



Руководство администратора платформы Business Intelligence

■ SAP BusinessObjects Business Intelligence platform 4.1

2013-07-02

Авторские права

© SAP AG или аффилированная компания SAP, 2013. Все права защищены. Полное или частичное воспроизведение или передача в какой-либо форме и в каких-либо целях настоящей публикации без явным образом выраженного разрешения SAP AG запрещены. Информация, содержащаяся в настоящей публикации, может быть изменена без предварительного уведомления. Некоторые программные продукты, предлагаемые на рынке компанией SAP AG и ее дистрибьюторами, содержат компоненты программного обеспечения, исключительными правами в отношении которых обладают иные поставщики программного обеспечения. Возможны различные варианты спецификаций продуктов для разных стран. Материалы предоставлены компанией SAP AG и ее аффилированными компаниями ("SAP Group") исключительно в информационных целях, без предоставления каких-либо гарантий. SAP Group не несет ответственности за ошибки или пропуски в настоящих материалах. Гарантии, если таковые предоставляются, в отношении продуктов и услуг SAP Group содержатся исключительно в документах, которые прилагаются к соответствующим продуктам и услугам. Ничто, изложенное в настоящем документе, не должно трактоваться как предоставление дополнительных гарантий. SAP, а также другие указанные продукты и услуги SAP, как и соответствующие логотипы являются товарными знаками или зарегистрированными товарными знаками SAP AG на территории Германии и других стран. Для получения дополнительных сведений и уведомлений о товарных знаках см. <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark>.

2013-07-02

Содержание

Глава 1	История документа.....	21
Глава 2	Начало работы.....	23
2.1	О справке.....	23
2.1.1	Для кого предназначена данная справка?.....	23
2.1.2	О платформе Business Intelligence	23
2.1.3	Переменные.....	24
2.2	Начало работы.....	24
2.2.1	Основные понятия.....	25
2.2.2	Основные инструменты администрирования.....	27
2.2.3	Ключевые задачи.....	29
Глава 3	Архитектура.....	33
3.1	Обзорная информация по архитектуре.....	33
3.1.1	Диаграмма компонентов.....	34
3.1.2	Уровни архитектуры.....	35
3.1.3	Базы данных.....	37
3.1.4	Серверы, хосты и кластеры.....	38
3.1.5	Серверы веб-приложений.....	38
3.1.6	Software Development Kit.....	40
3.1.7	Источники данных.....	42
3.1.8	Аутентификация и единый вход.....	43
3.1.9	Интеграция SAP.....	45
3.1.10	Интегрированное управление версиями.....	46
3.1.11	Путь обновления.....	47
3.2	Службы и серверы.....	47
3.2.1	Изменения сервера с версии XI 3.1.....	49
3.2.2	Службы.....	51
3.2.3	Категории служб.....	60
3.2.4	Типы серверов.....	63
3.2.5	Серверы.....	70
3.3	Клиентские приложения.....	72

3.3.1	Устанавливается вместе со средствами клиента платформы SAP BusinessObjects Business Intelligence.....	73
3.3.2	Устанавливается вместе с платформой SAP BusinessObjects Business Intelligence.....	78
3.3.3	Доступно отдельно.....	79
3.3.4	Клиенты веб-приложений.....	81
3.4	Рабочие процессы.....	85
3.4.1	Запуск и аутентификация.....	85
3.4.2	Объекты программ.....	87
3.4.3	Crystal Reports.....	88
3.4.4	Web Intelligence.....	93
3.4.5	Analysis.....	95
Глава 4	Мастер настройки системы.....	97
4.1	Вводные сведения о мастере настройки системы.....	97
4.2	Указание используемых продуктов.....	97
4.3	Выбор шаблона развертывания.....	99
4.4	Местоположение каталогов данных.....	101
4.5	Просмотр изменений.....	102
4.6	Файлы журнала и файлы ответов.....	103
4.6.1	Использование файла ответов.....	103
Глава 5	Управление лицензиями.....	107
5.1	Управление лицензионными ключами.....	107
5.1.1	Просмотр сведений лицензии.....	107
5.1.2	Для добавления ключа лицензии.....	107
5.1.3	Для просмотра текущей деятельности учетной записи.....	108
5.2	Измерение показателей использования лицензий.....	108
5.2.1	Проведение аудита лицензий.....	109
Глава 6	Управление пользователями и группами.....	111
6.1	Обзор управления учетными записями.....	111
6.1.1	Управление пользователями.....	111
6.1.2	Управление группами.....	112
6.1.3	Доступные типы аутентификации	113
6.2	Управление Enterprise и общими учетными записями.....	115
6.2.1	Создание учетной записи пользователя.....	116
6.2.2	Для изменения учетной записи пользователя.....	117
6.2.3	Чтобы удалить учетную запись пользователя.....	117
6.2.4	Чтобы создать новую группу.....	118
6.2.5	Для изменения свойств группы.....	118

6.2.6	Просмотр участников групп.....	119
6.2.7	Чтобы добавить подгруппы.....	119
6.2.8	Задание принадлежности к группе.....	120
6.2.9	Удаление группы.....	120
6.2.10	Массовое добавление пользователей или групп пользователей.....	121
6.2.11	Чтобы включить учетную запись Гостя.....	121
6.2.12	Добавление пользователей в группы.....	122
6.2.13	Изменение настроек пароля.....	123
6.2.14	Предоставление доступа пользователям и группам.....	125
6.2.15	Управление доступом к каталогам "Входящие" пользователей.....	126
6.2.16	Настройка параметров стартовой панели BI.....	126
6.3	Управление псевдонимами.....	130
6.3.1	Чтобы создать пользователя и добавить сторонний псевдоним.....	130
6.3.2	Для создания нового псевдонима существующего пользователя.....	131
6.3.3	Для присвоения псевдонима пользователю.....	131
6.3.4	Для удаления псевдонима.....	132
6.3.5	Для отключения псевдонима.....	133
Глава 7	Установка прав.....	135
7.1	Права на платформе BI.....	135
7.1.1	Уровни доступа.....	136
7.1.2	Параметры расширенных прав.....	136
7.1.3	Наследование.....	137
7.1.4	Права для конкретных типов объектов.....	143
7.1.5	Определение эффективных прав.....	144
7.2	Управление настройками безопасности для объектов в СМС.....	145
7.2.1	Для просмотра прав принципала на объект.....	145
7.2.2	Для назначения принципалов списку управления доступом к объекту.....	146
7.2.3	Для изменения безопасности объекта для принципала.....	147
7.2.4	Настройка прав на папку верхнего уровня в платформе BI.....	147
7.2.5	Проверка настроек безопасности для принципала.....	148
7.3	Работа с уровнями доступа.....	151
7.3.1	Выбор между уровнями доступа Просмотр и Просмотр по требованию.....	153
7.3.2	Чтобы скопировать существующий уровень доступа.....	154
7.3.3	Создание уровня доступа.....	155
7.3.4	Переименование уровня доступа.....	155
7.3.5	Для удаления уровня доступа.....	155
7.3.6	Изменение прав в уровне доступа.....	156
7.3.7	Трассировка связи между уровнями доступа и объектами.....	157
7.3.8	Управление уровнями доступа по сайтам.....	157
7.4	Отключение наследования.....	158

7.4.1	Отключение наследования.....	160
7.5	Использование прав передачи административных полномочий.....	160
7.5.1	Выбор параметров Изменить права пользователей на объекты.....	162
7.5.2	Права владельца.....	164
7.6	Сводка рекомендаций по управлению правами.....	164
Глава 8	Обеспечение безопасности платформы BI.....	167
8.1	Обзор вопросов безопасности	167
8.2	Планирование аварийного восстановления.....	167
8.3	Общие рекомендации по обеспечению безопасности развертывания.....	168
8.4	Настройка безопасности для связанных серверов сторонних производителей.....	169
8.5	Активные доверительные отношения.....	169
8.5.1	Маркеры входа.....	170
8.5.2	Механизм билетов для распределенной безопасности.....	171
8.6	Сеансы и отслеживание сеансов.....	171
8.6.1	Отслеживание сеансов центральным сервером управления.....	172
8.7	Защита среды.....	172
8.7.1	Веб-браузер с веб-сервером.....	172
8.7.2	Веб-сервер – платформа BI.....	173
8.8	Аудит изменений параметров безопасности	173
8.9	Аудит действий через Интернет.....	173
8.9.1	Защита от попыток выполнения входа злоумышленником.....	174
8.9.2	Ограничения для пароля.....	174
8.9.3	Ограничения на вход.....	174
8.9.4	Ограничения для пользователя.....	175
8.9.5	Ограничения учетной записи гостя.....	175
8.10	Расширения обработки.....	175
8.11	Обзор безопасности данных платформы BI.....	176
8.11.1	Защищенные режимы обработки данных.....	176
8.12	Криптография в платформе BI.....	179
8.12.1	Работа с ключами кластера.....	179
8.12.2	Специалисты по шифрованию.....	182
8.12.3	Управление криптографическими ключами с помощью CMC.....	183
8.13	Настройка серверов для SSL.....	189
8.13.1	Создание файлов ключа и сертификата.....	189
8.13.2	Настройка SSL при управлении сертификатом центром сертификации.....	191
8.13.3	Настройка протокола SSL.....	193
8.14	Основные сведения об обмене данными между компонентами платформы BI.....	198
8.14.1	Обзор серверов платформы BI и портов обмена данными.....	198
8.14.2	Взаимодействие между компонентами платформы BI	201
8.15	Настройка платформы BI для брандмауэров.....	209

8.15.1	Настройка системы для использования брандмауэров.....	209
8.15.2	Отладка развертывания брандмауэра.....	213
8.16	Примеры типовых сценариев развертывания брандмауэров.....	214
8.16.1	Пример: уровень приложений развернут в отдельной сети.....	215
8.16.2	Пример: толстый клиент и уровень БД отделены брандмауэром от платформы BI	217
8.17	Настройки брандмауэра для интегрированных сред.....	220
8.17.1	Рекомендации по настройке брандмауэра для интеграции SAP.....	220
8.17.2	Настройка брандмауэра для интеграции с JD Edwards EnterpriseOne.....	222
8.17.3	Конкретные рекомендации по настройке брандмауэра для Oracle EBS.....	223
8.17.4	Настройка брандмауэра для интеграции с PeopleSoft Enterprise	224
8.17.5	Настройка брандмауэра для интеграции с Siebel.....	226
8.18	Платформа BI и обратные прокси-серверы	228
8.18.1	Поддерживаемые обратные прокси-серверы	228
8.18.2	Понимание механизма развертывания веб-приложений	228
8.19	Настройка обратных прокси-серверов для веб-приложений платформы BI	229
8.19.1	Подробные инструкции по настройке обратных прокси-серверов.....	229
8.19.2	Настройка обратного прокси-сервера.....	230
8.19.3	Настройка обратного прокси-сервера Apache 2.2 для платформы BI	230
8.19.4	Настройка обратного прокси-сервера WebSEAL 6.0 для платформы BI	231
8.19.5	Настройка Microsoft ISA 2006 для платформы BI	232
8.20	Специальная настройка для платформы BI при развертывании с обратным прокси-сервером	234
8.20.1	Включение обратного прокси-сервера для веб-служб	234
8.20.2	Включение пути к корневому каталогу для файлов cookie сеанса для ISA 2006.....	237
8.20.3	Включение обратного прокси-сервера для приложения SAP BusinessObjects Live Office.....	239
Глава 9	Аутентификация.....	241
9.1	Параметры аутентификации платформы BI.....	241
9.1.1	Основная аутентификация.....	242
9.1.2	Подключаемые модули безопасности.....	243
9.1.3	Единый вход на платформу BI.....	244
9.2	Аутентификация Enterprise.....	246
9.2.1	Общая информация об аутентификации Enterprise.....	246
9.2.2	Настройки аутентификации Enterprise.....	247
9.2.3	Изменение параметров Enterprise.....	248
9.2.4	Включение доверительной аутентификации.....	250
9.2.5	Настройка доверительной аутентификации для веб-приложения.....	251
9.3	Аутентификация LDAP.....	262
9.3.1	Использование аутентификации LDAP.....	262
9.3.2	Настройка аутентификации LDAP.....	264
9.3.3	Сопоставление групп LDAP.....	274

9.4	Аутентификация Windows AD.....	285
9.4.1	Использование аутентификации Windows AD.....	285
9.4.2	Подготовка контроллера домена.....	286
9.4.3	Настройка аутентификации AD в СМС.....	287
9.4.4	Настройка сервиса платформы BI для запуска SIA.....	295
9.4.5	Настройка сервера веб-приложений для аутентификации AD.....	297
9.4.6	Настройка единственной подписи.....	305
9.4.7	Устранение неполадок с аутентификацией Windows AD.....	320
9.5	Аутентификация SAP.....	321
9.5.1	Настройка аутентификации SAP	322
9.5.2	Создание учетной записи пользователя для платформы BI.....	322
9.5.3	Подключение к системам контроля полномочий SAP.....	324
9.5.4	Настройка параметров аутентификации SAP.....	326
9.5.5	Импорт ролей SAP.....	332
9.5.6	Настройка защищенного обмена данными (SNC).....	336
9.5.7	Настройка единого входа в систему SAP.....	349
9.5.8	Настройка единого входа для SAP Crystal Reports и SAP Netweaver.....	353
9.6	Аутентификация PeopleSoft.....	354
9.6.1	Обзор.....	354
9.6.2	Включение аутентификации PeopleSoft Enterprise.....	355
9.6.3	Сопоставление ролей PeopleSoft в платформе BI.....	355
9.6.4	Планирование пользовательских обновлений.....	359
9.6.5	Использование моста безопасности PeopleSoft.....	361
9.7	Аутентификация JD Edwards.....	372
9.7.1	Обзор.....	372
9.7.2	Включение аутентификации JD Edwards EnterpriseOne.....	372
9.7.3	Сопоставление ролей JD Edwards EnterpriseOne в платформе BI.....	373
9.7.4	Планирование пользовательских обновлений.....	376
9.8	Аутентификация Siebel.....	378
9.8.1	Включение аутентификации Siebel.....	378
9.8.2	Сопоставление ролей платформе BI.....	379
9.8.3	Планирование пользовательских обновлений.....	382
9.9	Аутентификация Oracle EBS.....	384
9.9.1	Разрешение аутентификации Oracle EBS.....	385
9.9.2	Сопоставление ролей Oracle E-Business Suite с платформой BI.....	386
9.9.3	Неотображаемые роли	390
9.9.4	Настройка прав для назначенных групп и пользователей Oracle EBS	391
9.9.5	Настройка единого входа (SSO) для SAP Crystal Reports и Oracle EBS.....	392
Глава 10	Администрирование сервера.....	395
10.1	Работа с областью управления СМС "Серверы".....	395

10.2	Управление серверами с помощью скриптов в Windows	400
10.3	Управление серверами в UNIX	400
10.4	Просмотр и изменение статуса сервера.....	400
10.4.1	Просмотр состояний серверов.....	400
10.4.2	Запуск, остановка и перезапуск серверов.....	402
10.4.3	Остановка центрального сервера управления (CMS).....	405
10.4.4	Включение и выключение серверов.....	406
10.5	Добавление, клонирование и удаление серверов.....	407
10.5.1	Добавление, клонирование и удаление серверов.....	407
10.6	Кластеризация центральных серверов управления (CMS).....	410
10.6.1	Кластеризация центральных серверов управления (CMS).....	410
10.7	Управление группами серверов.....	415
10.7.1	Создание группы серверов.....	416
10.7.2	Работа с подгруппами серверов.....	417
10.7.3	Изменение принадлежности сервера к группе.....	418
10.7.4	Доступ пользователей к серверам и группам серверов.....	419
10.8	Настройка адаптивных серверов обработки для производственных систем.....	420
10.9	Оценка производительности системы.....	421
10.9.1	Мониторинг серверов платформы SAP BusinessObjects Business Intelligence.....	421
10.9.2	Анализ серверных показателей.....	421
10.9.3	Просмотр системных показателей.....	422
10.9.4	Регистрация деятельности сервера.....	423
10.10	Конфигурация настроек серверов.....	424
10.10.1	Для изменения свойств сервера.....	424
10.10.2	Применение параметров службы к нескольким серверам.....	425
10.10.3	Работа с шаблонами конфигурации.....	425
10.11	Настройка сетевых параметров сервера.....	428
10.11.1	Параметры сетевой среды.....	428
10.11.2	Параметры идентификации хоста сервера.....	429
10.11.3	Настройка группового компьютера.....	431
10.11.4	Настройка номеров портов.....	434
10.12	Управление узлами.....	437
10.12.1	Использование узлов.....	437
10.12.2	Добавление нового узла.....	440
10.12.3	Восстановление узла.....	445
10.12.4	Удаление узла.....	448
10.12.5	Переименование узла.....	450
10.12.6	Перемещение узла.....	452
10.12.7	Параметры скриптов.....	456
10.12.8	Добавление зависимостей сервера Windows.....	461
10.12.9	Изменение учетных данных пользователя для узла.....	462

10.13	Переименование компьютера в развертывании платформы BI.....	463
10.13.1	Изменение имен кластеров.....	463
10.13.2	Изменение IP-адресов.....	463
10.13.3	Переименование компьютеров.....	465
10.14	Использование 32-битных и 64-битных сторонних библиотек вместе с платформой BI.....	469
10.15	Управление заполнителями сервера и узла	470
10.15.1	Просмотр заполнителей для сервера.....	470
10.15.2	Просмотр и изменение заполнителей для узла.....	470
Глава 11	Управление базами данных центрального сервера управления (CMS).....	473
11.1	Управление соединением с системной базой данных центрального сервера управления.....	473
11.1.1	Выбор SAP HANA в качестве базы данных CMS.....	473
11.1.2	Выбор SAP HANA в качестве базы данных CMS.....	474
11.2	Выбор новой или существующей базы данных центрального сервера управления.....	475
11.2.1	Выбор новой или существующей базы данных CMS в Windows.....	476
11.2.2	Выбор новой или существующей базы данных центрального сервера управления в UNIX.....	477
11.3	Повторное создание базы данных системы центрального сервера управления.....	477
11.3.1	Восстановление системной базы данных CMS в ОС Windows.....	478
11.3.2	Восстановление системной базы данных CMS в ОС UNIX.....	479
11.4	Копирование данных из одной базы данных CMS в другую.....	480
11.4.1	Подготовка к копированию системной базы данных CMS.....	480
11.4.2	Копирование системной базы данных CMS в Windows.....	481
11.4.3	Для копирования данных из базы данных системы центрального сервера управления на UNIX.....	481
Глава 12	Управление серверами контейнера веб-приложений (WACS).....	483
12.1	WACS.....	483
12.1.1	Сервер контейнера веб-приложений (WACS).....	483
12.1.2	Добавление дополнительных серверов WACS в систему и их удаление.....	487
12.1.3	Добавление или удаление служб на сервере WACS.....	491
12.1.4	Настройка HTTPS/SSL.....	492
12.1.5	Поддерживаемые методы аутентификации.....	496
12.1.6	Настройка Kerberos AD для WACS	497
12.1.7	Настройка единого входа в AD Kerberos	503
12.1.8	Настройка веб-служб RESTful.....	506
12.1.9	Сервер контейнера веб-приложений (WACS) и ваша IT-среда.....	515
12.1.10	Настройка свойств веб-приложений.....	517
12.1.11	Устранение неполадок.....	518
12.1.12	Свойства WACS.....	523

Глава 13	Резервное копирование и восстановление системы.....	525
13.1	Обзор резервного копирования и восстановления.....	525
13.2	Терминология.....	525
13.3	Случаи использования резервного копирования и восстановления.....	527
13.4	Резервные копии.....	529
13.4.1	Резервное копирование всей системы.....	530
13.4.2	Резервное копирование настроек сервера.....	533
13.4.3	Резервное копирование платформы BI.....	536
13.5	Восстановление системы.....	537
13.5.1	Восстановление всей системы.....	537
13.5.2	Восстановление настроек сервера.....	543
13.5.3	Восстановление содержимого BI.....	546
13.6	Скрипты BackupCluster и RestoreCluster.....	546
Глава 14	Копирование развертывания платформы Business Intelligence.....	551
14.1	Обзор копирования системы.....	551
14.2	Терминология.....	551
14.3	Ситуации, в которых может потребоваться копирование системы.....	552
14.4	Планирование копирования системы.....	553
14.5	Рекомендации и ограничения.....	554
14.6	Процедура копирования системы.....	556
14.6.1	Экспорт из исходной системы.....	556
14.6.2	Импорт в целевую систему.....	562
Глава 15	Управление версиями.....	565
15.1	Управление разными версиями ресурсов BI	565
15.2	Использование параметра системных настроек управления версиями.....	566
15.2.1	Установка системы управления версиями ClearCase в Windows.....	567
15.2.2	Установка системы управления версиями ClearCase в Unix.....	567
15.3	Сравнение разных версий одного задания.....	568
15.4	Обновление содержимого вспомогательной версии.....	568
Глава 16	Управление повышением.....	571
16.1	Введение в управление повышением.....	571
16.1.1	Обзор средства управления повышением.....	571
16.1.2	Функции управления повышением.....	571
16.1.3	Права доступа к приложению.....	572
16.1.4	Поддержка WinAD в управлении повышением.....	573
16.2	Начало работы со средством управления повышением.....	573

16.2.1	Запуск приложения управления повышением.....	573
16.2.2	Компоненты пользовательского интерфейса.....	574
16.2.3	Использование параметра настройки.....	576
16.3	Использование средства управления повышением.....	582
16.3.1	Создание и удаление папки.....	583
16.3.2	Создание задания.....	584
16.3.3	Создание нового задания путем копирования существующего	587
16.3.4	Поиск задания.....	587
16.3.5	Изменение задания.....	588
16.3.6	Добавление информационных объектов в управление повышением.....	589
16.3.7	Управление зависимостями в приложении управления повышением	590
16.3.8	Поиск зависимых объектов	591
16.3.9	Повышение задания при соединении с репозиториями.....	592
16.3.10	Повышение задания с помощью файла BIAR.....	594
16.3.11	Планирование повышения задания.....	597
16.3.12	Просмотр журнала задания.....	598
16.3.13	Откат задания.....	599
16.4	Управление разными версиями объекта InfoObject.....	601
16.4.1	Права доступа к приложению управления версиями.....	603
16.4.2	Резервное копирование и восстановление файлов вспомогательных версий.....	604
16.5	Использование ключа командной строки.....	605
16.5.1	Запуск параметра командной строки в ОС Windows.....	605
16.5.2	Запуск параметра командной строки в UNIX.....	606
16.5.3	Параметры командной строки.....	606
16.5.4	Образец файла свойств.....	615
16.6	Использование Enhanced Change and Transport System.....	616
16.6.1	Предварительные условия.....	616
16.6.2	Настройка платформы Business Intelligence и интеграции CTS+.....	617
16.6.3	Повышение задания с использованием CTS.....	621
Глава 17	Визуальное отличие.....	627
17.1	Visual Difference в средстве управления повышением.....	627
17.1.1	Сравнение объектов и файлов с использованием функции визуального отличия.....	628
17.1.2	Сравнение объектов или файлов в системе управления версиями.....	629
17.1.3	Планирование сравнения.....	630
Глава 18	Управление приложениями.....	633
18.1	Управление приложениями с помощью CMC.....	633
18.1.1	Обзор.....	633
18.1.2	Общие настройки приложений.....	634

18.1.3	Настройки, зависящие от приложения.....	635
18.2	Управление приложениями с помощью свойств BOE.war.....	678
18.2.1	Файл BOE.war.....	679
18.3	Настройка точек входа в систему для стартовой панели BI и OpenDocument.....	691
18.3.1	Местоположения файлов стартовой панели BI и OpenDocument.....	691
18.3.2	Определение пользовательской страницы входа в систему.....	693
18.3.3	Добавление доверительной аутентификации при входе в систему.....	694
18.4	Настройка интерфейса Web Intelligence.....	694
18.4.1	Вкладка "Функции".....	695
18.4.2	Вкладка "Элементы пользовательского интерфейса".....	696
18.4.3	Настройка внешнего вида интерфейса Web Intelligence.....	707
Глава 19	Управление соединениями и юниверсами.....	709
19.1	Управление соединениями.....	709
19.1.1	Для удаления соединения юниверса.....	709
19.2	Управление Юниверсами.....	710
19.2.1	Удаление юниверсов.....	710
Глава 20	Мониторинг.....	713
20.1	О приложении мониторинга.....	713
20.2	Термины мониторинга.....	714
20.2.1	Архитектура.....	715
20.3	Настройка поддержки баз данных в приложении "Мониторинг"	717
20.3.1	Настройка для использования базы данных Derby.....	718
20.3.2	Настройка для использования базы данных аудита.....	718
20.4	Свойства конфигурации.....	725
20.4.1	URL-адрес конечной точки JMX.....	730
20.4.2	HTTPS-аутентификация для зондов мониторинга.....	731
20.4.3	Шифрование паролей для зондов.....	731
20.5	Интеграция с другими приложениями.....	732
20.5.1	Интеграция приложения мониторинга с IBM Tivoli.....	732
20.5.2	Интеграция приложения мониторинга с SAP Solution Manager	735
20.6	Поддержка кластеров для сервера мониторинга.....	736
20.7	Устранение неполадок.....	736
20.7.1	Панель мониторинга.....	736
20.7.2	Предупреждения.....	737
20.7.3	Список наблюдений.....	737
20.7.4	Зонды.....	738
20.7.5	Показатели.....	739
20.7.6	Диаграмма.....	739

Глава 21	Аудит.....	741
21.1	Обзор.....	741
21.2	Страница "Аудит СМС".....	747
21.2.1	Состояние аудита.....	747
21.2.2	Настройка аудита событий.....	749
21.2.3	Параметры конфигурации хранилища данных аудита.....	751
21.3	События аудита.....	753
21.3.1	События и сведения аудита.....	764
Глава 22	Поиск по платформе.....	783
22.1	Описание поиска по платформе.....	783
22.1.1	Platform Search SDK.....	783
22.1.2	Кластеризованная среда.....	784
22.2	Настройка поиска по платформе.....	784
22.2.1	Развертывание OpenSearch.....	784
22.2.2	Настройка обратного прокси.....	786
22.2.3	Настройка свойств приложения в СМС.....	787
22.3	Работа с поиском по платформе.....	793
22.3.1	Индексация содержимого в репозитории СМС.....	793
22.3.2	Список сбоев индексации.....	794
22.3.3	Результаты поиска.....	794
22.4	Интеграция поиска по платформе с SAP NetWeaver Enterprise Search.....	802
22.4.1	Создание соединителя в SAP NetWeaver Enterprise Search	803
22.4.2	Импорт роли пользователя в аутентификации SAP BusinessObjects Business Intelligence.....	804
22.5	Поиск из NetWeaver Enterprise Search.....	804
22.6	Выполнение аудита.....	805
22.7	Устранение неполадок.....	806
22.7.1	Самовосстановление.....	806
22.7.2	Проблемные сценарии.....	807
Глава 23	Интеграция.....	809
23.1	интеграция.....	809
23.2	Термины для функции интеграции.....	810
23.3	Управление правами безопасности.....	812
23.3.1	Права, необходимые на сайте-источнике.....	813
23.3.2	Права, необходимые на сайте-адресате.....	813
23.3.3	Права, характерные для интеграции.....	814
23.3.4	Тиражирование безопасности объекта.....	816
23.3.5	Тиражирование параметров безопасности с использованием уровней доступа.....	817

23.4	Параметры типов и режимов тиражирования.....	818
23.4.1	Однонаправленное тиражирование	818
23.4.2	Двунаправленное тиражирование	818
23.4.3	"Обновлять из источника" или "Обновлять из адресата".....	819
23.5	Тиражирование сторонних пользователей и групп.....	820
23.6	Тиражирование юниверсов и соединений юниверсов.....	821
23.7	Управление списками тиражирования.....	822
23.7.1	Создание списков тиражирования.....	823
23.7.2	Изменение списков тиражирования.....	825
23.8	Управление удаленными соединениями.....	826
23.8.1	Создание удаленных соединений.....	827
23.8.2	Изменение удаленных соединений.....	829
23.9	Управление заданиями тиражирования.....	830
23.9.1	Создание заданий тиражирования.....	830
23.9.2	Планирование заданий тиражирования.....	832
23.9.3	Изменение заданий тиражирования.....	833
23.9.4	Просмотр журнала после выполнения задания тиражирования.....	834
23.10	Управление очисткой объектов.....	835
23.10.1	Способ использования очистки объектов.....	835
23.10.2	Ограничения очистки объектов.....	836
23.10.3	Частота очистки объектов.....	836
23.11	Управление обнаружением и разрешением конфликтов.....	837
23.11.1	Разрешение конфликтов однонаправленного тиражирования.....	838
23.11.2	Разрешение конфликта двунаправленного тиражирования.....	839
23.12	Использование веб-служб в функции интеграции.....	843
23.12.1	Переменные сеанса	843
23.12.2	Кэширование файлов	843
23.12.3	Настраиваемое развертывание	844
23.13	Удаленное планирование и экземпляры, выполняемые локально.....	845
23.13.1	Удаленное планирование.....	845
23.13.2	Экземпляры, выполняемые локально.....	847
23.13.3	Совместное использование экземпляров.....	847
23.14	Импорт и перенос тиражированного содержимого.....	848
23.14.1	Импорт тиражированного содержимого.....	849
23.14.2	Импорт тиражированного содержимого и продолжение тиражирования	849
23.14.3	Перенос содержимого из тестовой среды.....	850
23.14.4	Повторное назначение сайта-адресата.....	851
23.15	Оптимальные методы работы.....	851
23.15.1	Текущие ограничения выпуска.....	854
23.15.2	Устранение неисправностей: сообщения об ошибках.....	856

Глава 24	Дополнительные конфигурации для сред ERP.....	859
24.1	Конфигурации для интеграции с SAP NetWeaver.....	859
24.1.1	Интеграция с SAP Netweaver Business Warehouse (BW).....	859
24.2	Настройка для интеграции с JD Edwards.....	909
24.2.1	Настройка единого входа (SSO) для SAP Crystal Reports.....	909
24.2.2	Настройка протокола SSL для интеграции с JD Edwards.....	910
24.3	Настройка для интеграции с PeopleSoft Enterprise.....	912
24.3.1	Настройка единого входа (SSO) для SAP Crystal Reports и PeopleSoft Enterprise.....	912
24.3.2	Настройка соединений по протоколу SSL.....	913
24.3.3	Настройка производительности для систем PeopleSoft.....	915
24.4	Настройка для интеграции с Siebel.....	916
24.4.1	Настройка Siebel для интеграции с платформой SAP BusinessObjects Business Intelligence.....	917
24.4.2	Создание пункта меню "Crystal Reports".....	918
24.4.3	Контекстуальная зависимость.....	919
24.4.4	Настройка единого входа (SSO) для SAP Crystal Reports и Siebel.....	922
24.4.5	Настройка соединений по протоколу SSL.....	922
Глава 25	Управление журналами и их настройка.....	925
25.1	Ведение журнала трассировок компонентов.....	925
25.2	Уровни журнала трассировки.....	925
25.3	Настройка трассировки для серверов.....	926
25.3.1	Настройка уровня журнала в CMC.....	927
25.3.2	Установка уровня журнала для нескольких серверов в CMC.....	927
25.3.3	Настройка серверной трассировки с использованием файла BO_trace.ini.....	928
25.4	Настройка трассировки для веб-приложений.....	930
25.4.1	Настройка уровня журнала трассировки веб-приложения в CMC.....	931
25.4.2	Настройка параметров трассировки с использованием файла BO_trace.ini.....	932
25.5	Настройка трассировки для средства управления обновлением.....	936
25.5.1	Настройка трассировки для средства управления обновлениями.....	937
25.6	Настройка трассировки для клиентских приложений платформы BI.....	937
Глава 26	Интеграция с SAP Solution Manager.....	939
26.1	Обзор интеграции.....	939
26.2	Контрольный список по интеграции SAP Solution Manager.....	939
26.3	Управление регистрацией System Landscape Directory.....	941
26.3.1	Регистрация платформы BI в System Landscape.....	941
26.3.2	Точки запуска SLD.....	942
26.3.3	Ведение журнала SLD-соединения	943

26.4	Управление агентами Solution Management Diagnostics.....	943
26.4.1	Обзор Solution Manager Diagnostics (SMD).....	944
26.4.2	Работа с SMD-агентами.....	944
26.4.3	Учетная запись пользователя SMAdmin.....	944
26.5	Инструментальные средства управления производительностью.....	945
26.5.1	Настройка инструментов мониторинга производительности для платформы BI.....	945
26.5.2	Настройка инструментальных средств мониторинга производительности для платформы BI.....	946
26.5.3	Настройка конфигурации производительности для веб-уровня.....	947
26.5.4	Файлы журнала настройки конфигурации	947
26.6	Трассировка с использованием SAP Passport.....	948
Глава 27	Администрирование в командной строке.....	949
27.1	Скрипты UNIX.....	949
27.1.1	Утилиты скриптов.....	949
27.1.2	Шаблоны скриптов.....	955
27.1.3	Скрипты, используемые платформой BI.....	955
27.2	Скрипты Windows.....	957
27.2.1	ssm.exe.....	957
27.3	Командные строки сервера.....	960
27.3.1	Обзор командных строк.....	960
27.3.2	Стандартные параметры для всех серверов.....	961
27.3.3	Центральный сервер управления.....	962
27.3.4	Сервер обработки Crystal Reports и кэш-сервер Crystal Reports.....	965
27.3.5	Сервер обработки и кэш-сервер Dashboards.....	966
27.3.6	Серверы заданий.....	967
27.3.7	Адаптивный сервер обработки.....	968
27.3.8	Сервер приложений отчетов.....	969
27.3.9	Сервер обработки Web Intelligence.....	971
27.3.10	Серверы репозитория входящих и исходящих файлов.....	972
27.3.11	Сервер событий.....	974
Глава 28	Repository Diagnostic Tool.....	977
28.1	Обзор инструмента Repository Diagnostic Tool.....	977
28.2	Использование Repository Diagnostic Tool.....	978
28.2.1	Использование Repository Diagnostic Tool.....	978
28.2.2	Параметры Repository Diagnostic Tool.....	979
28.3	Несоответствия между CMS и FRS.....	986
28.4	Несоответствия в метаданных CMS.....	988

Глава 29	Приложение "Права".....995
29.1	О приложении "Права".....995
29.2	Общие права.....995
29.3	Права для определенных типов объектов.....998
29.3.1	Права доступа к папке.....998
29.3.2	Категории.....998
29.3.3	Документы Desktop Intelligence.....999
29.3.4	Примечания.....1001
29.3.5	Отчеты Crystal.....1002
29.3.6	Документы Web Intelligence.....1002
29.3.7	Пользователи и группы.....1004
29.3.8	Уровни доступа.....1006
29.3.9	Права юниверсов (.unv).....1006
29.3.10	Права юниверсов (.unx).....1008
29.3.11	Уровни доступа к объектам для юниверсов.....1010
29.3.12	Права соединений.....1011
29.3.13	Приложения.....1013
 Глава 30	 Приложение "Свойства серверов".....1031
30.1	О приложении "Свойства серверов".....1031
30.1.1	Общие свойства сервера.....1031
30.1.2	Свойства основных служб.....1034
30.1.3	Свойства служб соединения.....1054
30.1.4	Свойства служб Crystal Reports.....1060
30.1.5	Свойства служб Analysis.....1071
30.1.6	Свойства служб объединения данных.....1072
30.1.7	Свойства служб Web Intelligence.....1073
30.1.8	Свойства служб Dashboards.....1085
 Глава 31	 Приложение "Показатели сервера".....1089
31.1	О приложении "Показатели сервера".....1089
31.1.1	Общие показатели сервера1090
31.1.2	Показатели центрального сервера управления.....1092
31.1.3	Показатели сервера соединений.....1097
31.1.4	Показатели сервера событий.....1097
31.1.5	Показатели сервера репозитория файлов.....1098
31.1.6	Показатели адаптивного сервера обработки.....1099
31.1.7	Показатели сервера контейнера веб-приложений.....1105
31.1.8	Показатели адаптивного сервера заданий.....1106

31.1.9	Показатели Crystal Reports Server.....	1108
31.1.10	Показатели сервера Web Intelligence.....	1112
31.1.11	Показатели сервера Dashboards.....	1113
Глава 32	Приложение заполнителя сервера и узла.....	1117
32.1	Заполнители сервера и узлов.....	1117
Глава 33	Приложение выполнения аудита схемы склада данных.....	1127
33.1	Обзор.....	1127
33.2	Диаграмма схемы.....	1127
33.3	Таблицы аудита склада данных.....	1127
Глава 34	Приложение "Мониторинг схемы базы данных".....	1139
34.1	Схема базы данных тенденций.....	1139
Глава 35	Приложение "Рабочая таблица системной копии".....	1143
35.1	Рабочая таблица системной копии.....	1143
Приложение А	Дополнительная информация.....	1145
Указатель		1149

История документа

В следующей таблице описываются наиболее важные изменения документа.

Версия	Дата	Описание
Платформа SAP BusinessObjects Business Intelligence 4.1	Май 2013 г.	Первый выпуск документа.

Начало работы

2.1 0 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*.

2.1.1 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.

2.1.2 0 платформе Business Intelligence

Платформа SAP BusinessObjects Business Intelligence (BI) – это гибкое и масштабируемое решение, предназначенное для составления интерактивных отчетов для конечных пользователей в любом

сетевом приложении в интра- и экстрасети, в Интернете и на корпоративном портале. 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. 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.

2.1.3 Переменные

В настоящем руководстве используются перечисленные ниже переменные.

Переменная	Описание
<code><INSTALLDIR></code>	Каталог, в котором установлена платформа BI. На компьютере под управлением Windows каталог по умолчанию – <code>C:\Program Files (x86)\SAP BusinessObjects</code> .
<code><PLATFORM64DIR></code>	Имя операционной системы Unix. Допустимы следующие значения: <ul style="list-style-type: none"> • <code>aix_rs6000_64</code> • <code>linux_x64</code> • <code>solaris_sparcv9</code> • <code>hpux_ia64</code>
<code><SCRIPTDIR></code>	Каталог, где расположены скрипты администрирования платформы BI. На компьютере под управлением ОС Windows это каталог <code><INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts</code> . На компьютере под управлением Unix это каталог <code><INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM64DIR>/scripts</code> .

2.2 Начало работы

2.2.1 Основные понятия

2.2.1.1 Службы и серверы

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 Web Intelligence является подсистемой, выполняемой на адаптивном сервере заданий.

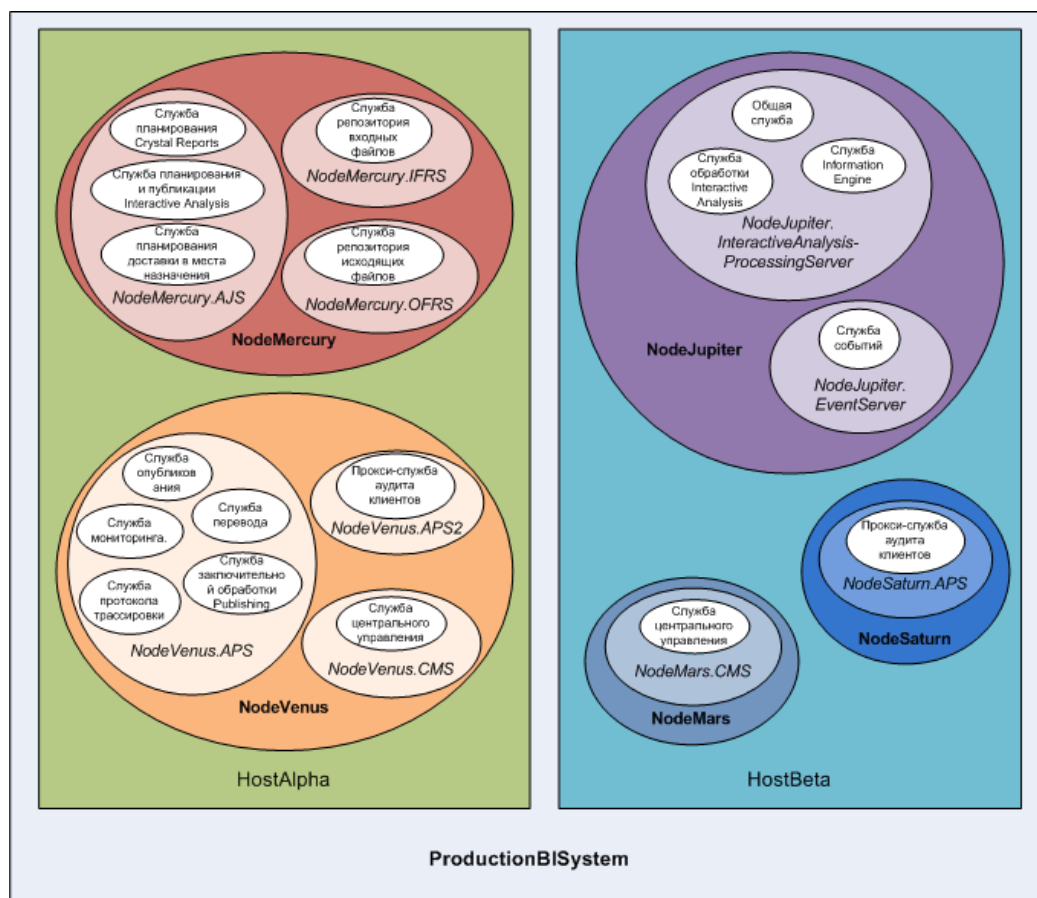
Термином "сервер" обозначается процесс уровня операционной системы (в некоторых системах он носит название "демон"), в котором размещаются одна или несколько служб. В качестве примера подобного сервера можно привести центральный сервер управления (CMS) и сервер адаптивной обработки. Сервер запускается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

Узел – это набор серверов платформы BI, работающих на одном хосте и управляемых одним агентом Server Intelligence Agent (SIA). 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).

Службы, серверы, узлы и хосты

На следующей диаграмме показана возможная установка платформы BI. В фактической установке число хостов, узлов, серверов и служб, а также типы серверов и служб, могут 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. Наличие CMS на двух компьютерах обеспечивает возможности балансировки нагрузки, отказоустойчивость и снижение рисков.
 - NodeJupiter содержит сервер обработки Web Intelligence (NodeJupiter.Web Intelligence) со службой предоставления отчетности Web Intelligence и сервер событий (NodeJupiter.EventServer) для мониторинга отчетов для файлов.

- NodeSaturn содержит адаптивный сервер обработки (NodeSaturn.APS) со службой предоставления аудита клиентов.

2.2.1.2 серверная аналитика

Server Intelligence – это основной компонент платформы Business Intelligence. Изменения процессов сервера, применяемые в Central Management Console (CMC), распространяются на соответствующие серверные объекты CMS. Server Intelligence Agent (SIA) используется для автоматического перезапуска или завершения работы сервера при возникновении неожиданной ситуации, а также позволяет администраторам управлять узлами.

CMS архивирует 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. SIA периодически запрашивает в CMS информацию об управляемых серверах, поэтому имеет сведения о необходимых серверах состояния и требуемых действиях.

Примечание:

На одном компьютере может находиться несколько узлов, и эти узлы могут располагаться в одном кластере платформы BI или в разных кластерах.

См. также

- [Серверы, хосты и кластеры](#)

2.2.2 Основные инструменты администрирования

2.2.2.1 Мастер настройки системы

Мастер настройки системы – это средство, которое можно использовать для быстрой и простой настройки развертывания платформы BI. Мастер предоставляет пошаговые инструкции по работе с основными функциями настройки, позволяющими обеспечивать функционирование развертывания с учетом основных условий, включая, например, следующие:

- какие серверы должны запускаться автоматически при использовании платформы BI;

- требуется ли оптимизировать развертывание таким образом, чтобы обеспечить максимальную производительность, или необходимо задействовать ограниченное количество аппаратных ресурсов;
- как размещаются системные папки.

По умолчанию настроен автоматический запуск мастера при входе в Central Management Console (CMC), но эту настройку можно изменить в самом мастере. Можно также в любое время запустить мастер из области «Управление» CMC.

2.2.2.2 Central Management Console (CMC)

Central Management Console (CMC) – это веб-средство, которое позволяет выполнять административные задачи (в т. ч. управление пользователями, содержимым и сервером), а также настраивать параметры безопасности. Поскольку CMC является веб-приложением, все вышеупомянутые административные задачи можно выполнять посредством веб-браузера на любом компьютере, который может подключаться к серверу веб-приложений.

Все пользователи могут входить в CMC для изменения предпочтений. Только участники группы "Администраторы" могут изменять параметры управления, если другим пользователям явно не предоставлены права на эти действия. В CMC можно назначить роли для предоставления пользователям полномочий на выполнение второстепенных задач администрирования (например, на управление пользователями в группе или управление отчетами в папках, которые относятся к данному отделу).

2.2.2.3 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 ОС Unix с помощью командного сценария CCM (`ccm.sh`) можно управлять серверами из командной строки.

CCM используется для создания и настройки узлов, а также для запуска и остановки сервера веб-приложений, если это стандартный сервер веб-приложений Tomcat, включенный в комплект. 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.

2.2.2.4 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.

2.2.2.5 Средство управления обновлением

Средство управления обновлением (ранее мастер импорта) устанавливается как часть платформы SAP BusinessObjects Business Intelligence 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 события, группы серверов, объекты репозитория и календари.

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

2.2.3 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 \(CMC\)](#)

2.2.3.1 Планирование или выполнение первого развертывания системы

Если вы планируете или осуществляете первое развертывание платформы BI, рекомендуется изучить следующие разделы данного руководства:

- Для ознакомления с компонентами платформы BI см. «Обзор архитектуры».
- «Взаимодействие между компонентами платформы BI»
- «Обзор систем безопасности»
- Если планируется использование сторонней аутентификации, см. раздел «Параметры аутентификации в платформе BI»
- После установки ознакомьтесь с разделом «Работа с областью управления серверами в среде СМС»

Дополнительные сведения об установке платформы BI см. в *руководстве по установке платформы Business Intelligence*. Чтобы оценить текущие потребности и разработать наиболее подходящую архитектуру развертывания, см. *Руководство по планированию развертывания платформы Business Intelligence*.

См. также

- [Обзорная информация по архитектуре](#)
- [Взаимодействие между компонентами платформы BI](#)
- [Обзор вопросов безопасности](#)
- [Параметры аутентификации платформы BI](#)
- [Работа с областью управления СМС "Серверы"](#)

2.2.3.2 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

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

2.2.3.3 Повышение производительности системы

Если необходимо оценить производительность системы и отрегулировать ее в целях максимальной оптимизации использования ресурсов, ознакомьтесь со следующими разделами:

- Если требуется осуществлять наблюдение за имеющейся системой, ознакомьтесь с разделом «Сведения о мониторинге».
- Для получения инструкций о выполнении повседневных процедур и задач обслуживания для работы с серверами в среде СМС, ознакомьтесь с разделом «Работа с областью управления серверами в среде СМС».

См. также

- [О приложении мониторинга](#)
- [Работа с областью управления СМС "Серверы"](#)

2.2.3.4 Работа с объектами в СМС

Объект — это документ или файл, созданный в платформе BI или другом программном обеспечении, который хранится и управляется в репозитории платформы BI. 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

3.1 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.

Примечание:

Списки поддерживаемых платформ, языков, баз данных, серверов веб-приложений, веб-серверов и других систем, поддерживаемых в данном выпуске, см. в *матрице доступности продуктов* (поддерживаемые платформы/PAR), доступной в разделе SAP BusinessObjects портала поддержки SAP по адресу <https://service.sap.com/bosap-support>.

Платформа Business Intelligence (BI) 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 BI 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 BI:
 - Web Intelligence Rich Client
 - Диспетчер Business View
 - Средство преобразования отчетов
 - Средство создания юниверсов
 - Query as a Web Service
 - Средство дизайна информации (ранее "Дизайнер информации")
 - Средство управления переводами (ранее "Диспетчер переводов")
 - Виджеты (ранее BI Widgets)

- Клиенты, доступные отдельно:
 - SAP Crystal Reports
 - SAP BusinessObjects Dashboards (панель Xcelsius)
 - SAP BusinessObjects Analysis (панель Voyager)
 - Рабочие пространства BI (панель Dashboard Builder)

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

- Средства просмотра отчетов
- Central Management Console (CMC)
- Central Configuration Manager (CCM)
- Средство диагностики репозитория (RDT)
- Средство администрирования объединения данных
- Средство управления обновлением (панель Мастер импорта)
- Средство создания юниверсов (панель Universe Designer)
- SAP BusinessObjects Mobile

Для обеспечения гибкости, надежности и расширяемости компоненты платформы BI можно установить на один или несколько компьютеров. Две различные версии платформы BI можно установить одновременно на один компьютер, хотя такая конфигурация рекомендуется 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 центрального сервера управления (CMS).

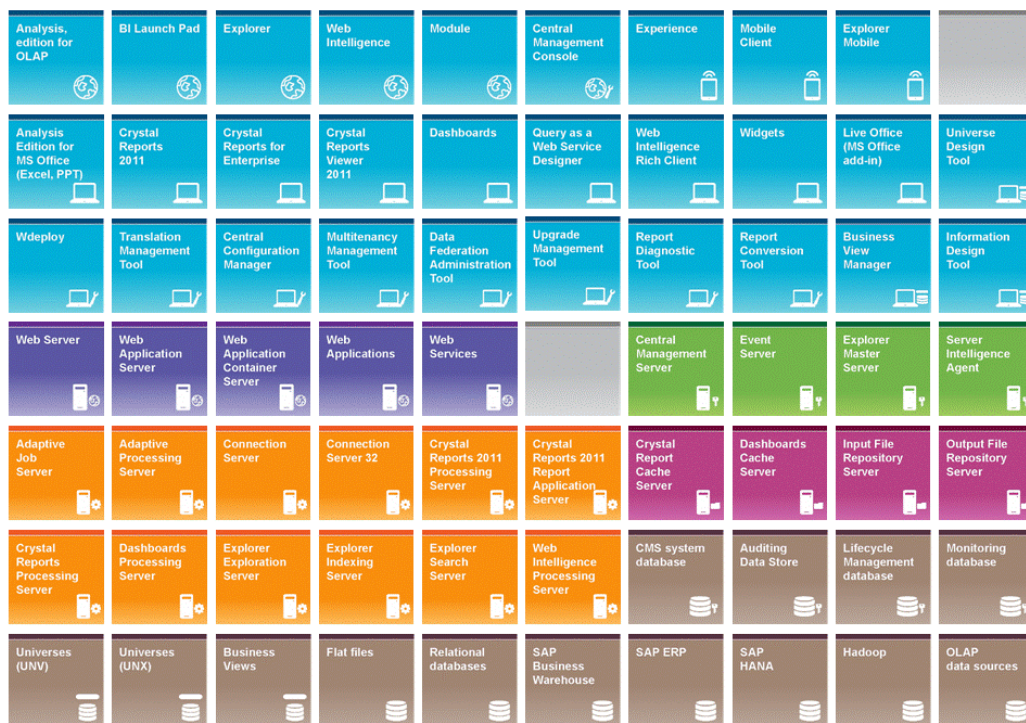
3.1.1 Диаграмма компонентов

Платформа SAP BusinessObjects Business Intelligence является платформой Business Intelligence (BI), которая 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. На следующем рисунке показаны компоненты платформы BI, в том числе серверы и средства клиента, а также дополнительные аналитические продукты, компоненты веб-приложений и базы данных, которые могут входить в состав среды платформы BI.

Совет:

Более подробное представление всех компонентов и серверов платформы BI можно получить с помощью [Interactive architecture diagram](#) в SAP Community Network.

SAP BusinessObjects Business Intelligence Platform 4.0



Платформа BI предоставляет данные в базы данных организации из соединения, доступного 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 BI – самодостаточная система, которая может существовать на одном компьютере (например, как небольшая среда разработки или предварительных производственных испытаний) или в группе нескольких компьютеров, на которых запущены различные компоненты (например, как крупномасштабная производственная среда).

3.1.2 Уровни архитектуры

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

Уровень клиента

Уровень клиента содержит все настольные приложения клиента, которые взаимодействуют с платформой SAP BusinessObjects Business Intelligence, и обеспечивает различные возможности создания отчетности, анализа и администрирования. Примерами является Central Configuration Manager (программа установки платформы BI), средство дизайна информации (программа установки клиентских средств платформы BI) и средство SAP Crystal Reports 2011 (доступное и установленное отдельно).

Веб-уровень

Веб-уровень 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 СМС и стартовая панель BI.

Веб-уровень 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.

Уровень управления

Уровень управления (уровень обработки данных) координирует и контролирует все компоненты, составляющие платформу SAP BusinessObjects Business Intelligence. Он состоит из центрального сервера управления (CMS) и сервера событий, а также связанных служб. 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 уровне хранения.

Уровень хранения

Уровень 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.

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

Уровень обработки

На уровне обработки анализируются данные и составляются отчеты. Это единственный уровень, который обращается к базам данных, содержащим данные отчетов. Этот уровень состоит из адаптивного сервера заданий, сервера соединений (32-разрядный и 64-разрядный) и серверов обработки (например, адаптивного сервера обработки и сервера обработки Crystal Reports).

Уровень данных

Уровень данных состоит из серверов базы данных, на которых находится база данных системы CMS и хранилище данных аудита. Он также состоит из серверов баз данных, содержащих реляционные, OLAP или другие типы данных для приложений отчетности и аналитики.

3.1.3 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 продуктах SAP BusinessObjects Business Intelligence Suite. 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 (например, сведений о пользователе, сервере, папке, документе, конфигурации 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.

3.1.4 Серверы, хосты и кластеры

Платформа SAP BusinessObjects Business Intelligence состоит из коллекций серверов, выполняющихся на одном или нескольких хостах. Небольшие установки (такие как тестовые системы или системы разработки) могут использовать единственный хост для сервера веб-приложений, сервера базы данных и всех серверов платформы BI.

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

В крупных установках несколько хостов серверов платформы BI 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 BI, что обеспечивает наличие достаточных ресурсов для обработки запросов от клиентов.

Преимущества использования нескольких серверов:

- Повышение производительности

На нескольких хостах сервера платформы BI обработка очереди данных отчетности ведется быстрее, чем на одном хосте сервера платформы BI.

- 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.

3.1.5 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.

Подробный список поддерживаемых серверов веб-приложений можно найти в документе *Поддерживаемые платформы/PAR*, доступном по адресу: <https://service.sap.com/bosap-support>.

Если сервер веб-приложений для платформы BI отсутствует, программа установки может автоматически установить и настроить сервер веб-приложений Tomcat. 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 BI и сервера веб-приложений на одном хосте в производственной среде может привести к снижению производительности.

3.1.5.1 Сервер 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 "Сервер контейнеров веб-приложений" (WACS).

WACS представляет собой сервер платформы SAP BusinessObjects Business Intelligence, который позволяет запускать веб-приложения платформы SAP BusinessObjects Business Intelligence, такие как консоль CMC, 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 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.

3.1.6 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.

- Пакет SDK веб-службы RESTful платформы SAP BusinessObjects Business Intelligence

Пакет SDK веб-службы RESTful платформы Business Intelligence обеспечивает доступ к платформе BI по протоколу HTTP. Этот пакет SDK используется для входа в платформу BI, обзора репозитория платформы BI, доступа к ресурсам и выполнения базовых функций планирования ресурсов. Для доступа к функциям этого пакета SDK можно создавать приложения на любом языке программирования, поддерживающем протокол HTTP, или использовать средства, поддерживающие запросы HTTP.

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

Внедрение веб-служб на базе протокола SOAP, позволяющих обрабатывать запросы аутентификации и безопасности, осуществлять доступ к документам и отчетам, планирование, публикации и управление серверами.

Веб-службы платформы SAP BusinessObjects Business Intelligence используют стандарты 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.
4. Сохранение сеансов на основе файлов cookie.

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.

- Пакеты SDK драйвера доступа к данным и соединений Java

С помощью этих пакетов SDK можно создавать драйверы базы данных для сервера соединений и управлять соединениями с базами данных.

- Semantic Layer Java SDK

Пакет Semantic Layer Java SDK используется для разработки приложений Java, позволяющих выполнять задачи по администрированию и обеспечению безопасности юниверсов и соединений. Например, можно реализовать службы для публикации юниверса в репозитории или извлечения защищенного соединения из репозитория в рабочее пространство. Это приложение можно встраивать в решения Business Intelligence, которые обеспечивают интеграцию платформы SAP BusinessObjects Business Intelligence, в виде приложений OEM.

- Report Application Server Java SDK и .NET SDK

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.

- Средства просмотра Java и .NET Crystal Reports

Эти средства 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, подсказки, поиск, выделение, экспорт и печать.
- Средство просмотра фрагментов отчета. Это средство позволяет просматривать отдельные компоненты отчета, включая диаграммы, текст и поля.

- Report Engine Java SDK и .NET SDK

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.

Комбинации пакетов SDK обеспечивают использование широкого диапазона функциональных возможностей BI в приложениях. Дополнительные сведения об этих пакетах SDK, в том числе руководства для разработчика и справочники по API-интерфейсу, см. на странице <http://help.sap.com>.

3.1.7 Источники данных

3.1.7.1 Универсы

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.

3.1.7.2 Объекты Business View

Средство Business Views упрощает создание отчетов и взаимодействие, абстрагируя сложность данных для разработчиков отчетов. Business Views помогает разделить соединения с данными, 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.

3.1.8 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 использования с такими методами аутентификации как SAML, X.509, SAP NW SSO и другими методами, поддерживаемыми данным сервером приложений.
- 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

3.1.8.1 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. Кроме того, можно создавать учетные записи пользователей, которые соответствуют каждой из сопоставленных записей внешней системы.

Подключаемые модули безопасности автоматически управляют списками пользователей и групп в системах сторонних производителей. То есть, после сопоставления группы облегченного протокола доступа к каталогу LDAP или Windows Active Directory (AD) с платформой Business Intelligence (BI) в систему на платформе BI могут входить все пользователи, принадлежащие к этой группе. Последующие изменения в членстве в группах сторонних разработчиков распространяются автоматически.

Платформа BI 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 BI или если 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 центральным сервером 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 BI 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.

3.1.8.2 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)
- 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 *Поддерживаемые платформы/PAR*, доступный по адресу <https://service.sap.com/bosap-support>.

Чтобы настроить интеграцию ERP, обратитесь к главе *Дополнительные конфигурации для сред ERP* этого руководства.

3.1.9 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 об SLD см. раздел «Регистрация платформы BI в System Landscape».

- 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 соединения с серверными системами. 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.

3.1.10 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.

3.1.11 Путь обновления

Существует возможность обновления предыдущей версии платформы SAP BusinessObjects Enterprise (например, версии XI 3.x), однако требуется установить платформу SAP BusinessObjects Business Intelligence 4.x, 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*.

3.2 Службы и серверы

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 Web Intelligence является подсистемой, выполняемой на адаптивном сервере заданий.

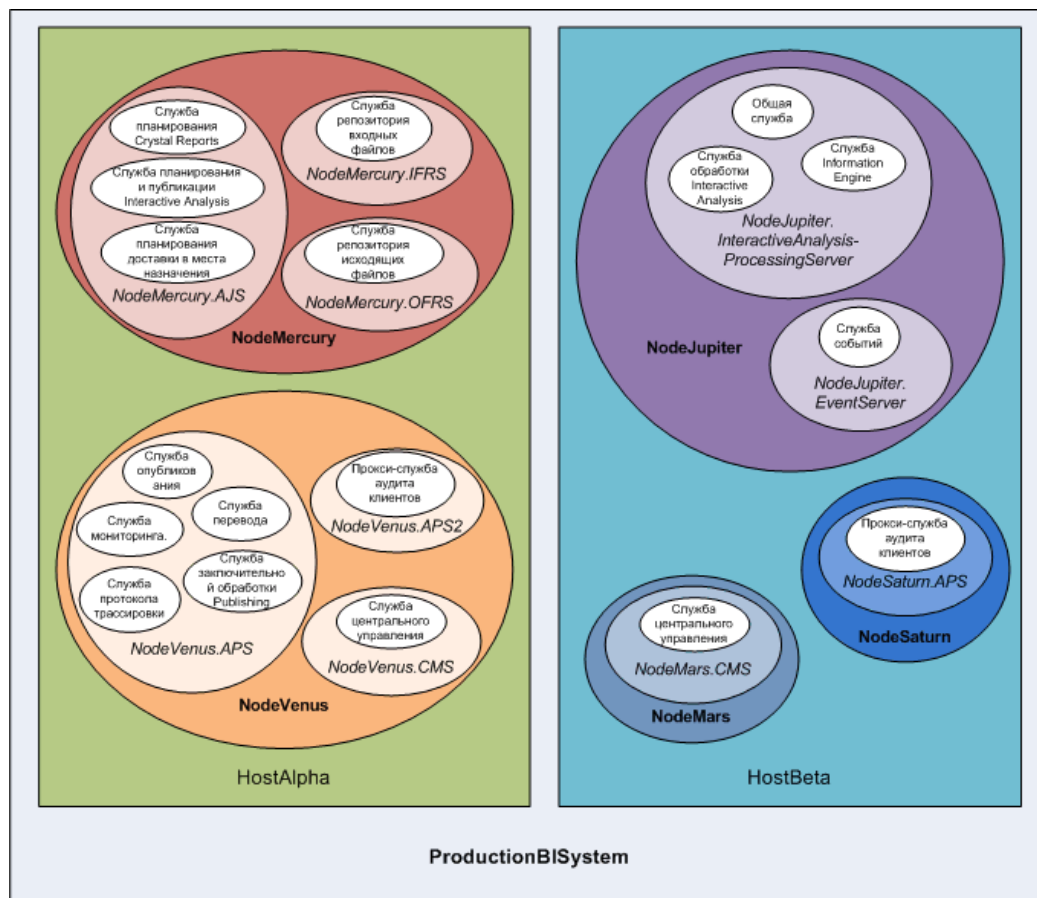
Термином "сервер" обозначается процесс уровня операционной системы (в некоторых системах он носит название "демон"), в котором размещаются одна или несколько служб. В качестве примера подобного сервера можно привести центральный сервер управления (CMS) и сервер адаптивной обработки. Сервер запускается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

Узел – это набор серверов платформы BI, работающих на одном хосте и управляемых одним агентом Server Intelligence Agent (SIA). 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).

Службы, серверы, узлы и хосты

На следующей диаграмме показана возможная установка платформы BI. В фактической установке число хостов, узлов, серверов и служб, а также типы серверов и служб, могут 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. Наличие CMS на двух компьютерах обеспечивает возможности балансировки нагрузки, отказоустойчивость и снижение рисков.

- NodeJupiter содержит сервер обработки Web Intelligence (NodeJupiter.Web Intelligence) со службой предоставления отчетности Web Intelligence и сервер событий (NodeJupiter.EventServer) для мониторинга отчетов для файлов.
- NodeSaturn содержит адаптивный сервер обработки (NodeSaturn.APS) со службой предоставления аудита клиентов.

3.2.1 Изменения сервера с версии XI 3.1

В следующей таблице описываются основные изменения серверов платформы BI с версии XI 3.1. Описанные типы изменений:

- Серверы, имена которых в новой версии изменились, а функциональность осталась прежней.
- Серверы, не предоставляемые в новых версиях
- Общие или связанные серверы, консолидированные в адаптивные серверы.

Например, службы планирования, предоставлявшиеся отдельными серверами заданий в версии XI 3.1, были перемещены на адаптивные серверы заданий в версии 4.0.

- Новые серверы

Таблица 3-1: Изменения серверов

XI 3.1	4.0	4.0 с пакетом компонентов 3	4.1
Сервер соединений [1]	Сервер соединений Сервер соединений 32	Сервер соединений Сервер соединений 32	Сервер соединений Сервер соединений 32
Сервер обработки Crystal Reports	Адаптивный сервер заданий	Адаптивный сервер заданий	Адаптивный сервер заданий
Сервер обработки Crystal Reports	Сервер обработки Crystal Reports 2011 Сервер обработки Crystal Reports (для отчетов SAP Crystal Reports для Enterprise)	Сервер обработки Crystal Reports 2011 Сервер обработки Crystal Reports (для отчетов SAP Crystal Reports для Enterprise)	Сервер обработки Crystal Reports 2011 Сервер обработки Crystal Reports (для отчетов SAP Crystal Reports для Enterprise)
Сервер информационных панелей (Dashboard Builder) [2]	Сервер информационных панелей (рабочее пространство BI)	Недоступно для версии 4.0 с пакетом компонентов 3	Недоступно в версии 4.1

XI 3.1	4.0	4.0 с пакетом компонентов 3	4.1
Сервер аналитики информационных панелей (Dashboard Builder) [2]	Сервер аналитики информационных панелей (рабочие пространства BI)	Недоступно для версии 4.0 с пакетом компонентов 3	Недоступно в версии 4.1
Сервер кэширования Desktop Intelligence [3]	Недоступно для версии 4.0	Недоступно для версии 4.0	Недоступно в версии 4.1 [3]
Сервер заданий Desktop Intelligence [3]	Недоступно для версии 4.0	Недоступно для версии 4.0	Недоступно в версии 4.1 [3]
Сервер обработки Desktop Intelligence [3]	Недоступно для версии 4.0	Недоступно для версии 4.0	Недоступно в версии 4.1 [3]
Сервер заданий для адресатов	Адаптивный сервер заданий	Адаптивный сервер заданий	Адаптивный сервер заданий
Сервер списка значений (LOV)	Сервер обработки Web Intelligence	Сервер обработки Web Intelligence	Сервер обработки Web Intelligence
Сервер многомерного анализа	Сервер адаптивной обработки	Сервер адаптивной обработки	Сервер адаптивной обработки
Сервер выполнения программы	Адаптивный сервер заданий	Адаптивный сервер заданий	Адаптивный сервер заданий
Сервер приложений отчетов (RAS)	Crystal Reports 2011 Report Application Server (RAS)	Crystal Reports 2011 Report Application Server (RAS)	Crystal Reports 2011 Report Application Server (RAS)
Сервер выполнения Web Intelligence	Адаптивный сервер заданий	Адаптивный сервер заданий	Адаптивный сервер заданий
Кэш-сервер Xcelsius [4]	Кэш-сервер Dashboard Design (Xcelsius) [5]	Кэш-сервер Dashboards (Xcelsius)	Кэш-сервер Dashboards (Xcelsius)
Сервер обработки Xcelsius [4]	Сервер обработки Dashboard Design (Xcelsius) [5]	Сервер обработки Dashboards (Xcelsius)	Сервер обработки Dashboards (Xcelsius)

- [1] В версии 4.0 сервер соединений 32 является 32-разрядным и выполняет подключения к источникам данных, которые не поддерживают работу с 64-разрядному компоненту доступа. Сервер соединений является 64-разрядным и выполняет подключения ко всем остальным источникам данных. Для получения дополнительных сведений см. *Руководство по доступу к данным*.

- [2] Сервер информационных панелей и сервер аналитики Dashboards удалены в версии 4.0 с пакетом компонентов 3. Конфигурация сервера не требуется для функционирования рабочих пространств BI (панель Dashboard Builder в версии XI 3.1).
- [3] Desktop Intelligence был недоступен в версии 4.0 и пакетах по обслуживанию для версии 4.0. Клиентское приложение Desktop Intelligence доступно в версии 4.1, но серверы Desktop Intelligence недоступны. Для преобразования отчетов Desktop Intelligence в документы Web Intelligence используется средство преобразования отчетов.
- [4] Службы кэша и обработки Xcelsius были введены в версии XI 3.1 с пакетом компонентов 3 для оптимизации запросов Query as a Web Service в реляционных источниках данных из Xcelsius. Эквивалентные службы кэша и обработки доступны в версии 4.0 с пакетом компонентов 3 в виде кэш-сервера Dashboards и сервера обработки Dashboards.
- [5] Серверы Dashboard Design из версии 4.0 переименованы в информационные панели в версии 4.0 с пакетом компонентов 3, чтобы привести их в соответствие с изменениями названия продукта на SAP BusinessObjects Dashboards.

3.2.2 Службы

При добавлении серверов необходимо включить некоторые службы в адаптивный сервер заданий, например службу планирования доставки в места назначения.

Примечание:

В будущих пакетах могут быть добавлены новые типы служб или серверов.

Служба	Категория службы	Тип сервера	Описание службы
Служба адаптивно-го соединения	Службы соединения	Адаптивный сервер обработки	Предоставляет службы соединений для драйверов на основе Java
Служба планирования обновления аутентификации	Основные службы	Адаптивный сервер заданий	Обеспечивает синхронизацию обновлений подключаемых модулей безопасности сторонних разработчиков.
Веб-служба приложений BEx	Службы Analysis Services	Сервер адаптивной обработки	Обеспечивает интеграцию веб-приложений SAP Business Warehouse (BW) Business Explorer (BEx) и стартовой панели BI.

Служба	Категория службы	Тип сервера	Описание службы
Служба веб-приложения BOE	Основные службы	Сервер контейнера веб-приложений	Предоставляет веб-приложения для WACS: включает СМС, стартовую панель BI и OpenDocument.
Служба Business Process BI	Основные 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.
Central Management Service	Основные службы	Центральный сервер управления	Обеспечивает управление сеансами, пользователями и серверами, а также управление безопасностью (правами доступа и аутентификацией). Для работы кластера в нем должна быть доступна по меньшей мере одна служба Central Management Service.
Прокси-служба аудита клиента	Основные службы	Адаптивный сервер обработки	Осуществляет сбор событий аудита, отправляемых с клиента, и направляет их на сервер CMS.
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	Категория службы	Тип сервера	Описание службы
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	Сервер приложений отчетов (RAS)	Обрабатывает запросы на просмотр и изменение для отчетов Crystal Reports 2011.
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	Категория службы	Тип сервера	Описание службы
Служба доступа к пользовательским данным	Службы Web Intelligence	Сервер адаптивной обработки	Обеспечивает динамическое подключение к источникам данных, для которого не требуется сервер соединений. Эта служба обеспечивает доступ и обновление отчетов, созданных с помощью поставщика персональных данных (например, CSV-файлов). См. раздел <i>Руководство пользователя SAP BusinessObjects Web Intelligence Rich Client</i> для получения дополнительных сведений о создании запроса или обновлении документа, основанного на текстовом файле.
Служба кэша Dashboards	Службы Dashboards	Кэш-сервер Dashboards	Ограничивает число обращений к базе данных из отчетов Dashboards и ускоряет создание отчетов посредством управления кэшем отчетов.
Служба обработки Dashboards	Службы Dashboards	Сервер обработки Dashboards	Принимает и обрабатывает отчеты Dashboards; может объединять данные для разных отчетов, что сокращает число обращений к базе данных.

Служба	Категория службы	Тип сервера	Описание службы
Служба объединения данных	Службы объединения данных	Адаптивный сервер обработки	Запрос и обработка базовых источников данных для юниверса с несколькими источниками
Служба планирования доставки в места назначения	Основные службы	Адаптивный сервер заданий	<p>Выполняет запланированные задания и публикует результаты в заданное местоположение, такое как файловая система, FTP-сервер, адрес электронной почты или папка входящей почты пользователя.</p> <p>Примечание: При добавлении серверов необходимо включить некоторые службы адаптивного сервера заданий, в том числе эту службу.</p>
Служба восстановления документов	Службы Web Intelligence	Сервер адаптивной обработки	Автоматическое сохранение и восстановление документа Web Intelligence
Служба DSL Bridge	Службы Web Intelligence	Сервер адаптивной обработки	Поддержка сеанса многомерного семантического слоя (DSL)
Служба событий	Основные службы	Сервер событий	Отслеживает события файлов на сервере репозитория файлов (FRS) и при необходимости запускает выполнение отчетов.

Служба	Категория службы	Тип сервера	Описание службы
Служба доступа к данным Excel	Службы Web Intelligence	Сервер адаптивной обработки	Поддерживает в качестве источников данных файлы Excel, загруженные в платформу Business Intelligence. См. раздел <i>Руководство пользователя SAP BusinessObjects Web Intelligence Rich Client</i> для получения дополнительных сведений о создании запроса или обновлении документа, основанного на файле Excel.
Служба Information Engine	Службы Web Intelligence	Сервер обработки Web Intelligence	Требуемая служба для обработки документов Web Intelligence
Служба хранилища входящих файлов	Основные службы	Сервер репозитория входящих файлов	Осуществляет ведение объектов опубликованных отчетов и программ, которые могут использоваться для создания новых отчетов, при получении входного файла.
Служба Insight to Action	Основные службы	Адаптивный сервер обработки	Обеспечивает вызов действий и поддержку RRI.
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	Категория службы	Тип сервера	Описание службы
Служба управления жизненным циклом	Службы управления жизненным циклом	Адаптивный сервер обработки	Корневая служба управления жизненным циклом
Служба мониторинга	Основные 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 (панель Voyager).
Служба прямого соединения	Службы соединения	Сервер соединений	Предоставляет службы прямого соединения для 64-разрядной архитектуры
Служба прямого соединения (32-битная)	Службы соединения	Сервер соединений	Предоставляет службы прямого соединения для 32-разрядной архитектуры
Служба хранилища выходных файлов	Основные службы	Сервер репозитория выходных файлов	Осуществляет сбор готовых документов
Служба планирования поиска по платформе	Основные службы	Адаптивный сервер заданий	Выполняет запланированный поиск для индексации всего содержимого в репозитории CMS
Служба поиска по платформе	Основные службы	Адаптивный сервер обработки	Обеспечивает функциональность поиска для платформы BI

Служба	Категория службы	Тип сервера	Описание службы
Служба планирования зонда	Основные службы	Адаптивный сервер заданий	Предоставляет запланированные задания зонда и публикует результаты в заданном выходном местоположении
Служба планирования программ	Основные службы	Адаптивный сервер заданий	Выполняет программы, запланированные для выполнения в заданное время.
Служба планирования публикаций	Основные службы	Адаптивный сервер заданий	Выполняет запланированные задания публикации и публикует результаты в заданном выходном местоположении.
Служба заключительной обработки публикаций	Основные службы	Адаптивный сервер обработки	Выполняет действия с отчетами после их завершения, например отправку отчета в конкретное выходное местоположение.
Служба публикации	Основные службы	Адаптивный сервер обработки	Осуществляет координацию со службой заключительной обработки публикаций и целевой службой заданий для публикации отчетов в заданном выходном местоположении, например, в файловой системе, на FTP-ресурсе, в электронной почте или в ящике входящих сообщений пользователя.
Служба Rebean	Службы Web Intelligence	Адаптивный сервер обработки	Пакет SDK, используемый приложениями Web Intelligence и Explorer.

Служба	Категория службы	Тип сервера	Описание службы
Служба тиражирования	Основные службы	Адаптивный сервер заданий	Выполняет запланированные задания объединения для репликации содержимого между объединенными узлами.
Веб-служба RESTful	Основные службы	Сервер контейнера веб-приложений (WACS)	Обеспечивает обработку сеансов для запросов веб-служб RESTful.
Служба планирования запросов безопасности	Основные службы	Адаптивный сервер заданий	Выполняет запланированные задания запросов безопасности
Служба маркера безопасности	Основные службы	Адаптивный сервер обработки	Поддержка единого входа для SAP
Служба преобразований	Основные 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	Адаптивный сервер обработки	Служба Common Visualization Object Model, используемая приложением Web Intelligence

Служба	Категория службы	Тип сервера	Описание службы
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 обработки Web Intelligence	Службы Web Intelligence	Сервер обработки Web Intelligence	Принимает и обрабатывает документы Web Intelligence
Служба планирования Web Intelligence	Службы Web Intelligence	Адаптивный сервер заданий	Обеспечивает поддержку запланированных заданий Web Intelligence
Пакет SDK для веб-служб и QaaWS	Основные службы	Сервер контейнера веб-приложений	Веб-службы на WACS

3.2.3 Категории служб

Примечание:

В будущих пакетах могут быть добавлены новые типы служб или серверов.

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 прямого соединения	Сервер соединений
Службы соединения	Служба прямого соединения (32-битная)	Сервер соединений
Основные службы	Служба планирования обновления аутентификации	Адаптивный сервер заданий

Категория службы	Служба	Тип сервера
Основные службы	Central Management Service	Центральный сервер управления
Основные службы	Прокси-служба аудита клиента	Адаптивный сервер обработки
Основные службы	Служба Dashboards	Сервер Dashboards
Основные службы	Служба настройки мест назначения	Адаптивный сервер заданий
Основные службы	Служба планирования доставки в места назначения	Адаптивный сервер заданий
Основные службы	Служба событий	Сервер событий
Основные службы	Служба Insight to Action	Адаптивный сервер обработки
Основные службы	Служба хранилища входящих файлов	Сервер репозитория входящих файлов
Основные службы	Служба мониторинга	Адаптивный сервер обработки
Основные службы	Служба хранилища выходных файлов	Сервер репозитория выходных файлов
Основные службы	Служба планирования поиска по платформе	Адаптивный сервер заданий
Основные службы	Служба поиска по платформе	Адаптивный сервер обработки
Основные службы	Служба планирования зонда	Адаптивный сервер заданий
Основные службы	Служба планирования программ	Адаптивный сервер заданий
Основные службы	Служба планирования публикаций	Адаптивный сервер заданий
Основные службы	Служба заключительной обработки публикаций	Адаптивный сервер обработки
Основные службы	Служба публикации	Адаптивный сервер обработки
Основные службы	Служба тиражирования	Адаптивный сервер заданий
Основные службы	Веб-служба RESTful	Сервер контейнера веб-приложений
Основные службы	Служба планирования запросов безопасности	Адаптивный сервер заданий

Категория службы	Служба	Тип сервера
Основные службы	Служба маркера безопасности	Адаптивный сервер обработки
Основные службы	Служба единого входа	Центральный сервер управления, сервер соединений, сервер обработки Crystal Reports, RAS, сервер обработки Dashboards и сервер обработки Web Intelligence
Основные службы	Служба протокола трассировки	Любой сервер
Основные службы	Служба преобразований	Адаптивный сервер обработки
Основные службы	Служба планирования импорта пользователей и групп	Адаптивный сервер заданий
Основные службы	Служба контейнера веб-приложений	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
Службы Crystal Reports	Служба просмотра и изменения Crystal Reports 2011	Сервер приложений отчетов (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 Dashboards	Служба кэша Dashboards	Кэш-сервер Dashboards
Службы Dashboards	Служба обработки Dashboards	Сервер обработки Dashboards
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

Категория службы	Служба	Тип сервера
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 доступа к пользовательским данным	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 доступа к данным Excel	Адаптивный сервер обработки
Службы Web Intelligence	Служба Information Engine	Сервер обработки Web Intelligence
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
Службы Web Intelligence	Основная служба Web Intelligence	Сервер обработки Web Intelligence
Службы Web Intelligence	Служба мониторинга Web Intelligence	Адаптивный сервер обработки
Службы Web Intelligence	Служба обработки Web Intelligence	Сервер обработки Web Intelligence
Службы Web Intelligence	Служба планирования Web Intelligence	Адаптивный сервер заданий

3.2.4 Типы серверов

Звездочка рядом с именем службы указывает на вторичность службы. Некоторые вторичные службы создаются автоматически. Другие вторичные службы необходимо включать после выбора первичной службы, от которой зависит вторичная служба.

Примечание:

В будущих пакетах могут быть добавлены новые типы служб или серверов.

Тип сервера	Служба	Категория службы
Любой сервер	Служба протокола трассировки	Основные службы
Адаптивный сервер заданий	Служба планирования обновления аутентификации	Основные 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 настройки мест назначения	Основные службы
Адаптивный сервер заданий	Служба планирования доставки в места назначения	Основные службы
Адаптивный сервер заданий	Служба планирования управления жизненным циклом	Службы управления жизненным циклом
Адаптивный сервер заданий	Служба планирования поиска по платформе	Основные службы
Адаптивный сервер заданий	Служба планирования зонда	Основные службы
Адаптивный сервер заданий	Служба планирования программ	Основные службы
Адаптивный сервер заданий	Служба планирования публикаций	Основные службы
Адаптивный сервер заданий	Служба тиражирования	Основные службы
Адаптивный сервер заданий	Служба планирования запросов безопасности	Основные службы
Адаптивный сервер заданий	Служба планирования импорта пользователей и групп	Основные 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

Тип сервера	Служба	Категория службы
Адаптивный сервер обработки	Веб-служба приложений BEx	Службы Analysis Services
Адаптивный сервер обработки	Прокси-служба аудита клиента	Основные службы
Адаптивный сервер обработки	Служба доступа к пользовательским данным	Службы Web Intelligence
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 Web Intelligence
Адаптивный сервер обработки	Служба Insight to Action	Основные службы
Адаптивный сервер обработки	Служба ClearCase управления жизненным циклом	Службы управления жизненным циклом
Адаптивный сервер обработки	Служба управления жизненным циклом	Службы управления жизненным циклом
Адаптивный сервер обработки	Служба мониторинга	Основные службы
Адаптивный сервер обработки	Служба многомерного анализа	Службы Analysis Services
Адаптивный сервер обработки	Служба поиска по платформе	Основные службы
Адаптивный сервер обработки	Служба заключительной обработки публикаций	Основные службы
Адаптивный сервер обработки	Служба публикации	Основные службы
Адаптивный сервер обработки	Служба Rebean	Службы Web Intelligence
Адаптивный сервер обработки	Служба маркера безопасности	Основные службы
Адаптивный сервер обработки	Служба преобразований	Основные службы
Адаптивный сервер обработки	Служба Visual Difference	Службы управления жизненным циклом
Адаптивный сервер обработки	Служба визуализации	Службы Web Intelligence
Адаптивный сервер обработки	Служба мониторинга Web Intelligence	Службы Web Intelligence

Тип сервера	Служба	Категория службы
Центральный сервер управления	Central Management Service	Основные службы
Центральный сервер управления	Служба единого входа	Основные службы
Сервер соединений	Служба прямого соединения	Службы соединения
Сервер соединений	Служба прямого соединения (32-битная)	Службы соединения
Сервер соединений	Служба единого входа	Основные службы
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 обработки Crystal Reports	Служба единого входа	Основные службы
Кэш-сервер Dashboards	Служба кэша Dashboards	Службы Dashboards
Сервер обработки Dashboards	Служба обработки Dashboards	Службы Dashboards
Сервер обработки Dashboards	Служба единого входа	Основные службы
Сервер Dashboards	Служба Dashboards	Основные службы
Сервер событий	Служба событий	Основные службы
Сервер репозитория входящих файлов	Служба хранилища входящих файлов	Основные службы
Сервер репозитория выходных файлов	Служба хранилища выходных файлов	Основные службы
Сервер приложений отчетов (RAS)	Служба просмотра и изменения Crystal Reports 2011	Службы Crystal Reports
RAS	Служба единого входа	Основные службы
Сервер контейнера веб-приложений	Веб-служба RESTful	Основные службы
Сервер контейнера веб-приложений	Служба контейнера веб-приложений	Основные службы

Тип сервера	Служба	Категория службы
Сервер обработки Web Intelligence	Служба Information Engine	Службы Web Intelligence
Сервер обработки Web Intelligence	Служба единого входа	Основные службы
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

Тип сервера	Служба	Категория службы
Адаптивный сервер заданий	Служба планирования обновления аутентификации	Основные 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	Основные службы
Адаптивный сервер заданий	Служба планирования управления жизненным циклом	Службы управления жизненным циклом
Адаптивный сервер заданий	Служба планирования поиска по платформе	Основные службы
Адаптивный сервер заданий	Служба планирования зонда	Основные службы
Адаптивный сервер заданий	Служба планирования программ	Основные службы
Адаптивный сервер заданий	Служба планирования публикаций	Основные службы
Адаптивный сервер заданий	Служба тиражирования	Основные службы
Адаптивный сервер заданий	Служба планирования запросов безопасности	Основные службы

Тип сервера	Служба	Категория 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	Основные службы
Адаптивный сервер обработки	Служба доступа к пользовательским данным	Службы Web Intelligence
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 Web Intelligence
Адаптивный сервер обработки	Служба Insight to Action	Основные службы
Адаптивный сервер обработки	Служба ClearCase управления жизненным циклом	Службы управления жизненным циклом
Адаптивный сервер обработки	Служба управления жизненным циклом	Службы управления жизненным циклом
Адаптивный сервер обработки	Служба мониторинга	Основные службы
Адаптивный сервер обработки	Служба многомерного анализа	Службы Analysis Services
Адаптивный сервер обработки	Служба поиска по платформе	Основные службы
Адаптивный сервер обработки	Служба заключительной обработки публикаций	Основные службы
Адаптивный сервер обработки	Служба публикации	Основные службы
Адаптивный сервер обработки	Служба Rebean	Службы Web Intelligence
Адаптивный сервер обработки	Служба маркера безопасности	Основные службы

Тип сервера	Служба	Категория службы
Адаптивный сервер обработки	Служба преобразований	Основные службы
Адаптивный сервер обработки	Служба Visual Difference	Службы управления жизненным циклом
Адаптивный сервер обработки	Служба визуализации	Службы Web Intelligence
Центральный сервер управления	Central Management Service	Основные 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
Кэш-сервер Dashboards	Служба кэша Dashboards	Службы Dashboards
Сервер обработки Dashboards	Служба обработки Dashboards	Службы Dashboards
Сервер Dashboards	Служба Dashboards	Основные службы
Сервер событий	Служба событий	Основные службы
Сервер репозитория входящих файлов	Служба хранилища входящих файлов	Основные службы
Сервер репозитория выходных файлов	Служба хранилища выходных файлов	Основные службы
Сервер приложений отчетов (RAS)	Служба просмотра и изменения Crystal Reports 2011	Службы Crystal Reports
Сервер контейнера веб-приложений	Веб-служба RESTful	Основные 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

Тип сервера	Служба	Категория службы
Сервер обработки Web Intelligence	Служба обработки Web Intelligence	Службы Web Intelligence

3.2.5 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	Общий сервер, на котором осуществляется обработка запланированных заданий. При добавлении сервера заданий в систему платформы SAP BusinessObjects Business Intelligence можно настроить на нем обработку отчетов, документов, программ или публикаций, а также отправку результатов в различные места назначения.
Адаптивный сервер обработки	<p>Общий сервер, на котором находятся службы, отвечающие за обработку запросов из различных источников.</p> <p>Программа установки устанавливает один адаптивный сервер обработки в системе хоста. В зависимости от состава установленных компонентов на этом APS может размещаться большое количество служб, в том числе служба мониторинга, служба управления жизненным циклом, Multi-Dimensional analysis service, служба публикации и другие службы.</p> <p>В производственных и тестовых системах рекомендуется создавать дополнительные адаптивные серверы обработки и настраивать их в соответствии с бизнес-требованиями. Подробную информацию см. в разделе Настройка адаптивных серверов обработки для производственных систем.</p>
Центральный сервер управления (CMS)	Обслуживает базу данных со сведениями о системе платформы Business Intelligence (BI) (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 за предоставление клиентам стандартного 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	Описание
Кэш-сервер Dashboards	Перехватывает запросы на отчет, отправленные клиентами на сервер Dashboards. Если кэш-сервер не может обработать запрос с использованием кэшированной страницы отчета, он передает запрос серверу Dashboards, который создает отчет и возвращает результаты. После этого кэш-сервер кэширует страницу отчета для возможного использования в будущем.
Сервер обработки Dashboards	Отвечает на запросы Dashboards 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 событий управляет относящимися к файлам событиями, которые возникают на уровне хранения.
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.

3.3 Клиентские приложения

Взаимодействие с платформой SAP BusinessObjects Business Intelligence осуществляется с помощью приложений для настольных систем двух основных 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 развертыванием платформы SAP BusinessObjects Business Intelligence осуществляется с использованием архитектуры CORBA или CORBA с шифрованием SSL.

Примеры приложений этого типа: SAP Crystal Reports 2011 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 развертывания 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.

3.3.1 Устанавливается вместе со средствами клиента платформы SAP BusinessObjects Business Intelligence

3.3.1.1 Web Intelligence Rich Client

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

Оно предоставляет пользователям доступ к данным через юниверсы (.unv и .unx), запросы BEx или другие источники при использовании понятных бизнес-терминов в интерфейсе с функцией перетаскивания. Рабочие процессы позволяют анализировать очень широкие или узкие вопросы, а также ставить уточняющие вопросы на любом этапе рабочего процесса анализа.

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

3.3.1.2 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 соединения с несколькими источниками 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.

3.3.1.3 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.

3.3.1.4 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.

3.3.1.5 Query as a Web Service

Query as a Web Service – 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. Query as a Web Service меняет ситуацию, предоставляя возможность доступа к содержимому Business Intelligence любому пользователю, в распоряжении которого находятся веб-службы.

Query as a Web Service, как и другие веб-службы, поддерживается любым приложением Microsoft Windows. Query as a Web Service построен на базе спецификаций веб-служб W3C SOAP, SDL и XML. Этот инструмент состоит из двух главных компонентов:

- Серверный компонент

В серверном компоненте (входит в состав платформы Business Intelligence) хранится каталог Query as a Web Service, 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, хранящемуся на сервере. Средство клиента обменивается данными с серверными компонентами через веб-службы.

Query as a Web Service позволяет использовать веб-запросы в составе ряда клиентских решений, в том числе:

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

3.3.1.6 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.

3.3.1.7 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 многоязычные юниверсы и позволяет управлять переводом юниверсов, а также других отчетов и аналитических источников в репозитории CMS.

Средство управления переводами

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

3.3.1.8 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.

3.3.1.9 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 Dashboards 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 Dashboards)
- Сохранение режима отображения
- Сохранение состояния контекста данных (только для частей отчета Web Intelligence)
- Ссылки Web Intelligence OpenDocument на подробные отчеты (только документы Web Intelligence)
- Представления с вкладками (только для моделей Dashboards)

3.3.2 Устанавливается вместе с платформой SAP BusinessObjects Business Intelligence

3.3.2.1 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 ОС Unix с помощью командного сценария CCM (`ccm.sh`) можно управлять серверами из командной строки.

CCM используется для создания и настройки узлов, а также для запуска и остановки сервера веб-приложений, если это стандартный сервер веб-приложений Tomcat, включенный в комплект. 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.

3.3.2.2 Средство управления обновлением

Средство управления обновлением (ранее мастер импорта) устанавливается как часть платформы SAP BusinessObjects Business Intelligence 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 события, группы серверов, объекты репозитория и календари.

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

3.3.2.3 Средство преобразования отчетов

Средство преобразования отчетов (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.

3.3.3 Доступно отдельно

3.3.3.1 SAP BusinessObjects Analysis, выпуск для Microsoft Office

SAP BusinessObjects Analysis, выпуск для Microsoft Office, – это альтернатива 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 взаимном влиянии направлений.
- Выявление, анализ, сравнение и прогнозирование критичных бизнес-факторов.
- Использование комплексного диапазона вычислений, связанных с бизнесом и временем.

3.3.3.2 SAP Crystal Reports

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

3.3.3.3 SAP BusinessObjects Dashboards

SAP BusinessObjects Dashboards (панель Xcelsius) представляет собой средство для визуализации данных и создания динамических интерактивных инструментальных 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.

3.3.3.4 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.

3.3.4 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*.

3.3.4.1 Central Management Console (CMC)

Central Management Console (CMC) – это веб-средство, которое позволяет выполнять административные задачи (в т. ч. управление пользователями, содержимым и сервером), а также настраивать параметры безопасности. Поскольку CMC является веб-приложением, все

вышеупомянутые административные задачи можно выполнять посредством веб-браузера на любом компьютере, который может подключаться к серверу веб-приложений.

Все пользователи могут входить в СМС для изменения предпочтений. Только участники группы "Администраторы" могут изменять параметры управления, если другим пользователям явно не предоставлены права на эти действия. В СМС можно назначить роли для предоставления пользователям полномочий на выполнение второстепенных задач администрирования (например, на управление пользователями в группе или управление отчетами в папках, которые относятся к данному отделу).

3.3.4.2 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 позволяет получать доступ к любым типам бизнес-аналитики, взаимодействовать с ними и экспортировать их. Это могут быть отчеты, аналитика, информационные панели и т. д.

