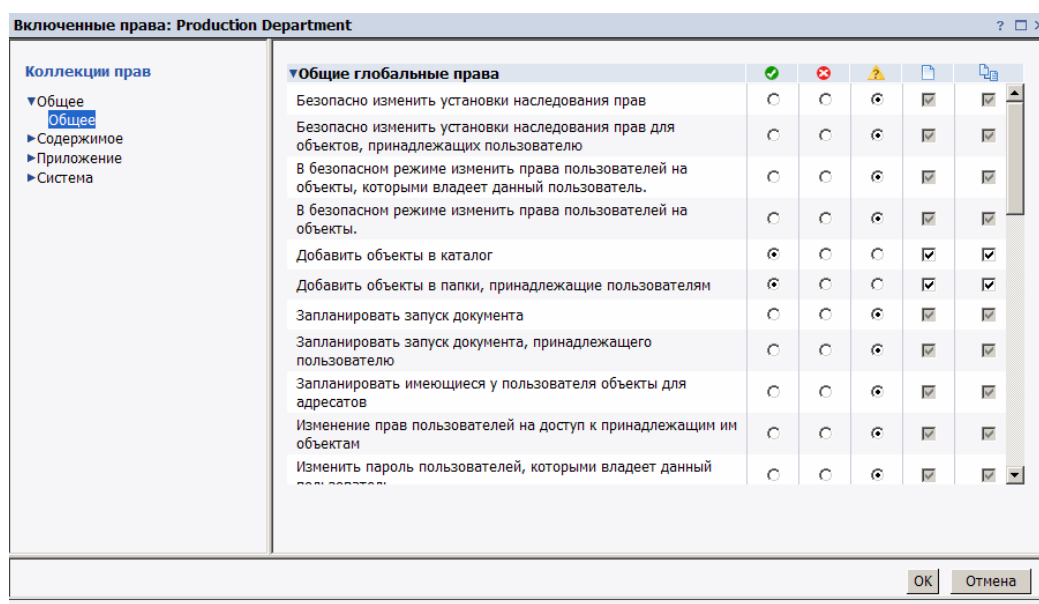
Информация об объектах, которые затрагивает данный уровень доступа, появится в диалоговом окне. Если удалять уровень доступа не требуется, нажмите кнопку **Отмена**, чтобы выйти из диалогового окна.

3. Нажмите кнопку **Удалить**.
Уровень доступа удалится, и вы вернетесь к области «Уровни доступа».

5.3.6 Чтобы изменить права в уровне доступа

Чтобы задать права для уровня доступа, сначала нужно задать общие глобальные права, которые применяются ко всем объектам, независимо от их типа, а затем нужно указать, когда требуется переопределить общие настройки на основе определенного типа объекта.

1. В области **Уровни доступа** на панели Сведения выберите уровень доступа, для которого требуется изменить права.
2. Выберите **Действия > Включенные права**.
Появится диалоговое окно **Включенные права** и отобразится список действующих прав.
3. Щелкните **Добавить/Удалить права**.



Диалоговое окно **Включенные права** отображает коллекции прав для уровня доступа в списке навигации. Раздел **Общие глобальные права** раскрывается по умолчанию.

4. Задайте общие глобальные права.
Каждое право может иметь статус **Предоставлено**, **Отказано** или **Не задано**. Можно выбрать, применить ли это право только к объекту, только к подобъектам, или и к тем, и к другим.
5. Чтобы задать права уровня доступа для определенного типа объектов, щелкните коллекцию прав в списке навигации, затем щелкните подколлекцию, которая применима к типу прав, для которого нужно задать права.
6. После завершения щелкните **ОК**.
Вы вернетесь к списку действующих прав.

См. также

- [Управление настройками безопасности для объектов в СМС](#)
- [Права для конкретных типов объектов](#)

5.3.7 Трассировка связи между уровнями доступа и объектами

До того, как вы измените или удалите уровень доступа, необходимо подтвердить, что любые изменения уровней доступа не повлияют отрицательно на объекты СМС. Это можно сделать, запустив запрос отношения на уровне доступа.

Запросы отношений очень полезны для управления правами, т.к. они позволяют вам увидеть объекты, подверженные влиянию уровня доступа, в одном удобном местоположении. Представьте себе ситуацию, в которой компания изменяет свою организационную структуру и соединяет два подразделения, подразделение А и подразделение В, в подразделение С. Администратор решает удалить все уровни доступа для подразделений А и В, т.к. больше они не существуют. Администратор запускает запрос связи для обоих уровней доступа перед тем, как удалить их. В области «Результаты запроса» администратор может увидеть объекты, которые будут затронуты при удалении уровней доступа. Панель Детали показывает местоположение объектов в СМС на случай, если права на объекты должны быть изменены до удаления уровней доступа.

Примечание:

- Для просмотра списка подверженных влиянию объектов у вас должно быть право **Просмотр** на этот объект.
- В результатах запроса связи отражаются только важные с точки зрения системы объекты, которым явно присвоен уровень доступа. Если же объект использует уровень доступа по правилам наследования, такой объект не появится в результатах запроса.

5.3.8 Управление уровнями доступа по сайтам

Уровни доступа являются одним из объектов, который можно тиражировать с исходного сайта на сайты-адресаты. Можно выбрать тиражирование уровней доступа, если они отображаются в списке контроля доступа тиражируемого объекта. Например, если принципалу предоставлен уровень доступа А к отчету Crystal, и этот отчет тиражируется по сайтам, уровень доступа А также тиражируется.

Примечание:

Если уровень доступа с тем же именем существует на сайте-адресате, тиражирование уровня доступа не будет выполнено. Ваш администратор или администратор сайта-адресата должен в таком случае переименовать уровень доступа перед тиражированием.

После тиражирования уровня доступа на сайты учитывайте примечания по администрированию, изложенные в данном разделе.

Изменение тиражированных уровней доступа на исходном сайте

При изменении тиражированного уровня доступа на исходном сайте уровень доступа на сайте-адресате обновится при следующем запуске тиражирования по расписанию. При двустороннем тиражировании, если вы измените уровень доступа на сайте-адресате, уровень доступа на исходном сайте тоже изменится.

Примечание:

Следите за тем, чтобы изменения уровней доступа на одном сайте не оказывали отрицательного влияния на объекты других сайтов. Обратитесь за помощью к администраторам сайта и попросите их выполнять запросы взаимосвязей для тиражированных уровней доступа до внесения изменений.

Изменение тиражированных уровней доступа на сайте-адресате

Примечание:

Это применимо только к одностороннему тиражированию

Никакие изменения тиражированных уровней доступа на сайте-адресате не отображаются на исходном сайте. Например, администратор сайта-адресата может предоставить право на планирование отчетов Crystal в тиражированном уровне доступа, даже если это право не было предоставлено на исходном сайте. В результате, хотя имена уровней доступа и тиражируемых объектов остаются одинаковыми, действующие права принципалов на объекты могут отличаться на разных сайтах-адресатах.

Если есть разница в уровне доступа исходного сайта и сайта-адресата, то эта разница в действующих правах будет обнаружена при следующем запланированном запуске задания на тиражирование. Можно сделать так, чтобы уровень доступа исходного сайта переопределял уровень доступа на сайте-адресате, или оставить уровень доступа на сайте-адресате нетронутым. Однако, если уровень доступа исходного сайта не будет переопределять уровень доступа сайта-адресата, все объекты, ожидающие тиражирования и имеющие этот уровень доступа, не будут тиражированы.

Чтобы ограничить изменение пользователями тиражированного уровня доступа на сайте-адресате, можно добавить пользователей сайта-адресата к уровню доступа как принципалов и предоставить им право только на **Просмотр**. Это значит, что пользователи сайта-адресата могут только просматривать уровень доступа, но не могут менять его настройки прав или назначать его для других пользователей.

См. также

- [интеграция](#)
- [Трассировка связи между уровнями доступа и объектами](#)

5.4 Отключение наследования

Наследование позволяет управлять настройками безопасности, не задавая права для каждого отдельного объекта. Однако в некоторых случаях наследование прав может не требоваться. Например, вы захотите настроить права для каждого объекта. Можно отключить наследование для принципала в списке контроля доступа объекта. Сделав это, вы сможете выбирать, отключить наследование группы, наследование папки или оба варианта.

Примечание:

При отключении наследования, оно отключается для всех прав; отключить наследование для каких-нибудь отдельных прав, не включая другие, нельзя.

На схеме «Отключение наследования» по умолчанию предполагается наследование группы и папки. Красный пользователь наследует права 1 и 5 как предоставленные, права 2, 3 и 4 – как неопределенные, а право 6 – как отозванное в явном виде. Эти права, заданные для группы на уровне папки, означают, что Красный пользователь и каждый член группы обладает такими правами на объекты папки, А и Б. Когда наследование отключается на уровне папки, набор прав Красного пользователя на объекты в этой папке аннулируется, пока администратор не назначит ему новые права.

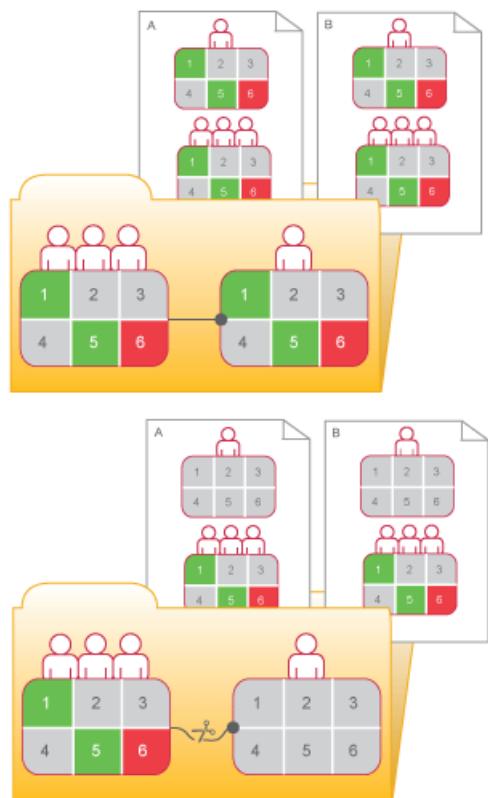


Рис. 5-9: Отключение наследования

5.4.1 Отключение наследования

Эта процедура позволяет отключить наследование групп и/или папок для принципала в списке управления доступом к объекту.

1. Выберите объект, для которого необходимо отключить наследование.
2. Выберите **Управление > Безопасность пользователя**.
Появляется диалоговое окно «Безопасность пользователя».
3. Выберите принципала, для которого необходимо отключить наследование, и щелкните **Назначить безопасность**.
Появляется диалоговое окно «Назначить безопасность».
4. Настройте параметры наследования.
 - Если необходимо отключить наследование группы (права, наследуемые принципом от элементов группы), снимите флажок **Наследовать от родительской группы**.
 - Если необходимо отключить наследование папки (настройки прав, наследуемые объектом от папки), снимите флажок **Наследовать от родительской папки**.
5. Нажмите кнопку **ОК**.

5.5 Использование прав передачи административных полномочий

С помощью прав можно не только контролировать доступ к объектам и настройкам, но и разделять административные задачи между функциональными группами внутри организации. Например, сотрудники из различных отделов смогут управлять собственными пользователями и группами. Или при наличии одного администратора, который осуществляет управление платформой BI на высоком уровне, управление всеми серверами может осуществляться сотрудниками вашего подразделения IT.

При условии, что структура групп и структура папок соответствует структуре безопасности делегированных административных полномочий, вы должны предоставить свои права делегированного администратора целым группам пользователей. Однако делегированному администратору следует предоставить не полный объем прав в отношении контролируемых им пользователей. Например, вы не хотите, чтобы делегированный администратор редактировал атрибуты пользователей или перераспределял их по другим группам.

В таблице «Права делегированных администраторов» суммированы права, необходимые делегированным администраторам для выполнения обычных действий.

Таблица 5-3: Права делегированных администраторов

Действия делегированных администраторов	Права, необходимые делегированному администратору
Создание новых пользователей	Право на добавление в отношении папки Пользователи высшего уровня
Создание новых групп	Право на добавление в отношении папки Группы пользователей высшего уровня
Удаление любых контролируемых групп, а также отдельных пользователей из данных групп	Право на удаление в отношении соответствующих групп
Удаление только пользователей, созданных данным делегированным администратором	Право владельца на удаление в отношении папки Пользователи высшего уровня
Удаление только пользователей и групп, созданных данным делегированным администратором	Право владельца на удаление в отношении папки Группы пользователей высшего уровня
Управление только пользователями, созданными данным делегированным администратором (включая добавление таких пользователей в соответствующие группы)	Права владельца на изменение и на безопасное изменение в отношении папки Пользователи высшего уровня
Управление только группами, созданными данным делегированным администратором (включая добавление пользователей в такие группы)	Права владельца на изменение и на безопасное изменение в отношении папки Группы пользователей высшего уровня
Изменение паролей пользователей в контролируемых группах	Право на изменение пароля в отношении соответствующих групп

Действия делегированных администраторов	Права, необходимые делегированному администратору
Изменение паролей только для принципалов, созданных данным делегированным администратором	<p>Право владельца на изменение пароля в отношении папки Пользователи высшего уровня, или соответствующих групп</p> <p>Примечание: Если вы присвоили права владельца на изменение пароля определенной группе, данной право вступит в действие для конкретного пользователя, только когда вы добавите его в соответствующую группу.</p>
Изменение имен пользователей, описания, других свойств, а также перераспределение пользователей по другим группам	<p>Право на изменение в отношении соответствующих групп</p>
Изменение имен пользователей, описания, других свойств, а также перераспределение пользователей по другим группам, но только в отношении пользователей, созданных данным делегированным администратором	<p>Право владельца на изменение в отношении папки Пользователи высшего уровня, или соответствующих групп</p> <p>Примечание: Если вы присвоили право владельца на изменение соответствующим группам, данное право вступит в действие для пользователя только тогда, когда вы добавите пользователя в соответствующую группу.</p>

5.5.1 Выбор параметров «Изменить права пользователей на объекты»

Делегируя полномочия администратора, передайте делегированному администратору права на контролируемые им принципалы. Можно предоставить полные права (**права на полный контроль**). Однако рекомендуется с помощью расширенной настройки прав ограничить для делегированного администратора **право на изменение прав** и вместо этого предоставить ему **право на безопасное изменение прав**. Также вы можете предоставить своему администратору **право на безопасное изменение установок наследования прав** вместо **права на изменение установок наследования прав**. Разница между этими правами вкратце описывается ниже.

Изменить права пользователей на объекты

Это право позволяет пользователю изменять любое право любого пользователя в отношении определенного объекта. Например, если пользователь А имеет **право на просмотр объектов** и **право на изменение прав пользователей в отношении объектов**, он может изменить права в отношении определенного объекта таким образом, чтобы получить полный контроль над данным объектом или предоставить такой контроль любому другому пользователю.

Изменять права пользователей на объекты в безопасном режиме

Данное право позволяет пользователю предоставлять, отзывать или отменять только ранее предоставленные ему права. Например, если пользователь А имеет **право на просмотр** и **на безопасное изменение прав пользователей на объекты**, он не может присваивать себе никакие дополнительные права, и может предоставлять другим пользователям или отказывать им в предоставлении только этих двух прав (**право на просмотр** и **безопасное изменение прав**). Кроме того, пользователь А может изменять только права пользователей на объекты, в отношении которых он имеет **право на безопасное изменение прав**.

Пользователь А может изменять права пользователя В на объект О при наличии следующих условий:

- Пользователь А имеет **право на безопасное изменение прав** в отношении объекта О.
- Каждое право или уровень доступа, изменяемые пользователем А для пользователя В, предоставлены пользователю А.
- Пользователь А имеет **право на безопасное изменение прав** пользователя В.
- Если назначается уровень доступа, пользователь А имеет право на **присвоение уровня доступа** пользователю В, для которого уровень доступа изменяется.

Объем прав может еще больше ограничивать действующие права, которые может назначать делегированный администратор. Предположим, что делегированный администратор имеет **право на безопасное изменение прав** и **право на редактирование** в папке, но объем данных прав ограничен только данной папкой и не применяется к ее подобъектам. Фактически, делегированный администратор может назначить право на **Редактирование** папки (но не объектов, содержащихся в ней) с областью действия «Применить к объектам». С другой стороны, если делегированному администратору представлено право на **Редактирование** папки с областью «Применить к подобъектам», другим принципалам может быть назначено право на **Редактирование** с обеими областями по отношению к вложенным объектам, но по отношению к папке может назначаться только право на **Редактирование** с областью «Применить к подобъектам».

Кроме того, делегированный администратор не может изменять права принципалов, в отношении которых не имеет права на Изменение прав пользователя в безопасном режиме. Например, это может быть полезным в том случае, если у вас имеется два делегированных администратора, ответственных за предоставление прав на работу с одной папкой различным группам пользователей, но вы не хотите, чтобы один из администраторов мог отменить доступ к группам, контролируемым другим администратором. Право на безопасное изменение прав гарантирует это, поскольку делегированные администраторы не будут иметь права на безопасное изменение прав в отношении друг друга.

Настройки наследования безопасного изменения прав

Данное право позволяет делегированному администратору изменять настройки наследования для других принципалов в отношении объектов, к которым делегированный администратор имеет доступ. Чтобы успешно изменять настройки наследования для других принципалов, делегированный администратор должен иметь соответствующее право в отношении объекта и учетных записей принципалов.

5.5.2 Права владельца

Права владельца – это права, которые имеет только владелец объекта, в отношении прав на который выполняется проверка. В платформе BI владельцем объекта является принципал, создавший объект; если этот принципал когда-либо будет удален из системы, владение перейдет к администратору.

Права владельца необходимы для управления безопасностью на основе владельца. Например, с их помощью можно создать папку или иерархию папок, в которой разные пользователи смогут создавать и просматривать любые документы, но смогут изменять или удалять только собственные документы. Кроме того, с помощью прав владельца можно разрешить пользователям управлять образцами создаваемых ими отчетов, но не какими-либо другими образцами. В случае планирования уровня доступа эти права позволяют пользователям редактировать, удалить, приостанавливать или заново планировать только собственные образцы.

Права владельца действуют аналогично соответствующим обычным правам. Однако права владельца эффективны, только если принципалу предоставлены права владельца, а обычные права запрещены или не указаны.

5.6 Сводка рекомендаций по управлению правами

Следует иметь в виду следующие рекомендации относительно управления правами:

- По возможности используйте уровни доступа. Эти предопределенные наборы прав упрощают управление путем группирования прав, связанных с общими потребностями пользователей.
- Настройте права и уровни доступа для папок верхнего уровня. Включение наследования способствует выполнению перемещения прав в системе с минимальным административным вмешательством.
- По возможности избегайте нарушения наследования. Это поможет уменьшить время на настройку безопасности содержимого, которое вы добавляете к платформе BI.
- Установите соответствующие права для пользователей и групп на уровне папки, затем опубликуйте объекты в эту папку. По умолчанию пользователи и группы с правами на доступ к папке наследуют права на доступ к любому объекту, который вы впоследствии опубликуете в этой папке.

- Разделите пользователей на группы, назначьте уровни доступа и права для всей группы, затем при необходимости назначьте уровни доступа и права для отдельных членов.
- Создайте отдельную учетную запись "администратор" для каждого администратора в системе и добавьте их в группу "Администраторы" для улучшения системы учета системных изменений.
- По умолчанию группа "Все" имеет очень ограниченные права на доступ к папкам верхнего уровня платформы BI. После установки рекомендуется просмотреть права для членов группы "Все" и настроить безопасность соответствующим образом.

Обеспечение безопасности платформы BI

6.1 Обзор вопросов безопасности

В данном разделе рассматриваются способы решения проблем безопасности на платформе BI, что позволяет дать ответ на распространенные вопросы администраторов и разработчиков систем, касающиеся безопасности.

Архитектура платформы Business Intelligence решает многие вопросы безопасности, затрагивающие современные предприятия и организации. В текущем выпуске для защиты от несанкционированного доступа поддерживаются такие функции, как распределенная защита, единый вход, защита доступа к ресурсам, гранулярные права объектов и сторонняя аутентификация.

Поскольку платформа BI обеспечивает структуру для растущего числа компонентов из семейства продуктов SAP BusinessObjects, в этот раздел включены подробные сведения о функциях безопасности и связанных с ними функциональных возможностях, чтобы показать, каким образом эта структура обеспечивает безопасность. Поэтому в данном разделе вместо подробных процедурных сведений рассматриваются принципиальные вопросы и даются ссылки на ключевые процедуры.

После краткого введения в принципы безопасности системы, будут предоставлены подробные сведения по следующим вопросам:

- Использование шифрования и режимов обеспечения безопасности обработки данных для защиты информации.
- Настройка уровня сокетов безопасности при развертывании платформы BI.
- Указания по настройке и поддержке брандмауэров на платформе BI.
- Настройка обратных прокси-серверов.

6.2 Планирование аварийного восстановления

Для защиты инвестиций организации в платформе BI нужно предпринять некоторые шаги, позволяющие обеспечить максимальную непрерывность бизнес-операций в случае аварии. В этом разделе представлено руководство по наброске плана аварийного восстановления для организации.

Общее руководство

- Регулярно выполняйте резервное копирование системы и в случае необходимости отправляйте копии некоторых носителей с резервными архивами вне сайта.
- Храните носители с программным обеспечением в надежном месте.
- Храните лицензионную документацию в надежном месте.

Конкретное руководство

Существуют три системных ресурса, требующие особого внимания в условиях планирования аварийного восстановления:

- Содержимое в серверах репозитория файлов: включает в себя патентованное содержимое, такое как отчеты. Следует регулярно делать резервные копии этого содержимого. В случае аварии нет способа восстановить такое содержимое, если не производилось регулярное резервное копирование.
- Системная база данных, используемая CMS: этот ресурс содержит важнейшие метаданные для развертывания, такие как сведения о пользователе, отчеты и другую информацию повышенной важности для организации.
- Ключевой файл информации базы данных (файл .dbinfo): этот ресурс содержит основной ключ к системной базе данных. Если по какой-либо причине этот ключ недоступен, доступ к системной базе данных будет невозможен. Настоятельно рекомендуется после развертывания платформы BI сохранить пароль для этого ресурса в надежном месте. Без пароля нельзя заново сформировать файл, и будет потерян доступ к системной базе данных.

6.3 Общие рекомендации по обеспечению безопасности развертывания

Ниже приведены рекомендации по безопасности развертывания платформы BI.

- Используйте брандмауэры для защиты обмена данными между CMS и другими компонентами системы. Если возможно, всегда скрывайте CMS за брандмауэром. По крайней мере следует убедиться, что системная база данных защищена брандмауэром.
- Добавьте дополнительное шифрование для серверов репозитория файлов. Когда система будет в состоянии готовности, патентованное содержимое будет сохраняться на этих серверах. Добавьте дополнительное шифрование через ОС или воспользуйтесь средством стороннего разработчика.
- Обратный прокси-сервер развертывается перед серверами веб-приложений, чтобы скрыть их за одним IP-адресом. При данной конфигурации весь Интернет-трафик, адресованный частным серверам веб-приложений, таким образом направляется через обратный прокси-сервер, скрывая частные IP-адреса.
- Следует строго придерживаться корпоративной политики относительно паролей. Убедитесь, что пользовательские пароли регулярно изменяются.
- Если была выбрана установка системной базы данных и сервера веб-приложений, поставляемого с платформой BI, требуется обратиться к соответствующей документации, чтобы убедиться, что эти компоненты будут развернуты с учетом необходимых настроек безопасности.

- Используйте протокол Secure Sockets Layer (SSL) для сетевого обмена данными между клиентами и серверами в развертывании.
- Доступ к консоли СМС ограничен исключительно локальным уровнем. Для получения сведений о параметрах развертывания консоли СМС см. *руководство по развертыванию веб-приложений платформы SAP BusinessObjects Business Intelligence*.

См. также

- [Требования для обмена данными между компонентами платформы BI](#)
- [Платформа BI и обратные прокси-серверы](#)
- [Настройка протокола SSL](#)
- [Ограничения для пароля](#)
- [Настройка безопасности для связанных серверов сторонних производителей](#)

6.4 Настройка безопасности для связанных серверов сторонних производителей

Если была выбрана установка компонентов сервера сторонних производителей, связанных с платформой BI, рекомендуется обратиться к документации для следующих связанных компонентов:

- Microsoft SQL Server 2008 экспресс-выпуск. Для получения подробных сведений об обеспечении безопасности этой системной базы данных для платформ Windows см. раздел <http://msdn.microsoft.com/en-us/library/bb283235%28v=sql.100%29.aspx>.
- IBM DB2 Express. Для получения подробных сведений об обеспечении безопасности этой системной базы данных для платформ UNIX см. раздел http://publib.boulder.ibm.com/infocenter/db2luw/v9r7/index.jsp?nav=/2_.
- Apache Tomcat 6.0. Для получения подробных сведений о безопасности для этого сервера веб-приложения см. <http://tomcat.apache.org/tomcat-6.0-doc/index.html>.

6.5 Активные доверительные отношения

В сетевой среде доверительное отношение между двумя доменами, как правило, представляет собой соединение, которое позволяет одному домену точно распознавать пользователей, аутентифицированных другим доменом. Поддерживая безопасность, доверительное отношение обеспечивает пользователям доступ к ресурсам в нескольких доменах без повторного ввода учетных данных.

В среде платформы BI активное доверительное отношение действует таким же образом, обеспечивая пользователям беспрепятственный доступ ко всем ресурсам системы. После того как пользователь прошел проверку подлинности и получил активный сеанс, все остальные компоненты платформы BI могут обрабатывать его запросы и действия, не запрашивая учетные

данные. По существу, активное доверительное отношение составляет основу распределенной системы безопасности платформы BI.

6.5.1 Маркеры входа

Маркер входа представляет собой кодированную строку, которая определяет собственные атрибуты использования и содержит сведения о сеансе пользователя. Атрибуты использования маркера входа определяются при его создании. Эти атрибуты позволяют установить ограничения маркера входа, чтобы снизить вероятность его использования злонамеренными пользователями. Текущие атрибуты использования маркера входа:

- **Число минут**

Этот атрибут ограничивает время жизни маркера жизни.

- **Число входов**

Этот атрибут ограничивает число возможных использований маркера для входа в платформу BI.

Оба атрибута затрудняют злонамеренным пользователям несанкционированный доступ к платформе BI с маркерами входа, извлеченными у полномочных пользователей.

Примечание:

Сохранение маркера входа в файлах cookie представляет собой потенциальный риск безопасности, если сеть между браузером и приложением или веб-сервером незащищена, например при подключении через публичную сеть без доверительной аутентификации или SSL. Для уменьшения риска безопасности между браузером и приложением или веб-сервером рекомендуется использовать протокол Secure Sockets Layer (SSL).

Если файлы cookie входа отключены и время ожидания веб-сервера или веб-браузера истекло, отображается экран входа в систему. Если файлы cookie входа разрешены и время ожидания веб-сервера или веб-браузера истекает, пользователь беспрепятственно возвращается в систему. Однако, поскольку сведения о состоянии привязаны к веб-сеансу, состояние пользователя будет утеряно. Например, если пользователь развернул дерево навигации и выбрал отдельный элемент, будет восстановлено исходное состояние дерева.

В платформе BI по умолчанию маркеры входа веб-клиента включены, однако можно отключить их для стартовой панели BI. При отключении маркеров входа на стороне клиента сеанс пользователя будет ограничен временем ожидания веб-сервера или веб-браузера. После окончания срока сеанса пользователю придется заново войти в систему платформы BI.

6.5.2 Механизм билетов для распределенной безопасности

Системы предприятия, предназначенные для обслуживания большого числа пользователей, обычно требуют определенной формы распределенной безопасности. Она может быть необходима для поддержки таких функций, как перенос доверия (возможность разрешения другому компоненту действовать от имени пользователя).

В платформе BI распределенная безопасность обеспечивается за счет реализации механизма билетов (аналогично механизму квитанций Kerberos). Центральный сервер управления (CMS) выдает билеты, разрешающие компонентам действовать от имени отдельного пользователя. Для платформы BI билет именуется маркером входа.

Этот маркер входа наиболее часто используется в сети Интернет. При первой аутентификации пользователей на платформе BI они получают маркеры входа с сервера CMS. Этот маркер входа хранится в кэш-памяти веб-браузера пользователя. Когда пользователь делает новый запрос, компоненты платформы BI могут считывать маркер входа из веб-браузера пользователя.

6.6 Сеансы и отслеживание сеансов

Как правило сеанс представляет собой соединение клиент-сервер, позволяющее обмениваться данными между двумя компьютерами. Состояние сеанса – это набор данных, описывающих атрибуты сеанса, его конфигурацию или содержимое. При установке клиент-серверного соединения через Интернет протокол HTTP ограничивает продолжительность каждого сеанса одной страницей информации, поэтому веб-браузер хранит в памяти состояние каждого сеанса только в течение отображения одной веб-страницы. При переходе от одной веб-страницы к другой состояние первого сеанса отменяется и заменяется состоянием следующего сеанса. Поэтому веб-сайты и веб-приложения должны тем или иным способом сохранять состояние одного сеанса, если оно должно повторно использоваться в другом.

Платформа BI для сохранения состояния сеансов использует два распространенных метода.

- **Файлы cookie.** Файл cookie представляет собой небольшой текстовый файл, в котором хранится состояние сеанса на стороне клиента: веб-браузер пользователя кэширует файлы cookie для последующего использования. Примером этого метода является маркер входа платформы BI.
- **Переменные сеанса.** Переменная сеанса – это раздел памяти, в котором хранится состояние сеанса на стороне сервера. Если BusinessObjects Enterprise присваивает пользователю активный идентификатор в системе, такие сведения, как тип аутентификации, хранятся в переменной сеанса. Пока сеанс поддерживается, система не должна вторично запрашивать информацию у пользователя или повторять любую задачу, необходимую для завершения следующего запроса.

Для Java-развертываний сеанс используется для обработки запросов .jsp; в развертываниях .NET – запросов .aspx.

Примечание:

В идеале система должна сохранять переменную сеанса, пока пользователь активен в системе. Чтобы гарантировать безопасность и свести к минимуму использование ресурсов, система должна уничтожить переменную сеанса сразу же после завершения работы пользователя в

системе. Однако, поскольку при взаимодействии между веб-браузером и веб-сервером информация о состоянии может не использоваться, если пользователь не выходит из системы явным образом, бывает затруднительно определить, когда он покинул систему. Для решения этой проблемы в платформе BI реализовано отслеживание сеансов.

6.6.1 Отслеживание сеансов центральным сервером управления

Центральный сервер управления реализует простой алгоритм отслеживания. Когда пользователь входит в систему, ему присваивается сеанс CMS, сохраняемый центральным сервером до выхода пользователя из системы или освобождения переменной сеанса сервера веб-приложений.

Сеанс сервера веб-приложений периодически уведомляет центральный сервер управления о своей активности, поэтому сеанс CMS сохраняется, пока существует сеанс сервера веб-приложений. Если сеансу сервера веб-приложений не удастся подключиться к CMS в течении десяти минут, центральный сервер управления удаляет сеанс CMS. Таким образом обрабатываются сеансы, где компоненты клиентской стороны беспорядочно завершают работу.

6.7 Защита среды

Безопасность среды подразумевает защиту всего окружения, в котором осуществляется взаимодействие клиентских и серверных компонентов. Хотя популярность Интернета и сетевых систем постоянно растет благодаря их гибкости и диапазону функциональных возможностей, они работают в среде, безопасность которой трудно обеспечить. При развертывании платформы BI защита среды осуществляется в двух областях взаимодействия.

6.7.1 Веб-браузер с веб-сервером

При передаче данных между веб-браузером и веб-сервером обычно требуется обеспечить определенную степень безопасности. Необходимые меры безопасности включают две общие задачи:

- обеспечение безопасного обмена данными;
- разрешение извлекать информацию с веб-сервера только допустимым пользователям.

Примечание:

Эти задачи обычно решаются веб-серверами с помощью различных механизмов защиты, в том числе протокола Sockets Layer (SSL) и других подобных механизмов. Для уменьшения риска

безопасности между браузером и приложением или веб-сервером рекомендуется использовать протокол Secure Sockets Layer (SSL).

Необходимо защитить обмен данными между веб-браузером и веб-сервером независимо от платформы BI. Сведения о клиентских подключениях см. в документации по веб-серверу.

6.7.2 Веб-сервер – платформа BI

Для защиты взаимодействия между веб-сервером и остальной частью корпоративной внутренней сети (включая платформу BI) обычно используются брандмауэры. Платформа поддерживает брандмауэры, использующие IP -фильтрацию или трансляцию статических сетевых адресов (NAT). Поддерживаемые среды могут включать несколько брандмауэров, веб-серверов или серверов приложений.

6.8 Аудит изменений параметров безопасности

В платформе BI не ведется аудит изменений в параметрах безопасности по умолчанию для следующего:

- Файлы свойств для веб-приложений (BOE, веб-службы)
- TrustedPrincipal.conf
- Настройка стартовой панели BI и открытого документа

В целом, не ведется аудит любых изменений параметров безопасности, выполняемых вне консоли СМС. Это также справедливо в отношении изменений, выполняемых в ССМ. Изменения, фиксируемые с использованием СМС, могут подвергаться аудиту.

6.9 Аудит действий через Интернет

Платформа BI позволяет понять, что происходит в системе, регистрируя действия, выполняемые через Интернет, и обеспечивая проверку и отслеживание необходимых сведений. Сервер веб-приложений дает возможность выбирать регистрируемые атрибуты сети, например время, дату, IP-адрес, номер порта и т.д. Данные аудита регистрируются на диске и сохраняются в текстовых файлах с разделяющими запятыми, благодаря чему можно легко создавать отчеты по данным или импортировать их в другие приложения.

6.9.1 Защита от попыток выполнения входа злоумышленником

Независимо от степени безопасности системы существует по крайней мере одно уязвимое для атак местоположение, точка подключения пользователей к системе. Почти невозможно полностью защитить это местоположение, потому что процесс простого угадывания действительного имени пользователя и пароля остается реальным способом попытаться "взломать" систему.

В платформе BI реализовано несколько методик снижения вероятности доступа злоумышленников к системе. Различные ограничения, приведенные ниже, применимы только к учетным записям Enterprise, т. е. эти ограничения не применимы к учетным записям, для которых создано соответствие в базе данных внешнего пользователя (LDAP или Windows AD). Обычно, тем не менее, внешняя система позволяет задать те же ограничения для внешних учетных записей.

6.9.2 Ограничения для пароля

Ограничения для пароля гарантируют, что для аутентификации в Enterprise пользователи по умолчанию будут создавать сравнительно сложные пароли. Можно использовать следующие опции:

- Принудительно устанавливать пароли с символами в разных регистрах

Этот параметр гарантирует, что пароль содержит по крайней мере два типа символов: буквы в верхнем регистре, буквы в нижнем регистре, цифры или знаки пунктуации.

- Должен содержать не менее N символов

Требования к минимальной сложности пароля понижают вероятность простого угадывания злоумышленником действительного пароля пользователя.

6.9.3 Ограничения на вход

Ограничения на вход служат в первую очередь для предотвращения словарных атак (метод, при котором злоумышленник узнает действительное имя пользователя и пытается угадать пароль перебором слов в словаре). С использованием скоростей современного аппаратного обеспечения злонамеренные программы могут перебирать миллионы паролей в минуту. Для предотвращения словарных атак в платформе BI используется внутренний механизм, включающий временную задержку (0,5-1,0 с) между попытками входа. Кроме того, в платформе BI предусмотрены несколько настраиваемых параметров, которые могут снизить риск словарных атак:

- Отключать учетную запись после N неудачных попыток входа

- Сбрасывать счетчик неудачных попыток через N мин
- Повторно включать учетную запись через N мин

6.9.4 Ограничения для пользователя

Ограничения для пользователя гарантируют, что для аутентификации в Enterprise пользователи по умолчанию будут регулярно создавать новые пароли. Вы можете использовать следующие опции:

- Должен изменять пароль каждые N дн.
- Не может повторно использовать N последних паролей
- Должен ждать N мин для изменения пароля

Эти параметры полезны с нескольких точек зрения. Во-первых, злоумышленник, предпринимающий словарную атаку, должен будет возобновлять ее при каждой смене паролей. Поскольку изменение пароля зависит от времени первого входа пользователя в систему, это затрудняет определение времени изменения каждого отдельного пароля. Кроме того, даже если злоумышленнику удастся угадать или получить каким-то иным способом другие учетные данные пользователя, срок их действия ограничен.

6.9.5 Ограничения учетной записи гостя

Платформа BI поддерживает анонимный единый вход для учетной записи гостя. Таким образом, когда пользователи подключаются к платформе BI, не указывая имя пользователя и пароль, система автоматически регистрирует их с учетной записью гостя. При назначении учетной записи гостя защищенного пароля или полном отключении учетной записи гостя это стандартное поведение отключается.

6.10 Расширения обработки

Платформа BI позволяет еще лучше защитить среду отчетов благодаря использованию настраиваемых расширений обработки. Расширение обработки – это динамически загружаемая библиотека кода, которая применяет бизнес-логику к определенному запросу на просмотр или планирование платформы BI перед их обработкой системой.

Благодаря поддержке расширений обработки административный SDK платформы BI предоставляет идентификатор, позволяющий разработчикам перехватить запрос. Разработчики при этом могут прикрепить к запросу формулу выбора перед его обработкой.

Типичным примером является расширение обработки отчета, которое усиливает защиту на уровне строк. Данный тип защиты ограничивает доступ к данным по строкам в одной или нескольких базах данных. Разработчик пишет динамически загружаемую библиотеку, которая перехватывает запросы на просмотр или планирование отчета (до того, как эти запросы будут обработаны сервером заданий, сервером обработки или сервером приложений отчетов). Код разработчика сначала определяет пользователя, который запустил задание обработки; затем он проверяет полномочия пользователя на доступ к данным в сторонней системе. Затем код создает и прикрепляет к отчету формулу выбора записи, чтобы ограничить данные, возвращаемые базой данных. В этом случае расширение обработки является способом интеграции настраиваемой защиты на уровне строк в среду платформы BI.

Совет:

Включив расширения обработки, пользователь настраивает соответствующие компоненты сервера платформы BI на динамическую загрузку расширений обработки в ходе выполнения. В SDK входит полностью документированный API, который могут использовать разработчики для написания расширений обработки. Дополнительную информацию см. в документации разработчика, поставляемой в комплекте с продуктом.

6.11 Обзор безопасности данных платформы BI

Администраторы систем платформы BI управляют защитой секретных данных, используя:

- Настройки безопасности на уровне кластера, которые определяют те приложения и клиенты, которые имеют доступ к CMS. Эта настройка управляется посредством диспетчера центральной конфигурации.
- Система двухключевой криптографии, которая управляет как доступом к репозиторию CMS, так и ключами, используемыми для шифрования/дешифрования объектов в репозитории. Доступ к репозиторию CMS задается посредством диспетчера центральной конфигурации, а Central Management Console имеет выделенную область управления для криптографических ключей.

Эти функции позволяют администраторам задавать развертываниям платформы BI определенные уровни безопасности данных и управлять ключами шифрования, используемыми для шифрования и дешифрования данных в репозитории CMS.

6.11.1 Защищенные режимы обработки данных

Платформа BI может работать в двух защищенных режимах обработки данных:

- Защищенный режим обработки данных по умолчанию. В определенных экземплярах, работающие в этом режиме системы будут использовать жестко запрограммированные ключи шифрования и не будут соответствовать указанному стандарту. Режим по умолчанию обеспечивает обратную совместимость с предыдущими версиями средств клиента и приложений платформы BI.
- Режим защищенной обработки данных, разработанный с учетом рекомендаций, указанных в Федеральном стандарте обработки информации (FIPS), а именно, в FIPS 140-2. В этом режиме для защиты секретных данных используются FIPS-совместимые алгоритмы и криптографические модули. Когда платформа запущена в FIPS-совместимом режиме, все клиентские инструменты и приложения, не отвечающие требованиям FIPS, автоматически отключаются. Средства клиента и приложения платформы отвечают стандарту FIPS 140.2. Если платформа SAP BusinessObjects Business Intelligence 4.0 запущена в FIPS-совместимом режиме, более ранние версии клиентов и приложений работать не будут.

Этот режим обработки данных прозрачен для пользователей системы. В обоих режимах защищенной обработки данных секретные данные шифруются и дешифруются в фоновом режиме встроенным механизмом шифрования.

Использование FIPS-совместимого режима рекомендуется в следующих случаях:

- Развертывание платформы SAP BusinessObjects Business Intelligence 4.0 не требует использования или взаимодействия с какими-либо устаревшими средствами клиента или приложениями платформы BI.
- В вашей организации стандарты и рекомендации обработки данных запрещают использование запрограммированных ключей шифрования.
- От вашей организации требуется защита секретных данных согласно требованиям FIPS 140-2.

Защищенный режим обработки данных задается в Central Configuration Manager на платформах Windows и UNIX. Каждый узел в кластеризованной среде должен быть переведен в защищенный режим.

6.11.1.1 Для включения FIPS-совместимого режима в Windows

По умолчанию, FIPS-совместимый режим отключается после установки платформы BI. Чтобы включить FIPS-совместимый режим для всех узлов в Вашем развертывании, воспользуйтесь инструкциями внизу.

1. Для запуска CCM выберите пункт **Программы > SAP BusinessObjects Enterprise XI 4.0 > SAP BusinessObjects Enterprise > Central Configuration Manager**.
2. В CCM щелкните правой кнопкой мыши Server Intelligence Agent (SIA) и выберите команду **Остановить**.

Предупреждение:

Не переходите к действию 3, пока статус SIA не изменится на «Остановлен».

3. Щелкните правой кнопкой мыши SIA и выберите команду **Свойства**.
Появится диалоговое окно «Свойства» с вкладкой **Свойства**.

4. Добавьте `-fips` в поле «Команда» и щелкните **Применить**.
5. Нажмите кнопку **ОК**, чтобы закрыть диалоговое окно «Свойства».
6. Перезапустите SIA.

Теперь SIA работает в FIPS-совместимом режиме.

Настройку FIPS-совместимости следует включить на всех SIA в развертывании платформы BI.

6.11.1.2 Для включения FIPS-совместимого режима на UNIX

Все серверы в развертывании платформы BI должны быть остановлены перед попыткой проведения следующей процедуры.

По умолчанию, FIPS-совместимый режим отключается после установки платформы BI. Чтобы включить FIPS-совместимый режим для всех узлов в Вашем развертывании, воспользуйтесь инструкциями внизу.

1. Перейдите к каталогу, в котором установлена платформа BI на компьютере под управлением ОС UNIX.
2. Внесите изменение в каталог `sap_bobj` .
3. Введите `ccm.config` и нажмите **Enter**.
Будет загружен файл `ccm.config`.
4. Добавьте `-fips` к параметру команды запуска узла.
Параметр команды запуска узла появится в виде `[ИМЯ_узлаЗапуск]`.
5. Сохраните изменения и нажмите **Выход**.
6. Перезапустите узел.

Теперь узел работает в FIPS-совместимом режиме.

Настройку FIPS-совместимости следует включить на всех узлах в развертывании платформы BI.

6.11.1.3 Для отключения FIPS-совместимого режима в Windows

Все серверы в развертывании платформы BI должны быть остановлены перед попыткой проведения следующей процедуры.

Если Ваше развертывание запущено в FIPS-совместимом режиме, используйте следующие инструкции для отключения этой настройки.

1. В CCM щелкните правой кнопкой мыши Server Intelligence Agent (SIA) и выберите команду **Остановить**.

Предупреждение:

Не переходите к действию 2, пока статус узла не изменится на «Остановлен».

2. Щелкните SIA правой кнопкой мыши и выберите команду **Свойства**.
Появится диалоговое окно «Свойства» с вкладкой **Свойства**.
3. Удалите `-fips` из поля «Команда» и щелкните **Применить**.
4. Нажмите кнопку **ОК**, чтобы закрыть диалоговое окно «Свойства».
5. Перезапустите SIA.

6.12 Криптография в платформе BI

Секретные данные

Криптография в платформе BI предназначена для защиты секретных данных в репозитории CMS. Секретные данные включают реквизиты пользователей, данные подключения источников данных и любые другие объекты информации с паролями. Эти данные шифруются, чтобы гарантировать их секретность, защиту от искажения и поддерживать контроль доступа. Все ресурсы шифрования реквизитов (включая систему шифрования, библиотеки RSA) по умолчанию устанавливаются в каждом развертывании платформы BI.

Система платформы BI использует систему двухключевой криптографии.

Криптографические ключи

Шифрование и дешифрование секретных данных производится в фоновом режиме, взаимодействием SDK с внутренним механизмом шифрования. Администраторы системы управляют защитой данных посредством симметричных ключей шифрования без прямой шифрации или дешифрации определенных блоков данных.

В платформе BI симметричные ключи шифрования, известные как криптографические ключи, используются для шифрования/дешифрования секретных данных. В Central Management Console есть выделенная область управления криптографическими ключами. Для просмотра, создания, деактивирования, отзыва и удаления «Криптографические ключи» для просмотра, создания, деактивации, отзыва и удаления ключей. Система гарантирует, что любой ключ, требующийся для дешифрования секретных данных не будет удален.

Ключи кластера

Ключи кластера – это симметричные ключи упаковывающие ключи, защищающие криптографические ключи, которые хранятся в репозитории CMS. Ключи кластера, использующие симметричные алгоритмы ключей, поддерживают уровень контроля доступа к репозиторию CMS. Каждому узлу в платформе BI во время установки назначается ключ кластера. Администраторы системы могут использовать CCM для сброса ключа кластера.

6.12.1 Работа с ключами кластера

При настройке установки платформы BI создается ключ кластера для агента SIA, состоящий из восьми символов. Этот ключ используется для шифрования всех криптографических ключей в репозитории CMS. Без правильного ключа кластера доступ к CMS невозможен. Ключ кластера хранится в зашифрованном виде в файле `dbinfo`. В установке Windows по умолчанию файл хранится в следующем каталоге: `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64`. В системах Unix файл хранится в каталоге платформы в `<INSTALLDIR>/sap_bobj/enterprise_xi40/`.

платформа Unix	Путь
AIX	<code><INSTALLDIR>/sap_bobj/enterprise_xi40/ aix_rs6000/</code>
Solaris	<code><INSTALLDIR>/sap_bobj/enterprise_xi40/ solaris_sparc/</code>
Linux	<code><INSTALLDIR>/sap_bobj/enterprise_xi40/ linux_x86/</code>
OC HP_UX	<code><INSTALLDIR>/sap_bobj/enterprise_xi40/ hpux_pa-risc/</code>

Имя файла основано на следующем соглашении: `_boe_<sia_name>.dbinfo`, где `<sia_name>` – имя Server Intelligence Agent для кластера.

Примечание:

Из файла `dbinfo` нельзя получить ключ кластера для любого заданного узла. Системным администраторам рекомендуется принять всесторонние меры для защиты кластерных ключей.

Только пользователи с полномочиями администратора могут сбрасывать ключи кластера. При необходимости воспользуйтесь CCM для сброса ключа кластера, состоящего из восьми символов, для каждого узла экземпляра системы. Новые ключи кластера автоматически используются для скрещения криптографических ключей в репозитории CMS.

6.12.1.1 Чтобы сбросить ключ кластера в Windows

Перед сбросом ключа кластера убедитесь, что все серверы, управляемые агентом SIA, остановлены.

Используйте следующую процедуру для сброса ключа кластера для узла.

1. Для запуска CCM выберите пункт **Программы > SAP BusinessObjects Enterprise XI 4.0 > SAP BusinessObjects Enterprise > Central Configuration Manager**.
2. В CCM щелкните правой кнопкой мыши Server Intelligence Agent (SIA) и выберите команду **Остановить**.

Предупреждение:

Не переходите к шагу 3 пока статус SIA не измениться на «Остановлено».

3. Щелкните правой кнопкой мыши Server Intelligence Agent (SIA) и выберите команду **Свойства**.
Открывается диалоговое окно «Свойства».
4. Откройте вкладку **Конфигурация**.
5. Нажмите кнопку **Изменить** в разделе «Конфигурация базы данных системы CMS».
Появится сообщение с предупреждением.
6. Нажмите кнопку **Да** для продолжения.
Будет открыто диалоговое окно «Изменение ключа кластера».
7. Введите одинаковое значение ключа из восьми символов в полях «Новый ключ кластера» и «Подтвердите новый ключ кластера».

Примечание:

В платформах Windows ключи кластера должны содержать комбинацию символов верхнего и нижнего регистра. Вместо этого пользователи также создают случайные ключи. Для FIPS-совместимости требуется случайный ключ.

8. Нажмите кнопку **ОК**, чтобы отправить новый ключ кластера в систему.
Появится сообщение, информирующее о том, что ключ кластера был переустановлен успешно.
9. Перезапустите SIA.

В кластере, состоящем из нескольких узлов, необходимо сбросить ключи кластера для всех агентов SIA в экземпляре развертывания платформы BI и установить новый ключ.

6.12.1.2 Сброс ключа кластера в UNIX

Перед сбросом ключа кластера для узла убедитесь, что все серверы, управляемые узлом, остановлены.

1. Перейдите к каталогу, в котором установлена платформа BI на компьютере под управлением ОС UNIX.
2. Измените его на каталог `sap bobj`.
3. Введите `cmsdbsetup.sh` и нажмите клавишу **Enter**.
Будет открыто окно «Настройка базы данных CMS».
4. Введите имя узла и нажмите клавишу **Enter**.
5. Введите значение 2, чтобы изменить ключ кластера.
Появится сообщение с предупреждением.
6. Нажмите **Далее** для продолжения.
7. В специальном поле введите новый ключ кластера, состоящий из восьми символов, и нажмите клавишу **Enter**.

Примечание:

В платформах UNIX допустимый ключ кластера содержит любую комбинацию из восьми символов без каких-либо ограничений.

8. Повторите ввод нового ключа кластера в соответствующем поле и нажмите клавишу **Enter**.
Появится сообщение, информирующее о том, что ключ кластера был создан успешно.
9. Перезапустите узел.

Чтобы использовать один ключ кластера для всех узлов, необходимо переустановить все узлы в экземпляре платформы BI.

6.12.2 Специалисты по шифрованию

Для управления криптографическими ключами в СМС необходимо быть членом группы специалистов по шифрованию. Учетная запись администратора, создаваемая для платформы BI по умолчанию, также входит в группу специалистов по шифрованию. Этой учетной записью следует пользоваться для добавления пользователей в группу специалистов по шифрованию. Членство в группе рекомендуется ограничивать.

Примечание:

Когда пользователи добавляются в группу администраторов, они не наследуют права для выполнения задач управления криптографическими ключами.

6.12.2.1 Для добавления пользователя в группу специалистов по шифрованию

Учетная запись пользователя должна быть в платформе BI до того, как она будет добавлена в группу специалистов по шифрованию.

Примечание:

Для добавления добавлена члена в группу специалистов по шифрованию, необходимо быть членом групп Администраторы и Специалисты по шифрованию.

1. В области управления «Пользователи и группы» в СМС, выберите группу **Специалисты по шифрованию**.
2. Нажмите **Действия > Добавить членов в группу**.
Откроется диалоговое окно «Добавить».
3. Щелкните **Список пользователей**.
Список **Доступные пользователи/группы** будет обновлен, и в нем отобразятся все учетные записи пользователей в системе.

4. Переместите учетную запись пользователя, которую нужно добавить в группу специалистов по шифрованию, из списка **Доступные пользователи/группы** в список **Выбранные пользователи/группы**.

Совет:

Чтобы найти какого-либо пользователя, используйте поле поиска.

5. Нажмите кнопку **ОК**.

Добавленный член группы специалистов по шифрованию получит доступ к области управления «Криптографические ключи» в СМС.

6.12.2.2 Просмотр криптографических ключей на консоли СМС

В приложении СМС есть специально предусмотренная область для криптографических ключей, которые используются в системе платформы BI. Доступ к этой области ограничен кругом участников группы "Специалисты по шифрованию".

1. Чтобы запустить СМС, выберите **Программы > SAP BusinessObjects XI 4.0 > SAP BusinessObjects Enterprise > SAP BusinessObjects Enterprise Central Management Console**.
Откроется домашняя страница СМС.
2. Перейдите на вкладку «Криптографические ключи».
Отобразится область управления «Криптографические ключи».
3. Дважды щелкните криптографический ключ, подробные сведения о котором нужно просмотреть.

См. также

- [Для просмотра объектов, связанных с криптографическим ключом](#)

6.12.3 Управление криптографическими ключами с помощью СМС

Область управления «Криптографические ключи» позволяет специалистам по шифрованию просматривать, создавать, отключать, отзываться и удалять ключи, с помощью которых шифруются конфиденциальные данные, которые хранятся в репозитории СМС.

В области управления «Криптографические ключи» отображается список всех определенных в системе криптографических ключей. Основные данные по каждому ключу приводятся в разделах, описанных в таблице ниже.

Заголовок	Описание
Название	Имя, идентифицирующее криптографический ключ
Состояние	Текущее состояние ключа
Время последнего изменения	Отметка даты и времени последнего изменения, связанного с криптографическим ключом
Объекты	Количество объектов, связанных с ключом

См. также

- [Статус криптографического ключа](#)
- [Создание криптографических ключей](#)
- [Удаление криптографических ключей из системы](#)
- [Отзыв криптографических ключей](#)
- [Для просмотра объектов, связанных с криптографическим ключом](#)
- [Обозначение криптографических ключей как рассекреченных](#)

6.12.3.1 Статус криптографического ключа

В следующей таблице приведены все возможные варианты статуса криптографических ключей в платформе BI:

Статус	Описание
Активный	Только один криптографический ключ в системе может быть «Активным». Этот ключ используется для шифрования текущих секретных данных, которые будут сохранены в базе данных CMS. Этот ключ также используется для дешифрования всех объектов, представленных в списке объектов. Когда создается новый криптографический ключ, текущий ключ меняет состояние с «Активного» на «Деактивированный». Активный ключ не может быть удален из системы.
Деактивирован	Ключ «Деактивированный» больше не может использоваться для шифрования данных. Но он может использоваться для дешифрования объектов, представленных в списке объектов. Если ключ был деактивирован, то его невозможно снова активировать. Ключ с пометкой «Деактивированный» не может быть удален из системы. Перед удалением статус ключа следует изменить на «Отозванный».
Рассекреченный	Криптографический ключ, который считается небезопасным, может быть помечен как рассекреченный. Отмечая такой ключ, позже можно запустить перешифровку объектов данных, все еще ассоциированных с этим ключом. Когда ключ помечен как рассекреченный, он должен быть отозван перед удалением из системы.
Отозван	Когда криптографический ключ отозван, запускается процесс, в котором все ассоциированные с этим ключом объекты перешифруются текущим "Активным" криптографическим ключом. Когда ключ отозван, он может быть безопасно удален из системы. Механизм отзыва гарантирует, что данные в базе данных CMS всегда могут быть дешифрованы. Отозванный ключ не может быть снова активирован.

Статус	Описание
Неактивно: повторное шифрование выполняется	Указывает, что криптографический ключ находится в процессе отзыва. После завершения процесса, ключ помечается как «Отозванный».
Неактивно: повторное шифрование остановлено	Указывает, что процесс отзыва криптографического ключа остановлен. Такое обычно происходит при намеренной остановке процесса или, если ассоциированный с ключом объект данных недоступен.
Отозван-рассекречен	Ключ помечается как отозван-рассекречен, если он был отмечен как рассекреченный, а все данные, ранее ассоциированные с ним, были зашифрованы новым ключом. Когда рассекреченный ключ помечен как «Деактивированный», есть возможность отозвать этот ключ. Когда рассекреченный ключ отозван, он может быть удален.

6.12.3.2 Для просмотра объектов, связанных с криптографическим ключом

1. Выберите ключ в области управления «Криптографические ключи» в СМС.
2. Щелкните **Управление > Свойства**.
Откроется диалоговое окно криптографических ключей «Свойства».
3. Нажмите кнопку «Список объектов» в панели навигации в левой части диалогового окна «Свойства».
Все объекты, ассоциированные с криптографическим ключом приведены в правой части панели навигации.

Совет:

Для просмотра определенного объекта следует использовать функцию поиска.

6.12.3.3 Создание криптографических ключей

Предупреждение:

При создании криптографического ключа система автоматически отключает текущий «Активный» ключ. Для отключенного ключа нельзя восстановить состояние «Активный».

1. В области управления «Криптографические ключи» консоли СМС последовательно выберите параметры **Управление > Создать > Криптографический ключ**.
Откроется диалоговое окно «Создать новый криптографический ключ» с предупреждением.
2. Нажмите кнопку **Продолжить**, чтобы создать криптографический ключ.

3. Введите имя и описание нового криптографического ключа и нажмите кнопку **ОК**, чтобы сохранить информацию.

В области управления «Криптографические ключи» новый ключ отображается как единственный активный. Предыдущий «Активный» ключ теперь помечен как «Неактивный».

Все новые конфиденциальные данные, которые создаются и хранятся в базе данных CMS, теперь будут шифроваться с помощью нового криптографического ключа. Есть возможность отозвать предыдущий ключ и повторно зашифровать все связанные с ним объекты данных новым активным ключом.

6.12.3.4 Обозначение криптографических ключей как рассекреченных

Криптографический ключ, который по каким-либо причинам больше нельзя считать безопасным, можно пометить как рассекреченный. Это полезно для отслеживания, например, когда нужно узнать, какой объект данных соответствует определенному ключу. Прежде, чем пометить ключ как рассекреченный, его необходимо отключить.

Примечание:

Ключ также можно пометить как рассекреченный после того, как он отозван.

1. Перейдите в область управления «Криптографические ключи» консоли CMS.
2. Выберите криптографический ключ, который нужно пометить как рассекреченный.
3. Выберите **Действия > Пометить как рассекреченный**.
В диалоговом окне «Пометить как рассекреченный» отобразится предупреждение.
4. Нажмите кнопку **Продолжить**.
5. Выберите в диалоговом окне «Пометить как рассекреченный» один из таких параметров:
 - **Да:** начнется повторное шифрование всех объектов данных, связанных с рассекреченным криптографическим ключом.
 - **Нет:** диалоговое окно «Пометить как рассекреченный» закроется, и криптографический ключ будет помечен как «Рассекреченный» в области управления «Криптографические ключи».

Примечание:

Если выбрать параметр **Нет**, конфиденциальные данные будут по-прежнему связаны с рассекреченным ключом. Рассекреченный ключ будет недоступен для использования в системе для расшифровки связанных с ним объектов.

См. также

- [Отзыв криптографических ключей](#)
- [Статус криптографического ключа](#)
- [Для просмотра объектов, связанных с криптографическим ключом](#)

6.12.3.5 Отзыв криптографических ключей

«Неактивный» криптографический ключ может использоваться связанным с ним объектом данных. Чтобы разорвать связь между зашифрованными объектами и отключенными ключами, необходимо отозвать ключ, выполнив указанные ниже действия.

1. Выберите ключ, который нужно отозвать, среди ключей, список которых приведен в области управления «Криптографические ключи».
2. Последовательно выберите пункты **Действия > Отозвать ключ**.
Откроется диалоговое окно «Отозвать ключ» с предупреждением.
3. Нажмите кнопку **ОК**, чтобы отозвать криптографический ключ.
Начнется шифрование всех объектов, связанных с отозванным ключом, с помощью текущего активного ключа. Если ключ связан с несколькими объектами данных, то он будет отмечен как «Неактивно: повторное шифрование выполняется» до завершения процесса повторного шифрования.

Отозванный криптографический ключ можно безопасно удалить из системы, поскольку в системе не останется конфиденциальных объектов данных, для шифрования которых необходим этот ключ.

6.12.3.6 Удаление криптографических ключей из системы

Перед удалением криптографического ключа из платформы ВІ следует убедиться, что он не является необходимым ни для какого объекта данных в системе. Благодаря этому ограничению все конфиденциальные данные, которые хранятся в репозитории СМС, всегда зашифрованы.

После того как криптографический ключ отозван, его можно удалить из системы с помощью приведенных ниже указаний.

1. Перейдите в область управления «Криптографические ключи» консоли СМС.
2. Выберите криптографический ключ, который нужно удалить.
3. Выберите команды **Управление > Удалить**.
В окне «Удалить ключ» отобразится предупреждение.
4. Нажмите кнопку **Удалить**, чтобы удалить криптографический ключ из системы.
Удаленный ключ больше никогда не отобразится в области управления «Криптографические ключи» консоли СМС.

Примечание:

Удаленный из системы криптографический ключ восстановить невозможно.

См. также

- [Отзыв криптографических ключей](#)
- [Статус криптографического ключа](#)

6.13 Настройка серверов для SSL

Можно использовать протокол SSL для сетевого обмена данными между клиентами и серверами в вашем развертывании платформы BI.

Чтобы установить SSL для всех обменов данными между серверами, необходимо выполнить следующие действия:

- Включено развертывание платформы BI с SSL.
- Создайте файлы ключа и сертификата для каждой машины вашего развертывания.
- Задайте местоположение этих файлов в Диспетчере центральной конфигурации (CCM) и на сервере веб-приложений.

Примечание:

Если используются толстые клиенты, такие как Crystal Reports или Designer, их также необходимо настроить для SSL, если они будут использоваться для подключения к CMS. В противном случае будут выдаваться ошибки при попытке подключения к CMS, настроенному для использования SSL, из толстого клиента, который не был настроен соответствующим образом.

6.13.1 Создание файлов ключа и сертификата

Чтобы установить протокол SSL для обмена данными между серверами, используйте инструмент командной строки SSLC для создания файла ключа и файла сертификата для каждой машины вашего развертывания.

Примечание:

- Необходимо создать сертификаты и ключи для всех машин развертывания, включая машины, на которых выполняются компоненты толстых клиентов, такие как Crystal Reports. Для настройки таких машин клиентов используйте инструмент командной строки `sslconfig`.
- Для максимальной безопасности все секретные ключи должны быть защищены и не должны передаваться по незащищенным каналам.
- Сертификаты, созданные для предыдущих версий платформы BI, не будут работать для платформы SAP BusinessObjects Business Intelligence 4.0. Эти сертификаты потребуются создать заново.

6.13.1.1 Создание файлов ключа и сертификата для компьютера

1. Запустите инструмент `SSLC.exe` из командной строки.

Инструмент SSLC устанавливается вместе с программным обеспечением платформы BI. (В системе Windows, к примеру, установка по умолчанию производится в `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`).

2. Введите следующую команду:

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

Эта команда создает два файла, запрос на сертификат в Орган сертификации (CA) (`cacert.req`) и секретный ключ (`privkey.pem`).

3. Для расшифровки секретного ключа введите следующую команду:

```
sslsc rsa -in privkey.pem -out cakey.pem
```

Эта команда создает файл расшифрованного ключа `cakey.pem`.

4. Чтобы подписать сертификат CA, введите следующую команду:

```
sslsc x509 -in cacert.req -out cacert.pem -req -signkey cakey.pem -days 365
```

Эта команда создает самозаверяющий сертификат, `cacert.pem`, срок действия которого истекает через 365 дней. Выберите количество дней, которое соответствует вашим требованиям безопасности.

5. Используя текстовый редактор, откройте файл `sslsc.cnf`, который хранится в той же папке, что и инструмент командной строки SSLC.

Примечание:

Использование текстового редактора настоятельно рекомендовано для Windows, так как Windows Explorer может неправильно распознать и отобразить файлы с расширением `.cnf`.

6. Выполните следующие действия на основе параметров в файле `sslsc.cnf`.

- Поместите файлы `cakey.pem` и `cacert.pem` в каталоги, заданные параметрами `certificate` и `private_key` файла `sslsc.cnf`.

По умолчанию параметры файла `sslsc.cnf` следующие:

```
certificate = $dir/cacert.pem
```

```
private_key = $dir/private/cakey.pem
```

- Создайте файл с именем, заданным параметром `database` файла `sslsc.cnf`.

Примечание:

По умолчанию это файл `$dir/index.txt`. Файл должен быть пустым.

Данное местоположение будет использоваться для настройки SSL для CCM и вашего сервера веб-приложений.

6.13.2 Настройка протокола SSL

После создания ключей и сертификатов для каждого компьютера развертывания и сохранения их в безопасном месте необходимо обеспечить безопасное местоположение для приложения Central Configuration Manager (CCM) и сервера веб-приложений.

Также потребуется выполнить конкретные шаги по настройке протокола SSL для сервера веб-приложений и для любого компьютера, где запущено приложение толстого клиента.

6.13.2.1 Настройка протокола SSL в CCM

1. В CCM щелкните правой кнопкой мыши элемент Server Intelligence Agent и выберите пункт **Свойства**.
2. В диалоговом окне "Свойства" выберите вкладку **Протокол**.
3. Убедитесь, что выбран параметр **Включить SSL**.
4. Введите путь к каталогу, в котором вы сохранили файлы ключа и сертификата.

Поле	Описание
Папка сертификатов SSL	Папка, в которой сохраняются все необходимые файлы и сертификаты SSL. Например: d:\ssl
Файл сертификатов SSL сервера	Имя файла для хранения сертификата SSL сервера. По умолчанию используется имя servercert.der
Файл надежных сертификатов SSL	Имя файла с надежным сертификатом SSL. По умолчанию используется имя sacert.der
Файл секретных ключей SSL	Имя файла секретных ключей SSL для доступа к сертификату. По умолчанию используется имя server.key
Файл идентификационных фраз секретных ключей SSL	Имя текстового файла, содержащего идентификационную фразу для доступа к секретному ключу. По умолчанию используется имя passphrase.txt

Примечание:

Убедитесь, что указан путь к каталогу на машине, на которой работает сервер.

6.13.2.2 Настройка протокола SSL в ОС UNIX

Для настройки протокола SSL для SIA нужно использовать скрипт `serverconfig.sh`. Этот сценарий запускает текстовую программу, которая позволяет вам просматривать информацию сервера, добавлять и удалять серверы из вашей установки. Скрипт `serverconfig.sh` устанавливается в каталог установки `sap_bobj`.

1. Используйте скрипт `ccm.sh` для остановки SIA и всех серверов SAP BusinessObjects.
2. Выполните скрипт `serverconfig.sh`.
3. Выберите пункт **3 – Изменить Server Intelligence Agent** и нажмите клавишу **Enter**.
4. Укажите целевой SIA и нажмите клавишу **Enter**.
5. Выберите параметр **Изменить конфигурацию Server Intelligence Agent SSL**.
6. Выберите **ssl**.
При запросе укажите местоположения сертификатов SSL.
7. Повторите шаги 1-6 для каждого SIA, если развертывание платформы BI является кластером SIA.
8. Запустите SIA с помощью `ccm.sh` и дождитесь, пока запустятся серверы.

6.13.2.3 Настройка протокола SSL для сервера веб-приложений

1. Для сервера веб-приложений J2EE запустите Java SDK со следующими заданными свойствами системы. Например:

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

В следующей таблице приводятся описания, соответствующие этим примерам:

Например	Описание
<code>DcertDir=d:\ssl</code>	Каталог для хранения всех сертификатов и ключей.
<code>DtrustedCert=cacert.der</code>	Файл доверенного сертификата. При указании более одного файла разделите их точкой с запятой.

Например	Описание
<i>DsslCert=clientcert.der</i>	Сертификат, используемый SDK.
<i>DsslKey=client.key</i>	Секретный ключ сертификата SDK.
<i>Dpassphrase=passphrase.txt</i>	Файл для хранения ключевой фразы (passphrase) секретного ключа.

- Для сервера веб-приложений IIS запустите инструмент `sslconfig` из командной строки и следуйте указаниям по конфигурации.

6.13.2.4 Настройка "толстых" клиентов

Перед выполнением следующей процедуры необходимо создать все требуемые ресурсы SSL, такие как сертификаты и личные ключи, и сохранить их в известном каталоге.

В приведенной ниже процедуре предполагается, что были выполнены инструкции по созданию следующих ресурсов SSL:

Ресурс SSL	
Папка сертификатов SSL	d:\ssl
Файл сертификата SSL сервера	servercert.der
имя файла доверенного сертификата SSL или корневого сертификата	cacert.der
Имя файла секретных ключей SSL	server.key
Файл, содержащий контрольную фразу для доступа к личному ключу SSL	passphrase.txt

После создания перечисленных выше ресурсов выполните следующие ниже инструкции, чтобы настроить приложения "толстых" клиентов, такие как ССМ или средство управления обновлениями.

- Убедитесь, что приложение толстого клиента не выполняет никаких операций.

Примечание:

Убедитесь, что указан путь к каталогу на компьютере, где работает сервер.

- Запустите инструмент `sslconfig.exe` из командной строки.

Инструмент SSLC устанавливается вместе с программным обеспечением платформы BI. (В системе Windows, к примеру, установка по умолчанию производится в <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64).

3. Введите следующую команду:

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

4. Повторно запустите приложение толстого клиента.

См. также

- [Создание файлов ключа и сертификата для компьютера](#)

6.13.2.4.1 Настройка SSL-входа для средства управления переводами

Чтобы обеспечить пользователям SSL-вход в средство управления переводами, необходимо добавить сведения о ресурсах SSL в файл конфигурации средства (INI-файл).

1. Найдите файл `TransMgr.ini` в следующем каталоге: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86.
2. Откройте файл `TransMgr.ini` в текстовом редакторе.
3. Добавьте следующие параметры:

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

4. Сохраните файл и закройте текстовый редактор.

Теперь пользователи могут использовать SSL при входе в средство управления переводами.

6.13.2.4.2 Настройка SSL для средства преобразования отчетов

Перед выполнением следующей процедуры необходимо создать все требуемые ресурсы SSL, такие как сертификаты и личные ключи, и сохранить их в известном каталоге. В дополнение к этому необходимо установить средство преобразования отчетов как часть развертывания платформы BI.

В приведенной ниже процедуре предполагается, что были выполнены инструкции по созданию следующих ресурсов SSL:

Ресурс SSL	
Папка сертификатов SSL	d:\ssl
Файл сертификата SSL сервера	servercert.der
имя файла доверенного сертификата SSL или корневого сертификата	cacert.der
Имя файла секретных ключей SSL	server.key
Файл, содержащий контрольную фразу для доступа к личному ключу SSL	passphrase.txt

После создания перечисленных выше ресурсов выполните следующие инструкции, чтобы настроить SSL для работы со средством преобразования отчетов.

1. Создайте переменную среды Windows `BOBJ_MIGRATION` на компьютере, где размещается средство преобразования отчетов.

Совет:

Этой переменной можно присвоить любое значение.

2. Откройте в текстовом редакторе файл `migration.bat` из следующего каталога:
`<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\scripts\.`
3. Найдите следующую строку::

```
start "" "%JRE%\bin\javaw" -Xmx512m -Xss10m -jar "%SHAREDIR%\lib\migration.jar"
```

4. Добавьте следующие данные после параметра `-Xss10m`:

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir=C:/ssl
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
-Dbusinessobjects.migration
```

Примечание:

Убедитесь, что параметры разделены знаком пробела.

5. Сохраните файл и закройте текстовый редактор.

Теперь пользователи имеют возможность использовать SSL при доступе к средству преобразования отчетов.

См. также

- [Создание файлов ключа и сертификата для компьютера](#)

6.14 Основные сведения об обмене данными между компонентами платформы BI

Если система платформы BI полностью развернута в одной защищенной подсети, отсутствует необходимость выполнения какой-либо специальной настройки брандмауэров. Однако можно выбрать развертывание некоторых компонентов в других подсетях, разделенных одним или несколькими брандмауэрами.

Важно понимать принципы обмена данными между серверами платформы BI, толстыми клиентами и сервером веб-приложений, на котором размещен пакет SAP BusinessObjects Enterprise SDK, перед настройкой системы для работы с брандмауэрами.

См. также

- [Настройка платформы BI для брандмауэров](#)
- [Примеры типовых сценариев развертывания брандмауэров](#)

6.14.1 Обзор серверов платформы BI и портов обмена данными

Необходимо знать принципы работы серверов платформы BI и их портов обмена данными, если система развернута с брандмауэрами.

6.14.1.1 Каждый сервер платформы BI связывается с портом запросов

Сервер платформы BI, например сервер репозитория входящих файлов, связывается с портом запросов при запуске. Другие компоненты платформы BI, включая серверы, толстые клиенты и пакеты SDK, размещенные на сервере веб-приложений, могут использовать этот порт запросов для обмена данными с сервером.

Сервер динамически выбирает номер порта запроса при запуске или перезапуске, если только он не настроен на использование конкретного номера порта. Определенный номер порта запроса необходимо настроить для серверов, обменивающихся данными с другими компонентами платформы BI через брандмауэр.

6.14.1.2 Все серверы платформы BI, зарегистрированные в CMS

Серверы платформы BI регистрируются в CMS при их запуске. При регистрации сервера сервер CMS записывает следующее:

- Имя хоста (или IP-адрес) компьютера хоста сервера.
- Номер порта запросов сервера.

6.14.1.3 Центральный сервер управления использует два порта

Центральный сервер управления использует два порта: порт запросов и порт сервера имен. Порт запросов выбирается динамически по умолчанию. По умолчанию используется порт сервера имен 6400.

Все серверы и клиентские приложения платформы BI будут первоначально обращаться к центральному серверу управления (CMS) через порт сервера имен. Центральный сервер управления (CMS) будет отвечать при первоначальной связи путем передачи значения своего порта запросов. Серверы будут использовать этот порт запросов для последующего обмена данными с центральным сервером управления (CMS).

6.14.1.4 На Центральном сервере управления (CMS) доступен каталог зарегистрированных служб

Центральный сервер управления (CMS) предоставляет каталог служб, зарегистрированных на нем. Другие компоненты платформы BI, такие как службы, толстые клиенты и пакеты SDK, размещенные на сервере веб-приложений, могут обращаться к CMS и запрашивать ссылку на определенную службу. В ссылке на службу содержится номер порта запросов службы, а также имя (или IP-адрес) хоста сервера и идентификатор службы.

Компоненты платформы BI должны располагаться в другой подсети относительно используемого сервера. Имя хоста (или IP-адрес), содержащиеся в ссылке на службу, должно быть маршрутизируемым от компьютера, на котором установлен компонент.

Примечание:

В ссылке на сервер платформы BI содержится имя хоста компьютера сервера по умолчанию. (Если компьютеру назначены несколько имен хоста, выбирается основное имя хоста). Можно настроить сервер таким образом, чтобы в ссылке вместо имени хоста содержался IP-адрес.

См. также

- [Взаимодействие между компонентами платформы BI](#)

6.14.1.5 Агент Server Intelligence (SIA) взаимодействует с Центральным сервером управления (CMS)

Если подобное взаимодействие невозможно, развертывание не будет работать. Убедитесь в том, что порты брандмауэра настроены соответствующим образом и не препятствуют взаимодействию всех агентов SIA и всех центральных серверов управления в кластере.

6.14.1.6 Дочерние процессы сервера заданий обмениваются данными с ярусом данных и сервером CMS

На большинстве серверов заданий дочерний процесс создается для обработки задачи, такой как создание отчета. Сервер заданий создает дочерние процессы. Для каждого дочернего процесса предусмотрен собственный порт запросов.

По умолчанию сервер заданий динамически выбирает порт запросов для каждого дочернего процесса. Можно указать диапазон номеров портов, из которого будет выбирать номер сервер заданий.

Все дочерние процессы обмениваются данными с сервером CMS. Если этот обмен данными осуществляется через брандмауэр, необходимо выполнить следующее:

- Укажите диапазон номеров портов, которые сможет выбирать сервер заданий, добавив параметры `-requestJSChildPorts<наименьший_порт>-<наибольший_порт>` и `-requestPort<порт>` к командной строке сервера. Обратите внимание, что диапазон портов должен быть достаточно большим, чтобы разрешить выполнение максимального числа дочерних процессов, как задано в параметре `-maxJobs`.
- Открыть указанный диапазон портов в брандмауэре.

Многие дочерние процессы обмениваются данными с ярусом данных. Например, дочерний процесс может подключаться к базе данных отчетов, извлекать данные и вычислять значения для отчета. Если дочерний процесс сервера заданий обменивается данными с уровнем данных через брандмауэр, необходимо выполнить следующее:

- Открыть путь обмена данными в брандмауэре от любого порта на компьютере сервера заданий к порту прослушивания базы данных на компьютере сервера баз данных.

См. также

- [Обзор командных строк](#)

6.14.2 Взаимодействие между компонентами платформы BI

Компоненты платформы BI, такие как клиенты браузеров, толстые клиенты, серверы и SDK, установленные на сервере веб-приложений, взаимодействуют друг с другом по сети в ходе выполнения обычных рабочих процессов. Понимание этих рабочих процессов необходимо для развертывания продуктов SAP BusinessObjects в различных подсетях, разделенных брандмауэром.

6.14.2.1 Требования для обмена данными между компонентами платформы BI

Развертывания платформы BI должны соответствовать следующим общим требованиям.

1. Каждый сервер должен иметь возможность инициировать обмен данными со всеми остальными серверами платформы BI через порт запросов сервера.
2. Центральный сервер управления использует два порта. Каждый сервер платформы BI, толстый клиент и сервер веб-приложений, на которых установлен SDK, должен иметь возможность инициировать обмен данными с центральным сервером управления (CMS) через оба порта.
3. Каждый из дочерних процессов сервера заданий должен иметь возможность обмениваться данными с центральным сервером управления.
4. Толстые клиенты должны иметь возможность инициировать обмен данными с портом запросов серверов репозитория входящих и исходящих файлов
5. Если для толстых клиентов и веб-приложений включен аудит, они должны иметь возможность инициировать обмен данными с портом запросов серверов адаптивной обработки, на которых выполняется прокси-служба аудита клиентов.
6. В общем случае сервер веб-приложений, на котором установлен SDK, должен иметь возможность обмениваться данными с портом запросов каждого из серверов платформы BI.

Примечание:

Серверу веб-приложений необходимо обмениваться данными только с серверами платформы BI, используемыми в развертывании. Например, если приложение Crystal Reports не используется, серверу веб-приложений не нужно обмениваться данными с серверами кэширования Crystal Reports.

7. Серверы заданий используют номера портов, указанные с помощью команды `-requestJSChildPorts <диапазон портов>`. Если в командной строке не указан диапазон, серверы используют случайные номера портов. Чтобы разрешить серверу заданий обмен данными с центральным сервером управления, FTP-сервером или почтовым сервером на другом компьютере, откройте в брандмауэре все порты из диапазона, указанного ключом `-requestJSChildPorts`, в брандмауэре.
8. Центральный сервер управления должен иметь возможность обмениваться данными с портом прослушивания базы данных центрального сервера управления.

9. Сервер соединений, большинство дочерних процессов сервера заданий, каждая системная база данных и каждый сервер обработки аудита должны иметь возможность инициировать обмен данными с портом прослушивания базы данных отчетов.

См. также

- [Платформа BI: требования к портам](#)

6.14.2.2 Платформа BI: требования к портам

В этом разделе перечислены порты обмена данными, используемые серверами платформы BI, толстыми клиентами, сервером веб-приложений, на котором установлен компонент SDK, и программными приложениями сторонних организаций. При развертывании платформы BI с брандмауэрами можно использовать эти сведения для открытия минимального числа портов этих брандмауэров.

6.14.2.2.1 Требования к портам для приложений платформы BI

В этой таблице перечислены серверы и номера портов, используемых приложениями платформы BI.

Продукт	Клиент-ское приложение	Связанный сервер	Требования к порту сервера
Crystal Reports	Конструктор SAP Crystal Reports 2011	<p>CMS</p> <p>Сервер репозитория входящих файлов</p> <p>Сервер репозитория исходящих файлов</p> <p>Crystal Reports 2011 Report Application Server (RAS)</p> <p>Сервер обработки Crystal Reports 2011</p> <p>Кэш-сервер Crystal Reports</p>	<p>Порт сервера имен CMS (по умолчанию 6400)</p> <p>Порт запросов CMS</p> <p>Порт запросов сервера репозитория входящих файлов</p> <p>Порт запросов сервера репозитория исходящих файлов</p> <p>Порт запросов сервера Crystal Reports 2011 Report Application Server</p> <p>Порт запросов сервера обработки Crystal Reports 2011</p> <p>Порт запросов кэш-сервера Crystal Reports</p>

Продукт	Клиент-ское приложение	Связанный сервер	Требования к порту сервера
Crystal Reports	Конструктор SAP Crystal Reports для Enterprise	<p>CMS</p> <p>Сервер репозитория входящих файлов</p> <p>Сервер репозитория исходящих файлов</p> <p>Сервер обработки Crystal Reports</p> <p>Кэш-сервер Crystal Reports</p>	<p>Порт сервера имен CMS (по умолчанию 6400)</p> <p>Порт запросов CMS</p> <p>Порт запросов сервера репозитория входящих файлов</p> <p>Порт запросов сервера репозитория исходящих файлов</p> <p>Порт для запросов сервера обработки Crystal Reports</p> <p>Порт запросов кэш-сервера Crystal Reports</p>
Dashboard Design	SAP Business Objects Dashboard Design	<p>CMS</p> <p>Сервер репозитория входящих файлов</p> <p>Сервер репозитория исходящих файлов</p> <p>Приложение поставщика веб-служб (dswsbobje.war), в котором размещаются Dashboard Design, Live Office и службы QaaWS, необходимые для некоторых соединений с источниками данных.</p>	<p>Порт сервера имен CMS (по умолчанию 6400)</p> <p>Порт запросов CMS</p> <p>Порт запросов сервера репозитория входящих файлов</p> <p>Порт запросов сервера репозитория исходящих файлов</p> <p>Порт HTTP (по умолчанию 80)</p>
Live Office	Клиент Live Office	<p>Приложение поставщика веб-служб (dswsbobje.war), в котором размещается веб-служба Live Office</p>	<p>Порт HTTP (по умолчанию 80)</p>

Продукт	Клиент-ское приложение	Связанный сервер	Требования к порту сервера
Платформа BI	Рабочий стол SAP Business Objects Web Intelligence	CMS Сервер репозитория входящих файлов	Порт сервера имен CMS (по умолчанию 6400) Порт запросов CMS Порт запросов сервера репозитория входящих файлов
Платформа BI	Средство создания универсов	CMS Сервер репозитория входящих файлов Сервер соединений	Порт сервера имен CMS (по умолчанию 6400) Порт запросов CMS Порт запросов сервера репозитория входящих файлов Порт сервера соединений
Платформа BI	Диспетчер Business View	CMS Сервер репозитория входящих файлов	Порт сервера имен CMS (по умолчанию 6400) Порт запросов CMS Порт запросов сервера репозитория входящих файлов

Продукт	Клиент-ское приложение	Связанный сервер	Требования к порту сервера
Платформа BI	Central Configuration Manager (CCM)	CMS Агент Server Intelligence (SIA)	<p>Следующие порты необходимо открыть, чтобы разрешить CCM управлять удаленными серверами платформы BI:</p> <p>Порт сервера имен CMS (по умолчанию 6400)</p> <p>Порт запросов CMS</p> <p>Следующие порты необходимо открыть, чтобы разрешить CCM управлять удаленными процессами SIA:</p> <p>Службы каталогов Microsoft (порт 445 TCP)</p> <p>Служба сеанса NetBIOS (порт 139 TCP)</p> <p>Служба диаграмм NetBIOS (порт 138 UDP)</p> <p>Служба имен NetBIOS (порт 137 UDP)</p> <p>DNS (порт 53 TCP/UDP)</p> <p>(Обратите внимание, что некоторые из перечисленных портов могут быть необязательными. Обратитесь к администратору Windows).</p>
Платформа BI	Агент Server Intelligence (SIA)	Все серверы платформы BI, включая центральный (CMS)	<p>Порт запросов SIA (по умолчанию 6410)</p> <p>Порт сервера имен CMS (по умолчанию 6400)</p> <p>Порт запросов CMS</p>

Продукт	Клиент-ское приложение	Связанный сервер	Требования к порту сервера
Платформа BI	Средство преобразования отчетов	CMS Сервер репозитория входящих файлов	Порт сервера имен CMS (по умолчанию 6400) Порт запросов CMS Порт запросов сервера репозитория входящих файлов
Платформа BI	Repository Diagnostic Tool	CMS Сервер репозитория входящих файлов Сервер репозитория исходящих файлов	Порт сервера имен CMS (по умолчанию 6400) Порт запросов CMS Порт запросов сервера репозитория входящих файлов Порт запросов сервера репозитория исходящих файлов
Платформа BI	SDK для платформы BI, расположенный на сервере веб-приложений	Все серверы платформы BI, необходимые для установленных продуктов. Например, обмен данными с портом запросов сервера обработки Crystal Reports 2011 требуется, если SDK извлекает отчеты Crystal из CMS и взаимодействует с ними.	Порт сервера имен CMS (по умолчанию 6400) Порт запросов CMS Порт запросов для каждого требуемого сервера. Например, порт запросов сервера обработки Crystal Reports 2011.

Продукт	Клиент-ское приложение	Связанный сервер	Требования к порту сервера
Платформа BI	Поставщик веб-служб (dswsdoobje.wat)	<p>Все серверы платформы BI, необходимые для доступа продуктов к веб-службам.</p> <p>Например, взаимодействие с портами запросов сервера кэширования Dashboard Design и сервера обработки требуется, если SAP BusinessObjects Dashboard Design получает доступ к соединениям с источниками данных Enterprise через поставщик веб-служб.</p>	<p>Порт сервера имен CMS (по умолчанию 6400)</p> <p>Порт запросов CMS</p> <p>Порт запросов для каждого требуемого сервера. Например, порт кэш-сервера Dashboard Design и порт запросов сервера обработки Dashboard Design.</p>
Платформа BI	SAP BusinessObjects Analysis, версия для OLAP	<p>CMS</p> <p>Адаптивный сервер обработки, на котором размещена служба многомерного анализа</p> <p>Сервер репозитория входящих файлов</p> <p>Сервер репозитория исходящих файлов</p>	<p>Порт сервера имен CMS (по умолчанию 6400)</p> <p>Порт запросов CMS</p> <p>Порт запросов настраиваемого сервера обработки</p> <p>Порт запросов сервера репозитория входящих файлов</p> <p>Порт запросов сервера репозитория исходящих файлов</p>

6.14.2.2.2 Требования к портам для сторонних приложений

В этой таблице перечислено стороннее программное обеспечение, используемое продуктами SAP Business Objects. Приведены определенные примеры для некоторых поставщиков программного обеспечения, но у различных поставщиков требования к портам отличаются.

Стороннее приложение	Компонент SAP Business Objects, использующий сторонний продукт	Требование к порту стороннего приложения	Описание
База данных системы CMS	Центральный сервер управления (CMS)	Порт прослушивания сервера баз данных	Сервер CMS является единственным сервером, обменивающимся данными с базой данных системы CMS.
База данных аудита CMS	Центральный сервер управления (CMS)	Порт прослушивания сервера баз данных	Сервер CMS является единственным сервером, обменивающимся данными с базой данных аудита CMS.
База данных отчетов	Сервер соединений Каждый дочерний процесс сервера заданий Каждый сервер обработки	Порт прослушивания сервера баз данных	Эти серверы получают данные из базы данных отчетов.
сервер веб-приложений	Все веб-службы SAP Business Objects и все веб-приложения, включая стартовую панель BI и CMS	Порт HTTP и порт HTTPS. Например, на сервере Tomcat портом HTTP по умолчанию является 8080, а портом HTTPS – 443.	Порт HTTPS необходим, только если используется защищенный обмен данными HTTP.
Сервер FTP	Каждый сервер заданий	Вход FTP (порт 21) Выход FTP (порт 22)	На сервере заданий порты FTP используются для разрешения отправки на FTP .
Сервер электронной почты	Каждый сервер заданий	SMTP (порт 25)	На сервере заданий порт SMTP используется для разрешения передачи электронной почты .

Стороннее приложение	Компонент SAP Business Objects, использующий сторонний продукт	Требование к порту стороннего приложения	Описание
Серверы Unix, на которые серверы заданий могут передавать содержимое	Каждый сервер заданий	выход rhexec (порт 512) (Только для Unix) выход rsh (порт 514)	(Только для Unix) Серверы заданий используют эти порты для разрешения отправки на диск .
Сервер аутентификации	CMS сервер веб-приложений, где расположен SDK любой "толстый" клиент, например Live Office.	Порт соединений для сторонней аутентификации. Например, сервер соединений для сервера Oracle LDAP определяет пользователя в файле ldap.ora.	Пользовательские учетные данные хранятся на стороннем сервере аутентификации. Компонентам CMS, SDK и толстым клиентам, перечисленным здесь, необходимо обмениваться данными со сторонним сервером аутентификации во время входа пользователя.

6.15 Настройка платформы BI для брандмауэров

В этом разделе приводятся пошаговые инструкции по настройке системы платформы BI для работы в среде брандмауэра.

6.15.1 Настройка системы для использования брандмауэров

1. Определите, какие компоненты платформы BI должны обмениваться данными через брандмауэр.
2. Настройте порт запросов для каждого сервера платформы BI, который должен обмениваться данными через брандмауэр.

3. Настройте диапазон портов для любых дочерних элементов сервера заданий, которые должны обмениваться данными через брандмауэр, добавив параметры `-requestJSChildPorts<наименьший_порт>-<наибольший_порт>` и `-requestPort<порт>` в командную строку сервера.
4. Настройте брандмауэр, разрешив обмен данными через порты запросов и диапазон портов сервера заданий на серверах платформы BI, которые были настроены в предыдущем действии.
5. При необходимости настройте файл хостов hosts на каждом компьютере, где имеется сервер платформы BI с обменом данными через брандмауэр.

См. также

- [Взаимодействие между компонентами платформы BI](#)
- [Настройка номеров портов](#)
- [Обзор командных строк](#)
- [Определение правил брандмауэра](#)
- [Настройка файла хостов для брандмауэров с NAT](#)

6.15.1.1 Определение правил брандмауэра

Необходимо настроить брандмауэр, чтобы разрешить передачу требуемых данных между компонентами платформы BI. Обратитесь к документации по брандмауэру для получения сведений об определении этих правил.

Укажите по одному правилу входящего доступа для каждого пути соединения через брандмауэр. Возможно, правила доступа следует определять не для каждого из серверов платформы BI за брандмауэром.

Используйте номер порта, указанный в поле **Порт** на сервере. Запомните, что для каждого сервера на компьютере необходимо использовать уникальный номер порта. Для некоторых серверов Business Objects используются несколько портов.

Примечание:

Если платформа BI развернута за брандмауэрами с поддержкой NAT, то для каждого из серверов на всех компьютерах необходимо определить уникальный номер порта запросов. То есть использование для двух серверов во всем развертывании одинакового порта запросов невозможно.

Примечание:

Отсутствует необходимость указывать какое-либо правило входящего доступа. Серверы платформы BI не инициируют обмен данными с сервером веб-приложений или каким-либо клиентским приложением. Серверы платформы BI могут инициировать обмен данными с другими серверами платформы в том же кластере. Развертывания с кластеризованными серверами в среде, в которой исходящие соединения защищаются брандмауэром, не поддерживаются.

Пример:

В этом примере показаны правила входящего доступа для брандмауэра между сервером веб-приложений и серверами платформы BI. В этом случае необходимо открыть два порта для сервера CMS: один порт для сервера репозитория входящих файлов (FRS) и один порт для сервера репозитория исходящих файлов. Номера порта запросов – это номера портов, установленные в поле **Порт** на странице конфигурации CMS для сервера.

Исходный компьютер	Порт	Целевой компьютер	Порт	Действие
сервер веб-приложений	Любой	CMS	6400	Разрешить
сервер веб-приложений	Любой	CMS	<Номер порта запросов>	Разрешить
сервер веб-приложений	Любой	Сервер репозитория входящих файлов	<Номер порта запросов>	Разрешить
сервер веб-приложений	Любой	Сервер репозитория исходящих файлов	<Номер порта запросов>	Разрешить
Любой	Любой	CMS	Любой	Отказ
Любой	Любой	Другие серверы платформы	Любой	Отказ

См. также

- [Взаимодействие между компонентами платформы BI](#)

6.15.1.2 Настройка файла хостов для брандмауэров с NAT

Это действие необходимо только в том случае, если серверы платформы BI должны обмениваться данными через брандмауэр, на котором включено преобразование сетевых адресов (NAT). Оно

позволяет клиентским компьютерам сопоставить имя хоста сервера с маршрутизируемым IP-адресом.

Примечание:

Платформу BI можно развернуть на компьютерах, на которых используется система имен доменов (DNS). В этом случае имена хостов компьютера сервера можно сопоставить с внешне маршрутизируемым IP-адресом на сервере DNS, а не в файле `hosts` на каждом компьютере.

Принцип преобразования сетевых адресов

Брандмауэр развернут для предотвращения несанкционированного доступа к внутренней сети. Брандмауэры, использующие преобразование методом «NAT», будут сопоставлять IP-адреса из внутренней сети с другим адресом, используемым во внешней сети. Подобное «преобразование адресов» позволяет повысить уровень защиты благодаря скрытию внутреннего IP-адреса от внешней сети.

Компоненты платформы BI, такие как серверы, толстые клиенты и сервер веб-приложений, на котором размещен пакет SAP BusinessObjects Enterprise SDK, будут использовать ссылку на службу для связи с сервером. В ссылке на службу содержится имя хоста компьютера сервера. Это имя хоста должно быть маршрутизируемым с компьютера компонента платформы BI. Это означает, что в файле `hosts` на компьютере компонента должно выполняться сопоставление имени хоста компьютера сервера с внешним IP-адресом компьютера сервера. Внешний IP-адрес компьютера сервера является маршрутизируемым с внешней стороны брандмауэра (в отличие от внутреннего IP-адреса).

Процедура настройки файла `hosts` для систем Windows и UNIX различается.

6.15.1.2.1 Настройка файла `hosts` в системе Windows

1. Определите каждый компьютер, на котором запущен компонент платформы BI, который должен обмениваться данными через брандмауэр с включенным «преобразованием сетевых адресов» («NAT»).
2. На каждом компьютере, определенном в предыдущем действии, откройте файл `hosts` с помощью текстового редактора, такого как Блокнот. Файл `hosts` находится в каталоге `\WINNT\system32\drivers\etc\hosts`.
3. Следуйте инструкциям в файле `hosts` для добавления записи для каждого компьютера за пределами брандмауэра, на котором запущен один или несколько серверов платформы BI. Сопоставьте имя хоста компьютера сервера или полное имя домена с его внешним IP-адресом.
4. Сохраните файл `hosts`.

6.15.1.2.2 Настройка файла `hosts` в системе UNIX

Примечание:

В операционной системе UNIX сначала необходимо настроить обращение к файлу «hosts» для разрешения имен доменов перед обращением к системе DNS. Обратитесь к документации UNIX для получения подробных сведений.

1. Определите каждый компьютер, на котором запущен компонент платформы BI, который должен обмениваться данными через брандмауэр с включенным «преобразованием сетевых адресов» («NAT»).

2. Откройте файл «hosts» с помощью редактора, такого как `vi`. Файл `hosts` находится в следующем каталоге: `\etc`
3. Следуйте инструкциям в файле `hosts` для добавления записи для каждого компьютера за пределами брандмауэра, на котором запущен один или несколько серверов платформы BI. Сопоставьте имя хоста компьютера сервера или полное имя домена с его внешним IP-адресом.
4. Сохраните файл `hosts`.

6.15.2 Отладка развертывания брандмауэра

Если один или несколько серверов платформы BI перестают работать при включении брандмауэра, хотя в брандмауэре открыты требуемые порты, можно просмотреть журналы событий, чтобы определить, по каким портам и IP-адресам сервера пытаются принимать данные. Можно или открыть эти порты в брандмауэре, или с помощью Central Management Console (CMC) изменить номера портов или IP-адреса, которые пытаются прослушать эти серверы.

При каждом запуске сервера платформы BI в журнал событий записывается следующая информация по каждому запрошенному порту, по которому производится попытка установления связи.

- «Сервер» – имя сервера и успешность запуска.
- «Опубликованные адреса» – Список сочетаний IP-адресов и портов, публикуемых в службу имен. Другие сервера будут использовать адреса и имена из списка для обмена данными с этим сервером.

Если сервер успешно установил связь через порт, в файл журнала также записывается «Прослушивание порта(портов)», IP-адрес и порт, которые прослушивает сервер. Если серверу не удалось установить связь через данный порт, то в файл журнала добавляется запись «Не удалось внести в список», IP-адрес и порт, на которых серверу не удалось начать прослушивание.

При запуске центрального сервера управления для порта службы имен сервера также регистрируются данные об опубликованном адресе(адресах), прослушиваемом порте(портах) и неудачных попытках прослушивания портов.

Примечание:

Если сервер настроен на использование автоматически назначаемого порта, а также на использование недопустимого имени хоста или IP-адреса, в журнале производится запись о неудачной попытке прослушать порт по имени хоста или IP-адрес и порт «0». Если указанное имя хоста или IP-адрес неверно, серверу не удастся связаться до того, как операционная система хоста сможет назначить порт.

Пример:

В следующем примере показана запись центрального сервера управления об успешном прослушивании двух портов запросов и порта службы имен.

```
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 Для отладки развертывания за брандмауэром

1. Ознакомьтесь с журналом событий для определения успешности установления связи сервера по указанному порту.

Если сервер не смог успешно установить связь с портом, вероятно существует конфликт порта между сервером и другим процессом, запущенным на этом же компьютере. Запись «Не удастся прослушать порты» указывает на порт, который сервер пытался прослушать. Запустите утилиту, подобную netstat, для определения процесса, использующего этот порт, а затем настройте другой процесс или задайте другой порт прослушивания сервером.

2. Если сервер успешно установил связь по порту, запись «Прослушивание портов» указывает на порт, который прослушивает сервер. Если сервер прослушивается по порту но он все еще не работает правильно, убедитесь, что этот порт открыт в брандмауэре или настройте сервер так, чтобы он прослушивал тот порт, который открыт.

Примечание:

Если все центральные серверы управления в вашем развертывании пытаются прослушивать порты или IP-адреса, которые недоступны, эти серверы не смогут запуститься и вы не сможете войти в консоль СМС. Если необходимо сменить номер порта или IP-адрес, который пытается прослушать центральный сервер управления, в Central Configuration Manager (CCM) следует указать допустимый порт или IP-адрес.

См. также

- [Настройка номеров портов](#)

6.16 Примеры типовых сценариев развертывания брандмауэров

В этом разделе приводятся примеры типовых сценариев развертывания брандмауэров.

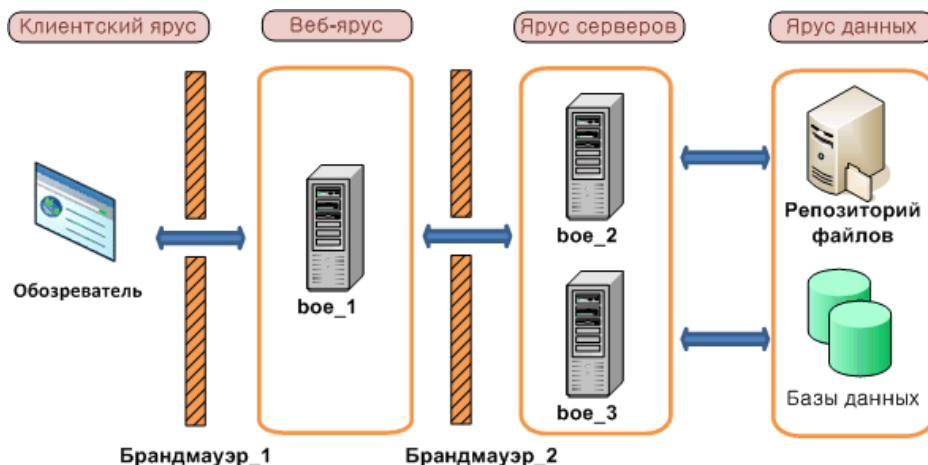
6.16.1 Пример: уровень приложений развернут в отдельной сети

В этом примере показан способ настройки брандмауэра и платформы BI для совместной работы в конфигурации, в которой брандмауэр разделяет сервер веб-приложений и серверы платформы BI.

В этом примере компоненты платформы BI развернуты на следующих компьютерах:

- На компьютере `boe_1` установлены сервер веб-приложений и SDK.
- На компьютере `boe_2` установлены серверы уровня Intelligence, включая Центральный сервер управления, сервер репозитория входящих файлов, сервер репозитория исходящих файлов и сервер событий.
- На компьютере `boe_3` установлены серверы уровня обработки, в том числе адаптивный сервер заданий, сервер обработки Web Intelligence, сервер приложений отчетности, кэш-сервер Crystal Reports и сервер обработки Crystal Reports.

Рис. 6-1: Уровень приложений развернут в отдельной сети



6.16.1.1 Настройка яруса приложений, развернутого в отдельной сети

Ниже приводятся действия по настройке, которые необходимо выполнить в этом примере.

1. Требования к обмену данными, применяемые в этом примере:

- Сервер веб-приложений, где установлен SDK, должен иметь возможность обмена данными с CMS по обоим портам.
- Сервер веб-приложений, где расположен SDK, должен иметь возможность обмена данными со всеми серверами платформы BI.
- Браузер должен иметь доступ к порту запросов http или https на сервере веб-приложений.

2. Сервер веб-приложений должен обмениваться данными со всеми серверами платформы BI на компьютере `boe_2` и `boe_3`. Настройте номера портов для каждого сервера, расположенного на этих машинах. Обратите внимание на то, что использовать можно любой свободный порт в пределах 1025-65535.

Номера портов, выбранных для этого примера, перечислены в следующей таблице:

Сервер	Номер порта
Центральный сервер управления	6400
Центральный сервер управления	6411
Сервер репозитория входящих файлов	6415
Сервер репозитория исходящих файлов	6420
Сервер событий	6425
Адаптивный сервер заданий	6435
Кэш-сервер Crystal Reports	6440
Сервер обработки Web Intelligence	6460
Сервер приложений отчетов	6465
Сервер обработки Crystal Reports	6470

3. Настройте брандмауэры `Firewall_1` и `Firewall_2`, чтобы разрешить обмен данными через назначенные порты на серверах платформы BI и сервере веб-приложений, которые были настроены в предыдущем действии.

В этом примере открывается порт HTTP для сервера приложений Tomcat.

Таблица 6-6: Конфигурация для `Firewall_1`

Порт	Целевой компьютер	Порт	Действие
Любой	<code>boe_1</code>	8080	Разрешить

Конфигурация для `firewall_2`

Исходный компьютер	Порт	Целевой компьютер	Порт	Действие
<code>boe_1</code>	Любой	<code>boe_2</code>	6400	Разрешить
<code>boe_1</code>	Любой	<code>boe_2</code>	6411	Разрешить
<code>boe_1</code>	Любой	<code>boe_2</code>	6415	Разрешить

Исходный компьютер	Порт	Целевой компьютер	Порт	Действие
boe_1	Любой	boe_2	6420	Разрешить
boe_1	Любой	boe_2	6425	Разрешить
boe_1	Любой	boe_3	6435	Разрешить
boe_1	Любой	boe_3	6440	Разрешить
boe_1	Любой	boe_3	6460	Разрешить
boe_1	Любой	boe_3	6465	Разрешить
boe_1	Любой	boe_3	6470	Разрешить

4. В этом брандмауэре не поддерживается NAT, поэтому настраивать файл `hosts` не требуется.

См. также

- [Настройка номеров портов](#)
- [Основные сведения об обмене данными между компонентами платформы BI](#)

6.16.2 Пример: толстый клиент и уровень БД отделены брандмауэром от платформы BI

В этом примере показан способ настройки брандмауэра и платформы BI для совместной работы в сценарии развертывания, в котором:

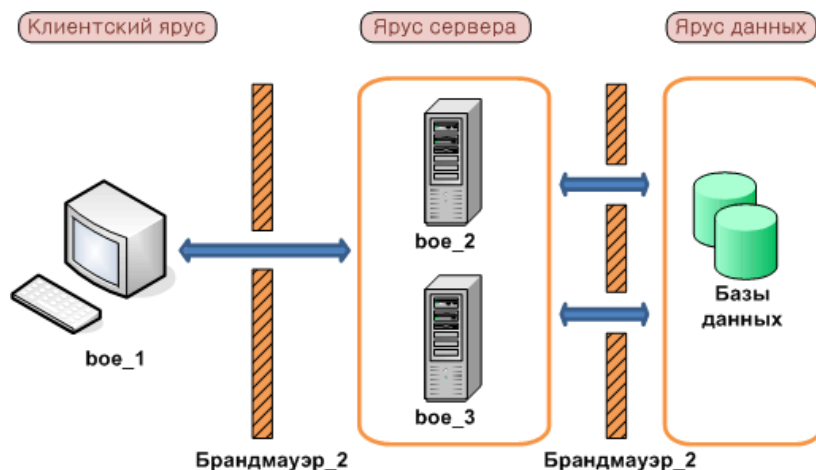
- Один брандмауэр разделяет серверы платформы BI и толстый клиент.
- Один брандмауэр разделяет серверы платформы BI и уровень БД.

В этом примере компоненты платформы BI развернуты на следующих компьютерах:

- На компьютере `boe_1` установлен Мастер публикаций. Мастер публикаций является толстым клиентом платформы BI.
- На компьютере `boe_2` установлены серверы яруса Intelligence, включая Центральный сервер управления (CMS), сервер репозитория входящих файлов, сервер репозитория исходящих файлов и сервер событий.
- На компьютере `boe_3` размещаются серверы уровня обработки, в том числе адаптивный сервер заданий, сервер обработки Web Intelligence, сервер приложений отчетности, сервер обработки Crystal Reports и кэш-сервер Crystal Reports.
- На компьютере `Databases` установлены база данных центрального сервера управления и база данных отчетов. Обратите внимание, что обе базы данных можно развернуть на одном

сервере баз данных или каждую базу данных можно развернуть на собственном сервере баз данных. В этом примере все базы данных центрального сервера управления CMS и база данных отчетов развернуты на одном сервере баз данных. Порт прослушивания сервера баз данных – 3306, что является портом прослушивания базы данных по умолчанию для сервера MySQL.

Рис. 6-2: Толстый клиент и уровень базы данных развернуты в отдельных сетях



6.16.2.1 Настройка уровней, отделенных брандмауэром от серверов платформы BI

Ниже приводятся действия по настройке, которые необходимо выполнить в этом примере.

1. В этом примере примените следующие требования к обмену данными:

- Мастер публикаций должен иметь возможность инициировать обмен данными с сервером CMS через оба порта.
- Мастер публикация должен иметь возможность инициировать обмен данными с сервером репозитория входящих файлов и сервером репозитория исходящих файлов.
- Сервер соединений, каждый дочерний процесс сервера заданий и каждый сервер обработки должны иметь доступ к порту прослушивания на сервере отчетов базы данных.
- Сервер CMS должен иметь доступ к порту прослушивания базы данных на сервере баз данных CMS.

2. Настройте определенный порт для сервера CMS, сервера репозитория входящих файлов и сервера репозитория исходящих файлов. Обратите внимание на то, что использовать можно любой свободный порт в пределах 1025-65535.

Номера портов, выбранных для этого примера, перечислены в следующей таблице:

Сервер	Номер порта
Центральный сервер управления	6411

Сервер	Номер порта
Сервер репозитория входящих файлов	6415
Сервер репозитория исходящих файлов	6416

- Отсутствует необходимость настройки диапазона портов для дочерних элементов сервера заданий, поскольку брандмауэр между серверами заданий и серверами баз данных будет настроен для разрешения инициирования обмена данными любым портом.
- Настройте брандмауэр *Firewall_1*, чтобы разрешить обмен данными с назначенными портами на сервере платформы BI, которые были настроены в предыдущем действии. Обратите внимание, что 6400 является номером порта по умолчанию для порта сервера имен CMS, поэтому его не нужно явно настраивать в предыдущем действии.

Порт	Целевой компьютер	Порт	Действие
Любой	boe_2	6400	Разрешить
Любой	boe_2	6411	Разрешить
Любой	boe_2	6415	Разрешить
Любой	boe_2	6416	Разрешить

Настройте брандмауэр *Firewall_2*, чтобы разрешить связь с портом прослушивания сервера баз данных. Сервер CMS (на компьютере **boe_2**) должен иметь доступ к системе CMS, базе данных аудита; серверы заданий (на компьютере **boe_3**) должны иметь доступ к системной базе данных и базе данных аудита. Обратите внимание, что отсутствует необходимость настройки портов для дочерних процессов серверов заданий, поскольку их обмен данными с сервером CMS осуществляется не через брандмауэр.

Исходный компьютер	Порт	Целевой компьютер	Порт	Действие
boe_2	Любой	Базы данных	3306	Разрешить
boe_3	Любой	Базы данных	3306	Разрешить

- В этом брандмауэре не поддерживается NAT, поэтому настраивать файл `hosts` не требуется.

См. также

- [Основные сведения об обмене данными между компонентами платформы BI](#)
- [Настройка платформы BI для брандмауэров](#)

6.17 Настройки брандмауэра для интегрированных сред

В этом разделе описываются особенности конфигурации и настройки портов для развертываний платформ BI, интегрируемых со следующими средами ERP.

- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

В число компонентов платформы BI входят клиенты-браузеры, толстые клиенты, серверы и SDK, размещаемые на сервере веб-приложений. Компоненты системы можно устанавливать на несколько компьютеров. Перед настройкой системы для работы с брандмауэрами следует ознакомиться с описанием основ взаимодействия между платформой BI и компонентами ERP.

Требования, предъявляемые к портам серверов платформы BI

Для соответствующих серверов на платформе BI требуются следующие порты:

Требования к порту сервера
<ul style="list-style-type: none"> • Порт сервера имени сервера центрального управления • Порт запросов Центрального сервера управления • Входной порт для запросов FRS • Выходной порт для запросов FRS • Порт запросов сервера приложений отчетов • Crystal Reports Порт запросов кэш-сервера • Crystal Reports Порт запросов сервера страниц • Crystal Reports Порт запросов сервера обработки

6.17.1 Рекомендации по настройке брандмауэра для интеграции SAP

В развертывании платформы BI должны выполняться следующие правила обмена данными:

- CMS должен иметь возможность инициировать обмен данными с системой SAP через порт шлюза системы SAP.
- Сервер заданий Crystal Reports и Сервер обработки Crystal Reports (наряду с компонентами Data Access) должны быть способны установить связь с системой SAP через порт шлюза системы SAP.

- Компонент BW Publisher должен быть способен установить связь с системой SAP через порт шлюза системы SAP.
- Компоненты платформы BI, развернутые на стороне портала SAP Enterprise (например, iViews и KMC), должны быть способны инициировать обмен данными с веб-приложениями платформы BI через порты HTTP/HTTPS.
- Сервер веб-приложений должен быть в состоянии инициировать обмен данными через порт шлюза системы SAP.
- Приложение Crystal Reports должно иметь возможность установить связь с ведущим узлом SAP через порт шлюза системы SAP и через порт диспетчера системы SAP.

Порт, который прослушивается службой шлюза SAP, совпадает с портом, указанным в установке.

Примечание:

Если для компонента требуется подключение к системе SAP с помощью маршрутизатора SAP, такой компонент можно настроить с помощью строки маршрутизатора SAP. Например, при настройке системы контроля полномочий SAP для импорта ролей и пользователей, строку маршрутизатора SAP можно заменить именем сервера приложений. Это гарантирует, что CMS будет обмениваться данными с системой SAP через SAP-маршрутизатор.

См. также

- [установка локального шлюза SAP](#)

6.17.1.1 Подробное описание требований к настройке портов

Требования, предъявляемые к портам SAP

В платформе BI используется средство подключения SAP Java Connector (SAP JCO) для обмена данными с SAP NetWeaver (ABAP). Необходимо настроить следующие порты и обеспечить их доступность.

- Порт службы шлюза SAP (например, 3300).
- Порт службы диспетчера SAP (например, 3200).

В следующей таблице собраны все требуемые конфигурации определенных портов.

Исходный компьютер	Порт	Целевой компьютер	Порт	Действие
SAP	Любой	Сервер веб-приложений платформы BI	Порт веб службы HTTP/HTTPS	Разрешить
SAP	Любой	CMS	Порт имени сервера CMS	Разрешить
SAP	Любой	CMS	Порт запрошенного CMS	Разрешить
Сервер веб-приложений	Любой	SAP	Порт службы шлюза системы SAP	Разрешить
Центральный сервер управления (CMS)	Любой	SAP	Порт службы шлюза системы SAP	Разрешить
Crystal Reports	Любой	SAP	Порт службы шлюза системы SAP и порт диспетчера системы SAP	Разрешить

6.17.2 Настройка брандмауэра для интеграции с JD Edwards EnterpriseOne

В развертываниях платформы BI, взаимодействующих с ПО JD Edwards, должны выполняться следующие общие требования к взаимодействию:

- Веб-приложения Central Management Console должны иметь возможность подключиться к JD Edwards EnterpriseOne и начать взаимодействие по порту JENET и по произвольно выбираемому порту.
- Crystal Reports с компонентом соединения данных со стороны клиента должен быть способен подключаться к JD Edwards EnterpriseOne по порту JENET. Для получения данных на стороне JD Edwards EnterpriseOne необходимо обеспечить возможность соединения с драйвером через произвольный (не настраиваемый) порт.
- Центральный сервер управления должен быть способен подключаться к JD Edwards EnterpriseOne по порту JENET и по произвольно выбираемому порту.
- Номер порта JENET указан в файле конфигурации сервера приложений JD Edwards EnterpriseOne (JDE.INI), в разделе JENET.

6.17.2.1 Требования, предъявляемые к портам серверов платформы BI

Продукт	Требования к порту сервера
Платформа SAP BusinessObjects Business Intelligence	<ul style="list-style-type: none"> Порт для запросов сервера регистрации BusinessObjects Enterprise

6.17.2.2 Порты, требуемые для JD Edwards EnterpriseOne

Продукт	Необходимые порты	Описание
JD Edwards EnterpriseOne	Порт JENET и произвольно выбираемый порт	Используется для взаимодействия между платформой BI и сервером приложений JD Edwards EnterpriseOne.

6.17.2.3 Настройка сервера веб-приложений для взаимодействия с JD Edwards

В этом разделе показан способ настройки брандмауэра и платформы BI для совместной работы в конфигурации, при которой брандмауэр отделяет сервер веб-приложений от других серверов платформы.

Для получения сведений о настройке работы брандмауэра с серверами и клиентами платформы BI см. раздел *Требования, предъявляемые к портам платформы BI* данного руководства. Помимо стандартной настройки брандмауэра, для доступа к серверам JD Edwards потребуется открыть некоторые дополнительные порты.

Таблица 6-14: Для JD Edwards EnterpriseOne Enterprise

Исходный компьютер	Порт	Целевой компьютер	Порт	Действие
CMS с функцией подключения службы безопасности для JD Edwards EnterpriseOne	Любой	JD Edwards EnterpriseOne	Любой	Разрешить

Исходный компьютер	Порт	Целевой компьютер	Порт	Действие
Сервера платформы BI с возможностью подключения к данным для JD Edwards EnterpriseOne	Любой	JD Edwards EnterpriseOne	Любой	Разрешить
Crystal Reports с функциональностью соединения с данными со стороны клиента для JD Edwards EnterpriseOne	Любой	JD Edwards EnterpriseOne	Любой	Разрешить
Сервер веб-приложений	Любой	JD Edwards EnterpriseOne	Любой	Разрешить

6.17.3 Конкретные рекомендации по настройке брандмауэра для Oracle EBS

В разворачивании платформы BI должно разрешаться подключение к порту прослушивания базы данных Oracle от следующих компонентов.

- Веб-компоненты платформы BI
- CMS (в частности, подключаемый модуль безопасности Oracle EBS)
- Внутренние серверы платформы BI (в частности, компонент доступа к данным EBS)
- Crystal Reports (в частности, компонент доступа к данным EBS)

Примечание:

По умолчанию во всех указанных выше случаях база данных Oracle прослушивает и принимает соединения на порту 1521.

6.17.3.1 Подробное описание требований к настройке портов

Кроме стандартной настройки брандмауэра для платформы BI, для работы с интегрированной средой Oracle EBS необходимо открыть несколько дополнительных портов:

Исходный компьютер	Порт	Целевой компьютер	Порт	Действие
Сервер веб-приложений	Любой	Oracle EBS	Порт базы данных Oracle	Разрешить

Исходный компьютер	Порт	Целевой компьютер	Порт	Действие
CMS с подключением службы безопасности для Oracle EBS	Любой	Oracle EBS	Порт базы данных Oracle	Разрешить
Сервера платформы BI с возможностью подключения к данным на стороне сервера для Oracle EBS	Любой	Oracle EBS	Порт базы данных Oracle	Разрешить
Crystal Reports с функциональностью подключения к данным со стороны клиента для Oracle EBS	Любой	Oracle EBS	Порт базы данных Oracle	Разрешить

6.17.4 Настройка брандмауэра для интеграции с PeopleSoft Enterprise

Развертывания платформы BI для PeopleSoft должны соответствовать следующим общим правилам взаимодействия.

- Центральный сервер управления (CMS) с компонентом "Подключение к системе безопасности" должен иметь возможность инициировать соединения с веб-службой PeopleSoft Query Access (QAS).
- Серверы платформы BI с компонентом "Подключение к данным" должны иметь возможность инициировать соединения с веб-службой PeopleSoft QAS.
- Crystal Reports с компонентом "Соединение с данными" на стороне клиента должен иметь возможность инициировать соединения с веб-службой PeopleSoft QAS.
- Мост управления предприятием (EPM) должен иметь возможность подключения к CMS и к серверу репозитория входных файлов.
- Мост EPM должен иметь возможность подключения к базе данных PeopleSoft с помощью соединения ODBC.

Номер порта веб-службы соответствует указанному в имени домена PeopleSoft Enterprise.

6.17.4.1 Требования, предъявляемые к портам серверов платформы BI

Продукт	Требования к порту сервера
Платформа SAP BusinessObjects Business Intelligence	<ul style="list-style-type: none"> Порт для запросов сервера регистрации BusinessObjects Enterprise

6.17.4.2 Необходимые порты для PeopleSoft

Продукт	Необходимые порты	Описание
PeopleSoft Enterprise: People Tools 8.46 или более новой версии	Порт HTTP/HTTPS веб-службы	Этот порт требуется при использовании соединения SOAP с PeopleSoft Enterprise для People Tools 8.46 и более новых версий.

6.17.4.3 Настройка платформы BI и PeopleSoft для брандмауэров

В этом разделе показан способ настройки брандмауэра и платформы BI для совместной работы в конфигурации, при которой брандмауэр отделяет сервер веб-приложений от других серверов платформы BI.

Описание настройки брандмауэра для работы с серверами и клиентами платформы BI см. в *Руководстве администратора платформы SAP BusinessObjects Business Intelligence*.

Помимо настройки брандмауэра для платформы BI требуется также ряд дополнительных настроек.

Таблица 6-18: Для PeopleSoft Enterprise: PeopleTools 8.46 или более новой версии

Исходный компьютер	Порт	Целевой компьютер	Порт	Действие
CMS с функцией "Подключение к системе безопасности" для PeopleSoft	Любой	PeopleSoft	Порт PeopleSoft для веб-служб HTTP/HTTPS	Разрешить

Исходный компьютер	Порт	Целевой компьютер	Порт	Действие
Серверы платформы BI с функцией "Подключение к данным" для PeopleSoft	Любой	PeopleSoft	Порт PeopleSoft для веб служб HTTP/HTTPS	Разрешить
CrystalReports с компонентом "Подключение к данным" на стороне клиента для PeopleSoft	Любой	PeopleSoft	Порт PeopleSoft для веб служб HTTP/HTTPS	Разрешить
Мост EPM	Любой	CMS	Порт сервера имен CMS	Разрешить
Мост EPM	Любой	CMS	Запрошенный порт CMS	Разрешить
Мост EPM	Любой	Сервер репозитория входящих файлов	Входной порт FRS	Разрешить
Мост EPM	Любой	PeopleSoft	Порт базы данных PeopleSoft	Разрешить

6.17.5 Настройка брандмауэра для интеграции с Siebel

В этом разделе приводятся конкретные порты, используемые для обмена данными между платформой BI и системами Siebel eBusiness Application при настройке работы через брандмауэры.

- Веб-приложение должно иметь возможность инициировать соединения с сервером регистрации платформы BI для Siebel. Для сервера регистрации для Siebel необходимы три порта:
 1. Порт эха (TCP) 7 для проверки доступности сервера регистрации.
 2. Порт сервера регистрации платформы BI для Siebel (по умолчанию – 8448) для порта прослушивания CORBA IOR.
 3. Произвольный порт POA для взаимодействия CORBA, который нельзя выбрать, поэтому должны быть открыты все порты.
- Центральный сервер управления (CMS) должен иметь возможность инициировать соединения с сервером регистрации платформы BI для Siebel. Порт прослушивания CORBA IOR, настроенный для каждого сервера регистрации (например, порт 8448). Также будет необходимо открыть порт POA со случайным номером, который станет известен только после установки платформы BI.
- Сервер регистрации платформы BI для Siebel должен иметь возможность инициировать подключения к порту SCBroker (брокера соединений Siebel), например к порту 2321.

- Внутренние серверы платформы BI (компонент доступа к данным Siebel) должны иметь возможность инициировать подключения к порту SCBroker (брокера соединений Siebel), например к порту 2321.
- Crystal Reports (компонент доступа к данным Siebel) должен иметь возможность инициировать подключения к порту SCBroker (брокера соединений Siebel), например к порту 2321.

Подробное описание портов

В этом разделе перечислены порты, используемые платформой BI. В случае развертывания платформы BI при наличии брандмауэров можно воспользоваться этой информацией, чтобы открыть в этих брандмауэрах необходимый минимум портов, используемых для интеграции с Siebel.

Таблица 6-19: Требования, предъявляемые к портам серверов платформы BI

Продукт	Требования к порту сервера
Платформа SAP BusinessObjects Business Intelligence	<ul style="list-style-type: none"> • Порт для запросов сервера регистрации BusinessObjects Enterprise

Таблица 6-20: Необходимые порты для Siebel

Продукт	Необходимые порты	Описание
Приложение Siebel eBusiness	2321	Порт SCBroker (брокера соединений Siebel) по умолчанию

Настройка брандмауэров платформы BI для интеграции с Siebel

В этом разделе показан способ настройки брандмауэра для Siebel и платформы BI для совместной работы в конфигурации, в которой брандмауэр отделяет сервер веб-приложений от других серверов платформы.

Исходный компьютер	Порт	Целевой компьютер	Порт	Действие
Сервер веб-приложений	Любой	Платформа BI – сервер регистрации Siebel	Любой	Разрешить
CMS	Любой	Платформа BI – сервер регистрации Siebel	Любой	Разрешить
Платформа BI – сервер регистрации Siebel	Любой	Siebel	Порт SCBroker	Разрешить

Исходный компьютер	Порт	Целевой компьютер	Порт	Действие
Серверы платформы BI с возможностью подключения к данным со стороны сервера Siebel	Любой	Siebel	Порт SCBroker	Разрешить
CrystalReports с функциональностью подключения к данным на стороне клиента для Siebel	Любой	Siebel	Порт SCBroker	Разрешить

6.18 Платформа BI и обратные прокси-серверы

Платформу BI можно развернуть в среде с одним или несколькими обратными прокси-серверами. Обратный прокси-сервер, как правило, развертывается перед серверами веб-приложений, чтобы скрыть их за одним IP-адресом. При данной конфигурации весь Интернет-трафик, адресованный частным серверам веб-приложений, направляется через обратный прокси-сервер, скрывая частные IP-адреса.

Так как обратный прокси-сервер преобразует публичные URL-адреса во внутренние, его конфигурация должна включать URL-адреса веб-приложений платформы BI, развернутых во внутренней сети.

6.18.1 Поддерживаемые обратные прокси-серверы

Платформа BI поддерживает следующие обратные прокси-серверы:

- IBM Tivoli Access Manager WebSEAL 6
- Apache 2.2
- Microsoft ISA 2006

6.18.2 Понимание механизма развертывания веб-приложений

Веб-приложения платформы BI развертываются на сервере веб-приложений. При установке с помощью средства WDeploy развертывание приложений выполняется автоматически. С его

помощью также можно развернуть приложение вручную после развертывания платформы BI. Веб-приложения расположены в следующем каталоге установки по умолчанию для Windows:

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise  
XI 4.0\warfiles\webapps
```

WDeploy используется для развертывания двух определенных WAR-файлов:

- **BOE:** включает консоль централизованного управления (CMC), стартовую панель BI, Open Document,
- **dswsbobje:** содержит приложение веб-службы

Если сервер веб-приложений находится за обратным прокси-сервером, то в конфигурации обратного прокси-сервера следует указать контекстные пути к WAR-файлам. Чтобы воспользоваться всеми функциональными возможностями BusinessObjects Enterprise, настройте контекстный путь для каждого установленного WAR-файла платформы BI.

6.19 Настройка обратных прокси-серверов для веб-приложений платформы BI

Обратный прокси-сервер должен быть настроен так, чтобы соотносить входящие запросы URL с правильным веб-приложением, когда веб-приложения платформы BI развернуты за обратным прокси-сервером.

В данном разделе содержатся конкретные примеры настройки некоторых поддерживаемых обратных прокси-серверов. Для получения дополнительных сведений см. документацию поставщика по обратному прокси-серверу.

6.19.1 Подробные инструкции по настройке обратных прокси-серверов

Настройка WAR-файлов

Веб-приложения платформы BI развертываются как WAR-файлы на сервере веб-приложений. Обязательно задайте директиву на обратном прокси-сервере для каждого WAR-файла, который требуется для развертывания. Можно воспользоваться WDeploy для развертывания WAR-файл BOE или dswsbobje. Для получения дополнительных сведений о WDeploy см. *Руководство по развертыванию веб-приложений для платформы BI*.

Укажите свойства BOE в каталоге настраиваемой конфигурации

WAR-файл BOE содержит глобальные свойства и свойства конкретного приложения. Если необходимо изменить какие-либо из этих свойств, используйте настраиваемый каталог конфигурации. По умолчанию каталог располагается здесь: `C:\Program Files (x86)\SAP`

```
BusinessObjects\SAP BusinessObjects Enterprise XI  
4.0\warfiles\webapps\BOE\WEB-INF\config\custom.
```

Не изменяйте свойства в каталоге config/default.

Примечание:

На некоторых серверах веб-приложений, например в версии Tomcat, поставляемой с платформой BI, возможен прямой доступ к BOE.war. В таком случае можно задать пользовательские настройки напрямую, без отмены развертывания WAR-файла. При отсутствии доступа к WAR-файлу BOE необходимо отменить развертывание файла, настроить файл и развернуть его повторно.

Единообразное использование символа '/'

Задайте контекстные пути в обратном прокси-сервере таким же образом, как они вводятся в URL-адресе в браузере. Например, если директива содержит символ "/" в конце пути зеркала на обратном прокси-сервере, введите этот символ в конце URL-адреса в браузере.

Используйте символ "/" последовательно в URL-адресе источника и адресата в директиве обратного прокси-сервера. Если символ "/" вставляется в конце URL-адреса источника, он также должен быть вставлен в конце URL-адреса адресата.

6.19.2 Настройка обратного прокси-сервера

Перечисленные ниже действия необходимы, чтобы обеспечить работу веб-приложений платформы BI под защитой поддерживаемого обратного прокси-сервера.

1. Убедитесь, что обратный прокси-сервер установлен в соответствии с инструкциями поставщика и топологией сети развертывания.
2. Определите необходимый WAR-файл для платформы BI
3. Настройте обратный прокси-сервер для каждого WAR-файла платформы BI. Обратите внимание на то, что для каждого типа обратного прокси-сервера правила устанавливаются по-разному.
4. Выполните необходимую настройку. Некоторые веб-приложения при развертывании на определенных серверах веб-приложений требуют специальной настройки.

6.19.3 Настройка обратного прокси-сервера Apache 2.2 для платформы BI

В этом разделе представлен рабочий процесс по настройке платформы BI для совместной работы с веб-сервером Apache 2.2.

1. Платформа BI и Apache 2.2 должны быть установлены на разных компьютерах.
2. Apache 2.2 должен быть установлен и настроен как обратный прокси-сервер в соответствии с документацией поставщика.

3. Настройте `ProxyPass` для каждого WAR-файла, развернутого за обратным прокси-сервером.
4. Настройте `ProxyPassReverseCookiePath` для каждого веб-приложения, развернутого за обратным прокси-сервером.

6.19.4 Настройка обратного прокси-сервера WebSEAL 6.0 для платформы BI

В данном разделе рассматривается настройка платформы BI и WebSEAL 6.0 для совместной работы.

Рекомендуется создать одно стандартное соединение для отображения всех веб-приложений платформы BI, размещенных на внутреннем сервере веб-приложений или веб-сервере, в одной точке установки.

1. Убедитесь, что платформа BI и WebSEAL 6.0 расположены на разных компьютерах.
Развертывание платформы BI и WebSEAL 6.0 на одном компьютере допускается, но не рекомендуется. Инструкции по настройке такого развертывания см. в документации поставщика по WebSEAL 6.0.
2. Убедитесь, что выполнена установка и настройка WebSEAL 6.0 в соответствии с документацией поставщика.
3. Запустите утилиту **pdadmin** командной строки WebSeal. Войдите в безопасный домен, такой как **sec_master**, через учетную запись пользователя с правами администратора.
4. Введите следующую команду в приглашении **pdadmin sec_master**:

```
server task <instance_name-webseald-host_name>create -t  
<type> -h <host_name> -p <port> <junction_point>
```

Где:

- `<instance_name-webseald-host_name>` указывает полное имя сервера установленного экземпляра WebSEAL. Используйте это полное имя сервера в формате, в котором оно отображено в исходящих данных команды `server list`.
- `<type>` указывает тип соединения. Используйте `tcp`, если соединение ведет на внутренний HTTP порт. Используйте `ssl`, если соединение ведет на внутренний порт HTTPS.
- `<host_name>` указывает имя хоста DNS или IP-адрес внутреннего сервера, который будет получать запросы.
- `<port>` указывает TCP порт внутреннего сервера, который будет получать запросы.
- `<junction_point>` указывает каталог в пространстве объекта, защищенном WebSEAL, в котором установлено пространство документов внутреннего сервера.

Пример:

```
server task default-webseald-webseal.rp.sap.com  
create -t tcp -h 10.50.130.123 -p 8080/hr
```

6.19.5 Настройка Microsoft ISA 2006 для платформы BI

В данном разделе рассматривается настройка платформы BI и ISA 2006 для совместной работы.

Рекомендуется создать одно стандартное соединение для отображения всех WAR- файлов платформы BI, размещенных на внутреннем сервере веб-приложений или веб-сервере, в одну точку монтирования. Сервер веб-приложений необходимо дополнительно настраивать для обеспечения успешной совместной работы с ISA 2006. Требуемые настройки зависят от типа сервера.

1. Убедитесь, что платформа BI и ISA 2006 расположены на разных компьютерах.
Развертывание платформы BI и ISA 2006 на одном компьютере допускается, но не рекомендуется. Инструкции по конфигурации такого развертывания см. в документации по ISA 2006.
2. ISA 2006 необходимо установить и настроить в соответствии с документацией поставщика.
3. Запустите служебную программу управления сервером ISA Server Management.
4. С помощью навигационной панели запустите новое правило публикации.

- a. Перейдите по следующим пунктам меню:

Массивы > Имя компьютера > Политика брандмауэра > Создать > Правило публикации веб-узла

Помните:

Пункт **Имя компьютера** необходимо заменить на имя компьютера, на котором размещается ISA 2006.

- b. Введите имя правила в поле **Имя правила веб-публикации** и нажмите **Далее**.
- c. Выберите **Разрешить** в качестве действия правила и нажмите **Далее**.
- d. Выберите **Публикация одного веб-узла или средства равномерного распределения нагрузки** в качестве типа публикации и нажмите **Далее**.
- e. Выберите тип соединения между сервером ISA и публикуемым веб-узлом и нажмите **Далее**.
Например, выберите **Использовать незащищенные соединения для подключения публикуемой фермы веб-серверов или серверов**.
- f. Введите внутреннее имя публикуемого веб-сайта (например, имя компьютера, на котором размещена платформа BI) в поле **Внутреннее имя сайта** и нажмите кнопку **Далее**.

Примечание:

Если хост ISA 2006 невозможно подключить к целевому серверу, выберите **Использовать имя или IP-адрес компьютера для подключения к публикуемому серверу** и введите имя или IP-адрес в соответствующие поля.

- g. В разделе «Сведения об общедоступном имени» выберите имя домена (например, **Любое имя домена**) и задайте любые сведения о внутренней публикации (например, /*). Нажмите **Далее**.

Теперь необходимо создать новое веб-средство прослушивания для отслеживания входящих веб-запросов.

5. Нажмите **Создать**, чтобы запустить мастер определения нового веб-средства прослушивания.
- Введите имя в поле **Имя веб-средства прослушивания** и нажмите **Далее**.
 - Выберите тип соединения между сервером ISA и публикуемым веб-узлом и нажмите **Далее**.
Например, выберите **SSL-подключение к клиентам не требуется**.
 - В разделе «IP-адреса веб-средства прослушивания» выберите следующие значения и нажмите кнопку **Далее**.
 - Внутренний
 - Внешний
 - Локальный хост
 - Все сетиТеперь сервер ISA настроен для публикации только через HTTP.
 - Выберите параметр «Настройка аутентификации» и нажмите кнопку **Далее**, а затем кнопку **Готово**.
Теперь новое средство прослушивания настроено в соответствии с правилом веб-публикации.
6. Нажмите кнопку **Далее** в разделе «Объединения пользователей», а затем нажмите кнопку **Готово**.
7. Нажмите кнопку **Применить**, чтобы сохранить все настройки правила веб-публикации и обновить конфигурацию ISA 2006.
Теперь необходимо обновить свойства правила веб-публикации для сопоставления путей к веб-приложениям.
8. На навигационной панели щелкните правой кнопкой мыши настроенную политику брандмауэра и выберите **Свойства**.
9. На вкладке «Пути» нажмите кнопку **Добавить**, чтобы сопоставить маршруты веб-приложениям SAP BusinessObjects.
10. На вкладке «Общее имя» выберите параметр **Запрос для следующих веб-узлов** и нажмите кнопку **Добавить**.
11. В диалоговом окне «Общедоступное имя» введите имя сервера ISA 2006 и нажмите кнопку **ОК**.
12. Нажмите кнопку **Применить**, чтобы сохранить все настройки правила веб-публикации и обновить конфигурацию ISA 2006.
13. Проверьте наличие подключения. Для этого попробуйте перейти по следующему URL-адресу:
`http://<Имя хоста сервера ISA>:<номер порта веб-средства прослушивания>/<Внешний путь к приложению>`
Например: `http://myISAServer:80/Product/BOE/CMC`

Примечание:

Возможно, окно веб-браузера придется обновлять несколько раз.

Необходимо изменить политику HTTP по отношению к правилу, которое вы только что настроили, чтобы гарантировать возможность входа в консоль СМС. Правой кнопкой мыши щелкните на правиле, созданном с помощью служебной программы ISA Server Management, и выберите **Настроить HTTP**. Снимите флажок **Проверять нормализацию** в области «Защита URL-адреса».

Для удаленного доступа к платформе BI необходимо создать правило доступа.

6.20 Специальная настройка для платформы BI при развертывании с обратным прокси-сервером

Некоторые продукты платформы BI требуют дополнительной настройки для правильной работы в развертываниях на обратном прокси-сервере. В данном разделе рассматриваются такие дополнительные настройки.

6.20.1 Включение обратного прокси-сервера для веб-служб

В этом разделе описаны процедуры, необходимые для включения обратных прокси-серверов для веб-служб.

6.20.1.1 Включение обратного прокси на сервере Tomcat 6

Для включения обратного прокси-сервера на сервере веб-приложений Tomcat, необходимо изменить файл `server.xml`. Среди необходимых изменений необходимо выполнить настройку параметра `proxyPort` в качестве порта прослушивания обратного прокси-сервера и добавление параметра `proxyName`. В этом разделе приводится описание процедуры.

1. Остановите сервер Tomcat.
2. Откройте файл `server.xml` для сервера Tomcat.

В Windows файл `server.xml` расположен в каталоге `C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\conf`

В UNIX файл `server.xml` расположен в каталоге `<CATALINA_HOME>/conf`. Значением по умолчанию для `<CATALINA_HOME>` является `<КАТАЛОГ_УСТАНОВКИ>/boobje/tomcat55`

3. Найдите этот раздел в файле `server.xml`:

```
<!-- 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. Удалите комментарии элемента соединителя путем удаления символов `<!--` и `-->`.
5. Измените значение параметра `proxyPort`, чтобы он соответствовал порту прослушивания обратного прокси-сервера.
6. Добавьте новый атрибут `proxyName` в список атрибутов соединителя. Значению атрибута `proxyName` должно соответствовать имя прокси-сервера, которое должно разрешаться правильным IP-адресом на сервере Tomcat.

Пример:

```
<!--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" />
```

Значения `мой_обратный_прокси_сервер.domain.com` и `ReverseProxyServerPort` следует заменить подходящими значениями имени обратного прокси-сервера и его порта прослушивания.

7. Сохраните и закройте файл `server.xml`.
8. Перезапустите сервер Tomcat.
9. Убедитесь, что обратный прокси-сервер сопоставляет свой виртуальный путь подходящему порту соединителя Tomcat. В примере выше используется порт 8082.

В следующем примере показана примерная конфигурация для HTTP-сервера Apache 2.2 для веб-служб SAP Business Objects обратного прокси-сервера при развертывании на сервере Tomcat:

```
ProxyPass /XI3.0/dswsbobje http://internalServer:8082/dswsbobje
ProxyPassReverseCookiePath /dswsbobje /XI3.0/dswsbobje
```

Для того чтобы активировать веб-службы, необходимо определить имя прокси и номер порта соединителя.

6.20.1.2 Включение обратного прокси-сервера для веб-служб на серверах веб-приложений, за исключением Tomcat

Для выполнения следующей процедуры необходимо, чтобы веб-приложения платформы BI были правильно настроены на выбранном сервере веб-приложений. Обратите внимание, что строка `wsresources` зависит от регистра.

1. Остановите сервер веб-приложений.
2. Укажите внешний URL веб-служб в файле `dsws.properties`.

Этот файл находится в веб-приложении dswsbobje. Например, если в качестве внешнего URL-адреса используется `http://my_reverse_proxy_server.domain.com/XI/dswsbobje/`, обновите следующие свойства в файле `dsws.properties`:

- `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. Сохраните и закройте файл `dsws.properties`.

4. Перезапустите сервер веб-приложений.

5. Убедитесь, что обратный прокси-сервер сопоставляет свой виртуальный путь подходящему порту соединителя сервера веб-приложений. В следующем примере показана примерная конфигурация HTTP-сервера Apache 2.2 для веб-служб SAP BusinessObjects обратного прокси-сервера, развернутых на выбранном сервере веб-приложений:

```
ProxyPass /SAP/dswsbobje http://внутреннийСервер:<порт прослушивания>/dswsbobje
```

```
ProxyPassReverseCookiePath /dswsbobje /SAP/dswsbobje
```

Где <порт прослушивания> – порт прослушивания сервера веб-приложений.

6.20.2 Включение пути к корневому каталогу для файлов cookie сеанса для ISA 2006

В этом разделе описан способ настройки определенных серверов веб-приложений для включения использования пути к корневому каталогу для файлов cookie сеанса при использовании ISA 2006 в качестве обратного прокси-сервера.

6.20.2.1 Настройка Apache Tomcat 6

Чтобы настроить путь к корневому каталогу для использования файлов cookie сеанса с сервером ISA 2006 в качестве обратного прокси-сервера, добавьте следующий элемент `<Connector>` в файл `server.xml`:

```
emptySessionPath="true"
```

1. Остановите сервер Tomcat
2. Откройте файл `server.xml`, расположенный в каталоге:

```
<CATALINA_HOME>\conf
```

3. Найдите следующий раздел в файле `server.xml`:

```
<!-- 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. Удалите комментарии элемента соединителя путем удаления символов `<!--` и `-->`.
5. Чтобы настроить путь к корневому каталогу для использования файлов cookie сеанса с сервером ISA 2006 в качестве обратного прокси-сервера, добавьте следующий элемент `<Connector>` в файл `server.xml`:

```
emptySessionPath="true"
```

6. Измените значение параметра `proxyPort`, чтобы он соответствовал порту прослушивания обратного прокси-сервера.
7. Добавьте новый атрибут `proxyName` в список атрибутов соединителя. В качестве значения необходимо использовать имя прокси-сервера, которое должно разрешаться правильным IP-адресом на сервере Tomcat.

Например:

```
<!--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. Сохраните и закройте файл `server.xml`.
9. Перезапустите сервер Tomcat.

Убедитесь, что обратный прокси-сервер сопоставляет свой виртуальный путь подходящему порту соединителя Tomcat. В примере выше используется порт 8082.

6.20.2.2 Настройка Sun Java 8.2

Необходимо изменить файл `sun-web.xml` для каждого веб-приложения платформы BI.

1. Перейдите в каталог `<SUN_WEBAPP_DOMAIN>\generated\xml\j2ee-modules\webapps\BOE\WEB-INF`
2. Откройте файл `sun-web.xml`
3. После контейнера `<context-root>` добавьте следующее:

```
<session-config>
  <cookie-properties>
    <property name="cookiePath" value="/" />
  </cookie-properties>
</session-config>
<property name="reuseSessionID" value="true"/>
```

4. Сохраните и закройте файл `sun-web.xml`.
5. Повторите действия с 1 по 4 для каждого веб-приложения.

6.20.2.3 Настройка сервера приложений Oracle 10gR3

Необходимо изменить файл `global-web-application.xml` или `orion-web.xml` для каждого каталога развертывания веб-приложений платформы BI.

1. Перейдите в каталог `<ORACLE_HOME>\j2ee\home\config\`
2. Откройте файл `global-web-application.xml` или `orion-web.xml`.
3. Добавьте следующую строку в контейнер `<orion-web-app>`:

```
<session-tracking cookie-path="/" />
```

4. Сохраните и закройте конфигурационный файл.
5. Выполните вход в консоль администрирования Oracle:
 - a. Перейдите к пункту **OC4J:home > Администрирование > Свойства сервера**.
 - b. Выберите **Параметры** в разделе «Параметры командной строки».
 - c. Выберите **Добавить строку** и введите следующее:

```
Doracle.useSessionIDFromCookie=true
```

6. Перезапустите сервер Oracle.

6.20.2.4 Настройка WebSphere Community Edition 2.0

1. Откройте консоль администрирования WebSphere Community Edition 2.0.
2. На левой панели навигации найдите пункт «Сервер» и выберите **Веб-сервер**.
3. Выберите соединители, затем выберите **Изменить**.
4. Установите флажок **emptySessionPath** и нажмите кнопку **Сохранить**.
5. Введите имя сервера ISA в поле **ProxyName**.
6. Введите номер порта прослушивания ISA в поле **ProxyPort**.
7. Остановите и перезапустите соединитель.

6.20.3 Включение обратного прокси-сервера для приложения SAP BusinessObjects Live Office

Чтобы включить функцию объекта просмотра SAP BusinessObjects Live Office в веб-браузере для обратных прокси-серверов, настройте URL-адрес средства просмотра по умолчанию. Это можно сделать с помощью Central Management Console (CMC) или параметров Live Office.

Примечание:

В этом разделе подразумевается, что обратные прокси-серверы для стартовой панели BI и веб-службы платформы BI успешно включены.

6.20.3.1 Настройка URL средства просмотра по умолчанию с использованием CMC

1. Выполните вход в CMC.
2. Перейдите на страницу программных приложений и выберите **CMC**.
3. Выберите **Расширения обработки** в меню **Действия**.
4. В поле URL задайте правильный URL средства просмотра по умолчанию и выберите **Задать URL**. Например:

```
http://ОбратныйПроксиСервер:ПортОбратногоПроксиСервера/BOE/OpenDocument.jsp?sIDType=CUID&iDocID=%SI_CUID%
```

Здесь `ОбратныйПроксиСервер` и `ПортОбратногоПроксиСервера` – это правильные имя обратного прокси сервера и его порт прослушивания.

Аутентификация

7.1 Параметры аутентификации платформы BI

Аутентификация представляет собой процесс проверки удостоверения пользователя, пытающегося получить доступ к системе, тогда как авторизация – это процесс проверки того, что пользователь имеет достаточно прав для выполнения запрошенного действия с заданным объектом.

Подключаемые модули безопасности расширяют способы аутентификации пользователей платформы BI. Подключаемые модули безопасности автоматизируют создание учетных записей и управление ими, позволяя сопоставлять учетные записи пользователей и групп из систем сторонних производителей с платформой BI. Учетные записи и группы из систем сторонних производителей можно сопоставлять существующим учетным записям и группам платформы BI, а также можно создавать учетные записи пользователей и группы Enterprise, которые соответствуют каждой из сопоставляемых записей внешней системы.

В настоящей версии поддерживаются следующие методы аутентификации:

- Enterprise
- LDAP
- Windows AD
- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

Поскольку платформа BI является полностью настраиваемой системой, процессы аутентификации в разных системах могут отличаться.

См. также

- [Включение аутентификации JD Edwards EnterpriseOne](#)
- [Разрешение аутентификации Oracle EBS](#)
- [Включение аутентификации PeopleSoft Enterprise](#)
- [Включение аутентификации Siebel](#)

7.1.1 Основная аутентификация

Основная аутентификация происходит при первой попытке пользователя получить доступ к системе. Во время основной аутентификации возможны две ситуации.

- Если единый вход не настроен, пользователь указывает свои учетные данные, в том числе имя пользователя, пароль и тип аутентификации.

Эти сведения вводятся пользователями на экране входа в систему.

- Если настроен метод единого входа, учетные данные пользователя заполняются автоматически.

Эти сведения извлекаются с помощью других методов, например, Kerberos или SiteMinder.

- Тип аутентификации может быть Enterprise, LDAP, Windows AD, SAP, Oracle EBS, Siebel, JD Edwards EnterpriseOne, PeopleSoft Enterprise, в зависимости от типов, которые были активированы и установлены в области управления аутентификацией Central Management Console (CMC). Веб-браузер пользователя отправляет информацию по протоколу HTTP на веб-сервер пользователя, который направляет информацию центральному серверу управления или соответствующему серверу платформы.

Сервер веб-приложений передает данные пользователя в сценарий серверной стороны. Этот сценарий взаимодействует с SDK и, в конечном счете, с соответствующим подключаемым модулем безопасности для аутентификации пользователя по базе данных пользователей.

Например, если пользователь входит в стартовую панель BI и выбирает аутентификацию Enterprise, пакет SDK обеспечивает выполнение аутентификации подключаемым модулем безопасности платформы BI. Центральный сервер управления (CMS) использует подключаемый модуль безопасности для проверки имени и пароля пользователя по системной базе данных. Если пользователь указывает метод аутентификации, комплект SDK использует для аутентификации пользователя соответствующий подключаемый модуль безопасности.

Если модуль безопасности подтверждает совпадение учетных данных, CMS назначает пользователю активный системный идентификатор, и выполняются следующие действия:

- Центральный сервер управления (CMS) создает для пользователя сеанс enterprise. Пока сеанс активен, он занимает одну пользовательскую лицензию в системе.
- CMS создает и шифрует маркер входа и отправляет его на сервер веб-приложений.
- Сервер веб-приложений сохраняет информацию пользователя в памяти в переменной сеанса. Активный сеанс хранит сведения, которые позволяют платформе BI отвечать на запросы пользователя.

Примечание:

Переменная сеанса не сохраняет пароль пользователя.

- Сервер веб-приложений хранит маркер входа в файле cookie в браузере клиента. Он используется только для восстановления после сбоя, например, при наличии кластеризованного CMS или когда стартовая панель BI кластеризована, для обеспечения соответствия сеансов.

Примечание:

Маркер входа можно блокировать, однако при этом также будет заблокирована функция восстановления после сбоя.

7.1.2 Подключаемые модули безопасности

Подключаемые модули безопасности расширяют способы аутентификации пользователей платформы BI. В данный момент платформа BI поставляется со следующими подключаемыми модулями:

- Enterprise
- LDAP
- Windows AD
- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

Подключаемые модули защиты автоматизируют создание учетных записей и управление ими, позволяя сопоставлять учетные записи пользователей и группы из систем сторонних производителей с платформой BI. Учетные записи и группы из систем сторонних производителей можно сопоставлять существующим учетным записям и группам платформы BI, а также можно создавать учетные записи пользователей и группы Enterprise, которые соответствуют каждой из сопоставляемых записей внешней системы.

Подключаемые модули безопасности автоматически управляют списками пользователей и групп в системах сторонних производителей. После сопоставления внешней группы платформе BI все пользователи, относящиеся к этой группе, смогут успешно выполнить вход в платформу BI. При последующих изменениях участников сторонних групп нет необходимости обновлять списки в платформе BI. Например, при сопоставлении группы LDAP платформе BI и последующем добавлении нового пользователя в группу подключаемый модуль безопасности автоматически создает псевдоним для этого нового пользователя при его первом входе в платформу BI с указанием действительных учетных данных LDAP.

Кроме того, подключаемые модули безопасности позволяют согласованно назначать права пользователям и группам, поскольку отображенные пользователи и группы обрабатываются как учетные записи Enterprise. Например, можно отобразить некоторые учетные записи или группы пользователей из Windows AD, а некоторые – из сервера каталогов LDAP. Затем, когда появляется необходимость назначить права или создать новые пользовательские группы в платформе BI, все настройки выполняются в консоли CMC.

Каждый подключаемый модуль безопасности действует как провайдер аутентификации, проверяющий учетные данные пользователя по соответствующей базе данных пользователей. При входе в платформу BI пользователи выбирают тип аутентификации из списка типов, которые были включены и настроены в области управления авторизацией в СМС.

Примечание:

Подключаемый модуль безопасности Windows AD не может выполнять аутентификацию пользователей, если компоненты сервера платформы BI выполняются под управлением ОС UNIX.

7.1.3 Единый вход на платформу BI

Единый вход на платформу BI означает, что после входа пользователей в операционную систему они получают доступ к приложениям, поддерживающим эту возможность, без повторного ввода учетных данных. При входе в систему для пользователя создается контекст безопасности. Этот контекст может быть передан в платформу BI для выполнения единого входа, в результате чего пользователь регистрируется как соответствующий пользователь BOE.

Термин «анонимный единый вход» также относится к функциональной возможности единой регистрации в платформе BI, но с учетной записью гостя. Если учетная запись гостя включена (по умолчанию), любое лицо может зарегистрироваться в платформе BI как гость и получить доступ к системе.

7.1.3.1 Поддержка единого входа

Термин "единый вход" используется для описания различных сценариев. На самом базовом уровне он относится к ситуациям, в которых пользователь имеет доступ к нескольким приложениям или системам, указывая свои учетные данные только один раз, что упрощает взаимодействие пользователей с системой.

Единый вход в стартовую панель BI может обеспечиваться платформой BI или другими средствами аутентификации в зависимости от типа используемого сервера приложений и операционной системы.

Следующие методы единого входа доступны при использовании сервера приложений Java в операционной системе Windows:

- Windows AD с Kerberos
- Windows AD с SiteMinder

Следующие методы единого входа доступны при использовании IIS в операционной системе Windows:

- Windows AD с Kerberos
- Windows AD с NTLM.
- Windows AD с SiteMinder

Эти методы поддержки единого входа доступны в ОС Windows или Unix с любым поддерживаемым для платформы сервером веб-приложений.

- LDAP с SiteMinder
- Доверительная аутентификация
- Windows AD с Kerberos

Примечание:

Windows AD с Kerberos поддерживается для приложений Java под управлением ОС UNIX. Однако службы платформы BI должны запускаться на сервере с ОС Windows.

В следующей таблице описываются методы поддержки единого входа в систему для стартовой панели BI.

Режим аутентификации	Сервер CMS	Параметры	Примечания
Windows AD	Только Windows	Только Windows AD с Kerberos	Аутентификация Windows AD для стартовой панели BI и CMS встроена в продукт и доступна сразу после установки.
LDAP	Любая поддерживаемая платформа	Поддерживаемые серверы каталогов LDAP только с SiteMinder	Аутентификация LDAP для стартовой панели BI и CMS встроена в продукт и доступна сразу после установки. Единый вход для InfoView и CMS требует SiteMinder.
Enterprise	Любая поддерживаемая платформа	Доверительная аутентификация	Аутентификация Enterprise для стартовой панели BI и CMS встроена в продукт и доступна сразу после установки. Единый вход с аутентификацией enterprise для InfoView и CMS требует доверительной аутентификации.

- [Единый вход на платформу BI](#)
- [Единый вход в базу данных](#)
- [Сквозной единый вход](#)

7.1.3.2 Единый вход в базу данных

После входа пользователей в платформу BI единый вход в базу данных позволяет им выполнять действия, требующие доступа к базе данных, в частности просмотр и обновление отчетов, без повторного ввода учетных сведений. Единый вход в базу данных может сочетаться с единым входом в платформу BI для упрощения доступа пользователей к необходимым ресурсам.

7.1.3.3 Сквозной единый вход

Сквозной единый вход означает такую конфигурацию, в которой у пользователей есть доступ с единым входом к платформе BI как на клиентской стороне, так и к серверным компонентам баз данных. Таким образом, чтобы получить доступ к платформе BI и иметь возможность выполнять действия, требующие доступа к базе данных (например, просмотр отчетов), пользователи должны вводить свои учетные данные для входа только один раз при входе в операционную систему.

На платформе BI сквозной единый вход поддерживается через Windows AD с использованием Kerberos.

7.2 Аутентификация Enterprise

7.2.1 Общая информация об аутентификации Enterprise

Аутентификация Enterprise является методом аутентификации, используемым в платформе BI по умолчанию. Она автоматически включается при первоначальной установке системы и не может быть отключена. При добавлении пользователей и групп и управлении ими платформа BI обновляет соответствующие сведения о них в базе данных.

Совет:

Аутентификация по умолчанию (Enterprise) используется в том случае, если нужно создать отдельные учетные записи и группы для использования в платформе BI или если иерархия пользователей и групп еще не настроена в стороннем сервере каталогов.

Настраивать или включать аутентификацию Enterprise не нужно. Однако параметры аутентификации Enterprise можно изменить в соответствии с конкретными требованиями организации к безопасности. Изменить параметры Enterprise можно только через Central Management Console (CMC).

7.2.2 Настройки аутентификации Enterprise

Настройки	Параметры	Описание
Ограничения для пароля		
	Принудительно устанавливать пароли с символами в разных регистрах	Этот параметр гарантирует, что пароль содержит по крайней мере два типа символов: буквы в верхнем регистре, буквы в нижнем регистре, цифры или знаки пунктуации.
	Должен содержать не менее N символов	Требования к минимальной сложности пароля понижают вероятность простого угадывания злоумышленником действительного пароля пользователя.
Ограничения для пользователя		
	Должен изменять пароль каждые N дн.	Этот параметр гарантирует, что пароль не будет использоваться постоянно, а будет регулярно обновляться.
	Не может повторно использовать N последних паролей	Благодаря этому параметру одни и те же пароли не будут регулярно использоваться повторно.
	Должен ждать N мин для изменения пароля	Благодаря этому параметру новые пароли невозможно изменить сразу же после ввода в систему.
Ограничения на вход		

Настройки	Параметры	Описание
	Отключать учетную запись после N неудачных попыток входа	В этом параметре безопасности указывается количество попыток входа в систему, которое может сделать пользователь, прежде чем его учетная запись будет отключена.
	Сбрасывать счетчик неудачных попыток через N мин.	В этом параметре указывается промежуток времени, по истечении которого сбрасывается счетчик попыток входа в систему.
	Повторно включать учетную запись через N мин.	В этом параметре указывается время, в течение которого учетная запись остается заблокированной после N неудачных попыток входа в систему.
Синхронизировать учетные данные для входа в систему и источник данных		
	Разрешить и обновить учетные данные пользователя для входа в источник данных при входе в систему	Этот параметр включает учетные данные пользователя для входа в источник данных после выполнения пользователем входа в систему.
Доверительная аутентификация		Позволяет использовать параметры для настройки доверительной аутентификации.

См. также

- [Включение доверительной аутентификации](#)

7.2.3 Изменение параметров Enterprise

1. Перейдите в область управления СМС «Аутентификация».
2. Дважды щелкните **Enterprise**.
Появится диалоговое окно «Enterprise».
3. Измените параметры.

Совет:

Для возврата всех параметров в значения по умолчанию нажмите кнопку **Сброс**.

4. Нажмите кнопку **Обновить**, чтобы сохранить изменения.

7.2.3.1 Изменение общих настроек пароля

1. Перейдите в область управления СМС «Аутентификация».
2. Дважды щелкните **Enterprise**.
Появится диалоговое окно «Enterprise».
3. Установите флажок в ячейке каждой необходимой настройки пароля и введите значение при необходимости.

В следующей таблице указаны минимальные и максимальные значения для каждой связанной с паролями настройки.

Таблица 7-1: Настройки пароля

Настройка пароля	Минимум	Рекомендованный максимум
Принудительно устанавливать пароли с символами в разных регистрах	Н/Д	Н/Д
Должен содержать не менее N символов	0 символов	64 символа
Должен изменять пароль каждые N дн.	1 день	100 дней
Не может повторно использовать N последних паролей	1 пароль	100 паролей
Должен ждать N мин. для изменения пароля	0 минут	100 минут
Отключать учетную запись после N неудачных попыток входа	1 неудачная попытка	100 неудачных попыток

Настройка пароля	Минимум	Рекомендованный максимум
Сбрасывать счетчик неудачных попыток через N мин.	1 минута	100 минут
Повторно включать учетную запись через N мин.	0 минут	100 минут

4. Нажмите кнопку **Обновить**.

7.2.4 Включение доверительной аутентификации

Доверительная аутентификация Enterprise применяется для реализации функции единого входа с использованием веб-сервера для идентификации пользователя. Такой метод аутентификации подразумевает установление отношений доверия между Центральным сервером управления (CMS) и сервером веб-приложений, на котором размещается веб-приложение платформы BI. После установления отношений доверия система передает функции идентификации пользователя на сервер веб-приложений. Доверительная аутентификация может применяться для поддержки таких методов аутентификации, как SAML, x.509 и другие, которые не используют выделенные подключаемые модули аутентификации.

Пользователи предпочитают однократный вход в систему, а не вводить пароль несколько раз за сеанс. Доверительная аутентификация обеспечивает единый вход для интеграции решения аутентификации платформы BI со сторонними решениями аутентификации. Приложения, которые установили доверительные отношения с Центральным сервером управления (CMS), могут использовать доверительную аутентификацию, чтобы дать пользователям возможность выполнять вход в систему без ввода пароля.

Для включения доверительной аутентификации нужно настроить на сервере общий секретный ключ через параметры аутентификации Enterprise, тогда как клиент должен быть настроен через свойства, указанные для файла `BOE.war`.

Примечание:

- Перед использованием доверительной аутентификации необходимо создать пользователей Enterprise или выполнить сопоставление для пользователей сторонних систем, которым потребуется вход в платформу BI.
- URL-адрес единого входа для стартовой панели BI: `http://server:port/BOE/BI`.

См. также

- [Настройка сервера на использование доверительной аутентификации](#)
- [Настройка доверительной аутентификации для веб-приложения](#)

7.2.4.1 Настройка сервера на использование доверительной аутентификации

Для использования доверительной аутентификации необходимо создать пользователей Enterprise или выполнить сопоставление для пользователей сторонних систем, которым потребуется вход в платформу BI.

1. Выполните вход в СМС.
2. Перейдите в область управления **Аутентификация**.
3. Нажмите параметр **Enterprise**.
Будет открыто диалоговое окно «Enterprise».
4. Выполните прокрутку вниз до пункта «Доверительная аутентификация».

- a. Выберите **Доверительная аутентификация включена**.
- b. Нажмите **Новый общий секретный ключ**.

На экран выводится следующее сообщение.

Общий секретный ключ создается, после чего он готов к загрузке.

- c. Нажмите **Загрузить общий секретный ключ**.

Примечание:

Общий секретный ключ используется клиентом и сервером CMS, чтобы установить доверительные отношения. Необходимо настроить клиент по завершении настройки доверительной аутентификации на сервере.

Открывается диалоговое окно «Загрузка файла».

- d. Нажмите «Сохранить» и укажите следующий каталог, в который нужно сохранить файл `TrustedPrincipal.conf`.
`<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`
- e. Чтобы указать период действия общего секретного ключа (в днях), введите значение в поле «Период действия общего секретного ключа».
- f. Укажите значение тайм-аута для запросов доверительной аутентификации.

Примечание:

Значение тайм-аута – это максимальная продолжительность (в миллисекундах) сохранения различия часов клиента и часов сервера CMS. Если указано значение 0, период времени различия двух часов неограничен. Не рекомендуется указывать значение 0, поскольку может повыситься уязвимость при атаках повторной передачи пакетов.

5. Нажмите кнопку **Обновить**, чтобы передать в систему общий секретный ключ.

Примечание:

Изменения, вносимые в параметры доверительной аутентификации, не проверяются платформой BI. Рекомендуется вручную выполнять резервное копирование всех сведений доверительной аутентификации.

Клиентом и CMS используется общий секретный ключ для установки доверительных отношений. Необходимо настроить клиент по завершении настройки доверительной аутентификации на сервере.

7.2.5 Настройка доверительной аутентификации для веб-приложения

Чтобы настроить доверительную аутентификацию для клиента, нужно открыть и изменить глобальные свойства для файла BOE.war и определенные свойства приложений стартовой панели BI и OpenDocument.

Существует два метода передачи общего секретного ключа на клиент.

- Веб-сеанс
- Файл `TrustedPrincipal.conf`

Дополнительно к общему секретному ключу нужно выбрать один из указанных далее методов передачи имени пользователя на клиент.

- Веб-сеанс
- Cookies
- Заголовок HTTP:
- URL-запрос

Вне зависимости от того, какой именно метод выбран, его нужно настроить в глобальных свойствах `Trusted.auth.user.retrieval` для файла BOE.war.

7.2.5.1 Использование доверительной аутентификации для единого входа SAML

SAML – это основанный на языке XML стандарт обмена данными удостоверений. SAML обеспечивает защищенное соединение для обмена данными удостоверений и сведениями о доверии, что дает возможность реализовать механизм единого входа, позволяющий исключить дополнительные операции входа в систему для надежных пользователей, которым требуется войти в платформу BI.

Включение аутентификации SAML

Если сервер приложений поддерживает работу в качестве поставщика услуг SAML, можно использовать доверительную аутентификацию для реализации единого входа SAML в платформу BI.

Для этого необходимо сначала настроить аутентификацию SAML на сервере приложений.

Ниже приведен образец файла Web.xml, настроенного на аутентификацию SAML.

```
<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>
```

Дополнительные инструкции по настройке см. в документации к конкретному серверу приложений.

Использование доверительной аутентификации

После настройки сервера веб-приложений в качестве поставщика услуг SAML можно использовать доверительную аутентификацию для реализации единого входа SAML.

Примечание:

Пользователи должны либо быть импортированы в платформу BI, либо иметь учетные записи Enterprise.

Для реализации функции единого входа используется динамическое присвоение псевдонимов. Когда пользователь впервые открывает страницу входа в систему с помощью SAML, отображается запрос на ввод данных существующей учетной записи платформы BI вручную. После проверки учетных данных пользователя система присваивает удостоверению SAML пользователя псевдоним, соответствующий его учетной записи в платформе BI. Последующие попытки входа в систему этого пользователя обрабатываются с применением функции единого входа, поскольку при этом система динамически сопоставляет псевдоним удостоверения пользователя с существующей учетной записью.

Примечание:

Для правильной работы этого механизма необходимо включить свойство `trusted.auth.user.namespace.enabled` для файла `BOE.war`.

7.2.5.2 Свойства доверительной аутентификации для веб-приложений

В следующей таблице перечислены параметры доверительной аутентификации, которые входят в состав установленного по умолчанию файла `global.properties` для файла `BOE.war`. Чтобы перезаписать параметры, создайте новый файл в каталоге `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Свойство	Значение по умолчанию	Описание
<code>sso.enabled=true</code>	<code>sso.enabled=false</code>	Включает или отключает единый вход в платформу BI. Чтобы включить доверительную аутентификацию, присвойте этому свойству значение <code>true</code> .
<code>trusted.auth.shared.secret</code>	Нет	Имя переменной сеанса, используемой для извлечения секретного ключа для доверительной аутентификации. Применяется только случае использования веб-сеанса для передачи общего секретного ключа.
<code>trusted.auth.user.param</code>	Нет	Задаёт переменную, используемую для извлечения имени пользователя для доверительной аутентификации.
<code>trusted.auth.user.retrieval</code>	Нет	Задаёт метод, используемый для извлечения имени пользователя для доверительной аутентификации. Может иметь одно из следующих значений: <ul style="list-style-type: none"> • "REMOTE_USER" • "HTTP_HEADER" • "COOKIE" • "QUERY_STRING" • "WEB_SESSION" • "USER_PRINCIPAL" Чтобы отключить доверительную аутентификацию, установите пустое значение.
<code>trusted.auth.saml.enabled</code>	<code>trusted.auth.saml.enabled=false</code>	Включает и отключает динамическую привязку псевдонимов к существующим учетным записям. Если этому свойству присвоено значение <code>true</code> , при доверительной аутентификации используется привязка псевдонимов для аутентификации пользователей в платформе BI. Благодаря привязке псевдонимов сервер приложений может работать как поставщик услуг SAML, что позволяет предоставлять функции единого входа SAML в систему при доверительной аутентификации. Если этому свойству присвоено значение <code>false</code> , при доверительной аутентификации для идентификации пользователей будет применяться сопоставление имен.

7.2.5.3 Настройка доверительной аутентификации для веб-приложения

Если планируется хранить общий секретный ключ в файле `TrustedPrincipal.conf`, убедитесь, что этот файл располагается в соответствующем каталоге:

Платформа	Каталог файла <code>TrustedPrincipal.conf</code>
ОС Windows, каталог установки по умолчанию	<code><INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\</code>
AIX	<code><INSTALLDIR>/sap_bobj/enterprise_xi40/aix_rs6000/</code>
Solaris	<code><INSTALLDIR>/sap_bobj/enterprise_xi40/solaris_sparc/</code>
ОС HP_UX	<code><INSTALLDIR>/sap_bobj/enterprise_xi40/hpux_pa-risc/</code>
Linux	<code><INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x86</code>

Поддерживаются различные механизмы заполнения переменной имени пользователя, которая используется при настройке доверительной аутентификации для клиента, на котором размещаются веб-приложения. Настройте или установите сервер веб-приложений таким образом, чтобы имена пользователей были доступны перед использованием этих методов извлечения имен пользователей. Для получения дополнительных сведений см. раздел <http://java.sun.com/j2ee/1.4/docs/api/javax/servlet/http/HttpServletRequest.html>.

Для настройки доверительной аутентификации для клиента требуется изменить свойства в файле `BOE.war`. Файл `BOE.war` содержит как общие, так и специальные свойства для веб-приложений стартовой панели BI и OpenDocument.

Примечание:

В зависимости от предполагаемого способа извлечения имени пользователя и общего секретного ключа могут потребоваться дополнительные шаги.

1. Откройте пользовательскую папку, содержащую файл `BOE.war`, на компьютере, на котором размещаются веб-приложения.

Если используется сервер веб-приложений Tomcat, входящий в комплект установки платформы BI, можно непосредственно перейти в следующую папку:

```
C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom\
```

Совет:

Если используется сервер веб-приложений, не поддерживающий прямой доступ к развернутым веб-приложениям, для изменения файла `BOE.war` можно использовать следующую папку в установке продукта.

```
<INSTALLDIR>\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\.
```

В этом случае измененный файл `BOE.war` впоследствии потребуется развернуть повторно.

2. Создайте новый файл.

Примечание:

Воспользуйтесь программой "Блокнот" или любым другим текстовым редактором.

3. Задайте свойства доверительной аутентификации, указав следующие данные:

```
sso.enabled=true
trusted.auth.user.retrieval=Method for user ID retrieval
trusted.auth.user.param=Variable
trusted.auth.shared.secret=WEB_SESSION
```

Параметры извлечения имени пользователя перечислены в следующей таблице:

Параметр	Способ получения имени пользователя
HTTP_HEADER	Имя пользователя извлекается из содержимого указанного заголовка HTTP. Необходимо указать заголовок HTTP, который будет использоваться в свойстве <code>trusted.auth.user.param</code> .
QUERY_STRING	Имя пользователя извлекается из указанного параметра URL-адреса запроса. Необходимо указать строку запроса, которая будет использоваться в свойстве <code>trusted.auth.user.param</code> .
COOKIE	Имя пользователя извлекается из указанного cookie-файла. Необходимо указать cookie-файл, который будет использоваться в свойстве <code>trusted.auth.user.param</code> .
WEB_SESSION	Имя пользователя извлекается из содержимого указанной переменной сеанса. Необходимо указать переменную веб-сеанса, которая будет использоваться в свойстве <code>trusted.auth.user.param</code> в файле <code>global.properties</code> .
USER_PRINCIPAL	Имя пользователя извлекается путем обращения к методу <code>getUserPrincipal().getName()</code> в объекте <code>HttpServletRequest</code> для текущего запроса в сервлете или JSP.

Примечание:

- На некоторых серверах веб-приложений требуется задать для переменной среды `REMOTE_USER` значение `true`. См. документацию по определенному серверу веб-приложений для получения сведений о необходимости выполнения этого действия. Если это действие является обязательным и используется этот метод извлечения имен пользователей, убедитесь, что для переменной среды задано значение `true`.
- Если для передачи имени пользователя используется параметр `USER_PRINCIPAL`, оставьте свойство `trusted.auth.user.param` пустым.

4. Сохраните файл под следующим именем:
`global.properties`

5. Перезапустите сервер веб-приложений.

Новые свойства вступают в силу только после повторного развертывания измененного веб-приложения `BOE` на компьютере, на котором запущен сервер веб-приложений. Воспользуйтесь `Wdeploy` для повторного развертывания `WAR`-файла на сервере веб-приложений. Для получения дополнительных сведений об использовании `WDeploy` см. *Руководство по развертыванию веб-приложений платформы BusinessObjects Business Intelligence*.

7.2.5.3.1 Примеры конфигурации

Передача общего секретного ключа с помощью файла `TrustedPrincipal.conf`

В следующем примере конфигурации предполагается, что в платформе `BI` создан пользователь `JohnDoe`.

Сведения о пользователе хранятся и передаются с использованием переменной веб-сеанса. Общий секретный ключ передается с помощью файла `TrustedPrincipal.conf`. Предполагается, что этот файл находится в каталоге `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. Пакетная версия `Tomcat 6` представляет собой сервер веб-приложений.

1. Откройте следующий каталог:

```
<INSTALLDIR>\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\
```

2. Создайте новый файл.

Примечание:

Воспользуйтесь программой "Блокнот" или любым другим текстовым редактором.

3. Задайте свойства доверительной аутентификации, указав следующие данные:

```
sso.enabled=true
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.user.param=MyUser
trusted.auth.shared.secret=
```

4. Сохраните файл под следующим именем:
`global.properties`
5. Откройте следующий файл:

C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp

6. Измените содержимое файла и включите в него следующие атрибуты:

```
<!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. Создайте файл myScript.js в следующем каталоге:

C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomResources

8. Добавьте следующий код в файл myScript.js:

```
function goToLogonPage() {
    window.location = "logon.jsp";
}
```

9. Завершите работу сервера Tomcat.

10. Удалите рабочую папку в следующем каталоге:

C:\Program Files (x86)\SAP BusinessObjects\Tomcat6

11. Перезапустите сервер Tomcat.

Чтобы проверить правильность настройки доверительной аутентификации, воспользуйтесь следующим URL-адресом для доступа к приложению стартовой панели BI: [http://\[имя_CMS\]:8080/BOE/BI/custom.jsp](http://[имя_CMS]:8080/BOE/BI/custom.jsp), где атрибут [имя_CMS] определяет имя компьютера, на котором размещается сервер CMS. Должна отображаться следующая ссылка: Щелкните эту ссылку, чтобы перейти на страницу входа в стартовую панель BI

Передача общего секретного ключа с использованием переменной веб-сеанса

В следующем примере конфигурации предполагается, что в платформе BI создан пользователь *JohnDoe*.

Сведения о пользователе хранятся и передаются с помощью веб-сеанса. Общий секретный ключ передается с использованием переменной веб-сеанса. Предполагается, что этот файл находится в каталоге C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86. Откройте файл и просмотрите его содержимое. В этом примере конфигурации предполагается использование следующего общего секретного ключа:

```
9ecb0778edcfff048edae0fcdde1a5db8211293486774a127ec949c1bdb98dae8e0ea388979edc65773
841c8ae5d1f675a6bf5d7c66038b6a3f1345285b55a0a7
```

Пакетная версия Tomcat 6 представляет собой сервер веб-приложений.

1. Откройте следующий каталог:

```
<INSTALLDIR>\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\
```

2. Создайте новый файл.

Примечание:

Воспользуйтесь программой "Блокнот" или любым другим текстовым редактором.

3. Задайте свойства доверительной аутентификации, указав следующие данные:

```
sso.enabled=true
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.user.param=MyUser
trusted.auth.shared.secret=MySecret
```

4. Сохраните файл под следующим именем:

global.properties

5. Откройте следующий файл:

```
C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-
INF\eclipse\plugins\webpath.InfoView\web\custom.jsp
```

6. Измените содержимое файла и включите в него следующие атрибуты:

```
<!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", "9ecb0778edc9f048edae0fcdde1a5db82112934
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. Создайте файл myScript.js в следующем каталоге:

```
C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-
INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomResources
```

8. Добавьте следующий код в файл myScript.js:

```
function goToLogonPage() {
    window.location = "logon.jsp";
}
```

9. Завершите работу сервера Tomcat.

10. Удалите рабочую папку в следующем каталоге:

```
C:\Program Files (x86)\ SAP BusinessObjects\Tomcat6
```

11. Перезапустите сервер Tomcat.

Чтобы проверить правильность настройки доверительной аутентификации, воспользуйтесь следующим URL-адресом для доступа к приложению стартовой панели BI: `http://[имя_CMS]:8080/BOE/BI/custom.jsp`, где атрибут [имя_CMS] определяет имя компьютера, на котором размещается сервер CMS. Должна отображаться следующая ссылка: Щелкните эту ссылку, чтобы перейти на страницу входа в стартовую панель BI

Передача имени пользователя с использованием принципа

В следующем примере конфигурации предполагается, что в платформе BI создан пользователь *JohnDoe*.

Сведения о пользователе хранятся и передаются с использованием параметра "Принципал пользователя". Общий секретный ключ передается с помощью файла `TrustedPrincipal.conf`. Предполагается, что этот файл располагается в каталоге `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. Пакетная версия Tomcat 6 представляет собой сервер веб-приложений.

1. Остановите сервер Tomcat.
2. Откройте файл `server.xml` для сервера Tomcat.
Этот файл по умолчанию располагается в следующем каталоге:

`C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\conf\.`

3. Измените значение атрибута `Realm className=` на следующее:
`Realm className=«org.apache.catalina.realm.MemoryRealm »`

4. Откройте файл `tomcat-users.xml`.
Этот файл по умолчанию располагается в каталоге
`C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\conf\.`

5. Измените тег `<tomcat-users>` следующим образом:

```
<user name=«JohnDoe» password=«password»
roles=«onjavauser»/>
```

6. Откройте файл `web.xml` в следующем каталоге:
`C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\`
7. Добавьте следующую строку перед тегом `</web-app>`:

```
<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>
```

Примечание:

Необходимо указать определенную страницу для параметра `<url-pattern></url-pattern>`. Обычно эта страница отличается от установленной по умолчанию для стартовой панели BI или любого другого веб-приложения.

8. Удалите рабочую папку в следующем каталоге:

`C:\Program Files (x86)\ SAP BusinessObjects\Tomcat6`

9. Перезапустите Tomcat.

Примечание:

В режиме удаленного пользователя используются такие же конфигурации сервера веб-приложений.

Для проверки правильности настройки доверительной аутентификации воспользуйтесь следующим URL-адресом для доступа к приложению стартовой панели BI: `http://[cmsname]:8080/BOE/BI`, где атрибут `[cmsname]` задает имя компьютера, на котором установлено CMS. Спустя некоторое время отображается диалоговое окно входа в систему.

7.3 Аутентификация LDAP

7.3.1 Использование аутентификации LDAP

В этом разделе приводится общее описание использования аутентификации LDAP в платформе BI. В нем также рассматриваются средства администрирования, которые позволяют управлять учетными записями LDAP и настраивать их для платформы.

При установке платформы BI подключаемый модуль аутентификации LDAP устанавливается автоматически, но по умолчанию он не включен. Для использования аутентификации LDAP сначала необходимо настроить соответствующий каталог LDAP. Для получения дополнительных сведений о LDAP см. документацию LDAP.

LDAP (Lightweight Directory Access Protocol – облегченный протокол доступа к каталогу) – это общий, не зависящий от приложений каталог, который позволяет пользователям использовать одни и те же данные в различных приложениях. Основанный на открытом стандарте, протокол LDAP обеспечивает средства доступа и обновления данных в каталоге.

В основе протокола LDAP лежит стандарт X.500, который использует для обмена данными между клиентом и сервером каталога протокол доступа к каталогам (DAP). Протокол LDAP представляет собой альтернативу DAP, поскольку для него требуется меньше ресурсов, и в нем упрощены и удалены некоторые операции и функции X.500.

В структуре каталогов LDAP записи упорядочены по определенной схеме. Каждая запись определяется соответствующим отличительным именем (DN) или общим именем (CN). Другими общими атрибутами являются имя подразделения (OU) и имя организации (O). Например, группу элементов можно найти в дереве каталога по следующим атрибутам: cn=пользователи платформы BI, ou=пользователи Enterprise A, o=исследования. Для получения дополнительных сведений см. документацию LDAP.

Поскольку протокол LDAP не зависит от приложений, доступ к его каталогам может получить любой клиент с надлежащей авторизацией. LDAP позволяет настроить вход пользователей в платформу BI с помощью аутентификации LDAP. Он также позволяет выполнять авторизацию пользователей при доступе к объектам в системе. При наличии LDAP-серверов и использовании протокола LDAP в имеющихся сетевых компьютерных системах можно использовать аутентификацию LDAP (наряду с аутентификацией Enterprise и Windows AD).

При необходимости подключаемый модуль защиты LDAP, поставляемый с платформой BI, может взаимодействовать с сервером LDAP по протоколу SSL с использованием аутентификации сервера или обоюдной аутентификации. При аутентификации сервера платформа BI использует для подтверждения подлинности сервера имеющийся у сервера LDAP сертификат безопасности; при этом сервер LDAP разрешает подключения от анонимных клиентов. При обоюдной аутентификации используются сертификаты безопасности сервера LDAP и платформы BI, и перед установлением соединения сервер LDAP также обязательно проверяет сертификат клиента.

Подключаемый модуль безопасности LDAP, поставляемый с платформой BI, можно настроить таким образом, чтобы взаимодействие с сервером LDAP осуществлялось по протоколу SSL, а для проверки учетных данных пользователей применялась базовая аутентификация. Перед тем как разворачивать аутентификацию LDAP в сочетании с платформой BI, необходимо изучить различия между типами LDAP. Подробности см. в документе RFC2251 по адресу <http://www.faqs.org/rfcs/rfc2251.html>.

См. также

- [Настройка аутентификации LDAP](#)
- [Сопоставление групп LDAP](#)

7.3.1.1 Подключаемый модуль безопасности LDAP

Подключаемый модуль безопасности LDAP позволяет сопоставлять учетные записи пользователей и группы сервера каталога LDAP с платформой BI. Он также позволяет системе проверять все запросы входа в систему, для которых указана аутентификация LDAP. Аутентификация пользователей производится с помощью сервера каталогов LDAP, и их участие в сопоставленной группе LDAP проверяется перед тем, как CMS предоставляет им активный сеанс платформы BI. Система динамически обновляет списки пользователей и их участие в группах. Для повышения безопасности можно настроить платформу на использование SSL-соединения с сервером каталогов LDAP.

Аутентификация LDAP для платформы BI аналогична аутентификации Windows AD в том, что можно сопоставлять группы и настраивать аутентификацию, авторизацию и создание псевдонимов. Как и в случае аутентификации NT или AD, можно создавать учетные записи Enterprise для существующих пользователей LDAP, а также назначать псевдонимы LDAP существующим пользователям, если имена пользователей должны совпадать с именами пользователей Enterprise. Кроме того, доступны перечисленные ниже действия.

- Сопоставление пользователей и групп из службы каталогов LDAP.
- Сопоставление LDAP с AD. При настройке LDAP в сочетании с AD существуют некоторые ограничения.
- Указание нескольких имен хостов и их портов.
- Настройка LDAP с SiteMinder.

После сопоставления пользователей и групп LDAP все клиентские средства платформы BI поддерживают аутентификацию LDAP. Также можно создавать собственные приложения, поддерживающие аутентификацию LDAP.

См. также

- [Настройка параметров SSL для LDAP-сервера или взаимной аутентификации](#)
- [Сопоставление LDAP и Windows AD](#)
- [Настройка подключаемого модуля LDAP для SiteMinder](#)

7.3.2 Настройка аутентификации LDAP

В целях упрощения администрирования платформа BI поддерживает аутентификацию LDAP для учетных записей пользователей и групп. Перед тем как пользователи смогут использовать свое имя пользователя и пароль LDAP для входа в систему, их учетные записи LDAP необходимо сопоставить с платформой BI. При сопоставлении учетной записи LDAP можно создать новую учетную запись или ссылку на существующую учетную запись в платформе BI.

Перед настройкой и включением аутентификации LDAP необходимо настроить каталог LDAP. Дополнительную информацию см. в документации LDAP.

Настройка аутентификации LDAP состоит из следующих перечисленных ниже задач.

- Настройка хоста LDAP
- Подготовка сервера LDAP для SSL (при необходимости)
- Настройка подключаемого модуля LDAP для SiteMinder (при необходимости)

Примечание:

Если настроить LDAP с AD, то можно будет сопоставлять пользователей, но нельзя будет настроить единый вход AD и единый вход в базу данных. Однако будут доступны способы единого входа LDAP, такие как SiteMinder и доверенная аутентификация.

7.3.2.1 Настройка хоста LDAP

Рекомендуется установить и запустить сервер LDAP, прежде, чем настраивать хост LDAP.

1. Перейдите в область управления СМС **Аутентификация** и дважды щелкните пункт **LDAP**.

Примечание:

Чтобы перейти в область управления **Аутентификация**, выберите в списке навигации пункт **Аутентификация**.

2. Введите имя и номер порта хостов LDAP в поле **Добавить хост LDAP (имя хоста:порт)** (например, "myserver:123"), щелкните **Добавить**, а затем нажмите кнопку **ОК**.

Совет:

Повторите этот шаг, чтобы добавить дополнительные хосты LDAP-серверов такого же типа, если требуется, чтобы они работали в качестве резервных. Для удаления хоста выделите его имя и нажмите кнопку **Удалить**.

3. Выберите в списке **Тип сервера LDAP** тип сервера.

Примечание:

Если выполняется сопоставление LDAP с AD, выберите тип сервера "Сервер Active Directory Application Microsoft".

4. Если требуется просмотреть или изменить какие-либо из назначений атрибутов сервера LDAP или принятых по умолчанию атрибутов поиска LDAP, щелкните **Показать отображения атрибутов**.

По умолчанию все сопоставления атрибутов и атрибуты поиска поддерживаемых типов серверов уже настроены.

5. Нажмите кнопку **Далее**.
6. В поле **Базовое известное имя LDAP** введите известное имя (например, o=SomeBase) LDAP-сервера и нажмите кнопку **Далее**.
7. В области учетных данных LDAP-сервера укажите известное имя и пароль учетной записи, у которой есть доступ на чтение каталога.

Примечание:

Учетные данные администратора не обязательны.

Примечание:

Если LDAP-сервер позволяет выполнять анонимную привязку, оставьте это поле пустым – серверы и клиенты платформы BI будут выполнять привязку к основному хосту с использованием анонимного входа.

8. Если настроены ссылки на LDAP-хост, введите информацию для аутентификации в области **Ссылочные идентификационные данные LDAP**, а затем введите количество ссылочных переходов в поле **Максимальное количество ссылочных узлов маршрутизации**.

Примечание:

В области "Ссылочные идентификационные данные LDAP" необходимо ввести параметры, если выполняются все из указанных ниже условий.

- Основной хост настроен ссылаться на другой сервер каталога, который обрабатывает запросы для записей определенной базы данных.
- Хост, на который осуществляются ссылки, не разрешает анонимную привязку.
- Группа хоста, на который настроены ссылки, будет сопоставлена платформе BI.

Примечание:

- Хотя можно сопоставлять группы с нескольких хостов, настроить можно только один набор учетных данных для ссылок. Поэтому при наличии нескольких хостов для ссылок необходимо создать на каждом хосте учетную запись пользователя с одинаковым отличительным именем и паролем.
- Если параметру "Максимальное количество ссылочных узлов маршрутизации" присвоено значение 0, ссылки осуществляться не будут.

9. Нажмите кнопку **Далее**.

10. Выберите тип используемой SSL-аутентификации и нажмите кнопку **Далее**.

Можно выбрать один из перечисленных ниже вариантов.

- Базовая (без SSL)
- Аутентификация сервера
- Взаимная аутентификация

11. Выберите способ аутентификации LDAP с единым входом и нажмите кнопку **Далее**.

Можно выбрать один из перечисленных ниже вариантов.

- Базовый (без SSO)
- SiteMinder

12. Выберите способ сопоставления псевдонимов и пользователей учетным записям платформы BI.

a. В пункте «Параметры нового псевдонима» выберите способ сопоставления новых псевдонимов учетным записям Enterprise. Выберите один из перечисленных ниже вариантов.

- **Назначить каждый добавленный псевдоним LDAP учетной записи с тем же именем**

Данный вариант используется в случае, когда известно, что у пользователей есть учетная запись Enterprise с таким же именем. То есть псевдонимы LDAP будут назначены существующим пользователям (включена функция автоматического создания псевдонимов). Пользователи, у которых нет учетной записи Enterprise, или для которых имя учетной записи Enterprise не совпадает с именем учетной записи, добавляются в качестве новых пользователей LDAP.

- **Создать новую учетную запись для каждого добавленного псевдонима LDAP**

Данный параметр используется в случае, когда необходимо создавать учетную запись для каждого пользователя.

- b. В поле «Параметры обновления псевдонимов» выберите способ управления обновлением псевдонимов для учетных записей Enterprise. Выберите один из перечисленных ниже вариантов.

- **Создавать новые псевдонимы при обновлении псевдонимов**

Данный вариант используется для автоматического создания псевдонима для каждого пользователя LDAP, сопоставленного платформе BI. Новые учетные записи LDAP добавляются для пользователей без учетных записей платформы BI или для всех пользователей, если выбран вариант **Создавать новую учетную запись для каждого добавленного псевдонима LDAP**.

- **Создавать новые псевдонимы только при входе пользователя в систему**

Данный вариант используется в случае, когда сопоставляемый каталог LDAP содержит много пользователей, но только некоторые из них будут использовать платформу BI. Система не будет автоматически создавать псевдонимы и учетные записи Enterprise ни для каких пользователей. Вместо этого программа создает псевдонимы (и учетные записи, при необходимости) только для пользователей, которые входят в платформу.

- c. В поле «Параметры нового пользователя» укажите, как создаются новые пользователи. Если лицензия платформы SAP BusinessObjects Business Intelligence основана на ролях пользователей, выберите один из перечисленных параметров в поле «Параметры нового пользователя».

- **BI Viewer**

Учетные записи новых пользователей создаются с ролью BI Viewer. Доступ к приложениям платформы BI для всех учетных записей роли BI Viewer определяется в лицензионном соглашении. Пользователи ограничены доступом к рабочим процессам приложений, которые определены для роли BI Viewer. Права доступа обычно ограничены просмотром документов Business Intelligence. Эта роль обычно подходит для пользователей, которые используют контент через приложения платформы BI.

- **BI Analyst** Учетные записи новых пользователей создаются с ролью BI Analyst. Доступ к платформе BI для всех учетных записей роли BI Analyst определяется в лицензионном соглашении. Пользователи могут обращаться ко всем рабочим процессам приложений, которые определены для роли BI Analyst. Права доступа включают просмотр и изменение документов Business Intelligence. Эта роль обычно подходит для пользователей, которые создают и изменяют контент для приложений платформы BI.

Если лицензия платформы SAP BusinessObjects Business Intelligence не основана на ролях пользователей, выберите один из перечисленных ниже параметров:

- **Новые пользователи создаются как именованные пользователи.**

Новые учетные записи пользователей настраиваются на использование именованных пользовательских лицензий. Именованные пользовательские лицензии связаны с конкретными пользователями и позволяют им входить в систему, используя имя пользователя и пароль. Это дает именованным пользователям право доступа к системе независимо от того, сколько других пользователей выполнили вход. Для каждой учетной записи, созданной с использованием данного параметра, должна существовать именованная пользовательская лицензия.

- **Новые пользователи создаются как конкурентные пользователи.**

Новые учетные записи пользователей настраиваются на использование конкурентных пользовательских лицензий. Лицензии на одновременный доступ указывают количество человек, которые могут подключиться к платформе SAP BusinessObjects Business Intelligence одновременно. Это очень гибкий тип лицензий, так как небольшое их количество поддерживает широкую пользовательскую базу. Например, в зависимости от того, как часто и как долго пользователи работают с платформой, лицензия на одновременный доступ для 100 пользователей может поддерживать 250, 500 или 700 пользователей.

13. В области «Параметры привязки атрибутов» можно указать приоритет привязки атрибутов для подключаемого модуля LDAP:
- Щелкните поле **Импортировать полное имя и адрес электронной почты**.
Полные имена и описания, используемые в учетных записях LDAP, импортируются и сохраняются в пользовательских объектах в платформе BI.
 - Укажите значение для параметра **Установка приоритета для привязки атрибута LDAP относительно других привязок атрибутов**.

Примечание:

Если задано значение «1», в сценариях, в которых включены LDAP и другие подключаемые модули (Windows AD и SAP), приоритет имеют атрибуты LDAP. Если задано значение «3», приоритет имеют атрибуты из других подключаемых модулей.

14. Нажмите кнопку **Готово**.

См. также

- [Настройка параметров SSL для LDAP-сервера или взаимной аутентификации](#)
- [Настройка подключаемого модуля LDAP для SiteMinder](#)
- [Лицензирование на основе ролей](#)

7.3.2.2 Управление несколькими хостами LDAP

При использовании LDAP и платформы BI можно обеспечить отказоустойчивость системы посредством настройки нескольких хостов LDAP. Система использует первый добавленный хост LDAP в качестве основного. Остальные хосты считаются резервными.

Основной хост LDAP и все резервные хосты должны быть настроены одинаково, и каждый хост LDAP должен ссылаться на все дополнительные хосты, с которых предполагается сопоставлять группы. Дополнительную информацию о хостах LDAP и ссылках см. в документации LDAP.

Чтобы добавить несколько хостов LDAP, укажите все хосты при настройке LDAP с использованием мастера настройки LDAP (подробности см. в разделе). Или, если серверы LDAP уже настроены, перейдите в область Central Management Console "Аутентификация" и откройте вкладку "LDAP". В области "Сводка по настройке сервера LDAP" щелкните имя хоста LDAP, чтобы открыть страницу, на которой можно добавлять и удалять хосты.

Примечание:

- Сначала добавьте основной хост, а затем – резервные.
- При использовании резервных хостов LDAP нельзя использовать максимальный уровень SSL-защиты (то есть нельзя выбрать вариант "Принимать сертификат сервера, если он приходит от заслуживающего доверия органа сертификации, и атрибут CN этого сертификата соответствует имени хоста DNS данного сервера").

См. также

- [Настройка аутентификации LDAP](#)

7.3.2.3 Настройка параметров SSL для LDAP-сервера или взаимной аутентификации

В этом разделе приведена информация для CMC по настройке взаимной аутентификации и взаимодействия с LDAP-сервером по SSL-протоколу. Предполагается, что настроен хост LDAP и выбран один из следующих видов SSL-аутентификации:

- Аутентификация сервера
- Взаимная аутентификация

Для получения дополнительных сведений или сведений о настройке хоста LDAP-сервера см. документацию поставщика LDAP.

См. также

- [Настройка хоста LDAP](#)

7.3.2.3.1 Настройка аутентификации LDAP-сервера или взаимной аутентификации

Ресурс	Необходимые предварительные действия
Сертификат CA	Нужно, чтобы центр сертификации создал сертификат CA. Этот сертификат затем нужно добавить на ваш LDAP-сервер. Для получения дополнительных сведений см. документацию поставщика LDAP. Это действие необходимо как для аутентификации сервера, так и для взаимной аутентификации при использовании SSL.
Сертификат сервера	Нужно запросить и создать сертификат сервера. Следует авторизовать этот сертификат, прежде чем добавлять его в LDAP-сервер. Это действие необходимо как для аутентификации сервера, так и для взаимной аутентификации при использовании SSL.
cert7.db key3.db	<p>Понадобится доступ к приложению certutil, которое может создать файл cert7.db. Загрузить это приложение можно с веб-страницы http://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_6_RTM/. Скопируйте сертификат CA в тот же каталог, в котором находится certutil. Создайте файлы cert7.dbkey3.db и secmod.db с помощью такой команды:</p> <pre>certutil -N -d .</pre> <p>Добавьте сертификат CA в файл cert7.db, воспользовавшись такой командой:</p> <pre>certutil -A -n <CA_alias_name> -t CT -d . -I cacert.cer</pre> <p>Сохраните эти три файла в известном каталоге на компьютере, где размещена платформа SAP BusinessObjects Business Intelligence. Эти файлы необходимы как для аутентификации сервера, так и для взаимной аутентификации при использовании SSL.</p>
cacerts	<p>Этот файл необходим только для аутентификации сервера или взаимной аутентификации при использовании SSL для приложений Java, таких как стартовая панель BI. Перейдите к своему файлу keytool в каталоге bin Java. Воспользуйтесь такой командой для создания файла cacerts:</p> <pre>keytool -import -v -alias <CA_alias_name> -file <CA_certificate_name> -trustcacerts -keystore</pre> <p>Сохраните файл cacerts в тот же каталог, в котором хранятся файлы cert7.db и key3.db.</p>
Сертификат клиента	

Ресурс	Необходимые предварительные действия
	<p>Необходимо создать отдельные клиентские запросы для файлов <code>cert7.db</code> и <code>.keystore</code>. Для настройки подключаемого модуля LDAP нужно создать запрос сертификата клиента с помощью <code>certutil</code>. Для создания запроса сертификата клиента воспользуйтесь такой командой:</p> <pre>certutil -R -s "<client_dn>" -a -o <certificate_request_name> -d .</pre> <p>Примечание: A <client_dn>, указав такую информацию, как "CN=<имя_клиента>, OU=организационное подразделение, O=Название_компании, L=город, ST=область, C=страна. Затем для этого запроса сертификата нужно выполнить аутентификацию с помощью центра сертификации. Для получения сертификата и его вставки в файл <code>cert7.db</code> воспользуйтесь приведенной ниже командой.</p> <pre>certutil -A -n <client_name> -t Pu -d . -I <client_certificate_name></pre> <p>Для облегчения аутентификации Java при использовании SSL нужно создать запрос сертификата клиента с помощью утилиты <code>keytool</code> из каталога <code>bin</code> Java. Создайте пару ключей, воспользовавшись такой командой:</p> <pre>keytool -genkey -keystore .keystore</pre> <p>После указания сведений о клиенте воспользуйтесь такой командой для создания запроса сертификата клиента:</p> <pre>keytool -certreq -file <certificate_request_name> -keystore .keystore</pre> <p>После аутентификации запроса сертификата клиента центром сертификации этот сертификат CA нужно вставить в файл <code>.keystore</code> с использованием следующей команды.</p> <pre>keytool -import -v -alias <CA_alias_name> -file <ca_certificate_name> -trustcacerts -keystore .keystore</pre> <p>Наконец, получите запрос сертификата клиента от ЦС и вставьте его в файл <code>.keystore</code>, воспользовавшись для этого показанной ниже командой:</p> <pre>keytool -import -v -file <client_certificate_name> -trustcacerts -keystore .keystore</pre> <p>Сохраните файл <code>.keystore</code> в тот же каталог, в котором хранятся <code>cert7.db</code> и <code>cacerts</code> на компьютере, где размещена платформа BI.</p>

1. Выберите один из доступных уровней SSL-защиты:

Примечание:

Java-приложения будут игнорировать первый и второй вариант и будут принимать сертификат сервера только в том случае, если он поступает от надежного органа сертификации.

- **Всегда принимать сертификат сервера**

Это самый небезопасный вариант защиты. Перед тем, как платформа BI установит SSL-соединение с LDAP-сервером (для аутентификации LDAP-пользователей и групп), она должна принять сертификат безопасности от LDAP-сервера. Платформа BI не проверяет получаемый сертификат.

- **Принимать сертификат сервера, если он приходит от заслуживающего доверия органа сертификации**

Это средний уровень безопасности. Перед тем, как платформа BI установит SSL-соединение с LDAP-сервером (для аутентификации LDAP-пользователей и групп), она должна принять сертификат безопасности от LDAP-сервера и проверить его. Для проверки сертификата системе необходимо найти в своей базе данных центр сертификации, выпустивший сертификат.

- **Принимать сертификат сервера, если он приходит от заслуживающего доверия органа сертификации, и атрибут CN этого сертификата соответствует имени хоста DNS данного сервера**

Это максимальный уровень защиты. Перед тем, как платформа BI установит SSL-соединение с LDAP-сервером (для аутентификации LDAP-пользователей и групп), она должна принять сертификат безопасности от LDAP-сервера и проверить его. Для проверки сертификата платформе BI необходимо найти в своей базе данных центр сертификации, выпустивший сертификат. Также у нее должна быть возможность проверить, чтобы атрибут CN сертификата сервера точно соответствовал имени хоста LDAP-сервера, введенного в поле "Добавить хост LDAP" на первом шаге мастера. То есть если имя хоста LDAP-сервера введено как ABALONE.rd.crystald.net:389, в сертификате нельзя будет указать атрибут CN =ABALONE:389.

Имя хоста сертификата безопасности сервера – это имя основного хоста LDAP. Поэтому если выбрать этот вариант, то нельзя будет использовать резервный хост LDAP.

2. В поле **Хост SSL** введите имя хоста каждого из компьютеров и щелкните **Добавить**.

Примечание:

Затем необходимо добавить имя хоста каждого компьютера в развертывание платформы BI, использующее пакет SDK платформы SAP BusinessObjects Business Intelligence. (Включая компьютер с центральным сервером управления и компьютер с сервером веб-приложений.)

3. Укажите параметры SSL для каждого хоста SSL, добавленного в список, и укажите параметры по умолчанию, которые будут использоваться для каждого хоста, отсутствующего в списке.

Примечание:

Параметры по умолчанию будут использоваться для всех параметров (для всех хостов), для которых установлен флажок "Использовать значение по умолчанию", или для каждого компьютера, имя которого не добавлено явно в список хостов SSL.

Чтобы указать параметры по умолчанию, выполните следующие действия:

- a. Выберите значение по умолчанию в списке SSL.
- b. Снимите флажки **Использовать значение по умолчанию**.
- c. Введите значения "Путь к файлам сертификатов и базы данных ключей" и "Пароль для базы данных ключей".
- d. Если указываются параметры для взаимной аутентификации, также можно ввести значение в поле "Мнемоническое имя для сертификата клиента в cert7.db".

Чтобы выбрать параметры для другого хоста, выберите его имя в списке слева. Затем введите соответствующие значения в поля справа.

4. Нажмите кнопку **Далее**.
5. Выберите из следующих вариантов способ аутентификации LDAP с единым входом:
 - Базовый (без SSO)
 - SiteMinder
6. Выберите способ создания пользователей и псевдонимов LDAP.
7. Щелкните **Готово**.

См. также

- [Настройка подключаемого модуля LDAP для SiteMinder](#)

7.3.2.4 Изменение параметров конфигурации LDAP

После настройки аутентификации LDAP с использованием мастера настройки LDAP можно изменить параметры подключения LDAP и группы-члены с помощью сводной страницы конфигурации LDAP-сервера.

1. Перейдите в область управления СМС **Аутентификация**.
2. Дважды щелкните **LDAP**.

Если настроена авторизация LDAP, откроется сводная страница конфигурации LDAP-сервера. На этой странице можно изменить любые параметры подключения. Также можно изменить группы в области "Отображенные группы членов LDAP".

3. Удалите сопоставленные группы, которые будут недоступны при использовании новых параметров подключения, и щелкните **Обновить**.
4. Измените параметры соединения и нажмите кнопку **Обновить**.
5. Измените параметры псевдонимов и создания пользователей и нажмите кнопку **Обновить**.
6. Сопоставьте новые группы-члены LDAP и нажмите кнопку **Обновить**.

7.3.2.5 Настройка подключаемого модуля LDAP для SiteMinder

В этом разделе описана настройка СМС для использования LDAP с SiteMinder. SiteMinder – это средство доступа и аутентификации от стороннего производителя, которое можно использовать с подключаемым модулем безопасности LDAP для использования единого входа в платформу BI.

Для использования SiteMinder и LDAP в платформе BI необходимо изменить конфигурацию в двух местах:

- Подключаемый модуль LDAP через CMC
- Свойства в файле BOE.war

Примечание:

Администратор SiteMinder должен включить поддержку агентов версии 4.x. Это должно быть сделано независимо от используемой поддерживаемой версии SiteMinder. Дополнительную информацию о средстве SiteMinder и его установке см. в документации SiteMinder.

См. также

- [Настройка хоста LDAP](#)

7.3.2.5.1 Настройка LDAP на использование единого входа с SiteMinder

1. Откройте окно **Задать настройку SiteMinder** с одним из следующих способов:
 - Выберите SiteMinder в окне "Выберите метод единой регистрации LDAP" в мастере настройки LDAP.
 - Выберите ссылку "Тип единого входа" на странице аутентификации LDAP, которая доступна в случае, если аутентификация LDAP уже настроена, и выполняется добавление поддержки единого входа.
2. В поле **Хост сервера политик** введите имя каждого из серверов политик и нажмите кнопку **Добавить**.
3. Для каждого хоста сервера политик укажите номера портов **учета, аутентификации и авторизации**.
4. Введите **Имя агента** и **Совместно используемый секретный ключ**. Введите совместно используемый секретный ключ еще раз.
5. Нажмите кнопку **Далее**.
6. Переходите к настройке параметров LDAP.

7.3.2.5.2 Включение LDAP и SiteMinder в файле BOE.war

Помимо настройки параметров SiteMinder для подключаемого модуля безопасности LDAP необходимо настроить параметры SiteMinder для свойств BOE.war.

1. Перейдите в следующий каталог в папке установки платформы BI:

```
<INSTALLDIR>\SAP BusinessObjects Enterprise XI  
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\.
```

2. Создайте новый файл.

Примечание:

Воспользуйтесь программой "Блокнот" или любым другим текстовым редактором.

3. Закройте этот файл и сохраните его с таким именем:
BIIlaunchpad.properties
4. Введите следующее выражение:

```
siteminder.authentication=secLDAP  
siteminder.enabled=true
```


5. Закройте этот файл и сохраните его с таким именем:

global.properties

Примечание:

Убедитесь в том, что файл с выбранным именем не сохраняется с каким-либо другим расширением кроме .txt.

6. Создайте другой файл в этом же каталоге.

7. Введите следующее выражение:

```
authentication.default=LDAP
cms.default=[enter your cms name]:[Enter the CMS port number]
```

Например:

```
authentication.default=LDAP
cms.default=mycms:6400
```

8. Закройте этот файл и сохраните его с таким именем:

bilaunchpad.properties

Новые свойства вступают в силу только после повторного развертывания измененного веб-приложения ВОЕ на компьютере, на котором запущен сервер веб-приложений. Воспользуйтесь Wdeploy для повторного развертывания WAR-файла на сервере веб-приложений. Для получения дополнительных сведений об использовании WDeploy см. *Руководство по развертыванию веб-приложений платформы BusinessObjects Business Intelligence*.

7.3.3 Сопоставление групп LDAP

После настройки хоста LDAP с помощью мастера настройки LDAP можно сопоставить группы LDAP группам Enterprise.

После сопоставления групп LDAP можно просмотреть их, выбрав параметр LDAP в области управления **Аутентификация**. Если настроена авторизация LDAP, в области "Группы членов LDAP с установленным соответствием" отображаются группы LDAP, сопоставленные платформе BI.

Также можно назначить группы Windows AD таким образом, чтобы аутентификация в платформе BI выполнялась через подключаемый модуль безопасности LDAP.

Примечание:

При настройке LDAP с AD в ходе этой процедуры будет выполнено сопоставление групп AD.

См. также

- [Сопоставление LDAP и Windows AD](#)

7.3.3.1 Сопоставление групп LDAP с использованием платформы BI

1. Перейдите в область управления СМС **Аутентификация**.

2. Дважды щелкните **LDAP**.

Если настроена авторизация LDAP, откроется страница сводной информации LDAP.

3. В области "Группы членов LDAP с установленным соответствием" укажите группу LDAP (с использованием общего либо отличительного имени) в поле **Добавить группу LDAP (по sn или dn)**. Нажмите кнопку **Добавить**.

Повторяя этот шаг, можно добавить дополнительные группы LDAP. Чтобы удалить группу LDAP, выделите ее и щелкните "Удалить".

4. "Параметры нового псевдонима" позволяют определить способ сопоставления псевдонимов LDAP учетным записям Enterprise. Выберите один из вариантов.

- **Назначить каждый добавленный псевдоним LDAP учетной записи с тем же именем**

Данный вариант используется в случае, когда известно, что у пользователей есть учетная запись Enterprise с таким же именем. То есть псевдонимы LDAP будут назначены существующим пользователям (включена функция автоматического создания псевдонимов). Пользователи, у которых нет учетной записи Enterprise, или для которых имя учетной записи Enterprise не совпадает с именем учетной записи LDAP, добавляются в качестве новых пользователей LDAP.

или

- **Создать новую учетную запись для каждого добавленного псевдонима LDAP**

Данный параметр используется в случае, когда необходимо создавать учетную запись для каждого пользователя.

5. Параметры обновления позволяют указать, будут ли автоматически создаваться псевдонимы LDAP для всех новых пользователей. Выберите один из вариантов.

- **Будут добавлены новые псевдонимы, и будут созданы новые пользователи**

Данный вариант используется для автоматического создания псевдонима для каждого пользователя LDAP, сопоставленного платформе BI. Новые учетные записи LDAP добавляются для пользователей без учетных записей платформы BI или для всех пользователей, если выбран вариант "Создать новую учетную запись для каждого добавленного псевдонима LDAP" и нажимается **Обновить**.

или

- **Новые псевдонимы не будут добавлены, и новые пользователи не будут созданы**

Данный вариант используется в случае, когда сопоставляемый каталог LDAP содержит много пользователей, но только некоторые из них будут использовать платформу BI. Система не будет автоматически создавать псевдонимы и учетные записи Enterprise ни

для каких пользователей. Вместо этого программа создает псевдонимы (и учетные записи, при необходимости) только для пользователей, которые входят в платформу BI.

6. "Параметры нового пользователя" позволяют определить свойства новых учетных записей Enterprise, создаваемых для сопоставления учетным записям LDAP.

Если лицензия платформы SAP BusinessObjects Business Intelligence основана на ролях пользователей, выберите один из перечисленных параметров в поле «Параметры нового пользователя».

- **BI Viewer**

Учетные записи новых пользователей создаются с ролью BI Viewer. Доступ к приложениям платформы BI для всех учетных записей роли BI Viewer определяется в лицензионном соглашении. Пользователи ограничены доступом к рабочим процессам приложений, которые определены для роли BI Viewer. Права доступа обычно ограничены просмотром документов Business Intelligence. Эта роль обычно подходит для пользователей, которые используют контент через приложения платформы BI.

- **BI Analyst**

Для новых учетных записей пользователя настраивается роль BI Analyst. Доступ к платформе BI для всех учетных записей роли BI Analyst определяется в лицензионном соглашении. Пользователи могут обращаться ко всем рабочим процессам приложения, определенным для роли BI Analyst. Права доступа включают просмотр и изменение документов Business Intelligence. Эта роль обычно подходит для пользователей, которые создают и изменяют контент для приложений платформы BI.

Если лицензия платформы SAP BusinessObjects Business Intelligence не основана на ролях пользователей, выберите один из перечисленных ниже параметров:

- **Новые пользователи создаются как именованные пользователи.**

Новые учетные записи пользователей настраиваются на использование именованных пользовательских лицензий. Именованные пользовательские лицензии связаны с конкретными пользователями и позволяют им входить в систему, используя имя пользователя и пароль. Это дает именованным пользователям право доступа к системе независимо от того, сколько других пользователей выполнили вход. Для каждой учетной записи, созданной с использованием данного параметра, должна существовать именованная пользовательская лицензия.

- **Новые пользователи создаются как конкурентные пользователи.**

Новые учетные записи пользователей настраиваются на использование конкурентных пользовательских лицензий. Лицензии на одновременный доступ указывают количество человек, которые могут подключиться к платформе BI одновременно. Это очень гибкий тип лицензий, так как небольшое их количество поддерживает широкую пользовательскую базу. Например, в зависимости от того, как часто и как долго пользователи работают с системой, лицензия на одновременный доступ для 100 пользователей может поддерживать 250, 500 или 700 пользователей.

7. Щелкните **Обновить**.

См. также

- [Лицензирование на основе ролей](#)

7.3.3.2 Отмена сопоставления групп LDAP с использованием платформы BI

1. Перейдите в область управления СМС **Аутентификация**.
2. Дважды щелкните **LDAP**.
Если настроена авторизация LDAP, откроется страница сводной информации LDAP.
3. В области "Группы членов LDAP с установленным соответствием" выберите группу LDAP, которую требуется удалить.
4. Щелкните **Удалить**, а затем – **Обновить**.

Пользователи этой группы больше не смогут получить доступ к платформе BI.

Примечание:

Единственным исключением из этого правила будет случай, когда у пользователя есть псевдоним для учетной записи Enterprise. Для ограничения доступа отключите или удалите учетную запись Enterprise для пользователя.

Чтобы запретить аутентификацию LDAP для всех групп, снимите флажок "Аутентификация LDAP включена" и щелкните **Обновить**.

7.3.3.3 Сопоставление LDAP и Windows AD

При настройке LDAP с Windows AD необходимо помнить о существующих ограничениях.

- Если настроить LDAP с AD, то можно будет сопоставлять пользователей, но нельзя будет настроить единый вход AD и единый вход в базу данных. Однако будут доступны способы единого входа LDAP, такие, как SiteMinder и доверенная аутентификация.
- Пользователи, которые являются только членами групп AD по умолчанию, не смогут осуществлять вход. Пользователи также должны быть членами другой явно созданной группы AD, которая, кроме того, должна быть сопоставлена. Примером такой группы может быть группа "пользователи домена".
- Если в сопоставленной локальной группе домена есть пользователь из другого домена леса, пользователь из другого домена леса не сможет осуществлять вход.
- Пользователи универсальной группы из домена, не принадлежащего контроллеру домена, который используется в качестве узла LDAP, не смогут осуществлять вход.

- Подключаемый модуль LDAP нельзя использовать для сопоставления пользователей и групп из лесов AD, отличных от леса, в котором установлена платформа BI.
- Отсутствует возможность сопоставления группы "Пользователи домена" в AD.
- Отсутствует возможность сопоставления локальных групп компьютеров.
- При использовании контроллера домена глобального каталога при сопоставлении LDAP с AD рекомендуется учитывать следующие факторы:

Ситуация	Рекомендации
Несколько доменов при указании на контроллер домена глобального каталога	<p>Сопоставление можно осуществлять со следующими элементами:</p> <ul style="list-style-type: none"> • универсальные группы в дочернем домене, • группы в этом же домене, которые содержат универсальные группы из дочернего домена, • универсальные группы в кросс-домене. <p>Сопоставление нельзя осуществлять со следующими элементами:</p> <ul style="list-style-type: none"> • глобальные группы в дочернем домене, • локальные группы в дочернем домене, • группы из того же домена, который содержит глобальную группу дочернего домена, • междоменные глобальные группы. <p>В общем случае, если группа является универсальной, она будет поддерживать пользователей из кросс-доменов и дочерних доменов. Другие группы, если в них есть пользователи из кросс-доменов и дочерних доменов, сопоставляться не будут. В целевом домене можно сопоставлять локальные, глобальные и универсальные группы.</p>
Сопоставление в универсальных группах	Для сопоставления в универсальных группах необходимо ссылаться на контроллер домена глобального каталога. Также вместо стандартного порта 389 необходимо использовать порт 3268.

- Если используется несколько доменов, но не выполняется указание на контроллер домена глобального каталога, то отсутствует возможность сопоставления с любым типом групп из кросс-доменов или дочерних доменов. Сопоставление можно производить с любыми типами групп только из определенного домена, на который выполняется указание.

7.3.3.4 Устранение неполадок с учетными записями LDAP

- Если создается учетная запись пользователя LDAP и она не относится к учетной записи группы, сопоставленной платформе BI, следует либо сопоставить группу, либо добавить новую учетную запись LDAP в группу, которая уже сопоставлена системе.
- Если создается учетная запись пользователя LDAP и она относится к учетной записи группы, сопоставленной платформе BI, следует обновить список пользователей.

См. также

- [Настройка аутентификации LDAP](#)
- [Сопоставление групп LDAP](#)

7.4 Аутентификация Windows AD

7.4.1 Обзор

7.4.1.1 Использование аутентификации Windows AD

В этом разделе приводится общее описание использования аутентификации Windows Active Directory (AD) в платформе BI. В нем также рассматриваются рабочие процессы администрирования, необходимые для включения учетных записей AD и управления ими в платформе BI. В конце раздела приведены общие рекомендации по устранению неполадок.

Требования к поддержке

Для упрощения использования аутентификации AD в платформе BI необходимо помнить следующие требования к поддержке.

- CMS необходимо всегда устанавливать на поддерживаемой платформе Windows.
- Хотя системы Windows 2003 и Windows 2008 поддерживают как аутентификацию Kerberos, так и NTLM, в некоторых приложениях платформы BI можно использовать только определенные

методы аутентификации. Например, такие приложения, как стартовая панель BI и Central Management Console поддерживают только аутентификацию Kerberos.

Общий рабочий процесс аутентификации AD

Для использования аутентификации AD в платформе BI необходимо выполнить описанные далее действия.

1. Настройте необходимые ресурсы контроллера домена.
2. Подготовьте хост платформы BI для аутентификации Windows AD.
3. Включите подключаемый модуль безопасности AD и сопоставьте группы AD.
4. Выберите способ аутентификации:
 - Windows AD с Kerberos
 - Windows AD с NTLM.
5. Установка SSO в приложениях платформы BI. Этот необязательный шаг можно выполнить следующими способами:
 - Windows AD с Vintela (Kerberos)
 - Windows AD с SiteMinder (Kerberos)

7.4.1.1.1 Подключаемый модуль безопасности Windows AD

Подключаемый модуль безопасности Windows AD позволяет сопоставлять учетные записи пользователей и групп из базы данных пользователей Microsoft Active Directory (AD) 2003 и 2008 с платформой BI. Он также позволяет системе проверять все запросы входа, для которых указана аутентификация Windows AD. Аутентификация пользователей осуществляется по базе данных пользователей AD, а также по участию в сопоставленной группе AD перед тем, как центральный сервер управления предоставит им активный сеанс платформы BI.

С помощью подключаемого модуля безопасности Windows AD можно настроить следующие компоненты:

- Аутентификация Windows AD с NTLM
- Аутентификация Windows AD с Kerberos
- Аутентификация Windows AD с функцией единого входа SiteMinder

Подключаемый модуль безопасности AD совместим с доменами Microsoft Active Directory 2003 и 2008, работающими в собственном или смешанном режиме.

После сопоставления пользователям и группам AD будет открыт доступ к инструментам клиента платформы BI с использованием аутентификации AD.

- Аутентификация AD работает только в том случае, если CMS работает в Windows. Для работы единого входа в базу данных серверы отчетов также должны работать в Windows. В противном случае все серверы и службы могут работать на любых поддерживаемых платформах.
- Подключаемый модуль Windows AD для платформы BI поддерживает домены в нескольких лесах.

7.4.1.1.2 Использование пользователей и групп Windows AD

Платформа BI поддерживает аутентификацию Active Directory (AD) при использовании подключаемого модуля безопасности Windows, который по умолчанию добавляется при установке продукта на платформе Windows. Поддержка аутентификации Windows AD означает, что пользователи и группы, созданные в Microsoft Active Directory (2003 и 2008) могут использоваться для аутентификации в платформе BI. Это позволяет системному администратору сопоставить существующие учетные записи AD вместо индивидуальной настройки каждого пользователя и каждой группы в платформе BI.

Планирование обновлений для групп Windows AD

Платформа BI позволяет администраторам планировать обновления для групп и псевдонимов пользователей Windows AD. Эта функция доступна для аутентификации AD с Kerberos или NTLM. СМС также позволяет просматривать время и дату последнего обновления.

Примечание:

Чтобы аутентификация AD работала в платформе BI, нужно настроить способ планирования обновлений для групп и псевдонимов AD.

При создании расписания обновления можно выбрать типы повтора, представленные в следующей таблице.

Тип повтора	Описание
Ежечасно	Обновление будет запускаться каждый час. Вы указываете в какое время должен выполняться объект, а также дату начала и окончания.
Ежедневно	Обновление будет запускаться ежедневно или через указанное количество дней. Можно указать, в какое время объект будет выполняться, а также дату начала и окончания.
Каждую неделю	Обновление будет запускаться каждую неделю. Оно может запускаться один или несколько раз в неделю. Можно указать, в какие дни и в какое время он будет выполняться, а также дату начала и окончания.
Ежемесячно	Обновление будет запускаться каждый месяц или каждые несколько месяцев. Можно указать время выполнения, а также даты начала и окончания.
N-й день месяца	Обновление будет запускаться в определенный день месяца. Можно указать день месяца, время запуска, а также дату начала и окончания.
Первый понедельник месяца	Обновление будет запускаться в первый понедельник каждого месяца. Можно указать время выполнения, а также даты начала и окончания.

Тип повтора	Описание
Последний день месяца	Обновление будет запускаться в последний день каждого месяца. Можно указать время выполнения, а также даты начала и окончания.
X день N-ной недели месяца	Обновление будет запускаться в указанный день указанной недели месяца. Можно указать время выполнения, а также даты начала и окончания.
Календарь	Обновление будет запускаться по датам, указанным в созданном календаре.

Планирование обновления групп AD

Платформа BI использует информацию о пользователях и группах Active Directory (AD). Для сведения объема запросов, отправляемых в AD, к минимуму, подключаемый модуль AD кэширует информацию о группах и их связях между собой, а также об участии пользователей в них. Если конкретное расписание не определено, обновление не выполняется.

Для настройки повтора обновления групп следует использовать СМС. Повтор следует запланировать так, чтобы он отражал частоту изменения сведений об участниках группы.

Планирование обновления псевдонимов пользователей AD

У объектов пользователя могут быть псевдонимы в учетной записи Windows Active Directory (AD). Это позволяет пользователям использовать учетные данные AD для входа в платформу BI. Обновления учетных записей AD распространяются на платформу BI с помощью подключаемого модуля AD. Учетные записи, созданные, удаленные или отключенные в AD будут соответственно созданы, удалены или отключены в платформе BI.

Если не запланировать обновление псевдонимов AD, такое обновление будет выполняться только в следующих случаях:

- Пользователь выполняет вход, его псевдоним AD обновляется.
- Администратор выбирает параметр **Обновить AD и псевдонимы сейчас** в области СМС «Обновление AD по требованию».

Примечание:

Пароли AD не хранятся в псевдонимах пользователей.

7.4.1.1.3 Единый вход с использованием Windows AD

Подключаемый модуль безопасности Windows AD поддерживает единый вход, что разрешает пользователям AD, прошедшим аутентификацию, не вводить свои учетные данные для входа в платформу BI. Требования к единому входу зависят от способа доступа пользователей в платформу: с использованием дополнительного ПО или через веб-браузер. В обоих случаях подключаемый модуль безопасности получает контекст безопасности для пользователя от поставщика аутентификации и предоставляет пользователю активный сеанс платформы BI, если пользователь является членом сопоставленной группы AD.

Наиболее распространенный сценарий подразумевает использование функции единого входа в веб-приложение стартовой панели BI.

Единый вход в базу данных

Подключаемый модуль Windows AD поддерживает единый вход в базу данных. При правильно настроенной аутентификации пользователей AD не требуется вводить данные своей учетной записи для доступа к отчетам из приложения стартовой панели BI.

См. также

- [Использование Windows AD с SiteMinder](#)
- [Настройка аутентификации Windows AD \(Kerberos\) с функцией единого входа Vintela](#)

7.4.2 Подготовка для аутентификации AD (Kerberos)

7.4.2.1 Использование аутентификации Windows AD с Kerberos

В этом разделе описываются задачи по подготовке, которые требуется выполнить, чтобы настроить аутентификацию Kerberos для платформы BI. После выполнения всех задач по подготовке можно перейти к настройке параметров аутентификации Windows AD для Kerberos в подключаемом модуле безопасности Windows AD.

Рекомендуемый рабочий процесс

Для правильной настройки аутентификации Windows AD необходимо выполнить следующие задачи по подготовке:

- Настройка учетной записи службы для запуска платформы BI
- Подготовка серверов платформы BI для аутентификации Windows AD с Kerberos
- Настройка сервера веб-приложений для аутентификации Windows AD с Kerberos.

7.4.2.1.1 Настройка учетной записи службы для аутентификации AD с Kerberos

Для настройки платформы BI на использование аутентификации Kerberos и Windows AD требуется учетная запись службы. Можно создать учетную запись домена или воспользоваться существующей. Учетная запись службы будет использоваться для работы серверов платформы BI.

Примечание:

После настройки учетной записи службы нужно будет назначить этой учетной записи соответствующие права.

Если используется домен Windows 2003 или 2008, также есть возможность настройки ограниченного делегирования.

Настройка учетной записи службы в домене Windows 2003 или 2008

Для успешной реализации аутентификации Windows AD с Kerberos необходимо настроить новую учетную запись службы на контроллере домена. Эта учетная запись службы будет использоваться, в частности, для реализации единого входа пользователей указанной группы Windows AD в стартовую панель BI. Эта задача выполняется на компьютере контроллера домена AD.

1. Создайте новую учетную запись с паролем на контроллере домена или используйте существующую.

Подробные инструкции см. в разделе <http://msdn.microsoft.com/>.

2. Выполните команду `keytab ktpass`, чтобы создать и поместить в нужный каталог файл ярлыков ключей Kerberos.

При этом необходимо указать параметры `ktpass`, перечисленные в следующей таблице:

Параметр	Описание
-out	Имя создаваемого файла ярлыков ключей Kerberos.
-mapuser	Имя учетной записи пользователя, с которой сопоставляется имя администратора доступа к службе (SPN). Это учетная запись, под которой выполняется агент Server Intelligence Agent.
-pass	Задает пароль, используемый учетной записью службы.
-kvno	Задает номер версии ключа, который используется для создания ключа.
-ptype	Задает тип администратора доступа. Задается следующим образом: -ptype KRB5_NT_PRINCIPAL
-crypto	Задает используемый с учетной записью службы тип шифрования. Используйте следующее значение: -crypto RC4-HMAC-NT

Пример.

```
ktpass -out -mapuser sbo.serviceDOMAIN.COM -pass password
-kvno 255 -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

В выходных данных команды `ktpass` должно отображаться подтверждение целевого контроллера домена, а также создания файла ярлыков ключей Kerberos, содержащего совместно используемый секретный ключ. Эта команда также сопоставляет имя администратора доступа с (локальной) учетной записью службы.

3. Выполните команду `setspn -l`, чтобы проверить успешность выполнения команды `ktpass`.

На экран выводится список всех имен администраторов доступа к службе, зарегистрированных для локальной учетной записи службы.

4. Щелкните правой кнопкой мыши учетную запись службы, созданную на шаге 1, и выберите **Свойства > Делегирование**.
5. Выберите пункт **Доверять этому пользователю делегирование служб (только Kerberos)**.
6. Нажмите кнопку **ОК**, чтобы сохранить параметры.

Созданной учетной записи службы необходимо предоставить права, а затем добавить ее в локальную группу администраторов.

Предоставление прав учетной записи службы

Для поддержки Windows AD и Kerberos необходимо предоставить учетной записи службы права на работу в качестве компонента операционной системы. Это необходимо сделать на каждом компьютере с агентом Server Intelligence (SIA) с сервером центрального управления (CMS).

Если требуется реализовать функцию единого входа в базу данных, агент SIA должен включать следующие серверы:

- Сервер обработки Crystal Reports
- Сервер приложений отчетов
- Сервер обработки Web Intelligence

Примечание:

Чтобы реализовать функцию единого входа в базу данных, учетная запись службы должна быть доверенной для делегирования.

Предоставление прав учетной записи службы

1. Щелкните **Пуск > Панель управления > Администрирование > Локальная политика безопасности**.
2. Разверните узел **Локальные политики**, а затем – **Назначение прав пользователя**.
3. Дважды щелкните пункт **Работа в режиме операционной системы**.
4. Нажмите кнопку **Добавить**.
5. Введите имя созданной учетной записи службы и нажмите кнопку **ОК**.
6. Установите флажок **Параметр локальной политики** и нажмите кнопку **ОК**.
7. Повторите описанные выше шаги на всех компьютерах с серверами платформы BI.

Примечание:

После настройки пункта **Работа в режиме операционной системы** обязательно должен быть выбран пункт завершения действующих прав. Обычно для этого требуется перезапуск сервера. Если после перезапуска этот параметр не включен, параметры локальной политики переопределяются параметрами доменной политики.

Добавление учетной записи службы в локальную группу администраторов

Для поддержки Kerberos учетная запись службы должна входить в локальную группу администраторов для каждого сервера с SIA, на котором развернута одна из следующих служб:

- CMS
- Сервер обработки Crystal Reports (требуется только для SSO2DB – единого входа в базу данных)
- Сервер приложений отчетов (требуется только для SSO2DB – единого входа в базу данных)
- Сервер обработки Web Intelligence (требуется только для SSO2DB – единого входа в базу данных)

Примечание:

При использовании единого входа в базу данных требуется учетная запись службы, доверенная для делегирования. Также необходимо обладать правами администратора на сервере.

Добавление учетной записи в группу "Администраторы"

1. На нужном компьютере щелкните правой кнопкой мыши **Мой компьютер** и выберите **Управление**.
2. Перейдите в **Служебные программы > Локальные пользователи и группы > Группы**.
3. Щелкните правой кнопкой группу **Администраторы** и выберите пункт **Добавить в группу**.
4. Нажмите кнопку **Добавить** и введите имя входа учетной записи группы.
5. Чтобы проверить правильность учетной записи, нажмите кнопку **Проверить имена**.
6. Нажмите кнопку **ОК**, а затем нажмите кнопку **ОК** еще раз.
7. Повторите эти шаги для каждого сервера платформы BI, который требуется настроить.

7.4.2.1.2 Подготовка серверов для аутентификации Windows AD с Kerberos

После создания учетной записи службы и ее настройки для аутентификации Windows AD с Kerberos можно запускать каждый агент SIA в развертывании платформы BI под этой учетной записью.

Настройка агента SIA под учетной записью службы

Необходимо выполнить следующие действия для любого агента SIA, который выполняет службы, используемые учетной записью службы, созданной для аутентификации Windows AD с Kerberos.

1. Выберите **Программы > SAP BusinessObjects Enterprise XI 4.0 > SAP BusinessObjects Enterprise > Central Configuration Manager**.
2. В CCM щелкните правой кнопкой мыши Server Intelligence Agent (SIA) и выберите команду **Остановить**.

Примечание:

При остановке агента SIA останавливаются все службы, которыми он управляет.

3. Щелкните SIA правой кнопкой мыши и выберите команду **Свойства**.
4. Очистите флажок **Системная учетная запись**.
5. Введите данные учетной записи службы (*ИМЯ_ДОМЕНА\ИМЯ_СЛУЖБЫ*) и нажмите кнопку **ОК**.
6. Перезапустите SIA.
7. При необходимости повторите шаги 1 – 5 для каждого агента SIA, управляющего службой, которую требуется настроить.

7.4.2.1.3 Подготовка сервера приложений для аутентификации Windows AD (Kerberos)

В этом разделе описаны задачи по настройке Kerberos для использования со следующими серверами приложений:

- Tomcat
- WebSphere
- WebLogic
- Oracle Application Server
- SAP NetWeaver 7.10

В этом разделе содержится следующая информация:

- Рабочий процесс, который относится к конкретному серверу веб-приложений. Этот рабочий процесс является обязательным, поскольку реализация службы аутентификации и авторизации Java (JAAS) различается для разных серверов приложений.
- Подробности процедур для каждого шага процесса.
- Образец файла Krb5.ini для серверов приложений Java.

Обзор

Конкретные процессы настройки Kerberos для сервера веб-приложений могут различаться для разных серверов приложений. Тем не менее, общий процесс настройки Kerberos включает в себя следующие шаги:

- Создание файла конфигурации Kerberos.
- Создание файла конфигурации входа JAAS.

Примечание:

Этот шаг не обязательно выполнять для сервера Java-приложений SAP NetWeaver 7.10. Тем не менее, необходимо добавить LoginModule на сервер SAP NetWeaver.

- Изменение параметров Java.
- Перезапуск сервера Java-приложений.

Создание файла конфигурации Kerberos для SAP NetWeaver, Tomcat, WebLogic, SAP NetWeaver или Oracle

Выполните указанные шаги, чтобы создать файл конфигурации Kerberos, если используется сервер приложений SAP Netweaver 7.10, Tomcat 6, Oracle Application Server или WebLogic.

1. Создайте файл `krb5.ini`, если он отсутствует, и сохраните его в каталоге `C:\WINNT` для Windows.

Примечание:

- Если сервер приложений установлен в UNIX, необходимо использовать один из следующих каталогов:

Solaris: /etc/krb5/krb5.conf

Linux: /etc/krb5.conf

- Этот файл можно сохранить и в другом каталоге, однако в этом случае его расположение необходимо будет указать в параметрах java. Для получения дополнительных сведений о krb5.ini см. раздел <http://docs.sun.com/app/docs/doc/816-0219/6m6njqb94?a=view>.

2. Добавьте в файл конфигурации Kerberos следующую обязательную информацию:

```
[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 =
```

Примечание:

DOMAIN.COM – DNS-имя домена, которое необходимо вводить в верхнем регистре в формате полного доменного имени. kdc – имя хоста контроллера домена. В раздел [realms] можно добавить несколько записей доменов, если пользователи выполняют вход из нескольких доменов. [capath] определяет доверие между доменами из другого леса AD. В приведенном выше примере DOMAIN2.COM – домен из внешнего леса, у него прямое двустороннее транзитивное доверие с DOMAIN.COM. В конфигурации с несколькими доменами в разделе [libdefaults] для параметра default_realm должен быть указан любой из исходных доменов. Рекомендуется использовать домен с максимальным количеством пользователей, аутентификация которых будет выполняться с использованием их учетных записей AD. Если при входе суффикс UPN не вводится, используется значение default_realm. Это значение должно соответствовать параметру **домен по умолчанию** в СМС.

См. также

- [Изменение параметров Java для Kerberos в Tomcat](#)

Создание файла конфигурации Kerberos для сервера приложений WebSphere

1. Создайте файл `krb5.ini`, если он отсутствует, и сохраните его в каталоге `C:\WINNT` для Windows.

Примечание:

Этой файл можно сохранить и в другом каталоге, однако в этом случае его расположение необходимо будет указать в параметрах `java`.

2. Добавьте в файл конфигурации Kerberos следующую обязательную информацию:

```
[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 =
```

Примечание:

- При использовании DES-шифрования измените `rc4-hmac` на `des-cbc-crc`.
- `DOMAIN.COM` – DNS-имя домена, которое необходимо вводить в верхнем регистре в формате полного доменного имени.
- `hostname` – имя хоста контроллера домена.

3. Сохраните и закройте файл.

См. также

- [Изменение параметров Java для Kerberos в WebSphere](#)

Пример файла `Krb5.ini` с несколькими доменами

Ниже приведен пример файла с несколькими доменами.

```
[domain_realm]
; trust relationship: childtest4<->sbopetest3<->sbopetest<->sbopetest2
[libdefaults]
default_realm = SBOPTEST.COM
[realms]
SBOPTEST.COM = {
kdc = VANPGVMBOBJ01.sbopetest.com
}
SBOPTEST2.COM = {
```



```

    kdc = VANPGVMBOBJ05.sboptest2.com
  }
  SBOPTTEST3.COM = {
    kdc = VANPGVMBOBJ07.sboptest3.com
  }
  CHILDTTEST4.SBOPTTEST3.COM = {
    kdc = vanpgvmbobj08.childtest4.sboptest3.com
  }
  [capaths]
  ; for clients in sboptest3 to login sboptest2
  SBOPTTEST3.COM = {
    SBOPTTEST2.COM = SBOPTTEST.COM
  }
  ; for clients in childtest4 to login sboptest2
  CHILDTTEST4.SBOPTTEST3.COM = {
    SBOPTTEST2.COM = SBOPTTEST.COM
    SBOPTTEST2.COM = SBOPTTEST3.COM
  }
}

```

Создание файла конфигурации входа Tomcat или WebLogic JAAS

1. Создайте файл с именем `bscLogin.conf`, если он еще не существует, и сохраните его в каталоге по умолчанию: `C:\WINNT`.

Примечание:

Этот файл можно сохранить в другом месте. Однако при этом его местоположение необходимо будет указать в параметрах `java`.

2. Добавьте в файл конфигурации JAAS `bscLogin.conf` следующий код:

```

com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};

```

3. Сохраните и закройте файл.

Создание файла конфигурации входа Oracle JAAS

1. Найдите файл `jazn-data.xml`.

Примечание:

По умолчанию он находится в каталоге `C:\OraHome_1\j2ee\home\config`. Если сервер Oracle Application Server установлен в другой каталог, найдите файл в соответствующем каталоге.

2. Добавьте в файл между тегами `<jazn-loginconfig>` следующее содержимое:

```

<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. Сохраните и закройте файл `jazn-data.xml`.

Создание файла конфигурации входа в систему WebSphere JAAS

1. Создайте файл с именем `bscLogin.conf`, если он еще не существует, и сохраните его в каталоге по умолчанию: `C:\WINNT`.
2. Добавьте в файл конфигурации JAAS `bscLogin.conf` следующий код:

```
com.businessobjects.security.jgss.initiate {
com.ibm.security.auth.module.Krb5LoginModule required;
};
```

3. Сохраните и закройте файл.

Добавление LoginModule для SAP NetWeaver

Для использования единого входа Kerberos и SAP NetWeaver 7.10 нужно выполнить настройку системы так, как при использовании сервера веб-приложений Tomcat. Нет необходимости создавать файл `bscLogin.conf`.

Когда это сделано, нужно добавить LoginModule и обновить некоторые настройки Java в SAP NetWeaver 7.10.

Для правильного сопоставления `com.sun.security.auth.module.Krb5LoginModule` и `com.businessobjects.security.jgss.initiate` нужно вручную добавить LoginModule в NetWeaver.

1. Откройте "Администратор" NetWeaver с помощью ввода следующего адреса в веб-браузере: `http://<название компьютера>:<порт>/nwa`.
2. Нажмите **Управление конфигурацией > Безопасность > Аутентификация > Модули входа > Изменить**.
3. Добавьте новый модуль входа в систему со следующими сведениями:

Отображаемое имя	Krb5LoginModule
Имя класса	com.sun.security.auth.module.Krb5LoginModule

4. Нажмите кнопку **Сохранить**.
NetWeaver создает новый модуль.
5. Выберите **Компоненты > Изменить**
6. Добавьте новую политику под названием `com.businessobjects.security.jgss.initiate`.
7. В стек аутентификации добавьте модуль входа в систему, который был создан на третьем шаге, и выберите для него параметр **Обязательно**.
8. Подтвердите отсутствие других записей в «Параметры выбранного модуля входа». Если же такие записи есть, удалите их.
9. Нажмите кнопку **Сохранить**.
10. Выполните выход из учетной записи администратора NetWeaver.

Изменение параметров Java для Kerberos в Tomcat

1. В меню **Пуск** выберите **Программы > Tomcat > Tomcat Configuration**.

2. Откройте вкладку **Java**.
3. Добавьте следующие параметры:

```
-Djava.security.auth.login.config=C:\XXXX\bscLogin.conf
-Djava.security.krb5.conf=C:\XXXX\krb5.ini
```

Замените XXXX на каталог, в котором был сохранен файл.

4. Закройте файл конфигурации Tomcat.
5. Перезапустите сервер Tomcat.

Изменение параметров Java для SAP NetWeaver 7.10

1. Найдите инструмент конфигурации Java (по умолчанию расположен в каталоге C:\usr\sap\<NetWeaver ID>\<instance>\j2ee\configtool\) и дважды щелкните файл configtool.bat.
Открывается инструмент конфигурации.
2. Нажмите **Вид > Экспертный режим**.
3. Разверните **Кластер-Шаблон > данных**.
4. Выберите экземпляр, соответствующий серверу NetWeaver (например, **Экземпляр – <system ID><machine name>**).
5. Нажмите **Параметры виртуальной машины**.
6. Выберите элемент **SAP** в списке **Поставщик** и **GLOBAL** в списке **Платформа**.
7. Нажмите **Система**.
8. Добавьте такую информацию в качестве параметров.

java.security.krb5.conf	<путь к файлу krb5.ini с указанием имени файла>
javax.security.auth.useSubjectCredsOnly	false

9. Нажмите кнопку **Сохранить**.
10. Нажмите **Редактор конфигураций**.
11. Выберите **Конфигурации > Безопасность > Конфигурации > com.businessobjects.security.jgss.initiate > Безопасность > Аутентификация**.
12. Нажмите **Режим редактирования**.
13. Щелкните правой кнопкой мыши узел **Аутентификация** и выберите команду **Создать дочерний узел**.
14. Выберите элемент **Ввод значения** в списке сверху.
15. Укажите следующее:

Имя	Create_security_session
Значение	false

16. Нажмите кнопку **Создать**.
17. Закройте окно.
18. Нажмите **Инструмент конфигурации**.
19. Нажмите кнопку **Сохранить**.

После обновления конфигурации необходимо перезапустить сервер NetWeaver.

Изменение параметров Java для Kerberos в WebLogic

При использовании Kerberos с WebLogic в параметрах Java необходимо указать расположение файла конфигурации Kerberos и модуля входа Kerberos.

1. Остановите домен WebLogic, в котором работают приложения платформы BI.
2. Откройте сценарий, запускающий домен WebLogic, в котором работают приложения платформы BI (startWeblogic.cmd для Windows, startWebLogic.sh для UNIX).
3. Добавьте в раздел Java_Options этого файла следующую информацию:

```
set JAVA_OPTIONS=-Djava.security.auth.login.config=C:/XXXX/bscLogin.conf -
Djava.security.krb5.conf=C:/XXX/krb5.ini
```

Замените XXXX на каталог, в котором сохранен файл.

4. Перезапустите домен WebLogic, в котором работают приложения платформы BI.

Изменение параметров Java для Kerberos в Oracle Application Server

При использовании Kerberos с Oracle Application Server в параметрах Java необходимо указать расположение файла конфигурации Kerberos.

1. Выполните вход в консоль администрирования сервера Oracle Application Server.
2. Щелкните имя экземпляра OC4J, в котором работают приложения платформы BI.
3. Выберите свойства сервера.
4. Прокрутите свойства до раздела "Multiple VM Configuration".
5. В разделе "Command Line Options" добавьте в конце текстового поля "Java Options" следующую строку: -Djava.security.krb5.conf=C:/XXXX/krb5.ini (вместо XXXX укажите каталог, где хранится файл).
6. Перезапустите экземпляр OC4J.

Изменение параметров Java для Kerberos в WebSphere

1. Войдите в консоль администрирования WebSphere.

Для IBM WebSphere 5.1 введите `http://servername:9090/admin`. Для IBM WebSphere 6.0 введите `http://servername:9060/ibm/console`

2. Разверните сервер, щелкните "Серверы приложений" и выберите имя сервера приложений, созданного для использования с платформой BI.
3. Перейдите на страницу JVM.

Если используется WebSphere 5.1, для перехода на страницу JVM выполните следующие шаги.

- a. Прокрутите страницу сервера вниз до пункта **Process Definition** (определение процесса) в столбце **Additional Properties** (дополнительные свойства).
- b. Щелкните **Process Definition** (определение процесса).
- c. Прокрутите окно вниз и щелкните **Java Virtual Machine** (виртуальная Java-машина).

Если используется WebSphere 6.0, для перехода на страницу JVM выполните следующие шаги.

- a. На странице сервера выберите **Java and Process Management** (управление Java и процессами).
- b. Выберите **Process Definition** (определение процесса).
- c. Выберите **Java Virtual Machine** (виртуальная Java-машина).

4. Щелкните **Generic JVM arguments** (общие аргументы JVM) и укажите расположение файлов Krb5.ini и bscLogin.conf.

-Djava.security.auth.login.config=C:\XXXX\bscLogin.conf

-Djava.security.krb5.conf=C:\XXXX\krb5.ini

Замените XXXX на каталог, в котором сохранен файл.

5. Щелкните **Применить**, а затем – **Сохранить**.
6. Остановите и перезапустите сервер.

7.4.3 Аутентификация AD с функцией единого входа

7.4.3.1 Параметры для аутентификации Windows AD с функцией единого входа

В платформе BI поддерживается два способа настройки аутентификации Windows AD:

- Функция единого входа Vintela – используется только с Kerberos.
- Функция единого входа SiteMinder – используется только с Kerberos.

Примечание:

Наиболее распространенный сценарий единого входа подразумевает доступ к приложению стартовой панели BI, которое может развертываться только на сервере Java-приложений. Функция единого входа для стартовой панели BI реализуется только с помощью протокола Kerberos.

7.4.3.2 Подготовка для аутентификации Windows AD с функцией единого входа

7.4.3.2.1 Настройка аутентификации Windows AD (Kerberos) с функцией единого входа Vintela

В следующем разделе описываются задачи по настройке платформы BI, которые необходимо выполнить, чтобы реализовать аутентификацию Windows AD и возможность единого входа Vintela.

Примечание:

Задачи по предварительной настройке аутентификации Windows AD и специальные задачи по настройке функции единого входа Vintela необходимо выполнить до того, как будет начата настройка параметров аутентификации Windows AD в CMC.

См. также

- [Настройка учетной записи службы для аутентификации AD с Kerberos](#)
- [Подготовка серверов для аутентификации Windows AD с Kerberos](#)
- [Подготовка сервера приложений для аутентификации Windows AD \(Kerberos\)](#)

7.4.3.2.2 Алгоритм настройки Kerberos и единого входа для стартовой панели BI Java

Чтобы настроить использование аутентификации Windows AD с функцией единого входа Vintela в платформе BI, необходимо выполнить следующие задачи:

1. Создайте и настройте учетную запись службы, которая будет использоваться для функции единого входа Vintela.
2. Настройте развернутую платформу BI на запуск под этой учетной записью.
3. Настройте общие свойства BOE и специальные свойства стартовой панели BI для функции единого входа Vintela.
4. Увеличьте предельный размер заголовка для сервера Java-приложений.
5. Настройте веб-браузеры для использования функции единого входа Vintela.
6. Настройте ограниченное делегирование для функции единого входа Vintela (необязательно).

После выполнения всех этих задач можно настроить параметры аутентификации Windows AD в CMC.

7.4.3.2.3 Настройка учетной записи службы для функции единого входа Vintela

Для успешной функции единого входа Vintela для аутентификации Windows AD необходимо настроить новую учетную запись службы на контроллере домена. Эта учетная запись службы будет использоваться, в частности, для реализации единого входа пользователей указанной группы Windows AD в стартовую панель BI. Эта задача выполняется на компьютере контроллера домена AD. Приведенные ниже шаги с 1 по 5 обязательны для использования Windows AD с Kerberos. Шаги 6 и 7 выполняются только при настройке функции единого входа Vintela.

1. Создайте новую учетную запись службы с паролем на основном контроллере домена.
2. Выполните команду установки файла ярлыков ключей Kerberos (`ktpass`) для создания соответствующего файла.

При этом необходимо указать параметры `ktpass`, перечисленные в следующей таблице:

Параметр	Описание
-out	Имя создаваемого файла ярлыков ключей Kerberos.
-princ	Имя администратора доступа к учетной записи службы. Этот параметр задается в формате имени администратора доступа к службе (SPN). Примечание: Для этого имени учитывается регистр. Имя SPN всегда включает имя компьютера хоста, на котором выполняется экземпляр службы. Совет: Имя SPN должно быть уникальным в лесу, в котором оно зарегистрировано. Для проверки можно использовать инструмент с поддержкой <code>Windows Ldp.exe</code> , с помощью которого выполняется поиск SPN.
-mapuser	Имя учетной записи пользователя, с которой сопоставляется имя, заданное описываемым выше параметром <code>-princ</code> . Это учетная запись, под которой выполняется агент Server Intelligence Agent.
-pass	Задает пароль, используемый учетной записью службы.
-kvno	Задает номер версии ключа, который используется для создания ключа.
-ptype	Задает тип администратора доступа. Задается следующим образом: <code>-ptype KRB5_NT_PRINCIPAL</code>
-crypto	Задает используемый с учетной записью службы тип шифрования. Используйте следующее значение: <code>-crypto RC4-HMAC-NT</code>

Пример.

```
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
```

В выходных данных команды `ktpass` должно отображаться подтверждение целевого контроллера домена, а также создания файла ярлыков ключей Kerberos, содержащего совместно используемый секретный ключ. Эта команда также сопоставляет имя администратора доступа с (локальной) учетной записью службы.

3. Выполните команду `setspn -l`, чтобы проверить успешность выполнения команды `ktpass`. На экран выводится список всех имен администраторов доступа к службе, зарегистрированных для локальной учетной записи службы.
4. Щелкните правой кнопкой мыши учетную запись службы, созданную на шаге 1, и выберите **Свойства > Делегирование**.
5. Выберите пункт **Доверять этому пользователю делегирование служб (только Kerberos)**.
6. Выполните команду `setspn -a`, чтобы добавить имена администраторов доступа к службе HTTP для учетной записи службы, созданной на шаге 1. Укажите имена администраторов доступа к службе для сервера, полное доменное имя сервера, а также IP-адрес компьютера, на котором развернута стартовая панель BI.

Пример.

```
setspn -a HTTP/servername servicename
setspn -a HTTP/servernamedomain servicename
setspn -a HTTP/<ip address of server> servicename
```

Здесь *servername* – это имя сервера, на котором развернута стартовая панель BI, а *servernamedomain* – полное доменное имя последнего.

7. Выполните команду `setspn -l servicename`, чтобы убедиться, что имена администраторов доступа к службе HTTP были добавлены для учетной записи службы.

В выходных данных команды должны отображаться все зарегистрированные имена администраторов доступа к службе, как показано ниже:

```
Registered ServicePrincipalNames for
CN=bo.service,OU=boe,OU=BIP,OU=PG,DC=DOMAIN,DC=com:
HTTP/<ip address of server>
HTTP/servername.DOMAIN.com
HTTP/servername
servername/servicenameDOMAIN.com
```

Для учетной записи службы добавлены все необходимые имена администраторов доступа к службе и создан нужный файл ярлыков ключей.

Для работы функции единого входа Vintela необходимо настроить серверы платформы BI, изменить свойства стартовой панели BI и скопировать файл ярлыков ключей в соответствующий каталог.

7.4.3.2.4 Подготовка серверов к использованию функции единого входа Vintela

Необходимо убедиться, что компьютер, на котором выполняется развертывание серверов платформы BI, добавлен в основной домен и при этом добавлены все необходимые суффиксы DNS.

Для выполнения следующей задачи используется файл ярлыков ключей, созданный для аутентификации Windows AD с Kerberos.

1. Скопируйте файл ярлыков ключей Kerberos в папку на компьютере, на котором размещаются серверы платформы BI.
2. Добавьте учетную запись службы Kerberos в группу администраторов на хосте.
Используйте следующий формат имени учетной записи: *ИМЯ_ДОМЕНА\имя_службы*.
3. Добавьте учетную запись службы Kerberos в следующие системные права в локальную политику безопасности консоли управления MMC:

Системное право	Влияние
Работа в режиме операционной системы	Позволяет процессу олицетворять любого пользователя без аутентификации.
Вход в систему в качестве пакетного задания	Позволяет пользователю входить в систему с использованием функции очереди пакетной обработки.
Вход в систему в качестве службы	Позволяет учетной записи службы зарегистрировать процесс в качестве службы.
Заменить маркер уровня процесса	Позволяет учетной записи вызывать API-интерфейс CreateProcessAsUser(), с помощью которого службы могут запускать друг друга.

Серверы платформы BI необходимо запускать под учетной записью службы.

4. Выберите **Программы > SAP BusinessObjects Enterprise XI 4.0 > SAP BusinessObjects Enterprise > Central Configuration Manager**.
5. В CCM щелкните правой кнопкой мыши Server Intelligence Agent (SIA) и выберите команду **Остановить**.
6. Щелкните SIA правой кнопкой мыши и выберите команду **Свойства**.
7. Очистите флажок **Системная учетная запись**.
8. Введите данные учетной записи Kerberos (*ИМЯ_ДОМЕНА\имя_службы*), указанные на шаге 2, и нажмите кнопку **ОК**.
9. Перезапустите SIA.

Для завершения настройки функции единого входа Vintela необходимо выполнить следующие задачи:

- Подготовьте свойства сервера веб-приложений и стартовой панели BI для функции единого входа Vintela.
- Настройте подключаемый модуль безопасности Windows AD для поддержки аутентификации Windows AD и функции единого входа Vintela.

7.4.3.2.5 Включение единого входа Vintela для стартовой панели BI и OpenDocument

Этот алгоритм можно использовать и для веб-приложений стартовой панели BI, и для OpenDocument. Помимо указания настроек единого входа Vintela для подключаемого модуля безопасности Windows AD настройки Vintela нужно указать для свойств файла BOE.war.

1. Откройте пользовательскую папку веб-приложения BOE на компьютере, на котором размещается сервер веб-приложений.

Если используется сервер веб-приложений Tomcat, входящий в комплект установки платформы BI, можно непосредственно перейти в следующую папку:

```
C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom\
```

Совет:

Если используется сервер веб-приложений, не поддерживающий прямой доступ к развернутым веб-приложениям, для изменения веб-приложения BOE можно использовать следующую папку в установке продукта.

```
<INSTALLDIR>\SAP BusinessObjects Enterprise XI  
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\.
```

Позднее потребуется повторно развернуть измененное веб-приложение BOE.

2. Создайте новый файл.

Примечание:

Воспользуйтесь программой "Блокнот" или любым другим текстовым редактором.

3. Введите следующую информацию.

```
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
```

Примечание:

Параметры `idm.realm` и `idm.princ` должны иметь допустимые значения. Значение параметра `idm.realm` должно совпадать со значением, указанным при настройке `default_realm` в файле `krb5.ini`. Значение должно быть указано в верхнем регистре. Параметр `idm.princ` определяет имя администратора доступа к службе (SPN), которое используется для учетной записи единого входа Vintela.

4. Если принято решение использовать файл ярлыков ключей, добавьте параметр ярлыков ключей и укажите путь к файлу, как показано в следующем примере:

```
idm.keytab=C:/WIN/filename.keytab
```

Если использовать ограниченное делегирование для аутентификации Windows AD с функцией единого входа Vintela не требуется, пропустите следующее действие.

5. Чтобы использовать ограниченное делегирование, добавьте следующее:

```
idm.allowS4U=true
```

6. Закройте этот файл и сохраните его с именем:

global.properties

Примечание:

Убедитесь в том, что файл с выбранным именем не сохраняется с каким-либо другим расширением, таким как .txt.

7. Создайте другой файл в этом же каталоге. Сохраните файл под именем `OpenDocument.properties` или `BIlaunchpad.properties` в зависимости от предъявляемых требований.
8. Введите следующее выражение:

```
authentication.default=secWinAD
cms.default=[enter your cms name]:[Enter the CMS port number]
```

Например:

```
authentication.default=secWinAD
cms.default=mycms:6400
```

9. Сохраните и закройте файл.
10. Перезапустите сервер веб-приложений.

Новые свойства вступают в силу только после повторного развертывания веб-приложения BOE на компьютере, на котором запущен сервер веб-приложений. Воспользуйтесь WDeploy для повторного развертывания BOE на сервере веб-приложений. Для получения дополнительных сведений об использовании Wdeploy для отмены развертывания веб-приложений см. *Руководство по развертыванию веб-приложений SAP BusinessObjects Business Intelligence Platform*.

Примечание:

Если в развертывании используется брандмауэр, обязательно откройте все необходимые порты. В противном случае веб-приложения не смогут подключаться к серверам платформы BI.

См. также

- [Пример файла Krb5.ini с несколькими доменами](#)
- [Подготовка сервера приложений для аутентификации Windows AD \(Kerberos\)](#)

7.4.3.2.6 Увеличение ограничения на размер заголовка для Tomcat

Active Directory создает маркер Kerberos, который используется в процессе аутентификации. Этот маркер хранится в HTTP-заголовке. У сервера Java-приложений настроен размер заголовка по умолчанию HTTP. Чтобы избежать ошибок, минимальный размер по умолчанию должен составлять 16384 байт. (Для некоторых систем может потребоваться больший размер. Для получения дополнительных сведений см. рекомендации корпорации Майкрософт на узле поддержки (<http://support.microsoft.com/kb/327825>).)

1. На компьютере, на котором установлен сервер Tomcat, откройте файл `server.xml`.
В Windows этот файл находится в каталоге `<TomcatINSTALLDIR>/conf`
 - Если используется версия Tomcat, установленная вместе с платформой BI в Windows, и местоположение установки по умолчанию не менялось,

замените <TomcatINSTALLDIR> на C:\Program Files (x86)\SAP BusinessObjects\Tomcat\.

- Если используется другой поддерживаемый сервер веб-приложений, обратитесь к документации по серверу веб-приложений, чтобы узнать путь, который следует указать.

2. Найдите соответствующий тег <Connector ...> для настроенного номера порта.

Если используется порт по умолчанию 8080, найдите тег <Connector ...> со значением порта =«8080».

Например:

```
<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. Добавьте в тег <Connector ...> следующее значение:

```
maxHttpHeaderSize="16384"
```

Например:

```
<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. Сохраните и закройте файл server.xml.

5. Перезапустите сервер Tomcat.

Примечание:

В случае использования других серверов Java-приложений см. документацию соответствующего сервера.

7.4.3.2.7 Настройка веб-браузеров

Для поддержки единого входа Kerberos необходимо настроить клиенты платформы BI. Это подразумевает настройку веб-браузера Internet Explorer (IE) на клиентских компьютерах.

Настройка браузера Internet Explorer на клиентских компьютерах

1. На клиентском компьютере откройте окно браузера IE.
2. Включение встроенной проверки подлинности Windows.
 - a. В меню **Сервис** выберите команду **Свойства браузера**.
 - b. Выберите вкладку **Дополнительно**.
 - c. Прокрутите окно до раздела **Безопасность**, установите флажок **Разрешить встроенную проверку подлинности Windows** и нажмите кнопку **Применить**.
3. Добавьте сервер Java-приложений или URL-адрес в список доверенных узлов. Можно ввести полное доменное имя узла.

- a. В меню **Сервис** выберите команду **Свойства браузера**.
 - b. Откройте вкладку **Конфиденциальность**.
 - c. Нажмите кнопку **Узлы** и выберите пункт **Дополнительно**.
 - d. Выберите или введите сайт и нажмите кнопку **Добавить**.
 - e. Нажимайте несколько раз кнопку **ОК**, чтобы закрыть окно свойств браузера.
4. Чтобы изменения вступили в силу, закройте окно браузера Internet Explorer и откройте его снова.
 5. Повторите описанные выше шаги на каждом клиентском компьютере с платформой BI.

Настройка браузер Firefox на клиентских компьютерах

1. Измените network.negotiate-auth.delegation-uris

- a. На клиентском компьютере откройте окно браузера Firefox.
- b. Введите в строке для URL-адресов about:config. Откроется список настраиваемых свойств.
- c. Дважды щелкните **network.negotiate-auth.delegation-uris**, чтобы отредактировать свойство.
- d. Введите URL-адрес, который будет использоваться для доступа к стартовой панели BI. Например, если стартовая панель BI имеет URL-адрес `http://machine.domain.com:8080/BOE/BI`, необходимо ввести `http://machine.domain.com`.

Примечание:

При вводе нескольких URL-адресов их следует разделять запятыми. Например, `http://machine.domain.com,machine2.domain.com`.

- e. Нажмите кнопку **ОК**.

2. Измените network.negotiate-auth.trusted-uris

- a. На клиентском компьютере откройте окно браузера Firefox.
- b. Введите в строке для URL-адресов about:config. Откроется список настраиваемых свойств.
- c. Дважды щелкните **network.negotiate-auth.delegation-uris**, чтобы отредактировать свойство.
- d. Введите URL-адрес, который будет использоваться для доступа к InfoView. Например, если стартовая панель BI имеет URL-адрес `http://machine.domain.com:8080/BOE/BI`, необходимо ввести `http://machine.domain.com`.

Примечание:

При вводе нескольких URL-адресов их следует разделять запятыми. Например, `http://machine.domain.com,machine2.domain.com`.

- e. Нажмите кнопку **ОК**.

3. Чтобы изменения вступили в силу, закройте окно браузера Firefox и откройте его снова.
4. Повторите описанные выше шаги на каждом клиентском компьютере с платформой BI.

7.4.3.2.8 Настройка ограниченного делегирования для функции единого входа Vintela

Для аутентификации AD с функцией единого входа Vintela применение ограниченного делегирования не обязательно. Оно является обязательным в тех сценариях развертывания, в которых используется единый вход в системную базу данных.

1. На компьютере контроллера домена AD откройте оснастку Active Directory «Пользователи и компьютеры».
2. Щелкните правой кнопкой мыши учетную запись службы, созданную для функции единого входа Vintela, а затем выберите **Свойства > Делегирование**.
3. Выберите пункт **Доверять этому пользователю делегирование указанных служб**.
4. Выберите параметр **Использовать только Kerberos**.
5. Выберите команду **Добавить > Пользователи и компьютеры**.
6. Введите имя учетной записи службы (используется для функции единого входа Vintela) и нажмите кнопку **ОК**.
Отображается список служб.
7. Выберите следующие службы и нажмите кнопку **ОК**.
 - Служба HTTP
 - Служба, используемая для запуска агента Service Intelligence Agent (SIA) на компьютере, на котором размещается платформа BI.Службы добавляются в список служб, которые могут быть делегированы для учетной записи (функция единого входа Vintela).

Чтобы учитывать это изменение, необходимо изменить свойства веб-приложения. Откройте файл BOE global.properties на сервере веб-приложений. Добавьте следующие команды и перезапустите сервер веб-приложений.

```
idm.allowS4U=true
```

7.4.3.3 Использование SiteMinder

7.4.3.3.1 Использование Windows AD с SiteMinder

В данном разделе описано использование AD и SiteMinder. SiteMinder – это средство доступа и аутентификации от стороннего производителя, которое можно использовать с подключаемым модулем безопасности AD для единого входа в платформу BI. SiteMinder можно использовать с Kerberos.

Перед настройкой аутентификации Windows AD для работы с SiteMinder убедитесь, что установлены и настроены ресурсы управления удостоверениями SiteMinder. Подробнее о средстве SiteMinder и его установке см. в документации SiteMinder.

Чтобы включить единый вход AD с использованием SiteMinder, необходимо выполнить еще два действия:

- Настроить подключаемый модуль AD на использование единого входа с SiteMinder
- Настройка свойств SiteMinder для веб-приложения BOE

Примечание:

Администратор SiteMinder должен включить поддержку агентов версии 4.x. Это должно быть сделано независимо от используемой поддерживаемой версии SiteMinder. Подробнее о конфигурации SiteMinder см. документацию по средству SiteMinder.

Изменение файла свойств BOE для аутентификации Windows AD с SiteMinder

Дополнительно к указанию настроек SiteMinder для подключаемого модуля безопасности Windows AD настройки SiteMinder нужно указать для свойств WAR-файла BOE.

1. Перейдите в следующий каталог в папке установки платформы BI:

```
<INSTALLDIR>\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\
```

2. Создайте новый файл.

Примечание:

Воспользуйтесь программой "Блокнот" или любым другим текстовым редактором.

3. Закройте этот файл и сохраните его под следующим именем:

```
BIlaunchpad.properties
```

4. Введите следующее выражение:

```
sso.enabled=true
siteminder.authentication=secWinAD
siteminder.enabled=true
```

5. Закройте этот файл и сохраните его с именем:

```
global.properties
```

Примечание:

Убедитесь в том, что файл с выбранным именем не сохраняется с каким-либо другим расширением, таким как .txt.

6. Создайте другой файл в этом же каталоге.

7. Введите следующее выражение:

```
authentication.default=secWinAD
cms.default=[enter your cms name]:[Enter the CMS port number]
```

Например:

```
authentication.default=LDAP
cms.default=mycms:6400
```

8. Закройте этот файл и сохраните его с именем:

```
BIlaunchpad.properties
```

Новые свойства вступают в силу только после повторного развертывания файла BOE.war на компьютере, где работает сервер веб-приложений. Воспользуйтесь Wdeploy для повторного развертывания WAR-файла на сервере веб-приложений. Для получения дополнительных сведений об использовании Wdeploy для отмены развертывания веб-приложений см. *Руководство по развертыванию веб-приложений SAP BusinessObjects Business Intelligence Platform*.

Отключение SiteMinder

Если требуется запретить настройку SiteMinder или отключить его после настройки в СМС, измените файл конфигурации сети для стартовой панели BI.

Отключение SiteMinder для клиентов Java

Помимо отключения параметров SiteMinder для подключаемого модуля безопасности Windows AD нужно отключить параметры SiteMinder для файла BOE.war на сервере веб-приложений.

1. Перейдите в следующий каталог в папке установки платформы BI:

```
<INSTALLDIR>\SAP BusinessObjects Enterprise XI  
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\
```

2. Откройте файл `global.properties`.
3. Измените значение параметра `siteminder.enabled` на "false".

```
siteminder.enabled=false
```

4. Сохраните изменения и закройте файл.

Изменения вступят в силу только после повторного развертывания файла `BOE.war` на компьютере, где работает сервер веб-приложений. Воспользуйтесь Wdeploy для повторного развертывания WAR-файла на сервере веб-приложений. Для получения дополнительных сведений об использовании Wdeploy для отмены развертывания веб-приложений см. *Руководство по развертыванию веб-приложений SAP BusinessObjects Business Intelligence Platform*.

7.4.4 Сопоставление групп AD и настройка аутентификации AD

7.4.4.1 Сопоставление пользователей и групп AD и настройка подключаемого модуля безопасности Windows AD

Перед настройкой аутентификации Windows AD для работы с заданным типом аутентификации сначала требуется выполнить все необходимые задачи по подготовке. Подробнее см. раздел "Связанные разделы" ниже.

Чтобы пользователи AD могли проходить аутентификацию, независимо от используемого протокола необходимо выполнить указанные ниже действия. Выполните шаги 1–8 приведенной ниже процедуры для импорта групп AD в платформу BI.

1. Перейдите в область управления «Аутентификация» в СМС.
2. Дважды щелкните **Windows AD**.

3. Установите флажок **Включить Windows Active Directory (AD)**.
4. В области **Сводка по настройке Windows AD** щелкните ссылку возле **Имя администрирования для AD**.

Примечание:

До настройки подключаемого модуля безопасности Windows AD эта ссылка отображается в виде двойных кавычек. После сохранения конфигурации в ссылке будут указаны имена администрирования для AD.

5. Введите имя и пароль включенной учетной записи пользователя домена. Платформа BI будет использовать эту учетную запись для запроса данных в AD.

Для учетных данных администратора можно использовать один из следующих форматов:

- Имя NT (Имя_домена\имя_пользователя)
- UPN (пользователь@доменное_имя_DNS)

Платформа BI никогда не изменяет, не добавляет содержимое в AD и не удаляет его. Информация только считывается, поэтому требуются соответствующие права.

Примечание:

Аутентификация AD не будет работать, если учетная запись AD, используемая для обращения в каталог AD, становится недействительной (например, если пароль учетной записи изменяется или истекает срок его действия, или если учетная запись отключается).

6. Заполните поле **Домен AD по умолчанию**.

Примечание:

- Пользователей из домена по умолчанию можно сопоставлять без указания имени домена в качестве префикса.
- Если ввести имя домена AD по умолчанию, пользователям из этого домена можно будет не указывать имя домена AD при входе в платформу BI с использованием аутентификации AD.

7. В области «Отображенные группы членов AD» введите домен\группа AD в поле **Добавить группу AD (домен/группа AD)**.

Сопоставление групп можно выполнять с использованием одного из следующих форматов:

- Имя учетной записи диспетчера учетных записей безопасности (SAM) (также называется именем NT (Имя_домена\имя_группы))
- DN (cn=имя_группы,, dc=имя_домена, dc=com)

Примечание:

Если требуется сопоставить локальную группу, можно использовать только формат имени NT (\\Имя_сервера\имя_группы). Службы AD не поддерживают локальных пользователей. Это означает, что локальные пользователи, принадлежащие сопоставленной локальной группе, не будут сопоставлены в платформе BI. Поэтому у них не будет доступа к системе.

8. Нажмите кнопку **Добавить**.

Группа будет добавлена в список.

Если требуется импортировать учетные записи групп AD, и при этом не нужно настраивать параметры аутентификации AD или обновления групп AD, шаги с 9 по 18 можно пропустить.

9. Если требуется настроить единый вход, выберите пункт **Включить единую регистрацию для выбранного режима аутентификации**.

Примечание:

Если выбран этот параметр, необходимо настроить общие свойства веб-приложения BOE и свойства стартовой панели BI, чтобы реализовать функцию единого входа.

10. Выберите параметр в области «Синхронизация учетных данных», чтобы активировать и обновить учетные данные источника данных пользователя AD во время регистрации. Это синхронизирует источник данных с текущими учетными данными пользователя.
11. В области **Параметры SiteMinder** страницы можно настроить использование SiteMinder в качестве функции единого входа для аутентификации AD с использованием Kerberos.

Примечание:

В качестве используемой функции единого входа можно настроить либо Vintela, либо SiteMinder, но не оба этих компонента одновременно. Если необходимо настроить параметры SiteMinder, удалите любые записи в поле **Имя администратора доступа к службе** (шаг 9б).

- a. Щелкните **Отключено**.

Откроется страница настройки Windows AD SiteMinder.

Примечание:

Если подключаемый модуль Windows AD не настроен, будет отображено предупреждение и запрос на продолжение. Нажмите кнопку **ОК**.

- b. Щелкните **Использовать единую регистрацию SiteMinder**.
- c. В поле «Хост сервера политик» введите имя каждого из серверов политик и нажмите кнопку **Добавить**.
- d. Для каждого хоста сервера политик укажите номера портов **учета, аутентификации и авторизации**.
- e. Введите **Имя агента** и **Совместно используемый секретный ключ**. Введите **Совместно используемый секретный ключ** еще раз.

Примечание:

Администратор SiteMinder должен включить поддержку агентов версии 4.x. Это должно быть сделано независимо от используемой поддерживаемой версии SiteMinder. Для получения дополнительных сведений о средстве SiteMinder и его установке см. в документации SiteMinder.

- f. Нажмите кнопку **Обновить**, чтобы сохранить данные и вернуться на главную страницу аутентификации AD.
12. В области «Параметры псевдонима AD» укажите способ добавления и обновления новых псевдонимов в платформе BI.
- a. В пункте «Параметры нового псевдонима» выберите способ сопоставления новых псевдонимов учетным записям Enterprise. Выберите один из перечисленных ниже вариантов.
- **Назначать каждый новый псевдоним AD учетной записи пользователя с таким же именем**

Данный вариант используется в случае, когда известно, что у пользователей есть учетная запись Enterprise с таким же именем. То есть псевдонимы AD будут назначены существующим пользователям (включена функция автоматического создания псевдонимов). Пользователи, у которых нет учетной записи Enterprise, или для которых имя учетной записи Enterprise не совпадает с именем учетной записи AD, добавляются в качестве новых пользователей.

- **Создавать учетную запись пользователя для каждого нового псевдонима AD.**

Данный параметр используется в случае, когда необходимо создавать учетную запись для каждого пользователя.

- b. В поле «Параметры обновления псевдонимов» выберите способ управления обновлением псевдонимов для учетных записей Enterprise. Выберите один из перечисленных ниже вариантов.

- **Создавать новые псевдонимы при обновлении псевдонимов**

Данный вариант используется для автоматического создания псевдонима для каждого пользователя AD, сопоставленного в платформе BI. Новые учетные записи AD добавляются для пользователей без учетных записей платформы BI или для всех пользователей, если был выбран вариант "Создать новую учетную запись для каждого нового псевдонима AD" и была нажата кнопка **Обновить**.

- **Создавать новые псевдонимы только при входе пользователя в систему**

Данный вариант используется в случае, когда сопоставляемый каталог AD содержит много пользователей, но только некоторые из них будут использовать платформу BI. Платформа не создает псевдонимы и учетные записи Enterprise для пользователей автоматически. Вместо этого программа создает псевдонимы (и учетные записи, при необходимости) только для пользователей, которые входят в платформу BI.

- c. В поле «Параметры нового пользователя» укажите способ создания пользователей, выбрав один из следующих вариантов.

Если лицензия платформы SAP BusinessObjects Business Intelligence основана на ролях пользователей, выберите один из перечисленных ниже параметров:

- **Пользователь BI Viewer**

Учетные записи новых пользователей создаются с ролью BI Viewer. Доступ к приложениям платформы BI для всех учетных записей роли BI Viewer определяется в лицензионном соглашении. Пользователи ограничены доступом к рабочим процессам приложений, которые определены для роли BI Viewer. Права доступа обычно ограничены просмотром документов Business Intelligence. Эта роль обычно подходит для пользователей, которые используют контент через приложения платформы BI.

- **Пользователь аналитики BI**

Для новых учетных записей пользователя настраивается роль BI Analyst. Доступ к платформе BI для всех учетных записей роли BI Analyst определяется в лицензионном соглашении. Пользователи могут обращаться ко всем рабочим процессам приложений, которые определены для роли BI Analyst. Права доступа включают просмотр и изменение документов Business Intelligence. Эта роль обычно подходит для пользователей, которые создают и изменяют контент для приложений платформы BI.

Если лицензия платформы SAP BusinessObjects Business Intelligence не основана на ролях пользователей, выберите один из перечисленных ниже параметров:

- **Новые пользователи создаются как именованные пользователи**

Новые учетные записи пользователей настраиваются на использование именованных пользовательских лицензий. Именованные пользовательские лицензии связаны с конкретными пользователями и позволяют им входить в систему, используя имя пользователя и пароль. Это дает именованным пользователям право доступа к системе независимо от того, сколько других пользователей выполнили вход. Для каждой учетной записи, созданной с использованием данного параметра, должна существовать именованная пользовательская лицензия.

- **Новые пользователи создаются как конкурентные пользователи**

Новые учетные записи пользователей настраиваются на использование конкурентных пользовательских лицензий. Лицензии на одновременный доступ указывают количество человек, которые могут подключиться к платформе BI одновременно. Это очень гибкий тип лицензий, так как небольшое их количество поддерживает широкую пользовательскую базу. Например, в зависимости от того, как часто и как долго пользователи работают с системой, лицензия на одновременный доступ для 100 пользователей может поддерживать 250, 500 или 700 пользователей.

13. Для настройки способа обновления псевдонимов AD щелкните **Запланировать обновления псевдонимов AD.**

- В диалоговом окне «Расписание» выберите в списке **Запустить объект** тип повторения.
- Задайте любые другие требуемые установки планирования.
- Щелкните **Запланировать**.

При обновлении псевдонимов также обновляются данные групп.

14. В области «Параметры привязки атрибутов» можно указать приоритет привязки атрибутов для подключаемого модуля AD:

- Щелкните поле **Импортировать полное имя и адрес электронной почты**.
Полные имена и описания, используемые в учетных записях AD, импортируются и сохраняются в пользовательских объектах в платформе BI.
- Укажите значение для параметра **Установка приоритета для привязки атрибута AD относительно других привязок атрибутов**.

Примечание:

Если задано значение «1», в сценариях, в которых включены AD и другие подключаемые модули (LDAP и SAP), приоритет имеют атрибуты AD. Если задано значение «3», приоритет имеют атрибуты из других подключаемых модулей.

15. Обновление данных групп AD можно настроить в области «Параметры группы AD».

- Щелкните **Запланировать обновления групп AD**.
Откроется диалоговое окно «Расписание».
- В списке **Запустить объект** выберите тип повторения.
- Задайте любые другие требуемые установки планирования.
- Щелкните **Запланировать**.

Система запланирует обновление и запустит его в соответствии с указанной в расписании информацией. Следующее запланированное обновление для учетных записей групп можно видеть в пункте «Параметры группы AD».

16. Чтобы выбрать объекты для обновления, воспользуйтесь параметрами в области «Обновление AD по требованию». Можно выбрать один из следующих вариантов:

- **Обновить группы AD сейчас**

Выберите данный вариант, если требуется обновить группы AD. Обновление будет выполнено после нажатия **Обновить**.

Примечание:

Этот параметр влияет на все запланированные обновления группы AD. Следующее запланированное обновление группы AD указано в пункте «Параметры группы AD».

- **Обновить группы AD и псевдонимы сейчас**

Выберите данный вариант, если требуется обновить группу AD и псевдонимы пользователей. Обновление будет выполнено после нажатия **Обновить**.

Примечание:

Этот параметр влияет на все запланированные обновления группы AD. Следующие запланированные обновления указаны в пунктах «Параметры группы AD» и «Параметры псевдонимов AD».

- **Не обновлять группы и псевдонимы AD сейчас**

Если щелкнуть **Обновить**, ни группы, ни псевдонимы пользователей не будут обновлены.

Примечание:

Этот параметр влияет на все запланированные обновления группы или псевдоним. Следующие запланированные обновления указаны в пунктах «Параметры группы AD» и «Параметры псевдонимов AD».

17. Нажмите кнопку **Обновить**.

18. Нажмите кнопку **ОК**.

См. также

- [Единый вход с использованием Windows AD](#)
- [Использование Windows AD с SiteMinder](#)
- [Использование аутентификации Windows AD с Kerberos](#)

7.4.5 Устранение неполадок с аутентификацией Windows AD

7.4.5.1 Устранение неполадок с конфигурацией

Описанные ниже шаги могут помочь при возникновении проблем с настройкой Kerberos.

- Включение регистрации событий
- Тестирование конфигурации Java SDK Kerberos

7.4.5.1.1 Включение регистрации событий

1. В меню **Пуск** выберите **Программы > Tomcat > Tomcat Configuration**
2. Откройте вкладку **Java**.
3. Добавьте следующие параметры:

```
-Dcrystal.enterprise.trace.configuration=verbose  
-sun.security.krb5.debug=true
```

При этом будет создан файл журнала в следующем каталоге:

```
C:\Documents and Settings\<user name>\.businessobjects\jce_verbose.log
```

7.4.5.1.2 Тестирование конфигурации Java Kerberos

- Выполните указанную ниже команду, чтобы протестировать конфигурацию Kerberos (здесь `servact` – учетная запись службы и домен, с которыми работает CMS, `password` – пароль этой учетной записи службы).

```
<Install Directory>\SAP Business Objects Enterprise XI 4.0\win64_64\jdk\bin servact@TESTM03.COM Password
```

Например:

```
C:\Program Files\SAP BusinessObjects\  
SAP Business Objects Enterprise XI 4.0\win64_64\jdk\bin\  
servact@TESTM03.COM Password
```

Если неполадки не устранены, проверьте, чтобы регистр, в котором введен домен и имя администратора доступа к службе, совпадали с указанными в Active Directory.

7.4.5.1.3 Ошибка входа в результате различия имен AD UPN и SAM

Идентификаторы пользователей Active Directory успешно сопоставлены платформе BI. Несмотря на это, им не удастся успешно выполнить вход в СМС или стартовую панель BI с использованием аутентификации Windows AD и Kerberos в следующем формате: `DOMAIN\ABC123`

Эта проблема может возникать в том случае, когда пользователь настроен в Active Directory с использованием несовпадающих UPN- и SAM-имен. Ниже приведен пример, в котором возможно возникновение проблемы:

- UPN – `abc123@company.com`, а SAM-имя – `DOMAIN\ABC123`.
- UPN – `jsmith@company`, а SAM-имя – `DOMAIN\johnsmith`.

Эту проблему можно устранить двумя способами:

- Пользователи должны выполнять вход с использованием UPN-имени, а не SAM-имени.
- SAM-имя учетной записи и UPN-имя должны совпадать.

7.4.5.1.4 Ошибка предварительной аутентификации

Пользователь, который раньше выполнял вход, больше не может успешно выполнять вход. Пользователю будет отображаться следующая ошибка: "Данные учетной записи не распознаны". В журналах ошибок Tomcat можно найти следующую ошибку: "Pre-authentication information was invalid (24)" (данные предварительной аутентификации недействительны)

Это может возникать по причине того, что база данных пользователей Kerberos не получила изменения, внесенные в UPN-имя в AD. Это может означать рассинхронизацию базы данных пользователей Kerberos и данных AD.

Для устранения данной проблемы выполните сброс пароля пользователя в AD. Это обеспечит правильность распространения изменений.

Примечание:

Эта проблема не возникает в J2SE 5.0.

7.5 Аутентификация SAP

7.5.1 Настройка аутентификации SAP

В этом разделе описаны способы настройки аутентификации платформы BI для среды SAP.

Аутентификация SAP позволяет пользователям SAP выполнить вход в платформу BI, используя свои имена пользователей и пароли, не сохраняя эти пароли в платформе BI. Аутентификация SAP также позволяет сохранить информацию о ролях пользователей в SAP и использовать ее в платформе BI для назначения прав на выполнение административных задач или доступ к содержимому.

Доступ к приложению аутентификации SAP

После установки аутентификации SAP необходимо предоставить платформе BI информацию о вашей SAP-системе. Специальное веб-приложение доступно из главного инструмента администрирования платформы BI, Central Management Console (CMC). Для доступа с домашней страницы CMC нажмите **Аутентификация**.

Аутентификация пользователей SAP

Подключаемые модули безопасности расширяют способы аутентификации пользователей платформы BI. Функция аутентификации SAP включает в себя подключаемый модуль безопасности SAP (`secSAPR3.dll`) для Центрального сервера управления платформы BI. Данный модуль безопасности SAP имеет несколько ключевых преимуществ:

- Он выполняет аутентификацию, посредством проверки учетных записей пользователей системы SAP от имени Центрального сервера управления. Если пользователи выполняют вход в платформу BI напрямую, они могут выбирать аутентификацию SAP и указывать свое имя пользователя SAP и пароль. Платформа BI также может проверять билеты входа Enterprise Portal в системах SAP.
- Это облегчает создание учетной записи, так как позволяет сопоставлять роли в SAP группам пользователей в платформе BI, а также облегчает управление учетными записями, так как позволяет согласованно назначать пользователям и группам права в платформе BI.
- Это обеспечивает динамическую поддержку ролевых списков SAP. Поэтому после сопоставления роли SAP платформе все пользователи, принадлежащие к данной роли, смогут входить в систему. В случае внесения дальнейших изменений в распределение ролей SAP нет необходимости обновлять списки в платформе.
- Компонент аутентификации SAP включает в себя веб-приложение для настройки расширения. Получить доступ к данному приложению можно в области «Аутентификация» консоли Central Management Console (CMC).

7.5.2 Создание учетной записи пользователя для платформы BI

Платформа BI требует наличия учетной записи пользователя SAP, которая авторизована для доступа к спискам принадлежностей к ролям SAP и аутентификации SAP. Учетные данные этой учетной записи понадобятся для подключения платформы BI к имеющейся SAP-системе. Общие инструкции по созданию учетных записей пользователей SAP и назначению прав через роли см. в документации к системе SAP BW.

Используйте транзакцию `SU01` для создания новой учетной записи пользователя SAP под именем `CRYSTAL`. Используйте транзакцию `PFCG` для создания новой роли под названием `CRYSTAL_ENTITLEMENT`. (Эти названия являются рекомендуемыми, но не обязательными.) Измените данные авторизации роли путем присвоения этих значений следующим объектам авторизации:

Объект авторизации	Поле	Значение
Авторизация для доступа к файлам (S_DATASET)	Действие (ACTVT)	Чтение, Запись (33, 34)
	Физическое имя файла (FILENAME)	* (отмечает Все)
	Название программы ABAP (PROGRAM)	*
Проверка авторизации для доступа к RFC (S_RFC)	Действие (ACTVT)	16
	Имя защищаемого RFC (RFC_NAME)	BDCH, STPA, SUSO, BDL5, SUUS, SU_USER, SYST, SUNI, RFC1, SDIFRUNTIME, PRGN_J2EE, /CRYSTAL/SECURITY
	Тип защищаемого объекта RFC (RFC_TYPE)	Группа функций (FUGR)
Поддержка основной записи пользователя: Группы пользователей (S_USER_GRP)	Действие (ACTVT)	Создать или сгенерировать, затем отобразить (03)
	Группа пользователей на экране поддержки основной записи пользователя (CLASS)	<p>*</p> <p>Примечание: В целях повышения безопасности можно непосредственно перечислить группы пользователей, элементам которых необходим доступ к платформе BI.</p>

Наконец, добавьте пользователя `CRYSTAL` к роли `CRYSTAL_ENTITLEMENT`.

Совет:

Если политика системы требует изменения пароля пользователя при первом входе в систему, войдите в систему под учетной записью пользователя `CRYSTAL` и задайте новый пароль.

7.5.3 Подключение к системам контроля полномочий SAP

Перед импортом ролей или публикацией содержимого модуля BW в платформу BI нужно предоставить информацию о системах контроля полномочий SAP, которые следует интегрировать. Платформа BI использует эту информацию для подключения к нужной SAP-системе при определении ролевых принадлежностей и аутентифицирует пользователей SAP.

7.5.3.1 Добавление системы контроля полномочий SAP

1. Перейдите в область управления «Аутентификация» CMC.
2. Дважды щелкните ссылку **SAP**.

Появятся настройки системы контроля полномочий.

Совет:

Если система контроля полномочий уже отображается в списке **Имя логической системы**, нажмите кнопку **Создать**.

3. В поле **Система** введите трехсимвольное имя системы (SID) вашей SAP-системы.
4. В поле **Клиент** введите номер клиента, который платформа BI будет использовать при входе в систему SAP.
Платформа BI объединяет системную и клиентскую информацию и добавляет записи в список **Имя логической системы**.
5. Убедитесь, что флажок **Отключено** не установлен.

Примечание:

Флажок **Отключено** указывает платформе BI, что данная SAP-система временно недоступна.

6. Заполните поля **Сервер сообщений** и **Группа входа в систему** соответствующими значениями, если задана такая балансировка загрузки, при которой платформа BI должна подключаться через сервер сообщений.

Примечание:

Необходимо ввести соответствующие записи в файл **Службы** на компьютере в платформе BI, чтобы разрешить балансировку загрузки, особенно в том случае, если развертывание охватывает несколько компьютеров. Особенное внимание необходимо уделить компьютерам, на которых установлен CMS, сервер веб-приложений, а также всем компьютерам, управляющим учетными записями и настройками аутентификации.

7. Если балансировка загрузки не установлена (или предпочтительна непосредственная регистрация платформы BI в SAP-системе), нужно заполнить поля **Сервер приложений** и **Номер системы** соответствующими данными.

8. В полях **Имя пользователя**, **Пароль** и **Язык** введите имя пользователя, пароль и код языка для учетной записи SAP, которую платформа BI будет использовать при входе в SAP.

Примечание:

Эти учетные данные должны соответствовать учетной записи пользователя, созданной для платформы BI.

9. Щелкните **Обновить**.

Если добавлено несколько систем контроля полномочий, нажмите вкладку **Параметры**, чтобы указать систему, которую платформа BI будет использовать по умолчанию (эта система будет идентифицировать пользователей, которые пытаются войти с учетными данными SAP, не выбирая конкретную SAP-систему).

См. также

- [Создание учетной записи пользователя для платформы BI](#)

7.5.3.2 Для проверки правильности добавления системы контроля полномочий

1. Нажмите вкладку **Импорт ролей**.
2. Выберите имя системы контроля полномочий из списка **Имя логической системы**.

Если система контроля полномочий была добавлена корректно, список **Доступные роли** будет содержать список ролей, которые вы выбрали для импорта.

Совет:

Если в списке **Имя логической системы** нет ролей, просмотрите сообщения об ошибках на странице. В них может содержаться необходимая информация для устранения проблемы.

7.5.3.3 Временное прерывание соединения с системой предоставления прав SAP

В СМС можно временно прервать соединение между платформой BI и системой предоставления прав SAP. Это может быть полезным для поддержания реакции платформы BI в случаях запланированного времени завершения работы системы предоставления прав SAP.

1. В СМС перейдите в область управления **Авторизация**.
2. Дважды щелкните ссылку **SAP**.
3. В списке **Имя логической системы** выберите систему, которую нужно отключить.
4. Установите флажок в ячейке **Отключено**.

5. Щелкните **Обновить**.

7.5.4 Настройка параметров аутентификации SAP

Аутентификация SAP содержит определенное число параметров, которые можно задать при интеграции платформы BI с SAP-системой. Существуют перечисленные ниже варианты.

- Включение или отключение аутентификации SAP
- Задание параметров соединения
- Связывание импортированных пользователей с моделями лицензий платформы BI.
- Настройка единого входа в систему SAP

7.5.4.1 Настройка параметров аутентификации SAP

1. Перейдите в область управления «Аутентификация» в СМС.
2. Дважды щелкните на ссылке **SAP** и затем выберите вкладку **Параметры**.
3. Просмотрите и, при необходимости, измените настройки.

Параметр	Описание
Включить аутентификацию SAP	Снимите этот флажок, если требуется полностью отключить аутентификацию SAP. (Отключить аутентификацию SAP для конкретных SAP-систем можно, установив флажок Отключено на вкладке Системы контроля полномочий).
Корневая папка содержимого	В этом поле укажите, где платформа BI будет тиражировать структуру каталогов BW в CMC и на стартовой панели BI. По умолчанию это папка /SAP/2.0, но при необходимости можно выбрать другую папку. Для изменения этого значения следует изменить его как в CMC, так и в инструменте Content Administration Workbench.
Система по умолчанию	<p>В этом списке выберите систему контроля полномочий SAP, которую платформа BI будет использовать по умолчанию (эта система будет идентифицировать пользователей, которые пытаются войти с учетными данными SAP, но не выбирая конкретную SAP-систему).</p> <p>Примечание: Если определена система по умолчанию, пользователям из этой системы не нужно будет вводить идентификатор системы и мандант при подключении с использованием SAP-аутентификации из таких средств клиента, как Live Office или Universe Designer. Например, если система SYS~100 является системой по умолчанию, SYS~100/пользователь1 сможет войти в систему как "пользователь1" при выборе SAP-аутентификации.</p>
Макс. число неудачных доступов системы контроля полномочий	

Параметр	Описание
	<p>Введите число, характеризующее количество попыток переподключения платформы к SAP-системе при выполнении запросов аутентификации. Если установить значение равным -1, платформа BI будут пытаться подключиться к системе контроля полномочий неограниченное количество раз. Если установить 0, платформа BI сделает одну попытку подключения к системам контроля полномочий.</p> <p>Примечание: Используйте эту настройку совместно с настройкой Отключить систему контроля полномочий [сек] для определения того, как платформа BI будет работать с временно недоступными системами контроля полномочий SAP. Система использует эти настройки для того, чтобы определить, когда остановить коммуникацию с недоступной SAP-системой и когда продолжить ее.</p>
Отключить систему контроля полномочий [сек]	<p>Введите число секунд, в течение которых платформа BI будут ожидать возобновления попыток аутентификации пользователей в SAP-системе. Например, если ввести 3 в поле Макс. число неудачных попыток доступа к системе контроля полномочий, платформа BI разрешит максимум 3 попытки переподключения пользователей к любой конкретной SAP-системе; четвертый неудачный результат подключения приведет к тому, что платформа BI прекратит попытки подключения пользователей к этой системе на указанное время.</p>
Макс . число параллельных соединений на систему	<p>Используйте это поле для определения максимального количества соединений с SAP, которые могут быть открыты в одно и то же время. Например, если ввести в это поле 2, то платформа BI будет поддерживать два отдельных соединения с SAP открытыми.</p>

Параметр	Описание
Число использований на одно соединение	В этом поле нужно указать, сколько операций следует разрешить в одном соединении с SAP-системой. Например, если указано 2 в поле Макс. число одновременных соединений на систему и 3 в поле Число пользователей на соединение , то при 3 регистрациях в системе на одно соединение платформа BI закроет соединение и перезапустит его.
BI Viewer и BI Analyst	<p>Эти варианты позволяют выбрать роли, с которыми создаются новые учетные записи пользователей: "BI Viewer" или "BI Analyst". Обычно роль "BI Viewer" присваивается пользователям, которые потребляют содержимое. Для этой роли характерен ограниченный доступ к рабочим процессам приложений в соответствии с лицензионным соглашением платформы SAP BusinessObjects Business Intelligence. Роль BI Analyst предназначена для пользователей, которые создают и изменяют содержимое для приложений платформы. У этой роли отсутствуют ограничения на доступ к рабочим процессам приложений.</p> <p>Примечание: Указанный здесь параметр не изменяет число или тип пользовательских лицензий, установленных в платформе BI. В системе должны быть доступны подходящие лицензии.</p>

Параметр	Описание
Конкурентные пользователи и Именованные пользователи	<p>Используйте эти параметры, чтобы указать, какие лицензии использовать для новых учетных записей пользователей: конкурентные (параллельные) или именованные. Лицензии на одновременный доступ указывают количество человек, которые могут подключиться к платформе BI одновременно. Это очень гибкий тип лицензий, так как небольшое их количество поддерживает широкую пользовательскую базу. Например, в зависимости от того, как часто и как долго пользователи работают с системой, лицензия на одновременный доступ для 100 пользователей может поддерживать 250, 500 или 700 пользователей. Именованные пользовательские лицензии связаны с конкретными пользователями и позволяют им входить в систему, используя имя пользователя и пароль. Это дает именованным пользователям право доступа к системе независимо от того, сколько человек уже зарегистрировано в ней.</p> <p>Примечание: Указанный здесь параметр не изменяет число или тип пользовательских лицензий, установленных в платформе BI. В системе должны быть доступны подходящие лицензии.</p>
Импортировать полное имя и адрес электронной почты	<p>Выберите этот параметр, если требуется установить уровень приоритета для подключаемого модуля аутентификации SAP. Полные имена и описания, используемые в учетных записях SAP, импортируются и сохраняются в пользовательских объектах в платформе BI.</p>
Установка приоритета для привязки атрибута SAP относительно других привязок атрибутов.	<p>Задает приоритет для привязки атрибутов пользователя SAP (полное имя и адрес электронной почты). Если задано значение «1», в сценариях, в которых включены SAP и другие подключаемые модули (Windows AD и LDAP), приоритет имеют атрибуты SAP. Если задано значение «3», приоритет имеют атрибуты из других подключаемых модулей.</p>

Для настройки службы единого входа используются следующие поля SAP:

Параметр	Описание
«Системный идентификатор»	Системный идентификатор, предоставляемый платформой BI в SAP-систему при выполнении единой регистрации SAP.
Просмотр	Используйте эту кнопку, чтобы загрузить файл хранилища ключей, созданный для включения единой регистрации SAP. Также можно вручную ввести полный путь к файлу в имеющемся поле.
«Пароль хранилища ключей»	Укажите пароль, необходимый для доступа к файлу хранилища ключей.
«Пароль личного ключа»	Укажите пароль, необходимый для доступа к сертификату, соответствующему файлу хранилища ключей. Этот сертификат хранится в SAP-системе.
«Псевдоним личного ключа»	Укажите псевдоним, необходимый для доступа к файлу хранилища ключей.

4. Щелкните **Обновить**.

См. также

- [Лицензирование на основе ролей](#)
- [Настройка аутентификации SAP](#)

7.5.4.2 Изменение корневой папки содержимого

1. Перейдите в область управления «Аутентификация» СМС.
2. Дважды щелкните ссылку **SAP**.
3. Выберите **Параметры** и введите имя папки в поле **Корневая папка содержимого**.
Папка, имя которой введено, – это папка, в которую платформа BI будет тиражировать структуру папок BW.
4. Нажмите кнопку **Обновить**.
5. В инструменте Content Administration Workbench модуля BW разверните **Система Enterprise**.
6. Разверните **Доступные системы** и двойным щелчком мыши выберите систему, к которой подключена платформа BI.
7. Нажмите вкладку **Макет** и в **Базовой папке содержимого** введите папку, которую требуется использовать в качестве корневой папки SAP в платформе BI (например, /SAP/2.0/).

7.5.5 Импорт ролей SAP

Благодаря импорту ролей SAP в платформу BI можно разрешить элементам ролей входить в систему с использованием обычных учетных данных SAP. Кроме того, включается единый вход (SSO), поэтому пользователи SAP могут автоматически выполнять вход в платформу BI при доступе к отчетам с использованием графического интерфейса пользователя SAP или портала SAP Enterprise Portal.

Примечание:

Часто существует много требований для включения SSO. Некоторые из них могут включать использование драйвера или приложения с возможностью SSO и обеспечение расположения сервера пользователя и веб-сервера в одном домене.

Для каждой импортируемой роли в приложении платформы BI создается группа. Для присвоения имени каждой из групп используется следующее соглашение:

SystemID~ClientNumber@NameOfRole. Новые группы можно просматривать в области управления «Пользователи и группы» СМС. Эти группы можно также использовать для определения безопасности объекта в платформе BI.

Рассмотрите возможность использования трех категорий пользователей при настройке платформы BI для публикации и при импорте ролей в систему:

- Администраторы платформы BI

Администраторы Enterprise настраивают систему для публикации содержимого из SAP. Они импортируют подходящие роли, создают необходимые папки и назначают права этим ролям и папкам в платформе BI.

- Издатели содержимого

Издатели содержимого – это пользователи, у которых в ролях настроены права публикации содержимого. Назначением этой категории пользователей является разделение обычных элементов ролей и пользователей, которым назначены права публикации отчетов.

- Элементы ролей

Элементы ролей – это пользователи, для которых настроены роли «носителей содержимого». То есть эти пользователи принадлежат ролям, в которых публикуются отчеты. Для них можно настроить такие права, как **Просмотр**, **Просмотр по требованию** и **Расписание** для любых отчетов, публикуемых в роли, элементами которой они являются. Однако обычные элементы ролей не могут публиковать новое содержимое или обновленные версии содержимого.

Необходимо импортировать все роли издателей содержимого и носителей содержимого в платформу BI перед размещением первой публикации.

Примечание:

Настоятельно рекомендуется устанавливать различия деятельности ролей. Например, несмотря на то что публикацию можно размещать с использованием роли администратора, лучше размещать публикации с использованием ролей издателей содержимого. Кроме того, функцией ролей издателей содержимого является только определение пользователей, которые могут публиковать содержимое. Поэтому в ролях издателей содержимого должно отсутствовать содержимое; издатели содержимого должны размещать публикации в ролях носителей содержимого, которые доступны обычным элементам ролей.

См. также

- [Права на платформе BI](#)
- [Управление настройками безопасности для объектов в СМС](#)

7.5.5.1 Чтобы выполнить импорт ролей SAP

1. Перейдите в область управления «Аутентификация» СМС.
2. Дважды щелкните ссылку **SAP**.
3. На вкладке **Параметры** выберите **BI Viewer**, **BI Analyst**, **Параллельные пользователи** или **Именованные пользователи** в зависимости от имеющегося лицензионного соглашения.
Обратите внимание на то, что выбранный здесь параметр не изменяет число или тип пользовательских лицензий, установленных в платформе BI. В системе должны быть доступны подходящие лицензии.
4. Нажмите кнопку **Обновить**.
5. На вкладке **Импорт ролей** выберите соответствующую систему контроля полномочий из списка **Имя логической системы**.
6. В области **Доступные роли** выберите роли, которые требуется импортировать, а затем нажмите кнопку **Добавить**.
7. Щелкните **Обновить**.

7.5.5.2 Проверка правильности импорта ролей и пользователей

1. Убедитесь, что для пользователя SAP, принадлежащего одной из ролей, которая была сопоставлена платформе BI, известны имя пользователя и пароль.
2. Для стартовой панели BI Java перейдите по адресу `http://webserver:portnumber/BOE/BI`.
Замените *webserver* именем веб-сервера, а *portnumber* – номером порта, который задан для платформы BI. Возможно понадобится обратиться к администратору, чтобы узнать имя веб-сервера, номер порта или точный URL-адрес для входа.
3. В списке **Тип аутентификации** выберите **SAP**.
4. Введите систему SAP и клиентскую систему, в которую требуется войти.
5. Введите имя пользователя и пароль для отображаемого пользователя.
6. Нажмите кнопку **Вход в систему**.
Выполните вход в стартовую панель BI под учетной записью выбранного пользователя.

7.5.5.3 Обновление ролей и пользователей SAP

После включения аутентификации Oracle EBS необходимо запланировать и запустить регулярные обновления по сопоставленным ролям, импортированным в платформу BI. Это обеспечит точное представление информации о роли SAP в платформе BI.

Существуют два варианта запуска и планирования обновлений для ролей SAP:

- Обновлять только роли: если используется этот вариант, будут обновлены только ссылки между сопоставленными в настоящий момент ролями, импортированными в платформу BI. Рекомендуется использовать этот вариант, если ожидаются частые запуски обновлений и если имеются проблемы с использованием системных ресурсов. Если обновляются только роли SAP, новых учетных записей создано не будет.
- Обновление ролей и псевдонимов: этот параметр обновляет не только ссылки между ролями, но также создает новые учетные записи пользователей в платформе BI для пользовательских псевдонимов, добавляемых к ролям в системе SAP.

Примечание:

Если не было указано автоматическое создание псевдонимов для обновлений при включенной аутентификации Oracle EBS, для новых псевдонимов не будут созданы учетные записи.

7.5.5.3.1 Планирование обновлений для ролей SAP

После сопоставления ролей платформе BI необходимо указать, как система будет обновлять эти роли.

1. Щелкните вкладку **Обновление пользователя**.
2. Щелкните **Расписание** в разделе «Обновлять только роли» или в разделе «Обновлять роли и псевдонимы».

Совет:

Если необходимо немедленно запустить обновление, щелкните **Обновить сейчас**.

Совет:

Используйте параметр «Обновлять только роли», если нужны частые обновления и имеются проблемы с системными ресурсами. Системе нужно больше времени на обновление ролей и псевдонимов.

Будет открыто диалоговое окно «Повтор».

3. Выберите параметр из раскрывающегося списка «Запуск объекта» и введите всю запрашиваемую информацию о планировании в предоставленные поля.

При создании расписания обновления можно выбрать типы повтора, представленные в следующей таблице.

Тип повтора	Описание
Ежечасно	Обновление будет запускаться каждый час. Вы указываете в какое время должен выполняться объект, а также дату начала и окончания.
Ежедневно	Обновление будет запускаться ежедневно или через каждый раз по истечении указанного количества дней. Можно указать, в какое время объект будет выполняться, а также дату начала и окончания.
Каждую неделю	Обновление будет запускаться каждую неделю. Он может быть запущен один раз или несколько раз в неделю. Можно указать, в какие дни и в какое время он будет выполняться, а также дату начала и окончания.
Ежемесячно	Обновление будет запускаться каждый месяц или каждые несколько месяцев. Можно указать время запуска, а также дату начала и окончания.
N-й день месяца	Обновление будет запускаться в определенный день месяца. Можно указать день месяца, время запуска, а также дату начала и окончания.
Первый понедельник месяца	Обновление будет запускаться в первый понедельник каждого месяца. Можно указать время запуска, а также дату начала и окончания.
Последний день месяца	Обновление будет запускаться в последний день каждого месяца. Можно указать время запуска, а также дату начала и окончания.
X день N-ной недели месяца	Обновление будет запускаться в указанный день указанной недели месяца. Можно указать время запуска, а также дату начала и окончания.
Календарь	Обновление будет запускаться по датам, указанным в созданном календаре.

4. Щелкните **Расписание** после того, как будет окончен ввод информации о планировании. Дата следующего запланированного обновления роли отображается на вкладке **Обновление пользователя**.

Примечание:

Всегда можно отменить следующее запланированное событие, щелкнув **Отменить запланированные обновления** в разделе «Обновлять только роли» или «Обновлять роли и псевдонимы».

7.5.6 Настройка защищенного сетевого соединения (SNC)

В настоящем разделе описывается процесс настройки SNC в рамках процесса настройки аутентификации SAP для платформы BI

Перед установкой доверия между системой SAP и платформой BI требуется настроить SIA для запуска и выполнения с использованием учетной записи, заданной для SNC. Необходимо также настроить доверенное соединение системы SAP и платформы BI. Рекомендуется следовать инструкциям, представленным в разделе *Настройка доверия SAP на сервере* в главе *Дополнительные конфигурации для сред ERP* настоящего руководства.

7.5.6.1 Общие сведения о настройке доверительных параметров сервера SAP

В этом разделе описан процесс настройки параметров доверия на стороне сервера между серверами веб-приложений SAP (версии 6.20 и выше) и платформы BI. Настраивать доверительные параметры со стороны сервера нужно в случае использования многопроходной пакетной передачи отчета (для публикаций, где запрос отчета зависит от контекста пользователя).

Доверительные параметры со стороны сервера подразумевают использование беспарольного заимствования прав. Для осуществления заимствования прав пользователя SAP без предоставления пароля пользователь должен пройти идентификацию на SAP с использованием более защищенного метода, чем обычный ввод имени и пароля. (Пользователь SAP с профилем авторизации SAP_ALL не может подменить другого пользователя SAP, не зная его пароль.)

Включение доверительных параметров со стороны сервера SAP с использованием библиотеки "SAP crypto"

Для включения параметров доверия на стороне сервера для платформы BI с использованием бесплатной библиотеки шифрования SAP нужно запустить соответствующие серверы с использованием идентификационных данных, прошедших проверку зарегистрированного провайдера защищенного сетевого обмена данными (SNC). Эти данные настраиваются в SAP и используются для заимствования прав без ввода пароля. На платформе BI нужно запустить серверы, осуществляющие пакетную отправку отчетов с использованием этих идентификационных данных SNC, например, сервер заданий Crystal Reports.

Для настройки доверительных параметров со стороны сервера необходима шифрующая библиотека. На веб-сайте SAP для загрузки доступна библиотека SAP Cryptographic Library. Обратите внимание, эта библиотека может использоваться только для настройки доверительных параметров со стороны сервера. Библиотека шифрования доступна в версии для Windows и UNIX. Дополнительные сведения см. в примечаниях SAP №711093, 597059 и 397175 на веб-сайте SAP.

Серверы SAP и платформе BI необходимо назначить сертификаты, чтобы они могли подтвердить друг другу свою подлинность. У каждого сервера будет свой собственный сертификат и список сертификатов для доверенных сторон. Для настройки параметров доверия на стороне сервера между SAP и платформой BI требуется создать набор сертификатов, защищенных паролем, который называется средой личной безопасности (PSE). В этом документе описывается процесс настройки и обслуживания сред персональной безопасности, а также перечисляются способы безопасной привязки PSE к серверам обработки платформы BI.

Отличия между интерфейсами SNC на клиенте и сервере

В интерфейсе SNC на клиенте идентификатор SNC сопоставляется с одним (или несколькими) именами пользователей SAP в SU01. Когда отправляется запрос на вход, имя SNC вместе с именем SAP передается в систему SAP, однако пароль при этом не передается. Вход разрешается, только если имя SNC сопоставляется указанному имени SAP. Ниже приводится строка входа со стороны клиента для прямого входа на хост приложений.

```
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"
```

Чтобы успешно выполнить вход, необходимо сопоставить пользователя SAP с именем USER123 со следующими параметрами: p:CN=TheUser, O=TheCompany, C=US в SU01. С другой стороны, в интерфейсе SNC на сервере необязательно явным образом сопоставлять идентификатор SNC и имя пользователя SAP. Вместо этого имя SNC настраивается в транзакции SNC0, это позволяет «любому» пользователю выполнять вход в режиме олицетворения без ввода пароля. Например:

```
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
```

Вход в режиме олицетворения через интерфейс SNC на сервере или вход с предоставлением внешнего идентификатора выполняется эффективнее, чем через его аналог на клиенте. Такой способ входа позволяет получить доступ к любой учетной записи SAP в системе. Вход с предоставлением внешнего идентификатора также можно выполнять с помощью билетов для входа и сертификатов клиента X.509.

Функции сервера платформы BI

Определенные серверы платформы BI обеспечивают интеграцию SAP в рамках единого входа (SSO). В следующей таблице перечисляются эти серверы и типы SNC, необходимые для отдельных областей ответственности.

Сервер	Тип SNC	Области ответственности
Сервер веб-приложений	клиент	список ролей для аутентификации SAP
	сервер	Списки выбора динамических параметров Crystal Reports и персонализация
CMS	клиент	Пароль, билет, проверка принадлежности к роли и списки пользователей
Сервер страниц	сервер	Просмотр отчетов Crystal по требованию

Сервер	Тип SNC	Области ответственности
Сервер заданий	сервер	Планирование отчетов Crystal
сервер обработки Web Intelligence;	сервер	Просмотр и планирование отчетов и приглашений на ввод в виде списков значений (LOV) для сервера Web Intelligence
Служба многомерного анализа	сервер	Анализ

Примечание:

Сервер веб-приложений и CMS используют SNC на клиенте, что требует явного сопоставления имени SNC с именем пользователя SAP. Это указано в транзакциях SU01 или SM30 для таблицы USRACL.

7.5.6.2 Настройка доверительных параметров SAP со стороны сервера

Процедура ниже описывает настройку SNC для использования с платформой BI. Обратите внимание, что необходимо ознакомиться с дополнительными сведениями или инструкциями по устранению неполадок, которые содержатся в документации SAP, прилагаемой к серверу SAP.

7.5.6.2.1 Настройка доверия сервера SAP

1. Со страницы SAP marketplace загрузите библиотеку SAP Cryptographic Library для всех необходимых платформ.

Примечание:

Для получения подробной информации о библиотеке Cryptographic Library см. ноты 711093, 597059 и 397175 на сайте SAP.

2. Убедитесь в наличии учетных данных администратора SAP в системе SAP и на компьютере, на котором выполняется система, а также идентификационные данные администратора для платформы BI и компьютера (или компьютеров), на котором она выполняется.
3. На компьютере с системой SAP скопируйте библиотеку SAP Cryptographic Library и инструмент SAPGENPSE в директорию <DRIVE>:\usr\sap\<SID>SYS\exe\run\ (в Windows).
4. Перейдите к файлу "ticket", установленному с библиотекой SAP Cryptographic Library, и скопируйте его в директорию <DRIVE>:\usr\sap\<SID>\<instance>\sec\ (в Windows).
5. Создайте переменную среды с именем SECUDIR, указывающую каталог, в котором находится квитанция.

Примечание:

Эта переменная должна быть доступна пользователю, запускающему процесс SAP disp+work/

6. В SAP GUI выполните транзакцию RZ10 и измените профиль экземпляра в режиме **Расширенное сопровождение**.

7. В режиме редактирования профиля свяжите переменные профиля SAP с библиотекой Cryptographic Library и присвойте системе SAP характерное имя. Эти переменные должны соответствовать следующим условиям LDAP-соглашения об именах:

Метка	Значение	Описание
CN	Стандартное имя	Обычное имя собственника сертификата.
OU	Организационная единица	Например, ГП для Группы Продуктов.
O	Организация	Наименование организации, для которой был выпущен сертификат
C	Страна	Страна, в которой расположена организация.

Например, для R21: `p:CN=R21, OU=PG, O=BOBJ, C=CA`.

Примечание:

Заметьте, что приставка `p:` используется для библиотеки SAP Cryptographic Library. Она необходима для ссылки на имя SAP-системы, но не является видимой при проверке сертификатов в транзакциях STRUST или с использованием SAPGENPSE.

8. Введите следующие значения профилей, подставляя SAP-системы там, где это необходимо:

Переменная профиля	Значение
ssf/name	SAPSECULIB
ssf/ssfapi_lib	Полный путь к криптографической библиотеке
sec/libsapsecu	Полный путь к криптографической библиотеке
snc/gssapi_lib	Полный путь к криптографической библиотеке
snc/identity/as	Имя вашей SAP-системы

9. Перезапустите экземпляр SAP.
10. Когда система снова будет запущена, войдите в нее и выполните транзакцию STRUST, в которой теперь должны быть новые записи для SNC и SSL.
11. Правой кнопкой мыши щелкните на узел SNC и нажмите **Создать**.
Теперь должен появиться идентификатор, который вы указали в транзакции RZ10.

12. Нажмите кнопку **ОК**.

13. Чтобы назначить пароль SNC PSE, нажмите на пиктограмму блокировки.

Примечание:

Не теряйте этот пароль. Каждый раз при запуске транзакции STRUST и просмотре или редактировании SNC PSE система будет приглашать вас ввести его.

14. Сохраните изменения.

Примечание:

Если вы не сохраните изменения и разрешите SNC, сервер приложений не сможет запуститься.

15. Вернитесь к транзакции RZ10 и добавьте оставшиеся параметры профиля SNC:

Переменная профиля	Параметр
snc/accept_insecure_rfc	1
snc/accept_insecure_r3int_rfc	1
snc/accept_insecure_gui	1
snc/accept_insecure_cplic	1
snc/permit_insecure_start	1
snc/data_protection/min	1
snc/data_protection/max	3
snc/enable	1

Минимальный уровень защиты равен 1 (только аутентификация), максимальный – 3 (конфиденциальность). Значение snc/data_protection/use определяет, что в этом случае будет использоваться только аутентификация, но также может использоваться (2) для целостности, (3) для конфиденциальности и (9) для максимальной доступности. Значения snc/accept_insecure_rfc, snc/accept_insecure_r3int_rfc, snc/accept_insecure_gui и snc/accept_insecure_cplic, установленные равными 1, гарантируют, что предыдущие (и потенциально небезопасные) методы коммуникации остаются разрешенными.

16. Перезапустите систему SAP.

Теперь необходимо настроить доверие на уровне сервера для платформы BI.

7.5.6.3 Настройка доверия к платформе BI на стороне сервера

Чтобы настроить доверие к платформе BI на стороне сервера, необходимо выполнить следующие действия. Обратите внимание, что эти шаги основаны на Windows, но поскольку инструмент SAP является инструментом командной строки, эти шаги очень схожи с действиями в UNIX.

1. Настройка среды
2. Создание среды личной безопасности (PSE)
3. Настройка серверов платформы BI
4. Настройка PSE-доступа
5. Настройка параметров SNC для аутентификации SAP
6. Настройка выделенных групп серверов SAP

См. также

- [Установка среды](#)
- [Для генерации PSE](#)
- [Настройка серверов платформы BI](#)
- [Настройка доступа PSE](#)
- [Для настройки SNC аутентификации SAP](#)
- [Использование групп серверов](#)

7.5.6.3.1 Установка среды

Перед началом убедитесь в следующем:

- Библиотека SAP Cryptographic Library загружена и развернута на хосте, на котором выполняются серверы обработки платформы BI.
- Соответствующие системы SAP были настроены на работу с Криптографической библиотекой SAP в качестве провайдера SNC.

Перед началом обслуживания PSE необходимо установить библиотеку, вспомогательный инструмент и среду, в которой хранятся PSE.

1. Копируйте SAP Cryptographic Library (включая средство обслуживания PSE) в папку на компьютере с платформой BI.

Например: `C:\Program Files\SAP\Crypto`

2. Добавьте папку в переменную среды `PATH`.
3. Добавьте общесистемную переменную среды `SNC_LIB`, которая указывает на Криптографическую библиотеку.

Например: `C:\Program Files\SAP\Crypto\sapcrypto.dll`

4. Создайте подпапку с именем `sec`.

Например: `C:\Program Files\SAP\Crypto\sec`

5. Добавьте общесистемную переменную среды *SECUDIR*, которая указывает на папку *sec*.
6. Скопируйте файл *ticket* из Криптографической библиотеки SAP в папку *sec*.

См. также

- [Настройка доверительных параметров SAP со стороны сервера](#)

7.5.6.3.2 Для генерации PSE

SAP принимает сервер платформы BI как доверенную сущность, если соответствующие серверы платформы BI имеют среду личной безопасности, которая связана с SAP. «Доверие» между компонентами SAP и платформы BI устанавливается благодаря совместному использованию публичной версии сертификатов друг друга. Первым шагом является создание PSE для платформы BI, которая автоматически создает собственный сертификат.

1. Откройте командную строку и запустите файл `sapgenpse.exe gen_pse -v -p BOE.pse`, находящийся в папке Cryptographic Library.
 2. Выберите PIN-код и отличительное имя для системы платформы BI.
Например, CN=MyBOE01, OU=PG, O=BOBJ, C=CA.
Теперь у вас есть PSE по умолчанию, со своим собственным сертификатом.
 3. Для экспорт сертификата в PSE используйте следующую команду:
`sapgenpse.exe export_own_cert -v -p BOE.pse -o MyBOECert.crt`
 4. В SAP GUI выполните транзакцию STRUST и откройте SNC PSE.
Система пригласит вас ввести пароль, который вы уже назначили.
 5. Импортируйте созданный ранее файл `MyBOECert.crt`:
Сертификаты SAPGENPSE представлены в кодировке Base64. Убедитесь, что при импорте вы выбрали кодировку Base64:
 6. Для добавления сертификата платформы BI к списку PSE-сертификатов на сервере SAP нажмите кнопку **Добавить в список сертификатов**.
 7. Чтобы добавить сертификат SAP в среду личной безопасности платформы BI, дважды щелкните сертификат SAP.
 8. Сохраните изменения в транзакции STRUST.
 9. Нажмите кнопку **Экспорт** и введите имя файла для сертификата.
Например, MySAPCert.crt.
- Примечание:**
Кодировка должна оставаться в формате Base64.
10. Выполните транзакцию SNC0.
 11. Введите новую запись, где:
 - Идентификатор системы является произвольным, однако он отражает используемую систему платформы BI.
 - Именем SNC должно быть отличительное имя (с приставкой p:), указанное при создании PSE платформы BI (шаг 2).

- Флажки **Ввод для RFC активирован** и **Ввод для экспортируемого Установлены оба активированные идентификатором флажка**:

12. Для добавления экспортированного сертификата к PSE платформы BI выполните в командной строке следующую команду:

```
sapgenpse.exe maintain_pk -v -a MySAPCert.crt -p BOE.pse
```

Библиотека SAP Cryptographic Library установлена на компьютере с платформой BI. Создана среда PSE, которая будет использоваться серверами платформы BI для идентификации на серверах SAP. Среда PSE системы SAP и платформы BI обменивались сертификатами. SAP разрешает сущностям с доступом к PSE платформы BI выполнять вызовы RFC и в анонимном режиме без пароля.

См. также

- [Настройка серверов платформы BI](#)

7.5.6.3.3 Настройка серверов платформы BI

После создания PSE для платформы BI необходимо настроить соответствующую структуру сервера для обработки SAP. В результате следующей процедуры создается узел для серверов обработки SAP, чтобы вы могли задать учетные данные операционной системы на уровне узла.

Примечание:

В данной версии платформы BI серверы больше не настраиваются в Central Configuration Manager (CCM). Вместо этого необходимо создать новый агент Server Intelligence Agent (SIA).

1. В CCM создайте новый узел для серверов обработки SAP.
Присвойте узлу подходящее имя, такое как SAPProcessor.
2. В CMC добавьте серверы обработки в новый узел, затем запустите новые серверы.

7.5.6.3.4 Настройка доступа PSE

После настройки узла и серверов платформы BI необходимо настроить доступ PSE с использованием инструмента SAPGENPSE.

1. Выполните следующую команду в командной строке:

```
sapgenpse.exe seclogin -p SBOE.pse
```

Примечание:

Появится приглашение на ввод PIN-кода PSE. Если инструмент запущен с учетными данными, совпадающими с теми, которые используются серверами обработки SAP платформы BI, имя пользователя указывать не нужно.

2. Чтобы убедиться в том, что ссылка для единого входа (SSO) установлена, просмотрите содержимое PSE с помощью следующих команд.

```
sapgenpse.exe maintain_pk -l
```

Результаты должны иметь следующий вид:

```
C:\Documents and Settings\hareskou\ Desktop\sapcrypto.x86\ntintel>sapgenpse.exe
maintain_pk -l
maintain_pk for PSE "C:\Documents and Settings\hareskou\My Documents\snc\sec\bobjsapproc.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:\Documents and Settings\hareskou\ Desktop\sapcrypto.x86\ntintel>
```

После успешного выполнения команды `seclogin` повторный запрос на ввод PIN-кода PSE появиться не должен.

Примечание:

При наличии проблем доступа к PSE используйте `-O`, чтобы указать права доступа к PSE. Например, чтобы предоставить доступ к PSE определенному пользователю в определенном домене, введите:

```
sapgenpse seclogin -p SBOE.pse -O <domain\user>
```

7.5.6.3.5 Для настройки SNC аутентификации SAP

После того как вы настроили PSE-доступ, вам необходимо задать настройки аутентификации SAP в CMC.

1. Перейдите в область управления CMC «Аутентификация».
2. Дважды щелкните ссылку **SAP**.
Появятся настройки системы контроля полномочий.
3. На странице аутентификации SAP перейдите на вкладку **Параметры SNC**.
4. Из списка **Имя логической системы** выберите вашу систему контроля полномочий.
5. В разделе "Базовые параметры" выберите **Включить защищенный сетевой обмен данными [SNC]**.
6. Введите путь к настройкам библиотеки SNC в поле **Путь к библиотеке SNC**.

Примечание:

Этот шаг необходимо выполнить даже в том случае, если библиотека уже указана в переменной среды `SNC_LIB`.

7. В меню "Качество защиты" выберите уровень защиты.
Например, выберите **Аутентификация**.

Примечание:

Убедитесь, что не был превышен уровень защиты, настроенный для всей системы SAP. Уровень защиты выбирается согласно потребностям вашей организации и возможностям библиотеки SNC.

8. Введите имя SNC системы SAP в **Настройках взаимной аутентификации**.

Формат имени SNC зависит от библиотеки SNC. При использовании библиотеки шифрования SAP рекомендуется выбирать имя в соответствии с соглашением именования LDAP. Оно должно содержать префикс "p:".

9. Убедитесь, что имя SNC учетных данных, с которыми работают серверы платформы BI, не отображается в поле **Имя SNC системы Enterprise**.

Примечание:

При настройке нескольких имен SNC данное поле должно оставаться пустым.

10. Укажите отличительные имена PSE системы SAP и платформы BI.

7.5.6.3.6 Использование групп серверов

Если серверы обработки (Crystal Reports или Web Intelligence) запускаются без учетных данных пользователей, у которых есть доступ к PSE, необходимо создать определенную группу серверов, куда будут входить только эти серверы вместе с необходимыми поддерживающими серверами. Для получения дополнительных сведений и описаний разных серверов платформы BI см. главу «Архитектура».

Существует три варианта настройки серверов обработки содержимого SAP.

1. Поддерживайте один SIA, включая все серверы платформы BI, выполняемый с учетными данными, которые обеспечивают доступ к PSE. Это самый простой вариант – нет необходимости создавать группы серверов. Данный подход является наименее безопасным, так как доступ к PSE будет у излишнего количества серверов.
2. Создайте второй SIA с доступом к PSE и добавьте его к серверам обработки Crystal Report или Interactive Analysis. Удалите повторяющиеся серверы в исходном SIA. Нет необходимости создавать группы серверов, но доступ к PSE имеет меньшее число серверов.
3. Создайте SIA исключительно для использования системой SAP с доступом к PSE. Добавьте его к серверам обработки Crystal Report или Web Intelligence. При данном подходе на серверах необходимо обрабатывать только содержимое SAP, и, что более важно, это содержимое нельзя будет обрабатывать на других серверах. Поскольку этот сценарий предусматривает направление содержимого на определенные серверы, необходимо создать группы серверов для SIA.

Рекомендации по использованию группы серверов

Группе серверов необходимо ссылаться на SIA, который используется исключительно для управления содержимым SAP. Кроме того, группе серверов необходимо ссылаться на следующие серверы:

- Адаптивные серверы
- Серверы публикаций
- Серверы заданий для адресата

Все содержимое SAP, документы Web Intelligence и отчеты Crystal необходимо строго ассоциировать с группой серверов, то есть их необходимо запускать на серверах этой группы. Если связь создана на уровне объектов, параметры этой группы серверов должны быть распространены как для параметров для прямого планирования, так и для параметров публикаций.

Чтобы предотвратить обработку содержимого (отличного от SAP) на серверах обработки, определенных для SAP, необходимо создать другую группу серверов, куда будут входить все серверы исходного SIA. Рекомендуется установить строгую связь между содержимым и группой серверов, не связанных с SAP.

7.5.6.4 Настройка многопроходных публикаций

Устранение неполадок многопроходных публикаций

При возникновении затруднений во время работы с многопроходными публикациями, включите трассировку драйвера CR или MDA и найдите строку входа, используемую для каждого задания или получателя. Строки входа должны иметь следующий вид:

```
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\sapcrypto.dll"  
SNC_PARTNERNAME="p:CN=R21Again, OU=PG, O=BOBJ, C=CA" EXTIDDATA=HENRIKRPT3 EXTIDTYPE=UN
```

В строке входа должен быть указан подходящий параметр EXTIDTYPE=UN (для имени пользователя) и для параметра EXTIDDATA должно быть указано имя пользователя-получателя SAP. В этом примере попытка входа выполнена успешно.

7.5.6.5 Рабочий поток для интеграции с защищенным сетевым обменом данными

Платформа BI поддерживает среды безопасных сетевых взаимодействий, или Secure Network Communication (SNC) для аутентификации и шифрования данных компонентов SAP. Если выполнялось внедрение библиотеки SAP Cryptographic Library (или другой продукт защиты, использующий интерфейс SNC), необходимо задать некоторые дополнительные значения для эффективной интеграции платформы BI в защищенной среде.

Чтобы платформа использовала интерфейс безопасных сетевых взаимодействий, необходимо проделать следующее:

1. Настройте платформу BI на запуск под конкретной учетной записью пользователя.
2. Настройте доверенное соединение системы SAP и системы платформы BI.
3. Задайте настройки SNC в ссылке SNC в Central Management Console.
4. Импортируйте роли и пользователей SAP в платформу BI.

См. также

- [Импорт ролей SAP](#)

- [Настройка доверительных параметров SAP со стороны сервера](#)
- [Настройка доверия к платформе BI на стороне сервера](#)

7.5.6.6 Изменение настроек SNC в Central Management Console (CMC)

Перед началом настройки SNC следует добавить новую систему контроля полномочий в платформу BI. Также следует скопировать файл библиотеки SNC в известный каталог и создать переменную среды `RFC_LIB` для обращения к этому файлу.

1. На странице аутентификации SAP перейдите на вкладку **Параметры SNC**.
2. Из списка **Имя логической системы** выберите вашу систему контроля полномочий.
3. В разделе "Базовые параметры" выберите **Включить защищенный сетевой обмен данными [SNC]**.
4. Введите путь к настройкам библиотеки SNC в поле **Путь к библиотеке SNC**.

Примечание:

На сервере приложений и CMS должен использоваться одинаковый тип ОС с одинаковым путем к библиотеке шифрования.

5. В меню "Качество защиты" выберите уровень защиты.
Например, выберите **Аутентификация**.

Примечание:

Уровень защиты выбирается согласно потребностям вашей организации и возможностям библиотеки SNC.

6. Введите имя SNC системы SAP в **Настройках взаимной аутентификации**.

Формат имени SNC зависит от библиотеки SNC. При использовании библиотеки шифрования SAP рекомендуется выбирать имя в соответствии с соглашением именования LDAP. Оно должно содержать префикс "р:".

7. Убедитесь, что имя SNC учетных данных, с которыми работают серверы платформы BI, не отображается в поле **Имя SNC системы Enterprise**.

Примечание:

В сценариях с изменением нескольких имен SNC данное поле должно оставаться пустым.

8. Нажмите **Обновить**.
9. На странице аутентификации SAP перейдите на вкладку **Системы контроля полномочий**.
10. Здесь, под полем **Язык**, находится другое поле под названием **Имя SNC**.
11. В необязательном для заполнения поле **Имя SNC** введите имя SNC, настроенное на сервере SAP BW. Это имя должно совпадать с именем, которое использовалось для настройки доверия системы SAP с платформой BI.

См. также

- [Подключение к системам контроля полномочий SAP](#)

7.5.6.7 Для связи пользователя с именем SNC

1. Войдите в систему SAP BW и выполните транзакцию SU01.
Откроется экран "Определение пользователя: Начальный экран"
2. В поле **Пользователь** введите учетную запись пользователя системы контроля полномочий и нажмите кнопку **Изменить** в панели инструментов.
Появится экран "Определение пользователя".
3. Выберите вкладку SNC.
4. В поле **Имя SNC** введите SNC USER ACCOUNT (эти данные вы вводили на 4 шаге – см. выше).
5. Нажмите кнопку **Сохранить**.

7.5.6.8 Добавление идентификатора системы в список контроля доступа SNC

1. Выполните вход в SAP BW и выполните транзакцию SNC0.
Откроется экран: Изменить представление "SNC: Список контроля доступа (ACL) для систем: обзор".
2. Выберите команду **Новые записи** в панели инструментов.
Появится экран: "Новые записи: детали добавленных записей".
3. Введите имя компьютера, на котором установлена платформа BI, в поле **Ид. системы**
4. Введите p:<SNC USER NAME> в поле **Имя пользователя SNC**, где SNC USER NAME — учетная запись, которая использовалась при настройке серверов платформы BI.

Примечание:

Если SNC-провайдером является gssapi32.dll, используйте заглавные буквы при вводе учетной записи SNC USER NAME. Указывая учетную запись пользователя, следует включить имя домена. Пример: domain\username.

5. Выберите **Запись для RFC активирована** и **Запись для вн. ид. активирована**.
6. Очистите все другие параметры и нажмите **Сохранить**.

7.5.7 Настройка единого входа в систему SAP

Для включения единого входа в систему SAP нужно создать файл хранилища ключей и соответствующий сертификат. Воспользуйтесь программой `keytool`, выполняемой в режиме командной строки, для создания такого файла и сертификата. По умолчанию программа `keytool` установлена в каталоге `sdk/bin` для каждой платформы.

Сертификат нужно добавить в систему SAP ABAP BW и в платформу BI с помощью CMC.

Примечание:

Прежде, чем можно будет настроить единый вход в базу данных SAP, должен быть настроен подключаемый модуль аутентификация SAP.

7.5.7.1 Создание файла хранилища ключей

Программа `PKCS12Tool` используется для создания файлов хранилища ключей и сертификатов, необходимых для настройки единого входа в базу данных SAP. В таблице ниже перечислены места размещения файла `PKCS12Tool.jar` для каждой из поддерживаемых платформ.

Платформа	Местоположение по умолчанию
Windows	<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib
Unix	sap_bobj/enterprise_xi40/java/lib

1. Запустите командную строку и перейдите в каталог, где расположена программа `PKCS12Tool`.
2. Для создание файла хранилища ключей с настройками по умолчанию выполните следующую команду:

```
java -jar PKCS12Tool.jar
```

Файлы `cert.der` и `keystore.p12` создаются в одном каталоге. Файлы содержат следующие значения по умолчанию:

Параметр	По умолчанию
-keystore	keystore.p12
-alias	myalias
-storepass	123456
-dname	CN=CA
-validity	365
-cert	cert.der

Совет:

Для переопределения значений по умолчанию запустите инструмент вместе с параметром `-?`. На экран выводится следующее сообщение.

```
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>
```

Для переопределения значений по умолчанию можно использовать параметры.

7.5.7.2 Экспорт сертификата общедоступного ключа

Нужно создать и экспортировать сертификат файла хранилища ключей.

1. Запустите командную строку и перейдите в каталог, где расположена программа `keytool`.
2. Для экспорта сертификата ключа для файла хранилища ключей воспользуйтесь такой командой.

```
keytool -exportcert -keystore <keystore> -storetype pkcs12 -file <filename>
       -alias <alias>
```

Замените `<keystore>` именем файла хранилища ключей.

Замените `<filename>` именем сертификата.

Замените `<alias>` псевдонимом, который использовался для создания файла хранилища ключей.

3. По запросу введите пароль, который указывали для файла хранилища ключей.

Теперь файл хранилища ключей и сертификат расположены в каталоге, где находится программа `keytool`.

7.5.7.3 Импорт файла сертификата в нужную систему ABAP SAP

Для выполнения этой задачи нужен файл хранилища ключей и соответствующий ему сертификат для данного развертывания платформы BI.

Примечание:

Это действие можно выполнить только в системе ABAP SAP.

1. Выполните подключение к своей системе SAP ABAP BW через графический пользовательский интерфейс SAP.

Примечание:

Подключение следует выполнять под учетной записью пользователя, имеющего административные полномочия.

2. Выполните STRUSTSSO2 в графическом пользовательском интерфейсе SAP.
Система подготавливается к импорту файла сертификата.
3. Перейдите на вкладку **Сертификат**.
4. Убедитесь, что установлен флажок **Использовать бинарный вариант**.
5. Нажмите кнопку пути к файлу, чтобы указать расположение файла сертификата.
6. Нажмите зеленую отметку.
Выполняется отправка файла сертификата.
7. Нажмите **Добавить в список сертификатов**.
Сертификат отображается в списке сертификатов.
8. Нажмите **Добавить к ACL** и задайте системный идентификатор и клиента.
Идентификатор системы должен совпадать с тем, который используется для идентификации платформы BI в SAP BW.
Этот сертификат добавляется в список контроля доступа (ACL). Клиент должен указываться в следующем виде: «000».
9. Сохраните настройки и выполните выход.
Изменения сохраняются в системе SAP.

7.5.7.4 Настройка единого входа в базу данных SAP в СМС

Для выполнения этого алгоритма нужен доступ к подключаемому модулю безопасности SAP под учетной записью администратора.

1. Перейдите в область управления «Аутентификация» в СМС.

2. Дважды щелкните на ссылке **SAP** и затем выберите вкладку **Параметры**.

Если никакие сертификаты не были импортированы, в разделе «Служба SAP SSO» будет выведено такое сообщение:

Файлы хранилища ключей не были загружены

3. Укажите идентификатор системы для платформы BI в соответствующем поле.
Это значение должно совпадать со значением, которое использовалось при импорте сертификата в нужную систему SAP ABAP.
4. Нажмите кнопку **Обзор**, чтобы выбрать файл хранилища ключей.
5. Укажите перечисленные ниже необходимые сведения.

Поле	Необходимая информация
«Пароль хранилища ключей»	Укажите пароль, необходимый для доступа к файлу хранилища ключей. Этот пароль указывался при создании файла хранилища ключей.
«Пароль личного ключа»	Укажите пароль, необходимый для доступа к сертификату, соответствующему файлу хранилища ключей. Этот пароль указывался при создании сертификата для файла хранилища ключей.
«Псевдоним личного ключа»	Укажите псевдоним, необходимый для доступа к файлу хранилища ключей. Этот псевдоним указывался при создании файла хранилища ключей.

6. Для применения параметров нажмите кнопку **Обновить**.

После успешной отправки параметров в поле "Ид. системы" отображается сообщение.

Файл хранилища ключей загружен

7.5.7.5 Добавление службы маркера безопасности на адаптивный сервер обработки

В кластеризованной среде служба маркеров безопасности добавляется отдельно на каждый адаптивный сервер.

1. Перейдите в область управления «Серверы» в СМС.
2. Дважды щелкните элемент **Корневые службы**.
Отображается перечень серверов под «корневыми службами».
3. Щелкните правой кнопкой мыши адаптивный сервер обработки и выберите команду **Остановить**.
Не переходите к следующему действию, пока статус сервера не изменится на «Остановлено».
4. Щелкните правой кнопкой мыши адаптивный сервер обработки и выберите команду **Выбрать службы**.
На экран выводится диалоговое окно «Выбрать службы».

5. Перенесите службу маркера безопасности из перечня доступных служб в список «Службы» справа.
С помощью кнопки **Добавить к выбранному** переместите выбранные объекты.
6. Нажмите кнопку **ОК**.
7. Перезапустите адаптивный сервер обработки.

7.5.8 Настройка единого входа для SAP Crystal Reports и SAP Netweaver

По умолчанию в параметрах платформы BI пользователям SAP Crystal Reports будет разрешен доступ к данным SAP с использованием функции единого входа (SSO).

7.5.8.1 Отключение единого входа для SAP Netweaver и SAP Crystal Reports

1. В приложении Central Management Console (CMC) выберите элемент **Приложения**.
2. Дважды щелкните элемент **Конфигурация Crystal Reports**.
3. Выберите элемент **Параметры единой регистрации в системе**.
4. Выберите один из следующих драйверов:

Драйвер	Отображаемое имя
Драйвер хранилища оперативных данных	crdb_ods
Драйвер Open SQL	crdb_opensql
Драйвер InfoSet	crb_infoset
Драйвер запросов BW MDX	crdb_bwmdx

5. Нажмите кнопку **Удалить**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. Перезапустите SAP Crystal Reports.

7.5.8.2 Повторная активация единого входа для SAP Netweaver и SAP Crystal Reports

Выполните следующие действия для повторной активации единого входа для SAP Netweaver (ABAP) и SAP Crystal Reports.

1. В приложении Central Management Console (CMC) выберите элемент **Приложения**.
2. Дважды щелкните элемент **Конфигурация Crystal Reports**.
3. Выберите элемент **Параметры единой регистрации в системе**.
4. В разделе «Использовать для входа в базу данных контекст SSO» введите следующее:

crdb_ods	Активация драйвера ODS
crdb_opensql	Активация драйвера Open SQL
crdb_bwmdx	Активация драйвера запросов SAP BW MDX
crdb_infoset	Активация драйвера InfoSet

5. Нажмите кнопку **Добавить**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. Перезапустите SAP Crystal Reports.

7.6 Аутентификация PeopleSoft

7.6.1 Обзор

Для использования имеющихся данных PeopleSoft Enterprise с платформой BI необходимо предоставить программе сведения о развертывании. Эти данные позволят платформе BI выполнять аутентификацию пользователей так, чтобы для входа в программу последние могли использовать свои учетные данные PeopleSoft.

7.6.2 Включение аутентификации PeopleSoft Enterprise

Чтобы информация PeopleSoft Enterprise могла использоваться платформой BI, платформе BI нужны сведения об аутентификации в системе PeopleSoft Enterprise.

7.6.2.1 Включение аутентификации PeopleSoft Enterprise в платформе BI

1. Выполните вход в систему Central Management Console под учетной записью администратора.
2. В области "Управление" щелкните **Аутентификация**.
3. Дважды щелкните **PeopleSoft Enterprise**.
На экран выводится страница «PeopleSoft Enterprise». У этой страницы четыре вкладки: **Параметры**, **Домены**, **Роли** и **Обновление пользователя**.
4. На вкладке **Параметры**, установить флажок **Включить аутентификацию PeopleSoft Enterprise**.
5. Внесите необходимые изменения в поля **Новый псевдоним**, **Обновить параметры** и **Параметры нового пользователя** в соответствии с параметрами развертывания платформы BI. Нажать кнопку **Обновить** для сохранения изменений перед переходом на вкладку **Системы**.
6. Нажмите вкладку **Серверы**.
7. В области «Пользователь системы PeopleSoft Enterprise» введите имя пользователя базы данных и пароль, которые следует использовать в платформе BI для выполнения входа в базу данных PeopleSoft Enterprise.
8. В области «Домен PeopleSoft Enterprise» введите имя домена и адрес QAS, используемые для подключения к имеющейся среде PeopleSoft Enterprise, после чего нажмите кнопку **Добавить**.

Примечание:

При наличии нескольких доменов PeopleSoft, повторить этот шаг для каждого дополнительного домена, к которому требуется получить доступ. Домен, в который будет выполнен вход вначале, станет доменом по умолчанию.

9. Нажмите кнопку **Обновить**, чтобы сохранить изменения.

7.6.3 Сопоставление ролей PeopleSoft в платформе BI

Платформа BI автоматически создает группу для каждой сопоставляемой роли PeopleSoft. Кроме того, программа создает псевдонимы для участников отображенных ролей PeopleSoft.

Можно создать учетную запись пользователя для каждого созданного псевдонима.

Однако если вы работаете с несколькими системами и пользователи имеют учетные записи более чем на одной системе, то можно назначить каждого пользователя псевдониму с тем же именем перед созданием учетных записей в платформе BI.