Стартовая панель BI позволяет осуществлять:

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

3.3.4.3 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 point and click
- Связывание содержимого между модулями для детализированного анализа данных

Примечание:

Рабочие пространства BI являются неотъемлемой частью приложения стартовой панели BI. В связи с этим, для использования функций рабочих пространств BI необходимо приобрести

лицензию платформы SAP BusinessObjects Business Intelligence, в рамках которой предусматривается использование стартовой панели BI.

3.3.4.4 Средства просмотра отчетов

Каждое средство просмотра отчетов поддерживает одну платформу и один браузер. Предпочтения могут быть заданы на стартовой панели BI и Central Management Console (CMC). Существуют две категории средств просмотра:

- 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. Чтобы выбрать клиентское средство просмотра отчетов, выберите **Настройки > Crystal Reports > Web ActiveX (требуется поддержка ActiveX)** или **Web Java (требуется поддержка Java)**.

- 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 Business Intelligence (BI) и создает страницы DHTML, которые отображаются в веб-браузере. Чтобы выбрать средство просмотра отчетов (DHTML) без ПО промежуточного уровня, выберите **Настройки > Crystal Reports > Web (загрузка из сети не требуется)**

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

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

3.3.4.5 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.

3.3.4.6 SAP BusinessObjects Analysis, версия для 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 максимально упростить анализ данных OLAP.

Примечание:

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

3.3.4.7 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. *Руководство по установке и развертыванию SAP BusinessObjects Mobile*. Для получения сведений об использовании SAP BusinessObjects Mobile см. *Руководство по использованию SAP BusinessObjects Mobile*.

3.4 Рабочие процессы

При выполнении заданий (например, входа в систему, внесения отчета в расписание или просмотра отчета) информация перемещается по системе, и серверы взаимодействуют друг с другом. В следующем разделе изложены принципы выполнения некоторых процессов в платформе BI.

Чтобы просмотреть дополнительные рабочие процессы с помощью наглядных средств, обратитесь к официальным руководствам по продуктам платформы SAP BusinessObjects Business Intelligence 4.x по адресу <http://scn.sap.com/docs/DOC-8292>

3.4.1 Запуск и аутентификация

3.4.1.1 Вход в платформу SAP BusinessObjects Business Intelligence

Данный рабочий процесс описывает вход пользователя в веб-приложение платформы SAP BusinessObjects Business Intelligence из веб-браузера. Этот рабочий процесс применяется к веб-приложениям (например, к стартовой панели BI) и Central Management Console (CMC).

1. Браузер (веб-клиент) отправляет запрос на вход через веб-сервер на сервер веб-приложений, где запущено веб-приложение.
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.
6. 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. Сервер веб-приложений создает следующую веб-страницу для отправки в веб-клиент.

7. Сервер веб-приложений направляет следующую веб-страницу на веб-сервер.
8. Веб-сервер направляет веб-страницу в веб-клиент, где она отображается в браузере пользователя.

3.4.1.2 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 центрального сервера управления (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.

Примечание:

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.

3.4.1.3 Отключение SIA

Server Intelligence Agent (SIA) автоматически прекращает работу при закрытии операционной системы на хосте. SIA также можно остановить вручную в Central Configuration Manager (CCM).

При отключении SIA выполняются следующие шаги.

- 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.

3.4.2 Объекты программ

3.4.2.1 Настройка расписания для программного объекта

Этот рабочий процесс описывает процесс планирования объекта программы для запуска в определенное время из веб-приложения, например из Central Management Console (CMC) или стартовой панели BI.

1. Пользователь отправляет запрос расписания из веб-клиента через веб-сервер на сервер веб-приложений.
2. Сервер веб-приложений интерпретирует 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 сервер CMS.
3. CMS определяет наличие прав на внесение объекта в расписание у пользователя. При наличии соответствующих прав пользователя CMS добавляет новую запись в базу данных системы CMS и экземпляр в список ожидающих расписаний.

4. CMS отправляет на сервер веб-приложения ответ об успешном завершении операции планирования.
5. Сервер веб-приложений создает следующую HTML-страницу и отправляет ее в веб-клиент через веб-сервер.

3.4.2.2 Выполнение запланированного объекта программы

Этот рабочий процесс описывает процесс выполнения запланированных объектов программы в запланированное время. При этом также должен быть запущен настраиваемый сервер заданий и сервер репозитория входных файлов.

Примечание:

Для этого рабочего процесса требуется выполнение CMS, настраиваемого сервера заданий и входящего файлового сервера репозитория.

1. Центральный сервер управления (CMS) проверяет базу данных системы CMS на наличие отчетов SAP Crystal, выполнение которых запланировано на это время.
2. При наступлении заданного времени выполнения задания CMS выполняет поиск службы планирования программ на адаптивном сервере заданий. CMS направляет информацию о задании в службу планирования программ.
3. Служба планирования программ взаимодействует с входящим файловым сервером репозитория (FRS) для получения объекта программы.

Примечание:

Этот этап также требует взаимодействия с CMS для поиска требуемого сервера и объектов.

4. Служба планирования программ запускает программу.
5. Служба планирования программ периодически обновляет на CMS информацию о состоянии выполнения задания. Текущее состояние имеет значение "Обработка".
6. Служба планирования программ отправляет файл журнала на сервер репозитория исходящих файлов. Сервер репозитория исходящих файлов уведомляет службу планирования программ о том, что объект внесен в расписание, путем отправки файла журнала объекта.

Примечание:

Этот этап также требует взаимодействия с CMS для поиска требуемого сервера и объектов.

7. Служба планирования программ обновляет на CMS информацию о состоянии выполнения задания. Текущее состояние имеет значение "Успешно".
8. CMS обновляет статус задания в собственной памяти, а затем записывает сведения об экземпляре объекта в базу данных системы CMS.

3.4.3 Crystal Reports

3.4.3.1 Просмотр кэшированной страницы отчета SAP Crystal

Этот рабочий процесс описывает запрос страницы в отчете SAP Crystal (например, из средства просмотра отчетов на стартовой панели BI), если страница отчета уже существует на кэш-сервере. Этот рабочий процесс применяется для SAP Crystal Reports 2011 и SAP Crystal Reports для Enterprise.

Примечание:

Для этого рабочего процесса необходимо выполнение CMS и сервера кэширования Crystal Reports.

1. Веб-клиент направляет на сервер веб-приложений URL-запрос на просмотр посредством веб-сервера.
2. Сервер веб-приложений интерпретирует данный запрос и определяет, что это запрос на просмотр выбранной страницы отчета. Сервер веб-приложений отправляет запрос на сервер CMS, чтобы убедиться в наличии у пользователя достаточных прав на просмотр отчета.
3. CMS проверяет базу данных системы CMS, чтобы убедиться в наличии у пользователя достаточных прав на просмотр 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 первой страницы отчета (файл `EPF`).
6. Кэш-сервер Crystal Reports определяет наличие запрошенного файла `EPF` в каталоге кэша. В этом примере файл `EPF` найден.
7. Кэш-сервер Crystal Reports возвращает запрашиваемую страницу на сервер веб-приложений.
8. Сервер веб-приложений отправляет страницу через веб-сервер в веб-клиент, в котором эта страница подготавливается к просмотру и отображается.

3.4.3.2 Просмотр некэшированной страницы SAP Crystal Reports 2011

Этот рабочий процесс описывает запрос страницы в отчете SAP Crystal Reports 2011 (например, из средства просмотра отчетов на стартовой панели BI), если страница отчета еще не существует на кэш-сервере.

Примечание:

Для данного рабочего процесса требуется выполнение CMS, сервера кэширования Crystal Reports, сервера обработки Crystal Reports 2011 и исходящего файлового сервера репозитория.

1. Пользователь направляет запрос на просмотр на сервер веб-приложений через веб-сервер.

2. На сервере веб-приложения запрос интерпретируется, определяется как запрос на просмотр выбранной страницы отчета и отправляется на центральный сервер управления (CMS) для проверки наличия у пользователя прав на просмотр отчета.
3. CMS проверяет базу данных системы CMS, чтобы убедиться в наличии у пользователя достаточных прав на просмотр 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 первой страницы отчета (файл EPF).
6. Кэш-сервер Crystal Reports определяет наличие запрошенного файла в каталоге кэша. В этом примере запрошенный файл EPF не найден в каталоге кэша.
7. Кэш-сервер Crystal Reports направляет запрос на сервер обработки Crystal Reports 2011.
8. Сервер обработки Crystal Reports 2011 отправляет запрос исходящему файловому серверу репозитория (FRS) на запрашиваемый экземпляр отчета, и исходящий FRS отправляет этот экземпляр отчета на сервер обработки Crystal Reports 2011.

Примечание:

Этот этап также требует взаимодействия с CMS для поиска требуемого сервера и объектов.

9. Сервер обработки Crystal Reports 2011 открывает данный экземпляр отчета и проверяет отчет на наличие в нем данных.
Сервер обработки Crystal Reports 2011 определяет, что отчет содержит данные, и создает файл EPF запрошенной страницы отчета, не подключаясь к производственной базе данных.
10. Сервер обработки Crystal Reports 2011 направляет страницу EPF на кэш-сервер Crystal Reports.
11. Кэш-сервер Crystal Reports записывает файл EPF в каталог кэша.
12. Кэш-сервер Crystal Reports направляет запрашиваемую страницу на сервер веб-приложений.
13. Сервер веб-приложений отправляет страницу через веб-сервер в веб-клиент, в котором эта страница подготавливается к просмотру и отображается.

3.4.3.3 Просмотр отчета SAP Crystal Reports 2011 по требованию

Этот рабочий процесс описывает процесс запроса страницы отчета SAP Crystal Reports 2011 по требованию для просмотра последних данных, например, из средства просмотра отчетов или со стартовой панели BI.

Примечание:

Для данного рабочего процесса требуется выполнение CMS, сервера кэширования Crystal Reports, сервера обработки Crystal Reports 2011 и входящего файлового сервера репозитория.

1. Пользователь направляет запрос на просмотр на сервер веб-приложений через веб-сервер.
2. Сервер веб-приложений интерпретирует данный запрос и определяет, что это запрос на просмотр выбранной страницы отчета. Сервер веб-приложений отправляет запрос на сервер CMS, чтобы убедиться в наличии у пользователя достаточных прав на просмотр отчета.

3. CMS проверяет базу данных системы CMS, чтобы убедиться в наличии у пользователя достаточных прав на просмотр 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 первой страницы отчета (файл ERF).
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 2011 запрос на создание страницы.
7. Сервер обработки Crystal Reports 2011 запрашивает объект отчета на сервере репозитория входящих файлов FRS. Сервер репозитория входящих файлов направляет копию объекта на сервер обработки Crystal Reports 2011.

Примечание:

Этот этап также требует взаимодействия с CMS для поиска требуемого сервера и объектов.

8. Сервер обработки Crystal Reports 2011 открывает отчет в собственной памяти и проверяет его на наличие данных. В этом примере объект отчета не содержит данных, поэтому сервер обработки Crystal Reports 2011 подключается к источнику данных для получения информации и создания отчета.
9. Сервер обработки Crystal Reports 2011 направляет страницу (файл ERF) на кэш-сервер Crystal Reports. Кэш-сервер Crystal Reports сохраняет копию файла ERF в каталоге кэша для новых запросов на просмотр.
10. Кэш-сервер Crystal Reports направляет страницу на сервер веб-приложений.
11. Сервер веб-приложений отправляет страницу через веб-сервер в веб-клиент, в котором эта страница подготавливается к просмотру и отображается.

3.4.3.4 Установка расписания для отчета SAP Crystal

Этот рабочий процесс описывает процесс планирования объекта отчета SAP Crystal для запуска в определенное время из веб-приложения, например из Central Management Console (CMC) или стартовой панели BI. Этот рабочий процесс применяется для SAP Crystal Reports 2011 и SAP Crystal Reports для Enterprise.

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 центральный сервер управления CMS.

3. CMS определяет наличие прав на внесение объекта в расписание у пользователя. При наличии у пользователя достаточных прав CMS добавляет новую запись в базу данных системы CMS. CMS также добавляет экземпляр в список отложенных расписаний.
4. CMS направляет ответ на сервер веб-приложений с информацией о том, что операция планирования выполнена успешно.
5. Сервер веб-приложений создает следующую HTML-страницу и отправляет ее в веб-клиент через веб-сервер.

3.4.3.5 Выполнение запланированного отчета SAP Crystal Reports 2011

Этот рабочий процесс описывает процесс выполнения запланированного отчета SAP Crystal Reports 2011 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 доступную службу планирования Crystal Reports 2011 на адаптивном сервере заданий (на основе значения **Максимально разрешенное число заданий**, настроенного для каждого из адаптивных серверов). CMS отправляет информацию о задании (идентификатор отчета, формат, место назначения, сведения о входе, параметры и формулы выбора) в службу планирования Crystal Reports 2011.
3. Служба планирования Crystal Reports 2011 обращается к серверу репозитория входящих файлов (FRS) для получения шаблона отчета согласно запрошенному идентификатору отчета.

Примечание:

Этот этап также требует взаимодействия с CMS для поиска требуемого сервера и объектов.

4. Служба планирования Crystal Reports 2011 запускает процесс JobChildserver.
5. Дочерний процесс (JobChildserver) запускает файл `ProcReport.dll` при получении шаблона от сервера репозитория входных файлов. `ProcReport.dll` содержит все параметры, переданные от CMS в службу планирования Crystal Reports 2011.
6. `ProcReport.dll` запускает файл `crpe32.dll`, который обрабатывает отчет в соответствии с переданными параметрами.
7. В ходе обработки отчета в файле `crpe32.dll` выполняется получение записей из источника данных в соответствии с определением в отчете.
8. Служба планирования Crystal Reports 2011 периодически обновляет на CMS информацию о состоянии выполнения задания. Текущее состояние имеет значение "Обработка".
9. После компиляции отчета в память службы планирования Crystal Reports 2011 его можно импортировать в другой формат, например, Portable Document Format (PDF). При экспорте в PDF используется `crxfpdf.dll`.
10. Отчет с сохраненными данными передается в запланированное расположение (например, на адрес электронной почты), а затем отправляется на сервер репозитория исходящих файлов.

Примечание:

Этот этап также требует взаимодействия с CMS для поиска требуемого сервера и объектов.

11. Служба планирования Crystal Reports 2011 обновляет на CMS информацию о состоянии выполнения задания. Текущее состояние имеет значение "Успешно".
12. CMS обновляет статус задания в собственной памяти, а затем записывает сведения об экземпляре объекта в базу данных системы CMS.

3.4.4 Web Intelligence

3.4.4.1 Просмотр документа SAP BusinessObjects Web Intelligence по запросу

Этот рабочий процесс описывает процесс просмотра документа SAP BusinessObjects Web Intelligence по требованию для вывода последних данных, например, из средства просмотра Web Intelligence на стартовой панели BI.

1. Веб-браузер направляет запрос на просмотр на сервер веб-приложений через веб-сервер.
2. Сервер веб-приложений интерпретирует данный запрос и определяет, что это запрос на просмотр документа Web Intelligence. Сервер веб-приложений отправляет запрос на сервер CMS, чтобы убедиться в наличии у пользователя достаточных прав на просмотр документа.
3. CMS проверяет базу данных системы CMS, чтобы убедиться в наличии у пользователя достаточных прав на просмотр документа.
4. CMS направляет на сервер веб-приложений подтверждение наличия у пользователя прав на просмотр документа.
5. Сервер веб-приложений направляет на сервер обработки Web Intelligence запрос на документ.
6. 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 о защите на уровне строк и столбцов.
7. Сервер репозитория входящих файлов направляет на сервер обработки Web Intelligence копию документа и файл юниверса, на котором основан запрашиваемый документ.

Примечание:

Этот этап также требует взаимодействия с CMS для поиска требуемого сервера и объектов.

8. Web Intelligence Report Engine на сервере обработки Web Intelligence открывает документ в памяти и запускает QT.dll и сервер соединений в процессе.
9. Библиотека QT.dll создает, проверяет и повторно создает SQL, а затем подключается к базе данных для выполнения запроса. Сервер соединений использует SQL для получения данных из базы данных для системы отчетов, в которой документ обрабатывается.
10. Сервер обработки Web Intelligence направляет запрошенную страницу документа в пригодном для просмотра формате на сервер веб-приложений.
11. Сервер веб-приложений отправляет документ через веб-сервер в веб-клиент, в котором эта страница подготавливается к просмотру и отображается.

3.4.4.2 Установка расписания для документа SAP BusinessObjects Web Intelligence

Этот рабочий процесс описывает процесс планирования документа SAP BusinessObjects Web Intelligence для запуска в определенное время из веб-приложения, например из Central Management Console (CMC) или стартовой панели BI.

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 центральный сервер управления CMS.
3. CMS определяет наличие прав на внесение объекта в расписание у пользователя. При наличии у пользователя достаточных прав CMS добавляет новую запись в базу данных системы CMS. CMS также добавляет экземпляр в список отложенных расписаний.
4. CMS направляет ответ на сервер веб-приложений с информацией о том, что операция планирования выполнена успешно.
5. Сервер веб-приложений создает следующую HTML-страницу и отправляет ее в веб-клиент через веб-сервер.

3.4.4.3 Выполнение запланированного документа SAP BusinessObjects Web Intelligence

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

1. Центральный сервер управления (CMS) проверяет системную базу данных CMS, чтобы определить наличие запланированного документа Web Intelligence.
2. При наступлении заданного времени выполнения CMS выполняет поиск доступной службы планирования Web Intelligence на адаптивном сервере заданий. CMS направляет запрос на внесение в расписание и все сведения о нем в службу планирования Web Intelligence.
3. Служба планирования Web Intelligence обнаруживает доступный сервер обработки Web Intelligence на основе значения **Максимальное число соединений**, настроенного для каждого сервера обработки Web Intelligence.
4. Сервер обработки Web Intelligence обращается к серверу репозитория входящих файлов (FRS), на котором размещается документ и файл слоя метаданных юниверса, на котором основан этот документ. Сервер обработки Web Intelligence запрашивает данный документ у сервера репозитория входящих файлов. Сервер репозитория входящих файлов обращается

к документу Web Intelligence и к файлу юниверса, на котором он основан, и направляет их на сервер обработки Web Intelligence.

Примечание:

Этот этап также требует взаимодействия с CMS для поиска требуемого сервера и объектов.

5. Документ Web Intelligence размещается во временном каталоге на сервере обработки Web Intelligence. Сервер обработки Web Intelligence открывает документ в памяти, а `QT.dll` создает SQL из юниверса, на котором основан документ. Библиотеки сервера соединений, включенные в сервер обработки Web Intelligence, подключаются к источнику данных. Данные запроса проходят через `QT.dll` в Report Engine сервера обработки Web Intelligence, где происходит обработка документа. Новый экземпляр создан успешно.
6. Сервер обработки Web Intelligence загружает экземпляр документа на сервер репозитория исходящих файлов.

Примечание:

Этот этап также требует взаимодействия с CMS для поиска требуемого сервера и объектов.

7. Сервер обработки Web Intelligence уведомляет службу планирования Web Intelligence на адаптивном сервере заданий о том, 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. Служба планирования 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.

3.4.5 Analysis

3.4.5.1 Просмотр рабочей области SAP BusinessObjects Analysis для OLAP

Этот рабочий процесс описывает запрос на просмотр рабочей области SAP BusinessObjects Analysis (выпуск для OLAP) со стартовой панели BI.

Примечание:

Для этого рабочего процесса требуется выполнение CMS, настраиваемого сервера обработки (с Multi-Dimensional Analysis Service (MDAS)) и входящего файлового сервера репозитория.

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 Multi-Dimensional Analysis Services (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 соответствующую рабочую область Analysis из основного каталога и направляет ее 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.

Мастер настройки системы

4.1 Вводные сведения о мастере настройки системы

После установки платформы SAP BusinessObjects Business Intelligence, вероятно, потребуется выполнить базовую настройку системы после установки, например выбрать шаблон развертывания и продукты SAP BusinessObjects, которые будут использоваться в вашей организации. Чтобы выполнить такую настройку и как можно скорее приступить к работе с платформой BI, запустите «Мастер настройки системы».

Важные преимущества использования мастера:

- Мастер объясняет важнейшие действия по настройке системы и указывает правильную последовательность выполнения этих действий.
- При использовании мастера сводится к минимуму вероятность неверной настройки системы.
- Мастер настраивает указанные пользователем параметры самостоятельно, что значительно ускоряет процесс настройки.

По умолчанию мастер запускается автоматически при входе пользователя в Central Management Console (СМС), однако мастер также можно запустить в области «Управление» этой же консоли. Можно повторно запустить мастер в любой момент и скорректировать конфигурацию. Кроме того, на странице управления «Серверы» на консоли СМС можно дополнительно настроить любые параметры, включая те, которые были настроены с помощью мастера.

Примечание:

- В целях безопасности доступ в мастер имеют только пользователи группы "Администраторы".
- Чтобы не допустить автоматического выполнения мастера, пользователь с правами «администратора» может установить флажок **Не показывать этот мастер, когда запущена СМС** на первой странице мастера.
- Если планируется установка дополнительных компонентов или добавление узлов в развертывание платформы BI, рекомендуется выполнить эти шаги перед запуском мастера настройки системы

4.2 Указание используемых продуктов

Можно упростить настройку серверов платформы BI, указав используемые вашей организацией программные продукты. Чтобы оптимизировать распределение ресурсов, нужно остановить

серверы, поддерживающие функционирование продуктов, которые не используются в организации. Для этого выберите соответствующие продукты на странице «Продукты». Если указаны используемые организацией продукты, мастер запускает все серверы и зависимости, необходимые для работы этих продуктов, а затем настраивает эти серверы и зависимости для автоматического запуска одновременно с запуском платформы BI. Кроме того, сняв флажки напротив неиспользуемых продуктов, можно улучшить показатели времени запуска и использования ресурсов на платформе BI.

Например, если выбрано приложение Crystal Reports, платформа BI автоматически запускает все серверы Crystal Reports и соответствующие зависимости.

Для просмотра списка серверов, которые будут автоматически запущены для конкретного продукта, щелкните значок ? рядом с названием продукта.

Мастер настраивает серверы продуктов следующим образом:

- Если выбран определенный продукт, то после завершения работы мастера запускаются все серверы, связанные с этим продуктом, а также все остальные серверы, необходимые для функционирования этого продукта (так называемые зависимости). Если выбран продукт, серверы продукта запускаются автоматически одновременно с платформой BI. Если на сервере размещены службы нескольких продуктов и выбраны какие-либо из этих продуктов, сервер будет запущен. Обратите внимание, что некоторые службы невыбранных продуктов могут выполняться, если они размещены на одном сервере со службами выбранных продуктов.
- При отмене выбора продукта серверы, используемые этим продуктом, останавливаются, при условии что на этих серверах не расположены службы выбранных продуктов или службы, которые относятся к категории основных служб. Остановленные серверы продуктов настраиваются таким образом, чтобы не происходил их автоматический запуск с платформой BI. Если на сервере размещены службы выбранных и невыбранных продуктов, сервер продолжает работать.
- Отмена выбора определенного продукта также может привести к остановке серверов, не относящихся к продукту, выбор которого был отменен, если на серверах имеются зависимые службы, используемые только отмененным продуктом. Это освобождает системные ресурсы, потому что указанные зависимые серверы больше не нужны.
- Всякий раз когда выделяется используемый продукт или отменяется выделение неиспользуемого продукта, все серверы, на которых размещены службы, относящиеся к категории корневых служб на платформе BI (кроме служб, размещенных на сервере WACS), запускаются автоматически. WACS остается в текущем состоянии.
- Отмена выбора неиспользуемых продуктов не приводит к отмене установки или удалению файлов этих продуктов.

Всякий раз при открытии страницы «Продукты» состояния продуктов на этой странице представляют текущее состояние системы.

Если все серверы продукта запущены, флажок напротив названия этого продукта установлен. Если все серверы продукта остановлены, флажок снят. Если запущены только некоторые серверы продукта, а другие серверы находятся в других состояниях, например остановлены, на странице «Продукты» отображается флажок **Сохранить существующую конфигурацию**, указывающий на то, что система была настроена вне мастера. Можно снять флажок, чтобы использовать мастер для изменения конфигурации.

Примечание:

- На странице «Продукты» отображаются все установленные в кластере продукты. Например, если на машине А установлены продукты П1 и П2, на машине Б – продукты П2 и П3, то на странице «Продукты» показаны продукты П1, П2 и П3. Неустановленные продукты не отображаются на странице «Продукты».
- Чтобы упростить развертывание, конфигурацию с этой страницы не нужно повторно создавать для каждого узла – конфигурация применяется к целому кластеру.
- Если какие-либо настройки были ранее изменены в СМС, в мастере отображается сообщение, информирующее о том, что параметры были изменены вне мастера. Можно сохранить существующую конфигурацию или перезаписать текущие параметры.
- Вносимые в мастере изменения не вступают в силу до тех пор, пока не будет нажата кнопка **Применить** на странице «Просмотр».

Внеся все необходимые изменения, нажмите кнопку **Далее**, чтобы перейти к следующей странице мастера. Кроме того, можно воспользоваться панелью навигации слева, чтобы сразу перейти к любой из страниц, на которых вы уже были.

4.3 Выбор шаблона развертывания

Установка платформы BI по умолчанию представляет собой небольшое по масштабу развертывание, которое подходит для демонстрационной среды на системном оборудовании с ограниченными возможностями. Чтобы подобрать оптимальное оборудование для соответствующего варианта использования (например, подготовка тестовой или рабочей системы) выберите один из предопределенных шаблонов развертывания на странице «Емкость». Эти шаблоны помогут быстро приступить к продуктивной работе с системой платформы BI и сократят продолжительность первоначального развертывания.

Несмотря на то что подходящий шаблон развертывания облегчает первоначальную настройку и является хорошей стартовой точкой, его использование не заменяет обязательные операции по изменению размера и настройке. Для обеспечения оптимальной производительности необходимо скорректировать масштабы системы, следуя руководству по изменению размера: <http://www.sap.com/bisizing>.

Выбор подходящего шаблона развертывания имеет большое значение по нескольким причинам.

- Выбранный шаблон развертывания влияет на возможности системы по обработке запросов. Более масштабное развертывание предоставляет ресурсы для обработки большего числа запросов или более сложных запросов. Однако более крупное развертывание требует больше системных ресурсов.
- Крупномасштабное развертывание не гарантирует более высокую производительность, особенно в условиях отсутствия достаточных аппаратных ресурсов.
- Выбранный шаблон развертывания должен соответствовать потребностям вашего бизнеса и доступным аппаратным ресурсам. Неверный выбор шаблона развертывания (слишком мелкого для потребностей бизнеса или слишком крупного для имеющихся аппаратных ресурсов) может снизить емкость и производительность системы.

- Более крупные шаблоны развертывания обеспечивают повышенное удобство фрагментации: сбой в работе одного продукта вряд ли повлияет на другие. Выберите шаблон, оптимально соответствующий использованию ресурсов (ОЗУ) и производительности. Например, если доступен большой объем ОЗУ, можно выбрать наибольший из поддерживаемых таким объемом ОЗУ шаблон развертывания. Это обеспечит более эффективную фрагментацию системы.

Можно выбрать шаблон развертывания с помощью регулятора, а затем указать в раскрывающемся списке доступный объем ОЗУ. По мере изменения настройки обратите внимание, что индикатор «Число адаптивных серверов обработки» меняется, характеризуя настройку системы в случае выбора соответствующего параметра.

Примечание:

- Выбранный шаблон развертывания влияет только на адаптивные серверы обработки (APS). Других серверов (CMS или адаптивного сервера заданий) это не касается.
- Требуемый объем ОЗУ – это минимальный объем ОЗУ, необходимый для серверов платформы SAP BusinessObjects Business Intelligence. Например, если на машине 16 ГБ ОЗУ, а ОС использует 1 ГБ ОЗУ, сервер базы данных использует еще 1 ГБ, а серверы платформы BI – 10 ГБ, требуемый объем ОЗУ составляет 10, а не 12 и не 16 ГБ. Требуемый объем ОЗУ – это приближенное стандартное значение. При большой нагрузке системе может потребоваться больше ОЗУ. Для оптимальной производительности системы нужно всегда корректировать размер системы.
- Если открыть страницу «Емкость», отображаемый на этой странице шаблон развертывания представляет текущее состояние системы, если текущее состояние системы соответствует одному из предопределенных шаблонов развертывания. Например, если с помощью CMS был вручную создан дополнительный адаптивный сервер обработки, текущее состояние системы не соответствует ни одному из шаблонов развертывания, поэтому на странице «Емкость» отображается флажок **Сохранить существующую конфигурацию**, указывающий, что система была настроена вне мастера. В развертываниях с большим количеством узлов флажок **Сохранить существующую конфигурацию** также отображается, если какой-либо узел имеет не соответствующее шаблону развертывания число APS или если число APS на других узлах отличается. Можно снять флажок, чтобы использовать мастер для изменения конфигурации.
- Чтобы упростить развертывание, выбранная конфигурация APS применяется к каждому узлу (если на этих узлах установлен APS), поэтому чем больше узлов, тем больше емкость кластера.
- Мастер не обеспечивает управление дополнительными компонентами, например, Data Services или Analysis Application Design Service (AADS). Переместить службы, созданные дополнительными компонентами, на другие адаптивные серверы обработки нельзя.

Примеры:

- Если служба AADS размещается на адаптивном сервере обработки параллельно с другими службами основной установки платформы BI, при запуске мастера и изменении размера шаблона развертывания с XS на M мастер создаст семь новых адаптивных серверов обработки и перенесет на них все службы, за исключением AADS, которая останется на исходном сервере.
- Дополнительный модуль Data Services создает выделенный адаптивный сервер обработки. Мастер не изменяет выделенный адаптивный сервер обработки и не учитывает его в общем числе таких серверов в системе.

Файл DeploymentTemplates.pdf

Подробное описание настроек, которые будут применены мастером к каждому из доступных шаблонов развертывания, можно посмотреть по ссылке на **шаблон развертывания** на странице «Емкость», позволяющей открыть файл DeploymentTemplates.pdf.

Файл DeploymentTemplates.pdf подробно описывает шаблоны развертывания. Обратите внимание, что шаблоны не указывают на возможное число поддерживаемых пользователей, потому что этот показатель зависит от нагрузки. Необходимо изменить размер системы, чтобы определить, какое число пользователей потребуется поддерживать и, следовательно, какой объем ОЗУ, параметры ЦП и т. д. для этого потребуются.

4.4 Местоположение каталогов данных

Воспользуйтесь страницей «Папки», чтобы задать требуемое место сохранения данных и файлов журнала платформой BI. Можно задать собственные местоположения каталогов или принять текущие.

Если развернутая платформа BI имеет несколько узлов, определить местоположения каталогов можно двумя способами:

- Если требуется настроить одни и те же местоположения папок для всех узлов, выберите параметр **Все узлы используют одинаковые местоположения папок**.
- Если серверы в кластере имеют разную настройку, пути установки или структуры каталогов файлов могут различаться. Можно выбрать параметр **Узлы используют разные местоположения папок**, чтобы настроить для каждого узла уникальные местоположения папок.

Всякий раз когда мастер открывает страницу «Каталоги», имена папок отображаются следующим образом:

- Если все узлы имеют папки с абсолютно идентичными значениями (то есть идентичны папки журнала на всех серверах кластера, папки данных на всех серверах кластера и т. д.), выбран параметр **Все узлы используют одинаковые местоположения папок** и показаны текущие имена папок.
- Если все папки определенного типа (журнал, данные, аудит, хранилище входящих файлов и хранилище исходящих файлов) идентичны в пределах одного узла, но различаются между узлами, выбран параметр **Узлы используют разные местоположения папок** и показаны текущие имена папок.
- Если папки определенного типа не идентичны в пределах узла и, кроме того, различаются между узлами, выбран параметр **Узлы используют разные местоположения папок**, однако имена папок оставлены пустыми.

Если меняются местоположения папок, мастер настраивает систему для использования новых папок. За исключением папки данных аудита мастер не копирует и не перемещает содержимое исходных папок в новые. Если новые папки еще не содержат нужное содержимое или если в исходных папках имеются данные и их нужно перенести, возможно, имеет смысл перенести или копировать эти данные в новые папки.

В папках "Хранилище входящих файлов", "Хранилище исходящих файлов" и "Данные" необходимо вручную копировать файлы из прежних местоположений или восстановить файлы из резервной копии, если новое местоположение папки пусто. Что касается папки "Журнал", необходимо копировать файлы из прежней папки, только если новая папка должна содержать файлы журнала, существующие в предыдущем местоположении.

Совет:

Если планируется копировать файлы в новые папки или восстановить их там, сделайте это до перезапуска узлов.

Примерные сценарии:

- Если изменено местоположение папки и исходная папка содержит отчеты, эти отчеты будут недоступны на платформе BI, пока пользователь не копирует эти файлы в новую папку и не перезапустит узлы.
- Если исходная папка содержала поврежденные или измененные отчеты и необходимо вернуться к резервной копии, которая точно не содержит ошибок, следует извлечь отчеты из резервной копии и поместить их в новую папку, а не копировать содержимое исходной папки.
- Если файлы данных первоначально располагались на диске, обозначаемом буквой X, а пользователь меняет обозначение диска в операционной системе на Y, нет необходимости копировать или перемещать файлы данных; достаточно изменить местоположение папки на платформе BI.

Если некоторые местоположения папок были изменены вручную и несколько серверов узла используют один набор папок, а другие серверы того же узла – другие папки, на странице «Папки» отображается флажок **Сохранить существующую конфигурацию**, указывающий, что система была настроена вне мастера. Например, возможно, имеется два файловых сервера репозитория одного и того же узла, настроенных использовать разные пути к папке журнала. Можно снять флажок, если нужно изменить текущую конфигурацию с помощью мастера.

Дополнительные сведения о типах файлов, сохраненных в каждой папке, см. значки ?.

Примечание:

Если изменить какие-либо из следующих местоположений папок, потребуется вручную перезапускать все узлы по окончании работы мастера, потому что только после этого изменения вступят в силу:

- Хранилище входящих файлов
- Хранилище исходящих файлов
- Папка журнала
- Папка данных

4.5 Просмотр изменений

После выбора параметров конфигурации они отображаются на странице «Просмотр», чтобы пользователь мог просмотреть их перед применением внесенных изменений в системе платформы BI. В каждой категории параметров можно щелкнуть **Сведения** и просмотреть подробное описание или список настроек и изменений, которые будут применяться.

Если требуется изменить какие-либо параметры, доступ к отдельным страницам можно осуществлять непосредственно из меню навигации в левой части мастера.

Выбранные значения сохраняются в файле журнала, который можно загрузить со страницы "Выполнено".

Также создается и сохраняется файл ответов. Файл ответов помогает автоматизировать настройку системы. Можно нажать кнопку **Загрузить** и просмотреть файл ответов или загрузить его на локальный диск.

Нажатие кнопки **Применить** применяет параметры конфигурации к развернутой платформе BI. Когда мастер завершает свою работу, отображается страница «Выполнено» со списком дальнейших шагов, которые требуется выполнить вручную.

См. также

- [Файлы журнала и файлы ответов](#)

4.6 Файлы журнала и файлы ответов

На странице «Выполнено» показан статус изменений. Кроме того, здесь можно загрузить и просмотреть файлы журнала и файлы ответов для соответствующего сеанса.

Файлы журнала и файлы ответов автоматически сохраняются в каталоге Мастер настройки системы, открыть который можно из СМС. Имена файлов имеют метки времени в формате год_месяц_день_час_минута_секунда. Файлы журнала используют расширение .log, а файлы ответов – расширение .ini.

Кроме того, можно нажать кнопку **Загрузить**, чтобы просмотреть файлы журнала и файлы ответа или загрузить их на локальный диск.

Файл журнала содержит следующее:

- Запись всех изменений, внесенных в ходе этого сеанса конфигурации.
- Место сохранения файла ответов.
- Список дальнейших действий.

См. также

- [Использование файла ответов](#)

4.6.1 Использование файла ответов

Каждый раз по окончании работы мастера он сохраняет файл ответов, который содержит выбранные пользователем значения и ответы на вопросы со всех страниц мастера. Файл ответов можно использовать для настройки других кластеров развернутой платформы BI, не повторяя для каждого из них уже выполненную процедуру в мастере. Файлом ответов можно воспользоваться впоследствии при необходимости вернуть систему в то же состояние конфигурации. Использование файла ответов позволяет автоматизировать развертывание и избежать ошибок оператора.

Файл ответов используется следующим образом: запускается скрипт, в котором соответствующий файл ответов выступает как параметр. Сначала нужно найти требуемый файл ответов и сохранить его на диск. Файлы ответов автоматически сохраняются в папке Мастер настройки системы, доступ к которой администраторы могут осуществлять с консоли СМС. Имена файлов имеют метки времени в формате `год_месяц_день_час_минута_секунда` и расширение `.ini`. На консоли СМС можно просмотреть файл ответов и сохранить его на диск либо воспользоваться командами меню **Организовать > Отправить > Местоположение файла**.

Файл ответов для текущего сеанса мастера также можно загрузить со страницы «Просмотр» или «Выполнено» и сохранить на диск.

Если перед использованием файла ответов требуется изменить в нем некоторые параметры, отредактировать файл можно в текстовом редакторе. См. пример файла ответов ниже.

Выполнение скрипта

Получив нужный файл ответов, используйте его как параметр командной строки для скриптов, выполняющих мастер:

- В Windows запустите пакетный файл `SCW.bat`.
- В Unix запустите файл скрипта `scw.sh`.

Пакетный файл и файл скрипта размещаются в одной папке с другими скриптами управления сервером:

- В Windows: `<каталог_установки>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.
- В Unix: `<каталог_установки>/sap_bobj/enterprise_xi40/linux_x64/scripts`.

Пакетный файл и файл скрипта принимают следующие параметры командной строки:

- `-help`: отображение справки командной строки.
- `-r`: путь и имя файла ответов.
- `-cms`: центральный сервер управления (CMS), на который требуется выполнить вход. Если этот параметр пропущен, CMS использует локальный компьютер и порт по умолчанию (6400).
Пример: `имя_компьютера:6500`
- `-username`: учетная запись, предоставляющая административные права на платформу BI. Если этот параметр пропущен, используется учетная запись администратора по умолчанию.
- `-password`: пароль учетной записи. Если пароль не указан, применяется пустой пароль. Чтобы воспользоваться параметром `-password`, необходимо также использовать параметр `-username`.

Примеры

В Windows: SCW.bat -r c:\папка\имя_файла.ini -cms имя_cms:6400 -имя пользователя "администратор" -пароль пример_пароля

В Unix: ./scw.sh -r /home/папка/имя_файла.ini -cms имя_cms:6400 -имя пользователя "администратор" -пароль пример_пароля

Пример файла ответов

```
# *****
# ***** Products *****
# *****

# Keep the existing configuration for products.
# Valid values = true or false.
# "true": the existing product configuration will be preserved.
# "false": the product configuration will be modified according to the "Products." settings below.

Products.KeepExistingConfiguration = true

# The "Products." settings below will be ignored if Products.KeepExistingConfiguration = true.

# Auto-start the servers for these products.
# Valid values = true or false.
# "true": the product's servers and their dependencies are auto-started with BI platform.
# "false": the product's servers are not auto-started with BI platform.

# Crystal Reports
Products.crystalreports = true

# Analysis edition for OLAP
Products.olap = true

# Web Intelligence
Products.webintelligence = false

# Dashboards (Xcelsius)
Products.dashboards = false

# Data Federator
Products.datafederator = true

# Lifecycle Manager
Products.LCM = true

# *****
# ***** Deployment Template *****
# *****

# Keep the existing configuration for the deployment template.
# Valid values = true or false.
# "true": the existing deployment template configuration will be preserved and the Capacity.DeploymentTemplate
# setting below will be ignored.
# "false": the deployment template configuration will be modified according to the Capacity.DeploymentTemplate
# setting below.

Capacity.KeepExistingConfiguration = true

# Specify the deployment template for all nodes.
# Valid values = xs, s, m, l, xl.

Capacity.DeploymentTemplate = xs

# *****
# ***** Folders *****
# *****

# Keep the existing configuration for folder locations.
# Valid values = true or false.
# "true": the existing folder configuration will be preserved.
# "false": the folder configuration will be modified according to the "Folders." settings below.

Folders.KeepExistingConfiguration = true
```

```
# The "Folders." settings below will be ignored if Folders.KeepExistingConfiguration = true.

# ----- All nodes use the same folders -----
# Use this section when you have one node, or when all nodes have the same folder locations. Otherwise,
# comment it out.

Folders.InputFileStore = <Path>
Folders.OutputFileStore = <Path>
Folders.Log = <Path>
Folders.Data = <Path>
Folders.Auditing = <Path>

# ----- Nodes use different folders -----
# Use this section when nodes have different folder locations. Otherwise, comment it out.

# ----- NodeOne -----
# Folders.NodeOne.InputFileStore = <Path>
# Folders.NodeOne.OutputFileStore = <Path>
# Folders.NodeOne.Log = <Path>
# Folders.NodeOne.Data = <Path>
# Folders.NodeOne.Auditing = <Path>

# ----- NodeTwo -----
# Folders.NodeTwo.InputFileStore = <Path>
# Folders.NodeTwo.OutputFileStore = <Path>
# Folders.NodeTwo.Log = <Path>
# Folders.NodeTwo.Data = <Path>
# Folders.NodeTwo.Auditing = <Path>
```

Необходимо задать все параметры в файле ответов, ни один параметр не может оставаться пустым. Исключение составляют следующие случаи:

- При наличии развертывания с несколькими узлами можно пропустить параметры папки для одного или нескольких узлов. В этом случае папки в этих узлах останутся без изменений. Однако для узлов, указанных в файле ответов, необходимо указать все местоположения папок.
- Если параметр `KeepExistingConfiguration` имеет значение `true`, можно пропустить остальные настройки на этой странице. Например, если `Products.KeepExistingConfiguration = true`, можно пропустить остальные параметры «Продукты» из файла ответов.

В некоторых случаях файл ответов включает продукты, отличающиеся от установленных в целевом кластере. В этих случаях применяется следующий подход:

- Если файл ответов не содержит определений продуктов, установленных в целевом кластере, операция завершается сбоем.
- Если файл ответов содержит определения продуктов, отсутствующих в целевом кластере, сообщение с предупреждением добавляется в файл журнала, а остальные продукты настраиваются соответственно.

Примечание:

- После настройки кластера с помощью файла ответов потребуется вручную выполнить дополнительные действия, описанные в разделе «Дальнейшие шаги» файла журнала.
- В целях безопасности поддерживается только аутентификация Enterprise (аутентификации Windows AD, LDAP и SAP не поддерживаются).
- Если нужно отложить перезапуск каких-либо узлов до следующего планового перезапуска, выполните скрипт непосредственно перед плановым простоем системы.

Управление лицензиями

5.1 Управление лицензионными ключами

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

См. также

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

5.1.1 Просмотр сведений лицензии

В области управления СМС «Ключи лицензий» указывается количество лицензий для параллельных 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

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

5.1.2 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. После добавления новых лицензионных ключей потребуется снова включить все серверы.

Примечание:

Если новые лицензионные ключи получены в связи с изменением используемого в вашей организации способа реализации лицензий на платформу BI, необходимо удалить все использовавшиеся ранее лицензионные ключи из системы. Только в этом случае будут выполнены лицензионные требования.

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](#)

5.1.3 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

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

5.2 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 SAP Global License Auditing Services (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 для именованных пользователей и лицензий для параллельных 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.

5.2.1 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

6.1 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, вы можете 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.

6.1.1 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 6-1: 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.

Примечание:

Миграции объектов лучше всего выполняются участниками группы "Администраторы", в частности владельцами учетной записи "Администратор". Чтобы перенести объект, может потребоваться также перенести большое количество связанных объектов. Получение требуемых прав безопасности для всех объектов может оказаться невозможным для делегированной учетной записи администратора.

6.1.2 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 6-2: Учетные записи групп по умолчанию

Имя учетной записи	Описание
Администраторы	Участники 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.

Имя учетной записи	Описание
Все	Каждый пользователь является участником группы Все .
Дизайнер группы QaaWS	Участники этой группы имеют доступ к средству Query as a Web Service.
Пользователи средства преобразования отчетов	Участники этой группы имеют доступ к средству преобразования отчетов.
Переводчики	Участники 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](#)

6.1.3 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 6-3: 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.
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.

Тип аутентификации	Описание
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.
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.

6.2 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.

6.2.1 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. В списке **Тип аутентификации** выберите параметр **Enterprise**.

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. Выполните одно из следующих действий для назначения учетной записи пользователя (в зависимости от лицензионного соглашения платформы SAP BusinessObjects Business Intelligence):

- Выберите **Параллельный пользователь**, если пользователь использует лицензионное соглашение, дающее право на подключение в параллельном 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](#)

6.2.2 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](#)

6.2.3 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](#)

6.2.4 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.

6.2.5 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 **Участник**.

4. Щелкните **Сохранить**.

6.2.6 Просмотр участников групп

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

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

6.2.7 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](#)

6.2.8 Задание принадлежности к группе

Группу можно сделать элементом другой группы. В этом случае ставшая элементом 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 «Элемент».
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 «Элемент», а в списке родительских групп отобразится данная родительская группа.

6.2.9 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.

6.2.10 Массовое добавление пользователей или групп пользователей

Для массового добавления пользователей или групп пользователей к СМС можно использовать файлы CSV (comma-separated values). В правильно подготовленном файле CSV запятыми отделяются данные в строке как показано в следующем примере:

```
Add,MyGroup,MyUser1,MyFullName,Password1,My1@example.com,ProfileName,ProfileValue
```

К процессу массового добавления применяются следующие условия:

- Из процесса импорта исключаются любые строки CSV-файла, содержащие ошибки.
- После импорта учетные записи пользователей по умолчанию отключены.
- При создании новых пользователей можно использовать пустые пароли. Тем не менее, при последующих обновлениях до существующих пользователей необходимо использовать действительный пароль аутентификации Enterprise.
- Если к учетной записи добавляется DBCredential, в профиле пользователя будут активированы реквизиты базы данных.

1. В области управления **Пользователи и группы** консоли СМС выберите **Управление > Импорт > Пользователь/Группа/DBCredential**.

Появится диалоговое окно «Импорт пользователя/группы/DBCredential».

2. Нажмите кнопку **Обзор**, выберите CSV-файл и щелкните **Проверить**.

Начнется обработка файла. Если данные в файле имеют правильный формат, кнопка **Импорт** станет активной. Если данные отформатированы некорректно, будет показано сообщение об ошибке. Устраните ошибку, после чего СМС выполнит проверку файла импорта.

3. Нажмите кнопку **Импорт**.

Пользователи или группы пользователей импортируются в СМС.

Чтобы просмотреть добавленных пользователей или группы пользователей, выберите команду **Управление > Импорт > Журнал** в области управления **Пользователи и группы**.

6.2.11 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 навигации.
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**.

6.2.12 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](#)

6.2.12.1 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 BI 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**.

6.2.12.2 Добавление 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 **мышь**, или же клавишу **CTRL +** и щелчок кнопки **мышь**.
 - 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**.

6.2.13 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, 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.

6.2.13.1 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**.

6.2.13.2 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 настройки.

Таблица 6-4: 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

Настройка пароля	Минимум	Рекомендованный максимум
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**.

Примечание:

Неактивные учетные записи пользователей не отключаются автоматически.

6.2.14 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](#)

6.2.15 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

- [Настройка расписания для программного объекта](#)
- [Управление настройками безопасности для объектов в СМС](#)

6.2.16 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.

6.2.16.1 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 СМС и типа аутентификации. Чтобы изменить этот параметр, потребуется изменить свойства стартовой панели BI для файла BOE.war.

6.2.16.1.1 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 установке платформы BI:

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

2. Создайте в текстовом редакторе новый файл.

3. Сохраните файл под следующим именем:

BIlaunchpad.properties

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

```
authentication.visible=true
```

5. Чтобы изменить тип аутентификации по умолчанию, добавьте следующую строку:

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

Замените <authentication> любым из следующих вариантов:

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

6. Чтобы запрашивать у пользователей имя CMS на экране входа в систему стартовой панели BI, добавьте следующую строку:

```
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. Дополнительные сведения об использовании WDeploy см. в *руководстве по развертыванию веб-приложений платформы SAP BusinessObjects Business Intelligence*

6.2.16.2 Настройка предпочтительных параметров стартовой панели BI для групп пользователей

Администраторы могут указывать значения по умолчанию для стартовой панели BI, которые будут применяться ко всем пользователям в группе.

Примечание:

Если пользователи устанавливают собственные предпочтения, то параметры, заданные администратором, не применяются к пользовательскому виду стартовой панели BI. В любое время можно переключаться между собственными предпочтениями и параметрами, заданными администратором.

По умолчанию ни для одной группы пользователей не заданы параметры стартовой панели BI. Администраторы могут указывать значения по умолчанию для следующих предпочтений:

- Вкладка "Домашняя страница"
- Место хранения документов
- Папки
- Категории
- Число объектов на страницу
- Столбцы, отображаемые на вкладке **Документ**
- Отображение документов на стартовой панели BI, во вкладке или в новом окне

6.2.16.2.1 Задание параметров стартовой панели BI для группы пользователей

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

6.3 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.

6.3.1 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.

6.3.2 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».

6.3.3 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**.

6.3.4 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».

6.3.5 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

7.1 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 IT-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 элементами 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](#)

7.1.1 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](#)

7.1.2 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 принципа 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 7-1: 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](#)

7.1.3 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.

7.1.3.1 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 элемент красной группы наследует эти права. Кроме того, все остальные права, которые настроены во вложенной группе, наследуются ее элементами. В этом примере зеленый пользователь является элементом красной группы, поэтому он наследует право 1 как предоставленное, права 2, 3, 4 и 6 как неопределенные и право 5 как запрещенное.



Рис. 7-1: 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 элементом 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.

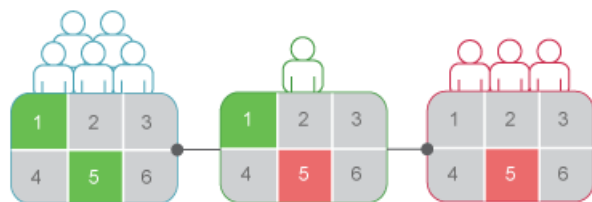


Рис. 7-2: Пример наследования группы 2

См. также

- [Переопределение прав](#)

7.1.3.2 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, участники "Красной группы" будут иметь права на уровне объекта, идентичные правам группы на уровне папки. Права 1 и 5 будут унаследованы, а остальные останутся неиспользованными.

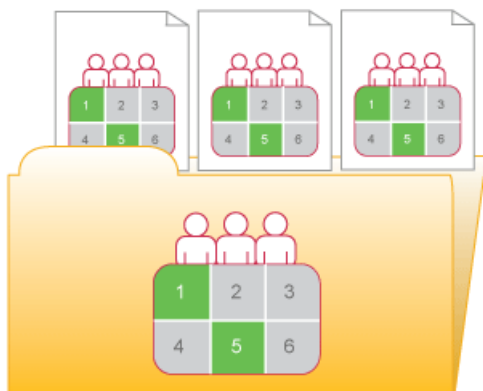


Рис. 7-3: Пример наследования папок

См. также

- [Переопределение прав](#)

7.1.3.3 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 участников 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.

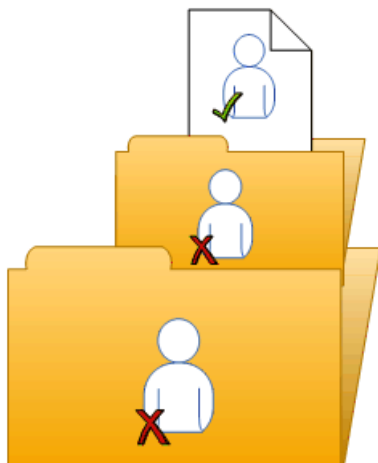


Рис. 7-4: Пример переопределения прав 1

«Пример переопределения прав 2» иллюстрирует, как переопределение прав работает с участниками и группами. Для группы Blue отменено право редактирования папки; подгруппа Blue унаследовала эту настройку. Однако администратор предоставляет пользователю Blue, который является участником 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.

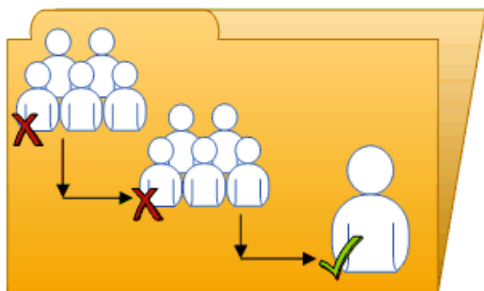


Рис. 7-5: Пример переопределения прав 2

«Комплексное переопределение прав» иллюстрирует ситуацию, в которой переопределение прав менее очевидно. Пользователь Purple является участником 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.

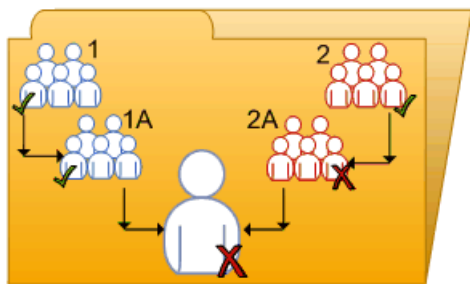


Рис. 7-6: Комплексное переопределение прав

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".

7.1.3.4 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.

7.1.4 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 участники группы Blue имеют права на **Редактирование** отчетов Crystal, но не XLF-файла в подпапке.

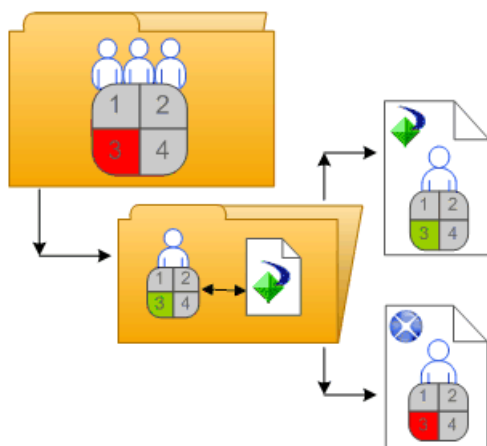


Рис. 7-7: Пример прав для конкретных типов объектов

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.

7.1.5 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.

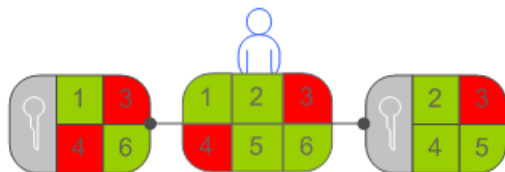


Рис. 7-8: Несколько уровней доступа

- 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.

7.2 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.

7.2.1 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 столбце «Источник», чтобы отобразился источник наследованных прав.

7.2.2 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](#)

7.2.3 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](#)

7.2.4 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](#)

7.2.5 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.

7.2.5.1 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 Просмотреть

Полномочия для запроса

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

☐ Не передается запрос по полномочиям Просмотреть

Коллекция	Тип	Имя права		
Общее	Общее	Добавить объекты в каталог	✓	✕
Общее	Общее	Добавить объекты в папки, принадлежащие пользователям	✓	✕

Контекст запроса

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

☒ Папки Просмотреть

(Все) ☒ Запросить подобъект

☐ Папки Просмотреть

(Все) ☐ Запросить подобъект OK Отмена

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 > Изменить 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.

7.3 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 7-2: 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 Про смотреть , 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

7.3.1 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 выполняют развертку 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**.

7.3.2 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.

7.3.3 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**.

7.3.4 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».

7.3.5 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.

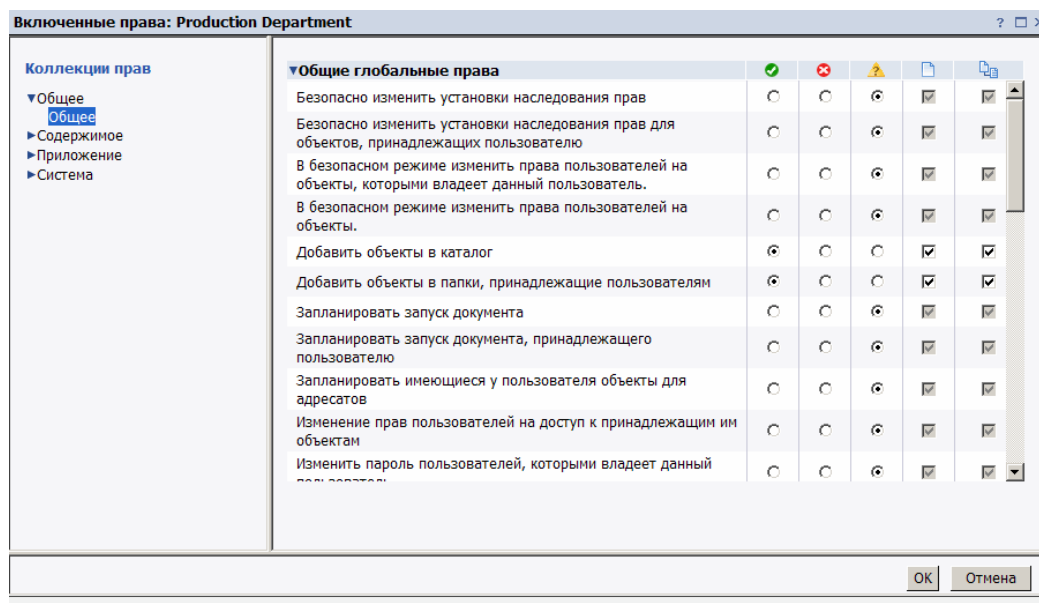
Информация об объектах, которые затрагивает данный уровень доступа, появится в диалоговом окне. Если удалять уровень доступа не требуется, нажмите кнопку **Отмена**, чтобы выйти из диалогового окна.

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

7.3.6 Изменение прав 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](#)

7.3.7 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.

7.3.8 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](#)

7.4 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 элемент 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.

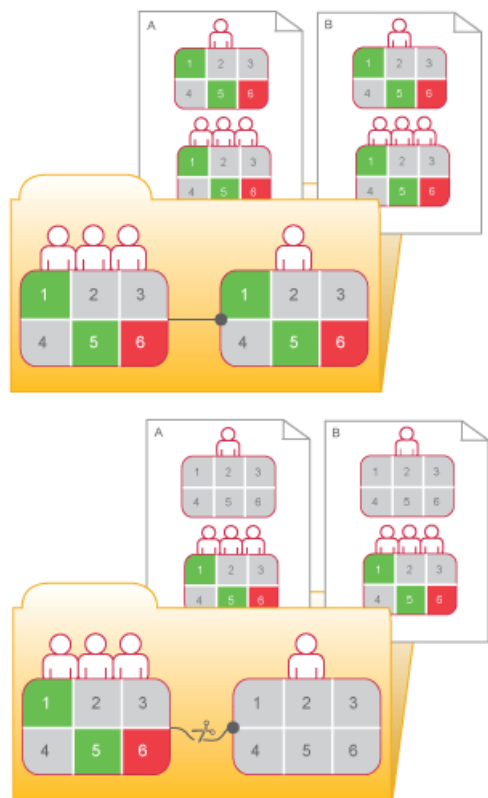


Рис. 7-9: Отключение наследования

7.4.1 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**.

7.5 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 делегированному администратору 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.

Примечание:

Миграции объектов лучше всего выполняются участниками группы "Администраторы", в частности владельцами учетной записи "Администратор". Чтобы перенести объект, может потребоваться также перенести большое количество связанных объектов. Получение требуемых прав безопасности для всех объектов может оказаться невозможным для делегированной учетной записи администратора.

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

Таблица 7-3: 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 атрибутов, а также перераспределение пользователей по другим группам	<p>Право на изменение в отношении соответствующих групп</p>
Изменение имен пользователей, описания, других атрибутов, 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>

7.5.1 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.

7.5.2 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.

7.6 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 участников.
- 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 участников группы "Все" и настроить безопасность соответствующим образом.

Обеспечение безопасности платформы BI

8.1 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 предоставляет структуру для растущего числа компонентов из семейства SAP BusinessObjects Platform Search, в этот раздел включены подробные сведения о функциях безопасности и связанных с ними функциональных возможностях для демонстрации того, 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.

8.2 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.

8.3 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.

Примечание:

Платформа BI не поддерживает SFTP. Если вам требуются функции SFTP, изучите SAP-указание 1556571 или используйте решение партнера SAP.

- 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.
- Убедитесь в том, что каталог установки платформы и его вложенные каталоги надежно защищены (в процессе эксплуатации системы в них могут храниться конфиденциальные данные).
- Доступ к консоли CMC ограничен исключительно локальным уровнем. Сведения о параметрах развертывания консоли CMC см. в *руководстве по развертыванию веб-приложений платформы SAP BusinessObjects Business Intelligence*.

См. также

- [Настройка протокола SSL](#)
- [Ограничения для пароля](#)
- [Настройка безопасности для связанных серверов сторонних производителей](#)

8.4 Настройка безопасности для связанных серверов сторонних производителей

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

- Sybase SQL Anywhere: подробные сведения об обеспечении безопасности этой системы см. в разделе <http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.help.sqlanywhere.12.0.0/dbadmin/dapart-securing.html>.
- Apache Tomcat: подробные сведения о безопасности этого веб-приложения см. в разделе <http://tomcat.apache.org/>.

8.5 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.

8.5.1 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 не защищена, 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.

8.5.2 Механизм билетов для распределенной безопасности

Системы предприятия, предназначенные для обслуживания большого числа пользователей, обычно требуют определенной формы распределенной безопасности. Система предприятия 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.

8.6 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.

8.6.1 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.

8.7 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 разделяется на две области коммуникации: "веб-браузер - веб-сервер" и "веб-сервер - платформа BI".

8.7.1 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.

8.7.2 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.

8.8 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.

8.9 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.

8.9.1 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, 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.

8.9.2 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.

8.9.3 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

8.9.4 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.

8.9.5 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.

8.10 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.

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.

8.11 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 Central Configuration Manager.
- 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 Central Configuration Manager, 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.

8.11.1 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 указанный стандарт. 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.

8.11.1.1 Для включения FIPS-совместимого режима в Windows

По умолчанию FIPS-совместимый режим отключен при установке платформы BI. Однако можно включить FIPS-совместимость для всех узлов развертывания.

1. Чтобы запустить CCM, последовательно щелкните **Программы > SAP Business Intelligence > Платформа SAP BusinessObjects BI 4 > 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 агента SIA не сменится на "Остановлен".

3. Щелкните SIA правой кнопкой мыши 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.

8.11.1.2 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. Из каталога `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj` откройте файл `ccm.config` для редактирования.
2. Добавьте `-fips` к параметру команды запуска узла.
Параметр команды запуска узла отображается в формате `<ИМЯ_УЗЛА>LAUNCH`. Например, для узла с именем «SAP» используется параметр команды запуска узла `SAPLAUNCH`.
3. Сохраните изменения и нажмите **Выход**.
4. Перезапустите узел.

Теперь узел работает в FIPS-совместимом режиме.

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

8.11.1.3 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**.

Отобразится 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.

8.12 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.

8.12.1 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`. Имя файла `dbinfo` определяется следующим соглашением: `_boe_<sia_name>.dbinfo`, где `<sia_name>` - это имя агента серверной аналитики для кластера.

В ОС Windows этот файл сохраняется в следующем каталоге: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.

В системах Unix файл хранится в каталоге платформы в `<INSTALLDIR>/sap_bobj/enterprise_xi40/`:

платформа Unix	Каталог платформы
AIX	<code><INSTALLDIR>/sap_bobj/enterprise_xi40/aix_rs6000_64/</code>
Solaris	<code><INSTALLDIR>/sap_bobj/enterprise_xi40/solaris_sparcv9/</code>
Linux	<code><INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64/</code>

Примечание:

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

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

8.12.1.1 Чтобы сбросить ключ кластера в Windows

Перед сбросом ключа кластера для соответствующего узла убедитесь, что остановлены все серверы под управлением агента Server Intelligence Agent.

1. Для запуска CCM щелкните **Программы > SAP Business Intelligence > Платформа SAP BusinessObjects BI 4 > 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 агента SIA не сменится на "Остановлен".

3. Щелкните правой кнопкой мыши агент Server Intelligence Agent (SIA) и выберите **Свойства**. Откроется диалоговое окно «Свойства».

4. Откройте вкладку **Конфигурация**.
5. Нажмите кнопку **Изменить** в разделе «Конфигурация ключа кластера CMS». Появится сообщение подтверждения.
6. Нажмите кнопку **Да** для продолжения. Будет открыто диалоговое окно «Изменение ключа кластера».
7. Введите тот же 8-значный ключ в полях **Новый ключ кластера** и **Подтверждение нового ключа 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. Отобразится сообщение, подтверждающее успешный сброс ключа кластера
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.

8.12.1.2 Сброс ключа кластера в UNIX

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

1. Перейдите к каталогу `<INSTALLDIR>/sap_bobj`.
2. Введите `./cmsdbsetup.sh` и нажмите клавишу **Enter**. Открывается экран «Настройка базы данных CMS».
3. Введите имя узла и нажмите клавишу **Enter**.
4. Введите значение 2, чтобы изменить ключ кластера. Появится сообщение подтверждения.
5. Нажмите **Далее** для продолжения.
6. В специальном поле введите новый ключ кластера, состоящий из восьми символов, и нажмите клавишу **ВВОД**.

Примечание:

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

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

8. Перезапустите узел.

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

8.12.2 Специалисты по шифрованию

Для управления криптографическими ключами в СМС необходимо быть участником 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.

8.12.2.1 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 участника в группу специалистов по шифрованию, необходимо быть участником групп Администраторы и Специалисты по шифрованию.

1. В области управления «Пользователи и группы» в СМС, выберите группу **Специалисты по шифрованию**.
2. Нажмите **Действия > Добавить участников в группу**.
Появится диалоговое окно «Добавление».
3. Щелкните **Список пользователей**.
Список **Доступные пользователи или 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 или группы** в список **Выбранные пользователи или группы**.

Совет:

Чтобы найти какого-либо пользователя, используйте поле поиска.

5. Нажмите кнопку **ОК**.

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

8.12.2.2 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. Для запуска СМС перейдите по пути **Программы > SAP Business Intelligence > Платформа SAP BusinessObjects BI 4 > SAP BusinessObjects BI platform Central Management Console**. Появится 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](#)

8.12.3 Управление криптографическими ключами с помощью СМС

Область управления «Криптографические ключи» позволяет специалистам по шифрованию просматривать, создавать, отключать, отзывать 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
Последнее изменение статуса	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](#)

8.12.3.1 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.

8.12.3.2 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.

8.12.3.3 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**.
Появится диалоговое окно «Создать новый криптографический ключ».
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.

8.12.3.4 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**.
Откроется диалоговое окно «Пометить как рассекреченный».
4. Нажмите кнопку **Продолжить**.
5. Выберите в диалоговом окне «Пометить как рассекреченный» один из следующих 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](#)

8.12.3.5 Отзыв криптографических ключей

Неактивный криптографический ключ может использоваться связанными с ним объектами данных. Чтобы разорвать связь между зашифрованными объектами и отключенными ключами, необходимо отозвать ключ.

1. Выберите ключ, который требуется отозвать из списка ключей в области управления «Криптографические ключи».
2. Последовательно выберите пункты **Действия > Отозвать**.
Откроется диалоговое окно «Отзыв».
3. Нажмите кнопку **ОК**.
Начнется шифрование всех объектов, связанных с отозванным ключом, с помощью текущего активного ключа. Если ключ связан с большим числом объектов данных, он будет помечен как «Неактивно: выполняется повторное шифрование» 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.

8.12.3.6 Удаление криптографических ключей из системы

Перед удалением криптографического ключа из платформы BI следует убедиться, что он не является необходимым ни для какого объекта данных в системе. Благодаря этому ограничению все конфиденциальные данные, которые хранятся в репозитории CMS, 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 CMS.
2. Выберите криптографический ключ, который нужно удалить.
3. Выберите команды **Управление > Удалить**.
Откроется диалоговое окно «Удалить».
4. Нажмите кнопку **Удалить**, чтобы удалить криптографический ключ из системы.
Удаленный ключ больше никогда не отобразится в области управления «Криптографические ключи» консоли CMS.

Примечание:

Удаленный из системы криптографический ключ восстановить невозможно.

См. также

- [Отзыв криптографических ключей](#)
- [Статус криптографического ключа](#)

8.13 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 всего обмена 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 Central Configuration Manager (CCM) и на сервере веб-приложений.
- Или настройте SSL для сертификатов под управлением центра сертификации.

Примечание:

Если используются толстые клиенты, такие как Crystal Reports, их также следует настроить для SSL, если подключение к CMS будет осуществляться с этих клиентов. В противном случае будут выдаваться ошибки при попытке подключения к CMS, настроенному для использования SSL, из толстого клиента, который не был настроен соответствующим образом.

8.13.1 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.

8.13.1.1 Создание файлов ключа и сертификата для компьютера

1. Запустите инструмент командной строки `sslsc`.

Инструмент SSLC устанавливается вместе с программным обеспечением платформы BI. (В системе Windows, например, установка по умолчанию производится в каталоге `<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 центра 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 самостоятельно подписанный сертификат, `cacert.pem`, срок действия которого истекает через 365 дней. Выберите количество дней, которое соответствует вашим требованиям безопасности.

5. В текстовом редакторе откройте файл `sslsc.cnf`, который хранится в той же папке, что и инструмент командной строки SSLC.

Примечание:

Необходимо использовать текстовый редактор для Windows, поскольку проводник Windows не может распознать и отобразить файлы с расширением `.cnf`.

6. Выполните следующие действия на основе параметров в файле `sslsc.cnf`.

- a. Поместите файлы `cakey.pem` и `cacert.pem` в каталоги, заданные параметрами `certificate` и `private_key` файла `sslsc.cnf`. По умолчанию используются следующие параметры файла `sslsc.cnf`:

```
certificate = $dir/cacert.pem
```

```
private_key = $dir/private/cakey.pem
```

- b. Создайте файл с именем, заданным параметром `database` файла `sslsc.cnf`.

Примечание:

По умолчанию файлу присвоено имя `$dir/index.txt` и он должен быть пуст.

- c. Создайте файл с именем, заданным параметром `serial` файла `sslsc.cnf`.

Файл должен содержать серийный номер в виде строки октетов (в шестнадцатеричном формате).

Примечание:

Чтобы обеспечить возможность создания и подписания большого количества сертификатов, выберите большой шестнадцатеричный номер с четным количеством цифр, например 11111111111111111111111111111111.

d. Создайте каталог, заданный параметром `new_certs_dir` файла `ssl.cnf`.

7. Чтобы создать запрос на сертификат и секретный ключ, введите следующую команду:

```
sslreq -config ssl.cnf -new -out servercert.req
```

Созданные файлы сертификата и секретного ключа размещаются в текущей рабочей папке.

8. Чтобы расшифровать ключ в файле `privkey.pem`, введите следующую команду:

```
sslrsa -in privkey.pem -out server.key
```

9. Чтобы подписать сертификат при помощи сертификата CA, введите следующую команду:

```
sslca -config ssl.cnf -days 365 -out servercert.pem -in servercert.req
```

Эта команда создает файл `servercert.pem`, который содержит подписанный сертификат.

10. Используйте следующие команды, чтобы преобразовать эти сертификаты в сертификаты, зашифрованные в соответствии со стандартом DER:

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

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

Примечание:

Сертификат CA (`cacert.der`) и соответствующий секретный ключ (`cakey.pem`) необходимо создать единожды в одном развертывании. Все компьютеры того же развертывания совместно используют одни и те же сертификаты CA. Все остальные сертификаты должны быть подписаны с использованием секретного ключа любого сертификата CA.

11. Создайте текстовый файл (`passphrase.txt`) для хранения обычного текста `passphrase`, используемого для расшифровки созданного секретного ключа.
12. Храните следующие файлы ключа и сертификата в безопасном местоположении (в одном и том же каталоге), которое доступно для компьютеров вашего развертывания платформы BI.
 - Файл доверенного сертификата (`cacert.der`)
 - Созданный файл сертификата сервера (`servercert.der`)
 - Файл серверного ключа (`server.key`)
 - Файл фразы-пароля (`passphrase.txt`)

Данное местоположение будет использоваться для настройки SSL для CCM и вашего сервера веб-приложений.

8.13.2 Настройка SSL при управлении сертификатом центром сертификации

При настройке SSL для связи с сервером выполните следующие шаги, если управление сертификатом осуществляет центр сертификации.

1. Экспортируйте требуемый сертификат с его секретным ключом в формат PKCS #12 (.PFX).

Он будет использоваться в качестве сертификата для центра сертификации.

2. С помощью OpenSSL выполните следующие команды:

- a. Экспортируйте файл секретного ключа из файла .pfx:

```
openssl pkcs12 -in filename.pfx -nocerts -out privkey.pem
```

- b. Экспортируйте файл сертификата из файла .pfx:

```
openssl pkcs12 -in filename.pfx -clcerts -nokeys -out cacert.pem
```

- c. Удалите фразу-пароль из секретного ключа:

```
openssl rsa -in privkey.pem -out cakey.pem
```

3. Настройте несколько обязательных файлов:

- Скопируйте cakey.pem в C:\SSL\private\cakey.pem.
- Скопируйте cacert.pem в C:\SSL\cacert.pem.
- Создайте пустой текстовый файл (файл индекса базы данных) с именем index.txt в папке C:\SSL.
- Создайте еще один текстовый файл: C:\SSL\serial.
- Откройте файл C:\SSL\serial в текстовом редакторе, введите следующее значение и сохраните файл: 11111111111111111111

4. В текстовом редакторе откройте файл C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86\sslc.cnf.

Выберите один из следующих параметров:

- Измените значение переменной policy на policy_anything. Это изменение позволит создать сертификат сервера, который имеет иные политики, чем ваш сертификат центра сертификации.
- Либо оставьте значение переменной policy без изменения как policy_match. В результате этого политики вашего сертификата сервера и политики сертификата центра сертификации будут одинаковыми. В этом случае требуется изменить свойства req_distinguished_name соответствующим образом.

5. Создайте запрос сертификата и секретный ключ.

В командной строке выполните следующую команду:

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

Примечание:

- Для фразы-пароля PEM введите любой пароль, включающий не менее четырех символов.
- В качестве общего имени введите полностью определенное имя домена компьютера, на котором запущены серверы платформы BI.
- Файл servercert.req создается в папке C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86.
- Файлы .rnd и privkey.pem изменяются.

6. Расшифруйте секретный ключ.

```
sslc rsa -in privkey.pem -out server.key
```

7. Подпишете сертификат.

```
sslc ca -config sslc.cnf -days 365 -out servercert.pem -in servercert.req
```

Примечание:

- Файл servercert.pem создается в папке C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86.
- Файл 11111111111111111111.pem создается в папке C:\SSL\newcerts.
- Резервная копия файла serial создается с именем serial.old.
- Значение serial увеличивается с 1111111111111111 до 11111111111111112.

- ## 8. Преобразуйте сертификаты в кодировку DER.

Выполните следующие команды:

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

Примечание:

- **Файл servercert.der создается в папке** C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86.
- **Файл cacert.der создается в папке** C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86.

9. Создайте текстовый файл с именем `passphrase.txt`.

Содержимым файла должна быть фраза-пароль PEM, которая использовалась ранее.

- 10.** Сохраните следующие файлы в защищенной папке, например C:\SSLCerts.

- файл доверенного сертификата `cacert.der`
- созданный файл сертификата сервера `servercert.der`
- файл серверного ключа `server.key`
- файл фразы-пароля `passphrase.txt`

8.13.3 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.

8.13.3.1 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. Укажите путь к каталогу, в котором сохранены файлы ключа и сертификата.

Поле	Описание
Папка сертификатов SSL	Папка, в которой сохраняются все необходимые файлы и сертификаты SSL. Например: <code>d:\ssl</code>
Файл сертификатов SSL сервера	Имя файла для хранения сертификата SSL сервера. По умолчанию используется имя <code>servercert.der</code>
Файл надежных сертификатов SSL	Имя файла с надежным сертификатом SSL. По умолчанию используется имя <code>cacert.der</code>
Файл секретных ключей SSL	Имя файла секретных ключей SSL для доступа к сертификату. По умолчанию используется имя <code>server.key</code>
Файл идентификационных фраз секретных ключей SSL	Имя текстового файла, содержащего идентификационную фразу для доступа к секретному ключу. По умолчанию используется имя <code>passphrase.txt</code>

Примечание:

Убедитесь, что указан путь к каталогу на машине, на которой работает сервер.

8.13.3.2 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 останова SIA и всех серверов SAP BusinessObjects.
2. Выполните скрипт `serverconfig.sh`.
3. Выберите пункт **3 – Изменить узел** и нажмите клавишу **Enter**.
4. Укажите целевой SIA и нажмите клавишу **Enter**.
5. Выберите **1 - 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 `scm.sh` и дождитесь, пока запустятся серверы.

8.13.3.3 Настройка протокола SSL для сервера веб-приложений

1. Для сервера веб-приложений J2EE запустите Java SDK со следующими заданными свойствами системы. Например:

```
-Dbusinessobjects.ora.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.
<code>DsslCert=clientcert.der</code>	Сертификат, используемый SDK.
<code>DsslKey=client.key</code>	Секретный ключ сертификата SDK.
<code>Dpassphrase=passphrase.txt</code>	Файл для хранения ключевой фразы (passphrase) секретного ключа.

2. Для сервера веб-приложений IIS запустите инструмент `sslconfig` из командной строки и следуйте указаниям по конфигурации.

8.13.3.4 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 CCM или средство управления обновлениями.

1. Убедитесь, что приложение толстого клиента не выполняет никаких операций.

Примечание:

Убедитесь, что указан путь к каталогу на компьютере, где работает сервер.

2. 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](#)

8.13.3.4.1 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.

8.13.3.4.2 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" -cp migration.jar;* -Xmx512m -Xss10m com.bo.migration.MigrationTool
```

4. Добавьте следующие данные после параметра `-Xss10m`:

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir=d:\ssl
-DtrustedCert=cacert.der
```

```
-DsslCert=servercert.der  
-DsslKey=server.key  
-Dpassphrase=passphrase.txt  
-Dbusinessobjects.migration
```

Примечание:

Убедитесь, что между всеми параметрами имеется пробел и нет пробелов в конце строк.

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](#)

8.14 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](#)

8.14.1 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.

8.14.1.1 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 вручную настроить для серверов, обменивающихся данными с другими компонентами платформы BI через брандмауэр.

8.14.1.2 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.

8.14.1.3 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).

8.14.1.4 Каталог зарегистрированных служб центрального сервера управления (CMS)

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:

Ссылка на сервер платформы BI по умолчанию содержит имя хоста компьютера сервера. (Если компьютеру назначено несколько имен хоста, используется первичное имя хоста.) Можно настроить сервер таким образом, чтобы в ссылке вместо имени хоста содержался IP-адрес.

См. также

- [Взаимодействие между компонентами платформы BI](#)

8.14.1.5 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.

8.14.1.6 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](#)

8.14.2 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.

8.14.2.1 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 сервером 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 <наименьший номер порта>-<наибольший номер порта>`. 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](#)

8.14.2.2 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.

8.14.2.2.1 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 2013	CMS Сервер репозитория входящих файлов Сервер репозитория исходящих файлов Сервер приложений отчетов Crystal Reports 2013 (RAS) Сервер обработки Crystal Reports 2013 Кэш-сервер Crystal Reports	Порт сервера имен CMS (по умолчанию 6400) Порт запросов CMS Порт запросов сервера репозитория входящих файлов Порт запросов сервера репозитория исходящих файлов Порт запросов сервера Crystal Reports 2013 Report Application Server Порт для запросов сервера обработки Crystal Reports Порт запросов кэш-сервера Crystal Reports
Crystal Reports	Конструктор SAP Crystal Reports для Enterprise	CMS Сервер репозитория входящих файлов Сервер репозитория исходящих файлов Сервер обработки Crystal Reports Кэш-сервер Crystal Reports	Порт сервера имен CMS (по умолчанию 6400) Порт запросов CMS Порт запросов сервера репозитория входящих файлов Порт запросов сервера репозитория исходящих файлов Порт для запросов сервера обработки Crystal Reports Порт запросов кэш-сервера Crystal Reports

Продукт	Клиент-ское приложение	Связанный сервер	Требования к порту сервера
Dashboards	SAP Business Objects Dashboards	<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 Dashboards, 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>
Платформа BI	SAP Business Objects Web Intelligence Rich Client	<p>CMS</p> <p>Сервер репозитория входящих файлов</p>	<p>Порт сервера имен CMS (по умолчанию 6400)</p> <p>Порт запросов CMS</p> <p>Порт запросов сервера репозитория входящих файлов</p>
Платформа BI	Средство создания универсов	<p>CMS</p> <p>Сервер репозитория входящих файлов</p> <p>Сервер соединений</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 сервера соединений</p>

Продукт	Клиент-ское приложение	Связанный сервер	Требования к порту сервера
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
Платформа BI	Central Configuration Manager (CCM)	CMS Агент Server Intelligence (SIA)	Следующие порты необходимо открыть, чтобы разрешить CCM управлять удаленными серверами платформы BI: Порт сервера имен CMS (по умолчанию 6400) Порт запросов CMS Следующие порты необходимо открыть, чтобы разрешить CCM управлять удаленными процессами SIA: Службы каталогов Microsoft (порт 445 TCP) Служба сеанса NetBIOS (порт 139 TCP) Служба диаграмм NetBIOS (порт 138 UDP) Служба имен NetBIOS (порт 137 UDP) DNS (порт 53 TCP/UDP) (Обратите внимание, что некоторые из перечисленных портов могут быть необязательными. Обратитесь к администратору Windows).

Продукт	Клиент-ское приложение	Связанный сервер	Требования к порту сервера
Платформа BI	Агент Server Intelligence (SIA)	Все серверы платформы BI, включая центральный (CMS)	Порт запросов SIA (по умолчанию 6410) Порт сервера имен CMS (по умолчанию 6400) Порт запросов CMS
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 2013 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 2013.

Продукт	Клиент-ское приложение	Связанный сервер	Требования к порту сервера
Платформа BI	Поставщик веб-служб (cswsboobje.wat)	<p>Все серверы платформы BI, необходимые для доступа продуктов к веб-службам.</p> <p>Например, взаимодействие с портами запросов кэш-сервера и сервера обработки Dashboards требуется, если SAP BusinessObjects Dashboards 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, порты запросов кэш-сервера и сервера обработки Dashboards.</p>
Платформа BI	SAP BusinessObjects Analysis, версия для OLAP	<p>CMS</p> <p>Адаптивный сервер обработки, на котором размещена служба Multi-Dimensional analysis service</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>

8.14.2.2.2 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.

8.15 Настройка платформы BI для брандмауэров

В этом разделе приводятся пошаговые инструкции по настройке системы платформы BI для работы в среде брандмауэра.

8.15.1 Настройка системы для использования брандмауэров

1. Определите, какие компоненты платформы BI должны обмениваться данными через брандмауэр.
2. Вручную 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 hosts на каждом компьютере, на котором установлен 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](#)

8.15.1.1 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, не потребуется определять правила доступа для каждого из серверов платформы BI за брандмауэром.

Используйте номер порта, указанный в поле сервера **Порт запросов** на странице свойств сервера СМС. Запомните, что для каждого сервера на компьютере необходимо использовать уникальный номер порта. Для некоторых серверов SAP BusinessObjects используется 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 запросов** 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](#)

8.15.1.2 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.

8.15.1.2.1 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 `\Windows\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`.

8.15.1.2.2 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`.

8.15.2 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
```

8.15.2.1 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](#)

8.16 Примеры типовых сценариев развертывания брандмауэров

В этом разделе приводятся примеры типовых сценариев развертывания брандмауэров.

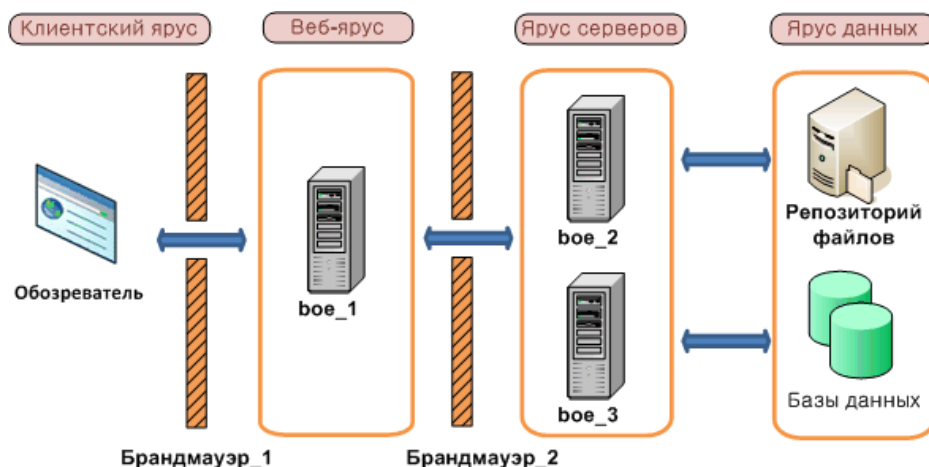
8.16.1 Пример: уровень приложений развернут в отдельной сети

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. 8-1: Уровень приложений развернут в отдельной сети



8.16.1.1 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 8-6: 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](#)

8.16.2 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:

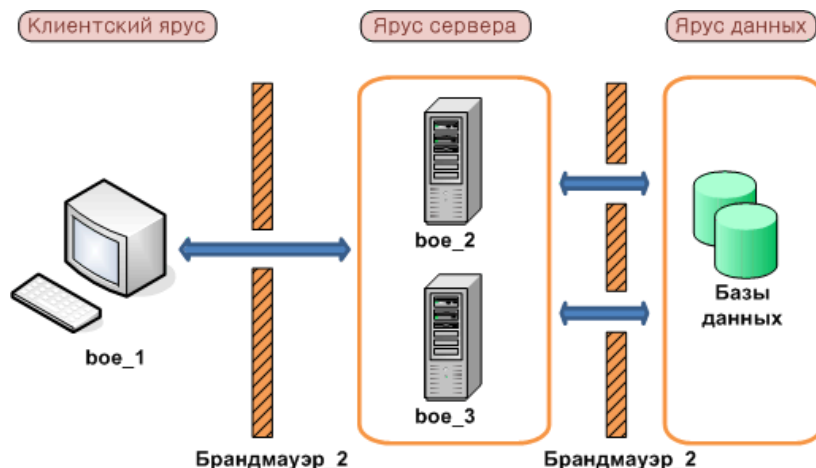
- Один брандмауэр разделяет серверы платформы BI и толстый клиент.
- Один брандмауэр разделяет серверы платформы BI и уровень БД.

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.

Рис. 8-2: Толстый клиент и уровень базы данных развернуты в отдельных сетях



8.16.2.1 Настройка уровней, отделенных брандмауэром от серверов платформы ВІ

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 репозитория входящих файлов	6415

Сервер	Номер порта
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](#)

8.17 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 центрального сервера 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

8.17.1 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.
- Адаптивный сервер заданий 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](#)

8.17.1.1 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

8.17.2 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 JDENET и по произвольно выбираемому порту.
- Crystal Reports с компонентом соединения данных со стороны клиента должен быть способен подключаться к JD Edwards EnterpriseOne по порту JDNET. 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 JDENET и по произвольно выбираемому порту.
- Номер порта JDENET указан в файле конфигурации сервера приложений JD Edwards EnterpriseOne (JDE.INI), в разделе JDENET.

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

Порты, требуемые для JD Edwards EnterpriseOne

Продукт	Необходимые порты	Описание
JD Edwards EnterpriseOne	Порт JDENET и произвольно выбираемый порт	Используется для взаимодействия между платформой BI и сервером приложений JD Edwards EnterpriseOne.

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 8-14: 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
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

8.17.3 Конкретные рекомендации по настройке брандмауэра для Oracle EBS

В развертывании 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.

8.17.3.1 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
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

8.17.4 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.

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

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.

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 8-18: 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
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

8.17.5 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 8-19: 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 8-20: 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, при 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

Исходный компьютер	Порт	Целевой компьютер	Порт	Действие
Платформа BI – сервер регистрации Siebel	Любой	Siebel	Порт SCBroker	Разрешить
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

8.18 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.

8.18.1 Поддерживаемые обратные прокси-серверы

Платформа BI поддерживает следующие обратные прокси-серверы:

- IBM Tivoli Access Manager WebSEAL 6
- Apache 2.2
- Microsoft ISA 2006

8.18.2 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, например, для развертывания следующих WAR-файлов:

- **BOE:** включает Central Management Console (CMC), стартовую панель BI и Open Document
- **dswsbobje:** содержит приложение веб-служб

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.

8.19 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.

8.19.1 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-файла 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

Файл BOE.war содержит глобальные свойства и свойства конкретного приложения. Если необходимо изменить свойства, используйте настраиваемый каталог конфигурации. По умолчанию

каталог имеет адрес `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Предупреждение:

Чтобы не перезаписывать файлы в каталоге по умолчанию, не изменяйте свойства в каталоге `config\default`. Пользователи должны обратиться к каталогу `custom`.

Примечание:

На некоторых серверах веб-приложений, например в версии Tomcat, поставляемой с платформой BI, возможен прямой доступ к файлу `BOE.war`. В таком случае можно задать пользовательские настройки напрямую, без отмены развертывания WAR-файла. При отсутствии доступа к файлу `BOE.war` необходимо отменить развертывание файла, изменить файл и развернуть его повторно.

Последовательное использование прямой наклонной черты (/)

Задавайте контекстные пути в обратном прокси-сервере таким же образом, как они вводятся в URL-адресе в браузере. Например, если директива содержит символ прямой наклонной черты (/) в конце пути зеркала на обратном прокси-сервере, введите / 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.

8.19.2 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.

8.19.3 Настройка обратного прокси-сервера Apache 2.2 для платформы BI

В этом разделе представлен рабочий процесс по настройке совместной работы платформы BI и Apache 2.2.

1. Убедитесь, что платформа BI и Apache 2.2 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. Например:

```
ProxyPass /C1/BOE/ http://<appservername>:80/BOE/
ProxyPassReverseCookiePath / /C1/BOE
ProxyPassReverse /C1/BOE/ http://<appservername>:80/BOE/
ProxyPass /C1/explorer/ http://<appservername>:80/explorer/
ProxyPassReverseCookiePath / /C1/explorer
ProxyPassReverse /C1/explorer/ http://<appservername>:80/explorer/
```

8.19.4 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 (например, **sec_master**) через учетную запись пользователя с правами администратора.
4. Введите следующую команду в подсказке **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
```

8.19.5 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 сети

Теперь 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 «Общедоступное имя» выберите параметр **Запрос для следующих веб-сайтов** 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 соединения. 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.

8.20 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.

8.20.1 Включение обратного прокси-сервера для веб-служб

В этом разделе описаны процедуры, необходимые для включения обратных прокси-серверов для веб-служб.

8.20.1.1 Активация обратного прокси на Tomcat

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 ОС Windows, `server.xml` находится в папке `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf`

В ОС UNIX `server.xml` находится в папке `<CATALINA_HOME>/conf`. Значением по умолчанию для `<CATALINA_HOME>` является `<INSTALLDIR>/sap_bobj/tomcat`.

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.

8.20.1.2 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/BICatalog`
- `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.

8.20.2 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.

8.20.2.1 Настройка Apache Tomcat

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.

8.20.2.2 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.

8.20.2.3 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.

8.20.2.4 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.

8.20.3 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.

8.20.3.1 Настройка URL средства просмотра по умолчанию с использованием CMC

1. Выполните вход в CMC.
2. На странице «Приложения» щелкните элемент **Central Management Console**.

3. Выберите команду **Действия > Настройка обработки**.
4. В поле **URL** выберите правильный URL-адрес средства просмотра по умолчанию и нажмите кнопку **Сохранить и закрыть**.

Например:

```
http://ОбратныйПроксиСервер:ПортОбратногоПроксиСерве  
ра/ВОЕ/OpenDocument.jsp?sIDType=CUID&iDocID=%SI_CUID%
```

Параметры `ReverseProxyServer` и `ReverseProxyServerPort` представляют правильные имя обратного прокси-сервера и его порт прослушивания.