Эта операция сокращает количество учетных записей, создаваемых для одного и того же пользователя в платформе BI.

Например, если вы работаете с PeopleSoft HR 8.3 и PeopleSoft Financials 8.4 и 30 ваших пользователей имеют доступ к обеим этим системам, то будет создано только 30 учетных записей. Если не назначать каждого пользователя псевдониmu с тем же именем, то для 30 пользователей в платформе BI будет создано 60 учетных записей.

Однако при работе с несколькими системами и совпадении имен пользователей нужно создать новую учетную запись участника для каждого создаваемого псевдонима.

Например, если вы работаете с PeopleSoft HR 8.3 под учетной записью пользователя Russell Aquino (имя пользователя "raqino"), а с PeopleSoft Financials 8.4 работаете под учетной записью пользователя Raoul Aquino (имя пользователя "raqino"), то необходимо создать отдельную учетную запись для каждого псевдонима пользователя. В противном случае в одну учетную запись платформы BI будут добавлены два пользователя; они смогут выполнять вход в платформу BI с учетными данными PeopleSoft и будут иметь доступ к данным обеих систем PeopleSoft.

7.6.3.1 Сопоставление роли PeopleSoft в платформе BI

1. Выполните вход в систему Central Management Console под учетной записью администратора.
2. Нажмите кнопку **Аутентификация**.
3. Дважды щелкните **PeopleSoft Enterprise for PeopleTools**.
4. На вкладке **Роли** в области "Домены PeopleSoft Enterprise" выберите домен, связанный с ролью, которую требуется сопоставить платформе BI.
5. Используйте один из следующих параметров, чтобы выбрать роли, которые нужно сопоставить:
 - В области Роли PeopleSoft Enterprise в поле "Поиск ролей" введите роль, которую нужно найти и для которой нужно установить соответствие в платформе BI, а затем щелкните значок >.
 - В списке «Доступные роли» выберите роль, которую требуется сопоставить платформе BI, а затем щелкните значок >.

Примечание:

- При поиске конкретного пользователя или конкретной роли можно использовать символ-шаблон %. Например, для поиска всех ролей, начинающихся с буквы "A", введите **A%**. При поиске также учитывается регистр слов.
 - Если требуется установить соответствие для роли из другого домена, нужно выбрать новый домен в списке доступных доменов.
6. Для принудительной синхронизации групп и пользователей между платформой BI и PeopleSoft установите флажок **Принудительно синхронизировать пользователя**. Чтобы удалить уже импортированные группы PeopleSoft из платформы BI, не устанавливайте флажок **Принудительно синхронизировать пользователя**.
 7. В области «Параметры нового псевдонима» выберите один из следующих параметров:
 - **Назначать каждому добавленному псевдониmu учетную запись с таким же именем**

Выберите этот параметр, если вы работаете с несколькими системами PeopleSoft Enterprise, и пользователи имеют учетные записи в нескольких системах (и нет двух одинаковых имен пользователя в разных системах для двух разных пользователей).

- **Создать новую учетную запись для каждого добавляемого псевдонима**

Выберите этот параметр, если вы работаете только с одной системой PeopleSoft Enterprise, если большинство пользователей имеют учетные записи только на одной из систем, или если имена пользователей совпадают для разных пользователей на двух или более системах.

8. В области **Параметры обновления** выберите один из следующих параметров:

- **Будут добавлены новые псевдонимы, и будут созданы новые пользователи**

Этот параметр используется для создания нового псевдонима для каждого пользователя, для которого устанавливается соответствие в платформе BI. Новые учетные записи создаются для пользователей, у которых нет учетных записей в платформе BI, или для всех пользователей, если выбран параметр "Создать новую учетную запись для каждого добавленного псевдонима".

- **Новые псевдонимы не будут добавлены, и новые пользователи не будут созданы**

Этот параметр используется в том случае, если роль, для которой устанавливается соответствие, содержит много пользователей, но только некоторые из них будут использовать платформу BI. Платформа не создает псевдонимы и учетные записи для пользователей автоматически. Вместо этого она создает псевдонимы (и при необходимости учетные записи) при первом входе пользователей в платформу BI. Этот параметр выставлен по умолчанию.

9. В области **Параметры нового пользователя** укажите, как создаются новые пользователи.

Если лицензия платформы SAP BusinessObjects Business Intelligence не основана на ролях пользователей, выберите один из перечисленных ниже параметров.

- **Новые пользователи создаются как BI Viewer**

Учетные записи новых пользователей создаются с ролью BI Viewer. Доступ к приложениям платформы BI для всех учетных записей роли BI Viewer определяется в лицензионном соглашении. Пользователи ограничены доступом к рабочим процессам приложений, которые определены для роли BI Viewer. Права доступа обычно ограничены просмотром документов Business Intelligence. Эта роль обычно подходит для пользователей, которые используют контент через приложения платформы BI.

- **Новые пользователи создаются как BI Analyst** Учетные записи новых пользователей создаются с ролью BI Analyst. Доступ к приложениям платформы BI для всех учетных записей роли BI Analyst определяется в лицензионном соглашении. Пользователи могут обращаться ко всем рабочим процессам приложений, которые определены для роли BI Analyst. Права доступа включают просмотр и изменение документов Business Intelligence. Эта роль обычно подходит для пользователей, которые создают и изменяют контент для приложений платформы BI.

Если лицензия платформы SAP BusinessObjects Business Intelligence не основана на ролях пользователей, выберите один из перечисленных ниже параметров.

- **Новые пользователи создаются как именованные пользователи.**

Новые учетные записи пользователей настраиваются на использование именованных пользовательских лицензий. Именованные пользовательские лицензии связаны с конкретными пользователями и позволяют им входить в систему, используя имя пользователя и пароль. Это дает именованным пользователям право доступа к системе независимо от того, сколько других пользователей выполнили вход. Для каждой учетной записи, созданной с использованием данного параметра, должна существовать именованная пользовательская лицензия.

- **Новые пользователи создаются как конкурентные пользователи.**

Новые учетные записи пользователей настраиваются на использование конкурентных пользовательских лицензий. В лицензии на одновременный доступ указывается количество человек, которые могут подключиться к платформе BI одновременно. Это очень гибкий тип лицензий, так как небольшое их количество поддерживает широкую пользовательскую базу. Например, в зависимости от того, как часто и как долго пользователи работают с платформой BI, лицензия на одновременный доступ для 100 пользователей может поддерживать 250, 500 или 700 пользователей.

Выбранные роли теперь отображаются как группы в платформе BI.

7.6.3.2 Выполнение переназначения

При добавлении пользователей в уже сопоставленную роль для их отображения в платформе BI следует повторно сопоставить эту роль. При повторном сопоставлении роли параметр сопоставления в качестве именованных пользователей или пользователей с одновременным доступом влияет только на новых пользователей, добавленных в роль.

Например, первоначально роль сопоставлена платформе BI с параметром "Новые пользователи создаются как именованные пользователи". Затем можно добавлять пользователей в ту же роль и заново сопоставлять роль с выбранным параметром "Новые пользователи создаются как параллельные пользователи".

В этом случае только новые пользователи сопоставляются платформе BI как пользователи с одновременным доступом; пользователи, которые уже были сопоставлены, остаются именованными пользователями. Такое же условие применяется, если изначально пользователи были сопоставлены как пользователи с одновременным доступом, а затем выполняется изменение настроек, и новые пользователи сопоставляются как именованные.

7.6.3.3 Отмена отображения роли

1. Выполните вход в систему Central Management Console под учетной записью администратора.
2. Нажмите кнопку **Аутентификация**.

3. Щелкните **PeopleSoft Enterprise**.
4. Нажмите кнопку **Роли**.
5. Выберите роль, которую требуется удалить, и нажмите кнопку **<**.
6. Нажмите кнопку **Обновить**.

У элементов роли теперь не будет доступа к платформе BI, пока не будут созданы другие учетные записи или псевдонимы.

Примечание:

Можно также удалять отдельные учетные записи или пользователей из ролей перед их сопоставлением платформе BI, чтобы запретить определенным пользователям выполнять вход в систему.

7.6.4 Планирование пользовательских обновлений

Чтобы изменения в данных пользователя в системе ERP отражались в данных пользователя платформы BI, можно запланировать регулярные обновления пользователей. Эти обновления автоматически синхронизируют пользователей ERP и платформы BI в соответствии с параметрами сопоставления, настроенными в Central Management Console (CMC).

Существуют два варианта запуска и планирования обновлений для импортированных ролей:

- Обновлять только роли: если используется этот параметр, будут обновлены только ссылки между сопоставленными в настоящий момент ролями, импортированными в платформу BI. Этот параметр следует использовать в тех случаях, когда планируется частое выполнение обновлений, и требуется обеспечить эффективное использование ресурсов системы. Если обновляются только роли, новых учетных записей создано не будет.
- Обновлять роли и псевдонимы: этот параметр не только обновляет ссылки между ролями, но также создает новые учетные записи пользователей в платформе BI для новых пользовательских псевдонимов, добавляемых в систему ERP.

Примечание:

Если не было указано автоматическое создание псевдонимов для обновлений при включенной аутентификации, для новых псевдонимов не будут созданы учетные записи.

7.6.4.1 Планирование обновлений пользователя

После сопоставления ролей в платформе BI необходимо указать, как система будет обновлять эти роли.

1. Щелкните вкладку **Обновление пользователя**.

2. Щелкните **Расписание** в разделе «Обновлять только роли» или в разделе «Обновлять роли и псевдонимы».

Совет:

Если необходимо немедленно запустить обновление, выберите команду **Обновить сейчас**.

Совет:

Используйте параметр «Обновлять только роли», если нужны частые обновления и имеются проблемы с системными ресурсами. Системе нужно больше времени на обновление ролей и псевдонимов.

Будет открыто диалоговое окно «Повтор».

3. Выберите параметр в списке «Запуск объекта» и введите всю запрашиваемую информацию о планировании.

При создании расписания обновления можно выбрать типы повтора, представленные в следующей таблице.

Тип повтора	Описание
Ежечасно	Обновление будет запускаться каждый час. Вы указываете в какое время должен выполняться объект, а также дату начала и окончания.
Ежедневно	Обновление будет запускаться ежедневно или через указанное количество дней. Можно указать, в какое время объект будет выполняться, а также дату начала и окончания.
Каждую неделю	Обновление будет запускаться каждую неделю. Оно может запускаться один или несколько раз в неделю. Можно указать, в какие дни и в какое время он будет выполняться, а также дату начала и окончания.
Ежемесячно	Обновление будет запускаться каждый месяц или каждые несколько месяцев. Можно указать время запуска, а также дату начала и окончания.
N-й день месяца	Обновление будет запускаться в определенный день месяца. Можно указать день месяца, время запуска, а также дату начала и окончания.
Первый понедельник месяца	Обновление будет запускаться в первый понедельник каждого месяца. Можно указать время выполнения, а также даты начала и окончания.
Последний день месяца	Обновление будет запускаться в последний день каждого месяца. Можно указать время выполнения, а также даты начала и окончания.

Тип повтора	Описание
X день N-ной недели месяца	Обновление будет запускаться в указанный день указанной недели месяца. Можно указать время выполнения, а также даты начала и окончания.
Календарь	Обновление будет запускаться по датам, указанным в созданном календаре.

4. Щелкните **Расписание** после того, как будет окончен ввод информации о планировании. Дата следующего запланированного обновления роли отображается на вкладке **Обновление пользователя**.

Примечание:

Всегда можно отменить следующее запланированное событие, щелкнув **Отменить запланированные обновления** в разделе «Обновлять только роли» или «Обновлять роли и псевдонимы».

7.6.5 Использование моста безопасности PeopleSoft

Функция моста безопасности в платформе BI позволяет импортировать параметры безопасности PeopleSoft EPM в платформу BI.

Мост безопасности работает в двух описанных далее режимах.

- Режим настройки

В режиме настройки мост безопасности предоставляет интерфейс, позволяющий создать файл ответов. Этот файл ответов определяет работу моста безопасности в режиме выполнения.

- Режим выполнения

В соответствии с параметрами, заданными в файле ответов, мост безопасности импортирует параметры безопасности таблиц измерений из PeopleSoft EPM в юниверсы в платформе BI.

7.6.5.1 Импорт настроек безопасности

Чтобы импортировать настройки безопасности, необходимо в указанном порядке выполнить перечисленные ниже действия.

- Определить, какие объекты будут управляться с помощью моста безопасности.

- Создать файл ответов.
- Запустить приложение "Мост безопасности".

Для получения сведений об управлении безопасностью после импорта настроек см. раздел Изменение настроек безопасности.

7.6.5.1.1 Определение управляемых объектов

Перед запуском моста безопасности необходимо определить объекты, которые будут управляться этим приложением. Мост безопасности управляет одной или несколькими ролями PeopleSoft, группой платформы BI и одним или несколькими юниверсами.

- Управляемые роли PeopleSoft

В системе PeopleSoft имеются различные роли. Исполнители этих ролей работают с данными PeopleSoft через PeopleSoft EPM. Необходимо выбрать роли, исполнителям которых требуется предоставить или обновить права доступа к управляемым юниверсам в платформе BI.

Права доступа, определяемые для исполнителей этих ролей, основываются на их правах в PeopleSoft EPM. Мост безопасности импортирует эти настройки безопасности в платформу BI.

- Управляемая группа платформы BI

При запуске моста безопасности эта программа создает пользователя в платформе BI для каждого исполнителя управляемой роли в PeopleSoft.

Группа, в которой создаются пользователи, — это управляемая группа платформы BI. Участниками этой группы являются пользователи, чьи права доступа к управляемым юниверсам регулируются с помощью моста безопасности. Поскольку пользователи создаются в одной группе, можно настроить мост безопасности так, чтобы настройки безопасности не обновлялись для определенных пользователей. Для этого достаточно удалить этих пользователей из управляемой группы платформы BI.

Перед запуском моста безопасности необходимо выбрать группу в платформе BI, в которой будут создаваться пользователи. Если указать несуществующую группу, мост безопасности создаст ее в платформе BI.

- Управляемые юниверсы

Юниверсы, в которые мост безопасности импортирует настройки защиты из PeopleSoft EPM, называются управляемыми. Необходимо выбрать, какие именно юниверсы из хранящихся в платформе BI будут управляться с помощью моста безопасности. Исполнители управляемых ролей PeopleSoft, также являющиеся членами управляемой группы платформы BI, не могут осуществлять доступ через эти юниверсы к тем данным, к которым у них нет доступа через PeopleSoft EPM.

7.6.5.1.2 Создание файла ответов

1. Откройте папку, указанную при установке моста безопасности, и запустите файл `crpsepmsecuritybridge.bat` (в системе Windows) или `crpsepmsecuritybridge.sh` (в системе Unix).

Примечание:

В системе Windows по умолчанию для установки предлагается папка "C:\Program Files\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\epm"

Появится диалоговое окно "Мост безопасности для PeopleSoft EPM".

2. Выберите **Создать**, чтобы создать файл ответа, либо нажмите **Открыть**, выберите **Обзор** и укажите файл ответа, который требуется изменить. Выберите язык файла.
3. Нажмите кнопку **Далее**.
4. Укажите каталоги **PeopleSoft EPM SDK** и **BI Platform SDK**.

Примечание:

- PeopleSoft EPM SDK обычно располагается на сервере PeopleSoft по адресу "<PS_HOME>/class/com.peoplesoft.epm.pf.jar".
- Пакет SDK платформы BI обычно располагается в папке C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib.

5. Нажмите кнопку **Далее**.

Появится диалоговое окно для ввода информации о соединении и драйверах для базы данных PeopleSoft.

6. Из списка "Базы данных" выберите надлежащий тип базы данных и заполните следующие поля:

Поле	Описание
База данных	Имя базы данных PeopleSoft.
Хост	Имя сервера, на котором размещена база данных.
Номер порта	Номер порта для доступа к серверу.
Местоположение класса	Местоположение файлов класса для драйвера базы данных.
Имя пользователя	Ваше имя пользователя.
Пароль	Ваш пароль.

7. Нажмите кнопку **Далее**.

В диалоговом окне отобразится список всех классов, которые будут использоваться при запуске моста безопасности. При необходимости можно добавить или удалить классы из списка.

8. Нажмите кнопку **Далее**.

Откроется диалоговое окно для ввода информации о подключении к платформе BI.

9. Введите соответствующую информацию в следующие поля:

Поле	Описание
Сервер	Имя сервера, на котором расположен центральный сервер управления (CMS).
Имя пользователя	Ваше имя пользователя.
Пароль	Ваш пароль.
Аутентификация	Ваш тип аутентификации.

10. Нажмите кнопку **Далее**.

11. Выберите группу платформы BI и нажмите кнопку **Далее**.

Примечание:

- В данном поле указывается группа, в которой мост безопасности создает пользователей для исполнителей подконтрольных ролей PeopleSoft.
- Если указать группу, которая в данный момент не существует, она будет создана мостом безопасности.

В диалоговом окне отобразится список ролей в вашей системе PeopleSoft.

12. Задайте параметр **Импортировано** для ролей, которыми должен управлять мост безопасности, а затем нажмите кнопку **Далее**.

Примечание:

Мост безопасности создаст пользователя в управляемой группе платформы BI (указанной на предыдущем этапе) для каждого из выбранных членов ролей.

Откроется диалоговое окно со списком юниверсов в платформе BI.

13. Выберите юниверсы, в которые мост безопасности должен произвести импорт настроек безопасности, а затем нажмите кнопку **Далее**.

14. Укажите имя файла журнала моста безопасности и каталог, в котором необходимо его сохранить. По файлу журнала можно будет определить, успешно ли импортированы настройки безопасности из PeopleSoft EPM с помощью моста безопасности.

15. Нажмите кнопку **Далее**.

В диалоговом окне будет выведен предварительный просмотр файла ответов, который будет использоваться мостом безопасности на этапе выполнения.

16. Нажмите **Сохранить** и укажите каталог, в котором требуется сохранить файл ответов.

17. Нажмите кнопку **Далее**.

Будет создан файл ответов для моста безопасности.

18. Нажмите **Выход**.

Примечание:

Файл ответов представляет собой файл свойств на языке Java, который также можно создавать и редактировать вручную. Для получения дополнительных сведений см. раздел «Файл ответов PeopleSoft».

7.6.5.2 Применение настроек безопасности

Чтобы применить настройки безопасности, запустите файл `crpsepmsecuritybridge.bat` (в ОС Windows) или `crpsepmsecuritybridge.sh` (в ОС UNIX) и в качестве аргумента укажите созданный ранее файл ответа (например, введите `crpsepmsecuritybridge.bat (Windows)` или `crpsepmsecuritybridge.sh (unix) myresponsefile.properties`).

Запустится приложение моста безопасности. Он создаст пользователей в платформе BI для элементов ролей PeopleSoft, указанных в файле ответов, и импортирует настройки безопасности из PeopleSoft EPM в соответствующие универсы.

7.6.5.2.1 Примечания по отображению ролей

В режиме выполнения мост безопасности создает пользователя в платформе BI для каждого члена управляемой роли в PeopleSoft.

Созданные пользователи имеют только псевдонимы для аутентификации в Enterprise, и платформа BI присваивает каждому пользователю пароль, сгенерированный случайным образом. Таким образом, пользователи не могут выполнить вход в платформу BI, воспользовавшись своими учетными данными из PeopleSoft, до тех пор, пока администратор не назначит им новые пароли вручную или не выполнит сопоставление ролей в платформе BI с помощью подключаемого модуля PeopleSoft Security.

7.6.5.3 Изменение настроек безопасности

Можно изменять указанные ранее настройки безопасности путем изменения объектов, управляемых мостом безопасности.

7.6.5.3.1 Управляемые пользователи

Мост безопасности управляет пользователями в соответствии со следующими критериями:

- Является ли пользователь исполнителем управляемой роли в PeopleSoft.
- Является ли пользователь членом управляемой группы в платформе BI.

Если пользователю необходимо предоставить доступ к данным PeopleSoft через юниверсы платформы BI, убедитесь, что он одновременно является как членом управляемой роли PeopleSoft, так и членом управляемой группы платформы BI.

- Для членов управляемых ролей в PeopleSoft, не имеющих учетной записи в платформе BI, мост безопасности самостоятельно создает учетные записи и назначает пароли, сгенерированные случайным образом. Администратор может предоставить пользователям возможность входа в платформу BI, назначив для них новые пароли вручную или выполнив сопоставление соответствующих ролей в платформе BI с помощью подключаемого модуля PeopleSoft Security.
- Для членов управляемых ролей PeopleSoft, которые также являются членами управляемой группы платформы BI, мост безопасности изменяет настройки безопасности, применяемые к этим пользователям, предоставляя им доступ к соответствующим данным из управляемых юниверсов.

Если у члена управляемой роли PeopleSoft имеется учетная запись в платформе BI, но он не является членом управляемой группы платформы BI, мост безопасности не изменяет настройки безопасности для этого пользователя. Как правило, эта ситуация возникает только в том случае, если администратор вручную удаляет учетные записи пользователей, созданные мостом безопасности, из управляемой группы платформы BI.

Примечание:

Это достаточно эффективный метод управления защитой: удаляя пользователей из управляемой группы платформы BI, можно указывать для них настройки безопасности, отличные от действующих в PeopleSoft.

И наоборот, если член управляемой группы платформы BI не является членом управляемой роли PeopleSoft, то мост безопасности не предоставляет ему доступ к управляемым юниверсам. Как правило, такая ситуация возникает только в том случае, если администратор PeopleSoft удаляет пользователей, для которых ранее было выполнено сопоставление в платформе BI с помощью моста безопасности из управляемой роли PeopleSoft.

Примечание:

Это еще один метод управления безопасностью: удаляя пользователей из управляемых ролей PeopleSoft, вы гарантировано лишаете их доступа к данным из PeopleSoft.

7.6.5.3.2 Управляемые юниверсы

Мост безопасности управляет юниверсами с помощью наборов ограничений, регулирующих доступ к данным из управляемых юниверсов для управляемых пользователей.

Наборы ограничений – это группы ограничений (например, ограничения для контроля запросов, создания SQL и т.п.). Мост безопасности применяет/обновляет ограничения на доступ к строке и доступ к объекту для подконтрольных юниверсов:

- Ограничения на доступ к строке применяются к таблицам измерений, заданным в PeopleSoft EPM. Данные ограничения можно настраивать для каждого пользователя в отдельности. Можно задать один из следующих параметров:
 - Пользователь имеет доступ ко всем данным.
 - Пользователь не имеет доступ ко всем данным.
 - Пользователь имеет доступ к данным согласно его уровню допуска, заданному в PeopleSoft, который выводится через таблицы Security Join Tables (SJT), определяемые в PeopleSoft EPM.
- Применяются ограничения на доступ для объектов величин в зависимости от полей, к которым эти объекты мер осуществляют доступ.

Если объект меры осуществляет доступ к полям, которые определены в PeopleSoft как показатели, то доступ к объекту меры разрешается или запрещается, в зависимости от наличия у пользователя прав на доступ к этой мере в PeopleSoft. Если пользователь не имеет доступ к какому-либо показателю, то доступ к объекту величины запрещается. Если пользователь имеет доступ ко всем показателям, то доступ к объекту величины разрешается.

Будучи администратором, вы также можете ограничить данные, к которым пользователи имеют доступ из системы PeopleSoft, ограничив количество юниверсов, управляемых с помощью моста безопасности.

7.6.5.4 Файл ответов PeopleSoft

Функция "Мост безопасности" платформы BI работает на основе параметров, указанных в файле ответов.

Как правило, файл ответов создается с помощью интерфейса, представленного мостом безопасности в режиме настройки. Однако, поскольку файл является файлом Java, его также можно создать или изменить вручную.

В данном приложении приводится информация о параметрах, которые необходимо включить в файл ответа, если он создается вручную.

Примечание:

При создании файла необходимо соблюдать требования символам выхода в файлах Java (например, ':' обозначается как '\:').

7.6.5.4.1 Параметры файла ответов

В таблице ниже описываются параметры, которые содержатся в файле ответа.

Параметр	Описание
classpath	<p>Путь класса для загрузки необходимых файлов .jar. Если указывается несколько путей классов, в качестве разделителя используется ';' (как в Windows, так и в UNIX).</p> <p>Пути классов, необходимые для файлов com.peoplesoft.epm.pf.jar и файлов .jar драйвера JDBC.</p>
db.driver.name	Имя драйвера JDBC, используемое для подключения базы данных PeopleSoft (например, "com.microsoft.jdbc.sqlserver.SQLServerDriver").
db.connect.str	Строка подключения JDBC, используемая для подключения к базе данных PeopleSoft (например, "jdbc:sqlserver://andps01:1433;DatabaseName=PRDMO")
db.user.name	Имя пользователя для подключения к базе данных PeopleSoft.
db.password	Пароль для подключения к базе данных PeopleSoft.
db.password.encrypted	Значение этого параметра определяет, зашифрован ли пароль в файле ответов. Допустимые значения: "true" и "false". Если значение не указано, по умолчанию принимается значение "false".
enterprise.cms.name	Центральный сервер управления, в котором размещены юниверсы.
enterprise.user.name	Имя пользователя для подключения к центральному серверу управления.
enterprise.password	Пароль для подключения к центральному серверу управления.

Параметр	Описание
enterprise.password.encrypted	Значение этого параметра определяет, зашифрован ли пароль в файле ответов. Допустимые значения: "true" и "false". Если значение не указано, по умолчанию принимается значение "false".
enterprise.authMethod	Метод аутентификации, используемый для подключения к центральному серверу управления.
enterprise.role	Управляемая группа платформы BI. Для получения дополнительных сведений см. Определение управляемых объектов .
enterprise.license	Определяет тип лицензии при импорте пользователей из Peoplesoft. "0" задает лицензию для именованных пользователей, а "1" – лицензию на одновременный доступ.
peoplesoft.role.n	<p>Список управляемых ролей PeopleSoft. Для получения дополнительных сведений см. Определение управляемых объектов.</p> <p><i>n</i> – целое число, и каждой записи присваивается свойство с помощью префикса "peoplesoft.role".</p> <p>Примечание: <i>n</i> не должно быть менее 1.</p> <p>Символом "*" можно обозначить все доступные роли PeopleSoft (при условии, что <i>n</i>=1, и что это единственное свойство, имеющее префикс "peoplesoft.role" в файле ответов).</p>

Параметр	Описание
mapped.universe.n	<p>Список юниверсов, которые мост безопасности должен обновить. Для получения дополнительных сведений см. Определение управляемых объектов.</p> <p>n – целое число, и каждой записи присваивается свойство с помощью префикса "mapped.universe".</p> <p>Примечание: n не должно быть менее 1.</p> <p>Символом "*" можно обозначить все доступные юниверсы (при условии, что $n=1$, и оно является единственным свойством, имеющим префикс "mapped.universe" в файле ответа).</p>
log4j.appender.file.File	Файл журнала, создаваемый мостом безопасности.
log4j.*	<p>Свойства log4j по умолчанию, необходимые для надлежащей работы log4j:</p> <p>log4j.rootLogger=INFO, file, stdout</p> <p>log4j.appender.file=org.apache.log4j.RollingFileAppender</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>Путь класса к файлам .jar PeopleSoft EPM API.</p> <p>Это необязательный параметр.</p>

Параметр	Описание
enterprise.classpath	Путь класса к файлам .jar SDK платформы BI. Это необязательный параметр.
db.driver.type	Тип базы данных PeopleSoft. Этот параметр может иметь одно из следующих значений: Microsoft SQL Server 2000 Oracle Database 10.1 DB2 UDB 8.2 Fixpack 7 Пользовательский Значение "Пользовательский" используется для указания базы данных, тип или версия которой отличаются от стандартных. Это необязательный параметр.
sql.db.class.location sql.db.host sql.db.port sql.db.database	Местоположение файлов .jar драйвера JDBC SQL Server, хост SQL Server, порт SQL Server и имя базы данных SQL Server. Эти параметры можно использовать, только если "db.driver.type" имеет значение "Microsoft SQL Server 2000". Это необязательные параметры.
oracle.db.class.location oracle.db.host oracle.db.port oracle.db.sid	Местоположение файлов .jar драйвера JDBC Oracle, хост базы данных Oracle, порт базы данных Oracle и SID базы данных Oracle. Эти параметры можно использовать, только если параметр "db.driver.type" имеет значение "Oracle Database 10.1". Это необязательные параметры.

Параметр	Описание
db2.db.class.location db2.db.host db2.db.port db2.db.sid	<p>Местоположение файлов .jar драйвера JDBC DB2, хост базы данных DB2, порт базы данных DB2 и SID базы данных DB2.</p> <p>Эти параметры можно использовать, только если параметр "db.driver.type" имеет значение "DB2 UDB 8.2 Fixpack 7"</p> <p>Это необязательные параметры.</p>
custom.db.class.location custom.db.drivertype custom.db.connectStr	<p>Местоположение, имя и строка подключения нестандартного драйвера JDBC.</p> <p>Эти параметры можно использовать, только если параметр "db.driver.type" имеет значение "Custom".</p> <p>Это необязательные параметры.</p>

7.7 Аутентификация JD Edwards

7.7.1 Обзор

Для использования имеющихся данных JD Edwards с платформой BI необходимо предоставить системе информацию о развертывании JD Edwards. Эта информация позволяет платформе BI выполнять аутентификацию пользователей так, что они могут использовать свои учетные данные JD Edwards EnterpriseOne для входа в платформу BI.

7.7.2 Включение аутентификации JD Edwards EnterpriseOne

Чтобы можно было использовать информацию JD Edwards EnterpriseOne в платформе BI, системе нужны данные об аутентификации в системе JD Edwards EnterpriseOne.

7.7.2.1 Включение аутентификации JD Edwards в платформе BI

1. Войдите в систему Central Management Console под учетной записью администратора.
2. В области "Управление" щелкните **Аутентификация**.
3. Дважды щелкните **JD Edwards EnterpriseOne**.
На экране будет отображена страница «JD Edwards EnterpriseOne». У этой страницы четыре вкладки: **Параметры**, **Серверы**, **Роли** и **Обновление пользователя**.
4. На вкладке **Параметры** установите флажок **Включить аутентификацию JD Edwards EnterpriseOne**.
5. Внесите необходимые изменения в поля **Создать псевдоним**, **Обновить параметры** и **Параметры нового пользователя** в соответствии с имеющимся развертыванием платформы BI. Нажмите кнопку **Обновить** для сохранения изменений перед переходом на вкладку **Системы**.
6. Нажмите вкладку **Серверы**.
7. В области «Пользователь системы JD Edwards EnterpriseOne» введите имя пользователя базы данных и пароль, которые следует использовать в платформе BI для выполнения входа в базу данных JD Edwards EnterpriseOne.
8. В области «Домен JD Edwards EnterpriseOne» введите имя, хост и порт, используемые для подключения к среде JD Edwards EnterpriseOne, введите имя среды и нажмите кнопку **Добавить**.
9. Нажмите кнопку **Обновить**, чтобы сохранить изменения.

7.7.3 Сопоставление ролей JD Edwards EnterpriseOne в платформе BI

Платформа BI автоматически создает группу для каждой сопоставляемой роли JD Edwards EnterpriseOne. Кроме того, система создает псевдонимы для участников отображенных ролей JD Edwards EnterpriseOne.

Можно создать учетную запись пользователя для каждого созданного псевдонима.

Однако если вы работаете с несколькими системами и пользователи имеют учетные записи более чем на одной системе, то можно назначить каждого пользователя псевдониму с тем же именем перед созданием учетных записей в платформе BI.

Эта операция сокращает количество учетных записей, создаваемых для одного и того же пользователя в платформе BI.

Например, если используется тестовая и продуктивная среда JD Edwards EnterpriseOne и 30 пользователей имеют доступ к обеим системам, то для них будет создано только 30 учетных записей. Если не назначать каждого пользователя псевдониmu с тем же именем, то для 30 пользователей в платформе BI будет создано 60 учетных записей.

Однако при работе с несколькими системами и совпадении имен пользователей нужно создать новую учетную запись участника для каждого создаваемого псевдонима.

Например, если в тестовой среде используется учетная запись Russell Aquino (имя пользователя "raquno"), а в производственной среде – учетная запись пользователя Raoul Aquino (имя пользователя "raquno"), то необходимо создать отдельную учетную запись для каждого псевдонима пользователя. Если этого не сделать, оба пользователя будут добавлены к одной и той же учетной записи платформы BI, и они не смогут входить в платформу BI, используя свои учетные данные JD Edwards EnterpriseOne.

7.7.3.1 Сопоставление роли JD Edwards EnterpriseOne

1. Войдите в систему Central Management Console под учетной записью администратора.
2. В области «Управление» щелкните **Аутентификация**.
3. Дважды щелкните **JD Edwards EnterpriseOne**.
4. В области **Параметры нового псевдонима** выберите один из следующих параметров:

- **Назначать каждому добавленному псевдониму учетную запись с таким же именем**

Выберите этот параметр, если вы работаете с несколькими системами JD Edwards EnterpriseOne Enterprise, и пользователи имеют учетные записи в нескольких системах (и нет двух одинаковых имен пользователя в разных системах для двух разных пользователей).

- **Создать новую учетную запись для каждого добавляемого псевдонима**

Выберите этот параметр, если вы работаете только с одной системой JD Edwards EnterpriseOne, если большинство пользователей имеют учетные записи только на одной из систем, или если имена пользователей совпадают для разных пользователей на двух или более системах.

5. В области **Параметры обновления** выберите один из следующих параметров:

- **Будут добавлены новые псевдонимы, и будут созданы новые пользователи**

Выберите этот параметр, чтобы создавать новый псевдоним для каждого пользователя, для которого устанавливается соответствие в платформе BI. Новые учетные записи создаются для пользователей, у которых нет учетных записей платформы BI, или для всех пользователей, если выбран параметр "Создать новую учетную запись для каждого добавляемого псевдонима".

- **Новые псевдонимы не будут добавлены, и новые пользователи не будут созданы**

Выберите этот параметр, если роль, для которой устанавливается соответствие, содержит много пользователей, но только некоторые из них будут использовать платформу BI.

Система не создает псевдонимы и учетные записи для пользователей автоматически. Вместо этого псевдонимы (и учетные записи, при необходимости) создаются только для пользователей, которые входят в платформу BI первый раз. Этот параметр выставлен по умолчанию.

6. В области **Параметры нового пользователя укажите, как создаются новые пользователи.**

Если лицензия платформы SAP BusinessObjects Business Intelligence основана на ролях пользователей, выберите один из перечисленных ниже параметров:

- **Новые пользователи создаются как BI Viewer**

Учетные записи новых пользователей создаются с ролью BI Viewer. Доступ к приложениям платформы BI для всех учетных записей роли BI Viewer определяется в лицензионном соглашении. Пользователи ограничены доступом к рабочим процессам приложений, которые определены для роли BI Viewer. Права доступа обычно ограничены просмотром документов Business Intelligence. Эта роль обычно подходит для пользователей, которые используют контент через приложения платформы BI.

- **Новые пользователи создаются как BI Analyst**

Учетные записи новых пользователей создаются с ролью BI Analyst. Доступ к платформе BI для всех учетных записей роли BI Analyst определяется в лицензионном соглашении. Пользователи могут обращаться ко всем рабочим процессам приложений, которые определены для роли BI Analyst. Права доступа включают просмотр и изменение документов Business Intelligence. Эта роль обычно подходит для пользователей, которые создают и изменяют контент для приложений платформы BI.

Если лицензия платформы SAP BusinessObjects Business Intelligence не основана на ролях пользователей, выберите один из перечисленных ниже параметров:

- **Новые пользователи создаются как именованные пользователи.**

Новые учетные записи пользователей настраиваются на использование именованных пользовательских лицензий. Именованные пользовательские лицензии связаны с конкретными пользователями и позволяют им входить в систему, используя имя пользователя и пароль. Это дает именованным пользователям право доступа к системе независимо от того, сколько других пользователей выполнили вход. Для каждой учетной записи, созданной с использованием данного параметра, должна существовать именованная пользовательская лицензия.

- **Новые пользователи создаются как конкурентные пользователи.**

Новые учетные записи пользователей настраиваются на использование конкурентных пользовательских лицензий. Лицензии на одновременный доступ указывают количество человек, которые могут подключиться к платформе BI одновременно. Это очень гибкий тип лицензий, так как небольшое их количество поддерживает широкую пользовательскую базу. Например, в зависимости от того, как часто и как долго пользователи работают с платформой BI, лицензия на одновременный доступ для 100 пользователей может поддерживать 250, 500 или 700 пользователей.

Выбранные роли теперь отображаются как группы в платформе BI.

7. Перейдите на вкладку **Роли.**

8. В **Выберите сервер** выберите сервер JD Edwards, содержащий роли, которые нужно сопоставить.
9. В «Импортированных ролях» выберите роли, которые требуется сопоставить платформе BI и нажмите <.
10. Щелкните **Обновить**.
Роли будут сопоставлены платформе BI.

7.7.3.2 Выполнение переназначения

При добавлении пользователей в уже сопоставленную роль для их отображения в платформе BI следует повторно сопоставить эту роль. При повторном сопоставлении роли параметр сопоставления в качестве именованных пользователей или пользователей с одновременным доступом влияет только на новых пользователей, добавленных в роль.

Например первоначально роль сопоставлена платформе BI с параметром "Новые пользователи создаются как именованные пользователи". Затем можно добавлять пользователей в ту же роль и выполнять ее повторное сопоставление с выбранным параметром "Новые пользователи создаются как параллельные пользователи".

В этом случае только новые пользователи сопоставляются платформе BI как пользователи с одновременным доступом; пользователи, которые уже были сопоставлены, остаются именованными пользователями. Такое же условие применяется, если изначально пользователи были сопоставлены как пользователи с одновременным доступом, а затем выполняется изменение настроек, и новые пользователи сопоставляются как именованные.

7.7.3.3 Отмена отображения роли

1. Выполните вход в систему Central Management Console под учетной записью администратора.
2. В области «Управление» щелкните **Аутентификация**.
3. Щелкните вкладку **JD Edwards EnterpriseOne**.
4. В области «Роли» выберите роль, которую необходимо удалить, и щелкните <.
5. Нажмите кнопку **Обновить**.

У элементов роли теперь не будет доступа к платформе BI, пока не будут созданы другие учетные записи или псевдонимы.

Примечание:

Можно также удалять отдельные учетные записи или пользователей из ролей перед их сопоставлением платформе BI, чтобы запретить определенным пользователям выполнять вход в систему.

7.7.4 Планирование пользовательских обновлений

Чтобы изменения в данных пользователя в системе ERP отражались в данных пользователя платформы BI, можно запланировать регулярные обновления пользователей. Эти обновления автоматически синхронизируют пользователей ERP и платформы BI в соответствии с параметрами сопоставления, настроенными в Central Management Console (CMC).

Существуют два варианта запуска и планирования обновлений для импортированных ролей:

- Обновлять только роли: если используется этот параметр, будут обновлены только ссылки между сопоставленными в настоящий момент ролями, импортированными в платформу BI. Этот параметр следует использовать в тех случаях, когда планируется частое выполнение обновлений, и требуется обеспечить эффективное использование ресурсов системы. Если обновляются только роли, новых учетных записей создано не будет.
- Обновлять роли и псевдонимы: этот параметр не только обновляет ссылки между ролями, но также создает новые учетные записи пользователей в платформе BI для новых пользовательских псевдонимов, добавляемых в систему ERP.

Примечание:

Если не было указано автоматическое создание псевдонимов для обновлений при включенной аутентификации, для новых псевдонимов не будут созданы учетные записи.

7.7.4.1 Планирование обновлений пользователя

После сопоставления ролей в платформе BI необходимо указать, как система будет обновлять эти роли.

1. Щелкните вкладку **Обновление пользователя**.
2. Щелкните **Расписание** в разделе «Обновлять только роли» или в разделе «Обновлять роли и псевдонимы».

Совет:

Если необходимо немедленно запустить обновление, выберите команду **Обновить сейчас**.

Совет:

Используйте параметр «Обновлять только роли», если нужны частые обновления и имеются проблемы с системными ресурсами. Системе нужно больше времени на обновление ролей и псевдонимов.

Будет открыто диалоговое окно «Повтор».

3. Выберите параметр в списке «Запуск объекта» и введите всю запрашиваемую информацию о планировании.

При создании расписания обновления можно выбрать типы повтора, представленные в следующей таблице.

Тип повтора	Описание
Ежечасно	Обновление будет запускаться каждый час. Вы указываете в какое время должен выполняться объект, а также дату начала и окончания.
Ежедневно	Обновление будет запускаться ежедневно или через указанное количество дней. Можно указать, в какое время объект будет выполняться, а также дату начала и окончания.
Каждую неделю	Обновление будет запускаться каждую неделю. Оно может запускаться один или несколько раз в неделю. Можно указать, в какие дни и в какое время он будет выполняться, а также дату начала и окончания.
Ежемесячно	Обновление будет запускаться каждый месяц или каждые несколько месяцев. Можно указать время запуска, а также дату начала и окончания.
N-й день месяца	Обновление будет запускаться в определенный день месяца. Можно указать день месяца, время запуска, а также дату начала и окончания.
Первый понедельник месяца	Обновление будет запускаться в первый понедельник каждого месяца. Можно указать время выполнения, а также даты начала и окончания.
Последний день месяца	Обновление будет запускаться в последний день каждого месяца. Можно указать время выполнения, а также даты начала и окончания.
X день N-ной недели месяца	Обновление будет запускаться в указанный день указанной недели месяца. Можно указать время выполнения, а также даты начала и окончания.
Календарь	Обновление будет запускаться по датам, указанным в созданном календаре.

4. Щелкните **Расписание** после того, как будет окончен ввод информации о планировании. Дата следующего запланированного обновления роли отображается на вкладке **Обновление пользователя**.

Примечание:

Всегда можно отменить следующее запланированное событие, щелкнув **Отменить запланированные обновления** в разделе «Обновлять только роли» или «Обновлять роли и псевдонимы».

7.8 Аутентификация Siebel

7.8.1 Включение аутентификации Siebel

Чтобы информация Siebel могла использоваться платформой BI, системе нужны сведения о том, как выполнять аутентификацию для входа в систему Siebel.

7.8.1.1 Включение аутентификации Siebel в платформе BI

1. Войдите в систему Central Management Console под учетной записью администратора.
2. В области "Управление" щелкните **Аутентификация**.
3. Дважды щелкните **Siebel**.
Откроется страница «Siebel». У этой страницы четыре вкладки: **Параметры**, **Системы**, **Ответственность** и **Обновление пользователя**.
4. На вкладке **Параметры** установите флажок в поле **Аутентификация Siebel включена**.
5. Внесите необходимые изменения в поля **Создать псевдоним**, **Обновить параметры** и **Параметры нового пользователя** в соответствии с имеющимся развертыванием платформы BI. Нажмите кнопку **Обновить** для сохранения изменений перед переходом на вкладку **Системы**.
6. Перейдите на вкладку **Домены**.
7. В поле **Имя Домена** введите имя домена для системы Siebel, к которой нужно подключиться.
8. В **Подключении** введите строку подключения для этого домена.
9. В области **Имя пользователя** введите имя пользователя базы данных и пароль, которые следует использовать в платформе BI для выполнения входа в базу данных Siebel.
10. В области **Пароль** введите пароль для выбранного пользователя.
11. Щелкните **Добавить**, чтобы добавить системную информацию к списку «Текущие домены».
12. Нажмите кнопку **Обновить**, чтобы сохранить изменения.

7.8.2 Сопоставление ролей платформе BI

Платформа BI автоматически создает группу для каждой сопоставляемой роли Siebel. Кроме того, программа создает псевдонимы для участников отображенных ролей Siebel.

Можно создать учетную запись пользователя для каждого созданного псевдонима.

Однако если вы работаете с несколькими системами и пользователи имеют учетные записи более чем на одной системе, то можно назначить каждого пользователя псевдониму с тем же именем перед созданием учетных записей в платформе BI.

Такая операция сокращает количество учетных записей, создаваемых для одного и того же пользователя в программе.

Например, при работе с тестовой Siebel eBusiness и средой производства, и 30 пользователей имеют доступ к обеим этим системам, то будет создано только 30 учетных записей. Если не назначать каждого пользователя псевдониму с тем же именем, то для 30 пользователей в платформе BI будет создано 60 учетных записей.

Однако при работе с несколькими системами и совпадении имен пользователей нужно создать новую учетную запись участника для каждого создаваемого псевдонима.

Например, если в тестовой среде используется учетная запись Russell Aquino (имя пользователя "raqino"), а в производственной среде – учетная запись пользователя Raoul Aquino (имя пользователя "raqino"), то необходимо создать отдельную учетную запись для каждого псевдонима пользователя. Если этого не сделать, оба пользователя добавятся к одной и той же учетной записи, и они не смогут выполнить вход в платформу BI, используя свои учетные данные Siebel eBusiness.

7.8.2.1 Сопоставление роли Siebel eBusiness платформе BI

1. Выполните вход в систему Central Management Console под учетной записью администратора.
2. Нажмите кнопку **Аутентификация**.
3. Дважды щелкните **Siebel**.
4. В области **Параметры нового псевдонима** выберите один из следующих параметров:
 - **Назначать каждому добавленному псевдониму учетную запись с таким же именем**
Выберите этот параметр, если ведется работа с несколькими системами Siebel eBusiness, и пользователи имеют учетные записи в нескольких системах (и нет двух одинаковых имен пользователя в разных системах для двух разных пользователей).
 - **Создать новую учетную запись для каждого добавляемого псевдонима**
Выберите этот параметр, если ведется работа с одной системой Siebel eBusiness, если большинство пользователей имеют учетные записи только на одной из систем, или если имена пользователей совпадают для разных пользователей на двух или более системах.
5. В области **Параметры обновления** выберите один из следующих параметров:
 - **Будут добавлены новые псевдонимы, и будут созданы новые пользователи**

Этот параметр используется для создания нового псевдонима для каждого пользователя, для которого устанавливается соответствие в платформе BI. Новые учетные записи создаются для пользователей, у которых нет учетных записей платформы BI, или для всех пользователей, если выбран параметр "Создать новую учетную запись для каждого добавляемого псевдонима".

- **Новые псевдонимы не будут добавлены, и новые пользователи не будут созданы**

Этот параметр используется в том случае, если роль, для которой устанавливается соответствие, содержит много пользователей, но только некоторые из них будут использовать платформу BI. Программа не создает псевдонимы и учетные записи для пользователей автоматически. Вместо этого она создает псевдонимы (и при необходимости учетные записи) при первом входе пользователей в платформу BI. Этот параметр выставлен по умолчанию.

6. В области **Параметры нового пользователя** укажите, как создаются новые пользователи.

Если лицензия платформы BI основана на ролях пользователей, выберите один из перечисленных ниже параметров.

- **Новые пользователи создаются как BI Viewer**

Учетные записи новых пользователей создаются с ролью BI Viewer. Доступ к приложениям платформы BI для всех учетных записей роли BI Viewer определяется в лицензионном соглашении. Пользователи ограничены доступом к рабочим процессам приложений, которые определены для роли BI Viewer. Права доступа обычно ограничены просмотром документов Business Intelligence. Эта роль обычно подходит для пользователей, которые используют контент через приложения платформы BI.

- **Новые пользователи создаются как BI Analyst**

Учетные записи новых пользователей создаются с ролью BI Analyst. Доступ к приложениям платформы BI для всех учетных записей роли BI Analyst определяется в лицензионном соглашении. Пользователи могут обращаться ко всем рабочим процессам приложений, которые определены для роли BI Analyst. Права доступа включают просмотр и изменение документов Business Intelligence. Эта роль обычно подходит для пользователей, которые создают и изменяют контент для приложений платформы BI.

Если лицензия на платформу BI не основана на ролях пользователей, выберите один из перечисленных ниже параметров.

- **Новые пользователи создаются как именованные пользователи.**

Новые учетные записи пользователей настраиваются на использование именованных пользовательских лицензий. Именованные пользовательские лицензии связаны с конкретными пользователями и позволяют им входить в систему, используя имя пользователя и пароль. Это дает именованным пользователям право доступа к системе независимо от того, сколько других пользователей выполнили вход. Для каждой учетной записи, созданной с использованием данного параметра, должна существовать именованная пользовательская лицензия.

- **Новые пользователи создаются как конкурентные пользователи.**

Новые учетные записи пользователей настраиваются на использование конкурентных пользовательских лицензий. В лицензии на одновременный доступ указывается количество

человек, которые могут подключиться к платформе BI одновременно. Это очень гибкий тип лицензий, так как небольшое их количество поддерживает широкую пользовательскую базу. Например, в зависимости от того, как часто и как долго пользователи работают с платформой BI, лицензия на одновременный доступ для 100 пользователей может поддерживать 250, 500 или 700 пользователей.

7. Перейдите на вкладку **Роли**.
8. Выберите домен, соответствующий серверу Siebel, для которого нужно сопоставить роли.
9. В списке «Доступные роли» выберите роли, которые нужно сопоставить, и нажмите кнопку **>**.

Примечание:

Поле **Поиск ролей, начинающихся с:** можно использовать для сужения круга поиска в случае большого количества ролей. Введите символы, с которых начинается роль или роли, затем символ шаблона (%) и щелкните **Поиск**.

10. Нажмите кнопку **Обновить**.
Роли будут сопоставлены платформе BI.

7.8.2.2 Выполнение переназначения

Для синхронизации групп и пользователей между платформой BI и Siebel установите флажок **Принудительно синхронизировать пользователя**.

Примечание:

Чтобы параметр **Принудительно синхронизировать пользователя** стал доступен, сначала нужно отметить **Будут добавлены новые псевдонимы, и будут созданы новые пользователи**.

При повторном сопоставлении роли параметр сопоставления в качестве именованных пользователей или пользователей с одновременным доступом влияет только на новых пользователей, добавленных в роль.

Например, первоначально роль сопоставлена платформе BI с параметром "Новые пользователи создаются как именованные пользователи". Затем можно добавлять пользователей в ту же роль и переназначать роль с выбранным параметром "Новые пользователи создаются как параллельные пользователи".

В этом случае только новые пользователи сопоставляются платформе BI как пользователи с одновременным доступом; пользователи, которые уже были сопоставлены, остаются именованными пользователями. Такое же условие применяется, если изначально пользователи были сопоставлены как пользователи с одновременным доступом, а затем выполняется изменение настроек, и новые пользователи сопоставляются как именованные.

7.8.2.3 Отмена отображения роли

1. Войдите в систему Central Management Console под учетной записью администратора.
2. В области «Управление» щелкните **Аутентификация**.
3. Дважды щелкните **Siebel**.
4. На вкладке **Домены** выберите домен Siebel, соответствующий роли или ролям, для которых нужно отменить отображение.
5. На вкладке **Роли** выберите роль, которую необходимо удалить, и щелкните **<**.
6. Нажмите кнопку **Обновить**.

У элементов ответственности теперь не будет доступа к платформе BI, пока не будут созданы другие учетные записи или псевдонимы.

Примечание:

Можно также удалять отдельные учетные записи или пользователей из ролей перед их сопоставлением платформе BI, чтобы запретить определенным пользователям выполнять вход в систему.

7.8.3 Планирование пользовательских обновлений

Чтобы изменения в данных пользователя в системе ERP отражались в данных пользователя платформы BI, можно запланировать регулярные обновления пользователей. Эти обновления автоматически синхронизируют пользователей ERP и платформы BI в соответствии с параметрами сопоставления, настроенными в Central Management Console (CMC).

Существуют два варианта запуска и планирования обновлений для импортированных ролей:

- Обновлять только роли: если используется этот параметр, будут обновлены только ссылки между сопоставленными в настоящий момент ролями, импортированными в платформу BI. Этот параметр следует использовать в тех случаях, когда планируется частое выполнение обновлений, и требуется обеспечить эффективное использование ресурсов системы. Если обновляются только роли, новых учетных записей создано не будет.
- Обновлять роли и псевдонимы: этот параметр не только обновляет ссылки между ролями, но также создает новые учетные записи пользователей в платформе BI для новых пользовательских псевдонимов, добавляемых в систему ERP.

Примечание:

Если не было указано автоматическое создание псевдонимов для обновлений при включенной аутентификации, для новых псевдонимов не будут созданы учетные записи.

7.8.3.1 Планирование обновлений пользователя

После сопоставления ролей в платформе ВІ необходимо указать, как система будет обновлять эти роли.

1. Щелкните вкладку **Обновление пользователя**.
2. Щелкните **Расписание** в разделе «Обновлять только роли» или в разделе «Обновлять роли и псевдонимы».

Совет:

Если необходимо немедленно запустить обновление, выберите команду **Обновить сейчас**.

Совет:

Используйте параметр «Обновлять только роли», если нужны частые обновления и имеются проблемы с системными ресурсами. Системе нужно больше времени на обновление ролей и псевдонимов.

Будет открыто диалоговое окно «Повтор».

3. Выберите параметр в списке «Запуск объекта» и введите всю запрашиваемую информацию о планировании.

При создании расписания обновления можно выбрать типы повтора, представленные в следующей таблице.

Тип повтора	Описание
Ежечасно	Обновление будет запускаться каждый час. Вы указываете в какое время должен выполняться объект, а также дату начала и окончания.
Ежедневно	Обновление будет запускаться ежедневно или через указанное количество дней. Можно указать, в какое время объект будет выполняться, а также дату начала и окончания.
Каждую неделю	Обновление будет запускаться каждую неделю. Оно может запускаться один или несколько раз в неделю. Можно указать, в какие дни и в какое время он будет выполняться, а также дату начала и окончания.
Ежемесячно	Обновление будет запускаться каждый месяц или каждые несколько месяцев. Можно указать время запуска, а также дату начала и окончания.
N-й день месяца	Обновление будет запускаться в определенный день месяца. Можно указать день месяца, время запуска, а также дату начала и окончания.

Тип повтора	Описание
Первый понедельник месяца	Обновление будет запускаться в первый понедельник каждого месяца. Можно указать время выполнения, а также даты начала и окончания.
Последний день месяца	Обновление будет запускаться в последний день каждого месяца. Можно указать время выполнения, а также даты начала и окончания.
X день N-ной недели месяца	Обновление будет запускаться в указанный день указанной недели месяца. Можно указать время выполнения, а также даты начала и окончания.
Календарь	Обновление будет запускаться по датам, указанным в созданном календаре.

4. Щелкните **Расписание** после того, как будет окончен ввод информации о планировании. Дата следующего запланированного обновления роли отображается на вкладке **Обновление пользователя**.

Примечание:

Всегда можно отменить следующее запланированное событие, щелкнув **Отменить запланированные обновления** в разделе «Обновлять только роли» или «Обновлять роли и псевдонимы».

7.9 Аутентификация Oracle EBS

7.9.1 Разрешение аутентификации Oracle EBS

Чтобы информация Oracle EBS могла использоваться платформой BI, системе нужны сведения о том, как выполнять аутентификацию в системе Oracle EBS.

7.9.1.1 Включение аутентификации Oracle E-Business Suite

1. Выполните вход в систему Central Management Console под учетной записью администратора.

2. В области "Управление" щелкните **Аутентификация**.
 3. Щелкните **Oracle EBS**.
На экран выводится страница «Oracle EBS». У этой страницы четыре вкладки: **Параметры**, **Системы**, **Ответственность** и **Обновление пользователя**.
 4. На вкладке **Параметры** установите флажок **Аутентификация Oracle EBS включена**.
 5. Внесите необходимые изменения в поля **Создать псевдоним**, **Обновить параметры** и **Параметры нового пользователя** в соответствии с имеющимся развертыванием платформы BI. Нажмите кнопку **Обновить** для сохранения изменений перед переходом к вкладке **Системы**.
 6. Перейдите на вкладку **Системы**.
 7. В области «Пользователь системы Oracle EBS» введите имя пользователя базы данных и пароль, которые следует использовать в платформе BI для выполнения входа в базу данных Oracle E-Business Suite.
 8. В области «Службы Oracle EBS» введите имя службы, используемой средой Oracle EBS, и нажмите кнопку **Добавить**.
 9. Нажмите кнопку **Обновить**, чтобы сохранить изменения.
- Теперь следует установить соответствия ролей Oracle EBS в системе.

См. также

- [Сопоставление ролей Oracle E-Business Suite](#)

7.9.2 Сопоставление ролей Oracle E-Business Suite с платформой BI

Платформа BI автоматически создает группу для каждой сопоставляемой роли Oracle E-Business Suite (EBS). Система также создает псевдонимы, представляющие элементы сопоставленных ролей Oracle E-Business Suite.

Можно создать учетную запись пользователя для каждого созданного псевдонима. Однако, если вы работаете с несколькими системами, и пользователи имеют учетные записи более чем на одной системе, то перед созданием учетных записей в BusinessObjects Enterprise можно сопоставить каждому пользователю псевдоним с тем же именем.

Такая операция сокращает количество учетных записей, создаваемых для одного и того же пользователя в системе.

Например, если ведется работа с тестовой средой EBS и средой производства, и 30 пользователей имеют доступ к обеим этим системам, будет создано только 30 учетных записей. Если предпочтительно не сопоставлять каждого пользователя с псевдонимом с тем же именем, то для 30 пользователей платформы BI будет создано 60 учетных записей.

Однако при работе с несколькими системами и совпадении имен пользователей нужно создать новую учетную запись участника для каждого создаваемого псевдонима.

Например, если в тестовой среде используется учетная запись Russell Aquino (имя пользователя "raqino"), а в производственной среде – учетная запись пользователя Raoul Aquino (имя пользователя "raqino"), то необходимо создать отдельную учетную запись для каждого псевдонима пользователя. В противном случае в одну учетную запись платформы BI будут добавлены два пользователя. Они смогут войти в систему с собственными учетными данными Oracle EBS и будут иметь доступ к данным обеих систем Oracle EBS.

7.9.2.1 Сопоставление ролей Oracle E-Business Suite

1. Выполните вход в систему Central Management Console под учетной записью администратора.
2. В области "Управление" щелкните **Аутентификация**.
3. Щелкните **Oracle EBS**.

На странице «Oracle EBS» отображена вкладка **Параметры**.

4. В области «Параметры нового псевдонима» выберите один из следующих параметров:

- **Назначить каждый добавленный псевдоним Oracle EBS учетной записи с тем же именем**

Выберите этот параметр, если вы работаете с несколькими системами Oracle E-Business Suite, и пользователи имеют учетные записи в нескольких системах (и нет двух одинаковых имен пользователя в разных системах для двух разных пользователей).

- **Создать новую учетную запись для каждого добавляемого псевдонима Oracle EBS**

Выберите этот параметр, если вы работаете только с одной системой Oracle E-Business Suite, если большинство пользователей имеют учетные записи только на одной из систем, или если имена пользователей совпадают для разных пользователей на двух или более системах.

5. В области «Параметры обновления» выберите один из следующих параметров:

- **Будут добавлены новые псевдонимы, и будут созданы новые пользователи**

Выберите этот параметр, чтобы создавать новый псевдоним для каждого пользователя, для которого устанавливается соответствие в платформе BI. Новые учетные записи добавляются для пользователей без учетных записей платформы BI или для всех пользователей, если выбран вариант **Создать новую учетную запись для каждого добавленного псевдонима Oracle EBS**.

- **Новые псевдонимы не будут добавлены, и новые пользователи не будут созданы**

Выберите этот параметр, если роль, для которой устанавливается соответствие, содержит много пользователей, но только некоторые из них будут использовать платформу BI. Платформа не создает псевдонимы и учетные записи для пользователей автоматически. Вместо этого псевдонимы (и учетные записи, при необходимости) создаются только для пользователей, которые входят в платформу BI первый раз. Этот параметр выставлен по умолчанию.

6. В «Параметрах нового пользователя» следует указать, как создаются новые пользователи, а затем нажать кнопку **Обновить**.

Если лицензия платформы SAP BusinessObjects Business Intelligence основана на ролях пользователей, выберите один из перечисленных ниже параметров:

- **Новые пользователи создаются как BI Viewer**

Учетные записи новых пользователей создаются с ролью BI Viewer. Доступ к приложениям платформы BI для всех учетных записей роли BI Viewer определяется в лицензионном соглашении. Пользователи ограничены доступом к рабочим процессам приложений, которые определены для роли BI Viewer. Права доступа обычно ограничены просмотром документов Business Intelligence. Эта роль обычно подходит для пользователей, которые используют контент через приложения платформы BI.

- **Новые пользователи создаются как BI Analyst**

Учетные записи новых пользователей создаются с ролью BI Analyst. Доступ к платформе BI для всех учетных записей роли BI Analyst определяется в лицензионном соглашении. Пользователи могут обращаться ко всем рабочим процессам приложений, которые определены для роли BI Analyst. Права доступа включают просмотр и изменение документов Business Intelligence. Эта роль обычно подходит для пользователей, которые создают и изменяют контент для приложений платформы BI.

Если лицензия платформы SAP BusinessObjects Business Intelligence не основана на ролях пользователей, выберите один из перечисленных ниже параметров:

- **Новые пользователи создаются как именованные пользователи.**

Новые учетные записи пользователей настраиваются на использование именованных пользовательских лицензий. Именованные пользовательские лицензии связаны с конкретными пользователями и позволяют им входить в систему, используя имя пользователя и пароль. Это дает именованным пользователям право доступа к системе независимо от того, сколько других пользователей выполнили вход. Для каждой учетной записи, созданной с использованием данного параметра, должна существовать именованная пользовательская лицензия.

- **Новые пользователи создаются как конкурентные пользователи.**

Новые учетные записи пользователей настраиваются на использование конкурентных пользовательских лицензий. Лицензии на одновременный доступ указывают количество человек, которые могут подключиться к платформе BI одновременно. Это очень гибкий тип лицензий, так как небольшое их количество поддерживает широкую пользовательскую базу. Например, в зависимости от того, как часто и как долго пользователи работают с платформой, лицензия на одновременный доступ для 100 пользователей может поддерживать 250, 500 или 700 пользователей.

Выбранные роли теперь отображаются как группы в платформе BI.

7. Перейдите на вкладку **Ответственность**.

8. Выберите **Принудительно синхронизировать пользователя**, если нужно синхронизировать сведения об учетной записи пользователя Oracle EBS после того, как была нажата кнопка **Обновить** на вкладке **Ответственность**.

9. В разделе **Текущие службы Oracle EBS** выберите службу Oracle EBS, содержащую роли, которые нужно сопоставить.
10. Фильтры для Oracle EBS можно задавать в разделе «Сопоставленные роли Oracle EBS».
 - a. Выберите, какие приложения пользователи используют для новых ролей из списка **Приложения**.
 - b. Выберите, какие приложения Oracle, функции, отчеты и одновременные программы, которые пользователь может запускать в списке **Ответственность**.
 - c. Выберите, какой группе безопасности назначается новая роль в группе безопасности в **Группе безопасности**.
 - d. Используйте кнопки **Добавить** и **Удалить** в «Текущей роли», чтобы изменить назначения группы безопасности для роли.
11. Нажмите кнопку **Обновить**.

Роли будут сопоставлены платформе BI.

После сопоставления ролей платформе BI необходимо указать, как система будет обновлять эти роли.

См. также

- [Лицензирование на основе ролей](#)

7.9.2.1.1 Обновление ролей и пользователей Oracle EBS.

После включения аутентификации Oracle EBS необходимо запланировать и запустить регулярные обновления по сопоставленным ролям, импортированным в платформу BI. Это обеспечит точное представление информации роли Oracle EBS в платформе BI.

Существует два варианта запуска и планирования обновлений для ролей Oracle EBS:

- Обновлять только роли: если используется этот вариант, будут обновлены только ссылки между сопоставленными в настоящий момент ролями, импортированными в платформу BI. Рекомендуется использовать этот параметр, если ожидаются частые запуски обновлений, и имеются проблемы с использованием системных ресурсов. Если обновляются только роли Oracle EBS
- Обновление ролей и псевдонимов: этот параметр обновляет не только ссылки между ролями, но также создает новые учетные записи пользователей в платформе BI для пользовательских псевдонимов, добавляемых к ролям в системе Oracle EBS.

Примечание:

Если не было указано автоматическое создание псевдонимов для обновлений при включенной аутентификации Oracle EBS, для новых псевдонимов не будут созданы учетные записи.

7.9.2.1.2 Планирование обновлений для ролей Oracle EBS

После сопоставления ролей платформе BI необходимо указать, как система будет обновлять эти роли.

1. Щелкните вкладку **Обновление пользователя**.

2. Щелкните **Расписание** в разделе «Обновлять только роли» или в разделе «Обновлять роли и псевдонимы».

Совет:

Если необходимо немедленно запустить обновление, щелкните **Обновить сейчас**.

Совет:

Используйте параметр «Обновлять только роли», если нужны частые обновления и имеются проблемы с системными ресурсами. Системе нужно больше времени на обновление ролей и псевдонимов.

Будет открыто диалоговое окно «Повтор».

3. Выберите параметр из раскрывающегося списка «Запуск объекта» и введите всю запрашиваемую информацию о планировании в предоставленные поля.

При создании расписания обновления можно выбрать типы повтора, представленные в следующей таблице.

Тип повтора	Описание
Ежечасно	Обновление будет запускаться каждый час. Вы указываете в какое время должен выполняться объект, а также дату начала и окончания.
Ежедневно	Обновление будет запускаться ежедневно или через указанное количество дней. Можно указать, в какое время объект будет выполняться, а также дату начала и окончания.
Каждую неделю	Обновление будет запускаться каждую неделю. Оно может запускаться один или несколько раз в неделю. Можно указать, в какие дни и в какое время он будет выполняться, а также дату начала и окончания.
Ежемесячно	Обновление будет запускаться каждый месяц или каждые несколько месяцев. Можно указать время запуска, а также дату начала и окончания.
N-й день месяца	Обновление будет запускаться в определенный день месяца. Можно указать день месяца, время запуска, а также дату начала и окончания.
Первый понедельник месяца	Обновление будет запускаться в первый понедельник каждого месяца. Можно указать время выполнения, а также даты начала и окончания.
Последний день месяца	Обновление будет запускаться в последний день каждого месяца. Можно указать время выполнения, а также даты начала и окончания.

Тип повтора	Описание
X день N-ной недели месяца	Обновление будет запускаться в указанный день указанной недели месяца. Можно указать время выполнения, а также даты начала и окончания.
Календарь	Обновление будет запускаться по датам, указанным в созданном календаре.

4. Щелкните **Расписание** после того, как будет окончен ввод информации о планировании. Дата следующего запланированного обновления роли отображается на вкладке **Обновление пользователя**.

Примечание:

Всегда можно отменить следующее запланированное событие, щелкнув **Отменить запланированные обновления** в разделе «Обновлять только роли» или «Обновлять роли и псевдонимы».

7.9.3 Неотображаемые роли

Для того, чтобы запретить конкретным группам пользователей вход в платформу BI, можно отменить сопоставление ролей, к которым они принадлежат.

7.9.3.1 Отмена отображения роли

1. Войдите в систему Central Management Console под учетной записью администратора.
2. В области "Управление" щелкните **Аутентификация**.
3. Дважды щелкните на имени системы ERP, для которой следует отменить сопоставление ролей.
Страница системы ERP отображает вкладку **Параметры**.
4. Щелкните вкладку **Ответственность** или **Роли**.
5. Выберите целевую роль из области **Импортированные роли** и щелкните < или **Удалить**, чтобы удалить ее.
6. Щелкните **Обновить**.
У элементов роли теперь не будет доступа к платформе BI, пока не будут созданы другие учетные записи или псевдонимы.

Примечание:

Можно также удалять отдельные учетные записи или удалять пользователей из ролей перед их назначением платформе BI, чтобы запретить определенным пользователям выполнять вход в систему.

7.9.4 Настройка прав для назначенных групп и пользователей Oracle EBS

При сопоставлении ролей в платформе BI можно назначать права или предоставлять разрешения создаваемым группам и пользователям.

7.9.4.1 Назначение прав администратора

Чтобы разрешить пользователям осуществлять поддержку платформы BI, необходимо включить их в группу "Администраторы", которая имеется в платформе BI по умолчанию. Члены этой группы получают полный контроль над всеми аспектами системы, включая учетные записи, серверы, папки, объекты, настройки и т. д.

1. Войдите в систему Central Management Console под учетной записью администратора.
2. В области «Упорядочение» щелкните **Пользователи**.
3. В столбце **Имя** щелкните **Администраторы**.
4. Щелкните элемент **Список групп**, затем в списке "Действия" выберите команду **Добавить**.
Появится страница "Доступные пользователи/группы".
5. В области **Список пользователей** или **Список групп** выберите роль, для которой нужно назначить права администратора.
6. Щелкните значок >, чтобы внести роль в подгруппу группы "Администраторы", и щелкните **ОК**.

Члены роли теперь обладают административными правами в платформе BI.

Примечание:

Можно также создать роль в Oracle EBS, добавить соответствующих пользователей к роли, установить для роли соответствие в платформе BI и сделать ее подгруппой группы "Администраторы", которая существует по умолчанию, чтобы предоставить членам роли административные права.

7.9.4.2 Назначение прав на публикацию

Если в системе есть пользователи, которые назначены в организации разработчиками содержимого, им можно назначить разрешения на публикацию объектов в платформе BI.

1. Выполните вход в систему Central Management Console под учетной записью администратора.
2. В области «Организовать» щелкните **Папки**.
3. Перейдите в папку, которая будет использоваться для хранения добавляемых пользователями объектов.
4. Щелкните **Управление, Безопасность верхнего уровня**, а затем **Все папки**.
5. Нажмите **Добавить принципалов**.

Появится страница "Добавление принципалов".

6. Выберите из списка **Доступные пользователи/группы** группу, членам которой следует дать права на публикацию.
7. Щелкните **>**, чтобы предоставить группе доступ к папке, а затем нажмите **Добавить и назначить безопасность**.

Появится страница "Назначение безопасности".

8. В списке **Доступные уровни доступа** выберите требуемый уровень доступа и щелкните **>**, чтобы назначить его.
9. Отмените выбор параметров **Наследовать от родительской папки** и **Наследовать от родительской группы**, если они выбраны, и нажмите **Применить**.
10. Нажмите кнопку **ОК**.

Члены роли теперь могут добавлять объекты в папку и во вложенные в нее папки. Для удаления назначенных разрешений щелкните **Убрать доступ**.

7.9.5 Настройка единого входа (SSO) для SAP Crystal Reports и Oracle EBS

По умолчанию в параметрах платформы BI пользователям SAP Crystal Reports будет разрешен доступ к данным Oracle EBS с использованием функции единого входа (SSO).

7.9.5.1 Отключение единого входа для Oracle EBS и SAP Crystal Reports

1. В приложении Central Management Console (CMC) выберите элемент **Приложения**.
2. Дважды щелкните элемент **Конфигурация Crystal Reports**.
3. Выберите элемент **Параметры единой регистрации в системе**.
4. Выберите **crdb_oraapps**.
5. Нажмите кнопку **Удалить**.

6. Нажмите кнопку **Сохранить и закрыть**.
7. Перезапустите SAP Crystal Reports.

7.9.5.2 Повторная активация единого входа для Oracle EBS и SAP Crystal Reports

Выполните следующие действия для повторной активации единого входа для Oracle EBS и SAP Crystal Reports.

1. В приложении Central Management Console (CMC) выберите элемент **Приложения**.
2. Дважды щелкните элемент **Конфигурация Crystal Reports**.
3. Выберите элемент **Параметры единой регистрации в системе**.
4. В области «Использовать для входа в базу данных контекст SSO» введите **crdb_oraapps**.
5. Нажмите кнопку **Добавить**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. Перезапустите SAP Crystal Reports.

Администрирование сервера

8.1 Администрирование сервера

8.1.1 Работа с областью управления СМС "Серверы"

Область управления серверами СМС – это основной инструмент управления заданиями серверов. В этой области приводится список всех серверов в данном развертывании. При выполнении большинства задач по управлению и настройке необходимо выбрать сервер в списке, а затем – команду в меню "Управление" или "Действие".

О дереве навигации

Дерево навигации в левой части области управления "Серверы" предлагает несколько способов просмотра списка "Серверы". Выберите элементы в дереве навигации, чтобы изменить информацию, которая отображается на панели «Сведения».

Параметр дерева навигации	Описание
Список серверов	Отображает полный список всех серверов развертывания.
Список групп серверов	Отображает простой список всех доступных серверных групп на панели "Сведения". Выберите этот параметр, если хотите изменить настройки или уровень безопасности серверной группы.
Группы серверов	Выводит серверных групп и серверов в каждой из них. При выборе серверной группы входящие в нее серверы и серверные группы отображаются на панели "Сведения" по иерархии.

Параметр дерева навигации	Описание
Узлы	<p>Выводит список узлов развертывания. Узлы настраиваются в ССМ. Можно выбрать узел, щелкнув его, с целью просмотра серверов для узла или управления ими.</p>
Категории служб	<p>Выводит список типов служб, которые могут быть в вашем развертывании. Категории служб подразделяются на корневые службы платформы BI и службы, связанные с конкретными компонентами SAP Business Objects. Категории служб включают в себя:</p> <ul style="list-style-type: none"> • Службы соединения • Корневые службы • Службы Crystal Reports • Службы объединения данных • Службы управления жизненным циклом • Службы Analysis • Службы Web Intelligence • Службы Dashboard Design <p>Выберите категорию службы в списке навигации для просмотра серверов категории или управления ими.</p> <p>Примечание: На сервере могут размещаться службы, принадлежащие нескольким категориям служб. Следовательно, один сервер может быть в нескольких категориях служб.</p>

Параметр дерева навигации	Описание
Состояние сервера	<p>Отображает серверы в соответствии с их текущими статусами. Этот инструмент полезен, когда необходимо посмотреть, какие серверы работают, а какие остановлены. Если, например, система работает медленно, с помощью списка «Состояние сервера» можно быстро определить, находится ли какой-либо из серверов в ненормальном состоянии. Возможны следующие состояния сервера:</p> <ul style="list-style-type: none"> • Остановлено • Запуск • Инициализация • Работает • Остановка • Запущен с ошибками • Сбой • Ожидание ресурсов

О панели "Сведения"

В зависимости от параметров, выбранных в дереве навигации, на панели «Сведения» в правой части области управления "Серверы" отображается список серверов, серверных групп, состояний, категорий или узлов. В таблице ниже перечислены данные по серверам, отображаемые на панели «Сведения».

Примечание:

На панели «Сведения» обычно отображаются имена и описания узлов, серверных групп, категорий и состояний.

Столбец панели "Сведения"	Описание
Имя сервера или Имя	Отображает имя сервера.

Столбец панели "Сведения"	Описание
Состояние	<p>Отображает текущее состояние сервера. С помощью списка «Состояние сервера» в дереве навигации можно выполнить упорядочивание по состоянию сервера. Возможны следующие состояния сервера:</p> <ul style="list-style-type: none"> • Остановлено • Запуск • Инициализация • Работает • Остановка • Запущен с ошибками • Сбой • Ожидание ресурсов
Включено	Отображает данные о том, что сервер включен или выключен.
Устаревший	Если сервер помечен как Устаревший , его необходимо перезапустить. Например, если изменены какие-либо настройки сервера в диалоговом окне «Свойства», может потребоваться его перезапуск, чтобы изменения вступили в силу.
Сорт	Отображает тип сервера.
Имя хоста	Отображает имя хоста для данного сервера.
Работоспособность	Показывает общую работоспособность сервера.
PID	Отображает уникальный идентификатор процесса сервера.
Описание	Отображает описание сервера. Это описание можно изменить на странице «Свойства» сервера.

Столбец панели "Сведения"	Описание
Дата изменения	Отображает дату последнего изменения на сервере или изменения состояния сервера. Данные из этого столбца часто бывают необходимы для проверки состояния недавно измененных серверов.

См. также

- [Управление группами серверов](#)
- [Использование узлов](#)
- [Просмотр состояний серверов](#)
- [Запуск, остановка и перезапуск серверов](#)
- [Для изменения свойств сервера](#)

8.1.2 Управление серверами с помощью скриптов в Windows

Исполняемый файл `ccm.exe` позволяет запускать, останавливать, перезапускать, включать и отключать сервера в существующем развертывании в Windows из командной строки.

См. также

- [ccm.exe](#)

8.1.3 Управление серверами в UNIX

Исполняемый файл `ccm.sh` позволяет запускать, останавливать, перезапускать, включать и отключать сервера в существующем развертывании UNIX в командной строке.

См. также

- [ccm.sh](#)

8.1.4 Управление лицензионными ключами

В этом разделе описывается управление лицензионными ключами для развертывания платформы BI.

См. также

- [Просмотр сведений лицензии](#)
- [Для добавления ключа лицензии](#)
- [Для просмотра текущей деятельности учетной записи](#)

8.1.4.1 Просмотр сведений лицензии

В области управления СМС **Ключи лицензий** указывается количество лицензий на основе ролей (BI Viewer и BI Analyst), лицензий для одновременно работающих пользователей, лицензий для именованных пользователей и лицензий на процессор, связанное с каждым ключом.

1. Перейдите в область управления **Ключи лицензий** в СМС.
2. Выберите ключ лицензии.

Детальная информация, связанная с данным ключом, появится в области **Сведения о лицензионных ключах**. Для приобретения дополнительных ключей лицензий обращайтесь к торговому представителю SAP.

См. также

- [Управление лицензионными ключами](#)
- [Для добавления ключа лицензии](#)
- [Для просмотра текущей деятельности учетной записи](#)

8.1.4.2 Для добавления ключа лицензии

Если вы переходите к коммерческой версии от демо-версии, убедитесь в том, что вы удалили ключ демонстрационной версии, чтобы добавить новые ключи лицензий или коды активации продукта.

1. Перейдите в область управления **Ключи лицензий** в СМС.
2. Введите ключ в поле **Добавить ключ**.

3. Щелкните **Добавить**.

Ключ добавится в список.

См. также

- [Просмотр сведений лицензии](#)
- [Для просмотра текущей деятельности учетной записи](#)

8.1.4.3 Для просмотра текущей деятельности учетной записи

1. Перейдите в область управления СМС **Параметры**.
2. Нажмите кнопку **Просмотреть глобальные системные показатели**.

Здесь отображается текущее использование лицензий, вместе с дополнительными показателями работы.

См. также

- [Управление лицензионными ключами](#)
- [Для добавления ключа лицензии](#)
- [Просмотр сведений лицензии](#)

8.1.5 Измерение показателей использования лицензий

Инструмент измерения лицензий BusinessObjects (BOLMT) – это программа командной строки на базе Java, используемая для сбора и хранения данных о лицензиях платформы BI. Выходной документ XML содержит результаты измерения показателей использования лицензий и направляется в службу глобального аудита лицензий SAP (GLAS) для включения в отчет об аудите лицензий.

Системный администратор устанавливает и запускает BOLMT для каждого кластера платформы BI при поступлении запроса на аудит лицензий. Программа BOLMT измеряет показатели использования лицензий, получаемых для ролей, лицензий для именованных пользователей и лицензий для одновременно работающих пользователей.

Администратор может указать конкретный выходной каталог для документа XML и настроить выходной документ так, чтобы в него не включались сведения, которые позволяли бы идентифицировать пользователей системы.

8.1.5.1 Проведение аудита лицензий

Для выполнения аудита лицензий необходимо иметь права администратора и возможность доступа к каталогу, содержащему файл `BOLMT.jar` в установленной платформе BI.

1. Откройте консоль командной строки.
2. Перейдите в каталог, содержащий исполняемые файлы Java для установленной платформы BI

По умолчанию требуемый файл устанавливается в следующем каталоге: `[INSTALLDIR]\SAP BusinessObjects Enterprise XI 4.0\java\lib`

3. Выполните файл `BOLMT.jar`.

Команда для выполнения файла вводится в следующем формате: `-jar BOLMT.jar [параметры] <выходной файл>`

Допустимые параметры описываются в следующей таблице:

Действие	Описание
-c --cms	Идентификационное имя и номер порта для центрального сервера управления (CMS). Используется формат <i>имя_CMS:номер_порта</i> . Если этот параметр не задан, по умолчанию используются настройки CMS для локального хоста.
-p --password	Пароль учетной записи администратора, используемый для подключения к CMS.
-a--auth	Метод аутентификации, используемый при подключении пользователя к CMS. По умолчанию используется метод Enterprise, задаваемый в виде <code>secEnterprise</code> .
-s--sanitize	Этот параметр задает исключение из выходного документа аудита любых личных сведений, которые позволяли бы идентифицировать пользователей.

Примечание:

Спецификация выходного файла всегда является последним аргументом командной строки. Это необязательный параметр. Если аргумент не указан, выходные данные направляются в стандартный поток вывода консоли. Можно также перенаправить вывод в скрипт как аргумент командной строки.

Пример:

```
C:\Program Files (x86)\SAP
Business Objects\SAP BusinessObjects Enterprise XI 4.0\java\lib>"C:\Program Files
(x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin
\java.exe" -jar BOLMT.jar --cms=myscms:6400 -uAdministrator
-p=7juujg --auth=secEnterprise --sanitize audit.xml
```


8.1.6 Просмотр и изменение статуса сервера

8.1.6.1 Просмотр состояний серверов

Состояние сервера – это его текущий режим работы: сервер может работать, запускаться, останавливаться, быть остановленным, находиться в состоянии сбоя, проходить инициализацию, быть запущенным с ошибками или ожидать предоставления ресурсов. Чтобы отвечать на запросы платформы SAP BusinessObjects Business Intelligence, сервер должен быть запущен и включен. Отключенный сервер продолжает выполняться как процесс, однако он не принимает запросы от других компонентов платформы SAP BusinessObjects Business Intelligence. Если сервер остановлен, его процесс не выполняется.

В этом разделе описывается изменение состояния серверов из CMC.

См. также

- [Просмотр статуса сервера](#)
- [Запуск, остановка и перезапуск серверов](#)
- [Включение и выключение серверов](#)
- [Остановка Центрального сервера управления \(CMS\)](#)
- [Для автоматического запуска сервера](#)

8.1.6.1.1 Просмотр статуса сервера

1. Перейдите в область управления «Серверы» в CMC.

В панели «Сведения» отображаются категории служб в развертывании.

2. Чтобы просмотреть список серверов для заданной группы серверов, узла или категории службы, выберите эту группу серверов, узел или категорию службы в дереве навигации. На панели «Сведения» выводится список серверов в данном развертывании. В столбце **Состояние** отображается статус для каждого из серверов в списке.
3. Если требуется просмотреть список всех серверов, которые имеют определенный статус, раскройте параметр **Статус сервера** в дереве навигации и выберите необходимый статус. Список серверов с выбранным статусом появится на панели "Сведения".

Примечание:

Эта функция очень полезна, если вам нужно быстро просмотреть список серверов, которые неправильно запускаются или неожиданно остановились.

8.1.6.2 Запуск, остановка и перезапуск серверов

Запуск, остановка и перезапуск серверов являются обычными действиями при настройке серверов или переводе их в автономный режим. Например, если вы хотите изменить имя сервера, его нужно сначала остановить. После внесения изменений нужно снова запустить сервер, чтобы изменения вступили в силу. При изменении параметров конфигурации сервера СМС выдаст запрос на перезапуск сервера при необходимости.

В оставшейся части раздела рассказывается о том, какие изменения конфигурации требуют остановки или перезапуска сервера. Однако, поскольку такие задачи встречаются часто, сначала дается объяснение понятий и различий, а общие процедуры приводятся для информации.

Действие	Описание
Остановка сервера	Перед изменением некоторых свойств и параметров требуется остановить серверы платформы SAP BusinessObjects Business Intelligence.
Запуск сервера	Если вы остановили сервер для его настройки, необходимо запустить его, чтобы изменения вступили в силу и сервер возобновил обработку запросов.
Перезапуск сервера	Перезапуск сервера – это его полная остановка с последующим повторным запуском. Если необходимо перезапустить сервер после изменения его параметров, СМС выдаст соответствующий запрос.
Автоматический запуск сервера	Можно настроить сервер на автоматический запуск при запуске Агента Server Intelligence.

Действие	Описание
Принудительное завершение	Сервер останавливается немедленно (тогда как при обычной остановке, сервер остановится после завершения текущих действий по обработке). Принудительное завершение работы сервера следует проводить только тогда, когда остановить сервер обычным образом не удастся, но его работу необходимо прекратить немедленно.

Совет:

При остановке (или перезапуске) сервера прекращается работа процесса сервера, то есть сервер полностью останавливается. Перед остановкой сервера рекомендуется

- отключить сервер, чтобы он смог завершить обработку любых уже выполняемых заданий, и
- убедиться, что в очереди отсутствуют события аудита. Чтобы просмотреть количество остающихся в очереди событий аудита, перейдите на экран «Показатели» и просмотрите показатель «Текущее число событий аудита в очереди».

См. также

- [Включение и выключение серверов](#)

8.1.6.2.1 Запуск, остановка или перезапуск серверов при помощи СМС

1. Перейдите в область управления «Серверы» в СМС.

В панели «Сведения» отображаются категории служб в развертывании.

2. Чтобы просмотреть список серверов для конкретных группы серверов, узла или категории служб, выберите соответствующий объект на панели навигации.

На панели «Сведения» отображается список серверов.

3. Если необходимо просмотреть список всех серверов, которые имеют определенный статус, раскройте параметр **Статус сервера** в дереве навигации и выберите необходимый статус.

Список серверов с выбранным статусом появится на панели «Сведения».

Примечание:

Эта функция очень полезна, если нужно быстро просмотреть список серверов, которые неправильно запускаются или неожиданно остановились.

4. Щелкните правой кнопкой мыши сервер, состояние которого требуется изменить, а затем, в зависимости от выполняемого действия, выберите команду **Запустить сервер**, **Перезапустить сервер**, **Остановить сервер** или **Принудительное завершение работы**.

См. также

- [Просмотр состояний серверов](#)

8.1.6.2.2 Запуск, остановка или перезапуск сервера Windows при помощи CCM

1. В CCM нажмите на панели инструментов кнопку **Управление серверами**.
2. При появлении приглашения на ввод войдите в систему сервера CMS под учетной записью с правами администратора.
3. В диалоговом окне «Управление серверами» выберите сервер, который нужно запустить, остановить или перезапустить.
4. Выберите команду **Запуск, Остановка, Перезапуск** или **Принудительное завершение работы**.
5. Щелкните **Заккрыть**, чтобы вернуться в CCM.

8.1.6.2.3 Для автоматического запуска сервера

По умолчанию, серверы в вашем развертывании должны запускаться автоматически при запуске SIA. Данная процедура показывает, где установить этот параметр.

1. Перейдите в область управления **Серверы** в CMC.
2. Дважды щелкните сервер, который требуется запускать автоматически.
Открывается диалоговое окно «Свойства».
3. В разделе «Общие свойства» установите флажок **Автоматически запускать этот сервер при запуске агента серверной аналитики**, а затем нажмите кнопку **Сохранить** или **Сохранить и закрыть**.

Примечание:

Если настройка автоматического запуска была отменена для всех CMS в кластере, вам потребуется использовать CCM для перезапуска системы. После остановки агента SIA с использованием CCM щелкните правой кнопкой мыши агент SIA и выберите команду **Свойства**. На вкладке "Запуск" измените значение параметра "Автозапуск" на "Да", затем нажмите "Сохранить". Перезапустите SIA.

8.1.6.3 Остановка Центрального сервера управления (CMS)

Если в установке платформы SAP BusinessObjects Business Intelligence имеется несколько активных Центральных серверов управления (CMS), можно выключить один из них без потери данных. Это никак не повлияет на работу системы. Другой CMS в узле возьмет на себя работу остановленного сервера. Кластеризация нескольких CMS позволяет осуществлять поддержку каждого из Центральных серверов управления по очереди, не оставляя платформу SAP BusinessObjects Business Intelligence без обслуживания.

Однако, если в развертывании платформы SAP BusinessObjects Business Intelligence есть только один CMS, его отключение сделает платформу SAP BusinessObjects Business Intelligence недоступной для пользователей и вызовет прерывание обработки отчетов и программ. Чтобы избежать этой проблемы, Server Intelligence Agent (SIA) проверяет, что на каждом узле остается как минимум один работающий CMS. Можно остановить CMS, остановив сначала его SIA, но

перед остановкой SIA следует остановить серверы обработки через CMC, чтобы они могли завершить свои задания перед выключением платформы SAP BusinessObjects Business Intelligence, так как все другие серверы в узле так же будут остановлены.

Примечание:

Можно столкнуться с ситуацией, когда CMS остановился, и возникла необходимо перезагрузить систему из CCM. Например, если выключены все CMS в узле, и не один из них не запускается автоматически при запуске SIA, вам потребуется использовать CCM для перезапуска системы. Для этого в CCM нажмите правой кнопкой мыши на SIA и выберите "Свойства". На вкладке "Запуск" измените значение параметра "Автозапуск" на "Да", затем нажмите "Сохранить". Перезапустите SIA.

Если нужно настроить систему так, чтобы можно было запускать и останавливать Central Management Server в кластере без необходимости запуска и остановки других серверов, следует поместить CMS на отдельный узел. Создайте новый узел и клонируйте в него CMS. Если CMS располагается в собственном узле, можно просто выключить этот узел, что никак не отразится на других серверах.

См. также

- [Использование узлов](#)
- [Клонирование серверов](#)
- [Кластеризация центральных серверов управления \(CMS\)](#)

8.1.6.4 Включение и выключение серверов

При отключении сервера платформы SAP BusinessObjects Business Intelligence для него блокируется получение новых запросов платформы SAP BusinessObjects Business Intelligence и ответ на них, однако выполняемые на нем процессы не приостанавливаются. Эта функция полезна, если нужно позволить серверу завершить обработку всех текущих запросов перед окончательным прекращением работы сервера.

Предположим, необходимо прекратить работу сервера заданий, чтобы перезагрузить компьютер, на котором он запущен. Тем не менее, следует, чтобы сервер завершил все невыполненные запросы отчетов, которые находятся в его очереди. Прежде всего, выключите сервер заданий, чтобы он не принимал новые запросы. Затем перейдите в Central Management Console (CMC) и отследите момент завершения сервером всех заданий, которые находятся в процессе выполнения. (В области управления «Серверы» щелкните правой кнопкой мыши сервер и выберите вкладку «Показатели».) Когда обработка текущих запросов будет успешно завершена, вы можете благополучно прекратить работу сервера.

Примечание:

- Чтобы вы могли включать и/или отключать другие серверы, система CMS должна быть запущена.
- CMS нельзя включить или выключить.

8.1.6.4.1 Включение и отключение серверов в CMC

1. Перейдите в область управления «Серверы» в CMC.
2. Щелкните правой кнопкой мыши сервер, состояние которого требуется изменить, а затем, в зависимости от выполняемого действия, выберите команду **Включить сервер** или **Отключить сервер**.

8.1.6.4.2 Включение или отключение сервера Windows в CCM

1. В CCM выберите **Управление серверами**.
2. При отображении соответствующего приглашения войдите в CMS под учетными данными пользователя платформы BI с правами администратора.
3. В диалоговом окне «Управление серверами» выберите сервер, который нужно включить или выключить.
4. Нажмите кнопку **Включить** или **Выключить**.
5. Щелкните **Заккрыть**, чтобы вернуться в CCM.

8.1.7 Добавление, клонирование и удаление серверов

8.1.7.1 Добавление, клонирование и удаление серверов

Если необходимо добавить новое оборудование к платформе SAP BusinessObjects Business Intelligence, установив компоненты сервера на дополнительных компьютерах, запустите программу установки платформы SAP BusinessObjects Business Intelligence из дистрибутива продукта. В программе установки существует возможность выполнить выборочную установку. Во время выборочной установки укажите CMS существующего развертывания и выберите компоненты, которые нужно установить на локальной машине. Для получения подробных сведений о параметрах выборочной установки см. *Руководство по установке платформы SAP BusinessObjects Business Intelligence*.

8.1.7.1.1 Добавление сервера

Можно запускать несколько экземпляров одного и того же сервера платформы BI на одном и том же компьютере. Чтобы добавить сервер, выполните следующие действия.

1. Перейдите в область управления «Серверы» в CMC.
2. В меню **Управление** щелкните **Создать > Новый сервер**.
Появится диалоговое окно «Создать новый сервер».
3. Выберите пункт **Категория службы**.

4. Выберите тип службы из списка **Выбрать службу**, затем нажмите кнопку **Далее**.
5. Для добавления дополнительной службы к серверу выберите службу в списке **Доступные дополнительные службы** и нажмите кнопку **>**.

Примечание:

Дополнительные службы доступны не для всех типов серверов.

6. После добавления необходимых дополнительных служб нажмите кнопку **Далее**.
7. Если архитектура платформы ВІ состоит из нескольких узлов, в списке **Узел** выберите узел, на который требуется добавить новый сервер.
8. В поле **Имя сервера** введите имя для сервера.
Каждый сервер на системе, должен иметь уникальное имя. Соглашение именования по умолчанию: `<ИМЯУЗЛА>.<типсервера>` (если на компьютере есть более одного сервера каждого типа, к имени добавляется номер).
9. Чтобы добавить описание сервера, введите его в поле **Описание**.
10. Если добавляется новый сервер центрального управления, задайте номер порта в поле **Порт сервера имен**.
11. Нажмите кнопку **Создать**.
Новый сервер появится в списке серверов в области **Серверы** консоли СМС, но при этом он не запускается и не включается.
12. Используйте СМС для включения и запуска нового сервера, если требуется, чтобы он начал отвечать на запросы платформы ВІ.

См. также

- [Службы и серверы](#)
- [Конфигурация настроек серверов](#)
- [Настройка номеров портов](#)
- [Просмотр состояний серверов](#)

8.1.7.1.2 Клонирование серверов

Если необходимо добавить новый экземпляр сервера к развертыванию, можно клонировать существующий сервер. Клонированный сервер сохраняет конфигурационные настройки исходного сервера. Это особенно необходимо при увеличении масштаба использования системы и создании новых экземпляров серверов, для которых необходимы почти те же серверные конфигурационные настройки, что и у существующего сервера.

Клонирование также позволяет упростить процесс перемещения серверов между узлами. Если необходимо переместить существующий сервер СМС в другой узел, можно клонировать его в новом узле. Клонированный сервер СМС появляется в новом узле с такими же конфигурационными настройками, что и у исходного сервера СМС.

Есть некоторые соображения, которые необходимо учитывать при клонировании серверов. Если отсутствует необходимость клонирования всех настроек, необходимо проверить клонированный сервер, чтобы убедиться, что он отвечает всем требованиям. Например, при клонировании

сервера CMS на тот же компьютер обязательно измените настройки номеров портов, которые были скопированы из исходного в сервера CMS в клонированный сервер CMS.

Примечание:

- Перед клонированием серверов убедитесь, что на всех компьютерах в системе установлена одинаковая версия платформы SAP BusinessObjects Business Intelligence (и всех обновлений, если имеются).
- Можно клонировать серверы с любого компьютера. Однако серверы можно клонировать только на компьютеры, на которых установлены необходимые двоичные файлы.
- Если вы клонировали сервер, то новый сервер не обязательно будет использовать такие же идентификационные данные ОС. Учетную запись пользователя контролирует Server Intelligence Agent, под управлением которого запущен соответствующий сервер.

Использование заполнителей для серверных параметров

Заполнители представляют собой переменные на уровне узла и используются серверами, запущенными на узле. Заполнители перечислены на отдельной странице в Central Management Console (СМС). При двойном щелчке любого сервера, перечисленного в списке «Серверы» на СМС, с левой стороны панели навигации предоставляется ссылка на страницу «Заполнители». На странице «Заполнители» перечислены все доступные имена заполнителей и связанные с ними значения для выбранного сервера. В заполнителях содержатся значения, доступные только для чтения, а имена заполнителей начинаются и заканчиваются символом процентов %.

Примечание:

Параметр заполнителя можно всегда перезаписать определенной строкой на странице «Свойства» сервера СМС.

Пример:

Заполнители можно использовать при клонировании серверов. К примеру, на компьютере с несколькими приводами А установлен SAP BusinessObjects Enterprise в C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0. Таким образом заполнитель %DefaultAuditingDir% будет иметь значение D:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\.

На другом компьютере, компьютере Б, установлен только один диск (диск D отсутствует) и система SAP BusinessObjects Enterprise установлена в каталоге C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0. В этом случае заполнитель %DefaultAuditingDir% будет иметь значение C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\.

Чтобы клонировать сервер событий с компьютера А на компьютер Б, если заполнители используются для временного каталога Auditing, заполнители будут разрешаться и сервер событий будет функционировать правильно. Если заполнители не используются, будет происходить сбой сервера событий, пока параметр временного каталога Auditing не будет перезаписан вручную.

Порядок клонирования сервера

1. На компьютере, где необходимо добавить клонированный сервер, войдите в область управления СМС «Серверы».
2. Щелкните правой кнопкой мыши сервер, который требуется клонировать, и выберите команду **Клонировать сервер**.
Появляется диалоговое окно «Клонировать сервер».
3. Введите имя сервера (или воспользуйтесь именем по умолчанию) в поле **Новое имя сервера**.
4. Если клонируется центральный сервер управления, задайте номер порта в поле **Порт сервера имен**.
5. В списке **Клонировать в узле** выберите узел, в который необходимо добавить клонированный сервер, а затем нажмите кнопку **ОК**.
В области управления СМС «Серверы» добавится новый сервер.

Примечание:

Настройки номеров портов тоже клонируются. В большинстве случаев, таких как клонирование сервера СМС, необходимо изменять номер порта, чтобы избежать возникновения конфликта между исходным сервером и его клоном.

8.1.7.1.3 Удаление сервера

1. Перейдите в область управления «Серверы» в СМС.
2. Остановите сервер, который хотите удалить.
3. Щелкните сервер правой кнопкой мыши и выберите команду **Удалить**.
4. При запросе подтверждения нажмите кнопку **ОК**.

8.1.8 Кластеризация центральных серверов управления (СМС)

8.1.8.1 Кластеризация центральных серверов управления (СМС)

Для крупного или критически важного развертывания платформы SAP BusinessObjects Business Intelligence может потребоваться использование нескольких компьютеров с СМС в кластере. Кластер состоит из двух или более серверов СМС, совместно работающих со стандартной базой данных системы СМС. Если на компьютере, где запущен один СМС, происходит сбой, другой компьютер с СМС продолжит обслуживать запросы платформы SAP BusinessObjects Business Intelligence. Такая "высокая доступность" позволяет убедиться, что пользователи платформы

SAP BusinessObjects Business Intelligence смогут продолжить работу с информацией даже в случае аппаратного сбоя.

В этом разделе рассказывается о том, как добавить новый сервер CMS в качестве члена кластера в продуктивную систему, которая уже работает. При добавлении CMS в существующий кластер вы подключаете его к существующей базе данных CMS и распределяете рабочую нагрузку между всеми существующими станциями CMS. Для получения информации о существующих CMS перейдите в область управления "Серверы" CMS.

До начала кластеризации CMS убедитесь, что каждый из серверов CMS установлен в системе, отвечающей необходимым требованиям (включая уровни версий и уровни патчей) к операционной системе, серверу баз данных, методу доступа к базе данных, драйверу базы данных и клиенту, описанным в файле `platforms.txt`, включенному в дистрибутив продукта.

Кроме этого, необходимо учесть следующие требования к кластеризации:

- Для улучшения быстродействия сервер баз данных, на котором расположена системная база данных, должен иметь возможность быстрой обработки небольших запросов. CMS очень часто взаимодействует с системной базой данных, отправляя ей небольшие запросы. Если серверу базы данных не удастся вовремя обработать эти запросы, производительность платформы SAP BusinessObjects Business Intelligence будет существенно снижена.
- Для улучшения быстродействия необходимо запускать каждый член кластера CMS на компьютерах с одинаковым количеством памяти и одинаковым типом ЦП.
- Настройте аналогичным образом каждый компьютер:
 - Установите одну и ту же операционную систему (это требование распространяется на версии, пакеты обновления и патчи).
 - Установите одну и ту же версию платформы SAP BusinessObjects Business Intelligence (включая исправления, если они доступны).
 - Убедитесь, что все CMS одинаковым способом подключены к базе данных системы (с использованием собственных драйверов или ODBC). Убедитесь, что драйверы и их версии на каждом компьютере одинаковы.
 - Убедитесь, что все CMS используют одинаковый клиент базы данных (и одну и ту же версию) для подключения к системной базе данных.
 - Проверьте, используют ли все CMS одинаковую учетную запись базы данных и пароль для соединения с системной базой данных. Эта учетная запись должна иметь права на создание, удаление и обновление системной базы данных.
 - Убедитесь в том, что узлы, на которых располагается каждый из серверов CMS, запущены под одной учетной записью операционной системы. (В Windows по умолчанию используется учетная запись "Local system").
 - Убедитесь, что текущая дата и время корректно установлены на каждом компьютере CMS (включая настройки для перехода на летнее время).
 - Убедитесь в том, что на всех серверах веб-приложений в кластере установлены одинаковые WAR-файлы. Дополнительную информацию о развертывании WAR-файла см. в *Руководстве по установке платформы SAP BusinessObjects Business Intelligence*.

- Убедитесь, что все CMS в кластере работают в одной и той же локальной сети.
- Если в вашем кластере более 8 серверов, убедитесь, что командная строка для каждого CMS включает параметр `-oobthreads <numCMS>`, где `<numCMS>` – количество серверов в кластере. Этот параметр гарантирует, что серверы поддерживают тяжелую загрузку. Для получения сведений о настройке командной строки сервера см. приложение "Командная строка сервера" в документе *Руководство администратора платформы SAP BusinessObjects Business Intelligence*.
- Если вы хотите разрешить проведение аудита, все CMS должны быть единым образом использовать одну и ту же базу данных аудита, и подключаться к ней одинаковым способом. Требования к базе данных аудита аналогичны требованиям к системной базе данных, исходя из серверов баз данных, клиентов, методов доступа, драйверов и информации о пользователях.

Совет:

По умолчанию, имя кластера отражает конкретное имя первого установленного CMS.

См. также

- [Изменение имени кластера CMS](#)

8.1.8.1.1 Добавление CMS в кластер

Существует несколько способов добавления CMS в кластер. Выполните соответствующую процедуру:

- Можно установить новый узел с помощью CMS на новом компьютере.
- Если узел с двоичными файлами CMS уже существует, можно добавить новый сервер CMS из CMS.
- Если узел с двоичными файлами CMS уже существует, также можно добавить новый сервер CMS путем клонирования существующего сервера CMS.

Примечание:

Перед внесением каких-либо изменений создайте резервную копию базы данных системы CMS и содержимого репозитория входных и выходных файлов. При необходимости обратитесь к администратору базы данных.

См. также

- [Добавление нового узла в кластер](#)
- [Добавление сервера](#)
- [Клонирование серверов](#)
- [Резервное копирование и восстановление системы](#)

8.1.8.1.2 Добавление нового узла в кластер

При добавлении узла, вам предложат создать новый CMS или разместить узел в кластере существующего CMS.

Для добавления узла в существующий кластер CMS, можно использовать программу установки. Запустите программу установки и настройки платформы SAP BusinessObjects Business Intelligence на компьютере, на котором требуется установить новый элемент кластера CMS. В программе установки существует возможность выполнить выборочную установку. Во время установки по умолчанию укажите требуемый CMS и выберите компоненты для установки на локальную машину. Укажите имя CMS, запущенного в текущей системе, и произведите установку нового CMS на локальную машину. Затем укажите данные для соединения программы установки с существующей системной базой данных CMS. После завершения установки нового CMS на локальную машину, сервер автоматически добавится в существующий кластер.

См. также

- [Использование узлов](#)

8.1.8.1.3 Добавление кластеров в файлы свойств веб-приложений

Если в развертывание были добавлены дополнительные сервера CMS, и при этом используется сервер приложений Java, необходимо изменить файл `PlatformServices.properties` в каталоге `\webapps\BOE\WEB-INF\config\custom` в развертывании веб-приложения.

Определение свойств кластера в веб-приложении BOE

1. Откройте пользовательскую папку для файла `BOE.war` на компьютере, на котором размещаются веб-приложения.

Если используется сервер веб-приложений Tomcat, входящий в комплект установки платформы SAP BusinessObjects Business Intelligence, можно непосредственно перейти в следующую папку:

```
C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom\
```

Совет:

Если используется сервер веб-приложений, не допускающий прямого доступа к развернутым веб-приложениям, для изменения файла `BOE.war` можно воспользоваться следующей папкой в существующей установке продукта.

```
<INSTALLDIR>\SAP BusinessObjects Business Intelligence platform  
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\.
```

Затем потребуется повторно развернуть измененный файл `BOE.war`.

2. Создайте новый файл.

Примечание:

Воспользуйтесь программой "Блокнот" или любым другим текстовым редактором.

3. Укажите свойства кластера CMS.

Свойство `cms.clusters` указывает все кластеры в развертывании. Перед каждым именем кластера должен идти символ @, имена кластеров разделяются запятыми. Например, `cms.clusters=@samplecluster,@samplecluster2, @samplecluster3`. Используйте

свойство `cms.clusters.[cluster name]` для указания каждого из содержащихся в кластере CMS. Например:

```
cms.clusters=@samplecluster,@samplecluster2, @samplecluster3
cms.clusters.samplecluster=cmsone:6400,cms2
cms.clusters.samplecluster2=cms3,cms4, cms5
cms.clusters.samplecluster3=aps05
```

Примечание:

Разделяйте имена CMS запятой. Номер порта отделите от имени CMS двоеточием; предполагаемый номер порта – 6400, если не указано иначе. Повторите процедуру для каждого имеющегося кластера.

4. Сохраните файл под следующим именем:

PlatformServices.properties

5. Перезапустите сервер приложений.

Новые свойства вступают в силу только после повторного развертывания измененного веб-приложения **BOE** на компьютере, на котором выполняется сервер веб-приложений. Используйте Wdeploy, чтобы повторно развернуть WAR-файл на сервере веб-приложений. Для получения дополнительных сведений об использовании WDeploy см. *Руководство по развертыванию веб-приложений платформы SAP BusinessObjects Business Intelligence*.

8.1.8.1.4 Изменение имени кластера CMS

Эта процедура позволяет изменить имя уже установленного кластера. После изменения имени кластера CMS агент Server Intelligences Agent автоматически выполняет перенастраивает каждый сервер SAP Business Objects для его регистрации кластером CMS, а не отдельным сервером CMS.

Примечание:

Обращаем внимание опытных администраторов платформы SAP BusinessObjects Business Intelligence на то, что параметр `-ns` больше не используется в командной строке для указания CMS, на котором регистрируется сервер. Теперь этот выбор автоматически выполняется SIA.

Изменение имени кластера в ОС Windows

1. Используйте CCM для остановки агента Server Intelligence Agent в узле, в котором содержится центральный сервер управления, являющийся членом кластера, имя которого необходимо изменить.
2. Щелкните правой кнопкой мыши Server Intelligence Agent и выберите **Свойства**.
3. В диалоговом окне "Свойства" выберите вкладку **Конфигурация**.
4. Установите флажок **Изменить имя кластера на**.
5. Введите новое имя кластера.
6. Нажмите кнопку **ОК**, а затем перезапустите агент Server Intelligence Agent.

Теперь имя кластера CMS изменено. Все остальные члены кластера CMS динамически уведомляются о новом имени кластера (распространение изменений между элементами кластера может занять несколько минут).

7. Перейдите в область управления **Серверы** консоли СМС и проверьте, что все серверы включены. При необходимости включите все серверы, которые были отключены при выполнении изменений.

Изменение имени кластера в ОС UNIX

Используйте скрипт `cmsdbsetup.sh`. Для получения дополнительных сведений см. главу "Инструменты Unix" в *Руководстве администратора платформы SAP BusinessObjects Business Intelligence*.

8.1.9 Управление группами серверов

С помощью групп серверов можно упорядочить серверы платформы SAP BusinessObjects Business Intelligence, чтобы ими было проще управлять. При управлении группой серверов нужно только просмотреть подмножество всех серверов системы. Более того, с помощью групп серверов можно эффективно настроить платформу SAP BusinessObjects Business Intelligence, чтобы оптимизировать систему по отношению к пользователям из разных местоположений или по отношению к различным типам объектов.

При группировке серверов по региону несложно ввести настройки обработки, расписания для повторного выполнения и места назначения расписания, подходящие для пользователей, которые работают в том или ином региональном офисе. Объект можно связать с отдельной группой серверов, чтобы его всегда обрабатывали одни и те же серверы. Внесенные в расписание объекты можно связать с определенной группой серверов, чтобы они всегда отправлялись на соответствующие принтеры, серверы файлов и т.д. Таким образом, группы серверов действительно обеспечивают значительную помощь при работе с системами, охватывающими несколько местоположений и часовых поясов.

При группировке серверов по типу можно настроить обработку объектов на серверах, которые оптимизированы для данного типа объектов. Например, серверы обработки должны часто связываться с базой данных, в которой содержатся данные для публикации отчетов. Если разместить серверы обработки поблизости от серверов базы данных, к которым им необходим доступ, производительность системы повысится, а сетевой трафик снизится до минимума. Таким образом, при наличии нескольких отчетов, выполняемых по базе данных DB2, может потребоваться создание группы серверов обработки исключительно для обработки отчетов с участием сервера базы данных DB2. Если затем соответствующие отчеты будут настроены на постоянное использование данной группы серверов обработки для просмотра, система будет оптимизирована для просмотра данных отчетов.

После создания групп серверов настройте объекты на использование определенных групп серверов для внесения в расписание, просмотра и изменения отчетов. Для просмотра групп серверов используйте дерево навигации в области управления "Серверы" консоли СМС. Параметр "Список групп серверов" отображает список групп серверов на панели сведений, а параметр "Группы серверов" предоставляет возможность просматривать серверы, включенные в группу.

8.1.9.1 Создание группы серверов

Чтобы создать группу серверов, необходимо ввести имя и описание группы, а затем добавить в нее серверы.

8.1.9.1.1 Чтобы создать группу серверов

1. Перейдите в область управления «Серверы» в СМС.
2. Выберите команду **Управление > Создать > Создать группу серверов**.
Открывается диалоговое окно «Создать группу серверов».
3. В поле **Имя** введите имя новой группы серверов.
4. При необходимости введите дополнительные сведения о группе серверов в поле **Описание**.
5. Нажмите кнопку **ОК**.
6. В области управления «Серверы» в дереве навигации щелкните **Группы серверов** и выберите новую группу серверов.
7. Выберите **Добавить членов** в меню **Действия**.
8. Выберите серверы, которые требуется добавить в группу, и нажмите кнопку **>**.

Совет:

Удерживая нажатой клавишу **CTRL +**, щелкните **кнопкой мыши**, чтобы выбрать несколько серверов.

9. Нажмите кнопку **ОК**.

Вы вернетесь в область управления «Серверы», в которой будут перечислены все серверы, добавленные вами в группу. Теперь можно изменить состояние, просмотреть показатели и задать другие свойства серверов из данной группы.

См. также

- [Просмотр состояний серверов](#)

8.1.9.2 Работа с подгруппами серверов

С помощью подгрупп серверов можно дополнительно упорядочить серверы. Подгруппа – это группа серверов, которая входит в другую группу серверов.

Например, если серверы сгруппированы по региону и по стране, каждая региональная группа является подгруппой группы серверов соответствующей страны. Чтобы упорядочить серверы

таким образом, сначала создайте группу для каждого региона и добавьте в каждую региональную группу соответствующие серверы. Затем создайте по группе для каждой страны и добавьте региональные группы в соответствующие группы стран.

Подгруппы можно задать двумя способами: изменить подгруппы определенной группы серверов или сделать одну группу серверов членом другой группы. Результат будет одинаковым в обоих случаях, поэтому используйте наиболее удобный для вас метод.

8.1.9.2.1 Чтобы добавить подгруппы в группу серверов

1. Перейдите в область управления «Серверы» в СМС.
2. В дереве навигации щелкните **Группы серверов** и выберите группу серверов, в которую нужно добавить подгруппы.
Эта группа является родительской группой.
3. Выберите **Добавить членов** в меню **Действия**.
4. В дереве навигации выберите пункт **Группы серверов**, выберите группы серверов, которые требуется добавить в данную группу, и нажмите кнопку **>**.

Совет:

Удерживая нажатой клавишу **CTRL +**, щелкните **кнопкой мыши**, чтобы выбрать несколько групп серверов.

5. Нажмите кнопку **ОК**.

Вы вернетесь в область управления «Серверы», в которой будут перечислены все группы серверов, добавленные вами в родительскую группу.

8.1.9.2.2 Чтобы сделать одну группу серверов участником другой

1. Перейдите в область управления «Серверы» в СМС.
2. Выберите группу, которую нужно добавить в другую группу.
3. Выберите **Добавить в группу серверов** в меню **Действия**.
4. В списке **Доступные группы серверов** выберите другие группы, в которые требуется добавить эту группу, и нажмите кнопку **>**.

Совет:

Удерживая нажатой клавишу **CTRL +**, щелкните **кнопкой мыши**, чтобы выбрать несколько групп серверов.

5. Нажмите кнопку **ОК**.

8.1.9.3 Изменение принадлежности сервера к группе

Принадлежность сервера к группе можно изменить, чтобы быстро добавить сервер в любую группу или подгруппу, созданную в системе (или удалить из нее).

Приведем пример: предположим, вы создали группы серверов для разных регионов. Вам нужно использовать единый Центральный сервер управления (CMS, Central Management Server) для нескольких регионов. Вместо того чтобы добавлять сервер CMS отдельно в группу каждого региона, можно воспользоваться ссылкой **Участник** для данного сервера и добавить его сразу во все три региона.

8.1.9.3.1 Чтобы изменить принадлежность сервера к группе

1. Перейдите в область управления «Серверы» в СМС.
2. Щелкните правой кнопкой мыши сервер, для которого требуется изменить сведения об участии в группе, и выберите команду **Существующие серверные группы**.

На панели свойств в списке **Доступные группы серверов** отобразятся группы, в которые можно добавить данный сервер. В списке **Член групп серверов** отобразятся все группы серверов, к которым сервер принадлежит в данный момент.

3. Чтобы изменить принадлежность сервера к группам, стрелками переместите соответствующие группы серверов из одного списка в другой и нажмите кнопку **ОК**.

8.1.9.4 Доступ пользователей к серверам и группам серверов

Можно использовать права для предоставления пользователям доступа к серверам и группам серверов, которые позволяют пользователям выполнять такие задачи, как запуск и остановка серверов.

С учетом конфигурации системы и из соображений безопасности можно ограничить возможность управления серверами для администратора платформы SAP BusinessObjects Business Intelligence. Однако для этого может потребоваться разрешение доступа другим людям, использующим эти серверы. Во многих организациях есть группа IT-специалистов, которые занимаются управлением серверами. Если команде управления серверами нужно выполнить обычные задачи по обслуживанию сервера, для которых необходимо выключать и включать сервер, необходимо предоставить им права доступа к серверам. Можно также делегировать задачи по администрированию серверов платформы SAP BusinessObjects Business Intelligence другим пользователям. Возможно, вы захотите передать управление серверами другим группам в рамках вашей организации.

8.1.9.4.1 Для предоставления доступа к серверу или группе серверов

1. Перейдите в область управления «Серверы» в СМС.
2. Щелкните правой кнопкой мыши сервер или группу серверов, к которым требуется предоставить доступ, и выберите пункт **Безопасность пользователя**.
3. Нажмите кнопку **Добавить принципалов**, чтобы добавить пользователей или группы, которые получают доступ к выбранному серверу или группе серверов.

Появится диалоговое окно «Добавить принципалов».

4. Выберите пользователя или группу, которым вы хотите предоставить доступ к указанному серверу или группе серверов, затем нажмите >.
5. Щелкните **Добавить и назначить безопасность**.
6. В диалоговом окне «Назначить защиту» выберите параметры безопасности для пользователя или группы и нажмите кнопку **ОК**.

Подробную информацию о назначении прав см. в главе "Настройка прав".

8.1.9.4.2 Права объектов для сервера приложений отчетов Report Application Server

Для разрешения пользователям создавать и изменять отчеты по сети с использованием Report Application Server (RAS) необходимо иметь установленные в системе лицензии на изменение отчетов RAS. Также необходимо предоставить пользователям минимальный набор прав объектов. При предоставлении пользователям этих прав они могут выбрать отчет в качестве источника данных для нового отчета или изменить сам отчет.

- Просмотр объектов (или «Просмотр экземпляров документа» соответственно)
- Редактировать объекты
- Обновить данные отчета
- Экспортировать данные отчета

Чтобы иметь возможность сохранять отчеты в платформе SAP BusinessObjects Business Intelligence, у пользователя должно быть разрешение на добавление объектов как минимум в одну папку.

Чтобы убедиться, что пользователь может выполнять дополнительные задачи по созданию отчетов (такие как копирование, планирование, печать и т.д.), рекомендуется сначала задать соответствующий уровень доступа и сохранить изменения. Затем измените уровень доступа на "Расширенный" и добавьте любые необходимые права, которые еще не были предоставлены. Например, если пользователи имеют права на "Просмотр по требованию" в отношении объекта отчета, им можно разрешить изменять отчет, изменив уровень доступа на "Расширенный" и открыто предоставив дополнительное право редактирования объектов.

При просмотре пользователями отчетов с помощью средства просмотра расширенного DHTML и RAS, уровня доступа "Просмотр" достаточно для отображения отчета, но чтобы действительно использовать функции расширенного поиска, необходимы права "Просмотр по требованию". Дополнительное право на "Изменение" объектов не требуется.

8.1.10 Оценка производительности системы

8.1.10.1 Мониторинг серверов платформы SAP BusinessObjects Business Intelligence

Приложение мониторинга позволяет фиксировать оперативные и исторические показатели серверов платформы SAP BusinessObjects Business Intelligence для ведения отчетности и создания уведомлений. Приложение мониторинга помогает системному администратору определять, нормально ли работает сервер и не вышло ли время отклика за допустимые пределы.

См. также

- [О приложении мониторинга](#)

8.1.10.2 Анализ серверных показателей

Консоль Central Management Console (CMC) позволяет просматривать показатели для серверов в составе системы. Эти показатели включают общую информацию о каждом компьютере, а также сведения, относящиеся к каждому типу сервера. Также CMC позволяет вам просматривать системные показатели, которые включают информацию о версии продукта, CMS и текущей деятельности системы.

Примечание:

Для просмотра доступны показатели только для серверов, запущенных в настоящее время.

8.1.10.2.1 Просмотр показателей сервера

1. Перейдите в область управления «Серверы» в CMC.
2. Щелкните правой кнопкой мыши сервер, показатели которого требуется просмотреть, и выберите команду **Показатели**.

На вкладке «Показатели» отображается список показателей для сервера.

См. также

- [Для изменения свойств сервера](#)
- [О приложении "Показатели сервера"](#)

8.1.10.3 Просмотр системных показателей

Область управления СМС «Настройки» отображает системные показатели, которые предоставляют общую информацию о данной установке платформы SAP BusinessObjects Business Intelligence. Раздел «Свойства» включает информацию о версии и сборке продукта. Также здесь перечислены источники данных, имена баз данных и пользователей базы данных СМС. Раздел «Просмотр глобальных параметров системы» включает информацию об активности текущей учетной записи и статистику текущих и обработанных заданий. В разделе «Кластер» указано имя СМС, к которому вы подключены в настоящий момент, имя кластера СМС и имена других элементов кластера.

8.1.10.3.1 Для просмотра системных показателей

1. Перейдите в область управления СМС «Параметры».
2. Нажмите на стрелки, чтобы развернуть и просмотреть информацию разделов «Свойства», «Просмотр глобальных параметров системы» и «Кластер».

8.1.10.4 Регистрация деятельности сервера

Платформа SAP BusinessObjects Business Intelligence позволяет регистрировать конкретную информацию о деятельности платформы SAP BusinessObjects Business Intelligence в сети.

- Кроме того, каждый из серверов платформы SAP BusinessObjects Business Intelligence регистрирует сообщения в стандартном журнале операционной системы.
 - В операционной системе Windows платформа SAP BusinessObjects Business Intelligence регистрирует записи в службе "Журнал событий". Вы можете просмотреть результаты с помощью программы просмотра событий (в журнале приложений).
 - В UNIX платформа SAP BusinessObjects Business Intelligence регистрирует события в демоне syslog как пользовательское приложение. В начале каждого сообщения записывается имя каждого сервера и PID.

Каждый сервер записывает сообщения в директорию протокола вашей инсталляции. Программная информация, записанная в эти файлы, обычно необходима только специалистам по поддержке SAP Business Objects при проведении расширенной отладки. Расположение файлов журналов зависит от используемой операционной системы:

- В Windows по умолчанию журналы ведутся в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Logging`.
- В UNIX по умолчанию журналы ведутся в каталоге `<INSTALLDIR>/sap_bobj/logging` существующей установки.

Необходимо отметить, что файлы журналов автоматически очищаются, и данные журнала никогда не занимают более чем 1 Мб на сервер.

Примечание:

Чтобы разрешить ведение журналов в функции (например, netcat) на компьютерах UNIX, содержащих серверы платформы SAP BusinessObjects Business Intelligence, необходимо установить и настроить системную регистрацию событий таким образом, чтобы записывались все сообщения, регистрируемые для типа источника «user» на уровне «info» и выше. Также необходимо настроить в демоне SYSLOGD включение удаленного ведения журнала.

Процедуры установки могут различаться в зависимости от систем. Для получения инструкций обратитесь к документации по вашей операционной системе.

8.1.10.5 Конфигурация серверов в СМС для оптимизации производительности функции Публикация.

В общем случае для оптимизации производительности задания Публикация можно выполнить следующие действия:

- В области «Серверы» консоли СМС отключите ненужные серверы. Например, если выполняется только публикация отчета Crystal, можно отключить серверы Desktop Intelligence и Web Intelligence. Однако перед этим убедитесь, что отключаемые серверы не используются другими пользователями системы.
- Убедитесь в том, что для серверов заданий, которые используются функцией Публикация, для параметра **Максимальное число одновременных заданий** задано значение "5 на ЦП". Для этого в области «Серверы» выберите нужный сервер заданий и нажмите **Управление > Свойства**.

Соответствующим образом измените уровень детализации, занесенный в журнал сервером адаптивной обработки.

Примечание:

При повышении уровня детализации в файлах журнала производительность сервера может снизиться.

Уровень детализации файлов журнала, используемый по умолчанию (и рекомендуемый), имеет значение **ОШИБКА**. Однако вашему публикатору или вам самим может потребоваться увеличить уровень детализации в файлах журнала сервера адаптивной обработки, чтобы более точно отслеживать выполнение заданий опубликования. Для этого в области «Серверы» выберите сервер адаптивной обработки и нажмите **Управление > Свойства**. В списке «Уровень журнала» выберите **ИНФО**. Уровень **ИНФО** обеспечивает более подробные данные, например, следующие:

- Публикация успешно доставлена получателю.
- Пакет получателей обработан успешно.
- Расширения публикации для заключительно обработки активированы.

Настройте сервер адаптивной обработки, чтобы обеспечить обработку большего количества заданий.

Производительность сервера адаптивной обработки можно повысить следующим образом:

- При одновременном выполнении нескольких публикаций создайте несколько экземпляров сервера адаптивной обработки. Как правило, рекомендуется создать по одному экземпляру сервера адаптивной обработки для каждой трех публикаций, выполняемых одновременно.
- Повысьте объем динамической памяти, отведенной для сервера адаптивной обработки. Для этого выберите **Управление > Свойства** и добавьте в командную строку следующий параметр:
–Xmx1024M.
- Запустите службу опубликования и службу заключительной обработки на разных экземплярах сервера адаптивной обработки.

Если публикатору необходимо активировать функции аудита и очистки, задайте соответствующие параметры аудита в CMS, чтобы в журнал заносились все подробности.

Для запуска объемных публикаций публикатору рекомендуется активировать функцию чистки для удаления ненужных файлов, создаваемым заданием публикации и экономии места на сервере. Для этого на этапе планирования публикации необходимо, чтобы публикатор снял флажок, определяющий местоположение Enterprise по умолчанию в качестве места назначения.

Если для функции "Публикация" активируется аудит, необходимо настроить на CMS поддержку данного сценария таким образом, чтобы подробные сведения об удаленных файлах все равно записывались. В области «Серверы» выберите CMS и нажмите **Управление > Свойства**. В отобразившемся диалоговом окне выберите **События аудита** в списке навигации. Убедитесь в том, что функция **Аудит** активирована и выбран флажок **Объект удален**.

Убедитесь, что настройки электронной почты заданы правильно для сервера заданий для адресатов.

Может произойти сбой публикаций, предназначенных для адресатов электронной почты, поскольку электронная почта настроена неправильно в качестве адресата для сервера заданий для адресатов. В области «Серверы» консоли СМС дважды щелкните мышью сервер заданий для адресатов. В диалоговом окне «Свойства» выберите **Адресат** в списке навигации, чтобы убедиться в следующем:

- **Электронная почта** добавлена в качестве адресата.
- Значения в полях **Имя домена**, **Хост** и **Порт** указаны правильно.
- В поле **Кому** указан адрес %SI_EMAIL_ADDRESS%.

Увеличьте количество одновременно выполняемых заданий, которое может обработать сервер заданий для адресатов.

Если публикации предназначены для местоположения платформы BI по умолчанию или для местоположения на диске, который не находится под управлением, и при этом для сервера репозитория исходящих файлов используются чередующиеся диски, то рекомендуется задать максимальное количество одновременно выполняемых заданий равным количеству дисков, умноженному на пять.

Если издатель использует динамические источники получателей отчета Crystal, убедитесь, что сервер приложений отчетов (RAS) настроен правильно.

На сервере RAS необходимо настроить, чтобы число читаемых записей базы данных было по крайней мере равно числу получателей в динамическом источнике получателей. Например, для обработки динамического источника получателей с данными для 100000 получателей на сервере RAS необходимо настроить чтение более чем 100000 записей базы данных.

Чтобы проверить эту настройку, в области «Серверы» консоли СМС выберите сервер RAS и перейдите к пункту **Управление > Свойства**. Убедитесь, что значение в поле **Число записей базы данных для чтения при предварительном просмотре или обновлении отчета** указано правильно, или укажите новое значение.

Устранение ошибок «Недостаточно памяти»

Если публикатор получает сообщение об ошибке `java.lang.ОшибкаНехваткиПамяти`: не удалось создать новый собственный поток при выполнении объемной публикации, это значит, что на сервере адаптивной обработки или в службе публикации недостаточно памяти стека для обработки числа создаваемых потоков функции Публикация. Эта ошибка может появиться, если память стека назначена как область динамической памяти Java.

Для сервера адаптивной обработки можно задать ограничение потоков. В области «Серверы» консоли СМС выберите настраиваемый сервер обработки и перейдите к пункту **Управление > Свойства**. В поле **Параметры командной строки** укажите следующий параметр командной строки:

```
-Dcom.businessobjects.publisher.threadpool.size=threadlimitnumber
```

Замените *threadlimitnumber* необходимым значением ограничения потоков.

Если издатель получает сообщение об ошибке `java.lang.OutOfMemoryError`: пространство динамической памяти Java при выполнении публикации большого объема, на настраиваемом сервере обработки недостаточно пространства динамической памяти. В области «Серверы» консоли СМС выберите настраиваемый сервер обработки и перейдите к пункту **Управление > Свойства**. В поле **Параметры командной строки** измените числовую составляющую значения параметра командной строки `-Xmx256m` на более крупное число (например, `-Xmx1024m`).

Примечание:

В некоторых случаях для устранения ошибок «Недостаточно памяти» необходимо создать дополнительные экземпляры сервера адаптивной обработки.

8.1.11 Конфигурация настроек серверов

Этот раздел включает техническую информацию и процедуры изменения настроек для серверов платформы SAP BusinessObjects Business Intelligence.

Большинство настроек, рассматриваемых в данном разделе, позволяет более эффективно интегрировать платформу SAP BusinessObjects Business Intelligence с текущим аппаратным и программным обеспечением, а также с конфигурацией сети. Поэтому выбранные вами настройки в большинстве случаев будут зависеть от ваших требований.

Настройки сервера можно изменить на Central Management Console (CMC) двумя способами.

- В окне «Свойства» для сервера.
- В окне «Изменение общих служб» для сервера.

Обратите внимание на то, что не все изменения отображаются сразу после внесения. Если какую-либо настройку невозможно сразу же изменить, в окнах «Свойства» и «Изменение общих служб» отображаются и текущие (выделено красным), и требуемые настройки. При возвращении в область управления "Серверы" данный сервер будет помечен как "устаревший". При перезапуске сервера будут применены нужные настройки и флаг "Устаревшие" будет удален для сервера.

Примечание:

В этом разделе не рассматривается настройка сервера веб-приложений для развертывания приложений платформы SAP BusinessObjects Business Intelligence. Эта задача обычно выполняется при установке продукта. Для получения дополнительной информации см. *Руководство по установке платформы SAP BusinessObjects Business Intelligence*.

См. также

- [Настройка номеров портов](#)
- [Для изменения свойств сервера](#)
- [Повторное создание базы данных системы центрального сервера управления](#)
- [Выбор новой или существующей базы данных центрального сервера управления](#)

8.1.11.1 Для изменения свойств сервера

1. Перейдите в область управления «Серверы» в СМС.
2. Дважды щелкните сервер, параметры которого требуется изменить.
Открывается диалоговое окно «Свойства».
3. Внесите необходимые изменения, а затем нажмите кнопку **Сохранить** или **Сохранить и закрыть**.

Примечание:

Не все настройки применяются сразу же после внесения. Если какую-либо настройку невозможно сразу же изменить, в диалоговом окне "Свойства" одновременно отображаются текущие (выделенные красным) и необходимые настройки. При возвращении в область управления "Серверы" данный сервер будет помечен как "устаревший". При перезапуске сервера будут применены нужные настройки из диалогового окна "Свойства", и пометка "Устаревший" будет снята для данного сервера.

8.1.11.2 Применение параметров службы к нескольким серверам

Чтобы применить один и тот же параметр к службам, размещенным на нескольких серверах,

1. Перейдите в область управления «Серверы» в СМС.

2. Правой кнопкой мыши щелкните серверы, на которых расположены службы, чьи параметры нужно изменить, а затем щелкните **Изменить общие службы**.

Диалоговое окно «Изменить общие службы» отображает службы, располагающиеся на всех выбранных серверах и имеющие изменяемые параметры.

3. Если в диалоговом окне «Изменить общие службы» перечислено несколько служб, выберите службу, которую нужно изменить и нажмите кнопку **Продолжить**.
4. Сделайте необходимые изменения и нажмите кнопку **ОК**.

Примечание:

Перенаправление в область управления СМС «Серверы». Если серверам требуется перезапуск, они помечаются как устаревшие. При перезапуске сервера будут применены нужные настройки и флаг "Устаревшие" будет удален с серверов.

8.1.11.3 Работа с шаблонами конфигурации

С помощью шаблонов конфигурации можно с легкостью настроить несколько экземпляров серверов. В шаблонах конфигурации сохраняется список настроек каждого типа службы, который можно использовать для настройки дополнительных экземпляров сервера. Например, если нужно ввести одинаковые настройки для двенадцати серверов обработки Web Intelligence, потребуется задать настройки только для одного из них. Затем можно будет сохранить введенные настройки службы в шаблоне конфигурации для серверов обработки Web Intelligence и применить данный шаблон к оставшимся 11 серверам.

Для каждого типа служб платформы SAP BusinessObjects Business Intelligence используется собственный шаблон конфигурации. Например, существует отдельный шаблон конфигурации для службы обработки Web Intelligence, отдельный шаблон для службы публикации и т.д. Шаблон конфигурации необходимо задать в свойствах сервера в консоли Central Management Console (СМС).

Если на сервере настроено использование шаблона конфигурации, существующие параметры сервера перезаписываются значениями шаблона. Если впоследствии решено приостановить использование шаблона, восстановление исходных параметров невозможно. Последующие изменения шаблона конфигурации не влияют на сервер.

Наиболее удобно использовать шаблоны конфигурации следующим способом:

1. Задайте шаблон конфигурации на одном сервере.
2. Если необходимо задать одинаковые параметры на всех серверах одного типа, поставьте флажок **Использовать шаблон конфигурации** для всех серверов одинакового типа, включая сервер, на котором был задан шаблон конфигурации.
3. Если впоследствии потребуется изменить конфигурацию всех служб данного типа, перейдите в раздел свойств любой из этих служб и снимите флажок **Использовать шаблон конфигурации**. Измените необходимые настройки, выберите **Задать шаблон конфигурации** для данного сервера и нажмите кнопку **Сохранить**. Все службы данного типа будут обновлены. Отсутствие сервера, всегда заданного в качестве шаблона конфигурации, гарантирует защиту от случайного изменения настроек конфигурации для всех серверов соответствующего типа.

См. также

- [Определение шаблона конфигурации](#)
- [Применение шаблона конфигурации к серверу](#)

8.1.11.3.1 Определение шаблона конфигурации

Шаблон конфигурации можно задать для каждого типа службы. Однако для одной службы нельзя задать несколько шаблонов конфигурации. Используйте страницу «Свойства» любого сервера для введения настроек, которые будут применяться шаблоном конфигурации к службе определенного типа, размещенной на сервере.

1. Перейдите в область управления «Серверы» в СМС.
2. Дважды щелкните сервер, на котором размещаются службы, для которых нужно задать шаблон конфигурации.
Открывается диалоговое окно «Свойства».
3. Настройте параметры службы, которые необходимо использовать в шаблоне, установите флажок **Задать шаблон конфигурации** и нажмите кнопку **Сохранить** или **Сохранить и закрыть**.

Шаблон конфигурации для выбранного типа службы будет задан согласно настройкам текущего сервера. Конфигурация других серверов того же типа, на которых размещена такая же служба, сразу же будет автоматически изменена в соответствии с данным шаблоном конфигурации, если в свойствах данных серверов активирован параметр **Использовать шаблон конфигурации**.

Примечание:

Если параметры для шаблона конфигурации не заданы явно, для службы используются параметры по умолчанию.

См. также

- [Применение шаблона конфигурации к серверу](#)

8.1.11.3.2 Применение шаблона конфигурации к серверу

Перед применением шаблона убедитесь в том, что вы задали настройки шаблона конфигурации для соответствующего типа сервера. Если параметры шаблона конфигурации явно не заданы, для службы используются параметры по умолчанию.

Примечание:

Серверы, на которых не активирована настройка "Использовать шаблон конфигурации", не будут обновляться при изменении шаблона конфигурации.

1. Перейдите в область управления «Серверы» в СМС.
2. Дважды щелкните сервер, на котором размещается служба, к которой нужно применить шаблон конфигурации.
Открывается диалоговое окно «Свойства».
3. Установите флажок **Использовать шаблон конфигурации** и нажмите кнопку **Сохранить** или **Сохранить и закрыть**.

Примечание:

Если сервер необходимо перезапустить, чтобы новые настройки вступили в силу, он будет отображаться в списке серверов как "устаревший".

К текущему серверу будет применен соответствующий шаблон конфигурации. Все последующие изменения шаблона конфигурации влияют на конфигурацию всех серверов, на которых используется этот шаблон.

При снятии флажка **Использовать шаблон конфигурации** для конфигурации сервера не восстанавливаются значения, которые использовались до применения шаблона конфигурации. Последующие изменения шаблона конфигурации не влияют на конфигурацию серверов, на которых используется этот шаблон.

См. также

- [Определение шаблона конфигурации](#)

8.1.11.3.3 Восстановление настроек системы по умолчанию

Возможно, вам потребуется восстановить конфигурацию службы до состояния на момент изначальной инициализации (например, если для серверов будут заданы неверные настройки или возникнут проблемы с работоспособностью системы).

1. Перейдите в область управления «Серверы» в СМС.
2. Дважды щелкните сервер, на котором размещается служба, для которой необходимо восстановить параметры по умолчанию.
Открывается диалоговое окно «Свойства».
3. Установите флажок **Восстановить параметры системы по умолчанию** и нажмите кнопку **Сохранить** или **Сохранить и закрыть**.
Будут восстановлены параметры по умолчанию для соответствующего типа службы.

8.1.12 Настройка сетевых параметров сервера

Управление сетевыми параметрами серверов платформы SAP BusinessObjects Business Intelligence осуществляется посредством СМС. Эти настройки разделены на две категории: настройки портов и идентификация узла.

Установки по умолчанию

При установке для параметра идентификации узла задается значение **Назначать автоматически**. Однако для каждого сервера можно назначить отдельный IP-адрес или имя хоста. Номер порта СМС по умолчанию: 6400. Другие серверы платформы SAP BusinessObjects Business Intelligence динамически устанавливают связь с доступными портами. Платформа SAP BusinessObjects Business Intelligence управляет номерами портов автоматически, однако их также можно задать в СМС.

8.1.12.1 Параметры сетевой среды

Платформа SAP BusinessObjects Business Intelligence поддерживает трафик по интернет-протоколам версий 6 (IPv6) и 4 (IPv4). Серверные и клиентские компоненты можно использовать в любой из следующих сред:

- Сеть IPv4: все серверные и клиентские компоненты работают только по протоколу IPv4.
- Сеть IPv6: все серверные и клиентские компоненты работают только по протоколу IPv6.
- Смешанная сеть IPv6/IPv4: серверные и клиентские компоненты могут работать по протоколам IPv6 и IPv4.

Примечание:

Настройка сети является обязанностью системного и сетевого администратора. В платформе SAP BusinessObjects Business Intelligence не предусмотрен механизм для определения сетевой среды. С помощью CMC определенный IP-адрес IPv6 или IPv4 можно связать с любым сервером платформы SAP BusinessObjects Business Intelligence.

8.1.12.1.1 Смешанная среда IPv6/IPv4

Смешанная сетевая среда IPv6/IPv4 обеспечивает следующие возможности.

- При работе в смешанном режиме IPv6/IPv4 серверы платформы SAP BusinessObjects Business Intelligence могут обслуживать запросы как IPv6, так и IPv4.
- Клиентские компоненты могут взаимодействовать с серверами в качестве узлов IPv6, IPv4, или в качестве узлов IPv6/IPv4.

Смешанный режим может быть особенно полезен в следующих ситуациях:

- Вы переходите от узла среды IPv4 к узлу IPv6. Все клиентские и серверные компоненты продолжают свое безошибочное взаимодействие в течение всего процесса перехода. Затем можно отключить настройки IPv4 для всех серверов.
- Стороннее программное обеспечение, не совместимое с IPv4, будет функционировать в среде с узлами IPv6/IPv4.

Примечание:

Если узел IPv6 используется с Windows 2003, разрешения для имен DNS могут быть некорректными. Если в Windows 2003 отключен стек протоколов IPv4, рекомендуется использовать в развертывании оба протокола IPv6/IPv4.

8.1.12.2 Параметры идентификации хоста сервера

Параметры идентификации хоста сервера можно задать в СМС для каждого сервера платформы SAP BusinessObjects Business Intelligence. В таблице ниже перечислены все параметры, доступные в области Общие параметры.

Действие	Описание
Назначать автоматически	<p>Это установка по умолчанию для всех серверов. Если выбран параметр Назначать автоматически, сервер автоматически связывает свой порт запросов с первым сетевым интерфейсом устройства.</p> <p>Примечание: Рекомендуется устанавливать флажок напротив параметра "Назначать автоматически" для настройки имени хоста. Однако в некоторых случаях, например, если сервер работает на машине, подключенной к нескольким сетям, или если серверу необходимо взаимодействовать с определенной конфигурацией брандмауэра, следует рассмотреть возможность использования определенного имени хоста или IP-адреса. Для получения дополнительных сведений см. главы «Настройка многосетевого компьютера» и «Работа с брандмауэрами» в <i>Руководстве администратора платформы SAP BusinessObjects Business Intelligence</i>.</p>
Имя хоста	Указывает имя хоста сетевого интерфейса, в котором сервер выполняет прослушивание запросов. Для CMS этот параметр определяет имя хоста сетевого интерфейса, с которым CMS связывает порт сервера имен и порт запросов.
IP-адрес	Указывает IP-адрес сетевого интерфейса, в котором сервер выполняет прослушивание запросов. Для CMS данная настройка определяет адрес сетевого интерфейса, с которым CMS связывает порт сервера имен и порт запросов. Для каждого сервера имеются отдельные поля для указания IP-адресов IPv4 и/или IPv6.

Предупреждение:

Важно: если на многосетевых компьютерах активирована функция **Назначать автоматически**, CMS может автоматически установить связь с неверным сетевым интерфейсом. Для предотвращения подобных ошибок необходимо убедиться в том, что сетевые интерфейсы перечислены на хосте в нужном порядке (используйте для этого средства ОС данного компьютера). Также необходимо задать параметры имени хоста CMS в СМС.

Примечание:

При работе с многосетевыми компьютерами или определенными настройками NAT межсетевого экрана необходимо указывать имя хоста в виде полностью определенных доменных имен, а не имен хоста.

См. также

- [Настройка группового компьютера](#)
- [Устранение неполадок при наличии нескольких сетевых интерфейсов](#)

8.1.12.2.1 Изменение идентификации хоста сервера

1. Перейдите в область управления «Серверы» в СМС.
2. Выберите сервер, а затем выберите пункт **Остановка сервера** в меню **Действия**.
3. Выберите **Свойства** в меню **Управление**.
4. В разделе **Общие параметры** выберите один из следующих параметров:

Действие	Описание
Назначать автоматически	Сервер установит связь с одним из доступных сетевых интерфейсов.
Имя хоста	Введите имя хоста сетевого интерфейса, в котором сервер выполняет прослушивание запросов.
IP-адрес	Введите в соответствующие поля IP-адрес IPv4 или IPv6 для сетевого интерфейса, в котором сервер выполняет прослушивание запросов. Примечание: Чтобы разрешить серверу работать в качестве двойного узла IPv4/IPv6, введите допустимый IP-адрес в оба поля.

5. Нажмите кнопку **Сохранить** или **Сохранить и закрыть**.
Изменения отражаются в командной строке на вкладке «Свойства».
6. Запустите и включите сервер.

8.1.12.3 Настройка группового компьютера

Групповой компьютер – это компьютер с несколькими сетевыми адресами. Такую конфигурацию можно создавать в нескольких сетевых интерфейсах, для каждого из которых предусмотрен один или несколько IP-адресов, или в одном сетевом интерфейсе, который назначен нескольким IP-адресам.

При наличии нескольких сетевых интерфейсов, для каждого из которых предусмотрен один IP-адрес, измените порядок привязки, чтобы сетевой интерфейс на верхнем уровне привязки использовался для связи с серверами платформы SAP BusinessObjects Business Intelligence. Если для интерфейса предусмотрено несколько IP-адресов, используйте параметр "Имя хоста" на консоли СМС для определения сетевой интерфейсной платы для сервера платформы SAP BusinessObjects Business Intelligence. Она может быть определена именем хоста или IP-адресом. Для получения дополнительных сведений о настройке параметра "Имя хоста" см. раздел «Обнаружение и устранение неполадок».

Совет:

В этом разделе описан способ настройки во всех серверах одного сетевого адреса, но также возможно выполнить привязку отдельных серверов к различным адресам. Например, может быть

необходимо привязать сервер репозитория файлов к личному файлу, который нельзя маршрутизировать с компьютеров пользователей. Для дополнительных настроек, подобных этой, требуется настройка DNS для эффективной маршрутизации связи между всеми компонентами сервера платформы SAP BusinessObjects Business Intelligence. В этом примере DNS должен маршрутизировать связи от других серверов платформы SAP BusinessObjects Business Intelligence к личному адресу сервера репозитория файлов.

См. также

- [Устранение неполадок при наличии нескольких сетевых интерфейсов](#)

8.1.12.3.1 Настройка привязки сервера CMS к сетевому адресу

Примечание:

На многосетевом компьютере необходимо задать параметр "Идентификатор хоста" для полного определенного имени домена или IP-адреса интерфейса, с которым необходимо связать сервер.

1. Перейдите в область управления **Серверы** в CMS.
2. Дважды щелкните CMS.
3. В разделе «Общие параметры» выберите один из следующих параметров:
 - **Имя хоста**
 - Введите имя хоста сетевого интерфейса, с которым будет связан сервер.
 - **IP-адрес**
 - Введите в имеющиеся поля IP-адреса IPv4 или IPv6 сетевого интерфейса, с которым будет связан сервер.

Примечание:

Чтобы разрешить серверу работать в качестве двойного узла IPv4/IPv6, введите допустимый IP-адрес в оба поля.

Предупреждение:

Не ставьте флажок в поле "Назначать автоматически".

4. Параметр **Порт запросов** можно задать одним из следующих методов:
 - Выберите **Назначать автоматически**.
 - Введите в поле **Порт запросов** номер порта.
5. Убедитесь, что номер порта указан в диалоговом окне "Порт сервера имен".

Примечание:

По умолчанию используется номер порта 6400.

8.1.12.3.2 Настройка остальных серверов для привязки к сетевому адресу

На остальных серверах платформы SAP BusinessObjects Business Intelligence порты выбираются динамически по умолчанию. Для получения сведений об отключении параметра автоматического назначения, который динамически распространяет эту информацию, см. раздел «Изменение порта, который используется сервером для приема запросов».

См. также

- [Изменение порта, который используется сервером для приема запросов](#)

8.1.12.3.3 Устранение неполадок при наличии нескольких сетевых интерфейсов

На многосетевом компьютере CMS может автоматически выполнить привязку к неверному сетевому интерфейсу. Чтобы предотвратить подобное, убедитесь, что сетевые интерфейсы на компьютере хоста перечислены в правильном порядке (используя инструменты операционной системы данного компьютера) и в СМС заданы параметры имени хоста CMS. Если маршрутизация основного сетевого интерфейса невозможна, выполните нижеуказанные инструкции для привязки платформы BI к дополнительному сетевому интерфейсу, пригодному для маршрутизации. Выполните данные действия сразу же после установки платформы BI на локальном компьютере, перед установкой платформы на других компьютерах.

1. Откройте CCM и остановите работу SIA на узле компьютера с несколькими сетевыми интерфейсами.
2. Щелкните SIA правой кнопкой мыши и выберите команду **Свойства**.
3. В диалоговом окне «Свойства» выберите вкладку «Конфигурация».
4. Для того чтобы связать SIA с определенным сетевым интерфейсом, введите в поле **Порт** один из следующих параметров:
 - имя хоста целевого сетевого интерфейса и номер порта (в формате имя хоста:номер порта)
 - IP-адрес целевого сетевого интерфейса и номер порта (в формате IP-адрес:номер порта)
5. Нажмите кнопку **ОК** и откройте вкладку «Запуск».
6. В списке «Локальные серверы CMS» выберите CMS и нажмите кнопку **Свойства**.
7. Для того чтобы связать CMS с определенным сетевым интерфейсом, введите в поле **Порт** один из следующих параметров:
 - имя хоста целевого сетевого интерфейса и номер порта (в формате имя хоста:номер порта)
 - IP-адрес целевого сетевого интерфейса и номер порта (в формате IP-адрес:номер порта)
8. Чтобы применить новые параметры, нажмите кнопку **ОК**.
9. Запустите SIA и подождите, пока не запустятся серверы.
10. Запустите консоль Central Management Console (CMC) и перейдите в область управления «Серверы». Повторите шаги 11-14 для каждого сервера.
11. Выберите сервер, а затем выберите пункт **Остановка сервера** в меню **Действия**.
12. Выберите **Свойства** в меню **Управление**.
13. В разделе **Общие параметры** выберите один из следующих параметров:
 - Имя хоста: введите имя хоста сетевого интерфейса, с которым будет связан сервер.
 - IP-адрес: введите в имеющиеся поля IP-адреса IPv4 или IPv6 сетевого интерфейса, с которым будет связан сервер.

Примечание:

Чтобы разрешить серверу работать в качестве двойного узла IPv4/IPv6, введите допустимый IP-адрес в оба поля.

Предупреждение:

Не ставьте флажок в поле "Назначать автоматически".

14. Нажмите кнопку **Сохранить** или **Сохранить и закрыть**.

15. Вернитесь в CCM и перезапустите SIA.

SIA выполнит перезапуск всех серверов на узле. Теперь все серверы на компьютере связаны с нужным сетевым интерфейсом.

8.1.12.4 Настройка номеров портов

Во время установки CMS настраивается на использование номеров портов по умолчанию. Номер порта CMS по умолчанию: 6400. Этот порт попадает в диапазон портов, зарезервированных продуктом Business Objects (от 6400 до 6410). Взаимодействие на этих портах не должно вступать в конфликт со сторонними приложениями.

При запуске и включении каждый из остальных серверов платформы SAP BusinessObjects Business Intelligence динамически устанавливает связь с доступным портом (выше чем 1024), регистрирует этот порт на сервере CMS, а затем прослушивает запросы платформы SAP BusinessObjects Business Intelligence. При необходимости можно выполнить настройки, чтобы каждый компонент сервера выполнял прослушивание на определенном порте (а не выбирал динамически любой доступный порт).

Номера портов можно указать в CMS на вкладке "Свойства" для каждого сервера. В этой таблице приведены параметры из меню «Общие параметры», относящиеся к использованию порта определенными серверами.

Параметр	CMS	Другие серверы
Порт запросов	Указывает порт, который CMS использует для приема всех запросов с других серверов (за исключением запросов сервера имен). Использует такой же сетевой интерфейс, что и порт сервера имен. При выборе параметра Назначать автоматически сервер автоматически использует номер порта, назначенный операционной системой.	Указывает порт, на котором сервер выполняет прослушивание всех запросов. Если выбран параметр Назначать автоматически , на сервере автоматически используется номер порта, назначенный ОС.

Параметр	CMS	Другие серверы
Порт сервера имен	Определяет порт платформы SAP BusinessObjects Business Intelligence, через который CMS прослушивает запросы службы имен. По умолчанию это порт 6400.	Не применимо.

8.1.12.4.1 Для изменения порта CMS по умолчанию в CMC

Если в кластере уже выполняется CMS, можно использовать CMC для изменения номера порта CMS по умолчанию. Если в кластере нет запущенных серверов CMS, для изменения номера порта необходимо использовать CCM в Windows или скрипт `serverconfig.sh` в UNIX.

Примечание:

CMS использует одну и ту же сетевую интерфейсную плату для порта запросов и порта сервера имен.

1. Перейдите в область управления «Серверы» в CMC.
2. В списке серверов дважды щелкните CMS.
3. Замените номер **порта сервера имен** на порт, на котором вы хотите, чтобы CMS выполнял прослушивание. (Порт по умолчанию: 6400).
4. Нажмите кнопку **Сохранить и закрыть**.
5. Перезапустите CMS.

CMS начинает прослушивание на порте, который вы указали. Server Intelligence Agent динамически распространяет новые параметры на остальные серверы на узле, если на этих серверах для порта запросов выбран параметр **Назначать автоматически**. (Чтобы внесенные изменения появились в параметрах меню «Свойства» для всех членов узла, потребуется несколько минут).

Параметры, выбранные на странице «Свойства», отражаются в командной строке сервера, которая также отображается на странице «Свойства».

8.1.12.4.2 Изменение порта CMS по умолчанию на сервере CCM в операционной системе Windows

Если в кластере отсутствуют доступные CMS, и нужно изменить порт CMS по умолчанию для части CMS в развертывании, это делается с помощью CCM.

1. Откройте CCM и остановите SIA для данного узла.
2. Щелкните SIA правой кнопкой мыши и выберите команду **Свойства**.
3. В диалоговом окне «Свойства» выберите вкладку «Запуск».
4. В списке «Локальные серверы CMS» выберите CMS, для которого нужно изменить номер порта, и щелкните пункт **Свойства**.

5. Для создания CMS для определенного порта введите в поле **Порт** один из следующих параметров:
 - номер порта
 - имя хоста и номер порта (используйте формат имя хоста:номер порта)
 - IP-адрес и номер порта (используйте формат IP-адрес:номер порта)
6. Чтобы применить новые параметры, нажмите кнопку **ОК**.
7. Запустите SIA и подождите, пока не запустятся серверы.

8.1.12.4.3 Изменение порта CMS по умолчанию на сервере CCM в операционной системе UNIX

Если в кластере нет доступных CMS и требуется изменить порт CMS по умолчанию для одного или нескольких серверов CMS в развертывании, для изменения порта CMS необходимо использовать скрипт `serverconfig.sh`.

1. Используйте скрипт `ccm.sh` для остановки SIA (Server Intelligence Agent), на котором размещается сервер CMS, номер порта которого требуется изменить.
2. Выполните скрипт `serverconfig.sh`. По умолчанию этот скрипт находится в каталоге `<InstallDir>/sap_bobj`.
3. Выберите пункт 3 – "Изменить Server Intelligence Agent" и нажмите клавишу **Enter**.
4. Выберите SIA, размещенный на сервере CMS, в который нужно внести изменения, и нажмите клавишу **Enter**.
5. Выберите пункт 4 – "Изменить узел" и нажмите клавишу **Enter**.
Отобразится список серверов CMS, размещенных в данный момент на SIA.
6. Выберите серверы CMS, который нужно изменить, и нажмите клавишу **Enter**.
7. Введите новый номер порта для CMS и нажмите клавишу **Enter**.
8. Укажите, должен ли CMS автоматически запускаться при запуске SIA, и нажмите клавишу **Enter**.
9. Введите аргументы командной строки для CMS или оставьте текущие аргументы и нажмите клавишу **Enter**.
10. Запустите SIA с помощью `ccm.sh` и дождитесь, пока запустятся серверы.

8.1.12.4.4 Изменение порта, который используется сервером для приема запросов

1. Перейдите в область управления «Серверы» в CMC.
2. Выберите сервер, а затем выберите пункт **Остановка сервера** в меню **Действия**.
3. Дважды щелкните на сервер.
Откроется окно «Свойства».
4. В меню «Общие параметры» снимите флажок **Назначать автоматически** для **Порта запроса**, затем введите номер порта, на котором сервер должен выполнять прослушивание.
5. Нажмите кнопку **Сохранить** или **Сохранить и закрыть**.
6. Запустите и включите сервер.

Сервер установит связь с новым портом, зарегистрирует его на сервере CMS и начнет прослушивание запросов платформы SAP BusinessObjects Business Intelligence на новом порте.

8.1.13 Управление узлами

8.1.13.1 Использование узлов

Узел представляет собой группу серверов платформы BI, работающих на одном хосте. Все серверы в узле запускаются под одной учетной записью.

На компьютере можно создать множество узлов, что позволяет запускать процессы под различными учетными записями.

Один Server Intelligence Agent (SIA) обеспечивает управление всеми серверами в узле и их мониторинг в целях обеспечения правильной их работы.

Примечание:

Для защищенного выполнения всех процедур управления узлом необходимо использовать учетную запись администратора с аутентификацией администратора. Тем не менее, если обмен данными между серверами ведется с использованием SSL, перед выполнением любых процедур управления узлами необходимо отключить SSL. Для получения дополнительных сведений см. раздел «Настройка SSL на серверах».

8.1.13.1.1 Переменные

В этой главе используются следующие переменные.

Переменная	Описание
<code><INSTALLEDIR></code>	Каталог, в котором установлена платформа BI. На компьютере под управлением ОС Windows это каталог <code>C:\Program Files (x86)\SAP BusinessObjects</code>
<code><SCRIPTDIR></code>	Каталог, в котором размещаются скрипты управления узлами. На компьютере под управлением ОС Windows это каталог <code><INSTALLEDIR>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\scripts</code> На компьютерах под управлением ОС Unix это каталог <code><INSTALLEDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/scripts</code>
<code><PLATFORM></code>	Имя операционной системы Unix. Допустимыми значениями являются следующие: <ul style="list-style-type: none"> • <code>aix_rs6000_64</code> • <code>linux_x64</code> • <code>solaris_sparcv9</code> • <code>hpux_ia64</code>

8.1.13.2 Добавление нового узла

Программа установки создает узлы при первой установке платформы BI.

При необходимости можно добавить дополнительные узлы, если требуется добавить в кластер новые компьютеры, повысить производительность кластера или запускать серверы под другими учетными записями пользователей в существующем развертывании.

Для добавления нового узла можно использовать Central Configuration Manager (CCM) или скрипт управления узлами. Если используется брандмауэр, убедитесь, что порты Server Intelligence Agent (SIA) и Центрального сервера управления (CMS) открыты.

Помните:

Узел можно добавить только на том компьютере, на котором он расположен.

8.1.13.2.1 Добавление узла на новый компьютер в существующем развертывании

При добавлении нового компьютера в существующее развертывание с помощью программы установки можно автоматически создать на этом компьютере первый узел.

Совет:

В процессе установки нажмите кнопку **Развернуть** и укажите существующий центральный сервер управления.

Для создания дополнительных узлов используйте Central Configuration Manager или скрипт.

Подробнее об установке см. *Руководство по установке платформы SAP BusinessObjects Business Intelligence*.

8.1.13.2.2 Добавление узла в Windows

Предупреждение:

Перед добавлением узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

1. В панели инструментов Central Configuration Manager (CCM) выберите команду **Добавить узел**.
2. В окне «Мастер добавления узлов» введите имя узла и номер порта для нового агента Server Intelligence (SIA).
3. Укажите, требуется ли создавать серверы в новом узле.
 - **Добавить узел без серверов**
 - **Добавить узел с CMS**
 - **Добавить узел с серверами по умолчанию**

При выборе этого параметра создаются только серверы, установленные на этом компьютере. При этом не включаются все возможные серверы.

4. Выберите CMS.
 - Если развертывание работает, выберите пункт **Использование существующего выполняющегося CMS** и нажмите кнопку **Далее**.

При появлении соответствующего запроса введите имя хоста и порт существующей системы CMS, учетные данные администратора, имя источника данных, учетные данные для системной базы данных и ключ кластера.
 - Если развертывание остановлено, выберите пункт **Запуск нового временного CMS** и нажмите кнопку **Далее**.

При появлении соответствующего запроса введите имя хоста и порт временной системы CMS, учетные данные администратора, имя источника данных, учетные данные для системной базы данных и ключ кластера. Временная система CMS будет запущена. По завершении процесса система будет остановлена.

Предупреждение:

Не рекомендуется использовать развертывание при работающей временной системе CMS. Убедитесь, что существующая и временная системы CMS используют разные порты.

5. Ознакомьтесь со сведениями на странице подтверждения и нажмите кнопку **Готово**.

Диспетчер CCM создает узел. При возникновении любых ошибок см. сведения о них в файле журнала.

После этого можно запустить новый узел с помощью CCM.

Добавление узла в Windows с помощью скрипта

Предупреждение:

Перед добавлением узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

Для добавления узла на компьютер под управлением Windows можно использовать скрипт `AddNode.bat`. Для получения подробных сведений см. раздел «Параметры скрипта для добавления, восстановления и удаления узлов».

Пример:

В связи с ограничениями командной строки необходимо использовать управляющий символ (^) перед пробелами, знаками равенства (=) и точками с запятой (;) в строке `-connect`.

```
<SCRIPTDIR>\AddNode.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
```

Примечание:

Чтобы избежать использования символа крышки в длинных строках, можно записать имя скрипта и все его параметры во временный файл `response.bat` и затем выполнить этот файл `response.bat` без параметров.

См. также

- [Переменные](#)
- [Параметры скрипта для добавления, восстановления и удаления узлов](#)

8.1.13.2.3 Добавление узла в Unix

Предупреждение:

Перед добавлением узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

1. Выполните скрипт `<INSTALLDIR>/sap_bobj/serverconfig.sh`
2. Выберите пункт **1 – Add node** и нажмите клавишу **Enter**.
3. Введите имя нового узла и нажмите клавишу **Enter**.
4. Введите номер порта нового агента SIA и нажмите клавишу **Enter**.
5. Укажите, требуется ли создавать серверы в новом узле.
 - **no servers**

Создание узла, который не содержит серверов.

- **cms**

Создание CMS в узле без создания каких-либо других серверов.

- **серверы по умолчанию**

Создание только серверов, установленных на этом компьютере. При этом не включаются все возможные серверы.

6. Выберите CMS.

- Если развертывание работает, выберите **существующий** и нажмите клавишу **Enter**.

При появлении соответствующего запроса введите имя хоста и порт существующей системы CMS, учетные данные администратора, сведения о соединении с базой данных и учетные данные для системной базы данных, а также ключ кластера.

- Если развертывание остановлено, выберите **временный** и нажмите клавишу **Enter**.

При появлении соответствующего запроса введите имя хоста и порт временной системы CMS, учетные данные администратора, сведения о соединении с базой данных и учетные данные для системной базы данных, а также ключ кластера. Временная система CMS будет запущена. По завершении процесса система будет остановлена.

Предупреждение:

Не рекомендуется использовать развертывание при работающей временной системе CMS. Убедитесь, что существующая и временная системы CMS используют разные порты.

7. Ознакомьтесь со сведениями на странице подтверждения и нажмите клавишу **Enter**.

Диспетчер CCM создает узел. При возникновении любых ошибок см. сведения о них в файле журнала.

После этого можно выполнить команду `<INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>` для запуска нового узла.

Добавление узла в Unix с помощью скрипта

Предупреждение:

Перед добавлением узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

Для добавления узла на компьютер под управлением Unix можно использовать скрипт `addnode.sh`. Подробнее см. раздел «Параметры скрипта для добавления, восстановления и удаления узлов».

Пример:

```
<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
```


См. также

- [Переменные](#)
- [Параметры скрипта для добавления, восстановления и удаления узлов](#)

8.1.13.3 Восстановление узла

Можно восстановить узел с помощью Central Configuration Manager (CCM) или скрипта управления узлами после восстановления конфигурации серверов для всего кластера, а также в случае сбоя, повреждения компьютера, на котором размещается развертывание, или повреждения файловой системы этого компьютера. Придерживайтесь следующих рекомендаций:

- Восстанавливать узел не требуется в случае переустановки развертывания на заменяющем компьютере с идентичными параметрами установки и таким же именем узла. Узел автоматически восстанавливается программой установки.
- Узел можно восстанавливать только на компьютере с существующим развертыванием с идентичными параметрами установки и уровнем обновления.
- Следует восстанавливать только узлы, которые не существуют на физических компьютерах в развертывании. Убедитесь в том, что этот узел не размещен на других компьютерах.
- Несмотря на то, что в развертывании допускается работа узлов под управлением различных операционных систем, следует восстанавливать узлы только на компьютерах, использующих такую же операционную систему.
- Если используется брандмауэр, убедитесь, что порты Server Intelligence Agent (SIA) и Центрального сервера управления (CMS) открыты.

Помните:

Восстановление узла возможно только на том компьютере, на котором он расположен.

См. также

- [Восстановление системы](#)

8.1.13.3.1 Восстановление узла в Windows

1. В панели инструментов Central Configuration Manager (CCM) выберите команду **Добавить узел**.
2. В окне «Мастер добавления узлов» введите имя узла и номер порта для восстановленного Server Intelligence Agent (SIA).

Примечание:

Имена исходного и восстановленного узлов должны совпадать.

3. Выберите команду **Повторно создать узел** и нажмите кнопку **Далее**.
 - Если узел существует в системной базе данных Central Management Server (CMS), он восстанавливается на локальном хосте.

Предупреждение:

Этот параметр следует использовать только в том случае, если узел не существует ни на одном хосте в кластере.

- Если узел не существует в системной базе данных CMS, добавляется новый узел с серверами по умолчанию. В набор серверов по умолчанию включаются все серверы, установленные на хосте.

4. Выберите CMS.

- Если система CMS работает, выберите пункт **Использование существующего выполняющегося CMS** и нажмите кнопку **Далее**.

При появлении соответствующего запроса введите имя хоста и порт существующей системы CMS, учетные данные администратора, имя источника данных, учетные данные для системной базы данных и ключ кластера.

- Если система CMS остановлена, выберите пункт **Запуск нового временного CMS** и нажмите кнопку **Далее**.

При появлении соответствующего запроса введите имя хоста и порт временной системы CMS, учетные данные администратора, имя источника данных, учетные данные для системной базы данных и ключ кластера. Временная система CMS будет запущена. По завершении процесса система будет остановлена.

Предупреждение:

Не рекомендуется использовать развертывание при работающей временной системе CMS. Убедитесь, что существующая и временная системы CMS используют разные порты.

5. Ознакомьтесь со сведениями на странице подтверждения и нажмите кнопку **Готово.**

CCM восстанавливает узел и добавляет сведения о нем на локальный компьютер. При возникновении любых ошибок см. сведения о них в файле журнала.

После этого можно запустить восстановленный узел с помощью CCM.

Восстановление узла в Windows с помощью скрипта

Для восстановления узла на компьютере под управлением Windows можно использовать скрипт `AddNode.bat`. Для получения подробных сведений см. раздел «Параметры скрипта для добавления, восстановления и удаления узлов».

Пример:

В связи с ограничениями командной строки необходимо использовать управляющий символ крышки (^) перед пробелами, знаками равенства (=) и точками с запятой (;) в строке `-connect`.

```
<SCRIPTDIR>\AddNode.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
```

Примечание:

Чтобы избежать использования символа крышки в длинных строках, можно записать имя скрипта и все его параметры во временный файл `response.bat` и затем выполнить этот файл `response.bat` без параметров.

См. также

- [Переменные](#)
- [Параметры скрипта для добавления, восстановления и удаления узлов](#)

8.1.13.3.2 Восстановление узла в Unix

1. Выполните скрипт `<INSTALLDIR>/sap_bobj/serverconfig.sh`
2. Выберите пункт **1 – Добавить узел** и нажмите клавишу **Enter**.
3. Введите имя нового узла и нажмите клавишу **Enter**.

Примечание:

Имена исходного и восстановленного узлов должны совпадать.

4. Введите номер порта нового агента SIA и нажмите клавишу **Enter**.
5. Выберите пункт **повторно создать узел** и нажмите клавишу **Enter**.
 - Если узел существует в системной базе данных Central Management Server (CMS), он восстанавливается на локальном хосте.

Предупреждение:

Этот параметр следует использовать только в том случае, если узел не существует ни на одном хосте в кластере.

- Если узел не существует в системной базе данных CMS, добавляется новый узел с серверами по умолчанию. В набор серверов по умолчанию включаются все серверы, установленные на хосте.
6. Выберите CMS.
 - Если развертывание работает, выберите **существующий** и нажмите клавишу **Enter**.

При появлении соответствующего запроса введите имя хоста и порт существующей системы CMS, учетные данные администратора, сведения о соединении с базой данных и учетные данные для системной базы данных, а также ключ кластера.
 - Если развертывание остановлено, выберите **временный** и нажмите клавишу **Enter**.

При появлении соответствующего запроса введите имя хоста и порт временной системы CMS, учетные данные администратора, сведения о соединении с базой данных и учетные данные для системной базы данных, а также ключ кластера. Временная система CMS будет запущена. По завершении процесса система будет остановлена.

Предупреждение:

Не рекомендуется использовать развертывание при работающей временной системе CMS. Убедитесь, что существующая и временная системы CMS используют разные порты.

7. Ознакомьтесь со сведениями на странице подтверждения и нажмите клавишу **Enter**.

CCM восстанавливает узел и добавляет сведения о нем на локальный компьютер. При возникновении любых ошибок см. сведения о них в файле журнала.

После этого можно выполнить команду `<INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>` для запуска восстановленного узла.

Восстановление узла в Unix с помощью скрипта

Для восстановления узла на компьютере под управлением Unix можно использовать скрипт `addnode.sh`. Подробнее см. раздел «Параметры скрипта для добавления, восстановления и удаления узлов».

Пример:

```
<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=database;PORT=3306"
-dbkey abc1234
-adopt
```

См. также

- [Переменные](#)
- [Параметры скрипта для добавления, восстановления и удаления узлов](#)

8.1.13.4 Удаление узла

Для удаления остановленного узла можно использовать Central Configuration Manager (CCM) или скрипт управления узлами. Придерживайтесь следующих рекомендаций:

- При удалении узла также безвозвратно удаляются серверы этого узла.
- Если кластер содержит несколько компьютеров, узлы следует удалять перед удалением компьютера из кластера и удалением с него программного обеспечения. Если компьютер удаляется из кластера до удаления узла, а также в случае сбоя файловой системы на компьютере, необходимо восстановить узел на другом компьютере с теми же серверами и в том же кластере, после чего удалить узел.

Помните:

Удаление узла возможно только на том компьютере, на котором он расположен.

См. также

- [Восстановление узла](#)

8.1.13.4.1 Удаление узла в Windows

Предупреждение:

Перед удалением узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

1. Запустите Central Configuration Manager (CCM).
2. В диспетчере CCM остановите узел, который требуется удалить.
3. Выберите узел и затем выберите команду **Удалить узел** на панели инструментов.
4. При появлении соответствующего запроса введите имя хоста, порт, учетные данные администратора системы CMS и ключ кластера.

Диспетчер CCM удаляет узел и все присутствующие в нем серверы.

Удаление узла в Windows с помощью скрипта

Предупреждение:

Перед удалением узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

Для удаления узла на компьютере под управлением Windows можно использовать скрипт `RemoveNode.bat`. Подробнее см. раздел «Параметры скрипта для добавления, восстановления и удаления узлов».

Пример:

```
<SCRIPTDIR>\RemoveNode.bat -name mynode2
-cms mycms:6400
-username Administrator
-password Password1
```

См. также

- [Переменные](#)
- [Параметры скрипта для добавления, восстановления и удаления узлов](#)

8.1.13.4.2 Удаление узла в Unix

Предупреждение:

Перед удалением узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

1. Выполните команду `<INSTALLDIR>/sap_bobj/ccm.sh -stop <nodeName>`, чтобы остановить узел, который требуется удалить.

2. Выполните скрипт `<INSTALLDIR>/sap_bobj/serverconfig.sh`
3. Выберите пункт **2 – Удалить узел** и нажмите клавишу **Enter**.
4. Выберите узел, который требуется удалить, и нажмите клавишу **Enter**.
5. При появлении соответствующего запроса введите имя хоста, порт, учетные данные администратора системы CMS и ключ кластера.

Узел и все присутствующие в нем серверы удаляются.

Удаление узла в Unix с помощью скрипта

Предупреждение:

Перед удалением узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

Для удаления узла на компьютере под управлением Unix можно использовать скрипт `removenode.sh`. Для получения подробных сведений см. раздел «Параметры скрипта для добавления, восстановления и удаления узлов».

Пример:

```
<SCRIPTDIR>\RemoveNode.sh -name mynode2  
-cms mycms:6400  
-username Administrator  
-password Password1
```

См. также

- [Переменные](#)
- [Параметры скрипта для добавления, восстановления и удаления узлов](#)

8.1.13.5 Переименование узла

Можно переименовать узел с помощью Central Configuration Manager (CCM). Чтобы переименовать узел, необходимо создать новый узел с нужным именем, клонировать серверы исходного узла на новый узел, а затем удалить исходный узел. Придерживайтесь следующих рекомендаций:

- При переименовании компьютера, на котором располагается узел, не требуется переименовывать сам узел. Можно использовать существующее имя узла.
- Если используется брандмауэр, убедитесь, что порты Server Intelligence Agent (SIA) и центрального сервера управления (CMS) открыты.

Помните:

Переименование узла возможно только на том компьютере, на котором он расположен.

См. также

- [Добавление нового узла](#)

- [Клонирование серверов](#)
- [Удаление узла](#)

8.1.13.5.1 Переименование узла в Windows

Предупреждение:

Перед переименованием узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

1. Запустите Central Configuration Manager (CCM).
2. В панели инструментов Central Configuration Manager (CCM) выберите команду **Добавить узел**.
3. В окне «Мастер добавления узлов» введите имя узла и номера порта для нового Server Intelligence Agent (SIA), учетные данные администратора, сведения о соединении с базой данных, учетные данные для системной базы данных и ключ кластера.
4. Выберите команду **Добавить узел без серверов**.
5. После создания узла на странице «Управление серверами» консоли Central Management Console выполните клонирование всех серверов исходного узла в новый узел.

Примечание:

Убедитесь, что при клонировании серверов не возникает конфликтов портов с серверами на старом узле.

6. Запустите новый узел в диспетчере CCM.
7. После того как новый узел выполняется в течение пяти минут, удалите исходный узел с помощью CCM.

См. также

- [Добавление нового узла](#)
- [Клонирование серверов](#)
- [Удаление узла](#)

8.1.13.5.2 Переименование узла в Unix

Предупреждение:

Перед переименованием узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

1. Выполните скрипт `<INSTALLDIR>/sap_bobj/serverconfig.sh`.
2. Выберите пункт **1 – Add node** и нажмите клавишу **Enter**.
3. Введите имя нового узла и нажмите клавишу **Enter**.
4. Введите номер порта нового агента SIA и нажмите клавишу **Enter**.
5. При появлении соответствующего запроса введите учетные данные администратора, сведения о соединении с базой данных, учетные данные для системной базы данных и ключ кластера.
6. Выберите пункт **без серверов** и нажмите клавишу **Enter**.

- После создания узла на странице «Управление серверами» консоли Central Management Console выполните клонирование всех серверов исходного узла в новый узел.

Примечание:

Убедитесь, что при клонировании серверов не возникает конфликтов портов с серверами на старом узле.

- Выполните команду `<INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>` для запуска нового узла.
- После того как новый узел проработает пять минут, удалите старый узел с помощью скрипта `serverconfig.sh`.

См. также

- [Добавление нового узла](#)
- [Клонирование серверов](#)
- [Удаление узла](#)

8.1.13.6 Перемещение узла

Можно переместить остановленный узел из одного кластера в другой с помощью Central Configuration Manager (CCM) или скрипта управления узлами. Придерживайтесь следующих рекомендаций:

- Убедитесь, что в целевом кластере отсутствует узел с таким же именем.
- Удостоверьтесь, что сервера всех типов, установленных на компьютере с исходным узлом, также установлены в производственном кластере.
- Чтобы добавить новый компьютер в рабочий кластер и запретить его использование до тех пор, пока не будет завершено тестирование, установите платформу BI на автономный компьютер, протестируйте компьютер, а затем переместите узел в рабочий кластер.

Помните:

Перемещение узла возможно только на том компьютере, на котором он расположен.

8.1.13.6.1 Перемещение существующего узла в Windows

В этом примере узел, который требуется переместить, установлен в целевой системе. Компьютер изначально не входит в состав кластера, однако его требуется добавить в целевой кластер.

Предупреждение:

Перед перемещением узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

- Остановите узел в Central Configuration Manager (CCM).
- Щелкните узел правой кнопкой мыши и выберите команду **Переместить**.

3. При появлении соответствующего запроса выберите имя источника данных и введите имя хоста, порт, сведения о соединении с базой данных, учетные данные администратора целевой системы CMS и ключ кластера.

4. Выберите CMS.

- Если исходное развертывание работает, выберите пункт **Использование существующего выполняющегося CMS** и нажмите кнопку **Далее**.

При появлении соответствующего запроса введите имя хоста и порт исходной существующей системы CMS, учетные данные администратора, имя источника данных, учетные данные для базы данных исходной системы и ключ кластера.

- Если исходное развертывание остановлено, выберите пункт **Запуск нового временного CMS** и нажмите кнопку **Далее**.

При появлении соответствующего запроса введите имя хоста и порт исходной временной системы CMS, учетные данные администратора, имя источника данных, учетные данные для базы данных исходной системы и ключ кластера. Временная система CMS будет запущена. По завершении процесса система будет остановлена.

Предупреждение:

Не рекомендуется использовать развертывание при работающей временной системе CMS. Убедитесь, что существующая и временная системы CMS используют разные порты.

5. Ознакомьтесь со сведениями на странице подтверждения и нажмите кнопку **Готово**.

Диспетчер CCM создает новый узел в целевом кластере с тем же именем и теми же серверами, что и у узла в исходном кластере. Копия узла сохраняется на исходном кластере. Шаблоны конфигурации для серверов в узле не перемещаются. При возникновении любых ошибок см. сведения о них в файле журнала.

Предупреждение:

Не используйте исходный кластер после удаления узла.

6. Запустите перемещенный узел в диспетчере CCM.

Перемещение узла в Windows с помощью скрипта

Предупреждение:

Перед перемещением узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

Для перемещения узла на компьютере под управлением Windows можно использовать скрипт `MoveNode.bat`. Подробнее см. раздел «Параметры скрипта для перемещения узлов».

Пример:

В связи с ограничениями командной строки необходимо использовать управляющий символ крышки (^) перед пробелами, знаками равенства (=) и точками с запятой (;) в строке `-connect`.

```
<SCRIPTDIR>\MoveNode.bat -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
```

Примечание:

Чтобы избежать использования символа крышки в длинных строках, можно записать имя скрипта и все его параметры во временный файл `response.bat` и затем выполнить этот файл `response.bat` без параметров.

См. также

- [Переменные](#)
- [Параметры скриптов для перемещения узлов](#)

8.1.13.6.2 Перемещение существующего узла в Unix

В этом примере узел, который требуется переместить, установлен в целевой системе. Компьютер изначально входит в состав автономного кластера, однако его требуется добавить в целевой кластер.

Предупреждение:

Перед перемещением узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

1. Выполните команду `<INSTALLDIR>/sap_bobj/ccm.sh -stop <nodeName>`, чтобы остановить узел.
2. Выполните скрипт `<INSTALLDIR>/sap_bobj/serverconfig.sh`
3. Выберите пункт **4 – Переместить узел** и нажмите клавишу **Enter**.
4. Выберите узел, который требуется переместить, и нажмите клавишу **Enter**.
5. При появлении соответствующего запроса выберите сведения о соединении с системной базой данных, введите имя хоста, порт, учетные данные администратора целевой системы CMS и ключ кластера.
6. Выберите CMS.
 - Если исходное развертывание работает, выберите **существующий** и нажмите клавишу **Enter**.
 При появлении соответствующего запроса введите имя хоста и порт исходной существующей системы CMS, учетные данные администратора, сведения о соединении с базой данных и учетные данные для базы данных исходной системы, а также ключ кластера.
 - Если исходное развертывание остановлено, выберите **временный** и нажмите клавишу **Enter**.

При появлении соответствующего запроса введите имя хоста и порт исходной временной системы CMS, учетные данные администратора, сведения о соединении с базой данных и учетные данные для базы данных исходной системы, а также ключ кластера. Временная система CMS будет запущена. По завершении процесса система будет остановлена.

Предупреждение:

Не рекомендуется использовать развертывание при работающей временной системе CMS. Убедитесь, что существующая и временная системы CMS используют разные порты.

7. Ознакомьтесь со сведениями на странице подтверждения и нажмите клавишу **Enter**.

Диспетчер CCM создает новый узел в целевом кластере с тем же именем и теми же серверами, что и у узла в исходном кластере. Копия узла сохраняется на исходном кластере. Шаблоны конфигурации для серверов в узле не перемещаются. При возникновении любых ошибок см. сведения о них в файле журнала.

Предупреждение:

Не используйте исходный кластер после удаления узла.

8. Выполните команду `<INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>` для запуска перемещенного узла.

Перемещение узла в Unix с помощью скрипта

Предупреждение:

Перед перемещением узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

Для перемещения узла на компьютере под управлением Unix можно использовать скрипт `movenode.sh`. Для получения подробных сведений см. раздел «Параметры скрипта для перемещения узлов».

Пример:

```
<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
```

См. также

- [Переменные](#)
- [Параметры скриптов для перемещения узлов](#)

8.1.13.7 Параметры скриптов

8.1.13.7.1 Параметры скрипта для добавления, восстановления и удаления узлов

Параметр	Описание	Пример
-adopt	Восстанавливает узел, если он уже существует в CMS.	-adopt
-cms	Имя и номер порта Central Management Server (CMS) Предупреждение: Не используйте этот параметр, если используется <code>-usetempcms</code> Примечание: Необходимо указать номер порта, если CMS запущен не на порте по умолчанию 6400.	-cms mycms:6409
-cmsport	<ul style="list-style-type: none"> Порт CMS при создании временного CMS. Ограничение: Также необходимо использовать параметры <code>-usetempcms</code> , <code>-dbdriver</code> , <code>-connect</code> , и <code>-dbkey</code> . <ul style="list-style-type: none"> Порт CMS при создании нового CMS. Ограничение: Также необходимо использовать параметры <code>-dbdriver</code> , <code>-connect</code> , и <code>-dbkey</code> .	-cmsport 6401

Параметр	Описание	Пример
-connect	Строка подключения CMS или временной системной базы данных CMS. Примечание: Пропустите атрибуты HOSTNAME и PORT при подключении к базам данных DB2, Oracle, SQL Server или Sybase.	-connect "DSN=BusinessObjects CMS 10.1.1.1:3306;UID=sa;PWD=passwd;CSNAME=cn=sa;PORT=3306"
-dbdriver	Драйвер базы данных CMS. Допустимые значения: <ul style="list-style-type: none"> • db2databasesubsystem • maxdbdatabasesubsystem • mysqldatabasesubsystem • oracledatabasesubsystem • sqlserverdatabasesubsystem • sybasedatabasesubsystem 	-dbdriver mysqldatabasesubsystem
-dbkey	Ключ кластера.	-dbkey abc1234
-name	Имя узла	-name mynode2
-noservers	Создается узел без серверов. Примечание: Дополнительный параметр -createcms создает узел с CMS, но без остальных серверов. Пропустите эти параметры для создания узла с серверами по умолчанию.	-noservers
-password	Пароль учетной записи администратора.	-password Password1
-siaport	Номер порта Server Intelligence Agent для узла.	-siaport 6409
-username	Имя пользователя администраторской учетной записи.	-username Administrator

Параметр	Описание	Пример
-usetempcms	<p>Предупреждение: Не используйте этот параметр, если используется <code>-cms</code></p> <p>Запускает и использует временный CMS.</p> <p>Примечание: Используйте временный CMS, когда развертывание не запущено.</p>	-usetempcms

См. также

- [Добавление узла в Windows с помощью скрипта](#)
- [Добавление узла в Unix с помощью скрипта](#)
- [Восстановление узла в Windows с помощью скрипта](#)
- [Восстановление узла в Unix с помощью скрипта](#)
- [Удаление узла в Windows с помощью скрипта](#)
- [Удаление узла в Unix с помощью скрипта](#)

8.1.13.7.2 Параметры скриптов для перемещения узлов

Параметр	Описание	Пример
-cms	<p>Имя исходного центрального сервера управления (CMS).</p> <p>Предупреждение: Не используйте этот параметр, если используется <code>-usetempcms</code></p> <p>Примечание: Необходимо указать номер порта, если CMS запущен не на порте по умолчанию 6400.</p>	-cms sourceMachine:6409

Параметр	Описание	Пример
-cmsport	<ul style="list-style-type: none"> Порт CMS при создании временного CMS. <p>Ограничение: Также необходимо использовать параметры -usetempcms, -dbdriver, -connect, и -dbkey.</p> <ul style="list-style-type: none"> Порт CMS при создании нового CMS. <p>Ограничение: Также необходимо использовать параметры -dbdriver, -connect, и -dbkey.</p>	-cmsport 6401
-connect	<p>Строка подключения исходного CMS или временной системной базы данных CMS.</p> <p>Примечание: Пропустите атрибуты HOSTNAME и PORT при подключении к базам данных DB2, Oracle, SQL Server или Sybase.</p>	-connect "DSN=Source DB2, DSN=Source, DRIVER=IBM, PORT=3005, USER=SYSADM, PWD=SYSADM, HOSTNAME=127.0.0.1, PORT=3005"
-dbdriver	<p>Драйвер базы данных исходного CMS.</p> <p>Допустимые значения:</p> <ul style="list-style-type: none"> db2databasesubsystem maxdbdatabasesubsystem mysqldatabasesubsystem oracledatabasesubsystem sqlserverdatabasesubsystem sybasedatabasesubsystem 	-dbdriver mysqldatabasesubsystem
-dbkey	Исходный ключ кластера.	-dbkey abc1234
-destcms	<p>Имя CMS назначения.</p> <p>Примечание: Необходимо указать номер порта, если CMS запущен не на порте по умолчанию 6400.</p>	-destcms destinationMachine:6401

Параметр	Описание	Пример
-destconnect	<p>Строка подключения конечной системной базы данных CMS.</p> <p>Примечание: Пропустите атрибуты HOSTNAME и PORT при подключении к базам данных DB2, Oracle, SQL Server или Sybase.</p>	<p>-destconnect "DSN=Destin DB2 DSN=Destin ORACLE DSN=Destin SQLSERVER DSN=Destin SYBASE DSN=Destin PORT=300</p>
-destdbdriver	<p>Драйвер базы данных конечного CMS</p> <p>Допустимые значения:</p> <ul style="list-style-type: none"> • db2databasesubsystem • maxdbdatabasesubsystem • mysqldatabasesubsystem • oracledatabasesubsystem • sqlserverdatabasesubsystem • sybasedatabasesubsystem <p>Примечание: sqlserverdatabase не поддерживается на Unix.</p>	<p>-destdbdriver sybasedatabasesubsystem</p>
-destdbkey	Ключ кластера назначения.	-destdbkey def5678
-destpassword	Пароль учетной записи администратора в целевом CMS.	-destpassword Password2
-destusername	Имя пользователя учетной записи администратора на целевом CMS.	-destusername Administrator
-password	Пароль учетной записи администратора в исходном CMS.	-password Password1
-username	Имя пользователя учетной записи администратора на исходном CMS.	-username Administrator

Параметр	Описание	Пример
-usetempcms	<p>Предупреждение: Не используйте этот параметр, если используется <code>-cms</code></p> <p>Запускает и использует временный CMS.</p> <p>Примечание: Используйте временный CMS, когда развертывание не запущено.</p>	-usetempcms

См. также

- [Перемещение узла в Windows с помощью скрипта](#)
- [Перемещение узла в Unix с помощью скрипта](#)

8.1.13.8 Добавление зависимостей сервера Windows

В среде Windows каждый экземпляр Server Intelligence Agent (SIA) зависит от служб журнала событий и вызова удаленной процедуры (RPC).

При возникновении ошибок в работе агента SIA убедитесь, что обе эти службы отображаются на вкладке «Зависимость» агента SIA.

8.1.13.8.1 Добавление зависимостей сервера Windows

1. Откройте Central Configuration Manager (CCM) и остановите Server Intelligence (SIA).
2. Щелкните SIA правой кнопкой мыши и выберите команду **Свойства**.
3. Выберите вкладку **Зависимость**.
4. Нажмите кнопку **Добавить**.
Открывается диалоговое окно «Добавление зависимости», в котором отображается список всех доступных зависимостей.
5. Выберите зависимость и нажмите кнопку **Добавить**.
6. Нажмите кнопку **ОК**.
7. С помощью диспетчера CCM перезапустите агент SIA.

8.1.13.9 Изменение учетных данных пользователя для узла

С помощью Central Configuration Manager (CCM) можно установить или обновить учетные данные пользователя для агента Server Intelligence (SIA) при изменении пароля операционной системы, а также в тех случаях, когда требуется запускать все серверы в узле под разными учетными записями.

Все серверы, управляемые агентом SIA, запускаются под одной учетной записью. Чтобы запустить сервер с использованием несистемной учетной записи, убедитесь, что эта учетная запись входит в группу "Локальные администраторы" на сервере, и ей назначено право «Замена маркера уровня процесса».

Ограничение:

На компьютере под управлением Unix запуск платформы BI должен осуществляться с использованием той же учетной записи, под которой эта система была установлена. Чтобы использовать другую учетную запись, следует переустановить развертывание под необходимой записью.

8.1.13.9.1 Изменение учетных данных пользователя для узла в Windows

1. Откройте Central Configuration Manager (CCM) и остановите агент Server Intelligence (SIA).
2. Щелкните SIA правой кнопкой мыши и выберите команду **Свойства**.
3. Очистите флажок **Системная учетная запись**.
4. Введите имя пользователя и пароль и нажмите кнопку **ОК**.
5. С помощью диспетчера CCM перезапустите агент SIA.

Агент SIA и сервер выполняют вход в систему локального компьютера с использованием новой учетной записи пользователя.

8.1.14 Переименование компьютера в развертывании платформы SAP BusinessObjects Business Intelligence

Имя компьютера в платформе SAP BusinessObjects Business Intelligence можно изменить в любое время, остановив все серверы платформы SAP BusinessObjects Business Intelligence, размещенные на этом компьютере, а затем переименовав компьютер. Если этот компьютер входит в кластер, останавливать все компьютеры и сервера в кластере не требуется; серверы можно переименовать в Central Management Console (CMC), когда другие компьютеры работают.

Если база данных системы CMS или база данных аудита размещены на компьютере, который переименуется, то после переименования потребуется обновить сведения о соединении с базой данных. Если для соединения с любой из этих баз данных используются соединения ODBC,

соединения потребуется обновить, указав новое имя компьютера. Для всех других соединений с базами данных необходимо выбрать существующую базу данных в Central Configuration Manager (CCM).

В случае переименования компьютера в разворачивании переименование узлов на этом компьютере не требуется.

См. также

- [Выбор новой или существующей базы данных центрального сервера управления](#)

8.1.15 Использование 32-битных и 64-битных библиотек сторонних разработчиков с платформой SAP BusinessObjects Business Intelligence

На серверах платформы SAP BusinessObjects Business Intelligence выполняются как 32-битные, так и 64-битные процессы. На некоторых серверах дополнительно запускаются 32-битные и 64-битные дочерние процессы. Чтобы использовать правильную версию сторонней библиотеки (32-битную или 64-битную) для процессов платформы SAP BusinessObjects Business Intelligence, необходимо задать отдельные переменные среды для каждой из версий на компьютере, где размещается платформа SAP BusinessObjects Business Intelligence. Затем требуется задать дополнительную переменную среды, которая содержит разделенный запятыми список переменных среды, которые имеют 32-битную и 64-битную версии. При запуске процесса платформы SAP BusinessObjects Business Intelligence будет выбрана переменная, соответствующая разрядности процесса.

- `<FIRST_ENV_VAR>`=значение, которое должно использоваться для 64-битных процессов платформы SAP BusinessObjects Business Intelligence.
- `<FIRST_ENV_VAR32>`=значение, которое должно использоваться для 32-битных процессов.
- `<SECOND_ENV_VAR>`=значение, которое должно использоваться для 64-битных процессов.
- `<SECOND_ENV_VAR32>`=значение, которое должно использоваться для 32-битных процессов.
- `BOE_USE_32BIT_ENV_FOR=<FIRST_ENV_VAR>,<SECOND_ENV_VAR>`

Например, если платформа SAP BusinessObjects Business Intelligence установлена на компьютере AIX с 32-битными и 64-битными клиентами Oracle, и требуется задать переменную LIBPATH, укажите следующие переменные:

- `ORACLE_HOME=<64-битная версия клиента Oracle>`
- `ORACLE_HOME32=<32-битная версия>`
- `LIBPATH=<64-битная версия>`
- `LIBPATH32=<32-битная версия>`
- `BOE_USE_32BIT_ENV_FOR=ORACLE_HOME,LIBPATH`

8.1.16 Управление заполнителями сервера и узла

8.1.16.1 Просмотр заполнителей для сервера

- В области управления «Серверы» консоли СМС щелкните сервер правой кнопкой мыши и выберите команду **Заполнители**.
Будет открыто диалоговое окно «Заполнители» со списком заполнителей для всех серверов в том же кластере, что и выбранный сервер. При необходимости изменения значения заполнителя измените заполнитель для узла.

См. также

- [Заполнители сервера и узлов](#)

8.1.16.2 Просмотр и изменение заполнителей для узла

1. В области управления «Серверы» Central Management Console щелкните правой кнопкой мыши узел, для которого необходимо изменить заполнители, и выберите команду **Заполнители**.
2. Внесите требуемые изменения параметров заполнителей и нажмите кнопку **ОК** для продолжения.

См. также

- [Заполнители сервера и узлов](#)

Управление базами данных центрального сервера управления (CMS)

9.1 Управление подключением к системной базе данных центрального сервера управления

Если системная база данных центрального сервера управления недоступна (например, по причине аппаратного или программного сбоя либо проблемы в сети), то центральный сервер управления переходит в состояние «Ожидание ресурсов». Если в разворачивании платформы SAP BusinessObjects Business Intelligence используется несколько Центральных серверов управления, последующие запросы с других серверов перенаправляются на любой Центральный сервер управления в кластере, имеющий активное подключение к системной базе данных. Пока CMS находится в состоянии «Ожидание ресурсов», любой текущий запрос, не требующий доступа к базе данных, продолжает успешно обрабатываться, однако при обработке запросов, требующих обращения к базе данных центрального сервера управления, происходит сбой.

По умолчанию центральный сервер управления в состоянии «Ожидание ресурсов» периодически выполняет определенное количество попыток подключения в соответствии с настройками свойства «Запросы соединений с системной БД». Сразу после установления по меньшей мере одного подключения к базе данных, в центральном сервере управления выполняется синхронизация всех необходимых данных, после чего он переключается в состояние «Выполнение» и возобновляет обычные операции.

В некоторых случаях может потребоваться запретить центральному серверу управления автоматически восстанавливать подключение к базе данных. Например, это может быть необходимо в случае проверки целостности базы данных перед восстановлением подключения к ней. Для этого на странице «Свойства» центрального сервера управления снимите флажок с параметра **Автоматическое повторное подключение к базе данных системы**.

См. также

- [Для изменения свойств сервера](#)

9.2 Выбор новой или существующей базы данных центрального сервера управления

Можно использовать CCM для указания новой или существующей базы данных центрального сервера управления для узла. Обычно существует только несколько случаев, в которых требуется выполнить эти шаги:

- Если изменить пароль для текущей базы данных центрального сервера управления, эти шаги позволят вам отключиться и переподключиться к текущей базе данных. При запросе системы нужно будет ввести новый пароль для центрального сервера управления.
- Если вы хотите выбрать и инициализировать пустую базу данных для платформы SAP BusinessObjects Business Intelligence, эти шаги позволят выбрать этот новый источник данных.
- Если восстановить базу данных центрального сервера управления из резервной копии (используя стандартные инструменты администрирования и обработки баз данных), а соединение перестало работать, вам потребуется переподключить центральный сервер управления к восстановленной базе данных. (Это может случиться, например, при восстановлении исходной базы данных центрального сервера управления на недавно установленном сервере баз данных).

9.2.1 Выбор новой или существующей базы данных CMS в Windows

1. Используйте консоль CCM для остановки агента Server Intelligence Agent (SIA).
2. Выберите SIA и нажмите кнопку **Указать источник базы данных системы CMS** на панели инструментов.
3. На вкладке **Конфигурация** диалогового окна «Свойства», в разделе **Источник данных CMS**, нажмите кнопку **Указать**.
4. Следующие шаги зависят от типа выбранного соединения:
 - Если вы выбрали ODBC, появится диалоговое окно Windows "Выберите источник данных". Выберите ODBC-источник, который требуется использовать в качестве базы данных CMS, а затем нажмите кнопку "ОК". (Для настройки нового DSN нажмите "Новый"). Система пригласит вас ввести учетные данные, после чего необходимо нажать "ОК".
 - Если вы выбрали собственный драйвер, необходимо будет ввести имя сервера базы данных, ваши логин и пароль. Введите эту информацию и нажмите "ОК".

CCM уведомит вас, когда установка базы данных CMS будет завершена.

5. В диалоговом окне «Свойства» нажмите кнопку **ОК**.
6. Перезапустите агент Server Intelligence Agent.

9.2.2 Выбор новой или существующей базы данных центрального сервера управления в UNIX

Используйте скрипт `cmsdbsetup.sh`. Для получения информации обратитесь к главе "Инструменты UNIX".

1. Выполните скрипт `cmsdbsetup.sh` (по умолчанию расположен по адресу `<INSTALLDIR>/sap_bobj/`).
2. Выберите действие обновления (опция 6).
3. Когда система пригласит вас, введите тип новой базы данных центрального сервера управления.
4. Введите информацию о базе данных (например, имя хоста, имя пользователя и пароль). Сообщение с уведомлением появляется, когда база данных центрального сервера управления назначена новому каталогу.
5. Если появляется приглашение восстановить Server Intelligence (SIA), укажите пароль администратора и необходимы номер порта, через который будет устанавливаться связь центральный сервер управления.

Примечание:

Это приглашение появится, только если назначение выполняется в пустой базе данных центрального сервера управления.

9.3 Повторное создание базы данных системы центрального сервера управления

В этой процедуре описаны способы восстановления (повторной инициализации) текущей системной базы данных центрального сервера управления. При выполнении этой задачи уничтожаются все данные, содержащиеся в базе данных. Эта процедура полезна, например, если платформа SAP BusinessObjects Business Intelligence установлена в среде разработки для создания и тестирования пользовательских настраиваемых веб-приложений. Повторную инициализацию системной базы данных центрального сервера управления в среде разработки можно выполнять каждый раз, когда необходимо удалить из системы все данные.

Предупреждение:

Выполняя инструкции данного раздела, можно удалить из базы данных центрального сервера управления все данные, а также объекты, например отчеты и пользователей. Не выполняйте данные действия по отношению к производственному развертыванию.

Очень важно выполнять резервное копирование всех параметров конфигурации сервера перед повторной инициализацией системной базы данных центрального сервера управления. При восстановлении базы данных параметры конфигурации сервера удаляются, поэтому необходимо иметь резервную копию для восстановления этой информации.

При восстановлении системной базы данных существующие ключи лицензий следует сохранять в базе данных. Однако, если необходимо повторно ввести лицензионные ключи, следует войти в консоль CMS под учетной записью администратора по умолчанию. Перейдите в область управления "Авторизация" и введите информацию на вкладке "Ключи лицензий".

Примечание:

При повторной инициализации системной базы данных центрального сервера управления все данные в текущей системной базе данных центрального сервера управления будут уничтожены. Перед началом операции рассмотрите возможность создания резервных копий текущей базы данных. При необходимости обратитесь к администратору базы данных.

См. также

- [Резервное копирование настроек сервера](#)

9.3.1 Восстановление системной базы данных CMS в ОС Windows

1. Используйте консоль CCM для остановки Server Intelligence Agent (SIA).

Примечание:

Для выполнения этой процедуры нельзя запускать CCM на удаленном компьютере; она должна быть запущена на компьютере, в котором есть хотя бы один действительный узел.

2. Щелкните правой кнопкой мыши SIA и выберите команду **Свойства**.
3. В диалоговом окне **Свойства** откройте вкладку «Конфигурация» и нажмите кнопку **Задать**.
4. В диалоговом окне **Настройка базы данных CMS** щелкните **Повторно создать текущий источник данных**.

Примечание:

Все серверы и объекты на компьютере, на котором запущена консоль CCM на шаге 1, будут также восстановлены.

5. Нажмите кнопку **ОК** и при появлении запроса на подтверждения нажмите кнопку **Да**.
6. Укажите пароль для базы данных системы CMS, а затем нажмите кнопку **ОК**.
На консоли CCM появляется уведомление по завершении установки системной базы данных CMS.
7. Нажмите кнопку **ОК**.
Выполняется обратный переход на консоль CCM.
8. Перезапустите агент Server Intelligence Agent и включите службы.
При запуске агент Server Intelligence Agent запускает сервер CMS. Сервер CMS записывает запрошенные системные данные в новый пустой источник данных.
9. Если в Вашем развертывании несколько компьютеров, необходимо повторно создать узлы на других компьютерах.

9.3.2 Восстановление системной базы данных CMS в ОС UNIX

Используйте скрипт `cmsdbsetup.sh`. Для получения сведений см. главу "Инструменты UNIX" в *Руководстве администратора платформы SAP BusinessObjects Business Intelligence*.

1. Выполните файл `cmsdbsetup.sh` (по умолчанию он расположен в каталоге `<INSTALLDIR>/sap_bobj/`).
2. Выберите параметр "reinitialize" (параметр 5), затем подтвердите выбор.
Скрипт `cmsdbsetup.sh` начинает воссоздание базы данных системы CMS.
3. Укажите пароль системной базы данных CMS.
4. По завершении создания базы данных выйдите из скрипта `cmsdbsetup.sh`.
5. Введите информацию о базе данных (например, имя хоста, имя пользователя и пароль).
Сообщение с уведомлением появляется, когда база данных центрального сервера управления назначена новому каталогу.
6. Если появляется приглашение восстановить Server Intelligence (SIA), укажите пароль администратора и необходимы номер порта, через который будет устанавливаться связь сервер CMS.

Примечание:

Это приглашение появится, только если назначение выполняется в пустой базе данных центрального сервера управления.

7. Выполните в каталоге `<INSTALLDIR>/sap_bobj/` следующую команду, чтобы запустить узел.

```
ccm.sh -start <nodename>
```

8. Для включения служб используйте следующую команду:

```
ccm.sh -enable all -cms <CMSNAME:PORT> -username administrator -password <password>
```

Примечание:

Поскольку база данных CMS только что восстановлена, пароль администратора не задан.

9.4 Копирование данных из одной базы данных CMS в другую.

Для копирования данных системы с одного сервера базы данных на другой можно использовать Central Configuration Manager (CCM). Например, если базу данных необходимо заменить на другую, так как проводится обновление базы данных или переход с одного типа базы данных на другой, перед прекращением использования существующей базы данных можно скопировать все ее содержимое в новую базу данных.

База данных адресата инициализируется до переноса в нее новых данных, поэтому ее содержимое будет временно удалено (все таблицы платформы BI будут временно удалены, а затем пересозданы). После завершения копирования данных целевая база данных устанавливается в качестве текущей базы данных для CMS.

Примечание:

Если требуется выполнить импорт пользователей, групп, папок и отчетов из предыдущей версии платформы BI в текущую версию, следует использовать средство управления обновлениями. Для получения дополнительных сведений см. *Руководство по обновлению платформы SAP BusinessObjects Business Intelligence*.

9.4.1 Подготовка к копированию системной базы данных CMS

Перед копированием системной базы данных CMS переведите исходную среду и среду назначения в автономный режим, выключив и остановив все серверы. Создайте резервные копии обеих баз данных CMS и резервные копии корневых каталогов, используемых всеми Серверами репозитория входных и выходных файлов. При необходимости обратитесь к вашему администратору баз данных или сетевому администратору.

Убедитесь, что у вас есть учетная запись пользователя базы данных, которая имеет разрешение на чтение всех данных в исходной базе данных, а также учетная запись пользователя базы данных, которая имеет права на Создание, Удаление и Обновление по отношению к базе данных адресата. Также убедитесь, что вы можете подключиться к обеим базам данных – посредством программного обеспечения клиента базы данных или посредством ODBC, в соответствии с настройками – с машины CMS, чью базу данных вы заменяете.

Если вы копируете базу данных CMS из текущего местоположения на другой сервер базы данных, текущая база данных CMS является исходной средой. Ее содержимое копируется в базу данных назначения, которая потом становится активной базой данных для текущего CMS. Выполнение этой процедуры позволяет переместить базу данных CMS по умолчанию из существующей локальной базы данных на выделенный сервер баз данных, такой как Microsoft SQL Server, Informix, Oracle, DB2 или Sybase. Через учетную запись администратора войдите в систему машины, на которой выполняется CMS, чью базу данных вы хотите переместить.

Примечание:

- При копировании данных из одной базы данных в другую целевую базу данных инициализируется перед копированием в нее новых данных. Это означает, что если целевая база данных не содержит системных таблиц платформы SAP BusinessObjects Business Intelligence, то эти таблицы будут созданы. Если системные таблицы платформы SAP BusinessObjects Business Intelligence содержатся в целевой базе данных, эти таблицы будут удалены навсегда, будут созданы новые системные таблицы, и данные из исходной базы данных будут скопированы в новые таблицы. Остальные таблицы в базе данных не изменяются.
- При копировании базы данных системы CMS в целевую базу данных в Windows необходимо убедиться, что путь к клиенту MaxDB включен в переменную среды *PATH*. Например,
`;C:\Program Files\sdb\MAXDB1\pgm.`

9.4.2 Копирование системной базы данных CMS в Windows

Перед копированием содержимого базы данных центрального сервера управления проверьте возможность входа в базу данных с учетной записью, у которой есть разрешение на добавление и удаление таблиц, а также на добавление, удаление и изменение данных в этих таблицах.

1. Откройте Диспетчер центральной конфигурации (CCM) и остановите агент Server Intelligence (SIA).
2. Щелкните правой кнопкой мыши SIA и выберите команду **Свойства**.
3. Перейдите на вкладку **Конфигурация** и нажмите кнопку **Указать**.
4. Выберите **Копировать** и нажмите кнопку **ОК**.
5. Выберите тип базы данных для источника данных CMS, а затем укажите информацию об этой базе данных (включая имя хоста, имя пользователя и пароль).
6. Выберите тип для целевой базы данных CMS, а затем укажите информацию об этой базе данных (включая имя хоста, имя пользователя и пароль).
7. По окончании копирования базы данных CMS нажмите кнопку **ОК**.

9.4.3 Для копирования данных из базы данных системы центрального сервера управления на UNIX

Перед копированием содержимого базы данных центрального сервера управления проверьте возможность входа в целевую базу данных с учетной записью, у которой есть разрешение на добавление и удаление таблиц, а также на добавление, удаление и изменение данных в этих таблицах.

Примечание:

В UNIX нельзя напрямую выполнять перенос из среды-источника, использующей соединение ODBC, в базу данных центрального сервера управления. Если база исходная база данных центрального сервера управления использует ODBC, необходимо сначала обновить эту систему до поддерживаемого подходящего драйвера.

1. Остановите центральный сервер управления, введя следующую команду:
`./ccm.sh -stop <nodename>`
2. Выполните файл `cmsdbsetup.sh` (по умолчанию расположен `<InstallDirectory>/sap_bobj/`).
3. Выберите параметр «копировать» (параметр 4) и подтвердите выбор.
4. Выберите тип базы данных для источника данных центрального сервера управления, а затем укажите информацию об этой базе данных (включая имя хоста, имя пользователя и пароль).
5. Выберите тип для целевой базы данных центрального сервера управления, а затем укажите информацию об этой базе данных (включая имя хоста, имя пользователя и пароль).

База данных центрального сервера управления будет скопирована в целевую базу данных.
По завершении копирования на экране появится сообщение.

Управление серверами контейнера веб-приложений (WACS)

10.1 WACS

10.1.1 Сервер контейнера веб-приложений (WACS)

Сервер контейнера веб-приложений (WACS) предоставляет платформу для размещения веб-приложений платформы BI. Например, Central Management Console (CMC) может размещаться на сервере WACS.

WACS упрощает систему администрирования путем упразднения нескольких рабочих потоков, которые ранее требовались для настройки серверов приложений и развертывания веб-приложений, а также путем предоставления упрощенного, согласованного административного интерфейса.

Развертывание веб-приложений на WACS выполняется автоматически. WACS не поддерживает ручное или с использованием WDeploy развертывание платформы BI или внешних веб-приложений.

10.1.1.1 Требуется ли WACS?

Если не нужно использовать сервер Java-приложений для размещения веб-приложений SAP BusinessObjects, то можно использовать для этого WACS.

Если планируется использование поддерживаемого сервера Java-приложений для развертывания веб-приложений платформы SAP BusinessObjects Business Intelligence или если установка платформы SAP BusinessObjects Business Intelligence выполняется в системе UNIX, установка и использование WACS не требуется.

10.1.1.2 Какие преимущества дает использование WACS?

При использовании WACS для размещения СМС вы получаете ряд преимуществ:

- Установка, обслуживание и конфигурация WACS требует минимальных усилий.
- Все размещаемые приложения предварительно развертываются на WACS, поэтому выполнять дополнительные действия вручную не требуется.
- WACS поддерживается SAP.
- Благодаря WACS не требуются особые навыки администрирования и обслуживания Java-серверов приложений.
- WACS предоставляет интерфейс администрирования, согласованный с другими серверами платформы SAP BusinessObjects Business Intelligence.

10.1.1.3 Общие задачи

Задача	Описание	Раздел
Как можно улучшить производительность веб-приложений или веб-служб, размещенных на WACS	Установив WACS на несколько компьютеров, можно улучшить производительность веб-приложений или веб-служб.	<ul style="list-style-type: none"> • Добавление дополнительных серверов WACS в систему и их удаление • Клонирование сервера контейнера веб-приложений
Как повысить доступность моего веб-яруса?	Создайте дополнительные WACS в своем развертывании, чтобы в случае сбоя аппаратного или программного обеспечения на одном сервере другой сервер мог продолжить обработку запросов.	Добавление дополнительных серверов WACS в систему и их удаление
Как создать среду, в которой можно легко устранить последствия неверной настройки СМС?	Создайте второй, резервный WACS, и используйте его для задания шаблона конфигурации. В случае сбоя конфигурации основного WACS используйте второй WACS, пока вы не настроите первый сервер, или примените к первому серверу шаблон конфигурации.	Добавление дополнительных серверов WACS в систему и их удаление
Как повысить безопасность связи между клиентами и WACS?	Настройте HTTPS на WACS.	<ul style="list-style-type: none"> • Настройка HTTPS/SSL • Использование WACS с брандмауэрами
Как повысить безопасность связи между WACS и другими серверами Business Objects в моем развертывании?	Настройте связь SSL между WACS и другими серверами платформы SAP BusinessObjects Business Intelligence в развертывании.	<ul style="list-style-type: none"> • Настройка серверов для SSL • Использование WACS с брандмауэрами
Можно ли использовать WACS с HTTPS и обратным прокси-сервером?	Использовать WACS с HTTPS и обратным прокси-сервером можно, если создать два WACS и настроить оба сервера с HTTPS. Используйте первый WACS для связи внутри своей внутренней сети, а другой WACS – для связи с внешней сетью через обратный прокси-сервер.	Настройка WACS для поддержки HTTPS с обратным прокси

Задача	Описание	Раздел
В какой IT-среде может быть развернут WACS?	WACS может быть развернут в IT-среде с веб-серверами, балансировщиками нагрузки аппаратного обеспечения, обратными прокси-серверами и межсетевыми экранами.	<ul style="list-style-type: none"> • Использование WACS с другими веб-серверами • Использование WACS с балансировщиком нагрузки • Использование WACS с обратным прокси • Использование WACS с брандмауэрами
Можно ли использовать WACS в развертывании с балансировщиком нагрузки?	Вы можете использовать WACS с развертыванием с балансировщиком нагрузки аппаратного обеспечения. Сам сервер WACS не может использоваться для балансировки нагрузки.	Использование WACS с балансировщиком нагрузки
Можно ли использовать WACS в развертывании с обратным прокси-сервером?	Вы можете использовать WACS в развертывании с обратным прокси-сервером. Сам сервер WACS не может использоваться в качестве обратного прокси-сервера.	Использование WACS с обратным прокси
Как устранять неисправности на серверах WACS?	При необходимости определения причин низкой производительности серверов WACS можно просмотреть файлы журнала и параметры системы.	<ul style="list-style-type: none"> • Настройка трассировки на WACS • Для просмотра серверных показателей

Задача	Описание	Раздел
Я не получаю никаких обработанных для меня страниц на конкретном порту. В чем проблема?	<p>Имеются несколько причин, почему вы не можете подключиться к WACS. Убедитесь, что:</p> <ul style="list-style-type: none"> • Порты HTTP, HTTP через прокси и HTTPS, которые вы указали для WACS, не заняты другими приложениями. • У сервера WACS имеется достаточно памяти. • Сервер WACS разрешает достаточное количество параллельных запросов. • В случае необходимости восстановите для WACS системные параметры по умолчанию. 	<ul style="list-style-type: none"> • Разрешение конфликтов порта HTTP • Изменение параметров памяти • Изменение количества одновременных запросов • Восстановление настроек системы по умолчанию
Как настроить свойства веб-приложений, размещенных на WACS	Процедура настройки свойств веб-приложений зависит от конкретного свойства и веб-приложения. Для получения дополнительных сведений см. раздел «Настройка свойств веб-приложений» этой главы.	Настройка свойств веб-приложений
Где можно найти список свойств WACS?	В приложении «Свойства сервера» данного руководства содержится список свойств WACS.	Свойства основных служб

10.1.2 Добавление дополнительных серверов WACS в систему и их удаление

Добавление дополнительных серверов WACS в систему позволяет обеспечить ряд преимуществ:

- Ускорение восстановления в случае неправильной настройки сервера.
- Повышение отказоустойчивости серверов.
- Улучшение распределения нагрузки.
- Повышение общей производительности.

Существует три способа добавления серверов WACS в систему:

- Установка сервера WACS на компьютер.
- Создание сервера WACS.
- Клонирование сервера WACS.

Примечание:

Из-за высокого расхода ресурсов системы не рекомендуется одновременно запускать несколько WACS на одном компьютере. Однако вы можете установить несколько WACS на одном компьютере, и запускать только один из них, что поможет вам быстро восстановить работу системы в случае сбоя или неверной настройки одного из серверов.

10.1.2.1 Установка WACS

Установка WACS на отдельных компьютерах может повысить производительность и улучшить распределение нагрузки в развертывании, а также увеличить доступность сервера. Если в вашем развертывании содержится два или несколько серверов WACS на разных компьютерах, доступность веб-приложений и веб-служб не будет зависеть от аппаратных или программных сбоев на конкретной машине, так как другие серверы WACS по-прежнему будут предоставлять службы.

С помощью программы установки платформы BI можно установить сервер контейнера веб-приложений. Существует два способа установки WACS:

- При полной установке на экране «Выберите веб-приложение Java» выберите **Установить сервер контейнеров веб-приложений и автоматически развернуть на нем веб-приложения и службы**.

При выборе сервера Java-приложений в новой установке WACS не устанавливается.

- В пользовательской / расширенной установке существует возможность выбора установки WACS на экране «Выбор компонентов», развернув узлы **Серверы > Службы платформы** и выбрав **Сервер контейнера веб-приложений**.

При установке WACS программа установки автоматически создает сервер с именем `<NODE>.WebApplicationContainerServer`, где `<NODE>` – имя узла. Веб-приложения и веб-службы платформы BI будут развернуты на этом сервере. Вмешательство пользователя для развертывания или настройки СМС не требуется. Система готова к использованию

При установке WACS программа установки запрашивает номер порта HTTP для WACS. Убедитесь, что указанный номер порта еще не используется. По умолчанию используется номер порта 6405. Если предполагается разрешить пользователям подключаться к WACS с внешней стороны брандмауэра, необходимо, чтобы на брандмауэре был открыт порт HTTP сервера.

WACS поддерживается только операционными системами Windows.

Примечание:

Веб-приложения, которые находятся на сервере WACS, автоматически разворачиваются при установке WACS или при применении обновлений и исправлений к нему или к веб-приложениям, которые находятся на сервере WACS. Развертывание веб-приложений занимает несколько минут. До завершения развертывания веб-приложений сервер WACS будет находиться в состоянии «Инициализация». Пользователи не получают доступа к веб-приложениям, которые находятся на сервере WACS до полного развертывания веб-приложений. Не останавливайте сервер до завершения начального развертывания. Состояние сервера WACS можно просмотреть в Диспетчере центральной конфигурации (CCM).

Эта задержка возникает только при первом запуске WACS после его установки или обновления. Эта задержка отсутствует при последующих запусках WACS.

Веб-приложения нельзя вручную разворачивать на сервере WACS. Для развертывания веб-приложений на сервере WACS нельзя использовать WDeploy.

10.1.2.2 Добавление нового сервера контейнера веб-приложений

Примечание:

Из-за высокого расхода ресурсов системы не рекомендуется одновременно запускать несколько WACS на одном компьютере. Однако вы можете установить несколько WACS на одном компьютере, и запускать только один из них, что поможет вам быстро восстановить работу системы в случае сбоя или неверной настройки одного из серверов.

1. Перейдите в область управления «Серверы» в CMC.
2. Выберите **Управление > Создать > Новый сервер**.
Откроется окно «Создать новый сервер».
3. В списке **Категория службы** выберите пункт **Корневые службы**.
4. В списке **Выбрать службу** выберите службы, которые должны размещаться на WACS, и щелкните **Далее**.
 - Если требуется, чтобы на WACS размещались такие веб-приложения, как CMC, стартовая панель BI или OpenDocument, выберите **Служба веб-приложения BOE**.
 - Если требуется, чтобы на WACS размещались такие веб-службы, как Live Office или QaaWS (Query as a Web Service), выберите **Веб-службы SDK и QaaWS**.
 - Если требуется, чтобы на WACS размещались веб-службы Business Process BI, выберите **Веб-служба Business Process BI**.
 - Если требуется, чтобы на WACS поддерживалась трассировка сервера, выберите **Служба протокола трассировки**.
5. На следующем экране «Создать новый сервер» выберите любые дополнительные службы для размещения на сервере WACS и нажмите кнопку **Далее**.
6. В следующем окне «Создать новый сервер» щелкните **Далее**.

7. В следующем окне «Создать сервер» выберите узел, в который будет добавлен сервер, введите имя сервера и описание, после чего щелкните **Создать**.

Примечание:

В списке **Узел** будут отображаться только те узлы, на которых установлены серверы WACS.

8. В окне «Серверы» щелкните только что созданный сервер WACS.
Откроется окно «Свойства».
9. Чтобы сервер WACS не запускался автоматически при перезапуске системы, на панели «Общие параметры» снимите флажок **Автоматически запускать этот сервер при запуске агента серверной аналитики**.
10. Нажмите кнопку **Сохранить и закрыть**.

Будет создан новый сервер WACS. К нему применяются параметры и свойства по умолчанию.

10.1.2.3 Клонирование сервера контейнера веб-приложений

В качестве альтернативы, для добавления сервера контейнера веб-приложений (WACS) к вашему развертыванию, можно клонировать WACS как на другой, так и на тот же самый компьютер. При добавлении нового WACS создается сервер с настройками по умолчанию, а клонирование WACS применяет настройки исходного WACS к новому WACS.

Серверы могут быть клонированы только на те компьютеры, на которых уже установлен WACS.

Примечание:

Из-за высокого расхода ресурсов системы не рекомендуется одновременно запускать несколько WACS на одном компьютере. Однако вы можете установить несколько WACS на одном компьютере, и запускать только один из них, что поможет вам быстро восстановить работу системы в случае сбоя или неверной настройки одного из серверов.

1. Перейдите в область управления «Серверы» в СМС.
2. Выберите сервер WACS, который требуется клонировать, щелкните его правой кнопкой мыши и выберите команду **Клонировать сервер**.
На экране «Клонировать сервер» отображается перечень узлов вашего развертывания, на которые можно клонировать WACS. В списке **Клонировать в узле** перечислены только те узлы, на которых сервер WACS уже установлен.
3. На экране «Клонировать сервер» введите имя нового сервера, выберите узел, на который требуется клонировать сервер, и нажмите кнопку **ОК**.

Будет создан сервер WACS. Он содержит такие же службы, как и сервер-источник клонирования. Новый сервер и размещенные на нем службы имеют те же настройки, как и клонированный сервер, за исключением имени сервера.

Примечание:

Если вы клонировали WACS на тот же самый компьютер, могут возникнуть конфликты портов с сервером, который использовался для клонирования. В таком случае необходимо изменить номера портов на новом экземпляре WACS.

См. также

- [Разрешение конфликтов порта HTTP](#)

10.1.2.4 Удаление серверов WACS из развертывания

Удаление WACS возможно только в том случае, если сервер в данный момент не обеспечивает службу СМС. Чтобы удалить WACS из развертывания, необходимо войти в центральную консоль управления с другого WACS или сервера Java-приложений. Удаление WACS, с которого в данный момент запущена служба СМС, невозможно.

1. Перейдите в область управления «Серверы» в СМС.
2. Остановите сервер, который требуется удалить, щелкнув его правой кнопкой мыши и выбрав команду **Остановить сервер**.
3. Щелкните сервер правой кнопкой мыши и выберите команду **Удалить**.
4. При запросе подтверждения нажмите кнопку **ОК**.

10.1.3 Добавление или удаление служб на сервере WACS

10.1.3.1 Добавление веб-приложения или веб-службы к WACS

Для добавления дополнительных веб-приложений или веб-служб платформы BI к WACS требуется остановить WACS. Поэтому необходимо оставить хотя бы одну дополнительную СМС на WACS в развертывании, которая предоставляет службу веб-приложения BOE во время остановки и добавления веб-службы к другим WACS.

При добавлении службы к WACS она автоматически развертывается на WACS при перезапуске сервера.

1. Перейдите в область управления «Серверы» в СМС.
2. Дважды щелкните WACS, к которому нужно добавить службу, и просмотрите свойства сервера, чтобы убедиться в отсутствии на нем добавляемой службы.

3. Нажмите **Отмена** для возврата к экрану «Серверы».
4. Остановите сервер, щелкнув его правой кнопкой мыши и выбрав команду **Остановить сервер**.
При попытке остановки WACS, на котором в настоящее время работает служба СМС, будет выведено предупреждающее сообщение. Не продолжайте, если в развертывании не работает хотя бы одна дополнительная служба веб-приложения BOE на другом WACS. В противном случае нажмите кнопку **ОК**, выполните вход на другой WACS и начните эту процедуру сначала.
5. Щелкните сервер правой кнопкой мыши и выберите команду **Выбрать службы**.
Будет открыт экран «Выбрать службы».
6. Выберите службу, добавляемую к серверу, и добавьте ее к серверу, нажав **>**, а затем – **ОК**.
7. Запустите сервер WACS, щелкнув его правой кнопкой мыши и выбрав команду **Запустить сервер**.

Служба добавлена к WACS. К службе применены параметры и свойства по умолчанию.

10.1.3.2 Удаление веб-приложения или веб-службы с WACS

Для удаления веб-приложения или веб-службы с WACS требуется выполнить вход для СМС на другом WACS или на сервере приложений Java. Остановка WACS, с которого в данный момент запущена служба СМС, невозможно.

Последняя служба не может быть удалена с WACS. Следовательно, при удалении веб-службы с сервера WACS необходимо убедиться, что на сервере осталась как минимум одна другая служба.

Для удаления последней службы необходимо удалить WACS.

1. Перейдите в область управления «Серверы» в СМС.
2. Дважды щелкните WACS, с которого следует удалить службу, и просмотрите свойства сервера, чтобы убедиться в присутствии на нем удаляемой службы.
3. Нажмите **Отмена** для возврата к экрану «Серверы».
4. Остановите сервер WACS, щелкнув его правой кнопкой мыши и выбрав команду **Остановить сервер**.
При попытке остановки WACS, на котором в настоящее время работает служба СМС, будет выведено предупреждающее сообщение. Не продолжайте, если в развертывании не работает хотя бы одна дополнительная служба веб-приложения BOE на другом WACS. В противном случае нажмите кнопку **ОК**, выполните вход на другой WACS и начните эту процедуру сначала.
5. Щелкните сервер WACS правой кнопкой мыши и выберите команду **Выбрать службы**.
Будет открыт экран «Выбрать службы».
6. Выберите удаляемую службу и щелкните **<**, а затем нажмите кнопку **ОК**.
7. Запустите сервер WACS, щелкнув его правой кнопкой мыши и выбрав команду **Запустить сервер**.

Служба удалена с WACS.

10.1.4 Настройка HTTPS/SSL

Можно использовать протокол SSL и HTTP для обмена данными по сети между клиентами и WACS в развертывании платформы SAP BusinessObjects Business Intelligence. SSL/HTTPS шифрует сетевой трафик и обеспечивает улучшенную защиту.

Существует два типа SSL:

- SSL, используемый между серверами платформы SAP BusinessObjects Business Intelligence, включая WACS и другие серверы платформы SAP BusinessObjects Business Intelligence в развертывании. Он называется CorbaSSL. Для получения дополнительных сведений об использовании SSL между серверами платформы SAP BusinessObjects Business Intelligence в системе см. раздел «Общие сведения об обмене данными между компонентами платформы SAP BusinessObjects Business Intelligence» главы «Работа с брандмауэрами» документа *Руководство администратора платформы SAP BusinessObjects Business Intelligence*.
- HTTP через SSL, возникающий между WACS и клиентами (например, обозревателями), которые взаимодействуют с WACS.

Примечание:

Если выполняется развертывание WACS в системе с прокси или обратным прокси, и требуется использование SSL для защиты обмена данными, необходимо создать два WACS. Для получения дополнительных сведений см. раздел *Использование WACS с инвертированным прокси-сервером*.

Для настройки HTTPS/SSL на WACS необходимо выполнить следующие шаги.

- Сгенерировать или приобрести хранилище сертификатов PKCS12 или хранилище ключей JKS, в котором будут содержаться ваши сертификаты и личные ключи. Вы можете использовать Microsoft Internet Information Service (IIS) и Microsoft Management Console (MMC) для генерации файла PKCS12, или же использовать openssl или командную строку Java-инструмента для генерации файла хранилища ключей.
- Если вы хотите подключить к WACS только нескольких клиентов, вы должны сгенерировать файл со списком надежных сертификатов.
- После создания хранилища сертификатов и, если необходимо, списка надежных сертификатов, скопируйте файлы на компьютер WACS.
- Настройка HTTPS на сервере WACS.

См. также

- [Основные сведения об обмене данными между компонентами платформы BI](#)
- [Использование WACS с обратным прокси](#)

10.1.4.1 Создание хранилища файла сертификата PKCS12

Имеются множество способов создания хранилищ файлов сертификатов PKCS12 и хранилищ ключей Java, а также инструментов, которые можно для этого использовать. Выбор способа зависит от инструментов, к которым у вас есть доступ и с которыми вы знакомы.

В данном примере показан способ создания файла PKCS12 с использованием служб Internet Information Services (IIS) Microsoft и консоли управления Microsoft Management Console (MMC).

1. Войдите в компьютер, на котором установлен WACS, под учетной записью администратора.
2. В IIS запросите сертификат у органа сертификации. Информацию о порядке запроса сертификата смотрите в справочной документации IIS.
3. Запустите MMC. Для этого нажмите **Начало > Запуск**, введите mmc.exe и нажмите **ОК**.
4. Добавьте встраиваемый файл сертификатов в MMC:
 - a. В меню **Файл** нажмите **Добавить/Удалить встраиваемый файл**.
 - b. Нажмите **Добавить**.
 - c. В диалоговом окне «Добавить автономный встраиваемый файл» выберите **Сертификаты** и нажмите **Добавить**.
 - d. Выберите **Учетная запись компьютера** и нажмите **Далее**.
 - e. Выберите **Локальный компьютер** и нажмите **Готово**.
 - f. Нажмите **Закрыть** и **ОК**.

Встраиваемый файл сертификатов добавлен в MMC.

5. В MMC откройте **Сертификаты** и выберите нужный сертификат.
6. В меню **Действие** выберите **Все задачи > Экспорт**.
Будет запущен «Мастер экспорта сертификатов».
7. Нажмите кнопку **Далее**.
8. Выберите **Да, экспортировать секретный ключ** и нажмите кнопку **Далее**.
9. Выберите **Обмен личной информацией – PKCS #12 (.PFX)** и нажмите **Далее**.
10. Введите пароль, который вы использовали при создании сертификата, и нажмите **Далее**.
Этот пароль нужно указать в поле **Пароль доступа к секретным ключам** при настройке HTTPS для WACS.

Хранилище файла сертификата PKCS12 создано.

10.1.4.2 Для генерации списка надежных сертификатов

1. Выполните вход в компьютер, на котором размещается WACS, в качестве администратора.
2. Запустите консоль управления Microsoft Management Console (MMC).

3. Добавьте интегрируемые службы Internet Information Services:
 - a. В меню **Файл** выберите **Добавить/Удалить интегрируемую службу** и нажмите **Добавить**.
 - b. В диалоговом окне «Добавить автономную интегрируемую службу» выберите **Internet Information Services (IIS) Manager** и нажмите **Добавить**.
 - c. Нажмите **Заккрыть** и **ОК**.
Теперь интегрируемая служба IIS добавлена в MMC.
4. На левой панели MMC найдите веб-сайт, для которого следует создать список надежных сертификатов.
5. Щелкните на веб-сайт правой кнопкой мыши и выберите **Свойства**.
6. Перейдите на вкладку **Директория безопасности** и в меню «Безопасные коммуникации» выберите **Изменить**.
7. Нажмите **Разрешить список надежных сертификатов**, а затем нажмите **Создать**.
Запустится «Мастер списка надежных сертификатов».
8. Нажмите кнопку **Далее**.
9. Нажмите **Добавить из хранилища** или **Добавить из файла**, выберите сертификат, который вы хотите добавить в список надежных сертификатов, нажмите **ОК** и **Далее**.
10. Введите имя и описание списка надежных сертификатов и нажмите **Далее**.
11. Нажмите **Готово**, а затем **ОК**.
Список надежных сертификатов отображается в поле **Текущий список надежных сертификатов**.
12. Выберите список надежных сертификатов и нажмите "Редактировать".
Запустится «Мастер списка надежных сертификатов».
13. Нажмите кнопку **Далее**.
14. В списке **Текущие надежные сертификаты** выберите список сертификатов и нажмите **Просмотр сертификатов**.
15. Перейдите на вкладку **Сведения** и нажмите **Копировать в файл**.
Будет запущен «Мастер экспорта сертификатов».
16. Нажмите кнопку **Далее**.
17. Выберите **Да, экспортировать секретный ключ** и нажмите кнопку **Далее**.
18. Выберите **Обмен личной информацией – PKCS #12 (.PFX)** и нажмите **Далее**.
19. Введите пароль, который вы использовали при создании сертификата, и нажмите **Далее**.
Необходимо указать этот пароль в поле **Пароль доступа к секретным ключам списка надежных сертификатов** при настройка HTTPS для WACS.

10.1.4.3 Настройка HTTPS/SSL

Перед началом настройки HTTPS/SSL на сервере WACS убедитесь, что вы уже создали файл PKCS12 или хранилище ключей JKS и скопировали или переместили его на компьютер, на котором установлен сервер WACS.

1. Перейдите в область управления «Серверы» в СМС.
2. Дважды щелкните по серверу WACS, для которого требуется включить HTTPS.
Откроется окно «Свойства».
3. В разделе «Конфигурация HTTPS» установите флажок в поле **Включить HTTPS**.
4. В поле **Связать с именем хоста или IP-адресом** укажите IP-адрес, для которого были выпущены сертификаты и с которым будет связан WACS.
Службы HTTPS будут предоставляться через указанный вами IP-адрес.
5. В поле **Порт HTTPS** укажите номер порта для WACS для предоставления услуг HTTPS.
Убедитесь, что этот порт свободен. Если вы планируете разрешить пользователям подключаться к WACS с внешней стороны брандмауэра, необходимо убедиться, что в брандмауэре этот порт тоже свободен.
6. Если вы настраиваете SSL с обратным прокси, то укажите имя хоста и порт прокси-сервера в полях **Имя хоста прокси** и **Порт прокси**.
7. В списке **Протокол** выберите протокол. Доступны следующие варианты:
 - **SSL**
SSL – это протокол безопасных соединений, предназначенный для шифрования сетевого трафика.
 - **TLS**
TLS – это протокол защиты транспортного уровня, представляющий собой более новый, улучшенный протокол по сравнению с SSL. Разница между протоколами SSL и TLS незначительна, однако TLS включает более мощные алгоритмы шифрования.
8. В поле **Тип хранилища сертификатов** укажите тип файла для сертификата. Доступны следующие варианты:
 - **PKCS12**
Выберите PKCS12, если вам удобнее работать с инструментами Microsoft.
 - **JKS**
Выберите JKS, если вам удобнее работать с инструментами Java.
9. В поле **Местоположение файла хранилища сертификатов** укажите путь, куда вы скопировали или переместили файл хранилища сертификатов или файл хранилища ключей Java.
10. В поле **Пароль доступа к секретным ключам списка надежных сертификатов** укажите пароль.
Чтобы предотвратить неавторизованный доступ, у хранилищ сертификатов PKCS12 и хранилищ ключей JKS имеются секретные ключи, защищенные паролями. Для того чтобы WACS мог получить доступ к секретным ключам, необходимо указать пароль.
11. Рекомендуется использовать хранилище файла сертификатов или хранилище ключей, в котором либо содержится один сертификат, либо сертификат, который требуется использовать,

стоит первым в списке. В случае, если вы используете хранилище файла сертификатов или хранилище ключей, в котором содержится более одного сертификата, и этот сертификат в хранилище файла не является первым, в поле **Псевдоним сертификата** необходимо указать псевдоним сертификата.

12. Если требуется, чтобы WACS принимал запросы HTTPS только от определенных клиентов, активируйте аутентификацию клиентов.

Аутентификация клиентов не устанавливает подлинность пользователей. Она гарантирует, что WACS обслуживает запросы HTTPS только определенных клиентов.

- a. Поставьте флажок в поле **Включить аутентификацию клиента**.
- b. В поле **Местоположение файла списка надежных сертификатов** укажите местоположение файла PKCS12 или хранилища ключей JKS, в котором содержится файл списка надежных сертификатов.

Примечание:

Тип списка надежных сертификатов должен быть таким же, как тип Хранилища сертификатов.

- c. В поле **Пароль доступа к секретным ключам списка надежных сертификатов** введите пароль, который защищает доступ к секретным ключам в файле списка надежных сертификатов.

Примечание:

Если вы активировали аутентификацию клиентов, а подлинность браузера или пользователя веб-службы не подтверждена, соединение HTTPS отклоняется.

13. Нажмите кнопку **Сохранить и закрыть**.
14. Перейдите в окно «Показатели» и убедитесь, что соединительное звено HTTPS отображается в Списке выполняемых соединителей WACS. Если HTTPS в списке нет, проверьте правильность настройки соединителя HTTPS.

10.1.5 Поддерживаемые методы аутентификации

WACS поддерживает следующие методы аутентификации:

- Enterprise
- LDAP
- AD Kerberos

WACS не поддерживает следующие методы аутентификации:

- NT
- AD NTLM
- LDAP с единым входом в систему

10.1.6 Настройка Kerberos AD для WACS

Чтобы настроить аутентификацию Kerberos AD для WACS необходимо настроить на компьютере поддержку AD. Необходимо выполнить следующие действия.

- Включить подключаемый модуль безопасности Windows AD.
- Сопоставить пользователей и группы.
- Настроить учетную запись службы.
- Настроить ограниченное делегирование.
- Включить аутентификацию Kerberos в подключаемом модуле Windows AD для WACS
- Создать файлы конфигурации.

После настройки компьютера, на котором находится WACS, на использование аутентификации Kerberos AD необходимо выполнить дополнительную настройку с помощью Central Management Console (CMC).

См. также

- [Использование пользователей и групп Windows AD](#)
- [Подключаемый модуль безопасности Windows AD](#)
- [Настройка учетной записи службы для аутентификации AD с Kerberos](#)
- [Подготовка серверов для аутентификации Windows AD с Kerberos](#)
- [Включение аутентификации Kerberos в подключаемом модуле Windows AD для WACS](#)
- [Создание файлов конфигурации.](#)
- [Конфигурация WACS для AD Kerberos](#)
- [Настройка единого входа в AD Kerberos](#)

10.1.6.1 Включение аутентификации Kerberos в подключаемом модуле Windows AD для WACS

Для поддержки Kerberos необходимо настроить подключаемый модуль безопасности Windows AD в CMC на использование аутентификации Kerberos. Настройка включает следующее:

- Включение аутентификации Windows AD.
- Ввод учетной записи администратора AD.

Примечание:

Для этой учетной записи требуется доступ к Active Directory только на чтение, другие права не требуются.

-

- Задайте имя администратора доступа к службе (SPN) для учетной записи службы.

10.1.6.1.1 Предварительные требования

Перед выполнением настройки подключаемого модуля защиты Windows AD для Kerberos необходимо выполнить следующие задачи:

- [Настройка учетной записи службы для аутентификации AD с Kerberos](#)
- [Предоставление прав учетной записи службы](#)
- [Подготовка серверов для аутентификации Windows AD с Kerberos](#)
- "Mapping Windows AD accounts"

10.1.6.1.2 Настройка подключаемого модуля безопасности Windows AD для Kerberos

1. Перейдите в область управления **Аутентификация** в СМС.
2. Дважды щелкните **Windows AD**.
3. Установите флажок **Аутентификация Windows Active Directory** включена.
4. В пункте **Параметры аутентификации** выберите **Использовать аутентификацию Kerberos**.
5. В поле **Имя администратора доступа к службе** введите учетную запись и домен учетной записи службы или сопоставление SPN с учетной записью службы.

Используйте указанный ниже формат, где *svcacct* – это имя учетной записи службы или SPN, созданное ранее, а *DNS.COM* – полное доменное имя в верхнем регистре. Например, учетная запись службы может называться *svcacct@DNS.COM*, а SPN – *BOBJCMS/some_name@DOMAIN.COM*.

Примечание:

- Если планируется разрешать вход пользователям не из домена по умолчанию, необходимо ввести SPN, сопоставленное ранее.
- Для учетной записи службы учитывается регистр. Регистр вводимой здесь учетной записи должен соответствовать введенному в домене Active Directory.
- Это должна быть та же учетная запись, которая используется для запуска серверов платформы SAP BusinessObjects Business Intelligence или SPN, сопоставленное этой учетной записи.

См. также

- [Настройка единого входа в AD Kerberos](#)

10.1.6.2 Создание файлов конфигурации.

В общем случае процесс настройки Kerberos на сервере приложений состоит из следующих шагов:

- Создание файла конфигурации Kerberos.
- Создание файла конфигурации входа JAAS.

Примечание:

- Домен Active Directory по умолчанию должен вводиться в формате DNS в верхнем регистре.
- Загрузка и установка MIT Kerberos для Windows не требуется. Также для учетной записи службы больше не требуется файл таблицы ключей (keytab).

10.1.6.2.1 Создание файла конфигурации Kerberos

Чтобы создать файл конфигурации Kerberos, выполните указанные ниже шаги.

1. Создайте файл `krb5.ini`, если он отсутствует, и сохраните его в каталоге `C:\WINNT` для Windows.

Примечание:

Этот файл можно сохранить в другом месте. Однако если это сделать, необходимо будет указать его местоположение в поле **Расположение файла Krb5.ini** на странице «Свойства» для сервера WACS в СМС.

2. Добавьте в файл конфигурации Kerberos следующую обязательную информацию:

```
[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 =
```

Примечание:

- `DNS.COM` – DNS-имя домена, которое необходимо вводить в верхнем регистре в формате полного доменного имени.
- `kdc` – имя хоста контроллера домена.
- В раздел `[realms]` можно добавить несколько записей доменов, если пользователи выполняют вход из нескольких доменов. Пример этого файла с несколькими записями доменов см. в разделе [Примеры файлов Krb5.ini](#).
- В конфигурации с несколькими доменами в разделе `[libdefaults]` для параметра `default_realm` должен быть указан любой из этих доменов. Рекомендуется использовать

домен с максимальным количеством пользователей, аутентификация которых будет выполняться с использованием их учетных записей AD.

10.1.6.2.2 Создание файла конфигурации входа JAAS

1. Создайте файл с именем `bscLogin.conf`, если он еще не существует, и сохраните его в каталоге по умолчанию : `C:\WINNT`.

Примечание:

Этот файл можно сохранить в другом месте. Однако если это сделать, необходимо будет указать его местоположение в поле **Расположение файла `bscLogin.conf`** на странице «Свойства» для сервера WACS в СМС.

2. Добавьте в файл конфигурации JAAS `bscLogin.conf` следующий код:

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
```

3. Сохраните и закройте файл.

10.1.6.2.3 Примеры файлов `Krb5.ini`

Пример файла `Krb5.ini` с несколькими доменами

Ниже приведен пример файла с несколькими доменами:

```
[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
}
```

Пример файла Krb5.ini с одним доменом

Ниже приведен пример файла krb5.ini с одним доменом.

```
[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 Конфигурация WACS для AD Kerberos

После настройки компьютера, на котором размещается средство аутентификации WACS для AD Kerberos, необходимо настроить WACS с Central Management Console (CMC).

10.1.6.3.1 Настройка WACS для AD Kerberos

1. Перейдите в область управления «Серверы» в CMC.
2. Дважды щелкните WACS, для которого необходимо настроить AD.
Откроется окно «Свойства».
3. В поле **Местоположение файла Krb5.ini** укажите путь к файлу конфигурации `krb5.ini`.
4. В поле **Местоположение файла bscLogin.conf** укажите путь к файлу конфигурации `bscLogin.conf`.
5. Нажмите кнопку **Сохранить и закрыть**.
6. Перезапустите WACS.

10.1.6.4 Устранение неполадок с Kerberos

Описанные ниже шаги могут помочь при возникновении проблем с настройкой Kerberos.

- Включение регистрации событий
- Тестирование конфигурации Kerberos

10.1.6.4.1 Включение регистрации событий Kerberos

1. Запустите Central Configuration Manager (CCM) и нажмите **Управление серверами**.
2. Укажите учетные данные для входа в систему.
3. Остановите WACS в окне «Управление серверами».

4. Щелкните **Конфигурация веб-ярусов**

Примечание:

Значок **Конфигурация веб-ярусов** доступен только при выборе остановленного сервера WACS.

Откроется окно «Конфигурация веб-ярусов».

5. В пункте **Параметры командной строки** скопируйте в конец параметров следующий текст:

```
«-Dcrystal.enterprise.trace.configuration=verbose  
-Djcsi.kerberos.debug=true»
```

6. Нажмите кнопку **ОК**.

7. Запустите WACS в экране «Управление серверами».

10.1.6.4.2 Тестирование конфигурации Kerberos

- Выполните указанную ниже команду, чтобы протестировать конфигурацию Kerberos (здесь `servact` – учетная запись службы и домен, с которыми работает CMS, `password` – пароль этой учетной записи службы).

```
<Install Directory>\Business Objects\javasdk\bin\kinit.exe servact@TESTM03.COM Password
```

Например:

```
C:\Program Files\Business Objects\javasdk\bin\kinit.exe servact@TESTM03.COM Password
```

Если неполадки не устранены, проверьте, чтобы регистр, в котором введен домен и имя администратора доступа к службе, совпадали с указанными в Active Directory.

10.1.6.4.3 Сопоставленному пользователю AD не удастся войти в BusinessObjects Enterprise в WACS

Несмотря на то, что пользователи сопоставлены с SAP BusinessObjects Enterprise, могут возникать две проблемы:

Ошибка входа в результате различия имен AD UPN и SAM

Идентификаторы пользователей Active Directory успешно сопоставлены SAP BusinessObjects Enterprise. Несмотря на это им не удастся успешно выполнить вход в CMC с использованием аутентификации AD и Kerberos в следующем формате: `DOMAIN\ABC123`

Эта проблема может возникать в случае, когда пользователь настроен в Active Directory с использованием несовпадающих UPN- и SAM-имен (несовпадение регистров или по иной причине). Ниже приведено два примера, из-за которых могут возникать проблемы:

- UPN – `abc123@company.com`, а SAM-имя – `DOMAIN\ABC123`.
- UPN – `jsmith@company`, а SAM-имя – `DOMAIN\johnsmith`.

Эту проблему можно устранить двумя способами:

- Пользователи должны выполнять вход с использованием UPN-имени, а не SAM-имени.
- SAM-имя учетной записи и UPN-имя должны совпадать.

Ошибка предварительной аутентификации

Пользователь, который раньше выполнял вход, больше не может успешно выполнять вход. Пользователю будет отображаться следующая ошибка: "Данные учетной записи не распознаны". В журналах WACS можно найти следующую ошибку: "Pre-authentication information was invalid (24)" (данные предварительной аутентификации недействительны)

Это может возникать по причине того, что база данных пользователей Kerberos не получила изменения, внесенные в UPN-имя в AD. Это может означать рассинхронизацию базы данных пользователей Kerberos и данных AD.

Для устранения данной проблемы выполните сброс пароля пользователя в AD. Это обеспечит правильность распространения изменений.

10.1.7 Настройка единого входа в AD Kerberos

При настройке службы единого входа AD Kerberos для стартовой панели BI или SDK веб-служб и QaaWS необходимо убедиться, что сервер WACS и компьютер, на котором размещается WACS, настроены для аутентификации AD Kerberos. Для получения дополнительных сведений см. [Настройка Kerberos AD для WACS](#).

Примечание:

Если планируется использование единого входа в среде обратного прокси, то перед продолжением работы рекомендуется ознакомиться с главой «Обеспечение безопасности платформы SAP BusinessObjects Business Intelligence» документа *Руководство администратора платформы SAP BusinessObjects Business Intelligence*.

10.1.7.1 Настройка компьютера для единого входа AD Kerberos

Чтобы настроить службу единого входа AD Kerberos для SDK и QaaWS для веб-служб, сначала необходимо настроить компьютер, на котором размещается WACS:

- [Настройка ограниченного делегирования для функции единого входа Vintela](#)
- "To create an SPN for your web application server"
- "To reset the service account password"
- "To create and place a keytab file"
- [Настройка нескольких SPN-имен](#)
- [Увеличение лимита размера заголовка WACS](#)

В разделах ниже описано выполнение каждого из этих шагов.

10.1.7.1.1 Настройка нескольких SPN-имен

Использование нескольких SPN не поддерживается.

10.1.7.1.2 Увеличение лимита размера заголовка WACS

Active Directory создает маркер Kerberos, который используется в процессе аутентификации. Этот маркер хранится в HTTP-заголовке. У WACS будет размер заголовка HTTP по умолчанию, которого достаточно для большинства пользователей. Этот размер заголовка можно изменить.

1. Перейдите в область управления «Серверы» в СМС.
2. Дважды щелкните WACS, для которого нужно изменить размер верхнего колонтитула. Откроется диалоговое окно «Свойства».
3. В разделе «Настройка HTTP», «Настройка HTTP через прокси» или «Настройка HTTPS» укажите значение в поле **Максимальный размер заголовка HTTP (в байтах)**.
4. Нажмите кнопку **Сохранить и закрыть**.
5. Перезапустите сервер.

10.1.7.2 Настройка WACS для единого входа AD Kerberos

Можно настроить на сервере WACS использование единого входа AD Kerberos. Служба единого входа AD Kerberos поддерживается. Служба AD NTLM не поддерживается.

Перед настройкой сервера WACS необходимо настроить службу единого входа AD Kerberos для компьютера, на котором размещается сервер WACS.

1. Перейдите в область управления «Серверы» в СМС.
2. Дважды щелкните сервер контейнера веб-приложений, который требуется настроить. Откроется окно «Свойства».
3. Установите флажок **Включить единый вход в Active Directory с Kerberos**.
4. Укажите значения свойств "Домен AD по умолчанию", "Имя принципала службы" и "Файл ярлыков ключей", после чего выберите команду **Сохранить и закрыть**.
5. Перезапустите WACS.

Служба единого входа Active Directory готова к использованию.

10.1.7.3 Настройка модуля Kerberos и режима единой регистрации в базе данных

Единый вход в базу данных поддерживается для систем, удовлетворяющих следующим требованиям:

- Развертывание платформы SAP BusinessObjects Business Intelligence осуществляется с помощью сервера WACS.
- Сервер WACS настроен на AD с Kerberos.
- Версия базы данных, для которой требуется единый вход, является поддерживаемой версией SQL Server или Oracle.
- Группам и пользователям, которым требуется доступ к базе данных, предоставлены разрешения в SQL Server или Oracle.
- На странице аутентификации AD в СМС установлен флажок "Контекст защиты кэша" (требуется для единого входа в базу данных).

Последний шаг заключается в изменении файла `krb5.ini` для поддержки единой регистрации в базе данных.

Примечание:

Эти инструкции объясняют, как настроить режим единой регистрации в базе данных. Если нужно настроить сквозной единый вход в базу данных, необходимо выполнить и шаги по настройке, обязательные для единого входа Vintela. Для получения дополнительных сведений см. раздел [Настройка единого входа в AD Kerberos](#).

10.1.7.3.1 Включение режима единой регистрации в базе данных

1. Откройте файл `krb5.ini`, используемый для развертывания платформы SAP BusinessObjects Business Intelligence.

По умолчанию он находится на сервере веб-приложений в каталоге WINNT.

2. Перейдите в раздел файла `[libdefaults]`.
3. Введите данную строку перед началом раздела файла `[realms]`:

```
forwardable = true
```

4. Сохраните и закройте файл.
5. Перезапустите WACS.

10.1.8 Сервер контейнера веб-приложений (WACS) и ваша IT-среда

В этом разделе содержится информация о настройках WACS в сложной среде.

10.1.8.1 Использование WACS с другими веб-серверами

Если сервер контейнера веб-приложений (WACS) установлен, то он работает как сервер приложений и веб-сервер, не требуя при этом дополнительной настройки. Вы можете настроить поддерживаемые веб-серверы, такие как Internet Information Services (IIS) и Apache для выполнения URL, направляемых на сервер WACS.

Примечание:

Направление запроса с IIS на WACS с использованием фильтра ISAPI не поддерживается.

WACS не поддерживает сценарий развертывания, с размещением статического содержимого на хостах веб-серверов, а динамического – на хостах WACS. Статическое и динамическое содержимое всегда должны размещаться на WACS.

10.1.8.2 Использование WACS с балансировщиком нагрузки

Для того чтобы использовать WACS в развертывании со средством равномерного распределения аппаратной нагрузки, необходимо настроить данное средство таким образом, чтобы оно использовало либо IP-маршрутизацию, либо активные файлы Cookies. В этом случае после установления на WACS сеанса пользователя все последующие запросы данного пользователя будут направляться на этот сервер WACS.

WACS не поддерживается с балансировщиками нагрузки аппаратного обеспечения, которые используют пассивные файлы cookies.

Если балансировщик нагрузки аппаратного обеспечения направляет SSL-зашифрованные запросы HTTPS на ваш WACS, то следует настроить HTTPS на WACS и на каждом WACS установить сертификаты SSL.

Если балансировщик нагрузки аппаратного обеспечения шифрует трафик HTTPS и направляет зашифрованные запросы HTTP на ваш WACS, то дополнительная настройка WACS не требуется.

См. также

- [Настройка HTTPS/SSL](#)

10.1.8.3 Использование WACS с обратным прокси

WACS можно использовать в развертывании с прямым или обратным прокси-сервером. Использовать WACS в качестве прокси-сервера нельзя.

10.1.8.3.1 Настройка WACS для поддержки HTTP с обратным прокси

Для того чтобы использовать WACS в развертывании с обратным прокси, следует настроить WACS таким образом, чтобы порт HTTP использовался для связи внутри межсетевого экрана (например, в защищенной сети), а порт HTTP через прокси – для связи за пределами межсетевого экрана (например, для сети Интернет).

1. Перейдите в область управления «Серверы» в СМС.
2. Дважды щелкните сервер контейнера веб-приложений, который требуется настроить. Откроется окно «Свойства».
3. В разделе «Настройка HTTP через прокси»:
 - a. Поставьте флажок рядом с полем **Включить HTTP через прокси**.
 - b. Укажите порт HTTP сервера WACS, который будет использоваться для связи через прокси.
 - c. Укажите имя хоста прокси и порт прокси прокси-сервера.
4. Нажмите кнопку **Сохранить и закрыть**.

10.1.8.3.2 Настройка WACS для поддержки HTTPS с обратным прокси

Некоторые балансировщики нагрузки и обратные прокси-серверы можно настроить на дешифровку трафика HTTPS и направление дешифрованного трафика на серверы приложений. В этом случае можно настроить WACS для использования портов HTTP или HTTP через прокси.

Если балансировщик нагрузки или обратный прокси-сервер направляет трафик HTTPS, и требуется настроить HTTPS с обратным прокси, создайте два сервера WACS. Настройте один WACS для HTTPS для внешнего трафика через обратный прокси-сервер, а другой WACS – для связи с клиентами на внутренней сети через HTTPS.

10.1.8.4 Использование WACS с брандмауэрами

Поддерживается развертывание WACS в IT-среде с брандмауэрами.

По умолчанию, WACS присваивается всем IP-адресам компьютера, на котором он установлен. Если планируется использовать брандмауэр между клиентами и вашим сервером контейнера веб-приложений (WACS), необходимо настроить WACS на привязку к конкретному IP-адресу для HTTP или HTTP через прокси. Для этого снимите флажок **Привязать ко всем IP-адресам**, а затем укажите имя хоста или IP-адрес, с которым должен связаться WACS.

Если планируется использование брандмауэра между сервером WACS и другими серверами платформы SAP BusinessObjects Business Intelligence в развертывании, обратитесь к разделу «Основные сведения об обмене данными между компонентами платформы SAP BusinessObjects Business Intelligence» *Руководства администратора платформы SAP BusinessObjects Business Intelligence*.

См. также

- [Основные сведения об обмене данными между компонентами платформы BI](#)

10.1.8.5 Настройка WACS на многосетевом компьютере

Групповой компьютер – это компьютер с несколькими сетевыми адресами. По умолчанию, экземпляры WACS (сервера контейнера веб-приложений) присваивают свои HTTP-порты всем IP-адресам. Если требуется привязать WACS к конкретному сетевому адаптеру, например для привязки HTTP-порта WACS к одной сетевой карте, а порта запросов – к другой:

1. Перейдите в область управления «Серверы» в СМС.
2. Дважды щелкните сервер контейнера веб-приложений, который требуется настроить. Откроется окно «Свойства».
3. В секции «Настройка HTTP через прокси» на панели «Служба контейнеров веб-приложений» снимите флажок **Привязать ко всем IP-адресам**, и введите IP-адрес, которому требуется присвоить WACS.
4. В секции «Конфигурация HTTPS» снимите флажок **Привязать ко всем IP-адресам**, и введите адрес или имя хоста, с которым требуется связать WACS.
5. В области «Общие параметры» снимите флажок **Назначать автоматически** и затем задайте имя хоста или IP-адрес сетевого адаптера, используемого для обмена данными между WACS и другими серверами платформы BI в данном развертывании.
6. Нажмите кнопку **Сохранить и закрыть**.
7. Перезапустите WACS.

10.1.9 Настройка свойств веб-приложений

Настроить свойства веб-приложений, размещаемых на WACS, можно одним из следующих способов:

- Часто изменяемые свойства представлены как настраиваемые свойства служб для WACS. Чтобы изменить эти свойства, откройте страницу «Свойства» на сервере WACS в консоли СМС, измените значение нужного свойства, а затем нажмите кнопку **Сохранить**.
- Чтобы изменить время ожидания завершения сеанса для веб-приложений, размещенных на сервере WACS, сначала определите, имеет ли соответствующее веб-приложение свойства, которые можно настроить в консоли СМС.

Если веб-приложение имеет свойства, доступные для настройки в СМС, следует изменить файл `web_xml.ino` для данного веб-приложения. Файл имеет имя `<WebAppName>_web_xml.ino`, где переменная `<WebAppName>` указывает имя веб-приложения. Файл находится в каталоге `<EnterpriseDirectory>/java/pjs/services/<WebAppName>`.

Если веб-приложение не имеет свойств, доступных для настройки в СМС, следует изменить файл `web.xml` для данного веб-приложения. Этот файл находится в каталоге `<EnterpriseDirectory>/warfile/webapps/<WebAppName>`, где переменная `<WebAppName>` указывает имя веб-приложения.

- Чтобы изменить свойства, отличные от времени ожидания завершения сеанса или доступные на экране «Свойства» сервера WACS в консоли СМС, следует изменить файл `.properties` для данного веб-приложения. Для получения дополнительных сведений см. раздел «Управление приложениями путем настройки свойств BOE.war» *Руководства администратора платформы SAP BusinessObjects Business Intelligence*.

Примечание:

- Не изменяйте файлы `web.xml`, `web_xml.ino`, или `.properties` в каталоге `<EnterpriseDirectory>/java/pjs/container/work/<ServerFriendlyName>`, поскольку изменения будут переопределяться при каждом запуске или перезапуске WACS.
- После изменения свойств для WACS необходимо перезапустить сервер.

См. также

- [Для изменения свойств сервера](#)
- [Файл BOE.war](#)

10.1.10 Устранение неполадок

10.1.10.1 Настройка трассировки на WACS

Чтобы настроить трассировку для WACS, см. раздел [Ведение журнала трассировок компонентов](#)

10.1.10.2 Для просмотра серверных показателей

Показатели сервера для WACS можно просмотреть, используя Central Management Console (СМС).

1. Перейдите в область управления «Серверы» в СМС.
2. Щелкните сервер WACS правой кнопкой мыши и выберите команду **Показатели**.

См. также

- [Показатели сервера контейнера веб-приложений](#)

10.1.10.3 Просмотр состояния сервера WACS

Для просмотра состояния сервера WACS перейдите в область «Серверы» СМС. В **Списке серверов** имеется столбец **Состояние**, в котором отображается состояние каждого сервера в списке.

У WACS имеется новое состояние сервера – «Запущено с ошибками». WACS, находящийся в этом состоянии, работает, но у него есть хотя бы один ненастроенный соединитель HTTP, HTTP через прокси, или HTTPS.

Если WACS имеет состояние «Запущено с ошибками», перейдите на страницу «Показатели» и просмотрите показатель «Список запущенных коннекторов WACS». Если включенного соединителя нет в списке, значит, он настроен неверно.

10.1.10.4 Устранение конфликтов портов

Если при попытке получить доступ к центральной консоли управления через определенный порт не отображается ни одна страница, убедитесь, что порты HTTP, HTTP через прокси или HTTPS, указанные для WACS, не заняты другим приложением.

Определить наличие конфликтов портов для заданного WACS можно двумя способами. Если в развертывании существует несколько WACS, войдите в центральную консоль управления и проверьте показатели "Выполняются соединители WACS" и "Ошибки запуска WACS". Если в списке выполняемых соединителей WACS отсутствуют соединители HTTP, HTTP через прокси или HTTPS, эти соединители не могут быть запущены из-за наличия конфликта портов.

Если развертывание содержит только один WACS или если центральная консоль управления недоступна ни с одного WACS, воспользуйтесь такой программой, как netstat, чтобы определить, занят ли порт WACS другим приложением.

10.1.10.4.1 Разрешение конфликтов порта HTTP

1. Запустите Central Configuration Manager (CCM) и нажмите значок **Управление серверами**.
2. Укажите учетные данные для входа в систему.
3. Остановите WACS в окне «Управление серверами».
4. Щелкните значок **Конфигурация веб-ярусов**.

Примечание:

Значок **Конфигурация веб-ярусов** доступен только при выборе остановленного сервера WACS.

Откроется окно «Конфигурация веб-ярусов».

5. В поле **Порт HTTP** укажите порт HTTP, который будет использоваться сервером контейнера веб-приложений, и нажмите кнопку **ОК**.
6. Запустите WACS в экране «Управление серверами».

10.1.10.4.2 Устранение конфликтов портов HTTP через прокси и HTTPS

Если нет возможности получить доступ к WACS через порты HTTP через прокси или HTTPS, но можно подключиться к Central Management Console (CMC) через порт HTTP, измените номера портов в CMC.

1. Перейдите в область управления «Серверы» в CMC.
2. Чтобы остановить сервер WACS, который требуется настроить, щелкните его правой кнопкой мыши и выберите команду **Остановить сервер**.
3. Дважды щелкните сервер контейнера веб-приложений, который требуется настроить. Откроется окно «Свойства».
4. В разделе «Настройка HTTP через прокси» укажите новый порт HTTP.
5. Для того чтобы изменить порт HTTPS, в разделе «Конфигурация HTTP» введите новое значение в поле **Порт HTTP**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. Чтобы запустить сервер WACS, щелкните его правой кнопкой мыши и выберите команду **Запустить сервер**.

10.1.10.5 Изменение параметров памяти

Для повышения производительности сервера WACS с помощью Central Configuration Manager (CCM) можно изменить количество памяти, выделяемой серверу.

1. Запустите CCM и щелкните значок **Управление серверами**.
2. Укажите учетные данные входа для CMC.
3. Остановите WACS в окне «Управление серверами».
4. Щелкните значок **Конфигурация веб-ярусов**.

Примечание:

Значок **Конфигурация веб-ярусов** доступен только при выборе остановленного сервера WACS.

Откроется окно «Конфигурация веб-ярусов».

5. В пункте «Параметры командной строки» укажите новое значение памяти посредством редактирования командной строки:

- a. Найдите параметр `-Xmx`. Обычно для этого параметра указано значение. Например, `«-Xmx1g»`. Это значение позволяет выделить для сервера один гигабайт памяти.
 - b. Укажите новое значение параметра.
 - Чтобы указать значение в мегабайтах, используйте параметр `«m»`. Например, `«-Xmx640m»` позволяет выделить для сервера WACS 640 мегабайт памяти.
 - Чтобы указать значение в гигабайтах, используйте параметр `«g»`. Например, `«-Xmx2g»` позволяет выделить для сервера WACS 2 гигабайта памяти.
 - c. Нажмите кнопку **ОК**.
6. Запустите WACS в экране «Управление серверами».

10.1.10.6 Изменение количества одновременных запросов

По умолчанию сервер WACS настроен на одновременную обработку 150 HTTP-запросов. Это количество подходит для большинства случаев развертывания. Для повышения производительности серверов WACS можно увеличить максимальное количество одновременных HTTP-запросов. Хотя увеличение количества одновременных запросов может повысить производительность, слишком большое значение может негативно сказаться на ней. Оптимальное значение параметра зависит от оборудования, программного обеспечения и ИТ-требований.

1. Перейдите в область управления «Серверы» в СМС.
2. Чтобы остановить сервер WACS, который требуется настроить, щелкните его правой кнопкой мыши и выберите команду **Остановить сервер**.
3. Дважды щелкните сервер контейнера веб-приложений, который требуется настроить. Откроется окно «Свойства».
4. В области «Параметры параллельного выполнения (на один блок соединения)» в поле **Максимальное число параллельных запросов** введите нужное число параллельных запросов и щелкните **Сохранить и закрыть**.
5. Чтобы запустить сервер WACS, щелкните его правой кнопкой мыши и выберите команду **Запустить сервер**.

10.1.10.7 Восстановление настроек системы по умолчанию

Если конфигурация WACS ошибочна, можно восстановить системные значения по умолчанию с помощью диспетчера Диспетчер центральной конфигурации (CCM).

1. Запустите CCM и щелкните значок **Управление серверами**.
2. Укажите учетные данные для входа в систему.
3. Остановите WACS в окне «Управление серверами».

4. Щелкните значок **Конфигурация веб-ярусов**.

Примечание:

Значок **Конфигурация веб-ярусов** доступен только при выборе остановленного сервера WACS.

Откроется окно «Конфигурация веб-ярусов».

5. Щелкните **Восстановить параметры системы по умолчанию**.
6. Если требуется, укажите свободный порт HTTP и нажмите кнопку **ОК**.
7. В окне «Управление серверами» запустите WACS.

10.1.10.8 Предотвращение подключения пользователей к WACS через HTTP

В ряде случаев может потребоваться предоставить доступ к серверу WACS через HTTP или HTTPS только для пользователей локальных компьютеров. Например, хотя закрыть порт HTTP нельзя, может потребоваться настройка WACS, при которой он будет принимать запросы HTTP только от клиентов, расположенных на том же компьютере, что и WACS. Благодаря этому вы можете выполнять задачи по техническому обслуживанию или настройке WACS через браузер с того же компьютера, где находится WACS, предотвращая доступ к серверу для других пользователей.

1. Перейдите в область управления «Серверы» в CMC.
2. Дважды щелкните по WACS, который требуется изменить.
Откроется окно «Свойства».
3. В разделе «Служба контейнеров веб-приложений» снимите флажок **Привязка ко всем IP-адресам**.
4. В поле **Связать с именем хоста или IP-адресом** введите 127.0.0.1 и нажмите кнопку **ОК**.
5. Чтобы запустить сервер WACS, щелкните его правой кнопкой мыши и выберите команду **Запустить сервер**.
WACS, настроенный таким образом, будет принимать только соединения с локальным компьютером.

10.1.11 Свойства WACS

Для получения полного списка конфигурационных свойств (общих, HTTP, HTTP с использованием прокси и HTTPS), которые можно настроить для WACS, см. раздел «Основные параметры серверов» в приложении «Свойства сервера».

См. также

- [Свойства основных служб](#)

Резервное копирование и восстановление

11.1 Резервное копирование и восстановление системы

В этой главе описаны предлагаемые процедуры для создания резервных копий системных файлов и файлов данных платформы SAP BusinessObjects Business Intelligence, а также процедуры восстановления при утрате данных или сбое в работе оборудования. Для выполнения плана требуется опытный специалист по BusinessObjects, системный администратор и администратор базы данных.

Процесс резервного копирования и восстановления одинаков для всех сред: разработки, тестирования и производственной. Таким образом, в этой главе не рассматриваются конкретные среды. Рекомендуется выполнять резервное копирование для всех сред.

План резервного копирования и восстановления состоит из мер предосторожности, предпринимаемых при системном сбое в результате стихийного бедствия или катастрофы. Этот план направлен на минимизацию влияния аварии на ежедневные операции, что позволит сохранить или быстро возобновить выполнение критически важных функций.

Рекомендуется регулярно копировать системную базу данных центрального сервера управления, содержимое репозитория входящих и исходящих файлов, а также файловую систему компьютеров, где установлена платформа SAP BusinessObjects Business Intelligence, для защиты системы от сбоев оборудования, программного обеспечения или неправильно настроенных параметров сервера.

Также рекомендуется регулярно копировать содержимое Business Intelligence, включая отчеты, пользователей и права доступа, при помощи консоли управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence 4.0 путем экспорта содержимого в файлы архива Business Intelligence (LCMBIAR-файлы). Если содержимое повреждено или отсутствует, можно будет восстановить это содержимое позже без необходимости восстанавливать всю базу данных центрального сервера управления или файловые репозитории. Для получения дополнительных сведений об использовании консоли управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence 4.0 см. *Руководство пользователя консоли управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence 4.0*. Если используется вспомогательная версия консоли управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence 4.0, см. главу «Резервное копирование файлов вспомогательных версий» в документе *Руководство пользователя консоли управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence 4.0*, в которой приведены дополнительные сведения о резервном копировании репозитория вспомогательной версии.

В остальной части этой главы описывается, как выполнять резервное копирование и восстановление системы при утрате или повреждении системной базы данных центрального сервера управления, файловых репозиториях или файловой системы. Здесь также описывается, как выполнить аварийное восстановление при неправильной конфигурации центрального сервера управления, если невозможно восстановить параметры сервера или содержимое Business Intelligence при помощи консоли управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence 4.0.

Примечание:

Можно выполнить резервное копирование платформы SAP BusinessObjects Business Intelligence и затем восстановить ее, чтобы создать копию системы.

11.1.1 Выполнение резервного копирования системы

Рекомендуется на регулярной основе выполнять резервное копирование следующих элементов:

- Системная база данных центрального сервера управления (CMS)

Критически важно часто копировать системную базу центрального сервера управления. Невозможно восстановить среду без наличия верной резервной копии системной базы данных центрального сервера управления. Перед началом резервного копирования системной базы данных центрального сервера управления необходимо остановить систему. Должно быть выполнено резервное копирование системной базы данных CMS с использованием средств резервного копирования базы данных от поставщика базы данных.

Первоначально нужно выполнить резервное копирование базы данных CMS. При запуске можно начать резервное копирование серверов репозитория файлов.

- Серверы репозитория входящих и исходящих файлов

Для сохранения целостности резервной копии рекомендуется выполнять резервное копирование содержимого серверов файловых репозиториях (FRS) одновременно с системной базой данных центрального сервера управления (CMS). Резервное копирование файловых репозиториях включает резервное копирование файлов, расположенных в папках, которые установлены в свойствах «Каталог хранилища файлов» на серверах репозиториях входящих и исходящих файлов. Перед резервным копированием файловых репозиториях необходимо остановить систему. Резервное копирование должно быть выполнено с использованием одного из средств резервного копирования файловой системы.

Частота, с которой выполняется резервное копирование системной базы центрального сервера управления, файловых репозиториях и файловой системы, зависит от потребностей организации.

Можно выбрать остановку системы платформы BI и выполнить холодное резервное копирование, что обеспечит статичное состояние БД и снизит вероятность изменения данных в процессе копирования, что повысит его качество.

Также следует рассмотреть возможность создания резервной копии следующих элементов.

- База данных аудита
- Временные файлы аудита
- Пользовательские приложения

Необходимо проводить резервное копирование всех пользовательских приложений и настроек при каждом их изменении.

- Подключения к базе данных

11.1.2 Резервное копирование настроек сервера

Чтобы защитить систему от неправильно настроенных параметров сервера, рекомендуется регулярное резервное копирование параметров сервера в файл BIAR. Наличие доступных резервных копий сервера позволяет восстанавливать параметры без необходимости восстановления системной базы данных CMS, репозитория файлов или содержимого Business Intelligence.

Необходимо выполнять резервное копирование параметров сервера каждый раз при внесении изменений в топологию системы. Включает в себя создание, переименование, перемещение и удаление узлов, а также создание или удаление серверов. Рекомендуется выполнять резервное копирование параметров сервера перед внесением каких-либо изменений в параметр, а затем еще раз после окончательного утверждения внесенных изменений.

Используйте Central Configuration Manager (CCM) или скрипт, чтобы выполнить резервное копирование параметров сервера платформы BI в файл BIAR, а затем сохраните файл на отдельном компьютере. Рекомендуется выполнять резервное копирование параметров сервера каждый раз при изменении параметров.

Примечание:

Если выполняется резервное копирование или восстановление параметров сервера с включенным протоколом SSL, необходимо сначала отключить протокол SSL с помощью CCM, а по завершении резервного копирования или восстановления снова включить его.

В Windows скрипт `BackupCluster.bat` расположен в каталоге `<INSTALLDIR>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\scripts`.

В UNIX скрипт `backupcluster.sh` расположен в каталоге `/<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform64>/scripts`.

См. также

- [Настройка протокола SSL](#)

11.1.2.1 Чтобы выполнить резервное копирование параметров сервера, используя CCM на Windows

Эта процедура выполняет резервное копирование параметров сервера для всего кластера. Нельзя выполнять резервное копирование параметров для отдельных серверов.

Примечание:

Если используется временный CMS, необходимо запустить CCM на компьютере, на котором есть локальный CMS.

1. Запустите CCM и на панели инструментов щелкните **Резервное копирование конфигурации сервера**.

Откроется «Мастер резервного копирования конфигурации сервера».

2. Чтобы запустить мастер, нажмите кнопку **Далее**.

3. Укажите, следует ли использовать существующий CMS для резервного копирования конфигурации параметров сервера, или же следует создать временный CMS.

- Чтобы выполнить резервное копирование параметров сервера из запущенной системы, выберите **Использовать существующий работающий CMS**, а затем нажмите кнопку **Далее**.
- Чтобы выполнить резервное копирование параметров сервера из неактивной системы, выберите команду **Запуск нового временного CMS**, а затем нажмите кнопку **Далее**.

4. Если используется временный CMS, выберите номер порта для запуска CMS и укажите сведения о подключении базы данных.

Чтобы минимизировать риск доступа пользователей к системе во время резервного копирования или восстановления, укажите номер порта, отличный от номеров порта, используемых существующими CMS.

5. При запросе войдите в CMS, указав системные и пользовательские имя и пароль для учетной записи с административными правами, а затем нажмите кнопку **Далее**, чтобы продолжить.

6. Укажите расположение и имя файла BIAR, для которого нужно выполнить резервное копирование параметров конфигурации сервера, а затем щелкните **Далее**, чтобы продолжить. Окно «Подтверждение» отображает предоставленную информацию.

7. Убедитесь, что информация, отображенная в окне «Подтверждение» верна, а затем щелкните **Готово**, чтобы продолжить.

CCM выполняет резервное копирование параметров конфигурации сервера для всего кластера в указанный файл BIAR. Подробные сведения о процедуре резервного копирования записываются в файл журнала. Имя файла журнала и путь к нему отображаются в диалоговом окне.

8. Если во время операции резервного копирования произошел сбой, проверьте файл журнала для установления причины.
9. Нажмите кнопку **ОК**, чтобы закрыть мастер.

11.1.2.2 Резервное копирование параметров сервера в ОС UNIX

На компьютерах под управлением UNIX используйте скрипт `serverconfig.sh` для резервного копирования параметров сервера развертывания в файл BIAR.

1. Выберите пункт "5 – резервное копирование сервера" и нажмите клавишу Enter.
2. Укажите, следует ли использовать существующий CMS для резервного копирования конфигурации параметров сервера, или же следует создать временный CMS.
 - Чтобы выполнить резервное копирование параметров сервера из активной системы, выберите элемент **существующий** и нажмите клавишу Enter.
 - Чтобы выполнить резервное копирование параметров сервера из неактивной системы или восстановить параметры сервера, выберите элемент **временный** и нажмите клавишу Enter.
3. Если для резервного копирования параметров сервера используется временный сервер CMS, на следующих экранах выберите номер порта, на котором будет выполняться временный сервер CMS, а также сведения о соединении с базой данных системы CMS.

Чтобы минимизировать риск доступа пользователей к системе во время резервного копирования или восстановления, укажите номер порта, отличный от номеров порта, используемых существующими CMS.
4. При выводе соответствующего запроса выполните вход в CMS, указав систему, имя пользователя и пароль для учетной записи с административными правами, а затем нажмите клавишу Enter.
5. При выводе соответствующего запроса укажите местоположение и имя файла BIAR, в который требуется скопировать конфигурацию сервера, и нажмите клавишу Enter.

Предоставленные сведения будут отображены на экране сводки.
6. Проверьте правильность отображаемой информации и нажмите клавишу Enter, чтобы продолжить.

Скрипт `serverconfig.sh` выполняет резервное копирование параметров конфигурации сервера для всего кластера в указанный файл BIAR. Подробные сведения о процедуре резервного копирования записываются в файл журнала. Имя и путь файла журнала отображаются на экране.
7. Если во время операции резервного копирования произошел сбой, проверьте файл журнала для установления причины.

11.1.2.3 Резервное копирование параметров серверов с использованием скрипта

Можно выполнить резервное копирование параметров сервера своего развертывания путем выполнения скрипта `backupcluster.bat` в ОС Windows или скрипта `BackupCluster.sh` в ОС UNIX.

В ОС Windows файл `BackupCluster.bat` расположен в каталоге `<INSTALLDIR>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\scripts`.

На компьютерах под управлением ОС UNIX файл `backupcluster.sh` расположен в каталоге `/<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform64>/scripts`.

Сведения об используемых скриптом параметрах см. в разделе [Параметры BackupCluster и RestoreCluster](#).

11.1.3 Резервное копирование содержимого Business Intelligence

Рекомендуется при помощи консоли управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence 4.0 регулярно выполнять резервное копирование содержимого Business Intelligence, такого как отчеты, пользователи и группы, а также юниверсы. Наличие актуальных копий содержимого позволяет восстановить систему Business Intelligence без восстановления параметров всей системы или сервера.

Для получения дополнительных сведений об использовании консоли управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence 4.0 см. *Руководство пользователя консоли управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence 4.0*.

Если используется вспомогательная версия консоли управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence 4.0, см. главу «Резервное копирование файлов вспомогательных версий» в документе *Руководство пользователя консоли управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence 4.0*, в которой приведены дополнительные сведения о резервном копировании репозитория вспомогательной версии.

11.1.4 Восстановление системы

Процедура восстановления системы будет зависеть от того, утеряны ли (либо повреждены) базы данных системы CMS, репозитории входных и выходных файлов или файловая система компьютера, на котором установлена платформа SAP BusinessObjects Business Intelligence, а также от наличия доступных резервных копий этих компонентов.

- Если база данных системы CMS повреждена или утеряна, и доступны резервные копии базы данных системы и репозитория файлов, см. [Восстановление системы платформы SAP BusinessObjects Business Intelligence при наличии резервных копий](#).

- Если база данных системы CMS повреждена или утеряна, а резервные копии базы данных и репозитория файлов отсутствуют, но есть резервная копия содержимого Business Intelligence в файле BIAR, см. [Повторное создание платформы SAP BusinessObjects Business Intelligence при отсутствии резервной копии](#).
- Если репозитории файлов повреждены или утеряны и имеются резервные копии базы данных системы CMS и репозитория файлов, см. [Восстановление системы платформы SAP BusinessObjects Business Intelligence при наличии резервных копий](#).
- Если репозитории файлов повреждены или утеряны, а резервные копии базы данных системы CMS и репозитория файлов недоступны, но имеется резервная копия файла BIAR, см. [Повторное создание платформы SAP BusinessObjects Business Intelligence при отсутствии резервной копии](#).
- Если серверы настроены неверно и требуется выполнить откат всей системы к предыдущему состоянию при наличии резервных копий базы данных системы CMS и репозитория файлов, см. [Восстановление системы платформы SAP BusinessObjects Business Intelligence при наличии резервных копий](#).

Перед восстановлением базы данных системы CMS или репозитория файлов необходимо:

1. Остановите работу платформы SAP BusinessObjects Business Intelligence.
2. Выполните резервное копирование базы данных системы CMS и репозитория файлов.

Примечание:

Если резервные копии базы данных системы CMS и репозитория файлов отсутствуют, параметры конфигурации сервера не были сохранены в файле BIAR, а репозитории файлов были сохранены в файле LCMBIAR, восстановление системы невозможно.

См. также

- [Repository Diagnostic Tool](#)

11.1.4.1 Восстановление системы платформы SAP BusinessObjects Business Intelligence при наличии резервных копий

Этот рабочий процесс подразумевает наличие:

- Доступная резервная копия базы данных системы CMS
- Доступная резервная копия репозитория файлов

В случае утраты или повреждения базы данных системы CMS или репозитория файлов восстановите базу данных системы CMS и репозитории файлов из текущих резервных копий.

Примечание:

При восстановлении базы данных системы CMS или репозитория файлов из резервной копии необходимо восстановить базу данных и репозитории файлов из резервных копий, созданных в одно и то же время. Чтобы обеспечить отсутствие несогласованностей между CMS и репозиториями файлов, не восстанавливайте их по отдельности. Для восстановления системной

базы данных CMS используются средства резервного копирования и восстановления от поставщика базы данных. Восстановление файловых репозиторий включает восстановление из резервной копии файлов, расположенных в папках, которые указаны в свойствах «Каталог хранилища файлов» на серверах репозиторий входящих и исходящих файлов. Восстановление должно выполняться с использованием одного из средств резервного копирования и восстановления файловой системы.

При восстановлении базы данных системы CMS или репозиторий файлов необязательно восстанавливать файловую систему компьютера, на котором установлена платформа BI.

1. Восстановите базу данных системы CMS из доступной резервной копии.
2. Восстановите репозитории файлов из доступной резервной копии.

Примечание:

Можно восстанавливать оба компонента параллельно для уменьшения времени простоя.

Система платформы BI восстанавливается в том же состоянии, в котором она находилась при создании резервной копии, включая содержимое системы, пользователей и параметры сервера.

После завершения восстановления:

1. Запустите инструмент диагностики репозитория, чтобы обеспечить отсутствие несогласованностей между базой данных системы CMS и репозиториями файлов. Для получения дополнительных сведений об инструменте диагностики репозитория см. *Руководство пользователя инструмента диагностики репозитория платформы SAP BusinessObjects Business Intelligence*.
2. Запустите платформу BI и проверьте ее работу.

Очередность запуска платформы BI и инструмента диагностики репозитория будет зависеть от того, насколько важно как можно быстрее вернуть систему в интерактивное состояние. Несогласованности, обнаруженные инструментом диагностики репозитория, не будут разрешены до завершения работы инструмента диагностики репозитория.

11.1.4.2 Повторное создание платформы SAP BusinessObjects Business Intelligence при отсутствии резервной копии

Если база данных системы CMS или репозитории файлов утеряны или повреждены, а резервные копии недоступны, можно воссоздать систему при наличии резервной копии параметров сервера в файле BIAR и резервной копии содержимого Business Intelligence в файле LCMBIAR.

1. В Central Configuration Manager воссоздайте базу данных системы CMS.
База данных системы CMS будет воссоздана в состоянии по умолчанию, с удалением всего существующего содержимого.
2. Восстановите параметры сервера из файла BIAR с помощью Central Configuration Manager или скрипта `RestoreCluster`.
3. Используйте LifeCycle Manager для восстановления содержимого Business Intelligence из файла LCMBIAR.

Для получения дополнительных сведений об использовании LifeCycle Manager см. Руководстве пользователя консоли управления жизненным циклом для платформы *SAP BusinessObjects Business Intelligence 4.0*.

См. также

- [Повторное создание базы данных системы центрального сервера управления](#)
- [Восстановление настроек сервера](#)

11.1.4.3 Восстановление настроек сервера

При необходимости восстановления настроек сервера системы из файла BIAR можно использовать Central Configuration Manager (CCM) или скрипт RestoreCluster. Восстановление содержимого сервера из файла BIAR не влияет на содержимое Business Intelligence (отчеты, пользователи и группы, параметры безопасности).

Примечание:

- В случае восстановления настроек сервера поддерживается только восстановление настроек для всего кластера. Нельзя восстановить настройки только для некоторых серверов кластера.
- Если выполняется резервное копирование или восстановление параметров сервера с включенным протоколом SSL, необходимо сначала отключить протокол SSL с помощью CCM, а по завершении резервного копирования или восстановления снова включить его.

См. также

- [Настройка протокола SSL](#)

11.1.4.3.1 Восстановление настроек сервера с помощью CCM под ОС Windows

Для восстановления настроек сервера можно использовать Central Configuration Manager (CCM). Когда настройки сервера восстановлены, необходимо повторно создать узлы системы на каждом компьютере кластера.

1. Остановите все узлы на всех компьютерах кластера, для которого восстанавливаются параметры конфигурации сервера, остановив агент SIA для каждого из этих узлов.
2. Запустите CCM на компьютере с CMS.
3. На панели инструментов выберите кнопку **Восстановление конфигурации сервера**. Появится окно «мастера восстановления конфигурации сервера».
4. Для запуска мастера нажмите кнопку **Далее**.
5. После приглашения укажите номер порта, используемый для временного центрального сервера управления (CMS), а также данные для соединения с системной базой данных CMS, затем нажмите кнопку **Далее** для продолжения.

6. После запроса выполните вход в систему CMS, указав имя пользователя и пароль CMS учетной записи с правами администратора. Чтобы продолжить нажмите кнопку **Далее**.
7. Укажите расположение и имя файла BIAR, содержащего параметры конфигурации сервера, которые требуется восстановить, и нажмите кнопку **Далее** для продолжения.
Появится экран со сводкой предоставленной информации.
8. Нажмите кнопку **Готово**, чтобы продолжить.
Сообщение с предупреждением о том, что существующие настройки сервера будут перезаписаны значениями, указанными в файле BIAR. В случае выполнения этой процедуры текущие настройки сервера будут потеряны.
9. Нажмите кнопку **Да**, чтобы восстановить параметры конфигурации сервера.
CCM восстанавливает параметры конфигурации сервера из файла BIAR для всего кластера. Сведения о выполнении операции записываются в файл журнала. Имя файла журнала и путь к нему показываются в диалоговом окне.
10. Если во время операции восстановления произошел сбой, проверьте файл журнала для установления причины.
11. Нажмите кнопку **ОК**, чтобы закрыть мастер.

В системе восстановлены настройки сервера из файла BIAR. Созданы все узлы и серверы, существующие в файле BIAR, но отсутствовавшие в системе до восстановления. Удалены все узлы и серверы, существовавшие в системе, но отсутствующие в файле BIAR.

После восстановления настроек сервера для всего кластера необходимо повторно создать узлы системы на каждом компьютере в этом кластере.

См. также

- [Восстановление узла](#)

11.1.4.3.2 Восстановление параметров сервера с помощью CCM в UNIX

На компьютерах под управлением UNIX используйте скрипт `serverconfig.sh` для восстановления параметров сервера развертывания из файла BIAR.

1. Выберите "6 – Восстановить конфигурацию сервера" и нажмите клавишу Enter.
2. Введите номер порта для использования временным сервером CMS и нажмите клавишу Enter.
3. На следующих нескольких экранах укажите сведения о подключении к базе данных системы CMS.
4. При выводе соответствующего приглашения выполните вход в CMS, указав систему, имя пользователя и пароль для учетной записи с административными правами, а затем нажмите клавишу Enter.
5. При выводе соответствующего приглашения укажите местоположение и имя файла BIAR, из которого требуется восстановить конфигурацию сервера, и нажмите клавишу Enter
Предоставленные сведения будут отображены на экране сводки.
6. Проверьте правильность отображаемой информации и нажмите кнопку..., чтобы продолжить.

Скрипт `serverconfig.sh` восстанавливает параметры конфигурации сервера для всего кластера из указанного файла BIAR. Подробности процедуры восстановления записываются в файл журнала. Имя и путь файла журнала отображаются на экране.

7. Если во время операции восстановления произошел сбой, проверьте файл журнала для установления причины.

11.1.4.3.3 Восстановление параметров сервера с помощью скрипта

При желании можно восстановить параметры сервера в развертывании посредством выполнения скрипта `RestoreCluster.bat` в Windows или скрипта `restorecluster.sh` в UNIX.

В Windows файл `RestoreCluster.bat` расположен в каталоге `<INSTALLDIR>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\scripts`.

В UNIX файл `backupcluster.sh` расположен в каталоге `/<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform64>/scripts`.

Сведения о параметрах, используемых данным скриптом, см. в разделе [Параметры BackupCluster и RestoreCluster](#).

11.1.4.4 Восстановление содержимого Business Intelligence

При наличии резервной копии содержимого Business Intelligence в файлах LCMBIAR содержимое можно восстановить без необходимости восстановления всей системы с использованием консоли управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence 4.0. Для получения дополнительных сведений см. Руководство пользователя платформы *Lifecycle management console for SAP BusinessObjects Business Intelligence 4.0*

11.1.5 Восстановление утерянных или поврежденных файлов платформы SAP BusinessObjects Business Intelligence 4.0 при наличии резервной копии

Если база данных системы CMS и репозитории файлов находятся в рабочем состоянии, однако файлы конфигурации платформы SAP BusinessObjects Business Intelligence утрачены или повреждены, при наличии резервных копий файлов можно восстановить с их помощью файловую систему. При восстановлении файловой системы необходимо восстановить базу данных системы CMS и репозитории файлов.

11.1.6 Повторное создание платформы SAP BusinessObjects Business Intelligence при утрате файлов

Эта процедура предполагает наличие следующих элементов:

- Резервной копии базы данных системы CMS
- Резервной копии содержимого серверов репозитория файлов

Если файловая система компьютера, на котором установлена платформа SAP BusinessObjects Business Intelligence, утрачена или повреждена, а резервная копия файловой системы отсутствует, можно выполнить попытку восстановления посредством переустановки платформы SAP BusinessObjects Business Intelligence на тот же самый или на другой компьютер.

1. Выполните новую установку платформы SAP BusinessObjects Business Intelligence с теми же параметрами, что и оригинальная. Новая установка должна иметь столько же узлов, сколько в исходной установке. Имена узлов должны быть такими же, как имена узлов в исходной установке. Необходимо установить платформу SAP BusinessObjects Business Intelligence в ту же папку, что использовалась для исходной установки. При установке платформы SAP BusinessObjects Business Intelligence укажите в качестве базы данных существующую базу данных CMS.

Примечание:

Если в процессе установке выбрана существующая база данных системы CMS, на экране «Настройка базы данных репозитория CMS» необходимо снять флажок **Сбросить существующую базу данных**. Если этот флажок установлен, будет удалено все содержимое существующей базы данных.

2. Восстановите репозитории файлов из доступной резервной копии.

11.1.7 Параметры BackupCluster и RestoreCluster

В следующей таблице описываются параметры командной строки, используемые скриптом BackupCluster.

Таблица 11-1: Параметры BackupCluster

Название	Описание	Пример
-backup	Имя и расположение BIAR-файла, в который планируется скопировать параметры сервера системы для восстановления.	-backup "C:\Users\Administrator\Desktop\my.biar"

Название	Описание	Пример
-cms	Имя хоста, на котором находится центральный сервер управления. Если порт, на котором работает центральный сервер управления, отличается от порта по умолчанию (6400), необходимо также указать номер порта.	-cms mycms:6400
-username	Имя пользователя учетной записи администратора.	-username Administrator
-password	Пароль учетной записи администратора.	-password Password1

В следующей таблице описываются параметры командной строки, используемые скриптом `RestoreCluster`.

Таблица 11-2: Параметры `RestoreCluster`

Название	Описание	Пример
-restore	Расположение и имя файла BIAR, содержащего параметры конфигурации сервера, которые требуется восстановить.	-restore "C:\Users\Administrator\Desktop\my.biar"
-username	Имя пользователя учетной записи администратора.	-username Administrator
-password	Пароль учетной записи администратора.	-password Password1
-displaycontents	Отображение списка узлов и серверов, которые содержатся в BIAR-файле.	-displaycontents "C:\Users\Administrator\Desktop\my.biar"

Примечание:

Рекомендуется выполнить скрипт `RestoreCluster` с параметром `-displaycontents` для отображения содержимого BIAR-файла перед восстановлением параметров сервера.

Приведенные ниже параметры требуются при резервном копировании параметров сервера из незапущенной системы, а также при восстановлении параметров сервера.

Таблица 11-3: Параметры при использовании временного центрального сервера управления

Название	Описание	Пример
<code>-usetempcms</code>	Создание временного центрального сервера управления для указанной операции. По завершении операции временный центральный сервер управления будет остановлен.	<code>-usetempcms</code>
<code>-cmsport</code>	Номер порта временного центрального сервера управления.	<code>-cmsport 6400</code>
<code>-dbdriver</code>	Драйвер системной базы данных центрального сервера управления. Допустимы следующие значения: <ul style="list-style-type: none"> • <code>db2databasesubsystem</code> • <code>maxdbdatabasesubsystem</code> • <code>mysqldatabasesubsystem</code> • <code>oracledatabasesubsystem</code> • <code>sqlserverdatabasesubsystem</code> • <code>sybasedatabasesubsystem</code> 	<code>-dbdriver sqlserverdatabasesubsystem</code>
<code>-connect</code>	Строка подключения к системной базе данных центрального сервера управления. Примечание: В связи с ограничениями командной строки необходимо использовать управляющий символ крышки (^) перед пробелами, знаками равенства (=) и точками с запятой (;) в строке <code>-connect</code> . Чтобы избежать использования символа крышки в длинных строках, можно записать имя скрипта и все его параметры во временный файл <code>response.bat</code> и затем выполнить этот файл <code>response.bat</code> без параметров.	<code>-connect "DSN^=BusinessObjects^ CMS^ 10Data Provider, CSMP, OR-35</code>

Название	Описание	Пример
-dbkey	Ключ кластера.	-dbkey abc1234

Пример:

В следующем примере показано, как выполнить резервное копирование параметров сервера в BIAR-файл с использованием центрального сервера управления.

```
-backup "C:\Users\Administrator\Desktop\my.biar"  
-cms mycms:6400  
-username Administrator  
-password Password1
```

Пример:

В следующем примере показано, как отобразить содержимое BIAR-файла.

```
-displaycontents "C:\Users\Administrator\Desktop\mybiar.biar"
```

Пример:

В следующем примере показано, как восстановить параметры из BIAR-файла. При восстановлении параметров сервера необходимо всегда использовать временный центральный сервер управления.

```
-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
```


Управление жизненным циклом

12.1 Консоль управления жизненным циклом

Консоль управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence 4.0 является веб-средством, которое позволяет перемещать ресурсы BI из одной системы в другую систему, не влияя на зависимости этих ресурсов. С его помощью также осуществляется управление различными версиями ресурсов BI и их зависимостями, а также откат перемещенного ресурса для восстановления предыдущего состояния целевой системы.

Консоль управления жизненным циклом является подключаемым программным модулем приложения платформы SAP BusinessObjects Business Intelligence. Можно повысить ресурс BI из одной системы в другую систему только в том случае, если и в исходной, и целевой системах установлена одинаковая версия платформы SAP BusinessObjects Business Intelligence.

В SAP BusinessObjects имеются следующие инструменты для импорта объектов между двумя развертываниями платформы SAP BusinessObjects Business Intelligence одинаковой версии.

- консоль управления жизненным циклом

Для получения дополнительных сведений об использовании консоли управления жизненным циклом см. *Руководство пользователя консоли управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence 4.0*.

- Инструмент командной строки BIAR

Дополнительные сведения об использовании инструмента командной строки BIAR см. в *Руководство пользователя консоли управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence 4.0*.

12.2 Параметры системы управления версиями для консоли управления жизненным циклом

12.2.1 Параметры системы управления версиями для консоли управления жизненным циклом

- Если вместе с платформой SAP BusinessObjects Business Intelligence установлена вспомогательная версия консоли управления жизненным циклом, параметры конфигурации настраиваются автоматически.
- Если требуется настроить уже установленную вспомогательную версию консоли управления жизненным циклом, введите соответствующие значения на странице «Параметры VMS» в **Параметрах администрирования** в инструменте консоли управления жизненным циклом.

На следующем рисунке представлены соответствующие значения для указания на странице «Настройки VMS»:

Системы управления версиями Вспомогательная версия ▾

Вспомогательная версия Настройки

☒ Использовать в качестве системы управления версиями по умолчанию

Имя сервера	localhost
Порт сервера	3690
Имя пользователя	LCM
Пароль	•••
Путь к каталогу установки	D:\Program Files (x86)\SAP Business
Имя репозитория	svn_repository
Каталог рабочего пространства	D:\checkout

- Если вспомогательная версия консоли управления жизненным циклом установлена позже платформы SAP BusinessObjects Business Intelligence,

Примечание:

Убедитесь, что выполняется служба вспомогательной версии и создан репозиторий.

1. Введите соответствующие значения на странице «Настройки VMS» в окне **Параметры администрирования** консоли управления жизненным циклом.
2. Перезапустите SIA.

12.3 Инструмент командной строки механизма BIAR

Инструмент командной строки BIAR позволяет администратору и лицам с полномочиями администратора распределять содержимое между средами разработки, контроля качества и

рабочей средой платформы SAP BusinessObjects Business Intelligence. Данный инструмент использует скрипты для автоматизации импорта и экспорта объектов.

Инструмент командной строки механизма BIAR поддерживает миграцию объектов только из одной системы платформы SAP BusinessObjects Business Intelligence 4.0 в другую. Этот инструмент нельзя использовать для импорта объектов из BusinessObjects, Crystal Enterprise или предыдущей версии платформы SAP BusinessObjects Business Intelligence. Для импорта содержимого из предыдущих версий необходимо использовать средство управления обновлениями платформы SAP BusinessObjects Business Intelligence.

Файл инструмента командной строки механизма BIAR называется `biarengine.jar`. В среде Windows этот файл расположен в папке `<InstallDir>\SAP BusinessObjects Enterprise XI 4.0\java\lib`. В среде UNIX этот файл расположен в папке `<InstallDir>/sap_bobj/java/lib/`.

Примечание:

- Для этого требуется установить среду Java Runtime. Список поддерживаемых сред JRE см. в интерактивном руководстве по работе с поддерживаемыми платформами SAP BusinessObjects Business Intelligence на веб-сайте службы поддержки.
- Для использования инструмента командной строки механизма BIAR необходимы учетные данные администратора для среды, в которую или из которой импортируется содержимое. Также можно использовать делегированную учетную запись администратора.
- Использование инструмента командной строки механизма BIAR для импорта файлов BIAR, созданных средством управления обновлениями платформы SAP BusinessObjects Business Intelligence, не поддерживается.

Инструмент командной строки механизма BIAR выполняет импорт следующих типов объектов:

Соединения Analysis	Документы Web Intelligence
Рабочие пространства Analysis	Пользователи LDAP
Агностические документы	Списки значений
Аналитические объекты	Пакеты объектов
Объекты BI Modeler	Перегрузки
Рабочие пространства BI	PDF-файлы
Business Views	Презентации PowerPoint
Календари	Профили
Категории	Объекты программ
Действия клиента	Группы приглашений
Пользовательское правило	Публикации
Документы Dashboard Design	Запросы в виде веб-сервисов
Дискуссии	Отчеты
Энциклопедии	Экземпляры отчета
Пользовательские группы Enterprise	Документы в формате RTF
Корпоративные пользователи	Группы серверов
События	Комбинации клавиш
Электронные таблицы Excel	Текстовые файлы
Файлы Flash	Юниверсы
Папки	Пользователи WinAD
FullClientAddins	Документы Word
FullClientTemplates	XcelsiusDMTTemplates
Гиперссылки	

Импорт взаимосвязи

Инструмент командной строки механизма BIAR сохраняет взаимоотношения между импортированными объектами только в том случае, если оба объекта импортированы вместе, или если один из объектов уже существует в целевой системе. Например, если имеется отчет Web Intelligence, использующий юниверс, то при импорте этого отчета без импорта юниверса взаимосвязь между ними оказывается разорвана. Такой отчет не будет выполняться в целевой системе.

Импорт пользователей и групп

Если при импорте групп и пользователей в систему платформы SAP BusinessObjects Business Intelligence группа уже существует в целевой системе, то сведения о принадлежности к группе в целевой системе будут перезаписаны сведениями, экспортированными из файла BIAR. Таким образом, если в целевой системе к данной группе принадлежат дополнительные пользователи, которые не содержатся в группе в файле BIAR, после импорта они не будут частью группы.

Импорт прав

Инструмент командной строки механизма BIAR импортирует права на объект только в том случае, если пользователь или группа экспортированы с объектом или уже существуют в месте назначения.

Если объект и пользователь или группа существуют в целевой системе, то импортированные права для данного объекта и пользователя перезапишут существующие права в целевой системе.

Однако если объект уже существует в целевой системе, где для него заданы права пользователя/группы, но в файле BIAR права этого пользователя/группы для объекта не заданы, инструмент не удаляет существующие права данного пользователя/группы.

Это означает, что существующие права на целевой объект могут быть перезаписаны, но не удалены.

Использование нескольких файлов BIAR

При использовании инструмента командной строки BIAR для экспорта содержимого это содержимое помещается в файл BIAR. Местоположение и имя файла BIAR определяется параметром *exportBiarLocation*. При экспорте содержимого, объем которого превышает допустимый для сохранения в одном файле BIAR, данный инструмент разделяет эту информацию и сохраняет ее в нескольких файлах BIAR. Для файлов используется заданное вами имя, после которого добавляются порядковые номера.

Например, если в настройках указать следующее: `exportBiarLocation = C:\Archive.biar`, и при этом экспортировать содержимое, которое по объему превышает вместимость одного файла BIAR, то данный инструмент создаст файлы `Archive.biar`, `Archive1.biar`, `Archive2.biar` и т. д. Инструмент создает файлы в каталоге `C:`.

Примечание:

Если необходимо импортировать содержимое, сохраненное в нескольких файлах BIAR, убедитесь в том, что все файлы BIAR расположены в одном каталоге.

12.3.1 Использование файла свойств

Для инструмента командной строки механизма BIAR требуется файл свойств, содержащий параметры, которые сообщают механизму BIAR, какие действия выполнить, к какой системе платформы SAP BusinessObjects Business Intelligence подключиться и т. п.

Данный файл должен обладать расширением `.properties`. Например:
`Myproperties.properties`

Файл свойств может содержать следующие параметры.

Параметр	Разрешенные значения	Описание	Например
<code>Action</code>	<code>exportXML</code> , <code>importXML</code>	Указывает, выполняет ли этот инструмент импорт содержимого из файла BIAR в систему платформы SAP BusinessObjects Business Intelligence или экспорт содержимого из развертывания в файл BIAR. Обязательно	<code>Action=exportXML</code>
<code>exportBiarLocation</code>	Текст произвольного формата. Должен содержать расширение <code>.biar</code> .	Указывает, где инструмент сохраняет экспортированный файл BIAR. Является обязательным при значении <code>action=exportXML</code> .	<code>exportBiarLocation=C:\BiaExport\Biar</code>
<code>importBiarLocation</code>	Текст произвольного формата. Должен содержать расширение <code>.biar</code> .	Указывает местоположение файла BIAR, предназначенного для импорта. Файлы BIAR разбиваются на несколько частей, если их содержимое слишком велико для файла BIAR. Можно ввести любые разделы файлов BIAR, однако необходимо убедиться, что все эти разделы находятся в одном каталоге. Является обязательным при значении <code>action=importXML</code> .	<code>importBiarLocation=C:\BiaImport\Biar</code>

Параметр	Разрешенные значения	Описание	Например
<i>userName</i>	Текст произвольного формата.	Имя пользователя учетной записи с правами администратора, которую инструмент должен использовать для подключения к Центральному серверу управления (CMS). Это может быть имя пользователя, относящееся к учетной записи делегированного администратора. Обязательно	userName=Administrator
<i>password</i>	Текст произвольного формата.	Пароль учетной записи с правами администратора. Обязательно	password=password
<i>аутентификация</i>	secEnterprise, secWinAd, secLdap	Используемый инструментом тип аутентификации. Необязательно. Если тип аутентификации не указан, по умолчанию используется значение secEnterprise.	аутентификация=secEnterprise
<i>CMS</i>	Текст произвольного формата.	Имя CMS, к которому нужно подключиться. Обязательно	CMS=mycms:6400

Параметр	Разрешенные значения	Описание	Например
<i>exportDependencies</i>	True, False	<p>Определяет, будут ли импортироваться все элементы, зависящие от объекта. При использовании данного параметра необходимо соблюдать осторожность, поскольку он активирует импорт всех объектов, связанных с выбранным объектом. В этом случае размер файла BIAR может значительно возрасти.</p> <p>Необязательно. Если значение не указано, по умолчанию используется значение False.</p> <p>Используется, только если задано значение <code>action=exportXML</code>.</p>	<code>exportDependencies=false</code>

Параметр	Разрешенные значения	Описание	Например
<i>includeSecurity</i>	True, False	<p>Указывает, будет ли инструмент экспортировать и импортировать настройки защиты, связанные с выбранными объектами и пользователями. Если настройки защиты необходимо сохранить, обязательно задайте для параметра <i>includeSecurity</i> значение "True" при экспорте и импорте содержимого.</p> <p>Примечание: При использовании уровней доступа необходимо экспортировать эти объекты явным образом.</p> <p>Необязательно. Если для данного параметра не указано значение, по умолчанию используется значение True.</p>	includeSecurity=false
<i>exportQuery</i>	Текст произвольного формата. Необходимо использовать формат запроса CMS.	<p>Указывает запросы, которые инструмент должен выполнить для сбора объектов, предназначенных для экспорта.</p> <p>В одном файле свойств можно использовать любое количество запросов, однако их имена должны быть следующими: «exportQuery1», «exportQuery2» и т.д.</p> <p>Является обязательным при значении action=exportXML.</p>	exportQuery=выберите * из ci_Infoobjects, где si_name = 'Xtreme Employees' и si_kind = 'Webi'

Параметр	Разрешенные значения	Описание	Например
<i>exportQueriesTotal</i>	Положительные целые числа.	<p>Определяет количество запросов на экспорт, которое выполняет инструмент. Если при наличии запросов на экспорт в количестве «х» нужно выполнить все эти запросы, то для данного параметра нужно задать значение «х».</p> <p>Необязательно. Если для данного параметра не указано значение, по умолчанию используется значение 1.</p> <p>Используется, только если задано значение <code>action=exportXML</code>.</p>	<code>exportQueriesTotal=5</code>

Примечание:

Для добавления комментариев к строкам используйте символ #. Например:

```
action=importXML
#exportLocation=C:/mybiar.biar
importLocation=C:/mybiar.biar
```

Это пример файла свойств для импорта содержимого из файла BIAR.

```
#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
```

Это пример файла свойств, выполняющего экспорт отчета Web Intelligence под именем «Xtreme Employees» в файл BIAR:

```
#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 Использование инструмента командной строки механизма BIAR

1. Откройте окно командной строки и перейдите в каталог, в котором располагается файл `biarengine.jar`.

Например, `<InstallDir>\SAP BusinessObjects Enterprise XI4.0\java\lib`.

2. Выполните файл `biarengine.jar`.

Например, `java -jar biarengine.jar <файл_свойств>`

Инструмент командной строки BIAR выполняет экспорт содержимого из развертывания платформы SAP BusinessObjects Business Intelligence в файл BIAR или импорт содержимого из файла BIAR в развертывание платформы SAP BusinessObjects Business Intelligence в зависимости от параметра действия, указанного в файле свойств.

Управление приложениями

13.1 Управление приложениями с помощью CMC

13.1.1 Обзор

Область CMC «Приложения» позволяет без программирования изменять внешний вид и функциональность веб-приложений, таких, как CMC и стартовая панель BI. Также вы сможете изменить доступ к этим приложениям для пользователей, групп и администраторов, изменяя права, связанные с каждым приложением.

В этом разделе содержится информация, процедуры и инструкции о выполнении различных настроек. Настройки следующих приложений можно изменить с помощью CMC:

- Analysis, выпуск для OLAP
- Оповещение
- стартовая панель BI
- Рабочие пространства BI
- Central Management Console
- Crystal Reports
- Dashboard Design
- Дискуссии
- Дизайнер информации
- Web Intelligence
- LifeCycle Manager
- Мониторинг
- OpenDocument
- Поиск по платформе
- Средство преобразования отчетов
- SAP BusinessObjects Mobile
- Средство управления переводами
- Средство создания юниверсов
- Средство управления обновлением
- Приложение VisualDiff

- Веб-служба
- Виджеты для платформы SAP BusinessObjects Business Intelligence

13.1.2 Общие настройки приложений

13.1.2.1 Настройка пользовательских прав на приложения

Для контроля доступа пользователей к некоторым функциям приложений можно использовать права. Область «Приложения» в СМС позволяет присвоить принципалов списку управления доступом для приложения, просмотреть права принципала и изменить права принципала на доступ к приложению. Для получения дополнительной информации об администрировании прав см. *Руководство администратора платформы SAP BusinessObjects Business Intelligence*.

13.1.2.2 Настройка уровня журнала трассировки веб-приложения в СМС

По умолчанию для уровня журнала трассировки для веб-приложений в СМС установлено значение «Не определен». Настройки журнала трассировки доступны для следующих приложений в СМС:

- Central Management Console
- Стартовая панель BI
- Открыть документ
- Веб-служба

Для трассировки всех остальных веб-приложений следует использовать метод настройки вручную соответствующего файла `BO_Trace`.

1. Перейдите в область управления «Приложения» в СМС.
Будет открыто диалоговое окно «Приложения».
2. Щелкните приложение правой кнопкой мыши и выберите команду **Настройки журнала трассировки**.
Будет открыто диалоговое окно «Настройки журнала трассировки».
3. Выберите нужный параметр в раскрывающемся списке **Уровень журнала**.
4. Нажмите кнопку **Сохранить и закрыть**, чтобы применить уровень журнала трассировки.

Новый уровень журнала трассировки вступит в силу после следующего входа в данное веб-приложение.

См. также

- [Уровни журнала трассировки](#)

13.1.2.2.1 Уровни журнала трассировки

В следующей таблице описаны доступные уровни журнала трассировки для компонентов платформы BI:

Уровень	Описание
Не определен	Уровень журнала трассировки устанавливается с использованием другого механизма, обычно файла <code>.ini</code> .
Нет	<p>Если для журнала трассировки установлен уровень «Нет», фильтр дополнительного подавления трассировки ниже заданного уровня важности отключен.</p> <p>Примечание: Уровень журнала трассировки «Нет» не означает отключения функции трассировки. Отслеживание системных ресурсов продолжается, а трассировки будут протоколироваться для редких критических событий, таких как нарушения утверждений.</p>
Низкий	<p>Фильтр журнала трассировки настроен на регистрацию сообщений об ошибках и пропуск предупреждений и большинства сообщений о статусе. Тем не менее, будут регистрироваться очень важные сообщения о статусе запуска компонента, завершения работы, а также сообщения о начале и завершении запроса.</p> <p>Примечание: Этот уровень не рекомендуется для целей отладки.</p>
Средний	<p>Фильтр журнала трассировки настроен на включение сообщений об ошибках, предупреждениях и большинства сообщений о статусе в выходной файл журнала. Менее важные или очень подробные сообщения о статусе отфильтровываются. Этот уровень не достаточно детальный для использования в целях отладки.</p>
Высокий	<p>Никакие сообщения не исключаются фильтром. Этот уровень рекомендуется для использования в целях отладки.</p> <p>Примечание: «Высокий» уровень трассировки в журнале может отрицательно отразиться на системных ресурсах. Он может увеличить загрузку ЦП и памяти в файловой системе.</p>

13.1.3 Настройки, зависящие от приложения

13.1.3.1 Управление настройками приложения СМС

13.1.3.1.1 Аутентификация и программные объекты

Необходимо знать потенциальные угрозы для безопасности, связанные с добавлением программных объектов в репозиторий. Требуемый уровень полномочий на доступ к файлу для учетной записи, под которой выполняется программный объект, определяет, какие изменения программа может вносить файл.

Можно управлять типами программных объектов, которые могут запускать пользователи, и настраивать реквизиты пользователей, необходимые для запуска программных объектов.

Включение и выключение типов программных объектов

В качестве первого уровня безопасности можно настроить доступные программные объекты.

Аутентификация на всех платформах

В области управления «Папки» консоли СМС необходимо настроить реквизиты учетной записи, под которой выполняется программа. Эта функция позволяет администратору настроить отдельную учетную запись пользователя для программы и предоставить ей соответствующие права, чтобы программный объект запускался вместе с этой учетной записью.

Также пользователи, которые добавляют программные объекты в платформу BI, могут присвоить свои учетные данные программному объекту, чтобы программа имела доступ к системе. Поэтому программа будет выполняться под этой учетной записью, а права программы будут ограничены правами пользователя. Если не указывается учетная запись пользователя для программного объекта, он запускается под системной учетной записью по умолчанию, которая обычно имеет права на компьютере, но не в сети.

Примечание:

По умолчанию при планировании выполнения программного объекта задание не удастся выполнить, если не указаны реквизиты. Для предоставления реквизитов по умолчанию выберите **СМС** в области управления «Программные приложения». В меню **Действия** выберите **Права для программного объекта**. Щелкните **Запланировать со следующими реквизитами операционной системы** и введите имя пользователя и пароль по умолчанию.

Аутентификация для программ Java

Платформа BI позволяет настраивать безопасность для всех объектов программы. Для программ Java платформа BI обеспечивает принудительное использование файла политики Java, параметр по умолчанию которого соответствует параметру по умолчанию Java для незащищенного кода. Используйте Инструмент политики Java (доступен вместе с набором Java Development Kit), чтобы изменить файл политики Java в соответствии с вашими потребностями.

Инструмент политики Java имеет две записи на основе кодов. Первая запись относится к SDK Java платформы BI и предоставляет полные права доступа ко всем JAR-файлам платформы BI. Вторая запись на основе кодов применяется для всех локальных файлов. Она использует те же параметры безопасности для незащищенного кода, что и параметр по умолчанию для незащищенного кода.

Примечание:

- Параметры политики Java являются общими для всех серверов выполнения программы, выполняющихся на одном компьютере.

- По умолчанию файл политики Java устанавливается в каталог Java SDK в корневом каталоге установки платформы BI. Например, типичное расположение в системе Windows: C:\Program Files\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\conf\crystal-program.policy

Для включения и выключения типа программного объекта

1. В области «Программные приложения» выберите **Central Management Console**.
2. Выберите **Действия > Права для программного объекта**.
Появится диалоговое окно «Права для программного объекта».
3. В области «Разрешить пользователям» выберите типы программных объектов, которые смогут запускать пользователи.

Можно выбрать **Запускать скрипты/двоичные файлы** или **Выполнять программы Java**.

При выборе **Выполнять программы Java** вы можете также установить или снять флажок напротив параметра **Использовать анонимный режим**. При выборе этого параметра программа Java получит маркер для входа в платформу BI.
4. Нажмите кнопку **Сохранить и закрыть**.

13.1.3.1.2 Регистрация расширений обработки в системе

Примечание:

Эта функция не применяется к документам Web Intelligence.

Перед применением расширений обработки к каким-либо объектам, необходимо открыть доступ к библиотеке кодов любому компьютеру, который будет обрабатывать применимое расписание или просматривать запросы. При установке платформы BI создается папка по умолчанию для расширений обработки на каждом сервере заданий, обработки и приложений отчетов (Report Application Server). Рекомендуется копировать расширения обработки в папку по умолчанию на каждом сервере. Папка по умолчанию в Windows: C:\Program Files\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win32_x86\ProcessExt. В UNIX это каталог sap_bobj/ProcessExt.

Совет:

К файлу расширения обработки можно открыть общий доступ.

В зависимости от функций, которые вы включили в расширение, скопируйте библиотеку на следующие компьютеры:

- Если расширение обработки охватывает только запросы расписания, скопируйте библиотеку на каждый компьютер, выполняющий функции адаптивного сервера заданий.
- Если расширение обработки охватывает только запросы просмотра, скопируйте библиотеку на каждый компьютер, выполняющий функции сервера обработки или RAS в Crystal Reports.
- Если расширение обработки охватывает запросы расписания и просмотра, скопируйте библиотеку на каждый компьютер, выполняющий функции адаптивного сервера заданий, сервера обработки Crystal Reports или сервера RAS.

Примечание:

Если расширение обработки используется только для запросов расписания или просмотра, отправленных определенной группой серверов, необходимо только скопировать библиотеку на каждый сервер обработки в группе.

См. также

- [Совместное использование обработки расширений несколькими серверами](#)

Регистрация расширения обработки в системе

1. Перейдите в область управления «Программные приложения» в СМС.
2. Выберите **Central Management Console**.
3. Выберите **Действия > Расширения обработки**.
Появится диалоговое окно «Расширения обработки: СМС».
4. В поле **Имя** введите имя, под которым будет отображаться расширение обработки.
5. В поле **Местоположение** введите имя файла расширения обработки, а также дополнительную информацию о пути.
 - Если вы скопировали расширение обработки в папку по умолчанию на каждом соответствующем компьютере, просто введите имя файла (не указывая расширение файла).
 - Если вы скопировали расширение обработки в подпапку, расположенную в иерархии на ступень ниже, чем папка по умолчанию, введите местоположение следующим образом:
подпапка/имя файла
6. В поле **Описание** добавьте информацию о расширении обработки.
7. Нажмите кнопку **Добавить**.

Совет:

Чтобы удалить расширение обработки, выберите его из списка **Существующие расширения** и нажмите кнопку **Удалить**. (Убедитесь, что на этом расширении не основано ни одно из повторно выполняемых заданий, поскольку впоследствии любые основанные на нем задания выполнить не удастся.)

8. Нажмите кнопку **Сохранить и закрыть**.
Расширение обработки зарегистрировано в СМС.

Теперь вы можете выбрать его, чтобы применить его логику к каким-либо объектам.

*Совместное использование обработки расширений несколькими серверами***Примечание:**

Эта функция не применима к документам и отчетам Web Intelligence, созданным на платформе BI.

Если требуется поместить все расширения обработки в одно местоположение, можно переопределить каталог расширений обработки по умолчанию для каждого адаптивного сервера заданий, сервера обработки Crystal Reports и RAS. Сначала скопируйте все обрабатываемые

расширения в совместно используемый каталог на сетевом ресурсе, доступном всем серверам. Укажите (или установите) сетевой диск на каждой серверной станции.

Примечание:

Указанные в Windows диски доступны только до перезагрузки компьютера.

Если вы работаете с серверами Windows и UNIX, вы должны скопировать .dll и .so-файлы каждого обрабатываемого расширения в совместно используемый каталог. Кроме того, разделяемый сетевой ресурс должен быть видимым как для компьютеров с операционной системой Windows, так и для UNIX (через Samba или другую систему совместного использования файлов).

В последнюю очередь необходимо изменить командную строку каждого сервера, чтобы изменился каталог обработки расширений, заданный по умолчанию. Для этого введите `-report_ProcessExtPath` *абсолютный путь* в командной строке. Замените *абсолютный путь* на путь к новой папке, используя то соглашение о написании пути к каталогу, которое используется в операционной системе данного сервера (например, `M:\code\extensions`, `/home/shared/code/extensions` и так далее).

Для изменения директории обработки расширений, используемой по умолчанию, остановите работу сервера с помощью СМС. Затем откройте "Свойства" сервера и введите необходимые данные в командной строке. По окончании снова запустите сервер.

13.1.3.2 Управление настройками дискуссии

В области «Приложения» СМС платформы ВІ можно задать настройки на уровне системы для тем дискуссий.

Для приложения «Дискуссии» доступны следующие способы управления и взаимодействия с темами дискуссий, включая:

- Поиск тем дискуссий согласно заданным критериям.
- Сортировка результатов поиска тем дискуссий.
- Удаление тем дискуссий.

Примечание:

Для приложения "Дискуссии" настройка прав пользователей недоступна. Однако вы можете установить права для отдельных отчетов.

13.1.3.2.1 Поиск темы дискуссии

По умолчанию на странице «Дискуссии» отображаются названия всех тем дискуссий. Отображаются только корневые уровни тем.

Для пролистывания списка тем дискуссий используйте кнопки "Предыдущая" и "Следующая". Можно также искать определенную тему или группу тем.

1. Перейдите к области «Приложения» в СМС и выберите пункт **Дискуссии**.

2. Щелкните **Управление > Свойства**.

Открывается диалоговое окно **Управление заметками**.

3. Выберите вариант в списке **Имя поля**.

Действие	Описание
Заголовок темы	Поиск по заголовку темы.
Дата создания	Поиск по дате создания.
Дата последнего изменения	Поиск по дате последнего изменения.
Автор	Поиск по автору.

4. Во втором списке уточните параметры поиска.

Примечание:

При поиске не учитывается регистр символов.

- Если выполняется поиск по параметру **Заголовок темы** или **Автор**, укажите один из следующих параметров во втором поле.

Действие	Описание
является	Поиск любых тем обсуждения, в которых заголовок темы или имя автора полностью соответствуют тексту, введенному в третьем поле.
не является	Поиск любых тем обсуждения, в которых заголовок темы или имя автора не полностью соответствуют тексту, введенному в третьем поле.
содержит	Поиск тем дискуссий, в которых содержится искомая текстовая строка в любой части заголовка темы или имени автора.
не содержит	Поиск тем дискуссий, которые не содержат текстовую строку в любой части заголовка темы.

- Если поиск выполняется по параметру **Дата создания** или **Дата последнего изменения**, выберите один из следующих параметров и укажите дату поиска.

Действие	Описание
перед	Поиск тем обсуждения, которые были созданы или изменены ранее искомой даты.
После	Поиск тем обсуждения, которые были созданы или изменены позднее даты поиска.
между	Поиск тем обсуждения, которые были созданы или изменены в период между двумя датами поиска.

5. Для дальнейшего уточнения параметров поиска используйте третье текстовое поле.

- Если в первых двух полях выбран поиск текста, введите текстовую строку.
- Для выполнения поиска по датам введите одну или несколько дат в соответствующие поля.

6. Нажмите кнопку **Поиск**.

13.1.3.2.2 Сортировка результатов поиска тем дискуссий

При поиске тем дискуссий можно выбирать способы отображения результатов поиска. Например, можно выполнить сортировку результатов в прямом алфавитном порядке и выбрать число отображаемых на странице результатов.

1. Перейдите к области «Приложения» в СМС и выберите пункт **Дискуссии**.

2. Щелкните **Управление > Свойства**.

Открывается диалоговое окно «Управление заметками».

3. В списке **Сортировать по** выберите вариант сортировки.

Действие	Описание
Заголовок темы	Сортировка по заголовкам тем дискуссий.
Дата создания	Сортировка по датам создания тем дискуссий.
Дата последнего изменения	Сортировка по дате последнего изменения тем дискуссий.
Автор	Сортировка по автору определенной темы дискуссии.

4. Во втором списке можно выбрать отображение записей в возрастающем или убывающем порядке.

5. В третьем текстовом поле укажите число отображаемых на одной странице результатов поиска тем дискуссий.

По умолчанию на одной странице отображаются 10 результатов.

6. Щелкните **Поиск**.

13.1.3.2.3 Удаление темы дискуссии

В области «Приложения» СМС в платформе ВІ можно удалить любую тему дискуссии.

1. Перейдите к области «Приложения» в СМС и выберите пункт **Дискуссии**.

2. Щелкните **Управление > Свойства**.

Открывается диалоговое окно «Управление заметками».

3. В списке результатов найдите тему дискуссии, которую требуется удалить, и выделите ее.

4. Щелкните **Удалить**.

13.1.3.3 Управление настройками стартовой панели BI

В области «Приложения» СМС платформы BI можно изменять параметры отображения стартовой панели BI. Для этого откройте **Управление > Свойства**.

При использовании стартовой панели BI пользователям и группам можно предоставить следующие возможности:

- Изменение предпочтений
- Организация каталогов
- Поиск
- Фильтрация списка объектов по типу объекта
- Просмотр папки "Избранное"

Например, если вы создали папки пользователей, используя стандартное соглашение имен, вам может понадобиться отменить возможность организации собственных папок для пользователей.

Примечание:

По умолчанию все пользователи имеют доступ к этим функциям.

13.1.3.3.1 Для изменения параметров отображения стартовой панели BI

1. Перейдите к области «Приложения» в СМС и выберите пункт **стартовая панель BI**.
2. Последовательно выберите **Управление > Свойства**.
Откроется диалоговое окно «Свойства стартовой панели BI».
3. Для включения дискуссий для пользователей стартовой панели BI выберите **Включить дискуссии**.
4. Для включения функции фильтров для планирования выберите **Отображать вкладку "Фильтры" на странице "Расписание"**.
Эта настройка определяет, могут ли пользователи вводить записи или формулы выбора группы при составлении расписания отчета Crystal.
5. Нажмите кнопку **Сохранить и закрыть**.

13.1.3.4 Управление настройками Web Intelligence

Для документов Web Intelligence можно определить, к каким функциям будут иметь доступ пользователи, задав свойства для приложения Web Intelligence.

13.1.3.4.1 Изменение параметров отображения для Web Intelligence

1. Перейдите в область «Программные приложения» в СМС и выберите пункт **Web Intelligence**.
2. Щелкните **Управление > Свойства**.
Появится диалоговое окно «Свойства» с параметрами отображения.
3. Определите любой из следующих параметров отображения:

Действие	Описание
«Измерения и сведения»	Параметры в данной области определяют, как добавленные данные будут отображаться в отчетах. Измените стиль шрифта, цвет текста и цвет фона. Изменения будут автоматически отображаться в окне предварительного просмотра. По завершении работы нажмите кнопку ОК .
«Изменяющиеся значения (числовые меры)»	Параметры в данной области позволяют изменить отображение и форматирование заголовка страницы. Измените стиль шрифта, цвет текста и цвет фона. Изменения будут автоматически отображаться в окне предварительного просмотра. По завершении работы нажмите кнопку ОК .
«Свойства внедренного изображения»	Введите максимальный размер внедренного изображения.
«Свойства режима быстрого отображения»	Введите в соответствующие поля максимальное количество записей по вертикали, по горизонтали, минимальную ширину и высоту страницы, значение заполнения справа и снизу.

4. Нажмите кнопку **Сохранить и закрыть**.

Примечание:

Чтобы вернуть значения отображения по умолчанию, нажмите кнопку **Сброс**.

13.1.3.5 Управление настройками оповещения

В области «Приложения» СМС платформы BI можно задать для оповещений настройки на уровне системы.

Приложение «Оповещение» позволяет управлять доступом пользователей системы к оповещениям и определять его следующим образом.

- Включать папку **Мои предупреждения** для подписчиков на предупреждения
- Включать и форматировать предупреждающие сообщения, пересылаемые по электронной почте
- Настройка предельного числа предупреждений в системе
- Настройка срока действия для предупреждающих сообщений

См. также

- [Настройка пользовательских прав на приложения](#)
- [Управление настройками оповещения](#)

13.1.3.5.1 Изменение свойств места назначения оповещений

1. Перейдите к области «Приложения» в СМС и выберите пункт **Приложение-источник предупреждения**.
2. Выберите **Управление > Свойства**.
Откроется диалоговое окно «Оповещение» с отображением свойств по умолчанию для места назначения.
3. Задайте соответствующие параметры.

Действие	Описание
«Включить мои предупреждения»	Выберите этот параметр, чтобы подписчики на предупреждения получали уведомления в разделе «Мои предупреждения» на странице Стартовая панель VI.
«Включить электронную почту»	Выберите этот параметр, чтобы подписчики на предупреждения получали уведомления по электронной почте. При выборе этого параметра на экране появляются глобальные настройки электронной почты для предупреждений.

Примечание:

Необходимо задать один или оба из указанных выше параметров места назначения.

Если выбрано «Включить электронную почту», доступны для изменения следующие глобальные параметры:

Действие	Описание
«От»	Задаёт адрес электронной почты, с которого отправляются оповещения. Подписчики будут получать предупреждения по электронной почте от заданного отправителя. Рекомендуется использовать действительный адрес электронной почты, известный системе.
«Кому»	Задаёт адреса электронной почты подписчика на предупреждения. Совет: Рекомендуется сохранить для этого параметра заполнитель %SI_EMAIL_ADDRESS%. Если указать конкретный адрес электронной почты или конкретного получателя, то по умолчанию все системные предупреждения будут передаваться на этот указанный адрес электронной почты.
«Копия»	Задаёт получателей копий предупреждений, передаваемых по электронной почте.
«Тема»	Задаёт заголовок темы по умолчанию, используемый в сообщениях электронной почты с системными предупреждениями.
«Сообщение»	Задаёт сообщение по умолчанию, включаемое в сообщения электронной почты с системными предупреждениями.
«Добавить вложение»	Выбор этого параметра позволяет добавлять вложения по умолчанию в сообщения электронной почты с системными предупреждениями. Этот параметр обычно используется для добавления отчётов Crystal Reports по умолчанию, связанных с инициированными предупреждениями.
«Имя файла»	При выборе параметра Добавить вложение следует указать, как должны создаваться имена вложений в сообщениях электронной почты, выбрав или Автоматическое создание , или Конкретное имя .

4. Нажмите кнопку **Сохранить и закрыть**.

См. также

- [Настройка пользовательских прав на приложения](#)
- [Управление настройками оповещения](#)

13.1.3.5.2 Изменение свойств оповещений по умолчанию

1. Перейдите к области «Приложения» в СМС и выберите пункт **Приложение-источник предупреждения**.
2. Выберите **Управление > Свойства > Параметры по умолчанию**.
3. Присвойте соответствующие значения следующим свойствам:

Действие	Описание
«Срок действия»	Указывает срок хранения предупреждающих сообщений в системе до того, как они будут удалены.
«Максимальное число предупреждающих сообщений»	Максимальное число предупреждающих сообщений, поддерживаемое системой. При достижении этого порога система удаляет 20% предупреждений, начиная с самых старых.

4. Нажмите кнопку **Сохранить и закрыть**.

См. также

- [Управление настройками безопасности для объектов в СМС](#)
- [Управление настройками оповещения](#)

13.1.3.6 Управление настройками виджетов

Виджеты для SAP BusinessObjects – это приложение, позволяющие пользователям добавлять мини-приложения на свой рабочий стол для упрощения доступа к содержимому business intelligence в платформе BI и приложениях Web Dynpro на серверах приложений SAP NetWeaver.

Из области СМС "Приложения" можно управлять доступом пользователей для создания и использования виджетов на рабочих столах, а также их возможностями по поиску в репозитории платформы BI с помощью приложений-виджетов на рабочем столе.

Вы можете предоставить пользователям следующие возможности:

- Использование виджетов
- Редактирование объектов, созданных виджетами
- Изменение прав пользователей на доступ к объектам

Примечание:

По умолчанию для всех основных пользователей настроен доступ к этим функциям.

См. также

- [Управление настройками безопасности для объектов в СМС](#)

13.1.3.7 Управление настройками SAP BusinessObjects Explorer

Можно определить компоненты SAP BusinessObjects Explorer, к которым у пользователей будет доступ, настраивая их права безопасности из области "Приложения" СМС.

См. также

- [Управление настройками безопасности для объектов в СМС](#)

13.1.3.7.1 Изменение свойств приложения SAP BusinessObjects Explorer

1. Перейдите в область «Программные приложения» СМС.
2. Выберите **Управление > Свойства**.
Появится диалоговое окно «Свойства».
3. Определите любую из следующих настроек SAP BusinessObjects Explorer:
 - Расположение папки индекса по умолчанию
 - Количество потоков
 - Действительность закладок
4. Нажмите кнопку **Сохранить и закрыть**.

13.1.3.8 Управление настройками поиска по платформе

В области «Приложения» СМС платформы BI можно задать настройки на уровне системы для приложения поиска по платформе.

См. также

- [Список сбоев индексации](#)
- [Настройка свойств приложения](#)

13.1.3.8.1 Настройка свойств приложения

Чтобы настроить свойства приложения поиска по платформе, выполните следующие действия:

1. Перейдите в область «Программные приложения» СМС.
2. Выберите **Приложение поиска по платформе**.
3. Выберите команду **Управление > Свойства**. Появится диалоговое окно «Свойства».
4. Выполните настройку требуемых параметров поиска по платформе.

Настраиваемые свойства описаны в следующей таблице:

Действие	Описание
Статистика поиска	<p>Поиск по платформе предлагает следующие статистики поиска:</p> <ul style="list-style-type: none"> • Статус индексации: показывает состояние процесса индексации • Число проиндексированных документов: показывает число документов, для которых индексация выполнена. • Последняя отметка времени индексации: показывает метку времени, когда документ был проиндексирован в последний раз.
Остановить / начать индексацию	<p>Параметры запуска и остановки индексации позволяют запустить или остановить процесс индексации, когда требуется перейти от непрерывного обхода на планируемый, либо в целях обслуживания.</p> <p>Чтобы остановить индексацию, щелкните Остановить индексацию и затем нажмите кнопку ОК в диалоговом окне подтверждения.</p>
Региональные параметры индекса	<p>При выборе другого языка для региональных параметров индекса поиска по платформе выполняет повторную индексацию документов на выбранном языке.</p> <p>Выберите региональные параметры индекса в одном из следующих языков: английский, бразильский, голландский, итальянский, испанский, китайский, корейский, немецкий, норвежский букмол, польский, португальский, русский, тайский, финский, французский, чешский, шведский или японский.</p> <p>Примечание: Английский язык выбран в качестве региональных параметров по умолчанию.</p>

Действие	Описание
Периодичность поиска	<p>Индексацию всего репозитория платформы BI можно выполнить, используя следующие параметры:</p> <ul style="list-style-type: none"> Непрерывный обход: при выборе этого варианта индексация выполняется непрерывно, т.е. репозиторий индексируется всякий раз при добавлении, изменении или удалении объекта. Это позволяет просматривать содержимое платформы BI или работать с ним. Выбираемый по умолчанию непрерывный обход постоянно обновляет репозиторий платформы BI по мере выполнения различных действий. Непрерывный обход не требует при работе вмешательства пользователя и сокращает время, требуемое на индексирование документа. Плановый обход: при выборе этого варианта индексация выполняется на основании расписания, задаваемого настройками "Расписание". <p>Для получения дополнительных сведений о включении объектов в расписание см. раздел <i>Включение объекта в расписание</i> интерактивной справки по поиску по платформе в <i>СМС платформы BI</i>.</p> <p>Примечание:</p> <ul style="list-style-type: none"> При выборе команды Запланировать обход и установке для параметра Повторение значения, отличного от Сейчас, поиск по платформе отображает дату и время временной метки следующей плановой индексации документа. При выборе планового обхода кнопка Начать индексацию активируется, а кнопка Остановить индексацию деактивируется. По окончании планирования кнопка Остановить индексацию деактивируется.

Действие	Описание
Расположение индекса	

Действие	Описание
	<p>Сведения об индексированных документах сохраняются в общих папках в следующих местах:</p> <ul style="list-style-type: none"> Расположение основного индекса (индексы и проверка орфографии): основной индекс и индексы проверки орфографии сохраняются в этом расположении. Во время рабочего процесса поиска начальные попадания извлекаются по основному индексу, а индексы проверки орфографии используются для извлечения предположений. В кластеризованном развертывании BOE это расположение должно находиться на общей (сетевой) файловой системе, доступной всем узлам в кластере. Постоянное расположение данных (Хранилища содержимого): хранилище содержимого находится в этом расположении. Оно создается из расположения основного индекса и остается синхронизированным с ним. Хранилище содержимого используется для создания фасетов и обработки начальных совпадений, созданных из расположения основного индекса. В кластеризованном развертывании платформы BI хранилища содержимого создаются в каждом из узлов. <p>Расположение постоянных данных – это единственное расположение индексов, на которое влияет наличие кластеризованной среды, так как оно содержит папки хранилищ содержимого. Если на компьютере имеется только одна служба поиска, на нем будет только одно расположение хранилища содержимого. Например, это может быть</p> <p><code>{obj.enterprise.home}\data\PlatformSearchData\workspace\Server\ContentStores.</code></p> <p>Однако в кластеризованной среде при наличии множества служб поиска у каждой из них будет по одному местоположению хранилища содержимого. Например, при наличии двух активных экземпляров сервера местоположения хранилища содержимого будут следующими:</p> <ol style="list-style-type: none"> <code>{obj.enterprise.home}\data\PlatformSearchData\workspace\Server\ContentStores.</code> <code>{obj.enterprise.home}\data\PlatformSearchData\workspace\Server1\ContentStores.</code> <ul style="list-style-type: none"> Расположение непостоянных данных (временных файлов, дельта-индексов): в этом расположении создаются и временно сохраняются дельта-индексы перед их слиянием с основным индексом. Индексированные документы из этого расположения удаляются после их слияния с основным индексом. Кроме того, суррогатные файлы (результат работы экстракторов) также создаются и временно сохраняются в этом расположении, до их преобразования в дельта-индексы. <p>Примечание:</p> <ul style="list-style-type: none"> Все места размещения индексов должны иметь общий доступ.

Действие	Описание
	<ul style="list-style-type: none"> • Чтобы изменить расположение индекса, нажмите кнопку Остановить индексацию. • При изменении расположения индекса необходимо скопировать существующее содержимое в новое расположение, иначе данные из существующего индекса будут утеряны.
Уровень индексации	<p>Можно выполнить настройку содержимого поиска, задав уровень индексации следующим образом:</p> <ul style="list-style-type: none"> • Метаданные платформы: индекс создается только для метаданных платформы, таких, как заголовки, ключевые слова и описания документов. • Метаданные платформы и документа – индекс создается по метаданным платформы и метаданным документов. К метаданным документа относятся дата создания, дата изменения и имя автора. • Содержимое в полном объеме: индекс создается по метаданным платформы, метаданным документов и другому содержимому, включая следующее: <ul style="list-style-type: none"> • Фактическое содержимое документа • Содержимое запросов и списков значений • Диаграммы, графики и метки <p>Примечание: При изменении уровня индексации процесс индексации инициализируется заново для всего репозитория платформы BI.</p>
Типы содержимого	<p>Для индексирования могут быть заданы следующие типы содержимого.</p> <ul style="list-style-type: none"> • Microsoft Word • Microsoft Excel • Microsoft PowerPoint • Текст • Adobe Acrobat • Формат RTF • Crystal Reports • Юниверс • Web Intelligence

Действие	Описание
Перестроить индекс	<p>Этот параметр удаляет все существующее проиндексированное содержимое и повторно индексирует весь документ с самого начала.</p> <p>Параметр Перестроить индекс можно выбрать независимо от состояния индексации. Однако параметр Перестроить индекс не будет работать в случае останова индексирования, выбора параметра Перестроить индекс, сохранения и закрытия приложения поиска по платформе после остановки индексации.</p> <p>В случае останова индексации и выбора параметра Перестроить индекс, сохраните и закройте приложение поиска по платформе, затем откройте повторно страницу конфигурации и нажмите кнопку Начать индексацию., после чего сохраненный параметр "Перестроить индекс" проведет автоматическую повторную индексацию всего документа.</p> <p>Чтобы отказаться от повторной индексации документов, снимите флажок Перестроить индекс перед нажатием кнопки Начать индексацию.</p>
Документы, исключенные из индексации	<p>Параметр Исключенные из индексирования документы позволяет исключить из индексирования некоторые документы. Например, чтобы избежать перегрузки сервера приложений отчета, может потребоваться отключение функции поиска в очень больших отчетах Crystal. Также может потребоваться исключение из индексирования публикаций с сотнями персонализированных отчетов.</p> <p>Исключение конкретных документов позволяет заблокировать доступ к ним при поиске по платформе. Важно отметить, что документ, проиндексированный до того, как был отнесен к данной группе, все еще может быть доступен для поиска. Чтобы документы, отнесенные к категории Исключенные из индексирования документы, были гарантированно недоступны для поиска, необходимо перестроить индекс.</p> <p>По умолчанию только учетной записи администратора предоставлено полное управление параметром Исключенные из индексирования документы. Другие пользователи с перечисленными ниже правами могут только добавлять документы в группу Исключенные из индексирования документы:</p> <ul style="list-style-type: none"> • Права просмотра и редактирования категории • Непосредственное редактирование документа

5. Нажмите кнопку **Сохранить и закрыть**.

Примечание:

Если пользователь не выбрал параметр **Перестроить индекс** и изменил уровень индексирования, выбрал или отменил выбор средств извлечения, то будет выполнено инкрементное обновление существующего индекса без его удаления.

13.2 Управление приложениями с помощью свойств BOE.war

13.2.1 Файл BOE.war

Можно изменять настройки веб-приложений платформы BI посредством перезаписи свойств по умолчанию для файла BOE.war. Развертывание этого файла выполняется на компьютере, на котором установлен сервер веб-приложений. Для получения дополнительной информации о развертывании этого файла см. *Руководство по развертыванию веб-приложений платформы SAP BusinessObjects Business Intelligence*.

Свойства, содержащиеся в файле BOE.war, определяют спецификации для входа в систему по умолчанию, методы аутентификации по умолчанию, а также настройки для единого входа. Для указания доступно два типа свойств:

- Глобальные свойства – влияют на все веб-приложения, содержащиеся в файле BOE.war.
- Свойства приложений – влияют только на заданные веб-приложения.

Чтобы изменить одно из свойств по умолчанию, используйте каталог пользовательской конфигурации для хранения новых настроек, как для глобальных свойств, так и свойств приложения. По умолчанию каталог располагается по адресу `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Не изменяйте свойства в каталоге `config\default`.

Примечание:

На некоторых серверах веб-приложений, например в версии Tomcat, поставляемой с платформой BI, возможен прямой доступ к BOE.war. В этом сценарии можно задать пользовательские настройки напрямую, без отмены развертывания WAR-файла. Если непосредственный доступ к развернутым веб-приложениям отсутствует, необходимо отменить развертывание, изменить настройки и выполнить повторное развертывание файла. Для получения дополнительных сведений см. *Руководство по развертыванию веб-приложений платформы SAP BusinessObjects Business Intelligence*.

13.2.1.1 Глобальные свойства файла BOE.war

В следующей таблице перечислены параметры доверительной аутентификации, которые входят в состав установленного по умолчанию файла `global.properties` для файла `BOE.war`. Чтобы перезаписать параметры, создайте новый файл в каталоге `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Параметр	Значения по умолчанию	Описание
<code>persistentcookies.enabled</code>	<code>persistentcookies.enabled=true</code>	Включает или отключает сохранение cookie-файлов на странице входа в приложение.
<code>siteminder.authentication</code>	<code>siteminder.authentication=secLDAP</code>	Указывает метод аутентификации, используемый в SiteMinder. Допустимые параметры: <code>secLDAP</code> и <code>secwinAD</code> .
<code>siteminder.enabled</code>	<code>siteminder.enabled=false</code>	Включает или отключает аутентификацию в SiteMinder.
<code>sso.enabled</code>	<code>sso.enabled=false</code>	Включает или отключает единый вход в платформу BI.
<code>sso.sap.primary</code>	<code>sso.sap.primary=false</code>	Присвойте этому параметру значение <code>true</code> , чтобы использовать функцию единого входа SAP в качестве основного механизма единого входа для приложения. Применяется только в тех случаях, когда одновременно используются функции единого входа SAP и SiteMinder.
<code>tree.pagesize</code>	<code>tree.pagesize=100</code>	Задаёт максимальное число записей, отображаемых в области навигации веб-приложения.
<code>trustedauth.sharedsecret</code>	Нет	Задаёт имя переменной сеанса, используемой для извлечения секретного ключа для доверительной аутентификации. Применяется только случае использования веб-сеанса для передачи общего секретного ключа.

Параметр	Значения по умолчанию	Описание
<code>trusted.auth.user.param</code>	Нет	<p>Задаёт переменную, используемую для извлечения имени пользователя для доверительной аутентификации. Может иметь одно из следующих значений:</p> <ul style="list-style-type: none"> Заголовок Параметр URL Cookie Сеанс
<code>trusted.auth.user.retrieval</code>	Нет	<p>Задаёт метод, используемый для извлечения имени пользователя для доверительной аутентификации. Может иметь одно из следующих значений:</p> <ul style="list-style-type: none"> "REMOTE_USER" "HTTP_HEADER" "COOKIE" "QUERY_STRING" "WEB_SESSION" "USER_PRINCIPAL" <p>Чтобы отключить доверительную аутентификацию, установите пустое значение.</p>
<code>trusted.auth.namespace.enabled</code>	<code>trusted.auth.user.namespace.enabled=false</code>	<p>Включает и отключает динамическую привязку псевдонимов к существующим учетным записям. Если этому свойству присвоено значение <code>true</code>, при доверительной аутентификации используется привязка псевдонимов для аутентификации пользователей в платформе BI. Благодаря привязке псевдонимов сервер приложений может работать как поставщик услуг SAML, что позволяет предоставлять функции единого входа SAML в систему при доверительной аутентификации. Если установлено значение <code>false</code>, для аутентификации пользователей при доверительной аутентификации используется сопоставление имен.</p>

Параметр	Значения по умолчанию	Описание
vintela.enabled	<pre>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</pre>	Используется для включения или отключения параметров Vintela для аутентификации Windows AD.
pinger.showWarningDialog.cmc	pinger.showWarningDialog.cmc=true	Указывает, отображается или нет диалоговое окно предупреждения с сообщением о скором истечении срока действия сеанса в СМС.
pinger.showWarningDialog.bl	pinger.showWarningDialog.bl.launchpad=true	Указывает, отображается или нет диалоговое окно предупреждения с сообщением о скором истечении срока действия сеанса в стартовой панели BI.
pinger.warmingPeriodInSecs	pinger.warmingPeriod.pingIncrementsInSecs=15	Указывает частоту отправки запросов веб-сервера во время отображения предупреждающего сообщения об истечении срока действия сеанса. Этот параметр важен для синхронизации диалоговых окон предупреждения между приложениями.
pinger.warmingPeriodInMins	pinger.warmingPeriod.lengthInMinutes=5	Указывает, за какое время до истечения срока действия сеанса отображается предупреждение.
logoff.on.websession.expiry	logoff.on.websession.expiry=true	Указывает необходимость выхода из системы для всех сеансов приложений в случае истечения срока действия веб-сеанса.
pinger.enabled	pinger.enabled=true	Включает или отключает механизм отображения предупреждающих сообщений об истечении срока действия сеанса.
system.console.bip.jmanager.destinations.size	system.console.bip.jmanager.destinations.size=1000	Указывает максимальное число кэшируемых соединений Java.

13.2.1.2 Свойства стартовой панели BI

В следующей таблице перечислены параметры доверительной аутентификации, которые входят в состав установленного по умолчанию файла `bi-launchpad.properties` для файла `BOE.war`. Чтобы перезаписать параметры, создайте новый файл в каталоге `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Параметр	Описание																		
<code>app.name</code>	Задаёт отображаемое имя приложения. Это имя отображается на странице заголовка веб-приложения и экране входа в систему. По умолчанию: <code>app.name=BI launch pad</code>																		
<code>app.name.greeting</code>	По умолчанию: <code>app.name.greeting=BusinessObjects</code>																		
<code>app.name.short</code>	Задаёт отображаемое имя приложения. Это имя отображается на странице заголовка веб-приложения и экране входа в систему. По умолчанию: <code>app.name.short=BI launch pad</code>																		
<code>app.url.name</code>	Задаёт URL-имя приложения, предваряемое символом «/». По умолчанию: <code>app.url.name=/BI</code>																		
<code>authentication.default</code>	<p>Задаёт метод аутентификации по умолчанию, используемый для аутентификации пользователей в приложении. Для этого параметра доступны любые из следующих параметров:</p> <table> <tr> <th>Аутентификация</th><th>Значение параметра</th></tr> <tr> <td>Enterprise</td><td><code>secEnterprise</code></td></tr> <tr> <td>LDAP</td><td><code>secLDAP</code></td></tr> <tr> <td>Windows AD</td><td><code>secWinAD</code></td></tr> <tr> <td>SAP</td><td><code>secSAPR3</code></td></tr> <tr> <td>PeopleSoft</td><td><code>secpseenterprise</code></td></tr> <tr> <td>JD Edwards</td><td><code>secPSE1</code></td></tr> <tr> <td>Siebel</td><td><code>secSiebel7</code></td></tr> <tr> <td>Oracles EBS</td><td><code>secOraApps</code></td></tr> </table> <p>По умолчанию: <code>authentication.default=secEnterprise</code></p>	Аутентификация	Значение параметра	Enterprise	<code>secEnterprise</code>	LDAP	<code>secLDAP</code>	Windows AD	<code>secWinAD</code>	SAP	<code>secSAPR3</code>	PeopleSoft	<code>secpseenterprise</code>	JD Edwards	<code>secPSE1</code>	Siebel	<code>secSiebel7</code>	Oracles EBS	<code>secOraApps</code>
Аутентификация	Значение параметра																		
Enterprise	<code>secEnterprise</code>																		
LDAP	<code>secLDAP</code>																		
Windows AD	<code>secWinAD</code>																		
SAP	<code>secSAPR3</code>																		
PeopleSoft	<code>secpseenterprise</code>																		
JD Edwards	<code>secPSE1</code>																		
Siebel	<code>secSiebel7</code>																		
Oracles EBS	<code>secOraApps</code>																		
<code>authentication.visible</code>	Указывает возможность просмотра и изменения режима аутентификации пользователем, выполняющим вход в стартовую панель BI. По умолчанию: <code>authentication.visible=false</code>																		
<code>cms.default</code>	Задаёт имя CMS по умолчанию. По умолчанию: <code>cms.default=[имя компьютера хоста]</code>																		

Параметр	Описание
<code>cms.visible</code>	Указывает возможность просмотра и изменения имени CMS пользователем, выполняющим вход в стартовую панель BI. По умолчанию: <code>cms.visible=true</code>
<code>dialogue.prompt.enabled</code>	Указывает необходимость запроса пользователя при переходе со страницы ввода в диалоговом окне. По умолчанию: <code>dialogue.prompt.enabled=false</code>
<code>logontoken.enabled</code>	Указывает, требуется ли включать создание маркеров для сеанса после входа пользователя в стартовую панель BI. Маркер будет храниться в cookie-файле. По умолчанию: <code>logontoken.enabled=false</code>
<code>SMTPFrom</code>	Включает или отключает поле «От кого» при планировании объекта для адресата. По умолчанию: <code>SMTPFrom=true</code>
<code>url.exit</code>	Задает URL-адрес, на который перенаправляются пользователи после завершения сеанса стартовой панели BI. Этот параметр применяется только для тех пользователей, которые выполнили вход в приложение с использованием внешнего процесса проверки.
<code>disable.locale.preference</code>	Разрешает или запрещает просмотр и изменение пользователями локальных параметров просмотра для стартовой панели BI. По умолчанию: <code>disable.locale.preference=false</code>
<code>extlogon.allow.logoff</code>	Включает или отключает автоматический выход из системы для сеансов пользователей после закрытия соответствующих сеансов стартовой панели BI. Чтобы отключить автоматическое завершение сеансов при выходе пользователей из стартовой панели BI, присвойте этому параметру значение <code>false</code> . По умолчанию: <code>extlogon.allow.logoff=true</code>

13.2.1.3 Свойства OpenDocument

В следующей таблице перечислены параметры доверительной аутентификации, которые входят в состав установленного по умолчанию файла `opendocument.properties` для файла `BOE.war`. Чтобы перезаписать параметры, создайте новый файл в каталоге `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Параметр	Описание																		
app.name	Задаёт отображаемое имя приложения. Это имя отображается на странице заголовка веб-приложения и экране входа в систему. По умолчанию: app.name=SAP BusinessObjects OpenDocument																		
app.name.short	Задаёт отображаемое имя приложения. Это имя отображается на странице заголовка веб-приложения и экране входа в систему. По умолчанию: app.name.short=OpenDocument																		
authentication.default	<p>Задаёт метод аутентификации по умолчанию, используемый для аутентификации пользователей в приложении. Для этого параметра доступны любые из следующих параметров:</p> <table> <tr> <th>Аутентификация</th><th>Значение параметра</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>По умолчанию: authentication.default=secEnterprise</p>	Аутентификация	Значение параметра	Enterprise	secEnterprise	LDAP	secLDAP	Windows AD	secWinAD	SAP	secSAPR3	PeopleSoft	secpsenterprise	JD Edwards	secPSE1	Siebel	secSiebel7	Oracles EBS	secOraApps
Аутентификация	Значение параметра																		
Enterprise	secEnterprise																		
LDAP	secLDAP																		
Windows AD	secWinAD																		
SAP	secSAPR3																		
PeopleSoft	secpsenterprise																		
JD Edwards	secPSE1																		
Siebel	secSiebel7																		
Oracles EBS	secOraApps																		
authentication.visible	Указывает возможность просмотра и изменения режима аутентификации пользователем, выполняющим вход в OpenDocument. По умолчанию: authentication.visible=false																		
cms.default	Задаёт имя CMS по умолчанию. По умолчанию: cms.default=[имя компьютера хоста]																		

Параметр	Описание
<code>cms.visible</code>	Указывает возможность просмотра и изменения имени СМС пользователем, выполняющим вход в OpenDocument. По умолчанию: <code>cms.visible=true</code>
<code>logontoken.enabled</code>	Указывает, требуется ли включать создание маркеров для сеанса после входа пользователя в OpenDocument. Маркер будет храниться в cookie-файле. По умолчанию: <code>logontoken.enabled=false</code>
<code>extlogon.allow.logoff</code>	Включает или отключает автоматический выход из системы для сеансов пользователей после закрытия соответствующих сеансов OpenDocument. Чтобы отключить автоматическое завершение сеансов при выходе пользователей из OpenDocument, присвойте этому параметру значение <code>false</code> . По умолчанию: <code>extlogon.allow.logoff=true</code>

13.2.1.4 Свойства СМС

В следующей таблице перечислены параметры доверительной аутентификации, которые входят в состав установленного по умолчанию файла `cms.properties` для файла `BOE.war`. Чтобы перезаписать параметры, создайте новый файл в каталоге `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Параметр	Описание																		
app.url.name	Задает URL-имя приложения, предваряемое символом «/». По умолчанию используется имя app.url.name=/CMC																		
authentication.default	<p>Задает метод аутентификации по умолчанию, используемый для аутентификации пользователей в приложении. Для этого параметра доступны любые из следующих параметров:</p> <table> <tr> <th>Аутентификация</th><th>Значение параметра</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>По умолчанию: authentication.default=secEnterprise</p>	Аутентификация	Значение параметра	Enterprise	secEnterprise	LDAP	secLDAP	Windows AD	secWinAD	SAP	secSAPR3	PeopleSoft	secpsenterprise	JD Edwards	secPSE1	Siebel	secSiebel7	Oracles EBS	secOraApps
Аутентификация	Значение параметра																		
Enterprise	secEnterprise																		
LDAP	secLDAP																		
Windows AD	secWinAD																		
SAP	secSAPR3																		
PeopleSoft	secpsenterprise																		
JD Edwards	secPSE1																		
Siebel	secSiebel7																		
Oracles EBS	secOraApps																		
authentication.visible	Указывает возможность просмотра и изменения режима аутентификации пользователем, выполняющим вход в СМС. По умолчанию: authentication.visible=false																		
cms.default	Задает имя СМС по умолчанию. По умолчанию: cms.default=[имя компьютера хоста]																		
cms.visible	Указывает возможность просмотра и изменения имени СМС пользователем, выполняющим вход в СМС. По умолчанию: cms.visible=true																		
dialogue.prompt.enabled	Указывает необходимость запроса пользователя при переходе со страницы ввода в диалоговом окне. По умолчанию: dialogue.prompt.enabled=false																		
logontoken.enabled	Указывает, требуется ли включать создание маркеров для сеанса после входа пользователя в СМС. Маркер будет храниться в cookie-файле. По умолчанию: logontoken.enabled=false																		

13.3 Настройка точек входа в систему для стартовой панели BI и OpenDocument

Можно настроить страницу входа в систему для веб-приложений стартовой панели BI и OpenDocument. Например, можно настроить использование на странице входа в систему логотипа компании или корпоративной таблицы стилей, а также создать пользовательскую страницу входа, обеспечивающую доверительную аутентификацию.

Чтобы настроить страницу входа в систему, измените файл `custom.jsp`, хранящийся в областях приложений стартовой панели BI и OpenDocument веб-приложения `BOE.war`, а затем повторно разверните веб-приложение `BOE.war` в платформе BI. Для доступа к пользовательской точке входа в систему требуется перейти по уникальному URL-адресу.

Для работы с этими примерами необходимо ознакомиться с принципами развертывания веб-приложений платформы BI. Для получения дополнительных сведений см. *Руководство по развертыванию веб-приложений платформы SAP BusinessObjects Business Intelligence*.

13.3.1 Местоположения файлов стартовой панели BI и OpenDocument

Веб-приложения стартовой панели BI и OpenDocument упакованы в файлы веб-архива `BOE.war`. Местоположение файла архива `BOE.war` определяется в файле `BOE.properties`.

В системах Windows файл `BOE.properties` располагается в следующей папке:

- `<BOE_INSTALL_DIR>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf\apps\BOE.properties`

В системах UNIX файл `BOE.properties` располагается в следующей папке:

- `<BOE_INSTALL_DIR>/sap_bobj/enterprise_xi40/wdeploy/conf/apps/BOE.properties`

В следующих таблицах определяется расположение общих файлов в файле веб-архива `BOE.war` для приложений стартовой панели BI и OpenDocument.

Таблица 13-2: Местоположения файлов стартовой панели BI

Примечание:

Веб-приложение стартовой панели BI ранее называлось InfoView.

Тип файла	Местоположение
Пользовательский скрипт входа в систему	WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp
Каталог для дополнительных файлов	WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomResources

Тип файла	Местоположение
Пользовательский URL-адрес для входа в систему	<code>http://<servername>:<port>/BOE/BI/custom.jsp</code>

Таблица 13-3: Местоположения файлов OpenDocument

Тип файла	Местоположение
Пользовательский скрипт входа в систему	WEB-INF\ eclipse \ plugins \ webpath . OpenDocument \ web \ opendoc \ custom . jsp
Каталог для дополнительных файлов	WEB-INF\ eclipse \ plugins \ webpath . OpenDocument \ web \ noCacheCustomResources
Пользовательский URL-адрес для входа в систему	<code>http://<servername>:<port>/BOE/OpenDocument/opendoc/custom.jsp</code>

13.3.2 Определение пользовательской страницы входа в систему

Можно настроить точку входа в платформу BI. Например, можно создать пользовательскую страницу входа в систему, на которой отображается логотип компании и используется корпоративная таблица стилей.

Измените файл `custom.jsp`, чтобы настроить интерфейс входа в систему для пользователей, и поместите вспомогательные файлы в папку `noCacheCustomResources`.

В этом примере показано создание пользовательской страницы входа в систему, с которой пользователь перенаправляется на стандартную страницу входа.

1. Создайте файл, содержащий пользовательский код входа в систему, и сохраните его под именем `custom.js` в папке `noCacheCustomResources`.

В этом примере определяется функция, перенаправляющая пользователя на стандартную страницу входа в систему – `logon.jsp`.