Аутентификация

9.1 Параметры аутентификации платформы BI

Аутентификация представляет собой процесс проверки идентичности пользователя, пытающегося получить доступ к системе, тогда как управление правами – 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

- [Общая информация об аутентификации Enterprise](#)
- [Настройка аутентификации SAP](#)
- [Использование аутентификации LDAP](#)
- [Требования к поддержке Windows AD и исходная настройка](#)
- [Включение аутентификации JD Edwards EnterpriseOne](#)
- [Разрешение аутентификации Oracle EBS](#)
- [Включение аутентификации PeopleSoft Enterprise](#)
- [Включение аутентификации Siebel](#)

9.1.1 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 другой метод аутентификации, то 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.

9.1.2 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 аутентификацией в СМС.

Примечание:

Подключаемый модуль безопасности Windows AD не может выполнять аутентификацию пользователей, если компоненты сервера платформы BI выполняются под управлением ОС UNIX.

9.1.3 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.

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.

9.1.3.1 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
- LDAP через Kerberos в ОС SUSE 11
- SAP NetWeaver SSO через доверительную аутентификацию

Примечание:

Windows AD с Kerberos поддерживается для приложений Java под управлением ОС UNIX. При этом 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 CMC 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 CMC встроена в продукт и доступна сразу после установки. Для использования функции единого входа в стартовую панель BI и CMC требуется модуль SiteMinder.
Enterprise	Любая поддерживаемая платформа	Доверительная аутентификация	Аутентификация Enterprise для стартовой панели BI и CMC встроена в продукт и доступна сразу после установки. Единый вход с аутентификацией Enterprise для стартовой панели BI и CMC требует доверительной аутентификации.

- [Единый вход на платформу BI](#)
- [Единый вход в базу данных](#)
- [Сквозной единый вход](#)

9.1.3.2 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.

9.1.3.3 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.

9.2 Аутентификация Enterprise

9.2.1 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).

9.2.2 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	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.

Настройки	Параметры	Описание
	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.
Синхронизация учетных данных для входа в систему и источника 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	Доверительная аутентификация включена	Позволяет использовать параметры для настройки доверительной аутентификации.

См. также

- [Включение доверительной аутентификации](#)

9.2.3 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.

9.2.3.1 Изменение общих настроек пароля

Примечание:

Учетные записи, неиспользуемые в течение длительного времени, не деактивируются автоматически. Администраторы должны вручную удалить неактивные учетные записи.

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.

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**.

Примечание:

Неактивные учетные записи Enterprise не отключаются автоматически. Такие учетные записи должны удаляться вручную системными администраторами.

9.2.4 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](#)

9.2.4.1 Настройка сервера на использование доверительной аутентификации

Перед настройкой доверительной аутентификации требуется создать пользователей Enterprise или сопоставленных пользователей третьей стороны, которые должны выполнить вход в платформу BI.

1. Выполните вход в СМС.

2. Перейдите в область управления «Аутентификация».

3. Нажмите параметр **Enterprise**.

Появится диалоговое окно «Enterprise».

4. В области «Доверительная аутентификация»:

a. Выберите **Доверительная аутентификация включена**.

b. Нажмите **Новый общий секретный ключ**.

Появится сообщение **Общий секретный ключ создается**, после чего он готов к загрузке.

c. Нажмите **Загрузить общий секретный ключ**.

Общий секретный ключ используется клиентом и сервером CMS, чтобы установить доверительные отношения. Необходимо сначала настроить сервер, а затем клиент для доверительной аутентификации.

Откроется диалоговое окно «Загрузка файла».

d. Нажмите **Сохранить** и сохраните файл `TrustedPrincipal.conf` в одном из следующих каталогов:

- `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\`
- `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`

Предупреждение:

Не устанавливайте для времени ожидания значение 0 (ноль). Значение 0 означает неограниченное время различия между двумя показаниями часов, что может увеличить уязвимость при атаках повторного воспроизведения.

e. В поле **Период действия совместно используемого секретного ключа** введите число дней действия совместно используемого секретного ключа.

f. Укажите максимальную допустимую разницу в миллисекундах между показаниями часов на клиентском компьютере и на сервере CMS для запросов доверительной аутентификации.

5. Нажмите кнопку **Обновить**, чтобы передать в систему общий секретный ключ.

Платформа BI не проверяет все изменения параметров доверительной аутентификации. Вы должны вручную создать резервную копию данных доверительной аутентификации.

Клиентом и CMS используется общий секретный ключ для установки доверительных отношений. Следующим шагом является настройка клиента для доверительной аутентификации.

9.2.5 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 панели запуска BI и OpenDocument.

Используйте один из следующих методов для передачи общего секретного ключа на клиент:

- Параметр `WEB_SESSION`
- Файл `TrustedPrincipal.conf`

Используйте один из следующих методов для передачи имени пользователя на клиент:

- `REMOTE_USER`
- `HTTP_HEADER`
- `COOKIE`
- `QUERY_STRING`
- `WEB_SESSION`
- `USER_PRINCIPAL`

Независимо от того, как передается общий секретный ключ, используемый метод должен быть настроен в глобальных свойствах `Trusted.auth.user.retrieval` файла `BOE.war`.

9.2.5.1 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.

Кроме того, необходимо использовать один из этих методов для передачи имени пользователя клиенту:

- `REMOTE_USER`
- `USER_PRINCIPAL`

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`.

9.2.5.2 Свойства доверительной аутентификации для веб-приложений

В следующей таблице перечислены настройки доверительной аутентификации в файле `global.properties` по умолчанию 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 и отключает единый вход в платформу BI. Чтобы включить доверительную аутентификацию, установите 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	<p>Задаёт метод, используемый для извлечения имени пользователя для доверительной аутентификации:</p> <ul style="list-style-type: none"> • <code>REMOTE_USER</code> • <code>HTTP_HEADER</code> • <code>COOKIE</code> • <code>QUERY_STRING</code> • <code>WEB_SESSION</code> • <code>USER_PRINCIPAL</code> <p>Чтобы отключить доверительную аутентификацию, установите пустое значение.</p>
<code>trusted.auth.saml.enabled</code>	Нет	<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.</p> <p>Если свойство пустое, в доверительной аутентификации будет использоваться сопоставление имен при аутентификации пользователей.</p>

9.2.5.3 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	<ul style="list-style-type: none"> <code><INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\</code> <code><INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\</code>
AIX	<code><INSTALLDIR>/sap_bobj/enterprise_xi40/ aix_rs6000/</code>
Solaris	<code><КАТАЛОГ_УСТАНОВКИ>/sap_bobj/enterprise_xi40/solaris_sparc/</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. Дополнительную информацию см. в разделе <http://java.sun.com/j2ee/1.4/docs/api/javax/servlet/http/HttpServletRequest.html>.

Чтобы настроить доверительную аутентификацию для клиента, нужно открыть и изменить глобальные свойства для файла `BOE.war`, к которым относятся общие и конкретные свойства веб-приложений панели запуска BI и OpenDocument.

Примечание:

В зависимости от предполагаемого способа извлечения имени пользователя и общего секретного ключа могут потребоваться дополнительные шаги.

1. Откройте пользовательскую папку с файлом `BOE.war` на компьютере, на котором размещаются веб-приложения:

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

Затем необходимо повторно развернуть измененный файл `BOE.war`.

2. Создайте новый файл с помощью Блокнота или другого текстового редактора.
3. Введите следующие свойства доверенной аутентификации:

```
sso.enabled=true
trusted.auth.user.retrieval=Method for user ID retrieval
trusted.auth.user.param=Variable
trusted.auth.shared.secret=WEB_SESSION
```

Для свойства `trusted.auth.shared.secret` выберите один из следующих параметров получения имени пользователя:

Параметр	Способ получения имени пользователя
HTTP_HEADER	Имя пользователя извлекается из содержимого заголовка HTTP. Необходимо указать заголовок HTTP, который будет использоваться в свойстве <code>trusted.auth.user.param</code> .
QUERY_STRING	Имя пользователя извлекается из 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> .
REMOTE_USER	Имя пользователя извлекается из вызова <code>HttpServletRequest.getRemoteUser()</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:

- Некоторые серверы веб-приложений требуют, чтобы переменной среды `REMOTE_USER` было присвоено значение `true` на сервере. Чтобы узнать, является ли это обязательным, изучите документацию вашего сервера веб-приложений. Если это необходимо, убедитесь, что значение переменной среды равно `true`.
- Если для передачи имени пользователя используется параметр `USER_PRINCIPAL` или `REMOTE_USER`, оставьте свойство `trusted.auth.user.param` пустым.

4. Сохраните файл с 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*.

9.2.5.3.1 Примеры конфигурации

Передача общего секретного ключа с помощью файла TrustedPrincipal.conf

В следующем примере конфигурации предполагается, что в платформе BI создан пользователь «JohnDoe».

Информация о пользователе хранится и передается с помощью веб-сеанса, а общий секретный ключ передается через файл TrustedPrincipal.conf, расположенный по умолчанию в каталоге C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86. Пакетная версия Tomcat представляет собой сервер веб-приложений.

1. Создайте новый файл в каталоге <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\, используя Блокнот или другой текстовый редактор.
2. Чтобы задать свойства доверительной аутентификации, введите следующие значения:

```
sso.enabled=true
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.user.param=MyUser
trusted.auth.shared.secret=
```

3. Сохраните файл с именем global.properties.
4. Откройте файл C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp.
5. Измените содержимое файла, включив в него следующие значения:

```
<!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>
```

6. Создайте файл myScript.js в каталоге C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomResources.

7. Добавьте в myScript.js следующие значения:

```
function goToLogonPage() {
    window.location = "logon.jsp"; }
```

8. Перезапустите сервер веб-приложений.

9. Воспользуйтесь Wdeploy для повторного развертывания WAR-файла на сервере веб-приложений.

Для получения сведений об использовании WDeploy см. *Руководство по развертыванию веб-приложений платформы BusinessObjects Business Intelligence*.

Для проверки правильности настройки доверительной аутентификации воспользуйтесь следующим URL-адресом для доступа к стартовой панели BI:

`http://[cmsname]:8080/BOE/BI/custom.jsp`, где `[cmsname]` задает имя компьютера, на котором установлен CMS. Должна появиться следующая ссылка: Щелкните здесь, 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 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 при помощи текстового редактора.

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\SAP BusinessObjects Enterprise
XI 4.0\warfiles\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", "9ecb0778edcfc048edae0fcdde1a5db82112934
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\SAP BusinessObjects Enterprise
XI 4.0\warfiles\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. Перезапустите сервер веб-приложений.

10. Воспользуйтесь Wdeploy для повторного развертывания WAR-файла на сервере веб-приложений.

Для получения сведений об использовании WDeploy см. *Руководство по развертыванию веб-приложений платформы BusinessObjects Business Intelligence*.

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 создание пользователя «JohnDoe» в платформе BI.

Информация о пользователе хранится и передается с помощью параметра "Принципал пользователя", а общий секретный ключ передается через файл `TrustedPrincipal.conf`, расположенный по умолчанию в каталоге `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. Пакетная версия Tomcat представляет собой сервер веб-приложений.

1. Остановите сервер Tomcat.

- Откройте файл `server.xml` для Tomcat, по умолчанию находящийся в каталоге `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf\`.

- Найдите строку `<Realm`
`className="org.apache.catalina.realm.UserDatabaseRealm"..../>` и поменяйте ее на следующее значение:

```
Realm className="orgapachecatalinarealmMemoryRealm".../
```

- Откройте файл `tomcat-users.xml`, по умолчанию находящийся в каталоге `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf\`.

- В теге `<tomcat-users>` измените следующее значение:

```
<user name="JohnDoe" password="password"
roles="onjavauser"/>
```

- Откройте файл `web.xml` в каталоге `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`.

- Перед тегом `</web-app>` добавьте следующие значения:

```
<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>
```

Введите 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.

- В пользовательском файле `global.properties` введите следующие значения:

```
trusted.auth.user.retrieval=USER_PRINCIPAL
trusted.auth.user.namespace.enabled=true
```

Примечание:

Необязательно задавать `trusted.auth.user.namespace.enabled=true`. Добавьте параметр, если требуется сопоставить внешнее имя пользователя с другим именем пользователя BOE.

- Перезапустите сервер веб-приложений.
- Воспользуйтесь Wdeploy для повторного развертывания WAR-файла на сервере веб-приложений.

Для получения сведений об использовании WDeploy см. *Руководство по развертыванию веб-приложений платформы BusinessObjects Business Intelligence*.

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 стартовой панели BI: `http://[cmsname]:8080/BOE/BI`, где `[cmsname]` задает имя компьютера, на котором установлен CMS. Спустя некоторое время отображается диалоговое окно входа в систему.

9.3 Аутентификация LDAP

9.3.1 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 надлежащими правами. LDAP позволяет настроить вход пользователей в платформу BI с помощью аутентификации LDAP. Он предоставляет пользователям права доступа 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 соединения 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](#)

9.3.1.1 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, права доступа 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](#)

9.3.2 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.

9.3.2.1 Настройка хоста LDAP

Рекомендуется установить и запустить сервер LDAP, прежде, чем настраивать хост LDAP.

1. Выберите пункт **Аутентификация** из списка навигации, чтобы перейти к области управления «Аутентификация» на центральной консоли управления.
2. Дважды щелкните **LDAP**.
3. При первой настройке аутентификации LDAP выберите **запуск мастера настройки LDAP**.

4. Введите имя и номер порта хостов LDAP в поле **Добавить хост LDAP (имя хоста:порт)** (например, "myserver:123"), щелкните **Добавить**, а затем щелкните **Далее**.

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**.

5. Выберите в списке **Тип сервера LDAP** тип сервера.

Примечание:

Если выполняется сопоставление LDAP с AD, выберите тип сервера **Сервер Active Directory Application Microsoft**.

6. Если требуется просмотреть или изменить какие-либо сопоставления атрибутов сервера LDAP или атрибуты поиска LDAP по умолчанию, щелкните **Показать отображения атрибутов**.

По умолчанию настроены сопоставления атрибутов сервера и атрибуты поиска каждого поддерживаемого типа сервера.

7. Нажмите кнопку **Далее**.

8. В поле **Базовое характерное имя LDAP** введите характерное имя (например, o=SomeBase) сервера LDAP и нажмите кнопку **Далее**.

9. В области «Реквизиты администрирования сервера LDAP» укажите известное имя и пароль учетной записи, для которой разрешен доступ на чтение каталога.

Учетные данные администратора не обязательны.

Если используемый сервер LDAP позволяет создавать анонимные привязки, оставьте эту область пустой. Серверы и клиенты платформы BI будут создавать привязки к основному хосту через анонимный вход.

10. Если настроены направления на хост LDAP, введите сведения об аутентификации в области «Реквизиты направления LDAP» и укажите число переходов для направления в поле **Максимальное число переходов для направления**.

Необходимо настроить область «Реквизиты направления LDAP», если соблюдаются все указанные ниже условия.

- 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 из хоста, на который осуществляются ссылки, будет сопоставлен 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 характерным именем и паролем.
- Если параметру **Максимальное количество ссылочных узлов маршрутизации** присвоено значение 0, ссылочные переходы осуществляться не будут.

11. Нажмите кнопку **Далее**.

12. Выберите тип используемой аутентификации SSL:

- **Базовая (без SSL)**
- **Аутентификация сервера**
- **Взаимная аутентификация**

В следующем разделе приведены подробные сведения и предварительные условия как для аутентификации сервера, так и для взаимной аутентификации. Перед началом выполнения описанной процедуры обратитесь к разделу *Настройка параметров SSL для LDAP-сервера или взаимной аутентификации* данного документа, в котором приведена информация по настройке аутентификации LDAP с использованием SSL.

13. Нажмите кнопку **Далее** и выберите метод единого входа LDAP:

- **Базовый (без SSO)**
- **SiteMinder**

14. Нажмите кнопку **Далее** и выберите способ сопоставления псевдонимов и пользователей учетным записям платформы BI.

- a. В области «Параметры нового псевдонима» выберите способ сопоставления новых псевдонимов учетным записям Enterprise:

- **Назначить каждый добавленный псевдоним LDAP учетной записи с тем же именем**

Используйте этот вариант, если известно, что у пользователя имеется учетная запись Enterprise с таким же именем, то есть псевдонимы LDAP будут назначены существующим пользователям (автоматическое создание псевдонимов включено). 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 области «Параметры обновления псевдонимов» выберите способ управления обновлениями псевдонимов для учетных записей Enterprise:

- **Создавать новые псевдонимы при обновлении псевдонимов**

Используйте этот вариант для автоматического создания нового псевдонима для каждого пользователя LDAP, сопоставленного платформе BI. Новые учетные записи LDAP добавляются для пользователей, у которых нет учетных записей на платформе BI или для всех пользователей, если был выбран вариант **Создать новую учетную запись для каждого добавленного псевдонима LDAP**.

- **Создавать новые псевдонимы только при входе пользователя в систему**

Используйте этот вариант, если сопоставляемый каталог LDAP включает большое число пользователей, но лишь немногие из них используют 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.

- с. В области «Параметры нового пользователя» укажите способ создания новых пользователей:

- **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 параллельные 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 регулярности и продолжительности работы пользователей с платформой лицензия параллельного доступа на 100 пользователей может обеспечивать работу 250, 500 или 700 пользователей.

15. Этот шаг следует выполнять при настройке сопоставлений атрибутов пользователей, или если планируется импорт адресов электронной почты с сервера LDAP. В области «Параметры привязки атрибутов» укажите приоритет привязки атрибутов для подключаемого модуля LDAP:

а. Щелкните поле **Импорт полного имени, адреса электронной почты и других атрибутов**.

Полные имена и описания, используемые в учетных записях LDAP, импортируются и сохраняются в пользовательских объектах в платформе BI.

б. Укажите значение для параметра **Установка приоритета для привязки атрибута LDAP относительно других привязок атрибутов**.

Примечание:

Если для этого параметра задано значение 1, атрибуты LDAP имеют приоритет в сценариях с включенными подключаемыми модулями LDAP и другими (Windows AD и SAP). Если задано значение 3, приоритет имеют атрибуты из других подключаемых модулей.

16. Нажмите кнопку **Готово**.

См. также

- [Настройка параметров SSL для LDAP-сервера или взаимной аутентификации](#)
- [Настройка подключаемого модуля LDAP для SiteMinder](#)

9.3.2.2 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](#)

9.3.2.3 Настройка параметров SSL для LDAP-сервера или взаимной аутентификации

В данном разделе приведена подробная информация об аутентификации сервера LDAP или обоюдной аутентификации с использованием SSL. Для настройки аутентификации с использованием SSL требуется выполнение некоторых предварительных шагов. В данном разделе также приведена информация о порядке настройки в CMC протокола SSL для аутентификации сервера LDAP или обоюдной аутентификации. Предполагается, что настроен хост LDAP и выбран один из следующих видов SSL-аутентификации:

Для получения дополнительных сведений или сведений о настройке хоста LDAP-сервера см. документацию поставщика LDAP.

См. также

- [Настройка хоста LDAP](#)

9.3.2.3.1 Настройка аутентификации LDAP-сервера или взаимной аутентификации

Ресурс	Выполните это действие перед переходом к данному заданию.
Сертификат CA	<p>Это действие необходимо как для аутентификации сервера, так и для взаимной аутентификации при использовании SSL.</p> <ol style="list-style-type: none"> 1. Нужно, чтобы центр сертификации создал сертификат CA. 2. Добавьте сертификат на сервер LDAP. <p>Дополнительные сведения см. в документации поставщика LDAP.</p>
Сертификат сервера	<p>Это действие необходимо как для аутентификации сервера, так и для взаимной аутентификации при использовании SSL.</p> <ol style="list-style-type: none"> 1. Запросите, а затем создайте сертификат сервера. 2. Авторизовать сертификат и затем добавить его на LDAP-сервер.
cert7.db или cert8.db, key3.db	<p>Эти файлы необходимы как для аутентификации сервера, так и для взаимной аутентификации при использовании SSL.</p> <ol style="list-style-type: none"> 1. Загрузите приложение certutil, которое создает файл cert7.db или cert8.db (в зависимости от требований) на основе ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_6_RTM/. 2. Скопируйте сертификат CA в тот же каталог, в котором находится certutil. 3. Используйте следующую команду для создания файла cert7.db или cert8.db, а также файлов key3.db и secmod.db: <pre>certutil -N -d .</pre> 4. Используйте следующую команду, чтобы добавить сертификат CA в файл cert7.db или cert8.db: <pre>certutil -A -n <CA_alias_name> -t CT -d . -I cacert.cer</pre> 5. Сохраните эти три файла в каталоге на компьютере, где размещена платформа Business Intelligence (BI).
cacerts	<p>Этот файл необходим для аутентификации сервера или взаимной аутентификации при использовании SSL для приложений Java, таких как стартовая панель BI.</p> <ol style="list-style-type: none"> 1. Перейдите к своему файлу keytool в каталоге bin Java. 2. Воспользуйтесь следующей командой для создания файла cacerts: <pre>keytool -import -v -alias <CA_alias_name> -file <CA_certificate_name> -trustcacerts -keystore</pre> 3. Сохраните файл cacerts в тот же каталог, в котором хранятся файлы cert8.db или cert7.db, а также файлы key3.db.
Сертификат клиента	

Ресурс	Выполните это действие перед переходом к данному заданию.
	<ol style="list-style-type: none"> Создайте отдельные клиентские запросы для файла <code>cert7.db</code> или <code>cert8.db</code> и файлов <code>.keystore</code>: <ul style="list-style-type: none"> Чтобы настроить подключаемый модуль LDAP, используйте приложение <code>certutil</code> для создания запроса клиентского сертификата. Используйте следующую команду для создания запроса клиентского сертификата: <pre>certutil -R -s "<client_dn>" -a -o <certificate_request_name> -d .</pre> <p><code><client_dn></code> содержит такую информацию, как "CN=<имя_клиента>, OU=организационное подразделение, O=Название_компании, L=город, ST=область, C=страна.</p> Используйте CA для аутентификации запроса сертификата. Используйте следующую команду, чтобы извлечь сертификат и вставить его в файл <code>cert7.db</code> или <code>cert8.db</code>: <pre>certutil -A -n <client_name> -t Pu -d . -I <client_certificate_name></pre> Реализация аутентификации Java с помощью SSL: <ul style="list-style-type: none"> Используйте утилиту <code>keytool</code> в каталоге <code>bin</code> Java, чтобы создать запрос клиентского сертификата. Используйте следующую команду, чтобы создать пару ключей: <pre>keytool -genkey -keystore .keystore</pre> После указания сведений о клиенте воспользуйтесь такой командой для создания запроса сертификата клиента: <pre>keytool -certreq -file <certificate_request_name> -keystore .keystore</pre> После аутентификации запроса клиентского сертификата центром сертификации используйте следующую команду, чтобы добавить сертификат CA в файл <code>.keystore</code>: <pre>keytool -import -v -alias <CA_alias_name> -file <ca_certificate_name> -trustcacerts -keystore .keystore</pre> Получите запрос клиентского сертификата от CA и используйте следующую команду, чтобы добавить его в файл <code>.keystore</code>: <pre>keytool -import -v -file <client_certificate_name> -trustcacerts -keystore .keystore</pre> Сохраните файл <code>.keystore</code> в тот же каталог, в котором хранится файл <code>cert7.db</code> или <code>cert8.db</code>, а также файл <code>cacerts</code> на компьютере, где размещена платформа BI.

1. Выберите уровень SSL-защиты.

Если используется мастер по настройке LDAP при первой настройке аутентификации LDAP, выберите **Взаимная аутентификация** в списке «типов аутентификации SSL» и нажмите

кнопку **Далее**. Или, при изменении настроек аутентификации LDAP, перейдите в область **СМС Аутентификация** и дважды щелкните **LDAP**. Будет открыта страница «Сводка по настройке сервера LDAP». Щелкните значение **типа SSL** и выберите **Взаимная аутентификация** в списке «типов аутентификации SSL».

- **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 доверенного 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 доверенного центра сертификации, и атрибут CN этого сертификата соответствует имени хоста DNS данного сервера**

Это максимальный 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. Чтобы проверить сертификат, платформа BI должна найти СА, выдавший сертификат, в своей базе данных сертификатов, и подтвердить, что атрибут CN в сертификате сервера полностью совпадает с именем хоста LDAP, введенным в поле **Добавить хост LDAP** на первом шаге мастера (если имя хоста LDAP введено как ABALONE.rd.crystald.net:389. (Нельзя использовать CN =ABALONE:389 в сертификате.)

Имя хоста сертификата безопасности сервера – это имя основного хоста LDAP. Если выбрать этот вариант, то нельзя будет использовать резервный хост LDAP.

Примечание:

Java-приложения будут игнорировать первый и последний вариант и будут принимать сертификат сервера только в том случае, если он поступает от надежного центра сертификации.

2. В поле **Хост SSL** введите имя хоста каждого из компьютеров и нажмите кнопку **Добавить**. Затем необходимо добавить имя хоста каждого компьютера в развертывание платформы BI, использующее пакет SDK платформы BI. (Включая компьютер с центральным сервером управления и компьютер с сервером веб-приложений.)
3. Укажите параметры SSL для каждого хоста SSL, добавленного в список:
 - a. Выберите значение **по умолчанию** в списке SSL.
 - b. Снимите флажки **Использовать значение по умолчанию**.
 - c. Введите значения в поля **Путь к файлам сертификатов и базы данных ключей** и **Пароль для базы данных ключей**.

- d. При указании настроек для взаимной аутентификации введите значение в поле **Псевдоним для сертификата клиента в базе данных сертификатов**.

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.

4. Введите параметры по умолчанию для каждого хоста, не присутствующего в списке, и нажмите кнопку **Далее**.

Чтобы ввести параметры для другого хоста, выберите его имя в списке слева и введите значения в поля справа.

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.

5. Выберите метод единого входа LDAP **Базовая (без SSL)** или **SiteMinder**.
6. Выберите способ создания пользователей и псевдонимов LDAP.
7. Щелкните **Готово**.

См. также

- [Настройка подключаемого модуля LDAP для SiteMinder](#)

9.3.2.4 Изменение параметров конфигурации LDAP

После настройки аутентификации LDAP с использованием мастера настройки LDAP можно изменить параметры соединения LDAP и группы-члены на странице «Сводка по настройке сервера LDAP».

1. Перейдите в область управления СМС **Аутентификация**.
2. Дважды щелкните **LDAP**.

Если настроена аутентификация LDAP, будет открыта страница «Сводка по настройке сервера LDAP». На этой странице можно изменять любые области или поля параметров соединения, а также изменять параметры в области «Группы элементов LDAP с установленным соответствием».

3. Удалите сопоставленные группы, которые будут недоступны при использовании новых параметров подключения, и щелкните **Обновить**.
Для удаления сопоставленной группы выберите группу пользователя и нажмите кнопку **Удалить** в области «Группы элементов LDAP с установленным соответствием».
4. Измените параметры соединения и щелкните **Обновить**.

5. При необходимости измените «Параметры нового псевдонима», «Параметры обновления псевдонимов» и «Параметры нового пользователя» и нажмите кнопку **Обновить**.
6. Сопоставьте новые группы элементов LDAP и нажмите кнопку **Обновить**.

9.3.2.5 Настройка подключаемого модуля LDAP для SiteMinder

В этом разделе описана настройка CMC 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, подключаемый через центральную консоль управления
- Свойства файла `BOE.war`

Примечание:

Администратор SiteMinder должен включить поддержку агентов версии 4.x. Это необходимо сделать независимо от используемой поддерживаемой версии SiteMinder. Для получения дополнительных сведений о средстве SiteMinder и его установке см. в документации SiteMinder.

См. также

- [Настройка хоста LDAP](#)

9.3.2.5.1 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 единого входа LDAP» мастера 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**. Повторно введите совместно используемый секретный ключ в поле «подтверждения совместно используемого секретного ключа».
5. Нажмите кнопку **Далее**.
6. Переходите к настройке параметров LDAP.

9.3.2.5.2 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 к каталогу <КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\ в каталоге установки платформы BI.
2. Создайте новый файл с помощью Блокнота или другого текстового редактора.
3. Введите следующее выражение:

```
siteminder.authentication=secLDAP  
siteminder.enabled=true
```

4. Закройте файл и сохраните его с именем global.properties без расширения файла.
5. Создайте другой файл в этом же каталоге.
6. Введите следующее выражение:

```
authentication.default=secLDAP  
cms.default=[your cms name]:[the CMS port number]
```

Например:

```
authentication.default=secLDAP  
cms.default=mycms:6400
```

7. Закройте файл и сохраните его с именем bilaunchpad.properties.

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 сведений об использовании WDeploy см. *Руководство по развертыванию веб-приложений платформы BusinessObjects Business Intelligence*.

9.3.3 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 аутентификация LDAP, в области "Группы элементов LDAP с установленным соответствием" отображаются группы LDAP, сопоставленные платформе BI.

Примечание:

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](#)

9.3.3.1 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 элементов LDAP с установленным соответствием» укажите группу LDAP (по общему или отличительному имени) в поле **Добавить группу LDAP (по cn или dn)** и нажмите кнопку **Добавить**.

Чтобы добавить дополнительные группы LDAP, повторите этот шаг. Чтобы удалить группу LDAP, выберите ее и щелкните **Удалить**.

4. В области «Параметры нового псевдонима» выберите соответствующий параметр, чтобы указать способ сопоставления псевдонимов LDAP учетным записям Enterprise:
 - **Назначить каждый добавленный псевдоним LDAP учетной записи с тем же именем**

Используйте этот вариант, если известно, что у пользователя имеется учетная запись Enterprise с таким же именем (то есть псевдонимы LDAP будут назначены существующим пользователям, автоматическое создание псевдонимов включено). 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.

- **Создать новую учетную запись для каждого добавленного псевдонима LDAP**

Данный параметр используется в случае, когда необходимо создавать учетную запись для каждого пользователя.

5. В области «Параметры обновления псевдонимов» выберите параметр, чтобы указать, нужно ли автоматически создавать псевдонимы LDAP для всех новых пользователей:

- **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 на платформе BI или для всех пользователей, если был выбран вариант **Создать новую учетную запись для каждого добавленного псевдонима LDAP** и нажата кнопка **Обновить**.

- **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 BI.

6. В области «Параметры нового пользователя» (если используемая лицензия на платформу BI учитывает роли пользователей) выберите параметр, чтобы указать свойства новых учетных записей Enterprise, которые создаются для сопоставления учетным записям LDAP:

- **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 параллельные пользователи**

Новые учетные записи пользователей настраиваются на использование пользовательских лицензий на одновременный доступ. 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. Нажмите **Обновить**.

9.3.3.2 Отмена сопоставления групп LDAP с использованием платформы BI

1. Перейдите в область управления СМС **Аутентификация**.
2. Дважды щелкните **LDAP**.
Если настроена аутентификация LDAP, откроется страница сводной информации LDAP.
3. В области "Группы элементов 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**.

9.3.3.3 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 участниками групп AD по умолчанию, не смогут осуществлять вход. Пользователи также должны быть участниками 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.

9.3.3.4 Настройка функции единого входа в базу данных SAP HANA с помощью подключаемого модуля LDAP

В данном разделе описываются действия, которые администратор должен выполнить для настройки единого входа (SSO) между платформой BI в системе SUSE Linux 11 и базой данных SAP HANA. Аутентификация LDAP с использованием Kerberos позволяет пользователям AD проходить аутентификацию на платформе BI в системе Linux, например SUSE. Данный сценарий также поддерживает единый вход в SAP HANA в качестве базы данных отчетов.

Примечание:

Сведения о настройке базы данных SAP HANA см. в документе *База данных SAP HANA. Руководство по установке и настройке сервера*. Сведения о настройке компонента Data Access для SAP HANA см. в *руководстве по Data Access*.

Общие сведения о реализации

Следующие компоненты необходимы для работы единого входа Kerberos.

Компонент	Требование
Контроллер домена	Должен размещаться на компьютере с установленной средой Active Directory, которая обеспечивает поддержку аутентификации Kerberos.
Центральный сервер управления	Должен быть установлен и запущен на компьютере под управлением SUSE Linux Enterprise 11 (SUSE).
Клиент Kerberos V5	Устанавливается вместе с необходимыми утилитами и библиотеками на хосте SUSE. Примечание: Используйте последнюю версию клиента Kerberos V5. Добавьте папки <code>bin</code> и <code>lib</code> в переменные среды <code>PATH</code> и <code>LD_LIBRARY_PATH</code> .
Подключаемый модуль аутентификации LDAP	Включено на хосте SUSE.
Файл конфигурации входа Kerberos	Создано на компьютере, на котором размещается сервер веб-приложений.

Рабочий процесс реализации

Следующие задачи необходимо выполнить, чтобы позволить пользователям платформы BI применять единый вход в SAP HANA с использованием аутентификации Kerberos через JDBC.

1. Настройка хоста AD.
2. Создание учетных записей и файлов ярлыков ключей для хоста SUSE и платформы BI на хосте AD.
3. Установка ресурсов Kerberos на хосте SUSE.
4. Настройка хоста SUSE для аутентификации Kerberos.
5. Настройка параметров Kerberos в подключаемом модуле аутентификации LDAP.
6. Создание файла конфигурации входа Kerberos для хоста веб-приложений.

9.3.3.4.1 Настройка контроллера домена

Может потребоваться настроить доверенные отношения между хостом SUSE и контроллером домена. Если хост SUSE расположен на контроллере домена Windows, настраивать доверенные отношения не требуется. Но если платформа BI и контроллер домена развернуты в различных доменах, может потребоваться настроить доверенные отношения между компьютером SUSE с Linux и контроллером домена. Для этого необходимо выполнить следующие действия.

1. Создать учетную запись пользователя для компьютера SUSE с платформой BI.
2. Создать имя участника-службы (SPN).

Примечание:

SPN-имя должно быть отформатировано в соответствии с соглашениями Windows AD: `хост/имя_хоста@ИМЯ_СФЕРЫ_DNS`. Для `/имя_хоста` используйте полное доменное имя (строчными буквами). `ИМЯ_СФЕРЫ_DNS` должно быть указано прописными буквами.

3. Выполните команду настройки ярлыков ключей Kerberos, `ktpass`, чтобы связать SPN с учетной записью пользователя:

```
c:\> ktpass -princ host/hostname@DNS_REALM_NAME-mapuser username -pass Password1 -crypto RC4-HMAC-NT -out usernamebase.keytab
```

Следующие действия необходимо выполнить на компьютере, на котором размещен контроллер домена.

1. Создайте учетную запись пользователя для службы, применяемой для работы платформы BI.
2. На странице «Учетные записи пользователя» щелкните правой кнопкой новую учетную запись службы и выберите **Свойства > Делегирование**.
3. Выберите пункт **Доверять этому пользователю делегирование служб (только Kerberos)**.
4. Выполните команду настройки ярлыков ключей Kerberos, `ktpass`, чтобы создать учетную запись SPN для новой учетной записи службы:

```
c:\>ktpass -princ sianame/service_name@DNS_REALM_NAME -mapuser service_name -pass password -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT -out sianame.keytab
```

Примечание:

SPN-имя должно иметь формат в соответствии с соглашениями Windows AD: `sianame/имя_службы@ИМЯ_СФЕРЫ_DNS`. Укажите `имя_службы` строчными буквами, иначе платформа SUSE не сможет разрешить его. `ИМЯ_СФЕРЫ_DNS` должно быть указано прописными буквами.

Параметр	Описание
-princ	Указывает имя принципала для аутентификации Kerberos.
-out	Имя создаваемого файла ярлыков ключей Kerberos. Оно должно совпадать со значением <code>sianame</code> , которое используется в -princ.
-mapuser	Имя учетной записи пользователя, с которой сопоставляется имя администратора доступа к службе (SPN). Server Intelligence Agent работает под этой учетной записью.

Параметр	Описание
-pass	Задаёт пароль, используемый учётной записью службы.
-ptype	Задаёт тип администратора доступа: -ptype KRB5_NT_PRINCIPAL
-crypto	Задаёт используемый для учётной записи службы тип шифрования: -crypto RC4-HMAC-NT

Вы создали необходимые файлы ярлыков ключей для доверенных отношений между компьютером SUSE и контроллером домена.

Необходимо переместить файлы ярлыков ключей на компьютер SUSE и сохранить их в каталоге /etc.

9.3.3.4.2 Настройка компьютера SUSE Linux Enterprise 11

Следующие ресурсы необходимы для настройки Kerberos на компьютере SUSE Linux с платформой BI:

- Файлы ярлыков ключей, созданные на контроллере домена. Файл ярлыков ключей для службы платформы BI является обязательным. Ярлык ключа для хоста SUSE рекомендуется для тех ситуаций, когда хост платформы BI и контроллера домена размещены в разных доменах.
- Последняя версия библиотеки Kerberos V5 (в том числе клиент Kerberos) должна быть установлена на хосте SUSE. Необходимо добавить расположение двоичных файлов в переменные среды PATH и LD_LIBRARY_PATH. Чтобы проверить правильность установки и настройки клиента Kerberos, убедитесь, что следующие утилиты и библиотеки присутствуют на хосте SUSE:

- kinit
- ktutil
- kdestroy
- klist
- /lib64/libgssapi_krb5.so.2.2
- /lib64/libkrb5.so.3.3
- /lib/libkrb5support.so.0.1
- /lib64/libk5crypto.so.3
- /lib64/libcom_err.so.2

Совет:

Выполните команду `rpm -qa | grep krb`, чтобы проверить версию этих библиотек. Сведения о последней версии клиента, библиотек Kerberos, а также конфигурации хоста Unix см. в разделе <http://web.mit.edu/Kerberos/krb5-1.9/krb5-1.9.2/doc/krb5-install.html#Installing%20Kerberos%20V5>.

После установки всех необходимых ресурсов на хосте SUSE следуйте инструкциям, указанным далее, чтобы настроить аутентификацию Kerberos.

Примечание:

Для выполнения этих действий требуются права доступа уровня root.

1. Чтобы объединить файлы ярлыков ключей, выполните следующую команду:

```
> ktutil
ktutil: rkt <susemachine>.keytab
ktutil: rkt <BI platform service>.keytab
ktutil: wkt /etc/krb5.keytab
ktutil:q
```

2. Измените файл `/etc/krb5.conf`, чтобы указать контроллер домена (на платформе Windows) как контроллер домена Kerberos (KDC).

Используйте пример ниже:

```
[domain_realm]
.name.mycompany.corp = DOMAINNAME.COM
.name.mycompany.corp = DOMAINNAME.COM

[libdefaults]
    forwardable = true
    default_realm = DOMAINNAME.COM
    default_tkt_enctypes = rc4-hmac
    default_tgs_enctypes = rc4-hmac

[realms]
    DOMAINNAME.COM = {
        kdc = machinename.domainname.com
    }
```

Примечание:

Файл `krb5.conf` содержит данные конфигурации Kerberos, в том числе расположение KDC и серверов для требуемых сфер Kerberos, приложений Kerberos и сопоставлений имен хостов со сферами Kerberos. Обычно файл `krb5.conf` устанавливается в каталог `/etc`.

3. Добавьте контроллер домена в каталог `/etc/hosts`, чтобы хост SUSE мог найти KDC.
4. Запустите программу `kinit` из каталога `/usr/local/bin`, чтобы проверить правильность настройки Kerberos. Убедитесь, что учетная запись пользователя AD может войти на компьютер SUSE.

Совет:

KDC должен выдать тикет предоставления тикета (TGT), который можно просмотреть в кэше. Используйте программу `klist` для просмотра TGT.

Пример:

```
> kinit <AD user>
Password for <AD user>@<domain>: <AD user password>

> klist
Ticket cache: FILE:/tmp/krb5cc_0Default principal: <AD user>@<domain>
Valid starting Expires Service principal
08/10/11 17:33:43 08/11/11 03:33:46 krbtgt/<domain>@<domain>renew
until 08/11/11 17:33:43
Kerberos 4 ticket cache: /tmp/tkt0klist: You have no tickets cached

>klist -k
Keytab name: FILE:/etc/krb5.keytabKVNO Principal=3hdb/<FQDN>@<Domain>
```

Также используйте программу `kinit` для проверки SPN.

9.3.3.4.3 Настройка параметров аутентификации Kerberos для LDAP

Перед настройкой аутентификации Kerberos для LDAP сначала требуется активировать и настроить подключаемый модуль аутентификации LDAP платформы BI для подключения к каталогу AD. Для использования аутентификации LDAP сначала необходимо настроить соответствующий каталог LDAP.

Примечание:

После запуска «мастера настройки LDAP» необходимо указать **Сервер приложений Microsoft Active Directory** и ввести нужные данные конфигурации.

После включения аутентификации LDAP и подключения к серверу приложений Microsoft Active Directory область «Включить аутентификацию Kerberos» будет отображена на странице "Сводка по настройке сервера LDAP". Используйте эту область для настройки аутентификации Kerberos, которая требуется для единого входа в базу данных SAP HANA из платформы BI, развернутой в системе SUSE.

1. Перейдите в область управления СМС **Аутентификация**.

2. Дважды щелкните **LDAP**.

Откроется страница «Сводка по настройке сервера LDAP», на которой можно изменить любые параметры соединения и поля.

3. Для настройки аутентификации Kerberos выполните следующие действия в области «Включить аутентификацию Kerberos»:

- a. Щелкните **Включить аутентификацию Kerberos**.
- b. Щелкните **Контекст безопасности кэша (требуется для SSO в базе данных)**.

Примечание:

Включение контекста безопасности кэша требуется, в частности, для единого входа в SAP HANA.

- c. Укажите SPN для учетной записи платформы BI в поле «Имя администратора доступа к службе».

Формат для указания SPN — `sianame/служба@ИМЯ_СФЕРЫ_DNS`, где

<code>sianame</code>	Имя SIA
<code>служба</code>	Имя учетной записи службы, используемой для работы платформы BI
<code>ИМЯ_СФЕРЫ_DNS</code>	Доменное имя контроллера домена прописными буквами

Совет:

При указании SPN помните, что аргумент *sianame/служба* учитывает регистр.

d. Укажите домен для контроллера домена в поле «Область Kerberos по умолчанию».

e. Укажите `userPrincipalName` в поле **Имя принципа пользователя**.

Это значение используется приложением аутентификации LDAP для указания значений идентификатора пользователя, необходимых для Kerberos. Указанное значение должно совпадать с именем, введенным при создании файлов ярлыков ключей.

4. Нажмите кнопку **Обновить**, чтобы отправить и сохранить изменения.

Вы настроили параметры аутентификации Kerberos для указания учетных записей пользователей в каталоге AD.

Требуется создать файл конфигурации входа Kerberos, `bscLogin.conf`, чтобы активировать вход в систему Kerberos и единый вход.

См. также

- [Настройка аутентификации LDAP](#)

9.3.3.4.4 Создание файла конфигурации входа Kerberos

Чтобы активировать вход в систему Kerberos и единый вход, необходимо добавить файл конфигурации входа на компьютер, на котором размещен сервер веб-приложений платформы BI.

1. Создайте файл с именем `bscLogin.conf` и сохраните его в каталог `/etc`.

Примечание:

Этот файл можно сохранить и в другом каталоге, однако в этом случае его расположение необходимо будет указать в параметрах Java. Рекомендуется размещать файл `bscLogin.conf` и файлы ярлыков ключей Kerberos в одном каталоге. В распределенном развертывании необходимо добавить файл `bscLogin.conf` для каждого компьютера, на котором размещается сервер веб-приложений.

2. Добавьте в файл конфигурации `bscLogin.conf` следующий код:

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
com.businessobjects.security.jgss.accept {
com.sun.security.auth.module.Krb5LoginModule required
storeKey=true
useKeyTab=true
keyTab="/etc/krb5.keytab"
principal="principal name";
};
```

Примечание:

Следующий раздел необходим для единого входа:

```
com.businessobjects.security.jgss.accept {
com.sun.security.auth.module.Krb5LoginModule required
storeKey=true
useKeyTab=true
keyTab="/etc/krb5.keytab"
```



```
principal="principal name";  
};
```

3. Сохраните и закройте файл.

9.3.3.5 Устранение неполадок с новыми 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](#)

9.4 Аутентификация Windows AD

9.4.1 Использование аутентификации Windows AD

9.4.1.1 Требования к поддержке Windows AD и исходная настройка

В этом разделе описана процедура настройки аутентификации Windows Active Directory (AD) на платформе BI. Все сквозные рабочие процессы, которые вам требуется выполнить, представлены вместе с проверками достоверности и другими обязательными тестами.

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 система Windows 2008 является поддерживаемой платформой для аутентификацию Kerberos и NTLM, в некоторых приложениях платформы BI могут использоваться только определенные методы аутентификации. Например, такие приложения, как стартовая панель BI и Central Management Console поддерживают только аутентификацию Kerberos.

Рекомендуемый порядок настройки AD

Для того чтобы изначально настроить неавтоматическую аутентификацию AD на платформе BI, воспользуйтесь следующим рабочим процессом:

1. Настройте контроллер домена.
2. Настройте аутентификацию AD в СМС.
3. Настройте учетную запись пользователя AD в агенте Server Intelligence Agent (SIA)
4. Настройте сервер веб-приложений для аутентификации AD с Kerberos.

Примечание:

Следующий порядок действий используется вне зависимости от необходимости использования единого входа (SSO). Приведенные в последующих разделах действия позволят выполнять ручной вход (с использованием имени и пароля пользователя AD) в платформу BI. После успешной настройки ручной аутентификации AD необходимо настроить SSO для аутентификации AD, что подробно будет описано в следующем разделе.

9.4.2 Подготовка контроллера домена

9.4.2.1 Настройка учетной записи службы для аутентификации AD с Kerberos

Чтобы настроить платформу BI на работу с аутентификацией Windows AD (Kerberos), необходимо наличие учетной записи службы. Можно создать учетную запись домена или воспользоваться существующей. Учетная запись службы будет использоваться для работы серверов платформы BI. После настройки учетной записи для нее потребуется настроить SPN. SPN используется для импорта групп пользователей AD в платформу BI.

Примечание:

Чтобы использовать AD с SSO, потребуется изменить настройки учетной записи и предоставить соответствующие права, после чего настроить ограниченное делегирование.

9.4.2.1.1 Настройка учетной записи службы в домене Windows 2008

Чтобы включить аутентификацию Windows AD с использованием протокола Kerberos необходимо выполнить настройку новой учетной записи службы. Эта учетная запись службы будет использоваться, в основном, 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 службы с паролем на основном контроллере домена.
2. Выполните команду `setspn -a`, чтобы добавить имена администраторов доступа к службе (SPN) для учетной записи службы, созданной на шаге 1. Укажите имена администраторов доступа к службе (SPN) для учетной записи службы, а также имя сервера, полное доменное имя сервера, а также IP-адрес компьютера, на котором развернута стартовая панель BI.

Например:

```
setspn -a BICMS/service_account_name.domain.com serviceaccountname
setspn -a HTTP/servername servicename
setspn -a HTTP/servername.domain.com servicename
setspn -a HTTP/<ip address of server> servicename
```

BICMS — это имя компьютера, на котором запущена SIA, *servername* — имя сервера, на котором развернута стартовая панель BI, а *servernamedomain* — полное доменное имя сервера.

3. Выполните скрипт `setspn -l servicename`, чтобы убедиться, что имена принципалов службы добавлены в учетную запись 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
```

Ниже приведен пример выходных данных:

```
C:\Users\Admin>setspn -l bossosvcacct

Registered ServicePrincipalNames for
CN=bossosvcacct,OU=svcaccts,DC=domain,DC=com:
    BICMS/bossosvcacct.domain.com
    HTTP/Tomcat HTTP/Tomcat.domain.com
    HTTP/Load_Balancer.domain.com
```

Созданной учетной записи службы необходимо предоставить права, а затем добавить ее в локальную группу администраторов. Администратор доступа службы будет использован в следующем разделе при импорте групп AD.

9.4.3 Настройка аутентификации AD в СМС

9.4.3.1 Подключаемый модуль безопасности Windows AD

Подключаемый модуль безопасности Windows AD позволяет сопоставлять учетные записи пользователей и групп из базы данных пользователей AD 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. Подключаемый модуль может быть использован для настройки обновлений импортированных групп AD.

С помощью подключаемого модуля безопасности Windows AD можно настроить следующие компоненты:

- Аутентификация Windows AD с Kerberos
- Аутентификация Windows AD с NTLM
- Аутентификация Windows AD с функцией единого входа SiteMinder

Подключаемый модуль безопасности AD совместим с доменами AD 2008, работающими в собственном или смешанном режиме.

После сопоставления пользователям и группам AD будет открыт доступ к инструментам клиента платформы BI с использованием аутентификации **Windows 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 ином случае все другие серверы и службы могут быть запущены на любой платформе, поддерживаемой платформой BI.
- Подключаемый модуль Windows AD для платформы BI поддерживает домены в нескольких лесах.

9.4.3.2 Сопоставление пользователей и групп AD

Перед импортом групп пользователей AD в платформу BI необходимо выполнить следующие действия:

- Создайте учетную запись службы в контроллере домена для платформы BI. Эта учетная запись будет использоваться для работы серверов платформы BI.

Примечание:

Чтобы реализовать аутентификацию AD с функцией единого входа Vintela (SSO), необходимо предоставить специально настроенное для этой цели имя администратора доступа к службе (SPN). Далее приведены шаги по настройке пользовательской аутентификации AD для

платформы BI. После настройки пользовательской аутентификации AD обратитесь к разделу *Настройка единого входа* данного руководства, в котором подробно описан процесс добавления SSO к конфигурации аутентификации AD.

- Убедитесь, что к учетной записи службы добавлено имя принципала службы, в которое входит имя компьютера, на котором выполняется SIA.

Для того чтобы импортировать группы AD на платформу BI, необходимо выполнить шаги с 1 по 11.

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 AD» щелкните ссылку возле **Имя администрирования для AD**.

Примечание:

Перед настройкой подключаемого модуля Windows AD эта ссылка отображается в виде кавычек. После сохранения конфигурации ссылка заполняется именами администраторов AD.

5. Введите имя и пароль включенной учетной записи пользователя домена.

Для учетных данных администратора можно использовать один из следующих форматов:

- Имя NT (Имя_домена\имя_пользователя)
- UPN (пользователь@доменное_имя_DNS)

Платформа BI использует эту учетную запись для запроса данных в AD. Платформа не вносит изменений в информацию AD, не добавляет и не удаляет ее. Поскольку платформа только считывает информацию, требуются только соответствующие права.

Примечание:

Идентификация AD нарушится, если учетная запись, используемая для чтения каталога AD, станет недействительной (например, если пароль учетной записи меняется, истекает срок его действия, или учетная запись заблокирована).

6. Введите в поле **Домен AD по умолчанию** домен AD по умолчанию.

Домен может быть указан как ПОЛНОЕ ИМЯ ДОМЕНА в ВЕРХНЕМ РЕГИСТРЕ или имя дочернего домена, из которого большинство пользователей будет осуществлять вход в платформу BI. Оно должно соответствовать домену по умолчанию, указанному в файлах конфигурации Керberos, используемых для настройки сервера приложений. Вы можете сопоставить группы с доменом по умолчанию, не указывая префикс доменного имени. 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/группу AD в поле **Добавить группу AD (домен/группа AD)**, используя один 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 \\ServerName\GroupName. AD не поддерживает локальных пользователей. Локальные пользователи, которые принадлежат сопоставленной локальной группе, не могут быть сопоставлены с платформой BI. Таким образом, такие пользователи не имеют доступа к системе.

Совет:

При входе в стартовую панель BI вручную пользователи из других доменов должны добавить имя домена в верхнем регистре после собственного имени пользователя. Например, CHILD.PARENTDOMAIN.COM — это домен в

```
user@CHILD.PARENTDOMAIN.COM
```

8. Нажмите кнопку **Добавить**.

Группа добавлена в список в разделе «Сопоставленные группы-участники AD»

9. В пункте «Параметры аутентификации» выберите **Использовать аутентификацию Kerberos**.
10. В поле **Имя администратора доступа к службе** введите имя принципа службы, сопоставленное с учетной записью службы, которая была создана для работы серверов платформы BI.

Примечание:

Для учетной записи службы, под которой работает SIA, требуется указать имя принципа службы. Например: BICMS/bossosvcacct.domain.com.

11. Нажмите **Обновить**.

Предупреждение:

В случае неверного отображения пользователей и/или групп переходить к следующему шагу не следует. Для решения проблем, связанных с сопоставлением групп AD, см. SAP-ноту 163734.

Примечание:

Если учетные записи групп AD были сопоставлены и на данном этапе не требуется настраивать параметры аутентификации AD или вносить изменения в группы AD, то шаги с 12 по 19 можно пропустить. Пользователь может вернуться к дополнительным параметрам после успешной настройки неавтоматической аутентификации AD с использованием протокола Kerberos.

12. Если имеющаяся конфигурация требует единственной SSO к базе данных, то выберите **Контекст безопасности кэша**.

Примечание:

Если настройка аутентификации AD выполняется впервые, рекомендуется сначала настроить неавтоматическую аутентификацию AD, а затем проанализировать, требуется ли дополнительная конфигурация для SSO.

13. Если для текущей настройки аутентификации AD требуется SSO, то выберите **Включить единый вход для выбранного режима аутентификации**.
14. В области «Синхронизация учетных данных» выберите параметр включения и обновления учетных данных для входа в источник данных пользователя AD.

Данный параметр позволяет синхронизировать источник данных с текущими учетными данными пользователя, что позволит формировать запланированные отчеты, даже если пользователь не выполнил вход в платформу BI, и доступ по принципу единого входа с использованием протокола Kerberos невозможен.

15. В области «Параметры псевдонима AD» укажите способ добавления и обновления новых псевдонимов в платформе BI.

- a. В области «Параметры нового псевдонима» выберите параметр для сопоставления новых псевдонимов учетным записям Enterprise:

- **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 области «Параметры обновления псевдонимов» выберите параметр для управления обновлениями псевдонимов для учетных записей Enterprise:

- **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 области «Параметры нового пользователя» укажите параметры создания новых пользователей:

- **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 на платформу BI, 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 параллельные 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.

16. Для настройки способа обновления псевдонимов AD щелкните **Запланировать**.

- а. В диалоговом окне «Расписание» выберите в списке **Запустить объект** тип повторения.
- б. Задайте оставшиеся необходимые параметры планирования.
- с. Нажмите кнопку **Планировать**

При обновлении псевдонимов также обновляются данные групп.

17. В области «Параметры привязки атрибутов» можно указать приоритет привязки атрибутов для подключаемого модуля AD:

- а. Установите флажок **Импорт полного имени, адреса электронной почты и других атрибутов**.

Полные имена и описания, используемые в учетных записях AD, импортируются и сохраняются в пользовательских объектах в платформе BI.

- б. Укажите значение для параметра **Установка приоритета для привязки атрибута AD относительно других привязок атрибутов**.

Если задано значение 1, приоритет имеют атрибуты AD, в которых включены AD и другие подключаемые модули (LDAP и SAP). Если задано значение 3, приоритет имеют атрибуты из других подключаемых модулей.

18. В области «Параметры групп AD» настройте обновления групп AD:

- а. Нажмите кнопку **Планировать**.
Откроется диалоговое окно «Расписание».
- б. В списке **Запустить объект** выберите тип повторения.
- с. Задайте оставшиеся необходимые параметры планирования.
- д. Нажмите кнопку **Планировать**

Система запланирует обновление и запустит его в соответствии с указанными настройками расписания. В области под «Параметрами группы AD» будет выведена информация о следующем запланированном обновлении учетных записей групп AD.

19. В области «Обновление AD по требованию» выберите один из следующих вариантов:

- **Обновить группы AD сейчас**

Выберите данный вариант, если при нажатии кнопки **Обновить** требуется обновлять все внесенные в расписание группы AD. Следующее запланированное обновление группы AD указано в пункте «Параметры группы AD».

- **Обновить группы AD и псевдонимы сейчас**

Выберите данный вариант, если при нажатии кнопки **Обновить** требуется обновлять все внесенные в расписание группы AD и пользовательские псевдонимы. Следующие запланированные обновления указаны в пунктах «Параметры группы AD» и «Параметры псевдонимов AD».

- **Не обновлять группы и псевдонимы AD сейчас**

При нажатии кнопки **Обновить** не требуется обновлять группы AD или пользовательские псевдонимы.

20. Нажмите кнопку **Обновить**, а затем нажмите **ОК**.

Чтобы убедиться в том, что учетные записи пользователей AD были импортированы,, выберите **СМС > Пользователи и группы > Иерархия групп** и выберите сопоставленную группу AD, чтобы просмотреть включенных в нее пользователей. Отобразятся текущие и вложенные пользователи из группы AD.

См. также

- [Создание файла конфигурации Kerberos](#)

9.4.3.3 Планирование обновлений для групп Windows AD

Платформа BI позволяет администраторам планировать обновления для групп и псевдонимов пользователей 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.

Тип повтора	Описание
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.
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 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 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 группы и псевдонимы AD сейчас** в области СМС **Обновление AD по требованию**.

Примечание:

Пароли AD не хранятся в псевдонимах пользователей.

9.4.4 Настройка сервиса платформы BI для запуска SIA

9.4.4.1 Запуск SIA под учетной записью службы платформы BI

Для поддержки аутентификации AD Kerberos для платформы BI 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).

В данном разделе приведено описание параметров операционной системы, изменение которых необходимо для обеспечения возможности учетной записи службы останавливать и запускать SIA.

Примечание:

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

9.4.4.2 Настройка агента SIA для работы под учетной записью службы

Перед включением работы учетной записи SIA под учетной записью службы платформа BI необходимо выполнить следующие действия:

- Для платформы BI на контроллере домена необходимо создать учетную запись службы.
- Проверить, что к учетной записи службы добавлены необходимые имена администраторов доступа к службе (SPN).
- Сопоставить группы пользователей AD с платформой BI.

Данное действие должно быть выполнено для всех агентов Server Intelligence Agent (SIA), на которых запущены службы, используемые учетной записью службы.

1. Для запуска CCM щелкните **Программы > SAP Business Intelligence > Платформа SAP BusinessObjects BI 4 > Central Configuration Manager**.

Откроется домашняя страница CCM.

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**.

На компьютере с SIA учетной записи службы должны быть предоставлены следующие права:

- Этой учетной записи должно быть явно назначено право «Работа в режиме операционной системы».
- Этой учетной записи должно быть явно назначено право «Вход в качестве службы».
- Права полного доступа к папке, в которой установлена платформа BI.
- Права полного доступа к разделу « HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects» системного реестра.

6. Щелкните **Пуск > Панель управления > Администрирование > Локальная политика безопасности**.
7. Разверните узел **Локальные политики**, а затем – **Назначение прав пользователя**.
8. Дважды щелкните пункт **Работа в режиме операционной системы**.
9. Щелкните **Добавить** и введите имя созданной учетной записью службы, а затем нажмите кнопку **ОК**.
10. 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.

11. Перезапустите SIA.
12. При необходимости повторите шаги 1 – 5 для каждого агента SIA, управляющего службой, которую требуется настроить.

После этого вы должны получить возможность войти в CCM с учетными данными AD.

9.4.4.3 Проверка учетных данных AD в CCM

Для выполнения этой задачи необходимо предварительно сопоставить пользовательскую группу AD платформе BI.

1. Запустите CCM и щелкните значок **Управление серверами**.
2. Убедитесь, что в поле «Система» отображается верная информация.
3. В списке параметров аутентификации выберите **Windows AD**.
Будет открыто диалоговое окно входа.
4. Выполните вход, используя существующую учетную запись AD из группы AD, сопоставленной с платформой BI.

Примечание:

В случае использования учетной записи AD, которая не входит в домен по умолчанию, имя следует вводить в формате `domain\username`.

При этом не должно быть выдано каких-либо сообщения об ошибках. Перед продолжением следует убедиться в возможности входа через CCM с использованием сопоставленной учетной записи AD.

Совет:

При получении сообщения об ошибке перейдите в раздел **Аутентификация > СМС > Windows AD**. В разделе «Параметры аутентификации» измените **Использовать аутентификацию Kerberos** на **Использовать аутентификацию NTLM** и щелкните **Обновить**. Повторите описанные выше шаги 1–4. Если все работает, проблема в конфигурации протокола Kerberos.

9.4.5 Настройка сервера веб-приложений для аутентификации AD

9.4.5.1 Подготовка сервера приложений для аутентификации Windows AD (Kerberos)

Процесс настройки протокола Kerberos для сервера веб-приложений незначительно различается в зависимости от конкретного сервера приложений. Тем не менее, общий процесс настройки Kerberos включает в себя следующие шаги:

- Создание файла конфигурации Kerberos (`krb5.ini`).
- Создание файла конфигурации входа JAAS `bscLogin.conf`.

Примечание:

Этот шаг не обязательно выполнять для сервера приложений Java SAP NetWeaver 7.3. Тем не менее, необходимо добавить LoginModule на сервер SAP NetWeaver.

- Изменения параметров Java на сервере приложений.

- Изменение параметров файла `BOE.war` для аутентификации Windows AD.
- Перезапуск сервера Java-приложений.

В этом разделе приведены подробные сведения по настройке Kerberos для использования со следующими серверами приложений:

- Tomcat
- WebSphere
- WebLogic
- Oracle Application Server
- SAP NetWeaver 7.3

9.4.5.1.1 Создание файлов конфигурации Kerberos

Создание файла конфигурации Kerberos

Прежде чем продолжить, убедитесь, что выполнены следующие обязательные задачи:

- Для платформы BI на контроллере домена необходимо создать учетную запись службы.
- Убедитесь, что имена принципалов службы (SPN) добавлены в учетную запись службы.
- Сопоставьте группы пользователей AD платформе BI.
- Проверить учетные данные AD в CCM.

Приведенные действия позволяют создать файл конфигурации Kerberos при использовании в качестве сервера веб-приложений SAP NetWeaver 7.3, Tomcat, Oracle Application Server, WebSphere или WebLogic для развертывания платформы BI.

1. Создайте файл `krb5.ini`, если он отсутствует, и сохраните его в каталоге `C:\Windows` 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:

Основные параметры подробно описываются в таблице ниже.

DOMAIN.COM	DNS-имя домена, которое необходимо ввести заглавными буквами в формате FQDN.
kdc	Имя узла контроллера домена.
[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.
default_realm	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. Как и в приведенном примере, имена всех доменов должны быть введены в верхнем регистре.

9.4.5.1.2 Создание файла конфигурации входа JAAS

Создание файла конфигурации входа Tomcat или WebLogic JAAS

Файл `bscLogin.conf` используется для загрузки модуля входа `java` и не требуется для аутентификации AD Kerberos на серверах веб-приложений Java.

Стандартный путь расположения файла: `C:\Windows`.

1. Создайте файл с именем `bscLogin.conf`, если он не существует, и сохраните его в каталоге `C:\Windows`.

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:\Windows`
2. Добавьте в файл конфигурации `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 7.3 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 7.3.

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 разделе **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.

9.4.5.1.3 Изменение настроек Java сервера приложений для загрузки файлов конфигурации

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 `bscLogin.conf`.

4. Закройте файл конфигурации Tomcat.
5. Перезапустите сервер Tomcat.

Изменение параметров Java для SAP NetWeaver 7.3

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. Щелкните **Система** и добавьте следующие сведения о пользовательских параметрах:

java.security.krb5.conf	<путь к файлу <i>krb5.ini</i> с указанием имени файла>
javax.security.auth.useSubjectCredsOnly	false

8. Щелкните **Сохранить** и выберите **Редактор конфигураций**.
9. Выберите **Конфигурации > Безопасность > Конфигурации > com.businessobjects.security.jgss.initiate > Безопасность > Аутентификация**.
10. Нажмите **Режим редактирования**.
11. Щелкните правой кнопкой мыши узел **Аутентификация** и выберите команду **Создать дочерний узел**.
12. Выберите элемент **Ввод значения** в списке сверху.
13. Укажите следующее:

Имя	create_security_session
Значение	false

14. Щелкните **Создать** и закройте окно.
15. Щелкните **Средство конфигурации** и выберите **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, на котором запущены 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 ОС4J, в котором работают приложения платформы BI.
3. Выберите **Свойства сервера**.
4. Прокрутите свойства до раздела "Multiple VM Configuration".
5. В разделе "Параметры командной строки" добавьте следующий текст в конце текстового поля «Параметры Java»: `-Djava.security.krb5.conf=C:/XXXX/krb5.ini`, заменив XXXX местом сохранения файла.
6. Перезапустите экземпляр ОС4J.

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 **Общие аргументы JVM** и укажите расположение файлов `Krb5.ini` и `bscLogin.conf`, как показано ниже.

`-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.

9.4.5.1.4 Проверка возможности Java принимать квитанции Kerberos

Перед проверкой получения Java квитанции Kerberos необходимо выполнить следующие предварительные действия:

- Создать файл `bscLogin.conf` для своего сервера приложений.
- Создать файл `krb5.ini`.

1. Откройте командную строку и перейдите в папку `jdk\bin` в месте установки платформы BI.

По умолчанию она расположена по следующему пути: `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\jdk\bin`.

2. Выполните команду `kinit <username>`.

3. Нажмите клавишу **Ввод**.

4. Введите пароль.

Если файл `krb5.ini` настроен правильно и модуль входа Java загружен, то будет выведено следующее сообщение:

Новая квитанция сохраняется в файле кэша
`C:\Users\Administrator\krb5cc_Administrator`

Не переходите к следующим шагам настройки AD, если квитанция Kerberos не была получена.

При возникновении проблем с получением квитанции можно сделать следующее:

- Обратиться к сведениям об устранении неполадок в конце данной главы.
- Если проблемы связаны с KDC, файлами конфигурации Kerberos или отсутствием учетных данных пользователя в базе данных Kerberos, см. следующие статьи базы знаний SAP: KBA 1476374 и KBA 1245178.

9.4.5.1.5 Настройка стартовой панели BI для входа в AD вручную

Перед настройкой приложений платформы BI для входа в AD вручную необходимо выполнить следующие обязательные действия:

- Создайте учетную запись службы в доменном контроллере для платформы BI.
- Убедитесь, что имена принципалов HTTP-службы (SPN) добавлены в учетную запись службы.
- Сопоставить группы пользователей AD с платформой BI.
- Проверить учетные данные AD в CCM.
- Создайте, настройте и проверьте необходимые файлы конфигурации для сервера веб-приложений.
- Измените настройки Java сервера приложений в соответствии с файлами конфигурации, чтобы обеспечить возможность их загрузки.

Для того чтобы включить возможность аутентификации Windows AD для обеих стартовых панелей BI, выполните следующие действия:

1. Откройте пользовательскую папку веб-приложения BOE на компьютере, на котором размещается сервер веб-приложений:

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

Все изменения следует вносить в директорию `config\custom`, а не `config\default`. В ином случае, при установке последующих пакетов исправления внесенные изменения будут утеряны.

Позднее потребуются повторно развернуть измененное веб-приложение BOE.

2. Создайте новый файл.

Примечание:

Воспользуйтесь программой "Блокнот" или любым другим текстовым редактором.

3. Сохраните файл под именем `BIlaunchpad.properties`.

4. Введите следующее:

```
authentication.visible=true  
authentication.default=secWinAD
```

5. Сохраните и закройте файл.

6. Перезапустите сервер веб-приложений.

Теперь вы сможете вручную выполнить вход в стартовую панель BI. Откройте какое-либо приложение в списке параметров аутентификации выберите "Windows AD".

Примечание:

Настройку Windows AD продолжать не следует, пока не будет включена возможность входа в стартовую панель BI вручную с использованием существующей учетной записи AD.

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.

9.4.6 Настройка единственной подписи

9.4.6.1 SSO в платформу BI с аутентификацией AD

Параметры SSO при использовании Windows AD

В платформе BI поддерживается два способа настройки единого входа (SSO) для аутентификации Windows AD:

- Vintela - данный способ может быть использован только в сочетании с Kerberos.
- SiteMinder - данный способ может быть использован только с Kerberos.

SSO в базу данных

Единый вход (SSO) в базу данных позволяет авторизованным пользователям выполнять действия, которые требуют доступ к базе данных, без повторного ввода своих учетных данных (например, для просмотра и обновления отчетов). Несмотря на то, что ограниченное делегирование не обязательно для аутентификации AD и единого входа Vintela, эта функция требуется для сценариев развертывания, в которых используется единый вход в системную базу данных.

Сквозной единый вход (SSO)

На платформе BI сквозной единый вход поддерживается через Windows AD с использованием Kerberos. В данном сценарии единый вход может быть применен как для доступа к платформе BI на клиентской стороне, так и для доступа к базе данных на сервере. 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.

Конфигурация аутентификации AD в ручном режиме и режиме единого входа

После того, как в развертываемом решении для учетных записей AD будет настроен ручной вход в стартовую панель BI, потребуется внести определенные изменения в параметры аутентификации AD в соответствии с требованиями SSO. В зависимости от выбранного метода единого входа данные требования будут различаться.

9.4.6.2 Использование Vintela SSO

9.4.6.2.1 Контрольный перечень настройки функции единого входа Vintela

Для настройки взаимодействия платформы BI и функции единого входа Vintela потребуется выполнить следующие операции:

1. Настроить учетную запись службы на работу с функцией единого входа Vintela.
2. Настроить ограниченное делегирование (необязательно).
3. Настроить в СМС параметры аутентификации Windows AD с использованием функции единого входа.
4. Настроить общие свойства BOE и специальные свойства стартовой панели BI для функции единого входа Vintela.
5. Если в качестве сервера веб-приложений разворачиваемого решения используется Tomcat, то потребуется увеличить предельный размер заголовка.

6. Настроить веб-браузеры на работу с Vintela.

9.4.6.2.2 Настройка учетной записи службы для функции единого входа Vintela

Средство командной строки `ktpass` позволяет выполнить настройку имени принципа сервера или службы в Active Directory и сформировать файл ярлыков ключей Kerberos с общим секретным ключом учетной записи службы. Данное средство обычно имеется на контроллерах домена. Также оно доступно на сайте поддержки Microsoft по адресу: <http://support.microsoft.com/kb/892777>

Потребуется создать учетную запись службы, которая позволит пользователям указанной группы Windows AD использовать функцию единого входа в стартовую панель BI с использованием своих учетных данных. Для этого можно изменить настройки учетной записи службы, созданной для аутентификации AD Kerberos на контроллере домена.

При попытке клиента выполнить вход в стартовую панель BI создается запрос к серверу генерации квитанций Kerberos. Для обработки данного запроса имя принципа учетной записи службы, созданной для платформы BI, должно соответствовать URL-адресу сервера приложений. На компьютере, на котором размещен контроллер домена, необходимо выполнить следующие действия.

1. Выполните команду установки файла ярлыков ключей Kerberos `ktpass` для создания файла ярлыков ключей.

Укажите параметры `ktpass`, перечисленные в следующей таблице:

Параметр	Описание
-out	Имя создаваемого файла ярлыков ключей Kerberos.
-princ	Имя принципа, используемого для учетной записи службы, в формате SPN: <code>MYSIAMYSERVER/sbo.service.domain.com@DOMAIN.COM</code> , где <code>MYSIAMYSERVER</code> — имя агента Service Intelligence Agent, указанного в Central Configuration Manager (CCM). Примечание: Для этого имени учитывается регистр. Имя SPN включает имя компьютера хоста, на котором выполняется экземпляр службы. Совет: Имя SPN должно быть уникальным в лесу, в котором оно зарегистрировано. Для проверки и поиска SPN можно использовать средство Windows <code>Ldp.exe</code> .
-pass	Задает пароль, используемый учетной записью службы.
-ptype	Задает тип администратора доступа: <code>-ptype KRB5_NT_PRINCIPAL</code>
-crypto	Задает используемый для учетной записи службы тип шифрования: <code>-crypto RC4-HMAC-NT</code>

Например:

```
ktpass -out keytab_filename.keytab -princ MYSIAMYSERVER/sbo.service.domain.com@DOMAIN.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.

2. Щелкните правой кнопкой мыши учетную запись службы выберите **Свойства > Делегирование**.
3. Выберите пункт **Доверять этому пользователю делегирование служб (только Kerberos)**.
4. Нажмите кнопку **ОК**, чтобы сохранить параметры.

После этого в учетную запись службы будут включены все имена принципалов для функции единого входа Vintela. Также для учетной записи службы будет создан файл ярлыков ключей с зашифрованным паролем.

Настройка ограниченного делегирования для функции единого входа Vintela

Ограниченное делегирование не является обязательным при настройке функции единого входа Vintela. Тем не менее, оно обязательно при развертывании решений, требующих единого входа в системную базу данных.

1. На компьютере контроллера домена AD откройте оснастку Active Directory «Пользователи и компьютеры».
2. Щелкните правой кнопкой на ранее созданной учетной записи службы и 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 и нажмите **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 будут добавлены в список служб, которые могут быть делегированы для учетной записи службы.

Чтобы учитывать это изменение, необходимо изменить свойства веб-приложения.

9.4.6.2.3 Изменение настроек SSO в CMC

1. Перейдите в область управления «Аутентификация» в CMC.
2. Дважды щелкните **Windows AD**.
3. Установите флажок **Включить Windows Active Directory (AD)**.

4. В области «Параметры аутентификации» установите флажок **Использовать аутентификацию Kerberos**.
5. Если имеющаяся конфигурация требует единственной SSO к базе данных, то выберите **Контекст безопасности кэша**.
6. Выберите **Включить единый вход для выбранного режима аутентификации**.
7. Нажмите **Обновить**.

9.4.6.2.4 Включение единого входа Vintela для стартовой панели BI и OpenDocument

Данная процедура применима для стартовой панели BI или OpenDocument. Чтобы задействовать функцию единого входа в веб-приложениях платформы BI, в файле `BOE.war` потребуется настроить определенные параметры Vintela и единого входа. При настройке единого входа рекомендуется сначала включить эту функцию для учетных записей AD в стартовой панели BI и только потом приступить к ее настройке для других приложений.

1. Откройте пользовательскую папку веб-приложения BOE на компьютере, на котором размещается сервер веб-приложений:

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

Все изменения следует вносить в директорию `config\custom`, а не `config\default`. В ином случае, при установке последующих пакетов исправления внесенные изменения будут утеряны.

Позднее потребуется повторно развернуть измененное веб-приложение BOE.

2. Создайте новый файл при помощи текстового редактора.
3. Введите следующую информацию.

```
sso.enabled=true
siteminder.enabled=false
vintela.enabled=true
idm.realm=DOMAIN.COM
idm.princ=MYSIAMYSERVER/sbo.service.domain.com@DOMAIN.COM
idm.allowUnsecured=true
idm.allowNTLM=false
idm.logger.name=simple
idm.keytab=C:/WIN/filename.keytab
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.
- В пути к файлу ярлыков ключей необходимо использовать знаки косой черты.

Если использовать ограниченное делегирование для аутентификации Windows AD с функцией единого входа Vintela не требуется, пропустите следующее действие.

4. Чтобы использовать ограниченное делегирование, добавьте следующее:

```
idm.allowS4U=true
```

5. Закройте 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. Сохраните файл под именем `OpenDocument.properties` или `BIlaunchpad.properties` в зависимости от предъявляемых требований.
7. Введите следующее:

```
authentication.default=secWinAD
cms.default=[enter your cms name]:[Enter the CMS port number]
```

Например:

```
authentication.default=secWinAD
cms.default=mycms:6400
```

8. Сохраните и закройте файл.
9. 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.

9.4.6.2.5 Включение единого входа Vintela для веб-служб

Для некоторых средств клиента потребуется аутентификация через веб-службы. Выполните следующие действия, чтобы включить единый вход (SSO) для веб-служб.

1. Создайте резервную копию следующего файла: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswebobje\WEB-INF\web.xml` и затем откройте его для изменения.
2. Отмените комментарии для разделов "Фильтр прокси Kerberos" и "Фильтр Kerberos", чтобы включить Kerberos SSO для аутентификации Windows Active Directory (secWinAD).

Обязательно задание следующих параметров (остальные необязательны):

- `idm.realm` (должен совпадать с `default_realm`, заданным в файле `Krb5.ini`).
- `idm.princ` (должен совпадать с заданным для `idm.princ` в файле `global.properties`, расположенном в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).
- `idm.keytab` (должен совпадать с заданным для `idm.keytab` в файле `global.properties`, расположенном в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).

Примечание:

При использовании встроенного пароля, заданного в параметрах Java Tomcat, не вносите изменений в строки ярлыков ключей в файле `web.xml`.

3. Если SSL не используется с сервером приложения Java, установите для параметра `idm.allowUnsecured` значение `true`.
Дополнительные сведения о Tomcat SSL см. в статье базы знаний с идентификатором 1484802.
4. Создайте резервную копию следующего файла: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswebobje\WEB-INF\classes\dsweb.properties` и затем откройте его для изменения.
5. Установите для параметра `kerberos.sso` значение `true` и сохраните файл.
6. Воспользуйтесь Wdeploy для повторного развертывания WAR-файла на сервере веб-приложений.
Для получения сведений об использовании WDeploy см. *Руководство по развертыванию веб-приложений платформы BusinessObjects Business Intelligence*.
7. Перезапустите Tomcat.
8. Чтобы протестировать настройки, на компьютере клиента с установленными средствами клиента запустите конструктор Query as a Web Service.
9. Добавьте новый управляемый хост.
10. Введите имя сервера приложений.
11. Введите URL-адрес веб-служб в следующем формате:
`http://<WebAppServer>:<portNumber>/dswebobje/services/Session`.
Пример: `http://BI4:8080/dswebobje/services/Session`.
12. Введите имя хоста центрального сервера управления.
13. Измените тип аутентификации на **Windows AD**.
14. Выберите **Разрешить единый вход Windows Active Directory**.
15. В запросе на вход оставьте незаполненными поля **Пользователь** и **Пароль** и нажмите кнопку **ОК**.

9.4.6.2.6 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.

9.4.6.2.7 Настройка веб-браузеров

Поддержка функции единого входа Vintela при аутентификации AD Kerberos возможна только при соответствующей настройке клиентов платформы BI. Это включает настройку веб-браузеров на компьютерах клиентов.

Настройка браузера Internet Explorer на клиентских компьютерах

1. На клиентском компьютере откройте окно браузера Internet Explorer.
2. Включение встроенной проверки подлинности Windows.
 - a. В меню **Сервис** выберите команду **Свойства обозревателя**.
 - 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 обозревателя**.
 - 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 **OK**.

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 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 **OK**.

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.

9.4.6.2.8 Проверка функции единого входа Vintela для аутентификации AD Kerberos

Проверка работы единого входа осуществляется на клиентской рабочей станции. Убедитесь, что клиент находится одном домене с разворачиваемой платформой BI, а также в том, что вход на рабочую станцию выполнен от имени сопоставленного пользователя AD. Для данной учетной записи должна быть включена возможность неавтоматического входа в стартовую панель BI.

Чтобы проверить работу функции единого входа, откройте браузер и введите URL-адрес стартовой панели BI. Если функция единого входа настроена правильно, то запрос на ввод учетных данных для входа выдан не будет.

Совет:

Рекомендуется проверить различные возможные сценарии входа пользователей AD. Например, если в текущем окружении имеются пользователи различных операционных систем, то следует проверить работу функции единого входа для всех имеющихся операционных систем. Также работу функции следует проверить во всех браузерах, имеющихся в организации. Если в окружении имеется несколько лесов или доменов, то работу функции единого входа учетной записи следует проверить для каждого из них.

9.4.6.2.9 Настройка Kerberos и единого входа в базу данных для серверов приложений

Единый вход в базу данных поддерживается для систем, удовлетворяющих следующим требованиям:

- Развертывание платформы BI осуществляется на веб-сервере приложений.
- Веб-сервер приложений настроен на использование функции единого входа Vintela при аутентификации AD.
- 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.

Последний шаг заключается в изменении файла `krb5.ini` для поддержки единого входа в базу данных для веб-приложений.

Включение единого входа в базу данных для серверов Java-приложений

1. Откройте файл `krb5.ini`, используемый в развертывании платформы BI.

По умолчанию он находится на сервере веб-приложений в каталоге WIN.

Примечание:

Если файл не удается найти в каталоге WIN, его местонахождение указано в следующем аргументе Java:

```
-Djava.security.auth.login.config
```

Эта переменная указывается при настройке AD с Kerberos на веб-сервере приложений.

2. Перейдите в раздел файла `[libdefaults]`.
3. Введите данную строку перед началом раздела файла `[realms]`:

```
forwardable=true
```

4. Сохраните и закройте файл.
5. Перезапустите сервер веб-приложений.

Чтобы включить функцию единого входа в базу данных, установите флажок **Контекст защиты кэша (требуется для SSO в базе данных)** на странице аутентификации Windows AD в CMC.

9.4.6.3 Использование SiteMinder

9.4.6.3.1 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.

Включение свойств SiteMinder для стартовой панели BI

Дополнительно к указанию настроек SiteMinder для подключаемого модуля безопасности Windows AD настройки SiteMinder нужно указать для свойств WAR-файла BOE.

1. Найдите каталог <КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\ в каталоге установки платформы BI.
2. Создайте новый файл в каталоге, используя Блокнот или другой текстовый редактор.
3. В новом файле введите следующие значения:

```
sso.enabled=true  
siteminder.authentication=secWinAD  
siteminder.enabled=true
```

4. Сохраните файл с именем `global.properties`.

Примечание:

Убедитесь в том, что файл с выбранным именем не сохраняется с каким-либо другим расширением, таким как `.txt`.

5. Создайте другой файл в этом же каталоге.

6. В новом файле введите следующие значения:

```
authentication.default=secWinAD
cms.default=[cms name]:[CMS port number]
```

Например:

```
authentication.default=LDAP
cms.default=mycms:6400
```

7. Сохраните файл с именем `BIlaunchpad.properties` и закройте его.

Новые свойства вступят в силу 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*.

Изменение настроек *SiteMinder* в *CMC*

Перед настройкой *CMC* для *SiteMinder* необходимо выполнить следующие предварительные действия:

- Сопоставить группы пользователей AD с платформой BI.
- Проверить учетные данные AD в *CCM*.

1. Перейдите в область управления «Аутентификация» в *CMC*.
2. Дважды щелкните **Windows AD**.
3. Установите флажок **Включить Windows Active Directory (AD)**.
4. В разделе Параметры аутентификации выберите **Использовать аутентификацию NTLM** или **Использовать аутентификацию Kerberos**.

Для настройки платформы BI на использование аутентификации Kerberos и AD с Kerberos требуется учетная запись службы. Можно создать учетную запись домена или воспользоваться существующей. Учетная запись службы будет использоваться для работы серверов платформы BI.

Совет:

При входе в стартовую панель BI вручную пользователи с других доменов должны добавить имя домена в верхнем регистре после собственного имени пользователя. Например, доменом в строке `user@CHILD.PARENTDOMAIN.COM` является «CHILD.PARENTDOMAIN.COM».

5. Если выбран параметр **Использовать аутентификацию Kerberos**:
 - a. Чтобы настроить единый вход в базу данных, выберите параметр **Контекст безопасности кэша**.
 - b. Очистите поле **Имя принципа службы**.
6. Если требуется настроить единый вход, выберите пункт **Включить единый вход для выбранного режима аутентификации**.
Также для включения единого входа потребуется настроить общие параметры веб-приложения BOE и параметры стартовой панели BI.
7. В области «Синхронизация учетных данных» выберите параметр включения и обновления учетных данных источника данных пользователя AD во время регистрации.

Это синхронизирует источник данных с текущими учетными данными пользователя.

8. В области «Параметры SiteMinder» можно настроить использование SiteMinder в качестве функции единого входа для аутентификации AD с использованием Kerberos.
 - a. Щелкните **Отключено**.

Будет открыта страница «Windows Active Directory».

Если модуль расширения Windows AD не был настроен, то будет выведено предупреждение с вопросом о продолжении. 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 в полях **Учет**, **Аутентификация** и **Авторизация** введите номер порта.
 - e. В поле **Имя агента** введите имя агента.
 - f. В поле **Секретный ключ** введите секретный ключ.

Убедитесь, что для администратора SiteMinder включена поддержка агентов версии 4.x, вне зависимости от используемой версии SiteMinder. Для получения дополнительных сведений о средстве SiteMinder и его установке см. документацию SiteMinder.
 - g. Нажмите кнопку **Обновить**, чтобы сохранить данные и вернуться на главную страницу аутентификации AD.
9. В области «Параметры псевдонима AD» укажите способ добавления и обновления новых псевдонимов в платформе BI.
 - a. В области «Параметры нового псевдонима» выберите параметр для сопоставления новых псевдонимов учетным записям Enterprise:
 - **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 области «Параметры обновления псевдонимов» выберите параметр для управления обновлениями псевдонимов для учетных записей Enterprise:
 - **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.

- В области «Параметры нового пользователя» укажите параметры создания новых пользователей:

- **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 параллельные 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.

- Для настройки способа обновления псевдонимов AD щелкните **Запланировать**.

- В диалоговом окне «Расписание» выберите в списке **Запустить объект** тип повторения.
- Задайте оставшиеся необходимые параметры планирования.
- Нажмите кнопку **Планировать**

При обновлении псевдонимов также обновляются данные групп.

- В области «Параметры привязки атрибутов» можно указать приоритет привязки атрибутов для подключаемого модуля AD:

- Установите флажок **Импорт полного имени, адреса электронной почты и других атрибутов**.

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**.

Если задано значение 1, приоритет имеют атрибуты AD, в которых включены AD и другие подключаемые модули (LDAP и SAP). Если задано значение 3, приоритет имеют атрибуты из других подключаемых модулей.

12. В области «Параметры групп AD» настройте обновления групп AD:

- a. Нажмите кнопку **Планировать**.
Откроется диалоговое окно «Расписание».
- b. В списке **Запустить объект** выберите тип повторения.
- c. Задайте оставшиеся необходимые параметры планирования.
- d. Нажмите кнопку **Планировать**

Система запланирует обновление и запустит его в соответствии с указанными настройками расписания. В области под «Параметрами группы AD» будет выведена информация о следующем запланированном обновлении учетных записей групп AD.

13. В области «Обновление AD по требованию» укажите, нужно ли обновлять группы или пользователей AD (или ничего из указанного) при нажатии кнопки **Обновить:**

- **Обновить группы AD сейчас**

Выберите данный вариант, если при нажатии кнопки **Обновить** требуется обновлять все внесенные в расписание группы AD. Следующее запланированное обновление группы AD указано в пункте «Параметры группы AD».

- **Обновить группы AD и псевдонимы сейчас**

Выберите данный вариант, если при нажатии кнопки **Обновить** требуется обновлять все внесенные в расписание группы AD и пользовательские псевдонимы. Следующие запланированные обновления указаны в пунктах «Параметры группы AD» и «Параметры псевдонимов AD».

- **Не обновлять группы и псевдонимы AD сейчас**

При нажатии кнопки **Обновить** не требуется обновлять группы AD или пользовательские псевдонимы.

14. Нажмите кнопку **Обновить, а затем нажмите **ОК**.**

Отключение SiteMinder

Если требуется запретить настройку SiteMinder или отключить его после настройки в CMC, 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*.

9.4.7 Устранение неполадок с аутентификацией Windows AD

9.4.7.1 Устранение неполадок с конфигурацией

Описанные ниже шаги могут помочь при возникновении проблем с настройкой Kerberos.

- Включение регистрации событий
- Тестирование конфигурации Java SDK Kerberos

9.4.7.1.1 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
```

9.4.7.1.2 Тестирование конфигурации Kerberos

- Выполните указанную ниже команду, чтобы протестировать конфигурацию Kerberos (здесь `servant` — учетная запись службы и домен, с которыми работает CMS, `password` — пароль этой учетной записи службы).

```
<InstallDirectory>\SAP BusinessObjects 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
```

Домен и SPN-имя должны полностью совпадать с доменом и SPN-именем в Active Directory. Если проблема остается, проверьте, введено ли то же имя. Помните, что имя учитывает регистр.

9.4.7.1.3 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.

9.4.7.1.4 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.

9.5 Аутентификация SAP

9.5.1 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 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 на доступ к содержимому.

Доступ к приложению 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 (CMS) 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 платформы 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 BI.
- 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).

9.5.2 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 новой роли, присвоив эти значения 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)

Объект авторизации	Поле	Значение
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:</p> <p>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.

9.5.3 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.

9.5.3.1 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](#)

9.5.3.2 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.

9.5.3.3 Временное прерывание соединения с системой предоставления прав SAP

В CMC 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 CMC перейдите в область управления **Аутентификация**.
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**.

9.5.4 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

9.5.4.1 Настройка параметров аутентификации SAP

1. Перейдите в область управления CMC «Аутентификация».
2. Дважды щелкните на ссылке **SAP** и затем выберите вкладку **Параметры**.
3. Просмотрите и при необходимости измените следующие параметры:

Параметр	Описание
Включить аутентификацию SAP	<p>Снимите этот флажок, чтобы отключить аутентификацию SAP.</p> <p>Примечание: Чтобы отключить аутентификацию SAP для конкретной системы SAP, установите соответствующий этой системе флажок Отключена на вкладке Системы контроля полномочий.</p>
Корневая папка содержимого	<p>Укажите место, с которого платформа BI должна начинать репликацию структуры папки BW на центральной консоли управления и на стартовой панели BI.</p> <p>По умолчанию это <code>/SAP/2.0</code>, однако можно указать и другую папку. Если требуется изменить значение, это нужно сделать и на центральной консоли управления, и на рабочей панели администрирования содержимого.</p>
Система по умолчанию	<p>Выберите систему контроля полномочий SAP, с которой должна связываться платформа BI с целью аутентификации пользователей, которые пытаются выполнить вход с учетными данными SAP, но не указывают конкретную систему SAP.</p> <p>Примечание: Если выбрать систему по умолчанию, пользователям из этой системы не придется вводить идентификатор системы или указывать клиент при подключении из клиентских средств, таких как Live Office или Universe Designer, с использованием аутентификации SAP. Например, если SYS~100 указана в качестве системы по умолчанию, пользователь SYS~100/user1 мог бы выполнить вход как пользователь user1 при использовании аутентификации SAP.</p>
Макс. число неудачных доступов системы контроля полномочий	

Параметр	Описание
	<p>Укажите, сколько раз платформа BI должна предпринимать попытки связаться с системой SAP для выполнения запросов аутентификации.</p> <p>Если задать значение -1, платформа будет пытаться связаться с системой контроля полномочий неограниченное число раз. Если задать значение 0, платформа BI предпримет одну попытку связаться с системой контроля полномочий.</p> <p>Примечание: Используйте эту настройку с параметром Отключить систему контроля полномочий на (сек), чтобы указать, как платформа BI обрабатывает временно недоступные системы контроля полномочий SAP. В системе используется два параметра, позволяющие определить, когда необходимо прекратить обмен данными с недоступной системой SAP и когда возобновить такой обмен.</p>
Отключить систему контроля полномочий [сек]	<p>Укажите, сколько секунд платформа BI должна подождать, прежде чем возобновлять попытки выполнить аутентификацию пользователей в системе SAP.</p> <p>Например, если для параметра Макс. число неудачных доступов системы контроля полномочий задано значение 3, платформа BI допускает не более трех неудачных попыток выполнить аутентификацию пользователей в любой системе SAP. Если четвертая попытка также завершается неудачей, система делает перерыв в попытках аутентифицировать пользователей в этой системе на указанное время.</p>
Макс . число параллельных соединений на систему	<p>Укажите, сколько открытых соединений необходимо одновременно оставлять открытыми в системе SAP.</p> <p>Например, если указать значение 2, платформа BI оставляет для SAP открытыми 2 соединения.</p>

Параметр	Описание
Число использований на одно соединение	<p>Укажите, сколько операций можно разрешить выполнять системе SAP на одно соединение.</p> <p>Например, если в качестве значения параметра Макс. число параллельных соединений на систему указано 2, а параметра Число использований на одно соединение — значение 3, то по достижении трех попыток входа по одному соединению платформа BI закрывает и перезапускает это соединение.</p>

Параметр	Описание
Параллельные пользователи и Зарегистрированные пользователи	<p>Укажите, какой тип лицензий будет использоваться для новых учетных записей пользователей: лицензии параллельного входа или именованные пользовательские лицензии.</p> <p>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.</p> <p>Именованные пользовательские лицензии связаны с пользователями. Они позволяют осуществлять доступ в систему с использованием имени пользователя и пароля. Это дает именованным пользователям право доступа к системе независимо от того, сколько человек уже зарегистрировано в ней.</p> <p>Примечание: Выбираемый вариант не меняет количество или тип пользовательских лицензий, установленных на платформе BI. В системе должны быть доступны подходящие лицензии.</p>
Импорт полного имени, адреса электронной почты и других атрибутов	<p>Укажите уровень приоритетности подключаемого модуля аутентификации SAP.</p> <p>Полные имена и описания, используемые в учетных записях SAP, импортируются и сохраняются с пользовательскими объектами на платформе BI.</p>
Установка приоритета для привязки атрибута SAP относительно других привязок атрибутов	<p>Задаёт приоритет для привязки атрибутов пользователя SAP (полное имя и адрес электронной почты).</p> <p>Если для этого параметра задано значение 1, атрибуты SAP являются приоритетными в сценариях с включенными подключаемыми модулями SAP и другими модулями (Windows AD и LDAP). Если задано значение 3, приоритет имеют атрибуты из других подключаемых модулей.</p>

Задайте значения следующих параметров, чтобы настроить службу единого входа SAP:

Параметр	Описание
Системный идентификатор	Системный идентификатор, предоставляемый платформой BI системе SAP при использовании службы единого входа SAP.
Просмотр	Щелкните, чтобы отправить файл <code>keystore</code> , созданный для включения механизма единого входа SAP. Кроме того, можно ввести полный путь к файлу вручную.
Пароль хранилища ключей	Укажите пароль, необходимый для доступа к файлу <code>keystore</code> .
Пароль личного ключа	Укажите пароль, необходимый для доступа к сертификату, соответствующему файлу <code>keystore</code> . Этот сертификат хранится в SAP-системе.
Псевдоним личного ключа	Укажите псевдоним, необходимый для доступа к файлу <code>keystore</code> .

4. Нажмите **Обновить**.

См. также

- [Настройка аутентификации SAP](#)

9.5.4.2 Изменение корневой папки содержимого

1. Перейдите в область управления «Аутентификация» CMC.
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/`).

9.5.5 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 издателя 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](#)

9.5.5.1 Чтобы выполнить импорт ролей SAP

1. Перейдите в область управления «Аутентификация» СМС.
2. Дважды щелкните ссылку **SAP**.
3. На вкладке **Параметры** выберите **Параллельные пользователи** или **Именованные пользователи** (в зависимости от условий лицензионного соглашения).
Этот параметр не меняет число или тип пользовательских лицензий, установленных на платформе BI. В системе должны быть доступны подходящие лицензии.
4. Нажмите кнопку **Обновить**.
5. На вкладке **Импорт ролей** выберите подходящую систему контроля полномочий в списке **Имя логической системы**.
6. В области «Доступные роли» выберите роль или роли, которые требуется импортировать, а затем нажмите кнопку **Добавить**.
7. Нажмите **Обновить**.

9.5.5.2 Проверка правильности импорта ролей и пользователей

Прежде чем приступить к выполнению этой задачи, запомните или запишите имя пользователя и пароль пользователя SAP, который относится к одной из ролей, сопоставленных службам информационной платформы.

1. Для стартовой панели BI Java перейдите по ссылке `http://веб-сервер:номер_порта/BOE/BI`.
Замените *веб-сервер* именем веб-сервера, а *номер_порта* номером порта платформы BI. Вам может понадобиться обратиться к администратору, чтобы узнать имя веб-сервера, номер порта или URL-адрес для входа.
2. В списке **Тип аутентификации** выберите **SAP**.

Примечание:

По умолчанию список **Тип аутентификации** скрыт на стартовой панели BI. Если список не видно, попросите системного администратора включить список **Тип аутентификации** в файл `BIlaunchpad.properties` и перезапустить сервер приложений.

3. Укажите систему SAP и системный клиент, в которые требуется выполнить вход.
4. Укажите имя пользователя и пароль сопоставленного пользователя.
5. Выберите **Вход в систему**.

Вы выполнили вход на стартовую панель BI как выбранный пользователь.

9.5.5.3 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.

9.5.5.3.1 Планирование обновлений для ролей SAP

После сопоставления ролей на платформе BI необходимо указать способ обновления ролей в системе.

1. Щелкните вкладку **Обновление пользователя**.
2. Щелкните **Расписание** в разделе «Обновить только роли» или области «Обновить роли и псевдонимы».

Совет:

Чтобы 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.

Появится диалоговое окно «Повтор».

3. Выберите параметр из списка **Запуск объекта** и укажите всю необходимую информацию о расписании в предоставленных полях.

При создании расписания обновления можно выбрать типы повтора, представленные в следующей таблице.

Тип повтора	Описание
Каждый час	Обновление будет запускаться каждый час. Необходимо указать время начала и даты начала и окончания.
Ежедневно	Обновление будет выполняться ежедневно или каждые n дней (где n – указанное пользователем число дней). Можно указать время начала и даты начала и окончания.
Еженедельно	Обновление будет выполняться каждую неделю, раз в неделю или несколько раз в неделю. Можно указать, в какие дни будет выполняться обновление, а также задать даты начала и окончания.
Ежемесячно	Обновление будет запускаться каждый месяц или каждые несколько месяцев. Можно указать время начала и даты начала и окончания.
N-ный 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. Нажмите кнопку **Планировать**

Дата следующего запланированного обновления роли отображается на вкладке **Обновление пользователя**.

Совет:

Чтобы отменить следующее плановое обновление, щелкните **Отменить обновления по расписанию** в области «Обновить только роли» или «Обновить роли и псевдонимы».

9.5.6 Настройка защищенного обмена данными (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.

9.5.6.1 Общие сведения о настройке доверительных параметров сервера SAP

В этом разделе описан процесс настройки параметров доверия между серверами веб-приложений SAP (версии 6.20 и выше) и платформа SAP BusinessObjects 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 бесплатной библиотеки "SAP crypto"

Для включения доверительных параметров со стороны сервера для платформы SAP BusinessObjects BI с использованием библиотеки "SAP crypto" нужно запустить серверы с использованием учетных данных, прошедших проверку провайдера SNC. Эти данные настраиваются в SAP и используются для заимствования прав без ввода пароля. В платформе SAP BusinessObjects BI нужно запустить серверы, осуществляющие пакетную отправку отчетов с использованием этих учетных данных SNC, например, адаптивный сервер заданий.

Для 32-битных процессов требуются 32-битные библиотеки SNC, а для 64-битных – 64-битные библиотеки. Библиотека SAP Cryptographic Library устанавливается на компьютер с платформой BI. 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.

Серверу SAP и платформе SAP BusinessObjects 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 доверительных параметров со стороны сервера между SAP и платформой SAP BusinessObjects BI требуется создать набор сертификатов, защищенных паролем (Среда персональной безопасности, PSE). В этом разделе описывается процесс создания и обслуживания PSE, а также способы безопасной привязки к серверам обработки платформы SAP BusinessObjects 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.

Задачи сервера платформа SAP BusinessObjects BI

Определенные серверы платформы SAP BusinessObjects 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
Служба BW Publisher	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 заданий	сервер	Планирование отчетов Crystal
сервер обработки Web Intelligence;	сервер	Просмотр и планирование отчетов и подсказок в виде списков значений (LOV) для сервера Web Intelligence
Multi-Dimensional analysis service	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.

9.5.6.2 Настройка доверительных параметров SAP со стороны сервера

Доверительные параметры со стороны сервера применимы только к отчетам Crystal и Web Intelligence, основанным на юниверсах (.unv). Необходимо настроить SNC для использования с платформой SAP BusinessObjects BI. Для получения дополнительной информации или помощи в устранении неполадок см. документацию SAP, предоставляемую с сервером SAP.

9.5.6.2.1 Настройка доверия сервера SAP

1. Убедитесь в наличии учетных данных администратора системы SAP и компьютера, на котором установлен SAP, а также учетные данные администратора платформы SAP BusinessObjects BI и компьютера (или компьютеров), на которых запускается система.
2. На компьютере с системой SAP проверьте наличие библиотеки SAP Cryptographic Library и инструмента SAPGENPSE в каталоге <ДИСК>:\usr\sap\<SID>\SYS\exe\run\ (в Windows).
3. Создайте переменную среды с именем SECUDIR, указывающую каталог, в котором находится квитанция.

Примечание:

Эта переменная должна быть доступна пользователю, запускающему процесс SAP **disp+work/**

4. В SAP GUI выполните транзакцию RZ10 и измените профиль экземпляра в режиме **Расширенное сопровождение**.
5. 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:

Префикс p: используется для библиотеки SAP Cryptographic Library. Он необходима для ссылки на имя SAP-системы, но не является видимым при проверке сертификатов в транзакциях STRUST или с использованием SAPGENPSE.

6. 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

7. Перезапустите экземпляр SAP.
8. Когда система снова будет запущена, войдите в нее и выполните транзакцию STRUST, в которой теперь должны быть новые записи для SNC и SSL.
9. Правой кнопкой мыши щелкните на узел SNC и нажмите **Создать**.

Теперь должен появиться идентификатор, который вы указали в транзакции RZ10.

10. Нажмите кнопку **ОК**.

11. 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.

12. Сохраните изменения.

Примечание:

Если вы не сохраните изменения и разрешите SNC, сервер приложений не сможет запуститься.

13. 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.

14. Перезапустите систему SAP.

Теперь необходимо настроить доверие на стороне сервера для платформы SAP BusinessObjects BI.

9.5.6.3 Настройка платформы SAP BusinessObjects BI для установления доверия на стороне сервера

Для настройки платформы SAP BusinessObjects BI с целью установления доверия на стороне сервера, необходимо выполнить следующие процедуры. 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 SAP BusinessObjects 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 SAP BusinessObjects BI](#)
- [Настройка доступа PSE](#)
- [Для настройки SNC аутентификации SAP](#)
- [Использование групп серверов](#)

9.5.6.3.1 Установка среды

Платформа BI включает библиотеку SAP Cryptographic Library по умолчанию. Если используется библиотека по умолчанию, необходимо выполнить только два последних шага: создать вложенную папку и добавить переменную среды. В противном случае для настройки пользовательской копии библиотеки SAP Cryptographic Library выполните все шаги.

Библиотека SAP Cryptographic Library по умолчанию находится в следующих папках.

- Windows: <КАТАЛОГ_УСТАНОВКИ>\sap\sapcrypto.dll
- Unix: <КАТАЛОГ_УСТАНОВКИ>/sap/libsapcrypto.so

Перед началом убедитесь в следующем:

- Криптографическая библиотека SAP загружена и развернута на хосте, на котором выполняются серверы обработки платформы SAP BusinessObjects 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. Скопируйте библиотеку SAP Cryptographic Library (включая инструмент обслуживания PSE) в папку на компьютере, на котором работает платформа SAP BusinessObjects 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`

Примечание:

Максимальная длина пути — 100 символов.

4. Создайте подпапку с именем `sec`.
Например: `C:\Program Files\SAP\Crypto\sec`
5. Добавьте общесистемную переменную среды `SECUDIR`, которая указывает на папку `sec`.

См. также

- [Настройка доверительных параметров SAP со стороны сервера](#)

9.5.6.3.2 Для генерации PSE

SAP принимает сервер платформы SAP BusinessObjects BI как доверенный, когда у соответствующих серверов платформы SAP BusinessObjects BI имеется PSE, связанный с SAP. Такое «доверие» между компонентами SAP и платформой SAP BusinessObjects BI устанавливается посредством совместного использования системами открытых сертификатов друг друга. Первым шагом будет формирование PSE для платформы SAP BusinessObjects 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 SAP BusinessObjects 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 выбрана кодировка Base64:
6. Для добавления сертификата платформы SAP BusinessObjects BI к списку PSE-сертификатов на сервере SAP, нажмите кнопку **Добавить в список сертификатов**.

7. Для добавления сертификата сервера SAP к PSE платформы SAP BusinessObjects 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, но представляет систему платформы SAP BusinessObjects BI.
 - Именем SNC должно быть отличительное имя системы (с префиксом p:), которое было указано при создании PSE платформы SAP BusinessObjects BI (на шаге 2).
 - Флажки **Ввод для RFC активирован** и **Ввод для экспортируемого Установлены оба активированные идентификатором** флажка:
12. Для добавления экспортированного сертификата к PSE платформы SAP BusinessObjects BI, выполните в командной строке следующую команду:

`sapgenpse.exe maintain_pk -v -a MySAPCert.crt -p BOE.pse`

Компонент SAP Cryptographic Library устанавливается на компьютер с платформой SAP BusinessObjects BI. Созданный PSE будет использоваться серверами платформы SAP BusinessObjects BI для их идентификации серверами SAP. SAP и платформа SAP BusinessObjects BI PSE обмениваются сертификатами. SAP разрешает сущностям с доступом к PSE платформы SAP BusinessObjects BI выполнять вызовы RFC и заимствование прав без пароля.

См. также

- [Настройка серверов платформы SAP BusinessObjects BI](#)

9.5.6.3.3 Настройка серверов платформы SAP BusinessObjects BI

После создания PSE для платформы SAP BusinessObjects BI необходимо настроить соответствующую структуру сервера для обработки SAP. В результате следующей процедуры создается узел для серверов обработки SAP, чтобы можно было задавать учетные данные операционной системы на уровне узлов.

Примечание:

В данной версии платформы SAP BusinessObjects BI серверы уже 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.

9.5.6.3.4 Настройка доступа PSE

После настройки узла и серверов платформы SAP BusinessObjects BI необходимо настроить доступ PSE с использованием средства SAPGENPSE.

1. Выполните следующую команду в командной строке:

```
sapgenpse.exe seclogin -p SBOE.pse
```

Примечание:

Появится подсказка для ввода PIN-кода PSE. Если средство будет запускаться с теми же учетными данными, что и сервера обработки SAP платформы SAP BusinessObjects BI, указывать имя пользователя не требуется.

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\username\Desktop\sapcrypto.x86\ntintel>sapgenpse.exe
maintain_pk -l
maintain_pk for PSE "C:\Documents and Settings\username\My Documents\snc\sec\boobjsapproc.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\username\Desktop\sapcrypto.x86\ntintel>
```

После успешного выполнения команды seclogin повторный запрос на ввод PIN-кода PSE появиться не должен.

Примечание:

В случае возникновения проблем при доступе PSE воспользуйтесь аргументом -O, чтобы указать права доступа к PSE. Например, чтобы предоставить доступ к PSE определенному пользователю в определенном домене в ОС Windows, введите:

```
sapgenpse seclogin -p SBOE.pse -O NT_AUTHORITY\SYSTEM
```

9.5.6.3.5 Для настройки SNC аутентификации SAP

После настройки доступа PSE необходимо задать настройки аутентификации SAP в CMC.

1. Перейдите в область управления «Аутентификация» CMC.
2. Дважды щелкните ссылку **SAP**.

Появятся настройки системы контроля полномочий.

3. На странице «Аутентификация SAP» откройте вкладку **Параметры SNC**.

4. Из списка **Имя логической системы** выберите вашу систему контроля полномочий.
5. Выберите **Включить защищенный сетевой обмен данными (SNC)** в разделе «Базовые параметры».
6. Чтобы использовать предлагаемый по умолчанию путь к библиотеке, выберите параметр **Использовать значение по умолчанию**. Чтобы задать другое местоположение, выберите параметр **Определение пользовательского пути**.
7. Выберите уровень защиты в поле «Качество защиты».
Например, выберите **Аутентификация**.

Примечание:

Не превышайте 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. Согласно библиотеке шифрования SAP, отличительное имя должно следовать правилам именования LDAP и иметь префикс `p:`.
9. Убедитесь, что SNC-имя учетных данных, под которыми работают серверы платформы SAP BusinessObjects BI, отображается в поле **SNC-имя системы Enterprise**.
При настройке нескольких имен SNC данное поле должно оставаться пустым.
10. Укажите отличительные имена системы SAP и PSE платформы SAP BusinessObjects BI.

9.5.6.3.6 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 подробных сведений и описаний различных серверов платформы SAP BusinessObjects BI см. главу «Архитектура».

Существует три варианта настройки серверов обработки содержимого SAP.

1. Поддерживайте один SIA, включая все серверы платформы SAP BusinessObjects BI, которые будут использовать учетные данные, позволяющие выполнить 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 Reports или Web Intelligence. 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 Reports 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
- Адаптивные серверы заданий

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.

9.5.6.4 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.

9.5.6.5 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 платформы SAP BusinessObjects BI для установления доверия на стороне сервера](#)

9.5.6.6 Настройка параметров SNC в Central Management Console

Прежде чем можно будет настроить параметры SNC, необходимо добавить новую систему контроля полномочий на платформу BI, скопировать файл библиотеки SNC в известный каталог и создать переменную среды `RFC_LIB`, указывающую на этот файл.

1. На странице «Аутентификация SAP» откройте вкладку **Параметры SNC**.
2. Из списка **Имя логической системы** выберите вашу систему контроля полномочий.
3. Выберите **Включить защищенный сетевой обмен данными (SNC)** в разделе «Базовые параметры».
4. Если вы настраиваете аутентификацию SAP для использования юниверсов `.unx` или соединений OLAP BICS и планируете использовать STS, установите флажок **Запретить незащищенные входящие соединения RFC**.
5. Чтобы использовать предлагаемый по умолчанию путь к библиотеке, выберите параметр **Использовать значение по умолчанию**. Чтобы задать другое местоположение, выберите параметр **Определение пользовательского пути**.

На сервере приложений и CMS должен использоваться одинаковый тип ОС с одинаковым путем к библиотеке шифрования.

6. Выберите уровень защиты в поле «Качество защиты».
Например, выберите **Аутентификация**.

Примечание:

Уровень защиты выбирается согласно потребностям вашей организации и возможностям библиотеки SNC.

7. Введите имя SNC системы SAP в «Настройках взаимной аутентификации».

Формат имени SNC зависит от библиотеки SNC. Согласно библиотеке шифрования SAP, отличительное имя должно следовать правилам именования LDAP и иметь префикс `p:`.

8. Подтвердите, что SNC-имя учетных данных, под которыми работают серверы платформы BI, отображается в поле **SNC-имя системы Enterprise**.
Если настроено несколько SNC-имен, оставьте это поле пустым.
9. Нажмите кнопку **Обновить**.
10. Перейдите на вкладку **Системы контроля полномочий** на странице «Аутентификация SAP». Параметр **SNC-имя** отображается в разделе параметров **Язык**.
11. В поле **SNC-имя** введите SNC-имя, настроенное на сервере SAP BW.
Это имя должно совпадать с именем, использованным для настройки доверия системы SAP платформе BI.
Если для включения интерфейса "Отчет–отчет" используется платформа Insight to Action, может пройти до 10 минут, прежде чем SNC будет включена или изменения параметров SNC вступят в силу. Чтобы запустить немедленное обновление, перезапустите сервер адаптивной обработки, на котором работает служба Insight to Action.

См. также

- [Подключение к системам контроля полномочий SAP](#)

9.5.6.7 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**.

9.5.6.8 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 активирован**.
6. Очистите все другие параметры и нажмите **Сохранить**.

9.5.7 Настройка единого входа в систему SAP

Разные клиенты платформы BI и фоновые службы взаимодействуют с бэкэнд-системами NetWeaver ABAP в интегрированной среде. Полезно будет настроить единый вход из платформы BI в эти бэкэнд-системы (обычно BW). После настройки системы ABAP как внешней системы аутентификации собственные маркеры SAP используются для обеспечения механизма, поддерживающего единый вход для всех клиентов и служб платформы BI, которые подключаются к системам NetWeaver ABAP.

Для включения единого входа в систему SAP нужно создать файл хранилища ключей `keystore` 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, используемую SAP BW, должен быть настроен подключаемый модуль аутентификации SAP.

9.5.7.1 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.

9.5.7.2 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.

9.5.7.3 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.

9.5.7.4 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

9.5.7.5 Добавление службы маркера безопасности на адаптивный сервер обработки

В кластеризованной среде службы маркеров безопасности добавляются отдельно на каждый адаптивный сервер.

1. Перейдите в область управления «Серверы» в СМС.
2. Дважды щелкните элемент **Основные службы**.
Список серверов будет открыт в разделе «Основные службы».
3. Щелкните правой кнопкой мыши адаптивный сервер обработки и выберите команду **Остановить сервер**.
Не переходите к следующему действию, пока статус сервера не изменится на "Остановлено".
4. Щелкните правой кнопкой мыши сервер адаптивной обработки и выберите пункт **Выбрать службы**.
Появится диалоговое окно «Выбор служб».
5. При помощи кнопки **Добавить** перенесите службу маркеров безопасности из списка **доступных служб** в список **служб**.
6. Нажмите кнопку **ОК**.
7. Перезапустите адаптивный сервер обработки.

9.5.8 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).

9.5.8.1 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 единого входа**.
4. Выберите один из следующих драйверов:

Драйвер	Отображаемое имя
Драйвер хранилища оперативных данных	crdb_ods
Драйвер Open SQL	crdb_opensql
Драйвер Infocet	crb_infocet
Драйвер запросов BW MDX	crdb_bwmdx

5. Нажмите кнопку **Удалить**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. Перезапустите SAP Crystal Reports.

9.5.8.2 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 единого входа**.
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.

9.6 Аутентификация PeopleSoft

9.6.1 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.

9.6.2 Включение аутентификации PeopleSoft Enterprise

Чтобы информация PeopleSoft Enterprise могла использоваться платформой BI, платформе BI нужны сведения об аутентификации в системе PeopleSoft Enterprise.

9.6.2.1 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 **Домены**.
6. Перейдите на вкладку **Домены**.
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 «Домены 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.

9.6.3 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 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 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.

9.6.3.1 Сопоставление роли PeopleSoft в платформе BI

Если у JVM платформы BI (виртуальной машины Java) нет сертификата для сервера PeopleSoft, перед выполнением основных шагов, приведенных далее, потребуется выполнить следующие дополнительные действия:

1. Получите файл .cer с сервера PeopleSoft.
2. Скопируйте файл .cer в каталог `<installdir>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security`.
3. Выполните следующую команду из каталога "security": `"<installdir>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin\keytool.exe" -import -file <peoplesoftserver>.cer -keystore cacerts -alias <peoplesoftserver>`.
4. Перезапустите сервер веб-приложений.

Основные шаги:

1. Выполните вход в систему Central Management Console под учетной записью администратора.
2. Нажмите кнопку **Аутентификация**.
3. Дважды щелкните **PeopleSoft Enterprise**.
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 "А", введите **А%**. При поиске также учитывается регистр слов.
 - Если требуется установить соответствие для роли из другого домена, нужно выбрать новый домен в списке доступных доменов.
6. Перейдите на вкладку **обновления для пользователя** и или нажмите кнопку **Обновить**, или спланируйте обновления.
 7. На вкладке **Параметры** перейдите к области «Параметры нового пользователя» и выберите один из следующих параметров:
 - **Назначать каждому добавленному псевдониму 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 псевдонимов» выберите один из следующих параметров:
 - **Создавать новые псевдонимы при обновлении псевдонимов**
 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".
 - **Создавать новые псевдонимы только при входе пользователя в систему**
 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. Это параметр по умолчанию.
 9. В области «Параметры нового пользователя» укажите, как создаются новые пользователи. Выберите один из следующих вариантов:

- **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 параллельные пользователи.**

Новые учетные записи пользователей настраиваются на использование пользовательских лицензий на одновременный доступ. 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.

9.6.3.2 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 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 параллельные пользователи, а затем выполняется изменение настроек, и новые пользователи сопоставляются как именованные.

9.6.3.3 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.

9.6.4 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.

9.6.4.1 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.

Появится 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».

9.6.5 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.

9.6.5.1 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".

Информацию об управлении защитой после импорта настроек см. в [Изменение настроек безопасности](#).

9.6.5.1.1 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 участниками управляемой группы платформы BI, не могут осуществлять доступ через эти юниверсы к тем данным, к которым у них нет доступа через PeopleSoft EPM.

9.6.5.1.2 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 соединении с платформой 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 участников 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».

9.6.5.2 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 юниверсы.

9.6.5.2.1 Примечания по отображению ролей

В режиме выполнения мост безопасности создает пользователя в платформе BI для каждого участника 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.

9.6.5.3 Изменение настроек безопасности

Можно изменять указанные ранее настройки безопасности путем изменения объектов, управляемых мостом безопасности.

9.6.5.3.1 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 участников 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 участников 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 участника управляемой роли PeopleSoft имеется учетная запись в платформе BI, но он не является участником 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 участник управляемой группы платформы BI не является участником 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.

9.6.5.3.2 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 какой-либо мере, то доступ к объекту величины запрещается. Если пользователь имеет доступ ко всем мерам, 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.

9.6.5.4 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 '\:').

9.6.5.4.1 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 <code>com.peoplesoft.epm.pf.jar</code> 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 соединения с базой 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 соединения нестандартного драйвера JDBC.</p> <p>Эти параметры можно использовать, только если параметр "db.driver.type" имеет значение "Custom".</p> <p>Это необязательные параметры.</p>

9.7 Аутентификация JD Edwards

9.7.1 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.

9.7.2 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.

9.7.2.1 Включение аутентификации JD Edwards в платформе BI

1. Выполните вход 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».
4. На вкладке **Параметры** установите флажок **Включить аутентификацию JD Edwards EnterpriseOne**.
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. Скопируйте файлы `jdeutil.jar`, `kernel.jar` и `log4j.jar` из установки JD Edwards в следующие папки (для Windows): `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\jdedwards\default\jdedwards\` и `<INSTALLDIR>\Tomcat\lib\`.
8. Перезапустите Tomcat и Server Intelligence Agent.
9. 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.
10. 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**.
11. Нажмите кнопку **Обновить**, чтобы сохранить изменения.

9.7.3 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 "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 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.

9.7.3.1 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. Выберите один из следующих вариантов:

- **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 параллельные пользователи.**

Новые учетные записи пользователей настраиваются на использование пользовательских лицензий на одновременный доступ. 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 **списке доменов** выберите сервер JD Edwards, содержащий роли, которые нужно сопоставить.
9. В «доступных ролях» выберите роли, которые требуется сопоставить платформе BI и нажмите <.
10. Щелкните **Обновить**.
- Роли будут сопоставлены платформе BI.

9.7.3.2 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 параллельные пользователи, а затем выполняется изменение настроек, и новые пользователи сопоставляются как именованные.

9.7.3.3 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.

9.7.4 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.

9.7.4.1 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.

Появится 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.

Тип повтора	Описание
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».

9.8 Аутентификация Siebel

9.8.1 Включение аутентификации Siebel

Чтобы информация Siebel могла использоваться платформой BI, системе нужны сведения о том, как выполнять аутентификацию для входа в систему Siebel.

9.8.1.1 Включение аутентификации Siebel в платформе BI

1. Выполните вход 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 поле **Соединение** 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.

9.8.2 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.

9.8.2.1 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. Установите флажок **Включить аутентификацию Siebel**.
5. 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.

6. В области **Параметры обновления псевдонимов** выберите один из следующих параметров:

- **Создавать новые псевдонимы при обновлении псевдонимов**

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".

- **Создавать новые псевдонимы только при входе пользователя в систему**

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. Это параметр по умолчанию.

7. В области **Параметры нового пользователя** укажите, как создаются новые пользователи. Если лицензия платформы BI основана на ролях пользователей, выберите один из перечисленных ниже параметров.

Выберите один из следующих вариантов:

- **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 параллельные 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.

8. Перейдите на вкладку **Роли**.

9. Выберите домен, соответствующий серверу Siebel, для которого нужно сопоставить роли.

10. 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**.
- Чтобы функция поиска работала, JAR-файл подключаемого модуля Siebel должен быть развернут в каталоге lib Tomcat: `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\lib` и в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\siebel\default\siebel`. После этого перезапустите сервер Tomcat и Server Intelligence Agent.

11. Нажмите **Обновить**.

Роли будут сопоставлены платформе BI.

9.8.2.2 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 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 параллельные пользователи, а затем выполняется изменение настроек, и новые пользователи сопоставляются как именованные.

9.8.2.3 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.

9.8.3 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.

9.8.3.1 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.

Появится 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.

Тип повтора	Описание
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».

9.9 Аутентификация Oracle EBS

9.9.1 Разрешение аутентификации Oracle EBS

Чтобы информация Oracle EBS могла использоваться платформой BI, системе нужны сведения о том, как выполнять аутентификацию в системе Oracle EBS.

9.9.1.1 Включение аутентификации Oracle E-Business Suite

Перед выполнением этой процедуры требуется развернуть файлы Oracle DLL и JAR на платформе BI:

1. Загрузите `ojdbc11.dll` из приложения клиента базы данных Oracle.
2. Скопируйте файл в следующую папку:
 - Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`
 - UNIX: `<INSTALLDIR>/sap_bobj/enterprise_xi40/platform`
3. Загрузите `ojdbc5.jar` из приложения клиента базы данных Oracle.
4. Скопируйте файл в следующую папку:
 - Windows: `<INSTALLDIR>\Tomcat\lib`
 - UNIX: `<INSTALLDIR>/sap_bobj/tomcat/lib`
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](#)

9.9.2 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.

9.9.2.1 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:

- **Создавать новые псевдонимы при обновлении псевдонимов**

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**.

- **Создавать новые псевдонимы только при входе пользователя в систему**

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**.

Выберите один из следующих вариантов:

- **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 параллельные пользователи.**

Новые учетные записи пользователей настраиваются на использование пользовательских лицензий на одновременный доступ. 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. В разделе **Текущие службы Oracle EBS** выберите службу Oracle EBS, содержащую роли, которые нужно сопоставить.
9. 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.
10. Щелкните **Обновить**.

Роли будут сопоставлены платформе BI.

После сопоставления ролей платформе BI необходимо указать, как система будет обновлять эти роли.

9.9.2.1.1 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.

9.9.2.1.2 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.

Появится 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».

9.9.3 Неотображаемые роли

Для того, чтобы запретить конкретным группам пользователей вход в платформу BI, можно отменить сопоставление ролей, к которым они принадлежат.

9.9.3.1 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. Перейдите на вкладку **Ответственность**.
5. Выберите **Текущая служба Oracle EBS**.
6. В области «Текущая роль» выберите роль и нажмите кнопку **Удалить**.
7. 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.

9.9.4 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.

9.9.4.1 Назначение прав администратора

Чтобы разрешить пользователям осуществлять поддержку платформы BI, необходимо включить их в группу "Администраторы", которая имеется в платформе BI по умолчанию. Участники 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 «Организовать» выберите **Пользователи и группы**.
3. В столбце «Имя» щелкните правой кнопкой мыши **Администраторы** и выберите **Добавить участников в группу**.
Будет открыта страница «Доступные пользователи или группы».
4. В области **Список пользователей** или **Список групп** выберите роль, для которой нужно назначить права администратора.
5. Щелкните значок >, чтобы внести роль в подгруппу группы "Администраторы", и щелкните **ОК**.

Участники 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 участникам роли административные права.

9.9.4.2 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 или группы** группу, участникам 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**.

Участники роли теперь могут добавлять объекты в папку и во вложенные в нее папки. Чтобы удалить назначенные разрешения, выберите группу и щелкните **Удалить**.

9.9.5 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).

9.9.5.1 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 единого входа в системе**.
4. Выберите **crdb_oraapps**.
5. Нажмите кнопку **Удалить**.

6. Нажмите кнопку **Сохранить и закрыть**.
7. Перейдите на страницу «Серверы» на консоли СМС и выберите **Службы отчетов Crystal Reports**.
8. Нажмите кнопку **Перезапустить сервер**.

9.9.5.2 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 (СМС) выберите элемент **Приложения**.
2. Дважды щелкните элемент **Конфигурация Crystal Reports**.
3. Выберите элемент **Параметры единого входа в системе**.
4. В разделе «Использовать для входа в базу данных контекст SSO с использованием следующих драйверов» введите `crdb_oraapps`.
5. Нажмите кнопку **Добавить**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. Перейдите на страницу «Серверы» на консоли СМС и выберите **Службы отчетов Crystal Reports**.
8. Нажмите кнопку **Перезапустить сервер**.

Администрирование сервера

10.1 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.
Узлы	Выводит список узлов развертывания. Узлы настраиваются в ССМ. Можно выбрать узел, щелкнув его, с целью просмотра серверов для узла или управления ими.

Параметр дерева навигации	Описание
Категории служб	<p>Выводит список типов служб, которые могут быть в вашем развертывании. Категории служб подразделяются на корневые службы платформы SAP BusinessObjects Business Intelligence и службы, связанные с конкретными компонентами SAP Business Objects. Категории служб включают в себя:</p> <ul style="list-style-type: none"> • Службы соединения • Основные службы • Службы Crystal Reports • Службы объединения данных • Службы управления жизненным циклом • Службы Analysis • Службы Web Intelligence • Службы Dashboards <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 (Подробные сведения см. в Управление соединением с центральной базой данных центрального сервера управления.)

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.

Столбец панели "Сведения"	Описание
Работоспособность	<p>Показывает общую работоспособность сервера.</p> <p>Возможны следующие состояния сервера:</p> <ul style="list-style-type: none"> • Зеленый (Работает нормально) • Янтарный (Внимание) • Красный (Осторожно) <p>Состояние работоспособности сервера напрямую зависит от статуса наблюдения сервера. Например, состояние работоспособности центрального сервера управления зависит от статуса <code><NODENAME>.CentralManagementServer Watch.</code></p> <p>Сведения о наблюдениях можно получить на странице «Мониторинг» в СМС: на вкладке «Список наблюдения» выберите наблюдение и нажмите кнопку Изменить. Отобразятся «Правило для состояния "Внимание"» и «Правило для состояния "Осторожно"» для просматриваемого наблюдения, соответствующие желтому и красному состояниям работоспособности соответственно.</p>
PID	Отображает уникальный идентификатор процесса сервера.
Описание	Отображает описание сервера. Это описание можно изменить на странице «Свойства» сервера.
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](#)

10.2 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](#)

10.3 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](#)

10.4 Просмотр и изменение статуса сервера

10.4.1 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 СМС.

См. также

- [Просмотр статуса сервера](#)
- [Просмотр состояния служб](#)
- [Запуск, остановка и перезапуск серверов](#)
- [Включение и выключение серверов](#)
- [Остановка центрального сервера управления \(CMS\)](#)
- [Автоматический запуск сервера](#)

10.4.1.1 Просмотр статуса сервера

1. Перейдите в область управления «Серверы» в СМС.
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 состояние каждого сервера в списке.
3. Если требуется просмотреть список всех серверов, которые имеют определенный статус, разверните 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.

См. также

- [Просмотр состояния служб](#)

10.4.1.2 Просмотр состояния служб

В случае сбоя какой-либо службы для хост-сервера устанавливается либо состояние «Запущено с ошибками» (означающее, что по крайней мере одна служба запущена успешно), либо состояние «Сбой» (означающее, что не удалось запустить ни одну из служб). Состояния сервера можно просмотреть в СМС и ССМ. Однако также можно просмотреть статус отдельных служб на странице «Свойства» сервера в СМС.

1. Перейдите в область управления «Серверы» в СМС.
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.
3. Щелкните дважды сервер, чтобы открыть для него страницу «Свойства».
На странице «Свойства» отображаются свойства сервера и служб, которые на нем располагаются. Для служб, которые не удалось запустить, также выводятся сообщения об ошибках.

См. также

- [Просмотр состояний серверов](#)

10.4.2 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, чтобы настроить его, требуется его перезагрузить перед тем, как изменения вступят в силу и сервер возобновит обработку запросов.

Действие	Описание
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.
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](#)

10.4.2.1 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, разверните 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](#)

10.4.2.2 Запуск, остановка или перезапуск сервера Windows при помощи CCM

1. В CCM нажмите на панели инструментов кнопку **Управление серверами**.
2. При появлении подсказки 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.

10.4.2.3 Автоматический запуск сервера

По умолчанию серверы развертывания автоматически запускаются во время запуска агента Server Intelligence. Эта задача показывает, где задаются параметры автозапуска.

1. Перейдите в область управления «Серверы» в CMC.
2. Дважды щелкните сервер, который должен запускаться 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 флажок **Автоматически запускать этот сервер при запуске агента серверной аналитики** снят для каждого сервера CMS в кластере, необходимо использовать CCM для перезапуска системы. Воспользовавшись CCM для остановки агента SIA, щелкните правой кнопкой мыши агент SIA и выберите **Свойства**. На вкладке **Запуск** щелкните **Свойства**, чтобы открыть страницу свойств сервера для CMS. Выберите **Автозапуск**, затем нажмите кнопку **ОК**, чтобы закрыть страницу свойств сервера, и снова нажмите кнопку **ОК**. Перезапустите SIA. Параметр **Автозапуск** доступен только в том случае, если флажок **Автоматически запускать этот сервер при запуске агента серверной аналитики** снят для всех CMS кластера.

10.4.3 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 Business Intelligence без обслуживания.

Однако если в развертывании платформы Business Intelligence имеется только один CMS, то его выключение сделает платформу 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. Сервер CMS можно остановить путем остановки его агента SIA, но перед остановкой SIA следует остановить серверы обработки через CMC, чтобы они смогли завершить свои задания перед выключением платформы Business Intelligence, так как все другие серверы в узле также будут остановлены.

Примечание:

Можно столкнуться с ситуацией, когда CMS остановился, и возникла необходимость перезагрузить систему из CCM. Например, если работа всех серверов CMS узла завершается, и при запуске SIA для каждого CMS снят флажок **Автоматически запускать этот сервер при запуске агента серверной аналитики**, то для перезапуска системы необходимо использовать CCM. Для этого в CCM щелкните SIA правой кнопкой мыши и выберите команду **Свойства**. На вкладке **Запуск** щелкните **Свойства**, чтобы открыть страницу свойств сервера для CMS. Выберите **Автозапуск**, затем нажмите кнопку **ОК**, чтобы закрыть страницу свойств сервера, и снова нажмите кнопку **ОК**. Перезапустите SIA. Параметр **Автозапуск** доступен только в том случае, если флажок **Автоматически запускать этот сервер при запуске агента серверной аналитики** снят для всех CMS кластера.

Если нужно настроить систему так, чтобы можно было запускать и останавливать центральный сервер управления 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 \(CMS\)](#)

10.4.4 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.

10.4.4.1 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**.

10.4.4.2 Включение или отключение сервера Windows в CCM

1. В CCM выберите **Управление серверами**.
2. При появлении соответствующей подсказки войдите в CMS, используя учетные данные пользователя с правами администратора для платформы SAP BusinessObjects Business Intelligence.
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.

10.5 Добавление, клонирование и удаление серверов

10.5.1 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*.

10.5.1.1 Добавление сервера

На одном компьютере можно запустить несколько экземпляров одного сервера платформы SAP BusinessObjects Business Intelligence. 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 используемая архитектура платформы SAP BusinessObjects Business Intelligence состоит из нескольких узлов, в списке **Узел** выберите узел, к которому следует 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 центральный сервер 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. Если требуется, чтобы новый сервер начал отвечать на запросы платформы SAP BusinessObjects Business Intelligence, запустите и активируйте его из консоли СМС.

См. также

- [Службы и серверы](#)
- [Конфигурация настроек серверов](#)
- [Настройка номеров портов](#)
- [Просмотр состояний серверов](#)

10.5.1.2 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 CMS появляется в новом узле с такими же конфигурационными настройками, что и у исходного сервера CMS.

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.

10.5.1.2.1 Использование заполнителей для серверных параметров

Заполнители представляют собой переменные на уровне узла, которые используются серверами, запущенными на узле. Заполнители перечислены на отдельной странице в Central Management Console (CMC). При двойном щелчке любого сервера, перечисленного в списке «Серверы» на CMC, 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 CMC.

Пример:

Заполнители можно использовать при клонировании серверов. Например, на компьютере с несколькими приводами A платформа BI установлена в каталоге 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 B, установлен только один диск (диск D отсутствует) и платформа BI 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 A на компьютер B, 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.

10.5.1.2.2 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.

10.5.1.3 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**.

10.6 Кластеризация центральных серверов управления (СМС)

10.6.1 Кластеризация центральных серверов управления (СМС)

Для крупного или критически важного развертывания платформы SAP BusinessObjects Business Intelligence может потребоваться использование нескольких компьютеров с CMS в кластере. Кластер состоит из двух или более серверов CMS, совместно работающих со стандартной базой данных системы CMS. Если на компьютере, на котором запущен один сервер CMS, происходит сбой, то другой компьютер с CMS продолжит обслуживать запросы платформы Business Intelligence. Такая высокая доступность позволяет убедиться в том, что пользователи платформы 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 элемента 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 пакетов исправлений) к операционной системе, серверу баз данных, методу доступа к базе данных, драйверу базы данных и клиенту, описанным в матрице доступности продуктов.

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, то производительность платформы Business Intelligence будет существенно снижена.
- Для улучшения быстродействия необходимо запускать каждый элемент 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 версию платформы 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 для подключения к системной базе данных, а его версия поддерживается.
 - 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, что на всех компьютерах кластера (в том числе, на тех, где размещается CMS), установлено одинаковое системное время. Чтобы обеспечить оптимальную производительность, синхронизируйте время компьютеров с сервером времени (например, `time.nist.gov`) или используйте центральное решение мониторинга.
 - Убедитесь в том, что на всех серверах веб-приложений в кластере установлены одинаковые WAR-файлы. Дополнительную информацию о разворачивании 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.
 - Потоки Out-of-Band (-oobthreads) используются тестовыми опросами и уведомлениями кластеризации. Так как обе операции выполняются быстро (уведомления являются асинхронными), платформа BI не требует нескольких потоков oobthread, и создается только один поток -oobthread.
- Если кластер содержит более 8 серверов, убедитесь, что командная строка для каждого CMS включает в себя параметр `-oobthreads <numCMS>`, где `<numCMS>` количество серверов CMS 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:

Имя кластера по умолчанию отражает имя хоста первого установленного CMS.

См. также

- [Изменение имени кластера CMS](#)

10.6.1.1 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 CMC.
- 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, конфигурации сервера и содержимого репозитория входящих и исходящих файлов. При необходимости обратитесь к администратору базы данных.

См. также

- [Добавление нового узла в кластер](#)
- [Добавление сервера](#)
- [Клонирование серверов](#)
- [Обзор резервного копирования и восстановления](#)

10.6.1.2 Добавление нового узла в кластер

При добавлении узла (узел — это коллекция серверов платформы BI, управляемых одним SIA) выводится приглашение на создание нового CMS или на кластеризацию узла в существующий 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. В этом случае укажите имя CMS, на котором запущена существующая система, выберите вариант установки CMS на локальном компьютере, а затем укажите в программе установки сведения, необходимые для подключения к существующей базе данных системы CMS. После завершения установки нового сервера CMS на локальный компьютер сервер будет автоматически добавлен в существующий кластер.

Примечание:

Прежде чем прикрепить новый узел в кластер существующей CMS, если новый узел является совершенно новым сервером, убедитесь, что установка платформы BI на этом сервере находится на том же уровне исправлений, что и имеющаяся среда платформы BI.

См. также

- [Использование узлов](#)

10.6.1.3 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.

10.6.1.3.1 Определение свойств кластера в веб-приложении BOE

1. Откройте пользовательскую папку, содержащую файл `BOE.war`, на компьютере, на котором размещаются веб-приложения:

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

Затем потребуется повторно развернуть измененный файл `BOE.war`.

2. Создайте новый файл при помощи текстового редактора.
3. Укажите свойства кластера CMS.

Используйте свойство `cms.clusters` для указания всех кластеров 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,cmstwo
cms.clusters.samplecluster2=cms3,cms4, cms5
cms.clusters.samplecluster3=aps05
```

Примечание:

Номер порта отделите от имени CMS двоеточием; предполагаемый номер порта - 6400, если не указано иначе.

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*.

10.6.1.4 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.

10.6.1.4.1 Изменение имени кластера в ОС Windows

1. Используйте CCM для остановки агента Server Intelligence Agent в узле, в котором содержится центральный сервер управления, являющийся элементом 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 CMC и проверьте, что все серверы включены. При необходимости включите все серверы, которые были отключены при выполнении изменений.

10.6.1.4.2 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*.

10.7 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.

10.7.1 Создание группы серверов

Чтобы создать группу серверов, необходимо ввести имя и описание группы, а затем добавить в нее серверы.

10.7.1.1 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 элементы** 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](#)

10.7.2 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 элементов другой группы. Результат будет одинаковым в обоих случаях, поэтому используйте наиболее удобный для вас метод.

10.7.2.1 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 элементы** 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.

10.7.2.2 Чтобы сделать одну группу серверов элементом 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.

10.7.3 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 (СМС) для нескольких регионов. Вместо того чтобы добавлять сервер СМС отдельно в группу каждого региона, можно воспользоваться ссылкой **Элемент** для данного сервера и добавить его сразу во все три региона.

10.7.3.1 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 сведений в списке **Доступные группы серверов** отобразятся группы, в которые можно добавить данный сервер. В списке **Элемент 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**.

10.7.4 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.

10.7.4.1 Для предоставления доступа к серверу или группе серверов

1. Перейдите в область управления «Серверы» в CMC.
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".

10.7.4.2 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.

10.8 Настройка адаптивных серверов обработки для производственных систем

Программа установки устанавливает по одному адаптивному серверу обработки (APS) на каждую хост-систему. В зависимости от состава установленных компонентов на этом APS может размещаться большое количество служб, в том числе служба мониторинга, служба управления жизненным циклом, служба Multi-Dimensional analysis service (MDAS), служба публикации и другие службы.

В производственных и тестовых системах рекомендуется создавать дополнительные адаптивные серверы обработки и настраивать их в соответствии с бизнес-требованиями.

Дополнительные адаптивные серверы обработки можно создавать двумя способами:

- При помощи мастера настройки системы.

Этот мастер обеспечивает базовую настройку системы платформы BI, включая настройку адаптивных серверов обработки с применением готовых шаблонов развертывания. При помощи мастера задаются основные настройки, однако следует выполнить отдельную настройку масштабирования системы.

Доступ к этому мастеру осуществляется из консоли Central Management Console (CMC). Дополнительные сведения об этом мастере см. в разделе [Вводные сведения о мастере настройки системы](#). Дополнительные сведения о шаблонах развертывания по умолчанию см. в документе *Шаблоны развертывания платформы SAP BusinessObjects BI*, который доступен в мастере, а также в разделе <http://help.sap.com/bobip41>.

- Создание и настройка дополнительных адаптивных серверов обработки вручную при помощи консоли CMC. Для получения дополнительных сведений см. [Добавление, клонирование и удаление серверов](#).

Помните:

После выбора шаблона развертывания в мастере или создания дополнительных адаптивных серверов обработки вручную в любом случае необходимо настроить масштабирование системы. Убедитесь, что масштабирование выполнено: <http://www.sap.com/bisizing>.

10.9 Оценка производительности системы

10.9.1 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](#)

10.9.2 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.

10.9.2.1 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"](#)

10.9.3 Просмотр системных показателей

Область управления CMC «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 CMS. Раздел «Просмотр глобальных параметров системы» включает информацию об активности текущей учетной записи и статистику текущих и обработанных заданий. В разделе «Кластер» указано имя CMS, к которому вы подключены в настоящий момент, имя кластера CMS и имена других элементов кластера.

10.9.3.1 Для просмотра системных показателей

1. Перейдите в область управления CMC «Параметры».

2. Щелкните стрелку, чтобы развернуть и просмотреть настройки в областях **Свойства**, **Просмотреть глобальные системные показатели**, **Кластер** или **Оперативное резервное копирование**.

10.9.4 Регистрация деятельности сервера

Платформа BI позволяет записывать в журнал определенную информацию об активности платформы BI.

- Кроме того, каждый из серверов платформы BI регистрирует сообщения в стандартном журнале операционной системы.
 - В операционной системе Windows платформа BI регистрирует записи в службе "Журнал событий". Вы можете просмотреть результаты с помощью программы просмотра событий (в журнале приложений).
 - В UNIX, платформа BI регистрирует события в системном процессе пользовательского приложения. 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 BusinessObjects 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 BI, необходимо установить и настроить системную регистрацию событий таким образом, чтобы записывались все сообщения, регистрируемые устройством «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.

10.10 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](#)

10.10.1 Для изменения свойств сервера

1. Перейдите в область управления «Серверы» в CMC.
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.

10.10.2 Применение параметров службы к нескольким серверам

Вы можете применить один и тот же параметр к службам, размещенным на нескольких серверах,

1. Перейдите в область управления «Серверы» в СМС.
2. Нажав клавишу **Ctrl**, щелкните каждый сервер, на котором размещаются службы, параметры которых нужно изменить, затем щелкните их правой кнопкой и выберите команду **Изменить общие службы**.

Откроется диалоговое окно «Изменить общие службы» со списком служб, размещенных на выбранных серверах, параметры которых вы можете изменить.

3. Если в диалоговом окне «Изменить общие службы» перечислено несколько служб, выберите службу, которую нужно изменить и нажмите кнопку **Продолжить**.
4. Внесите необходимые изменения и нажмите кнопку **ОК**.

Примечание:

Перенаправление в область управления СМС «Серверы». Если требуется перезагрузить сервер, он отмечается как устаревший. После перезапуска сервера он применяет новые настройки, а флаг "Устаревший" удаляется.

10.10.3 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](#)

10.10.3.1 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](#)

10.10.3.2 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](#)

10.10.3.3 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.

10.11 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.

10.11.1 Параметры сетевой среды

Платформа BI 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. Платформа BI не обеспечивает механизм для определения сетевой среды. С помощью СМС определенный IP-адрес IPv6 или IPv4 можно связать с любым сервером платформы BI.

10.11.1.1 Смешанная среда IPv6/IPv4

Смешанная сетевая среда IPv6/IPv4 обеспечивает следующие возможности.

- При работе в смешанном режиме IPv6/IPv4 серверы платформы BI могут обслуживать запросы IPv6 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.

10.11.2 Параметры идентификации хоста сервера

Параметры идентификации хоста сервера можно задать в СМС для всех серверов платформы SAP BusinessObjects Business Intelligence. В следующей таблице перечислены все параметры, доступные в области «Общие параметры».

Действие	Описание
Назначать автоматически	<p>Это установка по умолчанию для всех серверов. Если установлен этот флажок, сервер автоматически связывает свой порт запросов с первым сетевым интерфейсом устройства.</p> <p>Примечание: Рекомендуется устанавливать флажок Назначать автоматически для имени хоста. Однако в некоторых случаях, например, если сервер работает на компьютере, подключенном к нескольким сетям, или серверу необходимо взаимодействовать с определенной конфигурацией брандмауэра, следует рассмотреть возможность использования определенного имени хоста или IP-адреса. Для получения дополнительных сведений о настройке многосетевого компьютера и работе с брандмауэрами см. <i>руководство 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, который CMS использует для связывания порта сервера имен с портом запросов. Для всех серверов предоставляются отдельные поля для указания IP-адресов IPv4 и/или IPv6.

Предупреждение:

Если флажок **Назначать автоматически** установлен на многосетевых компьютерах, CMS может автоматически установить связь с неверным сетевым интерфейсом. Чтобы этого избежать, необходимо убедиться, что сетевые интерфейсы перечислены на хосте в правильном порядке (с использованием инструментов ОС компьютера). Следует указать имя хоста CMS в CMS.

Примечание:

При работе с многосетевыми компьютерами или определенными настройками NAT брандмауэра необходимо указывать имя хоста в виде полностью определенных доменных имен, а не имен хоста.

См. также

- [Настройка системы для использования брандмауэров](#)
- [Настройка группового компьютера](#)
- [Устранение неполадок при наличии нескольких сетевых интерфейсов](#)

10.11.2.1 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.

10.11.3 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 "Идентификаторы хоста" на консоли СМС для определения сетевой интерфейсной платы для сервера платформы Business Intelligence. Она может быть определена именем хоста или

IP-адресом. Дополнительные сведения о настройке параметра **Идентификаторы хоста** см. в разделе «Устранение неполадок при наличии нескольких сетевых интерфейсов».

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 выполнения дополнительных настроек требуется настройка DNS для эффективной маршрутизации связи между всеми компонентами сервера платформы Business Intelligence. В этом примере DNS должен маршрутизировать подключения других серверов платформы Business Intelligence к личному адресу сервера репозитория файлов.

См. также

- [Устранение неполадок при наличии нескольких сетевых интерфейсов](#)

10.11.3.1 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 СМС.
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.

10.11.3.2 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](#)

10.11.3.3 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 CMS заданы параметры имени хоста CMS. Если маршрутизация основного сетевого интерфейса невозможна, выполните нижеуказанные инструкции для привязки платформы SAP BusinessObjects Business Intelligence к дополнительному сетевому интерфейсу с возможностью маршрутизации. Выполните данные действия сразу же после установки платформы BI на локальном компьютере перед установкой платформы BI 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. Чтобы связать SIA с определенным сетевым интерфейсом, введите номер порта целевого сетевого интерфейса в поле **Порт**.
5. Нажмите кнопку **ОК** и откройте вкладку «Запуск».
6. В списке «Локальные серверы CMS» выберите CMS и нажмите кнопку **Свойства**.
7. Чтобы связать CMS с определенным сетевым интерфейсом, введите номер порта целевого сетевого интерфейса в поле **Порт**.
8. Чтобы применить новые параметры, нажмите кнопку **ОК**.
9. Запустите SIA и подождите, пока не запустятся серверы.

10. Запустите 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.

10.11.4 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 BI динамически устанавливает связь с доступным портом (выше чем 1024), регистрирует этот порт на сервере CMS, а затем прослушивает запросы платформы BI. При необходимости можно выполнить настройки, чтобы каждый компонент сервера выполнял прослушивание на определенном порте (а не выбирал динамически любой доступный порт). Например, потребуется вручную настроить порт запроса для каждого сервера платформы BI, который должен передавать данные через брандмауэр.

Номера портов можно указать в CMC 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.
Порт сервера имен	Определяет порт платформы SAP BusinessObjects Business Intelligence, через который CMS прослушивает запросы службы имен. По умолчанию это порт 6400.	Не применимо.

10.11.4.1 Для изменения порта CMS по умолчанию в CMS

Если в кластере уже выполняется CMS, можно использовать CMS 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 CMS.
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».

10.11.4.2 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. Чтобы привязать CMS к определенному порту, введите номер порта в поле **Порт**.
6. Чтобы применить новые параметры, нажмите кнопку **ОК**.
7. Запустите SIA и подождите, пока не запустятся серверы.

10.11.4.3 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 – Удалить узел** и нажмите клавишу **ВВОД**.
4. Выберите узел, размещенный на сервере CMS, в который нужно внести изменения, и нажмите клавишу **ВВОД**.
5. Выберите **3 - Изменить локальный CMS** и нажмите клавишу **Enter**.
Появится список CMS, размещенных на узле.
6. Выберите CMS для изменения 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 **ВВОД**.

9. Введите аргументы командной строки для CMS или оставьте текущие аргументы и нажмите клавишу **ВВОД**.
10. Введите quit для выхода из скрипта.
11. Запустите SIA с помощью `ccm.sh` и дождитесь, пока запустятся серверы.

10.11.4.4 Изменение порта, который используется сервером для приема запросов

Примечание:

С помощью этих действий невозможно изменить порт запроса для центрального сервера управления (CMS). См. раздел «Изменение порта, используемого CMS для приема запросов».

1. Перейдите в область управления «Серверы» в CMS.
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.

10.12 Управление узлами

10.12.1 Использование узлов

Узел - это группа серверов платформы SAP BusinessObjects Business Intelligence, которая выполняется на одном хосте и управляется одним агентом SIA. Все серверы в узле запускаются под одной учетной записью. Один компьютер может содержать множество узлов, поэтому процессы можно выполнять от имени разных учетных записей пользователя. Один агент SIA управляет всеми серверами узла и осуществляет их мониторинг, обеспечивая нормальную работу серверов.

Примечание:

Для защищенного выполнения всех процедур управления узлом необходимо использовать учетную запись администратора с аутентификацией администратора. Однако если между серверами включено взаимодействие SSL, необходимо отключить SSL, прежде чем выполнять задачи, связанные с управлением узлами.

Примечание:

Убедитесь, что имеются все драйверы БД, требуемые для подключения любых серверов платформы BI к их источникам данных (например, для подключения CMS к базе данных CMS), и уже настроена соответствующая среда (например, заданы соответствующие переменные среды).

См. также

- [Настройка серверов для SSL](#)
- [Подготовка компьютера под управлением ОС Unix для работы с SQL Anywhere](#)

10.12.1.1 Переменные

Переменная	Описание
<INSTALLDIR>	Каталог установки SAP BusinessObjects Business Intelligence. В ОС Windows: C:\Program Files (x86)\SAP BusinessObjects
<SCRIPTDIR>	Каталог, в котором размещаются скрипты управления узлами. <ul style="list-style-type: none"> В ОС Windows: <КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts В ОС Unix: <КАТАЛОГ_УСТАНОВКИ>/sap_bobj/enterprise_xi40/<PLATFORM64>/scripts
<PLATFORM32>	Имя операционной системы Unix. Допустимыми значениями являются следующие: <ul style="list-style-type: none"> aix_rs6000 linux_x86 solaris_sparc win32_x86
<PLATFORM64>	Имя операционной системы Unix. Допустимыми значениями являются следующие: <ul style="list-style-type: none"> aix_rs6000_64 linux_x64 solaris_sparcv9 win64_x64

10.12.1.2 Подготовка компьютера под управлением ОС Unix для работы с SQL Anywhere

Необходимо создать файл `odbc.ini` и определить его источник, прежде чем можно будет использовать SQL Anywhere в качестве источника данных ODBC на компьютере под управлением Unix.

Примечание:

Эта процедура является ненужной, если используется связанный SQL Anywhere, установленный вместе с платформой BI.

1. Создайте файл `odbc.ini` в папке

`<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM64>`.

2. Введите имя источника базы данных (DSN), имена базы данных и сервера SQL Anywhere, а также IP-адрес и номер порта компьютера, на котором размещается сервер БД SQL Anywhere.
3. Сохраните файл `odbc.ini`.
4. Включите среду SQL Anywhere в свою текущую среду.
Например, если в качестве оболочки командной строки используется Bash, определите в качестве источника 64-разрядную версию `sa_config.sh`.
5. Определите переменную среды с именем `ODBCINI`, которая указывает, где был создан файл `odbc.ini`.
Настройте переменную среды так, чтобы переменная среды `ODBCINI` могла быть видима дочерним процессам.

Пример:

Пример файла `odbc.ini`:

```
[ODBC Data Sources]
SampleDatabase=SQLAnywhere 12.0

[SampleDatabase]
UID=Administrator
PWD=password
DatabaseName=SampleDatabase
ServerName=SampleDatabase
CommLinks=tcipip(host=192.0.2.0;port=2638)
Driver=/build/bo/sqlanywhere12/lib64/libdbodbc12.so
```

Пример команды `source`:

```
source /build/bo/sqlanywhere12/bin64/sa_config.sh
ODBCINI=/build/bo/sap_bobj/enterprise_xi40/linux_x64/odbc.ini;export ODBCINI
```

См. также

- [Переменные](#)

10.12.2 Добавление нового узла

Программа установки создает один узел при первой установке платформы SAP BusinessObjects Business Intelligence.

Если требуется запускать серверы под различными учетными записями пользователей, могут потребоваться дополнительные узлы.

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.

Примечание:

Используйте CCM или скрипт управления узлами на компьютере, где требуется добавить узел. Добавление узла на удаленном компьютере невозможно.

Установка платформы BI является уникальным экземпляром файлов платформы BI, созданным программой установки на компьютере. Экземпляр установки платформы BI можно использовать только в одном кластере. Узлы, принадлежащие к разным кластерам, совместно использующим одну установку платформы BI, не поддерживаются, поскольку исправление и обновление для этого типа развертывания невозможны. Несколько установок программного обеспечения на одном компьютере поддерживаются только платформами UNIX и только в случае, если каждая установка выполняется под уникальной учетной записью пользователя и устанавливается в отдельной папке, так что установки не используют общие файлы.

Следует помнить, что все компьютеры в кластере должны иметь одинаковые версии и уровни пакетов исправлений.

10.12.2.1 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 `serverconfig.sh`.

Для получения дополнительных сведений см. *Руководство по установке платформы SAP BusinessObjects Business Intelligence*.

10.12.2.2 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 номер 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 номер порта 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 новая системы CMS используют разные порты.

5. Ознакомьтесь со сведениями на странице подтверждения и нажмите кнопку **Готово**.

Диспетчер SCM создает узел. При возникновении любых ошибок см. сведения о них в файле журнала.

После этого можно запустить новый узел с помощью SCM.

10.12.2.2.1 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:

Из-за ограничений командной строки в этих параметрах необходимо использовать знак крышки (^) для отключения пробелов, знак равенства (=) и точку с запятой (;), если текст не заключен в кавычки.

```
<SCRIPTDIR>\AddNode.bat -name mynode2
-siaport 6415
-cms mycms:6400
```

```
-username Administrator
-password My^ Password
-cmsport 7400
-dbdriver mysqldatabasesubsystem
-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
-dbkey abc1234
-noservers
-createcms
```

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](#)

10.12.2.3 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 номер порта 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 номер порта 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 новая системы CMS используют разные порты.

7. Ознакомьтесь со сведениями на странице подтверждения и нажмите клавишу **Enter**.

Диспетчер SCM 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.

10.12.2.3.1 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
-noservers
-createcms
```

См. также

- [Переменные](#)
- [Параметры скрипта для добавления, восстановления и удаления узлов](#)

10.12.3 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](#)

10.12.3.1 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 центрального сервера управления (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 номер 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 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.

5. Ознакомьтесь со сведениями на странице подтверждения и нажмите кнопку Готово.

ССМ 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 ССМ.

10.12.3.1.1 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:

Из-за ограничений командной строки в этих параметрах необходимо использовать знак крышки (^) для отключения пробелов, знак равенства (=) и точку с запятой (;), если текст не заключен в кавычки.

```
<SCRIPTDIR>\AddNode.bat -name mynode2
-slapport 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](#)

10.12.3.2 Восстановление узла в Unix

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**.

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 центрального сервера управления (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 номер порта 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 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.

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.

10.12.3.2.1 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
-slaport 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](#)

10.12.4 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](#)

10.12.4.1 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 и учетные данные администратора для службы CMS.

Диспетчер CCM удаляет узел и все присутствующие в нем серверы.

10.12.4.1.1 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](#)

10.12.4.2 Удаление узла в Unix

До и после удаления узла создайте резервную копию конфигурации сервера 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. Если потребуется, введите имя хоста, номер порта и учетные данные администратора для CMS.

Узел и все присутствующие в нем серверы удаляются.

10.12.4.2.1 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](#)

10.12.5 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](#)

10.12.5.1 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» 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](#)

10.12.5.2 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**.
7. После создания узла на странице «Управление серверами» 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.

8. Выполните команду `<INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>` для запуска нового узла.
9. 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](#)

10.12.6 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 серверы всех типов, установленных на компьютере с исходным узлом, также установлены в целевом кластере.
- Для добавления нового компьютера в рабочий кластер и запрета его использования до завершения тестирования установите платформу SAP BusinessObjects Business Intelligence на автономный компьютер, протестируйте компьютер, а затем переместите узел в рабочий кластер.
- Версия платформы BI и уровень пакета обновления для этого компьютера должны соответствовать остальной части кластера.

Помните:

Перемещение узла возможно только на том компьютере, на котором он расположен.

10.12.6.1 Перемещение существующего узла в Windows

В этом примере узел, который требуется переместить, установлен в целевой системе. Изначально исходная системная машина была автономной, но впоследствии она будет добавлена в целевой кластер.

Предупреждение:

Перед перемещением узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

1. Остановите узел в Central Configuration Manager (CCM).
2. 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 необходимости введите имя хоста и номер порта для существующего CMS исходной системы, а также учетные данные администратора.

- Если исходное развертывание остановлено, выберите пункт **Запуск нового временного CMS** и нажмите кнопку **Далее**.

При появлении соответствующего запроса введите имя хоста и номер порта 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.

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.

10.12.6.1.1 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`. Для получения подробных сведений см. раздел «Параметры скрипта для перемещения узлов».

Пример:

Из-за ограничений командной строки в этих параметрах необходимо использовать знак крышки (^) для отключения пробелов, знак равенства (=) и точку с запятой (;), если текст не заключен в кавычки.

```
<SCRIPTDIR>\MoveNode.bat -cms sourceMachine:6409
-username Administrator
-password Password1
-dbdriver mysqldatabasesubsystem
-connect "DSN=Source BOEXI40;UID=username;PWD=Password1;HOSTNAME=databasel;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](#)

10.12.6.2 Перемещение существующего узла в Unix

В этом примере узел, который требуется переместить, установлен в целевой системе. Изначально исходная системная машина была автономной, но впоследствии она будет добавлена 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 необходимости введите имя хоста и номер порта для существующего CMS исходной системы, а также учетные данные администратора.
 - 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.

10.12.6.2.1 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](#)

10.12.7 Параметры скриптов**10.12.7.1 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 центрального сервера управления (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

Параметр	Описание	Пример
-cmsport	<ul style="list-style-type: none"> Номер порта CMS при запуске временной системы CMS. <p>Ограничение: Также необходимо использовать параметры -usetempcms, -dbdriver, -connect, и -dbkey.</p> <ul style="list-style-type: none"> Номер порта CMS при создании новой системы CMS. <p>Ограничение: Также необходимо использовать параметры -dbdriver, -connect, и -dbkey.</p>	-cmsport 6401
-connect	<p>Строка соединения для системной базы данных CMS (или временной системы CMS).</p> <p>Примечание: Пропустите атрибуты HOSTNAME и PORT при соединении с базами данных DB2, Oracle, SQL Anywhere, SQL Server или Sybase.</p>	<p>-connect "DSN=BusinessObjects CMS 10.10.10.10:3306;UID=sa;PWD=sa;HOSTNAME=10.10.10.10;PORT=3306"</p>
-dbdriver	<p>Драйвер базы данных CMS.</p> <p>Допустимые значения:</p> <ul style="list-style-type: none"> db2databasesubsystem maxdbdatabasesubsystem mysqldatabasesubsystem oracledatabasesubsystem sqldatabasesubsystem sqlserverdatabasesubsystem sybasedatabasesubsystem newdbdatabasesubsystem 	-dbdriver mysqldatabasesubsystem
-dbkey	Ключ кластера.	-dbkey abc1234
-name	Имя узла	-name mynode2

Параметр	Описание	Пример
-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
-usetempcms	Предупреждение: Не используйте этот параметр, если используется -cms Запускает и использует временный CMS. Примечание: Используйте временный CMS, когда развертывание не запущено.	-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](#)

10.12.7.2 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
-cmsport	<ul style="list-style-type: none"> Номер порта CMS при запуске временной системы CMS. <p>Ограничение: Также необходимо использовать параметры <code>-usetempcms</code>, <code>-dbdriver</code>, <code>-connect</code>, и <code>-dbkey</code>.</p> <ul style="list-style-type: none"> Номер порта CMS при создании новой системы CMS. <p>Ограничение: Также необходимо использовать параметры <code>-dbdriver</code>, <code>-connect</code>, и <code>-dbkey</code>.</p>	-cmsport 6401
-connect	<p>Строка соединения исходного CMS или временной системной базы данных CMS.</p> <p>Примечание: Пропустите атрибуты <code>HOSTNAME</code> и <code>PORT</code> при соединении с базами данных DB2, Oracle, SQL Anywhere, SQL Server или Sybase.</p>	-connect "DSN=Source DB2, DSN=PD, DSN=CSNA, DSN=ORF30 HOSTNAME=hostname, PORT=3000"

Параметр	Описание	Пример
-dbdriver	<p>Драйвер базы данных исходного CMS.</p> <p>Допустимые значения:</p> <ul style="list-style-type: none"> db2databasesubsystem maxdbdatabasesubsystem mysqldatabasesubsystem oracledatabasesubsystem sqldatabasesubsystem sqlserverdatabasesubsystem sybasedatabasesubsystem newdbdatabasesubsystem 	-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
-destconnect	<p>Строка соединения конечной системой базы данных CMS.</p> <p>Примечание: Пропустите атрибуты HOSTNAME и PORT при соединении с базами данных DB2, Oracle, SQL Anywhere, SQL Server или Sybase.</p>	-destconnect "DSN=DestinationMachine;PORT=6401"
-destdbdriver	<p>Драйвер базы данных конечного CMS</p> <p>Допустимые значения:</p> <ul style="list-style-type: none"> db2databasesubsystem maxdbdatabasesubsystem mysqldatabasesubsystem oracledatabasesubsystem sqldatabasesubsystem sybasedatabasesubsystem newdbdatabasesubsystem 	-destdbdriver sybasedatabasesubsystem
-destdbkey	Ключ кластера назначения.	-destdbkey def5678

Параметр	Описание	Пример
-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
-usetempcms	<p>Предупреждение: Не используйте этот параметр, если используется -cms</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](#)

10.12.8 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.

10.12.8.1 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.

10.12.9 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 SAP BusinessObjects Business Intelligence должен осуществляться с использованием той же учетной записи, с которой эта система была установлена. Чтобы использовать иную учетную запись, следует переустановить систему с необходимой записью.

10.12.9.1 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.

10.13 Переименование компьютера в развертывании платформы BI

10.13.1 Изменение имен кластеров

Ниже представлены рекомендации по переименованию кластеров.

Предупреждение:

Никогда не развертывайте несколько кластеров с одинаковыми именами.

Условие	Действие
Имя кластера изменяется.	Проинформируйте пользователей о новом имени кластера и попросите их использовать это имя (после первого соединения с CMS с помощью синтаксиса <i><имя хоста>: <порт></i>). Обновите имя кластера в файлах свойств всех серверов веб-приложений на веб-уровне.
Вы устанавливаете другую версию портфеля решений SAP BusinessObjects на компьютере, на котором ранее выполнялся сервер CMS, или добавляете компьютер в другой кластер.	<ul style="list-style-type: none"> Убедитесь в том, что новый сервер CMS запущен на другом порте. Используйте разные пароли для различных кластеров, чтобы предотвратить вход пользователей на неверный кластер.

10.13.2 Изменение IP-адресов

Чтобы избежать внесения в конфигурацию изменений, ведущих изменение IP-адреса компьютера, выберите команду **Свойства сервера** на вкладке **СМС Серверы**, а затем убедитесь в том, что все серверы привязаны к именам хостов, или используйте параметр **Назначать автоматически**. Кроме того, необходимо учитывать следующие рекомендации:

Условие	Действие
Вы используете ODBC с базой данных CMS или базой данных аудита.	Убедитесь в том, что DSN использует имя хоста сервера базы данных CMS.

Условие	Действие
Вы используете другой тип соединения с базой данных CMS или базой данных аудита.	Используйте ССМ, чтобы обновить базу данных для использования имени хоста сервера базы данных.
База данных CMS или база данных аудита расположена на том же хосте, что и CMS.	Используйте <code>localhost</code> в качестве имени компьютера.
URL используется для веб-приложений платформы BI, к которым пользователи обращаются с помощью веб-браузера (например, СМС).	Используйте имена хостов вместо IP-адресов для URL-адреса по умолчанию. Чтобы обновить URL для средства просмотра по умолчанию, выберите Параметры обработки для выбранного приложения. Например, для Open Document откройте вкладку Приложения в СМС, щелкните правой кнопкой мыши Open Document и выберите Параметры обработки .
URL используется для клиентов платформы BI, основанных на веб-службах (например, Crystal Reports для Java или LiveOffice).	
Используется OpenDocument.	

Альтернативные указания

Примечание:

Следуйте этим указаниям, если приведенные выше рекомендации неприменимы.

Таблица 10-9: Для компьютеров, на которых размещаются серверы

Условие	Действие
Хост содержит серверы платформы BI, а серверы должны привязываться к определенным IP-адресам.	Измените IP-адреса на вкладке Серверы СМС, но не перезапускайте серверы до окончания полного обновления на компьютере. Затем перезагрузите компьютер, а не отдельные серверы платформы BI.
Соединение с базой данных должно использовать IP-адрес.	Измените IP-адрес.
В статической IP-сети необходимо изменение IP-адреса.	Измените IP-адрес компьютера платформы BI. Совет: Войдите в СМС, чтобы убедиться в работоспособности платформы BI.

Помните:

Перезапустите компьютер после выполнения этого действия.

Таблица 10-10: Для компьютеров, на которых размещен сервер веб-приложений

Условие	Действие
URL-адрес средства просмотра OpenDocument по умолчанию должен использовать IP-адрес.	Обновите IP-адрес в поле URL средства просмотра по умолчанию в разделе Настройка обработки вкладки СМС Приложения .
Пользователи обращаются к веб-приложениям платформы BI (например, к СМС) путем ввода в браузер URL-адреса с IP-адресом.	Проинформируйте пользователей о новом IP-адресе.
Клиенты платформы BI, основанные на веб-службах (например, Crystal Reports для Java или LiveOffice), должны использовать IP-адреса.	Настройте все клиенты на использование нового IP-адреса.

См. также

- [Выбор новой или существующей базы данных центрального сервера управления](#)

10.13.3 Переименование компьютеров

Компьютеры в развертывании платформы SAP BusinessObjects Business Intelligence можно переименовать в любой момент. Для этого остановите все серверы платформы BI на компьютере и переименуйте его. Ниже представлены рекомендации по переименованию компьютеров.

Условие	Действие
Вы входите в систему впервые.	Используйте имя компьютера CMS, а не имя кластера.
Развертывание содержит несколько компьютеров.	Убедитесь в том, что в ходе переименования работают все серверы CMS на других компьютерах.

10.13.3.1 Уровень сервера

Примечание:

Перед переименованием компьютера CMS следует ознакомиться с конфигурацией всех серверов на изменяемом компьютере на вкладке СМС «Управление серверами». Если свойство «Имя хоста» использует старое имя хоста CMS, измените его на новое имя хоста CMS.

Помните:

Не перезапускайте серверы до завершения всех процедур переименования компьютеров.

Следуйте приведенным ниже указаниям при переименовании компьютеров уровня сервера.

Условие	Действие
Переименованный компьютер содержит CMS, а пользователи ранее входили в систему, предоставляя имя старого компьютера.	Проинформируйте пользователей об имени компьютера CMS и попросите использовать его.
Переименованный компьютер содержит CMS, а файлы свойств по умолчанию для веб-приложения BI содержат старое имя хоста CMS в свойстве <code>cms.default</code> .	<p>Измените имя компьютера CMS в свойстве <code>cms.default</code> во всех настраиваемых файлах свойств на всех компьютерах веб-уровня. В Tomcat созданные файлы свойств по умолчанию размещаются в папке <code><INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom</code>.</p> <p>Примечание: Если настраиваемые файлы свойств не существуют, создайте новые файлы свойств. Скопируйте файлы свойств по умолчанию в настраиваемую папку и удалите из настраиваемых файлов свойств все содержимое за исключением строки <code>cms.default</code>.</p>
Переименованный компьютер содержит CMS, а на одном из компьютеров кластера установлен SAP BusinessObjects Explorer.	<p>Замените старое имя хоста CMS новым именем в свойстве <code>default.cms.name</code> файла <code>default.settings.properties</code> на всех компьютерах с серверами веб-приложений. По умолчанию в Tomcat файл <code>default.settings.properties</code> находится в папке <code><INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\explorer\WEB-INF\classes\</code>.</p> <p>Помните: Перезапустите веб-приложение Explorer или сервер приложений после выполнения этого действия.</p>

Условие	Действие
Вместе с Explorer используется SSO.	Обновите значение <code>cms</code> в файле <code>jsp-sso-provider.jsp</code> и измените значения <code>sso.global.cms</code> и <code>sso.trusted.auth.x509.cms</code> в файле <code>sso.properties</code> на новое имя хоста CMS.
Используются наборы Portal Integration Kit или настраиваемые приложения.	Настройте наборы Portal Integration Kit или настраиваемые приложения на использование нового имени хоста CMS.
Развертывание соответствует всем приведенным ниже условиям: <ul style="list-style-type: none"> • Кластер имеет несколько узлов. • Все серверы CMS выполняются только на переименованном компьютере. • Как минимум на одном из узлов не размещен CMS. • Переименовывается компьютер, содержащий как минимум один узел. • IP-адрес меняется при переименовании. 	Используйте CCM для выполнения рабочего процесса «Повторно создать узел» для всех узлов за исключением узла, содержащего CMS, а затем запустите все узлы платформы BI в развертывании. Дополнительные сведения см. в разделе «Управление узлами».

Помните:

Перезапустите веб-приложение или сервер приложений после выполнения этого действия.

См. также

- [Восстановление узла](#)

10.13.3.2 Веб-ярус

При переименовании компьютера с сервером веб-приложений платформы SAP BusinessObjects BI выполните следующие действия:

Условие	Действие
Вы изменяете имя компьютера с сервером веб-приложений платформы BI, а URL-адрес средства просмотра OpenDocument по умолчанию содержит имя хоста сервера веб-приложений.	Войдите в CMC и обновите URL-адрес средства просмотра по умолчанию в разделе Приложения > CMC > Настройка обработки .

Условие	Действие
Вы изменяете имя компьютера с сервером веб-приложений платформы BI, а пользователи обращаются к веб-приложениям платформы BI с помощью URL-адреса, который содержит новое имя хоста сервера веб-приложений.	Попросите пользователей обращаться к веб-приложениям платформы BI с помощью URL-адреса, который содержит новое имя хоста сервера веб-приложений.
Вы изменяете имя компьютера с сервером веб-приложений платформы BI, а клиенты платформы BI на основе веб-служб используют в URL-адресе имена хостов сервера веб-приложений.	Настройте все клиенты платформы BI на основе веб-служб для использования нового имени сервера веб-приложений.

10.13.3.3 Базы данных

При переименовании компьютера, на котором размещена база данных системы CMS или база данных аудита, руководствуйтесь следующими рекомендациями:

Условие	Действие
Вы хотите избежать обновления IP-адреса.	Используйте имя компьютера базы данных CMS или базы данных аудита в имени источника данных (DSN).
База данных CMS или база данных аудита расположена на том же хосте, что и CMS.	Используйте <code>localhost</code> в имени DSN, чтобы предотвратить изменения при изменении имени хоста.

База данных системы CMS

Условие	Действие
Вы используете ODBC и переименовываете компьютер с размещенной базой данных системы CMS.	Измените имя DSN базы данных CMS на новое имя хоста сервера баз данных.
Вы используете другой тип соединения с базой данных и переименовываете компьютер с размещенной базой данных системы CMS.	Используйте CCM, чтобы обновить базу данных CMS новым именем хоста сервера базы данных на всех узлах кластера.

База данных аудита

Условие	Действие
Вы используете ODBC и переименовываете компьютер с размещенной базой данных аудита.	Измените имя DSN базы данных аудита на новое имя хоста сервера баз данных.
Вы используете другой тип соединения с базой данных и переименовываете компьютер с размещенной базой данных аудита.	Измените имя компьютера сервера базы данных на новое имя на вкладке СМС Аудит .

10.13.3.4 Серверы репозитория файлов

При переименовании компьютера, на котором размещено хранилище файлов FRS, необходимо обновить серверы «репозитория входящих файлов» и «репозитория исходящих файлов» на странице СМС «Управление сервером» и убедиться в том, что свойства «Каталог хранилища файлов» и «Временный каталог» содержат новый путь к хранилищу, а затем перезапустить серверы.

10.14 Использование 32-битных и 64-битных сторонних библиотек вместе с платформой BI

На серверах платформы BI сочетаются 32-битные 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 BI, необходимо задать отдельные переменные среды для каждой из версий на компьютере, где размещается платформа BI. Затем требуется задать дополнительную переменную среды, которая содержит разделенный запятыми список переменных среды, которые имеют 32-битную и 64-битную версии. При запуске процесса платформой BI будет выбрана переменная, соответствующая разрядности процесса.

- `<FIRST_ENV_VAR>` = значение, которое будет использоваться 64-битными процессами платформы BI.
- `<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 ВІ установлена на компьютере АІХ наряду 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

Примечание:

В Linux и Solaris не используйте BOE_USE_32BIT_ENV_FOR=LD_LIBRARY_PATH для разделения 32-битных и 64-битных путей. Вместо этого добавьте и 32-битный, и 64-путь в LD_LIBRARY_PATH.

10.15 Управление заполнителями сервера и узла

10.15.1 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](#)

10.15.2 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 щелкните **Сохранить** для продолжения.

См. также

- [Заполнители сервера и узлов](#)

Управление базами данных центрального сервера управления (CMS)

11.1 Управление соединением с системной базой 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 соединение с системной базой 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 соединения с базой 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 соединение с базой данных. Например, это может быть необходимо в случае проверки целостности базы данных перед восстановлением соединения с 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](#)

11.1.1 Выбор SAP HANA в качестве базы данных CMS

Чтобы использовать в качестве базы данных CMS SQL Anywhere, необходимо выполнить следующие действия:

1. Остановите все узлы в системе.
2. Запустите следующее приложение:
 - В UNIX выполните `./cmsdbsetup.sh`.
 - В ОС Windows запустите Central Configuration Manager (CCM).
3. Скопируйте данные из базы данных CMS по умолчанию, выбрав SQL Anywhere в качестве целевой базы данных. Дополнительные сведения см. в связанном разделе «Копирование данных из одной базы данных CMS в другую».
4. В многоузловых развертываниях необходимо изменить источник данных CMS на каждом узле (за исключением узла, в который копируется база данных) на новую базу данных SQL Anywhere. Дополнительные сведения см. в связанном разделе «Выбор новой или существующей базы данных CMS».
5. Убедитесь в том, что развертывание работает (например, войдите в CMC и просмотрите отчет).

См. также

- [Копирование данных из одной базы данных CMS в другую.](#)
- [Выбор новой или существующей базы данных центрального сервера управления](#)

11.1.2 Выбор SAP HANA в качестве базы данных CMS

Чтобы использовать SAP HANA в качестве базы данных CMS, необходимо выполнить следующие действия.

1. Установите платформу BI с базой данных CMS по умолчанию.
2. Установите клиент SAP HANA.
3. Создайте подключение к SAP HANA.
 - В ОС Unix проверьте переменную среды ODBCINI. Если эта переменная существует и указывает на существующий файл `odbc.ini`, добавьте в этот файл следующие строки:

```
[ODBC Data Sources]
NewDB=<New_DB_version>

[NewDB]
SERVERNODE=<HANA Server IP address>:<HANA server port #>
```

<New_DB_version> – версия SAP HANA, например «NewDB 1.0»; <HANA Server IP address> – IP-адрес сервера SAP HANA; <HANA server port #> – номер порта сервера SAP HANA.

Если переменная среды ODBCINI не существует, создайте файл `odbc.ini` в каталоге <КАТАЛОГ_УСТАНОВКИ>/sap_bobj/enterprise_xi40/, добавьте в него описываемые выше строки, и присвойте переменной ODBCINI следующее значение:

```
ODBCINI=<INSTALLEDIR>/sap_bobj/enterprise_xi40/odbc.ini
```

- В ОС Windows создайте соединение ODBC с SAP HANA.

Примечание:

Для изменения соединения ODBC используйте 64-разрядную версию администратора источников данных ODBC: **Пуск > Панель управления > Средства администрирования > Источники данных (ODBC)**.

4. Убедитесь в том, что соединение с сервером SAP HANA устанавливается.
 - В ОС Unix можно проверить соединение с сервером SAP HANA с помощью указанной ниже команды. Переменные в следующем примере относятся к установке SAP HANA:


```
<INSTALLDIR>/odbcereg <SERVER>:<HDBINDEXSERVERPORT> <SYSTEMID> <NONADMINUSER> <NONADMINPASSWORD>
```
 - В ОС Windows можно использовать администратор источников данных ODBC для тестирования соединения ODBC с SAP HANA.
5. В ОС Unix скопируйте `libodbcHDB.so` из папки установки SAP HANA в папку `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj/enterprise_xi40/<ПЛАТФОРМА>`
6. Остановите все узлы в системе.
7. Запустите соответствующее приложение:
 - В UNIX выполните `./cmsdbsetup.sh`.
 - В ОС Windows запустите Central Configuration Manager (CCM).
8. Скопируйте данные из базы данных CMS по умолчанию, выбрав SAP HANA в качестве целевой базы данных. Дополнительные сведения см. в связанном разделе «Копирование данных из одной базы данных CMS в другую».
9. В многоузловых развертываниях необходимо изменить источник данных CMS на каждом узле (за исключением узла, в который копируется база данных) на новую базу данных SAP HANA. Дополнительные сведения см. в связанном разделе «Выбор новой или существующей базы данных CMS».
10. Убедитесь в том, что развертывание работает (например, войдите в CMC и просмотрите отчет).

См. также

- [Копирование данных из одной базы данных CMS в другую.](#)
- [Выбор новой или существующей базы данных центрального сервера управления](#)

11.2 Выбор новой или существующей базы данных центрального сервера управления

Можно использовать CCM или `cmsdbsetup.sh` 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).

Примечание:

- При использовании IBM DB2 в качестве базы данных CMS и обновлении этой базы данных с версии старше 9.5 Fix Pack 5 до версии 9.5 Fix Pack 5 или новее (для линейки 9.5) или обновлении с версии старше 9.7 Fix Pack 1 до версии 9.7 Fix Pack 1 или новее (для линейки 9.7) во время следующей перезагрузки узла платформы BI или CMS схема баз данных CMS автоматически обновится CMS и станет поддерживать совместимую с HADR схему.

Это продолжительный процесс, во время которого платформа BI недоступна для использования. Не прерывайте процесс обновления, чтобы не повредить базу данных CMS. Перед выполнением этой операции настоятельно рекомендуется создать резервную копию базы данных CMS. Не пытайтесь использовать IBM HADR с базой данных IBM DB2 CMS версии старше 9.5 Fix Pack 5 (для линейки 9.5) или 9.7 Fix Pack 1 (для линейки 9.7).

- Не настраивайте установленную платформу BI на использование базы данных системы CMS, относящейся к другому кластеру, если не выполняется рабочий процесс копии системы.

Если версии и уровни исправлений установленных платформ BI и баз данных CMS различаются, если пути установки различаются, если различаются установленные компоненты и т. д., возможно повреждение системы.

Чтобы предотвратить повреждение, не пытайтесь переносить содержимое BI из одной системы в другую, назначая развертывание платформы BI базе данных CMS другой системы платформы BI, особенно при различии версий и уровней исправлений.

11.2.1 Выбор новой или существующей базы данных CMS в Windows

1. Используйте консоль CCM для остановки Server Intelligence Agent (SIA).
2. Выберите SIA и нажмите кнопку **Указать источник данных CMS**.
3. Выберите **Обновить параметры источника данных** и щелкните **ОК**.
4. Выберите драйвер базы данных и щелкните **ОК**.
5. Эти шаги зависят от типа выбранного соединения:

- Если вы выбрали ODBC, появится диалоговое окно Windows «Выберите источник данных». Выберите источник данных ODBC, который требуется использовать в качестве базы данных CMS, а затем нажмите кнопку **ОК**. (Щелкните **Создать**, чтобы настроить новое DSN.) 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. После ввода этой информации нажмите **ОК**.
6. Укажите ключ кластера.
 7. Перезапустите агент Server Intelligence.

11.2.2 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. При запросе системы введите тип новой базы данных центрального сервера управления.
4. Введите информацию о базе данных (например, имя хоста, имя пользователя, пароль и ключ кластера).
Сообщение с уведомлением появляется, когда база данных центрального сервера управления назначена новому каталогу.
5. Если появляется запрос на восстановление Server Intelligence (SIA), укажите пароль администратора и необходимый номер порта, через который будет устанавливаться связь центральный сервер управления.

Примечание:

Эта подсказка появится, только если назначение выполняется в пустой базе данных центрального сервера управления.

11.3 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 CMS 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](#)

11.3.1 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. Кроме того, на этом компьютере должны быть установлены двоичные файлы CMS.

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:

Серверы и объекты на компьютере, на котором запущена консоль CCM на шаге 1, будут также восстановлены. Однако не все объекты будут созданы заново; возможно повторное создание только ключевых объектов по умолчанию. Например, примеры отчетов не создаются повторно.

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**.

Примечание:

Убедитесь, что вы задали новый пароль администратора. По умолчанию для учетной записи администратора пароль не задан.

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.

11.3.2 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 подсказка восстановить Server Intelligence (SIA), укажите пароль администратора и необходимы номер порта, через который будет устанавливаться связь центральный сервер управления.

Примечание:

Это подсказки появятся, 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.

11.4 Копирование данных из одной базы данных CMS в другую.

С помощью Central Configuration Manager (CCM) или `cmsdbsetup.sh` можно копировать системные данные с одного сервера баз данных на другой. 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.

Прежде чем новые данные копируются в целевую базу данных, выполняется ее инициализация с удалением содержимого (все таблицы платформы SAP BusinessObjects Business Intelligence удаляются, а затем создаются заново). После завершения копирования данных целевая база данных устанавливается в качестве текущей базы данных для CMS.

Примечание:

Если требуется импортировать пользователей, группы, папки и отчеты из предыдущей основной версии платформы BI в текущую основную версию, воспользуйтесь средством управления обновлением платформы SAP BusinessObjects Business Intelligence. Для получения дополнительных сведений см. *Руководство по обновлению платформы SAP BusinessObjects Business Intelligence*.

11.4.1 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.`

11.4.2 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 Central Configuration Manager (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**.

11.4.3 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)

12.1 WACS

12.1.1 Сервер контейнера веб-приложений (WACS)

Серверы Web Application Container Server (WACS) обеспечивают платформу для размещения веб-приложений платформы SAP BusinessObjects Business Intelligence. 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 развертывание платформы SAP BusinessObjects Business Intelligence или внешних веб-приложений вручную или с использованием WDeploy.

12.1.1.1 Требуется ли WACS?

Если вы не хотите использовать сервер Java-приложений для размещения веб-приложений SAP BusinessObjects, для этого можно использовать 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 требуются.

12.1.1.2 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 вам не требуются особые навыки администрирования и обслуживания серверов Java-приложений.
- WACS предоставляет интерфейс администрирования, согласованный с другими серверами платформы SAP BusinessObjects Business Intelligence.

12.1.1.3 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 SAP BusinessObjects 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 брандмауэрами.	<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 параллельных 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

12.1.2 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.

12.1.2.1 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.

Сервер контейнера веб-приложений можно установить с помощью программы установки платформы SAP BusinessObjects Business Intelligence. 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**.

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 SAP BusinessObjects Business Intelligence будут развернуты на этом сервере. Вмешательство пользователя для развертывания или настройки CMC 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 Central Configuration Manager (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.

12.1.2.2 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 **Основные 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**.
 - Чтобы размещать на WACS веб-службы вида 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**.
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 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.

7. В окне «Серверы» щелкните созданный сервер WACS.
Открывается диалоговое окно «Свойства».
 8. Чтобы сервер WACS не запускался автоматически при перезапуске системы, на панели «Общие параметры» снимите флажок **Автоматически запускать этот сервер при запуске агента серверной аналитики**.
 9. Нажмите кнопку **Сохранить и закрыть**.
- Будет создан новый сервер WACS. К нему применяются параметры и свойства по умолчанию.

12.1.2.3 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 CMC.
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](#)

12.1.2.4 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**.

12.1.3 Добавление или удаление служб на сервере WACS

12.1.3.1 Добавление веб-приложения или веб-службы к WACS

Для добавления дополнительных веб-приложений или веб-служб платформы SAP BusinessObjects Business Intelligence 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.

12.1.3.2 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.

12.1.4 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 BI, в том числе WACS, и другими серверами платформы BI в вашем развертывании. Он называется CORBA SSL. Для получения дополнительных сведений об использовании SSL между серверами платформы BI 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, браузерами), 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](#)

12.1.4.1 Создание хранилища файла сертификата PKCS12

Существует ряд 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 (MMS) для Windows Server 2008.