```
function load() {window.location = "logon.jsp";}
```

2. Измените файл `custom.jsp`, чтобы настроить страницу входа в систему.

В этом примере отображаются приветственное сообщение и гиперссылка, которая вызывает метод `load`, определенный в файле `custom.js`.

```
<!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. Выполните повторное развертывание файла `BOE.war` и перезапустите веб-сервер.

13.3.3 Добавление доверительной аутентификации при входе в систему

Чтобы добавить доверительную аутентификацию, установите надежного пользователя в качестве атрибута сеанса в файле `custom.jsp` и измените параметры аутентификации в копии файла `global.properties`. Значения пользовательской копии файла `global.properties` переопределяют значения по умолчанию.

1. Измените файл `custom.jsp` и установите в нем атрибут сеанса, определяющий надежного пользователя.

```
request.getSession().setAttribute("TrustedUserAttribute", "TrustedUser");
```

2. Создайте пользовательскую копию файла `global.properties`. Для этого скопируйте файл `WEB-INF\config\default\global.properties` в файл `WEB-INF\config\custom\global.properties`.
3. Измените файл `WEB-INF\config\custom\global.properties` и включите в нем функцию единого входа.

```
sso.enabled=true
```

4. Измените файл `WEB-INF\config\custom\global.properties` и установите параметры доверительной аутентификации, в том числе переменную сеанса пользователя и общий секретный ключ.

Замените строку `". . . "` общим секретным ключом для системы.

```
trusted.auth.user.param=TrustedUserAttribute
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.shared.secret=". . ."
```

5. Выполните повторное развертывание веб-приложения и перезапустите веб-сервер.

См. также

- [Включение доверительной аутентификации](#)

13.4 Настройка веб-интеграции BEx

Веб-приложения BEx представляют собой веб-приложения Business Explorer (BEx) для SAP NetWeaver Business Warehouse (BW) и предназначены для анализа данных, отчетности и аналитических приложений в веб.

Business Explorer – это пакет Business Intelligence SAP NetWeaver, предоставляющий гибкие инструменты создания отчетов и анализа, которые обеспечивают поддержку стратегического анализа и принятия решений. В этих инструментах реализованы функции запросов, создания отчетов и анализа. Применяя их, сотрудники с соответствующими правами доступа могут выполнять оценку хронологических или текущих данных на различных уровнях детализации и с различных ракурсов из веб-интерфейса или из Microsoft Excel.

Пользователь получает доступ к данным с портала SAP NetWeaver или со стартовой панели BI. Авторы веб-приложений BEx могут выполнять веб-приложения непосредственно в стартовой панели BI в конструкторе веб-приложений BEx.

Для интеграции веб-приложений BEx в платформе BI выполните следующие действия по настройке:

1. Настройте сервер для веб-приложений BEx в Central Management Console (CMC).

Для веб-приложений BEx можно использовать общий или отдельный сервер.

Совет:

Рекомендуется настроить для веб-приложений BEx отдельный сервер, поскольку на общем сервере, как правило, выполняются многие другие службы.

2. Настройте параметры сервера.
3. Проверьте подключение к системе BW.
4. Чтобы обеспечить авторам возможность выполнять веб-приложения BEx непосредственно в стартовой панели BI из конструктора веб-приложений BEx, необходимо настроить соответствующие параметры в таблице **Подключенные порталы** (RSPOR_T_PORTAL) в системе BW.

После настройки сервера платформы BI пользователи смогут открывать веб-приложения BEx в стартовой панели BI. Здесь они могут переходить к данным и сохранять веб-приложения BEx как избранные страницы в веб-браузере.

Ограничение:

Так как для интеграции этого рода Java-стек SAP NetWeaver не требуется, то имеют силу следующие ограничения:

- Многоадресная рассылка информации не поддерживается.
- Поскольку портал и управление знаниями SAP NetWeaver не требуются, интеграция документов и использование мотивов портала в веб-приложениях BEx не поддерживаются.
- Веб-элемент **Отчет** не поддерживается. Для создания форматированных отчетов рекомендуется использовать приложение SAP Crystal Reports.

- При создании версий веб-приложений BEx для печати используется библиотека экспорта для SAP Business Explorer. Службы Adobe Document (ADS) недоступны.
- Веб-приложения BEx, интегрируемые в платформу BI, могут содержать только такие источники данных, которые хранятся в главной системе BW. В параметрах администрирования системы определяется, какая система будет выбрана в качестве главной системы BW в платформе BI.
- Единый вход для платформы BI и SAP NetWeaver BW не включен. Для каждого сеанса работы в платформе BI пользователям веб-приложений BEx необходимо выполнить вход в соответствующую главную систему BW.
- Интерфейс "отчет-отчет" из веб-приложений BEx и в веб-приложения BEx не поддерживается. Соответствующие команды не будут выполняться.

Дополнительные сведения о функциях и особенностях веб-приложений BEx см. на Справочном портале SAP (<http://help.sap.com>) в разделах **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 Applications**.

Для получения дополнительных сведений о доступе к веб-приложениям BEx из стартовой панели BI и об их сохранении см. *Руководство пользователя по стартовой панели BI* по адресу <http://help.sap.com>.

См. также

- [Запуск сервера для веб-приложений BEx](#)
- [Запуск отдельного сервера для веб-приложений BEx](#)
- [Настройка параметров сервера](#)
- [Проверка подключения к системе BW](#)
- [Настройка соединения между конструктором веб-приложений BEx и платформы BI](#)

13.4.1 Запуск сервера для веб-приложений BEx

1. Войдите в Central Management Console (CMC).
2. Нажмите кнопку **Сервер**.
3. Разверните узел **Категории служб** и выберите пункт **Analysis Services**.
4. Выберите **Адаптивный сервер обработки**, а затем выберите в контекстном меню команду **Выбрать службы**.
5. Выберите в списке **Доступные службы** значение **BExWebApplicationsService** и переместите его в список **AdaptiveProcessingServerServices**.
6. Активируйте и запустите службу веб-приложений BEx при помощи контекстного меню.

13.4.2 Запуск отдельного сервера для веб-приложений BEx

1. Войдите в Central Management Console (CMC).
2. Нажмите кнопку **Сервер**.
3. Разверните узел **Категории служб** и выберите пункт **Analysis Services**.
4. Выберите **Адаптивный сервер обработки**, а затем выберите в контекстном меню команду **Клонировать сервер**.
5. Введите имя сервера (например, AdaptiveProcessingServer) и выберите нужный сервер в поле **Клонировать в узле**.
6. Выберите клонированный сервер и выберите в контекстном меню команду **Выбрать службы**.
7. Выберите в списке **Доступные службы** значение **BExWebApplicationsService** и переместите его в список **AdaptiveProcessingServerServices**.
8. Активируйте и запустите службу веб-приложений BEx при помощи контекстного меню.

13.4.3 Настройка параметров сервера

1. Войдите в Central Management Console (CMC).
2. Нажмите кнопку **Сервер**.
3. Разверните узел **Категории служб** и выберите пункт **Analysis Services**.
4. Выберите службу веб-приложений BEx, а затем в контекстном меню выберите команду **Свойства**.
5. В разделе **Конфигурация службы веб-приложений BEx** в области «Служба веб-приложений BEx» настройте следующие параметры:
 - a. Проверьте (и при необходимости измените) максимальное число сеансов работы клиентов.
 - b. В разделе **Главная система SAP BW** введите имя OLAP-подключения к системе BW, созданной в платформе BI. Имя по умолчанию – **SAP_BW**.
 - c. В поле **RFC-адресат JCo-сервера** введите имя, которое было введено в системе BW в разделе **Конфигурация RFC-подключений** (код транзакции sm59).
 - d. В поле **Хост шлюза JCo-сервера** введите имя, определенное в системе BW в разделе **Конфигурация RFC-подключений** (код транзакции sm59).
 - e. В поле **Служба шлюза JCo-сервера** введите имя, определенное в системе BW в разделе **Конфигурация RFC-подключений** (код транзакции sm59).
 - f. Проверьте и при необходимости измените значение в поле **Чисто подключений к JCo-серверу**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. Выберите службу веб-приложений BEx, а затем в контекстном меню выберите команду **Перезапустить сервер**.

Для применения выбранных параметров требуется перезапустить сервер.

Примечание:

Перед перезапуском сервера необходимо убедиться, что создан RFC-адресат в системе ABAP.

См. также

- [Создание RFC-адресата в системе ABAP](#)

13.4.4 Проверка подключения к системе BW

1. Войдите в Central Management Console (CMC).
2. Нажмите кнопку **Соединения OLAP**.
3. Проверьте, было ли установлено подключение к системе BW. Если нет, установите подключение. Имя по умолчанию для подключения – SAP_BW. Можно ввести другое имя.
4. Убедитесь, что выбран параметр **Предварительно задано** в разделе **Аутентификация**, и введены обязательные сведения о пользователе и пароле.

Примечание:

Эта учетная запись пользователя требуется для RFC-адреса сервера JCo для обеспечения интеграции конструктора веб-приложений BEx, системы BW и платформы BI.

Совет:

Чтобы обеспечить безопасность подключения, убедитесь, что права доступа к нему имеются только у администраторов.

- a. Для этого щелкните подключение к системе BW правой кнопкой мыши (по умолчанию его имя – SAP_BW) и выберите в контекстном меню команду **Безопасность пользователя**.
- b. Настройте требуемые параметры безопасности, по возможности предоставляя права доступа только администраторам.

13.4.5 Настройка соединения между конструктором веб-приложений BEx и платформы BI

Чтобы обеспечить авторам возможность выполнять веб-приложения BEx непосредственно в стартовой панели BI из конструктора веб-приложений BEx, необходимо настроить соответствующие параметры в таблице **Подключенные порталы** (RSPOR_T_PORTAL) в системе BW.

1. В системе BW вызовите транзакцию SM30 (**Сопровождение табличного представления**).
2. В поле **Таблица/Представление** введите значение RSPOR_T_PORTAL.

3. Нажмите кнопку **Сохранить**.
4. Чтобы создать новую запись, нажмите кнопку **Новые записи**.
5. Настройте следующие параметры:
 - a. Чтобы обеспечить интеграцию между системой BW и платформой BI, нужно создать RFC-адрес в транзакции SM59. Введите RFC-адресат в поле **Целевой объект**.
 - b. Выберите параметр **Стандартный портал**. В результате веб-приложения в конструкторе веб-приложений будут всегда вызываться в платформе BI.
 - c. В поле **Префикс URL** введите URL-адрес сервера WACS, включая протокол, имя хоста и порт, например `http://<wacs><домен>:<порт>`.
 - d. В поле **Платформа** выберите значение **BOE**.
 - e. Выберите значение **Использовать экспортную библиотеку SAP (PDF)**, чтобы включить экспортную библиотеку для SAP Business Explorer, что позволит экспортировать файлы PDF, PostScript и PCL из веб-приложений BEx.
6. Сохраните введенные сведения.

См. также

- [Создание RFC-адресата в системе ABAP](#)

13.4.5.1 Создание RFC-адресата в системе ABAP

Для интеграции системы BW и платформы BI требуется RFC-адрес. RFC-адрес обеспечивает взаимодействие между системой BW и платформой BI.

1. Запустите **Конфигурация RFC-подключений** (код транзакции SM59).
2. Нажмите кнопку **Создать**.
3. Обслуживание RFC-адресата:
 - a. Введите имя RFC-адресата.
 - b. Выберите тип подключения **T** для подключения **TCP/IP**.
 - c. Введите краткое описание.
Позже можно изменить описание RFC-адресата на соответствующем языке.
 - d. В разделе **Технические настройки** выберите в качестве типа активации **Зарегистрированная серверная программа**.
 - e. В разделе **Технические настройки** введите код программы.
Код программы должен совпадать с кодом программы (RFC-адрес сервера JCo), указанным при создании места назначения для данной системы BW на сервере платформы BI.
 - f. В разделе **Технические настройки** в подразделе **Параметры шлюза** введите хост шлюза и службу шлюза, которые используются сервером платформы BI для взаимодействия с системой BW.
4. На вкладке **Вход и безопасность** выберите параметр **Отправить квитанцию на вход в SAP**.

5. Сохраните введенные сведения.

См. также

- [Настройка параметров сервера](#)

Управление соединениями и юниверсами

14.1 Управление соединениями

Соединение – это именованный набор параметров, определяющий, как одно или несколько приложений SAP BusinessObjects смогут получить доступ к реляционной или OLAP базе данных. Сведения о соединении, такие как имя сервера, база данных, имя пользователя и пароль могут безопасно храниться в репозитории платформы BI в папке "Соединения".

Дизайнеры определяют юниверсы на основании соединений. Пользователи приложений запросов, анализа и отчетности получают доступ к базе данных с помощью юниверса, что избавляет их от необходимости знать о расположенных в основе базы данных структурах данных.

Соединения могут быть созданы с помощью следующих приложений:

- Средство создания юниверсов. Соединения хранятся в репозитории.
- Средство дизайна информации. Соединения можно создавать локально и публиковать в репозитории, а также создавать и обрабатывать их непосредственно в репозитории.

Примечание:

Подробнее об управлении соединениями с источниками данных OLAP см. в документе *Руководство администратора SAP BusinessObjects Analysis, выпуск для OLAP*.

Пользователи получают права на создание, редактирование и удаление соединений.

Вы предоставляете пользователю доступ к соединениям юниверса и позволяете пользователю создавать и просматривать документы, которые используют эти юниверсы и соединения.

См. также

- [Управление настройками безопасности для объектов в CMC](#)
- [Права соединений](#)

14.1.1 Для удаления соединения юниверса

Совет:

Также можно удалять соединения с помощью средства создания юниверсов и средства дизайна информации.

1. В области «Соединения» выберите в списке соединение юниверса.
2. Выберите **Управление > Удалить**.

14.2 Управление Юниверсами

Юниверс – это организованная коллекция объектов метаданных, позволяющая бизнес-пользователям анализировать корпоративные данные и создавать по ним отчеты, не используя при этом технический язык. К этим объектам относятся измерения, меры, иерархии, атрибуты, предопределенные расчеты, функции и запросы. Уровень объектов метаданных создается по схеме реляционной базы данных или в виде куба OLAP, поэтому объекты напрямую присваиваются структурам базы данных. Юниверс включает соединения с источниками данных, чтобы пользователи средств запросов и анализа могли соединиться с юниверсом для выполнения запросов и создания отчетов, используя объекты в юниверсе, без необходимости знать о расположенных в основе базы данных структурах данных.

Юниверсы можно создавать при помощи следующих средств:

- Средство создания юниверсов. Юниверсы, созданные с помощью этого средства, можно отличить по расширению .unv, и поэтому они называются юниверсами .unv. Юниверсы .unv определяются с защищенным соединением и хранятся в папке репозитория "Юниверсы".
- Средство дизайна информации. Юниверсы, созданные с помощью этого средства, построены на основе нового семантического уровня. Их можно отличить по расширению .unx, и поэтому они называются юниверсами .unx. Юниверсы .unx создаются локально и публикуются в папке репозитория "Юниверсы". Дизайнеры могут определять безопасность на уровне объекта с помощью редактора безопасности средства дизайна информации.

Пользователи могут получать права приложения и права юниверса, что позволяет им создавать, редактировать и удалять юниверсы, а также определять безопасность для юниверсов.

Вы предоставляете пользователям права юниверса, позволяя им создавать и просматривать документы, в которых используются юниверсы.

См. также

- [Управление настройками безопасности для объектов в СМС](#)
- [Права средства создания юниверсов](#)
- [Права юниверсов \(.unv\)](#)
- [Права средства дизайна информации](#)
- [Права юниверсов \(.unx\)](#)

14.2.1 Удаление юниверсов

Совет:

Юниверсы также можно удалять с помощью средства дизайна информации.

1. В области СМС «Юниверсы» выберите в списке юниверс.
2. Выберите **Управление > Удалить**.
3. При запросе подтверждения нажмите кнопку **ОК**.

Мониторинг

15.1 О приложении мониторинга

Мониторинг – это новое приложение платформы SAP Business Intelligence 4.0. Это приложение предоставляет возможность захвата оперативных и исторических показателей серверов платформы SAP BusinessObjects Business Intelligence 4.0 для отчетности и уведомления. Приложение мониторинга помогает системным администраторам определять, нормально ли работает то или иное приложение и соответствуют ли ожиданиям значения времени отклика. Предоставляя ключевые производственные показатели, приложение мониторинга дает более наглядное представление о состоянии платформы SAP BusinessObjects Business Intelligence 4.0.

Мониторинг позволяет выполнять следующие действия:

- Контроль производительности каждого из серверов: возможен благодаря использованию наблюдений, которые показывают состояние каждого сервера в виде цветowych индикаторов. Администратор системы может задавать пороговые значения для этих наблюдений и получать предупреждения в случае превышения порогов. Это помогает заранее предпринять профилактические меры в случае угрозы сбоя или перерыва в работе.
- Просмотр критически важных системных KPI: помогает при мониторинге активности и ресурсов. Эти KPI отображаются на странице информационной панели в приложении мониторинга.
- Проверьте доступность системы и время отклика: с помощью зондов можно моделировать рабочие процессы для проверки правильности работы служб в развертывании Enterprise. Периодически анализируя время выполнения этих тестов, администратор системы может оценить динамику ее использования.
- Анализ пиковой нагрузки и периодичности пиков для CMS: помогает администратору системы определить потребность в дополнительных лицензиях и системных ресурсах.
- Интеграция с другими приложениями уровня предприятия: приложение мониторинга в составе платформы SAP BusinessObjects Business Intelligence 4.0 можно интегрировать с другими приложениями уровня предприятия, такими как SAP Solution Manager и IBM Tivoli Monitoring.

15.2 Термины мониторинга

В следующем списке представлены термины, связанные с приложением мониторинга:

Информационная панель

Страница "Информационная панель" позволяет администратору системы централизованно представлять данные при мониторинге производительности всех серверов. Она предоставляет оперативные сведения о системных KPI и последних предупреждениях, а также о наблюдениях и графиках, построенных с учетом их состояния.

Наблюдение

Наблюдения предоставляют оперативные и исторические данные о серверах и рабочих процессах в среде платформы SAP BusinessObjects Business Intelligence. С наблюдением можно связывать пороговые значения и предупреждения. Можно создать наблюдение с использованием данных из зондов, серверов, SAPOSCOL или производных показателей.

Производные показатели

Производный показатель обеспечивает гибкость при создании показателей в соответствии с требованиями пользователя и последующем создании наблюдения с помощью такого показателя. Производный показатель можно создать путем объединения двух или более существующих показателей в математическом уравнении.

Ключевой показатель эффективности

KPI (ключевые показатели эффективности) – это стандартные показатели развернутого экземпляра платформы SAP BusinessObjects Business Intelligence. Они предоставляют сведения о расписаниях и сеансах входа в систему. Например, высокое значение **RunningJobs** указывает на хорошую производительность серверов. В то же время высокое значение **PendingJobs** указывает на плохую производительность и высокую загрузку системы.

Зонды

Зонды наблюдают за различными службами и моделируют различные функциональные возможности компонентов платформы SAP BusinessObjects Business Intelligence. Планируя запуск зондов с заданной периодичностью, администратор системы может отслеживать доступность и производительность ключевых служб, предоставляемых платформой SAP BusinessObjects Business Intelligence 4.0. Эти данные можно использовать и для планирования мощности.

Цветовые индикаторы трафика

Светофор представляет состояние наблюдения в данное время. Для индикации состояния наблюдения используются зеленый, оранжевый и красный цвета. Пользователи могут задать для наблюдения два или три состояния.

График тенденций

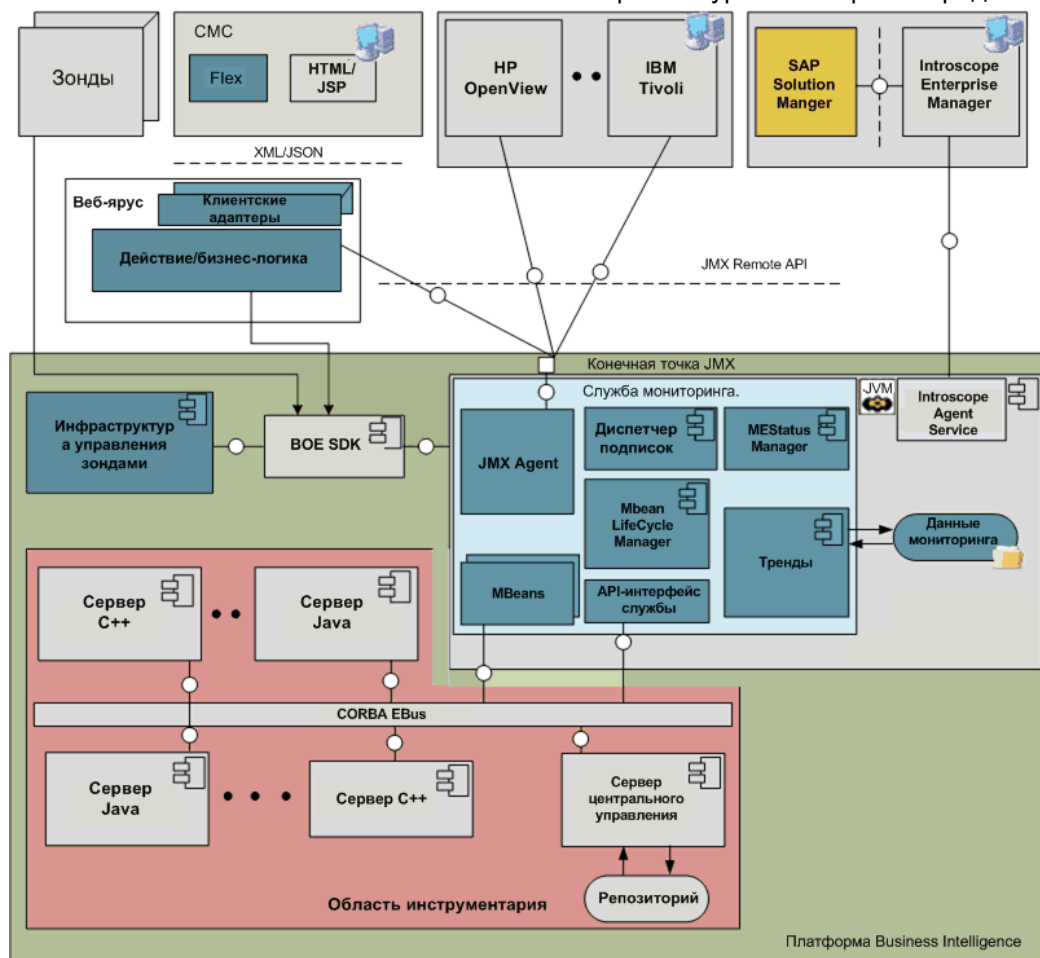
График тенденций – это графическое представление хронологии данных показателей, созданных зондами и серверами. Он помогает администратору отслеживать поведение системы в различные периоды времени и оценивать динамику ее использования.

Предупреждение

Предупреждение – это уведомление, создаваемое приложением мониторинга при достижении порогового значения, заданного пользователем для различных показателей, которые используются для наблюдения. Получать предупреждения можно либо по электронной почте, либо просматривать их на странице "Информационная панель".

15.2.1 Архитектура

В этом разделе представлен общий обзор архитектуры мониторинга и кратко поясняются роли, выполняемые ее компонентами. Ниже архитектура мониторинга представлена графически:



Далее перечислены компоненты архитектуры высокого уровня:

- Сервер на платформе Java (PJS)
- Агент и сервер для расширений Java Management (JMX)
- Объекты MBean
- Клиенты JMX
- Консоли управления
- База данных тенденций

Служба мониторинга размещена на сервере Java платформы. Приложение основано на технологии JMX.

Служба Java платформы мониторинга предоставляет базовые услуги, доступные в приложении мониторинга. Java-служба платформы мониторинга предоставляет следующие услуги:

- Предоставление услуг агента JMX.
- Динамическое создание объектов MBeans для серверов SAP BusinessObjects.
- Обеспечение управления жизненным циклом для объектов MBeans.
- Предоставляет механизм для регистрации новых зондов.
- Предоставление пользователям возможности создавать сложные пороговые условия с использованием показателей серверов.
- Предоставление порогового механизма для уведомлений и отправка предупреждений.
- Предоставление функции выявления тенденций в сохраненных исторических данных.

Служба планирования зонда, размещенная на адаптивном сервере заданий, управляет выполнением и планированием зондов. Поэтому для выполнения зондов должен быть запущен адаптивный сервер заданий.

Приложение мониторинга также предоставляет доступ к URL конечной точки JMX или удаленного вызова методов (RMI). Другие приложения масштаба предприятия, такие, как SAP Solution Manager и IBM Tivoli Monitoring, могут подключаться к приложению мониторинга и получать доступ к показателям SAP BusinessObjects, используя интерфейс JMX Remote API. Для хранения исторических данных и выявления тенденций приложение мониторинга использует выделенную базу данных Derby. Сведения о схеме базы данных тенденций см. в разделе [Схема БД выявления тенденций](#).

15.2.1.1 Схема БД выявления тенденций

В пояснениях к приведенным ниже диаграмме и таблице для базы данных тенденций показаны таблицы, в которых регистрируются сведения о показателях, тестах и наблюдениях, а также взаимосвязь этих таблиц.

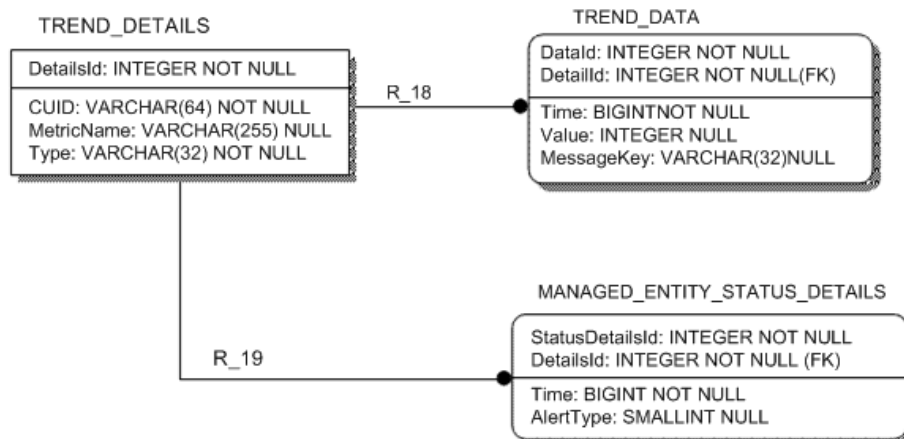


Таблица 15-1: TREND_DETAILS

В этой таблице регистрируются сведения об управляемых объектах, тестах и наблюдениях. Например, CUID и имена показателей.

Имя столбца	Описание	Первичный ключ
DetailsId		Создается автоматически
CUID (64)	CUID для InfoObject (или) уникальный ид. для объектов, которые не являются InfoObject	NOT NULL
MetricName	Имя показателя	NOT NULL
Тип (32)	Типы подписки или показателя	NOT NULL

Таблица 15-2: TREND_DATA

В этой таблице регистрируются данные тенденций из показателей, наблюдений и тестов. Например, значение показателя и время.

Имя столбца	Описание	Первичный ключ
DataId		Создается автоматически
DetailsId		Внешний ключ
Время	Время, когда были собраны данные	NOT NULL
Значение	Значение показателя или подписки	Нет

Таблица 15-3: MANAGED_ENTITY_STATUS_DETAILS

В этой таблице регистрируются данные о нарушениях подписки и сведения о доставке предупреждений. Например, время нарушения и время доставки предупреждения.

Имя столбца	Описание	Первичный ключ
StatusDetailsId		Создается автоматически
DetailsId		Внешний ключ
Время	Время, когда были собраны данные	NOT NULL
AlertType	Тип доставки уведомления о подписке (например, по электронной почте)	Нет

15.3 Поддержка кластеров для сервера мониторинга

Приложение мониторинга поддерживает кластеры. Кластеры просты в реализации и обеспечивают восстановление после сбоев.

При использовании поддержки кластера в каждый момент времени будет активна только одна служба, а все прочие службы будут пассивны. Предположим, что в кластеризованной среде имеется две службы мониторинга, s1 и s2. Доступной должна быть только одна из них. Однако активными пытаются стать и s1, и s2. Успеха сможет добиться только одна из служб, а другая останется неактивной или пассивной.

Пассивные службы продолжают периодически (раз в минуту) проверять доступность активной службы. Если активная служба недоступна, пассивная служба немедленно выполняет попытку стать активной.

Примечание:

Рекомендуется размещать службу мониторинга на отдельном экземпляре адаптивного сервера обработки (APS), чтобы исключить вероятность сбоев, перезагрузки или ухудшения производительности APS.

15.4 Показатели

Существует множество показателей, которые могут использоваться при создании наблюдений. Показатели бывают следующими:

- Показатели зонда
- Показатели сервера
- Показатели хоста
- Производные показатели

При запуске зонда по умолчанию генерируются показатели `Время выполнения` и `Пройдено`. Эти показатели называются виртуальными.

Показатели сервера платформы SAP BusinessObjects Business Intelligence 4.0 перечислены в следующей таблице:

Сервер	Показатели
Адаптивный сервер обработки	

Сервер	Показатели
	<ul style="list-style-type: none"> • Аудит полученных событий • AuditingMetrics.number для событий в очереди • Доступные процессоры • Занятые потоки на сервере • Процент использования ЦП • Число кубов • 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 • Число сбойных попыток извлечения с момента запуска службы • Объем свободной памяти • Счетчик заблокированных потоков JVM • Количество конфликтов при блокировках JVM • Максимальный объем памяти • Количество полноценных GC • Число страничных сбоях при GC • Процент остановок системы при GC • Число запросов • Состояние включения сервера • Состояние работы сервера • Число сеансов • Число успешных попыток извлечения с момента запуска сервера • Потоки на транспортном уровне

Сервер	Показатели
	<ul style="list-style-type: none">• Общий объем памяти• Размер пула потоков транспортного уровня
Центральный сервер управления	

Сервер	Показатели
	<ul style="list-style-type: none"> • Использование потока аудита • Среднее время реакции для фиксации с момента запуска (мс) • Среднее время ответа на запрос с момента запуска (мс) • Занятые потоки на сервере • ЦПУ • Завершенные задания • Текущие подключения к системной базе данных • Размер диска (Гбайт) • Установленные подключения к системной базе данных • Существующие учетные записи одновременно работающих пользователей • Существующие учетные записи именованных пользователей • Задания, завершившиеся сбоем • Максимальное время фиксации отклика с момента запуска (мс) • Максимальное время обработки запроса с момента запуска (мс) • Число фиксаций с момента запуска • Число объектов в системном кэше CMS • Число объектов в системной БД CMS • Число запросов с момента запуска • Число сеансов, созданных всеми пользователями • Число сеансов, созданных параллельно работающими пользователями • Число сеансов, созданных именованными пользователями • Число сеансов, созданных серверами • Число регистраций пользователей в системе с момента запуска • PID • Максимальное число пользовательских сеансов с момента запуска • Ожидающие задания • Незавершенные запросы в системную БД • ОЗУ (Мбайт) • Выполняющиеся задания • Состояние включения сервера • Состояние ожидания сервера • Используемое дисковое пространство (Гбайт) • Ожидающие задания • Последнее обновление базы данных аудита • Длительность последнего цикла опроса потока аудита (секунды)

Сервер	Показатели
	<ul style="list-style-type: none"> • Аудитор CMS • Лицензии для параллельно работающих пользователей • Подключение к базе данных аудита установлено • Текущее число событий аудита в очереди • Лицензии для именованных пользователей
Сервер соединений	<ul style="list-style-type: none"> • Занятые потоки на сервере • ЦПУ • Размер диска • PID • ОЗУ • Состояние включения сервера • Состояние работы сервера • Использованное дисковое пространство
Сервер подключений 32	<ul style="list-style-type: none"> • Занятые потоки на сервере • ЦПУ • Размер диска • PID • ОЗУ • Состояние включения сервера • Состояние работы сервера • Использованное дисковое пространство
Сервер обработки Crystal Reports 2010	<ul style="list-style-type: none"> • Занятые потоки на сервере • ЦПУ • Обслуживание CrystalReports через серверы страниц и кэширования • Размер диска (ГБ) • PID • ОЗУ (МБ) • Состояние включения сервера • Состояние работы сервера • Использованное дисковое пространство

Сервер	Показатели
Crystal Reports 2010 Report Application Server	<ul style="list-style-type: none"> • Занятые потоки на сервере • ЦПУ • Обслуживание CrystalReports через серверы Report Application Server • Размер диска (ГБ) • PID • ОЗУ (МБ) • Состояние включения сервера • Состояние работы сервера • Использованное дисковое пространство • Текущее число событий аудита в очереди • Текущее число потоков агента • Текущее число документов • Общее число потоков агента • Общее число документов
Кэш-сервер Crystal Reports	<ul style="list-style-type: none"> • Занятые потоки на сервере • ЦПУ • Размер диска (ГБ) • PID • ОЗУ (МБ) • Состояние включения сервера • Состояние работы сервера • Использованное дисковое пространство
Сервер обработки Crystal Reports	<ul style="list-style-type: none"> • Занятые потоки на сервере • ЦПУ • CrystalReportsservicethroughPageandCacheServer executiontime • Размер диска (ГБ) • PID • ОЗУ (МБ) • Состояние включения сервера • Состояние работы сервера • Используемое дисковое пространство (ГБ)

Сервер	Показатели
Сервер аналитики информационных панелей	<ul style="list-style-type: none"> • Занятые потоки на сервере • ЦПУ • Размер диска • PID • ОЗУ • Состояние включения сервера • Состояние работы сервера • Использованное дисковое пространство
Сервер информационных панелей	<ul style="list-style-type: none"> • Занятые потоки на сервере • ЦПУ • Размер диска • PID • ОЗУ • Состояние включения сервера • Состояние работы сервера • Использованное дисковое пространство • Текущее число событий аудита в очереди
Сервер событий	<ul style="list-style-type: none"> • Занятые потоки на сервере • ЦПУ • Размер диска (ГБ) • Отслеживаемые файлы • PID • ОЗУ (МБ) • Состояние включения сервера • Состояние работы сервера • Используемое дисковое пространство (ГБ) • Текущее число событий аудита в очереди

Сервер	Показатели
Репозиторий входящих файлов	<ul style="list-style-type: none"> • Активные соединения • Активные файлы • Доступное дисковое пространство в корневом каталоге (%) • Доступное дисковое пространство в корневом каталоге (Гбайт) • Занятые потоки на сервере • ЦПУ • Передано данных (Мбайт) • Записано данных (Мбайт) • Размер диска (ГБ) • Свободное дисковое пространство в корневом каталоге (Гбайт) • PID • ОЗУ (МБ) • Состояние включения сервера • Состояние работы сервера • Общее дисковое пространство в корневом каталоге (Гбайт) • Используемое дисковое пространство (ГБ)
Репозиторий исходящих файлов	<ul style="list-style-type: none"> • Активные соединения • Активные файлы • Доступное дисковое пространство в корневом каталоге (%) • Доступное дисковое пространство в корневом каталоге (Гбайт) • Занятые потоки на сервере • ЦПУ • Передано данных (Мбайт) • Записано данных (Мбайт) • Размер диска (ГБ) • Свободное дисковое пространство в корневом каталоге (Гбайт) • PID • ОЗУ (МБ) • Состояние включения сервера • Состояние работы сервера • Общее дисковое пространство в корневом каталоге (Гбайт) • Используемое дисковое пространство (ГБ)

Сервер	Показатели
Сервер репозитория РМ	<ul style="list-style-type: none">• Занятые потоки на сервере• ЦПУ• Размер диска• PID• ОЗУ• Состояние включения сервера• Состояние работы сервера• Использованное дисковое пространство
Сервер контейнера веб-приложений	<ul style="list-style-type: none">• Состояние включения сервера• Состояние работы сервера

Сервер	Показатели
Сервер обработки Web Intelligence	<ul style="list-style-type: none"> • Занятые потоки на сервере • Использование ЦП (%) • ЦПУ • Уровень максимального использования кеша • Размер кеша (кбайт) • Текущее число активных сеансов • Текущее число вызовов клиента • Текущее число сеансов • Текущее число задач • Размер диска (ГБ) • Верхний порог использования памяти • Уровень памяти • Максимальный порог использования памяти • Число операций подкачки документов • Число таймаутов документов • Число документов • Число подкаченных документов • Число пользователей • PID • ОЗУ (МБ) • Состояние включения сервера • Состояние работы сервера • Общее время работы ЦП (секунд) • Общее число вызовов клиента • Общее число сеансов • Общее число задач • Используемое дисковое пространство (ГБ) • Размер виртуальной памяти (МБ) • Размер памяти WebI (МБ) • Сервер WebI (таймаут) • Текущее число событий аудита в очереди
Сервер кэширования данных Xcelsius	<ul style="list-style-type: none"> • Занятые потоки на сервере • ЦПУ • Размер диска • PID • ОЗУ • Состояние включения сервера • Состояние работы сервера • Используемое дисковое пространство
Сервер обработки данных Xcelsius	

Сервер	Показатели
	<ul style="list-style-type: none"> • Занятые потоки на сервере • ЦПУ • Размер диска • PID • ОЗУ • Состояние включения сервера • Состояние работы сервера • Использованное дисковое пространство

Примечание:

При добавлении нового сервера или запуске существующего сервера, показатели которого не отображаются на странице показателей, следует подождать появления показателей на этой странице в течение примерно 10 минут.

15.5 Свойства конфигурации

В этом разделе описаны свойства приложения мониторинга и способы их изменения.

Чтобы просмотреть свойства конфигурации приложения мониторинга, выполните следующие действия:

1. Перейдите в область **Программные приложения СМС**.
2. Правой кнопкой мыши щелкните **Мониторинг** и выберите пункт меню **Свойства**. Откроется окно «Свойства приложения мониторинга». Настраиваемые свойства описаны в следующей таблице:

Раздел	Поле	Описание
	Включить приложение мониторинга	Установите этот флажок, чтобы включить функции мониторинга. Если сбросить флажок, будут отключены все функции мониторинга, кроме тестов. Выявление тенденций в тестах также будет отключено.
	URL конечной точки агента JMX по умолчанию (IIOP)	URL-адрес конечной точки агента JMX по умолчанию, использующего протокол IIOP. Этот адрес генерируется автоматически, если включить мониторинг и затем перезагрузить сервер. Этот протокол используется по умолчанию для службы мониторинга. Это поле доступно только для чтения.

Раздел	Поле	Описание
RMI	Включить протокол RMI для JMX	По умолчанию данный параметр отключен. При включении параметра необходимо указать номер порта RMI. Этот порт будет использоваться как записью RMI в реестре, так и коннектором порта RMI. Этот порт должен быть доступен службе, в противном случае запуск службы будет невозможен. Указав номер порта RMI, перезапустите сервер. После перезагрузки сервера создается URL-адрес конечной точки агента RMI JMX. Это свойство доступно только для чтения и содержит URL-адрес конечной точки агента JMX, использующего протокол RMI. Используйте этот URL-адрес, чтобы подключить к процессу мониторинга другие клиенты.
Показатели хоста	Включить показатели хоста	По умолчанию данный параметр отключен. При включении этого параметра необходимо указать путь к каталогу установки двоичного файла SAPOSCOL. Для включения показателей хоста необходимо установить SAPOSCOL. Дополнительные сведения о порядке установки SAPOSCOL см. в разделе Установка SAPOSCOL

Раздел	Поле	Описание
Другие настройки	Интервал обновления показателя (в секундах)	<p>Минимальный интервал, который можно указать, – 15 секунд. Этот интервал управляет следующими аспектами:</p> <ul style="list-style-type: none"> Расчет подписки наблюдений: правила предостережения и опасности постоянно рассчитываются с указанным здесь интервалом. Расчет состояния наблюдения: состояние наблюдения вычисляется постоянно с интервалом, указанным в периоде обновления показателя, если настройка "Событие" наблюдения выбрана с параметром Изменять статус наблюдения каждый раз, когда правило "Опасно" или "Внимание" принимает значение true. Период трендинга: режим журнала для графиков всегда анализируется с указанным здесь интервалом.
	Удалять старые данные, когда размер базы данных превышает (МБ)	В базе данных выявления тенденций будет проведена очистка данных, если ее размер превысит указанный предел. Для базы данных создается 30% буфер. Например, если размер указан равным 100 МБ и размер базы данных стал больше 100 МБ, при проверке системы база данных будет уменьшена до 70 МБ.
	Интервал автоматического обновления пользовательского интерфейса наблюдения (в секундах)	Этот интервал будет использоваться в пользовательском интерфейсе мониторинга (информационная панель, список наблюдений и зонды) для автоматического обновления. Минимальный интервал – 15 секунд. Автоматическое обновление не влияет на длительность в режиме Live на графиках, настроенную на 15 секунд по умолчанию.
	Запускать задание очистки базы данных ежедневно в	Задание по очистке базы данных запускается в указанное время. База данных будет очищена, когда ее размер превысит указанный минимум.
	Резервное копирование базы данных тренда	По умолчанию данный параметр отключен. Если этот параметр включен, задача резервного копирования базы данных тренда запускается в указанное время.

Раздел	Поле	Описание
	Каталог резервного копирования базы данных тренда	По умолчанию местоположение не указано. Можно указать местоположение, однако путь должен быть не относительным, а абсолютным. В случае общего каталога, следует предоставить разрешение на доступ к этому каталогу.
	Выполнение задач резервного копирования базы данных	Задача резервного копирования базы данных запускается при щелчке этого параметра. Перед выбором этого параметра укажите местоположение каталога резервного копирования базы данных.
	Местоположение базы данных тренда	По умолчанию база данных выявления тенденций находится в BOE_Install_Dir\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0/Data/TrendingDB. Можно указать и другой путь, однако он должен быть не относительным, а абсолютным. В случае кластеризованной среды местоположение может быть общим каталогом, и следует предоставить разрешение доступа к этому каталогу.

3. Нажмите кнопку **Сохранить**.

Примечание:

При изменении этих свойств, за исключением включения и выключения приложения мониторинга, необходимо перезапустить службу мониторинга, расположенную на адаптивном сервере обработки.

Установка SAPOSCOL

Выполните следующие действия для установки SAPOSCOL:

1. Загрузите SAPHOSTAGENT710_XX.SAR из SAP Marketplace (<http://service.sap.com>).
2. Извлеките SAPHOSTAGENT710_XX.SAR, выполнив команду `SAPCAR.EXE -xvf SAPHOSTAGENT710_XX.SAR`.
3. Установите saphostexec, выполнив команду `saphostexec.exe -install`. После установки saphostexec в качестве службы запускается SAPOSCOL.
4. Проверьте состояние SAPOSCOL, выполнив команду `saposcol -s`.

15.5.1 URL-адрес конечной точки JMX

Приложение мониторинга предоставляет URL-адрес конечной точки JMX, через которую могут подключиться другие клиенты, используя интерфейс JMX Remote API. По умолчанию связь в JMX предоставляется через транспортный уровень IIOP (протокол Internet Inter-Orb Protocol) или CORBA (архитектура Common Object Request Broker Architecture). URL-адрес подключения отображается на странице свойств приложения мониторинга. Возможность подключения по протоколу IIOP упраздняет необходимость беспокоиться о брандмауэрах и предоставлении доступа к портам. Порты CORBA доступны по умолчанию. Чтобы обеспечить возможность подключения, на стороне клиента JMX нужны jar-файлы, перечисленные в следующей таблице:

Jar-файлы
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

Другой вариант подключения – через порт RMI по умолчанию. Для получения дополнительных сведений о подключении через порт RMI см. раздел [Свойства конфигурации](#).

15.6 Интеграция с другими приложениями

Решения Enterprise, такие как SAP Solution Manager и IBM Tivoli Monitoring, интегрируются с приложением мониторинга как клиенты JMX, подключающиеся через URL конечной точки JMX. После интеграции показателя SAP BusinessObjects можно просматривать из пользовательского интерфейса клиента.

15.6.1 Интеграция приложения мониторинга с IBM Tivoli

Для интеграции приложения мониторинга с IBM Tivoli необходимо создать, установить и настроить агент мониторинга IBM Tivoli. Чтобы создать агент мониторинга IBM Tivoli, выполните следующие шаги:

1. Установите ПО конструктора агента мониторинга IBM Tivoli версии 6.2.1.
2. Создайте новый агент. Сведения о порядке создания нового агента см. в руководстве пользователя IBM Tivoli Monitoring Agent.
3. На этапе определения типов данных мониторинга выберите Данные с сервера в области **Категории данных мониторинга** и JMX в области **Источники данных**.
4. Нажмите кнопку **Далее**.
5. В окне «Сведения о JMX» нажмите кнопку **Просмотр**, чтобы просмотреть все объекты JMX MBeans на сервере MBean.

Примечание:

Если браузер используется впервые, необходимо добавить новое подключение.

6. В окне «Браузер для расширений Java Management (JMX)» щелкните + рядом с полем **Имя подключения**, чтобы добавить новое подключение.
7. В окне «Мастер подключения к серверу MBean» выберите Стандартные подключения к JMX (JSR-160).
8. В окне «Свойства соединения» введите следующие данные:

Поле	Описание
Имя соединения	Сервер, совместимый с JSR-160
Идентификатор пользователя	Имя пользователя, используемое для входа в систему SAP BusinessObjects Enterprise
Пароль	Пароль, используемый для входа в систему SAP BusinessObjects Enterprise
URL-адрес службы	Укажите URL-адрес конечной точки JMX

9. Нажмите кнопку **Готово**.

10. В области **Ключевые свойства MBean** выберите Домен и Тип.

Все объекты MBeans появятся в текстовом поле ниже.

11. Выберите все объекты MBeans с доменом "Серверы", поочередно и по одному, чтобы просмотреть список атрибутов. Выберите ключевой атрибут, если допускается наличие нескольких объектов MBeans одного типа. Например, если выполняется два экземпляра сервера, ключевым атрибутом может быть PID каждого из экземпляров.
12. В окне «Общие параметры агента JMX» выберите сервер и параметры для группы атрибутов JMX.
13. В окне «Определение источника данных» выделите добавленный агент и нажмите кнопку **Добавить к выбранным**. При этом будет выполнен переход к началу цикла создания агента и для добавления другого сервера в список отслеживаемых нужно повторить перечисленные выше шаги.
14. Созданный агент необходимо установить. дополнительные сведения о порядке установки агента см. в руководстве пользователя IBM Tivoli Monitoring Agent на рис. 154 и далее. В этом разделе представлены сведения о локальной установке агента, а также о создании для него устанавливаемого решения.

Примечание:

Если агент для SAP BusinessObjects Enterprise создается с помощью конструктора агента, то в той же системе должна быть установлена платформа SAP BusinessObjects Business Intelligence 4.0. Однако при установке уже созданного агента с помощью его файла установщика наличие установленного приложения мониторинга BOE не требуется, поскольку при настройке можно указать данные любой системы с конечной точкой JMX.

Для настройки установленного агента выполните следующие действия:

1. Откройте «Управление службами мониторинга Tivoli Enterprise» в режиме TEMS. Появится установленный агент.
2. Щелкните правой кнопкой мыши шаблон агента и выберите команду **Настроить по умолчанию**.
3. Выберите имя экземпляра.

Агент можно настроить на использование двух разных протоколов: RMI и BOEIIOP.

Чтобы использовался протокол RMI:

- Нажмите кнопку **Далее**. Не вносите какие-либо изменения в параметры Java.
- Задайте значения для учетных данных JMX, такие как идентификатор пользователя, пароль и URL службы. Для получения дополнительных сведений см. *Свойства конфигурации* в связанных разделах.
- Нажмите кнопку **ОК**.

Чтобы использовался протокол BOEIIOP:

- Скопируйте файлы `bcm.jar` и `cryptojFIPS.jar` из папки `%InstallDir%\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib` в папку системы.
- В другую папку скопируйте jar-файлы, перечисленные в следующей таблице.
- В параметрах Java задайте аргументы `JVM -Djmx.remote.protocol.provider.pkgs = com.businessobjects.sdk.monitoring` и `-Djmx.boeiiop.bcm.dir=<` для места

расположения папки, в которую были скопированы файлы `bcm.jar` и `cryptojFIPS.jar`.

- Выберите **Далее**.
- Задайте значения для учетных данных JMX, такие как идентификатор пользователя, пароль и URL службы. Для получения дополнительных сведений см. *Свойства конфигурации* в связанных разделах.
- В поле **<Каталоги Jar>** укажите путь к папке, в которую был скопирован список jar-файлов, перечисленных в таблице.
- Нажмите кнопку **ОК**.

Jar-файлы
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. Правой кнопкой мыши щелкните агент и выберите команду **Пуск** в окне «Управление службами мониторинга Tivoli Enterprise».

5. Откройте рабочий стол/клиент браузера портала IBM Tivoli Enterprise. В окне «Навигатор» появится кнопка.
6. Нажмите кнопку "Навигатор".
Агент будет добавлен в модуль навигатора.

См. также

- [Свойства конфигурации](#)

15.6.2 Интеграция приложения мониторинга с SAP Solution Manager

Чтобы интегрировать приложение мониторинга с SAP Solution Manager, на локальном компьютере необходимо установить и запустить [Wily Introscope](#). SAP Solution Manager должен быть настроен как рабочая станция Introscope. При установке платформы SAP BusinessObjects Business Intelligence 4.0 выполните следующие действия:

1. На этапе настройки связи с Introscope Enterprise Manager укажите данные для имени хоста и порта. Агент Introscope будет установлен в каталоге C:\Program Files (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\java\Wiley в процессе установки платформы SAP BusinessObjects Business Intelligence 4.0.
2. Запустите рабочую станцию Introscope и нажмите кнопку **Новый исследователь**. Можно просматривать показатели сервера SAP BusinessObjects и виртуальные показатели зондов в разделе JMX настроенного агента.

Примечание:

Можно настроить агент Introscope (IS), выбрав **СМС > Серверы > Узел сервера > Заполнители**. Здесь также указываются хост и порт IS Enterprise Manager для связи агента IS с приложением мониторинга. Дополнительные сведения см. в разделе *Управление серверами* в справочном руководстве *SAP BOE СМС*.

Для обеспечения доступности показателей JMX в IS убедитесь, что в экземпляре AdaptiveProcessingServer доступны как службы агента IS, так и служба мониторинга.

При включении инструментальных средств IS инструментарий кода включается автоматически.

15.7 Создание юниверса для базы данных Derby

Наличие юниверса для базы данных Derby позволяет выполнять запросы к базе данных Derby с целью создания отчетов и выполнения анализа данных. Для получения дополнительных сведений о создании юниверса см. руководство *SAP BOE Universe Designer*.

Примечание:

Создание юниверса для базы данных Derby возможно только после выполнения задач резервного копирования для базы данных. Для получения дополнительных сведений о выполнении задач см. раздел *Свойства конфигурации* в ссылках.

1. Для создания юниверса для базы данных Derby можно использовать средство создания юниверсов.

Для получения дополнительных сведений о создании юниверса с использованием этого мастера см. раздел *Использование мастера быстрого создания* в руководстве *SAP BOE Universe Designer*.

Для создания используются два подключения к базе данных – Apache и Generic.

2. Если выбрано подключение Apache, выполните следующие действия:

- a. Нажмите кнопку **Драйверы JDBC**
- b. Выберите файл `derby.sbo` по адресу `INSTALL_DIR\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer\jdbc`.
- c. Добавьте путь класса `<ClassPath> <Path>...\..\derby.jar</Path></ClassPath>`.
Перед добавлением пути класса загрузите последнюю версию файла `derby.jar` (версия 10.5.x) с веб-сайта Apache.
- d. Чтобы создать новое подключение к базе данных Apache, введите расположение папки базы данных Derby в поле **Сервер**.
Если база данных расположена по адресу `C:\Derby`, введите `C:\Derby;create=false`

3. Если выбрано подключение Generic, выполните следующие действия:

- a. Выберите команду **Generic JDBC**.
- b. Выберите файл `jdbc.sbo` из каталога `INSTALL_DIR\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer\jdbc`.
- c. Добавьте путь класса `<ClassPath> <Path>...\..\derby.jar</Path></ClassPath>` и сведения JDBC-класса `<Parameter Name="JDBC Class">org.apache.derby.jdbc.EmbeddedDriver</Parameter>`
- d. При создании нового подключения к базе данных Generic введите в поле URL строку `jdbc:derby:C:\Derby;create=false`.

См. также

- [Свойства конфигурации](#)

15.8 Устранение неполадок

В этом разделе приводятся пошаговые способы решения широкого диапазона проблем, которые могут возникать при работе с приложением мониторинга.

15.8.1 Панель мониторинга

На странице СМС не отображается ссылка для мониторинга

- Проверьте наличие у пользователя необходимых прав доступа.
- Убедитесь, что пользователь добавлен в группы "Пользователи приложения мониторинга", "Администраторы", либо в любую другую группу, входящую в состав упомянутых выше групп.

В панели мониторинга не отображаются ключевые показатели производительности (КРІ)

- Убедитесь, что отображаются обязательные показатели. Для этого выберите команды **Свойства сервера > Показатели**.
- Убедитесь, что отклик Центрального сервера управления соответствует ожиданиям.

Не удается запустить приложение мониторинга

Загрузите и установите последнюю версию приложения Flash Player (10.5.x)

15.8.2 Сигналы

Отсутствие сигналов на странице "Сигналы"

- Убедитесь, что выбран параметр **Включить оповещение** в параметрах области **Уведомление**.
- Проверьте наличие необходимых прав доступа для получения предупреждений.
- Убедитесь, что на информационной панели мониторинга отображаются последние предупреждения.
- Проверьте работоспособность сервера SMTP.
- Проверьте правильность идентификатора электронной почты, настроенного для получения предупреждений по электронной почте.
- Убедитесь, что включен экземпляр AdaptiveJobServer.
- Проверьте параметры SMTP в адресате экземпляра AdaptiveJobServer.

Примечание:

Можно отправить документ CR на заданный идентификатор электронной почты, чтобы проверить работоспособность протокола SMTP.

15.8.3 Список наблюдений

Не удается извлечь данные журнала для наблюдений

- Проверьте интервал опроса на странице **Свойства** приложения мониторинга.
- Проверьте файл трассировки в папке журнала.
- Проверьте, указан ли параметр **Местоположение базы данных тренда** на странице **Приложения СМС**. В кластеризованной среде проверьте наличие у пользователя разрешений на доступ к общему местоположению. Для получения дополнительных сведений см. *Свойства конфигурации* в связанных разделах.
- Убедитесь, что системное время сервера и клиента совпадает в пределах заданного часового пояса.

Произошла ошибка при извлечении синхронизированных данных реального времени

Убедитесь, что экземпляр AdaptiveProcessingServer работает.

Вкладка "Список наблюдений" отключена

- Убедитесь, что сервер, которому назначен показатель, работает.
- Убедитесь, что в соответствующем показателе на странице списка показателей отображаются сведения в режиме реального времени и журнала.
- Проверьте наличие сообщений об ошибках в журналах службы мониторинга.
- Убедитесь, что показатель отображается в jconsole.

См. также

- [Свойства конфигурации](#)

15.8.4 Зонды

Не удается запланировать зонды

- Убедитесь, что выполняется экземпляр AdaptiveJobServer.
- Проверьте правильность идентификатора CUID отчета, используемого для документов Crystal reports и Web Intelligence.
- Убедитесь, что пользователь имеет права администратора или является членом группы администраторов.
- Убедитесь, что пользователь обладает достаточными правами на открытие, обновление и экспорт документов Crystal Reports или Web Intelligence, которые используются в соответствующих зондах.

Зонд имеет состояние планирования «отложено»

- Проверьте, установлен ли экземпляр ProbeSchedulingService.
- Убедитесь, что выполняется экземпляр AdaptiveJobServer.

Произошла ошибка при извлечении данных тренда из базы данных

Убедитесь, что экземпляр AdaptiveProcessingServer работает.

Сбой выполнения probeRun.bat

- Убедитесь, что задано значение `java_home`
- Проверьте правильность ввода параметров в командной строке.

Примечание:

Введите команду `probeRun.bat -help` в командной строке, чтобы проверить правильность всех параметров

15.8.5 Показатели

Показатели хоста не приводятся

- Убедитесь, что выполняется SAPOSCOL.
- Убедитесь, что на странице **Свойства** приложения мониторинга выбран параметр **Включить показатели хоста**.
- Чтобы изменения вступили в силу, перезапустите экземпляр AdaptiveProcessingServer.
- Проверьте правильность параметра **Путь к установке двоичного файла SAPOSCOL**.

Произошла ошибка при извлечении клиента JMX

Убедитесь, что экземпляр AdaptiveProcessingServer работает.

Нулевое значение показателя SAPOSCOL на странице "Показатель"

- Убедитесь, что выполняется SAPOSCOL.
- Выполните следующие команды на хосте, на котором установлен SAPOSCOL:
 1. `saposcol -s` – проверка состояния
 2. `saposcol -m` – получение моментального снимка данных, собранных SAPOSCOL

15.8.6 Диаграмма

На диаграммах показываются различные периоды в динамическом режиме или режиме журнала

Убедитесь, что системное время сервера и клиента совпадает в пределах заданного часового пояса.

Данные диаграмм не отображаются в режиме журнала для кластерного сценария

Убедитесь, что все экземпляры AdaptiveProcessingServer указывают на одно и то же расположение базы данных.

Аудит

16.1 Обзор

Функция аудита позволяет хранить записи о значительных событиях на серверах и приложениях, что помогает отслеживать, к каким сведениям осуществляется доступ, как этот доступ осуществляется, как изменяется информация и кто выполняет эти операции. Эти сведения записываются в базе данных под названием "Хранилище данных аудита" (ADS). После записи данных в ADS можно создавать необходимые пользовательские отчеты для удовлетворения конкретных потребностей пользователя. Образцы универсов и отчетов можно найти в [SAP Developer Network](#).

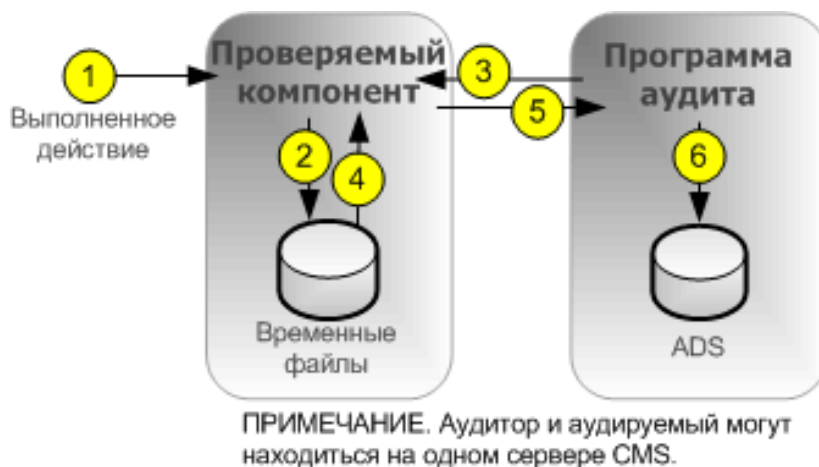
В целях, указанных в этом разделе, аудитор – система, отвечающая за запись или хранение информации о событии, а проверяемый компонент – любая система, отвечающая за выполнение проверяемого события. Существуют обстоятельства, когда одна система может выполнять обе функции.

Как работает аудит

Центральный сервер управления (CMS) выполняет роль аудитора системы, а сервер или приложение, инициирующее проверяемое событие, выполняют роль проверяемого компонента. Если происходит событие, подлежащее аудиту, в проверяемом компоненте создается запись, которая сохраняется в локальном временном файле. С регулярными интервалами CMS производит обмен данными с проверяемыми компонентами с целью запроса этих записей и записи данных в ADS.

Сервер CMS также управляет синхронизацией событий аудита, которые выполняются на различных компьютерах. Каждый проверяемый компонент предоставляет метку времени для записываемых им событий аудита. Для обеспечения согласованности меток времени событий на различных серверах сервер CMS периодически рассылает информацию о системном времени проверяемым компонентам. Затем проверяемые компоненты сверяют это время с внутренним временем. Если существует разница, проверяемые компоненты изменяют время записи для последующих событий аудита.

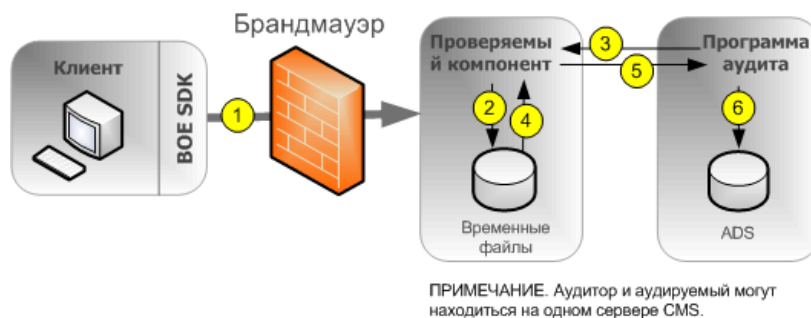
В зависимости от типа клиента для записи событий в системе используется один из следующих потоков.

Аудит сервера

1. Событие, подлежащее аудиту, выполняется сервером.
2. Проверяемый компонент записывает события во временный файл.
3. Аудитор опрашивает проверяемый компонент и запрашивает пакет событий аудита.
4. Проверяемый компонент извлекает события из временных файлов.
5. Проверяемый компонент передает события программе аудита.
6. Аудитор записывает события в ADS и сообщает проверяемому компоненту, что следует удалить события из временных файлов.

Аудит клиентского входа в систему для клиентов, подключающихся через CORBA.

Сюда относятся такие приложения, как SAP BusinessObjects Web Intelligence.



1. Клиент подключается к CMS, который выполняет роль проверяемого компонента. Клиент предоставляет IP-адрес и имя компьютера, а проверяемый компонент проверяет эти данные.

Примечание:

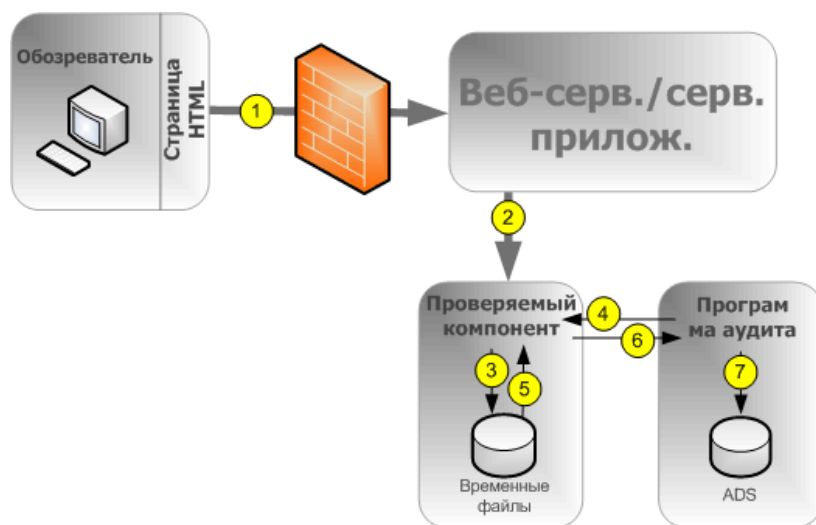
Следует открыть порт в межсетевом экране между клиентом и CMS. Для получения дополнительных сведений о брандмауэрах см. раздел, посвященный безопасности в *Руководстве администратора платформы SAP BusinessObjects Business Intelligence*.

2. Проверяемый компонент записывает события во временный файл.
3. Аудитор опрашивает проверяемый компонент и запрашивает пакет событий аудита.
4. Проверяемый компонент извлекает события из временных файлов.
5. Проверяемый компонент передает события программе аудита.

6. Аудитор записывает события в ADS и сообщает проверяемому компоненту, что следует удалить события из временных файлов.

Аудит клиентского входа в систему для клиентов, подключающихся через HTTP.

Сюда относятся такие интерактивные приложения, как стартовая панель BI, Central Management Console, SAP BusinessObjects Web Intelligence и другие.

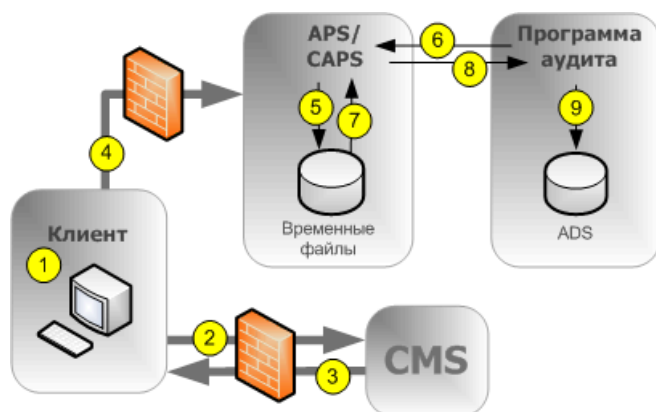


ПРИМЕЧАНИЕ. Аудитор и аудируемый могут находиться на одном сервере CMS.

1. Браузер подключается к серверу веб-приложения, и на него передаются данные входа в систему.
2. SDK платформы BI отправляет запрос входа, а также IP-адрес и имя компьютера, на котором установлен браузер, проверяемому компоненту (CMS).
3. Проверяемый компонент записывает события во временный файл.
4. Аудитор опрашивает проверяемый компонент и запрашивает пакет событий аудита.
5. Проверяемый компонент извлекает события из временных файлов.
6. Проверяемый компонент отправляет события аудитору.
7. Аудитор записывает события в ADS и сообщает проверяемому компоненту, что следует удалить события из временных файлов.

Аудит отсутствия входа в систему для клиентов, подключающихся через CORBA

Этот рабочий процесс применяется к аудиту событий SAP BusinessObjects Web Intelligence при подключении через CORBA.



1. Пользователь выполняет операцию, которая подлежит аудиту.
2. Клиент устанавливает связь с CMS для проверки, настроена ли операция на аудит.
3. Если для действия назначен аудит, CMS сообщает эту информацию клиенту.
4. Клиент отправляет сведения о событии прокси-службе аудита клиента (CAPS), размещенной на адаптивном сервере обработки.

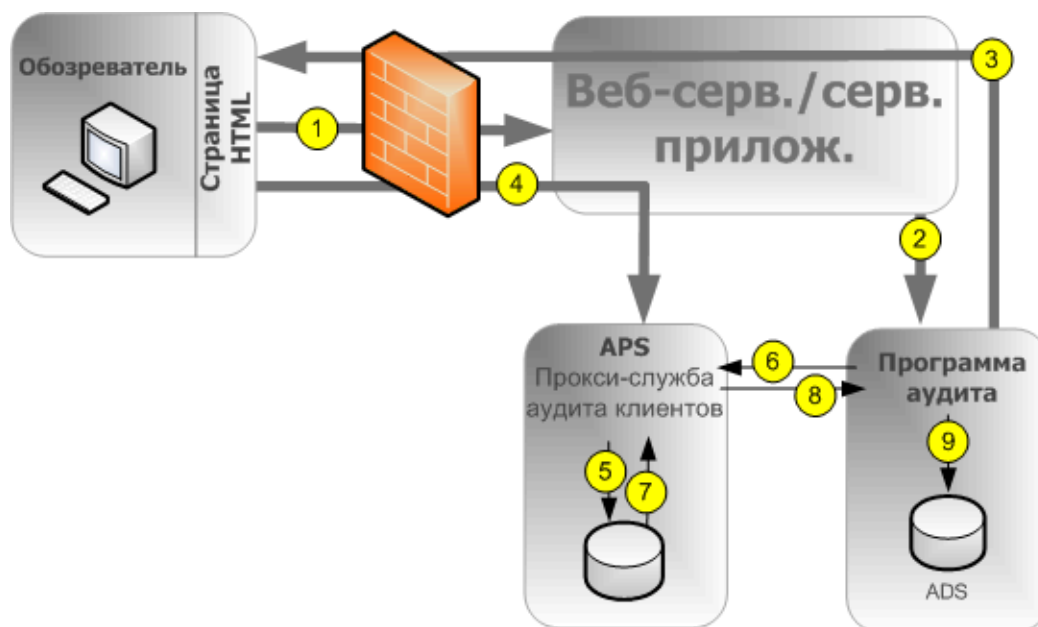
Примечание:

В брандмауэре должны быть открыты порты между каждым клиентом и любым адаптивным сервером обработки, размещающим CAPS, а также между каждым клиентом и CMS. Для получения дополнительных сведений о брандмауэрах см. раздел, посвященный безопасности в *Руководстве администратора платформы SAP BusinessObjects Business Intelligence*.

5. CAPS записывает события во временный файл.
6. Аудитор опрашивает CAPS и запрашивает пакет событий аудита.
7. CAPS извлекает события из временных файлов.
8. CAPS пересылает информацию о событиях программе аудита.
9. Аудитор записывает события в ADS и сообщает CAPS, что следует удалить события из временных файлов.

Аудит отсутствия входа в систему для клиентов, подключающихся через HTTP

Этот рабочий процесс применяется к аудиту событий SAP BusinessObjects Web Intelligence (за исключением событий входа в систему) при подключении через HTTP.



ПРИМЕЧАНИЕ. Аудитор и аудируемый могут находиться на одном сервере CMS.

1. Пользователь начинает выполнение события, подлежащего аудиту. Приложение клиента устанавливает связь с сервером веб-приложений.
2. Веб-приложение проверяет, настроено ли событие на аудит

Примечание:

На диаграмме показана программа аудита CMS, с которой устанавливается связь, для получения этой информации связь может быть установлена с любым сервером CMS в кластере.

3. Сервер CMS возвращает конфигурационную информацию аудита на сервер веб-приложений, который передает эту информацию обратно в приложение клиента.
4. Если настроен аудит события, клиент отправляет сведения о событии на сервер веб-приложений, который передает ее прокси-службе аудита клиента (CAPS), установленной на настраиваемом сервере обработки (APS).
5. CAPS записывает события во временный файл.
6. Аудитор опрашивает CAPS и запрашивает пакет событий аудита.
7. CAPS извлекает события из временных файлов.
8. CAPS пересылает информацию о событиях программе аудита.
9. Аудитор записывает события в ADS и сообщает CAPS, что следует удалить события из временных файлов.

Клиенты, поддерживающие аудит

Следующие клиентские приложения поддерживают аудит:

- Central Management Console (CMC)
- стартовая панель BI
- Open Document
- Analysis
- Поставщик веб-служб Live Office

- Рабочий стол Web Intelligence

Примечание:

Для сбора событий аудита от приведенных выше клиентов должен выполняться как минимум один экземпляр CAPS.

Клиенты, не перечисленные выше, не создают событий напрямую, однако при этом возможен аудит некоторых действий, выполняемых серверами по результатам операций клиентских приложений.

Согласованность аудита

В большинстве случаев, если функция Auditing правильно установлена, настроена и защищена и используются подходящие версии всех приложений клиентов, функция Auditing будет правильно и согласовано записывать все указанные события системы. Однако важно помнить, что определенные условия системы и среды могут оказывать неблагоприятное влияние на выполнение аудита.

Между возникновением события и окончательной передачей в базу данных программы аудита всегда существует задержка. Такие условия, как недоступность CMS или базы данных аудита, или потеря соединения с сетью могут стать причиной увеличения этих задержек.

Системный администратор должен предпринять действия, чтобы избежать появления одного из этих условий, которое может стать причиной неполной записи событий аудита:

- В устройстве, где хранятся данные аудита, достигнут максимальный объем. Рекомендуется обеспечить большой объем доступного дискового пространства для базы данных аудита и временных файлов проверяемого компонента.
- Сервер проверяемого компонента неправильно отключен от сети до окончания передачи всех событий аудита – при отключении сервера от сети необходимо убедиться, что выделено достаточное время для записи событий в базу данных аудита
- Удаление или изменение временных файлов проверяемого компонента.
- Отказ диска или аппаратного обеспечения.
- Физическое разрушение проверяемого компонента или главного компьютера программы аудита

При некоторых условиях события аудита также не могут быть переданы программе аудита CMS. В том числе:

- Пользователи с более старыми версиями клиентского приложения.
- Передача данных аудита может быть заблокирована неправильно настроенными межсетевыми экранами.

Примечание:

- События, формируемые клиентскими приложениями, содержат информацию, поданную со стороны клиента, другими словами, извне надежной области системы. Таким образом в некоторых случаях эта информация может не быть эквивалентно надежна информации, записанной системными серверами. Также включает в себя события, сформированные кэш-сервером рабочих пространств BI, поскольку этот сервер расположен вне надежной области.
- Если нужно удалить сервер из развертывания, рекомендуется сначала деактивировать этот сервер, но оставить его работающим и подключенным к сети, пока все события во временных файлах не будут перемещены в базу данных аудита. Показатель сервера «Текущее число

событий аудита в очереди» показывает, сколько событий аудита ожидает передачи; когда это число достигнет нуля, можно будет остановить сервер. Расположение временных файлов определено в **Заполнителях** для данного узла. Для получения дополнительных сведений о заполнителях см. раздел "Администрирование сервера".

- Если нужно использовать аудит клиента, рекомендуется создать выделенный настраиваемый сервер обработки для службы прокси аудита клиента. Это обеспечит наилучшую производительность системы. Чтобы увеличить отказоустойчивость системы, можно запускать CAPS на нескольких APS.

Связанные ссылки

[Заполнители сервера и узлов](#)

16.2 Страница "Аудит СМС"

Страница «Аудит» в консоли СМС содержит следующие области:

- «Сводка состояния»
- «Установить события»
- «Установить сведения о событии»
- «Настройка»

16.2.1 Состояние аудита

«Состояние аудита» отображает набор показателей, позволяющих оптимизировать настройку аудита и оповещать о любых проблемах, которые могут затронуть целостность данных аудита. Сводка состояния отображается в верхней части страницы **Аудит** в Central Management Console.

В следующих ситуациях в данной сводке отображаются предупреждения:

- Подключение к базе данных ADS (хранилище данных аудита) недоступно.
- Не запущена или не включена прокси-служба аудита клиента, препятствующая сбору событий.
- Проверяемый компонент содержит события, которые не могут быть извлечены (будут определены поврежденные серверы). Обычно это означает, что сервер был остановлен или выключен неправильно и для него все еще существуют события во временных файлах.

Показатели состояния аудита.

Показатель	Сведения
Последнее обновление ADS	Дата и время запуска последнего опроса проверяемых компонентов CMS-аудитором о событиях аудита.
Использование потока аудита	<p>Процентная доля цикла опроса, которую CMS затрачивает на сбор данных о проверяемых объектах. Остаток – это время в состоянии покоя между опросами.</p> <p>Если это значение становится равным 100%, оно отображается желтым цветом и означает, что когда уже должен начаться очередной опрос, аудитор продолжает собирать данные о проверяемых объектах в рамках предыдущего опроса. Это может стать причиной задержек в доставке данных о событиях в базу данных аудита.</p> <p>Если это случается часто или постоянно, рекомендуется либо обновить развертывание, чтобы позволить базе данных ADS получать данные с более высокой скоростью (например, за счет более быстрых сетевых подключений или более мощного аппаратного обеспечения базы данных), либо уменьшить число событий аудита, отслеживаемых системой.</p>
Последний цикл опроса: продолжительность	<p>Длительность последнего цикла опроса в секундах. Указывает максимальную задержку доставки данных о событии в базу данных аудита в течение предыдущего цикла опроса.</p> <ul style="list-style-type: none"> • Если продолжительность составляет менее 20 минут (1200 секунд), значение будет отображаться на зеленом фоне. • Если задержка составляет от 20 минут до 2 часов (7200 секунд), она отображается на желтом фоне. • Если длительность задержки составляет более 2 часов, значение отображается на красном фоне. <p>Если это случается часто или постоянно и задержка становится слишком длительной, рекомендуется либо обновить развертывание, чтобы позволить базе данных ADS получать данные с более высокой скоростью (например, за счет более быстрых сетевых подключений или более мощного аппаратного обеспечения базы данных), либо уменьшить число событий аудита, отслеживаемых системой.</p>
Аудитор CMS	Имя CMS, функционирующего в данный момент в качестве аудитора.
Имя подключения к базе данных ADS	

Показатель	Сведения
	Имя подключения к базе данных, используемого текущим CMS для подключения к хранилищу данных аудита (ADS). Для серверов SQL это будет имя подключения ODBC. Для других типов баз данных это будет имя базы данных, за которым следует имя сервера и порт соединения.
Имя пользователя базы данных ADS	Имя пользователя проверяющего CMS, используемое для входа в базу данных ADS.

16.2.2 Настройка аудита событий

Страница "Аудит CMC" может использоваться для активации аудита и выбора событий, которые будут отслеживаться во всей системе.

Если отдельные события или сведения о событиях не представляют интереса, можно не выбирать их, чтобы дополнительно повысить производительность системы.

Примечание:

Если ADS-подключение не настраивается при установке платформы BI, перед настройкой событий аудита потребуется настроить подключение к базе данных. См. *Параметры конфигурации хранилища данных аудита*.

16.2.2.1 Чтобы настроить события аудита

1. В консоли Central Management Console откройте вкладку **Аудит**.
Откроется страница **Аудит**.
2. Установите ползунок **Установить события** на нужный уровень.
В следующей таблице показаны четыре разных параметра настройки для ползунка и события, события, собираемые на каждом уровне.

Уровень аудита	Собираемые события
Откл.	Нет
Минимальный	<ul style="list-style-type: none"> • Вход в систему • Выход из системы • Изменение прав • Пользовательский уровень доступа изменен • Изменение аудита
По умолчанию	Минимальные события, плюс: <ul style="list-style-type: none"> • Вид • Обновить • Приглашение • Создание • Удаление • Изменение • Сохранение • Поиск • Изменить • Запуск • Доставка
Завершение	Минимальные события и события По умолчанию, плюс: <ul style="list-style-type: none"> • Извлечение • Триггер • Выйти из режима перехода по иерархии • Страница извлечена • Конфигурация LCM • Откат • Добавление VMS • Извлечение VMS • Возврат VMS • Изъятие VMS • Экспорт VMS • Блокировка VMS • Разблокирование VMS • Соединение с кубом • Сеанс MDAS
Пользовательский	Выбор пользовательского набора событий.

3. При выборе значения **Пользовательский** щелкните события для сбора в списке под ползунком **Установить события**.

4. В разделе «Установить сведения о событии» щелкните дополнительные сведения, которые следует записывать вместе с событиями. Меньшее количество записываемых сведений повысит производительность системы.

Сведения	Описание
Запрос	При установке этого значения для каждого события, запрашивающего базу данных, будут записываться сведения о событии «Запрос» (идентификатор сведений 25).
Сведения о пути к папке	При выборе этого параметра будут собираться следующие сведения: <ul style="list-style-type: none"> «Путь к каталогу объекта (идентификатор сведений 71)» «Имя верхней папки (идентификатор сведений 72)» «Путь к каталогу контейнера (идентификатор сведений 64)»
Сведения о правах	При выборе этого параметра будут собираться следующие сведения: <ul style="list-style-type: none"> «Право добавлено (идентификатор сведений 55)» «Право удалено (идентификатор сведений 56)» «Право изменено (идентификатор сведений 57)»
Сведения о группе пользователей	При выборе этого параметра будут собираться следующие сведения: <ul style="list-style-type: none"> «Имя группы пользователей (идентификатор сведений 16)» «Идентификатор группы пользователей (идентификатор сведений 15)»
Сведения о значении свойства	При выборе этого параметра при обновлении свойств объекта будут собираться сведения о событии «Значение свойства» (идентификатор сведений 29). Формируется только для СМС, стартовой панели BI или событий SharePoint.

5. Нажмите кнопку **Сохранить**.

Примечание:

При аудите клиента после внесения изменений может потребоваться около двух минут, прежде чем система начнет запись данных для любых новых событий. При внесении изменений в систему убедитесь, что эта задержка допустима.

16.2.3 Параметры конфигурации хранилища данных аудита

Если база данных аудита не настроена при установке платформы BI или необходимо изменить местоположение или параметры базы данных, можно использовать следующие шаги для настройки подключения к ADS.

Здесь также можно настроить продолжительность сохранения событий аудита в базе данных.

После выполнения обновления с предыдущей версии платформы BI и установки Business Objects Metadata Manager (BOMM) версии 3.x рекомендуется настроить для ADS использование той же базы данных или табличного пространства, что и для BOMM.

Примечание:

Если в качестве базы данных аудита используется существующая рабочая группа DB2 9.7, убедитесь, что в учетной записи базы данных настроен размер страницы, превышающий 8 КБ.

16.2.3.1 Чтобы настроить параметры базы данных ADS (хранилища данных аудита)

1. В консоли Central Management Console откройте вкладку **Аудит**.
Откроется страница **Аудит**.
2. Под заголовком «Конфигурация» щелкните **Тип базы данных ADS**.
Будет открыт список поддерживаемых типов базы данных.
3. Выберите тип базы данных, настроенный для данных аудита.
4. В поле **Имя соединения** введите имя соединения, настроенного для базы данных аудита. Для баз данных SQL это будет имя ODBC; все остальные базы данных принимают форму `<serverhostname>, <port>, <databasename>`.
 - a. При использовании базы данных Microsoft SQL с аутентификацией Windows включите параметр **Аутентификация Windows**.
5. В полях **Имя пользователя** и **Пароль** введите соответствующие значения, которые будут использоваться аудитором CMS при входе в базу данных.
6. В поле **Удалить события старше (в днях)** введите число дней, в течение которых информация должна храниться в базе данных. (Минимальное значение 1, максимальное значение 109 500.)

Предупреждение:

Данные старше числа дней, заданного в этом поле, будут удалены из хранилища данных аудита и не могут быть удалены. Если требуется сохранять долгосрочные записи, можно периодически перемещать их в архивную базу данных.

7. Чтобы вручную подключать CMS-аудитор в случае прерывания соединения, снимите флажок **Автоматическое повторное подключение ADS**.

Примечание:

Если флажок снят, в случае если соединение будет прервано, нужно будет вручную установить соединение с ADS. Для этого можно перезапустить CMS или установить флажок **Автоматическое повторное подключение ADS**. На время отключения ADS события будут записываться и сохраняться во временных файлах.

8. Нажмите кнопку **Сохранить**.
9. Перезапустите CMS.

16.3 События аудита

В следующей таблице представлены все события аудита в системе с кратким описанием. Список типов служб, создающих события.

Событие	Описание, а также серверы и клиенты, создающие тип события
Изменение аудита	Настройки аудита системы изменены. <ul style="list-style-type: none"> Служба центрального управления
Создать	В систему добавлен новый объект. <ul style="list-style-type: none"> Служба обработки Web Intelligence Служба просмотра и изменения Crystal Reports Служба центрального управления Web Intelligence Управление жизненным циклом
Соединение с кубом	Выполняется операция соединения с кубом OLAP. <ul style="list-style-type: none"> Служба многомерного анализа
Пользовательский уровень доступа изменен	Изменена информация по привилегиям. <ul style="list-style-type: none"> Служба центрального управления
Удалить	Объект удален из системы. <ul style="list-style-type: none"> Служба центрального управления Служба управления жизненным циклом
Доставка	Объект отправлен/назначен по месту назначения. <ul style="list-style-type: none"> Служба планирования доставки в места назначения Служба планирования Crystal Reports Служба планирования Crystal Reports для Enterprise Служба публикаций и планирования Web Intelligence Служба центрального управления Служба планирования программ
Выйти из режима перехода по иерархии	Пользователем документа Web Intelligence выполнен переход по иерархии до уровня детализации, находящегося за пределами предварительно загруженных данных отчета. <ul style="list-style-type: none"> Web Intelligence Служба обработки Web Intelligence

Событие	Описание, а также серверы и клиенты, создающие тип события
Изменить	<p>Содержимое объекта изменено.</p> <ul style="list-style-type: none"> • Служба обработки Web Intelligence • Служба информационных панелей • Web Intelligence
Конфигурация LCM	<p>Сведения конфигурации консоли управления жизненным циклом (LCM) изменены.</p> <ul style="list-style-type: none"> • Управление жизненным циклом
Вход в систему	<p>Пользователь входит в систему.</p> <ul style="list-style-type: none"> • Служба центрального управления
Выход из системы	<p>Пользователь выходит из системы</p> <ul style="list-style-type: none"> • Служба центрального управления
Изменить	<p>Свойства файла объекта изменены</p> <ul style="list-style-type: none"> • Web Intelligence • Управление жизненным циклом • Служба центрального управления
Сеанс MDAS	<p>Выполняется операция службы многомерного анализа</p> <ul style="list-style-type: none"> • Служба многомерного анализа
Страница извлечена	<p>Клиент SAP BusinessObjects Web Intelligence извлекает дополнительную информацию из репозитория.</p> <ul style="list-style-type: none"> • Служба обработки Web Intelligence
Приглашение	<p>Для приглашения объекта введена информация.</p> <ul style="list-style-type: none"> • Служба кэширования Dashboard Design • Live Office • Служба планирования Crystal Reports • Crystal Reports для Enterprise • Служба кэширования Crystal Reports • Служба обработки Web Intelligence • Web Intelligence
Обновить	<p>Данные в объекте обновлены из базы данных по запросу пользователя.</p> <ul style="list-style-type: none"> • Служба кэширования Dashboard Design • Live Office • Службы планирования Crystal Reports для Enterprise • Служба кэширования Crystal Reports • Служба планирования Crystal Reports • Служба обработки Web Intelligence • Web Intelligence

Событие	Описание, а также серверы и клиенты, создающие тип события
Извлечь	<p>Объект извлечен из репозитория.</p> <ul style="list-style-type: none"> • Служба центрального управления
Изменение прав	<p>Для пользователя, группы или объекта изменены параметры безопасности.</p> <ul style="list-style-type: none"> • Служба центрального управления
Откат	<p>LifeCycle Manager используется для восстановления предыдущей версии объекта.</p> <ul style="list-style-type: none"> • Управление жизненным циклом
Выполнить	<p>Задание выполняется.</p> <ul style="list-style-type: none"> • Служба планирования управления жизненным циклом • Служба планирования доставки в места назначения • Служба тиражирования • Служба планирования Crystal Reports • Служба планирования Crystal Reports для Enterprise • Служба планирования и публикаций Web Intelligence • Служба планирования публикаций • Служба планирования программ • Управление жизненным циклом
Сохранить	<p>Объект сохранен после обновления или изменения.</p> <ul style="list-style-type: none"> • Служба планирования Crystal Reports Enterprise • Служба кэширования Crystal Reports • Служба многомерного анализа • Служба управления жизненным циклом • Служба обработки Web Intelligence • Служба просмотра и изменения Crystal Reports • Служба планирования Crystal Reports
Поиск	<p>Выполнен поиск.</p> <ul style="list-style-type: none"> • Служба поиска
Триггер	<p>Запущено событие файла.</p> <ul style="list-style-type: none"> • Служба событий • Служба центрального управления

Событие	Описание, а также серверы и клиенты, создающие тип события
Просмотр	Объект просматривается. <ul style="list-style-type: none">• Web Intelligence• Служба обработки Web Intelligence• Central Management Console• стартовая панель BI• Служба кэширования Dashboard Design• Служба кэширования Crystal Reports• Служба просмотра и изменения Crystal Reports• Служба информационных панелей• Открыть документ
Добавление в VMS	Объект добавляется к системе контроля версий LCM. <ul style="list-style-type: none">• Управление жизненным циклом
Возврат VMS	Объект возвращен в систему контроля версий LCM. <ul style="list-style-type: none">• Управление жизненным циклом
Изъятие VMS	Объект изъят из системы контроля версий LCM. <ul style="list-style-type: none">• Управление жизненным циклом
Экспорт VMS	Ресурс экспортирован из VMS. <ul style="list-style-type: none">• Управление жизненным циклом

Событие	Описание, а также серверы и клиенты, создающие тип события
Блокировка VMS	Ресурс в VMS заблокирован. <ul style="list-style-type: none"> Управление жизненным циклом
Разблокирование VMS	Ресурс заблокирован в VMS. <ul style="list-style-type: none"> Управление жизненным циклом
Извлечение VMS	Объект извлечен из системы контроля версий LCM. <ul style="list-style-type: none"> Управление жизненным циклом

События по типам служб

Тип службы	Создаются типы событий
стартовая панель BI	Просмотр
Служба центрального управления	<ul style="list-style-type: none"> Изменение аудита Создать Пользовательский уровень доступа изменен Удалить Доставка Вход в систему Выход из системы Изменить Извлечь Изменение прав Триггер
Central Management Console	Просмотр
Служба кэша Crystal Reports	<ul style="list-style-type: none"> Приглашение Обновить Сохранить Просмотр
Службы планирования Crystal Reports для Enterprise	<ul style="list-style-type: none"> Доставка Приглашение Обновить Выполнить Сохранить

Тип службы	Создаются типы событий
Служба планирования Crystal Reports	<ul style="list-style-type: none"> • Доставка • Приглашение • Обновить • Выполнить • Сохранить
Служба просмотра и изменения Crystal Reports	<ul style="list-style-type: none"> • Создать • Сохранить • Просмотр
Служба кэширования Dashboard Design	<ul style="list-style-type: none"> • Приглашение • Обновить • Просмотр
Служба информационных панелей	<ul style="list-style-type: none"> • Изменить • Просмотр
Служба планирования доставки в места назначения	<ul style="list-style-type: none"> • Доставка • Выполнить
Служба событий	Триггер
Служба планирования LCM	Выполнить
Служба LCM	<ul style="list-style-type: none"> • Создание • Удаление • Конфигурация консоли LCM • Изменить • Откат • Выполнить • Сохранить • Версия • Добавление в VMS • Возврат VMS • Изъятие VMS • Блокировка VMS • Разблокирование VMS
Live Office	<ul style="list-style-type: none"> • Приглашение • Обновить
Служба многомерного анализа	<ul style="list-style-type: none"> • Соединение с кубом MDAS • Сеанс MDAS • Сохранить

Тип службы	Создаются типы событий
Открыть документ	Просмотр
Служба планирования программ	<ul style="list-style-type: none"> • Доставка • Выполнить
Служба планирования публикаций	Выполнить
Служба тиражирования	Выполнить
Служба поиска	Поиск
Web Intelligence	<ul style="list-style-type: none"> • Создать • Выйти из режима перехода по иерархии • Изменить • Изменить • Приглашение • Обновить • Сохранить • Просмотр
Служба обработки Web Intelligence	<ul style="list-style-type: none"> • Создать • Выйти из режима перехода по иерархии • Изменить • Страница извлечена • Приглашение • Обновить • Сохранить • Просмотр
Служба планирования и публикаций Web Intelligence	<ul style="list-style-type: none"> • Доставка • Выполнить

Свойства и сведения о событии

Каждое событие, записываемое платформой BI, включает набор свойств и сведений.

Свойства события всегда создаются с событием, однако, если информация неприменима к определенному событию, некоторые свойства могут не иметь значений. В ADS свойства события включены в таблицу, хранящую событие, что позволяет использовать их для сортирования или группирования событий при создании отчетов.

Сведения о событии содержат дополнительную информацию по событию, которая не включена в свойства события. Если сведения о событии нерелевантны определенному событию, данные сведения о событии не создаются. Существует набор общих сведений о событии, которые могут быть созданы для всех релевантных типов событий. Также существуют наборы дополнительных сведений о событии, которые создаются для событий определенного типа. Например, события

для приглашения записывают значения, введенные для запроса в сведениях о событии, но никакой другой тип события не генерирует сведения о событии значения запроса. В ADS сведения хранятся в отдельной таблице, связанной с родительским событием.

Любые многоязычные данные (например, имена объекта или папок) будут записаны локальным на языке по умолчанию аудитора CMS.

16.3.1 События и детали аудита

В следующих разделах перечислены все типы событий с описанием всех свойств и сведений, уникальных для данных событий. В начале раздела представлен список свойств и сведений, которые являются общими для всех типов событий.

Примечание:

Некоторые клиентские программы не обладают уникальными событиями, а для сбора соответствующей информации по их операциям основываются на общих событиях и событиях платформы.

16.3.1.1 Универсальные свойства и детали события

В следующей таблице представлены свойства и детали событий, характерные для всех событий.

Свойство события	Описание
Event_ID	Уникальный идентификатор события.
Client_Type_ID	Идентификатор для типа приложения, выполняющего событие.
Service_Type_ID	Отображает идентификатор типа службы или приложения, вызвавшего событие.
Start_Time	Дата и время начала события (по GMT)
Duration	Продолжительность события в миллисекундах.
Session_ID	Идентификатор сеанса, в котором вызвано событие.
Event_Type_ID	Тип события (например, 1002 для просмотра).
Status_ID	Указывает успешное выполнение события или сбой ("0" = успешное выполнение, "1" = сбой). Некоторые события обладают дополнительными типами состояния, данные о которых представлены в описании событий.

Свойство события	Описание
Object_ID	<p>CUID объекта (если применимо). CUID предупреждающего события для включающих событий.</p> <p>Примечание: Все объекты, которые не сохранены в репозитории CMS, имеют идентификатор 0. Этими объектами могут быть, например, документы, еще не сохраненные в базу данных CMS или хранящиеся локально на клиентской машине. Для дифференциации данных объектов потребуется использовать свойство Object_Name.</p>
User_ID	CUID пользователя, выполнившего событие.
User_Name	Имя пользователя, выполнившего событие.
Object_Name	Имя объекта (если применимо). Имя предупреждающего события для включающих событий.
Object_Type_ID	CUID типа объекта (например, документ, каталог и т. п.)
Object_Folder_Path	Полный путь к каталогу объекта в репозитории CMS. Например, Sales/North America/East Coast
Folder_ID	CUID каталога, в котором хранится объект.
Top_Folder_Name	Имя каталога верхнего уровня, в котором хранится объект. Например, если объект размещен Sales/North America/East Coast, значение будет Sales.

Свойство события	Описание
Top_Folder_ID	CUID каталога верхнего уровня, в котором хранится объект. Например, если объект размещен в Sales/North America/East Coast, значением будет CUID каталога Sales.
Cluster ID	CUID кластера CMS, записавшего событие.
Action_ID	Уникальный идентификатор, который может быть использован для связи последовательности событий, вызванных одним действием пользователя.

Подробности события	Идентификатор	Описание
Ошибка	1	Записывается только при сбое действия. Текст любого сообщения об ошибке в результате попытки.
Идентификатор элемента	2	Имя объекта, находящегося в контейнере объекта (например, документ Live Office или Dashboard (информационная панель)).
Имя элемента	3	Идентификатор, созданный для объекта, который содержится в контейнере объекта (например, документ Live Office или Dashboard (информационная панель)).
Идентификатор типа элемента	5	Тип объекта в просматриваемом или изменяемом контейнере объекта. Создается только, если применимо.
Идентификатор родительского документа	12	<ul style="list-style-type: none"> Для экземпляра документа: CUID родительского документа. Для родительских документов: собственный CUID.
Идентификатор юниверса	13	CUID юниверса, используемый документом или объектом. Если используется более одного юниверса, сведения события будут созданы для каждого.

Подробности события	Идентификатор	Описание
Имя юниверса	14	Имя юниверса, используемое документом/объектом. Если используется более одного юниверса, сведения события будут созданы для каждого.
Имя параметра "Группа пользователей"	15	Имя параметра "Группа пользователей", к которой принадлежит пользователь, выполняющий действие. Если пользователь принадлежит нескольким группам. Для каждой группы будут созданы сведения о событии.
Идентификатор группы пользователей	16	Идентификатор группы пользователей, к которой принадлежит пользователь, выполняющий действие. Если пользователь принадлежит нескольким группам. Для каждой группы будут созданы сведения о событии.

16.3.1.2 Общие события

Следующие события являются общими для всех компонентов SAP BusinessObjects XI.

Просмотр

Пользователь просмотрел документ/объект.

- Идентификатор типа события: 1002

Подробности события	Идентификатор	Описание
Размер	17	Размер объекта (в байтах) события.
Идентификатор контейнера	32	CUID объекта контейнера (например, информационная панель), в котором расположен объект (если применимо).
Тип контейнера	33	Тип приложения контейнера для объекта (если применимо).

Обновить

Объект обновлен из базы данных.

- Идентификатор типа события: 1003

Подробности события	Идентификатор	Описание
Размер	17	Размер объекта (в байтах) события. Примечание: Для Crystal Reports с просмотром по запросу будет установлено значение 0.
Число строк	63	Число записей, которое возвратил сервер базы данных. Примечание: Для Crystal Reports с просмотром по запросу будет установлено значение 0.
Запрос	25	Записывает SQL-запрос, используемый для обновления данных (необязательно, задается в СМС).
Имя объекта юниверса	31	Имя юниверса, используемого документом или объектом. Сведения о событии будут созданы для каждого юниверса, вызываемого документом или объектом.
Область действия документа	36	Записывает информацию по предназначенной области документа из его настроек публикации (например: Country=USA, Role=Manager). Применимо только к рабочим процессам публикации.
Идентификатор экземпляра публикации	37	Идентификатор экземпляра публикации. Применимо только к рабочим процессам публикации.
Тип объекта Live Office	10701	Идентифицирует тип объекта, обновляемого в документе Live Office (например, отчет Crystal). Создается только для документов Live Office.

Приглашение

Для приглашения введено значение.

- Идентификатор типа события: 1004

Подробности события	Идентификатор	Описание
Имя приглашения	26	Имя приглашения присвоено (например, "Дата"). Для каждого приглашения в документе или объекте будут созданы и сгруппированы отдельные сведения.
Значение приглашения	27	Значение приглашения введено. Отдельные сведения будут созданы для каждого введенного значения. Они могут быть сгруппированы и связаны с именем запроса.
Область действия документа	36	Информация о заданной области действия документа (например, Country=USA, Role=Manager).
Идентификатор экземпляра публикации	37	Идентификатор экземпляра публикации. Применимо только к рабочим процессам публикации.
Имя при конструировании	90	Имя документа Xcelsius во время конструирования. Создается только для обновлений Xcelsius или документов Xcelsius или Live Office, включающих приглашение.
Тип объекта Live Office	10701	Идентифицирует тип объекта, обновляемого в документе Live Office (например, отчет Crystal). Создается только для документов Live Office, если встроенный объект включает приглашение.

Создать

Пользователь создал объект.

- Идентификатор типа события: 1005

Подробности события	Идентификатор	Описание
Размер	17	Размер объекта (в байтах) события.
Перезаписать	21	Указывает на новый документ или объект или на перезапись существующего объекта (0=новый документ или объект, 1=перезапись существующего документа или объекта).
Обновлять при открытии	23	Указывает на автоматическое обновление документа или объекта при открытии (0=не обновлять, 1=обновлять при открытии). Создается только, если применимо.
Описание	24	Запись любой информации в поле описания документа или объекта.

Удалить

Пользователь удаляет объект.

- Идентификатор типа события: 1006

Изменить

Пользователь изменил свойство файла или свойства файла объекта.

- Идентификатор типа события: 1007

Подробности события	Идентификатор	Описание
Имя свойства	28	Имя измененного свойства. Сведения о событии будут созданы для каждого измененного свойства.
Значение свойства	29	Новое значение любого измененного свойства документа или объекта. Сведения о событии будут созданы для каждого измененного свойства.

Сохранить

Сохранение или экспортирование документа или объекта локально, удаленно или в репозиторий CMS в существующем формате или в другом формате.

- Идентификатор типа события: 1008
- Состояния:
 - "0" обозначает успешное локальное сохранение объекта
 - "1" обозначает сбой
 - "2" обозначает успешное сохранение или экспортирование объекта в репозиторий
 - "3" обозначает успешное сохранение или экспортирование объекта в новом формате

Подробности события	Идентификатор	Описание
Размер	17	Размер сохраненного или экспортированного объекта (в байтах).
Имя файла	18	Полное имя сохраненного документа или объекта. При локальном сохранении файла приложением клиента имя также включает путь.
Перезаписать	21	Указывает на новый документ или объект или на перезапись существующего файла. "0"=новый документ или объект, "1"=перезапись существующего документа или объекта.
Формат	22	Указывает формат документа для сохранения/экспортирования, который отображается в качестве трехбуквенного расширения (например, "doc" для файла Microsoft Word или "pdf" для файла Adobe PDF).
Обновлять при открытии	23	Указывает автоматическое обновления документа или объекта при открытии ("0"=не обновляется, "1"=обновляется при открытии). Данные записываются только в том случае, если они применимы.

Поиск

Выполнен поиск.

- Идентификатор типа события: 1009

Подробности события	Идентификатор	Описание
Ключевое слово	19	Ключевое слово выполненного поиска.
Категория	20	Категория, используемая в поиске (если применимо).
Число строк	63	Число строк, возвращенное поиском.

Изменить

Пользователь изменил содержимое объекта.

- Идентификатор типа события: 1010

Подробности события	Идентификатор	Описание
Размер	17	Размер объекта (в байтах) события.
Запрос	25	При изменении SQL-запроса записывается новый запрос. (Данная настройка является дополнительной и может быть выбрана на странице аудита СМС).
Имя объекта юниверса	31	Имя юниверса, используемого документом или объектом. Для каждого юниверса, вызываемого документом или объектом, будут созданы отдельные сведения.
Идентификатор контейнера	32	CUID контейнера (например, информационная панель), использующего объект (если применимо).
Тип контейнера	34	Тип приложения контейнера для объекта (если применимо).
Путь к каталогу контейнера	64	Путь к каталогу контейнера для объекта (если применимо).

Выполнить

Задание выполнено.

- Идентификатор типа события: 1011
- Состояния:
 - "0" обозначает успешно выполненное задание
 - "1" обозначает сбой задания
 - "2" обозначает сбой задания и повторную попытку выполнения
 - "3" обозначает отмену задания

Подробности события	Идентификатор	Описание
Размер	17	Размер выполненного документа (в байтах).
Область действия документа	36	Информация о заданной области действия документа (например, Country=USA, Role=Manager).

Доставка

Объект доставлен.

- Идентификатор типа события: 1012

Подробности события	Идентификатор	Описание
Размер	17	Размер доставленного объекта (в байтах).
Тип места назначения	35	Место назначения экземпляра документа или объекта. Например, электронная почта, FTP, неуправляемый диск, входящие или принтер.
Область действия документа	36	Информация о заданной области действия документа (например, country=usa, role=Manager)
Идентификатор экземпляра публикации	37	Идентификатор данного экземпляра документа или объекта.
Домен	38	Записывает имя домена SMTP-сервера для документов/объектов, распространяемых по электронной почте (если применимо).
Имя хоста	39	Записывает хост SMTP или FTP для документов/объектов, распространяемых по электронной почте или FTP (если применимо).
Порт	40	Записывает порт домена SMTP- или FTP-сервера для документов/объектов, распространяемых по электронной почте или FTP (если применимо).
Адрес отправителя	41	Записывает адрес отправителя для документов/объектов, распространяемых по электронной почте (если применимо).
Адрес получателя	42	Записывает адрес получателя для документов/объектов, распространяемых по электронной почте (если применимо). Также указывается наличие адреса в полях Кому, Копия и Скрытая копия. Сведения о событии будут созданы для каждого предназначенного получателя.
Имя файла	18	Записывает имя файла для документов/объектов, распространяемых по электронной почте или FTP или непосредственно записываемых на диск, не являющийся частью развертывания Business Objects.
Имя учетной записи	45	<p>Записываются следующие параметры:</p> <ul style="list-style-type: none"> • Для объектов, поставляемых посредством Входящие, список имен учетных записей пользователей BusinessObjects. • Для объектов, поставляемых посредством FTP, имя учетной записи FTP. • Для объектов, поставляемых посредством Автономный диск, используется имя учетной записи. • Для объектов, поставляемых посредством SMTP, используется имя учетной записи для SMTP-сервера.

Подробности события	Идентификатор	Описание
Имя принтера	46	Имя принтера, которому поставляется документ или объект (если применимо).
Число копий	47	Число копий печатаемого документа или объекта (если применимо).
Имя получателя	48	Имя пользователя получателя или имена пользователей получателей документа или объекта. Сведения о событии будут созданы для каждого предназначенного получателя.
Идентификатор предупреждающего события	92	CUID предупреждающего события. Создается только при запросе события предупреждением.
Имя предупреждающего события	93	Имя предупреждающего события Создается только при запросе события предупреждением.
Тип поставки	35	Указывает способ запуска поставки. <ul style="list-style-type: none"> • "0" обозначает планирование • "1" обозначает отправку по месту назначению • "2" обозначает публикацию • "3" обозначает запуск предупреждения

Получить

Объект извлекается из CMS.

- Идентификатор типа события: 1013

Вход в систему

Пользователь входит в систему.

- Идентификатор типа события: 1014
- Состояния:
 - "0" обозначает вход в систему конкурентного пользователя
 - "1" обозначает сбой входа в систему
 - "2" обозначает вход в систему именованного пользователя
 - "3" обозначает отличный от пользовательского (системный) вход в систему

Подробности события	Идентификатор	Описание
Число одновременных пользователей	50	Число пользователей системы во время вызова события.
Имя хоста, сообщенное клиентом	51	Имя хоста клиента согласно отчету клиента.
Имя хоста, разрешенное сервером.	52	Имя хоста, разрешенное сервером. Если сервер не может разрешить имя хоста, значение не записывается.
Адрес IP, сообщенный клиентом	53	Адрес IP клиента согласно отчету клиента.
Адрес IP, разрешенный сервером.	54	Адрес IP, разрешенный сервером. Если сервер не может разрешить IP клиента, значение не записывается.

Выход из системы

Пользователь выходит из системы.

- Идентификатор типа события: 1015

Подробности события	Идентификатор	Описание
Число одновременных пользователей	50	Число конкурентных пользователей в системе во время запуска события.

Триггер

Запущено событие файла.

- Идентификатор типа события: 10016

Подробности события	Идентификатор	Описание
Имя файла	17	Имя отслеживаемого файла, запустившего событие.

16.3.1.3 События платформы

Для платформы VI характерны следующие события.

Изменение прав

Право или права для объекта были изменены.

- Идентификатор типа события: 10003

Подробности события	Идентификатор	Описание
Права добавлены	55	Тип добавленного права, область нового права (какие объекты) и тип объекта, к которому оно применяется. Информация будет структурирована в соответствии со следующим примером: добавленное право=Экспорт; новое значение=Предоставлено; область=Текущий объект; применимый тип объекта=все типы объектов.
Права удалены	56	Тип удаленного права, область нового права (какие объекты) и тип объекта, к которому оно применяется. Информация будет структурирована в соответствии со следующим примером: удаленное право=Экспорт; предыдущее значение=Отклонено; область=Текущий объект; применимый тип объекта=все типы объектов.
Права изменены	57	Тип измененного права, область нового права (какие объекты) и тип объекта, к которому оно применяется. Информация будет структурирована в соответствии со следующим примером: измененное право=Экспорт; предыдущее значение=Предоставлено; область=Текущий объект; применимый тип объекта=все типы объектов.

Пользовательский уровень доступа изменен

Пользовательский уровень доступа был изменен.

- Идентификатор типа события: 10004

Подробности события	Идентификатор	Описание
Добавленные права	55	Тип добавленного права, область нового права (какие объекты) и тип объекта, к которому оно применяется. Информация будет структурирована в соответствии со следующим примером: добавленное право=Экспорт; новое значение=Предоставлено; область=Текущий объект; применимый тип объекта=все типы объектов.
Удаленные права	56	Тип удаленного права, область нового права (какие объекты) и тип объекта, к которому оно применяется. Информация будет структурирована в соответствии со следующим примером: удаленное право=Экспорт; предыдущее значение=Отклонено; область=Текущий объект; применимый тип объекта=все типы объектов.
Права изменены	57	Тип измененного права, область нового права (какие объекты) и тип объекта, к которому оно применяется. Информация будет структурирована в соответствии со следующим примером: измененное право=Экспорт; предыдущее значение=Предоставлено; область=Текущий объект; применимый тип объекта=все типы объектов.

Изменение аудита

Было выполнено изменение параметров аудита системы

- Идентификатор типа события: 10006

Подробности события	Идентификатор	Описание
Идентификатор типа события	58	Записывает идентификатор типа события аудита, которое было включено или отключено. Если включены несколько типов событий в одном действии, подробности события будут созданы для каждого типа события.
Действие	59	Записывает, какие события аудита были включены или отключены.
Новый уровень аудита	60	Если уровень аудита сведений изменен, записывает настройку нового уровня (например отключен, минимальный или по умолчанию).
Старый уровень аудита	61	Если уровень аудита сведений изменен, записывает настройку предыдущего уровня (например отключен, минимальный или по умолчанию).

Подробности события	Идентификатор	Описание
Параметр аудита	62	Если включены или отключены необязательные сведения, измененные подробности записываются, а также регистрируется, были ли включены или отключены сведения. Если включены или отключены несколько сведений в одном действии, запись сведений будет создана для каждого измененных сведений.
Соединение ADS	70	Если соединение с хранилищем данных аудита изменено, записываются новые параметры соединения с использованием следующего формата: DBType=Oracle, DBName=MyADS, Имя_пользователя=USR1, Пароль="*****", SSO=off, DBВосстановитьсоединение=on. Записываются только измененные сведения. Например, если изменено только имя пользователя, будет записано только Имя_пользователя="новое". Примечание: Данные пароля будут всегда скрыты в базе данных, и вместо них подставляются символы *.
Интервал автоматического удаления	105	Для этих подробностей будут записываться изменения в поле Удалить события старше, чем на странице аудита СМС аудита. Это определяет, сколько дней будут сохраняться данные аудита в ADS.

16.3.1.4 События SAP BusinessObjects Web Intelligence

Следующие события являются характерными для компонента SAP BusinessObjects Web Intelligence.

Выход за пределы области действия при переходе по иерархии

Пользователь вышел за пределы области действия отчета при переходе по иерархии

- Идентификатор типа события: 10201

Подробности события	Идентификатор	Описание
Экземпляр за- дания	11	Записывает, является ли событие результатом запланированного обновления, либо пользователь просматривает объект ("0" = в результате просмотра пользователем объекта, "1" = в результате запланированного обновления объекта).
Число строк	63	Число строк, которое возвратил сервер базы данных.
Запрос	25	Записывает запрос, используемый для обновления данных (необязательно, задается в СМС).
Имя объекта юниверса	31	Имя юниверса, используемого документом. Экземпляр будет записан для каждого юниверса, к которому обращается документ.
Идентификатор юниверса	32	CUID юниверса, используемого документом. Экземпляр будет записан для каждого юниверса, к которому обращается документ.

Страница извлечена

Страница документа Web Intelligence извлечена.

- Идентификатор типа события: 10202

16.3.1.5 SAP BusinessObjects Analysis, версия для событий OLAP

Сеанс MDAS

Выполняется операция сеанса MDAS

- Идентификатор типа события: 10300
- Статусы:
 - "0" = новый сеанс открыт успешно.
 - "1" = сбой нового сеанса.
 - "2" = существующий сеанс закрыт.

Соединение с кубом MDAS

Выполняется операция соединения с кубом.

- Идентификатор типа события: 10301
- Статусы:
 - "0" = новое соединение открыто успешно.
 - "1" = сбой нового соединения.
 - "2" = существующее соединение закрыто.

Подробности события	Идентификатор	Описание
Идентификатор соединения	94	Уникальный идентификатор для соединения.
Имя соединения	95	Имя соединения.
Тип поставщика	96	Тип поставщика для куба.
Имя куба	97	Полное имя используемого куба.

16.3.1.6 События консоли управления жизненным циклом SAP BusinessObjects

Следующие события являются уникальными для компонента Управление жизненным циклом SAP BusinessObjects.

Общие сведения о консоли управления жизненным циклом SAP BusinessObjects

Для всех событий управления жизненным циклом имеются следующие дополнительные сведения.

Сведения о событии	Идентификатор	Описание
Кластер элементов	6	CUID затронутых кластеров, если консоль управления жизненным циклом выполняет операцию на объектах, расположенных в разных кластерах. Сведения о событии будут созданы для каждого затронутого кластера.
Комментарий элемента	7	Дополнительные сведения об объекте.
Основной элемент	8	Если элемент является основным, для сведений будет установлено значение "1", а если зависимым для сведений будет установлено значение "0".
Статус элемента	9	При сбое элемента операции для сведений будет установлено значение "1", в противном случае – в "0".
Операция	10	Описывает тип выполняемой операции (например, добавление, удаление или изменение).

Конфигурация консоли управления жизненным циклом SAP BusinessObjects

Конфигурация управление жизненным циклом изменена.

- Идентификатор типа события: 10900

Подробности события	Идентификатор	Описание
Конфигурация	100	Пользователь просматривает конфигурацию консоли управления жизненным циклом. Конфигурация отображается в виде разделяемых запятыми пар значений, например: настройки отката=включено, порт=900.
Конфигурация до	101	Если настройки консоли управления жизненным циклом для объекта изменены, записывает предыдущие настройки конфигурации. Использует такой же формат, что и конфигурация.
Конфигурация после	102	Если настройки консоли управления жизненным циклом для объекта изменены, записывает новые настройки конфигурации. Использует такой же формат, что и конфигурация.
Тип VMS	10900	Тип системы управления версиями.

Откат

Для объекта был выполнен откат к предыдущей версии системы управления версиями (VMS).

- Идентификатор типа события: 10901

Добавление в VMS

Ресурс добавлен в VMS.

- Идентификатор типа события: 10902

Подробности события	Идентификатор	Описание
Версия	104	Записывает номер версии документа в системе управления версиями.

Извлечение VMS

Ресурс извлекается из VMS.

- Идентификатор типа события: 10903

Подробности события	Идентификатор	Описание
Восстановление удаленного объекта	103	Указывает, удален ли извлеченный объект из системы. "0" обозначает, что объект не был удален; "1" указывает, что объект был удален.
Версия	104	Записывает номер версии документа в VMS.

Возврат VMS

Ресурс был возвращен в VMS.

- Идентификатор типа события: 10904

Сведения о событии	Идентификатор	Описание
Версия	104	Записывает номер версии документа в VMS.

Изъятие VMS

Ресурс был изъят из VMS.

- Идентификатор типа события: 10905

Подробности события	Идентификатор	Описание
Версия	104	Записывает номер версии документа в VMS.

Экспорт VMS

Ресурс экспортирован из VMS.

- Идентификатор типа события: 10906

Подробности события	Идентификатор	Описание
Версия	104	Записывает номер версии документа в VMS.

Блокировка VMS

Ресурс в VMS заблокирован для предотвращения редактирования его пользователями.

- Идентификатор типа события: 10907

Подробности события	Идентификатор	Описание
Версия	104	Записывает номер версии документа в VMS.
Автор блокировки	10901	Имя пользователя, выполнявшего действие.

Разблокирование VMS

Ресурс в VMS разблокирован, позволяя пользователям изменять его.

- Идентификатор типа события: 10908

Подробности события	Идентификатор	Описание
Версия	104	Записывает номер версии документа в VMS.
Автор разблокирования	10901	Имя пользователя, выполнявшего действие.

Поиск по платформе

17.1 Обзор

Поиск по платформе позволяет выполнять поиск содержимого внутри репозитория платформы SAP BusinessObjects Business Intelligence. Результаты поиска уточняются, группируются в категории и ранжируются с учетом значимости. Также поддерживается публичный SDK, функционирующий в качестве интерфейса между клиентским приложением и поиском по платформе.

В данной версии платформы SAP BusinessObjects Business Intelligence поиск по платформе дополнен перечисленными ниже функциями.

- Поиск содержимого как платформы SAP BusinessObjects Business Intelligence, так и модуля Explorer
- Выдача запроса о создании документа в случае, если найти существующий документ не удастся.
- Поддержка как непрерывного индексирования, так и индексирования по расписанию
- Поддержка индексации в кластеризованной среде
- Установка и изменение уровня индексации
- Предоставление параметров конфигурации расширенного поиска
- Поддержка многоязыкового поиска и индексации
- Реализация расширенного синтаксиса поиска
- Поддержка фасетов метаданных, содержимого и динамических фасетов
- Поддержка самовосстановления, исходящего из загрузки системы

Примечание:

Если выполняется миграция с предыдущей версии на новую, предыдущий индекс не переносится.

17.2 Архитектура

В этом разделе описана архитектура поиска по платформе и кратко поясняется роль каждого компонента. Поиск по платформе размещается на адаптивном сервере обработки, в состав которого входят различные компоненты, обеспечивающие индексацию и поиск. Индексация в поиске по платформе производится с учетом типа индекса, который может быть основанным на расписании или обновляться непрерывно.

Поиск по платформе включает два основных процесса – индексацию и поиск. Кроме того, в службе предусмотрен механизм самовосстановления.

Индексация

Индексирование – это непрерывный процесс, включающий следующие последовательные задачи:

1. Обход – это механизм опроса репозитория CMS и идентификации объектов, которые были опубликованы, изменены или удалены. Существует два способа выполнения обхода – непрерывный обход и плановый обход.

Для получения дополнительных сведений о непрерывном и планируемом обходе см. главу *Настройка свойств приложения* в разделе ссылок.

2. Извлечение – это механизм вызова средств извлечения, основанных на типе документа. У каждого типа документов, доступных в репозитории, есть свой собственный процесс извлечения. Документы нового типа можно сделать доступными для поиска, если определить соответствующий подключаемый модуль процесса извлечения. Масштабируемость каждого из этих процессов извлечения достаточна, чтобы извлечь содержимое больших документов с множеством записей.

Поддерживаются следующие процессы извлечения:

- Процесс извлечения метаданных
- Процесс извлечения отчета Crystal
- Процесс извлечения для Web Intelligence
- Процесс извлечения для юниверсов
- Сторонние процессы извлечения (MS Office 2003 и 2007 и документы PDF)

Для получения дополнительных сведений о доступных для поиска типах документов см. раздел *Типы содержимого, доступные для поиска* в разделе ссылок.

3. Индексирование – это механизм, индексирующий все извлеченное содержимое при помощи сторонней библиотеки, которая называется Apache Lucene Engine. Время, необходимое для индексации значений, может меняться в зависимости от числа объектов в системе, их размера и структуры типа документов.

Поисковый индекс хранится в специально заданном расположении в файле и в его состав входит поддающееся поиску содержимое индексированных документов.

Для успешного выполнения индексации должны быть активны и подключены следующие серверы:

- InputFileRepositoryServer (IFRS)
- OutputFileRepositoryServer (OFRS)
- CentralManagementServer (CMS)
- AdaptiveProcessingServer (APS)

Если выбран тип объекта Web Intelligence или отчет Crystal, необходимо, чтобы соответствующие серверы WebIntelligenceProcessingServer или CrystalReportApplicationServer выполнялись и были активированы для соответствующих выбранных типов объектов.

4. В хранилище содержимого представлены такие данные, как идентификатор, CUID, имя, вид и экземпляр, извлеченные из основного индекса в формате, доступном для быстрого считывания. Это способствует ускорению процесса поиска.

Поиск

Когда пользователь производит поиск по ключевому слову в стартовой панели BI или любой другой программе, использующей функции SDK Platform Search, проверяется наличие условий поиска в главном индексе. В поисковой системе отображаются только те документы, на которые у пользователя есть права доступа.

Самовосстановление

В приложении поиска по платформе предусмотрен механизм самовосстановления. Поиск по платформе непрерывно отслеживает использование памяти службой поиска и автоматически останавливает индексацию, если потребление памяти превышает пороговое значение. При уменьшении объема используемой памяти до приемлемого предела индексация возобновляется автоматически. Пользователи могут продолжать поиск во время этого процесса, но в течение определенного времени не могут выполнять индексирование. По умолчанию в поиске по платформе настраивается число документов, которые могут быть индексированы в любой момент, основываясь на типе документа. Индексирование инициируется в зависимости от ресурсов системы, таких, как ЦП и память.

См. также

- [Настройка свойств приложения](#)
- [Типы содержимого, доступного для поиска](#)

17.3 Поддержка кластеров для поиска по платформе

Поиск по платформе поддерживает распределение нагрузки по нескольким узлам в кластеризованной рабочей среде. Развертывание в кластеризованной среде обеспечивает оптимальное использование ресурсов системы и повышает производительность сервера.

Поиск по платформе поддерживает и горизонтальную, и вертикальную кластеризацию как для функций поиска, так и для индексации. В кластеризованных средах это позволяет оптимизировать производительность как процессов поиска, так и индексации.

Балансировка нагрузки

Поиск по платформе поддерживает балансировку нагрузки как при индексации, так и при поиске.

В кластеризованной среде запросы на индексацию или поиск могут выполняться множеством узлов, обеспечивая распределение нагрузки. Каждый из узлов индексирует содержимое и создает разностные индексы независимо от других узлов. Однако только один узел кластера может выполнять роль основного индекса и выполнять добавление разностных индексов в основной индекс. Основной индекс доступен всем узлам. Это позволяет выполнять несколько поисковых запросов одновременно.

Обеспечение отказоустойчивости

Если один из узлов кластера становится недоступным из-за технического сбоя или в связи с проведением регламентных работ, адресованные ему запросы на индексацию и поиск начинает

выполнять другой узел. Механизм восстановления при отказе дает возможность пользователям в случае сбоя продолжать поиск и позволяет избежать прерывания операций индексирования.

17.4 SDK и открытый поиск

Поиск по платформе поддерживает как SDK, так и Open Search.

17.4.1 Platform Search SDK

Комплект Platform Search SDK – это интерфейс между клиентским приложением и поиском по платформе. Он общедоступен для помощи в настройке службы поиска и ее интеграции с используемым приложением.

Параметр запроса на поиск, отправленный через клиентское приложение на уровень SDK, преобразуется последним в XML-формат и передается в службу поиска по платформе.

Для получения дополнительных сведений об интерфейсе API поиска по платформе см. документ *SAP BusinessObjects Business Intelligence platform Java API Reference*.

17.4.2 Open Search

Поиск по платформе поддерживает стандарт OpenSearch, за счет чего клиентские приложения могут использовать стандарт или формат OpenSearch для обмена данными с поиском по платформе. По умолчанию OpenSearch не устанавливается в составе пакета платформы SAP BusinessObjects Business Intelligence, поэтому его необходимо развернуть вручную как отдельный WAR-файл (opensearch.war) на сервере приложений, например Tomcat, используемом для платформы SAP BusinessObjects Business Intelligence, или с помощью средства WDeploy. Программа установки копирует файл в каталог {BOE_INSTALL_DIR}\warfiles\OpenSearch.

Примечание:

- Для обмена данными с поиском по платформе программы-клиенты должны поддерживать стандарты OpenSearch.
- При установке платформы SAP BusinessObjects Business Intelligence по умолчанию устанавливается сервер приложений Tomcat.

17.4.2.1 Развертывание OpenSearch

Для развертывания OpenSearch в среде платформы SAP BusinessObjects Business Intelligence выполните следующие действия:

1. Перейдите в следующее расположение: {каталог_установки}/SAP BusinessObjects Enterprise 4.0\warfiles\
2. Скопируйте папку OpenSearch в {INSTALLDIR}\Tomcat6\webapps.
3. Измените параметры конфигурации в файле OpenSearch\WEB-INF\config.properties, как указано ниже:
 - CMS: имя CMS с номером порта в виде <CMS Name>:<Port Number>
 - OpenDocURL – URL-адрес приложения OpenDocument, например `http://<tomcat>host:<connector port>/BOE/OpenDocument/opendoc/openDocument.jsp`
 - Proxy.rpurl – имя обратного прокси-сервера необходимо для использования обратного прокси
 - Proxy.opendoc.rpurl – имя обратного прокси-сервера opendoc, необходимое для использования обратного прокси
4. Выполните повторный запуск сервера приложений Tomcat для развертывания OpenSearch.

17.4.2.2 Развертывание OpenSearch с помощью WDeploy

Чтобы развернуть OpenSearch с использованием средства WDeploy, выполните следующие шаги:

Примечание:

Команды для ОС Windows и UNIX приводятся соответственно как `wdeploy.bat <параметры>` и `wdeploy.sh <параметры>`.

1. Обновите файл конфигурации <app server server>, расположенный в каталоге <BOE_Install_Dir>\<Enterprise_DIR>\wdeploy\conf, указав требуемые параметры сервера веб-приложений, в том числе каталог установки, имя экземпляра, порт администрирования, имя пользователя и пароль администратора.
2. Измените параметры конфигурации в файле OpenSearch\WEB-INF\config.properties, как указано ниже:
 - CMS: имя CMS с номером порта в виде <Имя CMS>:<номер порта>
 - OpenDocURL: URL-адрес приложения OpenDocument, например `http://<хост сервера веб-приложений>:<порт соединения>/BOE/OpenDocument/opendoc/openDocument.jsp`
 - Proxy.rpurl: имя обратного прокси-сервера, требуемое для использования обратного прокси

- Proxy.opendoc.rpurl: имя обратного прокси-сервера opendoc, требуемое для использования обратного прокси.
3. Выполните команду `wdeploy.bat <WEB_APPLICATION_SERVER>`
`-Dapp_source_dir=<LOCATION_OF_OpenSearch_Webapp> -DAPP=OpenSearch deploy`
из каталога `<BOE_Install_Dir>\<Enterprise_DIR>\wdeploy location`
Например, с помощью следующей команды OpenSearch развертывается на сервере веб-приложений WebSphere 7:

```
wdeploy.bat websphere7 -Dapp_source_tree=<BOE_Install_Dir>\<Enterprise_DIR>\warfiles" -DAPP=OpenSearch deploy
```
 4. Перезапустите сервер приложений.

17.4.2.3 Настройка обратного прокси для OpenSearch

Для развертывания веб-приложений платформы SAP BusinessObjects Business Intelligence на сервере веб-приложений, расположенном за обратным прокси-сервером, необходимо настроить обратный прокси-сервер на отображение входящих URL-запросов на правильный WAR-файл:

Примечание:

Для наглядного представления шагов конфигурации в качестве примера используется обратный прокси-сервер Apache 2.2.

Настройка обратного прокси-сервера Apache 2.2 для системы OpenSearch

1. Настройте обратный прокси и внесите изменения в файл OpenSearch WEB-INF\config.properties.
2. Активируйте следующие контекстные параметры и соответственно измените их значения.
 - proxy.rpurl – это URL-адрес обратного прокси для OpenSearch, например `http://machineIPAddress/RP/OpenSearch/`.
 - proxy.opendoc.rpurl – это URL-адрес обратного прокси-сервера для OpenDoc, например `http://machineIPAddress/RP/BOE`
3. Обновите файл `httpd.conf`, расположенный в папке установки обратного прокси Apache, задав следующие параметры:
 - `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. Перезапустите обратный прокси-сервер Apache 2.2.

17.5 Настройка свойств приложения

Чтобы настроить свойства приложения поиска по платформе, выполните следующие действия:

1. Перейдите в область «Программные приложения» СМС.
2. Выберите **Приложение поиска по платформе**.
3. Выберите команду **Управление > Свойства**. Появится диалоговое окно «Свойства».
4. Выполните настройку требуемых параметров поиска по платформе.

Настраиваемые свойства описаны в следующей таблице:

Действие	Описание
Статистика поиска	Поиск по платформе предлагает следующие статистики поиска: <ul style="list-style-type: none"> • Статус индексации: показывает состояние процесса индексации • Число проиндексированных документов: показывает число документов, для которых индексация выполнена. • Последняя отметка времени индексации: показывает метку времени, когда документ был проиндексирован в последний раз.
Остановить / начать индексацию	Параметры запуска и остановки индексации позволяют запустить или остановить процесс индексации, когда требуется перейти от непрерывного обхода на планируемый, либо в целях обслуживания. Чтобы остановить индексацию, щелкните Остановить индексацию и затем нажмите кнопку ОК в диалоговом окне подтверждения.
Региональные параметры индекса	При выборе другого языка для региональных параметров индекса поиска по платформе выполняет повторную индексацию документов на выбранном языке. Выберите региональные параметры индекса в одном из следующих языков: английский, бразильский, голландский, итальянский, испанский, китайский, корейский, немецкий, норвежский букмол, польский, португальский, русский, тайский, финский, французский, чешский, шведский или японский. Примечание: Английский язык выбран в качестве региональных параметров по умолчанию.

Действие	Описание
Периодичность поиска	<p>Индексацию всего репозитория платформы ВІ можно выполнить, используя следующие параметры:</p> <ul style="list-style-type: none"> • Непрерывный обход: при выборе этого варианта индексация выполняется непрерывно, т.е. репозиторий индексируется всякий раз при добавлении, изменении или удалении объекта. Это позволяет просматривать содержимое платформы ВІ или работать с ним. Выбираемый по умолчанию непрерывный обход постоянно обновляет репозиторий платформы ВІ по мере выполнения различных действий. Непрерывный обход не требует при работе вмешательства пользователя и сокращает время, требуемое на индексирование документа. • Плановый обход: при выборе этого варианта индексация выполняется на основании расписания, задаваемого настройками "Расписание". <p>Для получения дополнительных сведений о включении объектов в расписание см. раздел <i>Включение объекта в расписание</i> интерактивной справки по поиску по платформе в <i>СМС платформы ВІ</i>.</p> <p>Примечание:</p> <ul style="list-style-type: none"> • При выборе команды Запланировать обход и установке для параметра Повторение значения, отличного от Сейчас, поиск по платформе отображает дату и время временной метки следующей плановой индексации документа. • При выборе планового обхода кнопка Начать индексацию активируется, а кнопка Остановить индексацию деактивируется. • По окончании планирования кнопка Остановить индексацию деактивируется.

Действие	Описание
Расположение индекса	

Действие	Описание
	<p>Сведения об индексированных документах сохраняются в общих папках в следующих местах:</p> <ul style="list-style-type: none"> Расположение основного индекса (индексы и проверка орфографии): основной индекс и индексы проверки орфографии сохраняются в этом расположении. Во время рабочего процесса поиска начальные попадания извлекаются по основному индексу, а индексы проверки орфографии используются для извлечения предположений. В кластеризованном развертывании BOE это расположение должно находиться на общей (сетевой) файловой системе, доступной всем узлам в кластере. Постоянное расположение данных (Хранилища содержимого): хранилище содержимого находится в этом расположении. Оно создается из расположения основного индекса и остается синхронизированным с ним. Хранилище содержимого используется для создания фасетов и обработки начальных совпадений, созданных из расположения основного индекса. В кластеризованном развертывании платформы BI хранилища содержимого создаются в каждом из узлов. <p>Расположение постоянных данных – это единственное расположение индексов, на которое влияет наличие кластеризованной среды, так как оно содержит папки хранилищ содержимого. Если на компьютере имеется только одна служба поиска, на нем будет только одно расположение хранилища содержимого. Например, это может быть</p> <pre>{obj.enterprise.home}\data\PlatformSearchData\workspace\Server\ContentStores.</pre> <p>Однако в кластеризованной среде при наличии множества служб поиска у каждой из них будет по одному местоположению хранилища содержимого. Например, при наличии двух активных экземпляров сервера местоположения хранилища содержимого будут следующими:</p> <ol style="list-style-type: none"> <code>{obj.enterprise.home}\data\PlatformSearchData\workspace\Server\ContentStores.</code> <code>{obj.enterprise.home}\data\PlatformSearchData\workspace\Server1\ContentStores.</code> <ul style="list-style-type: none"> Расположение непостоянных данных (временных файлов, дельта-индексов): в этом расположении создаются и временно сохраняются дельта-индексы перед их слиянием с основным индексом. Индексированные документы из этого расположения удаляются после их слияния с основным индексом. Кроме того, суррогатные файлы (результат работы экстракторов) также создаются и временно сохраняются в этом расположении, до их преобразования в дельта-индексы. <p>Примечание:</p> <ul style="list-style-type: none"> Все места размещения индексов должны иметь общий доступ. Чтобы изменить расположение индекса, нажмите кнопку

Действие	Описание
	<ul style="list-style-type: none"> • Остановить индексацию. • При изменении расположения индекса необходимо скопировать существующее содержимое в новое расположение, иначе данные из существующего индекса будут утеряны.
Уровень индексации	<p>Можно выполнить настройку содержимого поиска, задав уровень индексации следующим образом:</p> <ul style="list-style-type: none"> • Метаданные платформы: индекс создается только для метаданных платформы, таких, как заголовки, ключевые слова и описания документов. • Метаданные платформы и документа – индекс создается по метаданным платформы и метаданным документов. К метаданным документа относятся дата создания, дата изменения и имя автора. • Содержимое в полном объеме: индекс создается по метаданным платформы, метаданным документов и другому содержимому, включая следующее: <ul style="list-style-type: none"> • Фактическое содержимое документа • Содержимое запросов и списков значений • Диаграммы, графики и метки <p>Примечание: При изменении уровня индексации процесс индексации инициализируется заново для всего репозитория платформы BI.</p>
Типы содержимого	<p>Для индексирования могут быть заданы следующие типы содержимого.</p> <ul style="list-style-type: none"> • Microsoft Word • Microsoft Excel • Microsoft PowerPoint • Текст • Adobe Acrobat • Формат RTF • Crystal Reports • Юниверс • Web Intelligence

Действие	Описание
Перестроить индекс	<p>Этот параметр удаляет все существующее проиндексированное содержимое и повторно индексирует весь документ с самого начала.</p> <p>Параметр Перестроить индекс можно выбрать независимо от состояния индексации. Однако параметр Перестроить индекс не будет работать в случае останова индексирования, выбора параметра Перестроить индекс, сохранения и закрытия приложения поиска по платформе после остановки индексации.</p> <p>В случае остановки индексации и выбора параметра Перестроить индекс, сохраните и закройте приложение поиска по платформе, затем откройте повторно страницу конфигурации и нажмите кнопку Начать индексацию., после чего сохраненный параметр "Перестроить индекс" проведет автоматическую повторную индексацию всего документа.</p> <p>Чтобы отказаться от повторной индексации документов, снимите флажок Перестроить индекс перед нажатием кнопки Начать индексацию.</p>
Документы, исключенные из индексации	<p>Параметр Исключенные из индексирования документы позволяет исключить из индексирования некоторые документы. Например, чтобы избежать перегрузки сервера приложений отчета, может потребоваться отключение функции поиска в очень больших отчетах Crystal. Также может потребоваться исключение из индексирования публикаций с сотнями персонализированных отчетов.</p> <p>Исключение конкретных документов позволяет заблокировать доступ к ним при поиске по платформе. Важно отметить, что документ, проиндексированный до того, как был отнесен к данной группе, все еще может быть доступен для поиска. Чтобы документы, отнесенные к категории Исключенные из индексирования документы, были гарантированно недоступны для поиска, необходимо перестроить индекс.</p> <p>По умолчанию только учетной записи администратора предоставлено полное управление параметром Исключенные из индексирования документы. Другие пользователи с перечисленными ниже правами могут только добавлять документы в группу Исключенные из индексирования документы:</p> <ul style="list-style-type: none"> • Права просмотра и редактирования категории • Непосредственное редактирование документа

5. Нажмите кнопку **Сохранить и закрыть**.

Примечание:

Если пользователь не выбрал параметр **Перестроить индекс** и изменил уровень индексирования, выбрал или отменил выбор средств извлечения, то будет выполнено инкрементное обновление существующего индекса без его удаления.

17.6 Типы содержимого, доступного для поиска

Большая часть содержимого, опубликованного на платформе SAP BusinessObjects Business Intelligence, доступна для поиска с помощью модуля поиска по платформе. Далее перечислены типы объектов и соответствующее им индексируемое содержимое:

Тип объекта	Индексируемое содержимое
Crystal Reports (2008 и 2011)	Заголовок, описание, формула выбора, сохраненные данные, текстовые поля любого раздела, значения параметров и подотчеты.
Документы Web Intelligence	Заголовок, описание, имя фильтров юниверсов, используемых в отчете, сохраненные данные, константы в условии фильтра, заданном в отчете, имя мер юниверса, используемых в отчете, имя объектов юниверса, используемых в отчете, данные в наборе записей и статический текст в ячейках.
Документы Microsoft Excel (2003 и 2007)	Данные во всех непустых ячейках, поля на странице "Сводка" свойств документа (заголовок, тема, автор, компания, категория, ключевые слова и комментарии) и текст в верхнем и нижнем колонтитулах документа. Для ячеек, использующих вычисление или формулу, поиску поддается значение после определения. Для значений количества или даты/времени поиску поддаются необработанные данные.
Документы Microsoft Word (2003 и 2007)	Текст во всех абзацах и таблицах, поля на странице "Сводка" свойств документа (заголовок, тема, автор, компания, категория, ключевые слова и комментарии), текст в верхнем и нижнем колонтитулах документа и цифровой текст.

Тип объекта	Индексируемое содержимое
Файлы RTF, PDF, PPT и TXT	Весь текст в таких файлах подлежит поиску.
Задание LCM, юниверс, страница информационной панели AF, Dashboard Design, пакет объектов (ObjectPackage), запрос веб-службы (QaaWS), профиль, обсуждения, дизайнер информации, виджеты для платформы SAP BusinessObjects Business Intelligence, анализ MD, публикации, Flash, аналитика и гиперссылка	Содержимое метаданных доступно для поиска.
События	<p>По всем событиям, таким, как пользовательские, системные, события Crystal Reports и события мониторинга, можно выполнять поиск. Если событие связано с источником, поиск по платформе обнаружит как источник, так и событие.</p> <p>Примечание: Поиск по платформе поддерживает события для Crystal Reports для Enterprise.</p>

Примечание:

Максимальный поддерживаемый размер документов Agnostic (MS Office 2003 и 2007, а также документы PDF) составляет 15 МБ.

17.7 Предложенные запросы

При использовании поиска по платформе пользователь вместо поиска конкретного объекта может попытаться найти ответы на конкретный вопрос. На эти вопросы может быть найден ответ в отчетах, доступных в репозитории платформы SAP BusinessObjects Business Intelligence.

Проанализировав структуру юниверсов и существующих отчетов в репозитории платформы SAP BusinessObjects Business Intelligence и сравнив эти сведения с критериями поиска, указанными пользователем, поиск по платформе может предложить новые запросы SAP BusinessObjects Web Intelligence, которые, возможно, помогут пользователям найти ответы на их вопросы.

Для создания потенциальных отчетов поиск по платформе сравнивает слова во всех юниверсах на предмет измерения, меры, условия и значения фильтра.

Модуль поиска по платформе выполняет поиск соответствия в следующих сведениях о юниверсах или о существующих документах SAP BusinessObjects Web Intelligence:

- Меры в юниверсах, которые соответствуют словам в строке поиска.

Если показатель соответствует одному из критериев поиска, он будет использован в документе результатов SAP BusinessObjects Web Intelligence.

- Имена измерений в юниверсах, которые соответствуют словам в строке поиска.

Если имя измерения соответствует одному из критериев поиска, результирующий документ Web Intelligence проанализирует информацию этого измерения.

- Фильтры запроса могут использоваться при фокусировании на определенных данных документа. Эти фильтры запроса генерируются при анализе строки поиска.
 - Если имя условия юниверса соответствует критерию поиска, это условие используется в качестве фильтра.
 - Если в существующих документах SAP BusinessObjects Web Intelligence есть значения полей, имена которых соответствуют критериям поиска, фильтр будет создан из измерения исторического отчета с соответствующим значением и оператором "равно" в качестве условия.

Если модуль поиска по платформе нашел достаточно соответствий, чтобы результирующий документ содержал два поля результата и один фильтр, запрос считается готовым к выполнению. В этом случае пользователь может нажать кнопку и просмотреть выполненный отчет.

Если найдено недостаточное количество соответствий между юниверсами и документом, пользователь может изменить запрос перед тем, как запустить его.

Поиск по платформе предложит несколько запросов, если критерию поиска соответствует несколько юниверсов или при существовании двух разных совпадений для одного слова, например в имени измерения и в значении фильтра.

17.8 Фасеты

Поиск по платформе уточняет результаты поиска, группируя их в категории или фасеты сходных типов объектов и ранжируя по числу вхождений категории в результаты, возвращенные по условиям поиска. Фасеты позволяют переходить к точным результатам.

Поиск по платформе формирует фасеты из метаданных InfoObject, метаданных документов и содержимого документов. Отображаются только те фасеты, у которых с указанным запросом совпадают более двух документов. Фасеты – это поверхности, динамически основанные на документах, совпадающих с поисковыми запросами и сортированные по количеству документов.

Документы платформы SAP BusinessObjects Business Intelligence группируются в следующие общие фасеты или категории:

- Персональные или общедоступные (например HR, корпоративный или финансовый) на основании категории документов платформы BI.
- Тип документа: основывается на типе документа, например, это может быть тип Web Intelligence, Crystal Report, Microsoft Word (2003 и 2007), документы Microsoft Excel (2003 и 2007) и Xcelsius.

- Юниверс и подключения: основывается на источнике содержимого.
- Дата: включает дату последнего обновления (год, квартал и месяц).
- Время: включает время последнего обновления, например последние 24 часа или в течение прошлой недели.
- Автор: имя пользователя, создавшего документ.

17.9 Многоязыковая поддержка

Поиск по платформе реализует поддержку многих языков, позволяя индексировать содержимое, извлекать результаты поиска и получать предложения вариантов на необходимом языке. Извлекаемые результаты основываются на языке, выбранном в параметре **Языковой стандарт для индексирования** в приложении СМС вне зависимости от установленных в клиенте региональных параметров. Поиск по платформе индексирует метаданные, свойства документов и содержимое отчетов.

В процессе индексации используется средство анализа для региональных параметров, заданных на странице конфигурации. В любой момент времени для индексирования используется только один язык.

Для возвращения оптимальных результатов следует использовать один и тот же языковой стандарт и для поиска, и для индексации. По умолчанию в качестве языкового стандарта индексации установлен английский язык, то есть поиск по платформе использует английский язык и для индексирования, и для поиска. При изменении языкового стандарта, индекс будет либо повторно инициализирован, либо перестроен, в зависимости от установленного при сохранении новой конфигурации значения параметра. При индексации документов в будущем будут использоваться новые языковые параметры.

При изменении языкового стандарта приложении СМС на другой, например с английского на немецкий, весь индекс инкрементно обновляется с использованием средства анализа на немецком языке для всех существующих документов.

При переключении региональных параметров на другой язык, например, с английского на немецкий, и последующем выборе команды **Повторное построение индекса**, текущий индекс будет удален, и будет создан новый индекс на немецком языке.

17.10 Предложения

Поиск по платформе предлагает варианты замены неверно набранных поисковых запросов. Если исходный поисковый запрос не возвращает результатов, поиск по платформе предложит наиболее вероятные термины поиска, исходя из индексированного содержимого.

Предложения отображаются в виде ключевых слов с гиперссылкой. Щелкните ссылку, чтобы просмотреть список документов, содержащий ключевое слово, которое может соответствовать

первоначальному запросу. Эти предложения определяются алгоритмически на основании различных объективных факторов.

Если имеется ряд терминов, которые могут совпадать с исходным запросом, поиск по платформе предложит три самых подходящих варианта на языке, выбранном в качестве **Языкового стандарта индексации** в приложении СМС.

Примечание:

Поиск по платформе не формирует предложений:

- Если поисковые запросы содержат менее трех символов
- Для поиска по атрибутам, например с атрибутом "Тип: Crystal Report"
- Для метаданных и содержимого юниверсов
- Для многобайтных языков, таких, как китайский, японский и корейский

17.11 Объединение результатов поиска из SAP BusinessObjects Explorer

Поиск по платформе объединяет поисковый запрос из SAP BusinessObjects Explorer и поверхности InfoSpaces с содержимым платформы SAP BusinessObjects Business Intelligence.

Результаты поиска из SAP BusinessObjects Explorer группируются по категориям метаданных. Поддерживаемые фасеты для пространств InfoSpaces включают в себя тип, расположение и время обновления.

SAP BusinessObjects Explorer отправляет частоту термина в средство поиска по платформе для каждого термина поиска в запросе. Поиск по платформе рассчитывает релевантность по сумме квадратных корней частот терминов. Результирующее значение назначается в качестве показателя для каждого информационного пространства InfoSpace. Затем результаты сортируются по показателям и отправляются клиенту.

17.12 Интеграция времени поиска с SAP NetWeaver Enterprise Search

SAP NetWeaver Enterprise Search версий 7.20 и выше может использовать службы поиска, основанные на OpenSearch (RSS и ATOM). Запросы на поиск могут делегироваться удаленным поставщикам услуг поиска. В таком случае OpenSearch играет роль поставщика службы, NetWeaver Enterprise Search является потребителем результатов поиска, а поиск по платформе SAP BusinessObjects служит поставщиком службы поиска.

Когда пользователь вводит запрос на поиск, SAP NetWeaver Enterprise Search направляет запрос на поиск непосредственно поставщику OpenSearch. Поставщик принимает запрос на поиск и возвращает ответ в SAP NetWeaver Enterprise Search. Затем ответ объединяется с результатами, полученными из других соединителей объектов поиска, и объединенный результат поиска отображается в интерфейсе пользователя.

Для интеграции поиска в системе SAP NetWeaver Enterprise и поиска по платформе необходимо выполнить следующие действия:

1. Создайте соединитель в SAP NetWeaver Enterprise Search.
2. Импортируйте роль пользователя в разделе "Аутентификация" на платформу SAP BusinessObjects Business Intelligence.

17.12.1 Создание соединителя в SAP NetWeaver Enterprise Search

Соединитель объекта поиска типа OpenSearch можно использовать для интеграции внешних поставщиков поиска, предлагающих функции поиска, доступные посредством интерфейса OpenSearch.

Для создания соединителя в SAP NetWeaver Enterprise Search необходимо выполнить следующие предварительные условия.

1. URL-адрес службы описания OpenSearch.
2. Служба описания OpenSearch должна быть доступной только в формате RSS или ATOM.

Выполните следующие действия, чтобы создать соединитель в SAP NetWeaver Enterprise Search:

1. Запустите пульт администрирования и выберите команду "Создать".
2. Выберите тип соединителя объекта поиска "OpenSearch".
3. Нажмите кнопку **Далее**.
4. Введите URL-адрес службы описания OpenSearch для поставщика OpenSearch.
5. Выберите любой из следующих параметров аутентификации, чтобы запустить URL-адрес службы описания:
 - Нет аутентификации: аутентификация не проводится.
 - Билет принятия аутентификации SAP: этот пользователь используется при аутентификации посредством единого входа.
 - Пользователь/пароль: для аутентификации используется заранее определенный пользователь.
6. Выберите URL-адрес запуска поиска в параметрах URL-адреса OpenSearch.
Затем служба описания OpenSearch проверяется на наличие подходящей службы поиска. Система автоматически вводит значение для шаблона URL-адреса поиска и связанного с ним описания.
7. Выберите любой из следующих параметров аутентификации, чтобы настроить соединитель.
 - Нет аутентификации: аутентификация не проводится.
 - Билет принятия аутентификации SAP: этот пользователь используется при аутентификации посредством единого входа.
 - Пользователь/пароль: для аутентификации используется заранее определенный пользователь.
8. Нажмите кнопку **Далее**.

Отображается диалоговое окно сводки со значениями, указанными для этого соединителя объекта поиска.

9. Нажмите кнопку **Назад**, чтобы изменить параметры, или нажмите кнопку **Отмена**, чтобы удалить все введенные данные.
10. Чтобы сохранить параметры, нажмите кнопку **Завершить**.

17.12.2 Импорт роли пользователя в аутентификации SAP BusinessObjects Enterprise

Выполните следующие действия, чтобы импортировать роль пользователя в аутентификацию платформы SAP BusinessObjects Business Intelligence:

Примечание:

Администратор должен располагать подробными данными пользователя, сведениями по системе, информацией о хосте приложения и учетными данными пользователя.

1. Перейдите в область СМС «Аутентификация».
2. Выберите вариант **SAP**.
3. Укажите следующие значения на вкладке «Системы контроля полномочий»:
 - Система
 - Клиент
 - Сервер приложений
 - Номер системы
 - Имя пользователя
 - Пароль
 - Язык
4. Выберите вариант **Обновить**.
5. Перейдите на вкладку «Импорт роли» и выполните импорт пользовательских ролей.
6. Выберите вариант **Обновить**.
7. Выберите в СМС пункт меню **Управление > Безопасность пользователя**, чтобы назначить соответствующие права пользователя.

17.12.3 Поиск из NetWeaver Enterprise Search

Для выполнения поиска результатов в SAP NetWeaver Enterprise Search выполните следующие действия:

1. Войдите в приложение SAP NetWeaver Enterprise Search.
2. Выберите **Расширенный поиск**.

3. Выберите соединитель, созданный для поиска по платформе.

4. Выполните поиск по ключевому слову.

Консолидированные результаты по ключевому слову будут содержать результат из поиска по платформе, если будут найдены совпадения по этому ключевому слову.

17.13 Выполнение аудита

Все события запросов на поиск, отправленные любым клиентским приложением, использующим службу поиска по платформе, а также результаты запроса подвергаются аудиту. Для поиска по платформе аудит реализован на уровне службы.

Для поиска по платформе существует один идентификатор события (1009) и четыре специальных элемента сведений о событии, таких как:

- Keyword searched (поиск по ключевому слову) (ид. 19);
- Number of Search Results (число результатов поиска) (ид. 63);
- Facet Search (фасеточный поиск) (ид. 20);
- Search Exception (исключение при поиске) (ид. 1).

Помимо перечисленных выше элементов сведений события, также используются и несколько стандартных элементов сведений события, например sessionCuid и userCuid, которые поддерживаются любым аудитом в любом модуле платформы BI.

Работа аудита в поиске по платформе поясняется далее на примере.

При поиске по ключевому слову, такому как "Продажи", общее число результатов может быть равно 5. В этом случае аудит применяется к следующим событиям:

- Событие с ид. 1009
- Элемент сведений события с ид. 19 и значением "продажи"
- Элемент сведений события с ид. 63 и значением 5
- CUID сеанса
- CUID пользователя
- Статус со значением 0 (успешное выполнение)
- Время начала
- Продолжительность
- Объект
- Ид. со значением 0, поскольку аудит выполняется со стороны службы

Если созданы фасеты и выбраны одна или несколько из них, аудит применяется к следующим событиям:

- Событие с ид. 1009
- Элемент сведений события с ид. 19 и значением "продажи"
- Элемент сведений события с ид. 63 и значением 5
- Элемент сведений события с ид. 20 и разделенной запятыми строкой фасет

- CUID сеанса
- CUID пользователя
- Статус со значением 0 (успешное выполнение)
- Время начала
- Продолжительность
- Идентификатор объекта со значением 0, поскольку аудит выполняется со стороны службы

Если при поиске возникло исключение из-за недопустимости введенного значения, например **"a"**, аудит применяется к следующим сведениям о событии:

- Событие с ид. 1009
- Элемент сведений события с ид. 19 и значением "продажи"
- Элемент сведений события с ид. 63 и значением 0
- Элемент сведений события с ид. 1 и сообщением об исключении
- CUID сеанса
- CUID пользователя
- Статус со значением 1 (сбой при выполнении)
- Время начала
- Продолжительность
- Ид. объекта со значением 0, поскольку аудит выполняется со стороны службы

17.14 Список сбоев индексации

Список случаев сбоя индексации содержит перечень документов, которые не удалось проиндексировать. Поиск по платформе предлагает три попытки индексирования документа. Если индексировать документ не удастся, он указывается в списке случаев сбоя индексации.

Чтобы просмотреть список случаев сбоя индексации, выполните следующие шаги:

1. Перейдите в область «Программные приложения» СМС.
2. Выберите **Приложение поиска по платформе**.
3. Последовательно выберите **Действия > Список случаев сбоя индексации**.

Будет открыто диалоговое окно «Приложение поиска по платформе», содержащее список документов со следующими подробными сведениями:

- Название: отображается название документа, для которого произошел сбой индексации.
- Тип: отображается имя типа документа, например Crystal Report и Web Intelligence, и расположение документа.
- Тип сбоя: отображается код ошибки вместе с причиной сбоя индексации документа. Перейдите по гиперссылке "Дополнительная информация", чтобы узнать подробную информацию о трассировке стека причины ошибки.
- Время последней попытки: метка времени последней попытки проиндексировать документ.

17.15 Устранение неполадок

В этом разделе приводятся пошаговые решения для широкого круга проблем, которые могут возникнуть при получении результатов от поиска по платформе.

Не удалось получить результаты поиска из заново добавленного документа, содержащего ключевое слово

- Проверьте, поддерживает ли поиск по платформе тип предоставленного документа. Если тип документа не поддерживается, то документ не будет индексирован.

Для получения дополнительных сведений о поддерживаемых типах документов см. главу *Типы документов, поддерживающие поиск* в списке связанных разделов документации ниже.

- Проверьте выбранное значение параметра **Частота обхода**. Если установлено значение **Частоты обхода: Постоянный обход**, документы отбираются для индексации немедленно. Если установлено значение **Частоты обхода: Плановый обход**, индексация выполняется только в запланированные периоды времени, по расписанию.

Для получения дополнительных сведений о параметре *Частота обхода* см. раздел *Настройка свойств приложения* в приведенных ниже связанных темах справки.

- Проверьте список сбоев индексирования, чтобы убедиться, что индексирование документа прошло успешно. Если документ отображается в этом списке, то необходимо изменить список и отправить его повторно, после этого поиск по платформе будет обрабатывать документ при индексации.

Примечание:

Можно изменить документ, добавив или удалив поле и сохранив его повторно. При этом будет обновлена временная метка документа в репозитории платформы SAP BusinessObjects Business Intelligence, что инициирует повторную индексацию документа.

Для получения дополнительных сведений о документе, индексирование которого завершилось неудачно, см. раздел *Список случаев сбоев индексации* в списке связанных тем ниже.

- Проверьте журналы трассировки адаптивного сервера обработки, содержащие данные о сбое индексирования.
 1. В файловой системе перейдите в каталог {BOE Install Dir}\logging\, где содержится журнал трассировки APS с расширением .glf.
 2. Откройте файл журнала трассировки и выполните поиск документа SI_ID, который требуется индексировать.

Примечание:

SI_ID документа можно найти в его свойствах.

Не удалось получить документы отчетов Crystal в составе результатов поиска

Поиск по платформе индексирует содержимое отчетов Crystal только для версий 2008 и 2011. Индексация содержимого Crystal Reports для Enterprise не выполняется.

Однако в данных Crystal Reports для Enterprise можно выполнять поиск метаданных документа, таких, как заголовок, описание и ключевое слово, которые являются частью свойств документа.

Если документ содержит подлежащее индексации содержимое, необходимо следовать процессу, описанному в приведенном ранее разделе *Не удалось получить результаты поиска из недавно добавленного документа, содержащего ключевое слово*.

Не удалось получить результаты поиска на языке, заданном в качестве языкового стандарта продукта в стартовой панели BI

Поиск по платформе выполняет поиск и индексацию содержимого из репозитория платформы SAP BusinessObjects Business Intelligence, основываясь на языковом стандарте индексации, заданном в СМС. Если языковой стандарт продукта, заданный в стартовой панели BI, отличается от языкового стандарта, заданного в СМС, поиск по платформе не извлекает результатов.

Для получения дополнительных сведений о настройке языкового стандарта индексации см. раздел *Настройка свойств приложения* в списке связанных разделов документации ниже.

Не удалось получить информационные пространства InfoSpaces из SAP BusinessObjects Explorer в составе результатов поиска

Проверьте сервера SAP BusinessObjects Explorer, возможно, они остановлены или отключены. Обеспечьте средству поиска по платформе доступ к серверам для извлечения результатов поиска из SAP BusinessObjects Explorer.

SAP NetWeaver Enterprise Search не может получить результаты из репозитория платформы SAP BusinessObjects Business Intelligence.

- Проверьте, получает ли поиск по платформе результаты поиска с помощью стартовой панели BI, чтобы определить, связана ли проблема с интеграцией поиска по платформе и поиска в системе SAP NetWeaver Enterprise.
- Проверьте, правильно ли развернут OpenSearch на сервере веб-приложений. Конкретные действия по проверке развертывания OpenSearch зависят от типа используемого сервера веб-приложений.
- Проверьте, правильно ли создан и настроен соединитель в конфигурации SAP NetWeaver Enterprise Search. Для объединения результатов из поиска по платформе необходимо использовать правильный соединитель для поиска в системе SAP NetWeaver Enterprise.
- Убедитесь, что обмен данными между компьютерами, на которых выполняется SAP NetWeaver Enterprise Search и SAP BusinessObjects Enterprise, проходит нормально. В случае любых нарушений работы сети в распределенной сети при объединении результатов в SAP NetWeaver Enterprise Search может произойти сбой.
- Проверьте, добавлены ли пользователи SAP NetWeaver Enterprise Search к платформе SAP BusinessObjects Business Intelligence с предоставлением соответствующих прав. Для проверки прав пользователя перейдите в раздел **Аутентификация** в СМС и выберите **SAP**.

См. также

- [Список сбоев индексации](#)
- [Настройка свойств приложения](#)
- [Типы содержимого, доступного для поиска](#)

Интеграция

18.1 интеграция

Приложение для объединения данных – это средство тиражирования данных между сайтами, которое работает с несколькими вариантами развертывания платформы BI в глобальной среде.

Содержимое может создаваться и управляться из одного развертывания платформы BI, а затем тиражироваться в другие развертывания платформы BI в различных географических точках согласно расписанию. Вы можете задать задания одностороннего и двухстороннего тиражирования.

Преимущества интеграции заключаются в ее возможностях:

- Сокращать сетевой трафик
- Создавать содержимое и управлять им из единой системы
- Увеличивать производительность для конечных пользователей

При тиражировании содержимого с использованием интеграции, вы сможете:

- Упростить администрирование нескольких развертываний
- Обеспечить непротиворечивую политику прав сразу в нескольких офисах глобальной организации.
- Получать информацию быстрее, обрабатывать отчеты удаленных сайтов, на которых расположены данные.
- Экономить время, получая быстрее как локальные, так и распределенные данные.
- Синхронизировать содержимое из нескольких развертываний без написания пользовательского кода.

Приложение для объединения данных позволяет создавать отдельные модели безопасности, жизненные циклы, определять время тестирования и развертывания так же успешно, как и владелец организации или администратор. Например, можно распространить функции администрирования, запрещающие администратору приложения по управлению продажами изменять данные приложения по управлению персоналом.

Вы можете тиражировать большое количество объектов, используя интеграцию, как это описано в следующей таблице.

Категория	Типы объектов, которые можно тиражировать	Дополнительные примечания
Объекты Business View	Менеджер Business View Manager, соединения для передачи данных, списки значений, основания данных и т.д.	Поддерживаются все объекты, хотя и не на индивидуальном уровне.
Отчеты	отчеты Crystal, Web Intelligence и Dashboard Design.	Поддерживаются надстройки Full Client и шаблоны.
Сторонние объекты	Файлы Excel, PDF, PowerPoint, Flash, Word, TXT, RTF и Shockwave Flash	
Пользователи	Пользователи, группы, входящие, избранное и персональные категории	
Платформа Business Intelligence	Папки, события, категории, календари, уровни доступа, гиперссылки, ярлыки, программы, профили, пакеты объектов, агностические документы	
Юниверс	Юниверсы, соединения и перегрузки юниверсов	

В следующих примерах показаны два сценария использования интеграции в вашей организации.

Сценарий 1: Розница (централизованный дизайн)

Магазину ACME необходимо передавать ежемесячные отчеты о продажах во все остальные магазины данной фирмы, используя одностороннее тиражирование. Администратор создает отчет на сайте-источнике, который администраторы каждого сайта-адресата протиражируют и выполняют в базе данных магазина.

Совет:

Локализованные экземпляры могут быть отправлены назад, на исходный сайт, вместе с информацией, которая сопровождает каждый тиражированный объект. Например, можно вставить соответствующий логотип, информацию о соединении с базой данных и так далее.

Сценарий 2: Удаленное расписание (распределенный доступ)

Данные находятся на исходном сайте. Ожидающие задания тиражирования отправляются на исходный сайт для последующего запуска. Выполненные задания тиражирования направляются на сайты-адресаты для проверки. Например, данные отчета могут быть недоступны на сайте-адресате, но пользователь может запустить эти отчеты на исходном сайте перед тем, как заполненный отчет будет отправлен назад, на сайт-адресат.

18.2 Термины модуля "Интеграция"

В следующем списке терминов представлены слова и фразы, которые относятся к модулю "Интеграция" и могут облегчить его использование.

18.2.1 Приложение BI

Логическая группировка связанного содержимого Business Intelligence (BI), предназначенная для определенных задач и пользователей. Приложение BI не является объектом. В развертывании платформы BI могут существовать несколько приложений BI, для каждого из которых предусмотрены отдельная модель защиты, жизненный цикл, проверка и время разработки, а также отдельные бизнес-пользователи и администраторы.

18.2.2 Сайт-адресат

Система платформы BI, которая принимает тиражированное содержимое платформы BI с сайта-источника.

18.2.3 Локальный

Локальная система, к которой подключен пользователь или администратор. Например, администратор сайта-адресата считается «локальным» на сайте-адресате.

18.2.4 Выполняемые локально завершенные экземпляры

Экземпляры, обрабатываемые на сайте-адресате и передаваемые обратно на сайт-источник.

18.2.5 Несколько сайтов-источников

Несколько сайтов могут выступать в роли сайта-источника. Например, для нескольких центров разработки обычно предусмотрены несколько сайтов-источников. Однако для тиражирования можно использовать только один сайт-источник.

18.2.6 Однонаправленное тиражирование

Объекты тиражируются только в одном направлении: с сайта-источника на сайт-адресат. Любые обновления на сайте-адресате остаются на сайте-адресате.

18.2.7 Сайт-источник

Система платформы BI, из которой поступает содержимое.

18.2.8 Удаленный

Система, которая не является локальной для пользователя. Например, сайт-источник считается «удаленным» для пользователей и администраторов сайта-адресата.

18.2.9 Удаленное соединение

Объект, в котором содержится информация, используемая для подключения к платформе BI, включая имя пользователя и пароль, имя CMS, URI веб-служб и параметры очистки.

18.2.10 Удаленное планирование

Запросы планирования, которые передаются с сайта-адресата на сайт-источник. Отчеты на сайтах-адресатах можно запланировать удаленно, при этом экземпляр отчета будет передаваться обратно на сайт-источник для обработки. Затем выполненный экземпляр возвращается на сайт-адресат.

18.2.11 Тиражирование

Процесс копирования содержимого из одной системы платформы BI в другую.

18.2.12 Задание тиражирования

Объект, в котором содержится информация о планировании содержимого, содержанием, подлежащем тиражированию, и любых специальных условиях, которые должны выполняться при тиражировании содержимого.

18.2.13 Список тиражирования

Список объектов, подлежащих тиражированию. В списке тиражирования есть ссылки на другое содержимое, например пользователи, группы, отчеты и т. д. для платформы BI, тиражирование которого будет выполняться одновременно.

18.2.14 Объект тиражирования

Объект, тиражируемый с сайта-источника на сайт-адресат. Все тиражированные объекты на сайте-адресате будут отмечены значком тиражирования. При наличии конфликта объекты отмечаются значком конфликта.

18.2.15 Пакет тиражирования

В пакете тиражирования, созданном во время передачи, содержатся объекты из задания тиражирования. В нем могут содержаться все объекты, определенные в списке тиражирования, как в случае быстро изменяющейся среды или первоначального тиражирования. В нем также может содержаться подмножество списка тиражирования, если объекты изменяются нечасто по сравнению с планированием задания тиражирования. Пакет тиражирования выполняется как файл BIAR (программный ресурс BI).

18.2.16 Обновление тиражирования

Все объекты в списке тиражирования обновляются вне зависимости от последней измененной версии.

18.2.17 Двухнаправленное тиражирование

Действие равнозначно действию однонаправленного тиражирования, но при двухнаправленном тиражировании изменения также передаются в обоих направлениях. Обновления на сайте-источнике тиражируются на каждый сайт-адресат. Обновления и новые объекты на сайте-адресате пересылаются на сайт-источник.

18.3 Управление правами безопасности

Однако, поскольку модуль "Интеграция" тиражирует содержимое между отдельными системами, и требуется взаимодействие с другими администраторами, необходимо знать механизм работы безопасности перед использованием этого модуля.

Перед включением модуля "Интеграция" действия администраторов различных систем должны быть согласованы. После тиражирования содержимого администраторы могут изменять его.

Для выполнения определенных задач требуются определенные права в развертываниях источника и адресата:

- Права, необходимые на сайте-источнике
- Права, необходимые на сайте-адресате
- Права, необходимые для объектов модуля "Интеграция"
- Сценарии интеграции

Совет:

Перед началом использования модуля "Интеграция" рекомендуется прочитать этот раздел.

18.3.1 Права, необходимые на сайте-источнике

В этом разделе описаны действия на сайте-источнике и права, необходимые для подключения учетной записи пользователя к сайту-источнику. Это учетная запись, которая указана в объекте удаленного соединения на сайте-адресате.

Действие	Описание	Необходимые права
Однонаправленное тиражирование	Выполнение тиражирования только с сайта-источника на сайт-адресат. Примечание: Права «просмотра» и «тиражирования» требуются для всех тиражируемых объектов, включая объекты, которые тиражируются автоматически путем вычислений зависимостей.	<ul style="list-style-type: none"> Права «просмотра» и «тиражирования» всех тиражируемых объектов Право «просмотра» списка тиражирования
Двухнаправленное тиражирование	Выполнение тиражирования с сайта-источника на сайт-адресат и с сайта-адресата на сайт-источник.	<ul style="list-style-type: none"> Права «просмотра» и «тиражирования» всех тиражируемых объектов Право «просмотра» списка тиражирования Право «изменения прав» пользовательских объектов для тиражирования всех изменений пароля
Планирование	Разрешение удаленного планирования на сайте-источнике с сайта-адресата.	<ul style="list-style-type: none"> Право «планирования» для всех объектов, планируемых удаленно

См. также

- [Права, необходимые на сайте-адресате](#)

18.3.2 Права, необходимые на сайте-адресате

В этом разделе описаны действия на сайте-адресате и необходимые права учетной записи пользователя, который выполняет задание тиражирования. Это учетная запись пользователя, создавшего задание тиражирования.

Примечание:

Как и другие планируемые объекты, можно запланировать задание тиражирования от имени другого пользователя.

Действие	Описание	Необходимые права
Все объекты	Тиражирование объектов вне зависимости от режима тиражирования: однонаправленное или двунаправленное.	<ul style="list-style-type: none"> Права «просмотра», «добавления», «правки» и «изменения» для всех объектов Право «изменения пароля пользователя» для всех объектов пользователя
Первое тиражирование	При первом выполнении задания тиражирования объекты отсутствуют на сайте-адресате. Поэтому для учетной записи пользователя, который выполняется задание тиражирования, должны быть настроены права во всех папках верхнего уровня и объектах, в которые будет добавляться содержимое.	<ul style="list-style-type: none"> Права «просмотра», «добавления», «редактирования» и «изменения прав» во всех папках верхнего уровня и объектах по умолчанию.

См. также

- [Права, необходимые на сайте-источнике](#)

18.3.3 Права, характерные для интеграции

В этом разделе подробно описаны сценарии, которые встречаются при использовании модуля "Интеграция".

Действие	Описание	Необходимые права
Очистка объектов	При очистке объектов удаляются объекты на сайте-адресате.	<ul style="list-style-type: none"> Учетная запись, под которой выполняется задание тиражирования, требует наличия прав «удаления» для всех объектов, которые могут быть удалены.
Отключение очистки для определенных объектов	<p>При тиражировании определенных объектов с сайта-источника может потребоваться пропуск их удаления с сайта-адресата, если объекты удалены с сайта-источника. Для этого можно настроить права. Например, выберите этот параметр, если пользователи на сайте-адресате используют объект независимо от пользователей на сайте-источнике.</p> <p>Пример. Может потребоваться сохранение тиражированного юниверса, в котором пользователи на сайте-адресате создают собственные локальные отчеты, если юниверс удален с сайта-источника.</p>	<ul style="list-style-type: none"> Запретите права «удаления» пользовательской учетной записи, под которой выполняется задание тиражирования, для объектов, которые необходимо сохранить.
Двунаправленное тиражирование при отсутствии изменений на исходном сайте		<ul style="list-style-type: none"> Запретите права «изменения» пользовательской учетной записи, используемой для подключения в объекте удаленного соединения.

Действие	Описание	Необходимые права
	<p>В некоторых случаях можно выбрать двунаправленное тиражирование и запретить изменение некоторых объектов на сайте-источнике, даже если они изменяются на сайте-адресате. Это может потребоваться по нескольким причинам, в том числе, если объект является специальным и не должен изменяться пользователями на сайте-источнике, или если необходимо включить удаленное планирование, и отсутствует необходимость обратной передачи изменений.</p> <p>Примечание: Для удаленного планирования можно создать задание, в котором обрабатываются только объекты для удаленного планирования. Однако в этом случае будет выполняться тиражирование предшествующих объектов, включая отчет, папку, в которой содержится отчет, и родительскую папку этой папки. Любые изменения на сайте-адресате тиражируются обратно на сайт-источник, а изменения на сайте-источнике тиражируются на сайт-адресат.</p>	

18.3.4 Тиражирование безопасности объекта

Для сохранения прав безопасности объекта необходимо одновременно выполнить тиражирование как объекта, так и его пользователя или группы. В противном случае они должны существовать на сайте, на который выполняется тиражирование, и иметь идентичные уникальные идентификаторы (CUID) на каждом сайте.

Если выполняется тиражирование объекта без тиражирования пользователя или группы или пользователь или группа не существует на сайте, на который выполняется тиражирование, их права будут сброшены.

Пример:

Для группы А и группы Б права назначены в объекте А. Для группы А настроены права «просмотра», а для группы Б – права «запрета просмотра». Если в задании тиражирования тиражируются только группа А и объект А, на сайте-адресате объект А будет иметь только права «просмотра» группы А, связанной с ним.

При тиражировании объекта существует вероятность возникновения угрозы безопасности, если не выполняется тиражирование всех групп с явно заданными правами объекта. В предыдущем примере описана потенциальная угроза. Если пользователь А принадлежит группе А и группе Б, у него не будет прав просмотра объекта А на сайте-источнике. Однако пользователь А будет тиражирован на сайт-адресат, поскольку он принадлежит обеим группам. Поскольку тиражирование группы Б не выполняется, пользователь А будет иметь право просмотра объекта А на сайте-адресате, но не сможет просматривать объект А на сайте-источнике.

Объекты, ссылающиеся на другие объекты, не включенные в задание тиражирования, или не существующие на сайте-адресате, отображаются в файле журнала. В этих файлах отображается нетиражированный объект со ссылкой на объект и сброс этой ссылки.

Параметры безопасности объектов для определенного пользователя или группы тиражируются только с сайта-источника на сайт-адресат. Можно настроить параметры безопасности тиражированных объектов на сайте-адресате, но эти параметры не будут тиражироваться на сайт-источник.

18.3.5 Тиражирование параметров безопасности с использованием уровней доступа

Для хранения права должны быть определены на уровнях доступа. Объект, пользователь или группа и уровень доступа должны тиражироваться одновременно, или они должны существовать на сайте, на который выполняется тиражирование.

Объекты, задающие явные права для пользователя или группы, не включенных в задание тиражирования или не существующих на сайте-адресате, отображаются в своих файлах журнала, показывающих, что объекту назначены права, тиражирование которых не выполнено, и права были сброшены.

Кроме того, можно выбрать автоматическое тиражирование для «Уровней доступа», используемых в импортированных объектах. Этот параметр доступен в списке тиражирования.

Примечание:

Уровни доступа по умолчанию не тиражируются, но ссылки сохраняются.

18.4 Параметры типов и режимов тиражирования

В зависимости от выбранных типа и режима тиражирования можно создавать один из четырех видов заданий тиражирования:

- Однонаправленное тиражирование,
- Двухнаправленное тиражирование
- Обновлять из источника
- Обновлять из адресата.

18.4.1 Однонаправленное тиражирование

При однонаправленном тиражировании содержимое можно тиражировать только в одном направлении: с сайта-источника на сайт-адресат. Все изменения, внесенные в объект на сайте-источнике в список тиражирования, пересылаются на сайт-адресат. Однако изменения объектов на сайте-адресате не пересылаются в обратном направлении на сайт-источник.

Однонаправленное тиражирование идеально подходит для конфигураций с одним центральным развертыванием платформы BI, где создаются, изменяются и администрируются объекты. В остальных развертываниях используется содержимое центральной системы.

Для создания однонаправленного тиражирования выберите следующие параметры:

- Тип тиражирования = Однонаправленное тиражирование
- Режим тиражирования = Обычное тиражирование

18.4.2 Двухнаправленное тиражирование

При двухнаправленном тиражировании содержимое можно тиражировать в обоих направлениях между сайтом-источником и сайтом-адресатом. Любые изменения, внесенные в объект на сайте-источнике, тиражируются на сайты-адресаты, а изменения на сайте-адресате тиражируются на сайт-источник.

Примечание:

Для выполнения удаленного планирования и тиражирования локально выполненных экземпляров обратно на сайт-источник необходимо выбрать режим двухнаправленного тиражирования.

При наличии нескольких платформ BI, в которых содержимое создается, изменяется, администрируется и используется в обоих местоположениях, самым эффективным вариантом является двухнаправленное тиражирование. Оно также позволяет синхронизировать системы.

Для создания двунаправленного тиражирования выберите следующие параметры:

- Тип тиражирования = Двунаправленное тиражирование
- Режим тиражирования = Обычное тиражирование

См. также

- [Удаленное планирование и экземпляры, выполняемые локально](#)

18.4.3 "Обновлять из источника" или "Обновлять из адресата"

При тиражировании содержимого в режиме однонаправленного или двунаправленного тиражирования объекты в списке тиражирования тиражируются на сайт-адресат. Тем не менее, не все объекты могут тиражироваться при каждом выполнении задания тиражирования.

В модуле "Интеграция" предусмотрен механизм оптимизации, который способствует более быстрому завершению выполнения заданий тиражирования. В нем используется комбинация версии объекта и временного штампа для определения, был ли изменен объект с момента выполнения последнего тиражирования. Эта проверка выполняется для объектов, выбранных в списке тиражирования, и для всех объектов, тиражированных во время проверки зависимостей.

Однако в некоторых случаях механизм оптимизации может пропускать объекты, которые не будут тиражированы. В этих случаях можно использовать параметры «Обновлять из источника» и «Обновлять из адресата» для принудительного тиражирования содержимого и зависимостей без учета меток времени.

Параметр "Обновлять из источника" позволяет только отправить содержимое с сайта-источника на сайт-адресат. Параметр "Обновлять из адресата" позволяет только отправить содержимое с сайтов-адресатов на сайт-источник.

Пример:

В следующих трех примерах показаны сценарии использования параметров «Обновлять из источника» и «Обновлять из адресата», в которых определенные объекты будут пропущены во время оптимизации.

Сценарий 1. Добавление объектов, содержащих другие объекты, в область, подлежащую тиражированию.

Папка А тиражируется с сайта-источника на сайт-адресат. В настоящее время она существует на обоих сайтах. Пользователь перемещает или копирует папку Б с отчетом Б в папку А на сайте-источнике. При последующем тиражировании в модуль "Интеграция" будет передана информация, что метка времени папки Б изменена, и будет выполнено тиражирование папки на сайт-адресат. Однако метка времени отчета Б не изменена. Поэтому он будет пропущен при выполнении обычного однонаправленного или двунаправленного задания тиражирования.

Чтобы убедиться в правильности тиражирования содержимого папки Б, необходимо один раз выполнить задание тиражирования с параметром «Обновлять из источника». После этого

тиражирование будет выполняться правильно в обычном однонаправленном или двунаправленном задании тиражирования. Если действия в этом примере выполняются в обратном направлении и папка Б перемещается или копируется на сайт-адресат, необходимо использовать параметр «Обновлять из адресата».

Сценарий 2. Добавление новых объектов с помощью LifeCycle Manager или командной строки BIAR.

При добавлении объектов в область, тиражирование которой выполняется с использованием LifeCycle Manager или командной строки BIAR, объект можно не выбирать при выполнении обычного однонаправленного или двунаправленного задания тиражирования. Это происходит, поскольку внутренние часы в исходной и конечной системах могут быть не синхронизированы при использовании LifeCycle Manager или командной строки BIAR.

Примечание:

После импорта новых объектов в область, тиражируемую на сайт-источник, рекомендуется выполнять задание тиражирования «Обновлять из источника». После импорта новых объектов в область, тиражируемую на сайт-адресат, рекомендуется выполнять задание тиражирования «Обновлять из адресата».

Сценарий 3. В период между выполнением запланированного тиражирования.

Если объекты добавляются в тиражируемую область и необходимо тиражировать их, не дожидаясь выполнения следующего запланированного тиражирования, можно использовать задания тиражирования «Обновлять из источника» и «Обновлять из адресата». Содержимое можно быстро тиражировать, выбрав область, в которую были добавлены объекты.

Примечание:

- Этот сценарий может занять много времени для больших списков тиражирования, поэтому частое использование этого параметра не рекомендуется. Например, отсутствует необходимость создания заданий тиражирования для режима ежечасного обновления с сайта-источника на сайт-адресат. Эти режимы следует использовать при значении графика тиражирования «Запустить сейчас» или нечастого выполнения.
- В некоторых случаях нельзя использовать разрешение конфликтов, включая параметры: «Обновлять из источника»: параметр приоритета сайта-адресата заблокирован или «Обновлять из адресата»: параметр приоритета сайта-источника заблокирован.

18.5 Тиражирование сторонних пользователей и групп

В модуле "Интеграция" можно тиражировать сторонних пользователей и группы, например пользователей и группы Active Directory (AD) и LDAP.

Совет:

Прочитайте этот раздел, если планируется тиражирование этих типов пользователей и групп или их персонального содержимого, такого как папки "Избранное" или "Входящие".

Сопоставление пользователей и групп

1. Сопоставьте пользователей и группы на сайте-источнике для правильного тиражирования с помощью модуля "Интеграция".
2. Выполните тиражирование сопоставленных пользователей и групп на сайт-адресат.

Примечание:

Не сопоставляйте группы и пользователей отдельно на сайте-адресате. В противном случае они будут иметь различные уникальные идентификаторы (CUID) на сайте-адресате и сайте-источнике, и модуль "Интеграция" не сможет сопоставить пользователя или группы.

Пример:

Администратор сопоставляет группу А и пользователя А на сайте-источнике и сайте-адресате. Для группы А и пользователя А созданы различные уникальные идентификаторы на сайте-источнике и сайте-адресате. Во время тиражирования модулю "Интеграция" не удастся сопоставить их, и группа А или пользователь А не тиражируются из-за конфликта псевдонимов.

Примечание:

- Перед тиражированием сторонних пользователей и групп на сайте-адресате уже настроено использование аутентификации AD или LDAP. Однако необходимо также настроить на сайте-адресате использование AD или LDAP, чтобы он мог обращаться к серверу каталогов или контроллеру домена.
- После первого тиражирования группы AD или LDAP пользователи из этой группы не смогут выполнять вход до обновления группового графика AD/LDAP. Это выполняется автоматически приблизительно каждые 15 минут. Чтобы обновить граф групп AD/LDAP вручную, откройте страницу СМС «Аутентификация», дважды щелкните **Windows AD** или **LDAP** и щелкните **Обновить**.
- Будьте осторожны при тиражировании сторонних групп. При добавлении новых пользователей в группу на сервере каталогов они получают права входа в систему на обоих сайтах. Это вопрос защиты аутентификации AD или LDAP, который не зависит от модуля "Интеграция".

Если выполнен отдельный вход на сайте-адресате и сайте-источнике, или информация о принадлежности к группе обновляется с использованием кнопки обновления на странице аутентификации СМС, учетная запись пользователя создается на обоих сайтах. Учетным записям будут назначены различные идентификаторы, и модуль "Интеграция" не сможет правильно выполнить тиражирование.

Примечание:

Важно создать учетную запись на одном сайте, а затем тиражировать ее на другой сайт.

18.6 Тиражирование юниверсов и соединений юниверсов

При использовании модуля "Интеграция" для тиражирования юниверсов между развертываниями платформы ВІ важно уделить время предварительному планированию результатов. Объект юниверса не работает без соответствующего базового соединения юниверса.

Объекты соединений юниверсов содержат информацию, необходимую для соединения с базой данных отчетов. Для правильной работы объектов соединений юниверсов содержащаяся в них информация должна быть правильной и позволять устанавливать соединение с базой данных.

Примечание:

Если используется двустороннее тиражирование, и тиражирование юниверса с сайта-источника на сайт-адресат выполняется без соответствующего юниверсу соединения, при последующем тиражировании связь юниверса с соединением юниверса в источнике может быть перезаписана или удалена. Во избежание этого всегда тиражируйте подключения юниверсов вместе с юниверсами.

Чтобы обеспечить тиражирование зависимых соединений юниверсов вместе с соответствующими юниверсами, всегда выбирайте следующие параметры при создании или изменении списка тиражирования, в котором содержатся эти юниверсы:

- **Включить соединения, которые требуются для выбранных юниверсов**
- **Включить юниверсы, которые требуются для выбранных юниверсов**

Примечание:

Если связь юниверса с соединением юниверса переписывается или удаляется, откройте юниверс в Universe Designer и в меню **Файл > Параметры** измените информацию о соединении.

В следующих двух примерах показан пример тиражирования юниверсов и соответствующих им соединений.

Пример:

При тиражировании юниверсов и соединений юниверсов необходимо, чтобы среда соединения сайта-источника соответствовала среде соединения сайта-адресата.

Например, если соединение юниверса использует соединение ODBC под названием «TestODBC», в среде назначения должно быть правильно настроенное соединение ODBC под названием «TestODBC». Соединение ODBC может быть установлено с прежней или с другой базой данных. Чтобы у юниверсов, использующих это соединение, не возникало проблем с соединением, схемы баз данных должны быть одинаковыми.

Пример:

Если требуется, чтобы тиражированный юниверс на сайте-адресате использовал базу данных, отличную от используемой юниверсом на сайте-источнике, при тиражировании соединения юниверса укажите ссылку на нужную базу данных в сведениях о соединении на сайте-адресате.

Например, если соединение юниверса на сайте-источнике использует соединение ODBC под названием «Test», указывающее на базу данных «DatabaseA», на сайте-адресате также должно быть соединение ODBC под названием «Test», но указывающее на базу данных «DatabaseB».

18.7 Управление списками тиражирования

Списки тиражирования включают такое содержимое, как пользователи, группы и отчеты в развертывании платформы BI, которые могут тиражироваться совместно. Список тиражирования можно открыть с помощью консоли СМС.

Типы содержимого, которое можно тиражировать, перечислены в следующей таблице.

Категория	Поддерживаемые объекты
Объекты репозитория	Объекты, включающие бизнес-представления, соединения данных, списки значений, основу данных и так далее. Примечание: Поддерживаются все объекты, хотя и не на индивидуальном уровне.
Отчеты	отчеты Crystal, документы Web Intelligence и объекты Xcelsius. Примечание: Поддерживаются надстройки Full Client и шаблоны.
Сторонние объекты	Файлы Excel, PDF, PowerPoint, Flash, Word, текстовые файлы, rtf, Shockwave Flash
Пользователи	Пользователи, группы, "Входящие", "Избранное", персональная категория.
Платформа Business Intelligence	Папки, события, категории, календари, пользовательские роли, гиперссылки, ярлыки, программы, профили, пакеты объектов, агностические документы.
Юниверсы	Юниверсы, соединения, переопределение юниверсов.

Примечание:

Следующие объекты должны быть установлены на сайте-источнике и затем тиражированы на сайт-адресат. Если эти объекты создаются на сайте-адресате, а затем тиражируются на сайт-источник, они не будут функционировать на сайте-источнике.

- Бизнес-представления
- Бизнес-элементы
- Основания данных
- Соединения данных
- Список значений
- Переопределения юниверсов

18.7.1 Создание списков тиражирования

Списки тиражирования располагаются в области "Списки тиражирования" консоли СМС. Для упорядочения списков тиражирования можно создавать папки и вложенные папки.

18.7.1.1 Создание папки списка тиражирования

1. Перейдите в область «Списки тиражирования» консоли СМС.
2. Выберите **Списки тиражирования**.
3. Выберите команду **Управление > Создать > Папка**.
Открывается диалоговое окно «Создать папку».
4. Введите имя папки и нажмите кнопку **ОК**.
После этого в данной папке можно создавать списки тиражирования.

18.7.1.2 Создание списка тиражирования

1. Перейдите в область «Списки тиражирования» консоли СМС.
2. Выберите папку, в которой необходимо сохранить новый список тиражирования.
3. Выберите команду **Управление > Создать > Новый список тиражирования**.
Открывается диалоговое окно «Новый список тиражирования».
4. Введите заголовок и описание списка тиражирования.
5. Чтобы отобразить дополнительные параметры, щелкните ссылку **Свойства списка тиражирования**.
При этом можно задать зависимости, устанавливаемые для автоматического тиражирования с сайта-источника на сайт-адресат.
6. Выберите необходимые параметры согласно описанию, приведенному в таблице.

Параметры объекта зависимости	Определение
Включить личные папки для выбранных пользователей	Тиражирует личные папки выбранных пользователей и их содержимое.
Включить личные категории выбранных пользователей	Тиражирует личные категории выбранных пользователей.
Включить юниверсы для выбранных отчетов	Тиражирует любой юниверс, от которого зависят выбранные объекты отчета.
Включить участников выбранных групп пользователей	Тиражирует пользователей в выбранной группе.
Включить юниверсы, которые требуются для выбранных юниверсов	Тиражирует все юниверсы, которые зависят от других юниверсов.

Параметры объекта зависимости	Определение
Включить папки "Входящие" выбранных пользователей	Тиражирует папку "Входящие" выбранного пользователя и ее содержимое.
Включить группы пользователей для выбранных юниверсов	Тиражирует группы пользователей, связанные с перепределениями юниверса.
Включить уровни доступа, установленные для выбранных объектов	Тиражирует все уровни доступа, используемые в любом из выбранных объектов.
Включить документы для выбранных категорий	Тиражирует все документы, включая Word, Excel и PDF, содержащиеся в выбранных категориях.
Включить поддерживаемые зависимости для выбранных объектов Flash	Тиражирует все отчеты Crystal, гиперссылки, документы Web Intelligence или юниверсы, от которых зависит объект Flash.
Включить профили для выбранных пользователей и групп пользователей	Тиражирует все профили, связанные с выбранными пользователями или группами.
Включить соединения, которые требуются для выбранных юниверсов	Тиражирует все объекты соединения юниверсов, используемые выбранными объектами.

Примечание:

Некоторые объекты в платформе BI зависят от других объектов. Например: документ Web Intelligence зависит от юниверса, который лежит в основе его структуры и содержимого. Если тиражируется документ Web Intelligence, но не выбран используемый юниверс, тиражирование не будет выполняться на целевом сайте, пока на нем не будет выполнено тиражирование юниверса. Однако если выбрать параметр «Включить юниверсы для выбранных отчетов», модуль "Интеграция" автоматически тиражирует юниверсы, от которых зависит отчет.

7. Нажмите кнопку **Далее**.

8. Выберите один или несколько объектов для добавления в список тиражирования.

- Используйте кнопки со стрелками, чтобы добавить или удалить объекты в папке «Доступные объекты».
- Или выберите **Тиражировать все: Объекты репозитория** для тиражирования всех объектов Business View, бизнес-элементов, оснований данных, соединений для передачи данных, списки значений (LOV) и объектов репозитория, включая изображения и функции отчета.

Примечание:

Тиражирование папок верхнего уровня, расположенных в папке «Доступные объекты», невозможно.

9. Нажмите кнопку **Сохранить и закрыть**.

18.7.2 Изменение списков тиражирования

После создания списка тиражирования можно изменить его свойства или объекты.

18.7.2.1 Изменение свойств списка тиражирования

1. Перейдите в область «Списки тиражирования» консоли СМС.
2. Выберите **Список тиражирования**, который необходимо изменить.
3. Щелкните **Управление > Свойства**.
Открывается диалоговое окно **Общие свойства**.
4. Измените заголовок и описание. В диалоговом окне **Общие свойства** можно также изменить другие области списка тиражирования.
5. Чтобы изменить параметры зависимости, выберите команду **Свойства списка тиражирования** в списке навигации.
6. Нажмите кнопку **Сохранить и закрыть**.

См. также

- [Создание списков тиражирования](#)

18.7.2.2 Изменение объектов в списке тиражирования

1. Перейдите в область «Списки тиражирования» консоли СМС.
2. Выберите **список тиражирования**.
3. Выберите команду **Действия > Управление списком тиражирования**.
Открывается диалоговое окно «Управление списком тиражирования», в котором перечислены добавленные в настоящий момент в список объекты.
4. При необходимости добавьте или удалите объекты.
5. Нажмите кнопку **Сохранить и закрыть**.

См. также

- [Создание списков тиражирования](#)

18.8 Управление удаленными соединениями

В объекте удаленного соединения содержится информация, необходимая для подключения к удаленному развертыванию платформы BI.

Примечание:

Объект удаленного соединения создается в развертываниях платформы BI на сайте-адресате. Удаленное соединение представляет собой сайт-источник.

Удаленные соединения можно просмотреть в области «Интеграция» консоли СМС.

18.8.1 Создание удаленных соединений

Удаленное соединение в модуле "Интеграция" позволяет подключиться к удаленному развертыванию платформы BI. Чтобы установить соединение с сайтом-адресатом, на котором находится содержимое, подлежащее тиражированию, сначала необходимо создать удаленное подключение на сайте-адресате.

Для упорядочения удаленных соединений можно создавать папки и вложенные папки.

18.8.1.1 Создание папки удаленных соединений

1. Перейдите к области «Интеграция» консоли СМС.
2. Выберите **Удаленные соединения**.
3. Выберите команду **Управление > Создать > Папка**.
Открывается диалоговое окно **Создать папку**.
4. Введите имя папки и нажмите кнопку **ОК**.
После этого в данной папке можно создавать удаленные соединения.

18.8.1.2 Создание удаленного соединения

Чтобы подключиться к удаленному развертыванию платформы BI, необходимо создать удаленное соединение в модуле "Интеграция".

1. Перейдите к области «Интеграция» консоли СМС.
2. Выберите **Удаленные соединения**.
3. Выберите команду **Управление > Создать > Новое удаленное соединение**.
Открывается диалоговое окно «Новое соединение с удаленной системой».

4. Укажите заголовок, описание и необходимые соответствующие значения в полях:

Примечание:

Все поля, за исключением полей «Описание» и «Ограничить число объектов очистки», являются обязательными.

Поле	Описание
Название	Имя объекта удаленного соединения.
Описание	Описание объекта удаленного соединения. (Не обязательно)
URI веб-службы удаленной системы	Указатель URL веб-служб модуля "Интеграция", которые автоматически разворачиваются на сервере Java-приложений. Можно использовать любые веб-службы модуля "Интеграция" в платформе BI, в которой они являются сайтом-источником или сайтом-адресатом, или другое разворачивание. Используйте следующий формат: http:// <i>имя_компьютера_сервера_приложения.порт</i> /dswsbobje Пример: http:// <i>mymachine.mydomain.com:8080</i> /dswsbobje
CMS удаленной системы	Имя сервера CMS, к которому необходимо подключиться и который доступен через веб-службы модуля "Интеграция". Он будет использоваться как сервер CMS для сайта-источника. Используется следующий формат: имя_CMS:порт Пример: mymachine:6400 Примечание: Если используется порт по умолчанию 6400, номер порта можно не указывать.
Имя пользователя	Имя пользователя, которое будет использоваться для подключения к сайту-источнику. Примечание: Убедитесь, что для используемой учетной записи настроены права на просмотр списка тиражирования в системе на сайте-источнике.
Пароль	Пароль учетной записи пользователя, используемой для подключения к сайту-источнику.
Аутентификация	Тип аутентификации учетной записи, используемой для подключения к сайту-источнику. Доступные параметры: Enterprise, AD и LDAP.

Поле	Описание
Частота очистки (в часах)	Частота выполнения очистки объектов в заданиях тиражирования, в которых используется этот объект удаленного соединения. Необходимо указывать только целые положительные значения. В качестве единицы измерения используются часы. По умолчанию = 24.
Ограничить число объектов очистки до	Число объектов, очистка которых выполняется заданием тиражирования. (Не обязательно)

5. Нажмите кнопку **ОК**.

См. также

- [Управление очисткой объектов](#)

18.8.2 Изменение удаленных соединений

После создания удаленного соединения можно изменить его свойства и параметры безопасности.

Изменение удаленного соединения:

1. Перейдите к области «Интеграция» консоли СМС.

2. Выберите **Удаленные соединения**.

3. Дважды щелкните удаленное соединение, которое требуется изменить.

Открывается диалоговое окно «Свойства удаленного соединения». Поддерживается изменение следующих свойств:

- **Заголовок**
- **Описание**
- **URI веб-службы удаленной системы**
- **CMS удаленной системы**
- **имя пользователя.**
- **Пароль**
- **Аутентификация**
- **Частота очистки (в часах)**
- **Ограничить число объектов очистки до**



4. Укажите изменения.

5. Нажмите кнопку **Сохранить и закрыть**.

18.9 Управление заданиями тиражирования

Задание тиражирования – это тип объекта, который выполняется по расписанию и используется для тиражирования содержимого между двумя развертываниями платформы BI в модуле "Интеграция".

Примечание:

Тиражированные объекты на сайте-адресате будут отмечены значком тиражирования, как показано здесь:  При наличии конфликта объект отмечается значком конфликта, как показано здесь: 

Список заданий тиражирования можно просматривать в папке **Удаленные соединения** в области «Интеграция» консоли СМС.

18.9.1 Создание заданий тиражирования

Задание тиражирования требуется для тиражирования содержимого между двумя развертываниями платформы BI в модуле "Интеграция". Для каждого задания тиражирования должно быть создано только одно удаленное соединение и установлена связь с одним списком тиражирования.

18.9.1.1 Создание задания тиражирования

1. Перейдите к области «Интеграция» консоли СМС.
2. Выберите **Удаленные соединения**.
3. Выберите **Удаленное соединение**, в котором будет содержаться новое задание тиражирования.

Предупреждение:

Сервер СМС должен иметь возможность подключения к веб-службам в URI удаленного соединения для выполнения дальнейших действий с использованием мастера.

4. Выберите команду **Управление > Создать > Новое задание на тиражирование**.
Открывается диалоговое окно «Новое задание на тиражирование».
5. Введите заголовок и описание задания тиражирования.
6. Нажмите кнопку **Далее**.
Открывается список доступных на сайте-источнике списков тиражирования.

7. Выберите **Список тиражирования**, который необходимо использовать в задании тиражирования.
8. Нажмите кнопку **Далее**.
9. Выберите параметры конфигурации, как описано в следующей таблице.

Действие	Описание
Включить очистку объектов для места назначения	<p>Принудительное удаление заданием тиражирования всех тиражированных объектов на сайте-адресате, если исходный объект был удален с сайта-источника.</p> <p>Примечание: При очистке объектов не будут удаляться объекты, тиражированные с использованием зависимостей, или объектов, выбранных в списке тиражирования.</p>
Однонаправленное тиражирование	Указывает, что объект тиражируется только с сайта-источника на сайт-адресат. Все изменения, внесенные после тиражирования в объект на сайте-источнике, тиражируются на сайт-адресат, а изменения, внесенные на сайте-адресате, не тиражируются обратно на сайт-источник.
Двунаправленное тиражирование	Указывает, что объекты тиражируются в обоих направлениях: с сайта-источника на сайт-адресат и с сайта-адресата на сайт-источник. Изменения, внесенные в эти объекты после тиражирования на одном сайте, автоматически тиражируются на другой сайт.
Сайт-источник имеет приоритет	Указывает, что при обнаружении конфликта между объектом на сайте-источнике и его тиражированной версией на сайте-адресате версия на сайте-источнике имеет приоритет.
Без автоматического разрешения конфликтов	Указывает, что для разрешения обнаруженных конфликтов не предпринимается никаких действий.
Сайт-адресат имеет приоритет (доступен только при двунаправленном тиражировании)	Указывает, что при обнаружении конфликта между объектом на сайте-источнике и его тиражированной версией на сайте-адресате версия на сайте-адресате имеет приоритет.
Обычное тиражирование	Указывает, что задание тиражирования выполняется в обычном режиме.

Действие	Описание
Обновлять из источника	Тиражирует все содержимое с сайта-источника на сайт-адресат вне зависимости от его изменения. Можно тиражировать весь список тиражирования или только часть этого списка.
Обновлять из места назначения (доступен только при двунаправленном тиражировании)	Тиражирует все содержимое с сайта-адресата на сайт-источник вне зависимости от его изменения. Можно тиражировать весь список тиражирования или только часть этого списка.
Тиражировать все объекты (доступен только при двунаправленном тиражировании)	Тиражирует весь список тиражирования. Примечание: Это полный вариант, но для его выполнения требуется длительное время.
Тиражировать удаленные расписания (доступен только при двунаправленном тиражировании)	Тиражирует ожидающие удаленные экземпляры с сайта-адресата на сайт-источник и размещает готовые экземпляры с сайта-источника на сайте-адресате.
Тиражировать шаблоны документа	Тиражирует все объекты, не являющиеся экземплярами (выполняющиеся локально или отчеты, отмеченные для удаленного планирования). Учитываются пользователи, группы, папки, отчеты и так далее.
Тиражировать выполняемые локально завершенные экземпляры	Тиражирует завершенные экземпляры только с сайта-адресата на сайт-источник.

10. Нажмите кнопку **ОК**.

См. также

- [Управление очисткой объектов](#)
- [Управление обнаружением и разрешением конфликтов](#)
- [Удаленное планирование и экземпляры, выполняемые локально](#)

18.9.2 Планирование заданий тиражирования

После создания задания тиражирования можно запланировать его однократное или периодическое выполнение. Можно также запланировать несколько заданий тиражирования на одном сайте-адресате из одного сайта-источника.

Примечание:

Если несколько заданий тиражирования планируются на одном сайте-адресате, одновременно только одно задание тиражирования может подключаться к сайту-источнику. Все остальные задания тиражирования, пытающиеся подключиться, будут переведены в состояние ожидания, которое будет сохраняться, пока не будет установлено автоматическое подключение к сайту-источнику.

18.9.2.1 Планирование задания тиражирования

1. Перейдите к области «Интеграция» консоли СМС.
2. Выберите **задание тиражирования**, которое необходимо запланировать.
3. Выберите **Действия > Расписания**.
4. Выберите необходимые параметры планирования.

18.9.3 Изменение заданий тиражирования

После создания задания тиражирования в модуле "Интеграция" можно изменить его свойства.

18.9.3.1 Изменение задания тиражирования

1. Перейдите к области «Интеграция» консоли СМС.
2. Выберите папку **Удаленные соединения**.
3. Выберите объект **Удаленное соединение**, содержащий **задание тиражирования**, которое необходимо изменить.
4. Выберите **задание тиражирования**, которое необходимо изменить.
5. Выберите **Управление > Управление свойствами объектов**.
6. Просмотрите и при необходимости измените значения параметров **Свойства, Планирование, Журнал, Список тиражирования и Безопасность пользователей**.

Секции	Описание
Свойства	Изменение имени, описания и других общих свойств и параметров задания тиражирования.
Планирование	Настройка периодического повторения выполнения задания тиражирования.
Журнал	Просмотр и администрирование всех экземпляров задания тиражирования.
Список тиражирования	Изменение выбранного списка тиражирования.
Безопасность пользователя	Настройка прав для задания тиражирования.

18.9.4 Просмотр журнала после выполнения задания тиражирования

При каждом выполнении задания тиражирования модуль "Интеграция" на сайте-адресате создает файл журнала. Для файлов журналов используется стандарт XML 1.1, поэтому требуется веб-браузер с поддержкой XML 1.1.

Просмотр журнала тиражирования:

1. Перейдите к области «Интеграция» консоли СМС.
2. Щелкните **Все задания на тиражирование**.
3. Выберите **Задание тиражирования** из списка.
4. Нажмите кнопку **Свойства**.
Откроется страница «Свойства» задания тиражирования.
5. Нажмите кнопку **Журнал**.
6. Выберите **Время создания экземпляра** в файле журнала для просмотра успешно выполненных заданий тиражирования или состояние **Сбой** для просмотра файла журнала заданий тиражирования, выполненных неудачно.
7. Выберите необходимый экземпляр для просмотра файла журнала.
Файл журнала создается в формате XML, в нем используется форма XSL для форматирования данных на странице HTML.

Доступ к журналу XML можно получить на компьютере, на котором запущен Server Intelligence Agent, содержащий адаптивный сервер заданий. Файл журнала находится в следующем каталоге:

- Windows:<InstallDir>\SAP BusinessObjects XI 4.0\logging
- Unix:<InstallDir>/sap_bobj/logging

18.10 Управление очисткой объектов

В модуле "Интеграция" очистку объектов следует выполнять в течение жизненного цикла процесса тиражирования, чтобы убедиться, что все объекты, удаленные с сайта-источника, также удалены с каждого сайта-адресата.

В очистке объектов задействованы два элемента: удаленное соединение и задание тиражирования. В объекте удаленного соединения определяются общие параметры очистки, а задание тиражирования выполняет очистку по истечении соответствующего интервала времени.

18.10.1 Способ использования очистки объектов

Отдельные задания тиражирования, в которых используется такое же удаленное соединение, выполняют совместную работу в процессе очистки объектов. Это означает, что задание тиражирования очищает объекты в своем списке тиражирования, а также объекты в других списках тиражирования, использующих такое же удаленное соединение. Удаленное соединение считается одинаковым только в том случае, если родительским объектом задания тиражирования является такой же объект удаленного соединения.

Пример:

Задания тиражирования А и Б тиражируют объект А и объект Б. Они выполняют тиражирование с одного сайта-источника и используют одно удаленное соединение. Если объект Б удаляется на сайте-источнике, в задание тиражирования А передается информация о том, что объект Б удален. Несмотря на то, что задание тиражирования Б заменяет этот объект, объект Б также удаляется с сайта-адресата. При выполнении задания тиражирования Б отсутствует необходимость запуска очистки объектов.

Примечание:

Во время очистки объектов удаляются только объекты на сайте-адресате. При удалении объекта с сайта-источника, являющегося частью тиражирования, объект удаляется с сайта-адресата. Однако если объект удаляется с сайта-адресата, удаление с сайта-источника в процессе очистки объектов не выполняется, даже если задание тиражирования выполняется в режиме двунаправленного тиражирования.

Объекты, удаляемые или очищаемые из списка тиражирования, не удаляются с сайта-адресата. Для правильного удаления объекта, который задан в списке тиражирования, следует удалить его как на сайте-адресате, так и на сайте-источнике. Объекты, которые тиражируются посредством вычисления зависимостей, не удаляются.

18.10.2 Ограничения очистки объектов

В объекте удаленного соединения можно указать число объектов, которые будут одновременно очищаться при выполнении задания тиражирования. В модуле "Интеграция" автоматически отслеживается место завершения выполнения задания очистки. Поэтому при следующем выполнении задания тиражирования оно запускает следующее задание очистки в этой точке.

Совет:

Для более быстрого выполнения задания тиражирования задайте ограничение числа объектов для очистки.

Пример:

Задания тиражирования А и Б тиражируют объект А и объект Б. Оба объекта тиражируются с одного сайта-источника и используют одно удаленное соединение.

Если объект Б удаляется на сайте-источнике, и для ограничения объектов задано значение 1, при следующем запуске задания тиражирования А будет выполняться только проверка того, был ли удален объект А. При этом объект Б не проверяется и не удаляется.

Затем выполняется задание тиражирования Б и запуск процесса очистки объектов в той точке, в которой было завершено выполнение задания тиражирования А. Будет проверено, был ли объект Б удален и очищен с сайта-адресата. Этот параметр находится в свойстве объекта удаленного соединения «Ограничить число объектов очистки до».

Примечание:

Если этот параметр не выбран, во всех заданиях тиражирования, использующих данное удаленное соединение, будут проверяться все объекты для выявления необходимости выполнения очистки.

18.10.3 Частота очистки объектов

В поле «Частота очистки» можно настроить частоту выполнения очистки объектов во время задания тиражирования при удаленном соединении.

Примечание:

Необходимо ввести целое положительное число, которое будет представлять время ожидания в часах между выполнением очистки объектов.

Пример:

Задания тиражирования А и Б тиражируют объект А и объект Б. Оба объекта тиражируются с одного сайта-источника и используют одно удаленное соединение.

Если объект Б с сайта-источника и все следующие условия верны, задание тиражирования проверит, был ли удален объект А.

- Ограничение объекта – 1
- Частота очистки – 150 часов
- Затем выполняется задание тиражирования А

Поскольку ограничение объекта – 1, объект Б не проверяется и не удаляется на сайте-адресате.

Следующая очистка выполняется через 150 часов после первоначальной проверки заданием тиражирования А. Несмотря на то, что задания тиражирования А и Б могут выполняться много раз в течение 150 часов, при их выполнении очистка объектов запускаться не будет. По истечении 150 часов при выполнении следующего задания тиражирования будет предпринята попытка очистки. После этого определяется, что объект Б был удален на сайте-источнике, в результате чего этот объект удаляется и на сайте-адресате.

Включение и выключение параметров

Каждое задание тиражирования может быть задействовано в процессе очистки объектов. Используйте параметр «Включить очистку объектов для места назначения» в задании тиражирования, чтобы указать необходимость выполнения очистки объектов. В некоторых случаях при наличии заданий тиражирования с высоким приоритетом может потребоваться исключение участия заданий в процессе очистки объектов, чтобы они выполнялись как можно быстрее. Для этого отключите очистку объектов.

См. также

- [Ограничения очистки объектов](#)

18.11 Управление обнаружением и разрешением конфликтов

В модуле "Интеграция" может возникнуть конфликт, когда свойства объекта одновременно изменяются на сайте-источнике и сайте-адресате. Верхний уровень и вложенные свойства объекта проверяются на наличие конфликтов. Например, конфликт может возникнуть, если отчет или название отчета изменяются и на сайте-источнике и на сайте-адресате.

В некоторых экземплярах конфликты не возникают. Например, если название отчета изменяется на сайте-источнике, а описание тиражированной версии изменяется на сайте-адресате, изменения объединяются, и конфликт не возникает.

18.11.1 Разрешение конфликтов однонаправленного тиражирования

При однонаправленном тиражировании предусмотрены два варианта разрешения конфликтов.

Сайт-источник имеет приоритет

Если конфликт возникает при однонаправленном тиражировании, объект сайта-источника имеет приоритет. Любые изменения объектов на сайте-адресате перезаписываются данными с сайта-источника. Например, если отчет изменен и на сайте-источнике, и на сайте-адресате, изменение сайта-адресата будет перезаписано версией сайта-источника после следующего задания тиражирования.

Примечание:

Поскольку конфликт разрешается автоматически, запись в файле журнала не создается и не отображается в списке конфликтующих объектов.

Отсутствует автоматическое разрешение конфликтов

Если возникает конфликт и выбран параметр «Без автоматического разрешения конфликтов», конфликт не разрешается, файл журнала не создается и запись не отображается в списке конфликтующих объектов.

Администратор может получить доступ к списку всех тиражированных объектов, конфликтующих в области интеграции консоли СМС. Конфликтующие объекты группируются на основе удаленного соединения с сайтом-источником. Для получения доступа к этому списку в области "Интеграция" консоли СМС перейдите в папку "Ошибки тиражирования" и выберите необходимое удаленное соединение. Все тиражированные объекты на сайте-адресате будут отмечены значком тиражирования. При наличии конфликта объекты отмечаются значком конфликта. Сообщение с предупреждением также появляется на странице «Свойства».

Примечание:

- Этот список обновляется после завершения выполнения задания тиражирования, использующего удаленное соединение. В нем содержатся все конфликтующие объекты для всех заданий тиражирования, в которых используется данное удаленное соединение.
- Любой пользователь, который имеет доступ к консоли СМС и экземплярам задания тиражирования, может получить доступ к файлу XML, записываемому в каталог файла журнала. Значок объекта сайта-адресата отмечается для обозначения конфликта. Во время обработки создается журнал конфликтов.

Александр изменяет отчет А на сайте-источнике. Мария изменяет тиражированную версию на сайте-адресате. При следующем выполнении задания тиражирования возникает конфликт отчета, поскольку отчет был изменен на обоих сайтах, и разрешение конфликта не выполняется.

Отчет на сайте-адресате сохраняется, а изменения отчета на сайте-источнике не тиражируются. Последующие задания тиражирования выполняются аналогичным образом, пока конфликт не будет разрешен. Любые изменения на сайте-источнике не тиражируются, пока конфликт не будет разрешен вручную.

Примечание:

В этом случае тиражирование всего объекта не выполняется. Другие изменения, не являющиеся причиной возникновения конфликта, не переносятся.

Разрешить конфликт вручную можно тремя способами:

1. Создание задания тиражирования, в котором выполняется тиражирование только конфликтующих объектов. В нем необходимо использовать такой же объект удаленного соединения и список тиражирования.

Для сохранения изменений сайта-источника создайте задание тиражирования. Затем задайте для режима тиражирования значение «Обновлять из источника», а для автоматического разрешения конфликтов установите значение «Сайт-источник имеет приоритет».

Для сохранения изменений на сайте-адресате создайте задание тиражирования с типом тиражирования = «Двунаправленное тиражирование», режимом тиражирования = «Обновлять из адресата» и автоматическим разрешением конфликтов = «Сайт-адресат имеет приоритет»

Примечание:

В режиме тиражирования задайте параметр «Обновлять из источника» или «Обновлять из адресата», чтобы выбрать в списке тиражирования только конфликтующие объекты. При этом тиражирование других объектов не выполняется. Затем запланируйте выполнение задания тиражирования с указанием тиражирования выбранных объектов и разрешением конфликтов.

2. Создание задания тиражирования, в котором выполняется тиражирование только конфликтующих объектов. В нем необходимо использовать такой же объект удаленного соединения. В отличие от первого варианта, здесь новый список тиражирования можно создать на сайте-источнике. Используйте только конфликтующие объекты и создайте новое задание тиражирования, в котором будет использоваться заданный список тиражирования.

Для сохранения изменений на сайте-источнике задайте для автоматического разрешения конфликтов значение «Сайт-источник имеет приоритет».

Для сохранения изменений сайте-адресате задайте для автоматического разрешения конфликтов значение «Сайт-адресат имеет приоритет», а для типа тиражирования – «Двунаправленное тиражирование».

3. При выполнении заданий однонаправленного тиражирования можно только удалять объекты на сайте-адресате. При следующем выполнении задания тиражирования объекты сайта-источника тиражируются на сайт-адресат.

Примечание:

Будьте осторожны при удалении объекта, поскольку другие зависимые объекты могут быть удалены, перестать работать или утратить безопасность. Рекомендуется использовать варианты 1 и 2.

18.11.2 Разрешение конфликта двунаправленного тиражирования

При возникновении конфликта двунаправленного тиражирования предусмотрены три варианта обнаружения конфликта:

- Сайт-источник имеет приоритет
- Сайт-адресат имеет приоритет
- Отсутствует автоматическое разрешение конфликтов

Сайт-источник имеет приоритет

При возникновении конфликта сайт-источник имеет приоритет и выполняется перезапись всех изменений на сайте-адресате.

Пример:

Елена изменяет название отчета на "Отчет А". Михаил изменяет тиражированную версию на сайте-адресате на "Отчет Б". После выполнения следующего задания тиражирования для тиражированной версии на сайте-адресате будет возвращено название "Отчет А".

При этом запись конфликта не будет создана в файле журнала и не появится в списке конфликтующих объектов, поскольку конфликт был разрешен на сайте-источнике в соответствии с инструкциями пользователя.

Сайт-адресат имеет приоритет

При возникновении конфликта изменения сайта-адресата сохраняются и перезаписывают изменения на сайте-источнике.

Пример:

Николай изменяет название отчета на "Отчет А". Петр изменяет название тиражированной версии на сайте-адресате на "Отчет Б". Конфликт возникает при выполнении задания тиражирования. Название отчета на сайте-адресате сохраняется как "Отчет Б".

При двунаправленном тиражировании изменения также пересылаются обратно на сайт-источник. В этом сценарии сайт-источник обновляется, и название отчета изменяется на "Отчет Б". При этом запись о конфликте не создается в файле журнала и не отображается в списке конфликтующих объектов, поскольку конфликт был разрешен в соответствии с инструкциями пользователя.

Отсутствует автоматическое разрешение конфликтов

Если выбран параметр «Без автоматического разрешения конфликтов», разрешение конфликта не выполняется. Запись о конфликте будет сделана в файле журнала для администратора, который может разрешить конфликт вручную.

Примечание:

- Значок объекта отмечается для обозначения существования конфликта.
- Несмотря на то, что при двунаправленном тиражировании изменения тиражируются как на сайте-источнике, так и на сайте-адресате, только версии сайта-адресата будут отмечены значком конфликта.

Примечание:

Любой пользователь, который имеет доступ к консоли СМС и экземплярам задания тиражирования, может получить доступ к журналу XML, записываемому в каталог файла журнала. Значок объекта сайта-адресата отмечается для обозначения конфликта. Во время обработки создается журнал конфликтов.

Администратор может получить доступ к списку всех тиражированных объектов, конфликтующих в области интеграции консоли СМС. Конфликтующие объекты группируются на основе удаленного соединения с сайтом-источником. Для получения доступа к этим спискам перейдите к пункту **СМС > Интеграция > Ошибки тиражирования > Удаленное соединение**.

Примечание:

Этот список обновляется после завершения выполнения задания тиражирования, использующего удаленное соединение. В нем содержатся все конфликтующие объекты для всех заданий тиражирования, в которых используется данное удаленное соединение. Все тиражированные объекты на сайте-адресате будут отмечены значком тиражирования. При наличии конфликта объекты отмечаются значком конфликта.

Пример:

Михаил изменяет отчет А на сайте-источнике. Дмитрий изменяет тиражированную версию на сайте-адресате. При выполнении следующего задания тиражирования возникает конфликт отчета, поскольку отчет был изменен на обоих сайтах, и разрешение конфликта не выполняется.

Отчет на сайте-адресате сохраняется, а изменения отчета на сайте-источнике не тиражируются. Последующие задания тиражирования выполняются аналогичным образом, пока конфликт не будет разрешен. Тиражирование любых изменений на сайте-источнике выполняться не будет, пока конфликт не разрешен вручную администратором или делегированным администратором.

Примечание:

- В этом случае тиражирование всего объекта не выполняется. Другие изменения, не являющиеся причиной возникновения конфликта, не тиражируются.
- Любой пользователь, который имеет доступ к консоли СМС и экземплярам задания тиражирования, может получить доступ к журналу XML, записываемому в каталог файла журнала. Значок объекта сайта-адресата отмечается для обозначения конфликта. Во время обработки создается журнал конфликтов.

Администратор может получить доступ к списку всех тиражированных объектов, конфликтующих в области интеграции консоли СМС. Конфликтующие объекты группируются на основе удаленного соединения с сайтом-источником. Для получения доступа к этим спискам перейдите к пункту **СМС > Интеграция > Ошибки тиражирования > Удаленное соединение**.

Примечание:

Этот список обновляется после завершения выполнения задания тиражирования, использующего удаленное соединение. В нем содержатся все конфликтующие объекты для всех заданий тиражирования, в которых используется данное удаленное соединение. Все тиражированные объекты на сайте-адресате будут отмечены значком тиражирования. При наличии конфликта объекты отмечаются значком конфликта.

Разрешить конфликт вручную можно тремя способами:

1. Создание задания тиражирования, в котором выполняется тиражирование только конфликтующих объектов. В нем необходимо использовать такой же объект удаленного соединения и список тиражирования.

Для сохранения изменений сайта-источника создайте задание тиражирования. Затем задайте для режима тиражирования значение «Обновлять из источника», а для автоматического разрешения конфликтов настройте значение «Сайт-источник имеет приоритет».

Для сохранения изменений на сайте-адресате создайте задание тиражирования с типом тиражирования «Двунаправленное тиражирование», задайте для режима тиражирования значение «Обновлять из адресата», а для автоматического разрешения конфликтов значение «Сайт-адресат имеет приоритет».

Примечание:

В режиме тиражирования задайте параметр «Обновлять из источника» или «Обновлять из адресата», чтобы выбрать в списке тиражирования только конфликтующие объекты. При этом тиражирование других объектов не выполняется. Затем запланируйте выполнение задания тиражирования с указанием тиражирования выбранных объектов и разрешением конфликтов.

2. Создание задания тиражирования, в котором выполняется тиражирование только конфликтующих объектов. В нем необходимо использовать такой же объект удаленного соединения. Тем не менее, в отличие от первого варианта, здесь новый список тиражирования можно создать на сайте-источнике. Используйте только конфликтующие объекты и создайте новое задание тиражирования, в котором будет использоваться заданный список тиражирования.

Для сохранения изменений на сайте-источнике задайте для автоматического разрешения конфликтов значение: «Сайт-источник имеет приоритет».

Для сохранения изменений сайта-адресата задайте для автоматического разрешения конфликтов значение «Сайт-адресат имеет приоритет», а для типа тиражирования – «Двунаправленное тиражирование».

3. Удалите объект, который больше не должен находится на сайте.

Примечание:

Будьте осторожны при удалении объекта, поскольку другие зависимые объекты могут быть удалены, перестать работать или утратить безопасность. Рекомендуется использовать варианты 1 и 2.

Для сохранения изменений на сайте-адресате можно удалить объект на сайте-источнике. При следующем выполнении задания тиражирования объекты сайта-адресата тиражируются на сайт-источник.

Примечание:

Будьте осторожны при удалении копий на сайте-источнике, поскольку на других сайтах-адресатах, тиражирующих этот объект, задание тиражирования может выполняться перед обратным тиражированием копии. Это может стать причиной удаления копии на других сайтах-адресатах, так как копия будет недоступна, пока она не возвращена.

Для сохранения изменений на сайте-источнике можно удалить объект на сайте-адресате.

18.12 Использование веб-служб в модуле "Интеграция"

В модуле "Интеграция" веб-службы используются для передачи объектов и их изменений между сайтом-источником и сайтом-адресатом. Веб-службы модуля "Интеграция" автоматически устанавливаются и развертываются в платформе BI. Однако может потребоваться изменение свойств или настройка внедрений в веб-службах для расширения функциональных возможностей, как описано в этом разделе.

Совет:

Чтобы улучшить управления файлами и повысить функциональность, включите кэширование файлов в модуле "Интеграция".

18.12.1 Переменные сеанса

Если в одном задании тиражирования передается большое число файлов содержимого, может потребоваться увеличение времени ожидания сеанса веб-служб в модуле "Интеграция".

Это свойство находится в файле `dsws.properties`:

<Каталог установки сервера приложений>\dswsbobje\Web-INF\classes

Например:

`C:\Program Files\SAP BusinessObjects\Tomcat6\webapps\dswsbobje\WEB-INF\classes`

Для активации переменной сеанса введите:

`session.timeout = x`

Где «x» - необходимое время, «x» измеряется в секундах. Если значение не указано, по умолчанию используется 1200 секунд или 20 минут.

18.12.2 Кэширование файлов

Кэширование файлов позволяет веб-службам обрабатывать большие вложения без их буферизации в памяти. Если оно не включено, при передаче файлов больших размеров может использоваться вся память виртуальной машины Java и произойти сбой тиражирования.

Примечание:

При кэшировании файлов производительность падает, поскольку веб-службы осуществляют обработку в файлах, а не в памяти. Можно использовать комбинацию обоих параметров и передавать большие объемы в файл, а небольшие в память.

Для включения кэширования файлов измените файл `Axis2.xml`, расположенный в каталоге:

<Каталог установки сервера приложений>\dswsbobje\Web-Inf\conf

Например:

C:\Program Files\SAP BusinessObjects\Tomcat6\webapps\dswsbobje\WEB-INF\conf

Укажите следующее:

`<parameter name="cacheAttachments" locked="false">true</parameter>`

`<parameter name="attachmentDIR" locked="false">temp directory</parameter>`

`<parameter name="sizeThreshold" locked="false">4000</parameter>`

Примечание:

Пороговое значение измеряется в байтах.

18.12.3 Настраиваемое развертывание

Веб-службы модуля "Интеграция" можно развернуть автоматически, необходимо включить службы «federation», «biplatform» и «session». Чтобы отключить модуль "Интеграция" или любую другую веб-службу, измените соответствующий файл веб-служб `service.xml`.

Веб-службы платформы BI находятся в каталоге:

<Каталог установки сервера приложений>\dswsbobje\WEB-INF\services

Пример:

C:\Program Files\SAP BusinessObjects\Tomcat6\webapps\dswsbobje\WEB-INF\services

Отключение веб-служб:

- Добавьте свойство «activate» в тег имени службы в файл `service.xml` и задайте для него значение `false`.
- Перезапустите сервер Java-приложений.

Например, для блокировки функции объединения:

Файл `services.xml` находится в каталоге:

C:\Program Files\Business Objects\Tomcat55\webapps\dswsbobje\WEB-INF\services\federator\META-INF

Измените имя службы:

```
<service name="Federator">
```

До:

```
<service name="Federator" activate="false">
```

18.13 Удаленное планирование и экземпляры, выполняемые локально

В этом разделе приводятся подробные сведения об удаленном планировании, выполняемых локально экземплярах, а также совместном использовании экземпляров. Эти функции позволяют выполнять отчет в том месте, где находятся данные, и отправлять выполненные экземпляры в соответствующее местонахождение.

18.13.1 Удаленное планирование

При использовании модуля "Интеграция" можно запланировать отчет на сайте-адресате, а затем обработать его на сайте-источнике. Выполненные экземпляры будут возвращены на сайт-адресат.

Чтобы включить удаленное планирование, запланируйте отчет, используя обычную процедуру, и включите параметр «Выполнять на сайте-источнике». Чтобы включить этот параметр, выберите **Расписание > Планирование серверной группы > Выполнять на сайте-источнике**. После создания запланированных экземпляров, они переводятся в состояние ожидания.

Во время удаленного планирования информация, переданная на сайт-адресат, игнорируется, и экземпляр отчета остается в состоянии ожидания.

Если в следующем задании тиражирования, управляющем отчетом, включено удаленное планирование, выполняется копирование экземпляра на сайт-источник для обработки. Экземпляр остается в состоянии ожидания, пока он не будет обработан планировщиком. Тем временем задание тиражирования, отправившее экземпляр, возвратит все ранее выполненные экземпляры и изменения объекта.

После обработки экземпляра на сайте-источнике он переводится в выполненное состояние. Если в следующем задании тиражирования, управляющем отчетом, включено удаленное планирование, выполненный экземпляр используется для обновления копии на сайте-адресате. После обновления экземпляра на сайте-адресате является выполненным.

Примечание:

Задание тиражирования должно выполняться дважды для возвращения одного выполненного экземпляра.

Пример:

1. Антон составляет расписание отчета А для удаленного планирования.
2. Отчет А создан на сайте-адресате и переводится в состояние ожидания.
3. Выполняется задание тиражирования А. Сначала происходит тиражирование изменений с сайта-источника на сайт-адресат (включая ранее выполненные экземпляры). Затем на сайт-источник копируется экземпляр в состоянии ожидания, а также изменения, подлежащие тиражированию с сайта-адресата на сайт-источник.
4. На сайте-источнике планировщик выбирает экземпляр в состоянии ожидания и пересылает его на соответствующий сервер заданий для обработки. После этого экземпляр обрабатывается и переводится в выполненное состояние на сайте-источнике.
5. Задание тиражирования А выполняется повторно. Когда задание выполняет тиражирование содержимого с сайта-источника на сайт-адресат, выбирается выполненный экземпляр отчета А и изменения применяются к версии на сайте-адресате.
6. После завершения задания версия на сайте-адресате закончена.

Удаленное планирование работает только с двунаправленным заданием тиражирования. Необходимо включить параметр «Тиражировать удаленные расписания». Этот параметр находится на странице «Свойства задания тиражирования» в области «Фильтры тиражирования». В некоторых сценариях может потребоваться более частое тиражирование удаленно запланированных заданий, чем других объектов в списке тиражирования. Для этого создайте два задания тиражирования. Включите параметр «Тиражировать удаленные расписания» для одного задания тиражирования, которое выполняет только удаленное планирование. Включите для другого задания параметр «Тиражировать шаблоны документа» или «Тиражировать все объекты (без фильтра)».

Примечание:

При включении удаленного планирования выполненные и незавершенные экземпляры появляются как на сайте-источнике, так и на сайте-адресате.

Если пользователь составляет расписание отчета для удаленного планирования на сайте-адресате, но данный пользователь не существует на сайте-источнике, произойдет сбой выполнения экземпляра на сайте-источнике. В качестве владельца незавершенного экземпляра будет указана учетная запись пользователя объекта удаленного соединения, используемого для подключения к сайту-источнику.

В задании тиражирования можно настроить только удаленное планирование, при этом оно всегда выполняет тиражирование предшествующих объектов экземпляра отчета. Это означает, что, если между операциями по тиражированию вносятся изменения, выполняется тиражирование фактического отчета, папки отчета и т. д. Если тиражирование этих изменений с сайта-адресата на сайт-источник не требуется, можно использовать права безопасности для выбора тиражируемых изменений.

См. также

- [Управление правами безопасности](#)

18.13.2 Экземпляры, выполняемые локально

Экземпляры, выполняемые локально, – это экземпляры отчета, которые обрабатываются из отчетов на сайте-адресате. При использовании модуля "Интеграция" можно тиражировать выполненные экземпляры с сайта-адресата на сайт-источник.

Чтобы включить в задании тиражирования тиражирование выполненных и незавершенных экземпляров с сайта-адресата на сайт-источник, выберите **Свойства задания тиражирования > Фильтры тиражирования > Тиражировать выполняемые локально завершенные экземпляры**.

В некоторых случаях может потребоваться выполнение задания тиражирования только тиражированных экземпляров, выполняемых локально. Для этого включите параметр «Тиражировать выполняемые локально завершенные экземпляры».

Примечание:

При включении экземпляров, выполняемых локально, в задании тиражирования как выполненные, так и незавершенные экземпляры тиражируются на сайт-источник. Это означает, что копии будут созданы как на сайте-источнике, так и на сайте-адресате.

Тиражирование экземпляров в состоянии ожидания не выполняется.

Если владелец локально выполняемых экземпляров не существует на сайте-источнике, в качестве владельца будет указана учетная запись пользователя, используемая для подключения в объекте удаленного соединения.

18.13.3 Совместное использование экземпляров

При включении в задание тиражирования удаленного планирования и экземпляров, выполняемых локально, совместное использование экземпляра возникает, если один сайт-источник с несколькими сайтами-адресатами тиражируют один отчет.

Пример:

Отчет А создан на сайте-источнике, а сайты-адресаты А и Б тиражируют его. Совместное использование экземпляров осуществляется на обоих сайтах-адресатах:

- Включите для заданий тиражирования параметр «Тиражировать удаленные расписания» и/или «Тиражировать выполняемые локально завершенные экземпляры». Выполните тиражирование отчета А в том же задании тиражирования, как было указано выше
- Выполните планирование отчета А на сайте-адресате с параметром «Выполнять на сайте-источнике» и/или локальным выполнением

Если оба сайта-адресата А и Б тиражируют отчет А и соответствующие задания тиражирования тиражируют удаленные расписания и/или экземпляры, выполняемые локально, то любые экземпляры, обработанные на сайте-адресате и/или сайте-источнике в пользу сайта-адресата А, будут совместно использоваться с сайтом-адресатом Б.

Аналогично, любые экземпляры, обработанные на сайте-адресате Б и/или сайте-источнике, будут также совместно использоваться с сайтом-адресатом А. Наконец, на сайте-источнике и сайтах-адресатах А и Б будет существовать идентичный набор экземпляров.

Совместное использование экземпляров идеально подходит во многих случаях. Например, когда пользователям на других сайтах необходимо получить данные из систем, принадлежащих одной группе. В этом случае для предотвращения просмотра экземпляров пользователями на локальном сайте убедитесь, что настроены подходящие права безопасности. Например, в объекте отчета примените права, чтобы пользователи могли просматривать только собственные экземпляры.

Примечание:

Во всех объектах выполняются правила безопасности платформы BI. Чтобы убедиться, что пользователи и группы могут просматривать только подходящие экземпляры, рекомендуется настраивать права таким образом, чтобы пользователи могли просматривать только собственные экземпляры. Например, в объекте отчета примените права, чтобы пользователи могли просматривать только собственные экземпляры.

См. также

- [Управление правами безопасности](#)

18.14 Импорт и перенос тиражированного содержимого

В некоторых случаях можно выбрать импорт или перенос тиражированного содержимого из одной системы платформы BI в другую. В этом разделе приводится описание данных функций в модуле "Интеграция".

18.14.1 Импорт тиражированного содержимого

Если для импорта содержимого из одной платформы BI в другую используется LifeCycle Manager, импорт данных, относящихся к тиражированию и связанных с импортируемыми тиражированными объектами, не выполняется. Это означает, что после импорта поведение объектов аналогично их поведению до тиражирования. Этот пример относится к тиражированным объектам на сайте-адресате, его описание приводится в следующем сценарии.

Пример:

Платформа BI A – это сайт-адресат в процессе "Интеграция". Отчет A, тиражированный отчет в системе A, импортируется из системы A в систему B платформы BI с помощью LifeCycle Manager.

Результат. После копирования отчета A в систему B платформы BI в нем не содержатся тиражированные данные. Отчет A больше не отмечен значком тиражирования. Если объект находился в состоянии конфликта в системе A платформы BI, состояние конфликта будет отсутствовать в системе B. Фактически объект воспринимается как объект, созданный в системе B.

Примечание:

Идентификатор CUID может различаться в зависимости от параметров импорта, настроенных в LifeCycle Manager.

18.14.2 Импорт тиражированного содержимого и продолжение тиражирования

После импорта тиражированного содержимого может потребоваться включение импортированных объектов в процесс интегрирования. Существует две ситуации: рассмотрение системы, в которой находятся импортированные объекты, в качестве сайта-источника, или рассмотрение этой системы в качестве сайта-адресата. Чтобы использовать систему в качестве сайта-источника, используйте модуль "Интеграция" как обычно.

Чтобы использовать систему в качестве сайта-адресата и выполнить тиражирование импортированных объектов с сайта-источника, выполните следующие действия:

- При использовании LifeCycle Manager убедитесь, что идентификатор CUID объектов сохраняется.
- Убедитесь, что в первом задании тиражирования для разрешения конфликтов задано значение «Сайт-источник имеет приоритет» или «Сайт-адресат имеет приоритет».

Совет:

Вместо импорта объекта с одного сайта-адресата на другой с помощью LifeCycle Manager более эффективным и настоятельно рекомендуемым способом является использование модуля "Интеграция" для тиражирования объекта.

Пример:

Отчет A был создан в системе A платформы BI. В системе X модуль "Интеграция" использовался для тиражирования отчета A из системы A в систему X. Затем LifeCycle Manager использовался для импорта отчета A из системы X в систему Y.

План. В системе Y необходимо настроить модуль "Интеграция" для использования в системе A и сохранить отчет A в качестве части задания тиражирования. Система Y является адресатом, а система A – источником.

Действия. Во время импорта отчета А из системы Х в систему Y необходимо сохранить идентификатор CUID отчета А. Кроме того, при выполнении первого задания тиражирования будет предпринята попытка тиражирования отчета А. Поскольку объект уже существует в системе Y, во время тиражирования возникнет конфликт. Чтобы указать версию, которую необходимо использовать, для режима разрешения конфликтов задайте значение «Сайт-источник имеет приоритет» или «Сайт-адресат имеет приоритет».

Примечание:

В этом примере вместо импорта объекта с одного сайта-адресата на другой с помощью LifeCycle Manager рекомендуется использовать модуль "Интеграция" для тиражирования объекта. Тиражирование отчета А будет выполнено из системы А в систему Y, и не будет необходимости использования LifeCycle Manager для импорта объекта из системы Х в систему Y.

18.14.3 Перенос содержимого из тестовой среды

В любой организации проверка часто выполняется перед размещением любого компонента в среду производства. Обычно перед настройкой модуля "Интеграция" на производственных компьютерах выполняется его тестирование в системах платформы BI в среде разработки или тестирования. После создания сайта-источника и сайта-адресата, а также содержимого в среде тестирования эту систему можно перенести на производственные компьютеры, выполнив следующие шаги:

1. Используйте LifeCycle Manager для переноса содержимого с сайта-источника в среде тестирования на компьютер в среде производства, который будет выступать в роли сайта-источника.

Примечание:

При использовании LifeCycle Manager объект списка тиражирования выбрать нельзя.

2. Создайте список тиражирования на сайте-источнике в среде производства и включите необходимое содержимое.
3. Выберите один из двух следующих вариантов:
 - А) Создание объекта удаленного подключения и соответствующих заданий тиражирования на производственных компьютерах в среде производства, которые будут выступать в роли сайтов-адресатов.
 - Б) Использование LifeCycle Manager для импорта удаленного подключения и заданий тиражирования с сайта-адресата в среде Dev/QA на производственные компьютеры, которые будут выступать в роли сайтов-адресатов. Затем измените импортированные удаленные подключения, чтобы они указывали на компьютер в среде производства, который будет выступать в роли сайта-источника.

18.14.4 Повторное назначение сайта-адресата

В текущей версии после тиражирования объекта из исходного сайта он всегда должен тиражироваться именно оттуда. Попытки изменить объект удаленного соединения, чтобы он указывал на новую систему (платформу BI), приведут к сбою тиражирования. Чтобы выполнить тиражирование с другого сайта-источника, сначала удалите сайт-адресат.

Примечание:

После копирования тиражированного объекта идентификатор CUID копии изменяется, и в копии будет отсутствовать какая-либо информация о тиражировании.

18.15 Оптимальные методы работы

С помощью федерации можно оптимизировать производительность задания тиражирования.

Если отдельное задание тиражирования содержит большое число объектов, можно выполнить дополнительные действия, позволяющие гарантировать его успешное выполнение. Обычно в каждом задании тиражирования можно выполнить тиражирование до 32 000 объектов. Однако в некоторых системах может потребоваться настройка уменьшения или увеличения размеров тиражирования.

1) Получение выделенного поставщика веб-служб

В модуле интеграции тиражированное содержимое пересылается посредством веб-служб. При установке платформы BI по умолчанию для всех веб-служб используется один поставщик веб-служб. Выполнение крупных заданий тиражирования может повлечь за собой продолжительное снижение производительности поставщика веб-службы и увеличить время его ответа на запросы других веб-служб и обслуживаемых им приложений.

Если планируется одновременное тиражирование большого числа объектов или последовательное выполнение нескольких заданий тиражирования, можно рассмотреть возможность развертывания веб-служб интеграции на собственном сервере Java-приложений с использованием выделенного поставщика веб-служб.

Для этого используйте программу установки платформы BI, чтобы установить веб-службы. Необходимо, чтобы сервер Java-приложений был запущен. В противном случае выберите вариант полной установки "Компоненты веб-яруса", чтобы установить веб-службы и Tomcat.

Примечание:

- Необходимо предоставить сведения для существующей системы CMS (например, имя хоста, порт и пароль администратора).
- В поле URI удаленного соединения необходимо указать новый URI поставщика веб-служб.

2) Увеличение объема доступной памяти сервера Java-приложений

Если в одном задании тиражирования выполняется тиражирование большого числа объектов, или сервер приложений одновременно используется другими приложениями, следует увеличить объем доступной памяти сервера Java-приложений.

Если выполнена установка платформы BI и сервера Tomcat, доступный объем памяти по умолчанию равен 1 ГБ. Увеличение доступного объема памяти для сервера Tomcat:

В ОС Windows:

1. Выберите **Пуск > Программы > Tomcat > Конфигурация Tomcat**.
2. Выберите **Java**.
3. В поле **Параметры Java** найдите строку `-Xmx1024M`
4. Увеличьте значение `-Xmx1024M` до необходимого размера.

Пример:

Чтобы увеличить объем памяти до 2 ГБ, введите: `-Xmx2048M`

В ОС Unix:

1. В каталоге `<BOE_Install_Dir>/setup/` откройте файл `env.sh` в необходимом текстовом редакторе. Увеличьте значение параметра `-Xmx1024m` до необходимого размера.
2. Найдите следующие строки

```
# 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. Увеличьте значение параметра `-Xmx1024m` до необходимого размера.

Пример:

Чтобы увеличить объем памяти до 2 ГБ, введите: `-Xmx2048m`

Совет:

Для получения сведений об увеличении объема памяти на других серверах Java-приложений см. документацию о сервере Java-приложений.

3) Уменьшение размера создаваемых файлов BIAR.

В модуле "Интеграция" веб-службы используются для тиражирования содержимого с сайта-источника на сайт-адресат. Для повышения эффективности переноса объекты группируются и сжимаются в файлы BIAR.

При тиражировании большого числа объектов настройте на сервере Java-приложений создание файлов BIAR меньшего размера. В модуле "Интеграция" выполняются упаковывание и сжатие

объектов в несколько файлов BIAR меньшего размера, поэтому число объектов, которые необходимо тиражировать, будет неограниченным.

Для уменьшения размера создаваемых файлов BIAR добавьте следующие параметры Java на сервере Java-приложений:

```
Dbobj.biar.suggestSplit
and
Dbobj.biar.forceSplit
```

Параметр `bobj.biar.suggestSplit`, в котором предлагается подходящий размер файла BIAR, который по возможности будет учитываться. Предлагаемое новое значение равно 90 МБ.

Параметр `bobj.biar.forceSplit` позволяет принудительно остановить создание файла BIAR по достижении заданного размера. Предлагаемое новое значение равно 100 МБ.

Примечание:

Изменять настройки размера файла BIAR по умолчанию следует только в том случае, если на сервере приложений недостаточно памяти и дальнейшее увеличение максимального размера кучи невозможно.

Для сервера Tomcat в ОС Windows:

1. Чтобы открыть средство **Конфигурация Tomcat**, выберите **Пуск > Программы > Tomcat > Конфигурация Tomcat**.
2. Выберите **Java**.
3. В поле **Параметры Java** в конец добавьте следующие строки:

```
-Dbobj.biar.suggestSplit=90
-Dbobj.biar.forceSplit=100
```

Для сервера Tomcat в системе Unix/Linux:

1. Откройте файл `env.sh` в необходимом текстовом редакторе. Файл находится в каталоге `<Каталог_установки_BOE>/setup/`
2. Найдите следующие строки:

```
# 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
```

Добавьте необходимые параметры размера файлов BIAR.

Пример: `JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m -Dbobj.biar.suggestSplit=90 -Dbobj.biar.forceSplit=100"`

Для добавления системных свойств на других серверах Java-приложений см. документацию.

- 4) Увеличьте время ожидания для сокета.

Адаптивный сервер заданий предназначен для выполнения заданий тиражирования. Во время выполнения задания тиражирования настраиваемый сервер заданий устанавливает соединение с сайтом-источником. При получении больших объемов данных с исходного сайта важно, чтобы

на сокете, который используется адаптивным сервером заданий для получения данных, не истекло время ожидания.

По умолчанию используется значение 90 минут. При необходимости можно увеличить время ожидания для сокета.

Увеличение времени ожидания для сокета на адаптивном сервере заданий:

1. Откройте Центральную консоль управления (СМС)
2. Перейдите к разделу **Сервер** и выберите **Адаптивный сервер заданий**.
3. Нажмите **Свойства**.
4. Добавьте «параметры командной строки» в конец следующей строки:
 - В системе Windows: `-javaArgs Xmx1000m,Xincgc,server,Dbobj.federation.WSTimeout=<время ожидания в минутах>`
 - В системе Unix: `-javaArgs Xmx512m,Dbobj.federation.WSTimeout=<время ожидания в минутах>`

См. также

- [Устранение неисправностей: сообщения об ошибках](#)
- [Использование веб-служб в модуле "Интеграция"](#)
- [Текущие ограничения выпуска](#)

18.15.1 Текущие ограничения выпуска

Модуль "Интеграция" является гибким инструментом, однако определенные ограничения могут влиять на производительность во время производства. В этом разделе описаны области, которые можно изменить для оптимизации операций модуля "Интеграция".

- Максимальное количество объектов

Каждое задание тиражирования выполняет тиражирование объектов между развертываниями платформы BI. Рекомендуется, чтобы количество объектов, тиражируемых в одном задании, не превышало 100 000. Несмотря на то, что задание тиражирования может выполняться с более, чем 100 000 объектами, в модуле "Интеграция" поддерживается тиражирование не более 100 000 объектов.

- Права

В модуле "Интеграция" права тиражируются только с сайта-источника на сайт-адресат. Пользовательские права, общие для обеих систем, рекомендуется настраивать на сайте-источнике и тиражировать на сайт-адресат с использованием двунаправленного тиражирования. Администрирование пользовательских прав на определенном сайте выполняется способом, принятым в платформе BI, установленной на сайте, на котором создан пользователь.

- Объекты Business Views и связанные объекты

В платформе BI могут храниться объекты Business View, бизнес-элементы, основания данных, соединения для передачи данных и списки значений (LOV). Эти объекты используются для расширения функциональных возможностей Crystal Reports.

Если эти объекты сначала создаются на сайте-адресате, а затем тиражируются на сайт-источник с использованием двунаправленного тиражирования, они могут работать неправильно, и их данные могут не отображаться в приложении Crystal Reports.

Рекомендуется создавать объекты Business View, бизнес-элементы, основания данных, соединения для передачи данных и списки значений (LOV) на сайте-источнике, а затем тиражировать их на сайт-адресат. При выполнении обновлений объектов на сайте-адресате или сайте-источнике (при наличии прав) изменения правильно тиражируются в обоих направлениях.

- Переопределения юниверсов

На платформе BI могут храниться переопределения юниверсов. Если переопределения юниверсов создаются на сайте-адресате, а затем тиражируются на сайт-источник с использованием двунаправленного тиражирования, они могут работать неправильно.

Чтобы избежать этого, сначала создайте переопределения юниверсов на сайте-источнике, а затем выполните их тиражирование на сайт-адресат. Затем задайте параметры безопасности в переопределениях юниверсов на сайте-источнике, а потом выполните их тиражирование на сайт-адресат.

- Очистка объектов

При очистке объектов выполняется удаление объектов, которые были удалены с сайта. Очистка объектов в настоящее время выполняется только с сайта-источника на сайте-адресате.

- Файлы журналов интеграции

Файлы журналов интеграции записываются в формате XML 1.1. Для просмотра файлов журналов в браузере последний должен поддерживать стандарт XML 1.1.

См. также

- [Управление очисткой объектов](#)

18.15.2 Устранение неисправностей: сообщения об ошибках

В этом разделе описаны сообщения об ошибках, которые появляются в редких случаях при использовании модуля "Интеграция". Эти сообщения отображаются в журналах заданий тиражирования или области функций отчета.

1) Недопустимый GUID

Пример ошибки: ERROR 2008-01-10T00:31:08.234Z GUID ASXOOFyvy0FJnRcD0dZNTZg (находится в свойстве SI_PARENT_CUID в объекте с номером 1285) является недопустимым GUID.

Эта ошибка означает, что выполняется тиражирование объекта, родительский элемент которого не тиражирован и еще не существует на сайте-адресате. Например, объект тиражируется без папки, в которой он содержится. Тиражирование родительского объекта невозможно, поскольку для учетной записи, под которой тиражируются объекты, не настроены подходящие права в родительском объекте.

2) Crystal Reports не отображают данные на сайте-источнике

Эта ошибка может возникнуть, если в отчете Crystal используется объект Business View, бизнес-элемент, основание данных, соединение для передачи данных или список значений (LOV), которые были изначально созданы на сайте-адресате, а затем тиражированы на сайт-источник.

3) Переопределения юниверса применяются неправильно

Эта ошибка может возникнуть, если в отчете используется юниверс, в котором содержится переопределение юниверса, созданное на сайте-адресате и тиражированное на сайт-источник.

4) Приложению Java не хватает памяти

Пример ошибки: `java.lang.OutOfMemoryError`

Ошибка может появиться, если во время обработки задания тиражирования на сервере Java-приложений обнаружено недостаточно памяти. Возможно, задание тиражирования является слишком большим, или на сервере Java-приложений недостаточно памяти.

Увеличьте доступную память на сервере Java-приложений путем перемещения веб-служб модуля "Интеграция" на отдельный компьютер или сократите число объектов, тиражируемых в одном задании тиражирования.

5) Время ожидания сокета

Пример ошибки: Ошибка при осуществлении связи с исходным сайтом. Тайм-аут чтения.

Отправка данных с исходного сайта на адаптивный сервер заданий на сайте назначения занимает больше времени, чем настроенный период ожидания. Увеличьте время ожидания сокета на адаптивном сервере заданий или сократите число объектов, тиражируемых в задании тиражирования.

6) Ограничения запроса

Пример ошибки: Ошибка SDK на сайте-адресате. Недопустимый запрос. (FWB 00025)Строка запроса превышает ограничение длины запроса.

Эта ошибка может возникнуть, если одновременно тиражируется слишком большое число объектов и модуль "Интеграция" отправляет запрос, который является слишком большим для обработки на сервере CMS. Объекты с сайта-источника будут переданы на сайт-адресат. Однако необходимые изменения не будут передаваться на сайт-источник. Конфликты разрешаются

согласно настройкам, однако признаки разрешения конфликта вручную не будут настроены для объектов. Объекты, переданные на сайт-адресат, будут продолжать правильно функционировать.

Для устранения этой проблемы уменьшите число объектов, тиражируемых в одном задании тиражирования.

7) Тайм-аут задания тиражирования

Пример ошибки: Невозможно запланировать объект в пределах заданного интервала времени.

Это сообщение может появиться, если происходит тайм-аут задания тиражирования во время завершения другого задания тиражирования. Это может произойти при одновременном подключении к одному сайту-источнику нескольких заданий тиражирования. Повторная попытка выполнения неудачно выполненного задания тиражирования будет предпринята в следующее запланированное время.

Для устранения этой проблемы запланируйте неудачно выполненное задание тиражирования, чтобы отсутствовал конфликт с другими заданиями тиражирования, подключающимися к одному сайту-источнику.

8) Ограничение тиражирования

Пример ошибки: Ошибка SDK на сайте-адресате. Ошибка доступа к базе данных. Внутренняя ошибка процессора запросов: во время оптимизации запроса процессору запросов не хватило пространства стека. Ошибка выполнения запроса в `ExecWithDeadlockHandling`.

Это сообщение может появиться, если превышено число поддерживаемых объектов, которые можно тиражировать одновременно. Для устранения этой проблемы сократите число объектов, тиражируемых в задании, и повторите попытку.

9) Объект потерян

Пример ошибки: При проверке прав безопасности возникла ошибка или При упаковке объекта возникла ошибка.

Это сообщение может отображаться, если объект отсутствует в пакете репликации. Это может возникать в случае, когда модуль "Интеграция" запрашивает объект, который требует тиражирования, но до проверки прав и упаковки объекта.

10) Адаптивный сервер обработки

Пример ошибки: На сервере обработки заданий возникла ошибка.

Эта ошибка может возникать при загрузке модулем "Интеграция" слишком большого количества классов, когда для обработки задачи тиражирования недостаточно памяти.

Для устранения этой проблемы необходимо выполнить два следующих шага:

1. В аргументах командной строки настраиваемого сервера обработки добавьте следующую строку: `-javaArgs "XX:MaxPermSize=256m"`.
2. Добавьте указанные ниже параметры в Java-сервер приложений, который подключается к модулю "Интеграция", чтобы сократить размер используемых файлов BIAR.
 - `-Dbobj.biar.suggestSplit=100m`

- `-Dbobj.biar.forceSplit=100m`

11) Пространство диспетчера объектов

Пример ошибки: Невозможно построить пакет доставки. Возникло исключение ввода/вывода: "На устройстве не осталось места."

Это возникает в случае, когда во временном каталоге, который используется модулем "Интеграция", недостаточно места. Для устранения этой проблемы добавьте место во временном каталоге или используйте для временного каталога другое местоположение.

Чтобы указать другое местоположение для временного каталога на сайте-источнике, добавьте в файлы конфигурации Java-сервера приложений следующую строку:

```
-Dbobj.tmp.dir=<TempDir>.
```

Чтобы указать другое местоположение для временного каталога на сайте-адресате, добавьте в аргументы командной строки настраиваемого сервера обработки следующую строку: `-javaArgs «-Dbobj.tmp.dir=<TempDir>»`.

В приведенных выше примерах `<TempDir>` – это местоположение временного каталога, который требуется использовать.

12) Ошибка юниверса

Пример ошибки: При вызове интерфейса API `processDPCommands` произошла ошибка.

Это возникает в случае, когда у тиражированного юниверса недопустимая или отсутствует связь с соединением юниверс-юниверс. Для устранения этой проблемы запустите задание тиражирования с установленным параметром **Обновлять из источника** и проверьте, чтобы было выполнено тиражирование соединения юниверса.

Также можно открыть юниверс в Universe Designer, изменить подключение к юниверсу и повторно использовать его.

См. также

- [Оптимальные методы работы](#)
- [Текущие ограничения выпуска](#)

Дополнительные конфигурации для сред ERP

19.1 Конфигурации для интеграции с SAP NetWeaver

19.1.1 Интеграция с SAP Netweaver Business Warehouse (BW)

19.1.1.1 Обзор

В этом разделе демонстрируется, как настроить BW для включения и администрирования публикации отчетов из SAP NetWeaver Business Warehouse на платформу BI.

Перед началом ознакомления с разделом убедитесь, что выполнена настройка подключаемого модуля аутентификации SAP в CMC.

См. также

- [Настройка аутентификации SAP](#)

19.1.1.1.1 Настройка папок и безопасности для платформы BI

При определении системы контроля полномочий на платформе BI система создает логическую структуру папок для используемой системы SAP. При импортировании ролей и публикации содержимого на платформу BI создаются соответствующие папки. Администратору не требуется создавать эти папки вручную. Папки создаются автоматически в результате определения системы контроля полномочий при настройке подключаемого модуля аутентификации SAP, импорте ролей в CMC, а также публикации содержимого на платформе BI.

Примечание:

Администратор платформы BI отвечает за присвоение соответствующих прав следующим папкам:

- Папка SAP верхнего уровня

Убедитесь в том, что группа пользователей "Все" имеет ограниченный доступ в папке SAP верхнего уровня.

- Папки системных идентификаторов

Назначьте основному издателю следующие права в СМС:

- Добавить объекты в папку
- Просмотр объектов
- Редактировать объекты
- Изменить права пользователей на объекты
- Удалить объекты

Совет:

Для упрощения процесса администрирования можно создать пользовательский уровень доступа и предоставить его основному издателю для доступа к соответствующим папкам идентификаторов системы.

См. также

- [Работа с уровнями доступа](#)
- [Права на платформе BI](#)

19.1.1.1.2 Работа с шаблонами безопасности для папок по умолчанию

При публикации содержимого из SAP на платформу BI система автоматически создает остальные компоненты иерархии ролей, папок и отчетов. Иными словами, платформа BI организует отчеты Crystal по папкам с именами, состоящими из идентификатора системы, номера клиента и имени роли.

На диаграмме ниже показан принцип организации содержимого на платформе BI при публикации двух ролей из одной системы BW:

- При определении системы контроля полномочий платформа BI создает папки верхнего уровня (папки SAP, 2.0 и системные (SID) папки).
- Папки ролей создаются автоматически (импортируются как группы на платформу BI) при необходимости, когда роль публикуется из BW.
- Папка содержимого создается автоматически для каждой из ролей, в которую публикуется содержимое.
- На каждый объект отчета распространяется параметр безопасности, и пользователи могут просматривать только те отчеты, которые относятся к их роли.

Администратор обязан распределять права между членами различных ролей. Для этого необходимо назначить следующие права в Content Administration Workbench.

Папки содержимого

Платформа BI импортирует группу для каждой роли, добавляемой в систему контроля полномочий в соответствии с определением в СМС.

Чтобы гарантировать предоставление соответствующих прав по умолчанию всем членам роли носителей содержимого, необходимо предоставить соответствующие права в Content Administration Workbench для каждой системы контроля полномочий, определенной на платформе BI:

1. В Content Administration Workbench раскройте **Система Enterprise**, затем раскройте **Доступные системы**.
2. Дважды щелкните требуемую систему.
3. Щелкните вкладку **Компоновка**.
4. Настройте **Политика безопасности для отчетов по умолчанию** на **Вид**.
5. Настройте **Политика безопасности для папок ролей** на **Просмотр по запросу**.
6. Нажмите кнопку **ОК**.

Эти настройки отображаются на платформе BI для всех ролей содержимого. Т.е. ролей с опубликованным содержимым. Члены этих ролей теперь смогут просматривать запланированные экземпляры отчетов, опубликованных в другие роли и обновлять отчеты в ролях, членами которых они являются.

Примечание:

Настоятельно рекомендуется устанавливать различия деятельности ролей. Например, при наличии возможности опубликовать от имени администратора лучше все же использовать для этого роли издателей. К тому же, функция публикации ролей заключается лишь в определении пользователей, которым разрешено публиковать содержимое. Таким образом, роли издателей не должны содержать какое-либо содержимое; издатели должны публиковать в роли носителей содержимого, доступные для членов обычных ролей.

19.1.1.2 Настройка службы BW Publisher

BW Publisher позволяет публиковать отчеты Crystal Reports (.rpt) индивидуально или в пакетах из модуля BW в платформу BI.

В Windows можно настроить BW Publisher одним из следующих способов:

- Запустите BW Publisher, используя соответствующую службу на компьютере с платформой BI. Служба BW Publisher запустит требуемый экземпляр BW Publisher.
- Запустите BW Publisher, используя локальный шлюз SAP, для создания экземпляров BW Publisher.

Выбор метода конфигурации основан на требованиях вашего узла, а также на сопоставлении преимуществ и недостатков каждой конфигурации. После настройки BW Publisher и платформы BI необходимо настроить публикацию в Content Administration Workbench.

19.1.1.3 Настройка службы BW Publisher

В данном разделе объясняется, как включить публикацию отчетов из BW на платформу BI, используя в качестве службы приложение BW Publisher. Выполните следующие действия.

19.1.1.3.1 Распространение установки BW Publisher

В данном разделе описывается распределение службы BW Publisher и способы отделения BW Publisher от других компонентов платформы BI.

Можно выровнять нагрузку публикации из BW, установив службы BW Publisher на двух разных машинах на одной развернутой платформе BI.

При установке BW Publisher на компьютерах, на которых размещена платформа BI, необходимо настроить каждый из них на использование того же идентификатора программы, шлюзового хоста и шлюзовой службы SAP. После создания RFC-адреса, использующего данный идентификатор программы, BW выравнивает нагрузку публикации между компьютерами платформы BI. Более того, если одно приложение BW Publisher станет недоступным, BW продолжит использовать оставшееся приложение BW Publisher.

Можно добавить дополнительный уровень системной избыточности к любой конфигурации, которая включает в себя несколько серверов приложений BW. Настройте каждый сервер приложений BW на использование шлюза SAP. Для каждого из них установите отдельную службу BW Publisher на компьютере, на котором размещена платформа BI. Настройте каждую службу BW Publisher на использование шлюзового хоста и шлюзовой службы отдельного сервера приложений BW. При такой настройке публикация из BW может быть продолжена в случае сбоя либо BW Publisher, либо сервера приложений.

Если необходимо отделить BW Publisher от других компонентов платформы BI, установите BW с использованием автономного шлюза SAP.

В этом случае локальный шлюз SAP необходимо установить на том же компьютере, что и BW Publisher. Кроме того, BW Publisher требует доступа к пакету средств разработки платформы BI и подсистеме печати Crystal Reports. Таким образом, если BW Publisher и локальный шлюз SAP устанавливаются на специальном компьютере, необходимо также установить сервер SIA.

19.1.1.3.2 Запуск BW Publisher: UNIX

Выполните скрипт BW Publisher, чтобы создать экземпляр или экземпляры издателя для обработки запросов публикации. Рекомендуется запускать один экземпляр издателя.

После запуска BW Publisher устанавливает соединение со службой шлюза SAP, указанной при выполнении программы настройки платформы BI.

19.1.1.3.3 Запуск службы BW Publisher: Windows

Для запуска службы BW Publisher в операционной среде Windows используйте приложение Central Configuration Manager (CCM). Во время запуска служба BW Publisher создает экземпляр издателя для обслуживания запросов из системы BW. Если объем запросов на опубликование превышен, служба BW Publisher автоматически создает дополнительных издателей для обработки запросов.

После запуска BW Publisher устанавливает соединение со службой шлюза SAP, указанной при выполнении программы установки платформы BI.

19.1.1.3.4 Настройка адресата для службы BW Publisher

Для работы с BW Publisher необходимо настроить адресат RFC на сервере BW для соединения со службой BW Publisher. При использовании кластера BW необходимо настроить адресат RFC на каждом сервере, используя при этом основной экземпляр BW в качестве шлюза хоста во всех случаях.

При публикации из BW на несколько развернутых платформ BI следует создать отдельный RFC-адрес для службы BW Publisher на каждой установленной платформе BI. Для каждого адресата необходимо использовать уникальный идентификатор программы, но одинаковый шлюз хоста и службу шлюза.

19.1.1.3.5 Настройка BW Publisher с локальным шлюзом SAP

Примечание:

Не используйте эту конфигурацию, если платформа BI установлена в среде UNIX. Выполнение этих действий в системе UNIX может привести к её непредсказуемой работе.

Чтобы включить опубликование отчетов из BW на платформе BI с использованием локального шлюза SAP, выполните следующие действия:

- [установка локального шлюза SAP](#).
- [Настройка назначения для BW Publisher](#).

19.1.1.3.6 установка локального шлюза SAP

Локальный шлюз SAP должен быть установлен на компьютер, на котором установлен BW Publisher. Рекомендуется, чтобы администратор SAP BASIS выполнил установку одного из этих шлюзов SAP.

Последние инструкции по установке локального шлюза SAP см. в инструкциях по установке SAP, которые хранятся на диске SAP Presentation.

Подробный список протестированных для платформы BI сред см. в файле `platforms_EN.txt`, входящем в комплект поставки продукта. Этот файл включает в себя требования конкретных версий и пакетов обновления для серверов приложений, операционных систем, компонентов SAP и т. д.

После установки шлюза SAP используйте `regedit`, чтобы убедиться, что в записях реестров `TMP` и `TEMP` присутствуют вторичные ключи `HKEY_CURRENT_USER\Environment`. Обе записи в

реестрах должны содержать одно и то же строковое значение – правильный абсолютный путь к директории. Если в каждой записи содержится переменная %USERPROFILE%, замените ее на абсолютный путь к директории. Обычно в обеих записях реестра указывают путь C:\WINDOWS\TEMP.

19.1.1.4 Настройка назначения для BW Publisher

Чтобы задействовать BW Publisher необходимо настроить адресат RFC для определения местоположения вашей машины и места установки локального шлюза SAP в BW Publisher.

19.1.1.5 Настройка опубликования в рабочем месте управления содержимым Content Administration Workbench

После настройки аутентификации SAP и BW Publisher выполните действия, описанные в данном разделе, чтобы включить опубликование. Данные инструкции позволят:

- Задавать необходимые авторизации для различных пользователей рабочего места управления содержимым Content Administration Workbench.
- Настраивать подключения к развернутой платформе BI, на которой публикуется содержимое.
- Определять роли с правом публикации в каждой развернутой платформе BI.
- Публиковать содержимое из BW на платформе BI.

19.1.1.6 Пользователи, имеющие доступ к Content Administration Workbench

Существует три типа пользователей, имеющих доступ к Content Administration Workbench:

- Потребители содержимого, могут просматривать отчеты и принадлежат к ролям носителей содержимого. Их уровень доступа позволяет только просматривать отчеты.
- Издатели содержимого платформы BI, имеющие право на просмотр, публикацию, изменение или (дополнительно) удаление отчетов из BW.
- Администраторы платформы BI с неограниченными правами в пределах Content Administration Workbench. Сюда входит определение систем платформы BI, публикация отчетов и их обслуживание.

19.1.1.7 Создание ролей в BW для назначенных издателей содержимого

При настройке параметров интеграции BW с платформой BI проверьте, позволяет ли существующая структура ролей быстро назначать определенных пользователей BW в качестве издателей содержимого или системных администраторов.

Подразумевается, что создаваемые ярлыки для ролей носят описательных характер. Примерами описательных имен ролей могут послужить BOE_CONTENT_PUBLISHERS и BOE_SYSTEM_ADMINISTRATORS.

Совет:

На платформе BI можно предоставить администрирующему пользователю полные права на администрирование системы или определенную их часть.

Для изменения прав, предоставленных новым или существующим ролям на платформе BI, необходимо сначала настроить аутентификацию SAP и импортировать роли. Изменить набор прав каждой импортированной роли можно с помощью Central Management Console.

19.1.1.8 Настройка доступа к средству ContentAdministration Workbench

Для каждого типа пользователя, который может получать доступ к средству Content Administration Workbench, в BW необходимо применить соответствующий набор средств авторизации. Средства авторизации перечислены в следующих таблицах.

Таблица 19-1: Средства авторизации для пользователей с правами администратора

Объект авторизации	Поле	Значения
S_RFC S_TCODE	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/CE_SYNCH, SH3A, SUNI
	ACTVT	Выполнение (16)
	TCD	/CRYSTAL/RPTADMIN, RSCR_MAINT_PUBLISH

Объект авторизации	Поле	Значения
S_TABU_CLI	CLIIDMAINT	X
S_TABU_DIS	ACTVT	Изменение, отображение (02, 03)
	DICBERCLS	&NC&
	JOBACTION	DELE, RELE
	JOBGROUP	' '
S_RS_ADMWB	ACTVT	Выполнение (16)
	RSADMWBOBJ	WORKBENCH
	ACTVT	Создание, изменение, отображение, удаление (01, 02, 03, 06)
ZCNTADMJOB	ACTVT	Создание, удаление (01, 06)
ZCNTADMRPT	ACTVT	Отображение, удаление, активация, обслуживание, проверка (03, 06, 07, 23, 39)

Таблица 19-2: Средства авторизации для издателей содержимого

Объект авторизации	Поле	Значения
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/CE_SYNCH, SH3A, SUNI
	ACTVT	Выполнение (16)
	TCD	/CRYSTAL/RPTADMIN
S_BTCH_JOB	JOBACTION	DELE, RELE
	JOBGROUP	' '
	ACTVT	Выполнение (16)
	RSADMWBOBJ	WORKBENCH
ZCNTADMCES	ACTVT	Отображение (03)
ZCNTADMJOB	ACTVT	(Создание, удаление) 01, 06
ZCNTADMRPT	ACTVT	Отображение, активация, обслуживание, проверка (03, 07, 23, 39) Удаление (необязательно) (06) Редактирование (необязательно) (02)

Предоставление издателям содержимого права на удаление отчетов в BW Content Administration Workbench является необязательным. Однако следует помнить о том, что при удалении отчета в BW он также удаляется с платформы BI. Если у издателя нет прав на удаление отчетов с платформы BI, возникает ошибка.

Средства авторизации для потребителей содержимого

Объект авторизации	Поле	Значения
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SH3A, SUNI
	ACTVT	Выполнение (16)
	TCD	/CRYSTAL/RPTADMIN
S_RS_ADMWB	ACTVT	Выполнение (16)
	RSADMWBOBJ	WORKBENCH
	ACTVT	Отображение (03)

19.1.1.9 Определение системы платформы BI

Для каждой системы платформы BI, в которой требуется опубликовать отчеты, необходимо создать определение системы в Content Administration Workbench.

19.1.1.9.1 Добавление системы платформы BI

1. Для доступа к Content Administration Workbench выполните транзакцию `/crystal/rptadmin`.
2. На панели **Операции** выберите **Enterprise System**.
3. Дважды щелкните **Добавить новую систему**.
4. На вкладке **Система** введите следующие значения:
 - Введите описательное имя в поле **Псевдоним**. Не используйте пробелы или специальные символы, поскольку при использовании имени псевдонима при настройке порталов Enterprise эти символы требуют специальной обработки.
 - Введите имя компьютера, на котором выполняется Центральный сервер управления платформы BI. Если Центральный сервер управления настроен на прослушивание порта, отличного от порта по умолчанию, введите имя `CMSNAME:PORT`

- Выберите вариант **Система по умолчанию**, если необходимо публиковать в этой системе отчеты из любой роли, которая не была явно назначена системе платформы BI. Системой по умолчанию может быть только одна система платформы BI.

В списке доступных систем система по умолчанию обозначена зеленой меткой.

5. Нажмите кнопку **Сохранить**.

6. На вкладке **RFC-адреса** последовательно добавьте все RFC-адреса, связанные с системой платформы BI. Чтобы добавить адрес, нажмите кнопку **Вставить строку**. В открывшемся списке дважды щелкните имя RFC-адреса.

Примечание:

Для обеспечения избыточности системы платформы BI в ней может существовать несколько адресов назначения.

7. Затем проверьте адрес назначения. Выберите только что добавленный адрес, щелкнув на сером поле слева от его имени.

8. Щелкните **Проверить определение SE**.

При этом проверяется возможность связи BW с указанной службой BW Publisher и возможность входа в эту систему платформы BI с помощью учетной записи системы контроля полномочий Crystal.

9. На вкладке **HTTP** введите следующие значения:

- **Протокол**

Введите http (если веб-сервер, подключенный к платформе BI, не настроен на использование протокола https).

- **Узел и порт веб-сервера**

Введите полное доменное имя или IP-адрес веб-сервера, на котором размещена стартовая панель BI. Для установленной системы, использующей сервер приложений Java, включите номер порта. Например:

```
boserver01.businessobjects.com:8080
```

- **Путь**

Введите:

```
SAP
```

Данный путь по сути является виртуальным путем, который веб-сервер использует при ссылке на подкаталог `sap` веб-содержимого платформы BI. Введите альтернативное значение, только если выполнена пользовательская настройка веб-среды и местоположения файлов веб-содержимого платформы BI.

Не указывайте прямую наклонную черту в начале или в конце данной записи.

- **Приложение для просмотра**

Введите имя приложения для просмотра. Введите `reportview.do`, чтобы использовать средство просмотра по умолчанию для платформы BI, на которой используется InfoView

на базе Java. Если платформа BI установлена в среде Windows с использованием конфигурации ASP.NET по умолчанию, ведите report/report_view.aspx, чтобы использовать браузер по умолчанию.

10. На вкладке **Языки** выберите языки отчетов, которые будут публиковаться в данной системе платформы BI.
11. Воспользуйтесь вкладкой **Роли**, чтобы добавить роли с содержимым, которые необходимо связать с данной системой платформы BI.
12. Нажмите кнопку **Вставить строку**.

Отобразится список ролей, доступных для добавления в данную систему платформы BI.

Примечание:

Каждую из ролей можно публиковать только в одной системе платформы BI. Если роли, которые необходимо добавить на данную платформу BI, не отображаются в списке, щелкните **Отмена**, чтобы вернуться на вкладку **Роли**. Затем щелкните **Переназначить роли**.

13. Выберите роли, которые необходимо опубликовать в системе платформы BI, и нажмите кнопку **ОК**.
14. Затем настройте для содержимого, опубликованного в данной системе платформы BI, параметры безопасности по умолчанию. Откройте вкладку **Макет**, выберите параметры безопасности, которые по умолчанию используются для папок отчетов и ролей.

Примечание:

- На платформе BI автоматически создается папка для каждой роли, опубликованной в этой системе. В этой папке содержатся ярлыки для отчетов, опубликованных с этой ролью.
- После настройки системы платформы BI изменение уровней безопасности по умолчанию в этой папке не повлияет на уровни безопасности опубликованных папок ролей или отчетов. Чтобы изменить уровни безопасности по умолчанию для всех ролей и содержимого, опубликованного на платформе BI, удалите папки ролей и ярлыки на платформе BI. (При этом сами отчеты удалены не будут.) Затем измените здесь параметры безопасности и снова опубликуйте роли и отчеты.

15. Нажмите кнопку **ОК** внизу, чтобы сохранить настройки и создать систему платформы BI в Content Administration Workbench.

Теперь из BW можно публиковать отчеты на платформу BI.

19.1.1.10 Публикация отчетов с использованием приложения Content Administration Workbench

После сохранения отчета в BW его можно опубликовать с использованием Content Administration Workbench. Приложение Content Administration Workbench можно использовать для публикации отдельных отчетов или всех отчетов, сохраненных в определенной роли. Только пользователь, авторизованный как издатель содержимого Crystal, может использовать приложение Content Administration Workbench для публикации и обслуживания отчетов.

См. также

- [Создание и применение средств авторизации](#)

19.1.1.11 Публикация ролей или отчетов

1. Для доступа к Content Administration Workbench выполните транзакцию `/crystal/rptadmin`.
2. На панели **Операции** выберите **Опубликовать отчеты**.
3. Для поиска содержимого, сохраненного в системе BW, дважды щелкните мышью **Выбрать отчеты и роли для опубликования**.

Появляется диалоговое окно, необходимое для облегчения фильтрации доступных ролей и отчетов.

4. В списке **Система** выберите систему или системы платформы BI с содержимым, которое необходимо отобразить.

Примечание:

Список **Система** содержит все доступные системы, определенные в данной системе BW.

5. Затем отфильтруйте результаты, чтобы ограничить число отображаемых отчетов и ролей. Используйте следующие параметры:

- **Версия объекта**

При выборе "А: активный" отображаются все отчеты, которые можно опубликовать. При выборе пустого значения отображаются все отчеты. (Остальные параметры являются зарезервированными выражениями SAP.)

- **Статус объекта**

Выберите "АСТ Активный, исполняемый" для отображения только опубликованных отчетов. Выберите "INA Неактивный, неисполняемый" для отображения только неопубликованных отчетов. Не указывайте значение для отображения всех отчетов. (Остальные параметры являются зарезервированными выражениями SAP.)

- **Фильтр роли**

При вводе текста в поле отображаются только роли, которые соответствуют введенному тексту. Используйте * в качестве подстановочного знака. Например, для отображения всех ролей, названия которых начинаются с буквы "д", введите "д*".

- **Описание отчета**




При вводе текста в поле отображаются только отчеты, описание которых соответствует введенному тексту. Используйте * в качестве подстановочного знака для поиска соответствия любому числу символов. Используйте + в качестве подстановочного знака для поиска соответствия 0 или 1 символу. Например, для отображения всех отчетов, в описании которых содержится слово "доход", введите *доход*.

6. Нажмите кнопку **ОК**.

На правой панели отображается список отчетов, соответствующих критериям.

Отчеты упорядочены в следующей иерархии: система > Роли в этой системе > Отчеты, сохраненные в этой роли.

Каждый элемент в иерархии отмечен красной, желтой или зеленой точкой. Элементы, расположенные выше в иерархии, соответствуют состоянию содержащихся в иерархии элементов – наименее благоприятные условия расположены на верхнем уровне иерархии. Например, если один отчет в роли является желтым (активным), но все остальные – зелеными (опубликованными), роль отмечена желтым цветом (активна).

-  Зеленый: элемент полностью опубликован. Если этим элементом является система платформы BI или роль, публикуются все отчеты в этом элементе.
-  Желтый: элемент активен, но не опубликован. Если элемент является отчетом, то он доступен для опубликования. Если этим элементом является роль или система платформы BI, то все содержимое является активным и по крайней мере один элемент в этой роли или системе не опубликован.
-  Красный: элемент является содержимым SAP и недоступен для опубликования с использованием Content Administration Workbench. Содержимое недоступно для опубликования, пока оно не активировано с использованием BW Administration Workbench.

7. Выберите отчеты, которые необходимо опубликовать.

Для публикации всех отчетов в роли выберите роль. Выберите эту систему, чтобы опубликовать все роли в системе платформы BI.

Примечание:

При выборе роли (или системы) выбираются все отчеты, содержащиеся в роли (или системе). Чтобы очистить выделение, снимите флажок роли (или системы), а затем нажмите кнопку "Обновить".

8. Щелкните **Опубликовать**.

Примечание:

Отчеты, опубликованные в фоновом режиме, обрабатываются по мере высвобождения ресурсов системы. Для использования этого параметра щелкните **В фоновом режиме** вместо **Опубликовать**.

9. Щелкните **Обновить**, чтобы обновить отображение статуса систем, ролей и отчетов платформы BI в Content Administration Workbench.

Совет:

Для просмотра отчета щелкните правой кнопкой мыши на отчете и выберите **Вид**. Для просмотра запросов, используемый в отчете, щелкните правой кнопкой мыши на отчете и выберите **Используемые запросы**.

Примечание:

После публикации отчета на платформе BI нажмите кнопку **Перезапись**, чтобы перезаписать опубликованный отчет.

См. также

- [Планирование публикации в фоновом режиме](#)

19.1.1.12 Планирование публикации в фоновом режиме

Для публикации отчетов в фоновом режиме, которое может выполняться немедленно или в качестве запланированного задания, необходимы системные ресурсы. Отчеты рекомендуется публиковать в фоновом режиме для уменьшения времени отклика системы.

При периодической публикации отчетов в качестве запланированных заданий выполняется синхронизация информации об отчетах между BW и системой платформы BI. Рекомендуется планировать все отчеты (или роли, содержащие эти отчеты). Можно также синхронизировать роли и отчеты вручную с использованием параметра обновления состояния операции обслуживания отчетов.

19.1.1.13 Обновление системной информации опубликованных отчетов

Для обновления источника данных опубликованных отчетов BW Publisher использует введенную системную информацию SAP. Вы можете использовать сервер приложений BW либо главный экземпляр BW, если конфигурация с выравниванием нагрузки более предпочтительна.

19.1.1.14 Обслуживание отчетов

Задачи по обслуживанию отчетов включают в себя синхронизацию информации об отчетах между платформой BI и BW (Обновить статус), удаление ненужных отчетов (Удалить отчеты) и обновление отчетов, перенесенных из предыдущих версий платформы BI (После переноса).

19.1.1.14.1 Обновление статуса отчетов

При изменении опубликованного отчета в системе платформы BI (например, изменение роли, в которую публикуется отчет) это изменение не будет отражено в BW, пока не будет выполнена синхронизация платформы BI и BW. Можно запланировать публикацию так, чтобы периодически выполнять синхронизацию платформы BI и BW (см. раздел [Планирование публикации в фоновом режиме](#)), либо вручную обновлять статус отчета с использованием средства "Обслуживание отчетов".

19.1.1.14.2 Удаление отчетов

При удалении опубликованного отчета из BW с использованием инструмента Content Administration Workbench этот отчет также удаляется с платформы BI. Удалить отчеты смогут только те пользователи, у которых имеются необходимые права на удаление отчетов в BW и системе платформы BI.

Примечание:

Если у пользователя имеются права на удаление отчета в BW, но нет прав на удаление этого отчета из системы платформы BI, где он был опубликован, может возникнуть ошибка.

19.1.1.15 Настройка обработчика http-запросов SAP

Чтобы разрешить просмотр отчетов в BW, необходимо настроить BW для использования обработчика http-запросов, который является частью инструмента Content Administration Workbench. Тогда при открытии пользователем BW отчета Crystal из пользовательского интерфейса SAP станет возможным направить запрос на просмотр непосредственно через Интернет.

Для перехода к списку виртуальных хостов и активных служб вашей BW-системы используется транзакция SICF. Создайте новый узел `ce_url` в иерархии BW `default_host` и добавьте к списку обработчиков запись `/CRYSTAL/CL_BW_HTTP_HANDLER`. После создания службы может возникнуть необходимость включить ее вручную.

19.1.1.16 Конфигурации для обработки данных SAP

19.1.1.16.1 Обработка запланированных отчетов в пакетном режиме SAP

При установке в среде Windows можно запускать запланированные отчеты в платформе BI с использованием пакетного режима SAP. Драйверы InfoSet и Open SQL могут выполнять отчеты с использованием пакетного или фонового режима SAP, если для определенных переменных среды установлены значения 1. Соответствующими переменными среды являются:

- `CRYSTAL_INFOSET_FORCE_BATCH_MODE` (для драйвера InfoSet)
- `CRYSTAL_OPENSQ_L_FORCE_BATCH_MODE` (для драйвера Open SQL)

Однако эту функцию рекомендуется использовать только при распределенной установке платформы BI. Когда для этих переменных среды установлено значение 1, драйверы могут выполнять отчеты с использованием пакетного или фонового режима SAP вне зависимости от компонента отчета, который в действительности выполняет отчет. Поэтому, если эти переменные

среды создаются в качестве системных переменных среды на компьютере, на котором запущены различные серверы платформы BI, драйверы выполняют все отчеты в пакетном режиме (включая запросы отчетов по требованию с серверов обработки и серверов приложений отчетов Crystal Reports).

Чтобы убедиться, что драйверы выполняют только запланированные отчеты в пакетном режиме (т.е. отчеты, выполняемые сервером заданий для отчета), не настраивайте системные переменные среды на компьютере, на котором запущены различные серверы платформы BI. Вместо этого выполните следующие действия для настройки переменных среды для каждого сервера заданий для отчета.

Примечание:

Для пользователей SAP, запланировавших отчеты на платформе BI, может потребоваться дополнительная авторизация в системе SAP.

См. также

- [Планирование отчета в пакетном режиме посредством запроса Open SQL](#)

19.1.1.16.2 Обработка запланированных отчетов в пакетном режиме SAP

1. Создайте пакетный скрипт (файл .bat) в текстовом редакторе, таком как "Блокнот", со следующим содержанием:

```
@echo off
set CRYSTAL_INFOSET_FORCE_BATCH_MODE=1
set CRYSTAL_OPENSQLE_FORCE_BATCH_MODE=1
%*
```

Этот скрипт задает для переменных среды значения 1, а затем выполняет параметры, переданные из командной строки.

2. Сохраните файл как `jobserver_batchmode.bat` в папке на каждом компьютере сервера заданий для отчета.
3. Запустите приложение Central Configuration Manager (CCM) из группы программ платформы BI.
4. Щелкните правой кнопкой мыши **Crystal Report Job Server**, а затем в контекстном меню щелкните **Стоп**.
5. Щелкните правой кнопкой мыши **Crystal Report Job Server**, а затем в контекстном меню щелкните **Свойства**.
6. На вкладке **Свойства** найдите поле **Команда**.

Это команда запуска для сервера заданий для отчета. Например, команда может иметь следующий вид (записана в одной строке):

```
"\\SERVER01\C$\Program Files\SAO Business Objects\SAP BusinessObjects Enterprise\win32_x86\JobServer.exe"
-service -name SERVER01.report -ns SERVER01 -objectType BusinessObjects Enterprise.Report -lib procReport
-restart
```

7. Укажите перед командой по умолчанию полный путь к файлу `jobserver_batchmode.bat`, сохраненному на компьютере сервера заданий для отчета.

В этом примере файл пакета сохранен на компьютере с именем SERVER01 как:

```
C:\Crystal Scripts\jobserver_batchmode.bat
```

Поэтому новая команда запуска для сервера заданий для отчета принимает вид:

```
"\\SERVER01\C$\Crystal Scripts\jobserver_batchmode.bat" "\\SERVER01\C$\Program Files\SAP Business  
Objects\SAP  
BusinessObjects Enterprise 12.0\win32_x86\JobServer.exe" -service -name SERVER01.report -ns SERVER01  
-objectType BusinessObjects Enterprise.Report -lib procReport -restart
```

Эта новая команда запуска сначала выполняет файл пакета. В свою очередь файл пакета настраивает необходимые переменные среды перед выполнением исходной команды запуска для сервера заданий для отчета. Благодаря этому обеспечивается различие переменных среды, доступных серверу заданий для отчета, и переменных среды, доступных серверу, который отвечает за обработку отчетов по запросу (сервер обработки и сервер приложений отчетов Crystal Reports).

8. После изменения поля **Команда** в приложении CCM нажмите кнопку **ОК**.
9. Щелкните правой кнопкой мыши **Crystal Report Job Server**, а затем в контекстном меню щелкните **Запуск**.

Примечание:

Если происходит сбой запуска сервера заданий для отчетов, проверьте новую команду запуска.

10. На панели инструментов CCM щелкните **Включение/отключение серверов**, войдите в платформу BI под учетными данными администратора и убедитесь, что сервер заданий для отчета включен.

19.1.1.17 Конфигурации для транспортов SAP

19.1.1.17.1 Обзор

Платформа BI содержит 8 транспортов: связь Open SQL, связь InfoSet, определение безопасности на уровне строк, определение кластера, Content Administration Workbench, персонализация параметров запросов BW, MDX и ODS.

Существует два различных набора транспортов: Unicode-совместимые транспорты и транспорты ANSI. При работе в системе BASIC версии 6.20 или более новой следует использовать Unicode-совместимые транспорты. При работе с версией системы BASIC ниже 6.20 рекомендуется использовать транспорты ANSI. Все установленные транспорты расположены в следующем каталоге дистрибутивного носителя для продукта: \Collaterals\Add-Ons\SAP\Transports\.

Примечание:

При проверке возможных конфликтов при установке, убедитесь в том, что в системе SAP отсутствуют объекты с повторяющимися именами. По умолчанию объекты используют пространство имен /crystal/, так что создавать его вручную не требуется. При попытке создать пространство имен /crystal/ вручную, вас попросят предоставить ключи исправления лицензии, к которым у вас доступа нет.

19.1.1.17.2 Настройка транспорта

Чтобы задать компоненты Data Access или BW Publisher платформы BI, необходимо импортировать в систему SAP соответствующие файлы транспорта. Эти компоненты используют содержимое этих файлов транспорта при взаимодействии с системой SAP.

Процедуры установки и настройки, требуемые для системы SAP, должен выполнить специалист по BASIS, знакомый с системой изменений и транспорта, у которого есть права администратора для системы SAP. Точная процедура импорта файлов транспорта зависит от используемой версии BASIS. Точные сведения о процедуре см. в документации SAP.

По умолчанию при первом развертывании компонента Data Access все пользователи могут иметь доступ ко всем таблицам SAP. Чтобы обеспечить безопасность данных SAP, к которым пользователи могут получать доступ, используйте Редактор определения безопасности.

После импорта транспортов необходимо настроить соответствующие уровни доступа пользователей. Создайте нужные средства авторизации и примените их с помощью профилей или ролей к пользователям SAP, которые будут создавать, использовать или планировать отчеты Crystal.

См. также

- [Создание и применение средств авторизации](#)

Виды транспортов

Существует два различных набора транспортов: Unicode-совместимые транспорты и транспорты ANSI. При работе в системе BASIC версии 6.20 или более новой следует использовать Unicode-совместимые транспорты. При работе с версией системы BASIC ниже 6.20 рекомендуется использовать транспорты ANSI. Все установленные транспорты расположены в следующем каталоге дистрибутива продукта: \Collaterals\Add-Ons\SAP\Transports\. В файле transports.txt перечислены все файлы транспорта в Unicode и ANSI.

Далее описывается каждый тип транспорта.

- Транспорт Open SQL Connectivity

Транспорт Open SQL Connectivity позволяет драйверу Open SQL подключаться к системе SAP и формировать отчеты.

- Транспорт определения защиты на уровне строки

Этот транспорт позволяет использовать такой инструмент, как Редактор определения безопасности, являющийся графическим интерфейсом для таблиц /crystal/auth в транспорте взаимодействия Open SQL Connectivity.

- Транспорт Определения кластера

Этот транспорт позволяет использовать Инструмент определения кластера. Этот инструмент позволяет построить репозиторий метаданных для определений кластеров данных ABAP. Эти определения предоставляют драйверу Open SQL все необходимые данные для формирования отчетов об этих кластерах данных.

Примечание:

Кластеры данных ABAP отличаются от таблиц кластеров. Таблицы кластеров уже определены в DDIC.

- Транспорт InfoSet Connectivity

Транспорт InfoSet Connectivity разрешает драйверу InfoSet доступ к InfoSet и запросам SAP.

- Транспорт Content Administration Workbench

В этой службе транспорта доступны функции администрирования содержимого для систем BW. Он доступен только как UNICODE-транспорт.

- Транспорт персонализации параметров запроса BW

Этот транспорт обеспечивает поддержку персонализированных значений параметров и их значений по умолчанию на основании запросов BW.

Проверка на наличие конфликтов

Содержимое файлов транспорта автоматически регистрируется в пространстве имен SAP Business Objects при импорте этих файлов. С этой целью пространство имен Business Objects зарезервировано в последних версиях R/3 и MY SAP ERP. Однако имена некоторых объектов (например, объектов авторизации, классов авторизации и устаревших объектов) могут не содержать нужные префиксы. Перед импортом файлов транспорта рекомендуется проверить эти типы объектов на наличие конфликтов.

Если группа функций, любой из функциональных модулей или любой из других объектов уже существует в системе SAP, перед импортом файлов транспорта платформы BI необходимо разрешить пространство имен. Описание процедур, соответствующих версии SAP, см. в документации SAP.

Импорт файлов транспорта

Прочтите файл `transports_EN.txt`, расположенный в следующем каталоге дистрибутивного носителя для продукта: `\Collaterals\Add-Ons\SAP\Transports\`. В этом файле перечислены имена файлов для каждого транспорта. (Папки `cofiles` и `data` в директории транспорты соответствуют директориям `.../trans/cofiles` и `.../trans/data` на вашем сервере SAP).

Перед импортом транспортов для определения безопасности на уровне строки или определения кластера следует импортировать транспорт взаимодействия Open SQL Connectivity. Другие транспорты можно импортировать в любом порядке.

Примечание:

- Скопировав файлы с диска на сервер, перед импортом убедитесь, что все файлы доступны для записи. Если файлы доступны только для чтения, то при импорте произойдет ошибка.
- Так как транспорты являются двоичными файлами, в UNIX-инсталляциях необходимо добавить файлы через FTP с использованием двоичного режима (для предупреждения искажения файлов). Кроме этого, у пользователя должно быть разрешение производить запись файлов на сервер Unix.

Транспорты

Транспорт Open SQL Connectivity

Транспорт Open SQL Connectivity позволяет драйверам подключаться к системе SAP и составлять отчеты на ее базе.

Объект	Тип	Описание
/CRYSTAL/BC	Пакет	Класс разработки
/CRYSTAL/OPENSQL	Группа функций	Функции Open SQL
/CRYSTAL/OSQL_AUTH_FORMS	Программа	Вспомогательная программа
/CRYSTAL/OSQL_EXECUTE	Программа	Вспомогательная программа
/CRYSTAL/OSQL_TYPEPOOLPROG	Программа	Вспомогательная программа
/CRYSTAL/OSQL_TYPEPOOLS	Программа	Вспомогательная программа
/CRYSTAL/OSQL_UTILS	Программа	Вспомогательная программа
ZSSI	Класс объекта авторизации	Составление отчетов об объектах авторизации
ZSEGREPORT	Объект авторизации	Составление отчетов об объекте авторизации
/CRYSTAL/OSQL_CLU_ACTKEY_ENTRY	Таблица	Метаданные кластера
/CRYSTAL/OSQL_FCN_PARAM	Таблица	Метаданные функции
/CRYSTAL/OSQL_FCN_PARAM_FIELD	Таблица	Метаданные функции
/CRYSTAL/OSQL_FIELD_ENTRY	Таблица	Метаданные таблицы

Объект	Тип	Описание
/CRYSTAL/OSQL_OBJECT_ENTRY	Таблица	Метаданные таблицы
/CRYSTAL/OSQL_RLS_CHK_ENTRY	Таблица	Метаданные RLS
/CRYSTAL/OSQL_RLS_FCN_ENTRY	Таблица	Метаданные RLS
/CRYSTAL/OSQL_RLS_VAL_ENTRY	Таблица	Метаданные RLS
ZCLUSTDATA	Таблица	Метаданные кластера
ZCLUSTID	Таблица	Метаданные кластера
ZCLUSTKEY	Таблица	Метаданные кластера
ZCLUSTKEY2	Таблица	Метаданные кластера
/CRYSTAL/AUTHCHK	Таблица	Метаданные RLS
/CRYSTAL/AUTHFCN	Таблица	Метаданные RLS
/CRYSTAL/AUTHKEY	Таблица	Метаданные RLS
/CRYSTAL/AUTHOBJ	Таблица	Метаданные RLS
/CRYSTAL/AUTHREF	Таблица	Метаданные RLS
ZSSAUTHCHK	Таблица	Прежние метаданные RLS
ZSSAUTHOBJ	Таблица	Прежние метаданные RLS
ZSSAUTHKEY	Таблица	Прежние метаданные RLS
ZSSAUTHREF	Таблица	Прежние метаданные RLS

Объект	Тип	Описание
ZSSAUTH FCN	Таблица	Прежние метаданные RLS

Транспорт InfoSet Connectivity

Транспорт InfoSet Connectivity позволяет драйверу InfoSet получать доступ к объектам InfoSet. Этот транспорт совместим с R/3 4.6c и более поздними версиями. Не импортируйте этот транспорт при использовании SAP R/3 4.6a или более старой версии.

Объект	Тип	Описание
/CRYSTAL/BC	Пакет	Класс разработки
/CRYSTAL/FLAT	Группа функций	Функции-оболочки InfoSet
/CRYSTAL/QUERY_BATCH	Программа	Выполнение в пакетном режиме
/CRYSTAL/QUERY_BATCH_STREAM	Программа	Потоковое выполнение в пакетном режиме.

Транспорт определения безопасности на уровне строки

Этот транспорт обеспечивает Редактор определения безопасности, который представляет собой графический интерфейс для таблиц /CRYSTAL/AUTH в транспорте Open SQL Connectivity.

Объект	Тип	Описание
/CRYSTAL/BC	Пакет	Класс разработки
/CRYSTAL/TABMNT	Группа функций	Группа функций для обслуживания таблицы, просмотр ограничений функций
/CRYSTAL/RLSDEF	Программа	Главная программа

Объект	Тип	Описание
/CRYSTAL/RLS_INCLUDE1	Программа	Включает программу, которая содержит определения модулей
/CRYSTAL/RLS_INCLUDE2	Программа	Включает программу, которая содержит определения вспомогательных процедур
TDDAT [/CRYSTAL/AUTHFCN]	Содержимое таблицы	Определение обслуживания таблицы
TVDIR [/CRYSTAL/AUTHFCN]	Содержимое таблицы	Определение обслуживания таблицы
/CRYSTAL/AUTHFCNS	Определение транспорта и объекта обслуживания	Определение обслуживания таблицы
/CRYSTAL/RLS	Транзакция	Транзакция главной программы
/CRYSTAL/RLSFCN	Транзакция	Вспомогательная транзакция, вызываемая главной программой.

Транспорт Определения кластера

Этот транспорт позволяет использовать Инструмент определения кластера. Этот инструмент позволяет построить репозиторий метаданных для определений кластеров данных ABAP. Эти определения предоставляют драйверу Open SQL все необходимые данные для формирования отчетов об этих кластерах данных.

Примечание:

Кластеры данных ABAP отличаются от таблиц кластеров. Таблицы кластеров уже определены в DDIC.

Объект	Тип	Описание
ZCIMPRBG	Программа	Главная программа
ZCRBGTOP	Программа	Включение программы
ZCDD	Транзакция	Транзакция главной программы

Приложение *Content Administration Workbench*

В этой службе транспорта доступны функции администрирования содержимого для систем BW. Она доступна только как служба транспорта, совместимая с Юникод.

Объект	Тип	Описание
/CRYSTAL/BC	Пакет	Класс разработки
/CRYSTAL/CL_BW_HTTP_HANDLER	Класс	Обработчик запросов HTTP с множеством зависимостей CE
/CRYSTAL/OBJECT_STATUS_DOM	Домен	Активность по отчету
/CRYSTAL/OBJ_POLICY_DOM	Домен	Безопасность объекта CE
/CRYSTAL/OBJECT_STATUS	Элемент данных	Активность по отчету
/CRYSTAL/OBJ_POLICY	Элемент данных	Безопасность объекта CE
/CRYSTAL/CE_SYNCH	Группа функций	Программные заглушки Publisher
/CRYSTAL/CA_MSG	Класс сообщения	Сообщения о состоянии
/CRYSTAL/CE_SYNCH_FORMS	Программа	Программный компонент

Объект	Тип	Описание
/CRYSTAL/CONTENT_ADMIN	Программа	Программный компонент
/CRYSTAL/CONTENT_ADMIN_CLASS_D	Программа	Программный компонент
/CRYSTAL/CONTENT_ADMIN_CLASS_I	Программа	Программный компонент
/CRYSTAL/CONTENT_ADMIN_CTREE	Программа	Программный компонент
/CRYSTAL/CONTENT_ADMIN_FORMS	Программа	Программный компонент
/CRYSTAL/CONTENT_ADMIN_MODULES	Программа	Программный компонент
/CRYSTAL/CONTENT_ADMIN_PAIS	Программа	Программный компонент
/CRYSTAL/CONTENT_ADMIN_PBOS	Программа	Программный компонент
/CRYSTAL/CONTENT_ADMIN_TAB_FRM	Программа	Программный компонент
/CRYSTAL/CONTENT_ADMIN_TOP	Программа	Программный компонент
/CRYSTAL/PUBLISH_WORKER	Программа	Программный компонент
/CRYSTAL/PUBLISH_WORKER_DISP	Программа	Программный компонент
/CRYSTAL/PUBLISH_WORKER_DISP_I	Программа	Программный компонент
/CRYSTAL/PUBLISH_WORKER_FORMS	Программа	Программный компонент
/CRYSTAL/PUBLISH_WORKER_PROC	Программа	Программный компонент
/CRYSTAL/PUBLISH_WORKER_PROC_I	Программа	Программный компонент
/CRYSTAL/PUBLISH_WORKER_SCREEN	Программа	Программный компонент

Объект	Тип	Описание
/CRYSTAL/CA_DEST	Таблица	Состояние приложения
/CRYSTAL/CA_JOB	Таблица	Состояние приложения
/CRYSTAL/CA_JOB2	Таблица	Состояние приложения
/CRYSTAL/CA_LANG	Таблица	Состояние приложения
/CRYSTAL/CA_PARM	Таблица	Состояние приложения
/CRYSTAL/CA_ROLE	Таблица	Состояние приложения
/CRYSTAL/CA_SYST	Таблица	Состояние приложения
/CRYSTAL/MENU_TREE_ITEMS	Структура	Состояние приложения
/CRYSTAL/REPORT_ID	Таблица	Состояние приложения
/CRYSTAL/RPTADMIN	Транзакция	Транзакция главной программы
/CRYSTAL/EDIT_REPORT	Программа	Упаковщик для редактирования отчетов
/CRYSTAL/EDIT_REPORT	Группа функций	Функции для редактирования отчета
ZSSI	Класс объекта авторизации	Авторизации Crystal
ZCNTADMCES	Объект авторизации	Операции CE
ZCNTADMRPT	Объект авторизации	Операции отчета
ZCNTADMJOB	Объект авторизации	Операции фоновых заданий

Транспорт соединения ODS

Данный транспорт позволяет драйверу запросов ODS получить доступ к данным ODS. Данный транспорт совместим с BW 3.0B (патч 27 или выше) и с BW 3.1C (патч 21 или выше).

Объект	Тип	Описание
/CRYSTAL/BC	Пакет	Класс разработки
/CRYSTAL/ODS_REPORT	Группа функций	Функции ODS

Транспорт персонализации параметров запроса BW

Этот транспорт обеспечивает поддержку персонализированных значений параметров и их значений по умолчанию на основании запросов BW.

Объект	Тип	Описание
/CRYSTAL/BC	Пакет	Класс разработки
/CRYSTAL/PERS_VAR	Структура	Определение переменной
/CRYSTAL/PERS_VALUE	Структура	Определение значения
/CRYSTAL/PERS	Группа функций	Функции персонализации

Транспорт взаимодействия BW MDX

Этот транспорт позволяет драйверу запросов MDX осуществлять доступ к кубам BW и запросам. Данный транспорт совместим с BW 3.0B (патч 27 или выше) и с BW 3.1C (патч 21 или выше).

Объект	Тип	Описание
/CRYSTAL/BC	Пакет	Класс разработки
/CRYSTAL/MDX	Группа функций	Функции MDX

Объект	Тип	Описание
/CRYSTALMDX_STREAM_LAYOUT	Определение таблицы	Структура набора данных
/CRYSTAL/CX_BAPI_ERROR	Класс	Исключение
/CRYSTAL/CX_METADATA_ERROR	Класс	Исключение
/CRYSTAL/CX_MISSING_STREAMINFO	Класс	Исключение
/CRYSTAL/CX_NO_MORE_CELLS	Класс	Исключение
/CRYSTAL/CX_NO_MORE_MEMBERS	Класс	Исключение
/CRYSTAL/CX_NO_MORE_PROPERTIES	Класс	Исключение
/CRYSTAL/CX_SAVE_SESSION_STATE	Класс	Исключение
/CRYSTALMDX_APPEND_DATA	Класс	Процессор набора данных
/CRYSTALMDX_READER_BASE	Класс	Процессор набора данных
/CRYSTALMDX_READ_DIMENSIONS	Класс	Процессор набора данных
/CRYSTALMDX_READ_MEASURES	Класс	Процессор набора данных
/CRYSTALMDX_READ_PROPERTIES	Класс	Процессор набора данных
/CRYSTALMDX_PROPERTY_KEYS	Тип таблицы	Структура метаданных
/CRYSTALMDX_PROPERTY_KEYS	Тип таблицы	Структура метаданных
/CRYSTALMDX_PROPERTY_VALUES	Тип таблицы	Структура метаданных
/CRYSTALMDX_STREAM_LAYOUT_TAB	Тип таблицы	Структура метаданных

19.1.1.18 Обзор авторизаций

В настоящем разделе представлен список авторизаций SAP, которые согласно нашему опыту работы в нашей проверочной среде требуются при выполнении общих задач платформы BI в интегрированной среде SAP. В зависимости от индивидуальной реализации могут потребоваться дополнительные объекты или поля авторизации.

Из каждого объекта авторизации необходимо создать авторизацию и задать соответствующие значения в полях. После этого можно применить соответствующие авторизации к профилям (или ролям) пользователей SAP. В последующих разделах описываются требуемые авторизации и приводятся необходимые значения для полей. Подробную информацию об этих процедурах, соответствующих используемой вами версии SAP, см. в документации по SAP.

Примечание:

- Информация в данном приложении приводится только в целях рекомендации.
- Объект авторизации ZSEGREPORT принадлежит к классу объектов ZSSI, который устанавливается при импорте файлов переноса BusinessObjects XI Integration for SAP, необходимых для поддержки запросов Open SQL.

19.1.1.18.1 Создание и применение средств авторизации

Необходимо создать и применить средства авторизации, необходимые для доступа каждого из пользователей к информации с помощью Desktop Intelligence Integration для SAP. Точные процедуры создания, настройки и применения средств авторизации зависят от установленной версии SAP. В этом разделе представлен список средств авторизации SAP, которые, согласно нашему опыту работы в соответствующих тестовых средах, требуются для выполнения наиболее распространенных задач при использовании платформы BI, интегрированной в среду SAP NetWeaver ABAP. В зависимости от индивидуальной реализации могут потребоваться дополнительные объекты или поля авторизации.

См. также

- [Настройка опубликования в рабочем месте управления содержимым Content Administration Workbench](#)

19.1.1.19 Действия в BW

В этом разделе перечислены различные действия в модуле BW.

19.1.1.19.1 Действия в Crystal Reports

Создание отчета из запроса в роль BW

Объект авторизации	Поле	Значения
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_ROLE обозначает название любой роли, к которой принадлежит пользователь. В это поле можно ввести несколько значений.

* *QUERY_OWNER* указывает имя владельца запроса. Если указать имя, можно получить отчет только по запросам с данным владельцем. Для получения отчета по запросам со всеми владельцами введите символ "***".

** Чтобы указать для *INFO_AREA*, *INFO_CUBE* или *COMP_ID* любое значение, введите символ "***". Если вы укажете конкретное значение, можно составить отчеты по запросам, содержащим только конкретные информационные области, кубы и компоненты с указанными идентификаторами.

Открытие существующего запроса из роли BW

Объект авторизации	Поле	Значения
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	<i>INFO_AREA</i> **
	RSINFOCUBE	<i>INFO_CUBE</i> **
	RSZCOMPTP	REP
	RSZCOMPID	<i>COMP_ID</i> **
S_RS_COMP1	RSZCOMPID	<i>COMP_ID</i> **
	RSZCOMPTP	REP
	RSZOWNER	<i>QUERY_OWNER</i> *
	ACTVT	16

* *QUERY_OWNER* служит обозначением имени владельца запроса, из которого создается отчет. Если ввести имя владельца отчета, отчеты можно создавать только с использованием запросов для этого владельца. Введите "" для работы со всеми владельцами запросов.

** Чтобы указать для *INFO_AREA*, *INFO_CUBE* или *COMP_ID* любое значение, введите символ "". Если указать конкретное значение, можно составить отчеты по запросам, содержащим только конкретные информационные области, кубы и компоненты с указанными идентификаторами.

Предварительный просмотр или обновление отчета

Объект авторизации	Поле	Значения
S_RS_COMP	RSINFOAREA	<i>INFO_AREA</i> **
	RSINFOCUBE	<i>INFO_CUBE</i> **
	RSZCOMPTP	REP
	RSZCOMPID	<i>COMP_ID</i> **
S_RS_COMP1	RSZCOMPID	<i>COMP_ID</i> **
	RSZCOMPTP	REP
	RSZOWNER	<i>QUERY_OWNER</i> *
	ACTVT	16

* *QUERY_OWNER* служит обозначением имени владельца запроса, из которого создается отчет. Если ввести имя владельца отчета, отчеты можно создавать только с использованием запросов для этого владельца. Введите * для работы со всеми владельцами запросов.

** Чтобы указать для *INFO_AREA*, *INFO_CUBE* или *COMP_ID* любое значение, введите символ "". Если вы укажете конкретное значение, можно составить отчеты по запросам, содержащим только конкретные информационные области, кубы и компоненты с указанными идентификаторами.

Проверка базы данных (обновление определений таблицы в отчете)

Объект авторизации	Поле	Значения
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_OWNER* служит обозначением имени владельца запроса, из которого создается отчет. Если ввести имя владельца отчета, отчеты можно создавать только с использованием запросов для этого владельца. Введите "*" для работы со всеми владельцами запросов.

** Чтобы указать для *INFO_AREA*, *INFO_CUBE* или *COMP_ID* любое значение, введите символ "*". Если указать конкретное значение, можно составить отчеты по запросам, содержащим только конкретные информационные области, кубы и компоненты с указанными идентификаторами.

Настройка местоположения источника данных

Объект авторизации	Поле	Значения
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_OWNER* служит обозначением имени владельца запроса, из которого создается отчет. Если ввести имя владельца отчета, отчеты можно создавать только с использованием запросов для этого владельца. Введите "*" для работы со всеми владельцами запросов.

** Чтобы указать для *INFO_AREA*, *INFO_CUBE* или *COMP_ID* любое значение, введите символ "*". Если указать конкретное значение, можно составить отчеты по запросам, содержащим только конкретные информационные области, кубы и компоненты с указанными идентификаторами.

Сохранение отчета в роль BW

Объект авторизации	Поле	Значения
S_USER_AGR	ACT_GROUP	USER_ROLE *
	ACTVT	01, 02, 06
S_CTS_ADMI	CTS_ADMFCT	TABL

* *USER_ROLE* обозначает название любой роли, к которой принадлежит пользователь. В это поле можно ввести несколько значений.

Подготовка отчета к переводу во время сохранения в BW

Объект авторизации	Поле	Значения
S_USER_AGR	ACT_GROUP	<i>USER_ROLE</i> *
	ACTVT	01
S_CTS_ADMI	CTS_ADMFCT	TABL

* *USER_ROLE* обозначает название любой роли, к которой принадлежит пользователь. В это поле можно ввести несколько значений.

Сохранение отчета и одновременная публикация на платформе BI

Объект авторизации	Поле	Значения
S_USER_AGR	ACT_GROUP	<i>USER_ROLE</i> *
	ACTVT	01
S_CTS_ADMI	CTS_ADMFCT	TABL
S_RS_COMP	RSINFOAREA	<i>INFO_AREA</i> ***
	RSINFOCUBE	<i>INFO_CUBE</i> ***
	RSZCOMPTP	REP
	RSZCOMPID	<i>COMP_ID</i> ***

Объект авторизации	Поле	Значения
S_RS_COMP1	RSZCOMPID	COMP_ID ***
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER **
	ACTVT	16

* *USER_ROLE* обозначает название любой роли, к которой принадлежит пользователь. В это поле можно ввести несколько значений.

** *QUERY_OWNER* служит обозначением имени владельца запроса, из которого создается отчет. Если ввести имя владельца отчета, отчеты можно создавать только с использованием запросов для этого владельца. Введите "" для работы со всеми владельцами запросов.

*** Чтобы указать для *INFO_AREA*, *INFO_CUBE* или *COMP_ID* любое значение, введите символ "". Если вы укажете конкретное значение, вы сможете составить отчеты по запросам, содержащим только конкретные информационные области, кубы и компоненты с указанными идентификаторами.

Запуск BEx Query Designer

Объект авторизации	Поле	Значения
S_RS_COMP	RSINFOAREA	INFO_AREA **
	RSINFOCUBE	INFO_CUBE **
	RSZCOMPTP	REP
	RSZCOMPID	COMP_ID **

Объект авторизации	Поле	Значения
S_RS_COMP1	RSZCOMPID	COMP_ID**
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER*
	ACTVT	16
S_CTS_ADMI	CST_ADMFCT	TABL

* *QUERY_OWNER* служит обозначением имени владельца запроса, из которого создается отчет. Если ввести имя владельца отчета, отчеты можно создавать только с использованием запросов для этого владельца. Введите * для работы со всеми владельцами запросов.

** Чтобы указать для *INFO_AREA*, *INFO_CUBE* или *COMP_ID* любое значение, введите символ "***". Если вы укажете конкретное значение, вы сможете составить отчеты по запросам, содержащим только конкретные информационные области, кубы и компоненты с указанными идентификаторами.

19.1.1.19.2 Действия в стартовой панели BI

Вход на платформу BI с учетными данными SAP

Объект авторизации	Поле	Значения
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM

Просмотр отчета SAP BW по запросу

Объект авторизации	Поле	Значения
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	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* *QUERY_OWNER* служит обозначением имени владельца запроса, из которого создается отчет. Если ввести имя владельца отчета, отчеты можно создавать только с использованием запросов для этого владельца. Введите "*" для работы со всеми владельцами запросов.

** Чтобы указать для *INFO_AREA*, *INFO_CUBE* или *COMP_ID* любое значение, введите символ "*". Если указать конкретное значение, можно составить отчеты по запросам, содержащим только конкретные информационные области, кубы и компоненты с указанными идентификаторами.

Обновление отчета из средства просмотра

Объект авторизации	Поле	Значения
S_RS_COMP	RSINFOAREA	<i>INFO_AREA</i> **
	RSINFOCUBE	<i>INFO_CUBE</i> **
	RSZCOMPTP	REP
	RSZCOMPID	<i>COMP_ID</i> **
S_RS_COMP1	RSZCOMPID	<i>COMP_ID</i> **
	RSZCOMPTP	REP
	RSZOWNER	<i>QUERY_OWNER</i> *
	ACTVT	16
S_RS_ODSO	RSINFOAREA	<i>INFO_AREA</i> **
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* *QUERY_OWNER* служит обозначением имени владельца запроса, из которого создается отчет. Если ввести имя владельца отчета, отчеты можно создавать только с использованием запросов для этого владельца. Введите * для работы со всеми владельцами запросов.

** Чтобы указать для *INFO_AREA*, *INFO_CUBE* или *COMP_ID* любое значение, введите символ "***". Если вы укажете конкретное значение, вы сможете составить отчеты по запросам, содержащим только конкретные информационные области, кубы и компоненты с указанными идентификаторами.

Планирование отчета

Объект авторизации	Поле	Значения
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB, SUNI
	ACTVT	16
S_RS_COMP	RSINFOAREA	<i>INFO_AREA</i> **
	RSINFOCUBE	<i>INFO_CUBE</i> **
	RSZCOMPTP	REP
	RSZCOMPID	<i>COMP_ID</i> **
S_RS_COMP1	RSZCOMPID	<i>COMP_ID</i> **
	RSZCOMPTP	REP
	RSZOWNER	<i>QUERY_OWNER</i> *
	ACTVT	16

Объект авторизации	Поле	Значения
S_RS_ODSO	RSINFOAREA	INFO_AREA**
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* *QUERY_OWNER* служит обозначением имени владельца запроса, из которого создается отчет. Если ввести имя владельца отчета, отчеты можно создавать только с использованием запросов для этого владельца. Введите "*" для работы со всеми владельцами запросов.

** Чтобы указать для *INFO_AREA*, *INFO_CUBE* или *COMP_ID* любое значение, введите символ "*". Если указать конкретное значение, можно составить отчеты по запросам, содержащим только конкретные информационные области, кубы и компоненты с указанными идентификаторами.

Чтение динамических списков выбора в параметрах отчета

Объект авторизации	Поле	Значения
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB
	ACTVT	16

19.1.1.19.3 Действия в SAP Netweaver (ABAP)

Из Crystal Reports с помощью драйвера Open SQL

В данном разделе представлен список различных действий в SAP Netweaver (ABAP) в Crystal Reports с использованием драйвера Open SQL.

Вход на сервер SAP

Объект авторизации	Поле	Значения
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQ
	ACTVT	16

Создание нового отчета

Объект авторизации	Поле	Значения
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQ
	ACTVT	16
ZSEGREPORT	ACTVT	01

Открытие или предварительный просмотра существующего отчета

Объект авторизации	Поле	Значения
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQ
	ACTVT	16
ZSEGREPORT	ACTVT	02

Проверка базы данных (обновление определений таблицы в отчете)

Объект авторизации	Поле	Значения
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQ
	ACTVT	16

Настройка местоположения источника данных

Объект авторизации	Поле	Значения
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQ
	ACTVT	16

19.1.1.19.4 Действия в Crystal Reports с использованием драйвера InfoSet и отчеты из InfoSet

Вход на сервер SAP

Объект авторизации	Поле	Значения
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

Создание нового отчета из InfoSet в SAP Netweaver (ABAP)

Объект авторизации	Поле	Значения
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/FLAT, SKBW, AQRC
	ACTVT	16
S_CTS_ADMI	CTS_ADMFCT	TABL

Примечание:

Кроме того, добавьте достаточно прав для просмотра строк данных. Например, P_ORIG или P_APAP.

См. также

- [Настройка местоположения источника данных](#)

Проверка базы данных (обновление определений таблицы в отчете)

Объект авторизации	Поле	Значения
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM

Настройка местоположения источника данных

Объект авторизации	Поле	Значения
P_ABAP	REPID	AQTGSYSTGENERATESY, SAPDBPNP
	COARS	2

19.1.1.19.5 Действия в Crystal Reports с использованием драйвера InfoSet и отчеты из запроса ABAP*Вход на сервер SAP*

Объект авторизации	Поле	Значения
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

Создание нового отчета по запросу ABAP в SAP Netweaver

Объект авторизации	Поле	Значения
P_ABAP	REPID	AQTG02=====P6, SAPDBPNP
	COARS	2
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM
S_TABU_DIS	ACTVT	03
	GROUP	Имя группы таблиц

Проверка базы данных

Объект авторизации	Поле	Значения
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16

Настройка местоположения источника данных

Объект авторизации	Поле	Значения
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	Имя группы таблиц

19.1.1.19.6 Действия в платформе BI

Планирование отчета в диалоговом режиме (с запросом Open SQL)

Объект авторизации	Поле	Значения
S_USER_GRP	CLASS	
	ACTVT	03

Объект авторизации	Поле	Значения
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	02

Примечание:

Значением для CLASS является ПУСТО.

Планирование отчета в пакетном режиме посредством запроса Open SQL

Объект авторизации	Поле	Значения
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPENSQL, SH3A
	ACTVT	16
S_BTCH_JOB	JOBGROUP	''
	JOBACTION	RELE
ZSEGREPORT	ACTVT	02
S_BTCH_ADM	BTCADMIN	Y

Примечание:

Значением для CLASS является BLANK.

Система контроля полномочий Crystal

Объект авторизации	Поле	Значение
Авторизация для доступа к файлам (S_DATASET)	Действие (ACTVT)	Чтение, Запись (33, 34)
	Физическое имя файла (FILENAME)	* (отмечает Все)
	Название программы ABAP (PROGRAM)	*
Проверка авторизации для доступа к RFC (S_RFC)	Действие (ACTVT)	16
	Имя защищаемого RFC (RFC_NAME)	BDCH, STPA, SUSO, SUUS, SU_USER, SYST, SUNI, PRGN_J2EE, /CRYSTAL/SECURITY
	Тип защищаемого объекта RFC (RFC_TYPE)	Группа функций (FUGR)
Поддержка основной записи пользователя: Группы пользователей (S_USER_GRP)	Действие (ACTVT)	Создать или сгенерировать, затем отобразить (03)
	Группа пользователей на экране поддержки основной записи пользователя (CLASS)	<p>*</p> <p>Примечание: В целях повышения безопасности можно непосредственно перечислить группы пользователей, членам которых необходим доступ к платформе BI.</p>

19.2 Настройка для интеграции с JD Edwards

19.2.1 Настройка единого входа (SSO) для SAP Crystal Reports

По умолчанию в параметрах платформы BI пользователям SAP Crystal Reports будет разрешен доступ к данным JD Edwards EnterpriseOne с использованием функции единого входа (SSO).

19.2.1.1 Отключение единого входа для JD Edwards и SAP Crystal Reports

1. В приложении Central Management Console (CMC) выберите элемент **Приложения**.
2. Дважды щелкните элемент **Конфигурация Crystal Reports**.
3. Выберите элемент **Параметры единой регистрации в системе**.
4. Выберите **crdb_pseone**.
5. Нажмите кнопку **Удалить**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. Перезапустите SAP Crystal Reports.

19.2.1.2 Активация единого входа для JD Edwards и SAP Crystal Reports

Если функция единого входа для JD Edwards и SAP Crystal Reports отключена, и требуется повторно активировать ее.

1. В приложении Central Management Console (CMC) выберите элемент **Приложения**.
2. Дважды щелкните элемент **Конфигурация Crystal Reports**.
3. Выберите элемент **Параметры единой регистрации в системе**.
4. В области «Использовать для входа в базу данных контекст SSO» введите **crdb_pseone**.
5. Нажмите кнопку **Добавить**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. Перезапустите сервер Crystal Reports.

19.2.2 Настройка протокола SSL для интеграции с JD Edwards

Можно использовать протокол SSL для сетевого обмена данными между клиентами и серверами в развертывании платформы BI и развертывании JD Edwards EnterpriseOne.

Для работы с данными JD Edwards EnterpriseOne в платформе BI требуется внести некоторые изменения в конфигурацию SSL. Как и в случае настройки SSL для других серверов и клиентов платформы BI, сохраните следующий ключ и файлы сертификатов в безопасном месте (в одном каталоге), доступ к которому возможен с компьютеров в развертывании платформы BI.

- Файл доверенного сертификата (cacert.der).
- Сгенерированный файл сертификата сервера (servercert.der).
- Файл ключа сервера (server.key).
- Файл парольной фразы (passphrase.txt).

19.2.2.1 Включение соединений с данными JD Edwards EnterpriseOne по протоколу SSL

Примечание:

Для всех значений, описанных в следующей процедуре, учитывается регистр.

- Настройте два параметра реестра в следующем разделе.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Business  
Objects\Suite 12.0\Integration Kit for  
PeopleSoft EnterpriseOne\QRY\Instances\noname]  
"CommunicationProtocol"="ssl"  
"SSL Configuration File"="C:\Program  
Files\Business Objects\BusinessObjects XI 13.0\sslconf.properties"
```

Чтобы эти изменения вступили в силу, необходимо перезапустить службы отчетов платформы BI (например, сервер заданий Crystal Reports).

19.2.2.2 Файл свойств конфигурации SSL

Файл свойств `sslconf.properties` содержит все сведения для обязательных сертификатов, используемых в платформе BI. Например:

```
[default]  
businessobjects.orb.oci.protocol=ssl  
certDir=d:/ssl  
trustedCert=cacert.der
```

```
sslCert=servercert.der  
sslKey=server.key  
passphrase=passphrase.txt
```

Файл `sslconf.properties` следует поместить в папку, в которой установлена платформа BI. По умолчанию это папка `C:\Program Files\Business Objects\BusinessObjects 13.0`.

19.3 Настройка для интеграции с PeopleSoft Enterprise

19.3.1 Настройка единого входа (SSO) для SAP Crystal Reports и PeopleSoft Enterprise

По умолчанию в параметрах платформы BI пользователям SAP Crystal Reports будет разрешен доступ к данным PeopleSoft Enterprise с использованием функции единого входа (SSO).

19.3.1.1 Отключение единого входа для PeopleSoft Enterprise и SAP Crystal Reports

1. В приложении Central Management Console (CMC) выберите элемент **Приложения**.
2. Дважды щелкните элемент **Конфигурация Crystal Reports**.
3. Выберите элемент **Параметры единой регистрации в системе**.
4. Выберите **crdb_psenterprise**.
5. Нажмите кнопку **Удалить**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. Перезапустите SAP Crystal Reports.

19.3.1.2 Активация единого входа для PeopleSoft Enterprise и SAP Crystal Reports

Если функция единого входа для PeopleSoft Enterprise и SAP Crystal Reports отключена и требуется повторно активировать ее.

1. В приложении Central Management Console (CMC) выберите элемент **Приложения**.
2. Дважды щелкните элемент **Конфигурация Crystal Reports**.
3. Выберите элемент **Параметры единой регистрации в системе**.
4. В области «Использовать для входа в базу данных контекст SSO...» введите **crdb_psenprise**.
5. Нажмите кнопку **Добавить**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. Перезапустите SAP Crystal Reports.

19.3.2 Настройка соединений по протоколу SSL

Можно использовать протокол SSL для сетевого обмена данными между клиентами и серверами в вашем развертывании платформы BI.

Как и в случае настройки SSL для других серверов и клиентов платформы BI, сохраните следующий ключ и файлы сертификатов в безопасном месте (в одном каталоге), доступ к которому возможен с компьютеров в развертывании платформы BI.

- Файл доверенного сертификата (cacert.der).
- Сгенерированный файл сертификата сервера (servercert.der).
- Файл ключа сервера (server.key).
- Файл парольной фразы (passphrase.txt).

19.3.2.1 Файл свойств конфигурации SSL

Файл свойств `sslconf.properties` содержит все сведения для обязательных сертификатов, используемых компонентами платформы SAP BI. Например:

```
[default]
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

Файл `sslconf.properties` необходимо поместить в папку, в которой установлен продукт платформы BI для PeopleSoft. По умолчанию это папка `C:\Program Files\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\`.

19.3.2.2 Включение поддержки SSL для сервера запросов PeopleSoft

Примечание:

Для всех значений, описанных в следующей процедуре, учитывается регистр.

- Настройте два значения реестра в одном ключе реестра для каждого сервера регистрации, например:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Business
Objects\Suite 12.0\Integration Kit for
PeopleSoft\QRY\Instances\noname]
"CommunicationProtocol"="ssl"
"SSL Configuration File"="C:\Program
Files\Business Objects\BusinessObjects 12.0 Integration Kit for
PeopleSoft\sslconf.properties"
```

Чтобы эти изменения вступили в силу, необходимо перезапустить серверы отчетов BusinessObjects (например, сервер заданий Crystal Reports).

19.3.2.3 Включение моста безопасности с SSL

Примечание:

Для всех значений, описанных в следующей процедуре, учитывается регистр.

- Запустите `crpsepmsecuritybridge.bat` со следующими аргументами, добавив их в файл `.bat`.