1. Выполните вход в компьютер, на котором размещается WACS, в качестве 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 оснастку сертификатов в MMC:
 - a. В меню **Файл** выберите **Добавить/удалить оснастку**.
Открывается экран «Установка и удаление оснасток».
 - b. В списке «Доступные оснастки» выберите **Сертификаты** и нажмите кнопку **Добавить**.
 - c. Выберите **Учетная запись компьютера** и нажмите **Далее**.
 - d. Выберите **Локальный компьютер** и нажмите **Готово**.
 - e. Нажмите кнопку **ОК**.Встраиваемый файл сертификатов добавлен в MMC.
 5. В MMC разверните **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.

12.1.4.2 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 интегрируемый модуль**.
 - b. В списке «Доступные интегрируемые модули» выберите **Internet Information Services (IIS) Manager** и нажмите **Добавить**.
 - c. Нажмите кнопку **ОК**.Теперь интегрируемый модуль IIS добавлен в MMC.
4. Выполните описанные здесь шаги, чтобы создать список надежных сертификатов:
<http://www.iis.net/learn/install/installing-iis-7/compatibility-and-feature-requirements-for-windows-vista#NoWizard>.

12.1.4.3 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 планируется 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.

12.1.5 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

12.1.6 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).

При настройке единого входа с помощью Kerberos AD для Пакета SDK веб-служб и QaaWS также необходимо настроить как WACS, так и компьютер, на котором находятся службы WACS.

См. также

- [Подключаемый модуль безопасности Windows AD](#)
- [Сопоставление пользователей и групп AD](#)
- [Настройка учетной записи службы для аутентификации AD с Kerberos](#)
- [Запуск SIA под учетной записью службы платформы BI](#)
- [Включение аутентификации Kerberos в подключаемом модуле Windows AD для WACS](#)
- [Создание файлов конфигурации.](#)
- [Конфигурация WACS для AD Kerberos](#)
- [Настройка единого входа в AD Kerberos](#)

12.1.6.1 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.

- Включение аутентификации Kerberos и единого входа, если требуется единый вход.
- Задайте имя администратора доступа к службе (SPN) для учетной записи службы.

12.1.6.1.1 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](#)
- [Запуск SIA под учетной записью службы платформы BI](#)
- [Сопоставление пользователей и групп AD](#)

12.1.6.1.2 Настройка подключаемого модуля безопасности Windows AD для Kerberos

1. Перейдите в область управления **Аутентификация** в СМС.
2. Дважды щелкните **Windows AD**.
3. Убедитесь, что флажок **Включить Windows Active Directory (AD)** установлен.
4. В пункте **Параметры аутентификации** выберите **Использовать аутентификацию Kerberos**.
5. Если требуется настроить единый вход в базу данных, установите флажок **Контекст безопасности кэша (требуется для единого входа (SSO) в базу данных)**.
6. 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.
7. Если требуется настроить единый вход, выберите пункт **Включить единую регистрацию для выбранного режима аутентификации**.

Примечание:

При включении единого входа необходимо настроить WACS.

См. также

- [Настройка единого входа в AD Kerberos](#)

12.1.6.2 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).

12.1.6.2.1 Создание файла конфигурации Kerberos

Чтобы создать файл конфигурации Kerberos, выполните указанные ниже шаги.

1. Создайте файл `krb5.ini`, если он не существует, и сохраните его в каталоге `C:\Windows` для ОС 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.

12.1.6.2.2 Создание файла конфигурации входа JAAS

1. Создайте файл с именем `bscLogin.conf`, если он не существует, и сохраните его в каталоге по умолчанию: `C:\Windows`.

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 CMC.

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.

12.1.6.2.3 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
  }
```

12.1.6.3 Конфигурация WACS для AD Kerberos

После настройки компьютера, на котором размещается средство аутентификации WACS для AD Kerberos, необходимо настроить WACS с помощью Central Management Console (CMC).

12.1.6.3.1 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.

12.1.6.4 Устранение неполадок с Kerberos

Описанные ниже шаги могут помочь при возникновении проблем с настройкой Kerberos.

- Включение регистрации событий

- Тестирование конфигурации Kerberos

12.1.6.4.1 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».

12.1.6.4.2 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.

12.1.6.4.3 Сопоставленному пользователю AD не удастся войти в платформу BusinessObjects Business Intelligence в WACS

Несмотря на то, что пользователи сопоставлены с платформой BusinessObjects Business Intelligence, могут возникать две проблемы:

Ошибка входа в результате различия имен AD UPN и SAM

Идентификаторы пользователей Active Directory успешно сопоставлены с платформой BusinessObjects Business Intelligence. Несмотря на это им не удастся успешно выполнить вход в СМС 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.

12.1.7 Настройка единого входа в AD Kerberos

При настройке 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.

Перед настройкой сервера WACS на использование службы единого входа AD Kerberos необходимо сначала настроить компьютер, на котором размещается WACS, а затем настроить сам сервер WACS.

Примечание:

Если единый вход планируется использовать в среде обратного прокси, ознакомьтесь с приведенными в этом руководстве сведениями о безопасности.

См. также

- [Обзор вопросов безопасности](#)
- [Настройка Kerberos AD для WACS](#)
- [Настройка компьютера для единого входа AD Kerberos](#)
- [Настройка WACS для единого входа AD Kerberos](#)

12.1.7.1 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](#)
- [Настройка учетной записи службы для функции единого входа Vintela](#)
- [Настройка нескольких SPN-имен](#)
- [Увеличение лимита размера заголовка WACS](#)

В разделах ниже описано выполнение каждого из этих шагов.

12.1.7.1.1 Настройка нескольких SPN-имен

Использование нескольких SPN не поддерживается.

12.1.7.1.2 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.

12.1.7.2 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 принcipала службы" и "Файл ярлыков ключей", после чего выберите команду **Сохранить и закрыть**.
5. Перезапустите WACS.

Служба единого входа Active Directory готова к использованию.

12.1.7.3 Настройка модуля Kerberos и режима единого входа 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 единого входа в базе данных.

Примечание:

Эти инструкции объясняют, как настроить режим единого входа 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](#).

12.1.7.3.1 Включение режима единого входа 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 `C:\Windows`.
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.

12.1.8 Настройка веб-служб RESTful

Пакет веб-служб RESTful платформы Business Intelligence обеспечивает доступ к платформе BI по протоколу HTTP. Это позволяет пользователям переходить к репозиторию платформы BI и планировать объекты с использованием любого языка программирования, поддерживающего запросы HTTP. Веб-службы RESTful устанавливаются в составе сервера WACS.

В этом разделе описывается администрирование веб-служб RESTful. Подробнее о веб-службах RESTful см. в *руководстве разработчика веб-служб RESTful для платформы Business Intelligence*.

12.1.8.1 Приложения

12.1.8.1.1 Настройка базового URL-адреса для веб-служб RESTful

Если в развертывании платформы BI используется прокси-сервер или присутствует несколько экземпляров сервера контейнера веб-приложений, может потребоваться настройка базового URL-адреса, который будет использоваться веб-службами RESTful. Перед настройкой базового URL-адреса необходимо получить имя сервера и номер порта, на котором выполняется прослушивание запросов веб-службы RESTful.

Этот базовый URL-адрес будет использоваться в составе каждого запроса веб-службы RESTful. Разработчики программным способом определяют базовый URL-адрес и используют его для перенаправления запросов веб-службы RESTful на нужные сервер и порт. Базовый URL-адрес также используется в ответах веб-службы RESTful, определяя гиперссылки на другие ресурсы RESTful.

Примечание:

В установке платформы BI по умолчанию определяется базовый URL-адрес `http://<servername>:6405/biprws`. Замените параметр `<servername>` именем сервера, на котором размещаются веб-службы RESTful.

1. Войдите в Central Management Console в качестве пользователя с правами администратора.
2. В СМС щелкните пункт **Приложения**.
Откроется список приложений.
3. Щелкните правой кнопкой мыши элемент **Веб-служба REST > Свойства**
Откроется диалоговое окно «Свойства».
4. В текстовом поле **URL-адрес доступа** введите имя базового URL-адреса для веб-служб RESTful.

Например, введите `http://<servername>:<portnumber>/biprws`. Замените параметры `<servername>` и `<portnumber>` именем сервера и номером порта, на котором будет выполняться прослушивание запросов веб-службы RESTful, соответственно.

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

12.1.8.2 Свойства WACS

12.1.8.2.1 Настройка параметров командной строки Methods и Headers

Администратор может ограничить набор методов и заголовков, используемых веб-службами RESTful, путем добавления соответствующих параметров в раздел «Параметры командной строки» в свойствах службы контейнера веб-приложений (WACS). После изменения параметров необходимо перезапустить службу WACS.

1. Войдите в Central Management Console в качестве пользователя с правами администратора.
2. Щелкните **Серверы** и выберите элемент **Список серверов**.
3. Щелкните правой кнопкой мыши сервер контейнера веб-приложений, например `MySIA.WebApplicationContainerServer`, и выберите пункт **Свойства**.

Откроется вкладка **Свойства** для сервера контейнера веб-приложений.

4. В разделе «Параметры командной строки» укажите методы и заголовки, которые требуется разрешить.

Каждая группа параметров должна быть заключена в двойные кавычки. Не используйте методы GET, HEAD и POST. Для разделения значений параметров, таких как PUT и DELETE, используйте запятые, как показано в следующем примере.

```
"-Dcom.sap.bip.rs.cors.extra.methods= PUT, DELETE"
"-Dcom.sap.bip.rs.cors.extra.headers= X-SAP-LogonToken, X-SAP-PVL, WWW-Authenticate"
```

Примечание:

Значение по умолчанию для разрешения всех методов и заголовков: * (звездочка). Если не указать ни один параметр командной строки, также будут разрешены все методы и заголовки.

5. Нажмите кнопку **Сохранить и закрыть**.
6. Перезапустите службу, щелкнув правой кнопкой имя сервера WACS, например `MySIA.WebApplicationContainerServer`, и выбрав команду **Перезапустить сервер**.

12.1.8.2.2 Настройка системных свойств

Включение стека сообщений об ошибках

Администратор может настроить хранение сообщений об ошибках, возвращаемых веб-службами RESTful, в стеке ошибок. Это позволяет получить дополнительные сведения о том, где возникли ошибки, для более эффективной отладки.

Примечание:

В рабочих средах включение стека ошибок рекомендуется не во всех случаях, поскольку он может предоставлять те сведения о платформе BI, которые нежелательно раскрывать конечным пользователям. Включать стек ошибок в рабочих средах рекомендуется исключительно на время отладки, по завершении которой его следует отключить.

1. Войдите в Central Management Console в качестве пользователя с правами администратора.
2. Щелкните **Серверы** и выберите элемент **Список серверов**.
3. Щелкните правой кнопкой мыши сервер контейнера веб-приложений, например, `MySIA.WebApplicationContainerServer` и выберите пункт **Свойства**.
Откроется вкладка **Свойства** для сервера контейнера веб-приложений.
4. В области **Веб-служба RESTful** выберите параметр **Показать стек ошибок**.
5. Нажмите кнопку **Сохранить и закрыть**.

Сведения о стеке ошибок включаются в сообщения об ошибках веб-службы RESTful.

Настройка числа записей, отображаемых по умолчанию на каждой странице

Если ответ веб-службы RESTful содержит веб-канал с большим числом записей, он может быть разделен на несколько страниц. Вы можете настроить число записей, отображаемых по умолчанию на каждой странице. Разработчики, создающие запросы веб-службы RESTful, также могут задавать число записей на странице на этапе разработки. Если это значение не было задано разработчиком, используется значение по умолчанию.

1. Войдите в Central Management Console в качестве пользователя с правами администратора.
2. Щелкните **Серверы** и выберите элемент **Список серверов**.
3. Щелкните правой кнопкой мыши сервер контейнера веб-приложений, например, `MySIA.WebApplicationContainerServer` и выберите пункт **Свойства**.
Откроется вкладка **Свойства** для сервера контейнера веб-приложений.
4. В области **Веб-служба RESTful** введите размер страницы по умолчанию в текстовое поле **Число объектов по умолчанию на одной странице**.
5. Нажмите кнопку **Сохранить и закрыть**.

Настройка времени ожидания для маркера входа в систему

Срок действия маркера входа в систему истекает, если он не используется в течение заданного периода времени. Вы можете настроить время, в течение которого неиспользуемые маркеры входа в систему сохраняют свое действие.

Примечание:

По умолчанию маркер действует в течение одного часа.

1. Войдите в Central Management Console в качестве пользователя с правами администратора.
2. Щелкните **Серверы** и выберите элемент **Список серверов**.
3. Щелкните правой кнопкой мыши сервер контейнера веб-приложений, например, `MySIA.WebApplicationContainerServer` и выберите пункт **Свойства**.
Откроется вкладка **Свойства** для сервера контейнера веб-приложений.

4. В области **Веб-служба RESTful** введите срок действия маркера входа в систему в минутах в текстовое поле **Время ожидания токена сеанса Enterprise (в минутах)**.
5. Нажмите кнопку **Сохранить и закрыть**.

Настройка параметров пула сеансов

Применение пула сеансов позволяет оптимизировать производительность сервера. В нем кэшируются сеансы веб-службы RESTful, что позволяет повторно использовать их при отправке пользователем другого запроса, содержащего такой же маркер входа в систему в заголовке запроса HTTP. Размер пула определяет число одновременно кэшируемых сеансов, а время ожидания сеанса – продолжительность его хранения в кэше.

Эти значения доступны для настройки:

1. Войдите в Central Management Console в качестве пользователя с правами администратора.
2. Щелкните **Серверы** и выберите элемент **Список серверов**.
3. Щелкните правой кнопкой мыши сервер контейнера веб-приложений, например, `MySIA.WebApplicationContainerServer` и выберите пункт **Свойства**.
Откроется вкладка **Свойства** для сервера контейнера веб-приложений.
4. Введите максимальное число кэшируемых сеансов в текстовое поле **Размер пула сеанса** в области **Веб-служба RESTful**.
5. Введите время ожидания для пула сеансов в текстовое поле **Время ожидания пула сеанса (в минутах)** в области **Веб-служба RESTful**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. Щелкните правой кнопкой мыши сервер контейнера веб-приложений, например, `MySIA.WebApplicationContainerServer` и выберите пункт **Перезапуск сервера**.

Включение базовой аутентификации HTTP

Применение базовой аутентификации HTTP позволяет пользователям выполнять запросы веб-служб RESTful, не вводя маркер входа в систему. Если включена базовая аутентификация HTTP, пользователи вводят свои имя и пароль только при первом выполнении запроса веб-службы RESTful.

Примечание:

Если базовая аутентификация HTTP используется без протокола HTTPS, имена и пароли пользователей передаются в незащищенном виде.

При включении базовой аутентификации HTTP необходимо задать используемый по умолчанию тип аутентификации (SAP, Enterprise, LDAP или WinAD). После входа в систему пользователи могут устанавливать собственный тип базовой аутентификации HTTP.

Для входа в платформу BI с помощью базовой аутентификации HTTP используется лицензия. Если применяется кэширование пула сеансов, запрос использует лицензию, связанную с кэшированным сеансом. В противном случае лицензия используется в процессе выполнения запроса и освобождается после его завершения.

1. Войдите в Central Management Console в качестве пользователя с правами администратора.

2. Выберите **Сервер > Список серверов**.
3. Щелкните правой кнопкой мыши сервер контейнера веб-приложений, например, `MySIA.WebApplicationContainerServer` и выберите пункт **Свойства**.
Откроется вкладка **Свойства** для сервера контейнера веб-приложений.
4. В области «Веб-служба RESTful» выберите параметр **Включить базовую аутентификацию HTTP**.
5. (Необязательно) В списке **Схема аутентификации по умолчанию для базового HTTP** выберите используемый по умолчанию тип базовой аутентификации HTTP.
6. Нажмите кнопку **Сохранить и закрыть**.

Примечание:

После входа в систему с помощью базовой аутентификации HTTP пользователь может задать собственный тип аутентификации. Для этого в веб-браузере необходимо ввести `<authtype>\<username>` в подсказке для ввода имени пользователя и `<password>` в подсказке для ввода пароля.

Чтобы реализовать программный вход в систему с использованием базовой аутентификации HTTP, пользователю необходимо добавить атрибут `Authorization` в заголовок запроса HTTP и присвоить ему значение `Basic <authtype>\<username>:<password>`.

Параметры `<authtype>`, `<username>` и `<password>` заменяются типом аутентификации, именем пользователя и паролем соответственно. Значения этих параметров задаются в формате base64 в соответствии со спецификацией RFC 2617. При базовой аутентификации не поддерживаются имена пользователей, содержащие двоеточия :.

См. также

- [Настройка параметров пула сеансов](#)

12.1.8.2.3 Совместное использование ресурсов из различных источников

Настройка совместного использования ресурсов из нескольких источников

Параметр **Настройка совместного использования ресурсов из нескольких источников** позволяет добавить список имен доменов, благодаря которому пользователи могут получать данные из нескольких источников на веб-страницах, созданных на основе JavaScript. Это необходимо для обхода политики безопасности, используемой в языках JavaScript и Ajax для предотвращения междоменного доступа. В целях безопасности в список **Разрешить источники** в свойствах сервера WACS в СМС добавляются только те веб-сайты, к которым можно получить доступ.

Также доступен параметр **Максимальный срок существования (в минутах)**, служащий для настройки времени существования кэша в минутах, в течение которого браузеры могут хранить HTTP-запросы.

Примечание:

По умолчанию для разрешения доступа ко всем доменам используется * (звездочка).

1. Войдите в Central Management Console в качестве пользователя с правами администратора.
2. Выберите **Сервер > Список серверов**.
3. Щелкните правой кнопкой мыши сервер контейнера веб-приложений, например `MySIA.WebApplicationContainerServer`, и выберите пункт **Свойства**.
Откроется вкладка **Свойства** для сервера контейнера веб-приложений.
4. В области **Веб-служба RESTful** найдите текстовое поле **Настройка совместного использования ресурсов из нескольких источников** рядом со списком **Разрешить источники:** и замените * (звездочку) своим списком имен доменов, разделенных запятыми. Например: `http://origin1.server:8080, http://origin2.server:8080`
5. В текстовом поле **Максимальный срок существования (в минутах):** введите максимальное количество минут, в течение которых браузеры смогут хранить кэшированные HTTP-запросы.
6. Нажмите кнопку **Сохранить и закрыть**.

12.1.8.2.4 Аутентификация

Настройка web.xml для включения единого входа WinAD

Настройка веб-служб RESTful для распознавания единого входа Windows Active Directory предполагает внесение изменений в файл `web.xml`, расположенный на сервере платформы BI. Дополнительные сведения см. в разделе «Работа с SDK > Аутентификация > Получение маркера входа в систему с помощью учетной записи для единого входа Active Directory» в *руководстве для разработчиков веб-служб Business Intelligence Platform RESTful*.

Чтобы учетные данные для единого входа WinAD на клиентском компьютере распознавались сервером платформы BI, необходимо раскомментировать раздел `Kerberos Proxy filter` в файле `web.xml` и обновить значения `idm.realm`, `idm.princ` и `idm.keytab`, отражающие используемую среду Active Directory.

1. Поместите файл конфигурации `web.xml` в папку `<boe root>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\RestWebService\biprws\WEB-INF\`. Ниже приведен пример пути к файлу.

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\RestWebService\biprws\WEB-INF\web.xml
```

2. В файле `web.xml` раскомментируйте раздел `Kerberos Proxy Filter`, добавив закрывающий тег комментария `-->` перед тегом `<filter>`, и удалите закрывающий тег комментария `-->`.

```
<!-- Kerberos Proxy Filter
- Uncomment this filter and the corresponding filter-mapping to enable Kerberos SSO
- for Windows AD (secWinAD) authentication.
- The following options must be specified (the rest are optional):
-   idm.realm
-   idm.princ
-   idm.keytab (unless using password, see below)
-->

<filter>
  <filter-name>WrappedResponseAuthFilter</filter-name>
  .
  .
</filter>

<filter-mapping>
  <filter-name>WrappedResponseAuthFilter</filter-name>
```

```
<url-pattern>/logon/adsso</url-pattern>
</filter-mapping>

</web-app>
```

3. Обновите значение `<param-value>` для каждого параметра `idm.realm`, `idm.princ` и `idm.keytab`, изменив его на значение, используемое в среде Active Directory.

```
<init-param>
  <param-name>idm.realm</param-name>
  <param-value>ADDOM.COM</param-value>
  <description>
    Required: Set this value to the Kerberos realm to use.
  </description>
</init-param>

<init-param>
  <param-name>idm.princ</param-name>
  <param-value>BOE120SIAVMBOESRVR/bo.service.addom.com</param-value>

  <description>
    Set this value to the Kerberos service principal to use.
    This will be a name of the form HTTP/fully-qualified-host.
    For example, HTTP/example.vintela.com
    If not set, defaults to the server's hostname and the
    idm.realm property above.
  </description>
</init-param>

<init-param>
  <param-name>idm.kdc</param-name>
  <param-value></param-value>
  <description>
    The KDC against which secondary credentials must be validated.
    This can be used for BASIC fallback or credential delegation.
    By default the KDC will be discovered automatically and this
    parameter must only be used if automatic discovery fails, or
    if a different KDC to the one discovered must automatically be used.
  </description>
</init-param>

<init-param>
  <param-name>idm.keytab</param-name>
  <param-value>C:/winnt/BOE120SIAVMBOESRVR.keytab</param-value>
  <description>
    The file containing the keytab that Kerberos will use for
    user-to-service authentication. If unspecified, SSO will default
    to using an in-memory keytab with a password specified in the
    com.wedgetail.idm.sso.password environment variable.
  </description>
</init-param>
```

Примечание:

Значение `idm.keytab` указывает путь к файлу на сервере платформы BI. Значения для `idm.realm` и `idm.prince` можно просмотреть в Central Management Console. На вкладке **Аутентификация** в СМС дважды щелкните пункт **Windows AD**. Значение для `idm.realm` задается с помощью параметра «Default AD Domain» в разделе «Сводка конфигурации AD». Значение для `idm.prince` задается с помощью параметра «Имя администратора доступа к службе» в разделе «Параметры аутентификации».

4. Перезапустите службу WACS, чтобы изменения в файле `web.xml` вступили в силу.
5. С помощью клиентского компьютера проверьте возможность извлечения маркера входа в систему AD с использованием API-интерфейса веб-служб RESTful (например, `http://<boe host>:6405/biprws/logon/adsso`).
6. Протестируйте маркер с помощью запроса GET, содержащего строку `X-SAP-LogonToken` в заголовке, и API-интерфейса `/infostore`.

Включение и настройка доверительной аутентификации

Доверительная аутентификация включается и настраивается через Central Management Console (СМС) в следующих разделах: **Аутентификация > Предприятие**, где включается доверительная аутентификация и генерируется файл общего секретного ключа; **Пользователи и группы > Список пользователей**, где создается учетная запись для доверенного пользователя; **Серверы > Список серверов > WACS > Свойства**, где выбирается параметр «Метод извлечения» для запросов маркера входа в систему API /logon/trusted.

1. Войдите в Central Management Console в качестве пользователя с правами администратора.
2. Перейдите к разделу **Аутентификация > Предприятие**, затем щелкните **Доверительная аутентификация включена**.
3. Щелкните **Новый общий секретный ключ**, а затем выберите **Загрузить общий секретный ключ**.
4. Щелкните **Сохранить** и поместите файл `TrustedPrincipal.conf` в папку по умолчанию: `<EnterpriseDir>\<platform>`.

Пример расположения:

```
"C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjectsEnterprise XI 4.0\win64_x64\"
```

Примечание:

- Можно изменить расположение файла общего секретного ключа `TrustedPrincipal.conf` по умолчанию, добавив запись командной строки в СМС в разделе **Серверы > Список серверов > WACS > Свойства > Параметры командной строки**, а затем перезапустив службу WACS. Например, запись командной строки, включающая `-Dbobj.trustedauth.home=` и папку `SharedSecrets`, помещенную в корневой каталог диска `C:\` сервера платформы BI, будет выглядеть следующим образом:

```
"-Dbobj.trustedauth.home=C:\SharedSecrets"
```

- Можно оставить для параметра **Период действия общего секретного ключа (в днях)** значение по умолчанию, равное нулю (0); в этом случае срок действия ключа не будет истекать. Для параметра **Время ожидания доверительного входа истекает через N миллисекунд (0 - без ограничения)** можно также оставить значение по умолчанию, равное нулю (0), чтобы запросы на вход в систему не имели ограничений по времени.
5. Щелкните **Обновить**, чтобы сохранить изменения.
 6. Добавьте новое имя пользователя и пароль, например `bob` и `Passw0rd`, в разделе **Пользователи и группы > Список пользователей** с помощью команд **Управление > Создать > Создать пользователя**. Снимите флажок **Пользователю следует изменить пароль при следующем входе в систему**, а затем щелкните **Создать и закрыть**.

Примечание:

Нового пользователя также можно создать, щелкнув значок **Создать нового пользователя** или щелкнув правой кнопкой пустое пространство в окне со списком имен пользователей и выбрав пункты **Создать > Создать пользователя**.

7. Перейдите к разделу **Серверы > Корневые службы > WACS > Свойства**, прокрутите экран вниз до раздела «Конфигурация с доверительной аутентификацией» и в меню «Метод извлечения» выберите **HTTP_HEADER, QUERY_STRING** или **COOKIE**.

Примечание:

«Параметр имени пользователя» можно изменить со значения по умолчанию X-SAP-TRUSTED-USER на любое другое более удобное значение (например, UserName, kassir или medsestra), которое будут использовать разработчики веб-служб RESTful.

8. Перезапустите службу, щелкнув правой кнопкой имя сервера WACS, например MySIA.WebApplicationContainerServer, и выбрав команду **Перезапустить сервер**.

Примечание:

Для последующего изменения параметра «Метод извлечения», как показано в шаге 7, перезапуск службы WACS не потребуется.

9. Проверьте возможность извлечения маркера входа в систему с использованием API-интерфейса .../biprsw/logon/trusted/ путем отправки запроса GET с меткой заголовка по умолчанию X-SAP-TRUSTED-USER и именем пользователя, созданным в шаге 5.

Настройка параметра командной строки для перемещения файла конфигурации общего секретного ключа TrustedPrincipal.conf

Веб-службы RESTful содержат параметр командной строки для выбора другого расположения для файла доверительной аутентификации TrustedPrincipal.conf.

Файл TrustedPrincipal.conf содержит общий секретный ключ, генерируемый через СМС:

Аутентификация > Предприятие при нажатии кнопки **Новый общий секретный ключ** и сохранении файла (для этого нужно щелкнуть **Загрузить общий секретный ключ** и сохранить файл в расположении по умолчанию).

Обновите командную строку сервера контейнера веб-приложений, добавив пользовательский путь к файлу TrustedPrincipal.conf, как показано ниже.

1. Войдите в Central Management Console в качестве пользователя с правами администратора.
2. Щелкните **Серверы** и выберите элемент **Список серверов**.
3. Щелкните службу WACS, например MySIA.WebApplicationContainerServer, правой кнопкой мыши и выберите пункт **Свойства**.

Откроется вкладка **Свойства** для сервера контейнера веб-приложений.

4. В области «Параметры командной строки» введите путь к каталогу, в котором будет находиться файл TrustedPrincipal.conf.

Эту строку необходимо заключить в двойные кавычки, как показано в следующем примере.

```
"-Dbobj.trustedauth.home=C:\SharedSecrets"
```

Примечание:

Расположение по умолчанию для файла TrustedPrincipal.conf: <EnterpriseDir>\<platform>. Пример расположения:

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64
"
```

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

6. Перезапустите службу, щелкнув правой кнопкой имя сервера WACS, например `MySIA.WebApplicationContainerServer`, и выбрав команду **Перезапустить сервер**.

12.1.9 Сервер контейнера веб-приложений (WACS) и ваша IT-среда

В этом разделе содержится информация о настройках WACS в сложной среде.

12.1.9.1 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.

12.1.9.2 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](#)

12.1.9.3 Использование WACS с обратным прокси

WACS можно использовать в развертывании с прямым или обратным прокси-сервером. Использовать WACS в качестве прокси-сервера нельзя.

12.1.9.3.1 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 брандмауэра (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**.

12.1.9.3.2 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.

12.1.9.4 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](#)

12.1.9.5 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 разделе «Настройка HTTP через прокси» на панели «Служба контейнеров веб-приложений» снимите флажок **Привязать ко всем IP-адресам** и введите IP-адрес, к которому требуется привязать WACS.
4. В секции «Конфигурация HTTP» снимите флажок **Привязать ко всем IP-адресам** и введите адрес или имя хоста, к которому требуется привязать WACS.
5. В области «Общие параметры» снимите флажок **Назначать автоматически** и укажите имя хоста или IP-адрес сетевого адаптера, используемого для обмена данными между WACS и другими серверами платформы SAP BusinessObjects Business Intelligence в этом развертывании.
6. Нажмите кнопку **Сохранить и закрыть**.
7. Перезапустите WACS.

12.1.10 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 Central Management Console (CMC), 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 CMC.

Если веб-приложение имеет свойства, доступные для настройки в CMC, 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 CMC, 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 CMC, 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](#)

12.1.11 Устранение неполадок

12.1.11.1 Настройка трассировки на WACS

Чтобы настроить трассировку для WACS, см. раздел [Ведение журнала трассировок компонентов](#)

12.1.11.2 Для просмотра серверных показателей

Показатели сервера для WACS можно просмотреть, используя Central Management Console (CMC).

1. Перейдите в область управления «Серверы» в CMC.
2. Щелкните сервер WACS правой кнопкой мыши и выберите команду **Показатели**.

См. также

- [Показатели сервера контейнера веб-приложений](#)

12.1.11.3 Просмотр состояния сервера WACS

Для просмотра состояния сервера WACS перейдите в область «Серверы» CMC. В **Списке серверов** имеется столбец **Состояние**, в котором отображается состояние каждого сервера в списке.

WACS имеет серверное состояние «Запущено с ошибками». Это состояние означает, что WACS запущен, однако наблюдается одно или несколько из перечисленных ошибочных состояний:

- Неверная настройка модуля подключения HTTP, HTTP через прокси-сервер или HTTPS.
- Неверное выполнение службы, выполняемой на сервере WACS, например службы протокола трассировки.
- Сбой развертывания веб-приложения на сервере WACS.

Сведения о сбое служб см. также на странице «Свойства» сервера WACS.

12.1.11.4 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 имеется несколько серверов WACS, войдите в CMC и проверьте показатели

"Список выполняемых соединителей WACS" и "Сбой соединителей WACS". Если в списке выполняемых соединителей WACS отсутствуют соединители HTTP, HTTP через прокси или HTTPS, эти соединители не удастся запустить из-за конфликта портов.

Если развертывание содержит только один сервер WACS или если консоль CMC недоступна ни с одного WACS, воспользуйтесь такой служебной программой, как netstat, чтобы определить, не занят ли порт WACS другим приложением.

12.1.11.4.1 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».

12.1.11.4.2 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**.

12.1.11.5 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».

12.1.11.6 Изменение количества параллельных 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 параллельных HTTP-запросов. Хотя увеличение количества параллельных 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 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 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**.

12.1.11.7 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.

12.1.11.8 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 СМС.
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 **Сохранить и закрыть**.

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.

12.1.12 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 системы

13.1 Обзор резервного копирования и восстановления

В этой главе описывается, как выполнить резервное копирование платформы Business Intelligence и восстановить систему после аппаратного или программного сбоя, а также после потери данных. Для выполнения плана резервного копирования и восстановления требуется специалист по SAP BusinessObjects, системный администратор и администратор баз данных.

См. также

- [Резервное копирование всей системы](#)
- [Резервное копирование платформы BI](#)
- [Резервное копирование параметров сервера с помощью CCM в Windows](#)
- [Резервное копирование параметров сервера в ОС Unix](#)
- [Обзор копирования системы](#)

13.2 Терминология

Термин	Определение
Тиражирование данных	Тиражирование данных - это процесс создания одной или нескольких копий данных. Обновление копий происходит в реальном времени; например, при использовании отображенных дисков. Это обеспечивает защиту данных от повреждения в реальном времени. Тем не менее, поскольку содержимое дисков непрерывно обновляется, восстановить более раннее состояние поврежденных или случайно удаленных данных нельзя.

Термин	Определение
Управление версиями	<p>Средство создания версий формирует несколько версий определенного файла или файлов в системе. В данном случае можно вернуть систему в более раннее состояние.</p> <p>Все версии данных обычно сохраняются в одной хост-системе. При возникновении проблем в данной системе возникает риск потери как текущей, так и предыдущих версий. Аналогично, функции отмены удаления сохраняют копии удаленных файлов для последующего восстановления, но данные файлы также обычно сохраняются в той же хост-системе, что и исходные данные. В этом случае не обеспечивается защита от физического повреждения данных, например, в результате сбоя диска.</p>
Аппаратное резервное копирование системы	<p>Аппаратное резервное копирование системы - это резервное копирование целой файловой системы, включая операционную систему. Аппаратное резервное копирование системы предназначено для восстановления этой системы на аппаратные средства без установленных программных средств и операционной системы.</p> <p>При использовании аппаратного резервного копирования системы в случае сбоя вся файловая система (включая ОС) восстанавливается на идентичном аппаратном обеспечении, или, если средства восстановления поддерживают аппаратно-независимое восстановление, - на любом аппаратном обеспечении.</p>
Сравнение аппаратного резервного копирования системы с резервным копированием приложения	<p>Аппаратное резервное копирование системы создает копию всей файловой системы, включая операционную систему. Аппаратное резервное копирование позволяет восстановить систему в целом до более ранней версии.</p> <p>При резервном копировании приложения создаются резервные копии файлов, относящихся к отдельным приложениям.</p> <p>Платформой BI поддерживается аппаратное резервное копирование системы и не поддерживается резервное копирование приложения.</p> <p>При использовании аппаратного резервного копирования системы в случае сбоя вся файловая система (включая ОС) восстанавливается на идентичном аппаратном обеспечении, или, если средства восстановления поддерживают аппаратно-независимое восстановление, - на любом аппаратном обеспечении.</p> <p>Полное резервная копия системы платформы BI называется набором резервного копирования.</p>

Термин	Определение
Набор резервного копирования	<p>Набор резервного копирования включает следующие отдельные резервные копии, созданные одновременно:</p> <ul style="list-style-type: none"> Резервная копия базы данных системы CMS. Аппаратная резервная копия всей файловой системы, включая операционную систему, для всех компьютеров в развертывании платформы BI. Резервные копии хранилищ серверов репозитория входных и выходных файлов FRS (если они не входят в состав файловой системы платформы BI). Резервные копии компонентов веб-уровня (если они не входят в состав файловой системы платформы BI). Резервная копия базы данных аудита.
Сравнение "холодного" и оперативного резервного копирования	<p>"Холодное" резервное копирование выполняется в то время, когда система остановлена и недоступна пользователям. Оперативное резервное копирование выполняется при работающей и доступной для пользователей системе и меняющихся данных. Также при выполнении оперативного резервного копирования, в отличие от "холодного" резервного копирования, важен порядок выполнения действий.</p> <p>Платформой BI поддерживается как "холодное", так и оперативное резервное копирование.</p> <p>Оперативное резервное копирование называется также «резервированием онлайн».</p>

13.3 Случаи использования резервного копирования и восстановления

В следующей таблице описаны цели, достигаемые при наличии определенных ресурсов, и наиболее подходящее решение для резервного копирования в каждом случае.

цель	Необходимые ресурсы	Решение
<p>Цель: восстановление системы</p> <ol style="list-style-type: none"> 1. Система платформы BI повреждена. Следовательно, необходимо восстановить ее рабочее состояние на момент последнего резервного копирования. 2. Поврежден компьютер, на котором размещается платформа BI. Необходимо заменить его на новый компьютер. 	<ul style="list-style-type: none"> • Целевая система с аппаратными средствами, идентичными средствам исходной системы И • Резервные копии исходной системы 	<p>Используйте рабочий процесс для резервного копирования и восстановления системы, описанный в этом руководстве. См. процедуру Резервное копирование всей системы. Воссоздайте целевую систему из резервных копий исходной системы.</p>
<p>Цель: восстановление объектов</p> <p>Требуется восстановление документа или другого объекта, который был случайно удален.</p>	<ul style="list-style-type: none"> • Резервные копии баз данных и файлов исходной системы И • Подробные сведения о системе, описанные в Экспорт из исходной системы 	<p>Используя резервные копии, создайте копию системы на другом компьютере при помощи рабочего процесса копирования системы, описанного в главе «Копирование развертывания платформы BI». Затем при помощи средств Promotion Management перенесите случайно удаленные объекты из этой новой системы. См. рабочий процесс копирования системы начиная с Планирование копирования системы и следуйте инструкциям, указанным в остальной части главы.</p> <p>Примечание: Вы можете создать целевую систему на компьютере с существующим развертыванием BI с тем же уровнем выпуска, пакета поддержки и исправлений или на "чистом" компьютере без установленной платформы BI.</p>
<p>Цель: восстановление объектов 2</p> <p>Требуется восстановление документа или другого объекта, который был случайно удален.</p>	<p>Система, в которой используется управление версиями Promotion Management</p>	<p>Воспользуйтесь приложением Promotion Management для восстановления более ранней версии документа. Подробные сведения см. в соответствующей теме для Promotion Management.</p>

цель	Необходимые ресурсы	Решение
<p>Цель: резервное копирование объектов</p> <p>Требуется создать резервные копии небольшого количества объектов (например, документов, папок, пользователей).</p>	<p>Система, в которой используется управление версиями Promotion Management</p>	<p>Используйте приложение Promotion Management для резервного копирования содержимого BI и последующего экспорта содержимого в файлы архива Business Intelligence (LCMBIAR). Если содержимое повреждено или отсутствует, его можно восстановить позднее, не восстанавливая всю систему.</p> <p>Подробные сведения см. в соответствующей теме для Promotion Management.</p>

См. также

- [Резервные копии](#)
- [Планирование копирования системы](#)
- [Обзор средства управления повышением](#)

13.4 Резервные копии

План резервного копирования и восстановления состоит из шагов, предпринимаемых при системном сбое в результате стихийного бедствия или непредвиденного сбоя. Этот план направлен на минимизацию влияния аварии на ежедневные операции, что позволит сохранить или быстро возобновить выполнение критически важных функций.

Существует три подхода к резервному копированию развертывания платформы BI.

- Резервное копирование всей системы с возможностью ее последующего восстановления. В этом случае частичное восстановление системы невозможно. Чтобы выполнить реконструкцию платформы BI вместо ее восстановления из резервной копии, см. соответствующую тему с описанием копирования системы.
- Резервное копирование параметров сервера, что позволяет восстановить конфигурацию сервера (прочие объекты не восстанавливаются) и, тем самым, сохранить текущее состояние содержимого системы BI.
- Резервное копирование содержимого BI (например, документов), что позволяет выборочно восстанавливать нужные объекты содержимого BI.

Дополнительные сведения обо всех трех типах резервного копирования см. в соответствующих темах.

Совет:

- Во избежание утери данных выполняйте резервное копирование регулярно.
- Можно создать резервную копию системы платформы BI и затем восстановить ее на том же или другом хост-компьютере для создания копии системы.

См. также

- [Резервное копирование всей системы](#)
- [Резервное копирование настроек сервера](#)
- [Резервное копирование платформы BI](#)
- [Обзор копирования системы](#)

13.4.1 Резервное копирование всей системы

Создавайте резервную копию всей системы платформы BI, выполняя "холодное" или оперативное резервное копирование, в результате чего будет создан набор резервных копий. Для большего выбора вариантов восстановления рекомендуется хранить несколько наборов резервных копий по состоянию на разные моменты времени. Выполняйте резервное копирование системы регулярно в соответствии с потребностями бизнеса организации.

Поддерживается как "холодное" (при остановленной системе платформы BI), так и оперативное резервное копирование. В процессе оперативного резервного копирования система не отключается и остается доступной пользователям. Это позволяет избежать перерывов в работе системы.

Примечание:

- Рекомендуется сохранять журнал транзакций в файловой системе, отличной от системы сервера основной БД, регулярно создавать резервные копии журнала и включать его в состав набора резервного копирования.
- Если выполняется резервное копирование данных аудита, необходимо включить в набор резервных копий журнал транзакций для базы данных аудита. Включать в резервную копию временные файлы аудита не требуется.

13.4.1.1 Оперативное резервное копирование

Функция оперативного резервного копирования позволяет выполнять копирование платформы Business Intelligence, не прерывая работу системы и доступ к ней пользователей. Если деятельность организации необходимо продолжать даже во время резервного копирования системы, необходимо включить и настроить оперативное резервное копирование в Central Management Console.

Параметр **Максимальная продолжительность оперативного резервного копирования** задает ожидаемое максимальное время выполнения резервного копирования (с начала резервного копирования CMS до окончания резервного копирования FRS). Если указать слишком короткую продолжительность, файлы могут быть удалены до того, как система резервного копирования копирует их. Чтобы этого избежать, рекомендуется зависить ожидаемое время. Следует тщательно оценивать влияние величины этого параметра на производительность системы. При настройке слишком высокого значения возможно незначительное увеличение размера хранилища файлов FRS.

Примечание:

Оперативное резервное копирование включено, если на центральной консоли управления установлен флажок **Включить оперативное резервное копирование**; параметр **Максимальная продолжительность оперативного резервного копирования** не влияет на включение функции оперативного резервного копирования.

Самый простой вариант использования – восстановление состояния системы на заданный момент времени. Например, если резервное копирование системы выполняется ежедневно в 03:00, вы сможете легко восстановить состояние CMS на момент запуска операции резервного копирования (03:00 в выбранный вами день). Если включено ведение журнала транзакций, то после сбоя базы данных CMS или базы данных аудита можно будет восстановить состояние системы, предшествующее сбою.

Для обеспечения максимальной степени безопасности сохраняйте записи журнала транзакций не в том месте, где хранятся записи резервной копии основной базы данных. Это обеспечит в случае сбоя базы данных возможность ее восстановления в состояние, предшествующее сбою.

Примечание:

- В связи с ограничениями на размер журнала транзакций в предыдущих версиях IBM DB2, задачи, связанные с журналами оперативного резервного копирования и транзакций, поддерживаются только в том случае, если база данных системы CMS размещается на сервере базы данных DB2 версии 9.5 с пакетом исправлений 5 или более поздней (для семейства 9.5) и 9.7 с пакетом исправлений 1 или более поздней (для семейства 9.7).
- Рекомендуется сохранять журнал транзакций в файловой системе, отличной от системы сервера основной БД, регулярно создавать резервные копии журнала и включать его в состав набора резервного копирования.

Клиенты Crystal Reports 2011 Designer, Web Intelligence Rich Client и Universe Design Tool версии ниже 4.0 FP3 и разработанные пользователем "толстые" клиентские приложения, для компиляции которых использовались пакеты SDK версии ниже 4.0 FP3, могут не поддерживать изменение файлов в процессе оперативного резервного копирования. Изменение содержимого BI такими клиентами в процессе резервного копирования может привести к нарушению качества измененных данных. Вы можете запретить клиентским приложениям изменение документов, чтобы обеспечить согласованность копируемых данных. Обновите клиентские приложения до версии 4.0 FP3, если это возможно. Если такой возможности нет, рассмотрите доступные способы исправления этой ситуации. Например, вместо изменения можно порекомендовать пользователям таких клиентских приложений удалить существующие объекты и сохранить новые версии.

13.4.1.1.1 Включение оперативного резервного копирования

1. Откройте Central Management Console (CMC).

2. В области «Управление» откройте страницу **Параметры**.
3. В разделе «Оперативное резервное копирование» выберите **Включить оперативное резервное копирование**.
4. Укажите максимальную продолжительность резервного копирования в минутах в поле **Максимальная продолжительность оперативного резервного копирования (минуты)**. Не забудьте указать время, необходимое для резервного копирования базы данных CMS и файловой системы основного компьютера платформы BI.

Примечание:

Превышение фактической продолжительности резервного копирования над введенным значением может повлечь получение неполноценной резервной копии данных. Чтобы этого избежать, рекомендуется зависить ожидаемое время.

5. Чтобы разрешить устаревшим (ниже версии 4.0 FP3) клиентам Web Intelligence Rich Client, Crystal Reports Designer, а также разработанным пользователями с помощью пакетов SDK "толстым" клиентам изменять документы в системе, установите флажок **Включить поддержку устаревших приложений (ограничения резервного копирования)**.

Если таким клиентам разрешено изменение документов в процессе резервного копирования, это может привести к возникновению несогласованностей в документах, изменяемых во время резервного копирования. Для получения сведений об ограничениях при резервном копировании см. ссылку, относящуюся к оперативному резервному копированию.

6. Нажмите **Обновить**.

Оперативное резервное копирование включено.

После включения поддержки оперативного резервного копирования появляется возможность использовать средства резервного копирования поставщика базы данных или файловой системы при выполнении резервного копирования.

См. также

- [Оперативное резервное копирование](#)
- [Выполнение оперативного и "холодного" резервного копирования системы](#)

13.4.1.2 Выполнение оперативного и "холодного" резервного копирования системы

Перед выполнением оперативного резервного копирования ознакомьтесь со списком предварительных условий и с другими дополнительными сведениями в связанной теме об оперативном резервном копировании. При выполнении "холодного" резервного копирования необходимо остановить все узлы в развертывании платформы BI.

Предупреждение:

При выполнении резервного копирования без включения "горячего" резервного копирования и без остановки всех узлов могут появиться противоречия данных между базой данных CMS и хранилищем данных FRS.

Примечание:

При выполнении оперативного резервного копирования важен запуск процедур в описанном порядке. При выполнении "холодного" резервного копирования последовательность процедур не имеет значения. В любом случае завершение одного шага резервного копирования перед запуском следующего шага необязательно.

1. Используйте средства, предоставленные поставщиком базы данных, для резервного копирования системной базы данных центрального сервера управления (CMS).

Примечание:

При оперативном резервном копировании соответствующие инструменты поставщика БД необходимо использовать в интерактивном атомарном режиме.

2. Используйте средства, предоставленные поставщиком БД, в интерактивном атомарном режиме для резервного копирования базы данных аудита платформы BI.
3. Создайте резервную копию всей файловой системы, включая операционную систему, для всех компьютеров в развертывании платформы BI.
 - a. Если в резервную копию платформы BI не включены хранилища серверов репозитория входных и выходных файлов (размещаются на отдельных хостах), отдельно создайте их копии с использованием средств резервного копирования файлов.
 - b. Если компоненты веб-уровня не включены в платформу BI (отдельные хосты), создайте их резервную копию с помощью инструментов для резервного копирования файлов.

Для оперативного резервного копирования по возможности используйте средства атомарного резервного копирования файлов.

При выполнении "холодного" резервного копирования дождитесь завершения всех операций копирования и запустите узлы платформы BI.

См. также

- [Оперативное резервное копирование](#)

13.4.2 Резервное копирование настроек сервера

Чтобы защитить систему от неправильно настроенных параметров сервера, регулярно создавайте резервные копии параметров сервера в файле BIAR. Наличие доступных резервных копий сервера позволяет восстанавливать параметры без необходимости восстановления системной базы данных центрального сервера управления, репозитория файлов или содержимого Business Intelligence.

Резервное копирование параметров сервера необходимо выполнять каждый раз при внесении изменений в конфигурацию 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 или устройстве хранения данных.

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 Enterprise XI 4.0\win64_x64\scripts`.

В Unix скрипт `backupcluster.sh` расположен в каталоге `/ <КАТАЛОГ_УСТАНОВКИ>/sap_bobj/enterprise_xi40/<platform64>/scripts`.

См. также

- [Настройка протокола SSL](#)

13.4.2.1 Резервное копирование параметров сервера с помощью CCM в Windows

Эта процедура выполняет резервное копирование параметров сервера для всего кластера. Нельзя выполнять резервное копирование параметров для отдельных серверов.

Примечание:

Если используется временный сервер CMS, то CCM необходимо использовать на компьютере, на котором установлены локальные двоичные файлы 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 соединении с базой данных.
Чтобы минимизировать риск доступа пользователей к системе во время восстановления, укажите номер порта, отличный от номеров порта, используемых существующими CMS.
- 5. Введите ключ кластера и нажмите кнопку **Далее**.
- 6. 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.
- 7. Укажите расположение и имя файла BIAR, для которого нужно выполнить резервное копирование параметров конфигурации сервера, а затем щелкните **Далее**, чтобы продолжить.
Страница «Подтверждение» отображает предоставленную информацию.
- 8. Убедитесь, что информация, отображенная на странице «Подтверждение» верна, а затем нажмите кнопку **Готово**, чтобы продолжить.
ССМ 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.
- 9. Если во время операции резервного копирования произошел сбой, проверьте файл журнала для установления причины.
- 10. Нажмите кнопку **ОК**, чтобы закрыть мастер.

13.4.2.2 Резервное копирование параметров сервера в ОС Unix

В Unix используйте скрипт `serverconfig.sh` для резервного копирования параметров сервера развертывания в файл BIAR.

1. Выберите пункт **5 – резервное копирование сервера** и нажмите клавишу **ВВОД**.
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 **ВВОД**.
 - Чтобы выполнить резервное копирование параметров сервера из неактивной системы или восстановить параметры сервера, выберите элемент **временный** и нажмите клавишу **ВВОД**.
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 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 **ВВОД**.
5. При выводе соответствующего запроса укажите местоположение и имя файла BIAR, в который требуется скопировать конфигурацию сервера, и нажмите клавишу **ВВОД**.
Предоставленные сведения будут отображены на странице сводки.
6. Проверьте правильность отображаемой информации и нажмите клавишу **ВВОД**, 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. Отображается имя файла журнала и путь к нему.
7. Если во время операции резервного копирования произошел сбой, проверьте файл журнала для установления причины.

13.4.2.3 Резервное копирование параметров серверов с использованием скрипта

Можно выполнить резервное копирование параметров сервера своего развертывания путем выполнения файла `BackupCluster.bat` в ОС Windows или скрипта `BackupCluster.sh` в ОС Unix.

В Windows файл `BackupCluster.bat` расположен в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.

В Unix файл `backupcluster.sh` расположен в каталоге `/<КАТАЛОГ_УСТАНОВКИ>/sap_bobj/enterprise_xi40/<platform64>/scripts`.

См. также

- [Скрипты BackupCluster и RestoreCluster](#)

13.4.3 Резервное копирование платформы BI

Рекомендуется при помощи консоли управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence 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.

Дополнительные сведения об использовании консоли управления жизненным циклом см. в *руководстве пользователя консоли управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence*.

Если используется вспомогательная версия консоли управления жизненным циклом, см. главу о резервном копировании файлов вспомогательных версий в *руководстве пользователя консоли управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence*.

13.5 Восстановление системы

Если система повреждена, вы можете восстановить всю систему, при этом будет восстановлена и платформа BI. В зависимости от состояния системы полное восстановление может не требоваться. Если система работает нормально, но было утрачено или повреждено содержимое, можно восстановить только содержимое Business Intelligence (BI). Если содержимое BI не повреждено, но нарушена конфигурация серверов платформы, можно восстановить только параметры сервера.

Процедуры восстановления из оперативной и холодной резервной копии одинаковы.

См. также

- [Восстановление всей системы](#)
- [Восстановление настроек сервера](#)
- [Восстановление содержимого BI](#)

13.5.1 Восстановление всей системы

При восстановлении всей системы кластер платформы BI также восстанавливается. В зависимости от того, какой компонент системы отказал, по-прежнему могут присутствовать возможности для частичного восстановления системы.

При сбое или потере одного из следующих компонентов необходимо восстановить всю систему:

- База данных CMS

Примечание:

Если остальная платформа BI работает нормально, но произошел сбой базы данных CMS, можно восстановить базу данных CMS без восстановления всей системы.

- Хранилище сервера репозитория файлов (FRS)
- Файловая система компьютера

Примечание:

Для полного восстановления системы не требуется установленная в целевой системе платформа Business Intelligence.

Если повреждена или потеряна только база данных аудита, вы можете восстановить базу данных аудита без восстановления всей системы.

Если повреждена или потеряна база данных веб-уровня, вы можете восстановить содержимое веб-уровня без восстановления всей системы.

См. также

- [Восстановление всей системы](#)
- [Восстановление только базы данных аудита](#)
- [Восстановление содержимого веб-уровня](#)
- [Восстановление только базы данных CMS](#)

13.5.1.1 Восстановление всей системы

Перед восстановлением системы необходимо использовать Central Configuration Manager (CCM), чтобы остановить все узлы в развертывании платформы BI, после чего также требуется выбрать время для восстановления системы.

Примечание:

Если вы хотите восстановить текущее состояние системы, сначала создайте резервную копию системы.

1. Найдите следующие файлы резервной копии:

- Резервная копия базы данных CMS
- Резервные копии хранилища серверов репозитория входящих и исходящих файлов
- Резервные копии файловой системы для каждого хоста в кластере платформы BI

Примечание:

Проверьте правильность резервных копий и убедитесь, что все перечисленные выше файлы принадлежат одному набору резервных копий. Если набор резервных копий был получен при оперативном резервном копировании, следует убедиться, что метка времени базы данных CMS относится к более раннему времени, чем соответствующие метки времени файлового хранилища FRS, веб-уровня и файловой системы компьютера-хоста. Все эти файлы требуются даже в том случае, когда произошел сбой одного компонента.

2. С помощью средств восстановления файлов восстановите файловую систему на всех хостах кластера платформы BI.
3. С помощью средств восстановления файлов восстановите хранилища серверов репозитория входящих и исходящих файлов.
4. С помощью средств управления базой данных восстановите БД CMS.

5. Если после создания резервной копии был изменен пароль базы данных CMS, с помощью CCM обновите его на всех узлах и хостах платформы BI.
6. Если используется функция аудита:
 - a. Найдите последние резервные копии и журналы транзакций для базы данных аудита.
 - b. С помощью средств управления базой данных восстановите базу данных аудита.
 - c. Отмените откат базы данных аудита, для чего воспроизведите журнал транзакций.
7. Восстановите поисковый индекс одним из следующих способов:
 - Выполните инструкции по восстановлению поискового индекса с помощью скрипта, приведенные в разделе [Запуск скрипта восстановления поискового индекса](#). Этот способ позволяет быстро восстановить весь индекс.
 - Если требуется перестроить поисковый индекс без использования скрипта восстановления, перезапустите узлы платформы BI с помощью CCM. Эта процедура проще, однако во время перестроения индекса поиск по данным платформы будет частично недоступен.
8. Запустите систему и запишите время, которое будет использоваться в требуемых после процедуры шагах.
9. Убедитесь, что компоненты системы функционируют правильно, и выполните проверку ее работоспособности.

После проверки системы выполните следующие действия:

- Запустите средство Repository Diagnostic Tool, чтобы удалить все неиспользуемые временные файлы и проверить целостность репозитория. См. раздел "Repository Diagnostic Tool" этого руководства.
- Если скрипт восстановления не использовался, выполните перестроение поискового индекса.
- Для всех заданий публикации, выполняемых во время резервного копирования системы, отображается состояние сбоя. Не запускайте такие экземпляры повторно. Вместо них следует запустить новые задания публикации.
- Если была восстановлена база данных аудита, необходимо выполнить SQL-запрос, удаляющий все события, которые произошли в период между сбоем базы данных и ее перезапуском (время, записанное на шаге 8). Например: `delete from [ИМЯ_БД].ADS_EVENT where Start_Time > '[время_сбоя_БД]' and Start_Time < '[время_восстановления_БД]'`

См. также

- [Индексация содержимого в репозитории CMS](#)

13.5.1.2 Восстановление только базы данных аудита

Перед восстановлением системы воспользуйтесь Central Configuration Manager (CCM), чтобы остановить все узлы в развертывании платформы BI. Также необходимо выбрать момент времени, по состоянию на который будет восстановлена система.

Примечание:

Выполните эту операцию, только если вы уверены в том, что база данных аудита является единственным нарушенным компонентом платформы BI. Если затронуты дополнительные компоненты, необходимо выполнить полное восстановление системы.

1. Найдите последние резервные копии и журналы транзакций для базы данных аудита.
2. С помощью средств управления базой данных восстановите базу данных аудита.
3. Отмените откат базы данных аудита, для чего воспроизведите журнал транзакций.

См. также

- [Восстановление всей системы](#)

13.5.1.3 Восстановление содержимого веб-уровня

Перед восстановлением содержимого веб-уровня необходимо остановить все узлы в развертывании платформы BI с помощью Central Configuration Manager (CCM). Также необходимо выбрать момент времени, по состоянию на который будет восстановлено содержимое веб-уровня.

Чтобы иметь возможность вернуться к текущему состоянию системы, перед восстановлением необходимо выполнить ее резервное копирование.

В случае повреждения веб-уровня его можно восстановить отдельно от других компонентов.

1. С помощью средств восстановления файлов восстановите папки веб-уровня на хосте веб-уровня.
2. С помощью CCM перезапустите все узлы в развертывании платформы BI.

13.5.1.4 Восстановление только базы данных CMS

Примечание:

Эту процедуру следует выполнять только в случае сбоя базы данных CMS. Если база данных повреждена, или были затронуты другие компоненты, необходимо выполнить полное восстановление системы.

Восстановите или замените хост базы данных CMS. В случае замены убедитесь, что новому компьютеру назначены те же имя системы, порт и учетные данные базы данных, что и предыдущему хосту.

Примечание:

Если восстановить компьютер с использованием тех же имени и учетных данных невозможно, необходимо с помощью CCM обновить сведения об этом соединении с базой данных для каждого узла в кластере, после чего перезапустить эти узлы.

1. Остановите все узлы платформы BI с помощью CCM.
2. Найдите последний набор резервных копий базы данных CMS.
3. С помощью средств управления базой данных восстановите БД CMS.
4. Найдите последний журнал транзакций базы данных CMS, то есть журнал с транзакциями, выполненными после последнего резервного копирования.
5. Воспроизведите весь журнал транзакций для базы данных CMS.
6. Запустите узлы платформы BI с помощью CCM.

После проверки работоспособности системы выполните следующие действия:

- Запустите средство Repository Diagnostic Tool, чтобы удалить все неиспользуемые временные файлы и проверить целостность репозитория. См. раздел "Repository Diagnostic Tool" этого руководства.
- Для всех заданий публикации, выполняемых во время резервного копирования системы, отображается состояние сбоя. Не запускайте такие экземпляры повторно. Вместо них следует запустить новые задания публикации.

См. также

- [Индексация содержимого в репозитории CMS](#)

13.5.1.5 Восстановление поискового индекса

Компонент поиска по платформе хранит в системе ряд файлов индекса и данных, с помощью которых обеспечивается более эффективный поиск. При восстановлении системы в этих файлах данных могут обнаруживаться несогласованности. Чтобы устранить их, можно выполнить скрипт восстановления индекса или перестроить индекс.

Перестроение индекса выполняется достаточно просто, однако, требует значительных затрат ресурсов и времени. Поисковые запросы, выполняемые в процессе перестроения, возвращают результаты только из проиндексированного фрагмента базы данных. Скрипт восстановления реализован на основе более сложной процедуры, однако обеспечивает ускоренное создание полного рабочего индекса.

При восстановлении развертывания, содержащего несколько компьютеров, скрипт можно выполнять на любом компьютере с установленной службой поиска. Для первого компьютера в кластере используйте параметр `-Both`, а для всех последующих компьютеров используйте параметр `-ContentStore`.

См. также

- [Индексация содержимого в репозитории CMS](#)

13.5.1.5.1 Запуск скрипта восстановления поискового индекса

- Проверьте работоспособность CMS и остановите все адаптивные серверы обработки (APS) с установленной службой поиска.

Примечание:

Эти адаптивные серверы обработки (APS) необходимо остановить как можно быстрее после запуска узла.

- Присвойте переменной `JAVA_HOME` значение, определяющее положение папки `sapjvm/bin` в каталоге установки платформы BI.
- Каталог данных службы поиска по платформе доступен с компьютера, на котором выполняется скрипт.

1. Откройте окно командной строки (если используется ОС Windows) на хосте CMS или APS.

2. Перейдите в каталог `<каталог_установки>\SAP BuinessObjects Enterprise XI 4.0\java\lib\`.

На компьютерах под управлением UNIX используйте эквивалентный путь к файлу UNIX.

3. Введите `java -jar platformSearchOnlineHotbackupRestore.jar` и нажмите клавишу **ВВОД**.

4. При появлении соответствующей подсказки введите следующие данные и нажмите клавишу **ВВОД**:

- Папка установки платформы BI (например, `<каталог_установки>/SAP businessObjects Enterprise XI 4.0`)
- Учетные данные для входа в систему CMS, включая имя CMS, ИД и пароль пользователя, а также тип аутентификации. Поддерживаются следующие типы аутентификации.
 - `secEnterprise`
 - `secLDAP`
 - `secWinAD`
 - `secSAPR3`

5. При появлении соответствующей подсказки введите один из следующих параметров, определяющих тип восстановления индекса, и нажмите клавишу **ВВОД**.

Значение	Описание
-Both	<p>Должен использоваться для развертываний с одним сервером или (в развертываниях с несколькими серверами) для первого хост-компьютера сервера APS со службой поиска:</p> <p>В системе с несколькими серверами поиска APS при первом запуске скрипта используйте вариант <code>-Both</code> (обновляет базу данных и хранилище содержимого). Когда скрипт запускается для всех прочих серверов поиска APS, используйте вариант <code>-ContentStore</code> (обновляет только хранилище содержимого).</p>
-ContentStore	Используется при выполнении скрипта на хостах APS с установленной службой поиска, которые не являются первыми в кластере, где выполняется скрипт.
-Exit	Завершение работы скрипта без восстановления индекса.

6. После завершения работы скрипта закройте окно командной строки (на компьютере под управлением ОС Windows).

Запустите все остановленные адаптивные серверы обработки (APS).

13.5.2 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 серверов для SSL](#)

13.5.2.1 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 подсказки 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. Введите ключ кластера и нажмите кнопку **Далее**.
7. 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.
8. Укажите расположение и имя файла BIAR, содержащего параметры конфигурации сервера, которые требуется восстановить, и нажмите кнопку **Далее** для продолжения. Появится страница с содержимым BIAR-файла.
9. Нажмите кнопку **Далее**, чтобы продолжить. Предоставленные сведения будут отображены на странице сводки.
10. Нажмите кнопку **Готово**, чтобы продолжить. Предупреждение указывает на то, что существующие параметры сервера будут заменены значениями из файла BIAR, а если продолжить, текущие параметры сервера будут утеряны.
11. Нажмите кнопку **Да**, чтобы восстановить параметры конфигурации сервера. CCM восстанавливает параметры конфигурации сервера из файла BIAR для всего кластера. Сведения о восстановлении записываются в файл журнала. Имя файла журнала и путь к нему отображаются в диалоговом окне.
12. Если во время операции восстановления произошел сбой, проверьте файл журнала для установления причины.
13. 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.

Примечание:

Узлы и серверы, которые есть в системе, но которых нет в файле BIAR, удаляются из репозитория. Узлы и серверы все еще отображаются в CCM, но вы можете вручную удалить файлы `dbinfo` и `bootstrap` для узла.

Необходимо воссоздать узлы в системе на каждом компьютере в кластере.

См. также

- [Использование узлов](#)

13.5.2.2 Восстановление параметров сервера с помощью CSM 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 **ВВОД**.
2. Введите номер порта для использования временным сервером CMS и нажмите клавишу **ВВОД**.
3. На следующих экранах укажите сведения о соединении с базой данных системы 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 **ВВОД**.
5. При выводе соответствующего приглашения укажите местоположение и имя файла BIAR, из которого требуется восстановить конфигурацию сервера, и нажмите клавишу **ВВОД**.
Предоставленные сведения будут отображены на экране сводки.
6. Проверьте правильность отображаемой информации и нажмите клавишу **ВВОД**, 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.

13.5.2.3 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 `BackupCluster.bat` расположен в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.

В UNIX файл `backupcluster.sh` расположен в каталоге `/<КАТАЛОГ_УСТАНОВКИ>/sap_bobj/enterprise_xi40/<platform64>/scripts`.

См. также

- [Скрипты BackupCluster и RestoreCluster](#)

13.5.3 Восстановление содержимого BI

Если вы создали резервную копию содержимого Business Intelligence (BI) в файлах LCMBIAR, вы можете использовать консоль управления жизненным циклом для восстановления содержимого BI, не восстанавливая при этом всю систему. Дополнительные сведения см. в *руководстве пользователя консоли управления жизненным циклом для платформы SAP BusinessObjects Business Intelligence*.

13.6 Скрипты BackupCluster и RestoreCluster

В следующей таблице описываются параметры командной строки, используемые скриптом BackupCluster.

Примечание:

Этот скрипт выполняет только резервное копирование параметров сервера для кластера. Резервное копирование других данных требуется выполнять отдельно.

Таблица 13-2: 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"
-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

Название	Описание	Пример
-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 13-3: 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:

Выполните 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 13-4: Параметры при использовании временного центрального сервера управления

Название	Описание	Пример
-usetempcms	Создание временного центрального сервера управления для указанной операции. По завершении операции временный центральный сервер управления будет остановлен.	-usetempcms
-cmsport	Номер порта временного центрального сервера управления.	-cmsport 6700
-dbdriver	Драйвер системной базы данных центрального сервера управления. Допустимы следующие значения: <ul style="list-style-type: none"> db2databasesubsystem maxdbdatabasesubsystem mysqldatabasesubsystem oracledatabasesubsystem sqlserverdatabasesubsystem sybasedatabasesubsystem sqlanywheredatabasesubsystem newdbdatabasesubsystem Примечание: Параметр newdbdatabasesubsystem используется с базами данных SAP HANA.	-dbdriver sqlserverdatabasesubsystem
-connect	Строка соединения с системной базой данных центрального сервера управления.	-connect "DSN=BusinessObjects CMS 10Data Warehouse, CSNAME=, PORT=3355"
-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
```

Копирование развертывания платформы Business Intelligence

14.1 Обзор копирования системы

В этой главе описывается создание копии развертывания платформы BI для тестирования, резервирования и других целей.

См. также

- [Обзор резервного копирования и восстановления](#)

14.2 Терминология

Термин	Определение
Исходная система	Исходное развертывание платформы BI.
Целевая система	Новое развертывание, которое необходимо создать.
Копирование системы	Операция создания дубликата существующего развертывания платформы BI.
Копирование однородных систем	Операция создания дубликата системы, при которой у исходной и целевой систем совпадают типы операционной системы и базы данных. Платформа BI поддерживает только копирование однородных систем.
Копирование разнородных систем	Операция создания дубликата системы, в которой исходная и целевая системы используют различные типы операционных систем или СУБД, но основаны на одних и тех же данных.
Копирование базы данных	Операция создания дубликата системы CMS или базы данных аудита с помощью средств поставщика базы данных.

14.3 Ситуации, в которых может потребоваться копирование системы

В следующей таблице описаны цели, которых можно достичь при наличии соответствующих ресурсов, и приведены указания по выбору оптимального решения.

Цель	Требуемые ресурсы	Решение
<p>Цель: идентичная копия</p> <p>Создание дублирующей системы для резервирования или тестирования с идентичной аппаратной конфигурацией и теми же IP-адресами и именами компьютеров.</p>	<ul style="list-style-type: none"> • Целевая система с аппаратной конфигурацией, аналогичной исходной системе И • Резервные копии исходной системы или доступ к исходной системе для создания резервной копии. 	<p>Используйте рабочий процесс для резервного копирования и восстановления системы, описанный в этом руководстве. См. процедуру Резервное копирование всей системы. Воссоздайте целевую систему из резервных копий исходной системы.</p>
<p>Цель: копия</p> <p>Создание дублирующей системы для резервирования, тестирования или обучения с аппаратной конфигурацией или IP-адресами и именами компьютеров, отличными от исходной системы.</p>	<ul style="list-style-type: none"> • Исходная система (запущенная или остановленная) ИЛИ резервные копии баз данных и файлов исходной системы. И • Подробные сведения о системе, описанные в Экспорт из исходной системы 	<p>Используйте рабочий процесс копирования системы, начиная с Планирование копирования системы, и следуйте указаниям, приведенным в остальной части главы.</p> <p>Примечание:</p> <p>Можно создать целевую систему на компьютере с существующим развертыванием платформы BI той же версии, с тем же пакетом поддержки и уровнем исправлений или на "чистом" компьютере без установленной платформы BI.</p>

См. также

- [Резервные копии](#)
- [Планирование копирования системы](#)

14.4 Планирование копирования системы

Копия системы не обязательно должна соответствовать текущему состоянию системы. Можно создать копию системы и подождать некоторое время перед воспроизведением копии на целевой системе, или воспользоваться в качестве основы для целевой системы предыдущей копией исходной системы. Это будет означать, что копия будет представлять систему на момент создания копии. Например, если подождать один месяц, копия воссоздаст систему такой, какой она была месяц назад.

После просмотра сценариев использования в предыдущем разделе и выбора лучшей стратегии необходимо разработать план копирования системы.

Создание плана копирования системы

При планировании копирования системы необходимо заранее обдумать следующие моменты.

- Будет ли исходная система остановлена или останется активной во время создания копии? (Процедуру можно выполнить в каждом из этих вариантов)
 - Если исходная система остановлена, простой какой длительности потребуется на выполнение операции?
 - Выделите некоторое время на проверку для обеспечения целостности целевой системы.
- Какие средства базы данных будут использоваться для резервного копирования и восстановления базы данных?
- На каких компьютерах будет развернута целевая система, и где будет размещен каждый из узлов?
- Какие дополнительные компоненты следует скопировать?
- Тип базы данных, используемой для целевой базы данных CMS и для других необязательных баз данных, которые будут копироваться.

Следует также рассмотреть следующие вопросы.

- Какие компоненты платформы BI установлены в исходной системе. Можно использовать функцию **Добавить/Удалить > Изменить** программы установки, которая позволяет просмотреть список установленных компонентов.
- Если целевая система устанавливается на аппаратную конфигурацию, которая отличается от исходной системы, возможно, потребуется произвести настройку целевой системы для лучшей производительности. Сведения об улучшении производительности системы см. в руководстве *SAP BusinessObjects Business Intelligence sizing companion guide*.
- Возможно, в целевой системе следует включить формирование отчетов на основе баз данных отчетности, отличных от баз данных исходной системы. В этом случае потребуется изменить сведения о соединении с базами данных для баз данных отчетности. Это можно сделать, сохранив то же DSN-имя, но указав в DSN другую базу данных в целевой системе.

Требуемые компоненты исходной системы

- База данных системы CMS
- Хранилище сервера репозитория файлов
- Файлы конфигурации семантического уровня.
- База данных аудита (необязательно)
- База данных мониторинга (необязательно)
- База данных вспомогательной версии управления жизненным циклом (необязательно)

14.5 Рекомендации и ограничения

Следует помнить о следующих рекомендациях при создании копии развертывания платформы BI.

Диаграмма с областями	Рекомендация
Интеграции с SAP Business Warehouse	Если вы используете платформу BI и SAP ERP или BW в интегрированной среде, перед копированием системы прочитайте документацию по копии SAP-системы. Руководства по созданию копии системы доступны в http://www.sdn.sap.com/irj/sdn/systemcopy (требуется вход в SMP). Выберите версию SAP NetWeaver; соответствующие руководства хранятся в папке руководств по установке.
Версия программы	В исходной и целевой системах должны быть установлены одинаковые версии, пакеты обновления и исправления.
Параметры содержимого и конфигурации	Поддерживается только копирование исходной системы в целом. Копирование отдельных компонентов, контента или параметров конфигурации системы невозможно.
Путь установки	Путь установки в расположениях исходной и целевой систем должен в точности совпадать: например, если исходная система установлена в C:\SAP BusinessObjects Enterprise XI 4.0, то целевую систему следует установить в C:\SAP BusinessObjects Enterprise XI 4.0.
Операционная система хоста	В исходной и целевой системах должны использоваться одинаковые операционные системы.
Тип программного обеспечения базы данных CMS	Базы данных исходной и целевой системы CMS должны иметь одинаковый тип. Выбрать другой поддерживаемый тип базы данных можно только после копирования системы.
Тип программного обеспечения базы данных аудита	Если вы копируете данные аудита, исходная и целевая база данных аудита должны быть одного типа. После создания копии вы можете создать новую базу данных другого типа. Примечание: Если создана новая база данных, существующие события не будут скопированы в нее, в новую базу данных записываются только новые события.
Настройка веб-уровня	В процессе копирования не переносятся компоненты веб-уровня из исходной системы. Если вы настроили веб-уровень (например, изменены файлы <code>.properties</code> в папке <code>custom</code>), необходимо вручную применить эти настройки к целевому объекту.
Разделы, не описанные в этих инструкциях	В этом рабочем процессе не описывается порядок экспорт и импорта базы данных. Используйте инструменты поставщика базы данных для копирования и восстановления базы данных.

В процессе копирования системы переносятся следующие данные.

- База данных репозитория CMS. (содержит отчеты, аналитические данные, папки, права, пользователей и группы пользователей, параметры сервера и другое содержимое BI и системы)

- База данных аудита. (содержит события аудита, инициируемые серверами платформы BI и клиентскими приложениями)
- База данных мониторинга. (содержит данные тенденций от метрик, зондов и наблюдений)
- База данных управления жизненным циклом. (содержит разные версии отчетов, аналитических данных, других ресурсов BI и сведения о версии)

Примечание:

Описание баз данных и их содержимого см. в разделе [Базы данных](#) данного руководства.

- Файлы конфигурации семантического уровня.

Конфигурация веб-уровня, индекс поиска и другие данные, не указанные выше, не копируются.

Рекомендации по копиям для восстановления файлов

При копировании системы для восстановления определенного файла, который был случайно удален, следует помнить о следующих вопросах.

Используя вашу резервную копию, выполните в своей рабочей среде действия, описанные в процедуре [Импорт в целевую систему](#).

- Не устанавливайте все узлы, установите только первый узел с CMS и базой данных.
- Не устанавливайте базы данных аудита, LCM и мониторинга.
- Не воссоздавайте соединения с базами данных аудита и отчетов.

Используйте LCM для перемещения объекта, который вы хотите восстановить из целевой системы в исходной системе.

14.6 Процедура копирования системы

Далее описываются две стадии копирования платформы BI.

14.6.1 Экспорт из исходной системы

Также необходимо собрать следующие сведения об исходной системе. Если требуется записать эту информацию, то в [Рабочая таблица системной копии](#) доступна рабочая таблица, которую можно использовать.

Свойство	Местоположение
Ключ кластера CMS (обеспечьте безопасность записи).	Создается системным администратором при установке платформы BI.
Имя узлов.	Откройте вкладку Серверы CMS и разверните в левом дереве Узлы .
Имя компьютера и папка установки платформы BI для каждого компьютера в развертывании.	Откройте вкладку Серверы в CMS, щелкните правой кнопкой CMS и выберите Заполнители . Найдите значение заполнителя %INSTALLROOTDIR%.
Пароль администратора платформы BI (обеспечьте безопасность системы).	Создается системным администратором при установке платформы BI.
<p>Все подключения к базам данных, которые могут использоваться CMS, а также имена пользователей и пароли, связанные с этими соединениями. К ним может относиться и база данных аудита, если вы хотите скопировать эту информацию. Обязательно получите эти сведения для всех компьютеров в кластере.</p> <p>Примечание: Если вы копируете базу данных аудита, вам также необходимы имена и учетные данные соединения с базой данных аудита.</p>	<p>Откройте вкладку Серверы CMS, щелкните CMS правой кнопкой и выберите Метрики.</p> <p>Найдите следующие метрики:</p> <ul style="list-style-type: none"> «Имя соединения к системной базе данных» «Имя сервера системной базы данных» «Имя пользователя системной базы данных» «Имя источника данных» «Имя соединения с базой данных аудита» (необязательно) «Имя пользователя базы данных аудита» (необязательно)
Для каждого компьютера в кластере — сведения (типы и версии клиентов) о других соединениях с базой данных (например, используемых юниверсами и отчетами). Обязательно укажите имена пользователей и пароли.	Для отчетов Crystal, которые создаются непосредственно на основе баз данных, найдите сведения о соединении с помощью конструкторов SAP Crystal Reports 2011 или SAP Crystal Reports for Enterprise. Для получения сведений о соединении с юниверсами используйте средство дизайна информации (.unx) или средство дизайна юниверса (.unv).
Версия, пакет поддержки и уровень исправлений исходной системы.	<p>В Windows это можно определить, используя средство «Удаление или изменение программ».</p> <p>В ОС Unix можно воспользоваться утилитой <code>modifyOrRemoveProducts.sh</code> в каталоге установки платформы BI.</p>

Свойство	Местоположение
Расположения хранения файлов для каждого репозитория входящих и исходящих файлов FRS в развертывании.	<p>Откройте вкладку Серверы в СМС, щелкните правой кнопкой репозиторий входящих или исходящих файлов FRS и выберите Свойства. Найдите свойство «Каталог хранилища файлов».</p> <p>Примечание: Если значение начинается с символа "%", это заполнитель, и вам потребуется щелкнуть Заполнители и записать каталог, указанный для этого заполнителя.</p>

Свойство	Местоположение
Если планируется копирование приложения Lifecycle Management (LCM), расположение папки базы данных LCM и папок Subversion LCM.	<p>По умолчанию в установках LCM в ОС Windows база данных находится в папке <КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\Data\LCM\LCMOverride, а в ОС Unix — в папке <КАТАЛОГ_УСТАНОВКИ>/sap_bobj/data/LCM/LCMOverride.</p> <p>По умолчанию в ОС Windows используются следующие расположения файлов LCM Subversion:</p> <ul style="list-style-type: none"> • <КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\CheckOut • <КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository <p>, а в ОС UNIX – следующие:</p> <ul style="list-style-type: none"> • <КАТАЛОГ_УСТАНОВКИ>/check_out (Этот каталог создается только после извлечения файлов с помощью Subversion) • \$HOME/LCM_Repository
Если вы планируете копировать базу данных мониторинга, это папка базы данных мониторинга.	<p>Она устанавливается в СМС. Перейдите в область управления Приложения в СМС, выберите Приложение мониторинга > Свойства и найдите «Каталог резервного копирования базы данных тренда».</p> <p>Папка по умолчанию в установках в ОС Windows – <КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB, а в ОС Unix – <КАТАЛОГ_УСТАНОВКИ>/sap_bobj/Data/TrendingDB.</p>
Путь к папке семантического уровня.	Папка по умолчанию в Windows – <каталог_установки>\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionsServer\.

После записи информации, описанной выше:

1. Используйте инструменты поставщика базы данных для создания резервной копии следующих баз данных:

- база данных системы CMS;
- база данных аудита (необязательно).

2. Используя средства резервного копирования, создайте копии следующих наборов файлов:

- хранилища входящих и исходящих файлов FRS;
- база данных мониторинга трендов (необязательно). Для этого можно создать резервную копию файлов из папки мониторинга, как указано в рабочей таблице. По умолчанию в Windows это <КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB. В Unix: <КАТАЛОГ_УСТАНОВКИ>/sap_bobj/Data/TrendingDB.
- База данных управления жизненным циклом (необязательно). Для этого можно создать резервную копию файлов из папки базы данных, как указано в рабочей таблице. По умолчанию в Windows это <КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\Data\LCM\LCMOVERRIDE. В Unix: <КАТАЛОГ_УСТАНОВКИ>/sap_bobj/data/LCM/LCMOverride.
- База данных управления жизненным циклом Subversion (необязательно). Для этого можно создать резервную копию файлов из папок Subversion, как указано в рабочей таблице. По умолчанию в Windows это следующие каталоги:
 - <КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\CheckOut
 - <КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository

В ОС UNIX это следующие каталоги:

- <КАТАЛОГ_УСТАНОВКИ>/check_out (Этот каталог создается только после извлечения файлов с помощью Subversion)
- \$HOME/LCM_Repository
- Файлы конфигурации из папки семантического уровня: файл cs.cfg в папке connectionServer, а также любые SBO- и PRM-файлы во всех вложенных папках.

Примечание:

Сведения об ограничениях и подробное описание этого процесса см. в разделе [Оперативное резервное копирование](#).

3. Следующие файлы могут настраиваться пользователем. Если вы изменяли их содержание, создайте резервную копию этих файлов в исходной системе, затем восстановите их в ту же папку в целевой системе:

- BO_trace.ini, устанавливается в папку
 - [КАТАЛОГ_УСТАНОВКИ]SAP BusinessObjects Enterprise XI 4.0/conf
- clientsDKOptions.xml, устанавливается в папку:
 - [КАТАЛОГ_УСТАНОВКИ]SAP BusinessObjects Enterprise XI 4.0/java/lib
 - [КАТАЛОГ_УСТАНОВКИ]SAP BusinessObjects Enterprise XI 4.0/win32_x86
 - [КАТАЛОГ_УСТАНОВКИ]SAP BusinessObjects Enterprise XI 4.0/win64_x64
- CRConfig.xml, устанавливается в папку:
 - [КАТАЛОГ_УСТАНОВКИ]SAP BusinessObjects Enterprise XI 4.0/java
- mdas.properties, устанавливается в папку:
 - [КАТАЛОГ_УСТАНОВКИ]/SAP BusinessObjects Enterprise XI 4.0/java/pjs/services/MDAS/resources/com/businessobjects/multidimensional/services

- **Файлы конфигурации WDeploy, установленные в папку [КАТАЛОГ_УСТАНОВКИ] SAP BusinessObjects Enterprise XI 4.0/wdeploy/conf:**
 - config.apache
 - config.jboss7
 - config.sapappsrv73
 - config.tomcat6
 - config.tomcat7
 - config.weblogic11
 - config.websphere7
 - config.websphere8
 - wdeploy.conf
4. Следующие файлы веб-уровня могут настраиваться пользователем. Если вы внесли изменения в какие-либо из этих файлов, создайте резервную копию файлов на исходной системе. Затем потребуется восстановить эти файлы или воспроизвести изменения в целевой системе.
- **BO_trace.ini, устанавливается в папку**
 - [КАТАЛОГ_УСТАНОВКИ] SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/BOE/WEB-INF/TraceLog
 - [КАТАЛОГ_УСТАНОВКИ] SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/conf
 - **clientaccesspolicy.xml, устанавливается в папку:**
 - [КАТАЛОГ_УСТАНОВКИ] SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT
 - **clientSDKOptions.xml, устанавливается в папку:**
 - [КАТАЛОГ_УСТАНОВКИ] SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/clientapi/WEB-INF/lib
 - [КАТАЛОГ_УСТАНОВКИ] SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/lib
 - **crossdomain.xml, устанавливается в папку:**
 - [КАТАЛОГ_УСТАНОВКИ] SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT
 - [КАТАЛОГ_УСТАНОВКИ] tomcat/webapps/ROOT
 - **Любые измененные файлы в папке config/custom (в веб-уровне). Создайте резервную копию этих файлов, чтобы перенести изменения в целевую систему.**
5. Создайте резервную копию всех пользовательских расширений, которые вы вручную добавили в исходную систему, например, расширений публикации, пользовательских библиотек и т. д. Сохраните информацию, записанную ранее, с копией баз данных и файлов. Вы можете сохранить вторую копию, которую можно при необходимости обновлять для копирования системы в будущем.

14.6.2 Импорт в целевую систему

Для выполнения этой процедуры необходимо предварительно создать резервные копии баз данных и системных файлов исходной системы, которые будут использоваться в целевой системе. Все файлы резервных копий должны быть из одного набора резервного копирования. Вам также потребуются данные (например, ключ кластера и учетные данные для базы данных), описанные в разделе «Экспорт копии системы из исходной системы».

Если целевая система будет размещаться на сетевом ресурсе с доступом к ресурсам исходной системы, необходимо запретить попытки доступа к ним из целевой системы до тех пор, пока не будет изменена ее конфигурация. Для этого можно установить между исходной и целевой системами брандмауэр или остановить исходную систему до тех пор, пока не будет выполнена настройка целевой. После первого запуска целевой системы брандмауэр можно удалить, либо можно запустить исходную систему.

Если в целевой системе уже установлена платформа BI, убедитесь, что ее версия, пакет поддержки и уровень исправлений совпадают с исходной системой на момент создания копии. Также убедитесь, что используется тот же путь установки, что и в исходной системе.

1. В целевой системе создайте соединение с одной или несколькими базами данных, в которых будут размещены репозиторий CMS, база данных аудита и база данных отчетов.

Примечание:

Эти соединения могут указывать на разные базы данных, однако должны иметь те же имена или DSN и использовать те же учетные данные, что и в исходной системе.

2. Используйте средства базы данных для восстановления базы данных CMS и базы данных аудита (если требуется) из резервной копии исходной системы в целевой базе данных.

Если юниверсы или отчеты в целевой системе должны использовать другую базу данных отчетов, измените соединение базы данных, чтобы оно указывало на эту базу данных.

Если вам нужны более подробные инструкции по этой процедуре, см. раздел [Восстановление системы](#).

3. Если платформа BI уже установлена на целевой системе хоста, перейдите к шагу 4. Если платформа BI не установлена, установите ее на целевой системе хоста, помня о следующем:
 - a. Установите ту же версию программы, пакет поддержки и уровень исправлений, что и в исходной системе.
 - b. Используйте тот же путь установки, что и в исходной системе.
 - c. Выберите те же компоненты, которые были установлены в исходной системе.
 - d. При появлении запроса на создание базы данных CMS (кроме того, при необходимости и базы данных аудита) в ходе установки выберите параметр **Использовать существующую базу данных** и введите имя и учетные данные соединения, заданные на шаге 1.

Примечание:

Не выбирайте повторную инициализацию базы данных CMS.

- е. При запросе на ввод **имени узла** используйте те же имена, номера портов, пароль администратора платформы и ключ кластера, что и в исходной системе.

Для получения дополнительной информации см. *Руководство по установке платформы SAP BusinessObjects Business Intelligence*. После завершения установки системы перейдите к шагу 6.

Примечание:

Если вы не копируете данные аудита из исходной системы, вы можете создать новую базу данных аудита, настроив аудит во время установки.

- f. Остановите все узлы в CCM.
4. Если платформа BI уже установлена в целевой системе, остановите все узлы в CCM. Запустите CCM на компьютере целевой системы CMS.
 5. Если платформа BI уже установлена, добавьте новый узел, используя параметр **Повторно создать узел**.
 - a. Используйте значения параметров **Имя узла** и **Номер порта SIA** из исходной системы.
 - b. Выберите элемент **Запуск нового временного CMS**.
 - c. Выберите новые значения **Номер порта CMS** (любой свободный порт) и **Тип базы данных CMS** (в соответствии с типом восстановленной базы данных).
 - d. Введите данные для соединения с базой данных CMS, восстановленной на шаге 1.
 - e. Введите ключ кластера исходной системы.
 - f. Введите пароль администратора исходной системы.
 6. Восстановите хранилища файлов для серверов репозитория входящих и исходящих файлов в файловом хранилище целевой системы. Используйте ту же папку, что и на исходной системе.
 7. Восстановите папку базы данных мониторинга (если необходимо скопировать данные мониторинга) в ту же папку, что и в исходной системе.
 8. Восстановите папку базы данных LCM (если необходимо скопировать данные LCM) в ту же папку, что и в исходной системе.
 9. Восстановите файлы Subversion LCM (если необходимо скопировать данные LCM) в ту же папку, что и в исходной системе.
 10. Восстановите файлы конфигурации сервера для семантического уровня/соединения в ту же папку, что и на исходной системе.
 11. Перезапустите хосты целевой системы.
 12. Если установлена платформа BI на шаге 3, примените все пакеты поддержки и исправления, установленные в исходной системе.
 13. Если целевая система будет работать на нескольких хостах, повторите шаги 1–11 на каждом хосте.
Используйте параметр расширенной установки при установке дополнительных узлов платформы BI и помните, что следует использовать такие же имена узлов, как и в исходной системе.
 14. Если база данных CMS целевой системы будет использовать другой тип базы данных, с помощью CCM выполните процедуру [Копирование данных из одной базы данных CMS в другую](#), указав нужную базу данных.
 15. Восстановите все настраиваемые пользователем файлы, резервные копии которых были созданы на шаге 3 процедуры «Экспорт копии системы из исходной системы».

16. Восстановите все файлы веб-уровня, резервные копии которых были созданы на шаге 4 процедуры «Экспорт копии системы из исходной системы».

«Веб-уровень» относится к промежуточной области WDeploy, в которой можно осуществлять пользовательские настройки, а также к содержимому веб-уровня, развернутому на сервере приложений.

При применении изменений к целевой системе не применяйте изменения к каталогу сервера приложений; применяйте изменения в промежуточной области WDeploy, а затем повторно разверните веб-уровень на сервере приложений с помощью WDeploy.

Промежуточная область WDeploy в ОС Windows находится в следующей папке: <КАТАЛОГ_УСТАНОВКИ>/SAP BusinessObjects Enterprise XI 4.0/warfiles.

17. Восстановите все расширения, резервные копии которых были созданы на шаге 5 процедуры «Экспорт копии системы из исходной системы».

После копирования системы платформы BI:

1. При установке первого узла в целевой системе будет создан временный сервер CMS, который будет остановлен после установки. С помощью CMC откройте страницу "Серверы" и удалите этот сервер CMS.

Помните:

Если исходная система не удалена (или если она используется параллельно целевой системе), рекомендуется переименовать кластер целевой системы.

2. Запустите Repository Diagnostic Tool в целевой базе данных CMS.
3. Если это необходимо, настройте единый вход в систему Windows Active Domain (SSO) в целевой системе. См. раздел [SSO в платформу BI с аутентификацией AD](#).
4. При необходимости настройте SLD в целевой системе. Подробные сведения см. в заметке SAP №1508421: «SAP SLD Data Supplier для Apache Tomcat».
5. Проверьте работоспособность и целостность целевой системы.
6. Выполните полное индексирование поиска.

Управление версиями

15.1 Управление разными версиями ресурсов BI

Приложение управления повышением позволяет использовать разные версии ресурсов BI, которые находятся в репозитории платформы SAP BusinessObjects Business Intelligence. Для поддержки этой возможности в средстве реализованы системы контроля версий SubVersion и ClearCase.


Для управления разными версиями заданий или информационных объектов выполните следующие действия:

1. Войдите в приложение СМС и выберите **Управление версиями**.
2. В левой панели окна «Управление версиями» выберите папку для просмотра задания или информационных объектов, для которых будет выполняться управление версиями.
3. Выберите информационные объекты и нажмите кнопку **Добавить в VM**.

Примечание:

Если выбрать «Добавить в VM», это приведет к созданию базовой версии объекта в репозитории системы управления версиями (VMS). Базовая версия требуется для последующей регистрации.

4. При последующих изменениях документа и для создания версии инкрементно изменяемого документа нажмите **Возврат**. Документ, существующий в репозитории VMS, будет обновлен. Откроется диалоговое окно «Комментарии регистрации».
5. Введите свои комментарии и нажмите кнопку **ОК**.
Изменение номера версии выбранного информационного объекта отображается в столбцах систем управления версиями и содержимым.
6. Чтобы получить последнюю версию документа из VMS, выберите требуемый информационный объект и щелкните **Получить последнюю версию**.
Из репозитория VMS в CMS будет импортирована последняя версия.
7. Чтобы создать копию последней версии, нажмите кнопку **Создать копию**.
В репозитории VMS будет создана копия выбранной версии.
8. Выберите **Журнал**, чтобы просмотреть все версии, доступные для выбранного информационного объекта.
Откроется окно «Журнал». Будут отображены следующие возможные действия:

- **Получить версию** – если существует несколько версий и требуется определенная версия источника BI, можно выбрать требуемый информационный объект и нажать кнопку **Получить версию**.
 - **Получить копию версии** – позволяет получить копию выбранной версии.
 - **Экспортировать копию версии** – позволяет получить копию выбранной версии и сохранить ее на локальном компьютере.
 - **Сравнить** – позволяет сравнить метаданные двух версий содержимого.
9. Чтобы заблокировать информационный объект, выберите объект и нажмите **Блокировать**; для отмены блокировки информационного объекта выберите **Разблокировать**; для удаления всех версий содержимого из репозитория VMS нажмите **Удалить**. Содержимое CMS не изменится.
- Примечание:**
Если информационный объект заблокирован, с ним невозможно выполнять никаких действий.
10. Если версия в CMS более поздняя, чем версия в VMS, рядом с обновленным информационным объектом появляется индикатор. Если поместить курсор на этот индикатор, появится всплывающая подсказка с сообщением, что информационный объект CMS изменен.
11. Чтобы просмотреть список всех зарегистрированных ресурсов, существующих в VMS, но не в CMS, нажмите кнопку **Просмотреть удаленные ресурсы**.
- Для просмотра истории любого удаленного ресурса щелкните этот ресурс. Для просмотра версии удаленного ресурса выберите удаленный ресурс и нажмите **Получить версию**. Для получения копии выбранного ресурса нажмите **Получить копию версии**.
- Для полного удаления объекта из репозитория VMS нажмите **Удалить**.
- Примечание:**
При использовании **Получить версию** или **Получить копию версии** ресурс перемещается из пропавшего файла VMS в CMS.
12. Выберите информационный объект и нажмите кнопку , чтобы просмотреть свойства информационного объекта.
- Вместо этого можно щелкнуть информационный объект правой кнопкой мыши и выполнить шаги с 4 по 16.