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir="d:\ssl"
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
```

Убедитесь, что аргументы добавлены в правильное место в файле `.bat`, сразу после `java.exe` и перед указанием аргументов `jar`. Например:

```
@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\epm;
"C:\Program Files\Business Objects\javasdk\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\epm\crpsepmsecuritybridge.jar" %1 "language"
"C:\Program Files\Business
Objects\LanguagePacks.xml\LanguagePacks.xml"
```

В следующей таблице приводятся описания, соответствующие этим примерам:

DcertDir=d:\ssl	Каталог для хранения всех сертификатов и ключей.
DtrustedCert=cacert.der	Файл доверенного сертификата. При указании более одного файла разделите их точкой с запятой.
DsslCert=clientcert.der	Сертификат, используемый SDK.
DsslKey=client.key	Секретный ключ сертификата SDK.
Dpassphrase=passphrase.txt	Файл для хранения парольной фразы секретного ключа.

19.3.3 Настройка производительности для систем PeopleSoft

Для обеспечения оптимальной производительности при составлении отчетов на основе запросов PeopleSoft важно понимать, как выполняются запросы в Crystal Reports и на платформе BI.

При каждом обновлении или выполнении отчета, основанного на запросе PeopleSoft, устанавливается соединение с сервером PeopleSoft:

- В средах PeopleSoft Enterprise (PeopleTools 8.46 и более поздних версий) устанавливается соединение с сервером аналитики PeopleSoft.
- В средах PeopleSoft Enterprise (PeopleTools 8.21-8.45) устанавливается соединение с сервером приложений PeopleSoft.

19.3.3.1 Рекомендации

При оптимальном развертывании один или несколько серверов аналитики или приложений PeopleSoft настроены исключительно для обработки запросов на отчет. На каждом из данных серверов настройки минимального и максимального количества экземпляров определяют количество запросов от отчетов, которые можно обрабатывать одновременно. Данная настройка предоставляет следующие преимущества:

- Отсутствие конкуренции за ресурсы между запросами отчетов и другими запросами на транзакции, выполняемые сервером PeopleSoft.
- Можно осуществлять ремонтные работы на сервере, который обрабатывает запросы на отчет, не отключая сервер, который обрабатывает запросы на транзакции.

В среде, где запросы на транзакции и запросы отчетов обрабатываются одним сервером аналитики или сервером приложений PeopleSoft, необходимо настроить платформу BI таким образом, чтобы не выполнялось более одного отчета одновременно. В обратном случае пользователи не смогут посылать запросы на транзакции, если все процессы PSANALYTICSRV или PSAPPSRV используются для выполнения отчетов.

Примечание:

- Подробную информацию по ограничению количества заданий запланированных отчетов и заданий просмотра отчетов по требованию см. в разделе "Настройка и конфигурирование серверов" в *Руководстве администратора платформы SAP BusinessObjects Business Intelligence*.
- Систему невозможно для ограничения количества пользователей Crystal Reports, которые могут пытаться получить доступ к серверу одновременно.

Если производительность сервера оказывается недостаточной, определите при помощи средства настройки Psadmin, находятся ли в очереди запросы. Кроме того, можно отслеживать системные ресурсы на компьютере, поддерживающем сервер аналитики или сервер приложений PeopleSoft. Если из-за нехватки физической памяти используется виртуальная память, обработка также может выполняться медленнее.

19.3.3.2 Серверы PeopleSoft

На сервере аналитики PeopleSoft отчеты обновляются и выполняются процессом PSANALYTICSRV. На сервере приложений PeopleSoft отчеты обновляются и выполняются процессом PSAPPSRV. Количество процессов PSANALYTICSRV или PSAPPSRV определяет количество отчетов, которые можно выполнять одновременно.

Типичный файл конфигурации сервера приложений или сервера аналитики PeopleSoft содержит следующую информацию:

```
Min Instances=3
Max Instances=5
```

В данном примере в любое время доступно не менее трех процессов PSANALYTICSRV или PSAPPSRV с возможностью увеличивать количество процессов до пяти. Это не обязательно означает, что пять отчетов можно всегда выполнять одновременно; процессы также могут использоваться для обработки других задач в системе. При отсутствии процессов PSANALYTICSRV/PSAPPSRV для обработки запроса выполняется помещение запроса в очередь до тех пор, пока процесс не станет доступным.

Примечание:

Файл конфигурации для сервера приложений PeopleSoft также обычно содержит параметр Service Timeout, который определяет время ожидания доступного процесса запросом в

очереди. Если в указанный для параметра период не будет доступных процессов, то запрос отменяется по причине истечения времени ожидания.

19.4 Настройка для интеграции с Siebel

19.4.1 Настройка Siebel для интеграции с платформой SAP BusinessObjects Business Intelligence

Интеграция с платформой BI обеспечивает связь с Crystal Reports, что позволяет пользователям внедрять содержимое пакета BusinessObjects Business Intelligence в приложение Siebel. После установки и настройки с помощью нового меню пользователи смогут запускать приложение InfoView прямо из приложения Siebel.

По умолчанию необходимые файлы устанавливаются в папку C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\siebel\Siebel Files\.

Примечание:

Во вложенных папках Siebel 7.7 и Siebel 8.0 содержатся разные файлы для версий Siebel 7.7 и 8.0.

19.4.1.1 Импорт проекта интеграции с Siebel для платформы BI

1. Запустите инструменты Siebel.
2. Выберите команды **Сервис > Импортировать из архива**.
3. При появлении запроса на ввод файла архива перейдите в папку файлов Siebel в установке продукта Integration.
По умолчанию это папка <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Samples\siebel\Siebel Files\.
4. Перейдите в соответствующую вложенную папку (Siebel 7.7 или Siebel 8.0) и выберите файл BusinessObjectsEnterprise.sif.
Открывается окно мастера импорта.
5. Выберите параметр **Объединить определение объекта из файла архива с определением в репозитории**.

6. Выполните выводимые на экран инструкции мастера, чтобы завершить импорт проекта интеграции.
Проект интеграции добавляется в репозиторий.
7. Щелкните проект **SAP BusinessObjects Integration**.

19.4.2 Создание пункта меню "Crystal Reports"

1. В Siebel Tools найдите проект **Меню**.
2. В проводнике объектов выберите объект **Пункт меню**.

Примечание:

Если в проводнике объектов отсутствует объект меню, выберите команды **Вид > Параметры** в Siebel Tools, откройте вкладку **Проводник объектов** и выберите объект **Меню**.

3. В списке **Меню** выберите меню **Универсальный веб**.
4. Щелкните заголовок списка **Пункты меню**.
5. Выберите команды **Изменить > Новая запись**.
6. Соответствующим образом определите новый пункт меню. Рекомендованные значения:
 - Имя: View – Crystal Reports
 - Заголовок: Crystal Reports
 - Команда: Crystal Reports
 - Комментарии: меню интегрированных отчетов платформы BI
 - Неактивно: False
7. Задайте номер позиции, определяющий положение нового пункта меню в меню "Вид".
Чтобы упростить выбор номера позиции, отсортируйте пункты меню по позиции.
8. Теперь можно добавить записи региональных параметров, чтобы локализовать заголовок соответствующим образом.

Повторно откомпилируйте приложение Siebel. См. раздел [Повторная компиляция приложения Siebel](#).

19.4.2.1 Повторная компиляция приложения Siebel

После установки платформы BI и предоставления пользователям доступа к ней при помощи пункта меню Siebel необходимо повторно откомпилировать приложение Siebel с помощью обычных процедур. Для получения подробных сведений см. Siebel Bookshelf.

После повторной компиляции приложения Siebel воссоздайте его файлы JavaScript. В Siebel 7.7 и более поздних версиях можно автоматически воссоздать файлы JavaScript в рамках процесса повторной компиляции.

Поскольку действия, требуемые для компиляции репозитория Siebel, выполняются на рабочей станции Siebel Tools, необходимо развернуть результирующие файлы JavaScript с рабочей станции Siebel Tools на своем сервере Siebel Server. Как правило, созданные файлы JavaScript находятся в следующем местоположении (зависит от места установки Siebel):

```
C:\sea77\tools\PUBLIC\ENU\srf1096416329_444
```

Имя папки примера `srf1096416329_444` создается Siebel Tools и уникальным образом соответствует результирующему файлу репозитория.

Файлы JavaScript должны быть развернуты на сервере Siebel Server, как правило, в следующем местоположении (зависит от места установки Siebel):

```
C:\sea77\SWEApp\PUBLIC\ENU\srf1096416329_444
```

Убедитесь, что имя папки, созданное Siebel Tools, останется неизменным.

В дополнение к этому для обеспечения обслуживания необходимо обновить файл конфигурации Siebel на компьютере сервера Siebel Server. Найдите соответствующий файл конфигурации на своем компьютере Siebel Server. Например, при выполнении англоязычной версии Siebel Call Center следует использовать файл `uagent.cfg`. По умолчанию для Siebel 7.7 этот файл находится по адресу `C:\sea77\siebsrvr\bin\ENU\uagent.cfg`.

Добавьте в конец раздела SWE файла конфигурации следующую строку:

```
ClientBusinessServiceNUMBER = BusinessObjects Integration Service
```

Номера `ClientBusinessService` являются последовательными. Если в разделе SWE отсутствуют другие службы `ClientBusinessServices`, задайте для параметра `NUMBER` значение 0. В обратном случае задайте для параметра `NUMBER` следующее по величине значение.

Для Siebel 8.x или более поздней версии:

1. Войдите в Siebel Tools и найдите в проводнике объектов объект приложения **Siebel Universal Agent**.
2. Разверните объекты приложений, чтобы получить доступ к объекту **Application User Prop**.
3. Создайте новую запись каждой из подлежащих объявлению бизнес-служб. Для этого укажите значения свойств "Имя" и "Значение" следующим образом:
 - Имя = `ClientBusinessServiceX`
 - Значение = `BusinessObjects Integration`

Теперь требуется создать пункт меню "Crystal Reports", который будет вызывать импортированную команду Siebel.

19.4.3 Контекстуальная зависимость

Контекстуальная зависимость – это функция, которая предоставляет пользователю доступ к отчетам, которые, скорее всего, имеют отношение к его текущей задаче. В этом случае пользователи, обращающиеся к отчетам Crystal Reports непосредственно из клиентского приложения Siebel, автоматически получают отчеты, созданные с использованием данных Siebel.

19.4.3.1 Настройка контекстуальной зависимости

Перед настройкой следует удостовериться, что выполнены следующие действия.

- установлен продукт Siebel Integration
 - Настройка Siebel для интеграции с платформой BI
1. Откройте консоль Central Management Console (CMC) для платформы BI.
 2. Нажмите кнопку **Аутентификация**.
 3. Дважды щелкните **Siebel**.
Откроется интерфейс сопоставления Siebel.
 4. Щелкните **Домены**.
Откроется интерфейс сопоставления доменов.
 5. Запишите или запомните доменное имя, соответствующее серверу Siebel, который планируется использовать.
 6. Закройте интерфейс соответствия Siebel.
 7. Откройте стартовую панель BI.
 8. Создайте в CMC новую папку по адресу `PublicFolders\Siebel` с именем домена Siebel.
 9. Поместите в эту папку все отчеты, которые должны содержать данные Siebel.

19.4.3.2 Установка URL-адреса для контекстуальной зависимости

1. После воссоздания файлов JavaScript приложения перейдите в папку Siebel Files установленной платформы BI (по умолчанию `C:\Program Files\Business Objects\SAP BusinessObjects Enterprise XI\Siebel Files\`).
2. Скопируйте файл `BusinessObjectsEnterpriseServer.html`. Найдите общую папку, в которой программа `genbscript` создала новые файлы JavaScript, и поместите копию файла `BusinessObjectsEnterpriseServer.html` во вложенную папку соответствующего языка.
Например, если файлы JavaScript были созданы в папке `c:\sea752\SWEApp\PUBLIC\ENU` на сервере Siebel, скопируйте файл `BusinessObjectsEnterpriseServer.html` в папку `c:\sea752\SWEApp\PUBLIC\ENU`.
3. Откройте файл `BusinessObjectsEnterpriseServer.html`, находящийся в общей папке, в текстовом редакторе, например Блокноте, и найдите следующую строку:

```
Var userDomain = "SIEB78"  
  
var destAddr = "http://<SAP BusinessObjects  
server>:8080/BOE/BI/logon/siebelStart.do"
```

Примечание:

- При изменении переменной *userDomain* или *destAddr* необходимо очистить кэшированные веб-страницы браузера, чтобы гарантировать, что браузер будет использовать верный целевой адрес.
- Значение переменной "userDomain" является чувствительным к регистру.

19.4.3.3 Проверка контекстуальной зависимости

1. Войдите в приложение Siebel, где используется измененное меню "Универсальный веб".
2. Перейдите на любой экран и откройте меню **Вид**.
В меню должен отображаться новый пункт "Crystal Reports".

3. Выберите команду **Crystal Reports**.

На платформе BI будет открыто окно стартовой панели BI с запросом имени пользователя и пароля для подключения (требуется только при первом входе до истечения срока действия сеанса работы). Должны быть указаны настроенное доменное имя в виде HTML и аутентификация для Siebel.

Примечание:

Это действие служит для проверки установки только для данного момента. Нельзя войти в платформу BI с использованием аутентификации Siebel, пока полномочия Siebel не сопоставлены платформе BI.

19.4.3.4 Добавление папок к платформе BI

Для полноценного включения функции контекстуальной зависимости при интеграции платформы BI с Siebel требуется добавить ряд папок на стартовую панель BI.

Для правильной работы контекстуальной папки она должна иметь следующую структуру: *Корневой каталог\Siebel\Доменное имя*. В рамках функции контекстуальной зависимости отображаются только отчеты, хранящиеся во вложенной папке *Доменное имя*, для которых в системе Siebel настроена связь с конкретным бизнес-компонентом Business Objects. Используемое здесь значение *Доменное имя* должно совпадать с доменным именем, настроенным для Siebel в параметрах конфигурации аутентификации, а также со значением, настроенным в файле *BusinessObjectsEnterpriseServer.html* на стороне Siebel.

Примечание:

Для выполнения действий в этом разделе требуется инструментарий Siebel Tools.

19.4.4 Настройка единого входа (SSO) для SAP Crystal Reports и Siebel

По умолчанию в параметрах платформы BI пользователям SAP Crystal Reports будет разрешен доступ к данным Siebel с использованием функции единого входа (SSO).

19.4.4.1 Отключение единого входа для Siebel и Crystal Reports

1. В приложении Central Management Console (CMC) выберите элемент **Приложения**.
2. Дважды щелкните элемент **Конфигурация Crystal Reports**.
3. Выберите элемент **Параметры единой регистрации в системе**.
4. Выберите **crdb_siebel**.
5. Нажмите кнопку **Удалить**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. Перезапустите SAP Crystal Reports.

19.4.4.2 Активация единого входа для Siebel и SAP Crystal Reports

Если функция единого входа для Siebel и SAP Crystal Reports отключена и требуется повторно активировать ее.

1. В приложении Central Management Console (CMC) выберите элемент **Приложения**.
2. Дважды щелкните элемент **Конфигурация Crystal Reports**.
3. Выберите элемент **Параметры единой регистрации в системе**.
4. В области «Использовать для входа в базу данных контекст SSO...» введите **crdb_siebel**.
5. Нажмите кнопку **Добавить**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. Перезапустите серверы SAP Crystal Reports.

19.4.5 Настройка соединений по протоколу SSL

Можно использовать протокол SSL для сетевого обмена данными между клиентами и серверами в ваших развертываниях Siebel и платформы BI.

Как и в случае настройки SSL для других серверов и клиентов платформы BI, сохраните следующий ключ и файлы сертификатов в безопасном месте (в одном каталоге), доступ к которому возможен с компьютеров в развертывании Siebel.

- Файл доверенного сертификата (cacert.der).
- Сгенерированный файл сертификата сервера (servercert.der).
- Файл ключа сервера (server.key).
- Файл парольной фразы (passphrase.txt).

Файл свойств конфигурации SSL

Файл свойств `sslconf.properties` содержит все информацию для необходимых сертификатов и ключей, используемых BusinessObjects XI Integration для компонентов Siebel. Например:

```
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

Файл `sslconf.properties` необходимо поместить в папку, в которой установлен продукт платформы BI. По умолчанию это папка `C:\Program Files\Business Objects\SAP BusinessObjects Enterprise XI\`.

Управление журналами и их настройка

20.1 Ведение журнала трассировок компонентов

Трассировка позволяет администраторам системы и обслуживающему персоналу отслеживать производительность компонентов платформы BI (серверов и веб-приложений), а также операции, выполняющиеся в отслеживаемых компонентах.

Сообщения уровня системы, выдаваемые серверами платформы BI, отслеживаются и записываются в файлах журналов. Эти файлы журнала используются системными администраторами для мониторинга производительности или в целях отладки. Трассировка – это запись событий, происходящих во время работы отслеживаемого компонента. Трассированные события находятся в диапазоне от серьезных ошибок-исключений до простых сообщений состояния.

Журнал трассировок

Сообщения трассировки помещаются в файлы журнала, которые сохраняются в формате универсального файла журнала (`.glf`). При установке уровня журнала трассировки для компонента определяется тип и детальность информации, отправляемой в файл журнала. Уровень журнала трассировки фактически представляет собой фильтр, который подавляет трассировку ниже указанного уровня важности. Подавленные трассировки не записываются в выходной файл журнала. С помощью мониторинга журнала трассировки компонента можно определить, следует ли изменять текущий экземпляр компонента или же его конфигурацию для обработки увеличенной нагрузки, а так же имеет ли увеличенная нагрузка сколько-нибудь значимое влияние на производительность.

20.2 Уровни журнала трассировки

В следующей таблице описаны доступные уровни журнала трассировки для компонентов платформы BI:

Уровень	Описание
Не определен	Уровень журнала трассировки устанавливается с использованием другого механизма, обычно файла <code>.ini</code> .
Нет	<p>Если для журнала трассировки установлен уровень «Нет», фильтр дополнительного подавления трассировки ниже заданного уровня важности отключен.</p> <p>Примечание: Уровень журнала трассировки «Нет» не означает отключения функции трассировки. Отслеживание системных ресурсов продолжается, а трассировки будут протоколироваться для редких критических событий, таких как нарушения утверждений.</p>
Низкий	<p>Фильтр журнала трассировки настроен на регистрацию сообщений об ошибках и пропуск предупреждений и большинства сообщений о статусе. Тем не менее, будут регистрироваться очень важные сообщения о статусе запуска компонента, завершения работы, а также сообщения о начале и завершении запроса.</p> <p>Примечание: Этот уровень не рекомендуется для целей отладки.</p>
Средний	<p>Фильтр журнала трассировки настроен на включение сообщений об ошибках, предупреждениях и большинства сообщений о статусе в выходной файл журнала. Менее важные или очень подробные сообщения о статусе отфильтровываются. Этот уровень не достаточно детальный для использования в целях отладки.</p>
Высокий	<p>Никакие сообщения не исключаются фильтром. Этот уровень рекомендуется для использования в целях отладки.</p> <p>Примечание: «Высокий» уровень трассировки в журнале может отрицательно отразиться на системных ресурсах. Он может увеличить загрузку ЦП и памяти в файловой системе.</p>

20.3 Настройка трассировки для серверов

Трассировки для отслеживаемого сервера платформы BI записываются в специальный файл журнала (`.glf`) и хранятся в папке или каталоге ведения журнала. На платформах Windows каталог ведения журналов по умолчанию расположен в папке Program Files `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging`. В системах Unix каталог расположен в папке: `<INSTALLDIR>/sap_bobj/logging`.

Примечание:

Файл .glf форматируется как комбинация краткого идентификатора, имени сервера и числовой ссылки, например `aps_mysia.AdaptiveProcessingServer_trace.000012.glf`. Для наблюдаемого сервера создается новый файл журнала трассировки, как только размер старого файла достигает порога в 1 мегабайт.

Администраторы могут калибровать критичность и важность трассировок, собранных в файле журнала, путем задания уровня журнала трассировки для конкретных серверов или коллекции серверов. Уровень журнала трассировки можно изменять при помощи следующих рекомендуемых методов:

- Использование «службы TraceLog» для конкретного сервера или группы серверов в Central Management Console (CMC)
- Вручную изменить уровень журнала трассировки и другие параметры в файле `BO_trace.ini`.

Если нужно изменить уровень журнала трассировки только для конкретных серверов, в CMC рекомендуется использовать «Службу TraceLog». Чтобы изменить остальные параметры трассировки необходимо повторно настроить файл `BO_trace.ini`.

20.3.1 Настройка уровня журнала трассировки сервера в CMC

Уровень журнала трассировки для сервера можно отрегулировать, не затрагивая других параметров трассировки. Следуйте инструкциям, указанным ниже, чтобы отрегулировать уровень журнала трассировки.

1. Перейдите в область управления «Серверы» в CMC.
2. Доступ к серверам, уровень журнала трассировки которых следует изменить.
 - a. Выберите категорию сервера, чтобы получить доступ к одному или нескольким серверам из конкретной «категории» серверов.
 - b. Щелкните **Список серверов** в области навигации, чтобы получить доступ к полному списку серверов.
3. Щелкните сервер правой кнопкой мыши и выберите команду **Свойства**.
Откроется диалоговое окно «Свойства».
4. В области «Служба журналов трассировки» выберите нужный параметр в раскрывающемся списке «Уровень журнала».
5. Нажмите кнопку **Сохранить и закрыть**, чтобы применить измененный уровень журнала трассировки.

Новый уровень журнала трассировки вступит в силу в течение непродолжительного времени.

Чтобы указать другой каталог для файлов журнала используйте параметр `-loggingPath` вместе с путем к конечному каталогу в области «Параметры командной строки». Это изменение не вступит в силу до перезапуска сервера.

См. также

- [Уровни журнала трассировки](#)

20.3.2 Установка уровня журнала трассировки для нескольких серверов, управляемых в СМС

1. Перейдите в область управления «Серверы» в СМС.
Доступные категории служб отображаются на странице «Серверы».
2. Доступ к серверам, чей уровень журнала трассировки нужно сбросить.
 - a. Выберите категорию сервера, чтобы получить доступ к одному или нескольким серверам из конкретной категории.
 - b. Щелкните **Список серверов** в навигационной панели, чтобы получить доступ к полному списку серверов.
3. Выберите серверы.
Для выбора нескольких серверов удерживайте нажатой клавишу **Ctrl** при выборе элементов.
4. Правой кнопкой мыши щелкните **Изменить общие службы**.
Отобразится экран «Изменить общие службы».
5. В области «Служба журналов трассировки» выберите нужный параметр в раскрывающемся списке «Уровень журнала».
6. Нажмите кнопку **ОК**, чтобы отправить измененный уровень журнала трассировки.

Новый уровень журнала трассировки вступит в силу в течение непродолжительного времени.

Чтобы указать другой каталог для файлов журнала используйте параметр `-loggingPath` вместе с путем к конечному каталогу в области «Параметры командной строки». Это изменение не вступит в силу до перезапуска серверов.

См. также

- [Уровни журнала трассировки](#)

20.3.3 Настройка серверной трассировки с использованием файла **BO_trace.ini**

Чтение файла `BO_trace.ini` выполняется ежеминутно, по умолчанию в нем настроено отключение трассировки. Чтобы активировать и настроить трассировку с использованием файла `BO_trace.ini`, выполните следующие шаги:

1. Откройте файл `BO_trace.ini`.

- Расположение по умолчанию на Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf/.
 - Расположение по умолчанию на UNIX:
<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/.
2. Удалите комментарии обязательных строк в разделе «Trace Syntax and Setting» (Синтаксис и параметр трассировки).
 3. Измените параметры серверной трассировки подходящим образом.
В таблице ниже перечислены общие параметры, требуемые для настройки трассировки сервера.

Параметр	Возможные значения	Описание
active	false, true	При значении true будут трассироваться сообщения трассировки, достигшие порогового значения, которое установлено в параметре importance. При значении false трассировка сообщений по уровню важности не ведется. Значением по умолчанию является false.
importance	'<<', '<=', '==', '>=', '>>', xs, s, m, l, xl Примечание: importance = xs или importance = << – наиболее подробные варианты. Минимальные варианты – importance = xl или importance = >>.	Задаёт порог для сообщений трассировки. Будет выполняться трассировка сообщений, превышающих пороговое значение. Значением по умолчанию является m (среднее).
предупреждение	false, true	При значении true будут трассироваться сообщения трассировки, достигшие порогового значения, которое установлено в параметре severity. При значении false трассировка сообщений по уровню серьезности не ведется. Значением по умолчанию является true.
severity	', 'W', 'E', 'A', success, warning, error, assert	Определяет пороговое значение важности, за пределами которого можно выполнить трассировку сообщений. Значением по умолчанию является 'E'.
size	Возможными значениями являются целые числа ≥ 1000	Задаёт число сообщений в файле журнала трассировки, по достижении которого будет создан новый журнал. Значением по умолчанию является 100000.
keep_num	Возможными значениями являются целые числа ≥ 1000	Указывает число ведущихся журналов.

Параметр	Возможные значения	Описание
administrator	Строки или целые числа	Определяет комментарий, который необходимо использовать в выходном файле журнала. Например, если <pre>administrator = "hello"</pre> эта строка вставлена в файл журнала.
log_dir		Задаёт каталог выходного файла журнала. По умолчанию файлы журналов сохраняются в каталоге Logging.
always_close	on, off	Определяет необходимость закрытия файла журнала после записи трассировки в файл журнала. Значением по умолчанию является off.

4. Сохраните и закройте файл BO_trace.ini.

Новые параметры вступят в силу только после перезапуска всех затронутых серверов.

Пример:

```
active=false;
severity='E';
importance='==';
size=1000000;
keep_num=437;
```

20.3.3.1 Настройка трассировки по серверам

Файл BO_trace.ini используется для указания параметров трассировки для серверов платформы BI. Параметры затрагивают все управляемые серверы. Администраторы могут использовать файл BO_trace.ini, чтобы задавать конкретные параметры трассировки для конкретных серверов.

1. Откройте файл BO_trace.ini.

- Расположение по умолчанию на Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf/.
- Расположение по умолчанию на UNIX:
<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/.

2. Удалите комментарии обязательных строк в разделе «Trace Syntax and Setting» (Синтаксис и параметр трассировки).
3. Чтобы задать параметры трассировки для конкретного сервера используйте оператор IF, как показано в примере ниже:

```
if (process == "aps_MySIA.ProcessingServer")
{
    active = true;
    importance = '<<' ;
    alert = true;
    severity = ' ';
    keep_num = 487;
    size = 100 * 1000;
}
```

4. Сохраните и закройте файл BO_trace.ini.

Измененные параметры будут реализованы в соответствии с журналом. Новые параметры переопределяют уровень журнала трассировки, заданный в СМС для конкретного сервера.

20.4 Настройка трассировки для веб-приложений

Трассировки для отслеживаемого сервера платформы BI записываются в специальный файл журнала (.glf) и хранятся в папке на компьютере, где размещена папка веб-приложений. Файлы журнала трассировки по умолчанию будут расположены в следующей папке:

\$userHome/SBOPWebapp_\$application_\$IPaddress_\$port/

Администраторы могут калибровать критичность и важность трассировок, собранных в файле журнала, путем задания уровня журнала трассировки для конкретных веб-приложений или коллекции веб-приложений. Уровень журнала трассировки можно изменять при помощи следующих рекомендуемых методов:

- Использование параметров приложения «Журнал трассировки» в консоли СМС
- Вручную заново настройте уровень журнала трассировки и другие параметры трассировки в файле BO_trace.ini. Этот файл развертывается вместе с WAR-файлами BOE и dswebobje на сервере веб-приложений.

Чтобы изменить только уровень журнала трассировки для веб-приложения BOE, настоятельно рекомендуется использовать параметр СМС. Чтобы изменить все параметры трассировки, необходимо повторно настроить файл BO_trace.ini.

Примечание:

Перед изменением конфигурации файла BO_trace.ini необходимо воспользоваться средством WDeploy, чтобы отменить развертывание существующих веб-приложений с сервера веб-приложений. После повторной конфигурации BO_trace.ini его нужно повторно развернуть вместе с веб-приложениями на сервере веб-приложений. Для получения дополнительных сведений об использовании WDeploy для подготовки, развертывания и отмены развертывания веб-приложений см. *Руководство по развертыванию веб-приложений платформы SAP BusinessObjects Business Intelligence*.

20.4.1 Настройка уровня журнала трассировки веб-приложения в СМС

По умолчанию для уровня журнала трассировки для веб-приложений в СМС установлено значение «Не определен». Настройки журнала трассировки доступны для следующих приложений в СМС:

- Central Management Console
- Стартовая панель BI
- Открыть документ
- Веб-служба

Для трассировки всех остальных веб-приложений следует использовать метод настройки вручную соответствующего файла `BO_Trace`.

1. Перейдите в область управления «Приложения» в СМС.
Будет открыто диалоговое окно «Приложения».
2. Щелкните приложение правой кнопкой мыши и выберите команду **Настройки журнала трассировки**.
Будет открыто диалоговое окно «Настройки журнала трассировки».
3. Выберите нужный параметр в раскрывающемся списке **Уровень журнала**.
4. Нажмите кнопку **Сохранить и закрыть**, чтобы применить уровень журнала трассировки.

Новый уровень журнала трассировки вступит в силу после следующего входа в данное веб-приложение.

См. также

- [Уровни журнала трассировки](#)

20.4.2 Изменение параметров трассировки вручную при помощи файла `BO_trace.ini`

Файл `BO_trace.ini` развертывается вместе с WAR-файлами `BOE` и `dswsbobje` на сервере веб-приложений. Этот файл не всегда доступен на сервере веб-приложений. Необходимо предпринять следующий предварительный шаг. Для затронутого веб-приложения должно быть отменено развертывание на сервере веб-приложений.

1. При помощи WDeploy отмените развертывание веб-приложения с сервера веб-приложений. Для получения дополнительных сведений об использовании WDeploy для отмены развертывания веб-приложений см. *Руководство по развертыванию веб-приложений платформы SAP BusinessObjects Business Intelligence*.

Примечание:

Если используется сервер веб-приложения Tomcat, предоставленный вместе с установкой платформы BI, файл `BO_trace.ini` становится доступным в следующем каталоге. Не требуется отменять развертывание веб-приложений и изменять файл напрямую.

- Файл конфигурации трассировки для файла `BOE.war` доступен в каталоге `<INSTALLDIR>\Tomcat6\webapps\BOE\WEB-INF\TraceLog`.
- Файл конфигурации трассировки для файла `dswebobje.war` доступен в каталоге `<INSTALLDIR>\Tomcat6\webapps\dswebobje\WEB-INF\conf`.

Если используется связанный сервер веб-приложения Tomcat, перейдите к шагу 3.

2. Перейдите к предварительно развернутой версии файла `BO_trace.ini` для BOE или WAR-файлов `dswebobje`.
 - Предварительно развернутая версия файла конфигурации для `BOE.war` доступна по умолчанию в следующем каталоге: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`.
 - Предварительно развернутая версия файла конфигурации для `dswebobje.war` доступна по умолчанию в следующем каталоге: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswebobje\WEB-INF\conf`.
3. Откройте файл `BO_trace.ini`.
 - Расположением по умолчанию в системе Windows является: `<INSTALLDIR>\SAP BusinessObjects Enterprise 12.0\logging\logConfig`.
 - Расположение по умолчанию на UNIX:
`<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`.
4. Удалите комментарии обязательных строк в разделе «Trace Syntax and Setting» (Синтаксис и параметр трассировки).
5. Измените параметры серверной трассировки подходящим образом.
В таблице ниже перечислены все параметры, необходимые для настройки серверной трассировки.

Параметр	Возможные значения	Описание
active	false, true	Включает трассировку текущего процесса или сервера, если задано значение true. Значением по умолчанию является false.
importance	'<<', '<=', '==', '>=', '>>', xs, s, m, l, xl Примечание: importance = xs является наиболее подробным параметром, в то время как importance = xl является наименее подробным.	Задаёт порог для сообщений трассировки. Будет выполняться трассировка сообщений, превышающих пороговое значение. Значением по умолчанию является m (среднее).
предупреждение	false, true	Задаёт автоматическое включение трассировки серьёзных системных событий. Значением по умолчанию является true.
severity	'', 'W', 'E', 'A', success, warning, error, assert	Определяет пороговое значение важности, за пределами которого можно выполнить трассировку сообщений. Значением по умолчанию является 'E'.
size	Возможными значениями являются целые числа ≥ 1000	Задаёт число сообщений в файле журнала трассировки, по достижении которого будет создан новый журнал. Значением по умолчанию является 100000.
keep	false, true	Определяет необходимость или отсутствие необходимости сохранения старого файла журнала после создания нового. Значением по умолчанию является false.

Параметр	Возможные значения	Описание
Администратор	Строки или целые числа	Определяет комментарий, который необходимо использовать в выходном файле журнала. Например, если <pre>administrator = "hello"</pre> эта строка будет добавлена в файл журнала.
log_dir		Задаёт каталог выходного файла журнала. По умолчанию файлы журналов сохраняются в каталоге Logging.
always_close	on, off	Определяет необходимость закрытия файла журнала после записи трассировки в файл журнала. Значением по умолчанию является off.

```
active=false;
severity='E';
importance='';
size=1000000;
keep=false;
```

- Сохраните и закройте файл `BO_trace.ini`.
- При помощи WDeploy разверните WAR-файл на компьютере, где размещен сервер веб-приложений.

Измененные параметры трассировки вступают в силу после выполнения первого входа в веб-приложение.

20.4.2.1 Настройка трассировки для конкретного веб-приложения

Файл `BO_trace.ini` используется для указания параметров трассировки для веб-приложений платформы BI. Эти параметры затрагивают все приложения, связанные с развернутым WAR-файлом. Администраторы также могут использовать файл `BO_trace.ini`, чтобы задавать конкретные параметры трассировки для конкретных веб-приложений.

В текущем выпуске платформы BI представленная ниже таблица перечисляет веб-приложения и связанные с ними файлы WAR.

Веб-приложение	Файл WAR	Предварительно развернутое расположение
Central Management Console	BOE.war	<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
стартовая панель BI	BOE.war	<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
Открыть документ	BOE.war	<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
Веб-служба	dswebobje.war	<INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswebobje\WEB-INF\conf

1. При помощи WDeploy отмените развертывание веб-приложения с сервера веб-приложений. Для получения дополнительных сведений об использовании Wdeploy для отмены развертывания веб-приложений см. *Руководство по развертыванию веб-приложений SAP BusinessObjects Business Intelligence Platform*.

Примечание:

Если используется сервер веб-приложения Tomcat, предоставленный вместе с установкой платформы BI, файл `BO_trace.ini` становится доступным в следующем каталоге. Нет необходимости отменять развертывание веб-приложений. Доступно непосредственное изменение файла.

- Файл конфигурации трассировки для файла `BOE.war` доступен в каталоге `<INSTALLDIR>\Tomcat6\webapps\BOE\WEB-INF\TraceLog`.
- Файл конфигурации трассировки для файла `dswebobje.war` доступен в каталоге `<INSTALLDIR>\Tomcat6\webapps\dswebobje\WEB-INF\conf`.

Если используется связанный сервер веб-приложения Tomcat, перейдите к шагу 3.

2. Перейдите к предварительно развернутой версии файла `BO_trace.ini` для BOE или WAR-файлов `dswebobje`.
 - Предварительно развернутая версия файла конфигурации для `BOE.war` доступна по умолчанию в следующем каталоге: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`.
 - Предварительно развернутая версия файла конфигурации для `dswebobje.war` доступна по умолчанию в следующем каталоге: `<INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswebobje\WEB-INF\conf`.
3. Откройте файл `BO_trace.ini`.
4. Удалите комментарии обязательных строк в разделе «Trace Syntax and Setting» (Синтаксис и параметр трассировки).
5. Чтобы задать параметры трассировки для конкретного веб-приложения, используйте оператор IF, как показано в примере ниже:

```
if (device_name == "Webapp_opendocument_trace")
{
  active = true;
  importance = '<<' ;
}
```

```

alert = true;
severity = ' ';
keep_num = 332;
size = 100 * 1000;
}

```

В таблице ниже перечислены все параметры, необходимые для настройки трассировки веб-приложения.

Параметр	Возможные значения	Описание
active	false, true	Включает трассировку текущего процесса или сервера, если задано значение true. Значением по умолчанию является false.
importance	'<<', '<=', '==', '>=', '>>', xs, s, m, l, xl Примечание: importance = xs является наиболее подробным параметром, в то время как importance = xl является наименее подробным.	Задаёт порог для сообщений трассировки. Будет выполняться трассировка сообщений, превышающих пороговое значение. Значением по умолчанию является m (среднее).
предупреждение	false, true	Задаёт автоматическое включение трассировки серьёзных системных событий. Значением по умолчанию является true.
severity	'', 'W', 'E', 'A', success, warning, error, assert	Определяет пороговое значение важности, за пределами которого можно выполнить трассировку сообщений. Значением по умолчанию является 'E'.
size	Возможными значениями являются целые числа ≥ 1000	Задаёт число сообщений в файле журнала трассировки, по достижении которого будет создан новый журнал. Значением по умолчанию является 100000.
keep	false, true	Определяет необходимость или отсутствие необходимости сохранения старого файла журнала после создания нового. Значением по умолчанию является false.

Параметр	Возможные значения	Описание
Администратор	Строки или целые числа	Определяет комментарий, который необходимо использовать в выходном файле журнала. Например, если <pre>administrator = "hello"</pre> эта строка будет добавлена в файл журнала.
log_dir		Задаёт каталог выходного файла журнала. По умолчанию файлы журналов сохраняются в каталоге Logging.
always_close	on, off	Определяет необходимость закрытия файла журнала после записи трассировки в файл журнала. Значением по умолчанию является off.

6. Сохраните и закройте файл `BO_trace.ini`.
7. При помощи WDeploy разверните WAR-файл на компьютере, где размещен сервер веб-приложений.

20.5 Настройка трассировки для средства управления обновлением

Трассировка для средства управления обновлением выполняется посредством файла конфигурации `BO_trace.ini`.

Расположение по умолчанию на Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf/`.

Расположение по умолчанию на UNIX: `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`

Примечание:

В отличие от остальных компонентов платформы BI, настройка трассировки для средства управления обновлением не может быть произведена через CMC.

20.5.1 Настройка трассировки для средства управления обновлениями

1. Откройте файл BO_trace.ini.

- Расположение по умолчанию на Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf/.
- Расположение по умолчанию на UNIX:
<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/.

2. Удалите комментарии обязательных строк в разделе «Trace Syntax and Setting» (Синтаксис и параметр трассировки).**3. Чтобы задать параметры трассировки для конкретного сервера используйте оператор IF, как показано в примере ниже:**

```
if (process == "upgrademanagementtool")
{
  active = true;
  importance = '<<' ;
  alert = true;
  severity = ' ';
  keep = false;
  size = 100 * 1000;
}
```

Совет:

Процесс должен быть указан как `upgrademanagementtool`, чтобы параметр трассировки применялся к средству управления обновлениями.

4. Сохраните и закройте файл BO_trace.ini.

Измененные параметры будут скоро реализованы.

Интеграция с SAP Solution Manager

21.1 Обзор интеграции

Для обеспечения интеграции в SAP Solution Manager в платформе BI были добавлены функции обслуживания. Для поддержки развертывания платформы BI можно использовать следующие компоненты SAP Solution Manager:

- Solution Landscape Directory
- Solution Manager Diagnostics
- Introscope от CA Wily
- SAP Passport

Примечание:

Для доступа к portalу поддержки SAP для SAP BusinessObjects перейдите по следующему адресу: <https://websmp205.sap-ag.de/bosap-support>

21.2 Контрольный список по интеграции SAP Solution Manager

В следующей ниже таблице приводится сводка компонентов, которые требуются для включения в SAP Solution Manager поддержки платформы BI.

Поддержка в SAP Solution Manager	Требуется для платформы BI
Регистрация в SLD	<ul style="list-style-type: none"> Для включения регистрации на серверах платформы BI должен быть установлен агент SAPHOSTAGENT. <p>Примечание: Если агент SAPHOSTAGENT установлен, программа установки платформы BI выполнит регистрацию серверов автоматически.</p> <ul style="list-style-type: none"> Необходимо создать файл connect.key для поставщика данных, ведущего отчетность по обслуживаемым серверам. Для регистрации в SLD с WebSphere 6.1 или 7 необходимо установить инструмент регистрации SLDREG на каждом из серверов веб-приложений WebSphere (дополнительно). Дополнительные сведения см. в SAP-ноте 1482727. Для регистрации SLD с SAP NetWeaver 7.2 следует установить инструмент SLDREG на каждом хосте NetWeaver (дополнительно). Дополнительные сведения см. в SAP-ноте 1018839.
Интеграция SMD	<ul style="list-style-type: none"> Необходимо загрузить и установить SMD-агент (DIAGNOSTICS.AGENT) на всех хостах серверов платформы BI. Необходимо включить учетную запись пользователя SMAAdmin в платформе BI.
Настройка конфигурации для производительности	<ul style="list-style-type: none"> Для подключения к Enterprise Manager должен быть настроен агент Introscope. Для настройки соединений воспользуйтесь программой установки платформы BI или заполнителями узлов в СМС. Должен быть установлен SMD-агент. Для подключения к SMD-агенту необходимо настроить соответствующим образом платформу BI. Для настройки соединений воспользуйтесь программой установки платформы BI или заполнителями узлов в СМС.
SAP Passport	<ul style="list-style-type: none"> Необходимо загрузить и установить средство клиента SAP Passport.

21.3 Управление регистрацией System Landscape Directory

21.3.1 Регистрация платформы BI в System Landscape

Функция System Landscape Directory (SLD) представляет собой центральный репозиторий сведений о параметрах системы, которые связаны с управлением жизненным циклом программного обеспечения. Репозиторий SLD содержит описание параметров системы, а именно установленных в настоящий момент систем и программных компонентов. Поставщики данных SLD регистрируют системы на SLD-сервере и поддерживают информацию в актуальном состоянии. Управляющие приложения и бизнес-приложения обращаются к информации, хранящейся в SLD, при выполнении задач в объединенной вычислительной среде.

За регистрацию серверов платформы BI на сервере SLS отвечает приложение System Landscape Directory-Data Supplier (SLD-DS). Для каждой установки платформы BI используется отдельный поставщик данных, который предоставляет отчетность по следующим компонентам:

- Серверы платформы BI
- Веб-приложения и службы, размещаемые на сервере веб-приложений WebSphere.

Примечание:

SAP NetWeaver имеет встроенный поставщик SLD-DS, который регистрирует сервер приложений NetWeaver, а также размещенные веб-приложения и службы. Приложение SLD-DS используется при развертывании платформы BI, когда выполняется интеграция в среду SAP NetWeaver.

Для предоставления отчетности по серверам платформы BI с использованием SLD-DS требуется установить и настроить программу SLDREG. Программа SLDREG устанавливается при установке средства SAPHOSTAGENT. Для получения дополнительных сведений о доступе к средству SAPHOSTAGENT и его установке см. раздел "Подготовка" документа *Руководство по установке платформы SAP BusinessObjects Business Intelligence*. После установки SLDREG требуется создать файл `connect.key` для подключения к SLD-серверу.

Для получения сведений о настройке конкретного поставщика данных для работы с WebSphere см. *Руководство по развертыванию веб-приложений SAP*.

В ходе установки платформы BI информация, требуемая для регистрации платформы BI, хранится в файле конфигурации. Этот файл содержит сведения, используемые SLD-DS для подключения к базе данных платформы BI.

21.3.1.1 Создание файла `connect.key` для поставщика данных SLD

Платформа BI

Перед созданием файла `connect.key` для поставщика данных SLD необходимо загрузить и установить SAPHOSTAGENT. Для получения дополнительных сведений см. раздел "Подготовка" в документе *Руководство по установке платформы SAP BusinessObjects Business Intelligence*.

Примечание:

Файл `connect.key` требуется для регистрации SLD в поставщике данных, предоставляющем отчетность по серверам платформы BI.

1. Откройте консоль командной строки.
2. Перейдите в папку установки по умолчанию SAPHOSTAGENT.
 - В Windows: `Program Files\SAP\hostctrl\exe`
 - В Unix: `/usr/sap/hostctrl/exe`
3. Выполните следующую команду:
`sldreg -configure connect.key`
4. Введите следующие параметры конфигурации
 - Имя пользователя
 - Пароль
 - Хост
 - Номер порта
 - Выберите использование HTTP

Инструмент `sldreg` создаст файл `connect.key`, который будет автоматически использован поставщиком данных для передачи информации SLD-серверу.

21.3.2 Точки запуска SLD

Процесс регистрации в SLD инициируется поставщиком данных, создающим отчетность по обслуживающим серверам платформы BI, в следующих сценариях:

- Перезапуск узла сервера в развертывании платформы BI.
- Добавление в развертывание нового сервера или узла.
- Удаление сервера или узла

Примечание:

При удалении сервера или узла процесс регистрации в SLD не изменяет содержимое SLD-сервера.

Поставщик данных для регистрации в WebSphere SLD можно вызывать вручную. Также можно запланировать его выполнение с определенным интервалом, например раз в 24 часа. Дополнительные сведения о настройке поставщика данных см. в SAP-ноте 482727.

21.3.3 Ведение журнала SLD-соединения

Файл конфигурации поставщика данных

Файл конфигурации, используемый для SLD-регистрации, создается для развертываний платформы BI. Этот файл с именем `sldparserconfig.properties` расположен в следующей папке: `<INSTALLEDIR>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/`.

Ведение журнала SLD-соединения

Соединение между SLD-сервером и поставщиком данных в развертывании платформы BI управляется при помощи средства `sldreg` и файла `connect.key`.

Примечание:

Имя файла журнала указывается как свойство в файле `sldparserconfig.properties`.

Файл журнала для поставщика данных SLD, ведущего отчетность по обслуживающим серверам платформы BI, по умолчанию расположен в папке `<INSTALLEDIR>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/bobjsldds.log`. Этот файл перезаписывается при каждом запуске поставщика данных.

Файлы журнала для инструмента `sldreg` по умолчанию находятся в следующей папке: `<INSTALLEDIR>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/log`. Имена файлов журнала инструмента `sldreg` не могут изменяться. Они имеют следующий формат: `sldrg_<метка_времени>.log`.

Каждый раз при вызове инструмента `sldreg` в поставщике данных создается новый файл журнала.

21.4 Управление агентами Solution Management Diagnostics

21.4.1 Обзор Solution Manager Diagnostics (SMD)

Компонент SAP Solution Manager под названием Solution Manager Diagnostics (SMD) полностью обеспечивает функциональность для централизованного анализа и мониторинга всей системной среды. Если установлен SMD-агент, доступно отслеживание платформы BI с использованием SMD-сервера. SMD-агент (`DIAGNOSTICS.AGENT`) осуществляет сбор данных для SMD, на основе которых затем может выполняться анализ коренных причин. К данным, собираемым и направляемым на SMD-сервер, относятся параметры конфигурации обслуживающего сервера, а также местонахождение файлов журнала.

21.4.2 Работа с SMD-агентами

Платформа BI не устанавливает SMD-агент. Агент `DIAGNOSTICS.AGENT` можно загрузить по следующей ссылке: <http://service.sap.com/swdc>.

Сведения об установке и настройке агента доступны по адресу: <http://service.sap.com/diagnostics>

Рекомендации по работе с SMD-агентом

Ниже приводятся рекомендации по работе с SMD-агентами для мониторинга платформы BI:

- Порядок установки отслеживаемой системы и агента не имеет значения. Можно установить SMD-агент как до, так и после установки и развертывания платформы BI.
- При установке SMD-агента запишите имя хоста и порт прослушивания. Это критично для настройки платформы BI в качестве отслеживаемой системы. Если агент установлен раньше отслеживаемой системы, можно указать параметры конфигурации в ходе настройки установки платформы BI. Эти данные также можно задать позже при помощи заместителей узлов в консоли CMC развертывания.
- Если обслуживающие сервера развернуты в распределенной системе, следует установить SMD-агент на каждом компьютере, где размещен обслуживающий сервер.
- Для настройки конфигурации серверов, не являющихся Java-серверами, SMD-агент является обязательным.
- Для обеспечения доступа SMD-сервера к CMS необходимо активировать учетную запись пользователя SMAdmin.

21.4.3 Учетная запись пользователя SMAdmin

В каждом развертывании платформы BI существует учетная запись пользователя, созданная специально для обеспечения интеграции с SMD. Эта учетная запись только для чтения используется на SMD-сервере для входа на CMS и сбора параметров конфигурации сервера, а также других сведений о развертывании.

Учетная запись SMAdmin по умолчанию неактивна.

21.4.3.1 Активация учетной записи пользователя SMAdmin

1. В области управления CMC «Пользователи и группы» выберите значение **Список пользователей**.

Будет открыт список пользователей.

2. Найдите учетную запись пользователя «SMAAdmin ».
3. Выберите команду **Управление > Свойства**.
Отобразится диалоговое окно «Свойства».
4. Снимите флажок **Учетная запись отключена**.
5. Нажмите кнопку **Сохранить и закрыть**.

21.5 Инструментальные средства управления производительностью

21.5.1 Настройка инструментов мониторинга производительности для платформы BI

Для изменения инструментов мониторинга производительности платформы BI можно воспользоваться программой CA Wily Introscope, включенной в SAP Solution Manager. При установке платформы для развертывания предоставляются следующие ресурсы:

- Introscope-агент. Introscope-агенты ведут сбор показателей производительности на обслуживаемых Java-серверах платформы BI. Агенты также собирают информацию из окружающей вычислительной среды. Затем агенты передают эти метрики в Enterprise Manager.
- Предоставляемые файлы обеспечивают процесс настройки конфигурации. Один набор файлов служит для инструментирования серверов, не являющихся Java-серверами, а другой набор файлов – для настройки конфигурации Java-серверов. На стороне SAP Solution Manager требуется компонент Enterprise Manager (EM). EM выступает в качестве центрального репозитория для всех данных производительности Introscope и показателей, собранных в среде приложения. EM обрабатывает данные производительности и делает их доступными для пользователей с целью мониторинга работы и проведения диагностики.

21.5.2 Настройка инструментальных средств мониторинга производительности для платформы BI

Есть два способа настроить инструменты мониторинга производительности для рабочих процессов, выполняемых на серверах платформы BI.

1. В ходе настройки установки для платформы BI. Необходимо знать имя хоста и порт прослушивания для SMD-агента. Для получения дополнительных сведений см. документ *Руководство по установке платформы SAP BusinessObjects Business Intelligence*. При выборе

этого параметра настройка инструментов мониторинга по умолчанию будет выполнена один раз по завершении развертывания системы.

- После установки платформы SAP BusinessObjects Business Intelligence можно предоставить данные конфигурации для SMD-агента при помощи заполнителей в свойствах узла в консоли СМС.

Примечание:

Для настройки инструментов мониторинга рабочих процессов на серверах, не являющихся Java-серверами, необходимо предварительно установить SMD-агент (`DIAGNOSTICS.AGENT`).

См. также

- [Работа с SMD-агентами](#)

21.5.2.1 Настройка узлов для выполнения инструментальных средств

Если во время установки платформы SAP BusinessObjects Business Intelligence не были заданы конфигурационные данные для SMD-агента и Enterprise Manager, воспользуйтесь следующими инструкциями.

- Перейдите в область «Серверы» консоли СМС.
- В области навигации щелкните **Узлы**.
Будут отображены все доступные узлы.
- Щелкните правой кнопкой мыши узел, на котором нужно выполнить настройку конфигурации, и выберите команду **Заполните**.
Будет открыто диалоговое окно "Заполнители".
- Измените значения для следующих заполнителей.

Заполнитель	Описание
<code>%scopeAgentInstrumental%</code>	Включение и отключение инструментальных средств на Java-серверах. По умолчанию включено, если во время настройки установки были заданы конфигурационные сведения для Enterprise Manager. Установите значение <code>true</code> , чтобы включить инструментальные средства.
<code>%scopeAgentManagerHost%</code>	Имя хоста для компьютера, на котором установлено приложение Enterprise Manager.
<code>%scopeAgentManagerPort%</code>	Порт прослушивания, используемый Enterprise Manager.
<code>%scopeAgentManagerTransport%</code>	Протокол обмена данными, используемый Enterprise Manager. К поддерживаемым протоколам относятся TCP, SSL, HTTP Tunnel и HTTPS.

Заполнитель	Описание
%NCSInstrumentLevelThreshold%	Используется для настройки уровня инструментальных средств для серверов, не являющихся Java-серверами. Установите значение «0», чтобы отключить инструментальные средства. Задайте значение выше «0», чтобы включить инструментальные средства.
%SMDAgentHost%	Имя хоста для компьютера, на котором установлен SMD-агент (DIAGNOSTICS.AGENT).
%SMDAgentPort%	Порт прослушивания, используемый SMD-агентом.

5. Нажмите кнопку **Сохранить и закрыть**.

6. Перезапустите узел.

После перезапуска новые значения будут распространены на все управляемые серверы.

21.5.3 Настройка конфигурации производительности для веб-уровня

Данные инструментов мониторинга для компонентов веб-уровня не включены в платформу BI.

21.5.4 Файлы журнала настройки конфигурации

После настройки развертывания платформы BI для запуска инструментов мониторинга сообщения регистрируются в журнале в заданных местоположениях. Проверка файлов журнала является одним из способов проверки статуса настройки конфигурации.

Для настройки конфигурации на обслуживающих Java-серверах файл журнала находится в следующей папке: <INSTALLEDIR>/SAP BusinessObjects Enterprise XI 4.0/java/wily/logs. Для каждого из Java-процессов создается отдельный файл .log. Эта папка также содержит файлы AutoProbe.log, указывающие, какие методы были загружены для инструментальных средств.

Для настройки конфигурации на обслуживающих серверах, не являющихся Java-серверами, файлы журнала расположены в следующей папке: <INSTALLEDIR>/SAP BusinessObjects Enterprise XI 4.0/logging/. В системах Unix файлы расположены в папке <sap_bobj>\logging\. Относящиеся к настройке конфигурации файлы журнала для серверов, не являющихся Java-серверами, сохраняются в формате .trc.

Для настройки конфигурации на серверах веб-приложений файл журнала расположен в следующей папке: `<INSTALLEDIR>/SAP BusinessObjects Enterprise XI 4.0/java/wily/webapp/logs`. В этой папке доступно два типа файлов журнала: `Introscope.log` и `Autoprobe.log`.

21.6 Трассировка с использованием SAP Passport

В дополнение к трассировке компонентов платформы BI, таких как серверы и веб-приложения, механизм трассировки может поддерживать трассировку конкретного действия. Анализ трассировки всей цепи позволяет проанализировать производительность отдельной транзакции. Объединение сведений трассировки для конкретного действия позволяет сотрудникам службы поддержки SAP видеть все сведения трассировки, не отвлекаясь на сведения, относящиеся к другим действиям.

SAP Passport

Механизм, поддерживающий непрерывную трассировку для платформы BI, представляет собой инструмент, который называется SAP Passport. Клиентское средство SAP Passport вставляет уникальный идентификатор во все HTTP-запросы для конкретного рабочего потока; этот идентификатор пересылается всем серверам, задействованным в рабочем потоке. Сотрудники технической поддержки SAP могут установить непрерывную трассировку для рабочего потока, используя этот уникальный идентификатор.

Примечание:

Уровни журнала трассировки, установленные в СМС и файле конфигурации `BO_trace.ini`, используются в том случае, если они выше уровней, заданных в клиентском инструменте SAP Passport – `SAPIEPlugin.exe`.

Паспорта включаются в журналы обслуживающих серверов, веб-приложений и веб-служб.

Средство клиента SAP Passport не устанавливается как часть платформы BI. Средство доступно для загрузки по адресу <http://service.sap.com/swdc>.

Администрирование в командной строке

22.1 Скрипты UNIX

В этом разделе приводятся сведения по каждому из средств и скриптов администрирования, включенных в дистрибутив платформы SAP BusinessObjects Business Intelligence для UNIX. Основное назначение данного раздела – ссылки. Здесь также изложены основные принципы и процедуры настройки.

Дистрибутив платформы SAP BusinessObjects Business Intelligence для UNIX содержит ряд скриптов, которые в совокупности предоставляют все параметры конфигурации, доступные в версии CCM для Windows. Также включены другие скрипты, которые предоставляют параметры, доступные только в UNIX, либо служат шаблонами для создания собственных скриптов. Кроме того, есть несколько вспомогательных скриптов, которые используются в платформе SAP BusinessObjects Business Intelligence. Здесь рассматриваются все эти скрипты, а также применимые параметры командной строки.

22.1.1 Утилиты скриптов

В этом разделе описаны административные скрипты, помогающие в работе с платформой SAP BusinessObjects Business Intelligence в операционной системе UNIX. В оставшейся части справки обсуждаются основные принципы задач, которые можно выполнять с помощью этих скриптов. В справочном разделе предоставлены главные параметры командной строки и их аргументы.

22.1.1.1 ccm.sh

Скрипт `ccm.sh` устанавливается в каталог установки `<SCRIPTDIR>`. Этот скрипт предоставляет версию CCM для командной строки. В этом разделе перечислены параметры командной строки и приведены некоторые примеры.

Примечание:

- Аргументы в квадратных скобках [] являются необязательными.

- Если имя агента Server Intelligence не известно, посмотрите свойства команды в файле `ccm.config` и используйте значение, указанное после параметра `-name`.
- Скрипт `ccm.sh` может быть запущен только пользователем, который выполнял установку платформы SAP BusinessObjects Business Intelligence.
- Аргументы, отмеченные как *другая информация для аутентификации*, представлены во второй таблице.

Параметр CCM	Допустимые аргументы	Описание
<code>-help</code>	недоступно	Отображает справку по командной строке.
<code>-start</code>	все или <i>sianame</i>	Запускает каждого агента Server Intelligence в качестве процесса. Параметр <code>all</code> позволяет запустить все узлы на компьютере, включая узлы, входящие в разные кластеры.
<code>-stop</code>	все или <i>sianame</i>	Останавливает каждого агента SIA путем удаления ID его процесса. Параметр <code>all</code> позволяет запустить все узлы на компьютере, включая узлы, входящие в разные кластеры.
<code>-restart</code>	все или <i>sianame</i>	Останавливает каждого агента SIA путем удаления ID его процесса; затем каждый SIA запускается заново. Параметр <code>all</code> позволяет запустить все узлы на компьютере, включая узлы, входящие в разные кластеры.
<code>-managedstart</code>	<i><полное правильное имя сервера> [другая информация для аутентификации]</i>	Запустите сервер.

Параметр CSM	Допустимые аргументы	Описание
-managedstop	<i><полное правильное имя сервера> [другая информация для аутентификации]</i>	Остановите сервер.
-managedrestart	<i><полное правильное имя сервера> [другая информация для аутентификации]</i>	Остановите сервер, а затем запустите его.
-managedforceterminate	<i><полное правильное имя сервера> [другая информация для аутентификации]</i>	Немедленно останавливает сервер без завершения текущей обработки запросов.
-enable	<i><полное правильное имя сервера> [другая информация для аутентификации]</i>	Делает доступным запущенный сервер таким образом, что он регистрируется в системе и ожидает данные с подходящего порта. Используйте полную форму имени сервера.
-disable	<i><полное правильное имя сервера> [другая информация для аутентификации]</i>	Блокирует сервер таким образом, что он перестает обрабатывать запросы платформы SAP BusinessObjects Business Intelligence, но остается запущенным в качестве процесса. Используйте полную форму имени сервера.
-display	<i>[другая информация для аутентификации]</i>	Выводит сведения о текущем статусе всех серверов кластера, включая имена серверов, имена хостов, идентификаторы процессов, описания, состояние выполнения, а также статус активности (включены или отключены).

В следующей таблице представлены параметры, которые могут присутствовать в аргументе, отмеченном как *[другая информация для аутентификации]*.

Примечание:

С целью повышения уровня безопасности необходимо всегда указывать данные учетной записи пользователя с аутентификацией Enterprise. Другие типы аутентификации не поддерживаются.

Параметр аутентификации	Допустимые аргументы	Описание
-cms	<i>cmsname:port#</i>	Укажите CMS, в который следует выполнить вход. Если этот параметр не указан, ССМ обращается к локальному компьютеру и порту по умолчанию (6400).
-username	<i>ИМЯ ПОЛЬЗОВАТЕЛЯ</i>	Укажите учетную запись с наличием прав администрирования платформы SAP BusinessObjects Business Intelligence. Если запись не указана, по умолчанию применяется учетная запись Администратор.
-password	<i>пароль</i>	Укажите соответствующий пароль. Если пароль не указан, применяется пустой пароль. Примечание: Для указания аргумента -password вы должны также указать аргумент -username.

ССМ прочитывает строки запуска и другие значения конфигурации из файла `ccm.config`.

См. также

- [ccm.config](#)

22.1.1.1.1 Примеры

Две эти команды запускают и активируют все серверы платформы SAP BusinessObjects Business Intelligence. Центральный сервер управления (CMS) запускается на локальном компьютере и использует порт по умолчанию (6400):

```
ccm.sh -start all
ccm.sh -enable all
```

Две эти команды запускают и активируют все серверы платформы SAP BusinessObjects Business Intelligence. В этом случае Центральный сервер управления (CMS) запускается с использованием порта 6701 (вместо порта по умолчанию).

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701
```

Эти две команды запускают и делают доступными все серверы платформы SAP BusinessObjects Business Intelligence с помощью административной учетной записи SysAdmin:

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

Эта команда выполняет вход в систему с использованием указанной административной учетной записи и блокирует адаптивный сервер заданий, запущенный на втором компьютере:

```
ccm.sh -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

22.1.1.1.2 ccm.config

Этот файл конфигурации определяет строки запуска и другие значения, используемые CCM при запуске его команд. Этот файл определяется собственно CCM, а также другими утилитами скриптов платформы SAP BusinessObjects Business Intelligence. При изменении командной строки агента Server Intelligence Agent обычно следует изменить именно этот файл.

См. также

- [Обзор командных строк](#)

22.1.1.2 cmsdbsetup.sh

Скрипт `cmsdbsetup.sh` устанавливается в каталог установки `sap_bobj`. Этот скрипт предоставляет текстовую программу, которая позволяет выполнять следующие задачи.

- Настройка системной базы данных CMS
- Повторная инициализация системной базы данных CMS
- Копирование данных из другого источника данных
- Изменение ключа кластера
- Изменение имени кластера

Примечание:

Перед выполнением этого скрипта следует создать резервную копию базы данных системы CMS, а также содержимого репозитория входных и выходных файлов. Для получения дополнительных сведений см. раздел «Резервное копирование и восстановление системы». Кроме того, для получения дополнительных сведений о кластерах CMS и настройке базы данных CMS см. раздел «Кластеризация центральных серверов управления» в главе «Обслуживание сервера» документа *Руководство администратора платформы SAP BusinessObjects Business Intelligence*.

Этот скрипт запрашивает имя агента Server Intelligence (SIA). Для проверки имени SIA просмотрите его свойство "Команда". После параметра `-name` отображается текущее имя SIA.

См. также

- [Кластеризация центральных серверов управления \(CMS\)](#)
- [Резервное копирование и восстановление системы](#)

22.1.1.3 configpatch.sh

Скрипт `configpatch.sh` устанавливается в каталог установки `sap_bobj/enterprise/generic`. Скрипт `configpatch.sh` используется при установке исправлений, которые требуют обновления значений конфигурации системы. После установки исправления следует выполнить скрипт `configpatch.sh` с соответствующим именем файла `.cf` в качестве аргумента. Файл `readme.txt`, включаемый в исправления платформы SAP BusinessObjects Business Intelligence, содержит сведения о сценариях, требующих выполнения скрипта `configpatch.sh`, а также имя используемого файла `.cf`.

22.1.1.4 serverconfig.sh

Скрипт `serverconfig.sh` устанавливается в каталог установки `sap_bobj`. Этот скрипт предоставляет текстовую программу, позволяющую выполнять следующие операции.

- Добавить узел
- Удалить узел
- Изменить узел
- Переместить узел
- Резервное копирование конфигурации сервера
- Восстановление конфигурации сервера
- Список узлов

22.1.1.4.1 Для добавления, удаления, изменения или перечисления узлов в UNIX

1. Перейдите в каталог `<SCRIPTDIR>` каталога установки.
2. Вызовите следующую команду:

```
./serverconfig.sh
```

Скрипт предлагает список вариантов:

- 1 – Добавить агента Server Intelligence
 - 2 – Удалить агента Server Intelligence
 - 3 – Изменить агента Server Intelligence
 - 4 – Перечислить всех агентов Server Intelligence в файле конфигурации
3. Введите число, соответствующее действию, которое вы хотите выполнить.
 4. Если выполняется добавление, удаление или изменение сервера, предоставьте скрипту дополнительные запрашиваемые сведения.

Совет:

Скрипт запросит имя сервера CMS. По умолчанию, имя CMS – имя компьютера.cms. Таким образом, именем по умолчанию для CMS, установленного на станции MACHINE01, будет имя MACHINE01.cms. Однако в этом скрипте можно ввести имя хоста для проверки имени сервера CMS (или любого другого сервера), просмотра содержимого файла ccm.config и поиска строки запуска сервера. Текущее имя сервера находится после параметра "-name".

22.1.2 Шаблоны скриптов

Эти скрипты предоставлены в первую очередь как шаблоны, на основе которых можно создавать собственные скрипты.

22.1.2.1 startservers

Скрипт `startservers` устанавливается в каталог установки `<SCRIPTDIR>`. Этот скрипт может использоваться в качестве шаблона для пользовательских скриптов: он предоставляется в качестве примера, демонстрирующего возможности настройки скрипта, запускающего серверы платформы SAP BusinessObjects Business Intelligence посредством выполнения последовательности команд CCM. Для получения дополнительной информации о написании CCM-команд для серверов см. описание скрипта [ccm.sh](#).

22.1.2.2 stopservers

Скрипт `stopservers` устанавливается в каталог установки `<SCRIPTDIR>`. Он может использоваться в качестве шаблона для пользовательских скриптов: он предоставляется в качестве примера, демонстрирующего возможности настройки скрипта, останавливающего серверы платформы SAP BusinessObjects Business Intelligence посредством выполнения последовательности команд CCM. Для получения дополнительной информации о написании CCM-команд для серверов см. описание скрипта [ccm.sh](#).

22.1.3 Скрипты, используемые платформой SAP BusinessObjects Business Intelligence

Эти вспомогательные скрипты часто запускаются в фоновом режиме при выполнении основных скриптов платформы SAP BusinessObjects Business Intelligence. Самостоятельно их запускать не нужно.

22.1.3.1 bobjrestart.sh

Это внутренний скрипт CCM, выполняемый при запуске серверных компонентов платформы SAP BusinessObjects Business Intelligence. Если процесс сервера неожиданно завершается без возвращения нормального кода выхода, этот скрипт автоматически перезапускает новый процесс сервера. Не запускайте этот скрипт самостоятельно.

22.1.3.2 env.sh

Скрипт `env.sh` устанавливается в каталог установки `sap_bobj/setup`. Этот скрипт устанавливает переменные среды платформы SAP BusinessObjects Business Intelligence, которые необходимы некоторым другим сценариям. Скрипты платформы SAP BusinessObjects Business Intelligence при необходимости запускают `env.sh`. Если платформа SAP BusinessObjects Business Intelligence устанавливается в ОС UNIX, необходимо настроить на сервере Java-приложений использование этого скрипта при запуске. Для получения дополнительных сведений см. *Руководство по установке платформы SAP BusinessObjects Business Intelligence*.

22.1.3.3 env-locale.sh

Скрипт `env-locale.sh` используется для преобразования строк на языке скрипта в различные типы кодировок (например, UTF8, EUC или Shift-JIS). Этот скрипт запускается оболочкой `env.sh` по мере необходимости.

22.1.3.4 initlaunch.sh

Скрипт `initlaunch.sh` запускает оболочку `env.sh` для настройки переменных среды платформы SAP BusinessObjects Business Intelligence, а затем выполняет команды, добавленные в качестве аргументов командной строки для скрипта. Этот скрипт предназначен в первую очередь для использования SAP Business Objects в качестве средства отладки.

22.1.3.5 setup.sh

Скрипт `setup.sh` устанавливается в корневой каталог установки. Этот скрипт предоставляет текстовую программу, которая позволяет настроить установку платформы SAP BusinessObjects Business Intelligence. Этот скрипт выполняется автоматически при установке платформы SAP BusinessObjects Business Intelligence. Пользователю выводится приглашение ввести информацию, необходимую при первой установке платформы SAP BusinessObjects Business Intelligence.

Для получения дополнительных сведений о предоставлении ответов скрипту настройки при установке платформы SAP BusinessObjects Business Intelligence см. *Руководство по установке платформы SAP BusinessObjects Business Intelligence*.

22.1.3.6 setupinit.sh

Скрипт `setupinit.sh` устанавливается в каталог `/sap_bobj/init` при выполнении установки системы. Этот скрипт копирует скрипты управления выполнением в каталоги `rc#` для автоматического запуска. При выполнении установки системы предлагается выполнить этот скрипт после завершения работы скрипта `setup.sh`.

Примечание:

Для запуска этого скрипта необходимы привилегии суперпользователя (root).

22.2 Скрипты Windows

В этом разделе описываются все инструменты администрирования и скрипты, включенные в дистрибутив платформы SAP BusinessObjects Business Intelligence для Windows. Основное назначение данного раздела – ссылки. Здесь также изложены основные принципы и процедуры настройки.

Дистрибутив платформы SAP BusinessObjects Business Intelligence для Windows содержит версию Central Configuration Manager (CCM) для Windows. Помимо работы в графическом ИП для управления серверами можно запускать исполняемый файл CCM в командной строке с соответствующими параметрами.

22.2.1 ccm.exe

Исполняемый файл `ccm.exe` устанавливается в папку `<INSTALLDIR>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64`. Этот файл можно запустить непосредственно из командной строки для выполнения определенных операций. В этом разделе перечислены параметры командной строки и приведены некоторые примеры.

Примечание:

- Для использования параметров командной строки `ccm.exe` должны выполняться агент Server Intelligence Agent (SIA) и центральный сервер управления (CMS), которые обеспечивают взаимодействие с отдельным сервером.
- Аргументы в квадратных скобках [] являются необязательными.
- Аргументы, отмеченные как *другая информация для аутентификации*, представлены во второй таблице.

Параметр CCM	Допустимые аргументы	Описание
-help	недоступно	Отображает справку по командной строке.
-managedstart	all или <полное имя сервера> [другие данные аутентификации]	Запустите сервер.

Параметр CCM	Допустимые аргументы	Описание
-managedstop	all или <полное имя сервера> [другие данные аутентификации]	Остановите сервер.
-managedrestart	all или <полное имя сервера> [другие данные аутентификации]	Остановите сервер, а затем запустите его.
-managedforceterminate	all или <полное имя сервера> [другие данные аутентификации]	Немедленно останавливает сервер без завершения текущей обработки запросов.
-enable	all или <полное имя сервера> [другие данные аутентификации]	Делает доступным запущенный сервер таким образом, что он регистрируется в системе и ожидает данные с подходящего порта.
-disable	all или <полное имя сервера> [другие данные аутентификации]	Блокирует сервер таким образом, что он перестает обрабатывать запросы платформы SAP BusinessObjects Business Intelligence, но остается запущенным в качестве процесса.
-display	[другая информация для аутентификации]	Выводит сведения о текущем статусе всех серверов кластера, включая имена серверов, имена хостов, идентификаторы процессов, описания, состояние выполнения, а также статус активности (включены или отключены).

В следующей таблице представлены параметры, которые могут присутствовать в аргументе, отмеченном как *[другая информация для аутентификации]*.

Примечание:

Необходимо всегда указывать учетные данные учетной записи пользователя с аутентификацией Enterprise.

Параметр аутентификации	Допустимые аргументы	Описание
-cms	<i>cmsname:port#</i>	Укажите CMS, в который следует выполнить вход. Если этот параметр не указан, ССМ обращается к локальному компьютеру и порту по умолчанию (6400).
-username	<i>имя пользователя</i>	Укажите учетную запись с правами администратора платформы SAP BusinessObjects Business Intelligence. Если запись не указана, по умолчанию применяется учетная запись Администратор.
-password	<i>пароль</i>	Укажите соответствующий пароль. Если пароль не указан, применяется пустой пароль. Примечание: Для указания аргумента -password вы должны также указать аргумент -username.
-authentication	<i>тип аутентификации</i>	Укажите тип аутентификации. Поддерживается только secEnterprise.

ССМ прочитывает строки запуска и другие значения конфигурации из файла `ccm.config`.

См. также

- [ccm.config](#)

22.2.1.1 Примеры

В следующих примерах предполагается, что выполняются агент Server Intelligence Agent (SIA) и центральный сервер управления (CMS). Перед использованием параметров командной строки `ccm.exe` для взаимодействия с отдельным сервером можно запустить службу SIA при помощи следующей команды Windows:

```
net start "Server Intelligence Agent (MACHINE01)"
```

SIA можно также остановить при помощи команды `net stop "Server Intelligence Agent (MACHINE01) "`.

Эта команда запускает все серверы платформы SAP BusinessObjects Business Intelligence:

```
ccm.exe -managedstart all
```

Эта команда запускает адаптивный сервер заданий. В этом случае центральный сервер управления (CMS) запускается с использованием порта 6701 (вместо порта по умолчанию).

```
ccm.exe -managedstart MACHINE01.AdaptiveJobServer -cms MACHINE01:6701
```

Эта команда включает на адаптивном сервере заданий указанную административную учетную запись с именем SysAdmin:

```
ccm.exe -enable MACHINE01.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

Эта команда выполняет вход в систему с использованием указанной административной учетной записи и блокирует сервер адаптивных заданий, запущенный на втором компьютере:

```
ccm.exe -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

22.3 Командные строки сервера

22.3.1 Обзор командных строк

В этом разделе перечислены параметры командной строки, управляющие работой каждого из серверов платформы SAP BusinessObjects Business Intelligence.

При запуске или настройке сервера с помощью CMS сервер запускается или перезапускается с командной строкой по умолчанию, содержащей типичный набор параметров и значений. В большинстве случаев изменять напрямую командные строки по умолчанию не требуется. Кроме того, большинство чаще всего используемых параметров можно изменять на различных экранах настройки сервера в CCM. В справочных целях в этом разделе приводится полный список параметров командной строки, поддерживаемых каждым из серверов. При необходимости дополнительной настройки платформы SAP BusinessObjects Business Intelligence командную строку каждого из серверов можно изменить напрямую.

Значения, которые приведены в квадратных скобках [] в различных частях данного раздела, являются необязательными.

Примечание:

В следующих таблицах перечислены поддерживаемые параметры командной строки. Серверы платформы SAP BusinessObjects Business Intelligence используют ряд внутренних параметров, не перечисленных в этих таблицах. Изменять эти внутренние параметры не следует.

22.3.1.1 Просмотр и изменение командной строки сервера

1. Остановите сервер с помощью консоли Central Management Console (CMC).
2. Щелкните сервер правой кнопкой мыши и выберите команду **Свойства**.
3. На экране «Свойства» измените командную строку для сервера и нажмите кнопку **Сохранить и закрыть**.
4. Запустите сервер.

22.3.2 Стандартные параметры для всех серверов

Эти параметры командной строки применимы ко всем серверам платформы SAP BusinessObjects Business Intelligence, если не указывается иное. В оставшейся части данного раздела приведены параметры, особые для каждого типа сервера.

Параметр	Допустимые аргументы	Поведение
<code>-requestPort</code>	<i>port</i>	<p>Указывает порт, на котором сервер выполняет прослушивание (принимает соединения). Сервер регистрирует этот порт в CMS. Если значение не указано, сервер выбирает любой свободный порт с номером больше 1024.</p> <p>Примечание: Этот порт используется разными серверами в различных целях. Перед изменением значения ознакомьтесь с разделом <i>Руководства администратора платформы SAP BusinessObjects Business Intelligence</i>, посвященным изменению номеров портов сервера по умолчанию.</p>
<code>-loggingPath</code>	<i>абсолютный путь</i>	Укажите путь, в котором будут создаваться файлы журнала.

22.3.2.1 Обработка сигналов UNIX

В UNIX демоны платформы SAP BusinessObjects Business Intelligence обрабатывают следующие сигналы:

- `SIGTERM` вызывает постепенное завершение работы сервера (код выхода = 0).
- `SIGSEGV`, `SIGBUS`, `SIGSYS`, `SIGFPE` и `SIGILL` вызывают быстрое завершение работы (код выхода = 1).

22.3.3 Центральный сервер управления

В этом разделе содержится информация по особым параметрам командной строки, относящимся к CMS. Путь по умолчанию к серверу в ОС Windows – `<INSTALLDIR>\BusinessObjects Enterprise XI 4.0\win64_x64\CMS.exe`.

Путь по умолчанию к серверу в ОС UNIX –

`<INSTALLDIR>/sap_bobj/enterprise_xi40/<платформа>/boe_cmsd`.

Параметр	Допустимые аргументы	Поведение
<code>-threads</code>	<i>number</i>	Определяет количество рабочих потоков, инициализируемых и используемых CMS. Значение можно выбрать в диапазоне от 12 до 150. По умолчанию используется значение 50.
<code>-reinitializedb</code>		При указании этого параметра CMS удаляет базу данных и заново создает ее, добавляя только системные объекты по умолчанию. При пересоздании базы данных все содержащиеся в ней данные будут утеряны.
<code>-quit</code>		При выборе этого параметра CMS принудительно завершит работу после обработки параметра <code>-reinitializedb</code> .

Параметр	Допустимые аргументы	Поведение
<code>-receiverPool</code>	<i>number</i>	Задаёт количество потоков, создаваемых CMS для получения запросов клиентов. Клиентом может быть другой сервер Business Objects, Мастер публикации отчётов, Crystal Reports или произвольное клиентское приложение, созданное вами. По умолчанию используется значение 5. Как правило, увеличивать данное значение требуется только в том случае, если вы создали произвольное приложение с большим количеством клиентов.
<code>-maxobjectsincache</code>	<i>number</i>	Задаёт максимальное количество объектов, сохраняемых CMS в кэше памяти. При увеличении количества объектов уменьшается количество необходимых вызовов базы данных, благодаря чему значительно повышается работоспособность CMS. Однако при размещении чрезмерного количества объектов в памяти, оставшегося количества памяти CMS может не хватить на обработку запросов. Максимальный предел равен 100000.
<code>-ndbqthreads</code>	<i>number</i>	Указывает количество рабочих потоков CMS, направляющих запросы в базу данных. Каждый поток связан с базой данных, поэтому соблюдайте осторожность и не превышайте допустимых объёмов базы данных. В большинстве случаев максимально допустимым значением является 20.

Параметр	Допустимые аргументы	Поведение
<code>-oobthreads</code>	<i>number</i>	Если в кластере находится более восьми членов кластера CMS, командная строка для каждого CMS обязательно должна содержать этот параметр: Он определяет количество служб CMS в кластере. Этот параметр гарантирует, что кластер сможет выдерживать серьезную нагрузку.
<code>-AuditeeTimeSyncInterval</code>	<i>minutes</i>	Определяет интервал между событиями синхронизации времени. CMS распространяет свои системные настройки времени на отслеживаемые серверы с интервалом, который задает параметр <code>AuditeeTimeSyncInterval</code> . Отслеживаемые серверы сравнивают собственные внутренние настройки времени с настройками времени CMS и соответствующим образом изменяют метку времени, назначаемую всем последующим записям аудита. Таким образом, параметры времени данных записей синхронизируются с настройками времени CMS. По умолчанию данный интервал равен 60 минутам. (Максимальное значение равно 1 дню, или 1440 минутам.) Минимальное значение составляет 15 минут. Если для параметра интервала установлено значение 0, синхронизация времени отключается).

См. также

- [Стандартные параметры для всех серверов](#)

22.3.4 Сервер обработки Crystal Reports и кэш-сервер Crystal Reports

Управление сервером обработки Crystal Reports и кэш-сервером Crystal Reports осуществляется сходным образом посредством командной строки. Параметры командной строки определяют, будет ли сервер запущен в качестве сервера обработки, кэш-сервера или обоих видов серверов одновременно. Ниже перечислены параметры, применимые только к одному из данных типов серверов.

В Windows по умолчанию используются следующие пути к данным серверам:

- `<INSTALLDIR>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\cacheserver.exe.`
- `<INSTALLDIR>\BusinessObjects Business Intelligence platform XI 4.0\win64_x64\pageserver.exe.`

В UNIX по умолчанию используются следующие пути к данным серверам:

- `<INSTALLDIR>/sap_bobj/enterprise_xi40/<ПЛАТФОРМА>/boe_cachesd.`
- `<INSTALLDIR>/sap_bobj/enterprise_xi40/<ПЛАТФОРМА>/boe_procd.`

Параметр	Допустимые аргументы	Поведение
<code>-cache</code>		Активирует функции кэш-сервера.
<code>-deleteCache</code>		Удаляет каталог кэша при каждом запуске и прекращении работы сервера.
<code>-report_ProcessExtPath</code>	<i>absolute path</i>	Указывает каталог по умолчанию для расширений обработки. Для получения дополнительной информации см. <i>Руководство администратора платформы SAP BusinessObjects Business Intelligence.</i>

См. также

- [Стандартные параметры для всех серверов](#)

22.3.5 Сервер обработки Dashboard Design и кэш-сервер Dashboard Design

Управление сервером обработки Dashboard Design и кэш-сервером Dashboard Design осуществляется во многом аналогично, из командной строки. Параметры командной строки определяют, будет ли сервер запущен в качестве сервера обработки, кэш-сервера или обоих видов серверов одновременно. Ниже перечислены параметры, применимые только к одному из данных типов серверов.

В Windows по умолчанию используются следующие пути к данным серверам:

- `<INSTALLDIR>\SAP BusinessObjects\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\xccache.exe.`
- `<INSTALLDIR>\SAP BusinessObjects\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\xcproc.exe.`

В UNIX по умолчанию используются следующие пути к данным серверам:

- `<INSTALLDIR>/sap_bobj/enterprise_xi40/<платформа>_64/boe_xccached.`
- `<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>_64/xcprocd.`

Параметр	Допустимые аргументы	Поведение
-cache		Активирует функции кэш-сервера.
-dir	<i>absolute path</i>	Определяет каталог кэша для кэш-сервера и временный каталог для сервера обработки. Создаются следующие каталоги: <i>absolute path/cache</i> и <i>absolute path/temp</i> .
-deleteCache		Удаляет каталог кэша при каждом запуске и прекращении работы сервера.
-psdir	<i>absolute path</i>	Определяет временный каталог сервера обработки. Данный параметр заменяет своим значением значение параметра -dir.

Параметр	Допустимые аргументы	Поведение
-refresh	<i>minutes</i>	Предоставляет кэшированные страницы через указанное количество минут.
-auditMaxEventsPerFile	<i>number</i>	На кэш-сервере задает максимальное количество действий аудита, записываемых в файл журнала аудита. По умолчанию используется значение 500. Если максимальное количество записей превышено, сервер открывает новый файл журнала.

См. также

- [Стандартные параметры для всех серверов](#)

22.3.6 Серверы заданий

В этом разделе содержатся сведения о параметрах командной строки для адаптивных серверов заданий.

Путь по умолчанию к серверу в ОС Windows – `<INSTALLDIR>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\JobServer.exe`.

Путь по умолчанию к серверу в ОС UNIX – `<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/boe_reportjobsd`.

Параметр	Допустимые аргументы	Поведение
-dir	<i>absolute path</i>	Определяет каталог данных для сервера заданий.

Параметр	Допустимые аргументы	Поведение
<code>-maxJobs</code>	<i>number</i>	Задаёт максимальное количество одновременно выполняемых заданий, которое может обработать сервер. По умолчанию используется значение 5.
<code>-requestJSChildPorts</code>	<i>lowerbound-upperbound</i>	<p>Определяет диапазон портов, которые должны использовать дочерние процессы в среде брандмауэра. Например, значение 6800–6805 задаёт для дочерних процессов ограничение в шесть портов.</p> <p>Примечание: Чтобы данный параметр вступил в силу, необходимо также задать параметр <code>-requestPort</code>.</p>
<code>-report_ProcessExtPath</code>	<i>absolutepath</i>	Указывает каталог по умолчанию для расширений обработки. Для получения дополнительной информации см. <i>Руководство администратора платформы SAP BusinessObjects Business Intelligence</i> .

См. также

- [Стандартные параметры для всех серверов](#)

22.3.7 Адаптивный сервер обработки

Адаптивный сервер обработки использует параметры, определённые для виртуальной машины SAP Java (SAP JVM). Для получения дополнительных сведений см. документацию по SAP JVM.

22.3.8 Сервер приложений отчетов

В этом разделе содержится информация по особым параметрам командной строки, относящимся только к серверу приложений отчетов.

Путь по умолчанию к серверу в ОС Windows – `<INSTALLDIR>\SAP BusinessObjects Business Intelligence platform 4.0\win32_x86\crystalras.exe`.

Путь по умолчанию к серверу в ОС UNIX –
`<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/ras/boe_crystalrasd`.

Параметр	Допустимые аргументы	Поведение
<code>-ipport</code>	<i>port</i>	Указывает номер порта для приема запросов TCP/IP при работе в автономном режиме (за пределами платформы SAP BusinessObjects Business Intelligence).
<code>-report_ProcessExtPath</code>	<i>absolutepath</i>	Указывает каталог по умолчанию для расширений обработки. Для получения дополнительной информации см. <i>Руководство администратора платформы SAP BusinessObjects Business Intelligence</i> .

Параметр	Допустимые аргументы	Поведение
<code>-ProcessAffinityMask</code>	<i>mask</i>	<p>Использует маску, чтобы точно определить ЦП, используемый сервером приложений отчетов при выполнении на многопроцессорном устройстве.</p> <p>Данная маска задана в формате <code>0xffffffff</code>, где каждый символ <i>f</i> представляет процессор, а список процессоров читается справа налево (т.е. последний символ <i>f</i> представляет первый процессор). Каждый символ <i>f</i> необходимо заменить либо на 0 (использовать ЦП запрещается), либо на 1 (использовать ЦП разрешается).</p> <p>Например, если сервер приложений отчетов запущен на устройстве с 4 процессорами и вам необходимо использовать 3-й и 4-й процессоры, используйте маску <code>0x1100</code>. Чтобы использовать 2-й и 3-й процессоры, используйте маску <code>0x0110</code>.</p> <p>Примечание:</p> <ul style="list-style-type: none"> Сервер приложений отчетов использует первый разрешенный процессор в строке вплоть до максимального значения, определяемого лицензией. Если вы обладаете лицензией на два процессора, маска <code>0x1110</code> будет действовать так же, как и <code>0x0110</code>. Значение маски по умолчанию равно <code>-1</code>, что равносильно значению <code>0x1111</code>.

См. также

- [Стандартные параметры для всех серверов](#)

22.3.9 Сервер обработки Web Intelligence

В этом разделе содержится информация по особым параметрам командной строки, относящимся только к серверу обработки Web Intelligence.

Путь по умолчанию к серверу в ОС Windows – `<INSTALLDIR>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\WIReportServer.exe`.

Путь по умолчанию к серверу в ОС UNIX –

`<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/WIReportServer`.

Параметр	Допустимые аргументы	Поведение
-ConnectionTimeout Минуты	<i>minutes</i>	Определяет количество минут, по истечении которых сервер переходит в режим ожидания.
-MaxConnections	<i>number</i>	Определяет максимальное количество одновременных подключений, разрешенных сервером.
-DocExpressEnable		Активирует кэширование документов Web Intelligence при их просмотре.
-DocExpressRealTime CachingEnable		Активирует кэширование документов Web Intelligence в режиме реального времени.
-DocExpressCache DurationMinutes	<i>minutes</i>	Определяет количество времени (в минутах), в течение которого содержимое сохраняется в кэше.

Параметр	Допустимые аргументы	Поведение
-DocExpressMaxCacheSizeKB	<i>kilobytes</i>	Определяет размер кэша для документов.
-EnableListOfValuesCache		Активирует кэширование списка значений для каждого сеанса пользователя.
-ListOfValuesBatchSize	<i>number</i>	Определяет максимальное количество значений, возвращаемых на пакет списка значений.
-UniverseMaxCacheSize	<i>number</i>	Определяет максимальное количество юниверсов для сохранения в кэше.
-WIDMaxCacheSize	<i>number</i>	Определяет максимальное количество документов Web Intelligence для сохранения в кэше.

См. также

- [Стандартные параметры для всех серверов](#)

22.3.10 Серверы репозитория входящих и исходящих файлов

В этом разделе содержится информация об особых параметрах командной строки, относящимся только к серверу репозитория входящих файлов.

Пути по умолчанию к серверам в ОС Windows – <INSTALLDIR>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\fileserver.exe

В UNIX по умолчанию используются следующие пути к программе, реализующей оба сервера:

- <INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_inputfilesd.
- <INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_outputfilesd.

Параметр	Допустимые аргументы	Поведение
<code>-rootDir</code>	<code>absolutepath</code>	<p>Задаёт корневой каталог для различных каталогов нижежащего уровня и файлов, управляемых сервером. Пути к файлам, используемые для ссылки на файлы на файловом сервере репозитория, интерпретируются по отношению к данному корневому каталогу.</p> <p>Примечание: Все серверы репозитория входящих файлов должны использовать один и тот же корневой каталог, а все серверы репозитория исходящих файлов – также один и тот же, но уже другой корневой каталог (во избежание проблемы несовместимости экземпляров). Кроме того, входящий корневой каталог не должен совпадать с исходящим корневым каталогом. Рекомендуется тиражировать корневые каталоги, используя массивы RAID или другое аппаратное решение.</p>

Параметр	Допустимые аргументы	Поведение
<code>-tempDir</code>	<i>absolutePath</i>	<p>Задаёт местоположение временного каталога, используемого сервером репозитория файлов для передачи файлов. Используйте этот параметр командной строки, если вам необходимо контролировать местоположение временного каталога файлового сервера репозитория или если имя временного каталога файлового сервера репозитория, по умолчанию создаваемое данным сервером, превышает ограничения системного пути к файлам (что препятствует запуску данного сервера).</p> <p>Примечание: Не выбирайте существующий каталог для данного параметра. Заданный каталог будет очищен при запуске файлового сервера репозитория и удален при завершении его работы. Если вы выберете существующий каталог, он также будет очищен и удален.</p>
<code>-maxidle</code>	<i>minutes</i>	Определяет количество минут, по истечении которого выполняется очистка бездействующего сеанса.

См. также

- [Стандартные параметры для всех серверов](#)

22.3.11 Сервер событий

В этом разделе содержится информация по особым параметрам командной строки, относящимся к серверу событий.

Путь по умолчанию к серверу в ОС Windows – `<INSTALLDIR>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\EventServer.exe`

Путь по умолчанию к серверу в ОС UNIX –

`<INSTALLDIR>/sap_bobj/enterprise_xi40/<платформа>/boe_eventsd`

Параметр	Допустимые аргументы	Поведение
<code>-poll</code>	<i>секунды</i>	Укажите частоту (в секундах) проверки на наличие событий файлов, выполняемой сервером.
<code>-cleanup</code>	<i>minutes</i>	Укажите частоту (в минутах) очистки прокси приемного устройства, выполняемой сервером. Данное значение определяет количество времени, в течение которого выполняются две очистки. Например, если задано значение 10, очистка прокси выполняется каждые 5 минут.

См. также

- [Стандартные параметры для всех серверов](#)

22.3.12 Сервера информационных панелей и аналитики информационных панелей

У серверов информационных панелей и серверов аналитики информационных панелей отсутствуют уникальные параметры командной строки для администрирования из командной строки.

Приложение "Права"

23.1 0 приложении "Права"

В приложении "Права" перечислено и описано большинство прав для доступа к различным объектам в системе платформы BI. В этом приложении перечислены также дополнительные права, которые требуются для выполнения какой-либо задачи над объектом, а также сами объекты, по отношению к которым необходимо иметь эти права. Для получения дополнительных сведений о настройке прав см. раздел *Настройка прав* в *Руководстве администратора платформы SAP BusinessObjects Business Intelligence*.

23.2 Общие права

Права, рассмотренные в данном разделе, применимы к различным типам объектов.

Примечание:

- Многие из этих прав имеют аналогичные права владельца. Права владельца действуют только для владельца объекта, в отношении которого проверяются права.
- Следующие права применимы только к объектам, которые можно запланировать:
 - Право «Составить расписание для запуска документа».
 - Право «Планирование от имени других пользователей».
 - Право «Составить расписание для адресатов».
 - Право «Просмотр экземпляров документа».
 - Право «Удалить экземпляры».
 - Право «Установить паузу и возобновить экземпляры документа».
 - Право «Повторное планирование экземпляров».

Право	Описание
«Просмотр объектов»	Позволяет просматривать объекты и их свойства. Если такое право по отношению к объекту отсутствует, объект будет скрыт в системе платформы BI. Это право является базовым и требуется для выполнения всех задач.
«Добавить объекты в каталог»	Позволяет добавить объекты в папку. Это право применимо также к объектам, которые ведут себя, как папки, например папки "Входящие", папки "Избранное" или пакеты объектов.
«Изменить объекты»	Позволяет изменять содержимое объекта и свойства объектов и папок.
«Изменить права пользователей на объекты»	Позволяет изменить настройки безопасности объекта.
«В безопасном режиме изменить права пользователей на объекты»	Позволяет назначить права или уровни доступа, которые вы уже имеете по отношению к объекту, другим пользователям. Для этого необходимо иметь данное право по отношению к пользователю и самому объекту. Для получения дополнительных сведений об этом праве см. главу «Установка прав» <i>Руководства администратора платформы SAP BusinessObjects Business Intelligence</i> .
«Задать серверные группы для обработки заданий»	Позволяет указать группу серверов для использования при обработке объектов. Данное право применимо только к объектам, для которых можно указать серверы обработки. Для указания группы серверов необходимо также иметь право «Изменить объекты» по отношению к объекту.
«Удалить объекты»	Позволяет удалить объекты и их экземпляры.
«Копировать объекты в другой каталог»	Позволяет создавать копии объектов в других папках CMS. Для этого также необходимо иметь право «Добавить объекты в каталог» по отношению к папке назначения. Примечание: При копировании объекта, его явно заданные параметры безопасности не копируются; новый объект наследует параметры безопасности от папки назначения, но явно заданные параметры необходимо установить снова.
«Тиражировать содержимое»	Позволяет тиражировать объекты в другую систему интегрированного развертывания.

Право	Описание
«Составить расписание для запуска документа»	Позволяет планировать объекты.
«Планирование от имени других пользователей»	<p>Позволяет планировать объекты для других пользователей и групп. Пользователи или группы, для которых выполняется планирование объекта, становятся владельцами экземпляра этого объекта.</p> <p>Для планирования объекта для других пользователей или групп также необходимы следующие права:</p> <ul style="list-style-type: none"> • Данное право по отношению к пользователю или группе. • Право «Составить расписание для запуска документа» по отношению к объекту.
«Составить расписание для адресатов»	<p>Позволяет выполнять следующие действия:</p> <ul style="list-style-type: none"> • Планировать объекты для адресатов, отличных от местоположения Enterprise по умолчанию. • Изменять установленные при планировании адресаты по умолчанию. <p>Для планирования объекта для адресатов необходимы также следующие права:</p> <ul style="list-style-type: none"> • Право «Составить расписание для запуска документа» по отношению к планируемому объекту. • Право «Добавить объекты в каталог» по отношению к папке "Входящие" получателя (при планировании для папки "Входящие"). • Право «Копировать объекты в другой каталог» по отношению к планируемому объекту (для отправки копии в папку "Входящие" вместо создания ярлыка).
«Просмотр экземпляров документа»	Позволяет просматривать экземпляры объекта. Это право является базовым и требуется для выполнения всех задач в отношении экземпляров объектов.

Право	Описание
«Удалить экземпляры»	Позволяет удалять только экземпляры объектов. Если у вас есть право «Удалить объекты», вам необязательно иметь это право, чтобы удалить экземпляры.
«Установить паузу и возобновить экземпляры документа»	Позволяет приостановить и возобновить выполнение экземпляров объекта.
«Повторное планирование экземпляров»	Позволяет повторно составить расписание для экземпляров объекта.

См. также

- [Права владельца](#)
- [Выбор параметров Изменить права пользователей на объекты](#)

23.3 Права для определенных типов объектов

23.3.1 Права доступа к папке

Для облегчения управления правами рекомендуется задавать права для папок, чтобы их содержимое наследовало эти настройки безопасности. Права доступа к папке включают:

- Общие права на доступ к объекту папки.
- Права для конкретных типов объектов на доступ к содержимому папки (например, право **Печать данных отчета** для отчета Crystal).

См. также

- [Права для конкретных типов объектов](#)

23.3.2 Категории

В данном разделе рассматриваются общие права, которые имеют особое значение в контексте их принадлежности к общим или персональным категориям.

Примечание:

Объекты в категориях не наследуют права, заданные для категорий.

Право	Описание
«Добавить объекты в каталог»	Позволяет создавать в категориях новые категории. Это право не требуется для добавления объектов в категорию.
«Редактировать объекты»	<p>Позволяет выполнять следующие действия:</p> <ul style="list-style-type: none"> • Изменять свойства категорий. • Помещать одну категорию в другую в качестве подкатегории. • Добавлять объекты в категорию. • Удалять объекты из категории. <p>Для помещения одной категории в другую в качестве подкатегории требуются также следующие права:</p> <ul style="list-style-type: none"> • Право «Удалить объекты» по отношению к исходной категории. • Право «Добавить объекты в каталог» по отношению к категории назначения.
«Удалить объекты»	Позволяет удалить категорию.

23.3.3 Примечания

Примечания позволяют пользователям оставлять комментарии к объектам, используя приложение "Дискуссии". Примечания объединены в темах дискуссий, которые считаются дочерними объектами обсуждаемых объектов. Для управления темами дискуссий можно задать права на уровне объекта или папки.

Права, рассмотренные в данном разделе, применимы только к примечаниям.

Право	Описание
Разрешить темы дискуссий	<p>Данное право позволяет выполнять следующие действия:</p> <ul style="list-style-type: none"> Начинать и отвечать на темы дискуссий. Просматривать примечания в теме дискуссий. Изменять или удалять опубликованные вами примечания.

23.3.4 Отчеты Crystal

Права, рассмотренные в данном разделе, применимы только к отчетам Crystal.

Примечание:

Эти права применимы, только если отчеты Crystal находятся в среде платформы BI. При загрузке отчетов Crystal на локальный диск эти права не действуют. Во избежание таких ситуаций вы можете отказать в праве «Загрузить файлы, связанные с данным объектом» по отношению к отчету Crystal.

Право	Описание
«Печать данных отчета»	Позволяет распечатать отчет.
«Обновить данные отчета»	Позволяет обновить данные отчета.
«Экспортировать данные отчета»	<p>Позволяет экспортировать данные отчета в любой формат при просмотре отчета в Интернете, используя средство просмотра Crystal Reports.</p> <p>Для экспорта данных отчета в формат RPT также необходимо иметь право «Загрузить файлы, связанные с данным объектом».</p>
«Загрузить файлы, связанные с данным объектом»	<p>Данное право позволяет выполнять следующие действия:</p> <ul style="list-style-type: none"> Экспортировать отчет в формат RPT. Открывать отчет в конструкторе Crystal Reports. Планировать отчет формата RPT для внешних адресатов.

23.3.5 Документы Web Intelligence

Права, рассмотренные в данном разделе, применимы только к документам Web Intelligence.

Право	Описание
«Использовать списки значений»	Позволяет использовать списки значений.
«Экспортировать данные отчета»	Позволяет экспортировать данные документов в форматы Excel, PDF, и CSV. Если у вас нет этого права, вы должны иметь право «Сохранить как CSV», «Сохранить в формате Excel» или «Сохранить в формате PDF». Эти права позволяют экспортировать документы только в указанные форматы.
«Скрипт запроса – разрешить просмотр (SQL , MDX...)»	Позволяет просматривать скрипты запросов (SQL и MDX).
«Обновить данные отчета»	Позволяет обновить данные документа.
«Изменить запрос»	Позволяет редактировать запросы в документе.
«Обновить список значений»	Позволяет обновлять списки значений для приглашений при создании приглашения или просмотре документа. Для этого также необходимо иметь право «Использовать списки значений» по отношению к документу.
«Сохранить как CSV»	Позволяет экспортировать документы только в формат CSV. Если у вас уже есть право «Экспортировать данные отчета» по отношению к документу, вам не требуется это право.

Право	Описание
«Сохранить в формате Excel»	Позволяет экспортировать документы только в формат Excel. Если у вас уже есть право «Экспортировать данные отчета» по отношению к документу, вам не требуется это право.
«Сохранить в формате PDF»	Позволяет экспортировать документы только в формат PDF. Если у вас уже есть право «Экспортировать данные отчета» по отношению к документу, вам не требуется это право.
«Отправка»	Позволяет отправлять документы в планировщик, в папку "Входящие" платформы BI или отправлять их в виде гиперссылок по электронной почте. Это право также дает пользователям рабочего стола Web Intelligence возможность отправлять документы в виде вложений электронной почты.

23.3.6 Пользователи и группы

Можно задать права на доступ к пользователям и группам так же, как и на доступ к другим объектам в среде платформы BI. В данном разделе рассматриваются права, которые применимы только к объектам-пользователям и объектам-группам, или общие права, которые имеют особое значение в контексте пользователей и групп.

Примечание:

- Пользователи и подгруппы могут наследовать права от принадлежности к группе.
- Создатель учетной записи пользователя считается владельцем учетной записи. Однако после создания учетной записи пользователя пользователь, для которого предназначена учетная запись, также считается ее владельцем.

Право	Описание
«Изменить объекты»	<p>Позволяет выполнять следующие действия:</p> <ul style="list-style-type: none"> Изменить свойства пользователя или группы. Управлять принадлежностью к группе. <p>Для добавления пользователя или группы в другую группу необходимо иметь это право по отношению к пользователю или группе и по отношению к группе-адресату.</p>
«Изменить пароль пользователя»	<p>Позволяет выполнять следующие действия:</p> <ul style="list-style-type: none"> Изменять пароль вашей учетной записи пользователя. Для этого также требуется право «Изменить объекты» по отношению к учетной записи пользователя. Изменять пароль учетной записи другого пользователя. Для этого также требуется право «Изменить объекты» и право «Изменение прав пользователей на объекты» по отношению к учетной записи пользователя. <p>Примечание:</p> <ul style="list-style-type: none"> Это право не влияет на следующие настройки пароля пользователя: <ul style="list-style-type: none"> «Пароль не ограничен по сроку действия» «Пользователю следует изменить пароль при следующем входе в систему» «Пользователь не может изменить пароль» Это право неприменимо к учетным данным для доступа к источнику данных юниверсов Business Objects.
«Подписаться на публикации»	Позволяет добавить пользователя в качестве получателя публикации.
«Планирование от имени других пользователей»	Позволяет планировать объекты от имени пользователя, вследствие чего этот пользователь становится владельцем экземпляра объекта. Для этого также необходимо иметь право «Планирование от имени других пользователей» по отношению к объекту.

23.3.7 Уровни доступа

Права, рассмотренные в данном разделе, применимы только к уровням доступа.

Право	Описание
«Использовать уровень доступа для назначения защиты»	Позволяет установить уровень доступа при добавлении принципалов в списки управления доступом к объектам. Для этого также требуется иметь право «Изменение прав пользователей на объекты» или право «Безопасное изменение прав пользователей на объекты» по отношению к принципалу и объекту. В случаях предоставления права «Безопасное изменение прав пользователей на объекты» вы также должны иметь тот же уровень доступа по отношению к объекту.

См. также

- [Выбор параметров Изменить права пользователей на объекты](#)

23.3.8 Рабочие пространства VI

В данном разделе рассматриваются общие права, которые управляют действиями конкретных пользователей по отношению к рабочим пространствам VI.

Право	Описание
«Добавить объекты в данную папку»	Позволяет добавлять меню в рабочее пространство VI. Однако данное право не позволяет добавлять модули или другие объекты в рабочее пространство VI. Для добавления меню в рабочее пространство VI необходимо также иметь право «Редактировать рабочие пространства VI».
«Редактировать объекты»	Данное право позволяет выполнять следующие действия: <ul style="list-style-type: none"> • Изменять свойства и содержимое рабочего пространства VI. • Изменять меню рабочего пространства VI. • Удалять рабочее пространство VI.

Права модулей и рабочие пространства VI

Модули – это шаблоны, предназначенные для вставки данных, которые требуется отображать в рабочем пространстве VI. Рабочее пространство VI состоит из одного или нескольких модулей.

Способ добавления модулей в репозиторий влияет на их настройки безопасности. В случае добавления модулей в репозиторий в качестве самостоятельных объектов можно задать общие

права для самих модулей; эти права реализуются при использовании модулей в рабочих пространствах BI.

23.3.9 Права юниверсов (.unv)

Права, описанные в этом разделе, применимы к юниверсам, созданным в средстве создания юниверсов – юниверсам .unv. Перечисленные права являются зависимыми от типа правами, применимыми только к юниверсам, или общими правами, имеющими особое значение в контексте юниверсов.

Примечание:

Права на доступ к юниверсам применимы только при импорте юниверсов из CMS в приложение средства создания юниверсов. Эти права не применяются при сохранении юниверса на локальный диск.

Право	Описание
«Добавить объекты в каталог»	Позволяет добавить наборы ограничений или объекты в юниверс. Для этого также необходимо иметь право «Редактировать ограничения по доступу».
«Просмотр объектов»	Обеспечивает доступ к юниверсу и возможность его просмотра.
«Редактировать объекты»	<p>Данное право позволяет выполнять следующие действия:</p> <ul style="list-style-type: none"> • Изменять юниверс в СМС или в средстве создания юниверсов. • Устанавливать или снимать блокировку юниверса. <p>Для разблокирования юниверса вам также необходимо иметь право «Разблокировать юниверс».</p>
«Удалить объекты»	Позволяет удалять юниверс.
«Транслировать объекты»	<p>Позволяет сохранять переведенные имена объектов юниверса, используя средство управления переводами.</p> <p>Примечание: Переводы также можно сохранять при явно предоставленном праве «Редактировать объекты», если нет явного отказа в праве «Транслировать объекты».</p>

Право	Описание
«Новый список значений»	<p>Данное право позволяет выполнять следующие действия:</p> <ul style="list-style-type: none"> • Сопоставлять объектам новые списки значений. • Редактировать существующие списки значений. <p>Примечание: Это право не лишает вас возможности создавать каскадные списки значений.</p>
«Печать юниверса»	Позволяет распечатать юниверс.
«Отображать значения таблицы или объекта»	Позволяет видеть значения, связанные с таблицами или объектами в юниверсе.
«Редактировать ограничения по доступу»	Позволяет редактировать ограничения по доступу к юниверсу.
«Разблокировать юниверс»	<p>Позволяет выполнять следующие действия:</p> <ul style="list-style-type: none"> • Разблокировать юниверс, если он был заблокирован другим пользователем. • Экспортировать юниверс из CMS. <p>Для разблокирования юниверса также требуется право «Редактировать объекты».</p>
«Доступ к данным»	Позволяет извлекать данные из юниверса и обновлять документы на основе юниверса. Для этого вам необходимо иметь это право также по отношению к приложению средство создания юниверсов, документу и подключению юниверса.
«Создание и редактирование запросов на основе юниверса»	Позволяет создавать документы и редактировать запросы, основанные на юниверсе.

23.3.10 Права юниверсов (.unx)

Права, описанные в этом разделе, применимы к юниверсам, созданным в средстве дизайна информации – юниверсам .unx. Перечисленные права являются зависимыми от типа правами, применимыми только к юниверсам, или общими правами, имеющими особое значение в контексте юниверсов.

Примечание:

Права юниверсов применимы только к юниверсам, опубликованным в репозитории. Эти права не применяются к юниверсам, сохраненным в локальной папке.

Право	Описание
«Просмотр объектов»	Обеспечивает доступ к юниверсу и возможность его просмотра.
«Редактировать объекты»	Позволяет повторно публиковать юниверс.
«Удалить объекты»	Позволяет удалять юниверс.
«Извлечь юниверс»	<p>Позволяет извлекать опубликованный юниверс и изменять его основные ресурсы (бизнес-уровень и основание данных) в средстве дизайна информации.</p> <p>Примечание: Для этого также требуется следующее право приложения средства дизайна информации: «Извлечь юниверс».</p>
«Изменить профили безопасности»	<p>Позволяет вставлять, изменять и удалять профили безопасности для юниверса в редакторе безопасности средства дизайна информации.</p> <p>Примечание: Это право не является обязательным для просмотра профилей безопасности или изменения параметров агрегирования профиля безопасности.</p>
«Назначить профили безопасности»	Позволяет назначать и отменять назначение профилей безопасности для пользователей и групп в редакторе безопасности средства дизайна информации.

Право	Описание
«Доступ к данным»	Позволяет извлекать данные из юниверса и обновлять документы на основе юниверса. В средстве дизайна информации это право позволяет просматривать результат, заданный на панели запросов.
«Создавать и редактировать запросы, основанные на этом юниверсе»	Позволяет создавать и редактировать запросы, основанные на юниверсе. В средстве дизайна информации это право позволяет открывать панель запросов и выполнять запрос для юниверса.
«Сохранить для всех пользователей»	Позволяет сохранять юниверс для всех пользователей. Примечание: Для этого также должно быть предоставлено право приложения средства дизайна информации «Сохранить для всех пользователей».

23.3.11 Уровни доступа к объектам для юниверсов

Дизайнеры при создании юниверса в средстве создания юниверсов или бизнес-уровня в средстве дизайна информации выполняют назначение уровня доступа к объекту для каждого объекта в юниверсе. Имеются следующие уровни доступа к объектам:

- Общий (по умолчанию)
- Управляемый
- С ограничениями
- Конфиденциальный
- Частный

После публикации юниверса в репозитории можно предоставлять доступ к объектам юниверса на основе уровней доступа к объектам, назначенным в приложении. Например, можно предоставить группе "Все" доступ "Общий". При этом пользователям группы "Все" предоставляется возможность видеть объекты в юниверсе, обозначенные как "Общий".

Каждый последующий уровень доступа к объектам предоставляет больший доступ к объектам, чем предыдущий. "Общий" является самым низшим уровнем. Для принципалов с доступом "Общий" возможен только просмотр объектов с назначением "Общий". Для принципалов с доступом "Управляемый" возможен просмотр объектов с назначением "Общий" и "Управляемый".

Наивысшим уровнем является "Частный". Он предоставляет принципалам доступ ко всем уровням доступа к объектам, т.е. ко всем объектам в юниверсе.

Примечание:

- Настройки безопасности на уровне доступа к объекту переопределяют все наследуемые юниверсом настройки безопасности.
- Для юниверсов .ipx настройки безопасности на уровне доступа к объекту учитываются наряду с безопасностью объекта, определенной профилем безопасности. Для получения дополнительной информации о профилях безопасности см. *Руководство пользователя средства дизайна информации*.

См. также

- [Назначение уровней доступа к объектам для юниверсов](#)

23.3.11.1 Назначение уровней доступа к объектам для юниверсов

Для установки защиты на уровне доступа к объектам для юниверсов вам необходимо иметь право **Изменение прав пользователей на объекты** по отношению к юниверсу.

1. Выберите юниверс в области «Юниверсы» центрального сервера управления.
2. Выберите **Действие > Безопасность юниверса**.
3. В диалоговом окне «Безопасность юниверса» для пользователя или группы выберите уровень доступа к объектам в списке **Уровень безопасности объектов**.

23.3.12 Права соединений

В данном разделе рассматриваются права, которые применимы только к соединениям юниверсов, или общие права, которые имеют особое значение в контексте соединений юниверсов. Эти права применяются к соединениям, опубликованным в репозитории.

Права реляционного соединения

Право	Описание
«Просмотр объектов»	Позволяет просмотреть соединение.
«Изменить объекты»	Позволяет изменять параметры соединения.
«Удалить объекты»	Позволяет удалить соединение.
«Копировать объекты в другой каталог»	Позволяет копировать соединение из одной папки в другую.
«Доступ к данным»	<p>Позволяет извлекать содержимое из заданной для соединения базы данных.</p> <p>В средстве дизайна информации это право позволяет просматривать данные таблиц для редакторов основания данных и соединения. Оно также позволяет выполнять предварительный просмотр результата, заданного на панели запросов.</p>
«Использовать соединение с компонентом Stored Procedures (сохраняемые процедуры)»	<p>Позволяет использовать хранимые процедуры в базе данных, указанной в соединении юниверса.</p> <p>Примечание: Это право применимо только к юниверсам .unv.</p>

Права соединения OLAP

Право	Описание
«Просмотр объектов»	Позволяет просмотреть соединение.
«Изменить объекты»	Позволяет изменять параметры соединения в редакторе соединения средства дизайна информации.
«Удалить объекты»	Позволяет удалить соединение.
«Копировать объекты в другой каталог»	Позволяет копировать соединение из одной папки в другую.

23.3.13 Программные приложения

23.3.13.1 СМС

Права, рассмотренные в данном разделе, применимы только к СМС.

Право	Описание
«Входить в систему СМС и выполнять просмотр объекта в СМС»	Позволяет войти в систему СМС.
«Разрешить доступ к диспетчеру экземпляров»	Обеспечивает доступ к диспетчеру экземпляров.
«Разрешить доступ к запросу взаимосвязей»	Позволяет выполнять запросы взаимосвязей в СМС.
«Разрешить доступ к запросу безопасности»	Позволяет выполнять запросы безопасности в СМС.

23.3.13.2 Стартовая панель VI

Права, описываемые в данном разделе, применимы только к стартовой панели VI.

Право	Описание
«Организовать»	Позволяет выполнять следующие действия: <ul style="list-style-type: none"> • Перемещать и копировать объекты. • Добавлять объекты в папку "Избранное". • Создавать ярлыки для доступа к объектам.
«Отправить в папку "Входящие" Business Objects»	Позволяет отправлять объекты адресатам в папке входящих BI.
«Отправить адресату электронной почты»	Позволяет отправлять объекты адресатам в папке входящих BI.
«Отправить в расположение файла»	Позволяет сохранять объекты в файле.
«Отправить в расположение FTP»	Позволяет сохранять объекты на FTP.

23.3.13.3 Рабочие пространства BI

Права, рассмотренные в данном разделе, применимы только к рабочим пространствам BI.

Право	Описание
«Создание рабочих пространств BI»	Разрешает пользователю создавать новые рабочие пространства BI и изменять существующие рабочие пространства BI.
«Редактирование объектов»	Разрешает пользователю создавать новые модули и изменять существующие модули.
«Изменение рабочих пространств BI»	Разрешает пользователю изменять существующие рабочие пространства BI. Пользователь не может создавать новые рабочие пространства BI.

23.3.13.4 Web Intelligence

Права в этом разделе применимы только к SAP BusinessObjects Web Intelligence (включая интерфейс рабочего стола) и могут влиять на средства просмотра и панели запросов в этих приложениях.

Право	Описание
«Данные – включить отслеживание данных»	Включает отслеживание измененных данных.
«Данные – включить форматирование измененных данных»	Позволяет выбирать формат для измененных данных.
«Интерфейс рабочего стола – включить Web Intelligence Desktop»	Позволяет использовать интерфейс рабочего стола.
«Интерфейс рабочего стола – включить локальных поставщиков данных»	Позволяет использовать поставщиков личных данных в интерфейсе рабочего стола.
«Интерфейс рабочего стола – экспорт документов»	Позволяет экспортировать документы в CMS в интерфейсе рабочего стола.
«Интерфейс рабочего стола – импорт документов»	Позволяет импортировать документы из CMS в интерфейсе рабочего стола.
«Интерфейс рабочего стола – установка со стартовой панели BI»	Позволяет загружать интерфейс рабочего стола со стартовой панели BI.
«Интерфейс рабочего стола – печать документов»	Позволяет печатать документы из интерфейса рабочего стола.
«Интерфейс рабочего стола – удаление безопасности документа»	Позволяет удалять безопасность для документа из интерфейса рабочего стола.
«Интерфейс рабочего стола – сохранить документ для всех пользователей»	Разрешает сохранение документов для всех пользователей из интерфейса рабочего стола.
«Интерфейс рабочего стола – сохранить документы локально»	Разрешает сохранение документов на локальный диск в интерфейсе рабочего стола.
«Интерфейс рабочего стола – отправить по почте»	Разрешает отправку документов по электронной почте в интерфейсе рабочего стола.
«Интерфейс рабочего стола – включить локальных поставщиков данных»	Позволяет использовать поставщиков личных данных в интерфейсе рабочего стола.

Право	Описание
«Документы – отключить автоматическое обновление при открытии»	Отключает автоматическое обновление документов при их открытии.
«Документы – включить автосохранение»	Разрешает автосохранение документов (если автосохранение включено в СМС администратором).
«Документы – включить создание»	Разрешает создание новых документов.
«Документы – включить публикацию и управление содержимым»	Разрешает публикацию документов в СМС.
«Интерактивный режим: создание отчетов – создание и редактирование сигнализаторов»	Включает создание и редактирование сигнализаторов в интерактивном средстве просмотра.
«Интерфейсы – включить насыщенное Интернет-приложение»	Разрешает использование интерфейса просмотра и редактирования полного Интернет-приложения (в предыдущих версиях – панель отчетов Java).
«Интерфейсы – включить интерфейс веб-просмотра»	Разрешает использование интерфейса веб-просмотра (в предыдущих выпусках – средство просмотра DHTML).
«Интерфейсы – включить панель веб-запросов»	Разрешает использование панели веб-запроса ("Запрос – HTML" в предыдущих выпусках).
«Общее – редактировать "Мои предпочтения"»	Разрешает изменение предпочтительных значений на стартовой панели BI.
«Общее – активизировать меню, вызываемые правой кнопкой мыши»	Разрешает использование меню, вызываемых правой кнопкой мыши.
«Левая панель – активизировать сводку документов»	Разрешает вывод сводки документа в левой панели.
«Левая панель – включить структуру и фильтры документа»	Разрешает вывод структуры и фильтров документа в левой панели.
«Скрипт запроса – включить изменение (SQL, MDX...)»	Разрешает изменение скриптов запросов (SQL и MDX).

Право	Описание
«Скрипт запроса – включить просмотр (SQL, MDX...)»	Разрешает просмотр скриптов запросов (SQL и MDX).
«Создание отчетов – создать и изменить разрывы»	Разрешает создание и изменение разрывов.
«Создание отчетов – создать и изменить правила условного форматирования»	Разрешает создание и изменение правил условного форматирования.
«Создание отчетов – создать и изменить предварительно определенные вычисления»	Разрешает создание и изменение предварительно определенных вычислений.
«Создание отчетов – создать и изменить элементы управления входом»	Разрешает создание и изменение элементов управления входом.
«Создание отчетов – создать и изменить фильтры отчета и использовать элементы управления входом»	Разрешает создание и изменение фильтров отчета и элементов управления входом. (Панель "Элементы управления вводом" не отображается на левой панели, если она отключена).
«Создание отчетов – создать и изменить сортировки»	Разрешает создание и изменение сортировок.
«Создание отчетов – создать формулы и переменные»	Разрешает создание формул и переменных.

Право	Описание
«Создание отчетов – включить форматирование»	Разрешает изменение форматирования отчета. Если в этом праве отказано, то режимы разработки и данных должны быть недоступны для пользователя (отключены).
«Создание отчетов – включить объединенные измерения»	Разрешает синхронизацию данных при помощи объединенных измерений в отчетах и в диспетчере данных.
«Создание отчетов – вставить и удалить отчеты, таблицы, диаграммы и ячейки»	Разрешает вставку и удаление отчетов, таблиц, диаграмм и ячеек. Также управляет рабочим процессом повторений (копирование/вставка).

23.3.13.5 Strategy Builder (Построитель стратегии)

Построитель стратегий – это инструмент, относящийся к приложению Performance Management (Управление производительностью). Права, рассмотренные в данном разделе, применимы только к Построителю стратегий и влияют на управление целями в приложении Performance Manager или на конкретные функции Построителя стратегий.

Право	Описание
«Создание, изменение или удаление целей»	Позволяет добавлять, редактировать или удалять цели в приложении Performance Manager.
«Просмотр целей»	Позволяет просматривать цели в аналитических данных, содержащих цели.
«Доступ к приложению Goal Management (Управление целями)»	Позволяет просматривать цели на странице «Goals Management» в приложении Performance Manager.
«Публиковать цели»	Позволяет опубликовывать цели в приложении Performance Manager.

Право	Описание
«Доступ к приложению Strategy Builder (Строитель стратегии)»	Обеспечивает доступ к инструменту Strategy Builder в приложении Performance Manager.
«Создание, изменение или удаление ролевых имен»	Позволяет управлять ролями, используемыми для опубликования целей или показателей для конкретной аудитории в Strategy Builder.
«Создание, изменение или удаление стратегий»	Позволяет создавать стратегии, которые связывают роли и опубликовывают цели и показатели в Strategy Builder.

23.3.13.6 Права средства создания юниверсов

Права, описанные в этом разделе, применяются к приложению средства создания юниверсов.

Право	Описание
«Проверять целостность юниверса»	Позволяет проверить целостность юниверса.
«Обновлять окно структуры»	Позволяет обновить окно структуры.
«Использовать средство обзора таблиц»	Позволяет просматривать данные базы данных, используя средство обзора таблиц.
«Применить ограничения юниверса»	Позволяет применить предварительно заданные ограничения юниверса к пользователям импортированного юниверса.
«Связать юниверс»	Позволяет связать два юниверса для общего доступа к компонентам.
«Создать, изменить или удалить соединения»	Позволяет создавать, изменять и удалять соединения юниверсов, хранящиеся в репозитории или в качестве персональных или совместно используемых соединений.

23.3.13.7 Права средства дизайна информации

Права, описанные в этом разделе, применяются к приложению средства дизайна информации.

Право	Описание
«Администрирование профилей безопасности»	Позволяет открывать редактор безопасности. Примечание: Для работы с профилями безопасности необходимо иметь права, предоставленные для юниверса.
«Совместное использование проектов»	Позволяет совместно использовать локальный проект и открывать представление "Синхронизировать проект" для синхронизации совместно используемого проекта с локальным проектом.
«Создать, изменить или удалить соединения»	Позволяет выполнять следующие действия: <ul style="list-style-type: none"> • создавать и удалять защищенные соединения в представлении "Опубликованные ресурсы" • изменять соединения в редакторе соединений • публиковать соединения в репозитории
«Опубликовать юниверс »	Позволяет опубликовать юниверсы в репозитории
«Извлечь юниверс»	Позволяет извлекать опубликованные юниверсы в локальный проект для их изменения.
«Сохранить для всех пользователей»	Позволяет использовать параметр сохранения для всех пользователей при извлечении юниверсов.
«Вычисление статистики»	Позволяет выбирать таблицы и столбцы для расчета и публикации статистики.

23.3.13.8 Виджеты для платформы SAP BusinessObjects Business Intelligence

Права, рассмотренные в этом разделе, применимы только для виджетов платформы SAP BusinessObjects Business Intelligence.

Право	Описание
«Использовать проводник»	Позволяет пользователям просматривать содержимое на всех подключенных серверах платформы BI при помощи проводника списка документов.
«Использовать папку "Входящие" для оповещений»	(Не рекомендуется) Позволяет использовать папку "Входящие" для оповещений.
«Использовать поиск»	Позволяет пользователям выполнять поиск сразу по всем подключенным репозиториям платформы BI, используя контекстный поиск.

23.3.13.9 Оповещение

Права, рассмотренные в данном разделе, применимы только к приложению Оповещение.

Право	Описание
«"Активация предупреждений"»	<p>Позволяет запускать предупреждающие события</p> <p>Чтобы запустить предупреждение для документа, необходимы следующие права:</p> <ul style="list-style-type: none"> • Права на просмотр и составление расписаний для документа • Права на просмотр и активацию для соответствующего события
«"Подписка на объекты"»	<p>Позволяет подписаться на предупреждающее событие</p> <p>Чтобы подписаться на событие, необходимы следующие права:</p> <ul style="list-style-type: none"> • Право просмотра соответствующего события • Право подписки на собственную учетную запись пользователя <p>Чтобы подписаться на предупреждение в документе, необходимы следующие права:</p> <ul style="list-style-type: none"> • Право просмотра документа • Право просмотра экземпляра документа • Право просмотра соответствующего события • Право подписки на собственную учетную запись пользователя

23.3.13.10 Explorer

Права, рассмотренные в данном разделе, применимы только к проводнику Explorer.

Право	Описание
«Вход в Explorer и просмотр объекта в СМС»	Позволяет войти в Explorer. Это право требуется для выполнения других задач в компоненте Explorer.
«Исследование информационных пространств»	Позволяет исследовать информационную область. Для выполнения данной задачи также требуется право на «Вход в Explorer и просмотр объекта в СМС».
«Исследование информационных пространств: экспорт в закладки/электронную почту»	Позволяет создавать закладки и отправлять закладки по электронной почте. Для выполнения этой задачи также необходимы следующие права: <ul style="list-style-type: none"> • «Вход в Explorer и просмотр объекта в СМС» • «Исследование информационных пространств»
«Исследование информационных пространств: экспорт в файл CSV»	Позволяет экспортировать результаты просмотра в формат CSV или файл Excel. Для выполнения этой задачи также необходимы следующие права: <ul style="list-style-type: none"> • «Вход в Explorer и просмотр объекта в СМС» • «Исследование информационных пространств»
«Исследование информационных пространств: экспорт в изображение»	Позволяет экспортировать результаты просмотра в графический файл. Для выполнения этой задачи также необходимы следующие права: <ul style="list-style-type: none"> • «Вход в Explorer и просмотр объекта в СМС» • «Исследование информационных пространств»
«Исследование информационных областей: экспорт в Web Intelligence»	Позволяет экспортировать результаты просмотра в виде запроса. Для выполнения этой задачи также необходимы следующие права: <ul style="list-style-type: none"> • «Вход в Explorer и просмотр объекта в СМС» • «Исследование информационных пространств»

Право	Описание
«Управление информационными областями»	<p>Позволяет получить доступ к меню "Управление пространствами" и выполнить соответствующие задачи.</p> <p>Для выполнения данной задачи также требуется право на «Вход в Explorer и просмотр объекта в СМС».</p>
«Управление информационными областями: создание новой области»	<p>Позволяет создать новую информационную область.</p> <p>Для выполнения этой задачи также необходимы следующие права:</p> <ul style="list-style-type: none"> • «Вход в Explorer и просмотр объекта в СМС» • «Управление информационными областями»
«Управление информационными областями: изменение области»	<p>Позволяет изменить или удалить информационную область.</p> <p>Для выполнения этой задачи также необходимы следующие права:</p> <ul style="list-style-type: none"> • «Вход в Explorer и просмотр объекта в СМС» • «Управление информационными областями»
«Управление информационными областями: индексация по расписанию»	<p>Позволяет вносить индексацию данных информационной области в расписание.</p> <p>Для выполнения этой задачи также необходимы следующие права:</p> <ul style="list-style-type: none"> • «Вход в Explorer и просмотр объекта в СМС» • «Управление информационными областями»
«Управление информационными областями: выполнение индексации»	<p>Позволяет использовать функцию индексации по отношению к данным информационной области</p> <p>Для выполнения этой задачи также необходимы следующие права:</p> <ul style="list-style-type: none"> • «Вход в Explorer и просмотр объекта в СМС» • «Управление информационными областями»

23.3.13.11 SAP BusinessObjects Mobile

Права, рассмотренные в данном разделе, применимы только к приложению SAP BusinessObjects Mobile.

Право	Описание
«Вход в приложение SAP BusinessObjects Mobile»	Гарантирует доступ к платформе BI через приложение Mobile и просмотр документов.
«Подписка на предупреждения документа»	<p>Предоставляет доступ к подписке на предупреждения документа/повторений.</p> <p>Примечание:</p> <ul style="list-style-type: none"> Если право подписки на предупреждения документа было предоставлено ранее и на данный момент в нем отказано, то рассылка предупреждений, на которые есть подписка, будет продолжена. Необходимо отменить подписку на предупреждения, если не следует их получать. Чтобы подписаться на предупреждения по документу (или на повторные экземпляры) для расписаний, пользователь должен иметь безопасный доступ "Полное управление" к папке "Системные события" в разделе "События" Central Management Console (CMC).
«Сохранить документы в локальное хранилище устройства»	<p>Предоставляет доступ к сохранению документов на мобильном устройстве.</p> <p>Примечание:</p> <p>Если документы сохранены на устройстве в момент, когда пользователю предоставлено право "Сохранение документов локально на устройстве", то документы останутся на устройстве, даже если право на сохранение было отозвано. Однако эти документы не будут синхронизироваться в процессе синхронизации.</p>
«Отправить документы с устройства как сообщение электронной почты»	Предоставляет доступ к отправленным отчетам по электронной почте.

Для получения дополнительных сведений см. *Руководство по установке и развертыванию SAP BusinessObjects Mobile*.

Приложение "Свойства серверов"

24.1 О приложении "Свойства серверов"

В приложении "Свойства серверов" перечислены и описаны свойства, которые можно задать для каждого сервера платформ BI.

24.1.1 Общие свойства сервера

Представленные в этом разделе свойства серверов применимы к серверам любого типа.

Таблица 24-1: Свойства порта запросов

Свойство	Описание	Значение по умолчанию
Имя сервера	Имя сервера	Значение по умолчанию – имя узла, на котором находится сервер, за которым следует имя самого сервера.
ID, CUID	Короткий идентификатор сервера и уникальный идентификатор сервера в кластере. Доступен только для чтения.	Эти значения создаются автоматически.
Узел	Имя узла, на котором расположен сервер.	Это значение задается во время установки.
Описание	Описание сервера	Значение по умолчанию – имя сервера.
Параметры командной строки	Параметры командной строки для сервера.	Значение по умолчанию зависит от типа сервера.

Свойство	Описание	Значение по умолчанию
Порт запросов	<p>Задаёт порт, из которого сервер получает запросы. Если в среде присутствуют брандмауэры, может потребоваться принудительно назначить серверу прослушивание только портов, которые открыты на брандмауэре. При задании порта для сервера убедитесь, что он не занят другим процессом.</p> <p>Примечание: Если включена функция Назначать автоматически, сервер будет привязан к динамически выделяемому порту. Это означает, что при каждом перезапуске сервера ему назначается произвольный номер порта.</p>	По умолчанию для параметра Назначать автоматически задано значение true, а поле параметра Порт запросов не заполнено.
Назначать автоматически	Указывает, выполняется ли привязка сервера при каждом его перезапуске к динамически размещённому порту. Для привязки сервера к определённому порту задайте для параметра Назначать автоматически значение true и укажите допустимый Порт запросов .	По умолчанию используется значение true.

Таблица 24-2: Свойства автозапуска

Свойство	Описание	По умолчанию
Автоматически запускать этот сервер при запуске агента Server Intelligence	<p>Определяет, будет ли сервер запускаться автоматически при запуске или перезапуске агента Server Intelligence (SIA).</p> <p>Если для этого параметра задано значение false, при запуске или перезапуске агента SIA сервер не начинает работу.</p>	По умолчанию используется значение true.

Таблица 24-3: Свойства идентификатора хоста

Свойство	Описание	По умолчанию
Назначать автоматически	Указывает на наличие привязки сервера к автоматически назначаемому сетевому интерфейсу. При значении FALSE сервер привязывается к определенному сетевому интерфейсу. При значении TRUE сервер принимает запросы по первому из доступных IP-адресов. На многосетевых компьютерах можно задать определенный сетевой интерфейс для привязки, установив для данного параметра значение FALSE и указав допустимое имя хоста или IP-адрес.	По умолчанию используется значение true.
Имя хоста	Имя хоста сетевого интерфейса, к которому привязан сервер. Если указано имя хоста, сервером принимаются запросы на всех IP-адресах, связанных с именем хоста.	По умолчанию для параметра Автоматическое назначение задано значение TRUE, а поле Имя хоста не заполнено.
IP-адрес	IP-адрес сетевого интерфейса, к которому привязан сервер. Поддерживаются протоколы IPv4 и IPv6. Если задан IP-адрес, сервером принимаются запросы только по этому IP-адресу.	По умолчанию для параметра Автоматическое назначение задано значение TRUE, а поле IP-адрес не заполнено.

Таблица 24-4: Свойства шаблона конфигурации

Свойство	Описание	По умолчанию
Использовать шаблон конфигурации	Указывает на необходимость использования шаблона конфигурации.	По умолчанию используется значение false.
Восстановить системные значения по умолчанию	Определяет восстановление исходных значений по умолчанию для данного сервера.	По умолчанию используется значение false.

Свойство	Описание	По умолчанию
Задать шаблон конфигурации	Определяет использование текущих настроек службы в качестве шаблона конфигурации для всех служб такого типа. Если для данного параметра задано значение true, все службы такого же типа, для которых выбран параметр Использовать шаблон конфигурации , моментально изменяют свои параметры в соответствии с параметрами текущей службы.	Значение по умолчанию – FALSE.

Таблица 24-5: Свойства службы протокола трассировки

Свойство	Описание	Значение по умолчанию
Уровень журнала	<p>Определяет минимальную серьезность предупреждения, которое необходимо записать, и количество информации, записываемой в серверный файл журнала.</p> <p>Возможные уровни порога журнала:</p> <ul style="list-style-type: none"> • Не определен • Нет • Низкий • Средний • Высокий 	По умолчанию используется значение Не определен.

См. также

- [Работа с шаблонами конфигурации](#)
- [Уровни журнала трассировки](#)

24.1.2 Свойства основных служб

В категорию "Основные службы" входят следующие серверы:

- Адаптивный сервер заданий
- Сервер адаптивной обработки
- Центральный сервер управления
- Сервер информационных панелей

- Сервер аналитики информационных панелей
- Сервер событий
- Сервер репозитория входящих файлов
- Сервер репозитория исходящих файлов
- Сервер контейнера веб-приложений

Свойства адаптивного сервера заданий

Таблица 24-6: Общие свойства

Свойство	Описание	Значение по умолчанию
Временный каталог	<p>Определяет каталог, в котором при необходимости создаются временные файлы. Если для данного каталога не выделено достаточное место на диске, могут возникнуть проблемы с производительностью. Для улучшения производительности этот каталог должен размещаться на локальном диске.</p> <p>Примечание: Для вступления в силу изменений требуется перезапустить данный сервер.</p>	%DefaultDataDir%

На адаптивном сервере заданий могут размещаться несколько разных служб. Для каждой службы имеются следующие свойства

Таблица 24-7: Свойства служб

Свойство	Описание	По умолчанию
Максимальное число параллельных заданий	<p>Определяет количество параллельно выполняемых независимых (дочерних) процессов, максимально допустимое для сервера. Максимальное количество заданий можно настроить в соответствии со средой составления отчетов.</p> <p>Настройки по умолчанию приемлемы для большинства сценариев составления отчетов. Идеальные параметры для среды составления отчетов зависят от конфигурации аппаратного обеспечения, программного обеспечения базы данных и требований к отчетам.</p>	По умолчанию используется значение 5.
Максимальное число запросов дочерних объектов	Указывает количество заданий, которые дочерний объект обрабатывает перед повторным запуском.	По умолчанию для данной настройки используется значение 100.

Свойства сервера адаптивной обработки

Таблица 24-8: Общие свойства

Свойство	Описание	По умолчанию
Время ожидания запуска службы (сек)	<p>Определяет количество времени в секундах, в течение которого сервер ожидает запуска служб.</p> <p>Если в течение указанного времени не удалось запустить службу, подобный сбой может возникнуть по одной из двух причин:</p> <ul style="list-style-type: none"> Служба может дать сбой по причине того, что не найдены необходимые ресурсы (например, база данных), либо по причине конфликта порта. Служба не может запуститься в течение указанного времени, поскольку система работает слишком медленно. <p>Для обнаружения причины обратитесь к файлу журнала сервера. Если службу не удалось запустить в течение указанного времени, возможно, это значение следует увеличить.</p>	По умолчанию используется значение 1200 секунд.

Свойства центрального сервера управления**Примечание:**

При изменении любого из этих свойств сервера необходимо перезапустить сервер, чтобы изменения вступили в силу.

Таблица 24-9: Свойства центрального сервера управления

Свойство	Описание	По умолчанию
Порт сервера имен	Определяет порт, на котором CMS прослушивает начальные запросы к службе имен.	По умолчанию используется значение 6400.

Свойство	Описание	По умолчанию
Запросы соединений с системной БД	<p>Определяет количество попыток соединения с системной базой данных CMS, предпринимаемых CMS. Если серверу не удастся установить все запрошенные соединения с базой данных, CMS продолжает работу, но с меньшей производительностью, так как меньшее количество параллельных запросов может быть обслужено одновременно. CMS продолжает попытки установления дополнительных соединений до установления запрошенного количества соединений.</p> <p>Показатель CMS Установленные соединения с системной базой данных показывает текущее число установленных соединений.</p>	По умолчанию используется значение 14.
Автоматическое повторное подключение к системной базе данных	<p>Определяет, будет ли CMS автоматически предпринимать попытки восстановления подключения к базе данных CMS в случае прерывания службы. Если для данного параметра задано значение false, можно проверить целостность базы данных CMS перед возобновлением операций. В этом случае для восстановления подключения к базе данных потребуется перезапуск CMS.</p>	По умолчанию используется значение TRUE.

Таблица 24-10: Свойства службы единого входа

Свойство	Описание	По умолчанию
Истечение срока действия единого входа (сек)	<p>Определяет период времени (в секундах), в течение которого подключение SSO к источнику данных остается действительным до окончания срока действия. Это применимо к выполняющимся отчетам пользователей Windows AD, для которых настроена процедура Windows AD SSO к источнику данных.</p>	По умолчанию используется значение 86400 секунд.

Свойства сервера событий

Таблица 24-11: Свойства службы событий

Свойство	Описание	По умолчанию
Интервал очистки (мин)	<p>Определяет периодичность запуска служебной программы для очистки в минутах.</p>	По умолчанию используется значение 20 минут.

Свойство	Описание	По умолчанию
Интервал опроса событий (в секундах)	Определяет периодичность, с которой сервер опрашивает файл, инициирующий события (в секундах).	По умолчанию используется значение 10 секунд. Допускаются значения в диапазоне от 1 до 1200.

Свойства сервера репозитория входных файлов

Таблица 24-12: Свойства службы хранилища входных файлов

Свойство	Описание	По умолчанию
Максимальное число повторных попыток доступа к файлам	Определяет количество попыток сервера получить доступ к определенному файлу.	Значение по умолчанию равно 1.
Максимальное время простоя (мин)	Определяет время ожидания сервера, по завершении которого он закрывает неактивные соединения. Если выбрать для данного параметра слишком низкое значение, запрос пользователя может оказаться закрыт до завершения обработки. Если же установить значение слишком высоким, может возникнуть чрезвычайный расход ресурсов системы, таких как время обработки и пространство диска.	По умолчанию используется значение 10 минут.
Временный каталог	Определяет каталог, в котором при необходимости создаются временные файлы. Примечание: Если для данного каталога не выделено достаточное место на диске, могут возникнуть проблемы с производительностью. Для обеспечения лучшей производительности рекомендуется располагать Временный каталог в той же файловой системе, в которой расположен Каталог хранения файлов .	%DefaultInputFRSDir%
Каталог хранилища файлов	Определяет каталог, в котором хранятся объекты репозитория файлов. Примечание: Если для данного каталога не выделено достаточное место на диске, могут возникнуть проблемы с производительностью.	%DefaultInputFRSDir%

Свойства сервера репозитория выходных файлов

Таблица 24-13: Свойства службы хранилища выходных файлов

Свойство	Описание	По умолчанию
Максимальное число повторных попыток доступа к файлам	Определяет количество попыток сервера получить доступ к определенному файлу.	Значение по умолчанию равно 1.
Максимальное время простоя (мин)	Определяет время ожидания сервера, по завершении которого он закрывает неактивные соединения. Если выбрать для данного параметра слишком низкое значение, запрос пользователя может оказаться закрыт до завершения обработки. Если же установить значение слишком высоким, может возникнуть чрезвычайный расход ресурсов системы, таких как время обработки и пространство диска.	По умолчанию используется значение 10 минут.
Временный каталог	Определяет каталог, в котором при необходимости создаются временные файлы. Примечание: Если для данного каталога не выделено достаточное место на диске, могут возникнуть проблемы с производительностью.	%DefaultOutputDir%
Каталог хранилища файлов	Определяет каталог, в котором хранятся объекты репозитория файлов. Примечание: Если для данного каталога не выделено достаточное место на диске, могут возникнуть проблемы с производительностью.	%DefaultOutputDir%

Свойства сервера контейнера веб-приложений

Таблица 24-14: Общие свойства

Свойство	Описание	По умолчанию
Время ожидания запуска службы (сек)	<p>Время, в течение которого WACS ожидает запуска размещаемых на нем служб. Если время ожидания закончилось, WACS не будет предоставлять еще не запущенные службы. Если компьютер работает медленно, можно задать большее значение.</p> <p>Если задано недостаточное время ожидания, которое истекает раньше, чем происходит запуск WACS, следует восстановить настройки по умолчанию WACS в CCM.</p>	По умолчанию используется значение 600 секунд.

Таблица 24-15: Свойства службы веб-приложения BOE

Тип свойства	Описание	Значение по умолчанию
Тип аутентификации	<p>Тип аутентификации, который используется при входе пользователей на стартовую панель BI.</p> <p>Допустимы следующие значения:</p> <ul style="list-style-type: none"> • AD Kerberos • Служба SSO AD Kerberos • Enterprise • LDAP 	Значение по умолчанию – Enterprise .

Тип свойства	Описание	Значение по умолчанию
Домен AD по умолчанию	Используется домен Active Directory по умолчанию, чтобы пользователям не нужно было указывать домен при входе в систему. Например, если установлен домен по умолчанию «mydomain», а пользователь выполняет вход с именем пользователя «user», то система проверки регистрации Active Directory пытается выполнить аутентификацию «user@mydomain.com».	По умолчанию значение не указано.
Имя администратора доступа к службе	Имя принципала службы (SPN) используется клиентами для однозначной идентификации экземпляра службы. Служба аутентификации Kerberos использует SPN для проверки подлинности службы.	По умолчанию значение не указано.
Файл ярлыков ключей	Полный путь к файлу ярлыков ключей. Файл ярлыков ключей позволяет настраивать Kerberos Filters без предоставления пароля учетной записи пользователя компьютеру веб-приложений.	По умолчанию значение не указано.

Таблица 24-16: Свойства веб-служб Web Services SDK и QaaWS

Свойство	Описание	Значение по умолчанию
Включить единый вход в Active Directory с Kerberos	Включить ли единый вход в Kerberos AD для веб-служб Web Services SDK и QaaWS.	Значение по умолчанию – FALSE.
Домен AD по умолчанию	Используется домен Active Directory по умолчанию, чтобы пользователям не нужно было указывать домен при входе в систему.	По умолчанию значение не указано.

Свойство	Описание	Значение по умолчанию
Имя администратора доступа к службе	Имя принcipала службы (SPN) используется клиентами для однозначной идентификации экземпляра службы. Служба аутентификации Kerberos использует SPN для проверки подлинности службы.	По умолчанию значение не указано.
Файл ярлыков ключей	Полный путь к файлу ярлыков ключей. Файл ярлыков ключей позволяет настраивать Kerberos Filters без предоставления пароля учетной записи пользователя компьютеру веб-приложений.	По умолчанию значение не указано.

Таблица 24-17: Свойства конфигурации HTTP

Свойство	Описание	По умолчанию
Привязка ко всем IP-адресам	Разрешает или запрещает привязку ко всем сетевым интерфейсам. Если у сервера более одной сетевой интерфейсной платы и требуется привязка к определенному сетевому интерфейсу, снимите флажок с этого свойства.	По умолчанию используется значение TRUE.
Привязать к имени хоста или IP-адресу	Определяет сетевой интерфейс (IP-адрес или имя хоста), посредством которого предоставляется служба HTTP. Для указания значения снимите флажок с поля Привязка ко всем IP-адресам .	По умолчанию используется значение localhost.
Порт HTTP	Порт, через который предоставляется служба HTTP.	По умолчанию используется значение 6405. Допускаются значения в диапазоне от 1 до 65535.
Максимальный размер заголовка HTTP	Максимальный допустимый размер (в байтах) запроса и ответа заголовка HTTP.	По умолчанию используется значение 32768.

Таблица 24-18: Конфигурация свойств HTTP через прокси

Свойство	Описание	По умолчанию
Включить HTTP через прокси	Разрешает или запрещает активацию соединителя HTTP через прокси на WACS. Как правило, в развертываниях с обратным прокси флажок данного параметра бывает выставлен.	По умолчанию используется значение FALSE.
Привязка ко всем IP-адресам	Привязывать ли порт HTTP через прокси ко всем сетевым интерфейсам.	По умолчанию используется значение TRUE.
Привязать к имени хоста или IP-адресу	Определяет сетевой интерфейс (IP-адрес или имя хоста), посредством которого предоставляется служба HTTP через прокси. Для указания значения снимите флажок с поля Привязка ко всем IP-адресам .	По умолчанию используется значение localhost.
Порт HTTP	Порт, через который предоставляется служба HTTP в развертываниях с обратным прокси. Для указания значения поставьте флажок в поле Включить HTTP через прокси .	По умолчанию используется значение 6406. Допускаются значения в диапазоне от 1 до 65535.
Имя хоста прокси	Адрес IPv4, адрес IPv6, имя хоста или полностью определенное имя домена прокси-сервера. Для указания значения поставьте флажок в поле Включить HTTP через прокси .	По умолчанию значение не указано.
Порт прокси	Порт прямого или обратного прокси-сервера. Для указания значения поставьте флажок в поле Включить HTTP через прокси .	По умолчанию используется значение 0. Допускаются значения в диапазоне от 1 до 65535.
Максимальный размер заголовка HTTP	Максимальный допустимый размер (в байтах) запроса и ответа заголовка HTTP.	По умолчанию используется значение 32768.

Таблица 24-19: Свойства конфигурации HTTPS

Свойство	Описание	По умолчанию
Включить HTTPS	Включать ли связь HTTPS/SSL.	Значение по умолчанию – FALSE.
Привязать к имени хоста или IP-адресу	Определяет сетевой интерфейс (IP-адрес или имя хоста), посредством которого предоставляется служба HTTPS. Для указания значения поставьте флажок в поле Включить HTTPS .	По умолчанию используется значение localhost.
Порт HTTPS	Порт, через который предоставляется служба HTTPS. Для указания значения поставьте флажок в поле Включить HTTPS .	По умолчанию используется значение 443. Допускаются значения в диапазоне от 1 до 65535.
Имя хоста прокси	Адрес IPv4, адрес IPv6, имя хоста или полностью определенное имя домена прокси-сервера. Для указания значения поставьте флажок в поле Включить HTTPS .	По умолчанию значение не указано.
Порт прокси	Порт прямого или обратного прокси-сервера. Для указания значения поставьте флажок в поле Включить HTTPS .	По умолчанию используется значение 0. Допускаются значения в диапазоне от 1 до 65535.
Протокол	Используемый протокол шифрования. Для указания значения поставьте флажок в поле Включить HTTPS .	По умолчанию используется значение TLS. Допускаются значения TLS или SSL.
Тип хранилища сертификатов	Тип хранилища сертификатов, в котором содержатся сертификаты и секретные ключи. В большинстве случаев для данного параметра используется значение PKCS12 . Для указания значения поставьте флажок в поле Включить HTTPS .	По умолчанию используется значение PKCS12. Допускаются значения PKCS12 или JKS.

Свойство	Описание	По умолчанию
Местоположение файла хранилища сертификатов	Полный путь к файлу сертификатов. Для указания значения поставьте флажок в поле Включить HTTPS .	По умолчанию значение не указано.
Пароль доступа к секретным ключам	У хранилища сертификатов PKCS12 и хранилища ключей JKS имеются секретные ключи, которые защищены паролем для предотвращения неавторизованного доступа или кражи. Введите пароль, заданный на более раннем этапе при создании хранилища сертификатов, чтобы разрешить WACS доступ к личным ключам из хранилища сертификатов. Для указания значения поставьте флажок в поле Включить HTTPS .	По умолчанию значение не указано.
Псевдоним сертификата	Псевдоним сертификата внутри хранилища сертификатов. Если это не указано и используется хранилище сертификатов, в котором содержится более одного сертификата, то используется первый сертификат в хранилище. В большинстве случаев для данного параметра не нужно указывать значение. Для указания значения поставьте флажок в поле Включить HTTPS .	По умолчанию значение не указано.
Включить аутентификацию клиента	Если включена аутентификация клиентов, то получить доступ к службам WACS могут только клиенты, у которых есть ключи в файле списка надежных сертификатов. Другие клиенты отклоняются. Для включения аутентификации клиентов поставьте флажок в поле Включить HTTPS .	По умолчанию используется значение FALSE.

Свойство	Описание	По умолчанию
Местоположение файла списка надежных сертификатов	Полный путь к файлу списка надежных сертификатов. Для указания значения поставьте флажки в поля Включить HTTPS и Включить аутентификацию клиента .	По умолчанию значение не указано.
Пароль доступа к секретным ключам списка надежных сертификатов	Пароль, который защищает доступ к секретным ключам в файле списка надежных сертификатов. Для указания значения поставьте флажки в поля Включить HTTPS и Включить аутентификацию клиента .	По умолчанию значение не указано.
Максимальный размер заголовка HTTP	Максимальный допустимый размер (в байтах) запроса и ответа заголовка HTTP.	По умолчанию используется значение 32768.

Таблица 24-20: Параметры параллельного выполнения (на один соединитель)

Свойство	Описание	По умолчанию
Максимальное число параллельных запросов	Количество параллельных запросов HTTP или HTTPS, которое каждый из соединителей (HTTP, HTTP через прокси или HTTPS) может обработать одновременно.	Значение по умолчанию – 150. Допускаются значения в диапазоне от 1 до 1000.

Таблица 24-21: Параметры конфигурации Active Directory

Свойство	Описание	По умолчанию
Расположение файла Krb5.ini	Полный путь к файлу <code>krb5.ini</code> , в котором хранятся свойства конфигурации Kerberos.	По умолчанию значение не указано.
Расположение файла bscLogin.conf	Полный путь к файлу <code>bscLogin.conf</code> .	По умолчанию значение не указано.

24.1.3 Свойства служб соединения

Категория служб подключений включает следующие службы:

- Служба прямого соединения (расположена на автономном сервере)
- Служба прямого соединения (32-битная на автономном сервере)
- Служба адаптивного соединения (расположена на APS)

Все службы используют одни и те же параметры конфигурации.

Таблица 24-22: Свойства операции службы

Свойство	Описание	Значение по умолчанию
Помните: Нет необходимости перезапускать сервер после изменения следующих свойств операции службы.		
Создание пула соединений	Включает или отключает пул соединений. Возможные значения: <ul style="list-style-type: none"> • Включено – со временем ожидания • Включено – без времени ожидания • Отменено Примечание: Пул соединений является набором функций кэширования, которые поддерживают соединения в состоянии возможности повторного использования для повышения производительности сервера.	Включено – со временем ожидания
Время ожидания пула подключений	Задаёт максимальное время простоя для соединений в пуле (в минутах). Примечание: Это свойство эквивалентно параметру <code>Max Pool Time</code> файла <code>cs.cfg</code> . Отключение пула эквивалентно тому, что параметр <code>Max Pool Time</code> установлен в 0. Включение пула без времени ожидания эквивалентно тому, что параметр <code>Max Pool Time</code> установлен в -1. Для получения дополнительных сведений см. <i>Руководство по доступу к данным</i> .	60

Свойство	Описание	Значение по умолчанию
Время бездействия временных объектов	Задаёт, сколько минут должен сохраняться неиспользуемый временный объект на сервере. После этого интервала объект удаляется, а его ресурсы возвращаются.	60
Интервал таймера временных объектов	Задаёт время между проверками активности (в минутах). Через регулярные интервалы сервер ищет возможный объект для удаления.	5
Включить образование блоков HTTP	<p>Включает или отключает образование блоков HTTP.</p> <p>Примечание: Образование блоков HTTP относится только к трехуровневому развертыванию. Оно влияет на производительность открытия и обновления документа, поскольку большие ответы означают меньшие циклы при получении больших документов. Отключение образования блоков HTTP эквивалентно установлению размера блока HTTP в 0.</p>	Включено
Размер блока HTTP	Задаёт размер (в килобайтах) ответов HTTP, посылаемых сервером.	64

Таблица 24-23: Свойства отслеживания низкого уровня

Свойство	Описание	Значение по умолчанию
<p>Помните:</p> <p>Нет необходимости перезапускать сервер после изменения следующих свойств отслеживания низкого уровня.</p>		
Включение отслеживания заданий	<p>Включает отслеживание заданий сервера соединений.</p> <p>Примечание: Для отслеживания необходимо, чтобы свойство Уровень журнала было установлено в значение Высокий.</p>	Отменено

Свойство	Описание	Значение по умолчанию
Включить отслеживание программного обеспечения среднего яруса	<p>Включает трассировку всего промежуточного ПО. Для трассировки конкретного промежуточного ПО необходимо настроить файл <code>cs.cfg</code> и перезапустить сервер.</p> <p>Примечание: Для отслеживания необходимо, чтобы свойство Уровень журнала было установлено в значение Высокий.</p>	Отменено

Таблица 24-24: Свойства источников данных Active Data

Свойство	Описание	Значение по умолчанию
<p>Предупреждение: После изменения следующих свойств источников данных Active Data необходимо перезапустить сервер.</p>		
Активация источника данных	<p>Позволяет выбирать источники данных, для которых требуются соединения. Данное свойство используется в качестве фильтра для драйверов. Активные источники данных указываются для загрузки требуемых драйверов</p> <p>Предупреждение: По умолчанию сервер загружает все доступные драйверы. Этот параметр используется для специализации серверов. Он особенно полезен при развертывании нескольких серверов CORBA в сети.</p> <p>Помните: Драйверы загружаются только для выбранных источников данных. Все другие игнорируются. Если источники данных не выбраны, сервер загружает все доступные драйверы.</p> <p>Примечание: Проверьте в показателях сервера включение выбранных источников данных. Сетевые уровни и базы данных отображаются под «показателями службы соединений».</p>	Не отмечено

Свойство	Описание	Значение по умолчанию
Сетевой уровень	<p>Задаёт сетевой уровень, используемый соединением.</p> <p>Примечание: Рассматривается только не локализованное имя. Список доступных сетевых уровней содержится в файле <code>driver.cfg</code>, находящийся в папке <code>connectionserver-install-dir\connectionServer</code>.</p>	<ul style="list-style-type: none"> • ODBC для собственных серверов CORBA • JDBC для адаптивного сервера CORBA
База данных	<p>Задаёт базу данных, используемую соединением.</p> <p>Примечание: Рассматривается только не локализованное имя. Имена баз данных могут быть регулярными выражениями, если они представлены строками только в кодировке ASCII. Шаблоны используют синтаксис регулярных выражений GNU. Используйте шаблон <code>.*</code> для соответствия любому символу. Например <code>MS SQL Server</code>. Выражение <code>*\$</code> означает, что используются все базы данных MS SQL Server. Дополнительную информацию о регулярных выражениях см. на веб-сайте PERL по адресу http://www.perl.com/doc/manual/html/pod/perlte.html#Regular_Expressions.</p>	Поле остается пустым, пока в него не будет введено имя базы данных.

См. также

- [Общие свойства сервера](#)

24.1.4 Свойства служб Crystal Reports

В категорию служб Crystal Reports входят следующие серверы:

- Кэш-сервер Crystal Reports
- Сервер обработки Crystal Reports
- Свойства сервера приложений отчетов Crystal Reports 2011
- Сервер обработки Crystal Reports 2011

Свойства кэш-сервера Crystal Reports

Для любых свойств, применимых одновременно к кэш-серверу Crystal Reports и серверу обработки Crystal Reports, необходимо задать одинаковые значения. Например, если на кэш-сервер для параметра **При обновлении средства просмотра всегда выдаются текущие данные** задано значение true, необходимо задать для того же параметра значение true на сервере обработки.

Примечание:

При изменении любого из этих свойств сервера необходимо перезапустить сервер, чтобы изменения вступили в силу.

Таблица 24-25: Свойства службы кэша Crystal Reports

Свойство	Описание	По умолчанию
При обновлении средства просмотра всегда выдаются текущие данные	<p>Определяет, будут ли игнорироваться все станицы в кэше при явном обновлении отчета пользователем и будут ли при этом новые данные извлекаться непосредственно из базы данных.</p> <p>Примечание: Это свойство можно задать непосредственно в объекте отчета. Его значение для разных отчетов может отличаться, при этом значения, заданные в объекте отчета, имеют приоритет перед параметрами сервера. Для установки значения в объекте отчета выберите отчет в СМС и щелкните Установки по умолчанию > Просмотр группы серверов.</p>	По умолчанию используется значение true.
Предоставлять совместный доступ к данным отчета для клиентов	<p>Определяет необходимость совместного использования данных отчетов несколькими клиентами.</p> <p>Примечание: Это свойство можно задать непосредственно в объекте отчета. Его значение для разных отчетов может отличаться, при этом значения, заданные в объекте отчета, имеют приоритет перед параметрами сервера.</p>	По умолчанию используется значение true.
Тайм-аут простоя соединения (мин)	Определяет время в минутах, в течении которого кэш-сервер Crystal Reports ожидает запроса при простое соединения. Как правило, изменять значение по умолчанию не требуется.	По умолчанию используется значение 20 минут.
Таймаут кеша безопасности (в минутах)	Задает время (в минутах), когда сервером используется кэшированная информация об учетных данных для входа, параметрах отчета и соединении с базой данных для обслуживания отчетов перед отправкой запроса в СМС.	По умолчанию используется значение 20 минут.

Свойство	Описание	По умолчанию
Самые старые данные, выданные клиентам по запросам (сек)	<p>Определяет период времени (в секундах), в течение которого сервер использует кэшированные данные для обслуживания запросов из отчетов, открытых по запросу. Если сервер получает запрос, которому необходимы данные, использовавшиеся предыдущим запросом, и время, прошедшее с момента обработки предыдущего запроса, меньше указанного здесь значения, то сервер будет повторно использовать данные, необходимые следующему запросу. Такое повторное использование данных значительно повышает производительность системы в случае, если нескольким пользователям нужна одна и та же информация. При выборе значения для данного параметра следует определить, насколько важное значение имеет актуальность получаемых пользователями данных. Если это очень важно для всех пользователей (например, в случае, когда важные данные быстро меняются), вам может понадобиться отменить такое повторное использование данных, установив значение равным 0.</p> <p>Примечание: Это свойство можно задать непосредственно в объекте отчета. Его значение для разных отчетов может отличаться, при этом значения, заданные в объекте отчета, имеют приоритет перед параметрами сервера.</p>	По умолчанию используется значение 0 секунд.
Максимальный размер кэша (кбайт)	Определяет объем пространства жесткого диска (в Кб), используемого для кэширования отчетов. Значительный размер кэша может понадобиться в том случае, если серверу необходимо обрабатывать большое число отчетов или особо сложные отчеты.	По умолчанию используется значение 256000 Кб.
Каталог файлов кэша	Определяет местоположение каталога файлов кэша.	Default Crystal Reports
Аргументы Java VM	Задаёт аргументы командной строки, которые могут быть предоставлены JVM.	Значение по умолчанию не указано.

Свойства сервера обработки Crystal Reports

Для любых свойств, применимых одновременно к кэш-серверу Crystal Reports и серверу обработки Crystal Reports, необходимо задать одинаковые значения. Например, если на кэш-сервер для

параметра **При обновлении средства просмотра всегда выдаются текущие данные** задано значение true, необходимо задать для того же параметра значение true на сервере обработки.

Примечание:

При изменении любого из этих свойств сервера необходимо перезапустить сервер, чтобы изменения вступили в силу.

Таблица 24-26: Свойства службы обработки Crystal Reports

Свойство	Описание	По умолчанию
Предельное время простоя задания (мин)	Определяет продолжительность периода ожидания сервером обработки Crystal Reports между запросами определенного задания (в минутах).	По умолчанию используется значение 60 минут.
Максимальное количество заданий на весь срок службы для каждого дочернего объекта	Определяет максимальное количество заданий, которое может обработать каждый дочерний объект за весь срок службы.	По умолчанию используется значение 1000.
При обновлении средства просмотра всегда выдаются текущие данные	Определяет, будут ли игнорироваться все станицы в кэше при явном обновлении отчета пользователем и будут ли при этом новые данные извлекаться непосредственно из базы данных. Определяет необходимость совместного использования данных отчетов несколькими клиентами. Примечание: Это свойство можно задать непосредственно в объекте отчета. Его значение для разных отчетов может отличаться, при этом значения, заданные в объекте отчета, имеют приоритет перед параметрами сервера. Для установки значения в объекте отчета выберите отчет в СМС и щелкните Установки по умолчанию > Просмотр группы серверов .	По умолчанию используется значение true.
Предоставлять совместный доступ к данным отчета для клиентов	Определяет необходимость совместного использования данных отчетов несколькими клиентами. Определяет необходимость совместного использования данных отчетов несколькими клиентами. Примечание: Это свойство можно задать непосредственно в объекте отчета. Его значение для разных отчетов может отличаться, при этом значения, заданные в объекте отчета, имеют приоритет перед параметрами сервера.	По умолчанию используется значение true.

Свойство	Описание	По умолчанию
Тайм-аут простоя соединения (мин)	Определяет время в минутах, в течении которого сервер обработки Crystal Reports ожидает запроса при простое соединения. Как правило, изменять значение по умолчанию не требуется.	По умолчанию используется значение 20 минут.
Максимальное число параллельных заданий (0 для автоматического вычисления)	Определяет максимальное количество независимых заданий, одновременно выполняемое сервером обработки Crystal Reports. Если для данного свойства задано значение «0», сервер применяет соответствующее значение в зависимости от ЦП и памяти компьютера, на котором он запущен.	По умолчанию это значение равно 0.
Самые старые данные, выданные клиентам по запросам (сек)	<p>Определяет период времени (в секундах), в течение которого сервер использует кэшированные данные для обслуживания запросов из отчетов, открытых по запросу. Если сервер получает запрос, которому необходимы данные, использовавшиеся предыдущим запросом, и время, прошедшее с момента обработки предыдущего запроса, меньше указанного здесь значения, то сервер будет повторно использовать данные, необходимые следующему запросу. Такое повторное использование данных значительно повышает производительность системы в случае, если нескольким пользователям нужна одна и та же информация. При выборе значения для данного параметра следует определить, насколько важное значение имеет актуальность получаемых пользователями данных. Если это очень важно для всех пользователей (например, в случае, когда важные данные быстро меняются), вам может понадобиться отменить такое повторное использование данных, установив значение равным 0.</p> <p>Примечание: Это свойство можно задать непосредственно в объекте отчета. Его значение для разных отчетов может отличаться, при этом значения, заданные в объекте отчета, имеют приоритет перед параметрами сервера.</p>	По умолчанию это значение равно 0.

Свойство	Описание	По умолчанию
Максимальное число предварительно запущенных дочерних процессов	Определяет максимальное количество предварительно запущенных процессов, разрешенное сервером. Если для данного параметра задано слишком низкое значение, сервер создает дочерние процессы при поступлении запроса, что может вызвать задержку в обслуживании. Если же значение слишком велико, то простаивающие дочерние процессы могут напрасно расходовать системные ресурсы.	По умолчанию задан 1 дочерний процесс.
Временный каталог	Определяет каталог, в котором при необходимости создаются временные файлы. Примечание: Если для данного каталога не выделено достаточное место на диске, могут возникнуть проблемы с производительностью.	%TEMP%\Crystal Reports
Путь к классу Java	Имена классов Java и путь к этим классам, требуемые сервером.	%CommondH%\ocr.jar
Аргументы дочерней Java VM	Задаёт аргументы командной строки, поставляемые в дочерние процессы, созданные сервером.	java -Xmx1024M -Xms512M -XX:PermSize=256M -XX:MaxPermSize=256M

Таблица 24-27: Свойства службы единого входа

Свойство	Описание	По умолчанию
Истечение срока действия единого входа (сек)	Определяет период времени (в секундах), в течение которого подключение SSO остается действительным до окончания срока действия.	По умолчанию используется значение 86400 секунд.

Свойства сервера приложений отчетов Crystal Reports 2011

Примечание:

При изменении любого из этих свойств необходимо перезапустить сервер, чтобы изменения вступили в силу.

Таблица 24-28: Свойства службы просмотра и изменений Crystal Reports 2011

Свойство	Описание	Значение по умолчанию
Разрешить заданиям для отчетов сохранять соединение с БД до закрытия данного задания для отчета	Определяет, будет ли задание отчета сохранять подключение к базе данных после выполнения процесса.	Значение по умолчанию – FALSE.
Размер области просмотра данных (число записей)	Определяет количество отдельных записей, возвращаемых из базы данных при просмотре определенных значений полей. Сначала данные извлекаются из кэша клиента (если доступен), затем – из кэша сервера. Если ни в одном кэше данных нет, они извлекаются из базы данных.	По умолчанию используется значение, равное 100 записям.
Тайм-аут простоя соединения (мин)	Определяет период времени в минутах, в течение которого сервер приложений отчетов(RAS) ожидает запросов от бездействующего клиента. Выбор слишком низкого значения может вызвать преждевременное закрытие запроса пользователя, а выбор слишком высокого значения может затронуть масштабируемость сервера (например, если объект Документ клиентского отчета не закрыт, сервер будет долгое время ожидать закрытия задания).	По умолчанию используется значение 30 минут.
Размер пакета (количество записей)	Определяет количество строк результата, возвращаемое базой данных при каждой передаче данных. Например, если запрашивается 500 записей и для свойства "Размер пакета" задано значение 100, данные будут возвращены в 5 отдельных пакетах по 100 строк. Для повышения производительности сервера RAS необходимо установить особенности сетевой среды, базы данных и определить используемые типы запросов, чтобы задать соответствующий размер пакета.	По умолчанию используется значение, равное 100 записям.

Свойство	Описание	Значение по умолчанию
Число записей базы данных для считывания при предварительном просмотре или обновлении отчета (-1, если не ограничено)	<p>Определяет количество записей базы данных, считываемое при просмотре или обновлении отчета. Этот параметр предназначен для ограничения числа записей, которые сервер извлекает из базы данных при запуске пользователем запроса или отчета. Используйте его для предотвращения запуска отчетов, содержащих запросы, которые возвращают чрезмерно большой набор записей.</p> <p>Вам может понадобиться запланировать подобные отчеты, повысить их производительность для пользователей и сократить нагрузку на базу данных, создаваемую большими запросами.</p>	По умолчанию используется значение, равное 20000 записям.
Максимальное число одновременных заданий отчета (0, если не ограничено)	Определяет максимальное количество независимых заданий, одновременно выполняемое сервером RAS.	По умолчанию используется значение, равное 75 заданиям.
Максимальный срок хранения данных, предоставляемых клиенту по запросу (в минутах)	Определяет период времени в минутах, в течение которого в запросе по требованию хранятся данные из кэша.	По умолчанию используется значение 20 минут.
Временный каталог	<p>Определяет каталог, в котором при необходимости создаются временные файлы.</p> <p>Примечание: Если для данного каталога не выделено достаточное место на диске, могут возникнуть проблемы с производительностью.</p>	По умолчанию используется значение C:\Data\Temp\SSO\ap

Таблица 24-29: Свойства службы единого входа

Свойство	Описание	По умолчанию
Истечение срока действия единого входа (сек)	Определяет период времени (в секундах), в течение которого подключение SSO остается действительным до окончания срока действия.	По умолчанию используется значение 86400 секунд.

Свойства сервера обработки Crystal Reports 2011**Примечание:**

При изменении любого из этих свойств необходимо перезапустить сервер, чтобы изменения вступили в силу.