15.2 Использование параметра системных настроек управления версиями

Систему управления версиями можно настроить в Central Management Console. Допускается конфигурация параметров SubVersion и ClearCase.

Чтобы установить систему управления SubVersion, выполните следующие шаги:

1. На домашней странице CMS выберите **Приложения**.
2. Дважды щелкните **VMS**. Появится экран "Параметры управления версиями".
3. Выберите **Настройки VMS**.
4. В раскрывающемся списке **Системы управления версиями** выберите **SubVersion**.

В соответствующих полях появятся сведения о номере порте сервера, пароле, имени репозитория, имени сервера, имени пользователя, имени каталога рабочей области и имени каталога установки, указанные в процессе установки средства управления повышением.

5. При необходимости измените поля.

Убедитесь, что вводите расширение пути установки до файла `.exe`. К примеру, в Windows:
`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\subversion and In Unix -`
 в Unix:
`/usr/u/qaunix/aurora_730/sap_bobj/enterprise_40/subversion/bin.`

6. Для доступа к репозиторию вспомогательной версии можно использовать протокол `http` или `svn`; для выбора протокола установите соответствующий переключатель.

7. Проверить установленные параметры VMS можно путем выбора **Проверить VMS**.

8. Нажмите кнопку **Сохранить**.

Примечание:

- Если требуется наличие SubVersion как VMS по умолчанию, выберите **Использовать как VMS по умолчанию**.
- Если согласно шагу 3 поля были изменены, следует перезапустить Server Intelligence Agent.

15.2.1 Установка системы управления версиями ClearCase в Windows

Чтобы установить в Windows систему управления версиями ClearCase, выполните следующие шаги:

1. В окне «Параметры администрирования» нажмите кнопку **Настройки VMS**.
2. В раскрывающемся списке **Система управления версиями** выберите **ClearCase**.
3. Введите следующую информацию:
 - Диск сопоставления ClearCase – введите имя диска. По умолчанию установлен диск M. Например: M:
 - Имя тега VOB – введите имя Versioned Object Base (VOB). Например: пятницаVB
 - Просмотреть каталог хранилища – введите путь к общей папке. Например: \\Имя хоста\Имя папки

Примечание:

Имя хоста не должно быть написано как локальный хост.

4. Нажмите кнопку **Сохранить**.

15.2.2 Установка системы управления версиями ClearCase в Unix

Чтобы установить систему управления версиями ClearCase в Unix, выполните следующие шаги:

1. В окне "Параметры администрирования" нажмите кнопку **Настройки VMS**.
2. В раскрывающемся списке "Системы управления версиями" выберите **ClearCase**.
3. Введите следующую информацию:
 - Диск сопоставления ClearCase – введите имя папки, где расположена MVFS. По умолчанию это /просмотр
 - Имя тега VOB – введите имя VOB и папку, где расположен VOB. Например: Папка Vob/Имя Vob
 - Просмотреть каталог хранилища: введите путь каталога, в котором созданы представления.

Можно выбрать **Использовать как VMS по умолчанию**, если требуется использовать ClearCase как систему управления версиями по умолчанию.

15.3 Сравнение разных версий одного задания

Для просмотра различий между двумя версиями одного задания выполните следующие действия:

1. Войдите в приложение СМС.
2. На домашней странице СМС выберите **Управление версиями**.
3. На экране управления версиями выберите информационный объект, версии которого следует сравнить.
4. Нажмите кнопку **Журнал**.
Появится страница "Журнал" со всеми версиями выбранного информационного объекта.
5. Выберите любые две версии для сравнения.
6. Нажмите **Сравнить**.
Начнется процесс сравнения; отличия будут выделены оранжевым цветом, а отсутствующие объекты – красным.
7. Нажмите кнопку **Сохранить**, чтобы сохранить отчет об отличиях.

15.4 Обновление содержимого вспомогательной версии

При наличии старого содержимого вспомогательной версии, созданного в предыдущей версии платформы SAP BusinessObjects BI, для обновления этого содержимого до последней версии выполните следующие действия:

1. Войдите в VMS на компьютере с SAP BusinessObjects Enterprise 3.x.
2. Выполните возврат любого объекта. Например, дважды выполните возврат объектов администратора и гостя.

3. В СМС выберите **Пользователи** и убедитесь, что в качестве номера версии VMS и CMS указано 2.
4. Выйдите из VMS.
5. В командной строке наберите `C:\Program Files\Subversion\bin` и запустите команду экспорта: `svnadmin dump c:/LCM_repository/svn_repository > dumrepo`
6. Скопируйте файл `dumrepo` на компьютер, на котором установлена платформа SAP BusinessObjects BI.
7. В командной строке на компьютере, на котором установлена платформа SAP BusinessObjects BI, перейдите к `C:\Program Files (x86)\SAP` и выполните следующие команды:

```
svnadmin.exe load "C:/Program Files (x86)/SAP
BusinessObjects/SAPBusinessObjects Enterprise XI
4.0/LCM_repository/svn_repository" < c:/dumrepo
svnadmin.exe upgrade "C:/Program Files (x86)/SAP BusinessObjects/SAP
BusinessObjects Enterprise XI 4.0/LCM_repository/svn_repository"
```
8. После успешного выполнения команд перезапустите SIA.
9. Войдите в СМС и выберите **Управление версиями**.
10. Выберите **Пользователи** и убедитесь, что в качестве версии VMS указано 2.
11. Выберите объект **Администратор** и нажмите **Получить последнюю версию**.
12. Номера версий VMS и CMS теперь совпадают.

Управление повышением

16.1 Введение в управление повышением

16.1.1 Обзор средства управления повышением

Приложение управления повышением позволяет переносить ресурсы BI из одного репозитория в другой, осуществлять управление зависимостями ресурсов и при необходимости выполнять откат перенесенных ресурсов в целевой системе. Также приложение поддерживает управление различными версиями одного ресурса BI.

Приложение управления повышением интегрировано в Central Management Console. Можно повысить ресурс BI из одной системы в другую только в том случае, если и в исходной и целевой системах установлена одинаковая версия платформы SAP BusinessObjects Business Intelligence.

16.1.2 Функции управления повышением

В приложении управления повышением поддерживаются следующие функции:

- Повышение – эта функция позволяет создавать или обновлять информационные объекты в целевой системе. Помимо продвижения информационных объектов эта функция позволяет выполнять следующие задачи:
 - Создать новое задание
 - Скопировать существующее задание
 - Изменить задание
 - Планировать повышение задания
 - Просмотреть журнал задания
 - Экспортировать как LCMBIAR
 - Импортировать BIAR и LCMBIAR
- Управление зависимостями – эта функция позволяет выбирать, фильтровать зависимые элементы информационных объектов и управлять ими в задании, которое требуется повысить.

- Планирование – эта функция позволяет указать время повышения задания вместо повышения задания сразу после его создания. Можно задать время повышения задания, выбрав один из следующих параметров: ежечасно, ежедневно, еженедельно или ежемесячно.
- Безопасность – эта функция позволяет повышать информационные объекты вместе с соответствующими правами безопасности и, при необходимости, повышает информационные объекты, связанные с правами приложения.
- Повышение проверки – с помощью этой функции можно проверять или тестировать повышение с целью убедиться, что все защитные меры приняты до фактического повышения информационных объектов.
- Откат – эта функция позволяет после повышения задания восстановить целевую систему в ее предшествующем состоянии. Можно выполнить откат всего задания или его части.
- Аудит – события, сгенерированные средством управления повышением, сохраняются в базе данных аудита. Эта функция позволяет контролировать события, записанные в базу данных аудита.
- Настройка переопределения LCM – эта функция позволяет просматривать и повышать переопределения посредством повышения задания.

16.1.3 Права доступа к приложению

В этом разделе описаны права доступа к приложению управления повышением.

- Консоль СМС позволяет задавать права доступа к приложению управления повышением.
- Для разных функций приложения управления повышением можно задавать разные права доступа к разным приложениям.

Чтобы задать отдельные права доступа в приложении управления повышением, выполните следующие действия.

1. Выполните вход в систему на СМС и выберите **Приложения**.
2. Дважды щелкните **управление повышением**.
3. Щелкните **Безопасность пользователя** и выберите пользователя. Можно просмотреть или назначить права безопасности пользователю.
4. Доступны следующие права безопасности на управление повышением:
 - Права на доступ к изменению переопределений
 - Права на доступ к включению безопасности
 - Права на доступ к администрированию LCM
 - Права на доступ к управлению зависимостями
 - Создать задание
 - Удалить задание
 - Изменить задание
 - Изменение LCMBIAR
 - Экспортировать как LCMBIAR
 - Импортировать LCMBIAR
 - Повысить задание

- Откатить задание
 - Просмотр и выбор объектов BOMM (метаданные BusinessObjects)
 - Просмотр и выбор бизнес-представлений
 - Просмотр и выбор календарей
 - Просмотр и выбор соединений
 - Просмотр и выбор профилей
 - Просмотр и выбор QaaWS
 - Просмотр и выбор объектов отчетов
 - Просмотр и выбор настроек безопасности
 - Просмотр и выбор универсов
5. Если необходимо назначить права выбранному пользователю, выберите соответствующее право и нажмите кнопку **Назначить безопасность**.

Права доступа к приложению управления повышением устанавливаются на консоли СМС.

16.1.4 Поддержка WinAD в управлении повышениями

Для бесппроблемной работы приложения управления повышениями необходимо добавить для всех аргументов `javaargs` для всех адаптивных серверов заданий следующие документы:

```
Djava.security.auth.login.config=bsclogin.conf,Djava.security.krb5.conf=krb5.ini
```

Помните:

Укажите верный путь к `bsclogin.conf` и `krb5.ini` в своем развертывании.

16.2 Начало работы со средством управления повышением

16.2.1 Запуск приложения управления повышением

Для запуска приложения управления повышением выберите **Управление повышением** на начальной странице СМС.

При наличии у пользователя прав просмотра папки **Задания повышения** он может запустить приложение управления повышением. Однако для создания, планирования или повышения уровня задания пользователь должен получить у администратора дополнительные права.







16.2.2 Компоненты пользовательского интерфейса


В этой главе описываются компоненты пользовательского интерфейса средства управления повышением.

- панель инструментов рабочего пространства управления повышением
- Панель рабочего пространства
- Панель дерева
- Панель деталей
- Корзина покупок и страница средства просмотра заданий

панель инструментов рабочего пространства управления повышением

В следующей таблице приведен список параметров, входящих в панель инструментов рабочего пространства управления повышением, и описаны задачи, которые можно выполнять с помощью этих параметров:

Действие	Описание
	Позволяет создавать новую папку. Новая папка создается как вложенная папка в папке Задания повышения .
	Позволяет копировать и удалять выделенное задание или папку из текущего местоположения.
	Позволяет копировать задание или папку из текущего местоположения.
	Позволяет вставлять скопированное задание или папку в новое место.
	Позволяет удалять существующее задание.
	Позволяет обновлять домашнюю страницу для получения обновленного списка заданий или папок, доступных для повышения.
Свойства	Позволяет изменять свойства выбранного задания. Можно изменять заголовок, описание и ключевые слова выбранного задания.
Журнал	Позволяет просматривать журнал выбранного задания.
Создать задание	Позволяет создавать новое задание.
Импорт	Позволяет импортировать файлы BIAR и файлы переопределения.

Действие	Описание
Изменить	Позволяет изменить выбранное задание.
Повысить	Позволяет повышать выбранное задание.
Откат	Позволяет искать повышенное задание из целевой системы.
	Позволяет переходить между страницами списка заданий. Этот параметр можно использовать для перехода на одной странице или перехода на конкретную страницу с помощью введенного номера соответствующей страницы.
Поиск	Позволяет искать определенные задания. Можно искать задание по имени, ключевым словам, описанию или всем этим параметрам.
Задания повышения	Позволяет просматривать повышенные задания.
Состояние повышения	Показывает повышенные задания в соответствии с их состоянием, например, "Выполнено успешно", "Сбой" или "Выполнено частично".

Панель рабочего пространства

На панели рабочего пространства, доступной на домашней странице средства управления повышением, выводится список только что созданных заданий. Панель можно использовать для просмотра имени задания, его состояния и информации о его создании, краткие сведения о повышении, о повышении теста, экраны управления зависимостями, а также для просмотра информации о целевой системе.

Панель дерева

На панели дерева, доступной на домашней странице средства управления повышением, выводится древовидная структура, включающая папки **Задания повышения** и **Состояние повышения**. Только что созданные задания отображаются в иерархической структуре в папке **Задания повышения**. В папке **Состояние повышения** отображаются повышенные задания в соответствии с их состоянием.

Панель деталей

Эта панель также содержит ссылку **Предпочтения**, которая позволяет администратору и пользователям устанавливать предпочтения для этого средства. По ссылкам **Справка** и **О программе** можно получить дополнительные сведения о работе со средством управления повышением.

Корзина покупок и страница средства просмотра заданий

Корзина покупок представляет собой динамически созданное дерево, которое содержит список информационных объектов для повышения. Она также делит информационные объекты по группам пользователей, юниверсам, соединениям и т. д. Страница средства просмотра заданий позволяет просматривать информационные объекты, добавленные в задание.

16.2.3 Использование параметра настройки

Параметр настройки позволяет настраивать параметры до переноса информационных объектов из одной системы SAP BusinessObjects Business Intelligence в другую систему SAP BusinessObjects Business Intelligence и SAP. В этом разделе описано, как использовать параметры настройки.

Выберите раскрывающийся список **Настройка** на экране «Задания повышения». В этом раскрывающемся списке представлены следующие элементы:

- **Управление системами** — позволяет добавить все системы, необходимые для операций управления жизненным циклом.
- **Настройка отката** – позволяет выбрать систему, для которой включен откат.
- **Настройка задания** – позволяет выбрать просмотр завершенных экземпляров на странице "Зависимости", а также управлять операциями очистки экземпляра задания.
- **Настройка CTS** – позволяет добавить информацию о веб-службах и системе SAP BW для интеграции системы Enhanced Change Transport System.
- **Настройка переопределения LCM** – позволяет просматривать, переносить и изменять информацию о соединении базы данных для подключений Crystal Reports и юниверсов. Также здесь можно изменить URL QAAWA.

16.2.3.1 Использование параметра "Управление системами"

В этом разделе описывается использовать параметра "Управление системами". С помощью этой функции можно добавлять и удалять хост-системы.

Чтобы добавить хост-систему, выполните следующие шаги:

1. В окне «Параметры администрирования» нажмите параметр **Управление системами**.

Откроется окно «Управление системами». В этом окне содержится список систем с указанием имени хоста, номера порта, отображаемого имени и описания.

2. Выберите **Добавить**.

Откроется диалоговое окно «Добавить систему».

3. Добавьте имя хоста, номер порта, отображаемое имя и описание в соответствующие поля.

Примечание:

Выберите **Назначить исходной**, чтобы определить систему как исходную, т. е. систему, из которой исходит информация о соединении.

4. Нажмите кнопку **ОК**, чтобы добавить систему.

Хост-система добавляется в список.

Примечание:

Чтобы удалить хост-систему, выберите ее в списке и нажмите кнопку **Удалить**.

См. также

- [Использование параметра настройки отката](#)
- [Использование параметра установки задания](#)

16.2.3.2 Использование параметра настройки отката

Процесс отката включен на уровне системы по умолчанию. Параметр **Настройки отката** позволяет отключить процесс отката на системном уровне.

Для отключения процесса отката на системном уровне выполните следующие шаги:

1. В окне «Откат», в списке базисных систем, выберите базисную систему для отключения процесса отката.
2. Нажмите кнопку **Сохранить и закрыть**, чтобы сохранить изменения.

См. также

- [Использование параметра установки задания](#)

16.2.3.3 Использование параметра установки задания

Параметр "Настройки задания" позволяет указать число экземпляров задания, которые могут существовать в системе. Можно выбрать один из следующих параметров:

- Удалить экземпляры при наличии более чем N экземпляров задания – этот параметр позволяет указать максимальное число экземпляров одного задания, которые могут существовать в системе.
- Удалять экземпляры через N дней – этот параметр позволяет задать удаление всех экземпляров задания, созданных раньше, чем указанное число дней назад.
- В раскрывающемся списке **Показать созданные задания** можно выбрать интервал времени и просмотреть задания, созданные за этот период.

Для установки параметра **Настройки задания** выполните следующие шаги:

1. Выберите параметр и введите требуемое значение.
2. Выберите **Сохранить**, чтобы сохранить обновленные изменения.

Можно выбрать **Установки по умолчанию**, чтобы установить значения по умолчанию, и нажать кнопку **Заккрыть**, чтобы закрыть окно.

Примечание:

Старые экземпляры задания удаляются только при следующем выполнении задания.

См. также

- [Использование параметра системных настроек управления версиями](#)

16.2.3.4 Использование параметра настройки переопределения LCM

Параметр настроек переопределения LCM позволяет повысить уровень переопределения посредством повышения задания или через файлы BIAR.

Примечание:

- Термин "система" используется в следующих процедурах. Существует три типа систем:
 - Исходная: система, которая является исходной для любой информации о соединении.
 - Центральная LCM: система, подключение к которой устанавливается по умолчанию.
 - Целевая: конечная система, в которую выполняется перенос повышаемых ресурсов BI.
- С платформы BI 4.0 SP4 данные переопределения сохраняются в локальной, централизованной базе данных, созданной на компьютере, где выполняется служба PJS. Во избежание повторного ввода данных и противоречивых данных переопределения, получаемых в результате ведения нескольких баз данных, для всех серверов PJS можно задать единственное расположение баз данных переопределения. В СМС на странице «Приложения» щелкните правой кнопкой мыши «Promotion Management» и выберите команду "Параметры переопределения LCM". После отображения списка всех серверов PJS, на которых выполняется служба LCM, убедитесь в совпадении расположения для всех каталогов.

16.2.3.4.1 Повышение переопределений

Добавьте базисную систему перед повышением переопределений. Для получения дополнительных сведений о добавлении базисных систем см. раздел [Использование параметра "Управление системами"](#).

Для повышения переопределений выполните следующие шаги.

1. В окне «Параметры администрирования» нажмите параметр **Настройки переопределений**. Откроется окно «Параметры переопределения».
2. Если вы находитесь в центральной системе управления повышением, выйдите из нее.
3. Нажмите **Вход в систему** для входа в исходную систему. Откроется окно «Вход в систему».

4. Выберите исходную систему, помеченную как **Исходная**, чтобы выполнить сканирование объектов, а затем выполните вход в систему, используя действительные учетные данные.
5. Из раскрывающегося списка **Пуск** рядом с полем **Сканирование** выберите параметр **Пуск**. Начнется процесс сканирования. Откроется «список уникальных соединений».

Примечание:

Чтобы назначить сканирование в предпочтительное время, выберите в раскрывающемся списке вариант **Настройки повторения**.

6. В списке переопределений измените состояние объектов, которые нужно повысить, на "Активен", а затем щелкните **Сохранить**.
7. Нажмите кнопку **Повысить уровень переопределений**.
В месте отображения списка конечных систем отобразится окно «Повысить уровень переопределений».
8. Выберите **Вход**, чтобы войти в систему-адресат, используя действующие учетные данные. Можно указать несколько систем-адресатов.
9. Нажмите кнопку **Повысить**.
Повышение переопределений завершено.

Примечание:

Если при продвижении информационных объектов переопределение завершается со сбоем в целевой системе, для задания будет установлен статус "Частично успешно", а для объекта статус предупреждения "Сбой переопределения".

10. Выйдите из исходной системы.
11. На экране «Переопределение параметров» нажмите кнопку **Вход**.
Будет открыто окно "Вход в систему".
12. Войдите в одну из целевых систем, используя действительные идентификационные данные. Список всех повышенных объектов отображается в «Списке переопределений». Эти задания имеют статус "Неактивное".
13. Установите флажок **Выбрать** для объектов, которые нужно изменить, и нажмите кнопку **Изменить**.
14. Обновите требуемые значения и нажмите кнопку **Готово**.
15. Измените статус объектов на "Активный" и нажмите кнопку **Сохранить**.

16.2.3.4.2 Повышение переопределений с помощью файлов BIAR

Добавьте базисную систему перед повышением переопределений. Для получения дополнительных сведений о добавлении базисных систем см. раздел [Использование параметра "Управление системами"](#).

Чтобы повысить переопределения с помощью файлов BIAR, выполните следующие действия:

1. В окне «Параметры администрирования» нажмите параметр **Настройки переопределений**.
Откроется окно «Параметры переопределения».
2. Если вы находитесь в центральной системе управления жизненным циклом, выйдите из нее.

3. Нажмите **Вход в систему** для входа в исходную систему.
Откроется окно «Вход в систему».
4. В окне «Настройки переопределений» выберите исходную систему, помеченную как **Исходная**, чтобы выполнить сканирование объектов, и войдите в систему, используя действительные учетные данные.
5. Из раскрывающегося списка **Начало** рядом с полем **Сканирование** выберите параметр **Начало**.
Запустится процесс сканирования. Отобразится список переопределений.

Примечание:

Чтобы назначить сканирование в предпочтительное время, выберите в раскрывающемся списке вариант **Настройки повторения**.

6. В списке переопределений измените состояние требуемых объектов на "Активен", а затем щелкните **Сохранить**.
7. Нажмите кнопку **Повысить уровень переопределений**.
Окно «Продвижение переопределений» откроется в месте отображения списка систем-адресатов.
8. Чтобы защитить файл BIAR паролем, отметьте флажок **Защита паролем**.
Поля **Пароль** и **Подтверждение пароля** активированы.
9. Введите пароль в поле **Пароль**. Повторите ввод нового пароля в поле **Подтверждение нового пароля**.
10. Нажмите кнопку **Экспорт** и сохраните файл переопределений BIAR в файловой системе.
11. Войдите в систему назначения посредством средства LCM и выберите **Импорт > Переопределить файл**.
Откроется окно «Импорт файла LCMBIAR».
12. Нажмите **Обзор** для просмотра файла BIAR.
13. Введите пароль к файлу BIAR в поле **Пароль**.

Примечание:

Поле **Пароль** отображается только в случае, если выбранный файл BIAR защищен паролем.

14. Нажмите кнопку **ОК**. Повышение переопределений завершено.
15. Выйдите из исходной системы.
16. На экране «Переопределение параметров» нажмите кнопку **Вход**.
Будет открыто окно «Вход в систему».
17. Выполните вход в систему-адресат, используя действительные учетные данные.
Список импортированных объектов отображается в "Списке переопределений". Состояние этих объектов – "неактивен".
18. Установите флажок **Выбрать** для объектов, которые нужно изменить, и нажмите кнопку **Изменить**. Измененные объекты будут отмечены значком.

Примечание:

Для удаления объектов переопределения нажмите значок.

19. Обновите требуемые значения и нажмите кнопку **Готово**.
20. Измените статус объектов на «Активный» и нажмите кнопку **Сохранить**.

16.2.3.4.3 Повышение переопределений с использованием CTS+

Добавьте базисную систему перед повышением переопределений. Для получения дополнительных сведений о добавлении базисных систем см. раздел [Использование параметра "Управление системами"](#).

Чтобы повысить переопределения через CTS+, выполните следующие шаги:

Примечание:

Чтобы этот параметр стал доступным, запустите средство управления повышением с использованием аутентификации SAP.

1. В окне «Параметры администрирования» нажмите параметр **Настройки переопределений**.
Откроется окно «Параметры переопределения».
2. Если вы находитесь в центральной системе управления жизненным циклом, выйдите из нее.
3. Нажмите **Вход в систему** для входа в исходную систему.
Откроется окно «Вход в систему».
4. Выберите исходную систему, помеченную как **Исходная**, чтобы выполнить сканирование объектов, а затем выполните вход в систему, используя действительные учетные данные.
5. Из раскрывающегося списка **Начало** рядом с полем **Сканирование** выберите параметр **Начало**.
Начнется процесс сканирования. Будет открыт «список переопределений».

Примечание:

Чтобы назначить сканирование в предпочтительное время, выберите в раскрывающемся списке вариант **Настройки повторения**.

6. В списке переопределений измените состояние объектов, которые нужно повысить, на "Активен", а затем щелкните **Сохранить**.
7. Нажмите кнопку **Повысить уровень переопределений**.
Окно «Продвижение переопределений» откроется в месте отображения списка систем-адресатов.
8. В раскрывающемся списке **Параметры повышения** выберите значение **Повышение с использованием CTS+**.
9. Нажмите кнопку **Повысить**.
10. Выпустите переопределения в систему назначения, выполнив следующие шаги:
 - a. Войдите в контроллер домена CTS+ и откройте веб-интерфейс «организатора переносов». Для получения дополнительных сведений об использовании веб-интерфейса организатора переносов см. http://help.sap.com/saphelp_nw70ehp1/helpdata/en/b5/6d03660d3745938cd46d6f5f9cef2e/frameset.htm
 - b. Если запрос имеет статус **Изменяемый**, нажмите кнопку **Выпустить**, чтобы выпустить запрос на перенос переопределений. Для получения дополнительных сведений об

освобождении запросов на перенос с объектами, не связанными с ABAP, см.

http://help.sap.com/saphelp_nw70ehp1/helpdata/en/55/07c497db8140ef8176715d4728eec1/frameset.htm

- c. Закройте веб-интерфейс пользователя «организатора переносов».

11. Импортируйте переопределения в систему назначения, выполнив следующие шаги:

- a. Выполните вход в контроллер домена CTS+.
- b. Вызовите транзакцию STMS, чтобы выполнить вход в систему управления переносами.
- c. Щелкните по значку **Обзор импорта**.

Откроется окно «Обзор импорта», и можно будет просмотреть элементы в очереди на импорт из всех систем.

- d. Щелкните по идентификатору системы-адресата LCM.
Можно просмотреть список запросов на перенос, которые можно импортировать в систему.
- e. Нажмите кнопку **Обновить**.
- f. Импортируйте соответствующие запросы на перенос. Для получения дополнительных сведений см.

http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a39e7acc11d1899e0000e829fbbd/frameset.htm.

12. Повышение переопределений завершено.

13. Войдите в одну из целевых систем, используя действительные идентификационные данные.
Список всех повышенных объектов будет отображен в поле "Список переопределений". Эти задания имеют статус "Неактивное".

14. Установите флажок **Выбрать для объектов, которые нужно изменить, и нажмите кнопку **Изменить**.**

15. Обновите требуемые значения и нажмите кнопку **Готово.**

16. Измените статус объектов на "Активный" и нажмите кнопку **Сохранить.**

16.2.3.5 Использование параметра настройки CTS

Этот параметр можно использовать для добавления веб-служб и управления системами BW в ИТ-ландшафте. См. в разделе [Настройка параметров CTS+ при помощи средства управления повышением](#) дополнительную информацию по использованию параметра настройки CTS и настройке CTS для использования с приложением управления повышением.

16.3 Использование средства управления повышением

При запуске приложения управления повышением, по умолчанию открывается страница «Задания повышения ».

Экран домашней страницы «Задания повышения» содержит различные вкладки, которые позволяют выполнять следующие задачи:

- Выберите **Создать задание**, чтобы выбрать связанные с заданием процессы. Также можно щелкнуть правой кнопкой мыши экран домашней страницы и выбрать связанные с заданием процессы из списка.
- Выберите **Импорт > Импортировать файл**, чтобы импортировать файл BIAR или LCMBIAR напрямую из файловой системы и не выполнять полную процедуру создания нового задания.
- Для импорта файлов переопределения перейдите по меню **Импорт > Файл переопределения**.
- Выберите **Изменить**, чтобы изменить существующие задания.
- Выберите **Повысить**, чтобы повысить задание из исходной системы в целевую систему, или экспортировать задание в файл BIAR.
- Выберите **Откат**, чтобы отменить повышение заданий в целевую систему.
- Выберите **Журнал**, чтобы просмотреть предыдущие экземпляры повышения задания.
- Выберите **Свойства**, чтобы просмотреть свойства выбранного экземпляра задания, например заголовок, идентификатор, имя файла, описание и т. д.

Область приложения «Задания повышения» отображает список заданий, существующих в системе, вместе со следующей информацией о каждом задании:

- **Имя:** имя созданного задания.
- **Статус:** статус задания, например "Создано", "Успешно", "Частично успешно", "Выполняется" или "Сбой".
- **Создано:** дата и время создания задания.
- **Последний запуск:** дата и время последнего повышения задания.
- **Исходная система:** имя системы, из которой повышается задание.
- **Целевая система:** имя системы, в которую повышается задание.
- **Автор:** имя пользователя, создавшего конкретное задание.

Примечание:

В приложении управления повышением для всех операций используется SDK платформы SAP BusinessObjects Business Intelligence.


16.3.1 Создание и удаление папки

Этот раздел описывает процесс создания и удаления папки на домашней странице заданий повышения.

16.3.1.1 Создание папки

Этот раздел описывает процесс создания папки.

Чтобы создать папку, выполните следующие шаги:

1. На панели инструментов управления повышением нажмите  .
2. В диалоговом окне «Создать папку» введите имя папки.
3. Нажмите кнопку **ОК**.

Создана новая папка.


См. также

- [Создание задания](#)
- [Удаление папки](#)

16.3.1.2 Удаление папки

Этот раздел описывает процесс удаления папки.

Для удаления папки выполните следующие шаги:

1. Выберите папку или задание на домашней странице «Задания повышения».
2. Щелкните  .

Откроется диалоговое окно «Удалить».

3. Нажмите кнопку **ОК**.

Выбранная папка удалена.

См. также

- [Создание задания](#)

16.3.2 Создание задания

В этом разделе описывается процесс создания нового задания с использованием средства управления повышением.

В следующей таблице представлены элементы GUI и поля, которые можно использовать для создания нового задания:

Поле	Описание
Имя	Имя задания, которое требуется создать.
Описание	Описание задания, которое требуется создать.
Ключевые слова	Ключевые слова для содержания задания, которое требуется создать.
Сохранить задание в	Отображается папка, выбранная по умолчанию.
Исходная система	Имя системы платформы SAP BusinessObjects Business Intelligence, из которой требуется повысить задание.
Целевая система	Имя системы платформы SAP BusinessObjects Business Intelligence, в которую требуется повысить задание.
Имя пользователя	Идентификатор входа в систему, который требуется использовать для входа в исходную или целевую систему.
Пароль	Пароль, который требуется использовать для входа в исходную или целевую систему.
Аутентификация	<p>Тип аутентификации, используемый для входа в исходную или целевую систему.</p> <p>Средство управления повышением поддерживает следующие типы аутентификации:</p> <ul style="list-style-type: none"> • Enterprise • Windows AD • LDAP (облегченный протокол доступа к каталогу) • SAP

Примечание:

Перед созданием задания убедитесь, что все переопределения изменены и обновлены в системе назначения и содержимое платформы BI автоматически обновлено. Для получения дополнительных сведений см. раздел "Использование параметра настройки переопределения".

Для создания нового задания с помощью средства управления повышением выполните следующие действия:

1. Запустите средство управления повышением.
2. На домашней странице «Задания повышения» нажмите вкладку **Создать задание**.
3. Введите имя, описание и ключевые слова задания в соответствующих полях.

Примечание:

Необязательно предоставлять информацию в полях "Описание", "Ключевые слова" и "Целевая система".

4. В поле **Сохранить задание как** просмотрите папки и выберите ту, в которой требуется сохранить задание.

Примечание:

По умолчанию в поле **Сохранить задание в...** подставляется имя папки, выделенной в области папок перед выбором команды **Создать задание**.

5. В раскрывающемся списке **Выбор зависимых объектов** выберите параметры добавления зависимых элементов в задание. Следует явным образом указать зависимые объекты, которые требуется повысить. Например, если выбрать "Все юниверсы" в раскрывающемся списке "Выбор зависимых объектов", будут отображены все юниверсы из списка зависимых объектов. Затем можно выбрать зависимые объекты по отдельности.
6. Выберите исходную и целевую систему из соответствующих раскрывающихся списков.
Если имя системы отсутствует в раскрывающемся списке, нажмите параметр **Войти в новый CMS**. Запускается новое окно. Введите имя системы с именем пользователя и паролем.
7. Нажмите кнопку **Создать**.

Новое созданное задание хранится в репозитории CMS в исходной системе.

Примечание:

Если создается задание с папкой в качестве главного объекта, а задание является повторяющимся, задание будет включать любое содержимое, добавленное в папку во время следующего выполнения.

См. также

- [Использование параметра настройки переопределения LCM](#)

16.3.2.1 Вход в новый CMS

Этот раздел описывает, как войти в новый CMS.

Чтобы войти в новый CMS, выполните следующие шаги:

1. Запустите приложение управления повышением.
2. Создайте новое задание.

Для получения дополнительных сведений о создании нового задания см. [Создание задания](#)

3. В раскрывающемся списке **Исходная система** выберите **Выполнить вход в новую CMS**.
Откроется диалоговое окно «Вход в систему».
4. Введите реквизиты пользователя, выберите соответствующий тип аутентификации и нажмите кнопку **Вход в систему**.

5. В раскрывающемся списке **Целевая система** выберите **Вход в новую CMS**.
6. Введите учетную запись и пароль пользователя, выберите соответствующий тип аутентификации и выберите **Вход**.

См. также

- [Изменение задания](#)
- [Добавление информационных объектов в управление повышением](#)
- [Повышение задания при соединении с репозиториями](#)
- [Планирование повышения задания](#)

16.3.3 Создание нового задания путем копирования существующего

В этом разделе описан процесс создания нового задания путем копирования существующего.

Для создания нового задания путем копирования существующего выполните следующие шаги:

1. Запустите приложение управления повышением.
2. На домашней странице «Задания повышения» выберите **Создать задание**.
3. Нажмите параметр **Копировать существующее задание**.

Появится окно «Копия существующего задания», где отображается список заданий в папке **Задания повышения**.

4. Выберите в списке требуемое задание и нажмите кнопку **Создать**.

Отображаются имя, ключевые слова и описание задания. При необходимости эти поля можно изменить. Однако изменение имени исходной системы не допускается.

5. В поле **Сохранить задание в** выберите папку, в которой необходимо сохранить задание, и нажмите кнопку **Создать**.

Создано новое задание, откроется страница «Добавить объекты – имя задания».

См. также

- [Добавление информационных объектов в управление повышением](#)
- [Изменение задания](#)
- [Повышение задания при соединении с репозиториями](#)

16.3.4 Поиск задания

Функция поиска средства управления повышением используется для поиска задания, которое доступно в репозитории.

Для поиска задания выполните следующие действия:

1. В поле **Поиск** на домашней странице введите текст, который требуется найти.
2. Нажмите на список, открывающийся рядом с полем **Поиск**, чтобы указать параметры поиска. Можно указать следующие параметры поиска:
 - Найти заголовок – этот параметр позволяет искать задание по имени.
 - Найти ключевое слово – этот параметр позволяет искать задание по ключевым словам.
 - Найти описание – этот параметр позволяет искать задание по описанию.
 - Найти все поля – этот параметр позволяет искать задание по заголовку, ключевым словам и описанию.
3. Щелкните значок поиска.

См. также

- [Добавление информационных объектов в управление повышением](#)
- [Изменение задания](#)

16.3.5 Изменение задания

В этом разделе описывается процесс изменения задания.

Примечание:

Изменение задания не является созданием нового задания.

Чтобы изменить задание, выполните следующие шаги:

1. Запустите приложение управления повышением.
2. На домашней странице «Задания повышения» выберите задание, которое требуется изменить.
3. Щелкните **Изменить**.

Появится подробная информация о выбранном задании. В зависимости от требований можно добавлять или удалять информационные объекты, управлять зависимостями или повышать задания.

Во время изменения задания имя исходной системы не может быть изменено.

См. также

- [Добавление информационных объектов в управление повышением](#)
- [Повышение задания при соединении с репозиториями](#)
- [Планирование повышения задания](#)

16.3.6 Добавление информационных объектов в управление повышением

Каждое задание должно содержать набор информационных объектов и их зависимые объекты. Поэтому следует добавлять информационные объекты в задание до передачи его в целевую систему.

Примечание:

При повышении отчета Crystal на основе InfoObjects Business View (соединение данных, основание данных, бизнес-элементы и бизнес-представление) необходимо включить данные безопасности (право DataAccess в соединении данных и право ViewDataField в основании данных и бизнес-элементах) для просмотра данных в отчете в системе назначения.

Примечание:

При добавлении информационных объектов в задание необходимо выполнить вход в целевую систему.

Для добавления информационного объекта в задание выполните следующие шаги:

1. Запустите средство управления повышением.
2. Создайте новое задание.
Сведения о создании нового задания см. в разделе [Создание задания](#)
3. Щелкните **Добавить объекты**.
Откроется диалоговое окно «Добавить объекты» со списком объектов.
4. Перейдите к папке, в которой требуется выбрать инфообъект.
В выбранной папке появится список информационных объектов.
5. Выберите информационный объект, который требуется добавить в задание, и нажмите кнопку **Добавить**.
Если требуется добавить информационный объект и выйти из диалогового окна «Добавить объекты – имя исходной системы», выберите **Добавить и закрыть**. Информационный объект добавлен к заданию, диалоговое окно «Добавить объекты – имя исходной системы » будет закрыто.

После добавления объекта InfoObject в задание можно щелкнуть правой кнопкой мыши страницу «Средство просмотра заданий» и выберите связанные с заданием процессы для повышения. Объектами, зависимыми от объекта InfoObject, выбранного с помощью параметра **Управление зависимостями** в окне «Средство просмотра заданий», можно управлять.

Примечание:

- В корзине покупок, которая отображается на левой панели страницы «Средство просмотра заданий», показано задание вместе с зависимыми элементами в виде простой древовидной структуры.

- Для сохранения изменений нажмите кнопку **Сохранить** после добавления информационных объектов. В противном случае пользователю предлагается сохранить задание при закрытии вкладки.

Передовая практика: для оптимальной производительности средства управления повышением рекомендуется выбирать для повышения небольшое количество информационных объектов, не более 100 одновременно.

См. также

- [Управление зависимостями в приложении управления повышением](#)
- [Повышение задания при соединении с репозиториями](#)
- [Планирование повышения задания](#)

16.3.7 Управление зависимостями в приложении управления повышением

Этот раздел описывает процесс управления зависимыми объектами информационного объекта.

Чтобы управлять зависимыми объектами информационного объекта, выполните следующие шаги:

1. Запустите средство управления повышением.
2. Создайте новое задание.

Для получения сведений о создании нового задания см. [Создание задания](#).


3. Добавьте требуемые информационные объекты в новое задание.
Появится экран «Задания повышения».

4. Выберите **Управление зависимостями**.

Появится окно «Управление зависимостями». В этом окне представлен список информационных объектов и их зависимых объектов. Для просмотра только невыбранных зависимых объектов установите флажок **Показать невыбранные зависимые объекты**.

5. В раскрывающемся списке **Выбор зависимых объектов** выберите параметры добавления зависимых элементов в задание. Зависимые объекты не выбираются по умолчанию; необходимо явно выбрать зависимые элементы, которые требуется повысить.

Например, при выборе **Все юниверсы** в раскрывающемся списке **Отображение только невыбранных зависимых объектов** будут выбраны все юниверсы, включенные в список зависимых объектов. Также можно выбирать зависимые объекты по отдельности.

Для просмотра поддерживаемых параметров фильтрации информационных объектов щелкните **Тип** . Появится раскрывающийся список. Этот список содержит поддерживаемые параметры фильтрации. Выберите параметр фильтрации и нажмите кнопку **ОК**. Появятся отфильтрованные информационные объекты.

При выборе зависимых объектов в столбце **Зависимые объекты** зависимые объекты автоматически перемещаются в столбец **Объекты в задании**.

Также можно набрать имя зависимого объекта в поле **Искать зависимые объекты**, чтобы найти зависимый объект.

Более подробную информацию о поиске зависимых объектов см. в [Поиск зависимых объектов](#).

6. Нажмите кнопку **Применить изменения**, чтобы обновить список зависимых объектов, и выберите **Принять изменения и закрыть**, чтобы сохранить изменения.

Зависимые объекты рассчитываются средством автоматически. Эти зависимые объекты рассчитываются на базе отношений информационных объектов или свойств информационных объектов. Зависимые объекты, не соответствующие ни одному из этих условий, в этой версии средства не рассчитываются.

Примечание:

Если выбрана папка для повышения, содержащиеся в ней объекты рассматриваются как основные ресурсы.

См. также

- [Повышение задания при соединении с репозиториями](#)

16.3.8 Поиск зависимых объектов

Функция расширенного поиска в средстве управления повышением позволяет находить зависимые объекты информационных объектов, доступных в репозитории.

Для поиска зависимых объектов информационного объекта выполните следующие действия:

1. Запустите приложение управления повышением.
2. Создайте новое задание или измените существующее.

Если создано новое задание, добавьте в него информационные объекты. Если выполняется изменение существующего задания, в него при необходимости можно добавить объекты.

3. Щелкните **Управление зависимостями**.
4. В поле **Искать зависимые объекты** введите имя зависимого объекта, который требуется разместить.
5. Щелкните значок поиска.

См. также

- [Управление зависимостями в приложении управления повышением](#)

16.3.9 Повышение задания при соединении с репозиториями

В этом разделе описывается процесс повышения задания из исходной в целевую систему при подключенных репозиториях.

В следующей таблице содержится список типов информационных объектов, которые можно повышать с помощью средства управления повышением:

Категория	Типы объектов, которые можно повысить
Отчеты	Отчеты Crystal, Web Intelligence, Dashboards, QaaWS, Explorer
Сторонние объекты	RTF, текстовый документ, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Flash, Adobe Acrobat
Пользователи	Пользователи и группы пользователей
Сервер	Группы серверов
Платформа Business Intelligence	Папка, программа, события, профили, пакет объектов, гиперссылка, категории, предупреждения, документ папки "Входящие", персональная папка и папка "Избранное"
Юниверс, рабочее пространство	Юниверсы (UNV), соединения
Информационная панель EPM	Юниверсы, соединения, отчеты, информационная панель и аналитика
Бизнес-представление	Фонд данных
Интеграция <ul style="list-style-type: none"> Список тиражирования Задания на тиражирование 	Список тиражирования обеспечивает повышение следующих объектов: Flash, .txt, дискуссии, Dashboards, .pdf, гиперссылка, .xls, пакет объектов, Crystal Reports, документы Web Intelligence, юниверсы, программа, соединения, DataFoundation, бизнес-представления, .rtf, профиль, событие, пользователи и группы пользователей. Соединения для тиражирования обеспечивают повышение заданий тиражирования, удаленного соединения, публикаций, дискуссии, соединения Pioneer
Службы BI	Документы Web Intelligence, юниверсы и соединения
Новые информационные объекты	Отчеты Crystal (rpt/rptr), Pioneer, Dashboard Design, DSL Universe (UNX), WEBI, Explorer, Data Federator, Data Steward, BI Workspace и т. д.

Чтобы повысить уровень задания, выполните следующие шаги:

1. Запустите приложение управления повышением.
2. На домашней странице «Задания повышения» выберите задание, которое требуется повысить. Также можно щелкнуть правой кнопкой мыши экран домашней страницы и выбрать команду **Повысить**.
3. В раскрывающихся списках **Источник** и **Место назначения** выберите исходную и целевую системы.

Примечание:

Прежде, чем продолжать процесс повышения, убедитесь, что выполнен вход в исходную и целевую системы.

4. В поле **Идентификатор управления изменениями** введите соответствующее значение и нажмите кнопку **Сохранить**.

Примечание:

Идентификатор управления изменениями используется для получения информации о регистрации, аудите, журнале задания и пр. Средство управления повышением позволяет сопоставить каждый экземпляр создания задания с идентификатором управления изменениями. Идентификатор управления изменениями устанавливается пользователем в определении задания при создании нового задания. Средство автоматически создает идентификатор для каждого задания.

5. При необходимости выберите **Настройки безопасности**. Будут отображены следующие параметры:
 - Не повышать безопасность – это параметр по умолчанию.
 - Повысить безопасность – используйте этот параметр для повышения заданий вместе с соответствующими правами безопасности.
 - Повысить безопасность объекта – используйте этот параметр для повышения безопасности объектов и папок.
 - Повысить безопасность пользователя – позволяет повысить права пользователей, участвующих в задании.
 - Включить права приложения – этот параметр можно выбрать, только если выбран параметр **Повысить безопасность**. Если объекты задания наследуют какие-либо права приложения, задание повышается вместе с этими правами.

Также можно выбрать **Права просмотра** для просмотра зависимостей безопасности информационных объектов задания.

6. Выберите **Проверить повышение**, чтобы убедиться в отсутствии конфликтов между идентификаторами CUID информационных объектов исходной и целевой системах. Сведения о повышении отображаются на вкладках **Выполнено успешно**, **Сбой** и **Внимание**. В первом столбце отображаются объекты для повышения, а во втором – состояние повышения каждого информационного объекта. В средстве управления повышением выбранные объекты разделяются на пользователей, группы, юниверсы и т. д.

Примечание:

Этот параметр не передает какие-либо информационные объекты на повышение.

Результатом тестирования повышения может быть один из следующих вариантов:

- Перезаписан – информационный объект в конечной системе перезаписан информационным объектом в исходной системе.
 - Скопирован – информационный объект исходной системы скопирован в целевую систему.
 - Оставлен – информационный объект не повышен из исходной системы в целевую.
 - Предупреждение – информационный объект целевой системы имеет более новую версию и может удалить информационный объект из задания. Однако если требуется, информационный объект будет повышен.
7. Нажмите кнопку **Планировать задание**, если требуется запланировать повышение экземпляра задания.
8. Нажмите кнопку **Повысить**.
Выбранное задание повышено.

Если повышать задание не требуется, можно использовать параметр **Сохранить**, чтобы сохранить изменения, такие как настройки безопасности, идентификатора управления изменениями и планирования.

16.3.10 Повышение задания с помощью файла BIAR

Повышение относится к активности передачи источника BI из одного репозитория в другой. Если между исходной и целевой системой установлено соединение, средство управления повышением передает информационный объект через локальную или глобальную сеть. Однако средство управления повышением поддерживает повышение информационных объектов даже при отсутствии соединения между исходной и целевой системами.

На случай отсутствия соединения между исходной и целевой системами средство управления повышением поддерживает перенос заданий в целевую систему путем экспорта задания из исходной системы в файл BIAR и последующего импорта того же задания из файла BIAR в целевую систему.

В этом разделе описывается выполнение экспорта задания в файл BIAR и импорт задания из файла BIAR в целевую систему.

Примечание:

Не допускается использовать файл BIAR, созданный с помощью инструмента "Мастер импорта".

См. также

- [Экспорт задания в файл BIAR](#)
- [Импорт задания из файла BIAR](#)

16.3.10.1 Экспорт задания в файл BIAR

Этот раздел описывает экспорт задания в файл BIAR.

Чтобы экспортировать задание в файл BIAR, выполните следующие шаги:

1. Запустите приложение управления повышением и создайте новое задание.
Для получения дополнительных сведений о создании нового задания см. [Создание задания](#)
2. В раскрывающемся списке **Место назначения** выберите пункт **В файл LCMBIAR** и нажмите кнопку **Создать**.
3. Выберите **Добавить объекты**, чтобы добавить в задание информационные объекты.
Можно использовать параметр **Управление зависимостями**, чтобы управлять зависимостями выбранного задания.
4. Выберите **Повысить**.
Откроется окно «Повысить уровень».
5. Измените эти параметры в соответствии с текущими требованиями и нажмите кнопку **Экспорт**.
Создан файл BIAR. Можно сохранить файл BIAR в файловой системе или на FTP.
6. В раскрывающемся списке **Место назначения** выберите пункт **В файл LCMBIAR** и нажмите кнопку **Место назначения файла LCMBIAR**.
Откроется панель **Место назначения файла LCMBiar**.
7. Выполните одно из следующих действий:
 - Выберите **Файловая система**.
 - Выберите **FTP** и введите соответствующие значения в полях хоста, порта, имени пользователя, пароля, каталога и имени файла.
8. Чтобы защитить файл LCMBIAR паролем, отметьте флажок **Защита паролем**.
9. Введите пароль в поле **Пароль**.
10. Повторно введите пароль в поле **Подтверждение пароля**.
11. Нажмите кнопку **Экспорт**.
Файл BIAR будет экспортирован в файловую систему или на сайт FTP, в зависимости от того, какой вариант был выбран на шаге 7.
12. Можно запланировать экспорт задания в файл BIAR. Для получения дополнительных сведений см. раздел [Планирование повышения задания](#).

См. также

- [Добавление информационных объектов в управление повышением](#)
- [Управление зависимостями в приложении управления повышением](#)

16.3.10.2 Импорт задания из файла BIAR

Задания можно импортировать из традиционных файлов BIAR или из файла LCMBIAR. Файл BIAR копируется из устройства хранения в целевую систему.

Чтобы импортировать файл BIAR, выполните следующие действия:

1. Запустите приложение управления повышением.
2. На домашней странице «Задания повышения» выберите **Импорт > Импорт файла**.
Откроется окно «Импорт из файла».
3. Файл BIAR можно импортировать с локального компьютера или с любого другого исходного компьютера.

- Для импорта файла BIAR с локального компьютера выполните следующие действия:
 - a. Выберите **файловую систему**.
 - b. Нажмите кнопку **Обзор** и выберите файл BIAR в файловой системе.

Примечание:

Если существует задание с этим именем, появится всплывающее окно подтверждения сохранения. Для перезаписи существующего задания нажмите "Да". Для создания задания с новым CUID и именем Имя_задания_копия нажмите "Нет".

- c. В поле **Пароль** введите пароль для файла LCMBIAR.

Примечание:

Поле "Пароль" отображается только в случае, если файл LCMBIAR защищен паролем.

- d. Нажмите кнопку **Создать**. Задание создано.

- Для импорта файла BIAR с любого исходного компьютера, на котором включен FTP, выполните следующие действия:
 - a. Выберите **FTP**.
 - b. Введите в соответствующие поля информацию о хосте, порте, имени пользователя, пароле, каталоге и имени файла и нажмите **ОК**.

Примечание:

Можно импортировать только файлы LCMBIAR или обновить файлы BIAR.

4. Нажмите кнопку **Повысить**.
Появится окно «Повысить – имя задания».
5. Выберите целевую систему в раскрывающемся списке **Место назначения**. Если был выбран параметр **Вход в новую систему CMS**, будет предложено ввести учетные данные. Подтвердите учетную запись и пароль пользователя в целевой системе.
6. Выберите **Повысить**, чтобы повысить содержимое в целевую систему.

Также можно нажать параметр **Проверить повышение**, чтобы просмотреть объекты к повышению и состояние повышения.

См. также

- [Управление зависимостями в приложении управления повышением](#)

16.3.11 Планирование повышения задания

Этот раздел описывает процесс планирования повышения экземпляра задания. В нем также описано, как указать параметры периодичности.

Чтобы спланировать повышение экземпляра задания, выполните следующие шаги:

1. В диалоговом окне «Повышение» выберите параметр **Расписание**.
2. Установите требуемое значение параметра планирования и нажмите **Запланировать**.

Если добавить инфо-объекты в существующую папку после планирования повышения задания, эти объекты также будут перенесены в место назначения в установленное время.

Планирование в место назначения возможно при экспорте задания в файл BIAR.

Совет:

Когда повышение инфо-объекта завершится, можно будет просмотреть все запущенные экземпляры данного инфо-объекта. Для этого щелкните объект правой кнопкой мыши и выберите **История**.

Повышение задания может также произойти на основе триггеров событий.

Для каждого статуса повышения задания (например, успешно/частично успешно/сбой) можно выбрать уведомление по электронной почте. Для получения дополнительных сведений о различных параметрах планирования и о настройке уведомлений см. раздел "Планирование".




См. также

- [Экспорт задания в файл BIAR](#)

16.3.11.1 Обновление повторяющихся и ожидающих экземпляров повышения заданий

При использовании средства управления повышением можно отслеживать и обновлять статус планового повышения экземпляра задания с помощью параметра **Повторяющиеся и ожидающие экземпляры**.

Для отслеживания и обновления экземпляров запланированного повышения задания, выполните следующие шаги.

1. Запустите средство управления повышением.
2. На домашней странице «Задания повышения» выберите задание.
3. Нажмите кнопку **Журнал**.
Откроется окно «Журнал задания».
4. Щелкните **Повторяющиеся и ожидающие экземпляры**.
Откроется окно «Журнал повторяющихся заданий и ожидающих обработки экземпляров». В этом окне отображается список повторяющихся и ожидающих экземпляров повышения задания.
В зависимости от ваших требований можно использовать следующие параметры:
 - Выберите **Повысить экземпляры**, чтобы просмотреть список экземпляров планового повышения задания.
 - Выберите параметр **Пауза**, чтобы прервать плановое повышение.
 - Выберите параметр **Продолжить**, чтобы возобновить прерванный экземпляр планового повышения задания.
 - Выберите параметр **Изменить расписание**, чтобы повторно спланировать экземпляр повышения задания.
 - Выберите , чтобы удалить плановый экземпляр повышения задания.
 - Выберите , чтобы обновить статус планового экземпляра повышения задания.
 - Этот параметр  можно использовать для перехода на отдельную страницу или на определенную страницу путем ввода соответствующего номера страницы.

Примечание:

Столбец статуса в окне «Журнал повторяющихся заданий и ожидающих обработки экземпляров» отображает статус экземпляра повышения задания, например повторяющийся, ожидающий обработки и т. д.

См. также

- [Откат задания](#)

16.3.12 Просмотр журнала задания

В этом разделе описывается процесс просмотра журнала заданий.

Примечание:

Чтобы просмотреть журнал задания, следует убедиться, что задание имеет один из следующих статусов:

- Успешно
- Сбой
- Частично выполнено

Чтобы просмотреть журнал задания, выполните следующие шаги:

1. Запустите средство управления повышением.
Откроется домашняя страница «Задания повышения».
2. Выполните любую из следующих операций:
 - Щелкните правой кнопкой мыши задание, историю которого требуется просмотреть, и выберите команду **История**.
 - Выберите задание, историю которого требуется просмотреть, и нажмите на вкладку **История**.

Появится следующая информация: экземпляр задания, имя задания, имена исходной и целевой систем, идентификатор пользователя, повысившего задание, статус ("Выполнено успешно", "Сбой" или "Выполнено частично").

Статус задания можно просмотреть с помощью ссылки, отображенной в столбце **Статус**.

16.3.13 Откат задания

Параметр "Откат" позволяет восстановить целевую систему в ее предыдущем состоянии после повышения задания.

Для отката задания выполните следующие шаги:

1. Запустите средство управления повышением.
Откроется домашняя страница «Задания повышения».
2. Выполните любую из следующих операций:
 - Щелкните правой кнопкой мыши задание, откат которого требуется выполнить, и выберите команду **Откат**.
 - Выберите задание, которое требуется откатить, и нажмите на вкладку **Откат**.Откроется окно «Откат».
3. Выберите задание, которое требуется откатить, и нажмите кнопку **Полный откат**.
Будет выполнен откат задания.

Можно выполнить откат только самого последнего экземпляра повышения задания. Не допускается выполнение отката двух экземпляров задания одновременно.

16.3.13.1 Использование параметра частичного отката

Средство управления повышением позволяет выполнить полный или частичный откат информационных объектов задания из целевой системы.

Чтобы выполнить частичный откат информационных объектов, выполните следующие шаги:

1. Запустите средство управления повышением.
Откроется домашняя страница «Задания повышения».
2. Выполните любую из следующих операций:
 - Щелкните правой кнопкой мыши задание, откат которого требуется выполнить, и выберите команду **Откат**.
 - Выберите задание, которое требуется откатить, и нажмите на вкладку **Откат**.Откроется окно «Откат».
3. Выберите задание из списка и нажмите кнопку **Частичный откат**.
Список информационных объектов в выбранном задании появится на странице «Средство просмотра заданий».
4. Выберите информационные объекты, для которых требуется выполнить откат, и нажмите кнопку **Откат**.

Примечание:

Убедитесь, что выполнен откат всех объектов задания, прежде чем выполнять откат информационных объектов в следующем задании.

Важно: если задание повышается с применением настроек безопасности, то в процессе частичного отката информационных объектов выбранные зависимые информационные объекты могут не получить предшествующего состояния безопасности, которое было до осуществления отката.

См. также

- [Управление разными версиями ресурсов VI](#)

16.3.13.2 Откат задания по истечению срока действия пароля

В этом разделе описывается процесс отката задания после того, как истек срок действия пароля, использованного для повышения.

Чтобы откатить задание по истечению срока действия пароля, выполните следующие шаги:

1. Выберите задание, которое требуется откатить, и нажмите кнопку **Откат**.
2. В окне «Откат» выберите **Полный откат**.
Появится сообщение об ошибке. Это сообщение уведомляет о невозможности откатить данное задание. Также пользователю будет предложено войти в исходную или целевую систему.
3. Введите новые реквизиты для входа и выберите **Вход в систему**.

Откроется диалоговое окно с сообщением о завершении процесса отката.

Примечание:

Задания, повышенные с помощью входных данных исходной или целевой системы, обновляются автоматически.

См. также

- [Откат информационных объектов по истечении срока действия пароля](#)
- [Использование параметра частичного отката](#)

16.3.13.2.1 Откат информационных объектов по истечении срока действия пароля

В этом разделе описывается процесс отката информационных объектов после того, как истек срок действия пароля исходной или целевой системы.

Чтобы откатить информационные объекты по истечении срока действия пароля, выполните следующие шаги:

1. Выберите задание, которое требуется откатить, и нажмите кнопку **Откатить**.

Откроется окно «Откат».

2. Выберите параметр **Частичный откат**.

Появится сообщение об ошибке. Это сообщение говорит о том, что откат информационных объектов не может быть выполнен. Также пользователю будет предложено войти в исходную или целевую систему.

3. Введите новые реквизиты для входа и выберите **Вход в систему**.

Откроется страница «Средство просмотра задания». На этой странице представлен список информационных объектов.

4. Выберите требуемые информационные объекты и нажмите кнопку **Откат**.

Примечание:

Задания, которые были повышены с помощью учетной записи исходной или целевой системы, обновляются автоматически.

См. также

- [Откат задания](#)
- [Использование параметра частичного отката](#)
- [Откат задания по истечению срока действия пароля](#)

16.4 Управление разными версиями объекта InfoObject

Приложение управления версиями позволяет управлять версиями ресурсов BI, которые находятся в репозитории платформы SAP BusinessObjects Business Intelligence. Консоль поддерживает


системы управления версиями Subversion и ClearCase. В этом разделе описывается использование функции управления версиями в консоли управления жизненным циклом.

Для создания версий информационного объекта и управления ими выполните следующие действия:

1. Запустите приложение управления повышением.
2. На домашней странице выберите в раскрывающемся списке **Управление версиями**.
Будет открыто диалоговое окно «Войти в систему».
3. Введите данные для входа и нажмите кнопку **Вход в систему**.
Откроется окно «Управление версиями».

Примечание:

В систему управления версиями (VMS) можно войти только в том случае, если она уже настроена.

4. Если требуется изменить хост-систему, щелкните  .
Откроется диалоговое окно «Вход в систему».
5. Введите данные для входа и нажмите кнопку **Вход в систему**.
6. В левой панели окна «Управление версиями» выберите папку, чтобы просмотреть информационные объекты, версиями которых требуется управлять.
7. Выберите информационные объекты и нажмите кнопку **Добавить в VM**.

Примечание:

Нажатие «Добавить в управление версиями» приведет к созданию базовой версии объекта в репозитории VMS. Базовая версия требуется для последующей регистрации.

8. Нажмите кнопку **Возврат**, чтобы обновить документ, существующий в репозитории VMS.
Откроется диалоговое окно «Комментарии регистрации».
9. Введите свои комментарии и нажмите кнопку **ОК**.
Изменение номера версии выбранного информационного объекта отображается в столбцах VMS и CMS.
10. Чтобы получить последнюю версию документа из VMS, выберите требуемый информационный объект и щелкните **Получить последнюю версию**.
11. Чтобы создать копию последней версии, нажмите кнопку **Создать копию**.
Создана копия выбранной версии.
12. Выберите **Журнал**, чтобы просмотреть все версии, доступные в выбранном ресурсе.
Откроется окно «Журнал». Будут отображены следующие возможные действия:
 - **Получить версию** – при наличии нескольких версий и, если требуется определенная версия ресурса BI, можно выбрать требуемый ресурс и нажать **Получить версию**.
 - **Получить копию версии** – позволяет получить копию выбранной версии.
 - **Экспорт копии версии** – этот параметр позволяет получить копию выбранной версии и сохранить ее в локальной системе.

13. Выберите информационный объект и нажмите кнопку **Блокировать**, чтобы заблокировать информационный объект, и кнопку **Разблокировать**, чтобы разблокировать информационный объект.

Примечание:

Если информационный объект заблокирован, с ним невозможно выполнять никаких действий.


14. CMS и синхронизация VMS – при обновлении версии CMS информационного объекта рядом с обновленным информационным объектом появляется индикатор. Если поместить курсор на этот индикатор, появится всплывающая подсказка с сообщением, что информационный объект CMS изменен.

15. Чтобы просмотреть список всех зарегистрированных ресурсов, существующих в VMS, но не в CMS, выберите **Просмотреть удаленные ресурсы**.

Для просмотра истории любого удаленного ресурса щелкните этот ресурс. Для просмотра версии удаленного ресурса выберите удаленный ресурс и нажмите **Получить версию**. Для получения копии выбранного ресурса нажмите **Получить копию версии**.

Примечание:

При использовании параметра **Получить версию** или **Получить копию версии** ресурс перемещается в CMS из списка отсутствующих файлов VMS.

16. Выберите ресурс и выберите  , чтобы просмотреть свойства ресурса. Вместо этого можно щелкнуть информационный объект правой кнопкой мыши и выполнить шаги с 4 по 16.

16.4.1 Права доступа к приложению управления версиями

В этом разделе описаны права доступа к приложению управления версиями.

- Консоль СМС позволяет задавать права доступа к приложению управления версиями.
- Для разных функций в приложении управления версиями можно задавать разные права доступа в приложении.

Чтобы задать особые права в приложении управления версиями, выполните следующие действия.

1. Войдите в СМС и выберите **Приложения**.
2. Дважды щелкните **Управление версиями**.
3. Щелкните **Безопасность пользователей** и выберите пользователя. Можно просмотреть и присвоить права доступа для выбранного пользователя.
4. На данный момент доступны следующие особые права для управления версиями:
 - Разрешить возврат
 - Разрешить создание копии
 - Разрешить удаление версии
 - Разрешить получение версии
 - Разрешить блокировку и разблокировку
 - Представление и версия объектов BOMM

- Представление и версия бизнес-представлений
 - Представление и версия календарей
 - Представление и версия соединений
 - Представление и версия профилей
 - Представление и версия QaaWS
 - Представление и версия объектов отчета
 - Представление и версия объектов безопасности
 - Представление и версия универсов
 - Просмотр удаленных ресурсов
5. Если необходимо назначить права выбранному пользователю, выберите соответствующее право и нажмите кнопку **Назначить безопасность**.

16.4.2 Резервное копирование и восстановление файлов вспомогательных версий

В этом разделе описываются предлагаемые процедуры по выполнению резервного копирования и восстановления файлов вспомогательных версий. План резервного копирования и восстановления состоит из мер предосторожности, предпринимаемых при системном сбое в результате стихийного бедствия или катастрофы.

16.4.2.1 Резервное копирование файлов вспомогательных версий

Выполните следующие шаги для резервного копирования вспомогательной версии:

1. Перейдите в каталог **<каталог_установки>\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise 4.0\CheckOut**
2. Скопируйте папку *CheckOut* и сохраните ее на любом устройстве резервного копирования.
3. Скопируйте репозиторий *LCM_Repository* целиком и сохраните его на любом устройстве резервного копирования.

16.4.2.2 Восстановление файлов вспомогательных версий

Для восстановления файлов вспомогательных версий выполните следующие шаги:

1. Восстановите папку "CheckOut" из местоположения, в которое ранее было выполнено резервное копирование.

Примечание:

Выбрав команды **LCM > Параметры администрирования > Параметры VMS > Вспомогательная версия**, убедитесь, что в поле **Каталог рабочего пространства** введен верный путь извлечения.

2. Восстановите репозиторий "LCM_Repository" из местоположения, в которое ранее было выполнено резервное копирование.

Примечание:

Выбрав команды **LCM > Параметры администрирования > Параметры VMS > Вспомогательная версия**, убедитесь, что в поле **Путь установки** введен верный путь извлечения.

16.5 Использование ключа командной строки

Ключ командной строки средства управления повышением позволяет перемещать объекты с помощью командной строки из одной системы SAP BusinessObjects Business Intelligence в другую.

Средство управления повышением поддерживает следующее повышение задания с помощью ключа командной строки:

- Экспорт существующего шаблона заданий LCM в LCMBIAR с использованием шифрования пароля.
- Экспорт существующего шаблона заданий LCM в LCMBIAR без шифрования пароля.
- Повышение с помощью существующего шаблона заданий
- Импортируйте и повысьте существующий LCMBIAR
- Экспорт одного/нескольких запросов платформы
- Повышение нескольких запросов платформы

16.5.1 Запуск параметра командной строки в ОС Windows

Для запуска средства командной строки выполните следующие шаги.

1. Откройте окно или оболочку командной строки.
2. Перейдите в соответствующий каталог.

Например, каталог для Windows -C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib

3. Выполните одно из следующих действий.
 - Выполните программу LCM CLI, при этом перед запуском программы убедитесь в том, что установлен путь к java.

Команда: `java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <файл свойств>`

- Запустите BAT-файл в каталоге `C:\Program Files (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts\lcm_cli.bat`

Команда: `lcm_cli.bat -lcmproperty <property file>`

Примечание:

При появлении подсказки введите действительный пароль.

Средство командной строки для управления повышением принимает файл *свойств* в качестве параметра. Файл *свойств* содержит требуемые параметры для взаимодействия со средством командной строки для управления повышением, касающегося выполняемых действий, выбора развертывания платформы SAP BusinessObjects Business Intelligence для выполнения соединения, методов соединения, повышаемых объектов и пр.

Файл должен иметь форму `<File Name>.properties`

Например: `Myproperties.properties`

16.5.2 Запуск параметра командной строки в UNIX

Для запуска средства командной строки выполните следующие шаги.

1. Оболочка запуска.
2. Перейдите в соответствующий каталог.

Например, `/usr/u/qaunix/Aurora604/sap_bobj/enterprise_40/java/lib`

3. Выполните одно из следующих действий.

- Выполните программу LCM CLI, при этом перед запуском программы убедитесь в том, что установлен путь к java.

Команда: `java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <property file>`

- Выполните файл BAT из `<installdir_path>\sap_bobj\lcm_cli.sh`

Команда: `lcm_cli.sh -lcmproperty <property file>`

Примечание:

При появлении подсказки введите действительный пароль.

16.5.3 Параметры командной строки

В следующей таблице описываются параметры и допустимые значения ключа командной строки для приложения управления повышением уровня.

Параметр	Разрешенные значения	Описание	Обязательный или необязательный
action	Экспорт, повышение уровня Пример: action=export	Этот параметр позволяет указать операцию, которую следует выполнить через интерфейс командной строки. Эта операция может выполнить любое из следующих действий: <ul style="list-style-type: none"> • Перенос объектов из файла LCMBiar или из задания управления повышением в систему платформы SAP BusinessObjects Business Intelligence. • Экспорт объектов из системы платформы SAP BusinessObjects Business Intelligence в файл LCMBIAR. 	Обязательный
exportLocation	Текст произвольного формата. Должен иметь расширение <i>.lcmbar</i> Пример: exportLocation=C:\Backup\lcmbar	Этот параметр позволяет пользователю задать папку для размещения файла LCMBIAR после экспорта и упаковки объектов.	Является обязательным при значении action=export

Параметр	Разрешенные значения	Описание	Обязательный или необязательный
importLocation	Текст произвольного формата. Должен иметь расширение <i>.lcmbiar</i> Пример: <code>importLocation=C:\Backup\lcmbiar</code>	Этот параметр позволяет пользователю указать расположение файла LCMBIAR, который содержит объекты, уровень которых следует повысить.	Является обязательным при значении <code>action=promote</code>
LCM_CMS	Текст произвольного формата. Пример: <code>LCM_CMS=<CMSname:port no.></code>	Этот параметр позволяет указать CMS для приложения управления повышением.	Является обязательным при значении <code>action=promote</code> или <code>export</code>
LCM_userName	Текст произвольного формата. Пример: <code>LCM_userName=<username></code>	Этот параметр позволяет указать имя пользователя учетной записи, которое будет использоваться средством для подключения к CMS приложения управления повышением. Примечание: Поддерживается делегированный администратор	Является обязательным при значении <code>action=promote</code> или <code>export</code>
LCM_password	Текст произвольного формата. Пример: <code>LCM_password=<password></code>	Этот параметр позволяет пользователю указать пароль для учетной записи пользователя.	Является обязательным при значении <code>action=promote</code> или <code>export</code>

Параметр	Разрешенные значения	Описание	Обязательный или необязательный
LCM_authentication	secEnterprise, secWinAD, secLDAP,secSAPR3 Пример: LCM_authentication=<authentication>	Этот параметр определяет используемый тип аутентификации.	Необязательный. Если тип аутентификации не задан, используется secEnterprise
LCM_systemID	Идентификатор системы Пример: LCM_systemID=<systemID>	Этот параметр используется для аутентификации SAP.	Является обязательным для аутентификации SAP.
LCM_clientID	Идентификатор клиента Пример: LCM_clientID=<clientID>	Этот параметр используется для аутентификации SAP.	Является обязательным для аутентификации SAP.
Source_CMS	Текст произвольного формата. Пример: Source_CMS=<имя_CMSname: номер_порта>	Этот параметр позволяет указать CMS, к которому будет подключаться средство.	Является обязательным при значении action=export

Параметр	Разрешенные значения	Описание	Обязательный или необязательный
Source_userName	Текст произвольного формата. Пример: Source_username=<username>	Этот параметр определяет учетную запись пользователя, которая будет использоваться инструментом для подключения к серверу CMS платформы SAP BusinessObjects Business Intelligence. Примечание: Поддерживается делегированный администратор.	Является обязательным при значении action=export
Source_password	Текст произвольного формата. Пример: Source_password=<password>	Этот параметр определяет связанный пароль учетной записи пользователя.	Является обязательным при значении action=export
Source_authentication	secEnterprise, secWinAD, secLDAP, secSAPR3 Пример: Source_authentication=<authentication>	Этот параметр определяет используемый тип аутентификации.	Необязательный. Если тип аутентификации не задан, используется secEnterprise
Source_systemID	Идентификатор системы SAP Пример: Source_systemID=<systemID>	Этот параметр используется только для аутентификации SAP.	Является обязательным для аутентификации SAP.

Параметр	Разрешенные значения	Описание	Обязательный или необязательный
Source_clientID	Идентификатор клиента SAP Пример: Source_clientID=<systemID>	Этот параметр используется только для аутентификации SAP.	Является обязательным для аутентификации SAP.
Destination_userName	Текст произвольного формата. Пример: Destination_username=<username>	Этот параметр определяет учетную запись пользователя, которая будет использоваться инструментом для подключения к серверу CMS платформы SAP BusinessObjects Business Intelligence. Примечание: Поддерживается делегированный администратор.	Является обязательным при значении action=probe
Destination_password	Текст произвольного формата. Пример: Destination_password=<password>	Этот параметр определяет связанный пароль учетной записи пользователя.	Является обязательным при значении action=probe
Destination_authentication	secEnterprise, secWinAD, secLDAP, secSAPR3 Пример: Destination_authentication=<authentication>	Этот параметр определяет используемый тип аутентификации.	Необязательный. Если тип аутентификации не задан, используется secEnterprise

Параметр	Разрешенные значения	Описание	Обязательный или необязательный
Destination_systemID	Идентификатор системы Пример: <code>Destination_systemID=<systemID></code>	Этот параметр используется только для аутентификации SAP.	Является обязательным для аутентификации SAP.
Destination_clientID	Идентификатор клиента Пример: <code>Destination_clientID=<systemID></code>	Этот параметр используется только для аутентификации SAP.	Является обязательным для аутентификации SAP.
includeSecurity	False, True Пример: <code>includeSecurity=<True или False></code>	Этот параметр дает инструменту команду на экспорт или импорт параметров защиты, связанных с выбранными объектами и пользователями. Если используются уровни доступа, они также будут экспортированы/импортированы.	Необязательный, если значение не указано, используется значение по умолчанию. Используется при значении <code>action=promote</code> или <code>export</code>
JOB_CUID	Уникальный идентификатор кластера сохраненного задания LCM	Этот параметр дает инструменту команду на экспорт всех объектов в задании в файл LCMBIAR.	Необязательно, используется при значении <code>action=export</code> или <code>promote</code>

Параметр	Разрешенные значения	Описание	Обязательный или необязательный
exportQuery	<p>Текст произвольного формата. Необходимо использовать формат языка запроса CMS.</p> <p>Пример: <code>exportQuery1=select*from ci_Infoobjects, где si_name='Xtreme Employees' и si_kind='Webi'</code></p> <p>Примечание: В одном файле свойств может содержаться любое количество запросов, однако они должны именоваться следующим образом: exportQuery1, exportQuery2 и т. д.</p>	<p>Это запросы, которые инструмент должен выполнять для сбора объектов, предназначенных для экспорта.</p>	<p>Необязательно, используется при значении <code>action=export</code></p>
exportQueriesTotal	<p>Целые положительные числа <code>exportQueriesTotal=<целое число></code></p>	<p>Этот параметр позволяет пользователю указать число запросов на экспорт для выполнения. Если при наличии запросов на экспорт в количестве x нужно выполнить все эти запросы, то для данного параметра нужно задать значение x.</p>	<p>Необязательно, используется при значении <code>action=export</code></p> <p>Если значение не указано, используется значение по умолчанию 1.</p>

Параметр	Разрешенные значения	Описание	Обязательный или необязательный
stacktrace	True или False Пример: stacktrace=<True или False>	Этот параметр позволяет пользователю отслеживать все вызовы.	Необязательно; если не указано, по умолчанию – False
lcmbiarpassword	Текст произвольного формата Пример: java -jar upgradeManagementTool.jar -mode livetobiar -biarfile "C:\TEMP\abc.biar" -lcmbiarpassword "testpassword"	Этот параметр позволяет шифровать и дешифровать файлы BIAR с использованием пароля.	Дополнительно, если не указано иное, или строка пуста, подразумевается, что шифрования нет.
lcmproperty	Полный путь к расположению, где сохранен файл свойства lcm_cli.bat - lcmproperty <путь к файлу свойств>	Этот параметр ссылается на значения, требуемые для выполнения команды, сохраненные в файле.	Принудительный
consolelog	True или False	Этот параметр используется для отображения полного журнала команды, выполненной пользователем в командном журнале.	Дополнительно

Примечание:

- Аналогично созданию задания перед экспортом, параметр командной строки создает временное задание в реальном времени. Имя задания должно представлять комбинацию Query_<USER>_<Timestamp>. Относится только к *exportQuery*.

- В соответствии с соглашением об именах имя экспортируемого файла LCMBIAR может представлять комбинацию <JobName>_<Timestamp>.lcmbar, чтобы гарантировать уникальность. если имя файла LCMBIAR не указано в файле *exportLocation*.
- Откат задания возможен только из приложения управления повышением. Командная строка не поддерживает откат заданий.

16.5.4 Образец файла свойств

Ниже приведен образец файла свойств:

Пример:

```
importLocation=C:/Backup/CR.lcmbar  
  
action=promote  
  
LCM_CMS=<CMS name:port number>  
  
LCM_userName=<username>  
  
LCM_password=<password>  
  
LCM_authentication=<authentication>  
  
LCM_systemID=<ID>  
  
LCM_clientID=<client ID>  
  
Destination_CMS=<CMS name:port number>  
  
Destination_userName=<username>  
  
Destination_password=<password>  
  
Destination_authentication=<authentication>  
  
Destination_systemID=<ID>  
  
Destination_clientID=<client ID>  
  
lcmbarpassword=<password>
```

Примечание:

Если в файле свойств отсутствует личная информация, в интерфейсе командной строки LCM в консоли будет выдана подсказка ввести такую информацию.

16.6 Использование Enhanced Change and Transport System

Change and Transport System (CTS) организует и настраивает проекты разработки в ABAP Workbench, а затем перемещает эти изменения между системами SAP в системном ландшафте. Усовершенствованная система изменений и транспортировки (CTS+) является модулем расширения для CTS, которое обеспечивает распространение содержимого, не относящегося к ABAP, в репозитории, не относящиеся к ABAP, с поддержкой CTS+.

Содержимое SAP Business Warehouse в качестве источника данных может использоваться информационными объектами платформы SAP BusinessObjects Business Intelligence (платформой BI). Интеграция CTS+ со средством управления повышением обеспечивает обработку репозитория платформы SAP BusinessObjects Business Intelligence аналогично репозиторию SAP Business Warehouse (BW) посредством использования запросов транспорта CTS для повышения заданий. CTS+ обеспечивает возможность транспортировки объектов не из SAP в рамках системного ландшафта. Например, объекты, созданные в системе разработки, могут быть прикреплены к запросу транспорта и перенаправлены в другие системы в ландшафте.

Для получения дополнительных сведений о системе изменений и транспорта см.

http://help.sap.com/saphelp_nw70ehp1/helpdata/en/3b/dfba3692dc635ce10000009b38f839/frameset.htm

Для получения дополнительных сведений о CTS+ и транспортах, не относящимся к ABAP, см.

http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bb/6fab6036a146baa58e42fac032ab7b/frameset.htm

16.6.1 Предварительные условия

Пункты, перечисленные ниже, являются предварительными условиями для передачи содержимого Business Intelligence из одной системы в другую с помощью CTS+:

1. Платформа SAP BusinessObjects Business Intelligence platform 4.0 (платформа BI) успешно установлена.
2. Решение SAP Solution Manager 7.1 или SAP Solution Manager 7.0 EHP1 (минимум SP25), предназначенное по меньшей мере для конфигурации систем SAP BusinessObjects, установлено и используется в качестве контроллера домена CTS+.

Для получения дополнительных сведений о настройке домена транспорта см.

http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a0a77acc11d1899e0000e829fbbd/frameset.htm

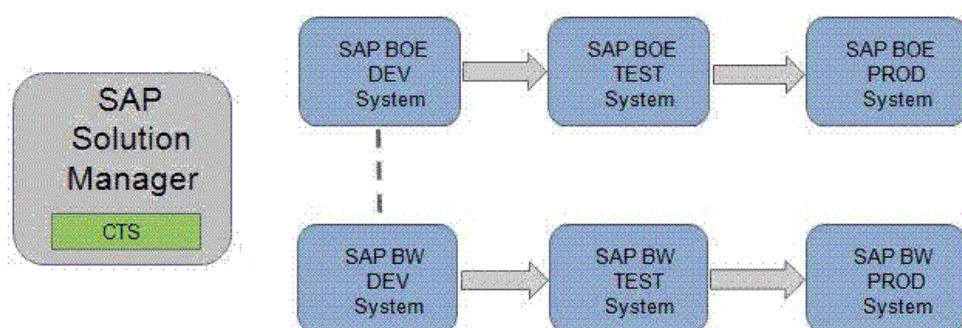
3. Модуль расширения CTS для SAP Solution Manager установлен (модуль CTS взят из SL Toolset 1.0 SP02. Рекомендуется использовать последнюю доступную версию модуля расширения CTS).

Сведения о настройке модуля расширения CTS см. в SAP-ноте:

<https://service.sap.com/sap/support/notes/1533059>

4. Установлены системы *SAP Business Warehouse 7.0* (SPS 24 или более новая версия). Для получения дополнительных сведений см. SAP-ноту <https://service.sap.com/sap/support/notes/1369301>
5. Настроен ландшафт транспорта *SAP Business Warehouse* (*SAP BW*) в системе настройки и транспортировки (*CTS*).

16.6.2 Настройка платформы *Business Intelligence* и интеграции *CTS+*



Система управления транспортом (TMS), которая является частью системы изменений и транспорта, используется для транспортировки изменений между системами SAP в рамках ландшафта. Эта система осуществляет управление подключенными системами, их маршрутами, а также выполнением импорта в ее системы. Для получения дополнительных сведений о системе управления переносом см.

http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a0137acc11d1899e0000e829fbbd/frameset.htm

CTS+ позволяет осуществлять сбор данных извне, а также распространять их в рамках ландшафта переноса. Веб-интерфейс организатора переносов, который является частью CTS+, осуществляет управление содержащимися в ней запросами на перенос и объектами переноса. Для получения дополнительных сведений см.

http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a0137acc11d1899e0000e829fbbd/frameset.htm.

При помощи запросов на перенос CTS средство управления повышением платформы SAP BusinessObjects Business Intelligence можно интегрировать с CTS+ и SAP BW.

Примечание:

Для активации интеграции платформы Business Intelligence с системой SAP Solution Manager необходимо определить вид приложения "BOLM" в ландшафте SAP Solution Manager.

Для настройки взаимодействия платформы BI и CTS+ выполните следующие шаги:

1. Активируйте веб-службу экспорта в CTS.
2. Выполните настройку параметров CTS при помощи средства управления повышением.
3. Выполните настройку системы импорта платформы Business Intelligence в SAP Solution Manager

См. также

- [Активация веб-службы экспорта в CTS](#)
- [Настройка параметров CTS+ при помощи средства управления повышением](#)
- [Настройка платформы Business Intelligence и интеграции CTS+](#)

16.6.2.1 Активация веб-службы экспорта в CTS

Для настройки системы платформы BI необходимо активировать веб-службу экспорта в CTS при помощи веб-средства SOA Management.

1. Для запуска этого приложения введите код транзакции SOAMANAGER в менеджере решений SAP Solution Manager.

Для получения дополнительной информации о SOA Management и настройке конечной точки службы см. справочный портал SAP по адресу

http://help.sap.com/saphelp_nw70ehp1/helpdata/en/33/06820d9d174c2884576bd78ac5629d/frameset.htm

После выполнения входа в веб-браузере будет открыта консоль управления SOA.

2. На вкладке **Управление службой** выберите **Настройка единой службы**.

Имя веб-службы экспорта CTS: EXPORT_CTS_WS

3. Создайте или измените конечную точку службы на вкладке **Настройка**.
4. На вкладке **Безопасность** можно настроить протокол передачи и метод аутентификации.
5. Для удобства доступа конечной точки службы на вкладке **Настройки передачи** можно задать вспомогательный URL-адрес.

16.6.2.2 Настройка параметров CTS+ при помощи средства управления повышением

В следующем разделе описываются шаги по настройке, которые должны быть выполнены в приложении CMS для настройки использования CTS+ совместно с приложением управления повышением.

1. На странице «Задания повышения» щелкните **Настройки CTS**, а затем выберите **Системы BW**.
2. На странице «Системы BW» выберите **Добавить** для добавления системы BW в ландшафт.
3. На странице «Добавить систему» введите следующие сведения:
 - **SID BW хоста:** укажите идентификатор системы (SID) компьютера SAP BW/ABAP, выполняющего функцию хоста.
 - **Имя хоста:** укажите IP-адрес компьютера, выполняющего функцию хоста.
 - **Системный номер:** введите системный номер системы хоста.

- **Клиент:** указывает сведения о системе клиентского компьютера.
- **Пользователь и Пароль:** укажите в этих полях имя пользователя и пароль на клиентском компьютере.
- **Язык:** укажите в этом поле выбранный язык.

4. Щелкните **Сохранить**, чтобы добавить систему в ландшафт.

Примечание:

После добавления системы BW в ландшафт можно использовать кнопки **Изменить** или **Удалить** на странице «Системы BW» для изменения систем в ландшафте.

5. На странице «Задания повышения» щелкните **Настройки CTS**, а затем выберите **Настройки веб-службы**.

6. На странице «Настройки веб-службы» введите URL-адрес веб-службы и сведения о пользователе.

Примечание:

При отсутствии этих сведений получите их от администратора Solution Manager.

7. Щелкните **Сохранить** и **Заккрыть**, чтобы завершить добавление настроек веб-службы.

8. Создание файла сопоставления в исходной системе BI.

Выполните следующие действия в системе разработки платформы BI для создания текстового файла со сведениями о соединении для обеспечения возможности сопоставления:

- В CMS управления повышением платформы BI перейдите в корневой каталог и создайте папку с именем LCM по пути <путь установки платформы SAP BusinessObjects Business Intelligence>/SAP BusinessObjects Business Intelligence platform 4.0/
- Создайте текстовый файл с именем LCM_SOURCE_CMS_SID_MAPPING.properties и введите в него следующие данные:
 - **<Дополните имя исходной системы платформы SAP BusinessObjects Business Intelligence строкой domain>@<номер порта CMS> = <логическое имя исходной системы, используемое в конфигурации CTS >**
 - **<IP-номер исходной системы платформы SAP BusinessObjects Business Intelligence >@<номер порта CMS> = <логическое имя исходной системы, используемое в конфигурации CTS >**

Например:

DEWDFTH04171S@6400=WJ3

10.208.112.177@6400=WJ3

DEWDFTH04171S.pgdev.sap.corp@6400=WJ3

Примечание:

В случае кластерной среды скопируйте файлы LCM_SOURCE_CMS_SID_MAPPING.properties и LCM_SID_RFC_MAPPING.properties в систему, где запущен адаптивный сервер обработки.

Для получения дополнительных сведений о выполнении шагов по настройке для систем, отличных от ABAP, см.

http://help.sap.com/saphelp_nw70/helpdata/en/d4/3bab83106941f08ad1f2e1ec14375e/frameset.htm

16.6.2.3 Настройка системы импорта платформы Business Intelligence в SAP Solution Manager

1. Выполните вход в систему SAP Solution Manager.
2. Введите **stms** транзакции и нажмите **Enter**.
3. Настройка BOLM в качестве типа приложения.
 - a. Выберите **Обзор > Системы**.
 - b. Выберите **Дополнительно > Тип приложения > Настройка**.
 - c. Выберите **Добавить записи**.
 - d. В поле **Тип приложения** введите BOLM.
 - e. Введите описание.
 - f. В поле **Сведения о поддержке** введите <http://service.sap.com> (ACH: BOJ-BIP-DEP)
 - g. Выберите команды **Представление в виде таблицы > Сохранить**
 - h. В открывшемся сообщении подтверждения нажмите **Да**.
4. Для работы с разными языками можно сохранить переведенные тексты следующим образом:
 - a. Выберите команды **Перейти > Перевод**.
 - b. Выберите языки, на которые требуется перевести текст.
 - c. Введите переведенные значения в поля **Описание** и **Вспомогательные сведения**.
 - d. Подтвердите сведения в диалоговом окне.
 - e. Выберите **Продолжить**.
 - f. Выберите команды **Представление в виде таблицы > Сохранить**
 - g. Подтвердите выбор в подсказке.

Домен TMS готов к поддержке использования содержимого бизнес-аналитики в CTS.
5. В CTS+ определите исходную систему платформы SAP BusinessObjects Business Intelligence в качестве системы экспорта.

Примечание:

Для получения дополнительных сведений о создании системы, отличной от ABAP, в качестве исходной, см.

http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bf/e4626214504be18b2f1abeeaf4f8e4/frameset.htm
[\(http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bf/e4626214504be18b2f1abeeaf4f8e4/frameset.htm\)](http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bf/e4626214504be18b2f1abeeaf4f8e4/frameset.htm)

6. В CTS+ настройте систему импорта платформы SAP BusinessObjects Business Intelligence, выполнив следующие шаги:

Примечание:

SID можно определить как ссылку на систему импорта платформы SAP BusinessObjects Business Intelligence.

- a. Создайте систему, отличную от ABAP, в качестве системы импорта.
Для получения дополнительных сведений см.
http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bf/e4626214504be18b2f1abeeaf4f8e4/frameset.htm
(http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bf/e4626214504be18b2f1abeeaf4f8e4/frameset.htm).
- b. Укажите метод развертывания **Другие** и отмените выбор всех других параметров.
- c. Выберите **Сохранить**.
- d. Подтвердите выбор в диалоговом окне..
Откроется табличное представление для настройки параметров системы импорта.
- e. Выберите команды **Изменить > Создать записи**.
- f. На экране "Изменить представление CTS: системные сведения для обработки видов приложений" выполните следующие шаги:
 1. В поле **Метод развертывания** выберите **инструмент развертывания в зависимости от приложения (EJB)**.
 2. В поле **URI развертывания** введите следующий URI: `http://<BOE (http://%3cboe/) web server name>:<Webserver port>/BOE/LCM/CTSServlet?&cmsName=<BOE destination name>:<CMSport>&authType=<BOE authentication type>`
где:
 - "BOE web server name" – имя или IP-адрес компьютера, на котором установлен веб-сервер платформы Business Intelligence.
 - "Web server port" – номер порта сервера приложений платформы Business Intelligence.
 - "BOE destination name" – имя компьютера, на котором установлен центральный сервер управления (CMS) платформы Business Intelligence.
 - "CMS port" – номер порта CMS.
 - "BOE authentication type" – тип аутентификации пользователя для импорта контента платформы Business Intelligence. Поддерживаемые виды аутентификации: secEnterprise, secLDAP, secWinAD, and secSAPR3.
 3. В поле **Пользователь** введите имя пользователя платформы Business Intelligence.
 4. В поле **Пароль** введите пароль доступа к платформе Business Intelligence.
 5. Нажмите "Сохранить" для сохранения параметров настройки.

Если требуется несколько систем импорта, повторите описанные выше шаги для создания всех требуемых систем назначения. Сведения о настройке маршрутов переноса между исходной и целевой системами после создания систем назначения см.

http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a1df7acc11d1899e0000e829fbbd/frameset.htm

16.6.3 Повышение задания с использованием CTS

В этом разделе описывается рабочий процесс, поддерживаемый приложением управления повышением для переноса объектов CMS платформы SAP BusinessObjects Business Intelligence из исходной системы в целевую систему с использованием Change Transport System. Чтобы выполнить повышение задания с использованием CTS, выполните следующие шаги:

1. Запустите приложение управления повышением с использованием аутентификации SAP и создайте задание.

Дополнительные сведения о создании нового задания см. в разделе "Создание задания" в соответствующих ссылках.

Примечание:

Убедитесь, что на экране входа в исходную систему выбран вид аутентификации "SAP".

2. В раскрывающемся списке **Место назначения** выберите параметр **Повысить уровень с**



помощью CTS.

3. Нажмите кнопку **Создать**.

Откроется окно «Добавить объекты из системы». Здесь папка и вложенные папки отображаются в структуре дерева.

4. Перейдите к папке, в которой требуется выбрать инфообъект.

5. Выберите инфообъект, который нужно добавить к заданию, а затем щелкните **Добавить**. Если нужно добавить инфообъект и закрыть окно «Добавить объекты», щелкните **Добавить и закрыть**.

Информационный объект прикреплен к заданию, появится окно «Задания повышения».

Примечание:

Окно "Задания повышения" используется для выполнения следующих действий:

- Используйте вариант **Добавить объекты** для добавления инфообъектов к заданию. Для получения подробных сведений см. раздел "Добавление инфообъекта к заданию".
- При помощи параметра **Управление зависимостями** доступно управление зависимостями выбранного инфообъекта. Зависимости объекта SAP BW отображаются в интерфейсе пользователя и могут быть выбраны там.