Таблица 24-30: Свойства службы обработки Crystal Reports 2011

Свойство	Описание	По умолчанию
Предельное время простоя задания (мин)	Определяет продолжительность периода ожидания сервером обработки Crystal Reports между запросами определенного задания (в минутах).	По умолчанию используется значение 60 минут.
Максимальное количество заданий на весь срок службы для каждого дочернего объекта	Определяет максимальное количество заданий, которое может обработать каждый дочерний объект за весь срок службы.	По умолчанию используется значение 1000.
При обновлении средства просмотра всегда выдаются текущие данные	<p>Определяет, будут ли игнорироваться все станицы в кэше при явном обновлении отчета пользователем и будут ли при этом новые данные извлекаться непосредственно из базы данных. Определяет необходимость совместного использования данных отчетов несколькими клиентами.</p> <p>Примечание: Это свойство можно задать непосредственно в объекте отчета. Его значение для разных отчетов может отличаться, при этом значения, заданные в объекте отчета, имеют приоритет перед параметрами сервера. Для установки значения в объекте отчета выберите отчет в СМС и щелкните Установки по умолчанию > Просмотр группы серверов.</p>	По умолчанию используется значение true.
Предоставлять совместный доступ к данным отчета для клиентов	<p>Определяет необходимость совместного использования данных отчетов несколькими клиентами. Определяет необходимость совместного использования данных отчетов несколькими клиентами.</p> <p>Примечание: Это свойство можно задать непосредственно в объекте отчета. Его значение для разных отчетов может отличаться, при этом значения, заданные в объекте отчета, имеют приоритет перед параметрами сервера.</p>	По умолчанию используется значение true.

Свойство	Описание	По умолчанию
Тайм-аут простоя соединения (мин)	Определяет время в минутах, в течении которого сервер обработки Crystal Reports ожидает запроса при простое соединения. Как правило, изменять значение по умолчанию не требуется.	По умолчанию используется значение 20 минут.
Максимальное число параллельных заданий (0 для автоматического вычисления)	Определяет максимальное количество независимых заданий, одновременно выполняемое сервером обработки Crystal Reports. Если для данного свойства задано значение «0», сервер применяет соответствующее значение в зависимости от ЦП и памяти компьютера, на котором он запущен.	По умолчанию это значение равно 0.
Самые старые данные, выданные клиентам по запросам (сек)	<p>Определяет период времени (в секундах), в течение которого сервер использует кэшированные данные для обслуживания запросов из отчетов, открытых по запросу. Если сервер получает запрос, которому необходимы данные, использовавшиеся предыдущим запросом, и время, прошедшее с момента обработки предыдущего запроса, меньше указанного здесь значения, то сервер будет повторно использовать данные, необходимые следующему запросу. Такое повторное использование данных значительно повышает производительность системы в случае, если нескольким пользователям нужна одна и та же информация. При выборе значения для данного параметра следует определить, насколько важное значение имеет актуальность получаемых пользователями данных. Если это очень важно для всех пользователей (например, в случае, когда важные данные быстро меняются), вам может понадобиться отменить такое повторное использование данных, установив значение равным 0.</p> <p>Примечание: Это свойство можно задать непосредственно в объекте отчета. Его значение для разных отчетов может отличаться, при этом значения, заданные в объекте отчета, имеют приоритет перед параметрами сервера.</p>	По умолчанию это значение равно 0.

Свойство	Описание	По умолчанию
Максимальное число предварительно запущенных дочерних процессов	Определяет максимальное количество предварительно запущенных процессов, разрешенное сервером. Если для данного параметра задано слишком низкое значение, сервер создает дочерние процессы при поступлении запроса, что может вызвать задержку в обслуживании. Если же значение слишком велико, то простаивающие дочерние процессы могут напрасно расходовать системные ресурсы.	По умолчанию задан 1 дочерний процесс.
Временный каталог	Определяет каталог, в котором при необходимости создаются временные файлы. Примечание: Если для данного каталога не выделено достаточное место на диске, могут возникнуть проблемы с производительностью.	%TEMP%\DataDir
Разрешить заданиям для отчетов сохранять соединение с БД до закрытия данного задания для отчета	Определяет, будет ли задание отчета сохранять подключение к базе данных после закрытия задания.	По умолчанию используется значение false.
Записи, считываемые из базы данных при предварительном просмотре или обновлении	Определяет количество записей базы данных, считываемое при просмотре или обновлении отчета. Этот параметр предназначен для ограничения числа записей, которые сервер извлекает из базы данных при запуске пользователем запроса или отчета. Используйте его для предотвращения запуска отчетов, содержащих запросы, которые возвращают чрезмерно большой набор записей. Вам может понадобиться запланировать подобные отчеты, повысить их производительность для пользователей и сократить нагрузку на базу данных, создаваемую большими запросами.	По умолчанию используется значение 20000.

Таблица 24-31: Свойства службы единого входа

Свойство	Описание	По умолчанию
Истечение срока действия единого входа (сек)	Определяет период времени (в секундах), в течение которого подключение SSO остается действительным до окончания срока действия.	По умолчанию используется значение 86400 секунд.

24.1.5 Свойства служб Analysis

Категория служб Analysis включает адаптивный сервер обработки:

Таблица 24-32: Свойства службы многомерного анализа

Свойство	Описание	Значение по умолчанию
Максимальное количество сеансов клиента	Задаёт максимальное число сеансов MDAS, которые можно одновременно открыть на сервере. Когда количество открытых сеансов достигнет этого значения, все попытки запустить сеанс MDAS будут приводить к выдаче сообщения об ошибке «server unavailable» (Сервер недоступен). Этот параметр можно изменить, чтобы оптимизировать производительность сервера MDAS в зависимости от потребностей и имеющегося оборудования, однако увеличение этого значения может привести к проблемам с производительностью сервера MDAS и базы данных. Значение по умолчанию 15 сеансов является оценкой с запасом. В установках, в которых пользовательские запросы являются небольшими, можно значительно увеличить это значение, в то время как в установках, в которых пользовательские запросы являются большими, может потребоваться понижение значения.	По умолчанию задано значение 15. Допустимым диапазоном является от 1 до 100.
Максимальное число ячеек, возвращаемых запросом	Указывает число ячеек, возвращаемых пользователю в одном запросе. Предотвращается выполнение пользователем запросов, возвращающих чересчур большое число ячеек, для чего требуется большой объем памяти. Если запрос пользователя превышает этот предел для ячеек, пользователь получает сообщение об ошибке.	По умолчанию используется значение 100000 ячеек.

Свойство	Описание	Значение по умолчанию
Максимальное число элементов, возвращаемых при фильтрации	Задаёт число элементов, извлекаемых при фильтрации по элементам. Очень большое число извлекаемых элементов может потребовать потребления большого объема памяти.	По умолчанию используется значение 3000 элементов.

Таблица 24-33: Свойства службы веб-приложений BEx

Свойство	Описание	Значение по умолчанию
Максимальное количество сеансов клиента	Максимальное количество клиентских сеансов, допустимых в службе.	Значение по умолчанию составляет 15 сеансов.
Главная система SAP BW	Имя OLAP-соединения с системой BW, созданного в платформе BI.	Имя по умолчанию – SAP_BW.
Назначение RFC сервера JCo	Имя RFC-назначения сервера JCo Server, введенное в системе BW.	По умолчанию значение не указано.
Хост шлюза сервера JCo	Имя хоста шлюза сервера JCo Server, определенное в системе BW.	По умолчанию значение не указано.
Служба шлюза сервера JCo	Имя службы шлюза сервера JCo Server, определенное в системе BW.	По умолчанию значение не указано.
Количество соединений с сервером JCo	Указывает число автоматически созданных программ, которые могут использоваться для обработки запросов на обслуживание из ABAP в Java.	Значение по умолчанию равно 3 соединениям.

24.1.6 Свойства служб объединения данных

Категория служб объединения данных включает адаптивный сервер обработки:

Таблица 24-34: Свойства службы объединения данных

Свойство	Описание	Значение по умолчанию
Максимальное число соединений	Задаёт максимальное число соединений, разрешённых на сервере.	По умолчанию используется значение 32767.
Размер пула потока выполнения	Задаёт максимальное число запросов, которые могут выполняться параллельно в данный момент.	Значением по умолчанию является 10.
Время ожидания неактивного соединения	Задаёт время (в секундах), по истечении которого неактивное соединение закрывается.	По умолчанию используется значение 1080 секунд.
Время ожидания неактивного оператора	Задаёт время (в секундах), по истечении которого неактивный оператор запроса закрывается.	По умолчанию используется значение 60 секунд.

24.1.7 Свойства служб Web Intelligence

К категории служб Web Intelligence относятся следующие серверы:

- Адаптивный сервер обработки
- Сервер обработки Web Intelligence

Параметры сервера адаптивной обработки

Таблица 24-35: Служба мониторинга Web Intelligence APS

Свойство	Описание	Значение по умолчанию
Включить мониторинг	Определяет, включен ли мониторинг для службы.	По умолчанию используется значение «TRUE».
Задержка цикла потока мониторинга (секунды)	Указывает длительность интервалов между попытками службы направлять проверочные запросы клиентам, в секундах.	По умолчанию используется значение 300 секунд.
Таймаут очистки отслеживаемых ресурсов по умолчанию (в секундах)	Задаёт время (в секундах) ожидания службой неактивного клиента перед выполнением очистки сеанса клиента.	По умолчанию используется значение 1200 секунд.

Свойство	Описание	Значение по умолчанию
Таймаут обмена отслеживаемых ресурсов по умолчанию (в секундах)	Задаёт время (в секундах) ожидания службой неактивного клиента перед выполнением выгрузки сеанса клиента на жесткий диск. Рекомендуется, чтобы это значение было меньше значения свойства "Таймаут очистки отслеживаемых ресурсов по умолчанию" (сек).	По умолчанию используется значение 600 секунд.

Таблица 24-36: Свойства службы визуализации

Свойство	Описание	Значение по умолчанию
Время ожидания очистки системы визуализации (сек)	Задаёт время (в секундах) ожидания службой неактивного клиента перед выполнением очистки сеанса клиента.	По умолчанию используется значение 1200 секунд.
Время ожидания подкачки системы визуализации (сек)	Определяет время ожидания службой неактивного клиента перед выполнением выгрузки сеанса клиента на жесткий диск (в секундах). Рекомендуется, чтобы это значение было меньше значения свойства Время ожидания очистки системы визуализации (сек) .	По умолчанию используется значение 600 секунд.

Свойства сервера обработки Web Intelligence

Свойства сервера обработки Web Intelligence сгруппированы по следующим службам:

- Information Engine
- Web Intelligence Core
- Web Intelligence Processing
- Web Intelligence Common

Параметры пороговых значений описаны в отдельных таблицах.

Таблица 24-37: Параметры службы Information Engine

Свойство	Описание	По умолчанию
Включить список значений кэша	Определяет необходимость включения кэширования списка значений на сервере обработки Web Intelligence.	По умолчанию используется значение TRUE.
Размер пакета списка значений (записи)	Определяет максимальное число записей (или значений) для каждого пакета списка значений.	Значением по умолчанию является 1000 записей для каждого пакета.
Макс. размер пользовательской сортировки (элементы)	Определяет максимальное число элементов при пользовательской сортировке.	Значением по умолчанию является 100 элементов для каждой пользовательской сортировки.
Макс. размер кэша юниверсов (юниверсы)	Определяет число Юниверсов, которые могут быть кэшированы на сервере обработки Web Intelligence.	По умолчанию значение равно 20 Юниверсам.
Максимальный размер списка значений (записи)	Определяет максимальное число записей (или значений) для каждого списка значений.	По умолчанию используется 50000 записей для каждого списка значений.

Таблица 24-38: Параметры службы Web Intelligence Core

Свойство	Описание	Значение по умолчанию
Тайм-аут перед утилизацией (сек)	Определяет время (в секундах), в течение которого сервер бездействует перед тем, как агент Server Intelligence Agent (SIA) останавливает и запускает сервер, когда общее число обработанных документов превысило значение, заданное в свойстве Макс. документов до утилизации .	По умолчанию используется значение 1200 секунд.

Свойство	Описание	Значение по умолчанию
Время простоя документа (сек)	Определяет период времени (в секундах) перед переключением сеанса сервера обработки Web Intelligence. Поэтому, если клиент не создает запрос в течение этого периода, этот сеанс будет передан на жесткий диск, что позволит высвободить ресурсы для активного сеанса.	По умолчанию используется значение 300 секунд. Допустимым диапазоном является от 100 до 1000 секунд.
Интервал опроса сервера (сек)	Определяет интервал (в секундах), по истечении которого сервер опрашивает наличие новых запросов потоков. Во время опроса сервер также выполняет действия по очистке, такие как перемещение неиспользуемых документов, чтобы серверная память не превысила верхнего порогового значения.	По умолчанию используется значение 120 секунд.
Максимальное число документов на одного пользователя	Определяет максимальное число активных сеансов (документов Web Intelligence), которые могут быть связаны с пользователем в любое заданное время. Поэтому, если значением по умолчанию является 5, пользователь может одновременно использовать до 5 активных сеансов.	По умолчанию используется значение 5. Допустимым диапазоном является от 1 до 20.

Свойство	Описание	Значение по умолчанию
Макс. документов до утилизации	Определяет число документов Web Intelligence, которые могут быть обработаны до утилизации сервера. Если число обработанных документов достигнуто и сервер бездействует, сервер закрывается и агент Server Intelligence Agent (SIA) запускает новый экземпляр сервера. Однако перед запуском нового экземпляра сервера существует задержка. Эта задержка определяется свойством Таймаут до повторного использования .	Значением по умолчанию является 50 документов.
Разрешить ошибки макс. размера карты документа	Определяет наличие ограничения свойства <i>Максимальное число соединений</i> . Если это свойство включено, значение, заданное для свойства <i>Максимальное число соединений</i> , распознается сервером; в противном случае свойство игнорируется.	По умолчанию используется значение TRUE.
Тайм-аут простоя соединения (мин)	Определяет период времени (в минутах), в течение которого сервер ожидает запроса при простое соединения. Если указано слишком низкое значение, может произойти преждевременное закрытие запроса. Если указано слишком высокое значение, запросы могут быть поставлены в очередь, пока сервер будет ожидать закрытия неиспользуемых запросов.	По умолчанию используется значение 20 минут.

Свойство	Описание	Значение по умолчанию
Максимальное число соединений	<p>Определяет максимальное число одновременно открытых сеансов. Это число является приблизительным; при использовании этого параметра не учитываются неактивные переключенные сеансы или сеанс, созданный для анализа числа сеансов. Если достигнуто это ограничение и другие серверы недоступны для обработки запроса, пользователь получает сообщение об ошибке.</p> <p>Примечание: Свойство <i>Разрешить ошибки макс. размера карты документа</i> должно быть включено, чтобы это свойство могло быть распознано сервером.</p>	Значением по умолчанию является 50 сеансов. Допустимым диапазоном является от 5 до 65535.
Включить анализ памяти	<p>Определяет необходимость включения анализа памяти. Если это свойство включено, то следующие свойства будут активны и распознаны сервером:</p> <ul style="list-style-type: none"> • <i>Максимальный порог памяти</i> • <i>Верхний порог памяти</i> • <i>Нижний порог памяти</i> <p>Если память серверного процесса превышает значение <i>Верхний порог памяти</i>, единственной разрешенной операцией является сохранение документов. Если память процесса превышает значение <i>Максимальный порог памяти</i>, все операции останавливаются и завершаются неудачно.</p>	По умолчанию используется значение TRUE.

Свойство	Описание	Значение по умолчанию
Макс. порог памяти (Мбайт)	Определяет максимальное пороговое значение использования памяти.	Значением по умолчанию является 6000 МБ.
Верхний порог памяти (Мбайт)	Определяет верхнее пороговое значение использования памяти.	Значением по умолчанию является 4500 МБ.
Нижний порог памяти (Мбайт)	Определяет нижнее пороговое значение использования памяти.	Значением по умолчанию является 3500 МБ.
Включить мониторинг службы PJS	Включает мониторинг сервера службой PJS, размещаемой на адаптивном сервере обработки.	Значением по умолчанию является TRUE.
Число повторных попыток при сбое тестового опроса службы PJS	Указывает количество выполняемых сервером попыток установить связь со службой PJS перед решением о невозможности выполнения этой задачи.	По умолчанию используются три попытки.
Период потока мониторинга службы PJS	Указывает период задержки между попытками достижения службы PJS.	По умолчанию используется значение 300 секунд.

Таблица 24-39: Параметры службы Web Intelligence Processing

Свойство	Описание	Значение по умолчанию
Включить использование HTTP URL	Указывает, может ли сервер получать доступ к файлам, сохраненным удаленно.	Значением по умолчанию является TRUE.
Значение прокси	Задает адрес прокси-сервера данной сети. Это значение необходимо задавать только в случае, если в сети имеется прокси-сервер и выполняется попытка доступа к файлам, сохраненным удаленно.	Значение по умолчанию не указано.

Таблица 24-40: Параметры общей службы Web Intelligence

Свойство	Описание	Значение по умолчанию
Таймаут кэша (мин)	Определяет период времени (в минутах) перед выполнение очистки содержимого кэша документов. Тайм-аут зависит от даты последнего доступа к каждому документу.	По умолчанию используется значение 4370 минут.
Интервал очистки кэша документов (в минутах)	Определяет интервал времени (в минутах) для сканирования и проверки кэша документов на соответствие параметрам <i>Максимальный размер кэша документов</i> , <i>Макс. сжатие кэша документов</i> и <i>Максимальное число документов в кэше</i> .	По умолчанию используется значение 120 минут.
Отключить совместное использование кэша	Определяет необходимость отключения совместного использования кэша. По умолчанию совместное использование кэша включено, что означает, что все экземпляры сервера обработки Web Intelligence будут совместно использовать один кэш. Однако, если необходимо использовать один кэш для каждого экземпляра сервера обработки Web Intelligence, необходимо включить это свойство.	Значением по умолчанию является FALSE.
Включить кэш документов	Определяет необходимость включения кэша документов. Если свойство включено, в кэш можно загрузить предварительно запланированные документы Web Intelligence.	Значением по умолчанию является TRUE.

Свойство	Описание	Значение по умолчанию
Включить кэш реального времени	Определяет необходимость включения кэша реального времени. Если это свойство включено, кэш можно загружать динамически. Поэтому сервер обработки Web Intelligence кэширует документы Web Intelligence во время просмотра. Также сервер осуществляет кэширование документов при их запуске согласно расписанию, при условии, что предварительное кэширование разрешено в документе.	Значением по умолчанию является TRUE.
Максимальный размер кэша документов (кбайт)	Определяет максимальный размер кэша для документов. По достижении ограничения кэш документов будет очищен на основе свойства <i>Максимальное сжатие кэша документов</i> .	По умолчанию значение равно 1000000 байт.
Максимальное сжатие кэша документов	Определяет процентное соотношение кэш-памяти, которое будет высвобождено, чтобы разрешить сохранение новых действий и результатов в кэш-памяти. Документы с самым ранним значением «времени последнего доступа» будут очищены.	Значением по умолчанию является 70%.
Макс. размер символьного потока (Мбайт)	Определяет максимальный размер символьного потока, переданного клиенту Web Intelligence. Примечание: Если значение свойства Макс. размер символьного потока превышено, документ Web Intelligence создан не будет и клиент получит сообщение об ошибке.	Значением по умолчанию является 5 Мбайт. Допустимым диапазоном является от 1 до 65535 Мбайт.

Свойство	Описание	Значение по умолчанию
Макс. размер потока двоичных данных (Мбайт)	<p>Определяется максимальный размер (в мегабайтах) потока двоичных данных, переданных клиенту Web Intelligence.</p> <p>Примечание: Если значение свойства Макс. размер потока двоичных данных превышено, документ Web Intelligence создан не будет и клиент получит сообщение об ошибке.</p>	Значением по умолчанию является 50 Мбайт. Допустимым диапазоном является от 1 до 65535 Мбайт.
Максимальное число документов в кэше	<p>Максимальное количество документов Web Intelligence, которые можно сохранить в кэш-памяти. Число сохраненных в кэше документов не должно превышать значение этого параметра; общий размер кэша не превышает значение параметра Макс. сжатие кэша документов (Мбайт).</p> <p>Примечание: Для повышения производительности системы задайте это значение, равным 0, если выбран параметр <i>Включить кэш реального времени</i>. Но, если параметр <i>Включить кэш реального времени</i> не выбран, необходимо указать значение.</p>	По умолчанию это значение равно 0. Допустимым диапазоном является от 0 до 65535 документов.
Каталог изображений	Определяет расположение каталога изображений.	Значение по умолчанию не указано.
Выходной каталог кэша	Определяет расположение кэша.	Значение по умолчанию не указано.

Таблица 24-41: Общие свойства

Свойство	Описание	По умолчанию
Истечение срока действия единого входа (сек)	Определяет период времени (в секундах), в течение которого подключение SSO остается действительным до окончания срока действия.	По умолчанию используется значение 86400 секунд.

См. также

- [Параметры пороговых значений серверной памяти Web Intelligence](#)

24.1.7.1 Параметры пороговых значений серверной памяти Web Intelligence

В следующих разделах описаны действия, которые происходят на сервере Web Intelligence, когда достигнуты ограничения "Максимальный порог памяти", "Верхний порог памяти" или "Нижний порог памяти".

Максимальный порог памяти

Если достигнуто ограничение *Максимальный порог памяти*, все текущие операции прерываются.

Верхний порог памяти

Если достигнуто ограничение *Верхний порог памяти*, на сервере будут выполняться следующие действия для высвобождения ресурсов и защиты сервера:

- Сервер запрещает создание новых подключений и выполнение любых потоков, использующих память. В документах Web Intelligence разрешено только использование параметра **Сохранить**. Пользователи, запрашивающие выполнение операций, для которых требуется выделение памяти, получают сообщение Сервер занят, а также уведомление о том, что следует сохранить все непримененные изменения.
- Сервер включает очистку системы для высвобождения достаточного количества ресурсов, чтобы объем выделенной памяти не превышал ограничения, заданного в свойстве *Верхний порог памяти*.
- Сервер предпринимает попытку удаления документов, предназначенных только для чтения.
- Если во время очистки системы высвобождено недостаточное количество памяти, сервер начинает закрывать документы, открытые в режиме «Просмотр». Сервер начнет закрывать документы на основе протокола LIFO; последний активный документ удаляется из списка первым. Сервер продолжает закрывать документы, пока не будет достигнут безопасный уровень; этот уровень рассчитывается по следующей формуле: *Верхний порог памяти – (20%*(Верхний порог памяти))*. Например, если для свойства "Верхний порог памяти" задано значение 4500 МБ, безопасным уровнем является:

$$4500\text{МБ} - .20 * 4500\text{МБ} = 3600\text{МБ}$$

- Если при закрытии документов в режиме «Просмотр» высвобождено недостаточное количество памяти, сервер начинает закрывать все остальные открытые документы, включая документы, открытые в режиме «Редактирование». Сервер начнет закрывать документы на основе протокола LIFO; последний активный документ удаляется из списка первым. Сервер продолжает закрывать документы, пока не будет достигнут безопасный уровень; этот уровень рассчитывается по следующей формуле: *Верхний порог памяти – (20%*(Верхний порог памяти))*. Например, если для свойства "Верхний порог памяти" задано значение 4500 МБ, безопасным уровнем является:

$$4500\text{МБ} - .20 \times 4500\text{МБ} = 3600\text{МБ}$$

Нижний порог памяти

Если достигнуто ограничение *Нижний порог памяти*, сервер переносит неактивные документы на жесткий диск, выделяя дополнительную память для активных документов.

24.1.8 Свойства служб Dashboard Design

Свойства кэш-сервера Dashboard Design

Таблица 24-42: Свойства кэш-службы Dashboard Design

Свойство	Описание	Значение по умолчанию
Максимальный размер кэша (кбайт)	Определяет объем пространства жесткого диска (в Кб), используемого для кэширования запросов. Большой объем кэша может понадобиться при необходимости обработки сервером большого числа запросов или очень сложных запросов.	По умолчанию используется значение 256000 Кб.
Тайм-аут простоя соединения (мин)	Определяет время в минутах, в течении которого кэш-сервер Dashboard Design ожидает запроса при простое соединения. Как правило, изменять значение по умолчанию не требуется.	По умолчанию используется значение 15 минут.
Совместный доступ к данным для клиентов	Определяет необходимость совместного использования данных отчетов несколькими клиентами.	Значением по умолчанию является «true».

Свойство	Описание	Значение по умолчанию
<p>Самые старые данные, выданные клиентам по запросам (сек)</p>	<p>Определяет период времени (в секундах), в течение которого сервер использует кэшированные данные для обслуживания запроса из запросов, открытых по требованию. Если сервер получает запрос, которому необходимы данные, использовавшиеся предыдущим запросом, и время, прошедшее с момента обработки предыдущего запроса, меньше указанного здесь значения, то сервер будет повторно использовать данные, необходимые следующему запросу. Такое повторное использование данных значительно повышает производительность системы в случае, если нескольким пользователям нужна одна и та же информация. При выборе значения для данного параметра следует определить, насколько важное значение имеет актуальность получаемых пользователями данных. Если получение актуальных данных очень важно для всех пользователей (например, если важные изменения происходят часто), вам может понадобиться отменить такое повторное использование данных, установив значение равным 0.</p> <p>Примечание: Это свойство можно задать в самом объекте отчета. Значения, задаваемые в объекте отчета, переопределяют настройки сервера.</p>	<p>По умолчанию используется значение 0 секунд.</p>

Свойство	Описание	Значение по умолчанию
Таймаут кэша безопасности (в минутах)	Задаёт время (в минутах), когда сервером используется кэшированные учетные данные для входа, свойства запроса и информация о соединении с базой данных для обслуживания отчетов перед отправкой запроса в CMS.	По умолчанию используется значение 20 минут.
Аргументы Java VM	Задаёт аргументы командной строки, которые могут быть предоставлены JVM.	

Свойства сервера обработки Dashboard Design

Таблица 24-43: Свойства службы обработки Dashboard Design

Свойство	Описание	По умолчанию
Максимальное число параллельных заданий	Задаёт максимальное число независимых заданий, которые могут выполняться на сервере параллельно. Если для данного свойства задано значение «0», сервер применяет соответствующее значение в зависимости от ЦП и памяти компьютера, на котором он запущен.	По умолчанию это значение равно 0.
Максимальное количество заданий на весь срок службы для каждого дочернего объекта	Определяет максимальное количество заданий, которое может обработать каждый дочерний объект за весь срок службы.	По умолчанию используется значение 1000.

Свойство	Описание	По умолчанию
Максимальное число предварительно запущенных дочерних процессов	Определяет максимальное количество предварительно запущенных процессов, разрешенное сервером. Если для данного параметра задано слишком низкое значение, сервер создает дочерние процессы при поступлении запроса, что может вызвать задержку в обслуживании. Если же значение слишком велико, то простаивающие дочерние процессы могут напрасно расходовать системные ресурсы.	Значение по умолчанию равно 1.
Тайм-аут простоя соединения (мин)	Определяет период времени (в минутах), в течение которого сервер ожидает запроса при простое соединения. Как правило, изменять значение по умолчанию не требуется.	По умолчанию используется значение 20 минут.
Предельное время простоя задания (мин)	Определяет время ожидания сервером между запросами для определенного задания (в минутах).	По умолчанию используется значение 15 минут.
Аргументы дочерней Java VM	Задаёт аргументы командной строки, поставляемые в дочерние процессы, созданные сервером.	

Таблица 24-44: Свойства службы единого входа

Свойство	Описание	По умолчанию
Истечение срока действия единого входа (сек)	Определяет период времени (в секундах), в течение которого подключение SSO остается действительным до окончания срока действия.	По умолчанию используется значение 86400 секунд.

Приложение "Показатели сервера"

25.1 О приложении "Показатели сервера"

Если не указано иное, в этом приложении термин "сервер" обозначает сервер платформы BI, а не компьютер, на котором установлена или выполняется платформа.

Показатели сервера недоступны на серверах, которые не работают.

См. также

- [Анализ серверных показателей](#)

25.1.1 Общие показатели сервера

Приведенные ниже показатели относятся к компьютеру, на котором работает указанный сервер.

Таблица 25-1: Показатели работы компьютера

Показатель	Описание
Имя компьютера	Имя компьютера, на котором выполняется сервер.
Операционная система	Операционная система на компьютере, на котором выполняется сервер.
Тип ЦПУ	Тип центрального процессора на компьютере, на котором выполняется сервер. Этот показатель недоступен на адаптивных серверах обработки или серверах контейнеров веб-приложений (WACS).
ЦПУ	Количество ЦПУ, доступных для сервера. Для многоядерных систем этот показатель может означать количество логических ЦПУ, а не число физических процессоров. Этот показатель недоступен на адаптивных серверах обработки или серверах контейнеров веб-приложений (WACS).

Показатель	Описание
ОЗУ (Мбайт)	Выраженный в мегабайтах объем памяти, доступный на компьютере, на котором работает сервер. Этот показатель недоступен на адаптивных серверах обработки или серверах контейнеров веб-приложений (WACS).
Местное время	Местное время.
Размер диска (Гбайт)	Размер диска в гигабайтах, на котором установлена платформа BI. Этот показатель недоступен на адаптивных серверах обработки или серверах контейнеров веб-приложений (WACS).
Использованное дисковое пространство (Гбайт)	Используемый объем диска (в гигабайтах), на котором установлена платформа BI. Учитывается место, которое занимает платформа BI и другие программы на компьютере. Этот показатель недоступен на адаптивных серверах обработки или серверах контейнеров веб-приложений (WACS).

Следующие показатели описывают указанный сервер SAP BusinessObjects.

Таблица 25-2: Показатели сервера

Показатель	Описание
Имя сервера	Имя и номер порта сервера CMS, где этот сервер публикует свой адрес.
Зарегистрированное имя	Внутреннее имя сервера. Это имя отображается на экране «Серверы» сервера CMS.
Версия	Версия сервера.
Время запуска	Время последнего запуска сервера.
PID	Уникальный идентификатор процесса на сервере. Операционная система на компьютере, на котором выполняющийся сервер создает PID. С помощью этого PID можно идентифицировать нужный сервер.
Имя хоста	Список имен хостов (через запятую), которые в данный момент используются сервером.
IP-адрес хоста	Список IP-адресов (через запятую), на которых сервер прослушивает ответы.

Показатель	Описание
Порт запросов	Порт, с которого сервер получает запросы от других серверов. Если сервер прослушивает отчеты с нескольких IP-адресов, порт запросов для сервера всегда будет одним и тем же. Если этот порт используется каким-то другим процессом, сервер не запустится. Проверьте, не используется ли этот порт другими процессами.
Занятые потоки на сервере	Число потоков на сервере, которые обслуживают запрос в данный момент. Если это число равно максимальному размеру пула потоков сервера, это указывает на то, что система не может параллельно обрабатывать дополнительные запросы, и новые запросы должны ожидать, пока занятые потоки не станут доступными.

Таблица 25-3: Показатели аудита

Показатель	Описание
Текущее число проверяемых событий, ожидающих своей очереди	<p>Число проверяемых событий, которые записал проверяемый компонент, но пока не извлек аудитор CMS. Неограниченный рост этого показателя может свидетельствовать о неправильной настройке аудита или о том, что система перегружена и создает события аудита быстрее, чем аудитор может извлекать.</p> <p>Примечание: При остановке сервера сначала отключите его и подождите, пока этот показатель не достигнет значения «0». В противном случае некоторые события аудита могут остаться в очереди и не достичь хранилища данных аудита до перезапуска сервера и выполнения опроса CMS.</p>

Таблица 25-4: Регистрация показателей службы

Показатель	Описание
Каталог протоколирования	Файлы журналов для сервера, доступные в этом местоположении.

25.1.2 Показатели центрального сервера управления

В таблице ниже приведены показатели сервера, которые отображаются на экране «Показатели» центральных серверов управления (CMS).

Таблица 25-5: Показатели центральной службы управления

Показатель	Описание
Соединение с базой данных аудита установлено	Указывает, есть ли работоспособное соединение сервера CMS к базе данных аудита. Значение «1» свидетельствует о наличии соединения. Значение «0» свидетельствует об отсутствии соединения с базой данных аудита. Если CMS играет роль аудитора, это значение должно быть равно «1». Если оно равно «0», следует определить, почему не удастся установить соединение с базой данных аудита.
Аудитор CMS	Указывает, работает ли центральный сервер управления (CMS) как аудитор. Значение «1» свидетельствует, что CMS работает как аудитор. Значение «0» свидетельствует, что CMS не работает как аудитор.
Имя соединения с базой данных аудита	Имя соединения с базой данных аудита. Оно не обязательно совпадает с именем самой базы данных. Пустой показатель указывает на невозможность установления соединения с базой данных аудита.
Имя пользователя базы данных аудита	Имя пользователя в учетной записи, с помощью которой выполняется соединение с базой данных.
Последнее использование базы данных аудита	Время и дата последнего начала успешного извлечения событий сервером CMS из проверяемого объекта. Если CMS является аудитором, значение этого показателя должно быть временем, близким ко времени загрузки страницы «Показатели». Если это значение приходится более чем на два часа раньше времени загрузки страницы, возможно, это признак неправильной работы аудита.

Показатель	Описание
Длительность последнего цикла опроса потока аудита (секунды)	<p>Длительность последнего цикла опроса в секундах. Указывает максимальную задержку доставки данных о событии в базу данных аудита в течение предыдущего цикла опроса.</p> <ul style="list-style-type: none"> • Значение меньше 20 минут означает, что система работоспособна. • Значение в пределах от 20 минут до 2 часов означает, что система загружена. • Значение, превышающее 2 часа, означает, что система очень загружена. Если такое состояние сохраняется, и данные доставляются с большой задержкой, рекомендуется обновить развертывание всех баз данных аудита, чтобы получать данные быстрее, или уменьшить количество событий аудита в системе.
Использование потока аудита	<p>Процентная доля цикла опроса, которую CMS затрачивает на сбор данных о проверяемых объектах. Все остальное время CMS находится в состоянии покоя между опросами.</p> <p>Если значение достигает 100%, значит, на момент необходимости начала следующего запроса аудитор все еще выполняет сбор данных из проверяемого компонента. Это может стать причиной задержек в доставке данных о событиях в базу данных аудита. Если интенсивность использования потока аудита достигает 100% и остается таким в течение нескольких дней, рекомендуется обновить развертывание, чтобы база данных могла быстро получать данные, или уменьшить количество событий аудита в системе.</p>
Кластеризованные серверы CMS	Разделяемый точками с запятыми список имен хостов и номеров портов выполняющихся серверов Central Management Server в кластере.
Число сеансов пользователей с лицензиями на одновременный доступ	Общее число сеансов для пользователей с лицензиями на одновременный доступ.
Число сеансов, установленных именованными пользователями	Полное число сеансов для пользователей с лицензиями по зарегистрированному пользователю.
Максимальное число пользовательских сеансов с момента запуска	Максимальное число параллельных пользовательских сеансов, которые обрабатывал сервер CMS с момента запуска.

Показатель	Описание
Число сеансов, установленных серверами	Число параллельных сеансов, созданных серверами платформы BI с помощью CMS. Если это число превышает 250, создайте дополнительный CMS.
Число сеансов, установленных всеми пользователями	Число параллельных сеансов, которые обрабатываются сервером CMS в момент загрузки экрана «Показатели». Чем больше это число, тем больше пользователей работает в системе. Если это число превышает 250, создайте дополнительный CMS.
Задания, завершившиеся сбоем	Полное число завершившихся сбоем заданий на сервере CMS с момента его запуска.
Отложенные задания	Текущее число ожидающих заданий.
Выполняющиеся задания	Текущее число выполняющихся заданий. Включает запланированные задания, еще не готовые к выполнению, так как их плановое время еще не наступило.
Завершенные задания	Полное число завершенных заданий на сервере CMS с момента его запуска.
Ожидающие задания	Текущее число ожидающих заданий на CMS. Оно включает задания, которые вошли в расписание и ожидают освобождения ресурсов.
Лицензии на параллельный доступ пользователей	Количество лицензий на параллельный доступ пользователей, указанное в коде ключа.
Лицензии для именованных пользователей	Количество лицензий именованных пользователей, указанное в коде ключа.
Дата построения	Дата построения CMS.
Имя подключения к системной базе данных	Имя соединения с системной базой данных CMS. Оно не обязательно совпадает с именем самой базы данных CMS.
Имя сервера системной базы данных	Имя сервера, на котором работает сервер системной базы данных. Оно не обязательно совпадает с именем самой базы данных CMS.
Имя пользователя системной базы данных	Имя пользователя в учетной записи, с помощью которой выполняется соединение с базой данных CMS.
Имя источника данных	Имя соединения с системной базой данных CMS.

Показатель	Описание
Номер построения	Номер построения CMS. С помощью этого номера можно идентифицировать установленную версию платформы BI.
Версия продукта	Версия продукта CMS.
Версия ресурса	Версия ресурса CMS.
Среднее время ответа при фиксации с момента запуска (мсек)	Средняя длительность (в миллисекундах) выполнения операций на сервере CMS с момента его запуска. Если время ответа превышает 1000 миллисекунд, это может указывать на необходимость настройки CMS или системной базы данных CMS.
Среднее время ответа на запрос с момента запуска (мсек)	Средняя длительность (в миллисекундах) выполнения операций запроса на сервере CMS с момента его запуска. Если время ответа превышает 1000 миллисекунд, это может указывать на необходимость настройки CMS или системной базы данных CMS.
Максимальное время обработки фиксации с момента запуска (мсек)	Максимальная длительность (в миллисекундах) выполнения операций на сервере CMS с момента его запуска. Если время ответа превышает 10000 миллисекунд, это может указывать на необходимость настройки CMS или системной базы данных CMS.
Максимальное время обработки запроса с момента запуска (мсек)	Максимальная длительность (в миллисекундах) выполнения операций запроса на сервере CMS с момента его запуска. Если время ответа превышает 10000 миллисекунд, это может указывать на необходимость настройки CMS или системной базы данных CMS.
Число фиксаций с момента запуска	Число фиксаций системной базы данных CMS с момента запуска сервера.
Число запросов с момента запуска	Полное число запросов, поступивших в базу данных с момента запуска сервера. Большое значение указывает на высокую активность или загруженность системы.
Число входов в систему с момента запуска	Число входов пользователей в систему с момента запуска сервера. Большое значение указывает на высокую активность или загруженность системы.

Показатель	Описание
Установленные соединения с системной БД	Число соединений с системной базой данных CMS, которые удалось установить серверу CMS. При обрыве соединения CMS пытается его восстановить. Если число установленных с базой данных соединений постоянно ниже, чем число соединений с системной базой данных, указанное в свойстве Запросы соединений с системной БД на экране «Свойства», это может свидетельствовать о том, что сервер CMS не может установить дополнительные соединения, и функционирование системы далеко от оптимального. Возможным решением будет настройка сервера базы данных таким образом, чтобы было разрешено больше соединений с базой данных для CMS.
Параллельно использующиеся соединения с системной БД	Число соединений с системной базой данных CMS, которые сервер CMS использует в данный момент. Число текущих используемых соединений может быть меньше или равно числу соединений, установленных с системной базой данных. Если в течение некоторого времени число установленных соединений равно числу используемых соединений, это может указывать на наличие в системе "узкого места". Увеличение значения свойства Запросы соединений с системной БД на экране «Свойства» может повысить производительность сервера CMS. Настройка системной базы данных CMS также может привести к повышению производительности.
Незавершенные запросы в системную БД	Число запросов в системную базу данных CMS, ожидающих, пока для них станут доступны соединения. При больших значениях этого параметра следует рассмотреть возможность увеличения значения свойства Запросы соединений с системной БД . Настройка системной базы данных CMS также может привести к повышению производительности.
Число объектов в системном кэше CMS	Полное текущее число объектов, которые содержатся в системном кэше CMS.
Число объектов в системной БД CMS	Полное текущее число объектов, которые содержатся в системной базе данных CMS.
Существующие учетные записи пользователей с лицензиями на параллельный доступ	Полное число существующих в кластере пользователей с лицензиями на параллельный доступ.

Показатель	Описание
Существующие учетные записи именованных пользователей	Полное число имеющихся в кластере пользователей с именованными лицензиями на параллельный доступ.

25.1.3 Показатели сервера соединений

Для сервера соединений характерны следующие показатели.

Таблица 25-6: Показатели службы соединений

Показатель	Описание
Источники данных	<p>Списки в таблице являются источниками данных, активируемые на странице «Свойства». Выводится следующая информация для каждой пары сетевого уровня и базы данных:</p> <ul style="list-style-type: none"> «Статус» («Загружено» или «Сбой!»): текущий статус драйвера «Доступные соединения: число соединений пула, которые могут использоваться» «Задания (CORBA): число обрабатываемых заданий (развертывание 2-го яруса)» «Задания (HTTP): число обрабатываемых заданий (развертывание веб-яруса)» <p>Примечание: Для получения дополнительных сведений о пулах соединений см. <i>Руководство по доступу к данным</i>.</p>

25.1.4 Показатели сервера событий

В следующей таблице приведены показатели сервера, которые отображаются на экране «Показатели» серверов событий.

Таблица 25-7: Показатели службы событий

Показатель	Описание
Список отслеживаемых файлов	Таблица, в которой указаны файлы, контролируемые сервером событий. В столбце «Имя файла» указывается имя файла и путь к файлу. В столбце «Время последнего уведомления» указывается последняя метка времени, когда сервер выполнял опрос и обнаружил, что файл существует.
Отслеживаемые файлы	Полное число файлов, которые отслеживаются сервером событий.

25.1.5 Показатели сервера репозитория файлов

В следующей таблице приведены показатели сервера, которые отображаются на экране «Показатели» серверов репозитория входных и выходных файлов.

Таблица 25-8: Показатели службы хранилища файлов

Показатель	Описание
Активные файлы	Число файлов на сервере репозитория файлов, к которым в данный момент осуществляется доступ.
Записано данных (Мбайт)	Полное количество мегабайтов, записанных в файлы на сервере.
Передано данных (Мбайт)	Суммарное количество мегабайтов, прочтенных из файлов на сервере.
Список активных файлов	Таблица, в которой представлены файлы на сервере репозитория файлов, к которым в данный момент осуществляется доступ.
Активные соединения	Полное число активных соединений между клиентами и другими серверами.
Доступное дисковое пространство в корневом каталоге (Гбайт)	Суммарный объем доступного пространства на диске, на котором размещен исполняемый файл сервера (в гигабайтах).

Показатель	Описание
Свободное дисковое пространство в корневом каталоге (Гб)	Полный объем свободного места на диске (в гигабайтах), на котором содержится исполняемый файл сервера.
Общее дисковое пространство в корневом каталоге (Гб)	Общий объем дискового пространства на диске, на котором размещен исполняемый файл сервера (в гигабайтах).
Доступное дисковое пространство в корневом каталоге (%)	Доля доступного пространства на диске, на котором размещен исполняемый файл сервера (в процентах).

25.1.6 Показатели адаптивного сервера обработки

В следующей таблице приведены показатели сервера, которые отображаются на экране «Показатели» адаптивного сервера обработки.

Таблица 25-9: Показатели адаптивного сервера обработки

Показатель	Описание
Потоки на транспортном уровне	Общее число потоков во всех пулах потоков на транспортном уровне.
Размер пула потоков транспортного уровня	Общее число совместных потоков транспортного уровня. Эти потоки могут использовать любые службы, размещенные на настраиваемом сервере обработки.
Доступные процессоры	Число процессоров, доступных виртуальной машине Java (JVM), на которой выполняется сервер.
Максимальный объем памяти (Мбайт)	Выраженный в мегабайтах максимальный объем памяти, которую будет пытаться использовать виртуальная машина Java.
Свободная память (Мбайт)	Выраженный в мегабайтах объем памяти, доступный JVM для размещения новых объектов.
Всего памяти (Мбайт)	Выраженный в мегабайтах объем памяти в виртуальной машине Java. Это значение меняется со временем в зависимости от состояния гостевой среды.

Показатель	Описание
Процент использования ЦПУ (последние 5 минут)	Процентная доля использования времени ЦП сервером в течение последних пяти минут. Например, если какой-то поток полностью использует ЦПУ четырехпроцессорной системы, ее процент использования равен 25%. Принимаются во внимание все процессоры, назначенные JVM. Значение, превышающее 80%, может указывать на критическую ситуацию для ЦП.
Процент использования ЦПУ (последние 15 минут)	Процентная доля использования времени ЦП сервером в течение последних пятнадцати минут. Например, если какой-то поток полностью использует ЦПУ четырехпроцессорной системы, ее процент использования равен 25%. Принимаются во внимание все процессоры, назначенные JVM. Значение, превышающее 70%, может указывать на критическую величину нагрузки.
Процент остановленной системы в течение GC (последние 5 минут)	<p>Выраженная в процентах часть системы, остановленная во время очистки памяти (GC, Garbage Collections) в течение последних пяти минут. В этом состоянии предотвращается выполнение всех служб APS, пока виртуальной машиной выполняется критичный этап очистки памяти, для которого необходим монопольный доступ.</p> <p>В общем случае даже при нагрузке нормальным считается небольшое (однозначное) число. Если в течение длительного времени этот параметр выражается двузначным числом, это может свидетельствовать о низкой пропускной способности. В таком случае требуется проверка.</p>
Процент остановленной системы в течение GC (последние 15 минут)	<p>Выраженная в процентах часть системы, остановленная во время очистки памяти (GC, Garbage Collections) в течение последних пятнадцати минут. В этом состоянии блокируется выполнение всего кода приложений на виртуальной машине Java во время важного этапа очистки памяти, на котором требуется монопольный доступ.</p> <p>В общем случае даже при нагрузке нормальным считается небольшое (однозначное) число. Если в течение длительного времени этот параметр выражается двузначным числом, это может свидетельствовать о низкой пропускной способности. В таком случае требуется проверка.</p>

Показатель	Описание
Количество ошибок страниц в течение GC (последние 5 минут)	Количество ошибок страниц, возникших во время сборки мусора в памяти в течение предыдущих пяти минут. Любое положительное число свидетельствует о высокой нагрузке на систему и недостатке в ней памяти.
Количество ошибок страниц в течение GC (последние 15 минут)	Количество ошибок страниц, возникших во время сборки мусора в памяти в течение предыдущих пятнадцати минут. Любое положительное число свидетельствует о высокой нагрузке на систему и недостатке в ней памяти.
Количество полных GC	Количество полных очисток памяти с момента запуска системы. Быстрое увеличение этого значения может свидетельствует о недостатке памяти в системе.
Количество конфликтов при блокировках JVM	Количество синхронизированных объектов, в которых есть ожидающие доступа потоки. Любое значение, намного превышающее 0, может свидетельствовать о наличии потоков, которые больше не будут выполняться. Иницилируйте дампы потоков, чтобы получить больше сведений о причине проблемы.
Сведения об отладке JVM	Доступны отладочные сведения о виртуальной машине Java SAP, включая данные о состоянии, номер порта, а также о прикрепленном клиенте (при его наличии).
Сведения о версии JVM	Сведения о версии виртуальной машины Java SAP.
Счетчик заблокированных потоков JVM	Количество заблокированных потоков. Любое значение, намного превышающее 0, свидетельствует о наличии потоков, которые больше не будут выполняться. Иницилируйте дампы потоков, чтобы получить больше сведений о причине проблемы.
Флаги трассировки JVM	Флаги трассировки, настроенные в данный момент на JVM. Указывает уровень трассировки JVM.
Службы	Список служб (через запятую), размещенных на сервере.

Таблица 25-10: Показатели службы моста DSL

Показатель	Описание
DSLServiceMetrics.queryCount	Число открытых запросов данных между клиентами и службой
DSLServiceMetrics.activeConnectionCount	Количество открытых соединений между клиентами и службой.
DSLServiceMetrics.activeSessionCount	Количество открытых сеансов между клиентами и службой.
DSLServiceMetrics.activeOLAPConnectionCount	Количество открытых соединений между клиентами OLAP и службой.

Таблица 25-11: Показатели службы прокси аудита клиента

Показатель	Описание
Полученные события аудита	Число событий аудита клиента, полученных службой с момента ее запуска. С помощью этого показателя можно проверять правильность настройки аудита клиента. Значения больше «0» указывают на успешную маршрутизацию через данную службу аудита клиента событий аудита, поступающих от клиентов.

Таблица 25-12: Показатели службы поиска по платформе

Показатель	Описание
Число успешных попыток извлечения с момента запуска службы	Число успешных попыток извлечения документов с момента запуска службы поиска по платформе.
Число успешных попыток извлечения с момента запуска службы	Число успешных попыток извлечения документов с момента запуска службы поиска по платформе.
Метка времени создания последнего хранилища контента	Дата и время создания последнего хранилища контента.
Число неудачных попыток извлечения с момента запуска службы	Число неудачных попыток извлечения документов с момента запуска службы поиска по платформе.
Доступная служба	TRUE, если служба доступна. В противном случае – значение FALSE.

Показатель	Описание
Выполняемая индексация	TRUE, если выполняется индексация. В противном случае – значение FALSE.
Число индексируемых документов	Отображений числа документов, индексируемых с момента запуска службы.

Таблица 25-13: Показатели службы многомерного анализа

Показатель	Описание
Число сеансов	Текущее число соединений клиентов MDAS с сервером.
Число кубов	Число источников данных, используемых для предоставления данных для соединений, в которых не закончилось время ожидания.
Число запросов	Число запросов данных, открытых между клиентами MDS и сервером.

Таблица 25-14: Показатели службы объединения данных

Показатель	Описание
Число выполняющихся запросов	Число выполняющихся запросов (использующих или не использующих память).
Число соединений	Общее число подключений пользователей к подсистеме запросов объединения данных.
Общее число байтов, переданных из источников данных	Объем данных, считанных из источников данных (в байтах).
Общее число записей, переданных из источников данных	Общее число строк, сосчитанных из источников данных.
Общее число байтов, созданных выполнением запроса	Объем данных, созданных в качестве выходных данных запросов (в байтах).
Общее число записей, созданных выполнением запроса	Общее число строк, созданных в качестве выходных данных запросов (в байтах).
Число запросов, использующих память	Число выполняющихся запросов, использующих память.
Общее число байтов памяти, используемых выполнением запроса	Объем памяти, используемой в настоящее время выполняемыми запросами (в байтах).

Показатель	Описание
Общее число байтов объема диска, используемого выполнением запроса	Объем дискового пространства, используемого в настоящее время выполняемыми запросами (в байтах).
Число запросов, использующих диск	Общее число выполняющихся запросов, использующих диск.
Число запросов, ожидающих ресурсов	Общее число выполняющихся запросов, ожидающих в настоящее время ресурсов.
Число активных потоков	Общее число активных потоков, используемых для выполнения запросов.
Общее число байтов памяти, используемых кэшем метаданных	Объем памяти, используемой для кэширования метаданных, статистических данных и конфигураций блоков соединений (в байтах).
Число сбоев запросов	Общее число сбоев запросов (вызывающих исключение).
Число запросов на стадии анализа запроса	Общее число выполняющихся в настоящий момент запросов на стадии анализа.
Число запросов на стадии оптимизации запроса	Общее число выполняющихся в настоящий момент запросов на стадии оптимизации.
Число запросов на стадии выполнения запроса	Общее число выполняющихся в настоящий момент запросов на стадии выполнения.
Число загруженных соединителей	Общее число блоков соединений, загруженных в службу.
Число активных соединений на загруженных блоках соединений	Общее число активных соединений на блоках соединений, загруженных в службу.
Служба объединения данных доступна	«TRUE», если служба доступна. В противном случае этот параметр имеет значение «FALSE».

25.1.7 Показатели сервера контейнера веб-приложений

В следующей таблице приведены показатели сервера, которые отображаются на экране «Показатели» серверов контейнера веб-приложений.

Примечание:

Серверы контейнеров веб-приложений также имеют все показатели, описанные в разделе "Показатели адаптивного сервера обработки".

Таблица 25-15: Показатели сервера контейнера веб-приложений

Показатель	Описание
Список выполняющихся средств связи WACS	Список всех работающих средств связи на сервере. Если отображаются не все средства связи (HTTP, HTTPS и HTTP через прокси), то средство соединения не включено или в нем возник сбой во время запуска
Ошибка запуска одного или нескольких соединителей WACS	Показывает, имеются ли отказавшие соединители. Если true – произошел сбой при запуске хотя бы одного коннектора. "false" – все соединители работают. Не используйте сервер, если при загрузке хотя бы одного соединителя произошел сбой; необходимо определить причину сбоя и устранить неполадки, чтобы все соединители загружались правильно.

См. также

- [Показатели адаптивного сервера обработки](#)

25.1.8 Показатели адаптивного сервера заданий

Таблица 25-16: Показатели сервера заданий

Показатель	Описание
Полученные запросы заданий	Количество заданий, которые предположительно выполняются на сервере.
Параллельные задания	Количество заданий, которые сейчас выполняются на сервере. Если это количество большое, сервер занят.
Пиковые задания	Максимальное количество параллельных заданий, которые одновременно выполнялись на сервере. Если сервер не перезагружался, это число не становится меньше.

Показатель	Описание
Создания заданий, завершившиеся сбоем	Количество заданий на сервере, в которых возникли сбои.
Временный каталог	Каталог, в котором создаются временные файлы. Этот параметр задается в окне «Свойства» сервера. Если для этого каталога недостаточно места на диске, могут возникнуть проблемы.
Установка по умолчанию адресатов системы файлов допустима	Принимает значение «TRUE», если сервер может отправлять документы в файловую систему назначения, указанную в окне «Адресат» сервера. В противном случае этот параметр имеет значение «FALSE».
Установка по умолчанию адресатов FTP допустима	Принимает значение «TRUE», если сервер может отправлять документы на целевой сервер FTP, указанный в окне «Адресат» сервера. В противном случае этот параметр имеет значение «FALSE».
Установка по умолчанию адресатов папки "Входящие" допустима	Принимает значение «TRUE», если сервер может отправлять объекты в целевую папку "Входящие", указанную в окне «Адресат» сервера. В противном случае этот параметр имеет значение «FALSE».
Установка по умолчанию адресатов эл. почты допустима	Принимает значение «TRUE», если сервер может отправлять объекты по адресу электронной почты, указанному в окне «Адресат» сервера. В противном случае этот параметр имеет значение «FALSE».
Службы планирования	Таблица, в которой представлены службы, выполняемые на сервере.
Дочерние элементы	Таблица, в которой представлены дочерние процессы, выполняемые на сервере.

В следующей таблице описываются показатели для каждой из служб планирования, выполняющихся на сервере.

Таблица 25-17: Показатели службы планирования

Показатель	Описание
Служба планирования	Имя службы.

Показатель	Описание
Полученные запросы заданий	Количество заданий, которые предположительно выполняются на сервере.
Параллельные задания	Количество одновременно выполняющихся в службе заданий. Если это количество большое, служба занята.
Пиковые задания	Максимальное количество параллельных заданий, которые одновременно выполнялись на службе.
Максимально допустимое число параллельных заданий	Количество параллельно выполняемых независимых (дочерних) процессов, максимально допустимое для службы. Этот параметр задается в окне «Свойства» сервера.
Создания заданий, завершившиеся сбоем	Количество заданий в службе, в которых возник сбой.

В следующей таблице описываются показатели для каждого дочернего процесса, который выполняется на сервере.

Таблица 25-18: Показатели дочернего процесса

Показатель	Описание
Служба планирования	Имя дочернего процесса.
PID	Идентификатор дочернего процесса.
Полученные запросы заданий	Количество заданий, предположительно выполненных в дочернем процессе.
Параллельные задания	Количество заданий, параллельно выполняющихся в дочернем процессе. Нормальным для этого параметра считается значение «1».
Пиковые задания	Максимальное количество параллельных заданий, которые одновременно выполнялись в дочернем процессе.
Максимально разрешенное число заданий	Количество параллельных заданий, которое допускает дочерний процесс.

Показатель	Описание
Связь Сбои	Количество возникших сбоев связи с родительским настраиваемым сервером заданий. Если это число большое, дочерний процесс перезапустится.
Инициализация	Этот параметр имеет значение «TRUE», если выполняется инициализация дочернего процесса. В противном случае этот параметр имеет значение «FALSE».
Завершение работы	Этот параметр имеет значение «TRUE», если дочерний процесс завершает свою работу. В противном случае этот параметр имеет значение «FALSE».

25.1.9 Показатели сервера Crystal Report

В следующей таблице приведены показатели сервера, которые отображаются на экране «Показатели» для серверов Crystal Reports Processing и Crystal Reports 2011 Processing.

Таблица 25-19: Показатели сервера обработки Crystal Reports

Показатель	Описание
Открытых заданий	Таблица со списком текущих заданий, выполняющихся на сервере. В этой таблице содержится идентификатор и имя документа, имя пользователя, выполняющего задание, дата последнего доступа к документу, а также время нахождения задания в процессе выполнения.
Число обслуживаемых запросов	Общее число запросов, обслуженных сервером с момента его запуска.
Число открытых заданий	Число текущих заданий, обрабатываемых сервером и его дочерними процессами.
Тип объекта	Тип для InfoObject, используемого сервером в первую очередь. Значение этого показателя не меняется.

Показатель	Описание
Среднее время обработки (мс)	Среднее время (в миллисекундах), затраченное сервером на обработку последних полученных им 500 запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.
Максимальное время обработки (мс)	Максимальное время (в миллисекундах), затраченное сервером на обработку одного из последних 500 запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.
Минимальное время обработки (мс)	Минимальное время (в миллисекундах), затраченное сервером на обработку одного из последних 500 запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.
Число запросов в очереди	Число обрабатываемых и ожидающих обработку запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.
Имя Dll объекта	Имя подключаемого модуля обработки для сервера. Значение этого показателя не меняется.
Число открытых соединений	Число соединений, открытых в данный момент между сервером и клиентами.
Частота сбоев запросов	Число запросов, выполненных сервером с ошибкой, в процентном соотношении относительно последних 500 запросов, полученных сервером.
Передано данных (КБ)	Общий объем данных, переданных клиентам с момента запуска сервера.
Число запросов, выполненных с ошибкой	Число запросов, которые серверу не удалось завершить с момента его запуска.
Макс. число дочерних процессов	Максимальное число параллельных дочерних процессов, разрешенное на сервере.

В следующей таблице приведены показатели сервера, которые отображаются на экране «Показатели» для серверов кэширования Crystal Reports.

Таблица 25-20: Показатели кэш-сервера Crystal Reports

Показатель	Описание
Удачных обращений в кэш (%)	Процент запросов, относительно последних 500 запросов, выполненных с кэшированными данными.
Подключенные серверы обработки	Таблица со списком серверов обработки Crystal Reports в данном развертывании. В этой таблице выводится имя сервера и количество текущих соединений, открытых с этим сервером.
Число обслуживаемых запросов	Общее число запросов, обслуженных сервером с момента его запуска.
Тип объекта	Тип для InfoObject, используемого сервером в первую очередь. Значение этого показателя не меняется.
Среднее время обработки (мс)	Среднее время (в миллисекундах), затраченное сервером на обработку последних полученных им 500 запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.
Максимальное время обработки (мс)	Максимальное время (в миллисекундах), затраченное сервером на обработку одного из последних 500 запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.
Минимальное время обработки (мс)	Минимальное время (в миллисекундах), затраченное сервером на обработку одного из последних 500 запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.
Число запросов в очереди	Число обрабатываемых и ожидающих обработку запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.
Имя Dll объекта	Имя подключаемого модуля обработки для сервера. Значение этого показателя не меняется.
Объем кэш-памяти	Объем данных (в килобайтах), кэшируемых в настоящий момент сервером на диск.
Число открытых соединений	Число соединений, открытых в данный момент между сервером и клиентами.

Показатель	Описание
Передано данных (КБ)	Общий объем данных, переданных клиентам с момента запуска сервера.

В следующей таблице приведены показатели сервера, которые отображаются на экране «Показатели» для серверов приложений отчетов Crystal Reports 2011.

Таблица 25-21: Показатели сервера приложений отчетов Crystal Reports 2011

Показатель	Описание
metric_currentdoccount	Количество документов, обрабатываемых в настоящий момент сервером.
metric_totaldoccount	Количество документов, обработанных сервером с момента его запуска.
metric_currentagentthreadcount	Количество потоков, обрабатываемых в настоящий момент сервером.
metric_totalagentthreadcount	Количество потоков, обработанных сервером с момента его запуска.

25.1.10 Показатели сервера Web Intelligence

Таблица 25-22: Показатели службы обработки Web Intelligence

Показатель	Описание
Размер кэша (кбайт)	Текущий размер (в килобайтах) данных, сохраненных в кэше.
Максимальное количество документов в кэше	Число документов, удаленных из кэша с момента запуска сервера, по причине их устаревания.
Уровень максимального использования кэша	Число случаев достижения кэшем максимально допустимого значения на сервере с момента его запуска.
Использование ЦП (%)	Процент от общего времени ЦП, затраченный сервером с момента его запуска.

Показатель	Описание
Общее время работы ЦП (секунд)	Общее время ЦП (в секундах), затраченное сервером с момента его запуска.
Верхний порог использования памяти	Число случаев достижения верхнего порога использования памяти на сервере с момента его запуска.
Максимальный порог использования памяти	Число случаев достижения максимального порога использования памяти на сервере с момента его запуска.
Размер виртуальной памяти (Мб)	Общий объем памяти (в мегабайтах), назначенный серверу.
Текущее число вызовов клиентов	Текущее число вызовов CORBA, обрабатываемых сервером.
Текущее число задач	Текущее число задач, выполняемых на сервере.
Общее число вызовов клиентов	Общее число вызовов CORBA, полученных сервером с момента его запуска.
Общее число задач	Общее число задач, выполненных на сервере с момента его запуска.
Время простоя (сек)	Время (в секундах), прошедшее с момента последнего запроса, полученного сервером от клиента.
Текущее число активных сеансов	Текущее число сеансов, которые могут принять запросы от клиентов.
Число документов	Число текущих открытых на сервере документов.
Текущее число сеансов	Текущее число сеансов, созданных на сервере.
Число операций подкачки документов	Число документов, для которых в потоке очистки имеются запланированные запросы подкачки.
Число подкачанных документов	Число документов, подкачанных в результате запросов подкачки.
Число таймаутов сеансов	Число сеансов, для которых истекло время ожидания с момента запуска сервера.
Общее число сеансов	Число сеансов, созданных на сервере с момента его запуска.

Показатель	Описание
Число пользователей	Общее число пользователей, подключенных к серверу.

25.1.11 Показатели сервера Dashboard Design

Таблица 25-23: Показатели сервера обработки Dashboard Design

Показатель	Описание
Открытых заданий	Таблица со списком текущих заданий, выполняющихся на сервере. В этой таблице содержится идентификатор и имя документа, имя пользователя, выполняющего задание, дата последнего доступа к документу, а также время нахождения задания в процессе выполнения.
Число обслуживаемых запросов	Общее число запросов, обслуженных сервером с момента его запуска.
Число открытых заданий	Число текущих заданий, обрабатываемых сервером и его дочерними процессами.
Тип объекта	Тип для InfoObject, используемого сервером в первую очередь. Значение этого показателя не меняется.
Среднее время обработки (мс)	Среднее время (в миллисекундах), затраченное сервером на обработку последних полученных им 500 запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.
Максимальное время обработки (мс)	Максимальное время (в миллисекундах), затраченное сервером на обработку одного из последних 500 запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.
Минимальное время обработки (мс)	Минимальное время (в миллисекундах), затраченное сервером на обработку одного из последних 500 запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.

Показатель	Описание
Число запросов в очереди	Число обрабатываемых и ожидающих обработку запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.
Имя DII объекта	Имя подключаемого модуля обработки для сервера. Значение этого показателя не меняется.
Число открытых соединений	Число соединений, открытых в данный момент между сервером и клиентами.
Частота сбоев запросов	Число запросов, выполненных сервером с ошибкой, в процентном соотношении относительно последних 500 запросов, полученных сервером.
Передано данных (КБ)	Общий объем данных, переданных клиентам с момента запуска сервера.
Число запросов, выполненных с ошибкой	Число запросов, которые серверу не удалось завершить с момента его запуска.
Макс. число дочерних процессов	Максимальное число параллельных дочерних процессов, разрешенное на сервере.

Таблица 25-24: Показатели размера кэша

Показатель	Описание
Удачных обращений в кэш (%)	Процент запросов, относительно последних 500 запросов, выполненных с кэшированными данными.
Подключенные серверы обработки	Таблица со списком серверов обработки Dashboard Design в данном развертывании. В этой таблице выводится имя сервера и количество текущих соединений, открытых с этим сервером.
Число обслуживаемых запросов	Общее число запросов, обслуженных сервером с момента его запуска.
Тип объекта	Тип для InfoObject, используемого сервером в первую очередь. Значение этого показателя не меняется.

Показатель	Описание
Среднее время обработки (мс)	Среднее время (в миллисекундах), затраченное сервером на обработку последних полученных им 500 запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.
Максимальное время обработки (мс)	Максимальное время (в миллисекундах), затраченное сервером на обработку одного из последних 500 запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.
Минимальное время обработки (мс)	Минимальное время (в миллисекундах), затраченное сервером на обработку одного из последних 500 запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.
Число запросов в очереди	Число обрабатываемых и ожидающих обработку запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.
Имя DII объекта	Имя подключаемого модуля обработки для сервера. Значение этого показателя не меняется.
Размер кэша (кбайт)	Объем данных (в килобайтах), кэшируемых в настоящий момент сервером на диск.
Число открытых соединений	Количество открытых в настоящий момент соединений с клиентами.
Передано данных (КБ)	Общий объем данных, переданных клиентам с момента запуска сервера.

Приложение заполнителя сервера и узла

26.1 Заполнители сервера и узлов

За исключением «%SERVER_FRIENDLY_NAME%» и «%SERVER_NAME%», эти заполнители относятся ко всем серверам на одном узле.

Таблица 26-1: Заполнители

Заполнитель	Описание	Значения по умолчанию
%AAANALYTICS_EXE%	Имя выполняемого файла сервера Dashboard Analytics.	В ОС Windows это AAAnalytics.exe. В UNIX, AAAnalytics.
%AADASHBOARD_EXE%	Имя выполняемого файла сервера Dashboard Analytics.	В ОС Windows это AADashboard.exe. В UNIX, AADashboard.
%AuditingDatabaseConnection%	Соединение базы данных аудита, используемое CMS.	Это значение задается во время установки.
%AuditingDatabaseDriver%	Тип драйвера базы данных, используемого для подключения к базе данных аудита.	В Windows по умолчанию используется значение sqlserverauditdbss.
%BINDIR%	Папка, где расположены 64-битные двоичные файлы платформы BI.	В ОС Windows это <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/win64_x64. В UNIX это <INSTALLDIR>/bin64_x64/platform
%BINDIR32%	Папка, где расположены 32-битные двоичные файлы платформы BI.	В ОС Windows это <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/win32_x86. В UNIX это <INSTALLDIR>/bin32_x86/platform

Заполнитель	Описание	Значения по умолчанию
%CACHESERVER_EXE%	Имя исполняемого файла кэш-сервера Crystal Reports.	В ОС Windows это <code>crcache.exe</code> . В ОС UNIX это <code>boe_crcached</code> .
%CMS_EXE%	Имя выполняемого файла центрального сервера управления.	В ОС Windows это <code>cms.exe</code> . В ОС UNIX это <code>boe_cmsd</code> .
%CONNECTIONSERVER32_EXE%	Имя выполняемого файла для 32-битного сервера соединений.	В Windows, <code>ConnectionServer32.exe</code> . В UNIX, <code>ConnectionServer32</code> .
%CONNECTIONSERVER_DIR%	Корневая папка сервера соединений.	В ОС Windows это <code><INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/dataAccess/connectionServer</code> . В UNIX это <code><INSTALLDIR>/sap_bobj/enterprise_xi40/platform</code> .
%CONNECTIONSERVER_EXE%	Имя выполняемого файла для 64-битного сервера соединений.	В ОС Windows это <code>ConnectionServer.exe</code> . В UNIX это <code>ConnectionServer</code> .
%CR2011_BINDIR%	Каталог, где расположены двоичные файлы сервера Crystal Reports 2011.	В Windows это <code><INSTALLDIR>/SAP BusinessObjectsEnterprise XI 4.0/win32_x86</code> .
%CR2011_DefaultWorkingDir%	Рабочий каталог по умолчанию для серверов Crystal Reports 2011.	В Windows это <code><INSTALLDIR>/SAP BusinessObjectsEnterprise XI 4.0/win32_x86</code> .
%CRYSTALRAS_EXE%	Имя выполняемого файла сервера Report Application Server.	В ОС Windows это <code>crystalras.exe</code> . В ОС UNIX это <code>boe_crystalrasd</code> .
%CR_ODBCINI%	Полное имя (включая путь) файла <code>.odbc.ini</code> . **	В UNIX это <code><INSTALLDIR>/bobje/odbc.ini</code> . Для Windows это пустая строка.
%CommonJavaBundlesDir%	Папка, где находится OSGI.	В ОС Windows это <code><INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/java/bundles</code> . В UNIX это <code><INSTALLDIR>/sap_bobj/enterprise_xi40/java/bundles</code> .

Заполнитель	Описание	Значения по умолчанию
%CommonJavaLibDir%	Папка, где находятся общие библиотеки Java.	В ОС Windows это <code><INSTALLEDIR>/SAP BusinessObjects Business Intelligence platform 4.0/java/lib</code> . В UNIX это <code><INSTALLEDIR>/sap_bobje/enterprise_xi40/java/lib</code>
%DLLEXT%	Расширение по умолчанию DLL- или SO-файла.	В ОС Windows это <code>.dll</code> . В ОС UNIX это <code>.so</code> .
%DLLPATH%	На компьютере с установленной платформой BI – это имя переменной среды, обозначающее каталоги, где интерпретатор будет искать исполняемые файлы.	В ОС Windows это «Path». В ОС UNIX это «LD_LIBRARY_PATH».
%DLLPATH32%	В 32-битных системах Solaris, на компьютере с установленной платформой BI – это имя переменной среды, обозначающее каталоги, где интерпретатор будет искать исполняемые файлы.	На компьютерах Solaris это путь «LD_LIBRARY_PATH_32». Для других операционных систем этот заполнитель представляет собой пустую строку.
%DLLPATH64%	В 64-битных системах Solaris, на компьютере с установленной платформой BI – это имя переменной среды, обозначающее каталоги, где интерпретатор будет искать исполняемые файлы.	На компьютерах Solaris это путь «LD_LIBRARY_PATH_64». Для других операционных систем этот заполнитель представляет собой пустую строку.
%DLLPREFIX%	Префикс по умолчанию DLL- или SO-файла.	В UNIX, «lib». Для компьютеров с ОС Windows этот заполнитель представляет собой пустую строку.
%DLLPRELOAD%	Имя переменной среды LD_PRELOAD для платформы.	В ОС UNIX это LD_PRELOAD. Для компьютеров с ОС Windows этот заполнитель представляет собой пустую строку.
%DLLPRELOAD32%	Имя переменной среды LD_PRELOAD в 32-разрядных системах AIX.	В ОС AIX это «LDR_PRELOAD». На остальных компьютерах этот заполнитель представляет собой пустую строку.

Заполнитель	Описание	Значения по умолчанию
%DLLPRELOAD64%	Имя переменной среды LD_PRELOAD в 64-битных системах AIX.	В ОС AIX это «LDR_PRELOAD64». На остальных компьютерах этот заполнитель представляет собой пустую строку.
%DP%	Разделитель пути.	В ОС Windows это «;». В ОС UNIX это «:».
%DefaultAuditingDir%	Каталог, куда записываются временные файлы аудита. Для оптимизации производительности это местоположение должно быть на локальном диске сервера.	В ОС Windows это <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/Auditing. В UNIX это <INSTALLDIR>/sap_bobj/data/Auditing/.
%DefaultDataDir%	Временный каталог, используемый сервером заданий.	В ОС Windows это <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/Data. В UNIX это <INSTALLDIR>/sap_bobj/data/.
%DefaultInputFRSDir%	Корневая папка на сервере репозитория входных файлов.	В ОС Windows это <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/FileStore/Input. В UNIX это <INSTALLDIR>/sap_bobj/data/frsinput.
%DefaultLoggingDir%	Местоположение, где хранятся файлы журнала.	В ОС Windows это <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/logging. В UNIX это <INSTALLDIR>/sap_bobj/logging.
%DefaultOutputFRSDir%	Корневая папка на сервере репозитория входных файлов.	В ОС Windows это <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/FileStore/Output. В UNIX это <INSTALLDIR>/sap_bobj/data/frsoutput.

Заполнитель	Описание	Значения по умолчанию
%DefaultWorkingDir%	Рабочий каталог для 64-битных серверов.	В Windows это <INSTALLDIR>/SAP BusinessObjectsEnterprise XI 4.0/win64_x64. В UNIX это <INSTALLDIR>/sap_bobj/enterprise_xi40/platform
%DefaultWorkingDir32%	Рабочий каталог для 32-битных серверов.	В OC Windows это <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/win32_x86. В UNIX это <INSTALLDIR>/sap_bobj/enterprise_xi40/platform
%EPM_LD_PRELOAD_ONCE%	Имя переменной среды LD_PRELOAD_ONCE для платформы.	\$LD_PRELOAD_ONCE\$
%EVENTSERVER_EXE%	Имя исполняемого файла сервера событий.	В OC Windows это EventServer.exe. В OC UNIX это boe_eventsd.
%EXEEXT%	Расширение по умолчанию исполняемых файлов.	В OC Windows это .exe. В OC UNIX этот заполнитель не используется.
%EXEPATH%	На компьютере с установленной платформой BI это имя переменной среды, обозначающее каталоги, где интерпретатор будет искать исполняемые файлы.	В OC Windows это «Path». В OC UNIX это «PATH».
%EnterpriseDir%	Местоположение установленной 64-битной платформы BI.	В OC Windows это <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/. В UNIX это <INSTALLDIR>/sap_bobj/enterprise_xi40.
%EnterpriseDir32%	Местоположение установленной 32-битной платформы BI.	В OC Windows это <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/. В UNIX, <INSTALLDIR>/sap_bobj/enterprise_xi40.

Заполнитель	Описание	Значения по умолчанию
%ExternalJavaLibDir%	Папка, где находятся внешние библиотеки Java сторонних организаций.	В ОС Windows это <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/java/lib/external. В UNIX это <INSTALLDIR/sapobje/enterprise_x4/java/lib/external
%FILESERVER_EXE%	Имя выполняемого файла файлового сервера	В ОС Windows это fileserver.exe. В ОС UNIX это boe_filesd.
%HOARD_PATH%	Местоположение диспетчера памяти.	По умолчанию значение не указано.
%HOARD_PRELOAD%	Указывает, требуется ли предварительная загрузка диспетчера памяти.	По умолчанию значение не указано.
%INSTALLROOTDIR%	Папка с установленной 64-битной платформой BI.	Это значение задается во время установки.
%INSTALLROOTDIR32%	Папка с установленной 32-битной платформой BI.	Это значение задается во время установки.
%IntroscopeAgentEnableInstrumentation%	Указывает, включены ли инструментальные средства для серверов Java, которые используют агент Introscope Agent Enterprise.	Допустимы значения – TRUE и FALSE. Значение зависит от того, был ли включен диспетчер Introscope Agent Enterprise во время установки платформы BI.
%IntroscopeAgentEnterpriseManagerHost%	Имя хоста диспетчера Introscope Agent Enterprise, куда отправляются данные инструментальных средств.	Это значение задается во время установки.
%IntroscopeAgentEnterpriseManagerPort%	Имя хоста диспетчера Introscope Agent Enterprise, куда отправляются данные инструментальных средств.	Это значение задается во время установки.

Заполнитель	Описание	Значения по умолчанию
%IntroscopeAgentEnterpriseManagerTransport%	Транспорт, используемый при отправке данных инструментальных средств диспетчеру Introscope Agent Enterprise. Допустимые значения: <ul style="list-style-type: none"> • TCP • HTTP • HTTPS • SSL 	TCP
%IntroscopeAgentEnterpriseManagerTransportHTTP%	Класс, используемый при отправке данных инструментальных средств диспетчеру Introscope Agent Enterprise через HTTP.	com.wily.introscope.agent.transport.http.HttpTransportFactory
%IntroscopeAgentEnterpriseManagerTransportHTTPS%	Класс, используемый при отправке данных инструментальных средств диспетчеру Introscope Agent Enterprise через HTTPS.	com.wily.introscope.agent.transport.https.HttpsTransportFactory
%IntroscopeAgentEnterpriseManagerTransportSSL%	Класс, используемый при отправке данных инструментальных средств диспетчеру Introscope Agent Enterprise через SSL.	com.wily.introscope.agent.transport.ssl.SslTransportFactory
%IntroscopeAgentEnterpriseManagerTransportTCP%	Класс, используемый при отправке данных инструментальных средств диспетчеру Introscope Agent Enterprise через TCP.	com.wily.introscope.agent.transport.tcp.TcpTransportFactory
%IntroscopeDir%	Папка, в которой установлен Introscope Agent Enterprise Manager.	В ОС Windows это <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/java/wily. В UNIX это <INSTALLDIR>/sap_bobj/enterprise_xi40/java/wily
%JAVAW_EXE%	Имя исполняемого файла для виртуальной машины Java, в которой нет окна консоли.	В ОС Windows это javaw.exe. В ОС UNIX это java.
%JAVA_EXE%	Имя исполняемого файла для виртуальной машины Java.	В ОС Windows это java.exe. В ОС UNIX это java.
%JOBSEVERCHILD_EXE%	Имя исполняемого файла дочернего настраиваемого сервера заданий.	В ОС Windows это JobServerChild.exe. В ОС UNIX это boe_jobcd.

Заполнитель	Описание	Значения по умолчанию
%JOBSEVER_EXE%	Имя исполняемого файла настраиваемого сервера заданий.	В ОС Windows это JobServer.exe. В ОС UNIX это boe_jobsd.
%JdkBinDir%	Папка, где находятся двоичные файлы JDK.	В ОС Windows это <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/win64_x64/sapjvm/bin. В UNIX это <INSTALLDIR>/sap_bobje/<PLATFORM>/sapjvm/bin
%JreBinDir%	Папка, где находятся двоичные файлы JRE.	В ОС Windows это <INSTALLDIR>/javasdk/bin. В UNIX это <INSTALLDIR>/sap_bobje/<PLATFORM>/sapjvm/jre/bin
%JVM_ARCH_ENVIRONMENT%	Указывает, на какой JVM работает компьютер: 32-битной или 64-битной.	Для компьютеров с 32-битной ОС UNIX используется значение по умолчанию «-d32». Для 64-битных компьютеров используется значение по умолчанию «-d64». Для компьютеров с ОС Windows это пустая строка.
%JVM_HEADLESS_MODE%	Аргумент командной строки, который указывает, работает ли JVM в режиме с неполным набором устройств ввода-вывода.	В ОС Windows - Djava.awt.headless=false. В ОС UNIX -Djava.awt.headless=true
%JVM_HEAP_DUMP_ON_OUT_OF_MEMORY_ERROR%	Параметры командной строки, задающие поведение JVM при обнаружении ошибок "Недостаточно памяти".	"-XX:+HeapDumpOnOutOfMemoryError" " XX:HeapDumpPath=%DefaultLoggingDir%" " XX:+ExitVMOnOutOfMemoryError"
%JVM_SHARED_MEMORY_SEGMENT%	Параметры командной строки для включения расширений JVM и задания номера экземпляра JVM.	По умолчанию этот заполнитель является пустым.
%LANGUAGEPACKSDIR%	Папка, в которой хранятся языковые пакеты развертывания.	В Windows и UNIX, <INSTALLDIR>.
%LANGUAGEPACKSDIR32%	Папка, в которой установлены языковые пакеты развертывания в 32-битных системах.	В Windows и UNIX, <INSTALLDIR>.

Заполнитель	Описание	Значения по умолчанию
%LSTDir%	Папка, в которой хранятся файлы конфигурации LST.	В ОС Windows это <code><INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/conf/lst</code> . В UNIX это <code><INSTALLDIR>/sap_bobj/enterprise_xi40/conf/lst</code> .
%MDAS_JVM_OS_STACK_SIZE%	Указывает размер стека JVM для службы многомерного анализа.	По умолчанию этот заполнитель является пустым.
%NCSInstrumentLevelThreshold%	Пороговый уровень регистрации трассировки для библиотеки NCS.	Это значение определяется во время установки.
%PAGESERVER_EXE%	Имя исполняемого файла сервера обработки Crystal Reports 2011.	В ОС Windows это <code>crproc.exe</code> . В UNIX это <code>boe_crprocd.bin</code> .
%PJSContainerDir%	Папка, в которой расположены JAR-файлы контейнера APS.	В ОС Windows это <code><INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/java/pjs/container</code> . В UNIX это <code><INSTALLDIR>/sap_bobj/enterprise_xi40/java/pjs/container</code> .
%PJSServicesDir%	Папка, в которой расположены JAR-файлы службы APS.	В ОС Windows это <code><INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/java/pjs/services</code> . В UNIX это <code><INSTALLDIR>/sap_bobj/enterprise_xi40/java/pjs/services</code> .
%Platform%	Операционная система на компьютере, на котором выполняется платформа BI.	Операционная система на компьютере, на котором выполняется платформа BI.
%Platform32%	Операционная система компьютера, на котором выполняется 32-битная платформа BI.	Операционная система на компьютере, на котором выполняется платформа BI.
%RasBinDir%	Корневая папка сервера приложений отчетов.	В ОС Windows это <code><INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/win32_x86</code> . В UNIX, <code><INSTALLDIR>/sap_bobj/enterprise_xi40/BATCH/ras</code> .

Заполнитель	Описание	Значения по умолчанию
%SERVER_FRIENDLY_NAME%	Полное имя сервера.	Полное имя сервера.
%SERVER_NAME%	Полное имя сервера.	Полное имя сервера.
%SMDAgentHost%	Имя хоста агента SMD, куда отправляются данные инструментальных средств.	Это значение задается во время установки.
%SMDAgentPort%	Порт агента SMD, куда отправляются данные инструментальных средств.	Это значение задается во время установки.
%TRACE_CONFIGFILE_INI%	Полное имя (включая путь) файла BO_Trace.ini.	В OC Windows это <INSTALLDIR>/SAP BusinessObjects Business Intelligence platform 4.0/logging/logConfig/BO_Trace.ini. В UNIX это <INSTALLDIR>/sapobj/enterprise_xi140/conf/BO-trace.ini.
%WEBI_LD_PRELOAD%	Имя переменной среды LD_PRELOAD для платформы.	\$LD_PRELOAD\$
%WEBISERVER_EXE%	Имя исполняемого файла сервера обработки Web Intelligence.	В OC Windows это wireportserver.exe. В OC UNIX это WIReportServer.
%WEBI_LD_PRELOAD_ONCE%	Имя переменной среды LD_PRELOAD_ONCE для платформы.	\$LD_PRELOAD_ONCE\$
%XCCACHE_EXE%	Имя исполняемого файла для кэш-сервера Dashboard Design.	В OC Windows это xccache.exe. В UNIX. boe_xccached.
%XCPROC_EXE%	Имя исполняемого файла для сервера обработки Dashboard Design.	В OC Windows это xcproc.exe. В UNIX это boe_xcprocd.

Примечание:

Следующие заполнители можно изменять на уровне узла. Описатели и значения по умолчанию можно найти в вышеприведенной таблице. Заполнители, не отображаемые в этом списке, доступны только для чтения.

- %DefaultAuditingDir%
- %DefaultDataDir%
- %DefaultLoggingDir%
- %IntroscopeAgentEnableInstrumentation%

- %IntroscopeAgentEnterpriseManagerHost%
- %IntroscopeAgentEnterpriseManagerPort%
- %IntroscopeAgentEnterpriseManagerTransport%
- %NCSInstrumentLevelThreshold%
- %SMDAgentHost%
- %SMDAgentPort%

См. также

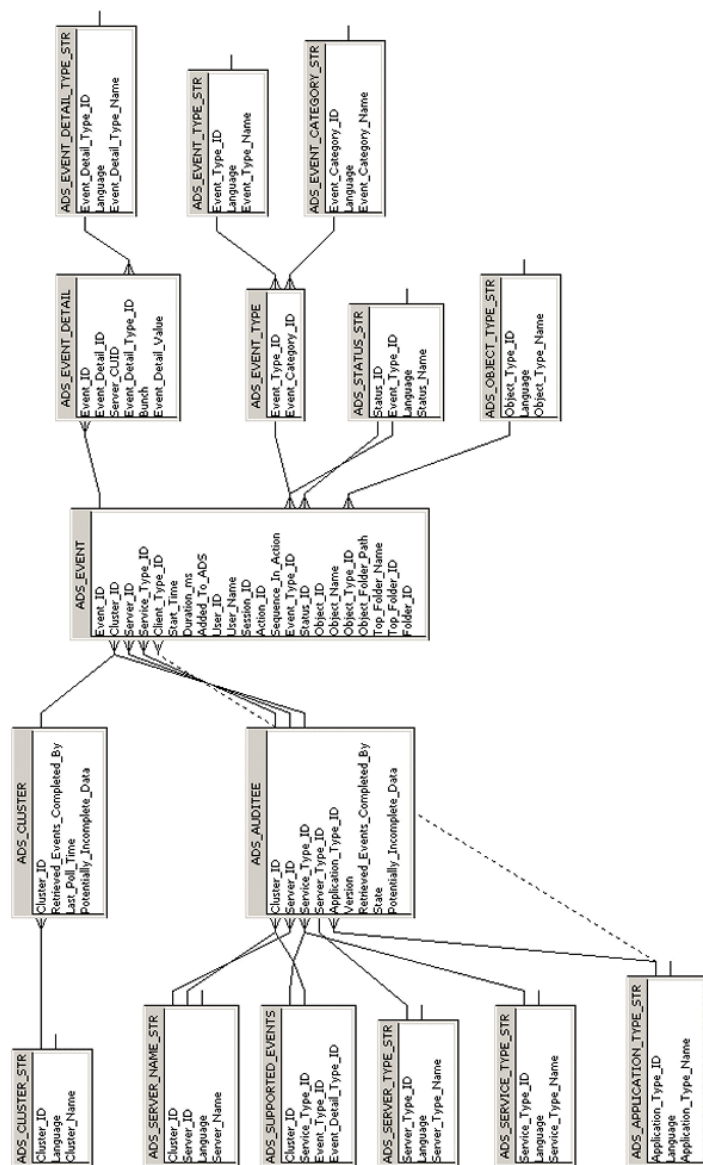
- [Просмотр и изменение заполнителей для узла](#)

Приложение выполнения аудита схемы склада данных

27.1 Обзор

Это приложение является справочным материалом для дизайнеров отчетов, на которое можно ссылаться и по которому можно производить отчеты из таблиц хранилища данных аудита. В пояснениях к приведенным ниже диаграмме и таблице показаны таблицы, куда записываются данные аудита, а также взаимосвязь этих таблиц.

27.2 Диаграмма схемы



27.3 Таблицы аудита склада данных

Таблица ADS_EVENT

Данная таблица содержит основные свойства каждого события, центральную точку связи для других таблиц в схеме.

Имя столбца	Тип поля	Ключ	Описание
Event_ID	Символ (64)	Основной ключ	Уникальный идентификатор, созданный для события.
Cluster_ID	Символ (64)	Внешний ключ в таблице ADS_Auditee.	GUID кластера аудита. Записывается, так как несколько кластеров могут использовать одну ADS.
Server_ID	Символ (64)	Внешний ключ в таблице ADS_Auditee.	CUID сервера, запустившего событие.
Service_Type_ID	Символ (64)	Внешний ключ в таблице ADS_Auditee.	<ul style="list-style-type: none"> CUID типа службы, запустившей событие. Службы на серверы содержат собственные CUID типа службы. Клиентские приложения (например, стартовая панель BI или Web Intelligence) записывают собственный идентификатор CUID типа приложения.
Client_Type_ID	Символ (64)	Внешний ключ в таблице ADS_Auditee.	Содержит идентификатор типа клиента, который установил сеанс.
Start_Time	Дата и время	Нет данных	Дата и время запуска операции события (включая миллисекунды).
Duration_ms	Целое	Нет данных	Длительность операции в миллисекундах.
Added_to_ADS	Дата и время	Нет данных	Дата и время записи события в ADS.
User_ID	Символ (64)	Нет данных	CUID пользователя, выполнившего действие.
User_Name	Символ (255)	Нет данных	Имя, связанное с идентификатором пользователя, выполнившего действия. Записывается на языке по умолчанию для аудитора CMS.
Session_ID	Символ (64)	Нет данных	GUID сеанса, во время которого было запущено событие. При отсутствии связанного сеанса поле будет пустым.
Action_ID	Символ (64)	Нет данных	Идентификатор действия пользователя, запустившего событие. Используется для группировки событий, которые являются результатами одного действия пользователя.

Имя столбца	Тип поля	Ключ	Описание
Sequence_In_Action	Целое	Нет данных	Для многосерверных событий (или клиентских и многосерверных) приложение сервера или клиента в последовательности, запустившее событие. Во всех рабочих процессах планирования идентификатор последовательности будет всегда 0.
Event_Type_ID	Целое	Внешний ключ в таблице ADS_Event_type.	Тип события (например, Просмотр или Сохранить).
Status_ID	Целое	Внешний ключ в таблице ADS_Status_Str.	Состоянии операции (например, "0" = выполнено, "1" = сбой).
Object_ID	Символ (64)	Нет данных	CUID объекта, над которым выполнена операция.
Object_Name	Символ (255)	Нет данных	Имя объекта, над которым выполнена операция. Записывается на языке по умолчанию для аудитора CMS.
Object_Type_ID	Символ (64)	Внешний ключ в таблице ADS_Object_Type_Str.	CUID типа объекта, над которым выполнена операция.
Object_Folder_Path	Символ (255)	Нет данных	Полный путь к папке (например, Country/Region/City) для объекта, над которым выполнена операция. CUID типа объекта, над которым выполнена операция. Если путь к папке не может быть определен, данное значение остается пустым.
Folder_ID	Символ (64)	Нет данных	CUID папке для объекта, над которым выполнена операция.
Top_Folder_Name	Символ (255)	Нет данных	Имя папки верхнего уровня объекта. Например, если объект размещен в Country/Region/City, значением будет Country.
Top_Folder_ID	Символ (64)	Нет данных	CUID папки верхнего уровня, в которой расположен объект. Например, если объект размещен в Country/Region/City, будет записан CUID папки Country.

Таблица ADS_EVENT_DETAIL

Данная таблица содержит свойства сведений события.

Имя столбца	Тип	Ключ	Описание
Event_Detail_ID	Целое	Основной ключ	GUID для сведений события.
Event_ID	Символ (64)	Внешний ключ в ADS_Event.	GUID родительского события.
Event_Detail_Type_ID	Целое	Внешний ключ в ADS_Event_Detail	Тип сведений события.
Набор	Целое	Нет данных	<p>Если сведения являются частью серии, данный параметр используется для их связки.</p> <p>Например, если отчет содержит приглашения для Штата и Страны, пользователь может ввести для запроса страны "США", а для приглашения для штата "Калифорния" и "Невада". При этом будут созданы сведения о событии с двумя наборами. Первый набор будет содержать:</p> <ul style="list-style-type: none"> Имя приглашения: Страна Значение приглашения: США <p>Второй набор будет содержать:</p> <ul style="list-style-type: none"> Имя приглашения: Штат Значение приглашения: Калифорния Значение приглашения: Невада
Event_Detail_Value	Символ (подробный текст)	Нет данных	Значение сведений о событии.

Таблица ADS_AUDITEE

Данная таблица содержит информацию по свойству для всех серверов аудита, являющихся частью развертывания.

Имя столбца	Тип	Ключ	Описание
Cluster_ID	Символ (64)	Основной ключ	GUID для кластера, к которому принадлежит проверяемый компонент.

Имя столбца	Тип	Ключ	Описание
Server_ID	Символ (64)	<ul style="list-style-type: none"> Основной ключ ADS_Server_Name_STR 	CUID сервера, запустившего событие. В случае запуска события клиентом будет записан CUID адаптивного сервера обработки, обработавшего событие.
Service_Type_ID	Символ (64)	<ul style="list-style-type: none"> Основной ключ ADS_Service_Type_STR ADS_Supported_Event 	CUID типа службы для службы, запустившей событие. События, запущенные клиентом, записывают CUID типа приложения.
Server_Type_ID	Символ (64)	ADS_Server_Type_STR	CUID типа сервера для сервера, запустившего событие.
Код Application_Type_ID	Символ (64)	ADS_Application_Type_STR	CUID типа приложения для клиента, запустившего событие. Для событий сервера записывается идентификатор типа службы.
Версия	Символ (64)	Нет данных	Версия сервера или клиента, запустившего событие, во время записи.
Retrieved_Events_Completed_By	Дата и время	Нет данных	Последнее время, когда аудитор CMS опрашивал проверяемый компонент относительно временных файлов. Указывает на то, что все события от данного проверяемого компонента завершены до данной даты/времени в ADS.
Состояние	Целое	Нет данных	Состояние (выполняется, не выполняется, удалено), в котором был проверяемый компонент.
Potentially_Incomplete_Data	Целое	Нет данных	Указывает на возможность наличия для проверяемого компонента событий, которые не были переданы в ADS.

Таблица ADS_SERVER_NAME_STR

Данная таблица содержит многоязычный словарь имен серверов. Значения обновляются при смене имен.

Имя столбца	Тип	Ключ	Описание
Cluster_ID	Символ (64)	Основной ключ	GUID кластера, которому принадлежит сервер.
Server_ID	Символ (64)	Основной ключ	CUID сервера.
Язык	Символ (10)	Основной ключ	Код языка имени сервера, например <i>EN</i> или <i>DE</i> .
Server_Name	Символ (255)	Нет данных	Имя сервера

Таблица ADS_SERVICE_TYPE_STR

Данная таблица содержит многоязычный словарь для имен типов службы.

Имя столбца	Тип	Ключ	Описание
Service_Type_ID	Символ (64)	Основной ключ	CUID типа службы или категории службы для службы.
Язык	Символ (10)	Основной ключ	Код языка, на котором записано имя типа службы, например <i>EN</i> или <i>DE</i> .
Service_Type_Name	Символ (255)	Нет данных	Имя типа службы.

Таблица ADS_APPLICATION_TYPE_STR

Данная таблица содержит многоязычный словарь имен типов приложений клиента.

Имя столбца	Тип	Ключ	Описание
Код Application_Type_ID	Символ (64)	Основной ключ	CUID типа приложения для приложения.
Язык	Символ (10)	Основной ключ	Код языка типа приложения; например, <i>EN</i> или <i>DE</i> .
Application_Type_Name	Символ (255)	Нет данных	Текстовое имя типа приложения, например, Crystal Reports или Web Intelligence.

Таблица ADS_SUPPORTED_EVENTS

Данная таблица содержит список поддерживаемых событий и связанных сведений событий для каждого типа службы или приложения клиента.

Имя столбца	Тип	Ключ	Описание
Cluster_ID	Символ (64)	Основной ключ	GUID кластера, которому принадлежит служба.
Service_Type_ID	Символ (64)	Основной ключ	CUID типа службы, запустившей событие. Если событие запущено приложением клиента, записывается CUID типа службы.
Event_Type_ID	Целое	Внешний ключ в ADS_Event_Type	Идентификатор типа записанного события (например, идентификатор "Сохранить").
Event_Detail_Type_ID	Целое	Внешний ключ в ADS_Event_Type	CUID, идентифицирующий тип сведений события, собранных для данного события (например, Путь к файлу).

Таблица ADS_CLUSTER

Данная таблица содержит информацию по кластерам, содержащим проверяемый компонент.

Имя столбца	Тип	Ключ	Описание
Cluster_ID	Символ (64)	<ul style="list-style-type: none"> Основной ключ ADS_Cluster_Str 	GUID кластера.
Retrieved_Events_Completed_By	Дата и время	Нет данных	Указывает оперативность информации аудита в базе данных для данного кластера. Записывает самую старую метку времени аудита для всех текущих выполняемых серверов аудита в любой заданный момент времени. Указывает на завершение всех событий до данной даты в ADS.
Last_Poll_Time	Дата и время	Нет данных	Последнее время, когда аудитор CMS опрашивал проверяемый компонент в данном кластере.

Имя столбца	Тип	Ключ	Описание
Potentially_Incomplete_Data	Целое	Нет данных	Указывает на потенциально неполную информацию аудита в рамках кластера: "0" = все серверы передали данные нормально и "1" = не менее одного запущенного или незапущенного сервера в кластере имеют флаг Потенциально неполные данные , что указывает на то, что один проверяемый компонент имеет события, которые не были переданы в ADS.

Таблица ADS_CLUSTER_STR

Данная таблица содержит ссылочную запись различных кластеров в развертывании.

Имя столбца	Тип	Ключ	Описание
Cluster_ID	Символ (64)	Основной ключ	Уникальный идентификатор кластера.
Язык	Символ (10)	Нет данных	Код настройки языка для кластера, например <i>EN</i> или <i>DE</i> .
Cluster_Name	Символ (255)	Нет данных	Имя кластера.

Таблица ADS_EVENT_TYPE

Данная таблица содержит ссылочную запись для различных категорий событий.

Имя столбца	Тип	Ключ	Описание
Event_Type_ID	Целое	Составной: <ul style="list-style-type: none"> Основной ключ ADS_Event_Type_Str 	Уникальный идентификатор типа события.
Event_Catagory_ID	Целое	Таблица ADS_Event_Category_Str	Категория события. Например, общее, Web Intelligence или Управление жизненным циклом.

Таблица ADS_EVENT_TYPE_STR

Данная таблица содержит многоязычный словарь для имен типов события.

Имя столбца	Тип	Ключ	Описание
Event_Category_ID	Целое	Основной ключ	Идентификатор типа события для события.
Язык	Символ (10)	Основной ключ	Код языка, на котором записано имя категории события, например <i>EN</i> или <i>DE</i> .
Event_Type_Name	Символ (255)	Нет данных	Текстовое имя типа события, например "Просмотр" или "Вход в систему".

Таблица ADS_EVENT_CATEGORY_STR

Данная таблица содержит многоязычный словарь имен категорий событий.

Имя столбца	Тип	Ключ	Описание
Event_Type_ID	Целое	Основной ключ	Идентификатор категории события.
Язык	Символ (10)	Основной ключ	Код языка, на котором записано имя категории события, например <i>EN</i> или <i>DE</i> .
Event_Category_Name	Символ (255)	Нет данных	Имя категории события.

Таблица ADS_EVENT_DETAIL_TYPE_STR

Данная таблица содержит многоязычный словарь имен типов сведений события.

Имя столбца	Тип	Ключ	Описание
Event_Detail_ID	Целое	Основной ключ	Идентификатор типа сведений события для сведений события.
Язык	Символ (10)	Основной ключ	Код языка, на котором записано имя сведений о событии, например <i>EN</i> или <i>DE</i> .
Event_Detail_Type_Name	Символ (255)	Нет данных	Тестовое имя типа сведений о событии.

Таблица ADS_OBJECT_TYPE_STR

Данная таблица содержит многоязычный словарь для имен объектов событий.

Имя столбца	Тип	Ключ	Описание
Object_Type_ID	Символ (64)	Основной ключ	CUID типа объекта для объекта.
Язык	Символ (10)	Основной ключ	Код языка, на котором записано имя типа объекта, например <i>EN</i> или <i>DE</i> .
Object_Type_Name	Символ (255)	Нет данных	Имя типа объекта.

Таблица ADS_STATUS_STR

Данная таблица содержит многоязычный словарь имен статусов событий.

Имя столбца	Тип	Ключ	Описание
Status_ID	Целое	Основной ключ	Числовое представление состояния операции.
Event_Type_ID	Целое	Основной ключ	Идентификатор типа события для события. Например, 1002 для события Просмотр.
Язык	Символ (10)	Основной ключ	Код языка, на котором записано состояние события, например <i>EN</i> или <i>DE</i> .
Status_Name	Символ (255)	Нет данных	Текстовое описание состояния события, например "Выполнено" и "Сбой".

ADS_EVENT_DELETES

Не использовать отчеты из этой таблицы. Предназначено только для внутреннего использования системой и может быть исключено в последующих выпусках.

Дополнительная информация

Источник информации	Местоположение
Информация о продуктах SAP BusinessObjects	http://www.sap.com
Справочный портал SAP	<p>Перейдите к http://help.sap.com/businessobjects/ и на боковой панели «BusinessObjects Overview» выберите All Products.</p> <p>Справочный портал SAP предоставляет доступ к актуальной документации по всем продуктам SAP BusinessObjects и их развертыванию. Можно загрузить документы в формате PDF или устанавливаемые HTML-библиотеки.</p> <p>Некоторые руководства находятся на веб-сайте SAP Service Marketplace и недоступны на справочном портале SAP. На данном портале перечислены эти руководства и даны соответствующие ссылки на SAP Service Marketplace. Клиенты, заключившие соглашение о техническом обслуживании, получают идентификатор авторизованного пользователя для доступа к этому веб-сайту. Для получения идентификатора обратитесь к представителю службы поддержки пользователей.</p>
SAP Service Marketplace	<p>http://service.sap.com/bosap-support > Документация</p> <ul style="list-style-type: none"> • Руководства по установке: https://service.sap.com/bosap-instguides • Примечания к выпуску: http://service.sap.com/releasenotes <p>На веб-сайте SAP Service Marketplace содержатся некоторые руководства по установке, модернизации, миграции и развертыванию, а также примечания к версиям и документация по поддерживаемым платформам. Клиенты, заключившие соглашение о техническом обслуживании, получают идентификатор авторизованного пользователя для доступа к этому веб-сайту. Для получения идентификатора обратитесь к представителю службы поддержки пользователей. Если вас перенаправили на веб-сайт SAP Service Marketplace со справочного портала SAP, с помощью меню в навигационной панели слева перейдите в категорию, содержащую нужные вам документы.</p>

Источник информации	Местоположение
Docupedia	https://cw.sdn.sap.com/cw/community/docupedia Docupedia предоставляет дополнительные ресурсы документации, объединенную среду для создания контента и интерактивный канал обратной связи.
Ресурсы разработчика	https://bos.sdn.sap.com/ https://www.sdn.sap.com/irj/sdn/businessobjects-sdclibrary
Статьи SAP BusinessObjects в сети сообщества SAP	https://www.sdn.sap.com/irj/boc/businessobjects-articles Подобные статьи ранее назывались технической документацией.
Примечания	https://service.sap.com/notes Эти примечания ранее назывались статьями базы знаний.
Форумы в сети сообщества SAP	https://www.sdn.sap.com/irj/scn/forums
Обучение	http://www.sap.com/services/education Мы можем предложить обучающий пакет, соответствующий вашим потребностям и предпочтительным формам обучения – от классических занятий в классах до специализированных курсов eLearning.
Интерактивная служба поддержки пользователей	http://service.sap.com/bosap-support На портале службы поддержки SAP представлены сведения о программах и услугах поддержки. Здесь также содержатся ссылки на самую разнообразную техническую информацию и множество файлов для загрузки. Клиенты, заключившие соглашение о техническом обслуживании, получают идентификатор авторизованного пользователя для доступа к этому веб-сайту. Для получения идентификатора обратитесь к представителю службы поддержки пользователей.

Источник информации	Местоположение
Консалтинговые услуги	http://www.sap.com/services/bysubject/businessobjectsconsulting Наши консультанты готовы оказывать вам поддержку на всех этапах – от начального анализа до развертывания системы. Советы экспертов можно найти, например, в темах, посвященных относительным и многомерным базам данных, возможностям подключения, средствам разработки баз данных и технологии встраивания с индивидуальными настройками.

Указатель

Символы

.NET Software Development Kit (SDK)
31

A

Analysis, выпуск OLAP 74

B

BackupCluster.bat 481
backupcluster.sh 481
BExWebApplicationsService 540
BOLMT 90, 375
BW
 включение просмотра 710
 интеграция с платформой BI 695
BW Publisher
 настройка в UNIX 698
 настройка в качестве службы 698
 распространение компонентов
 698

C

CA Wily Introscope 38
cacert.der 171, 172
cakey.pem 171, 172
ccm.config 789
ccm.exe 794, 796
ccm.sh 785, 789
 восстановление настроек
 сервера 486
Central Configuration Manager (CCM)
21, 68
Central Management Console (CMC)
21, 71
ClearCase 40
CMS 295, 328, 554
 аутентификация 224
 добавление в кластер 387
 параметры командной строки 800
 переменные сеанса 153
 аутентификация 224
 отслеживание 154
 показатели 396
 распределенная безопасность
 152
 свойства 848

cmsdbsetup.sh 789
Consumer SDK платформы SAP
 BusinessObjects Business
 Intelligence 31
Content Administration Workbench 704
 добавление систем платформы
 BI 704
 обзор публикации отчета 700
 обновление источников данных
 отчетов 709
 определение уровней доступа
 пользователей 701
 публикация отчетов в фоновом
 режиме 709
 синхронизация информации
 отчета 709
 удаление отчетов 710
Crystal Reports
 права 820
 см. SAP Crystal Reports 70
Crystal Reports 2010 Report
 Application Server 554
Crystal Reports Viewers SDK 31
custom.jsp 537

D

Dashboard Builder 72
Data Access
 обзор установки 713

E

env.sh 792
Explorer 635
 права 840
 см. SAP BusinessObjects Explorer
 70

F

FIPS-совместимый режим
 Включение UNIX 160
 включение Windows 159
 отключение Windows 160
 параметр безопасности 158
 Федеральный стандарт
 обработки информации 158

G

GWSETUP 699

H

HTTP 153, 224
HTTPS
 настройка серверов контейнера
 веб-приложений (WACS) 455,
 457, 470

I

InfoView 72
initlaunch.sh 793
INSTALLDIR 18
Introscope 574
IPv6
 настройка адреса в CMC 406
 параметры 404
 CMC 404
ISA 2006
 конфигурация для Oracle 10gR3
 218
 конфигурация для Sun Java 8.2
 218
 конфигурация для Tomcat 5.5 218
 конфигурация для WebSphere
 CE 2.0 218
iView
 включение просмотра 710

J

JAAS, файл конфигурации 273, 274,
463
Java Software Development Kit (SDK)
31
Java, Kerberos 276
JD Edwards EnterpriseOne 38
JMX MBeans 571
JMX Remote API 570

K

Kerberos 270, 461
Krb5.ini 272, 463
единый вход для Java 468

Kerberos (*(продолжение)*)
 единый вход для Java InfoView 278
 и NetWeaver SSO 274
 устранение неполадок 294, 464
 файл конфигурации 270, 272, 462
 KPI (ключевой показатель эффективности) 549
 Krb5.ini 272, 463

L

LDAP
 Secure Sockets Layer (SSL) 244
 аутентификация 244
 настройка 246
 группы
 сопоставление 257
 настройка единого входа 255
 подключаемый модуль аутентификации 245
 подключаемый модуль безопасности 245
 сопоставление с Windows AD 260
 учетные записи 244
 устранение неполадок 262
 хосты
 настройка 247, 252
 управление несколькими 250
 Live Office
 конфигурация для обратных прокси-серверов 216
 logon.csp 224

M

MBean 551
 Mobile
 права 842

O

ODBC
 база данных CMS
 взаимодействие 442
 OpenDocument
 настройка входа в систему 536
 OpenSearch 622
 OpenSearch с помощью WDeploy 623
 Oracle
 JAAS 273
 Kerberos 270
 параметры Java 276

Oracle E-Business Suite 38
 сопоставление ролей со службами информационной платформы 360
 Oracle EBS
 обновить псевдонимы 363
 обновить роли 363

P

PeopleSoft Enterprise 38
 PLATFORM64DIR 18
 PlatformServices.properties 388
 PSE
 доверие со стороны сервера 310
 настройка доступа 317

Q

Query as a Web Service
 см. "Средство запросов веб-служб" 65

R

Report Application Server SDK 31
 Report Engine SDK 31
 Repository Diagnostic Tool 22, 69
 restart.sh 792
 RestoreCluster.bat 487
 restorecluster.sh 487
 RFC-адресат 699
 для локального шлюза SAP 700
 для службы BW Publisher 699

S

SAML
 SSO 234
 SAP
 интеграция 38
 настройка брандмауэра 201
 обновление псевдонимов 308
 обновление ролей 308
 SAP Business Explorer 539
 SAP BusinessObjects Analysis, выпуск для Microsoft Office 69
 SAP BusinessObjects Dashboard Design 70
 SAP BusinessObjects Enterprise
 права 117
 трассировки 759
 SAP BusinessObjects Explorer 70, 520
 свойства приложения 520
 управление настройками 520

SAP BusinessObjects Mobile 74
 SAP BusinessObjects Web Intelligence 73
 SAP Crystal Reports 70
 SAP ERP 38
 SAP Passport 784
 SAP Solution Manager 38
 SLD 777
 SMD 779
 обзор 775
 SAPGENPSE 317
 SCRIPTDIR 18
 SDK
 Platform Search 622
 Веб-службы SDK 32
 см. Software Development Kit 31
 SDK платформы SAP
 BusinessObjects Business Intelligence 31
 Secure Network Communication (SNC), интеграция с настройками SNC 320
 Secure Socket Layer (SSL)
 настройка для 746, 748
 Secure Sockets Layer (SSL) 154, 171, 174, 175, 244
 и LDAP 244
 и балансировка нагрузки 152
 Server Intelligence Agent 20
 зависимости сервера Windows, добавление 433
 узлы 412, 413, 417, 420, 422
 воссоздание 417, 418, 419, 420, 421, 422, 428
 добавление 414, 415, 416, 428
 новый компьютер,
 добавление на 413
 переименование 423
 перемещение 424, 425, 426, 427, 430
 удаление 421, 428
 учетные данные
 пользователя, изменение для 434
 Server Intelligence Agent (SIA)
 рабочий процесс отключения 76
 serverconfig.sh 790, 791
 узлы
 воссоздание 419
 добавление 415
 переименование 423
 перемещение 426
 удаление 421
 setup.sh 793
 SI_AVAILABILITY_PROPERTY 554

Siebel Enterprise 38
 SiteMinder
 Windows AD 286
 настройка WAR-файла BOE 256
 настройка единого входа с использованием протокола LDAP 255, 286
 настройка подключаемого модуля LDAP 255
 ошибка 256
 устранение неполадок 256
 SMD 779
 SMD-агент 780
 SNC
 см. Безопасный сетевой обмен данными 310
 Software Development Kit (SDK)
 Consumer SDK платформы SAP BusinessObjects Business Intelligence 31
 Crystal Reports Viewers SDK 31
 Report Application Server SDK 31
 Report Engine SDK 31
 SDK платформы SAP BusinessObjects Business Intelligence 31
 Solution Manager 549
 учетная запись SAdmin 780
 SSL 171, 174, 175
 sslconfig.exe 176
 ключи 171, 172
 конфигурация серверов 171, 174, 175
 настройка серверов контейнера веб-приложений (WACS) 455, 457
 сертификаты 171, 172
 средство преобразования отчетов 177
 средство управления переводами 177
 толстые клиенты 176
 SSL, настройка для 758
 SSL. См. Secure Sockets Layer (SSL) 244
 sslc.cnf 171
 sslc.exe 171
 stopservers 792
 Strategy Builder, права 836
 Subversion 40
 syslog 396
 System Landscape Directory (SLD) 38
 запуски 778
 проверка регистрации 779
 регистрация 777
 файл connect.key 778

T

Tomcat
 JAAS 273
 Kerberos 270

U

Universe Designer
 см. "Средство создания юниверсов" 64
 UNIX
 syslog 396

V

Vintela 278
 особенности WebLogic 282
 Voyager 74
 см. SAP BusinessObjects Analysis 69

W

war-файл BOE 108, 109
 WDeploy 71
 Web Intelligence 515, 805
 права 832
 права доступа к HTML-запросам 515
 права приложения 515
 Сервер обработки 809
 Web Intelligence Desktop 63
 WebLogic
 Kerberos 270
 параметры Java 276
 файл конфигурации JAAS 273
 WebSphere
 JAAS 274
 Kerberos 272
 параметры Java 276
 Windows
 журнал событий 396
 зависимости сервера, добавление 433
 Windows AD
 Vintela 282
 активация Kerberos 460, 461
 аутентификация 262
 единый вход 279, 282
 конфигурация Kerberos сервер приложений 270
 подключаемый модуль безопасности 263
 сопоставление LDAP 260

Windows AD (*продолжение*)
 сопоставление групп 264
 сопоставление учетных записей 264
 учетная запись службы 279
 учетные записи и группы 264
 планирование обновлений 264

X

Xcelsius
 см. SAP BusinessObjects Dashboard Design 70

A

автоматический запуск серверов 380
 авторизации
 Content Administration Workbench 701
 для доступа к данным SAP 724
 для служб информационной платформы 296
 права на платформе BI 695
 применение 724
 агент Server Intelligence
 автоматический запуск серверов 380
 Агент Server Intelligence (SIA)
 рабочий процесс запуска 76
 Агент мониторинга 571
 Адаптивный сервер заданий 19, 42, 848, 909
 время ожидания сокета 687
 параметры командной строки 805
 Адаптивный сервер обработки 19, 42, 554
 администрирование
 входящие 108
 группы 107
 делегирование 142
 назначение прав 366
 пользователи 107
 права 142
 приложения 506
 серверы и группы серверов 393
 СМС 506
 стартовая панель BI 506
 активные данные 135
 активные доверительные отношения 151
 анализ 69
 анонимный единый вход 226
 архитектура 25, 551
 Поиск по платформе 619

архитектура, диаграмма 26
 атрибуты, маркеры входа 152
 аудит
 идентификатор сведений о
 событии 598, 609, 612, 613,
 614
 идентификатор типа события
 598, 609, 612, 613, 614
 настройка 585
 общие события 598
 параметры соединения базы
 данных 589
 показатели 585
 сведения о событии 598, 609,
 612, 613, 614
 сводка состояния 585
 свойства события 598, 612, 613,
 614
 события
 настройка 587
 события 591
 сохранение базы данных 589
 список 591
 события Web Intelligence 612
 события анализатора 613
 события консоли управления
 жизненным циклом 614
 события платформы 609
 Страница CMC 585
 типы событий
 Блокировка VMS 614
 Возврат VMS 614
 вход в систему 598
 выполнить 598
 выход за пределы области
 действия при переходе по
 иерархии 612
 выход из системы 598
 Добавление VMS 614
 доставка 598
 Извлечение VMS 614
 изменение аудита 609
 изменение прав 609
 изменить 598
 Изъятие VMS 614
 откат 614
 поиск 598
 получить 598
 пользовательский уровень
 доступа изменен 609
 представление 598
 приглашение 598
 Разблокирование VMS 614
 Сеанс MDAS 613
 Соединение с кубом MDAS
 613

аудит ((*продолжение*))
 типы событий ((*продолжение*))
 создать 598
 сохранить 598
 страница извлечена 612
 триггер 598
 удалить 598
 Экспорт VMS 614
 хранилище данных аудита
 диаграмма схемы 933
 таблицы схемы 934
 аудит лицензий 90, 375
 процедура 91, 376
 аутентификация 36
 enterprise 228
 LDAP 244, 245
 Windows AD 262
 Доверительная аутентификация
 232
 основная 224
 подключаемые модули
 безопасности 225
 Сервер контейнера
 веб-приложений (WACS) 460
 типы 96
 Аутентификация SAP 295
 параметры CMC 300

Б

база данных аудита 478
 база данных системы CMS 438, 439,
 484
 воссоздание 439, 440, 441
 восстановление 482, 483, 484
 выбор 438, 439
 изменение пароля 438
 копирование 441, 442, 443
 удаление 439, 440, 441
 база данных системы центрального
 сервера управления
 создание резервной копии 478
 База данных тенденций 551
 базы данных 27
 выбор для CMS 438, 439
 доступ с единым входом 228
 инициализация CMS 439, 440,
 441
 представления 35
 юниверс 34
 балансировка загрузки 152
 добавление CMS 387
 и распределенная безопасность
 152
 кластеризация 385

балансировка загрузки
 ((*продолжение*))
 Серверы контейнера
 веб-приложений (WACS) 469
 безопасности
 подключаемые модули 37
 безопасность 36, 335, 366, 696
 активные доверительные
 отношения 151
 аудит действий через Интернет
 155
 брандмауэры 155
 веб-браузер с веб-сервером 154
 веб-серверы 154
 запросы 130, 131
 защита от попыток выполнения
 входа злоумышленником 156
 защита среды 154
 импорт настроек 335
 на платформе BI 695
 настройка прав 366
 обработка расширений 157
 объекты юниверса 828
 ограничения 157
 ограничения для пароля 156
 ограничения для пользователя
 157
 ограничения на вход 156
 ограничения учетной записи
 гостя 157
 отслеживание сеансов 153
 папки верхнего уровня 129
 подключаемые модули 37, 225
 применение 339
 распределенный 152
 управление 127
 управление настройками 339
 уровень папок 695
 шаблоны по умолчанию 696
 безопасность данных
 FIPS-совместимый режим 158
 двухключевая криптография 158
 обзор 158
 обратная совместимость 158
 режим обработки данных по
 умолчанию 158
 безопасность низкого уровня,
 обработка расширений 157
 безопасность объекта юниверса 828
 Безопасный сетевой обмен данными
 библиотека шифрования SAP
 310
 группы серверов 319
 клиент относительно сервера
 310
 конфигурация SAP 312

Безопасный сетевой обмен данными
 ((продолжение))
 конфигурация серверов 317
 многопроходные публикации 320
 настройки CMC 318
 рабочий процесс 315
 серверы BusinessObjects
 Enterprise 310
 создание PSE 316
 установка среды 315
 брандмауэры 155
 конфигурация
 Интеграция SAP 201
 настройка 190
 для интеграции с Oracle
 E-Business 205
 интеграция с JD Edwards
 EnterpriseOne 203
 интеграция с PeopleSoft
 Enterprise 206
 интеграция с Siebel 208
 обмен данными между
 серверами, и 179
 отладка 194, 195
 принудительная регистрация
 серверов по имени 411
 Сервер контейнера
 веб-приложений (WACS) 470
 сценарии настройки 195

В

веб-клиенты 62
 веб-приложения BEx 539
 веб-серверы
 защита 154
 веб-службы
 добавление на сервер Web
 Application Container Server
 453
 конфигурация для обратных
 прокси-серверов 216, 217
 кэширование файлов 679
 настраиваемое развертывание
 679, 680
 переменная сеанса 679
 удаление с сервера Web
 Application Container Server
 454
 Веб-службы 32
 Средство запросов веб-служб 33
 верхний уровень
 папки, права 129
 виджеты
 права 838
 управление настройками 519

Виджеты BI
 см. виджеты для платформы SAP
 BusinessObjects Business
 Intelligence 67
 виджеты для платформы SAP
 BusinessObjects Business
 Intelligence 67
 виртуальные показатели 554
 включение
 серверы 381, 382
 владельцы учетных записей
 назначение прав 128
 назначение расширенных прав
 129
 права просмотра для 127
 права, на папки верхнего уровня
 129
 проверка прав 130, 131
 восстановление 484
 установки системы по
 умолчанию 403, 475
 восстановление SAP
 BusinessObjects Enterprise
 база данных системы CMS 483
 восстановление платформы BI
 настройки сервера 485
 восстановление платформы SAP
 BusinessObjects Business
 Intelligence 477
 база данных системы CMS 482
 настройки сервера 485, 486, 487
 файловая система 482, 487, 488
 время нарушения 552
 время ожидания сокета 687
 время отклика 549
 вход в систему
 защита от попыток выполнения
 злоумышленником 156
 настройка 536
 рабочий процесс 75
 стартовая панель BI 109
 входящие
 контролирование доступа к 108
 Вызов удаленного метода (RMI) 551
 вызов удаленной процедуры 433
 выполнение аудита
 архитектура 579
 веб-действия 155
 информационный поток 579
 выполняется публикация
 в нескольких системах
 платформы BI 704
 в фоновом режиме 709
 нескольких отчетов с
 использованием ролей 706

выполняется публикация
 ((продолжение))
 определения ролей для, в BW
 701
 отчеты в пакетном режиме 710
 отчеты в роли или системе 706
 планирование в фоновом
 режиме 709
 установка 700

Г

глобальные показатели системы 396
 График тенденций 549
 группы 306
 добавление подгрупп 102
 добавление пользователей к 104
 изменение 101
 назначение прав 128
 параметры стартовой панели BI
 110
 по умолчанию 95
 права 822
 на папки высшего уровня 129
 нарушение наследования 141
 наследование 120
 переопределение прав 122
 предоставление доступа к 107
 проверка прав 130, 131
 просмотр
 права для 127
 члены 102
 создание 101
 сопоставление 329, 347, 354, 360
 специалисты по шифрованию
 164
 удаление 103
 указание принадлежности к
 группе 103
 управление 95
 группы серверов
 доступ к 393
 подгруппы 391, 392
 подгруппы серверов 390, 392
 создание 391
 узлы 369

Д

данные
 активно 135
 постоянный 40
 сохранено 135
 двунаправленное тиражирование
 654
 действительные права 126

делегированное администрирование 142
 демоны, обработка сигналов 799
 дерево навигации
 серверы 369
 диаграмма архитектуры 26
 динамически подключаемые
 библиотеки, обработка
 расширений 157
 дискуссии
 управление настройками 512
 Диспетчер Business View 64
 добавление 385
 CMS 387
 подгруппы 102
 пользователей к группе 104
 серверы 382
 члены кластера 385
 доверие, активные доверительные
 отношения 151
 доверительная аутентификация 538
 пример конфигурации 240
 свойства 236
 Доверительная аутентификация 232
 SAML 234
 принципал пользователя 243
 документы Web Intelligence
 права 821
 дополнительный сетевой интерфейс 408
 доставка уведомления 552
 доступ 117
 входящие 108
 группы 107
 группы серверов 393
 панель HTML-запросов 515
 пользователи 107
 приложения 506
 серверы 393
 СМС 506
 соединения с юниверсами 545
 стартовая панель BI 506

Е

единая регистрация 36, 226
 анонимный 226
 к базе данных 228
 на платформу BI 226
 сквозной 228
 единый вход 286, 295
 Kerberos 278, 468
 аутентификация
 Windows AD 265
 импорт ролей 306

единый вход ((*продолжение*))
 настройка
 LDAP 255
 SiteMinder 255, 286
 Windows AD 265
 устранение неполадок 256
 учетная запись службы 279
 единый вход, настройка для JD
 Edwards 745
 единый вход, настройка для Oracle
 EBS 367
 единый вход, настройка для
 PeopleSoft 747
 единый вход, настройка для SAP
 Netweaver 327
 единый вход, настройка для Siebel
 757

Ж

журнал событий 396, 433
 журнал трассировки
 уровни 507, 759

З

зависимости сервера
 вызов удаленной процедуры 433
 добавление 433
 Журнал событий 433
 Задания тиражирования
 изменение 669
 параметры конфигурации 666
 планирование 668, 669
 просмотр 666
 создание 666
 заполнители 921
 инструментальные средства 782
 заполнители сервера 921
 заполнители узлов 921
 запросы
 безопасность 130, 131
 запросы отношений
 для уровней доступа 139
 запуск серверов 791
 защита данных
 ключи кластера 161
 ключи шифрования 161
 криптографические ключи 161
 криптография 161
 зеленый флажок, для систем по
 умолчанию 704
 Зонд 549

И

индексирование 619
 инициализация базы данных
 системы CMS 439, 440, 441
 инструмент Content Administration
 Workbench
 опубликование отчетов 706
 применение авторизаций 701
 инструмент командной строки BIAR
 493
 инструмент командной строки
 механизма BIAR 494, 497, 503
 Инструмент определения кластера
 713, 718
 инструментальные средства 783
 веб-ярус 783
 заполнители 782
 не Java-серверы 781
 проверка 783
 регистрация 783
 инструменты мониторинга
 обзор 781
 интеграция 643
 SAP 38
 SNC 320
 веб-службы 679, 680
 двунаправленное тиражирование
 654, 655
 задания тиражирования 666
 изменение 669
 планирование 668, 669
 создание 666
 импортирование и повышение
 уровня растажированного
 содержимого 684, 685, 686
 локальный запуск экземпляров
 681, 683
 обновлять из адресата 654, 655
 обновлять из источника 654, 655
 однонаправленное
 тиражирование 654, 655
 очистка объекта 671, 672
 повышение производительности
 690
 практический опыт 687
 преимущества 643
 просмотр журналов 670
 режимы репликации 654, 655
 списки тиражирования 659
 папки 659, 660
 создание 659, 660
 управление 662
 сторонние пользователи и
 группы, тиражирование 656
 термины 644

интеграция *((продолжение))*
 тиражирование больших
 объектов 687
 удаленное планирование 681,
 683
 удаленные соединения 663
 изменение 665
 создание 663
 узлы назначения для отчетов
 684, 687
 управление безопасностью 648,
 649, 650, 652, 653
 уровни доступа 139
 устранение конфликтов 673,
 674, 675
 устранение неполадок 691
 Интеграция времени поиска с NWES
 635
 интеграция с JD Edwards
 EnterpriseOne
 настройка брандмауэра 203
 интеграция с Oracle E-Business Suite
 настройка брандмауэра 205
 интеграция с PeopleSoft Enterprise
 настройка брандмауэра 206
 интеграция с Siebel
 меню "Crystal Reports", создание
 753
 настройка брандмауэров 208
 повторная компиляция
 приложения Siebel 753
 проект интеграции 752
 интеллектуальный ярус 399
 Интернационализация 35
 Информационная панель 549
 исходные сайты
 уровни доступа 139

К

карточки 152
 для распределенной
 безопасности 152
 маркеры входа 152
 каталог установки, расположение
 412
 категории 110
 права 818
 Категории данных мониторинга 571
 категории служб 52, 369
 кластеры 385, 387
 добавление CMS 387
 изменение имен 389
 просмотр подробностей 396
 узлы 385

клиенты
 Data Federator. См. "Средство
 администрирования
 объединения данных" 66
 SAP BusinessObjects Analysis,
 выпуск для Microsoft Office 69
 SAP BusinessObjects Dashboard
 Design 70
 SAP Crystal Reports 70
 Web Intelligence Desktop 63
 веб 62
 виджеты для платформы SAP
 BusinessObjects Business
 Intelligence 67
 Дизайнер информации. См.
 "Средство дизайна
 информации" 65
 Диспетчер Business View 64
 настольные 62
 Средство администрирования
 объединения данных 66
 Средство дизайна информации
 65
 Средство запросов веб-служб 65
 Средство преобразования
 отчетов 64
 Средство создания юниверсов
 64
 Средство управления
 переводами 66
 клиенты на основе браузеров 62
 клиенты рабочих станций 62
 клиенты, на базе браузера 71
 Analysis, выпуск OLAP 74
 Central Management Console
 (CMC) 21, 71
 SAP BusinessObjects Mobile 74
 SAP BusinessObjects Web
 Intelligence 73
 рабочие пространства BI 72
 стартовая панель BI 72
 Клиенты, на базе браузера
 Средства просмотра отчетов 73
 клиенты, настольные ПК
 Central Configuration Manager
 (CCM) 21, 68
 Repository Diagnostic Tool 22, 69
 Средство управления
 обновлением 22, 68
 клонирование
 серверы 383, 385
 Серверы контейнера
 веб-приложений (WACS) 452
 ключи кластера 161
 обзор 162
 сброс в UNIX 163

ключи кластера *((продолжение))*
 сброс в Windows 162
 файл dbinfo 162
 ключи реестра 256
 количество минут, маркеры входа
 152
 количество попыток входа, маркеры
 входа 152
 компоненты 713, 718
 Инструмент определения
 кластера 713, 718
 консоль управления жизненным
 циклом
 инструмент командной строки
 механизма BIAR 494, 503
 Консоль управления жизненным
 циклом
 инструмент командной строки
 BIAR 493
 Конструктор агента 571
 контекстуальная зависимость 755
 настройка 755, 756
 конфигурация 566
 конфигурация Kerberos 270
 конфигурирование
 Secure Sockets Layer 758
 ярус приложений 399
 конфликты объектов
 двунаправленное тиражирование
 673, 675
 однонаправленное
 тиражирование 673, 674
 копирование
 уровни доступа 136
 криптографические ключи 161
 обозначение как рассекреченных
 169
 CMC 165
 список объектов 168
 статус 166
 криптографический ключ
 отзыв 170
 создать новый 168
 Кэш-сервер 803, 804
 Кэш-сервер Crystal Reports 554

Л

лицензионные ключи
 и миграция базы данных CMS
 442
 лицензионный ключ 90, 375
 добавление 90, 374
 измерение показателей
 использования 90, 375
 обзор 89, 374

лицензионный ключ ((*продолжение*))
приобретение 89, 374
просмотр 89, 374
Локализация 35

М

маркеры входа 152
аутентификация 224
отслеживание сеансов 153
распределенная безопасность 152
Мастер импорта
см. "Средство управления обновлением" 22, 68
многосетевые компьютеры 406, 407
Сервер контейнера веб-приложений (WACS) 471
Многоязыковая поддержка 634
Мониторинг 549
Мост безопасности PeopleSoft EPM файл ответов 336

Н

Наблюдение 549
наследование 119
группа 120
нарушение 141
ограничение 124
папка 121
переопределение прав 122
наследование папок 121
переопределение прав 122
настройка
Apache 2.2 212
ISA 2006 214
WebSEAL 6.0 213
база данных CMS 438, 439
база данных системы CMS 439, 440, 441
брандмауэры 190
Доверительная аутентификация 233
интеллектуальный ярус 399
кластеры 385
кластеры CMS 389
несколько серверов 401
обрабатывающий ярус 399
обратные прокси-серверы 211, 212
узлы 385
шаблоны настройки 402
Настройка OpenSearch 623
настройка аудита, см. аудит 585

настройка входа в систему
OpenDocument 536
стартовая панель BI 536
настройка обратного прокси 624
настройки
дискуссии 512
Оповещение 516
права доступа к папкам верхнего уровня 129
стартовая панель BI 515
настройки сервера
csm.sh
резервное копирование параметров сервера 481
восстановление 485, 486, 487
создание резервной копии 479, 480, 481
неотображаемые роли 332, 365
непрерывная трассировка 784
номера портов
изменение 409, 410
конфликты 473, 474
Сервер контейнера веб-приложений (WACS) 473

О

О показателях сервера
общие показатели
IP-адрес хоста 893
PID 893
Версия 893
Занятые потоки на сервере 893
Зарегистрированное имя 893
Имя компьютера 893
Имя хоста 893
Использованное дисковое пространство (Гбайт) 893
Каталог протоколирования 893
Местное время 893
ОЗУ (Мбайт) 893
Операционная система 893
Порт запросов 893
Размер диска (Гбайт) 893
Сервер имен 893
Тип ЦПУ 893
ЦПУ 893
Показатели аудита
Текущее число проверяемых событий, ожидающих своей очереди 893
Обзор 619
область действия прав 124

Облегченный протокол доступа к каталогам. См. LDAP 244
обмен данными 224
между браузером и сервером веб-приложений 224
между серверами платформы BI 179
обновления 41
обрабатывающий ярус 399
обработка расширений 157
регистрация 510
совместное использование 511
обработка сигналов 799
обратные прокси-серверы
Live Office 221
Tomcat 216
URL-адрес средства просмотра 221
веб-службы 216, 217
использование с серверами контейнера веб-приложений (WACS) 470
конфигурация Apache 2.2 212
конфигурация ISA 2006 214
конфигурация WebSEAL 6.0 213
настройка на платформе BI 211, 212
поддерживаемые 210
развертывание на платформе BI 210
развертывание с помощью Сервера контейнера веб-приложений (WACS) 470
специальная конфигурация 216
файлы cookies сеансов 218
общий доступ к экземпляру 681, 683
объекты
права 695, 815
настройка 128
просмотр 127
объекты отчета
права 820
права на создание/изменение 394
объекты программы
аутентификация 509
включение, отключение 509, 510
ограничение
область действия прав 124
ограничения 157
вход в систему 156
пароль 156
пользователь 157
учетная запись гостя 157
однаправленное тиражирование 654

Оповещение 516
 права 839
 свойства места назначения 517
 свойства по умолчанию 518
 управление 516
 управление настройками 516
 определенные права
 рабочие пространства BI 824, 832
 основная аутентификация 224
 основной сетевой интерфейс 408
 отключение
 псевдонимы 115
 серверы 381, 382
 учетные записи гостя 104
 отображаемые пользователи,
 управление псевдонимами 112
 отображение ролей 306, 329, 347, 354, 360
 отслеживание
 сквозной 784
 отслеживание, сеансы 153
 отчеты
 выполняется публикация 706
 в пакетном режиме 710
 обновление источников данных 709
 удаление 710

П

Пакет SDK для SAP BusinessObjects 157
 панель HTML-запросов, права доступа 515
 папки
 права 818
 права объекта
 наследование 121
 параметры командной строки 797, 798, 809, 813
 CMS 800
 SSL 171
 Адаптивный сервер заданий 805
 все серверы 798
 Кэш-сервер 803, 804
 Сервер аналитики
 информационных панелей 813
 Сервер информационных панелей 813
 Сервер обработки 803, 804
 Сервер приложений отчетов 807
 Сервер событий 813
 Серверы репозитория входящих и исходящих файлов 810

параметры памяти
 изменение на Сервере
 контейнера веб-приложений (WACS) 474
 параметры профиля 320
 параметры режима обновления, для интеграции 654, 655
 параметры скриптов, узлы
 воссоздание 428
 добавление 428
 перемещение 430
 удаление 428
 пароли 438, 439
 изменение 106
 для базы данных CMS 438
 параметры 106, 231
 ограничения 156
 перевод доверия 152
 перезагрузка серверов 378, 379, 380
 переименование, уровни доступа 137
 переменные
 каталог скриптов 18
 каталог установки 18, 412
 операционная система UNIX 18
 скрипты управления узлами 412
 переменные сеанса 153
 аутентификация 224
 Персональная среда безопасности см. PSE 310
 планирование аварийного восстановления 149
 Планирование ресурсов предприятия (ERP) 38
 платформа BI
 импорт ролей 306
 обмен данными между серверами 179
 отображение ролей 354
 папки верхнего уровня, права 129
 планирование аварийного восстановления 149
 процесс основной аутентификации 224
 развертывание с использованием обратных прокси-серверов 210
 рекомендации по безопасности 150
 Сервер контейнера веб-приложений (WACS) 445
 платформа SAP BusinessObjects Business Intelligence
 диаграмма архитектуры 26

платформа SAP BusinessObjects Business Intelligence
 ((продолжение))
 резервное копирование и восстановление 478
 подгруппы, добавление 102
 поддержка кластеров 554, 621
 поддержка отчета 709
 подключаемые модули безопасности 225, 295
 Аутентификация LDAP 245
 аутентификация Windows AD 263
 подключаемые модули безопасности третьих производителей 225
 подключаемые модули, безопасность 225
 Подключение к Open SQL 713
 поиск 512, 619
 темы дискуссии 512
 Поиск из NetWeaver Enterprise Search 637
 Поиск по платформе 520, 625
 показатели
 просмотр 395
 показатели сервера 893
 Показатели Crystal Reports Server
 Имя Dll объекта 912
 Макс. число дочерних процессов 912
 Максимальное время обработки (мс) 912
 Минимальное время обработки (мс) 912
 Обслужено запросов 912
 Объем кэш-памяти 912
 Открытые в данный момент задания отчетов 912
 Открытые в данный момент соединения 912
 Открытые задания 912
 Передано данных (КБ) 912
 Среднее время обработки (мс) 912
 Тип объекта 912
 Удачных обращений в кэш (%) 912
 Частота сбоев запросов 912
 Число запросов в очереди 912
 Число запросов, выполненных с ошибкой 912
 Число открытых соединений 912
 Показатели адаптивного сервера заданий
 PID 909
 Временный каталог 909
 дочерние элементы 909
 Завершение работы 909
 Инициализация 909
 Максимально разрешенное число заданий 909

показатели сервера ((продолжение))	показатели сервера ((продолжение))	показатели сервера ((продолжение))
Показатели адаптивного сервера заданий ((продолжение))	Показатели адаптивного сервера обработки ((продолжение))	Показатели сервера Dashboard Design ((продолжение))
Максимальное разрешенное количество параллельных заданий 909	Общее число записей, переданных из источников данных 903	Размер кэша (кбайт) 917
Параллельные задания 909	Общее число записей, созданных выполнением запроса 903	Среднее время обработки (мс) 917
Пиковые задания 909	Потоки на транспортном уровне 903	Тип объекта 917
Полученные запросы заданий 909	Процент использования ЦПУ (последние 15 минут) 903	Удачных обращений в кэш (%) 917
СвязьСбой 909	Процент использования ЦПУ (последние 5 минут) 903	Частота сбоев запросов 917
Служба планирования 909	Процент остановленной системы в течение GC (последние 15 минут) 903	Число запросов в очереди 917
Службы планирования 909	Процент остановленной системы в течение GC (последние 5 минут) 903	Число запросов, выполненных с ошибкой 917
Создания заданий, завершившиеся сбоем 909	Размер пула потоков транспортного уровня 903	Число обслуживаемых запросов 917
Установка по умолчанию адресатов FTP допустима 909	Сведения о версии JVM 903	Число открытых соединений 917
Установка по умолчанию адресатов папки "Входящие" допустима 909	Сведения об отладке JVM 903	Показатели сервера Web Intelligence
Установка по умолчанию адресатов файловой системы допустима 909	Свободная память (Мбайт) 903	Верхний порог использования памяти
Установка по умолчанию адресатов эл. почты допустима 909	Служба объединения данных доступна 903	Время простоя (сек) 915
Показатели адаптивного сервера обработки	DSLServiceMetrics.activeConnectionCount 903	Использование ЦП (%) 915
DSLServiceMetrics.activeConnectionCount 903	DSLServiceMetrics.activeOLAPConnectionCount 903	Максимальное количество документов в кэше 915
DSLServiceMetrics.activeSessionCount 903	DSLServiceMetrics.queryCount 903	Максимальный порог использования памяти 915
Аудит полученных событий 903	Всего памяти (Мбайт) 903	Общее время работы ЦП (сек) 915
Выполняемая индексация 903	Доступная служба 903	Общее число вызовов клиента 915
Доступные процессоры 903	Количество конфликтов при блокировках JVM 903	Общее число задач 915
Количество ошибок страниц в течение (последние 15 минут) 903	Количество ошибок страниц в течение (последние 5 минут) 903	Общее число сеансов 915
Количество ошибок страниц в течение (последние 5 минут) 903	Количество полных GC 903	Размер виртуальной памяти (Мб) 915
Количество полных GC 903	Максимальный объем памяти (Мбайт) 903	Размер кэша (КБ) 915
Максимальный объем памяти (Мбайт) 903	Метка времени последнего обновления индекса 903	Текущее число активных сеансов 915
Метка времени последнего обновления индекса 903	Метка времени создания последнего хранилища содержимого 903	Текущее число вызовов клиента 915
Общее число байтов объема диска, используемого выполнением запроса 903	Общее число байтов памяти, используемого выполнением запроса 903	Текущее число задач 915
Общее число байтов памяти, используемого кэшем метаданных 903	Общее число байтов, переданных из источников данных 903	Текущее число сеансов 915
Общее число байтов, созданных выполнением запроса 903	Общее число байтов, созданных выполнением запроса 903	Уровень максимального использования кэша 915
		Число документов 915
		Число операций подкачки документов 915
		Число подкачанных документов 915
		Число пользователей 915
		Число таймаутов для сеанса 915
		Показатели сервера контейнера веб-приложений
		Ошибки запуска одного или нескольких соединителей WACS 908
		Список выполняющихся средств связи WACS 908
		Показатели сервера репозитория файлов
		Активные файлы 902
		Активных соединений 902
		Доступное дисковое пространство в корневом каталоге (%) 902
		Доступное дисковое пространство в корневом каталоге (Гб) 902
		Записано данных (Мб) 902

показатели сервера ((<i>продолжение</i>))	показатели сервера ((<i>продолжение</i>))	последовательности операций
Показатели сервера репозитория файлов ((<i>продолжение</i>))	показатели центральной службы управления ((<i>продолжение</i>))	назначение расширенных прав 129
Общее дисковое пространство в корневом каталоге (ГБ) 902	Параллельно использующиеся соединения с системной БД 896	настройка прав доступа к папкам верхнего уровня 129
Передано данных (Мб) 902	Подключение к базе данных аудита установлено 896	права просмотра 127
Свободное дисковое пространство в корневом каталоге (ГБ) 902	Последнее использование базы данных аудита 896	списки контроля доступа, назначение владельцев учетных записей 128
Список активных файлов 902	Среднее время ответа на запросы момента запуска (мсек) 896	постоянные данные 40
Показатели сервера событий	Среднее время ответа при фиксации момента запуска (мсек) 896	права 117, 366, 815
Отслеживаемые файлы 901	Существующие учетные записи именованных пользователей 896	Crystal Reports 820
Список отслеживаемых файлов 901	Существующие учетные записи пользователей с лицензиями на параллельный доступ 896	Explorer 840
показатели сервера соединений	Установленные соединения с системной БД 896	Mobile 842
Источники данных 901	Число входов в систему с момента запуска 896	Web Intelligence 832
Показатели центральной службы управления	Число запросов с момента запуска 896	администрирование 142, 146
Аудитор CMS 896	Число объектов в системной БД CMS 896	виджеты 838
Версия продукта 896	Число объектов в системном кэше CMS 896	входящие 108
Версия ресурса 896	Число сеансов пользователей с лицензиями на параллельный доступ 896	группы 107, 822
Выполняющиеся задания 896	Число сеансов, установленных всеми пользователями 896	группы серверов 393
Дата сборки 896	Число сеансов, установленных зарегистрированными пользователями 896	действительные права 126
Длительность последнего цикла опроса потока аудита (секунды) 896	Число сеансов, установленных серверами 896	документы Web Intelligence 821
Завершенные задания 896	Число фиксаций с момента запуска 896	независимые от типа 125
Задания, завершившиеся сбоем 896	Показатели сервера просмотра 395	Запрос безопасности 130, 131
Имя источника данных 896	показатели системы, просмотр 396	категории 818
Имя подключения к базе данных аудита 896	Сервер контейнера веб-приложений (WACS) 472	значение владельцам учетных записей 128
Имя подключения к системной базе данных 896	пользователь 552	наследование 119
Имя пользователя базы данных аудита 896	пользователи	группа 120
Имя пользователя системной базы данных 896	назначение прав 128	нарушение 141
Имя сервера системной базы данных 896	назначение расширенных прав 129	папка 121
Использование потока аудита 896	Максимальное число пользовательских сеансов с момента запуска 896	область действия прав 124
Кластеризованные серверы CMS 896	Незавершенные запросы в системной БД 896	общее 815
Лицензии для именованных пользователей 896	Номер построения 896	Оповещение 839
Лицензии на параллельный доступ пользователей 896	Ожидающие задания 896	папки 818
Максимальное время обработки запроса с момента запуска (мсек) 896	Отложенные задания 896	папки верхнего уровня 129
Максимальное время обработки фиксации с момента запуска (мсек) 896		переопределение прав 122
Максимальное число пользовательских сеансов с момента запуска 896		пользователи 107, 822
Незавершенные запросы в системной БД 896		Построитель стратегий 836
Номер построения 896		права
Ожидающие задания 896		тиражирование 648, 649, 650, 652, 653
Отложенные задания 896		права администрирования 366
		права владельца 146
		права на публикацию 367
		приложения 506
		примечания 819
		просмотр 127
		просмотр и просмотр по запросу 135
		рабочие пространства BI 824, 832
		расширенные права 118, 129
		Сервер приложений отчетов 394
		серверы 393
		CMS 506, 831

права ((*продолжение*))
 соединения с юниверсами 829
 средство дизайна информации 837
 средство создания юниверсов 837
 стартовая панель BI 506, 831
 управление 127
 управление безопасностью 648, 649, 650, 652, 653
 уровни доступа 118, 823
 задачи 133
 запросы отношений 139
 изменение включенных прав 138
 тиражированный 139
 управление на уровне нескольких сайтов 139
 юниверсы (.unv) 825
 юниверсы (.unx) 826
 права владельца 146
 права для конкретных типов объектов
 виджеты 838
 права учетной записи службы 268
 предоставление 269
 права, зависящие от типа 125
 Crystal Reports 820
 Web Intelligence 832
 группы 822
 документы Web Intelligence 821
 категории 818
 Оповещение 839
 папки 818
 пользователи 822
 Построитель стратегий 836
 примечания 819
 CMC 831
 соединения с юниверсами 829
 средство дизайна информации 837
 средство создания юниверсов 837
 стартовая панель BI 831
 уровни доступа 823
 юниверсы (.unv) 825
 юниверсы (.unx) 826
 Предложения 634
 представления 35
 преобразование сетевых адресов
 настройка, файл хостов сервера 192
 приложения 505
 Поиск по платформе 520, 625
 свойства 520, 625
 примечания, права 819

производительность 549
 балансировка нагрузки 152
 кластеры 385
 просмотр
 подробности кластера CMS 396
 Показатели Сервера контейнера веб-приложений (WACS) 472
 показатели системы 396
 права для владельцев учетных записей 127
 текущие показатели 395
 Просмотр полномочий 127
 просмотр текущей учетной записи 90, 375
 протокол RMI 566
 Процесс PSANALYTIC 751
 Процесс PSAPPSRV 751
 псевдонимы
 назначение пользователям 114
 отключение 115
 создание 113
 для новых пользователей 113
 для существующих пользователей 113
 удаление 115
 управление 112
 псевдонимы пользователей 114
 назначение 114
 отключение 115
 создание 113
 для новых пользователей 113
 для существующих пользователей 113
 удаление 115
 Публикация
 рекомендации по администрированию 397
 публикация, назначение прав на 367

Р

рабочие потоки 75
 рабочие пространства BI 72
 Рабочие пространства BI, права 824, 832
 рабочие процессы
 вход пользователя в систему 75
 выполнение отчета Crystal 78
 запланированный документ Web Intelligence 79, 80
 запланированный объект 81
 Запуск узла SIA 76
 Отключение SIA 76
 отправка экземпляра по назначению 81
 планирование отчета Crystal 77

рабочие процессы ((*продолжение*))
 просмотр кэшированного отчета Crystal 83
 просмотр некешированного отчета Crystal 82
 Просмотр отчета Crystal по требованию 85
 просмотр отчета Crystal с помощью Web Java 86
 просмотр отчета Web Intelligence по запросу 85
 просмотр рабочего пространства Analysis 84
 распространение
 компоненты BW Publisher 698
 Расширения Java Management (JMX) 551
 расширения, обработка 157
 расширенные права 118, 126, 129
 регистрация 396, 783
 веб-действия 155
 работа сервера 396
 Редактор параметров безопасности
 транспорт 713, 717
 режим выполнения 335
 режим настройки 335
 резервное копирование SAP BusinessObjects Enterprise
 настройки сервера 481
 резервное копирование платформы BI
 настройки сервера 479, 480
 резервное копирование платформы SAP BusinessObjects Business Intelligence 477, 478
 настройки сервера 481
 рекомендации по увеличению производительности 750
 Репозиторий входящих файлов 19, 42, 554, 848
 Репозиторий исходящих файлов 19, 42, 554, 848
 роли 329, 347, 354, 360, 701
 импорт 306
 назначение 306, 329, 332, 347, 354, 360
 назначение прав 366
 неотображаемые 332, 365
 переназначение 356
 преобразование 350
 создание для администрирования 701

С

- сайты
 - управление правами 648, 649, 650, 652, 653
 - уровни доступа 139
- сайты-адресаты
 - уровни доступа 139
- свойства серверов 845
- Связь 574
- сеансы 153
 - отслеживание 153
- сервер Java-приложений, Kerberos 270
- Сервер адаптивной обработки 848
- Сервер аналитики PeopleSoft 751
- Сервер аналитики информационных панелей 554, 848
 - параметры командной строки 813
- Сервер информационных панелей 554, 848
 - параметры командной строки 813
- Сервер контейнера веб-приложений (WACS) 30, 554, 848
 - AD Kerberos 464
 - HTTPS 455, 457, 470
 - SSL 455, 457
 - балансировка нагрузки 469
 - брандмауэры 470
 - восстановление установок
 - системы по умолчанию 475
 - добавление 449
 - добавление веб-служб к 453
 - изменение параметров памяти 474
 - использование с другими веб-серверами 469
 - использование с прокси-серверами 469, 470
 - клонирование 452
 - на многосетевых компьютерах 471
 - обзор 445
 - общие задания 446
 - ошибки сервера 472
 - показатели 908
 - показатели системы 472
 - свойства 476
 - служба СМС 445
 - соединители 445
 - создание серверов 451
 - удаление 449, 453
 - удаление веб-служб с 454
 - установка 450
 - устранение конфликтов портов 473, 474
- Сервер контейнера веб-приложений (WACS) ((*продолжение*))
 - устранение неполадок 472
 - файлы JAAS 463
 - файлы конфигурации Kerberos 462
- Сервер кэширования данных Xcelsius 554
- сервер мониторинга 554
- Сервер на платформе Java 551
- Сервер обработки Web Intelligence 809
 - параметры командной строки 803, 804
- Сервер обработки Crystal Reports 554, 803
 - параметры командной строки 803
- Сервер обработки Dashboard Design 804
 - параметры командной строки 804
- Сервер обработки Web Intelligence 19, 42, 554
- Сервер обработки в Crystal Reports 2010 554
- Сервер обработки данных Xcelsius 554
- Сервер подключений 554
- Сервер подключений 32 554
- Сервер приложений отчетов
 - необходимые права объекта 394
 - параметры командной строки 807
- Сервер репозитория РМ 554
- Сервер событий 554, 848
 - параметры командной строки 813
- серверы 28
 - URL агента мониторинга 848
 - Автоматическое повторное подключение к системной базе данных 848
 - адрес IPv6 406
 - варианты идентификации узлов 404
 - включение 381, 382
 - Включить HTTP через прокси 848
 - Включить HTTPS 848
 - Включить аутентификацию клиента 848
 - Временный каталог 848
 - Время ожидания очистки системы визуализации (сек) 848
 - Время ожидания подкачки системы визуализации (сек) 848
 - время простоя соединения 848
 - выполнение входа 396
- серверы ((*продолжение*))
 - группирование 390
 - действия, регистрация 396
 - дерево навигации 369
 - добавление 382
 - доступ к 393
 - заполнители 384
 - Запросы соединений с системной базой данных 848
 - запуск 378, 379, 380
 - автоматически 378, 379
 - изменение 377
 - состояние 377
 - статус 377
 - изменение принадлежности к группе 392, 393
 - имя хоста 406
 - Имя хоста прокси 848
 - Интервал опроса событий 848
 - Интервал очистки 848
 - Истечение срока действия единого входа 848
 - Каталог хранилища файлов 848
 - клонирование 383, 385
 - коммуникация 179
 - конфигурирование 399
 - Максимальное время простоя 848
 - Максимальное число запросов дочерних объектов 848
 - Максимальное число параллельных заданий 848
 - Максимальное число параллельных запросов 848
 - Максимальное число повторных попыток доступа к файлам 848
 - Максимальное число попыток 848
 - Максимальный размер заголовка HTTP 848
 - Местоположение файла bscLogin.conf 848
 - Местоположение файла Krb5.ini 848
 - Местоположение файла списка надежных сертификатов 848
 - Местоположение файла хранилища сертификатов 848
 - настройка IP-адреса 406
 - настройка серверов на использование учетной записи службы 269
 - настройка учетной записи службы 266

серверы ((продолжение))

настройки производительности 400
 Начальный номер порта 848
 обработка сигналов UNIX 799
 общие свойства сервера
 Автоматический запуск сервера при запуске SIA 845
 Восстановить системные значения по умолчанию 845
 Задать шаблон конфигурации 845
 Идентификаторы хостов 845
 Использовать шаблон конфигурации 845
 Назначать автоматически 845
 Порт запросов 845
 Уровень журнала 845
 остановка 378, 379, 380
 отключение 381, 382
 Параметры сервера Desktop Intelligence
 Верхний порог памяти 887
 Максимальный порог памяти 887
 Нижний порог памяти 887
 Пароль доступа к секретным ключам 848
 Пароль доступа к секретным ключам списка надежных сертификатов 848
 перезагрузка 378, 379, 380
 Порт 848
 Порт HTTP 848
 Порт HTTPS 848
 Порт прокси 848
 Порт сервера имен 848
 предоставление прав учетной записи службы 268, 269
 Привязка к имени хоста или IP-адресу 848
 Привязка ко всем IP-адресам 848
 просмотр статуса сервера 377
 Протокол 848
 Псевдоним сертификата 848
 регистрация по имени 411
 свойства 400
 Свойства основных служб
 URL агента мониторинга 848
 Автоматическое повторное подключение к системной базе данных 848
 Включить HTTP через прокси 848

серверы ((продолжение))

Свойства основных служб ((продолжение))
 Включить HTTPS 848
 Включить аутентификацию клиента 848
 Временный каталог 848
 Время ожидания очистки системы визуализации (сек) 848
 Время ожидания подкачки системы визуализации (сек) 848
 время простоя соединения 848
 Запросы соединений с системной базой данных 848
 Имя хоста прокси 848
 Интервал опроса событий 848
 Интервал очистки 848
 Истечение срока действия единого входа 848
 Каталог хранилища файлов 848
 Максимальное время простоя 848
 Максимальное число запросов дочерних объектов 848
 Максимальное число параллельных заданий 848
 Максимальное число параллельных запросов 848
 Максимальное число повторных попыток доступа к файлам 848
 Максимальное число попыток 848
 Максимальный размер заголовка HTTP 848
 Местоположение файла bscLogin.conf 848
 Местоположение файла Krb5.ini 848
 Местоположение файла списка надежных сертификатов 848
 Местоположение файла хранилища сертификатов 848
 Начальный номер порта 848

серверы ((продолжение))

Свойства основных служб ((продолжение))
 Пароль доступа к секретным ключам 848
 Пароль доступа к секретным ключам списка надежных сертификатов 848
 Порт 848
 Порт HTTP 848
 Порт HTTPS 848
 Порт прокси 848
 Порт сервера имен 848
 Привязка к имени хоста или IP-адресу 848
 Привязка ко всем IP-адресам 848
 Протокол 848
 Псевдоним сертификата 848
 Таймаут запуска службы 848
 Таймаут простаивающих временных объектов 848
 Тип хранилища сертификатов 848
 Уровень журнала 848
 свойства сервера Crystal Reports
 Аргументы Java VM 864
 Аргументы дочерней Java VM 864
 Временный каталог 864
 Истечение срока действия единого входа 864
 Каталог файлов кэша 864
 Количество записей БД, прочитываемых для предварительного просмотра или обновления отчета 864
 Максимальное количество заданий на весь срок жизни для каждого дочернего объекта 864
 Максимальное число параллельных заданий 864
 Максимальное число предварительно запущенных дочерних процессов 864
 Максимальный размер кэша 864
 Максимальный срок хранения данных, предоставляемых клиенту 864

серверы ((продолжение))

свойства сервера Crystal Reports
((продолжение))

Предоставлять совместный доступ к данным отчета для клиентов 864
 При обновлении средства просмотра всегда выдаются текущие данные 864
 Путь к классу Java 864
 Размер данных просмотра 864
 Размер пакета 864
 Разрешить заданиям для отчетов сохранять соединение с БД до закрытия данного задания для отчета 864
 Таймаут кэша безопасности 864
 Таймаут простоя задания 864
 Таймаут простоя соединения 864
 Число записей, прочитываемое в базе данных для предварительного просмотра или обновления 864

Свойства сервера Dashboard Design

Аргументы Java VM 888
 Аргументы дочерней Java VM 888
 Время ожидания кэша безопасности (в минутах) 888
 Максимальное количество заданий на весь срок жизни для каждого дочернего объекта 888
 Максимальное число параллельных заданий 888
 Максимальное число предварительно запущенных дочерних процессов 888
 Максимальный размер кэша (в КБ) 888
 Предельное время простоя соединения (мин) 888

серверы ((продолжение))

Свойства сервера Dashboard Design ((продолжение))

Разрешить заданиям для отчетов сохранять соединение с БД до закрытия данного задания для отчета 888
 Самые старые данные, выданные клиентам по запросам (сек) 888
 Совместный доступ к данным для клиентов 888
 Таймаут простоя задания 888
 Таймаут простоя соединения 888
 Число записей, прочитываемое в базе данных для предварительного просмотра или обновления 888

Свойства сервера соединений

Активация источника данных 861
 База данных 861
 Включение отслеживания заданий 861
 Включить образование блоков HTTP 861
 Включить отслеживание программного обеспечения среднего яруса 861
 Время бездействия временных объектов 861
 Время ожидания пула подключений 861
 Интервал таймера временных объектов 861
 Размер блока HTTP 861
 Сетевой уровень 861
 Создание пула соединений 861

Свойства служб Web Intelligence

Верхний порог памяти 877
 Включить анализ памяти 877
 Включить кэш документов 877
 Включить кэш реального времени 877
 Включить мониторинг 877
 Включить мониторинг с помощью службы PJS 877
 Включить список значений кэша 877

серверы ((продолжение))

Свойства служб Web Intelligence ((продолжение))

Время ожидания очистки системы визуализации (сек) 877
 Время ожидания подкачки системы визуализации (сек) 877
 Выходной каталог кэша 877
 Задержка цикла потока мониторинга (секунды) 877
 Значение прокси 877
 Интервал опроса сервера 877
 Интервал очистки кэша документов 877
 Истечение срока действия единого входа 877
 Каталог изображений 877
 Макс. размер пользовательской сортировки 877
 Макс. размер потока двоичных данных 877
 Макс. размер символического потока 877
 Максимальное количество документов в кэше 877
 Максимальное количество документов до утилизации 877
 Максимальное сжатие кэша документов 877
 Максимальное число документов на одного пользователя 877
 Максимальное число соединений 877
 Максимальный порог памяти 877
 Максимальный размер кэша документов 877
 Максимальный размер кэша юниверсов 877
 Максимальный размер списка значений 877
 Не удастся использовать HTTP URL 877
 Нижний порог памяти 877
 Отключить совместное использование кэша 877
 Период потока мониторинга службы PJS 877
 Размер пакета списка значений 877

серверы ((продолжение))

Свойства служб Web Intelligence ((продолжение))

Размер пакета списка значений (элементы) 877
Разрешить ошибки макс. размера карты документа 877

Таймаут до повторного использования 877

Таймаут кэша 877

Таймаут обмена отслеживаемых ресурсов по умолчанию (секунды) 877

Таймаут очистки отслеживаемых ресурсов по умолчанию (секунды) 877

Таймаут простоя документа 877

Таймаут простоя соединения 877

Число повторных попыток при сбое тестового опроса службы PJS 877

Свойства служб веб-приложений BEx

Главная система SAP BW 875

Количество соединений сервера JCo 875

Максимальное число сеансов клиентов 875

Назначение RFC сервера JCo 875

Служба шлюза сервера JCo 875

Хост шлюза сервера JCo 875

Свойства службы многомерного анализа

Максимальное число сеансов клиента 875

Максимальное число элементов, возвращаемых при фильтрации 875

Максимальное число ячеек, возвращаемых запросом 875

Свойства службы объединения данных

Время ожидания неактивного оператора 876

Время ожидания неактивного соединения 876

серверы ((продолжение))

Свойства службы объединения данных ((продолжение))

Максимальное число

соединений 876

Размер пула потока выполнения 876

состояние 377

список 369

сравнение со службами 19, 42

стандартные параметры командной строки 798

статус 369

строки команд 797, 798

Таймаут запуска службы 848

Таймаут простаивающих

временных объектов 848

Тип хранилища сертификатов 848

удаление 385

узлы 19, 42

Уровень журнала 848

установки по умолчанию 403

шаблоны настройки 401

настройка 402

применение 402

Серверы SAP BusinessObjects

Enterprise 571

серверы веб-приложений 29

Software Development Kit (SDK)

31

аутентификация 224

серверы каталогов 245

о протоколе LDAP 244

подключаемый модуль

безопасности 245

серверы платформы BI

настройка Kerberos и браузеров

270

настройка файла хостов для

брандмауэра 192

серверы платформы SAP

BusinessObjects Business

Intelligence

настройка Kerberos и браузеров

461

Серверы репозитория файлов 19,

42, 848

восстановление 482, 483

параметры командной строки 810

Серверы файлового репозитория

создание резервной копии 478

сетевой интерфейс

устранение неполадок

нескольких 408

сетевые интерфейсы для

устранения неполадок 409

сетевые среды

IPv4

двойные узлы IPv4/IPv6 404

IPv6 404

синхронизация информации отчета

709

синхронизация сведений отчета 709

система контроля полномочий 298

системная учетная запись 296

сквозной единый вход 228

скрипты UNIX, обзор 785

скрипты Windows, обзор 794

скрипты управления узлами,

расположение 412

скрипты, UNIX 785

скрипты, Windows 794

Служба Business Process BI

добавление на сервер Web

Application Container Server

453

удаление с сервера Web

Application Container Server

454

служба BW Publisher 698

выполняется настройка 698

запуск 698

создание RFC-адресата 699

служба мониторинга 566

службы 44

сравнение с серверами 19, 42

шаблоны настройки 401

Службы информационной

платформы

административные права 366

отображение ролей 329, 347, 360

права на публикацию 367

создание учетной записи для 296

служебная программа SPN 266

CMS

включение и отключение других

серверов 381, 382

запуск 380

изменение имени кластера 389

как сервер имен 409, 410

кластеризация 385, 388

требования 385

установка нового члена

кластера 387

настройка 409, 410, 438, 439,

440, 441

остановка 380

поиск и устранение

неисправностей 380

порт по умолчанию 409, 410

- CMS (*продолжение*)
устранение неполадок на
многосетевых компьютерах
409
- CMC
включение и отключение
серверов 381, 382
зависимости сервера Windows,
добавление 433
запуск, остановка и перезагрузка
серверов 378, 379
клонирование серверов 383, 385
контролирование доступа к 506
криптографические ключи 165
права 831
удаление сервера 385
управление серверами 369
- совместно используемые
библиотеки, обработка
расширений 157
- соединения с источниками данных
545
- соединения с юниверсами
права 829
тиражирование 657
удаление 545
управление 545
- создание
группы 101
подгруппы серверов 391, 392
уровни доступа 137
учетные записи пользователей
98
- состояние, просмотр и изменение
для серверов 377
- состояния сервера 369
- сохраненные данные 135
- специалисты по шифрованию 164
добавление членов 164
- списки контроля доступа
добавление владельцев учетных
записей к 128
просмотр 127
- списки надежных сертификатов 456
- списки тиражирования
изменение 662
параметры зависимостей 659,
660
поддерживаемые объекты 659
создание 659, 660
управление 662
- Список случаев сбоя индексации 639
- Средства просмотра отчетов 73
- Средство администрирования
объединения данных 66
- Средство дизайна информации,
права 837
- Средство запросов веб-служб 33, 65
- средство преобразования отчетов
SSL 177
- Средство преобразования отчетов
64
- Средство создания юниверсов 64
- средство создания юниверсов,
права 837
- Средство управления обновлением
22, 68
- средство управления переводами
SSL 177
- Средство управления переводами
66
- CCM
включение и отключение
серверов 381, 382
для UNIX 785, 789
для Windows 794, 796
добавление сервера 382
запуск, остановка и перезагрузка
серверов 378, 380
удаление сервера 385
узлы 412
воссоздание 417
добавление 414
переименование 423
перемещение 424
удаление 421
учетные данные
пользователя, изменение
для 434
- стартовая панель BI 72
- вход в систему 108, 109
- контролирование доступа к 506
- настройка 108
- настройка входа в систему 536
- параметры группы 110
- права 831
- управление 515
- статистика, аудит действий через
Интернет 155
- сторонние группы, репликация 656
- сторонние пользователи,
репликация 656
- сходство, и SSL 152
- Т**
- темы дискуссии 512
- отмена поиска 512
- поиск 512
- сортировка результатов поиска
514
- тест 552
- типы серверов 56, 59
- Типы содержимого, доступного для
поиска 631
- тиражирование
объекты 643
сторонние пользователи и
группы 656
- Транспорт CTS (CTS+) 38
- Транспорт InfoSet Connectivity 713
- Транспорт Open SQL Connectivity
713
- транспорт определения кластера
713, 718
- транспорты 713, 714
- Content Administration Workbench
719
- взаимодействие InfoSet 717
- взаимодействие Open SQL 715
- группы функций 712
- импорт 714
- общие сведения 712
- объекты 712
- определение безопасности на
уровне строки 717
- определение кластера 718
- Определение кластера 713
- персонализация параметров
713, 722
- Подключение к InfoSet 713
- проверка на конфликты 714
- программы 712
- Редактор параметров
безопасности 713
- таблицы 712
- трассировка 759
- серверы 760
- настройка INI-файла 762
- требования
кластеризация 385
- У**
- уведомление 551
- удаление 439, 440, 441
- база данных системы CMS 439,
440, 441
- группы 103
- псевдонимы 115
- серверы 385
- Серверы контейнера
веб-приложений (WACS) 453
- соединения с юниверсами 545
- уровни доступа 137
- учетные записи пользователей
100

удаление ((*продолжение*))
 юниверсы 547
 удаленное планирование 681, 683
 удаленные соединения
 безопасность 665
 изменение 665
 просмотр 663
 создание 663
 создание папок 663
 узлы 19, 42, 412
 воссоздание 428
 AddNode.bat 418
 addnode.sh 420
 RemoveNode.bat 421
 removenode.sh 422
 serverconfig.sh 419
 скрипты для 417
 CCM 417
 добавление 413, 428
 AddNode.bat 415
 addnode.sh 416
 CMS 387
 serverconfig.sh 415
 в кластер 387
 новый компьютер 413
 CCM 414
 кластеризация 385
 переименование 422
 serverconfig.sh 423
 CCM 423
 перемещение 424, 430
 MoveNode.bat 425
 movenode.sh 427
 serverconfig.sh 426
 CCM 424
 CMC 369
 удаление 420, 428
 serverconfig.sh 421
 CCM 421
 управление версиями 40
 управление жизненным циклом
 инструмент командной строки
 механизма BIAR 497
 Управление жизненным циклом
 (LCM) 40
 управление приложениями 505
 war-файл BOE 527
 темы дискуссии, удаление 514
 управляемые объекты 336
 Группа BusinessObjects
 Enterprise 336, 340
 роли PeopleSoft 336, 340
 юниверсы 336, 340
 уровень журнала трассировки
 Параметр сервера CMC 761, 762

уровни доступа 118, 126, 142
 RAS 394
 администрирование 142
 задачи, права, требуемые для
 133
 изменение прав в 138
 копирование 136
 назначение владельцам учетных
 записей 128
 Отношения к объектам 139
 переименование 137
 права 823
 предопределенный 133
 просмотр 127
 просмотр и просмотр по запросу
 135
 создание 137
 удаление 137
 управление на уровне
 нескольких сайтов 139
 установка
 уровни безопасности по
 умолчанию 696
 шлюза SAP в Windows 699
 установки по умолчанию
 порты 409, 410
 серверы 403
 устранение неполадок 640
 Kerberos 464
 единый вход 256
 настройка Kerberos 294
 Серверы контейнера
 веб-приложений (WACS) 472
 сообщения об ошибках 691
 учетные записи LDAP 262
 учетная запись SMCAdmin 780
 учетная запись службы
 делегирования 266
 конфигурация серверов 269
 установка 266
 учетные данные пользователя,
 изменение для узлов 434
 учетные записи
 службы информационной
 платформы 296
 управление 93, 98
 учетные записи гостя
 отключение 104
 учетные записи пользователей
 изменение 100
 по умолчанию 93
 создание 98
 удаление 100
 управление 93, 98

Ф

файл ответов 336
 применение 339
 создание 336
 Файл ответов PeopleSoft 341
 параметры 341
 файл хостов, настройка для
 брандмауэра с NAT 192
 файловая система
 восстановление 487, 488
 создание резервной копии 478
 файлы cookie 153
 маркеры входа 152
 отслеживание сеансов 153
 файлы WAR
 BOE 210, 527, 528, 530, 532
 dswebobje 210
 OpenDocument 278
 war-файл BOE
 глобальные свойства 528
 свойства CMC 534
 свойства OpenDocument 532
 свойства стартовой панели
 BI 530
 Веб-приложения для платформы
 BI 210
 и веб-приложения для
 платформы BI 210
 файлы журнала аудита 478
 файлы ключа 171, 172
 файлы сертификатов 171, 172, 456
 фасеты 633

Х

хосты
 настройка LDAP 247, 252

Ц

Цветовые индикаторы трафика 549
 Центральный сервер управления
 19, 42
 центральный сервер управления.
 См. CMS. 295

Ш

шаблоны безопасности по
 умолчанию 696
 шаблоны настройки 401
 восстановление установок
 системы по умолчанию 403
 настройка 402

шаблоны настройки *((продолжение))*
 практический опыт 401
 применение 402
шифрование, маркеры входа 152
шлюз SAP 320
 и SNC 320
 публикация с использованием
 локального 699
 распространение компонентов
 698

шлюз SAP *((продолжение))*
 установка 699

Ю

юниверс 34
юниверсы
 права (.unv) 825
 права (.unx) 826

юниверсы *((продолжение))*
 тиражирование 657
 управление 546

Я

языки 35
ярус приложений 399
ярусы 41