Более подробные сведения можно получить в разделе "Управление зависимыми объектами задания".

6. Нажмите кнопку **Повысить**.

Откроется окно «Повысить», на котором отображены индикатор, владелец и краткое описание заданного в текущий момент запроса на перенос по умолчанию.

7. Гиперссылку **Запросы транспорта** можно использовать для выполнения следующих действий:

- Просмотр сведений о запросе транспорта
- Изменение параметров запроса транспорта по умолчанию.
- Выбор другого запроса транспорта.
- Создание запроса транспорта.

- a. Щелкните ссылку **Запросы на перенос**, чтобы открыть веб-интерфейс пользователя «организатора переносов».
- b. При запросе учетных данных для входа в систему выполните вход с использованием допустимых учетных данных системы контроллера домена CTS.
- c. Обновите экран «Повысить», чтобы просмотреть обновления.

Для получения дополнительных сведений об использовании веб-интерфейса пользователя «организатора переносов» см.

http://help.sap.com/saphelp_nw70ehp1/helpdata/en/b5/6d03660d3745938cd46d6f5f9cef2e/frameset.htm

- 8. Чтобы просмотреть сведения о зависимостях объектов SAP BW, щелкните гиперссылку **Зависимости второго уровня**.

Примечание:

При щелчке гиперссылки **Зависимости второго уровня** отображаются только объекты, заблокированные в запросе. Если запрос был выпущен, просмотр зависимостей недоступен. Помимо этого, данная гиперссылка затенена при отсутствии активных зависимостей второго уровня.

- 9. Нажмите кнопку **Повысить**.
- 10. Закройте задание.
Появится главный экран приложения управления повышением. Теперь созданное задание имеет статус **Экспортировано в CTS**.
- 11. Выпустите объект платформы SAP BusinessObjects Business Intelligence в систему назначения, выполнив следующие шаги:
 - a. Щелкните по ссылке, отображенной в столбце "состояние" задания, которое нужно повысить. Откроется окно «Состояние продвижения».
 - b. Нажмите **Состояние запроса**.
Откроется веб-интерфейс пользователя «организатора переносов».
 - c. Если запрос имеет статус **Изменяемый**, нажмите кнопку **Выпустить**, чтобы выпустить запрос на перенос объекта платформы SAP BusinessObjects Business Intelligence. Для получения дополнительных сведений о выпуске запросов на перенос, содержащих объекты, не связанные с ABAP, см.
http://help.sap.com/saphelp_nw70ehp1/helpdata/en/55/07c497db8140ef8176715d4728eec1/frameset.htm
 - d. Закройте веб-интерфейс пользователя «организатора переносов».
- 12. Чтобы просмотреть зависимости для объектов SAP BW, щелкните гиперссылку **Список зависимостей BW**.

Примечание:

Рекомендуется обратиться к группе SAP BW, чтобы получить обновления по зависимостям SAP BW и их версии, поскольку данная группа ведет работу по этим объектам.

- 13. Закройте окно «Состояние повышения».
- 14. Импортируйте объект платформы SAP BusinessObjects Business Intelligence в конечную систему, выполнив следующие шаги:
 - a. Войдите в контроллер домена CTS+.
 - b. Вызовите транзакцию STMS, чтобы выполнить вход в систему управления переносами.
 - c. Щелкните по значку **Обзор импорта**.

Откроется окно «Обзор импорта», и можно будет просмотреть элементы в очереди на импорт из всех систем.

- d. Выберите системный идентификатор LCM-системы назначения.
Можно просмотреть список запросов на перенос, которые можно импортировать в систему.
- e. Нажмите кнопку **Обновить**.
- f. Импортируйте соответствующие запросы на перенос. Для получения дополнительных сведений см.

http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a39e7acc11d1899e0000e829fbbd/frameset.htm.

Для получения общих сведений об импорте запросов транспорта с содержимым BOLM см.
http://help.sap.com/saphelp_nw70ehp1/helpdata/en/09/ca0f3a878f46e9a5a32e666131d2ba/frameset.htm

15. Если выбранный объект имеет зависимости SAP BW, выполните следующие шаги:

- a. Выпустите зависимости SAP BW в систему назначения, выполнив следующие шаги:
 - 1. Выполните вход в исходную систему SAP BW.
 - 2. Вызов транзакции SE09. Откроется окно «организатора переносов».
 - 3. Нажмите кнопку **Отобразить**. Будет открыт запрос SAP BW.
 - 4. Щелкните запрос BW и разверните его, чтобы просмотреть задачи, созданные для зависимостей.
 - 5. Щелкните правой кнопкой мыши запрос, связанный с основным объектом SAP BW, и выберите команду **Выпустить напрямую**. Повторите этот шаг, чтобы выпустить все задачи, связанные отдельно с каждым зависимым объектом.
 - 6. Правой кнопкой мыши щелкните по запросу, связанному с основным объектом BW и выберите **Выпустить напрямую**.
 - 7. Обновляйте экран, пока не будут выпущены все запросы.

Примечание:

Можно просмотреть журналы запроса, дважды щелкнув его.

- b. Выпустите зависимости SAP BW в систему назначения, выполнив следующие шаги:
 - 1. Выполните вход в систему назначения SAP BW.
 - 2. Вызовите транзакцию STMS, чтобы выполнить вход в систему управления переносами.
 - 3. Щелкните значок **Обзор импорта**. Появится экран «Обзор импорта».
 - 4. Дважды щелкните идентификатор системы назначения SAP BW. Можно просмотреть список запросов на перенос, которые можно импортировать в систему.
 - 5. Импортируйте соответствующие запросы на перенос. Для получения дополнительных сведений см.

http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a39e7acc11d1899e0000e829fbbd/frameset.htm.

Для получения дополнительных сведений о переносах с использованием очередей импорта см.

http://help.sap.com/saphelp_nw70ehp1/helpdata/en/65/8a99386185c064e10000009b38f8cf/frameset.htm

16. Для просмотра статуса повышенного задания войдите в целевую систему.

Дополнительные сведения об интерактивной документации для общего CTS см. в разделе

http://help.sap.com/saphelp_ctsplug100/helpdata/en/52/700dbe608e4752a8e2e96a1876f865/frameset.htm

См. также

- [Создание задания](#)
- [Управление зависимостями в приложении управления повышением](#)

Визуальное отличие

17.1 Visual Difference в средстве управления повышением

Visual Difference позволяет просматривать различия между двумя версиями поддерживаемого типа файла (LCM BIAR) или поддерживаемого типа объекта (задание LCM) либо обеими. Эту функцию можно использовать для обнаружения различий между файлами или объектами, чтобы разработать и вести разные типы отчетов. Эта функция устанавливает статус сравнения между исходной и конечной версиями. Например, если предыдущая версия отчета пользователя является точной, а текущая – нет, можно сравнить и проанализировать файл, чтобы определить точную проблему.

Далее перечислены три типа визуальных отличий, которые можно обнаружить в файле или объекте:

- Удалено. Если в одной из версий файла отчета отсутствует элемент, отображается тип отличия "Удалено". Например, таким элементом может быть строка, экземпляр раздела или даже блок.
- Изменено. Если в исходной и конечной версиях отчета содержатся разные значения, отличию присваивается тип "Изменено". Например, значением может быть содержимое ячейки или результат локальной переменной.
- Вставлено. Если в конечной версии отчета содержится элемент, который отсутствует в исходной версии, отличие имеет тип "Вставлено".

Типы объектов, для которых поддерживается функция визуального отличия:

- LCMBIAR
- Задание LCM

Сравнение возможно для следующих комбинаций:

- Задание LCM с другим заданием LCM
- Задание LCM с файлом LCMBIAR
- Файл LCMBIAR с другим файлом LCMBIAR
- Файл LCMBIAR с заданием LCM

Предпочтения

На домашней странице визуальных отличий можно задать предпочтительные параметры, например языковой стандарт программного продукта, просмотра, максимальное количество объектов на странице, часовой пояс и подсказку для несохраненных данных.

Домашняя страница

Домашняя страница визуальных отличий содержит следующие вкладки и панели:

- Создать сравнение. Эта вкладка позволяет создавать новое сравнение между объектами
- Поиск сравнений. Это поле позволяет выполнять поиск объектов, которые уже сравнивались
- Область "Функции сравнения". На этой панели перечислены вкладки фильтров и отличий
- Область "Сравнения: отличия". На этой панели перечислены сравниваемые объекты с указанием имени сравнения, даты/времени и статуса отличий

17.1.1 Сравнение объектов и файлов с использованием функции визуального отличия

Параметр визуального отличия позволяет сравнивать файлы и объекты BIAR.

Для сравнения файлов с использованием визуального отличия выполните следующие шаги.

1. Войдите в приложение СМС.
2. На домашней странице СМС на вкладке «Управление» щелкните ссылку **Визуальное отличие**. Будет открыта страница "Визуальное отличие". Сравниваемые файлы хранятся в папке "Отличия" или в любой созданной пользователем вложенной папке.

Примечание:

Чтобы создать новую вложенную папку, щелкните значок "Папка".

3. Выберите **Новое сравнение**. Будет открыт экран «Сравнения».
4. Выберите эталонную систему из раскрывающегося списка **Выбор системы** в области "Эталонная система".
Можно подключиться к любой из следующих эталонных систем:
 - CMS
 - VMS
 - локальная файловая система
5. Щелкните **Обзор**, чтобы выбрать сравниваемый объект или файл в локальной системе.
6. Из раскрывающегося списка **Выбор системы** в области "Целевая система" выберите целевую систему.

Можно подключиться к любой из следующих эталонных систем:

- CMS
- VMS
- локальная файловая система

Примечание:

При входе в систему CMS или VMS выбранный объект в эталонной системе может быть также автоматически сопоставлен объекту, имеющему то же имя в эталонной системе.

7. Щелкните **Обзор**, чтобы выбрать сравниваемый объект или задание в локальной системе.
8. Нажмите кнопку **Добавить**.

Объекты, выбранные для сравнения, добавляются в корзину.

При наличии нескольких пар объектов, добавленных в корзину, объекты можно планировать для последующего сравнения. Однако, если в корзине находится только одна пара объектов, их можно сравнить.

Чтобы сравнить файлы, перейдите к следующему шагу. Для получения сведений о планировании сравнения, см. [Планирование сравнения](#).

9. Нажмите кнопку **Сравнить**, чтобы сравнить объекты или папки.

Примечание:

Сравнение файла задания LCMBIAR/LCM включает:

- Метаданные LCMBIAR: сравнение сведений о задании, таких как имя, создатель, время и т. п.
- Основные объекты: сравнение каждого явным образом выбранного объекта в LCMBIAR с подобным объектом в целевом LCMBIAR по CUID.
- Зависимые объекты: сравнение выбранного зависимого объекта в файле с подобным объектом в целевом файле по CUID.

Если выбраны объекты, отличные от задания LCMBIAR или LCM, выводится следующее сообщение об ошибке : Подключаемый модуль не найден.

Процесс сравнения начнется сразу, различия (если они есть) будут отображены в «средстве просмотра визуальных отличий». Отличия выделяются оранжевым цветом, а отсутствующие объекты – красным.

При помощи фильтра можно также просмотреть сравниваемые объекты по типу, а также с отличиями или с общими атрибутами.

10. Нажмите кнопку **Сохранить**, чтобы сохранить отчет об отличиях.
11. Укажите папку, в которой следует сохранить отчет, и нажмите кнопку **ОК**.

17.1.2 Сравнение объектов или файлов в системе управления версиями

Можно сравнивать объекты или файлы в системе управления версиями с помощью параметра визуального отличия.

Чтобы сравнить объекты в системе управления версиями, выполните следующие шаги:

1. Выполните вход в приложение СМС.
2. На домашней странице СМС на вкладке «Управление» щелкните ссылку **Визуальное отличие**.

Будет открыта страница "Визуальное отличие". Сравниваемые файлы хранятся в папке "Отличия" или в любой созданной пользователем вложенной папке.

Примечание:

Чтобы создать новую вложенную папку, щелкните значок "Папка".

3. Выберите Новое сравнение.

Будет открыт экран «Сравнения».

4. Выберите значение Вход в систему VMS в раскрывающемся списке Выбор системы в разделе "Ссылка".**5. Введите реквизиты для входа в систему VMS и нажмите кнопку Вход в систему.**

Будет открыто диалоговое окно «Визуальное отличие – Автовыбор целевой системы»

6. Щелкните Нет, чтобы выбрать другую целевую систему, или Да, чтобы установить эталонную систему в качестве целевой.**7. Нажмите кнопку Обзор, чтобы выбрать объекты или задания для сравнения из эталонной и целевой систем.****8. Нажмите кнопку Добавить.**

Объекты, выбранные для сравнения, перечислены на панели Создать сравнение.

Можно сравнить файлы немедленно или запланировать сравнение на более позднее время. Чтобы сравнить файлы, перейдите к следующему шагу. Для получения сведений о планировании сравнения, см. [Планирование сравнения](#).

9. Нажмите кнопку Сравнить, чтобы сравнить объекты или папки.

Процесс сравнения начнется сразу, различия (если они есть) будут отображены в «средстве просмотра визуальных отличий». Отличия выделяются оранжевым цветом, а отсутствующие объекты – красным.

При помощи фильтра можно также просмотреть сравниваемые объекты по типу, а также с отличиями или с общими атрибутами.

10. Нажмите кнопку Сохранить, чтобы сохранить отчет об отличиях.**11. Укажите папку, в которой следует сохранить отчет, и нажмите кнопку ОК.**

17.1.3 Планирование сравнения

Для планирования сравнения файлов или объектов выполните следующие шаги.

1. Нажмите кнопку Планировать.

Откроется окно «График».

2. Выберите частоту для планирования сравнения из раскрывающегося списка Выполнение сравнения.**3. Укажите в соответствующих полях разрешенное количество попыток и интервал между попытками.****Примечание:**

Интервал между попытками можно указывать, если только указано число попыток.

4. Укажите имя отчета и нажмите кнопку **Обзор**, чтобы перейти в месторасположение, в котором нужно сохранить отчет.

Откроется окно «Сохранить задание в».

5. Укажите нужную папку, в которой нужно сохранить отчет, и нажмите кнопку **ОК**.

Примечание:

В зависимости от параметра, выбранного в раскрывающемся списке **Выполнение сравнения**, необходимо указать дату и время для сравнения.

6. Нажмите кнопку **Планировать**.

Пользователь может просмотреть объект сравнения или отчет об отличиях в средстве просмотра Visual Difference в последующий момент времени. Появится страница «Сравнение: отличия» со списком папок и файлов или отчетах о результатах сравнений.

Страница "Отличия при сравнении" содержит также следующие параметры:

- **История:** параметр **История** позволяет просматривать историю сравнений.
- **Повторное выполнение:** параметр **Повторное выполнение** вновь иницирует выполнение сравнения.
- **Планирование:** параметр **Планирование** позволяет планировать сравнение.

Управление приложениями

18.1 Управление приложениями с помощью CMC

18.1.1 Обзор

Область управления «Приложения» в CMC позволяет изменить внешний вид и функциональные возможности веб-приложений, например CMC и стартовой панели BI, без программирования. 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:

- Выпуск Analysis для OLAP
- Приложение-источник предупреждения
- стартовая панель BI
- Рабочие пространства BI
- Central Management Console
- Сотрудничество (с SAP Jam или SAP StreamWork)
- Конфигурация Crystal Reports
- Dashboards
- Дискуссии
- Дизайнер информации
- Приложение мониторинга
- Управление несколькими организациями
- OpenDocument
- Приложение Platform Search
- Управление повышением
- Средство преобразования отчетов
- SAP BusinessObjects Mobile
- Средство управления переводами
- Средство создания юниверсов
- Средство управления обновлением

- Визуальное отличие
- Web Intelligence
- Веб-служба
- виджеты

18.1.2 Общие настройки приложений

18.1.2.1 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*.

18.1.2.2 Настройка уровня журнала трассировки веб-приложения в СМС

Для трассировки других веб-приложений следует вручную сконфигурировать соответствующий файл `BO_trace.ini`.

1. В поле «Приложения» консоли СМС щелкните приложение правой кнопкой мыши и выберите **Настройки журнала трассировки**.

Примечание:

Эти приложения имеют следующие параметры журнала трассировки: Стартовая панель BI, СМС, Open Document, Promotion Management, Управление версиями, Visual Difference, Веб-служба.

Будет открыто диалоговое окно «Настройки журнала трассировки».

2. Выберите параметр в раскрывающемся списке **Уровень журнала**.
3. Нажмите **Сохранить и закрыть**.

Новый уровень журнала трассировки вступит в силу после следующего входа в данное веб-приложение.

См. также

- [Уровни журнала трассировки](#)

18.1.2.2.1 Уровни журнала трассировки

Для компонентов платформы VI доступны следующие уровни журнала трассировки:

Уровень	Описание
Не определен	Уровень журнала трассировки устанавливается с использованием другого способа, обычно через файл <code>.ini</code> .
Нет	Трассировка не происходит.
Нижняя	Фильтр журнала трассировки позволяет протоколировать сообщения об ошибках, игнорируя предупреждающие сообщения и сообщения о статусе. Протоколируются важные статусные сообщения, относящиеся к запуску компонента, к запросам на запуск, а также к запросам на окончание. Этот уровень не рекомендуется для целей отладки.
Средний	Фильтр журнала трассировки настроен на включение сообщений об ошибках, предупреждениях и большинства сообщений о статусе. Менее важные или слишком детальные статусные сообщения отфильтровываются. Этот уровень не достаточно детальный для использования в целях отладки.
Высокий	<p>Нет отфильтрованных сообщений. Этот уровень рекомендуется для использования в целях отладки.</p> <p>Предупреждение: Этот уровень трассировки оказывает значительное влияние на ресурсы системы, повышая нагрузку на процессор и занимая место на диске.</p>

18.1.3 Настройки, зависящие от приложения

18.1.3.1 Управление настройками приложения СМС

18.1.3.1.1 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» в 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». Выберите **Действия > Права для программного объекта**, затем выберите **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 адаптивных серверов заданий, 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 Business Intelligence.

4. Нажмите **Сохранить и закрыть**.

18.1.3.1.2 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 стандартный каталог 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.

Регистрация расширения обработки в системе

1. Перейдите в область управления «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 применяется к документам Web Intelligence или отчетам, созданным в SAP Crystal Reports для Enterprise.

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 изменения командной строки перейдите на вкладку «Серверы» в СМС, выберите нужный сервер и откройте страницу «Свойства». Для этого в командной строке введите `-report_ProcessExtPath` *абсолютный путь*. 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.

18.1.3.1.3 Управление доступом к вкладкам СМС

Делегированное администрирование и доступ к вкладкам СМС

Системный администратор платформы Business Intelligence обычно осуществляет управление большим числом документов, папок, пользователей, серверов и других объектов. Естественно, в крупных корпоративных средах один администратор физически не в состоянии осуществлять управление всеми ресурсами. Если системному администратору требуется сконцентрироваться на выполнении ключевых задач, он или она может создать делегированных администраторов, которым будут назначено ограниченное подмножество задач управления (например, администрирование отдела или содержимого клиента). В отличие от системного администратора, делегированные администраторы выполняют ограниченный набор задач и имеют меньший объем прав на объекты системы.

В конфигурации Central Management Console по умолчанию пользователи имеют права доступа ко всем существующим вкладкам СМС. Системный администратор может управлять видимостью вкладок СМС для принципалов (пользователи или группы пользователей) и соответствующими правами доступа. Чтобы оптимизировать пользовательский интерфейс и упростить работу делегированного администратора, системный администратор также может скрыть те вкладки СМС, доступ к которым делегированному администратору не требуется.

Предупреждение:

Управление доступом к вкладкам СМС влияет только на внешний вид пользовательского интерфейса СМС. Скрытие вкладок СМС не может рассматриваться как увеличение уровня безопасности, поскольку в этом случае не устанавливаются и не изменяются права безопасности на объекты, расположенные на вкладках. Чтобы предотвратить выполнение пользователями запрещенных операций с несанкционированными объектами (например, управление серверами с помощью Central Configuration Manager или сторонних программ на основе пакета SDK платформы BI), необходимо установить соответствующие права безопасности для объектов (например, объектов сервера).

См. также

- [Управление доступом других пользователей к вкладкам СМС](#)
- [Управление разрешениями на настройку доступа других пользователей и групп к вкладкам СМС](#)

Доступ к вкладкам СМС

Управление доступом к вкладкам СМС для других пользователей

Системный администратор обладает полным доступом ко всем вкладкам СМС. В следующем списке приводятся рекомендации по администрированию вкладок СМС, доступных принципалам:

- Чтобы упростить процесс управления и снизить частоту проведения процедур по обслуживанию и устранению неполадок, администраторам рекомендуется настраивать управление доступом к вкладкам СМС на уровне групп пользователей, а не отдельных пользователей.
- Для вкладок СМС, содержащих папки верхнего уровня, администратор должен предоставлять права на доступ к вкладкам и «Просмотр» непосредственно на папку верхнего уровня. Следующие вкладки СМС поддерживают папки верхнего уровня:

- **Уровни доступа**
 - **Календари**
 - **Категории**
 - **Подключения (юниверсов)**
 - **Криптографические ключи**
 - **События**
 - **Интеграции**
 - **Папки**
 - **Входящие**
 - **Соединение OLAP**
 - **Личные категории**
 - **Личные папки**
 - **Профили**
 - **Списки тиражирования**
 - **Серверы и группы**
 - **Временное хранилище**
 - **Юниверсы**
 - **Пользователи и группы**
 - **Запрос веб-службы**
- Для повышения безопасности системы доступ к следующим вкладкам СМС имеют только пользователи из группы "Администраторы": Пользователи из группы "Администраторы", которые по сути являются системными администраторами, имеют доступ к любой вкладке СМС независимо от установленных разрешений на доступ к вкладкам СМС. Разрешения на доступ к вкладкам СМС призваны контролировать доступ назначенных администраторов (то есть пользователей, не являющихся участниками группы "Администраторы") к вкладкам СМС.
- **Аудит**
 - **Аутентификации**
 - **Криптографические ключи**
 - **Лицензионные ключи**
 - **Мониторинг**
 - **Сеансы**

- **Параметры**
- **Управление пользовательскими атрибутами**

Предупреждение:

Управление доступом к вкладкам СМС влияет только на внешний вид пользовательского интерфейса СМС. Скрытие вкладок СМС не может рассматриваться как увеличение уровня безопасности, поскольку в этом случае не устанавливаются и не изменяются права безопасности на объекты, расположенные на вкладках. Чтобы предотвратить выполнение пользователями запрещенных операций с несанкционированными объектами (например, управление серверами с помощью Central Configuration Manager или сторонних программ на основе пакета SDK платформы BI), необходимо установить соответствующие права безопасности для объектов (например, объектов сервера).

Управление доступом других пользователей к вкладкам СМС

1. Выполните вход в СМС.
2. На вкладке «Пользователи и группы» щелкните правой кнопкой мыши принцепала и выберите пункт **Конфигурация вкладок СМС**.

Примечание:

Если доступ к вкладкам СМС неограничен, отображается следующее сообщение: Предупреждение. Доступ к вкладке СМС не ограничен. Чтобы ограничить доступ к СМС, перейдите к вкладке "Приложение", выберите "СМС" и установите ограниченный доступ к вкладке СМС. Приведенные ниже настройки не будут применены, пока доступ к вкладке СМС не будет ограничен:

Права доступа к вкладкам СМС можно настраивать. Тем не менее, внесенные изменения вступят в силу только после того, как будет ограничен доступ к вкладкам СМС.

В диалоговом окне «Конфигурация доступа к вкладкам СМС» отображается таблица:

- Значки **✓** или **✗** обозначают вкладки СМС, к которым принцепал имеет доступ.
 - «Унаследовано» – право доступа к вкладкам было унаследовано от родительской группы пользователей.
 - «В явном виде» – право доступа к вкладкам было предоставлено явно на уровне принцепала.
3. Проверьте права доступа к вкладкам СМС. Для изменения прав используйте следующие кнопки в панели инструментов:
 - **Предоставить** – явное предоставление права доступа к вкладкам.
 - **Запретить** – явное отклонение права доступа к вкладкам.
 - **Унаследовать** – назначение унаследованного права доступа.

Примечание:

При нажатии перечисленных выше кнопок изменения прав доступа принцепала вступают в силу немедленно.

4. По окончании внесения изменений нажмите **Заккрыть**.

В столбце «Разрешение» таблицы отображается действующее право доступа к вкладкам.

См. также

- [Ограничение доступа к вкладкам СМС](#)

Наследование прав доступа к вкладкам СМС

Права на доступ к вкладкам СМС и разрешения на их настройку для других пользователей и групп применяются и наследуются так же, как и любые другие права безопасности платформы BI. Принципалы, которым явно не назначены права доступа к вкладкам, будут наследовать права доступа групп, участниками которых они являются.

Для пользователей, являющихся участниками двух групп, права доступа к вкладкам рассчитываются аналогично любым другим правам платформы Business Intelligence. Например, если в одной из групп пользователю предоставляются права доступа к вкладкам СМС, а в другой – нет, пользователь соответствующие права не получает.

Примечание:

- Изменение прав доступа к вкладкам СМС для группы влияет на всех пользователей и все группы, которые наследуют их (если для этих пользователей и групп выбран параметр назначения прав **Унаследовано**).
- Права доступа, назначаемые на уровне пользователя, имеют более высокий приоритет по сравнению с наследуемыми от групп.

Группы делегированных администраторов

Чтобы упростить управления вкладками СМС, можно создать набор групп делегированных администраторов. Назначив существующих пользователя или группу пользователя участником группы делегированных администраторов, вы сможете избежать необходимости настраивать доступ к отдельным вкладкам СМС. Рекомендуется следующая конфигурация (при необходимости ее можно изменить в соответствии с конкретными бизнес-требованиями).

Примечание:

Если пользователь или группа участвуют в нескольких группах, права с атрибутом **Унаследовано** суммируются.

Группа делегированных администраторов	Рекомендуемые права
Системные администраторы	Доступ ко всем вкладкам.
Администраторы пользователей	Доступ к вкладкам Уровни доступа, Папки, Входящие, Личные папки, Личные категории, Результаты запросов, Сеансы и Пользователи и группы . Всем остальным вкладкам присвойте атрибут Унаследовано .
Администраторы содержимого	Доступ к вкладкам Календари, Категории, События, Папки, Диспетчер экземпляров, Личные категории, Личные папки, Профили, Результаты запросов и Универсы . Всем остальным вкладкам присвойте атрибут Унаследовано .
Администраторы серверов	Доступ к вкладкам Серверы и Приложения . Всем остальным вкладкам присвойте атрибут Унаследовано .

Управление разрешениями на настройку доступа других пользователей и групп к вкладкам СМС

В крупных корпоративных средах у системного администратора может возникнуть необходимость делегировать функции управления доступом к вкладкам СМС делегированному администратору. Кроме того, в многопользовательской системе каждый клиент может назначать своего делегированного администратора, который отвечает за управление доступом других пользователей и групп к вкладкам СМС.

1. Выполните вход в СМС.
2. На вкладке «Пользователи и группы» щелкните правой кнопкой мыши принципа и выберите пункт **Конфигурация вкладок СМС**.

В диалоговом окне «Конфигурация доступа к вкладкам СМС» для принципа отображается **Разрешение на конфигурацию доступа к вкладке СМС для других пользователей или групп пользователей**.

Примечание:

Если это разрешение предоставлено, принцип имеет право на управление доступом к вкладкам СМС (распространяется только на доступные принципу вкладки) для пользователей, на которых принципу назначено право «Изменение прав в безопасном режиме». Кроме того, такой принцип может делегировать права на управление доступом к вкладкам СМС другим пользователям. Для этого требуется предоставить **Разрешение на конфигурацию доступа к вкладке СМС для других пользователей или групп пользователей** пользователям, на которых принципу назначено право «Изменение прав в безопасном режиме».

- Значки **✓** или **✗** указывают на наличие у принципа разрешений на конфигурацию доступа к вкладкам СМС для других пользователей или групп пользователей.
- «Унаследовано» – разрешение было унаследовано от родительской группы пользователей.
- «В явном виде» – разрешение было предоставлено явно на уровне принципа.

3. Проверьте разрешения на настройку доступа других пользователей и групп к вкладкам СМС. Чтобы изменить разрешения, выберите один из следующих параметров в списке:

- Выберите **Предоставить**, чтобы явно предоставить разрешение на конфигурацию доступа к вкладкам СМС для других пользователей или групп пользователей.
- Выберите **Запретить**, чтобы явно отозвать разрешение на конфигурацию доступа к вкладкам СМС для других пользователей или групп пользователей.
- Выберите **Унаследовать**, чтобы унаследовать разрешение на конфигурацию доступа к вкладкам СМС для других пользователей или групп пользователей.

Примечание:

Изменения разрешений принcipала, выбранные в списке, вступают в силу немедленно.

4. По окончании внесения изменений нажмите **Заккрыть**.

Отображается действующее на данный момент разрешение.

См. также

- [Делегированное администрирование и доступ к вкладкам СМС](#)
- [Наследование прав доступа к вкладкам СМС](#)

Добавление вкладки "Настройка" для пользователя или группы пользователей

Доступ к вкладке СМС должен быть «Ограничен» – только после этого можно будет добавить вкладку **Настройка** для определенного пользователя или группы пользователей.

1. В СМС перейдите в область управления **Пользователи и группы**.
2. Щелкните пользователя или группу пользователей правой кнопкой мыши и выберите **Конфигурация вкладок СМС**.

Отобразится диалоговое окно «Конфигурация вкладок СМС», на которой будет указано название каждой вкладки СМС и ее уровень разрешений для группы пользователей.

Если вверху диалогового окна отобразится следующее предупреждение красным шрифтом, необходимо задать статус доступа к вкладке СМС "Ограничен" – только после этого можно добавить вкладку **Настройка**:

Предупреждение. Доступ к вкладке СМС не ограничен. Чтобы ограничить доступ к СМС, перейдите к вкладке "Приложение", выберите "СМС" и установите ограниченный доступ к вкладке СМС. Приведенные ниже настройки не будут применены, пока доступ к вкладке СМС не будет ограничен:

3. (При необходимости) Ограничение доступа к вкладке СМС:
 - a. В области управления СМС **Приложения** щелкните правой кнопкой мыши **Central Management Console** и выберите **Конфигурация доступа к вкладкам СМС**.
 - b. В разделе **Доступ к вкладкам СМС** выберите **Ограничен** и щелкните **Сохранить и закрыть**.

4. В диалоговом окне «Настройка вкладок СМС» для соответствующей группы пользователей выберите для каждой вкладки СМС одно из следующих значений из списка: **Предоставлен**, **Запрещен** или **Унаследован**.

Всякий раз при изменении разрешения для вкладки в диалоговом окне "Настройка вкладок СМС" обновляется разрешение группы пользователей на настройку доступа к вкладке других пользователей или групп пользователей.

5. Нажмите кнопку **Заккрыть**.

Ограничение доступа к вкладкам СМС

Рекомендуется ограничить доступ к вкладкам СМС после того, как будут настроены права доступа к вкладкам СМС для принципалов. Если ограничить доступ к вкладкам до того, как он будет настроен, пользователи не смогут работать с любыми вкладками СМС, пока администратор не предоставит им соответствующие права.

Чтобы обеспечить согласованность конфигурации с предыдущими версиями платформы Business Intelligence, доступ к вкладкам СМС после установки платформы BI изначально не ограничен, в связи с чем пользователи с правами доступа к СМС могут работать с любыми существующими вкладками. Чтобы запретить пользователям доступ к вкладкам, на которые у них нет прав, системный администратор может ограничить доступ к вкладкам СМС.

Ограничение на доступ к вкладкам СМС рекомендуется снимать только в экстренном случае или для устранения неполадок с конфигурацией доступа (например, если делегированному администратору не удастся получить доступ к важной вкладке СМС).

1. Выполните вход в СМС.
2. На вкладке «Приложения» щелкните правой кнопкой мыши элемент **Central Management Console** и выберите пункт **Конфигурация доступа к вкладкам СМС**.
Откроется диалоговое окно «Доступ к вкладке СМС».
3. Настройте правила доступа к вкладкам СМС.
 - Чтобы ограничить доступные пользователям вкладки только теми, на которые у них есть права, выберите **Ограничен**.
 - Чтобы разрешить пользователям доступ ко всем вкладкам, выберите **Неограничен**.
4. По окончании внесения изменений нажмите кнопку **Сохранить и закрыть**.

Правило доступа к вкладкам СМС применяется к системе.

См. также

- [Устранение неполадок с доступом к вкладкам СМС](#)

Устранение неполадок с доступом к вкладкам СМС

Чтобы запретить несанкционированный доступ или устранить неполадки, связанные с ограничением доступа пользователей к вкладкам СМС, можно изменить права доступа пользователей к вкладкам СМС.

1. Войдите в консоль СМС с правами администратора.

Примечание:

Убедитесь, что у вас есть права доступа к вкладке, для которой требуется устранить неполадки, а также право «Изменение прав в безопасном режиме» для нужного пользователя.

2. На вкладке «Пользователи и группы» щелкните правой кнопкой мыши принципала и выберите пункт **Конфигурация вкладок СМС**.

Откроется окно «Конфигурация доступа к вкладкам СМС».

3. Проверьте действующие права доступа к вкладкам СМС. При необходимости вы можете явно предоставить или отозвать права доступа к доступным вкладкам.

Если права доступа к вкладкам СМС унаследованы, однако действующие права доступа не соответствуют потребностям пользователя, выполните следующие действия:

- a. Составьте список всех групп, участником которых является выбранный принципал.
- b. Повторите шаги с 1 по 3 для каждой группы, права доступа к вкладкам которой наследует пользователь.
- c. При необходимости исправьте права доступа к вкладкам СМС на уровне принципала или ниже уровня группы.

Примечание:

Выполнение этой задачи на уровне группы повлияет на права доступа к вкладкам СМС для всех пользователей, являющихся участниками этой группы, а также всех унаследованных от нее групп (если для этих пользователей настроен параметр прав доступа к вкладкам СМС **Унаследовано**).

4. По окончании внесения изменений нажмите **Заккрыть**.

См. также

- [Управление доступом других пользователей к вкладкам СМС](#)
- [Наследование прав доступа к вкладкам СМС](#)

18.1.3.2 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.

18.1.3.2.1 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 > Управление темами**.
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 дискуссии, в которых заголовок темы или имя автора полностью соответствуют тексту, введенному в третьем поле.
не является	Поиск любых тем дискуссии, 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 дискуссии, которые были созданы или изменены ранее иско- мой даты.
После	Поиск тем дискуссии, которые были созданы или изменены позднее даты поиска.
между	Поиск тем дискуссии, которые были созданы или изменены в период между двумя датами поиска.

- 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.
- Нажмите кнопку **Поиск**.

18.1.3.2.2 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.

- Перейдите к области «Приложения» в СМС и выберите пункт **Дискуссии**.
- Щелкните **Управление > Управление темами**.
Открывается диалоговое окно «Управление заметками».
- 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 измене- ния	Сортировка по дате последнего изменения тем дискуссий.
Автор	Сортировка по автору определенной темы дискуссии.

- Во втором списке можно выбрать отображение записей в возрастающем или убывающем порядке.
- В третьем текстовом поле укажите число отображаемых на одной странице результатов поиска тем дискуссий.
По умолчанию на одной странице отображаются 10 результатов.
- Щелкните **Поиск**.

18.1.3.2.3 Удаление темы дискуссии

В области «Приложения» СМС в платформе BI можно удалить любую тему дискуссии.

1. Перейдите к области «Приложения» в СМС и выберите пункт **Дискуссии**.
2. Щелкните **Управление > Управление темами**.
Открывается диалоговое окно «Управление заметками».
3. В списке результатов найдите тему дискуссии, которую требуется удалить, и выделите ее.
4. Щелкните **Удалить**.

18.1.3.3 Управление настройками стартовой панели BI

Чтобы открыть свойства стартовой панели BI, в области **Приложения** консоли СМС платформы BI выберите **Управление > Свойства**.

При использовании стартовой панели BI пользователям и группам можно предоставить следующие возможности:

- Изменение предпочтений
- Организация папок
- 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.

18.1.3.3.1 Для изменения параметров отображения стартовой панели BI

1. Перейдите к области **Приложения** в СМС и выберите пункт **Стартовая панель BI**.
Откроется диалоговое окно «Свойства стартовой панели BI».
2. Для включения дискуссий для пользователей стартовой панели BI выберите **Включить дискуссии**.
3. Чтобы использовать фильтры при планировании, установите флажок **Отображать вкладку "Фильтры" на странице "Расписание"**.
Эта настройка определяет, могут ли пользователи вводить записи или формулы выбора группы при планировании отчетов Crystal.
4. Нажмите **Сохранить и закрыть**.

18.1.3.4 Управление настройками Web Intelligence

Для документов Web Intelligence можно определить, к каким функциям будут иметь доступ пользователи, задав свойства для приложения Web Intelligence.

18.1.3.4.1 Изменение параметров отображения для Web Intelligence

1. Перейдите в область «Программные приложения» в СМС и выберите пункт **Web Intelligence**.
2. Выберите команду **Управление > Свойства**.
Отобразится диалоговое окно «Свойства».
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.
«Настройки автоматического сохранения»	Установите периодичность автоматического сохранения документов. Отсчет этого интервала времени сбрасывается каждый раз при сохранении документа вручную или автоматически. При сохранении документа вручную автоматически сохраненная копия документа удаляется.

Действие	Описание
«Автоматическое обновление»	<p>Активирует автоматическое обновление документов Web Intelligence, если выбрано свойство документа Web Intelligence Автоматическое обновление.</p> <p>Для получения подробных сведений см. <i>Руководство пользователя SAP BusinessObjects Web Intelligence</i>.</p>

Действие	Описание
«Автоматическое слияние»	<p>Включение автоматического объединения измерений, если выбрано свойство документа Web Intelligence Автоматическое объединение измерений.</p> <p>Для получения подробных сведений см. <i>Руководство пользователя SAP BusinessObjects Web Intelligence</i>.</p>
«Автоматическое обновление документов в настройке права на открытие системы безопасности»	<p>Этот флажок следует снять, чтобы включить в Web Intelligence автоматическое обновление документов при их открытии, без включения параметра Обновлять при открытии в свойствах документа Web Intelligence. При выборе этого параметра выбирается право системы безопасности Документы - отключить автоматическое обновление по открытию.</p>
«Smart View»	<p>Этот параметр определяет, какая версия документа будет отображаться, когда пользователи открывают документы в Web Intelligence.</p> <ul style="list-style-type: none"> Просмотреть последний экземпляр <p>Будет открыт последний экземпляр объекта. Например, если для документа запланировано обновление с периодичностью раз в час, а документ был сохранен и закрыт пять часов назад, открывается последний экземпляр. Когда пользователь сохраняет этот экземпляр, исходный документ обновляется соответствующим образом.</p> Просмотр объекта <p>Документ открывается в том же состоянии, в котором он был сохранен в последний раз, независимо от выполненных запланированных обновлений.</p>

4. Нажмите кнопку **Сохранить и закрыть**.

Примечание:

Чтобы вернуть значения отображения по умолчанию, нажмите кнопку **Сброс**.

18.1.3.5 Управление настройками предупреждений

В области «Приложения» СМС платформы ВІ можно задать для предупреждений настройки на уровне системы.

Приложение «Предупреждения» 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](#)

18.1.3.5.1 Изменение свойств места назначения предупреждений

1. В области **Приложения** в СМС дважды щелкните **Приложение предупреждения**.

2. Выберите **Управление > Свойства**.

Откроется диалоговое окно «Предупреждения».

3. (Обязательно) Выполните одно из следующих действий:

- Выберите **Включить мои предупреждения**, чтобы предоставить возможность подписчикам на предупреждения получать уведомления в разделе **Мои предупреждения** на стартовой панели ВІ.
- Выберите **Включить электронную почту**, чтобы предоставить подписчикам на предупреждения возможность получать уведомления по электронной почте.

Откроется окно глобальных параметров электронной почты для предупреждений.

4. Если выбран параметр **Включить электронную почту**, выполните следующие действия:

- В поле **От** введите адрес электронной почты, с которого будут отправляться уведомления о предупреждениях.

Подписчики будут получать электронную почту с предупреждениями с этого адреса.

Рекомендуется использовать действительный адрес электронной почты, известный системе.

- В поле **Кому** введите адрес электронной почты получателя предупреждений.

По умолчанию на этот адрес будут отправляться все системные предупреждения.

Совет:

Не указывайте адрес или получателя электронной почты. Введите заменитель **%SI_EMAIL_ADDRESS%**.

- В поле **Копия** введите адреса электронной почты получателей копии предупреждения.
- В поле **Тема** введите заголовок темы, который по умолчанию должен использоваться в сообщениях электронной почты с предупреждениями.
- В поле **Сообщение** введите сообщение по умолчанию для электронной почты с предупреждениями.
- Выберите **Добавить приложение**, чтобы в электронную почту с предупреждениями по умолчанию добавлялись приложения.

Например, выберите этот параметр, чтобы включать связанные отчеты Crystal с инициированными предупреждениями.

- Если выбран параметр **Добавить приложение**, в поле **Имя файла** выберите **Создаваемый автоматически** или **Конкретное имя**, чтобы указать, как должны именоваться приложения в сообщениях электронной почты.

5. Нажмите **Сохранить и закрыть**.

См. также

- [Настройка пользовательских прав на приложения](#)
- [Управление настройками предупреждений](#)

18.1.3.5.2 Изменение свойств предупреждений 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 предупреждений](#)

18.1.3.6 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.

18.1.3.7 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.

18.1.3.7.1 Изменение свойств приложения SAP BusinessObjects Explorer

1. Перейдите в область «Программные приложения» СМС.
2. Выберите **Управление > Свойства**.
Отобразится диалоговое окно «Свойства».
3. Определите любую из следующих настроек SAP BusinessObjects Explorer:
 - Действительность закладок
 - Расширенная конфигурация
4. Нажмите **Сохранить и закрыть**.

18.1.3.8 Управление интеграцией приложений сотрудничества

Включить и настроить сотрудничество с приложениями SAP Jam и SAP StreamWork можно в области **Приложения** консоли СМС платформы BI.

В агенте Enterprise приложения сотрудничества необходимо выполнить следующие дополнительные настройки:

- Установить соединение HTTPS с поставщиком услуг.
- Выполнить предварительные требования для аутентификации.

В связи с использованием разных методов аутентификации (SAML 2.0 и OAuth 1.0a) описание занимает большую часть документа. После настройки приложения сотрудничества в стартовой панели BI будут доступны веб-каналы приложений SAP Jam и SAP StreamWork.

Целевая аудитория

Администраторы платформы SAP BusinessObjects BI, отвечающие за интеграцию платформы BI с приложениями сотрудничества SAP Jam и SAP StreamWork.

18.1.3.9 Предварительные условия для сотрудничества

В этом разделе приводятся основные предварительные условия для использования платформы Business Intelligence (BI) с приложениями сотрудничества.

- Установлена платформа BI как минимум с одним центральным сервером управления (CMS).
- В консоли CMS настроено приложение сотрудничества (SAP Jam или SAP StreamWork).
- Определена организация Enterprise для приложения сотрудничества (SAP Jam или SAP StreamWork).
- В организацию Enterprise добавлены пользователи SAP Jam или SAP StreamWork.

Примечание:

SAP StreamWork Enterprise Agent используется только для подготовки пользователей с применением локальной службы каталогов LDAP/AD.

18.1.3.10 Конфигурация платформы BI

18.1.3.10.1 Параметры настройки сотрудничества

В этой таблице описываются параметры консоли CMS на платформе BI, относящиеся к интеграции с SAP Jam или SAP StreamWork.

В диалоговом окне консоли CMS «Свойства: сотрудничество» доступны перечисленные ниже параметры. Для доступа к этим параметрам перейдите на вкладку **Приложения**, щелкните **Сотрудничество** и в меню **Управление** выберите **Свойства**.

Действие	Описание
Включить сотрудничество	Установите этот флажок и выберите приложение SAP Jam или SAP StreamWork .
URL соединения	Введите URL приложения сотрудничества.
Уникальный идентификатор поставщика сущности	<p>Введите значение, используемое для развертывания платформы BI. Это значение будет связано с сертификатом, используемым для настройки интеграции в консоли администрирования приложения сотрудничества.</p> <p>Примечание: Приложение, добавляющее сущность для единого входа, должно быть настроено как приложение администрирования OAuth.</p>
Сертификат Base64 поставщика сущности	После нажатия кнопки Создать в поле Сертификат Base64 поставщика сущности создается сертификат. Используйте этот сертификат в консоли администрирования SAP StreamWork для создания ключа клиента OAuth. Этот сертификат позволяет установить отношение доверия между приложением сотрудничества и платформой BI. Сам внешний поставщик сущностей определяется сертификатом X509, который используется для подписи всех добавляемых сущностей. Сертификат должен быть закодирован в формате Base64.
Ключ потребителя OAuth	Используйте это поле для ввода ключа потребителя OAuth, созданного в консоли администрирования приложения сотрудничества.

Действие	Описание	
Подключе- ние через прокси	<p>Установите этот флажок, чтобы включить соединение через прокси. Необходимо указать определенные сведения о прокси-хосте в полях Хост прокси HTTP и Порт.</p> <p>Совет: Чтобы разрешить входящие соединения от серверов приложений сотрудничества с корпоративной сетью, требуется обратный прокси в демилитаризованной зоне.</p> <p>Примечание: Для добавления доверенного сертификата от поставщика сертификатов SSL на обратный прокси вам потребуется имя домена или поддомена для обратного прокси.</p>	
	Хост прокси HTTP	<p>В настройках обратного прокси введите внешний адрес, доступный приложению сотрудничества. Например, введите <code>https://ReverseProxy/</code>, где атрибут <code>ReverseProxy</code> определяет имя домена или поддомена для обратного прокси.</p> <p>Этот адрес используется приложением сотрудничества для отправки данных на платформу BI. Обратный прокси использует этот адрес для перенаправления данных, полученных от приложения сотрудничества, на компьютер с агентом Enterprise Agent приложения сотрудничества.</p>
	Порт	Агент Enterprise Agent приложения сотрудничества настраивается для прослушивания порта 8443.

18.1.3.10.2 Включение и настройка сотрудничества в консоли СМС

Для выполнения этой задачи требуется действующее соединение с консолью администрирования приложения сотрудничества (SAP Jam или SAP StreamWork). Потребуется передавать в консоль данные о безопасности и извлекать их оттуда.

В целях безопасности следующим учетным записям запрещено передавать или планировать содержимое в SAP Jam или SAP StreamWork:

- Гость
- SMAdmin
- Администратор
- WaaWSServletPrincipal

1. В консоли СМС в платформе BI перейдите в область **Приложения** и дважды щелкните **Сотрудничество**.
2. В диалоговом окне «Свойства: сотрудничество» установите флажок **Включить сотрудничество** и выберите приложение **SAP Jam** или **SAP StreamWork**.
3. В поле **URL соединения** введите URL приложения сотрудничества.
4. В поле **Уникальный идентификатор поставщика удостоверения** введите значение уникального идентификатора поставщика удостоверений для вашего развертывания платформы BI.
Запишите это значение поставщика удостоверений, оно будет использоваться впоследствии для настройки приложения сотрудничества.
5. Щелкните **Сгенерировать** (или **Регенерировать**, если сертификат был создан ранее).
В поле **Сертификат Base64 поставщика удостоверений** будет создан сертификат. Это значение сертификата будет использоваться для настройки приложения сотрудничества.
6. В поле **Ключ потребителя OAuth** введите действительный ключ потребителя OAuth.
Ключ потребителя OAuth создается в приложении сотрудничества.
7. Если соединение с сервером SAP Jam или SAP StreamWork осуществляется через прокси, выполните следующие действия:
 - a. Установите флажок **Подключение через прокси**.
 - b. В поле **Хост прокси HTTP** введите имя хоста прокси для сервера.
 - c. В поле **Порт** введите номер порта для сервера.
8. Нажмите **Сохранить и закрыть**.

18.1.3.11 Конфигурация SAP Jam

18.1.3.11.1 Регистрация нового доверенного IDP SAML для SAP Jam

Перед регистрацией нового доверенного IDP SAML:

- Необходимо добавить и настроить компанию в SAP Jam.
- Необходимо создать действительную учетную запись пользователя SAP Jam, связанную с вашей компанией в SAP Jam.
- Необходимо получить права администратора компании в SAP Jam и полные права администратора платформы BI и стартовой панели BI.
- Стартовая панель BI должна быть зарегистрирована в SAP Jam в качестве клиента OAuth, который является ее представлением в SAP Jam.

Примечание:

Каждый пользователь должен быть зарегистрирован в SAP Jam при помощи уникального адреса электронной почты, соответствующего адресу Enterprise пользователя в стартовой панели BI. Адреса электронной почты в платформе BI и SAP Jam сопоставляются.

1. В верхнем правом углу в меню **Администратор** SAP Jam выберите пункт **Администратор**. На экран будут выведены сведения о вашей компании в SAP Jam, включая лицензию SAP Jam. Запомните или запишите эту информацию.
2. В меню **Администратор** выберите **Доверенные IDP SAML** и щелкните **Регистрация поставщика удостоверений**.
Необходимо зарегистрировать IDP, созданный в стартовой панели BI.
3. (Обязательно) В поле **IDP ID** введите значение уникального поставщика удостоверений, который был создан при настройке SAP Jam в платформе BI.
Если это значение неизвестно, обратитесь к администратору внешних приложений.
Например, введите `<имя_компании>_<Ид._системы>_<клиент>`
4. В поле **URL для единого входа** введите URL прямой ссылки на SAP Jam.
Приложение SAP Jam использует этот URL для единого входа в уникальный поставщик удостоверений.
5. В поле **URL для единого выхода** введите URL, который будет отображаться при выходе из SAP Jam.
Приложение SAP Jam использует этот URL для единого выхода из уникального поставщика удостоверений.
6. В поле **Формат идентификатора имени по умолчанию** введите формат идентификатора имени, который должен использоваться в запросах на аутентификацию.
7. В поле **Классификатор имени принципа службы для идентификатора имени по умолчанию** введите квалификатор имени принципа, который будет использоваться в запросах аутентификации.
8. (Обязательно) В списке **Allowed Assertion Scope** выберите **Users in my company**.
Этот параметр определяет набор пользователей, для которых приложение SAP Jam будет принимать утверждения из IDP.
9. (Обязательно) В поле **Сертификат X509 (Base64)** введите значение сертификата Base64, созданное при настройке SAP Jam в платформе BI.
Если это значение неизвестно, обратитесь к администратору внешних приложений.
10. Нажмите кнопку **Зарегистрировать**.

18.1.3.11.2 Создание клиента OAuth для SAP Jam

Перед созданием ключа потребителя OAuth:

- Необходимо добавить и настроить компанию в SAP Jam.
- Необходимо создать действительную учетную запись пользователя SAP Jam, связанную с вашей компанией в SAP Jam.
- Необходимо получить права администратора компании в SAP Jam и полные права администратора платформы BI и стартовой панели BI.
- Стартовая панель BI должна быть зарегистрирована в SAP Jam в качестве клиента OAuth, который является ее представлением в SAP Jam.

Примечание:

Каждый пользователь должен быть зарегистрирован в SAP Jam при помощи уникального адреса электронной почты, соответствующего адресу Enterprise пользователя в стартовой панели BI. Адреса электронной почты в платформе BI и SAP Jam сопоставляются.

1. В верхнем правом углу в меню **Администратор** SAP Jam выберите пункт **Администратор**.
На экран будут выведены сведения о вашей компании в SAM Jam, включая лицензию SAP Jam.
2. В меню **Администратор** выберите **Клиенты OAuth** и щелкните **Добавить клиент OAuth**.
3. В диалоговом окне «Регистрация нового клиента OAuth» в поле **Имя** введите уникальное имя поставщика удостоверений, созданное при настройке SAP Jam в платформе BI.
Если это значение неизвестно, обратитесь к администратору внешних приложений.
При выполнении действий от имени пользователя в SAP Jam имя приложения отображается в виде гиперссылки на введенный URL-адрес.
Например, введите `<имя_компании>_<Ид._системы>_<клиент>_<приложение>`
4. В поле **URL интеграции** введите URL-адрес для прямого доступа к стартовой панели BI.
При выполнении действий от имени пользователя в SAP Jam имя приложения отображается в виде гиперссылки на этот URL.
5. В поле **Сертификат X509 (Base64)** введите значение сертификата Base64, созданное при настройке SAP Jam в платформе BI.
Если это значение неизвестно, обратитесь к администратору внешних приложений.
Если это поле не заполнено, приложение SAP Jam использует секретный ключ потребителя.
6. Нажмите кнопку **Сохранить**.
Ключ потребителя OAuth сгенерирован. Запишите значение ключа потребителя OAuth для дальнейшего использования администратором платформы BI.

18.1.3.12 Конфигурация SAP StreamWork

18.1.3.12.1 Пример интеграции с SAP StreamWork

На этом рисунке показаны компоненты платформы BI, SAP StreamWork и SAP StreamWork Enterprise Agent, необходимые для интеграции с SAP StreamWork.

В этом рабочем процессе описываются шаги по интеграции систем и приводится обзор действий, которые пользователи могут выполнять после интеграции:

- SAP StreamWork Enterprise Agent обеспечивает подготовку пользователей Enterprise из LDAP для SAP StreamWork.

- В консоли CMC платформы BI администраторы могут создавать пользователей и сопоставлять их с пользователями Enterprise.
- В стартовой панели BI пользователи могут создавать мероприятия и просматривать их в браузере, не создавая учетной записи и не входя в SAP StreamWork.
- В стартовой панели BI пользователи могут просматривать каналы SAP StreamWork и отвечать на них.

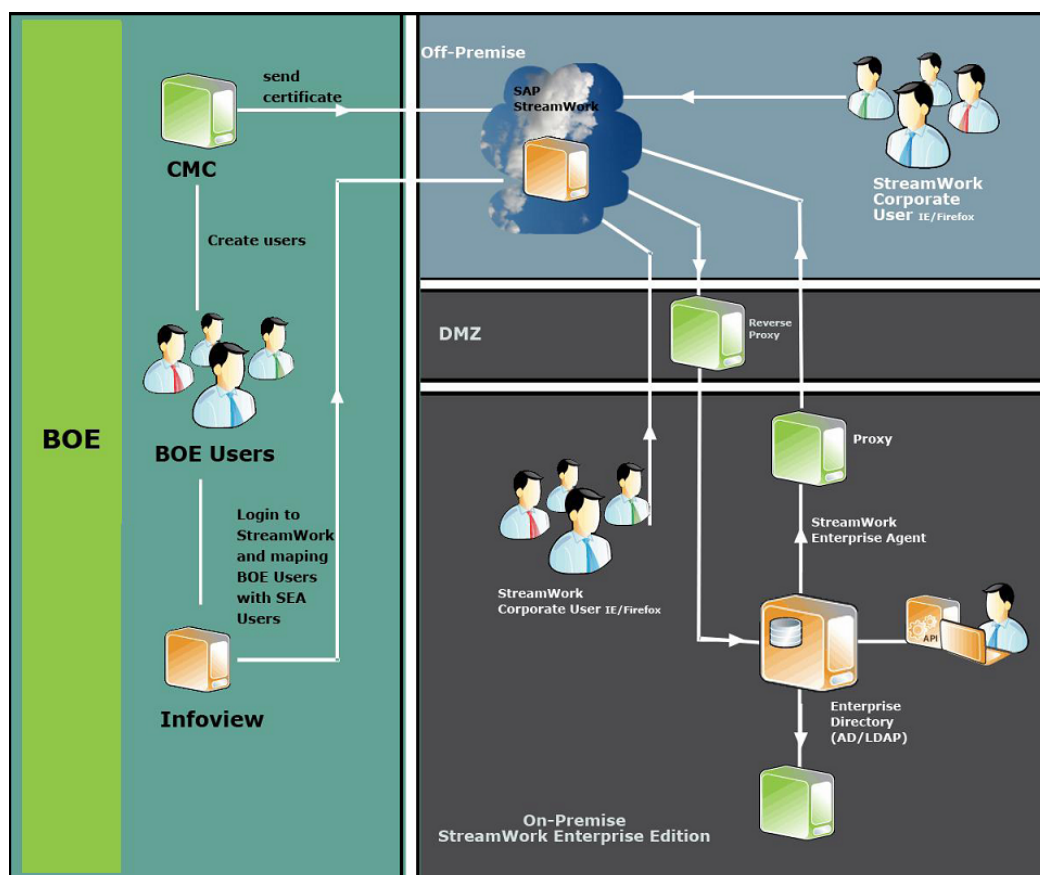


Рис. 18-1: System landscape

18.1.3.12.2 Создание ключа потребителя OAuth для SAP StreamWork

Для создания ключа потребителя OAuth требуются права администратора организации SAP StreamWork Enterprise.

1. В консоли администрирования SAP StreamWork на вкладке **Администрирование** выберите **Доверенные IDP SAML** и войдите в SAP StreamWork с использованием учетной записи с правами администратора организации Enterprise.
2. Щелкните **Регистрация поставщика удостоверений**.
3. Выберите **Щелкните здесь, чтобы создать новое приложение администрирования OAuth** и примите соглашение об условиях использования.
4. Выполните следующие действия в окне **Зарегистрировать новое приложение OAuth**:

- a. В поле **Имя приложения** введите имя экземпляра приложения, используемого для интеграции.
Эти сведения определяют приложение, которое будет выполнять действия от лица пользователя, например, публиковать каналы SAP StreamWork. Имя приложения должно быть понятно пользователям.
- b. В поле **URL интеграции** введите URL-адрес для прямого доступа к стартовой панели BI.
- c. В поле **Сертификат Base64 X509** введите значение сертификата Base64, созданное при настройке SAP StreamWork в Central Management Console (CMC) в платформе BI.

Если у вас нет значения, обратитесь к администратору приложения.

5. Нажмите кнопку **Зарегистрировать.**

Ключ потребителя OAuth сгенерирован. Запишите значение ключа потребителя OAuth для дальнейшего использования администратором платформы BI.

6. Нажмите кнопку **Назад, чтобы отобразить доверенные поставщики удостоверений SAML.**

7. Выполните следующие действия в окне «Регистрация нового доверенного поставщика удостоверений SAML»:

- a. В поле **Отображаемое имя** введите имя развертывания платформы BI.
Это имя будет отображаться для пользователей SAP StreamWork.
- b. В поле **IDP ID** введите уникальное значение поставщика удостоверений, созданное при настройке SAP StreamWork в платформе BI.
Если у вас нет этого значения, обратитесь к администратору приложения.
- c. В поле **Сертификат Base64 X509** введите значение сертификата Base64, созданное при настройке SAP StreamWork в платформе BI.
Если у вас нет этого значения, обратитесь к администратору приложения.

8. Нажмите кнопку **Зарегистрировать.**

18.1.3.12.3 Добавление SAP StreamWork в рабочее пространство BI

SAP StreamWork не отображается, необходимо вручную включить отображение в списке модулей стартовой панели BI, которые можно добавить в рабочее пространство BI.

1. Найдите файл `home-analyticlist.xml` в папке

`C:\BusinessObjects\tomcat\work\Catalina\localhost\BOE\eclipse\plugins\webpath.PerformanceManagement\web\WEB-INF\lib\asdk-ivdm_ext.jar\conf-syst\conf-syst\.`

Содержимое файла должно начинаться со следующего текста:

```
<?xml version="1.0" encoding="UTF-8"?>

<CHOICE>

<!--<SW_ACTIVITIES NAME="$MSG_SW_ACTIVITIES$"
DESCRIPTION="$MSG_SW_ACTIVITIESDESC$"/>-->

<!--SW_FEED NAME="$MSG_SW_FEED$" DESCRIPTION="$MSG_SW_ACTIVITIESDESC$"/-->
```

```
<HOMEINBOX NAME="$MSG_HOMEINBOX$" DESCRIPTION="$MSG_HOMEINBOXDESC$"/>

<HOMEAPPLICATIONS NAME="$MSG_HOMEAPPLICATIONS$"
DESCRIPTION="$MSG_HOMEAPPLICATIONSDESC$"/>

<HOMERECENTLYRUNDOCS NAME="$MSG_HOMERECENTLYRUNDOCS$"
DESCRIPTION="$MSG_HOMERECENTLYRUNDOCSDESC$"/>

<HOMERECENTDOCS NAME="$MSG_HOMERECENTDOCS$"
DESCRIPTION="$MSG_HOMERECENTDOCSDESC$"/>

<HOMEALERTS NAME="$MSG_ALERTNOTIFICATIONS$"
DESCRIPTION="$MSG_ALERTNOTIFICATIONSDESC$"/>

</CHOICE>
```

2. Удалите символы `!--` из строк `SW_ACTIVITIES NAME=` и `SW_FEED NAME=`.
3. Перезапустите сервер Tomcat.

Канал **SAP StreamWork** появится в списке **Модули стартовой панели BI** в библиотеке модулей для рабочих пространств BI, расположенной в стартовой панели BI.

18.1.3.13 Управление настройками поиска по платформе

В области «Приложения» CMC платформы BI можно задать настройки на уровне системы для приложения поиска по платформе.

См. также

- [Список сбоев индексации](#)
- [Настройка свойств приложения в CMC](#)

18.1.3.13.1 Настройка свойств приложения в CMC

Чтобы настроить свойства приложения поиска по платформе, выполните следующие действия:

1. Перейдите в область «Программные приложения» CMC.
2. Выберите **Приложение поиска по платформе**.
3. Выберите команду **Управление > Свойства**. Появится диалоговое окно «Свойства».
4. Выполните настройку следующих параметров платформы:

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>Для остановки индексации нажмите Остановить индексацию.</p>
Региональные параметры индекса по умолчанию	<p>При поиске на платформе используются региональные параметры, указанные на странице СМС для индексации всех нелокализованных документов VI. Когда документ локализован, для индексации используется соответствующий файл анализа языка.</p> <p>Поиск основан на региональных параметрах продукта клиента, приоритет отдается региональным параметрам продукта клиента.</p> <p>Приоритет можно настроить на странице настройки СМС.</p>

Действие	Описание
Периодичность поиска	<p>Индексацию всего репозитория платформы SAP BusinessObjects 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 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> справки по поиску по платформе в <i>интерактивной справке СМС по платформе SAP BusinessObjects Business Intelligence</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>Индексы хранятся 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 процесса поиска начальные попадания извлекаются по основному индексу, а индексы проверки орфографии используются для извлечения предположений. В кластеризованном развертывании платформы BI 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, {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Имя сервера>\ContentStores.</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"> {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Имя сервера>\ContentStores. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Имя сервера 1>\ContentStores. <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. Индексы 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>

Действие	Описание
	<ul style="list-style-type: none"> • Все места размещения индексов должны иметь общий доступ. • Чтобы изменить расположение индекса, нажмите кнопку Остановить индексацию. • При изменении расположения индекса скопируйте 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 подсказок 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"> • Crystal Reports • Web Intelligence • Юниверс • Рабочее пространство BI • Microsoft PowerPoint • Adobe Acrobat • Формат RTF • Текст • Microsoft Word • Microsoft Excel

Действие	Описание
Перестроить индекс	<p>Эта функция удаляет все существующие индексы и повторно индексирует весь репозиторий.</p> <p>Функцию Перестроить индекс можно использовать независимо от состояния индексации. Существующий индекс удаляется при сохранении изменений, внесенных на странице свойств. Тем не менее, если индексация остановлена, индекс не будет перестроен до перезапуска индексации.</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.

18.1.3.14 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 платформы SAP BusinessObjects Business Intelligence. Авторы веб-приложений BEx могут выполнять веб-приложения непосредственно в стартовой панели BI в конструкторе веб-приложений BEx.

Для интеграции веб-приложений BEx в платформу SAP BusinessObjects Business Intelligence 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 соединение с системой 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 SAP BusinessObjects Business Intelligence 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:

Интеграция поддерживается, начиная со следующих выпусков SAP NetWeaver:

- SAP NetWeaver 7.0 с пакетом расширения 1 и накопительным пакетом поддержки 8
- SAP NetWeaver 7.3 с накопительным пакетом поддержки 1

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 SAP BusinessObjects Business Intelligence, 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 SAP BusinessObjects Business Intelligence и SAP NetWeaver BW не включен. Для каждого сеанса платформы BusinessObjects Business Intelligence 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.
- Инструментальные панели на основе запросов или представлений запросов BEx, созданные в SAP BusinessObjects Dashboards, не поддерживаются.

Подробнее о возможностях веб-приложений BEx см. на справочном портале SAP в разделе <http://help.sap.com>: **SAP NetWeaver 7.3 > SAP NetWeaver Library: Function-Oriented View > Business Warehouse > SAP 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 соединения с системой BW](#)
- [Настройка соединения между конструктором веб-приложений BEx и платформы BusinessObjects Business Intelligence](#)

18.1.3.14.1 Запуск сервера для веб-приложений BEx

Перед выполнением этой задачи адаптивный сервер обработки должен быть в состоянии "Остановлено".

1. Войдите в Central Management Console (CMC).
2. Выберите **Серверы**.
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. Переместите **службу веб-приложений ВЕх** из списка **доступных служб** в список служб справа.
6. Перезапустите службу веб-приложений ВЕх, перезапустив настраиваемый сервер обработки.

18.1.3.14.2 Запуск отдельного сервера для веб-приложений ВЕх

1. Войдите в Central Management Console (CMC).
2. Выберите **Серверы**.
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 узел в поле **Клонировать в узле**.
6. Выберите клонированный сервер и выберите в контекстном меню команду **Выбрать службы**.
7. Выберите **службу веб-приложений ВЕх** в списке **доступных служб** и переместите ее в список служб справа.
8. Запустите службу веб-приложений ВЕх, запустив новый настраиваемый сервер обработки.

18.1.3.14.3 Настройка параметров сервера

1. Войдите в Central Management Console (CMC).
2. Выберите **Серверы**.
3. Разверните узел **Категории служб** и выберите пункт **Analysis Services**.
4. Выберите сервер, на котором установлена служба веб-приложений ВЕх, а затем в контекстном меню выберите команду **Свойства**.
5. В разделе **Конфигурация службы веб-приложений ВЕх** в области «Служба веб-приложений ВЕх» настройте следующие параметры:
 - a. Проверьте (и при необходимости измените) максимальное число сеансов работы клиентов.
 - b. В разделе **Главная система SAP BW** введите имя OLAP-соединения с системой BW, созданной в платформе SAP BusinessObjects Business Intelligence. Имя по умолчанию – **SAP_BW**.
 - c. В поле **RFC-адресат JCo-сервера** введите имя, которое было введено в системе BW в разделе **Конфигурация RFC-соединений** (код транзакции sm59).
 - d. В поле **Хост шлюза JCo-сервера** введите имя, определенное в системе BW в разделе **Конфигурация RFC-соединений** (код транзакции sm59).
 - e. В поле **Служба шлюза JCo-сервера** введите имя, определенное в системе BW в разделе **Конфигурация RFC-соединений** (код транзакции sm59).
 - f. Проверьте и при необходимости измените значение в поле **Число соединений с JCo-сервером**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. Выберите сервер, на котором установлена служба веб-приложений ВЕх, 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](#)

18.1.3.14.4 Проверка соединения с системой BW

1. Войдите в Central Management Console (CMC).
2. Нажмите кнопку **Соединения OLAP**.
3. Проверьте, было ли установлено соединение с системой BW. Если нет, установите его, нажав кнопку **Новое соединение**. Имя по умолчанию для соединения – 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 соединения, убедитесь, что права доступа к нему имеются только у администраторов.

- a. Для этого щелкните соединение с системой 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.

18.1.3.14.5 Настройка соединения между конструктором веб-приложений BEx и платформы BusinessObjects Business Intelligence

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 BusinessObjects Business Intelligence, нужно создать RFC-адресат 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 BusinessObjects Business Intelligence.
 - c. В поле **Префикс URL** введите URL-адрес сервера WACS платформы BusinessObjects Business Intelligence, 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](#)

Создание RFC-адресата в системе ABAP

Для интеграции системы BW и платформы BusinessObjects Business Intelligence требуется RFC-адресат. RFC-адресат делает возможным взаимодействие между системой BW и платформой BusinessObjects Business Intelligence.

1. Запустите **Конфигурация RFC-соединений** (код транзакции SM59).
2. Нажмите кнопку **Создать**.
3. Обслуживание RFC-адресата:
 - a. Введите имя RFC-адресата.
 - b. Выберите тип соединения **Т 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-адресат сервера JCo), указанным при создании места назначения для данной системы BW на сервере платформы BusinessObjects Business Intelligence.
 - f. В разделе **Технические настройки** в подразделе **Параметры шлюза** введите хост шлюза и службу шлюза, которые используются сервером платформы BusinessObjects Business Intelligence 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](#)

18.1.3.15 Настройка единого входа в SAP HANA

В области «Приложения» консоли СМС в платформе BI можно настроить единый вход для соединений с базой данных SAP HANA. Единый вход реализован с использованием языка SAML.

После запуска сеанса работы платформы BI появляется возможность создать SAML-билет, который можно использовать для входа в SAP HANA без необходимости указывать пароль.

Это базовый рабочий процесс, связанный с подключением к источникам данных SAP HANA:

1. Отношения доверия между SAP HANA и платформой BI настраиваются администратором в консоли СМС.
2. Пользователь может войти в платформу BI с использованием любого из поддерживаемых поставщиков аутентификации.
3. Если идентификаторы пользователей SAP HANA и платформы BI совпадают, платформа BI может создать утверждение SAML, принимаемое SAP HANA для установки соединения для текущего пользователя. В SAP HANA передается идентификатор пользователя, выполнившего вход в платформу BI.
4. Клиентское приложение платформы BI создает соединение с SAP HANA.

Примечание:

Перед настройкой единого входа SAP HANA с SAML необходимо настроить SSL на компьютере SAP HANA. Для получения подробных сведений см. документацию SAP HANA.

18.1.3.15.1 Создание соединения SAP HANA

1. Получите нужные параметры базы данных SAP HANA.
 - a. Откройте приложение SAP HANA Studio.
 - b. Откройте страницу свойств для своей системы и найдите URL-адрес для соединения с базой данных.
 - c. Запишите имя компьютера и номер порта.
Эти данные потребуются в шаге 2.
2. Настройте соединение SAP HANA в Платформе BI.
 - a. Перейдите к области «Приложения» консоли СМС и дважды щелкните **Аутентификация HANA**.
 - b. В диалоговом окне «Аутентификация HANA» нажмите кнопку **Создать соединение**.
Откроется диалоговое окно «Создание соединения для аутентификации HANA».
 - c. Введите для хоста имя компьютера и номер порта, записанные в шаге 1.
 - d. В поле «Уникальный идентификатор поставщика удостоверения» введите значение, которое будет использоваться для развертывания Платформы BI.
 - e. Нажмите кнопку **Генерировать**.
В поле «Сертификат Base64 поставщика удостоверений» будет создан сертификат.
3. Настройте развертывание SAP HANA.

- a. В приложении SAP HANA Studio выполните следующую SQL-команду для включения платформы BI в качестве поставщика удостоверения:

```
CREATE SAML PROVIDER <УНИКАЛЬНЫЙ ИД> WITH SUBJECT 'C=CA, ST=BC, O=SAP,
OU=BOE, CN=<УНИКАЛЬНЫЙ ИД>' ISSUER 'C=CA, ST=BC, O=SAP, OU=BOE,
CN=<УНИКАЛЬНЫЙ ИД>'
```

Вместо <УНИКАЛЬНЫЙ ИД> следует подставить значение «Уникальный идентификатор поставщика удостоверения», указанное в шаге 2.

- b. Скопируйте сертификат из СМС в файл `trust.pem` в каталоге `~/ .ssl` для пользователя, созданного при установке SAP HANA.

Имя пользователя – <3-значный код>adm. Например, если данный экземпляр SAP HANA имеет идентификатор `xyz`, имя пользователя `xyzadm`.

Примечание:

На этом этапе можно проверить наличие файла `key.pem` в каталоге `~/ .ssl`. Если файл отсутствует, для SAP HANA неверно настроено использование SSL. Перед настройкой единого входа SAP HANA с SAML необходимо настроить SSL на компьютере SAP HANA. Для получения подробных сведений см. документацию SAP HANA.

- c. Перезапустите SAP HANA.
d. При помощи следующих команд создайте пользователя в SAP HANA, для которого платформа BI сможет создавать билеты:

```
CREATE USER <HANASUserName> PASSWORD <HANASUserPassword>;
ALTER USER <HANASUserName> ENABLE SAML;
ALTER USER <HANASUserName> ADD IDENTITY '<BIPIUserName>' FOR SAML PROVIDER <BIPIUniqueIdentityProviderID>;
```

Полное имя пользователя платформы BI – <ИМЯ_ПОЛЬЗОВАТЕЛЯ_BIP>.

Пример:

```
CREATE USER Administrator PASSWORD Abcd1234;
ALTER USER Administrator ENABLE SAML;
ALTER USER Administrator ADD IDENTITY 'Administrator' FOR SAML PROVIDER BIPDeployment1;
```

Также можно выбрать существующего пользователя и выполнить только приведенные выше команды ALTER.

4. Проверьте конфигурацию SAP HANA.

- a. Перейдите к области «Приложения» консоли СМС и дважды щелкните **Аутентификация HANA**.
b. В диалоговом окне «Аутентификация HANA» откройте соединение, созданное в шаге 2. Откроется диалоговое окно «Редактирование соединения для аутентификации HANA».
c. В разделе «Проверить соединение для этого пользователя» введите имя пользователя и нажмите кнопку **Проверить соединение**, чтобы убедиться в правильности параметров соединения.

Например, введите имя пользователя Администратор. Если эти параметры недопустимы, отображается сообщение об ошибке. Для устранения неполадки можно попробовать выполнить следующие шаги:

- Убедитесь, что другие сертификаты в файле `trust.pem` не содержат тему или издателя с аналогичным значением свойства CN. Чтобы просмотреть компоненты сертификата,

найдите в Интернете декодер сертификата, выполнив поиск по фразе «декодер сертификата x509».

- Для проверки конфигурации на стороне HANA попробуйте выполнить следующие команды:

```
select * from "SAML_PROVIDERS"
select user_name, is_saml_enabled from users where user_name = '<UserName>'
select * from "PUBLIC"."SAML_USER_MAPPINGS"
```

Примечание:

Если в каталоге `.ssl` отсутствует файл `key.pem`, в SAP HANA неверно настроено использование SSL.

18.1.3.15.2 Настройки соединения SAP HANA

В следующей ниже таблице представлены общие сведения о параметрах, доступных в СМС для настройки SAP HANA.

Параметр	Описание
«Имя хоста HANA»	Имя хоста SAP HANA.
«Порт HANA»	Номер порта для хоста SAP HANA.
«Уникальный идентификатор поставщика сущности»	Уникальное имя в конкретной установке HANA. Данная установка HANA будет принимать должным образом подписанные билеты от поставщика удостоверений с этим именем при входе в систему.
«Сертификат Base64 поставщика сущности»	После нажатия кнопки Создать в поле «Сертификат Base64 поставщика сущности» создается сертификат. Этот сертификат копируется в файл <code>trust.pem</code> в разворачивании SAP HANA. Этот сертификат устанавливает отношения доверия между SAP HANA и платформой BI. Сам внешний поставщик сущностей определяется сертификатом X509, который используется для подписи всех добавляемых сущностей. Сертификат должен быть закодирован в формате Base64.

18.2 Управление приложениями с помощью свойств `BOE.war`

18.2.1 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*.

18.2.1.1 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>max.tree.children.threshold</code>	<code>max.tree.children.threshold=200</code>	Устанавливает пороговое значение, при достижении которого в иерархических списках вместо отображения всех узлов будет отображаться сообщение "слишком много дочерних узлов".
<code>trusted.auth.shared.secret</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.
<code>trusted.auth.user.param</code>	Нет	Задаёт переменную, используемую для извлечения имени пользователя для доверительной аутентификации. Может иметь одно из следующих значений: <ul style="list-style-type: none"> Заголовок Параметр URL Cookie Сеанс

Параметр	Значения по умолчанию	Описание
<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>	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.
<code>vintela.enabled</code>	<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.
<code>pinger.showWarningDialog.cmc</code>	<code>pinger.showWarningDialog.cmc=true</code>	Указывает, отображается или нет диалоговое окно предупреждения с сообщением о скором истечении срока действия сеанса в СМС.

Параметр	Значения по умолчанию	Описание
<code>pinger.showWarningDialog</code>	<code>pinger.showWarningDialog.bilaunchpad=true</code>	Указывает, отображается или нет диалоговое окно предупреждения с сообщением о скором истечении срока действия сеанса в стартовой панели BI.
<code>pinger.warningPeriod</code>	<code>pinger.warningPeriod.pingIncrementsInSeconds=15</code>	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.
<code>pinger.warningPeriodLength</code>	<code>pinger.warningPeriod.lengthInMinutes=5</code>	Указывает, за какое время до истечения срока действия сеанса отображается предупреждение.
<code>logoff.on.websession.expiry</code>	<code>logoff.on.websession.expiry=true</code>	Указывает необходимость выхода из системы для всех сеансов приложений в случае истечения срока действия веб-сеанса.
<code>pinger.enabled</code>	<code>pinger.enabled=true</code>	Включает или отключает механизм отображения предупреждающих сообщений об истечении срока действия сеанса.
<code>system.console.bip.jmanager.destinations.size</code>	<code>system.console.bip.jmanager.destinations.size=1000</code>	Указывает максимальное число кэшируемых соединений Java.
<code>httpproxy.username</code>	<code>httpproxy.username=myusername</code>	Указывает имя пользователя для входа на прокси-сервер HTTP.
<code>httpproxy.password</code>	<code>httpproxy.password=mypassword</code>	Указывает пароль для входа на прокси-сервер HTTP.
<code>logon.embed.secret</code>	Нет	Общий секрет между порталом, в который встроены приложения платформы BI, и сервером приложений BI, используемый для определения возможности безопасного встраивания приложений платформы BI на другие страницы.

Параметр	Значения по умолчанию	Описание
<code>logon.embed.timeout</code>	<code>logon.embed.timeout=300</code>	Интервал времени в секундах, по прошествии которого для приложений платформы BI, таких как стартовая панель BI, будет отклоняться встраивание в портал. Убедитесь, что расхождение системного времени на веб-сервере платформы BI и сервере портала не превышает указанное значение.
<code>iview.autologoff</code>	<code>iview.autologoff=true</code>	При значении <code>true</code> включен незамедлительный автоматический выход для SAP NetWeaver iViews.
<code>pinger.showWarningDialog</code>	<code>pinger.showWarningDialog=true</code>	Указывает, должно ли отображаться диалоговое окно предупреждения с сообщением о скором истечении срока действия сеанса. Не применяется для CMC и стартовой панели BI.

18.2.1.2 Свойства стартовой панели BI

В следующей таблице перечислены параметры доверительной аутентификации, которые входят в состав установленного по умолчанию файла `bilaunchpad.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=BI launch pad																		
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=BI launch pad																		
app.url.name	Задаёт URL-имя приложения, предваряемое символом «/»". По умолчанию: app.url.name=/BI																		
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>secSiebel17</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	secSiebel17	Oracles EBS	secOraApps
Аутентификация	Значение параметра																		
Enterprise	secEnterprise																		
LDAP	secLDAP																		
Windows AD	secWinAD																		
SAP	secSAPR3																		
PeopleSoft	secpsenterprise																		
JD Edwards	secPSE1																		
Siebel	secSiebel17																		
Oracles EBS	secOraApps																		
authentication.visible	Указывает возможность просмотра и изменения режима аутентификации пользователем, выполняющим вход в стартовую панель BI. По умолчанию: authentication.visible=false																		
cms.default	Задаёт имя CMS по умолчанию. По умолчанию: cms.default=[имя компьютера хоста]																		
cms.visible	Указывает возможность просмотра и изменения имени CMS пользователем, выполняющим вход в стартовую панель BI. По умолчанию: cms.visible=true																		

Параметр	Описание
<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>	<p>Включает или отключает поле «От кого» при планировании объекта для адресата. По умолчанию: <code>SMTPFrom=true</code></p> <p>Если значение задано как <code>false</code>, поле «От» не будет отображаться, а система попытается получить значение «От» следующим образом:</p> <ol style="list-style-type: none"> 1. Сначала система пытается получить данные из отчета объекта отчета по умолчанию. 2. Затем использует адрес электронной почты в профиле пользователя, выполнившего вход в систему. 3. И, наконец, использует значение по умолчанию сервера заданий.
<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>

Параметр	Описание
<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>
<code>logon.allowInsecureEmbedding</code>	Указывает, разрешено ли другим приложениям встраивать это приложение (в качестве кадра) без допустимого маркера встраивания. По умолчанию: <code>logon.allowInsecureEmbedding=false</code>
<code>sso.types.and.order</code>	<p>Указывает разделенный запятыми список типов единого входа, которые будут включены, а также порядок их выполнения.</p> <p>Пустой список указывает, что должен использоваться прежний порядок.</p> <p>Если список указан, прежние параметры игнорируются.</p> <p>Допустимые параметры: <code>vintela</code>, <code>trustedIIS</code>, <code>trustedHeader</code>, <code>trustedParameter</code>, <code>trustedCookie</code>, <code>trustedSession</code>, <code>trustedUserPrincipal</code>, <code>trustedVintela</code>, <code>trustedX509</code>, <code>sapSSO</code> и <code>siteminder</code>.</p> <p>Если ни один из параметров не требуется, укажите <code>none</code></p>

18.2.1.3 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	Задает 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	Задает 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>Задает метод аутентификации по умолчанию, используемый для аутентификации пользователей в приложении. Для этого параметра доступны любые из следующих параметров:</p> <table border="1"> <thead> <tr> <th>Аутентификация</th><th>Значение параметра</th></tr> </thead> <tbody> <tr> <td>Enterprise</td><td>secEnterprise</td></tr> <tr> <td>LDAP</td><td>secLDAP</td></tr> <tr> <td>Windows AD</td><td>secWinAD</td></tr> <tr> <td>SAP</td><td>secSAPR3</td></tr> <tr> <td>PeopleSoft</td><td>secpenterprise</td></tr> <tr> <td>JD Edwards</td><td>secPSE1</td></tr> <tr> <td>Siebel</td><td>secSiebel7</td></tr> <tr> <td>Oracles EBS</td><td>secOraApps</td></tr> </tbody> </table> <p>По умолчанию: authentication.default=secEnterprise</p>	Аутентификация	Значение параметра	Enterprise	secEnterprise	LDAP	secLDAP	Windows AD	secWinAD	SAP	secSAPR3	PeopleSoft	secpenterprise	JD Edwards	secPSE1	Siebel	secSiebel7	Oracles EBS	secOraApps
Аутентификация	Значение параметра																		
Enterprise	secEnterprise																		
LDAP	secLDAP																		
Windows AD	secWinAD																		
SAP	secSAPR3																		
PeopleSoft	secpenterprise																		
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	Задает имя CMS по умолчанию. По умолчанию: cms.default=[имя компьютера хоста]																		
cms.visible	Указывает возможность просмотра и изменения имени CMS пользователем, выполняющим вход в OpenDocument. По умолчанию: cms.visible=true																		

Параметр	Описание
<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>

Параметр	Описание
<code>SAPLogonToken.enabled</code>	Разрешает или запрещает использование маркеров входа в систему SAP веб-службы RESTful для аутентификации на платформе BI. Маркер входа в систему SAP задается с помощью значения X-SAP-LogonToken в заголовке запроса после успешного входа в систему с помощью URL-адреса веб-службы RESTful. По умолчанию: <code>SAPLogonToken.enabled=true</code>
<code>logon.allowInsecureEmbedding=false</code>	Указывает, разрешено ли другим приложениям встраивать это приложение (в качестве кадра) без допустимого маркера встраивания. По умолчанию: <code>logon.allowInsecureEmbedding=false</code>
<code>sso.types.and.order</code>	<p>Указывает разделенный запятыми список типов единого входа, которые будут включены, а также порядок их выполнения.</p> <p>Пустой список указывает, что должен использоваться прежний порядок.</p> <p>Если список указан, прежние параметры игнорируются.</p> <p>Допустимые параметры: <code>serializedSession</code>, <code>sapLogonToken</code>, <code>trustedIIS</code>, <code>trustedHeader</code>, <code>trustedParameter</code>, <code>trustedCookie</code>, <code>trustedSession</code>, <code>trustedUserPrincipal</code>, <code>trustedVintela</code>, <code>vintela</code>, <code>infoview</code>, <code>trustedX509</code>, <code>sapSSO</code> и <code>siteminder</code>.</p> <p>Если ни один из параметров не требуется, укажите <code>none</code></p>

18.2.1.4 Свойства СМС

В следующей таблице перечислены параметры доверительной аутентификации, которые входят в состав установленного по умолчанию файла `smc.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	Задаёт URL-имя приложения, предваряемое символом «/». По умолчанию используется имя app.url.name=/CMC																		
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 СМС. По умолчанию: authentication.visible=false																		
cms.default	Задаёт 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																		

Параметр	Описание
<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 СМС. Маркер будет храниться в cookie-файле. По умолчанию: <code>logontoken.enabled=false</code>
<code>SMTPFrom</code>	<p>Включает или отключает поле «От кого» при планировании объекта для адресата. По умолчанию: <code>SMTPFrom=true</code></p> <p>Если значение задано как <code>false</code>, поле «От» не будет отображаться, а система попытается получить значение «От» следующим образом:</p> <ol style="list-style-type: none"> 1. Сначала система пытается получить данные из отчета объекта отчета по умолчанию. 2. Затем использует адрес электронной почты в профиле пользователя, выполнившего вход в систему. 3. И, наконец, использует значение по умолчанию сервера заданий.

18.3 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*.

18.3.1 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 18-4: 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
Пользовательский URL-адрес для входа в систему	http://<servername>:<port>/BOE/BI/custom.jsp

Таблица 18-5: 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

Тип файла	Местоположение
Пользовательский URL-адрес для входа в систему	http://<servername>:<port>/BOE/OpenDocument/opendoc/custom.jsp

18.3.2 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.

18.3.3 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="..."
```

Для получения дополнительной информации см. раздел о настройке доверительной аутентификации для веб-приложений по ссылке.

5. Выполните повторное развертывание веб-приложения и перезапустите веб-сервер.
6. Включите доверительную аутентификацию в консоли СМС.
На вкладке «Аутентификация» дважды щелкните **Enterprise** и установите флажок **Доверительная аутентификация включена**.

См. также

- [Включение доверительной аутентификации](#)
- [Настройка доверительной аутентификации для веб-приложения](#)

18.4 Настойка интерфейса Web Intelligence

В консоли СМС можно настроить внешний вид элементов интерфейса Web Intelligence для групп пользователей, например для панели инструментов целиком или только для конкретных элементов панели инструментов, а также настроить доступ к конкретным режимам документа.

По умолчанию отображаются все элементы интерфейса. Если вывод конкретных элементов нежелателен, отмените их выбор в консоли СМС: на вкладке **Пользователи и группы** выберите пользователя или группу, а затем щелкните **Действия > Настройка**.

Раздел "Настройка" содержит следующие вкладки:

- **Функции**

На этой вкладке можно скрыть кнопки, связанные с определенной функцией, например кнопку "Обновить".

- **Элементы пользовательского интерфейса**

На этой вкладке можно скрыть отдельные элементы интерфейса, такие как панель инструментов или вкладка, либо их подчиненные элементы, например команду кнопки.

Примечание:

Такая настройка применима для всех клиентов приложения Web Intelligence: веб-клиентов, Java-апплетов и многофункциональных клиентов.

18.4.1 Вкладка "Функции"

Функция	Описание	Элементы интерфейса, на которые оказывается влияние
Обновить	Пользователи могут обновлять документы для загрузки данных из источника данных.	Кнопка "Обновить" находится на панели инструментов "Группа стандартных действий", которая используется в режимах чтения и разработки.
Детализация	Пользователи могут свернуть и развернуть элементы данных в документе.	Кнопка "Детализация" доступна в следующих местоположениях: <ul style="list-style-type: none"> • Панель инструментов "Группа анализа" в режиме чтения; • Дополнительная вкладка "Взаимодействие" вкладки "Анализ" в режиме разработки.
Режим чтения	Пользователи могут просматривать документ в режиме чтения.	Кнопка "Чтение" доступна в следующих местоположениях: <ul style="list-style-type: none"> • Контекстное меню приложения • Панель инструментов управления приложением


Функция	Описание	Элементы интерфейса, на которые оказывается влияние
Режим разработки	Пользователи могут просматривать документ в режиме разработки.	Кнопка "Разработка" доступна в следующих местоположениях: <ul style="list-style-type: none"> • Контекстное меню приложения • Панель инструментов управления приложением
Режим данных	Пользователи могут просматривать документ в режиме данных.	Кнопка "Данные" доступна в следующих местоположениях: <ul style="list-style-type: none"> • Контекстное меню приложения • Панель инструментов управления приложением

18.4.2 Вкладка "Элементы пользовательского интерфейса"

Некоторые из элементов пользовательского интерфейса, которые можно настраивать, показаны на диаграммах в последующих подразделах. Для определения пунктов элементов интерфейса на диаграммах воспользуйтесь следующей таблицей.

Пункт элемента пользовательского интерфейса	Пункт подчиненного элемента	Описание	Номер на диаграмме
Экран заставки		Этот пункт позволяет скрыть экран, который отображается, когда пользователь открывает Web Intelligence.	
Контекстное меню приложения		Этот пункт позволяет скрыть меню, которое отображается, когда пользователь выполняет щелчок правой кнопкой мыши на экране Web Intelligence.	1
	Режим приложения	Этот пункт позволяет скрыть команду изменения режима приложения в контекстном меню приложения.	1a
	Панель фильтра	Этот пункт позволяет скрыть команду "Панель фильтра" в контекстном меню приложения.	1b
	Структура	Этот пункт позволяет скрыть команду "Структура" в контекстном меню приложения.	1c

Пункт элемента пользовательского интерфейса	Пункт подчиненного элемента	Описание	Номер на диаграмме
	Панель формул	Этот пункт позволяет скрыть команду "Панель формул" в контекстном меню приложения.	1d
	Боковая панель	Этот пункт позволяет скрыть команду "Боковая панель" в контекстном меню приложения.	1e
	Вкладки отчетов	Этот пункт позволяет скрыть команду "Вкладки отчетов" в контекстном меню приложения.	1f
	Строка состояния	Этот пункт позволяет скрыть команду "Строка состояния" в контекстном меню приложения.	1g
Боковая панель		Этот пункт позволяет скрыть боковую панель рядом с панелью отчетов, которая обеспечивает доступ пользователей к различным информационным вкладкам.	2
	Сводная информация документа	Этот пункт позволяет скрыть вкладку "Сводка документа" на боковой панели.	2a
	Карта навигации	Этот пункт позволяет скрыть вкладку "Карта навигации" ("Карта отчетов" в HTML-интерфейсе) на боковой панели.	2b
	Элементы управления вводом	Этот пункт позволяет скрыть вкладку "Элементы управления вводом" на боковой панели.	2c
	Ввод подсказки пользователя	Этот пункт позволяет скрыть вкладку "Ввод подсказки пользователя" на боковой панели.	2d
	Доступные объекты	Этот пункт позволяет скрыть вкладку "Доступные объекты" на боковой панели.	2e
	Структура и фильтры документа	Этот пункт позволяет скрыть вкладку "Структура и фильтры документа" на боковой панели.	2f
	Web Service Publisher	Этот пункт позволяет скрыть вкладку "Web Service Publisher" на боковой панели.	2g
	Данные	Этот пункт позволяет скрыть вкладку "Данные" на боковой панели.	2h

Пункт элемента пользовательского интерфейса	Пункт подчиненного элемента	Описание	Номер на диаграмме
Строка состояния		Этот пункт позволяет скрыть строку состояния, где пользователю доступны статусы действий с документами, а также можно выполнять задачи масштабирования, навигации по страницам и активирования строки формул.	3
	Раскрывающийся список отчетов	Этот пункт позволяет скрыть раскрывающийся список отчетов в строке состояния.	3a
	Значок состояния печати	Этот пункт позволяет скрыть значок состояния печати в строке состояния.	3b
	Отслеживание изменений в данных	Этот пункт позволяет скрыть состояние отслеживания изменений в данных в строке состояния.	3c
	Навигация по странице	Этот пункт позволяет скрыть панель навигации по странице в строке состояния.	3d
	Режим разбивки по страницам	Этот пункт позволяет кнопки режима разбивки по страницам в строке состояния.	3e
	Список масштабов	Этот пункт позволяет скрыть раскрывающийся список масштабов в строке состояния.	3f
	Ползунок масштаба	Этот пункт позволяет скрыть панель ползунка масштаба в строке состояния.	3g
	Состояние рабочей области	Этот пункт позволяет скрыть индикатор состояния рабочей области в строке состояния. Примечание: Индикатор "Состояние рабочей области" () отображается между ползунком масштаба и датой последнего обновления при возникновении проблемы в рабочей области.	Не отображается
	Дата последнего обновления	Этот пункт позволяет скрыть дату обновления документа в строке состояния.	3i

Пункт элемента пользовательского интерфейса	Пункт подчиненного элемента	Описание	Номер на диаграмме
	Состояние соединения	Этот пункт позволяет скрыть состояние соединения с многофункциональным клиентом Web Intelligence в строке состояния.	3j
Зона отчета		Этот пункт позволяет скрыть зону отчета в Web Intelligence.	4
	Вкладки отчетов	Этот пункт позволяет скрыть вкладки отчетов в зоне отчета.	4a
	Двунаправленная прокрутка страницы	Этот пункт позволяет скрыть функцию двунаправленной прокрутки страницы в нижнем углу страницы зоны отчета.	4b
	Панель формул	Этот пункт позволяет скрыть строку формул в верхней части зоны отчета.	4c
Панель инструментов режима чтения		Этот пункт позволяет скрыть панели инструментов, отображаемые в режиме чтения.	5
	Раскрывающийся список "Web Intelligence"	Этот пункт позволяет скрыть раскрывающийся список Web Intelligence в режиме чтения.	5a
	Группа файлов	Этот пункт позволяет скрыть панель инструментов "Группа файлов" в режиме чтения.	5b
	Группа стандартных действий	Этот пункт позволяет скрыть панель инструментов "Группа стандартных действий" в режиме чтения.	5c
	Группа "Анализ"	Этот пункт позволяет скрыть панель инструментов "Группа Анализ" в режиме чтения.	5d
Панель инструментов "Режим разработки"		Этот пункт позволяет скрыть панели инструментов и вкладки, отображаемые в режиме разработки.	6
	Вкладка "Файл"	Этот пункт позволяет скрыть вкладку "Файл" в режиме чтения.	6a

Пункт элемента пользовательского интерфейса	Пункт подчиненного элемента	Описание	Номер на диаграмме
	Вкладка "Свойства"	Этот пункт позволяет скрыть вкладку "Свойства" в режиме чтения.	6b
	Группа стандартных действий	Этот пункт позволяет скрыть панель инструментов "Группа стандартных действий" в режиме чтения.	6c
	Вкладка "Элементы отчета"	Этот пункт позволяет скрыть вкладку "Элементы отчета" в режиме чтения.	6d
	Вкладка "Формат"	Этот пункт позволяет скрыть вкладку "Формат" в режиме чтения.	6e
	Вкладка "Доступ к данным"	Этот пункт позволяет скрыть вкладку "Доступ к данным" в режиме чтения.	6f
	Вкладка "Анализ"	Этот пункт позволяет скрыть вкладку "Анализ" в режиме чтения.	6g
	Вкладка "Параметры страницы"	Этот пункт позволяет скрыть вкладку "Параметры страницы" в режиме чтения.	6h
Начальная панель инструментов		Этот пункт позволяет скрыть начальные панели инструментов, которые отображаются, когда пользователь открывает приложение Web Intelligence.	7
	Раскрывающийся список "Web Intelligence"	Этот пункт позволяет скрыть раскрывающийся список Web Intelligence в начальной панели инструментов.	7a
	Группа файлов	Этот пункт позволяет скрыть панель инструментов "Группа файлов" на начальной панели инструментов.	7b
Панель инструментов управления приложением		Этот пункт позволяет скрыть панель инструментов управления приложением, которая отображается в верхней панели инструментов Web Intelligence.	8

Пункт элемента пользовательского интерфейса	Пункт подчиненного элемента	Описание	Номер на диаграмме
	Кнопки режима приложения	Этот пункт позволяет скрыть кнопки режима приложения (чтение, разработка и данные), которые отображаются в верхней панели инструментов Web Intelligence.	8a
	Инструменты	Этот пункт позволяет скрыть значок "Инструменты" в верхней панели инструментов Web Intelligence.	8b
	Справка	Этот пункт позволяет скрыть значок "Справка" в верхней панели инструментов Web Intelligence.	8c
	Закрытие	Этот пункт позволяет скрыть значок "Закрытие" в верхней панели инструментов Web Intelligence.	8d

Экран заставки

На экране СМС "Настройка пользователей и групп", можно скрыть экран заставки Web Intelligence. На следующем ниже рисунке показан экран заставки, который отображается по умолчанию, когда пользователь открывает Web Intelligence.



Рис. 18-2: Экран заставки (пример на английском языке)

Контекстное меню приложения

На следующих диаграммах показаны элементы, которые можно скрыть в контекстном меню.

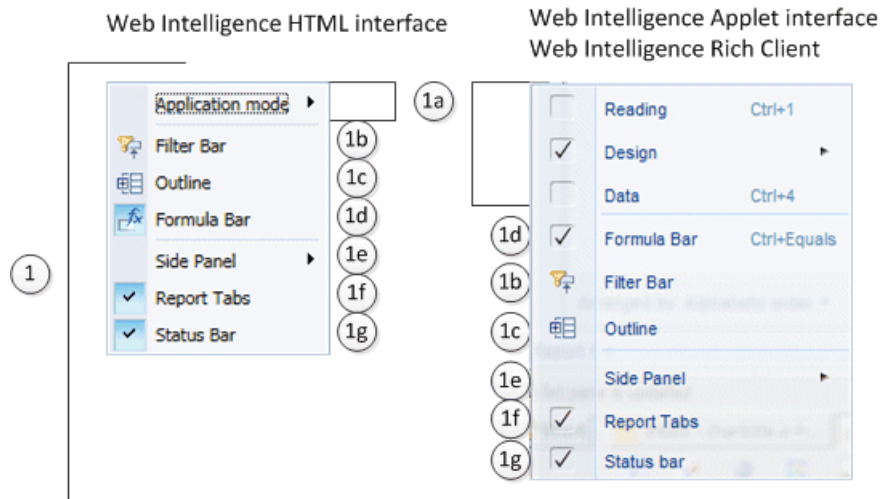
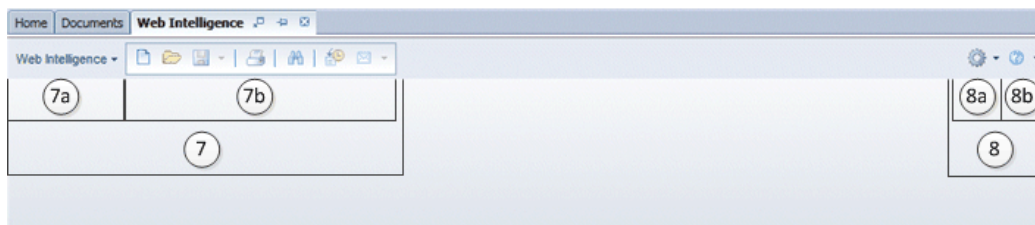


Рис. 18-3: Контекстное меню приложения (пример на английском языке)

Начальная панель инструментов

На следующих диаграммах показаны элементы, которые можно скрыть на панелях инструментов Web Intelligence в случае, если не открыт ни один документ

Web Intelligence Applet interface
Web Intelligence Rich Client



Web Intelligence HTML interface

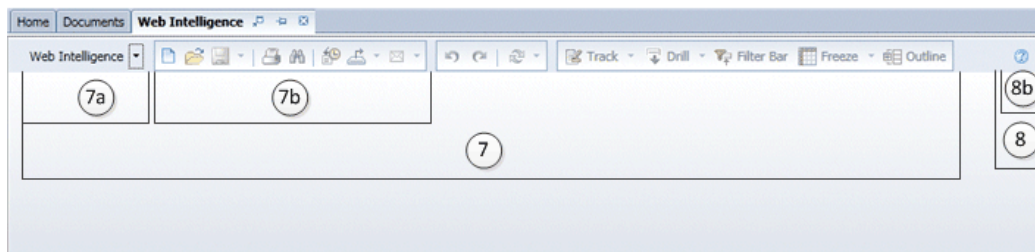
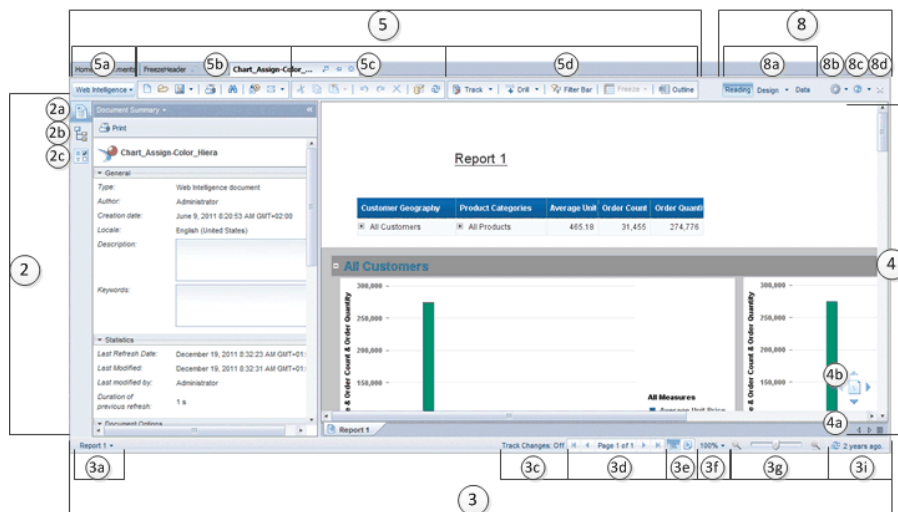


Рис. 18-4: Начальная панель инструментов (пример на английском языке)

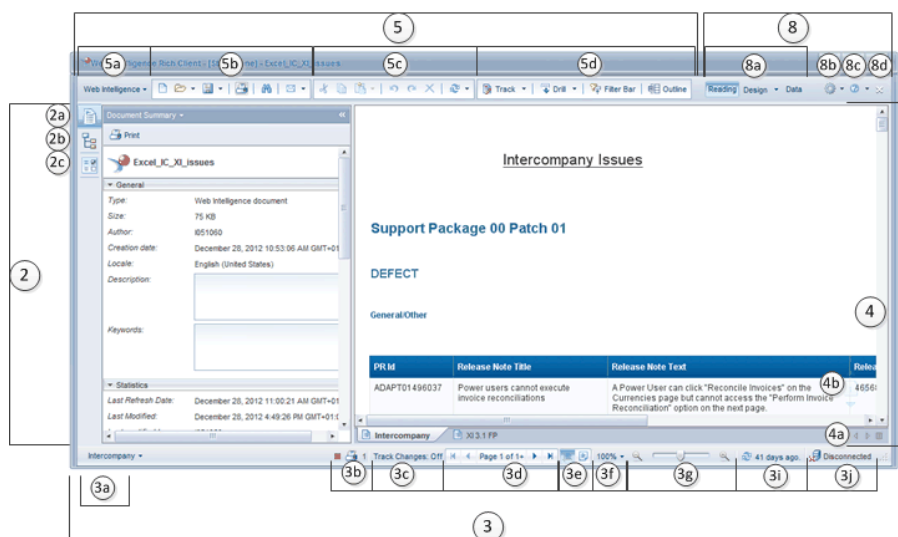
Режим чтения

На следующих диаграммах показаны элементы, которые можно скрыть в режиме чтения Web Intelligence.

Web Intelligence Applet interface



Web Intelligence Rich Client



Web Intelligence HTML interface

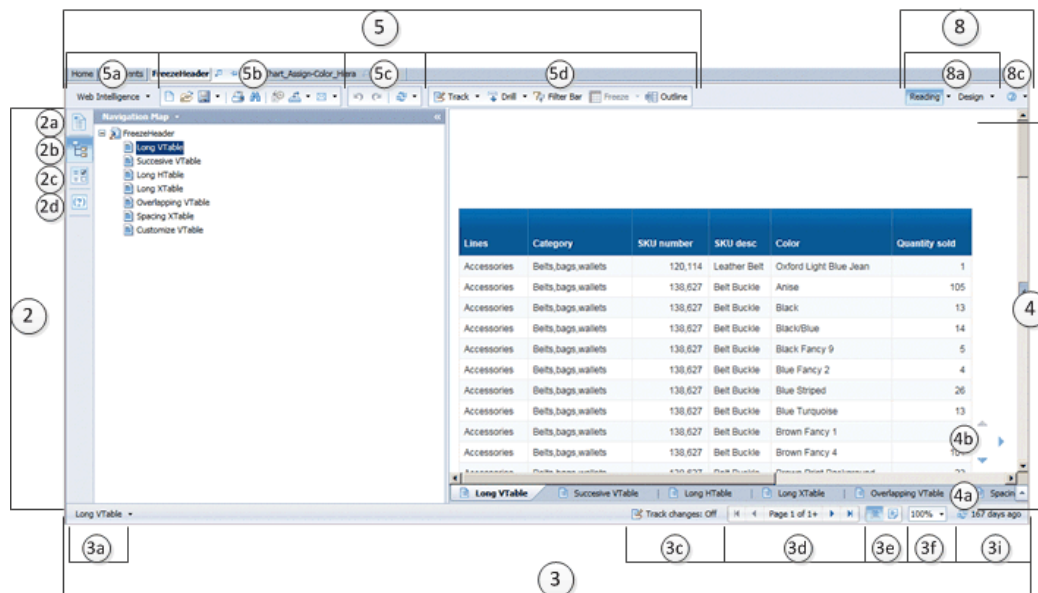
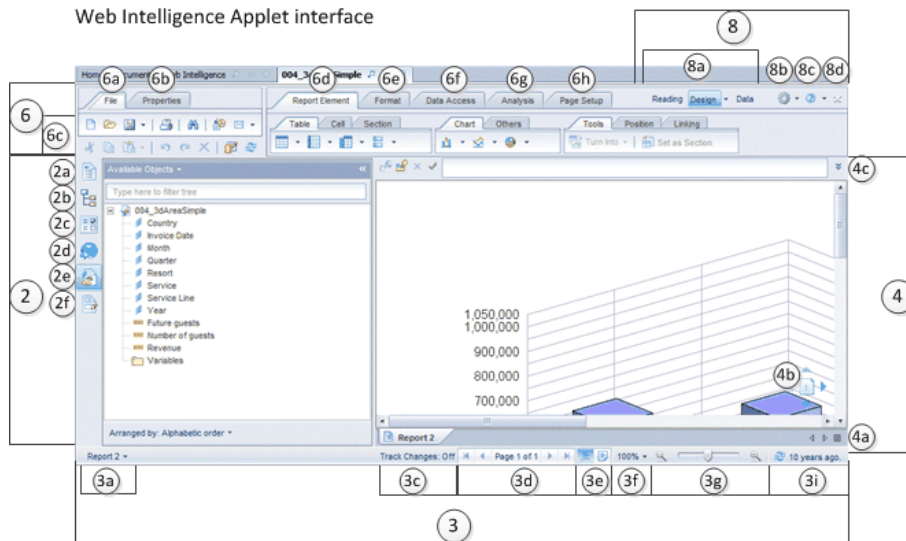


Рис. 18-5: Режим чтения (пример на английском языке)

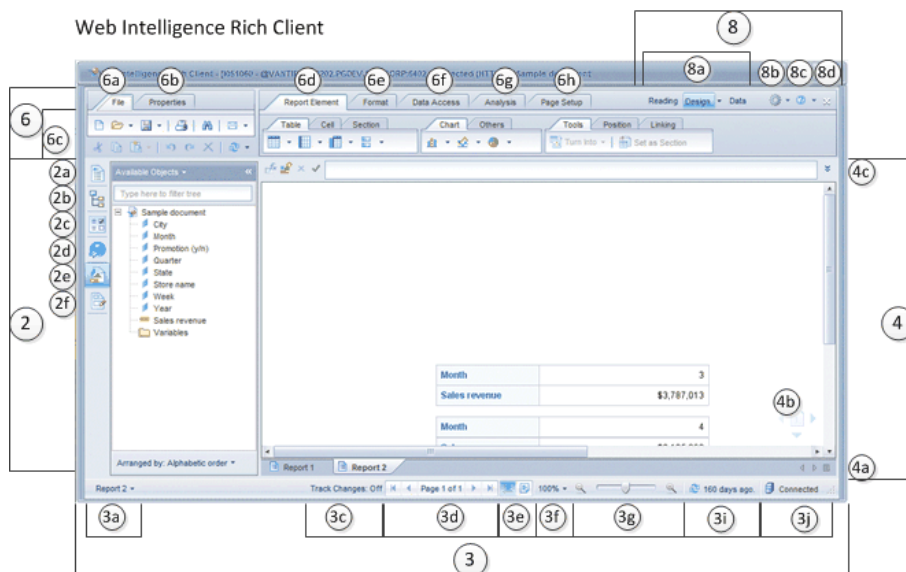
Режим разработки

На следующих диаграммах показаны элементы, которые можно скрыть в режиме разработки Web Intelligence.

Web Intelligence Applet interface



Web Intelligence Rich Client



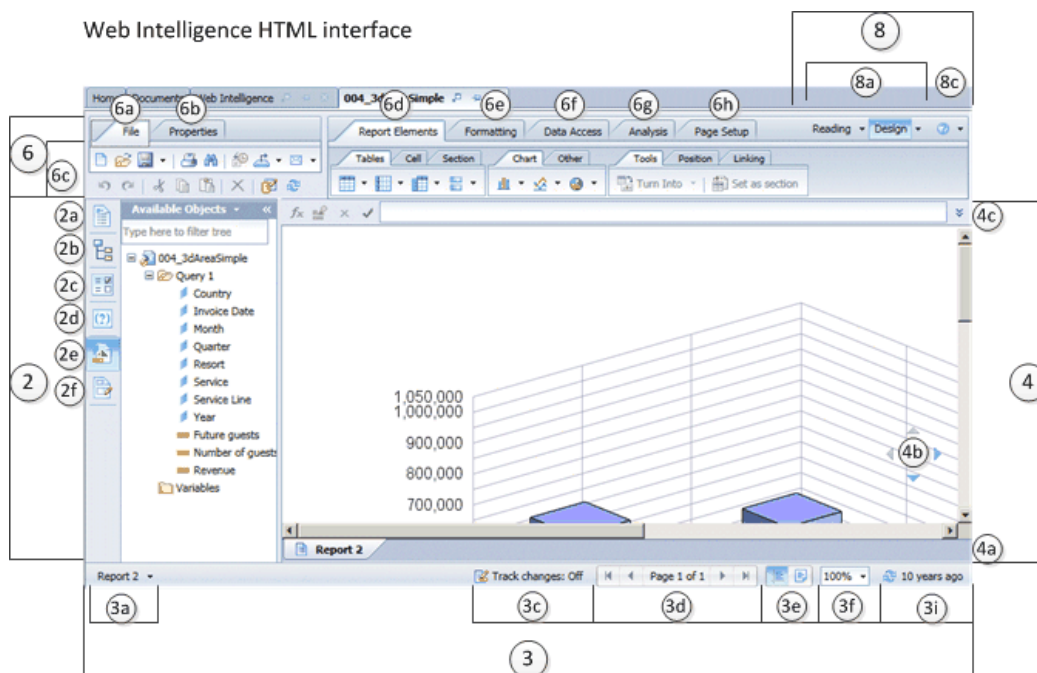
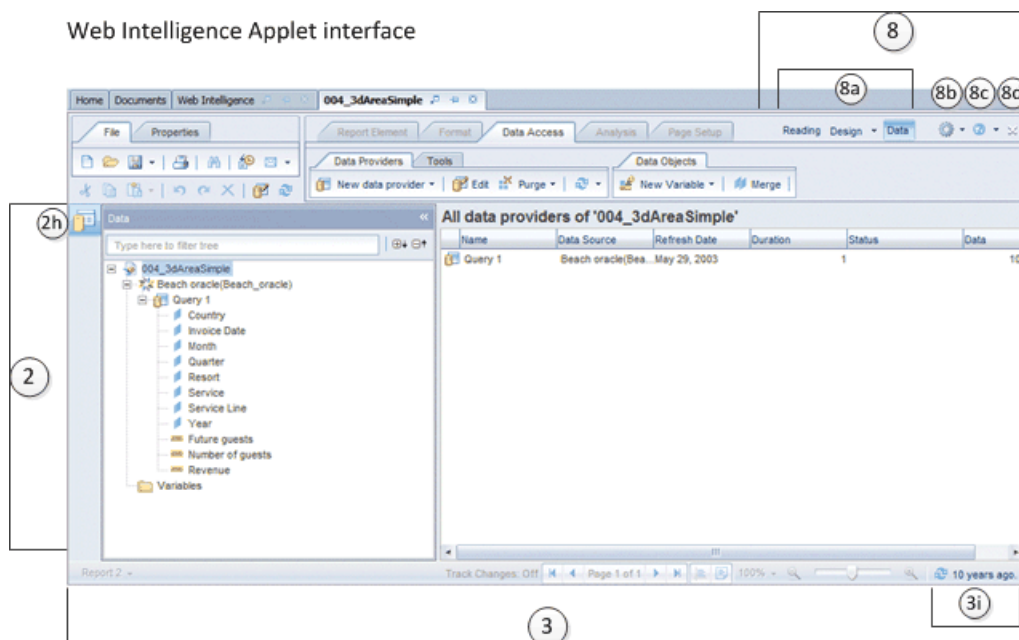


Рис. 18-6: Режим разработки (пример на английском языке)

Режим данных

На следующих диаграммах показаны элементы, которые можно скрыть в режиме данных Web Intelligence.

Web Intelligence Applet interface



Web Intelligence Rich Client

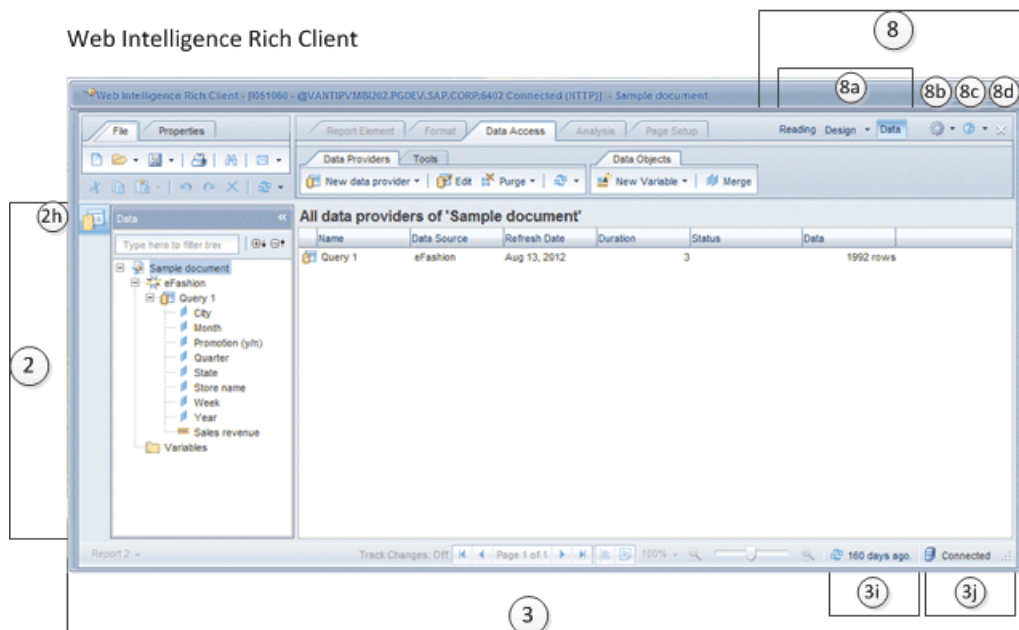


Рис. 18-7: Режим данных (пример на английском языке)

18.4.3 Настройка внешнего вида интерфейса Web Intelligence

Внешний вид пользовательского интерфейса Web Intelligence можно настраивать, скрывая элементы, дополнительные элементы меню, а также функции из всех элементов выбранной группы пользователей.

1. Войдите в консоль СМС с правами администратора.
2. В списке «Организовать» выберите **Пользователи и группы**.
3. В списке «Иерархия группы» выберите пользовательскую группу.
4. В списке «Управление» выберите **Свойства**.
5. На боковой панели выберите **Настройка**.
6. Выполните одно из следующих действий.
 - Чтобы скрыть элементы в Web Intelligence, выберите их на вкладке "Элементы или функции пользовательского элемента".
 - Чтобы отобразить скрытые элементы в Web Intelligence, отмените их выбор на вкладке "Элементы или функции пользовательского интерфейса".
7. Нажмите **Сохранить и закрыть**.

При сохранении настроек все пользователи выбранной группы увидят эти изменения при следующем входе в Панель запуска BI, когда откроют Web Intelligence.

Примечание:

Рекомендуется войти в Панель запуска BI под именем пользователя из только что настроенной группы, запустить Web Intelligence и удостовериться, что интерфейс был изменен в соответствии с параметрами настройки.

Управление соединениями и юниверсами

19.1 Управление соединениями

Соединение – это именованное множество параметров, определяющее, 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 SAP BusinessObjects Enterprise 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](#)

19.1.1 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**.

19.2 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 вычисления, 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 \(.unx\)](#)

19.2.1 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

20.1 О приложении мониторинга

Приложение мониторинга позволяет фиксировать оперативные и исторические показатели серверов платформы BI для ведения отчетности и создания уведомлений. 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 глубокое понимание данных платформы BI.

Мониторинг позволяет выполнять следующие задачи:

- 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 пороговых значений. 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.
- Просмотр всего развертывания платформы BI по группам серверов, категориям служб и узлам Enterprise в графическом и в табличном виде.
- Просмотр сведений о последних сбоях на экране инструментальной панели.
- Проверка доступности системы и времени отклика: с помощью зондов можно моделировать рабочие процессы для проверки правильности работы служб в развертывании платформы BI. 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 BI можно интегрировать с другими приложениями уровня предприятия, такими как SAP Solution Manager и IBM Tivoli Monitoring.

См. также

- [О приложении "Показатели сервера"](#)

20.2 Термины мониторинга

В следующем списке представлены термины, связанные с приложением мониторинга:

Тенденция

Запись или отображение исторических данных для выявления тенденций.

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 позволяют получить сведения о статусе серверов и рабочих процессов в среде платформы BI в реальном времени и историческую информацию о них. С наблюдением пользователи могут связывать пороговые значения и предупреждения. Можно создать наблюдение с использованием данных из зондов, серверов, SAPOSCOL или производных показателей.

Производный показатель

Производные показатели – это показатели, создаваемые в результате сочетания двух или более существующих показателей в математическом уравнении. Можно создать показатель с учетом требований пользователя, а затем создать на основе этого показателя наблюдение.

Топологический показатель

Топологические показатели предоставляют сведения об общем состоянии каждой категории службы в платформе BI. Например, служба Crystal Reports предоставляет объединенное состояние работоспособности всех наблюдений, связанных с серверами Crystal Reports.

Состояние работоспособности

Доступны следующие значения состояния работоспособности:

- "0" - "ОПАСНО"
- "1" - "ЖЕЛТЫЙ"
- "2" - "ЗЕЛЕНый"

Ключевой показатель эффективности

KPI (ключевые показатели эффективности) – это стандартные показатели платформы BI. 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.

Тест

Зонды наблюдают за различными службами и моделируют различные функциональные возможности компонентов платформы BI. Планируя запуск зондов с заданной периодичностью, администратор системы может отслеживать доступность и производительность ключевых служб, предоставляемых платформой BI. Эти данные можно использовать и для планирования мощности.

Светофор

Светофор – это значок, который имеет зеленый, желтый или красный цвет в зависимости состояния наблюдения в конкретный момент времени. Пользователи могут задать для наблюдения два или три состояния.

График тенденций

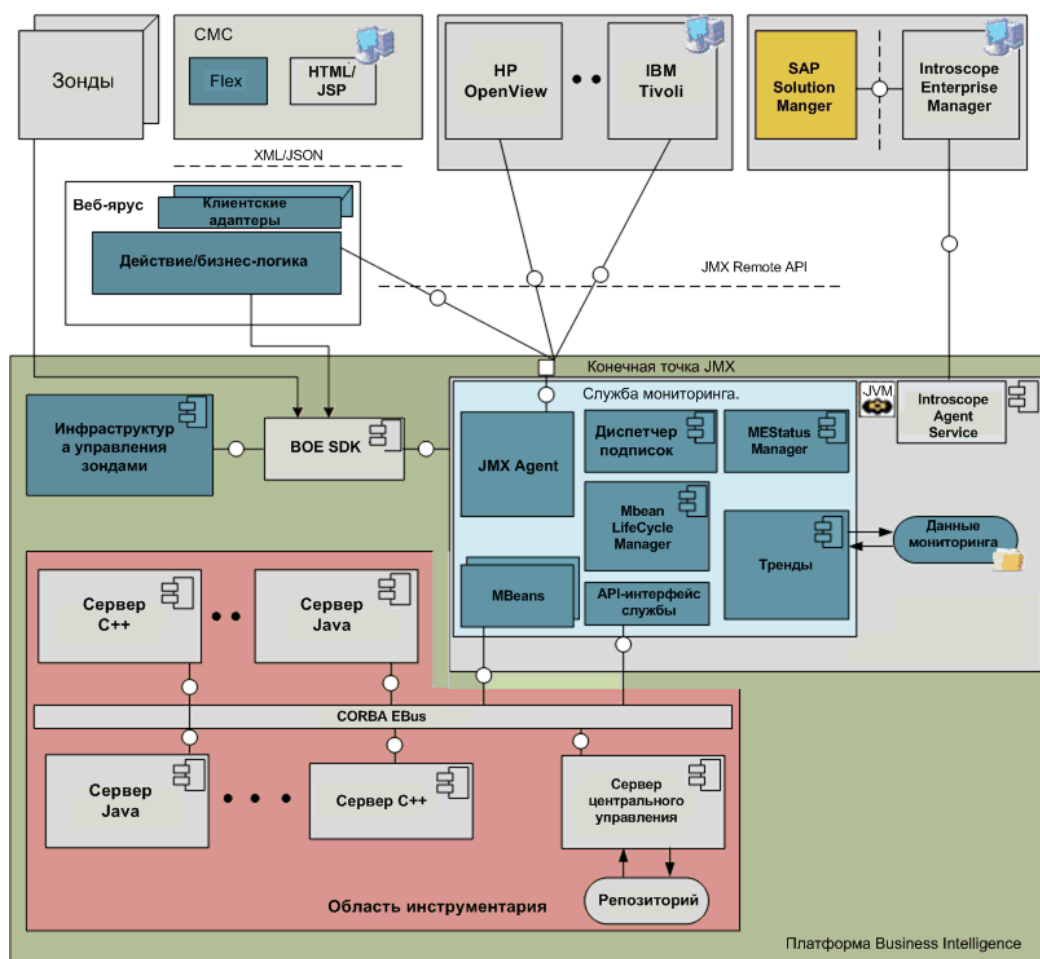
График тенденций – это графическое представление хронологии данных показателей, созданных зондами и серверами. Он помогает администратору отслеживать поведение системы в различные периоды времени и оценивать динамику ее использования.

Предупреждение

Предупреждение – это уведомление, создаваемое приложением мониторинга при достижении порогового значения, заданного пользователем для различных показателей, которые используются для наблюдения. Можно выбрать получение предупреждений по электронной почте или на странице «Информационная панель».

20.2.1 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:

- Адаптивный сервер обработки (APS)
- Агент и сервер для расширений Java Management (JMX)
- Объекты MBean
- Клиенты JMX
- Консоли управления
- База данных тенденций

Служба мониторинга размещается на адаптивном сервере обработки. Приложение основано на технологии JMX.

Служба мониторинга предоставляет основные службы, доступные в приложении мониторинга. Служба мониторинга предоставляет следующие службы:

- 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.
- Хранение данных истории.

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 IBM Tivoli Monitoring, могут подключаться к приложению мониторинга и получать доступ к показателям платформы BI, 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 базы данных тенденций](#).

20.3 Настройка поддержки баз данных в приложении "Мониторинг"

В этом разделе описывается настройка мониторинга и отчетности по данным мониторинга.

Примечание:

Сведения мониторинга заносятся в базу данных тенденций только по показателям, для которых установлен флажок **Запись в базу данных тенденций**.

Для записи сведений мониторинга доступно два параметра базы данных:

- Запись информации во встроенную базу данных Derby (по умолчанию).

Приложение мониторинга включает встроенную базу данных Apache Derby, которая часто называется «базой данных тенденций», где данные мониторинга хранятся по умолчанию. Пользователи могут создавать отчеты по базе данных Derby; тем не менее, она не обеспечивает откат при сбое и не имеет средств резервного копирования и восстановления, которые есть у традиционных реляционных баз данных. Кроме того, для получения последних сведений необходимо обновлять базу данных Derby вручную.

- Запись данных в базу данных аудита (реляционная база данных, где сервер CMS хранит данные аудита).

Вместо использования предлагаемой по умолчанию базы данных Derby можно выбрать базу данных аудита, часто называемую хранилищем данных аудита (ADS). В качестве базы данных аудита можно использовать базу данных аудита, включенную в платформу BI, или другую поддерживаемую базу данных, настроенную в качестве базы данных аудита. Использование базы данных аудита позволяет пользователям строить отчетность по данным аудита наряду с информацией мониторинга. Хранение данных в реляционной базе данных обеспечивает возможности резервного копирования и восстановления, а также их доступность в режиме реального времени.

См. также

- [Настройка для использования базы данных Derby](#)
- [Настройка для использования базы данных аудита](#)

20.3.1 Настройка для использования базы данных Derby

Приложение мониторинга по умолчанию хранит данные мониторинга во встроенной базе данных Derby. Если требуется использовать базу данных Derby, проверьте следующие параметры базы данных в консоли СМС:

1. В области «Управление» на домашней странице СМС щелкните **Приложения**.
2. Дважды щелкните **Приложение мониторинга**, чтобы открыть страницу свойств.
3. В области «Параметры базы данных тенденций» убедитесь, что выбран параметр **Использовать встроенную базу данных**.

Чтобы выполнять запросы в базе данных Derby для создания отчетов и выполнения анализа данных, для базы данных Derby требуется юниверс. Такой юниверс предоставляется в развертывании платформы BI по следующему пути в консоли СМС: **Юниверсы > Юниверсы данных тенденций мониторинга**.

20.3.2 Настройка для использования базы данных аудита

Чтобы использовать базу данных аудита для данных мониторинга, потребуется выполнить дополнительные шаги настройки:

- Если база данных тенденций Derby содержит данные, потребуется выполнить перенос базы данных Derby в базу данных аудита, а затем настроить в платформе BI регистрацию информации мониторинга в базе данных аудита. Ниже приводится общее описание шагов, которые потребуется выполнить. Для получения подробных сведений см. соответствующие разделы.
 1. Выполните перенос базы данных Derby.
 2. Настройте файлы SBO и добавьте псевдонимы.
 3. Перейдите в базу данных аудита.
 4. Перезапустите сервер адаптивной обработки, на котором размещается служба мониторинга.
 5. На информационной панели мониторинга убедитесь, что все работает корректно. Удостоверьтесь, что в базе данных созданы следующие таблицы мониторинга:
 - MOT_MES_DETAILS
 - MOT_MES_METRICS
 - MOT_TREND_DATA
 - MOT_TREND_DETAILS

- Если в базе данных тенденций отсутствуют данные (чистая установка), нет необходимости выполнять перенос данных; достаточно настроить в платформе BI регистрацию информации мониторинга в базе данных аудита. Ниже приводится общее описание шагов, которые потребуются выполнить. Для получения подробных сведений см. соответствующие разделы.
 1. Проверьте работоспособность базы данных аудита и правильную работу функций аудита.
 2. Создайте таблицы мониторинга в ADS.
 3. Настройте файлы SBO и добавьте псевдонимы.
 4. Перейдите в базу данных аудита.
 5. Перезапустите сервер адаптивной обработки, на котором размещается служба мониторинга.
 6. На информационной панели мониторинга убедитесь, что все работает корректно. Удостоверьтесь, что в базе данных созданы следующие таблицы мониторинга:
 - MOT_MES_DETAILS
 - MOT_MES_METRICS
 - MOT_TREND_DATA
 - MOT_TREND_DETAILS

Примечание:

Если данные мониторинга фиксируются в базе данных аудита и требуется создавать отчетность по этим данным, потребуется создать собственный юниверс. Юниверс, включенный в платформу BI, предназначен только для встроенной базы данных Derby.

См. также

- [Миграция базы данных Derby в базу данных аудита](#)
- [Настройка SBO-файлов](#)
- [Добавление псевдонимов в SBO-файл](#)
- [Переход на базу данных аудита](#)
- [Создание таблиц мониторинга в ADS](#)

20.3.2.1 Миграция базы данных Derby в базу данных аудита

Если требуется использовать для данных мониторинга базу данных аудита, а в базе данных тенденций Derby уже есть данные, потребуется выполнить миграцию базы данных Derby в базу данных аудита.

Перед запуском миграции данных проверьте следующие предварительные требования:

- Проверьте работоспособность базы данных аудита и правильную работу функций аудита.
- Убедитесь, что у вас есть достаточные привилегии и необходимые клиентские приложения для целевой базы данных, позволяющие создавать новые таблицы, импортировать CSV-файлы дампа и выполнять другие нужные операции.
- База данных аудита поддерживает импорт CSV-файлов.

Для миграции базы данных выполните следующие шаги:

1. [Резервное копирование базы данных Derby](#)
2. [Экспорт данных в CSV-файлы](#)
3. [Создание таблиц мониторинга в ADS](#)
4. [Восстановление содержимого в целевой базе данных](#)

Примечание:

В кластеризованной среде все экземпляры приложения "Мониторинг" будут использовать один и тот же экземпляр базы данных Derby. Если в кластеризованной среде пользователь имеет несколько экземпляров базы данных Derby, ему следует импортировать данные только из одного экземпляра Derby. Импорт данных из нескольких экземпляров Derby может повлечь за собой возникновение несогласованностей в данных и поэтому настоятельно не рекомендуется.

20.3.2.1.1 Резервное копирование базы данных Derby

1. В области «Управление» на домашней странице СМС щелкните **Приложения**.
2. Дважды щелкните **Приложение мониторинга**, чтобы открыть страницу свойств.
3. В области «Настройки базы данных тенденций» введите файловый ресурс для резервного копирования базы данных тенденций Derby и нажмите кнопку **Сохранить**.
4. Рядом с полем «Выполнять задачу резервного копирования базы данных» нажмите кнопку **Сейчас**.

Если резервное копирование базы данных выполнено успешно, появится сообщение с подтверждением. Также следует проверить местоположение папки, введенное для местоположения резервной копии, и убедиться, что сюда помещены файлы резервной копии.

20.3.2.1.2 Экспорт данных в CSV-файлы

В этом разделе описывается порядок создания файла дампа в формате CSV для миграции. В CSV-файле содержатся значения встроенной базы данных Derby, разделенные запятыми.

1. В области «Управление» на домашней странице СМС щелкните **Приложения**.
2. Дважды щелкните **Приложение мониторинга**, чтобы открыть страницу свойств.
3. В области «Настройки базы данных тенденций» рядом с полем «Экспорт данных из встроенной базы данных в виде CSV-файлов» нажмите кнопку **Экспорт**.

В установленном по умолчанию расположении базы данных тренда (<каталог_установки_BOE>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB) по умолчанию создаются следующие четыре CSV-файла:

- Mot_Mes_Details.csv
- Mot_Trend_Data.csv
- Mot_Trend_Details.csv
- Mot_Mes_Metrics.csv

20.3.2.1.3 Создание таблиц мониторинга в ADS

Для подготовки целевой базы данных аудита выполните следующие шаги:

1. После установки платформы BI DDL-библиотеки, связанные со всеми поддерживаемыми базами данных аудита CMS, доступны по пути <каталог_установки>\SAP

BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB. В этой папке находится семь разных файлов с расширением SQL и именами, соответствующими именам баз данных. Например: Oracle.sql для Oracle, Sybase ASE.sql для базы данных Sybase ASE и так далее.

2. Перейдите в целевую базу данных (в данном случае это БД, в которой хранятся данные аудита CMS) и запустите файл с расширением SQL. Создаются следующие таблицы мониторинга: MOT_TREND_DETAILS, MOT_TREND_DATA, MOT_MES_DETAILS и MOT_MES_METRICS. Для этих таблиц автоматически создаются индексы.

Если все таблицы создаются с правильными типами данных, как указано в SQL-файле, создается схема базы данных, необходимая для приложения мониторинга.

20.3.2.1.4 Восстановление содержимого в целевой базе данных

Для восстановления содержимого в целевой базе данных необходимо выполнить следующие действия.

1. Включите вставку идентификаторов.

Таблица "Мониторинг" содержит несколько столбцов "УДОСТОВЕРЕНИЕ". Эти столбцы автоматически формируют свои значения. В некоторых базах данных (например, MS SQL Server и SYBASE ASE) явная вставка значений в такие столбцы не поддерживается. Тем не менее, в процессе миграции эти столбцы также требуется переносить. Поэтому необходимо разрешить явную вставку этих значений с помощью следующей команды SQL: SET IDENTITY_INSERT <ИМЯ_ТАБЛИЦЫ> ON

2. Импортируйте CSV-файл дампа в целевую таблицу.

Все клиентские приложения баз данных поддерживают импорт данных из CSV-файлов в таблицу с помощью команды меню или командной строки. Соответствующую команду необходимо использовать для импорта данных из CSV-файла в таблицу. Импортируйте файлы данных в новые таблицы в следующем порядке:

- a. MOT_TREND_DETAILS
- b. MOT_TREND_DATA
- c. MOT_MES_DETAILS
- d. MOT_MES_METRICS

3. Отключите вставку идентификаторов.

После завершения импорта данных необходимо отключить вставку компонента Identity для таблицы с помощью следующей команды SQL: SET IDENTITY_INSERT <ИМЯ_ТАБЛИЦЫ> OFF

Пользователи должны отключить вставку сущностей в таблице после импорта данных, чтобы включить вставку сущностей в следующей таблице. Это связано с тем, что операцию вставки сущностей можно включить только в одной таблице за раз.

Примечание:

Включение и отключение вставки сущностей применимо только к MS SQL Server и Sybase ASE. Для других баз данных, таких как Oracle, MaxDb, Db2, MySQL или SQL Anywhere, это не требуется. Можно импортировать данные непосредственно в таблицы.

20.3.2.2 Настройка SBO-файлов

Приложение "Мониторинг" в своей работе использует библиотеки сервера соединений. При этом для установления соединения между сервером соединений и драйвером базы данных задается конфигурация SBO. Для этого необходимо определить драйвер базы данных и его расположение в SBO-файле.

Пример:

- Если в поле имени соединения на странице "Аудит СМС" установлено значение ODBC DSN, драйвер необходимо настроить в файле `<каталог_установки>\dataAccess\connectionServer\odbc\<dbType>.sbo`
- Если используется база данных аудита в формате MS SQL Server, драйвер следует настраивать в файле `<каталог_установки>\dataAccess\connectionServer\odbc\newdb.sbo`.
- Если используется база данных аудита в формате MS SQL Server, драйвер следует настраивать в файле `<каталог_установки>\dataAccess\connectionServer\odbc\sqlsrv.sbo`.
- Если используется база данных аудита в формате DB2, драйвер следует настраивать в файле `<каталог_установки>\dataAccess\connectionServer\odbc\db2iseries.sbo`.
- Если в поле имени соединения на странице "Аудит СМС" установлено значение `<hostName><Portnum><dbName>`, JAR-файл драйвера необходимо настраивать в файле `dataAccess\connectionServer\jdbc\<dbType>.sbo`.

Настройка SBO-файлов

В SBO-файлах библиотеки ODBC обычно уже настроены, поэтому необходимо лишь добавить псевдонимы. Если эти библиотеки не настроены, выполните конфигурацию SBO-файлов, приведенную в следующих примерах:

Пример:

- Если для аудита используется база данных в формате SAP HANA, SBO-файл должен иметь следующую конфигурацию:

```
<DataBase Active="Yes" Name="SAP HANA database 1.0" Platform="MSWindows">
  <Aliases>
    <Alias>SAP High-Performance Analytic Appliance (SAP HANA) 1.0</Alias>
    <Alias>Hana</Alias>
  </Aliases>
  <Libraries>
    <Library Platform="MSWindows">dbd_wnewdb</Library>
    <Library Platform="MSWindows">dbd_newdb</Library>
  </Libraries>
  <Parameter Name="Driver Name">HDBODBC</Parameter>
</DataBase>
```

- Если используется база данных аудита MS SQL Server 2008, SBO-файл должен иметь следующую конфигурацию:

```
<DataBase Active="Yes" Name="MS SQL Server 2008">
  <Libraries>
    <Library>dbd_wmssql</Library>
    <Library>dbd_mssql</Library>
  </Libraries>
  <Parameter Name="Extensions">sqlsrv2008,sqlsrv,odbc</Parameter>
  <Parameter Name="CharSet Table" Platform="Unix">datadirect</Parameter>
  <Parameter Name="Driver Name">SQL (Server|Native Client)</Parameter>
  <Parameter Name="SSO Available" Platform="MSWindows">True</Parameter>
</DataBase>
```

- Если для аудита используется база данных в формате DB2, SBO-файл должен иметь следующую конфигурацию:

```
<DataBase Active="Yes" Name="DB2 UDB for iSeries v5">
  <!-- You can add an alias here if you are using some connections that are defined with an older database engine -->
  <Alias>DB2/400 V5</Alias>
  <Alias>DB2/400 V4</Alias>
  <Alias>DB2 for iSeries v4</Alias>
  <Alias>DB2</Alias>
</Aliases>
```

- Если используется база данных аудита MySQL 5, SBO-файл должен содержать следующую строку:

```
<DataBase Active="Yes" Name="MySQL 5">
  <JDBCdriver>
    <ClassPath>
      <Path>C:\mysqljdbcdriver.jar</Path>
    </ClassPath>
    <Parameter Name="JDBC Class">com.mysql.jdbc.Driver</Parameter>
    <Parameter Name="URL Format">jdbc:mysql://$DATASOURCE$/ $DATABASE$</Parameter>
  </JDBCdriver>
  <Parameter Name="Driver Capabilities">Query,Procedures</Parameter>
  <Parameter Name="Force Execute">Always</Parameter>
  <Parameter Name="Extensions">mysql5,mysql,jdbc</Parameter>
</DataBase>
```

Дополнительные сведения о настройке драйвера в SBO-файлах см. в *руководстве по доступу к данным*.

20.3.2.3 Добавление псевдонимов в SBO-файл

Помимо настройки драйвера в SBO-файл, соответствующий используемой версии базы данных аудита, также требуется добавить псевдоним. В следующей таблице перечислены псевдонимы, которые следует использовать для соответствующих баз данных.

Имя БД	Псевдоним в SBO-файле
SAP HANA	HANA
Microsoft SQL Server	MS SQL Server
My SQL	MySQL
SAP Max DB	MaxDB
IBM DB2	DB2
Sybase SQL Anywhere	Sybase SQL Anywhere
Sybase Adaptive Server Enterprise	Sybase Adaptive Server Enterprise
Oracle	Oracle

Эти имена необходимо использовать, поскольку приложение "Мониторинг" осуществляет их поиск в SBO-файле.

Пример:

Если используется база данных аудита MS SQL Server 2008, необходимо добавить псевдоним в SBO-файл следующим образом:

```
<DataBase Active="Yes" Name="MS SQL Server 2008">
  <Aliases>
    <Alias>MS SQL Server</Alias>
  </Aliases>
  <Libraries>
    <Library>dbd_wmssql</Library>
    <Library>dbd_mssql</Library>
  </Libraries>
  <Parameter Name="Extensions">sqlsrv2008,sqlsrv,odbc</Parameter>
  <Parameter Name="CharSet Table" Platform="Unix">datadirect</Parameter>
  <Parameter Name="Driver Name">SQL (Server|Native Client)</Parameter>
  <Parameter Name="SSO Available" Platform="MSWindows">True</Parameter>
</DataBase>
```

20.3.2.4 Переход на базу данных аудита

Можно изменить базу данных таким образом, чтобы информация о тенденциях из приложения "Мониторинг" хранилась в базе данных аудита.

1. В области «Управление» на домашней странице СМС щелкните **Приложения**.
2. Дважды щелкните **Приложение мониторинга**, чтобы открыть страницу свойств.
3. В области «Настройки базы данных тенденций» выберите **Использовать базу данных аудита**.

20.4 Свойства конфигурации

В этом разделе описаны свойства приложения мониторинга и способы их изменения.

Чтобы просмотреть свойства конфигурации приложения мониторинга, выполните следующие действия:

1. Перейдите на вкладку **Приложения** консоли СМС.
2. Щелкните правой кнопкой **Приложение мониторинга** и выберите **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. Для службы мониторинга это протокол, используемый по умолчанию. 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	<p>По умолчанию данный параметр отключен. При включении этого параметра необходимо указать путь к каталогу установки двоичного файла SAPOSCOL.</p> <p>Для включения показателей хоста необходимо установить SAPOSCOL. Дополнительные сведения о порядке установки SAPOSCOL см. в разделе Установка SAPOSCOL</p>

Раздел	Поле	Описание
Параметры базы данных тренда	Использовать базу данных аудита	Выберите этот параметр, чтобы хранить журнал трендов показателей в базе данных аудита CMS. Примечание: Для этого требуется настроить аудит CMS.
	Использовать встроенную базу данных	Выберите этот параметр, чтобы хранить журнал тенденций показателей и наблюдения во встроенной базе данных приложения "Мониторинг".
	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, а размер базы данных превысил 100 МБ, при проверке системы база данных будет уменьшена до 70 МБ.
	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 тенденций каждые	Периодичность резервного копирования базы данных тенденций в часах. Если это значение указано, резервное копирование выполняется при запуске системы, при перезапуске APS, а также через указанный промежуток времени.
	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.
	Запустить задание резервного копирования базы данных	

Раздел	Поле	Описание
		Задача резервного копирования базы данных запускается при щелчке этого параметра. Перед выбором этого параметра укажите местоположение каталога резервного копирования базы данных.
	Экспорт данных из встроенной базы данных в формате CSV	Нажмите кнопку Экспорт , чтобы экспортировать базу данных в виде CSV-файлов.
	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.

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 интервалом времени. Расчет состояния наблюдения: состояние наблюдений 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 тенденции: режим журнала для графиков всегда анализируется с указанным здесь интервалом.
	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.
	Частота напоминаний о предупреждении (дни)	Число дней до создания напоминания о предупреждении.

3. Нажмите кнопку **Сохранить**.

Примечание:

После изменения любого из этих свойств (кроме включения и отключения приложения мониторинга) необходимо перезапустить серверы адаптивной обработки, на которых размещается служба мониторинга.

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`.

20.4.1 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 соединения 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
cescore.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

Jar-файлы
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](#).

20.4.2 HTTPS-аутентификация для зондов мониторинга

Для зондов мониторинга поддерживается аутентификация на HTTPS-сервере. Для использования такой аутентификации требуется предварительно выполнить следующие настройки:

1. Импортируйте сертификат сервера в хранилище надежных сертификатов клиента. Это позволяет клиентской стороне (зонд) проверять идентификационные данные сервера. Выполните следующую команду: `<КОРЕНЬ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\lib> keytool -import -alias ca -keystore "<КОРЕНЬ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security\cacerts" -file ca.cer`
`ca.cer` может быть самостоятельным сертификатом сервера или сертификатом Центра сертификации, (обычно внутренний ЦС), создавшим сертификат для этого сервера. Если сертификат сервера создан известным ЦС, нет необходимости импортировать его и этот шаг можно пропустить. Это связано с тем, что сертификат сервера будет проверяться по ЦС, открытый ключ которого по умолчанию находится в хранилище надежных сертификатов.
2. Измените «Базу URL-адреса» в параметрах зонда панели запуска BI на `https://<URL>/BOE/BI`, где `<URL>` указывает хост по имени, использованном в сертификате.

Аутентификация HTTPS-клиентов не поддерживается.

20.4.3 Шифрование паролей для зондов

Чтобы обеспечить шифрование паролей при использовании зондов, необходимо добавить параметр `true` в каждый из параметров пароля зонда мониторинга при создании зонда в

командной строке. Для получения дополнительной информации и просмотра примеров синтаксиса см. раздел *Управление зондами из командной строки* в справке по консоли СМС.

20.5 Интеграция с другими приложениями

Решения Enterprise, такие как 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.

20.5.1 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 «Определение 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 соединение.

6. В окне «Браузер для расширений Java Management (JMX)» щелкните + рядом с полем **Имя соединения**, чтобы добавить новое подключение.
7. В окне «Мастер подключения к серверу MBean» выберите **Стандартные соединения с JMX (JSR-160)**.
8. В окне «Свойства соединения» введите следующие данные:

Поле	Описание
Имя соединения	Сервер, совместимый с JSR-160
Идентификатор пользователя	Имя пользователя, которое используется для входа в платформу SAP BusinessObjects BI
Пароль	Пароль, который используется для входа в платформу SAP BusinessObjects BI
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 платформы SAP BusinessObjects Enterprise BI создается с помощью конструктора агента, то платформа SAP BusinessObjects BI должна быть установлена в той же системе. Однако при установке уже созданного агента с помощью его файла установщика наличие установленного приложения платформы BI 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 использовать 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

Jar-файлы
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](#)

20.5.2 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 BI выполните следующие действия:

1. На этапе «Настройка 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 при установке платформы BI.
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. Для получения дополнительных сведений см. раздел *Управление серверами* в *Руководстве администратора платформы SAP BusinessObjects Business Intelligence*.

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.

20.6 Поддержка кластеров для сервера мониторинга

Приложение мониторинга поддерживает кластеризацию, что обеспечивает отказоустойчивость.

При использовании поддержки кластера в определенный момент времени активна только одна служба, а все прочие службы пассивны. Если в кластеризованной среде есть две службы мониторинга, s1 и s2, будет доступна только одна из них. Обе службы предпринимают попытку стать активными, однако если одной из них это удастся, другая становится неактивной (пассивной).

Пассивная служба периодически (раз в минуту) проверяет 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 или ухудшения производительности APS.

20.7 Устранение неполадок

В этом разделе приводятся пошаговые инструкции для решения широкого диапазона проблем, которые могут возникать при работе с приложением мониторинга.

20.7.1 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 (KPI)

- Убедитесь, что отображаются обязательные показатели. Для этого выберите команды **Свойства сервера > Показатели**.

- Убедитесь, что ответ центрального сервера управления соответствует ожиданиям.

Не удается запустить приложение мониторинга

Загрузите и установите последнюю версию приложения Flash Player.

20.7.2 Предупреждения

Отсутствие предупреждений на странице "Предупреждения"

- Проверьте, выбран ли параметр **Включить пользовательские предупреждения** в свойствах приложения предупреждений.
- Проверьте наличие необходимых прав доступа для получения предупреждений.
- Убедитесь, что на информационной панели мониторинга отображаются последние предупреждения.

Примечание:

Можно отправить документ Crystal Reports на заданный идентификатор электронной почты для проверки правильности работы протокола SMTP.

Не удается получить уведомления по электронной почте

- Проверьте, выбран ли параметр **Включить электронную почту** в свойствах приложения предупреждений.
- Проверьте, правильны ли настройки адреса электронной почты для получения предупреждений по электронной почте.
- Проверьте работоспособность сервера SMTP.
- Убедитесь, что включен экземпляр настраиваемого сервера заданий.
- Проверьте настройки SMTP в месте назначения экземпляра настраиваемого сервера заданий.

20.7.3 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

Проверьте, выполняется ли экземпляр настраиваемого сервера обработки.

Вкладка "Список наблюдений" отключена

- Убедитесь, что служба мониторинга запущена.
- Проверьте наличие сообщений об ошибках в журналах службы мониторинга.
- Убедитесь, что серверы и их показатели видны в jConsole.

См. также

- [Свойства конфигурации](#)

20.7.4 Зонды

Не удается запланировать зонды

- Проверьте, выполняется ли экземпляр AdaptiveJobServer, на котором расположена служба планирования зонда.
- Проверьте правильность идентификатора CUID отчета, используемого для документов Crystal Reports и Web Intelligence.
- Убедитесь, что пользователь имеет права администратора или является участником группы администраторов.
- Убедитесь, что пользователь обладает достаточными правами на открытие, обновление и экспорт документов Crystal Reports и Web Intelligence, которые используются в соответствующих зондах.

Зонд имеет состояние планирования "Отложено"

- Проверьте, установлен ли экземпляр ProbeSchedulingService.
- Проверьте, выполняется ли экземпляр AdaptiveJobServer, на котором расположена служба планирования зонда.

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

20.7.5 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

20.7.6 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

21.1 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 просмотреть в сети сообщества SAP <http://scn.sap.com/>.

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.

Выполнение аудита

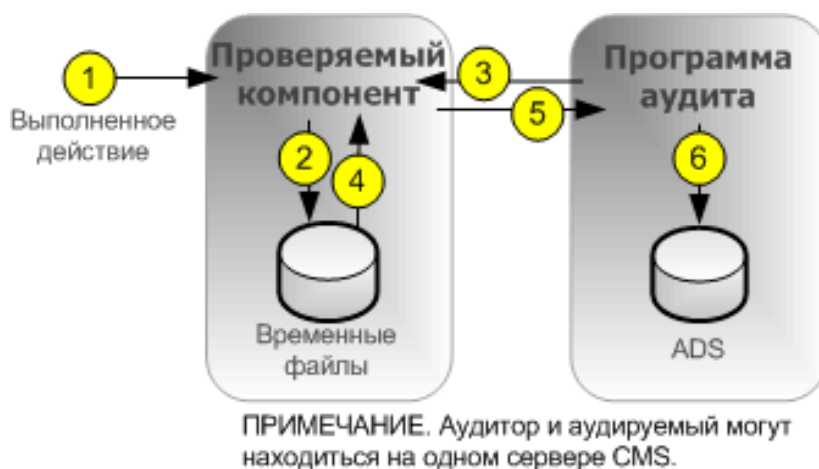
Центральный сервер управления (CMS) выполняет роль аудитора системы, а сервер или приложение, инициирующее проверяемое событие, выполняют роль проверяемого компонента. Если происходит событие, подлежащее аудиту, в проверяемом компоненте создается запись, которая сохраняется в локальном временном файле. 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

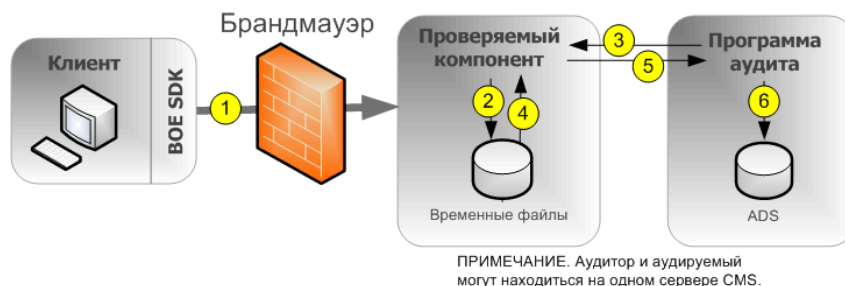
При возникновении событий, созданных сервером, CMS может выступать в роли аудитора и проверяемого.



1. Событие, подлежащее аудиту, выполняется сервером.
2. Проверяемый компонент записывает события во временный файл. Шаги 1 и 2 могут выполняться несколько раз до перехода к шагу 3.
3. Аудитор опрашивает проверяемый компонент и запрашивает пакет событий аудита через равные промежутки времени.
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 брандмауэре 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. Шаги 1 и 2 могут выполняться несколько раз до перехода к шагу 3.
3. Аудитор опрашивает проверяемый компонент и запрашивает пакет событий аудита через равные промежутки времени.

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.

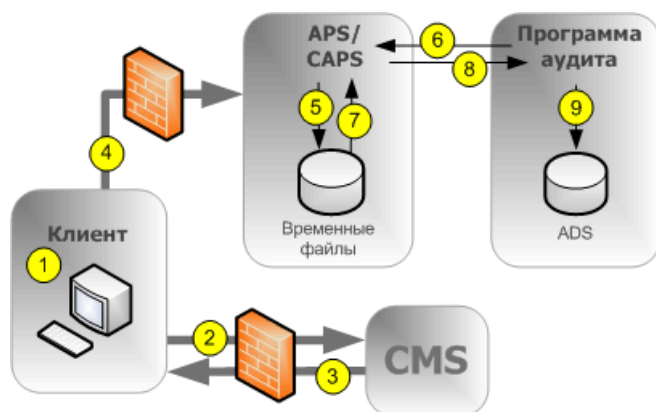
Сюда относятся такие интерактивные приложения, как стартовая панель BI, Central Management Console, SAP BusinessObjects Web Intelligence и другие.



1. Браузер подключается к серверу веб-приложения, и на него передаются данные входа в систему.
2. SDK платформы BI отправляет проверяемому компоненту (CMS) запрос входа, а также IP-адрес и имя компьютера, на котором установлен браузер.
3. Проверяемый компонент записывает события во временный файл. Шаги с 1 по 3 могут выполняться несколько раз до перехода к шагу 4.
4. Аудитор опрашивает проверяемый компонент и запрашивает пакет событий аудита через равные промежутки времени.
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.

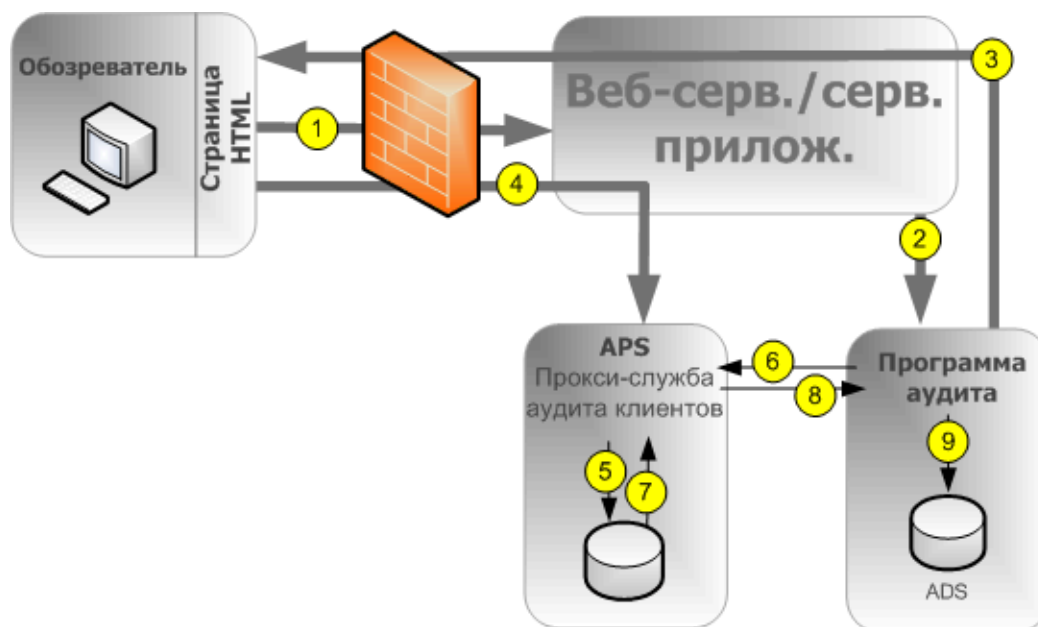
Примечание:

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. Шаги с 1 по 5 могут выполняться несколько раз до перехода к шагу 6.
6. Аудитор опрашивает CAPS и запрашивает пакет событий аудита через равные промежутки времени.
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 адаптивном сервере обработки (APS).
5. CAPS записывает события во временный файл. Шаги с 1 по 5 могут выполняться несколько раз до перехода к шагу 6.
6. Аудитор опрашивает CAPS и запрашивает пакет событий аудита через равные промежутки времени.
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
- Web Intelligence Rich Client

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 аудита правильно установлена, настроена и защищена и используются подходящие версии всех приложений клиентов, функция аудита 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 ADS 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 брандмауэрами.

Примечание:

- События, формируемые клиентскими приложениями, содержат информацию, отправленную со стороны клиента, другими словами, извне надежной области системы. Таким образом в некоторых случаях эта информация может быть не так же надежна, как информация, записанная системными серверами.
- 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. Число ожидающих перемещения событий аудита отражено в показателе сервера «Текущее число событий аудита в очереди». Когда значение этого показателя становится равным нулю, сервер можно остановить. Расположение временных файлов определяется заполнителем %DefaultAuditingDir% для данного узла. Для получения дополнительных сведений о заполнителях см. раздел "Администрирование сервера".

- Если нужно использовать аудит клиента, рекомендуется создать выделенный адаптивный 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](#)

21.2 Страница "Аудит СМС"

Страница «Аудит» в консоли СМС содержит следующие области:

- «Сводка состояния»
- «Установить события»
- «Установить сведения о событии»
- «Настройка»

21.2.1 Состояние аудита

«Сводка состояния» 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:

- Соединение с базой 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.

Примечание:

Показатели сводки состояния помечены зеленым, желтым или красным цветом. Цвета отражают состояние функции аудита.

Показатели состояния аудита.

Показатель	Сведения
Последнее обновление ADS	Дата и время окончания 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 соединения с базой данных ADS	

Показатель	Сведения
	Имя соединения с базой данных, используемого текущим CMS для подключения к хранилищу данных аудита (ADS). Для серверов SQL Anywhere, SQL и SAP HANA это имя соединения ODBC. Для баз данных других типов это имя базы данных и порт подключения, за которыми следует имя сервера.
Имя пользователя базы данных ADS	Имя пользователя проверяющего CMS, используемое для входа в базу данных ADS.

21.2.2 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 соединение с базой данных. Сбор событий будет выполняться и без соединения, а после установления соединения события будут записаны в ADS. Для выключения аудита уровень должен быть выключен. См. *Параметры конфигурации хранилища данных аудита*.

21.2.2.1 Чтобы настроить события аудита

1. В Central Management Console откройте вкладку **Аудит**.

Откроется страница **Аудит**.

2. Установите ползунок **Установить события** на нужный уровень.

В следующей таблице показаны различные параметры настройки для ползунка и 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 • Подсказка • Создание • Удаление • Изменение • Сохранение • Поиск • Изменить • Запуск • Доставка
Завершение	Минимальные события и события По умолчанию , плюс: <ul style="list-style-type: none"> • 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 • Удаление VMS • Соединение с кубом • Сеанс MDAS <p>Примечание: При наличии установленных дополнительных компонентов число событий может быть больше.</p>
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.

21.2.3 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 соединения с ADS.

Здесь также можно настроить продолжительность сохранения событий аудита в базе данных.

После выполнения обновления с предыдущей версии SAP BusinessObjects Enterprise XI 3.x 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.

21.2.3.1 Чтобы настроить параметры базы данных ADS (хранилища данных аудита)

1. В Central Management Console откройте вкладку **Аудит**.
2. В области «Конфигурация» под заголовком «База данных ADS» выберите тип базы данных, установленный для данных аудита.
3. В поле «Имя соединения» введите имя соединения, настроенного для базы данных аудита.

Тип базы дан-ных	Имя соединения
IBM DB2	имя службы
Microsoft SQL Server	ODBC DSN
MySQL	<имя_хоста_сервера>, <порт>, <имя_базы_данных>
Oracle	Имя службы TNS
SAP HANA	ODBC DSN
SAP MaxDB	<имя_хоста_сервера>, <порт>, <имя_базы_данных>
Sybase Adaptive Server Enterprise	имя службы
Sybase SQL Anywhere	ODBC DSN

- a. Если используется база данных Microsoft SQL с аутентификацией Windows, включите параметр **Аутентификация Windows**.
4. В полях **Имя пользователя** и **Пароль** введите соответствующие значения, которые будут использоваться аудитором CMS при входе в базу данных.

Если в качестве базы данных по умолчанию для платформы BI установлена IBM DB2, оставьте поля **Имя пользователя** и **Пароль** пустыми.

5. 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.

6. 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.

7. Нажмите кнопку **Сохранить**.
8. Перезапустите все CMS в кластере.

Примечание:

В «сводке состояния» в верхней части страницы отображаются текущие значения ADS, которые могут отличаться от значений в разделе «База данных ADS» до перезапуска CMS.

21.3 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"> Central Management service
Создать	В систему добавлен новый объект. <ul style="list-style-type: none"> Central Management Service Служба просмотра и изменения Crystal Reports Desktop Intelligence Служба Information Engine Управление жизненным циклом Web Intelligence Общая служба Web Intelligence Основная служба Web Intelligence Служба обработки Web Intelligence
Соединение с кубом	Выполняется операция соединения с кубом OLAP. <ul style="list-style-type: none"> Multi-Dimensional analysis service
Пользовательский уровень доступа изменен	Изменена информация по привилегиям. <ul style="list-style-type: none"> Central Management Service
Удалить	Объект удален из системы. <ul style="list-style-type: none"> Central Management Service Служба управления жизненным циклом
Доставка	Объект отправлен/назначен по месту назначения. <ul style="list-style-type: none"> Служба планирования обновления аутентификации Central Management Service Службы планирования Crystal Reports для Enterprise Служба планирования Crystal Reports Desktop Intelligence Служба планирования доставки в места назначения Служба планирования поиска по платформе Служба планирования зонда Служба планирования программ Служба планирования запросов безопасности Служба планирования импорта пользователей и групп Служба планирования и публикаций Web Intelligence

Событие	Описание, а также серверы и клиенты, создающие тип события
Выйти из режима перехода по иерархии	<p>Пользователем документа Web Intelligence выполнен переход по иерархии до уровня детализации, находящегося за пределами предварительно загруженных данных отчета.</p> <ul style="list-style-type: none"> • Web Intelligence • Служба обработки Web Intelligence • Общие службы Web Intelligence • Основные службы Web Intelligence • Служба Information Engine
Изменить	<p>Содержимое объекта изменено.</p> <ul style="list-style-type: none"> • Приложение "Рабочие пространства BI" • Desktop Intelligence • Служба Information Engine • Web Intelligence • Общая служба Web Intelligence • Основная служба Web Intelligence • Служба обработки 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"> • Central Management service
Выход из системы	<p>Пользователь выходит из системы</p> <ul style="list-style-type: none"> • Central Management service
Изменить	<p>Свойства файла объекта изменены</p> <ul style="list-style-type: none"> • Web Intelligence • Управление жизненным циклом • Central Management service
Сеанс MDAS	<p>Выполняется операция службы многомерного анализа</p> <ul style="list-style-type: none"> • Multi-Dimensional analysis service
Страница извлечена	<p>Клиент SAP BusinessObjects Web Intelligence извлекает дополнительную информацию из репозитория.</p> <ul style="list-style-type: none"> • Служба обработки Web Intelligence • Общие службы Web Intelligence • Основные службы Web Intelligence • Служба Information Engine

Событие	Описание, а также серверы и клиенты, создающие тип события
Подсказка	<p>Для подсказки объекта введена информация.</p> <ul style="list-style-type: none"> • Служба кэша Crystal Reports • Службы планирования Crystal Reports для Enterprise • Служба планирования Crystal Reports • Служба кэша Dashboards • Desktop Intelligence • Служба Information Engine • Live Office • Web Intelligence • Общая служба Web Intelligence • Основная служба Web Intelligence • Служба обработки Web Intelligence
Обновить	<p>Данные в объекте обновлены из базы данных по запросу пользователя.</p> <ul style="list-style-type: none"> • Служба кэша Crystal Reports • Службы планирования Crystal Reports для Enterprise • Служба планирования Crystal Reports • Служба кэша Dashboards • Desktop Intelligence • Служба Information Engine • Live Office • Web Intelligence • Общая служба Web Intelligence • Основная служба Web Intelligence • Служба обработки Web Intelligence
Извлечь	<p>Объект извлечен из репозитория.</p> <ul style="list-style-type: none"> • Central Management service • Desktop Intelligence
Изменение прав	<p>Для пользователя, группы или объекта изменены параметры безопасности.</p> <ul style="list-style-type: none"> • Central Management service
Откат	<p>LifeCycle Manager используется для восстановления предыдущей версии объекта.</p> <ul style="list-style-type: none"> • Управление жизненным циклом

Событие	Описание, а также серверы и клиенты, создающие тип события
Выполнить	<p>Задание выполняется.</p> <ul style="list-style-type: none"> • Служба планирования обновления аутентификации • Службы планирования Crystal Reports для Enterprise • Служба планирования Crystal Reports • Desktop Intelligence • Служба планирования доставки в места назначения • Служба планирования LCM • Управление жизненным циклом • Служба планирования поиска по платформе • Служба планирования зонда • Служба планирования программ • Служба планирования публикаций • Служба тиражирования • Служба планирования запросов безопасности • Служба планирования импорта пользователей и групп • Служба планирования Visual Difference • Служба планирования и публикаций Web Intelligence
Сохранить	<p>Объект сохранен после обновления или изменения.</p> <ul style="list-style-type: none"> • Analysis, выпуск для OLAP • Служба кэша Crystal Reports • Службы планирования Crystal Reports для Enterprise • Служба планирования Crystal Reports • Служба просмотра и изменения Crystal Reports • Dashboards • Desktop Intelligence • Служба Information Engine • Управление жизненным циклом • Multi-Dimensional analysis service • SAP BusinessObjects Mobile • Web Intelligence • Общая служба Web Intelligence • Основная служба Web Intelligence • Служба обработки Web Intelligence
Поиск	<p>Выполнен поиск.</p> <ul style="list-style-type: none"> • Служба поиска • Explorer • Управление жизненным циклом
Триггер	<p>Запущено событие файла.</p> <ul style="list-style-type: none"> • Служба событий • Central Management service

Событие	Описание, а также серверы и клиенты, создающие тип события
Просмотр	<p>Объект просматривается.</p> <ul style="list-style-type: none"> • Analysis, выпуск для OLAP • Стартовая панель BI • Приложение "Рабочие пространства BI" • СМС • Служба кэша Crystal Reports • Служба просмотра и изменения Crystal Reports • Служба кэша Dashboards • Desktop Intelligence • Служба Information Engine • Открыть документ • SAP BusinessObjects Mobile • Web Intelligence • Общая служба Web Intelligence • Основная служба Web Intelligence • Служба обработки Web Intelligence
Добавление в VMS	<p>Объект добавляется к системе контроля версий LCM.</p> <ul style="list-style-type: none"> • Управление жизненным циклом
Возврат VMS	<p>Объект возвращен в систему контроля версий LCM.</p> <ul style="list-style-type: none"> • Управление жизненным циклом
Изъятие VMS	<p>Объект изъят из системы контроля версий LCM.</p> <ul style="list-style-type: none"> • Управление жизненным циклом
Экспорт VMS	<p>Ресурс экспортирован из VMS.</p> <ul style="list-style-type: none"> • Управление жизненным циклом
Блокировка VMS	<p>Ресурс в VMS заблокирован.</p> <ul style="list-style-type: none"> • Управление жизненным циклом

Событие	Описание, а также серверы и клиенты, создающие тип события
Разблокирование VMS	Ресурс заблокирован в VMS. • Управление жизненным циклом
Извлечение VMS	Объект извлечен из системы контроля версий LCM. • Управление жизненным циклом
Удаление VMS	Объект удален из системы контроля версий LCM. • Управление жизненным циклом

События по типам служб

Тип службы	Создаются типы событий
Служба планирования обновления аутентификации	<ul style="list-style-type: none"> • Доставка • Выполнить
Стартовая панель BI	Просмотр
Central Management Service	<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 планирования Crystal Reports	<ul style="list-style-type: none"> • Доставка • Подсказка • Обновить • Выполнить • Сохранить
Служба кэша Crystal Reports	<ul style="list-style-type: none"> • Подсказка • Обновить • Сохранить • Просмотр

Тип службы	Создаются типы событий
Службы планирования Crystal Reports для Enterprise	<ul style="list-style-type: none"> • Доставка • Подсказка • Обновить • Выполнить • Сохранить
Служба планирования Crystal Reports	<ul style="list-style-type: none"> • Доставка • Подсказка • Обновить • Выполнить • Сохранить
Служба просмотра и изменения Crystal Reports	<ul style="list-style-type: none"> • Создать • Сохранить • Просмотр
Служба кэша Dashboards	<ul style="list-style-type: none"> • Подсказка • Обновить • Просмотр
Приложение Dashboards	<ul style="list-style-type: none"> • Сохранить
Desktop Intelligence (клиент)	<ul style="list-style-type: none"> • Доставка • Подсказка • Получить • Выполнить
Процесс планировщика Desktop Intelligence	<ul style="list-style-type: none"> • Доставка • Выполнить
Служба планирования доставки в места назначения	<ul style="list-style-type: none"> • Доставка • Выполнить
Служба событий	Триггер
Служба Information Engine	<ul style="list-style-type: none"> • Создать • Выйти из режима перехода по иерархии • Изменить • Страница извлечена • Подсказка • Обновить • Сохранить • Просмотр

Тип службы	Создаются типы событий
Служба планирования LCM	Выполнить
Служба LCM	<ul style="list-style-type: none"> • Создание • Удаление • Конфигурация LCM • Изменить • Откат • Выполнить • Сохранить • Добавление в VMS • Возврат VMS • Изъятие VMS • Удаление VMS • Экспорт VMS • Блокировка VMS • Извлечение VMS • Разблокирование VMS • Поиск
Live Office	<ul style="list-style-type: none"> • Подсказка • Обновить
Multi-Dimensional analysis service	<ul style="list-style-type: none"> • Соединение с кубом • Сеанс MDAS • Сохранить
OpenDocument	Просмотр
Служба планирования поиска по платформе	<ul style="list-style-type: none"> • Доставка • Выполнить
Служба поиска по платформе	Поиск
Служба планирования зонда	<ul style="list-style-type: none"> • Доставка • Выполнить
Служба планирования программ	<ul style="list-style-type: none"> • Доставка • Выполнить
Служба планирования публикаций	Выполнить
Служба тиражирования	Выполнить
Служба планирования запросов безопасности	<ul style="list-style-type: none"> • Запуск • Доставка

Тип службы	Создаются типы событий
Служба планирования импорта пользователей и групп	<ul style="list-style-type: none">• Запуск• Доставка
Служба планирования Visual Difference	Выполнить
Приложение Web Intelligence	<ul style="list-style-type: none">• Создать• Выйти из режима перехода по иерархии• Изменить• Изменить• Подсказка• Обновить• Сохранить• Просмотр
Общая служба Web Intelligence	<ul style="list-style-type: none">• Создать• Выйти из режима перехода по иерархии• Изменить• Страница извлечена• Подсказка• Обновить• Сохранить• Просмотр

Тип службы	Создаются типы событий
Основная служба Web Intelligence	<ul style="list-style-type: none"> • Создать • Выйти из режима перехода по иерархии • Изменить • Страница извлечена • Подсказка • Обновить • Сохранить • Просмотр
Служба обработки Web Intelligence	<ul style="list-style-type: none"> • Создать • Выйти из режима перехода по иерархии • Изменить • Страница извлечена • Подсказка • Обновить • Сохранить • Просмотр
Служба планирования и публикаций Web Intelligence	<ul style="list-style-type: none"> • Доставка • Выполнить

Свойства и сведения о событиях

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 подсказки 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.

В некоторых случаях сведения о событии могут содержать несколько значений. Эти сведения можно сгруппировать при помощи группового идентификатора. Дополнительные сведения см. в соответствующем разделе о групповых идентификаторах.

Любые многоязычные данные (например, имена объекта или папок) будут записаны локально на языке аудитора CMS по умолчанию.

См. также

- [Таблицы аудита склада данных](#)

21.3.1 События и сведения 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.

Универсальные свойства и детали события

В следующей таблице представлены свойства и детали событий, характерные для всех событий.

Примечание:

Представленные в этой таблице свойства являются столбцами в таблице ADS_EVENT в хранилище данных аудита.

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 папке объекта в репозитории CMS. Например, Sales/North America/East Coast
Folder_ID	CUID папки, в которой хранится объект.
Top_Folder_Name	Имя папки верхнего уровня, в которой хранится объект. Например, если объект размещен Sales/North America/East Coast, значение будет Sales.
Top_Folder_ID	CUID папки верхнего уровня, в которой хранится объект. Например, если объект размещен в Sales/North America/East Coast, значением будет CUID папки Sales.
Cluster ID	CUID кластера CMS, записавшего событие.
Action_ID	Уникальный идентификатор, который может быть использован для связи последовательности событий, вызванных одним действием пользователя.

Примечание:

Представленные в этой таблице свойства являются столбцами в таблице ADS_EVENT_DETAIL_TYPE_STR в хранилище данных аудита.

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 информационная панель).
Имя элемента	3	Идентификатор, созданный для объекта, который содержится в контейнере объекта (например, документ Live Office или 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.
Имя юниверса	14	Имя юниверса, используемое документом/объектом. Если используется более одного юниверса, сведения события будут созданы для каждого.
Имя группы 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.

Общие события

Следующие события являются общими для всех серверов и клиентов SAP BusinessObjects.

Представление

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).

Примечание:

При использовании службы поиска в процессе индексации документов может появляться большое число событий просмотра, созданных пользователем "Системная учетная запись". Это связано с тем, что для построения поискового индекса документы открываются службой индексации.

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 юни-верса	31	Имя юниверса, используемого документом или объектом. Сведения о событии будут созданы для каждого юниверса, вызываемого документом или объектом.

Подробности события	Идентификатор	Описание
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.

Подсказка

Для подсказки введено значение.

- Идентификатор типа события: 1004

Подробности события	Идентификатор	Описание
Имя подсказки	26	Имя подсказки присвоено (например, "Дата"). Для каждой подсказки в документе или объекте будут созданы и сгруппированы отдельные сведения.
Значение подсказки	27	Введено значение подсказки. Отдельные сведения будут созданы для каждого введенного значения. Они могут быть сгруппированы и связаны с именем подсказки.
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 Dashboards, заданное на этапе его разработки. Создается только для обновлений Dashboards, либо документов Dashboards или Live Office, включающих подсказку.
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 подсказку.

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 папке контейнера	64	Путь к папке 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	Записываются следующие параметры: <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	75	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

Извлечение

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 клиента, сообщенное клиентом	51	Имя хоста клиента согласно отчету клиента.
Имя хоста клиента, разрешенное сервером	52	Имя хоста, разрешенное сервером. Если сервер не может разрешить имя хоста, значение не записывается.
IP-адрес клиента, сообщенный клиентом	53	IP-адрес клиента согласно отчету клиента.
IP-адрес клиента, разрешенный сервером.	54	IP-адрес, 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.

Инициация

Запуск события файла.

- Идентификатор типа события: 1016

Подробности события	Идентификатор	Описание
Имя файла	18	Имя отслеживаемого файла, запустившего событие.

21.3.1.1 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.
Принципал	118	Идентификатор пользователя или группы пользователей (принципала), для которых были изменены права безопасности.
Имя принципала	119	Имя пользователя или группы пользователей (принципала), для которых были изменены права безопасности.

Пользовательский уровень доступа изменен

Пользовательский уровень доступа был изменен.

- Идентификатор типа события: 10004

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.
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.
Принципал	118	Идентификатор пользователя или группы пользователей (принципала), для которых были изменены права безопасности.

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	78	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 СМС аудита. Это определяет, сколько дней будут сохраняться данные аудита в ADS.

21.3.1.2 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

21.3.1.3 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.

21.3.1.4 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, пользователи могут его редактировать.

- Идентификатор типа события: 10908

Подробности события	Идентификатор	Описание
Версия	104	Записывает номер версии документа в VMS.
Автор разблокирования	10902	Имя пользователя, выполнявшего действие.

Удаление VMS

Ресурс удаляется из VMS.

- Идентификатор типа события: 10909

Подробности события	Идентификатор	Описание
Версия	104	Записывает номер версии документа в системе управления версиями.

Поиск по платформе

22.1 Описание поиска по платформе

Поиск по платформе позволяет выполнять поиск содержимого внутри репозитория SAP BusinessObjects Business Intelligence. Результаты поиска уточняются, группируются в категории и ранжируются с учетом значимости.

В данной версии SAP BusinessObjects Business Intelligence поиск по платформе дополнен перечисленными ниже функциями:

- Поиск содержимого BOE и 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.

22.1.1 Platform Search SDK

Поиск по платформе поддерживает публичный SDK, функционирующий в качестве интерфейса 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 прикладного программирования (API) поиска по платформе см. в *Справочнике по Java API для SAP BusinessObjects Enterprise*.

22.1.2 Кластеризованная среда

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

Механизм восстановления при отказе дает возможность пользователям в случае сбоя продолжать поиск и позволяет избежать прерывания операций индексирования. 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.

22.2 Настройка поиска по платформе

22.2.1 Развертывание OpenSearch

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 BI по умолчанию устанавливается сервер приложений Tomcat.

22.2.1.1 Развертывание вручную

Чтобы развернуть OpenSearch в среде платформы BI, выполните следующие действия:

1. Перейдите в папку `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\`.
2. Скопируйте папку OpenSearch в `<INSTALLDIR>\tomcat\webapps\`.
3. Измените параметры конфигурации в файле `OpenSearch\WEB-INF\config.properties`:
 - CMS: имя CMS и порт — `<имя CMS>:<номер порта>`.
 - OpenDocURL — URL-адрес приложения OpenDocument:
`http://<tomcat>host:<connector port>/BOE/OpenDocument/opendoc/openDocument.jsp`.
 - Proxy.rpurl — имя обратного прокси-сервера, необходимое 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.

22.2.1.2 Развертывание 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 `config.<сервер приложений>` в папке `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf` необходимыми параметрами сервера веб-приложений, в т.ч. каталогом установки, именем экземпляра, портом администрирования, именем пользователя и паролем администратора.
2. Измените параметры конфигурации в файле `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\OpenSearch\WEB-INF\config.properties`:
 - CMS: имя CMS и порт — `<имя CMS>:<номер порта>`.

- OpenDocURL — URL-адрес приложения OpenDocument: `http://<хост сервера веб-приложений>:<порт_соединения>/BOE/OpenDocument/opendoc/openDocument.jsp`
 - Proxy.rpurl — имя обратного прокси-сервера, необходимое для использования обратного прокси.
 - Proxy.opendoc.rpurl: имя обратного прокси-сервера opendoc, требуемое для использования обратного прокси.
3. Выполните команду `wdeploy.bat <сервер веб-приложений>`
- ```
-Dapp_source_tree=<родительская папка веб-приложения OpenSearch>
-DAPP=OpenSearch deploy в папке <INSTALLDIR>\SAP BusinessObjects Enterprise
XI 4.0\wdeploy.
```
- Например, с помощью следующей команды OpenSearch разворачивается на сервере веб-приложений WebSphere 7:
- ```
wdeploy.bat websphere7 -Dapp_source_tree="<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles"
-DAPP=OpenSearch deploy
```
4. Перезапустите сервер приложений.

22.2.2 Настройка обратного прокси

Для разворачивания веб-приложений Business Intelligence на сервере веб-приложений, расположенном за обратным прокси-сервером, необходимо настроить обратный прокси-сервер на сопоставление входящих URL-запросов с верным WAR-файлом.

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 соответствующим образом 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 для Open Doc (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://<хост Tomcat>:<порт соедините ля>/BOE/OpenDocument/`
 - `ProxyPass /RP/OpenSearchRP/ http://<хост Tomcat>:<порт соедините ля>/OpenSearch/`
 - `ProxyPassReverseCookiePath /BOE /RP/BOE`
 - `ProxyPassReverseCookiePath /OpenSearchRP /RP/OpenSearchRP`

4. Перезапустите обратный прокси-сервер Apache 2.2.

22.2.3 Настройка свойств приложения в СМС

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 следующих параметров платформы:

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. Для остановки индексации нажмите Остановить индексацию .
Региональные параметры индекса по умолчанию	При поиске на платформе используются региональные параметры, указанные на странице СМС для индексации всех нелокализованных документов BI. Когда документ локализован, для индексации используется соответствующий файл анализа языка. Поиск основан на региональных параметрах продукта клиента, приоритет отдается региональным параметрам продукта клиента. Приоритет можно настроить на странице настройки СМС.

Действие	Описание
Периодичность поиска	<p>Индексацию всего репозитория платформы SAP BusinessObjects 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 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> справки по поиску по платформе в <i>интерактивной справке СМС по платформе SAP BusinessObjects Business Intelligence</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>Индексы хранятся 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 процесса поиска начальные попадания извлекаются по основному индексу, а индексы проверки орфографии используются для извлечения предположений. В кластеризованном развертывании платформы BI 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, {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Имя сервера>\ContentStores.</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"> a. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Имя сервера>\ContentStores. b. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Имя сервера 1>\ContentStores. <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. Индексы 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>

Действие	Описание
	<ul style="list-style-type: none"> • Все места размещения индексов должны иметь общий доступ. • Чтобы изменить расположение индекса, нажмите кнопку Остановить индексацию. • При изменении расположения индекса скопируйте 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 подсказок 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"> • Crystal Reports • Web Intelligence • Универс • Рабочее пространство BI • Microsoft PowerPoint • Adobe Acrobat • Формат RTF • Текст • Microsoft Word • Microsoft Excel

Действие	Описание
Перестроить индекс	<p>Эта функция удаляет все существующие индексы и повторно индексирует весь репозиторий.</p> <p>Функцию Перестроить индекс можно использовать независимо от состояния индексации. Существующий индекс удаляется при сохранении изменений, внесенных на странице свойств. Тем не менее, если индексация остановлена, индекс не будет перестроен до перезапуска индексации.</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.

22.3 Работа с поиском по платформе

22.3.1 Индексация содержимого в репозитории CMS

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.

Для успешного выполнения индексации должны быть активны и подключены следующие серверы:

- Входящий файловый сервер репозитория (IFRS)
- Исходящий файловый сервер репозитория (OFRS)
- Центральный сервер управления (CMS)
- Настраиваемый сервер обработки (APS), на котором размещена служба Platform Search

Если выбран тип объекта Web Intelligence или отчет Crystal, то соответствующие серверы обработки Web Intelligence или серверы приложений Crystal Reports должны быть запущены и активированы для 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.

См. также

- [Настройка свойств приложения в СМС](#)
- [Типы содержимого, доступного для поиска](#)

22.3.2 Список сбоев индексации

Список случаев сбоя индексации содержит перечень документов, которые не удалось проиндексировать. Поиск по платформе предоставляет три попытки индексирования документа. Если индексировать документ не удастся, он указывается в списке случаев сбоя индексации.

Для просмотра списка ошибок индексирования выполните следующие действия:

1. Перейдите в область СМС "Приложения".
2. Выберите **Приложение поиска по платформе**.
3. Выберите **Действия > Список ошибок индексирования**.

Будет открыто диалоговое окно "Приложение Platform Search", 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.

22.3.3 Результаты поиска

22.3.3.1 Предварительный поиск

22.3.3.1.1 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 SAP BusinessObjects Business Intelligence.

Проанализировав структуру юниверсов и существующих отчетов в репозитории 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 мера 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 анализирует 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.

22.3.3.1.2 Типы содержимого, доступного для поиска

Содержимое, опубликованное в платформе BI, доступно 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.
Файлы RTF, PDF, PPT и TXT	Весь текст в таких файлах подлежит поиску.

Тип объекта	Индексируемое содержимое
LCMJob, страница AFDashboard, инструментальные панели, ObjectPackage, запрос веб-службы (QaaWS), профиль, обсуждения, InformationDesigner, виджеты для платформы SAP BusinessObjects BI, MDAnalysis, 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>

Тип объекта	Индексируемое содержимое
Рабочее пространство BI	<ul style="list-style-type: none"> Заголовок, описание и содержимое индексируются для следующих модулей BIW: <ul style="list-style-type: none"> Текстовый модуль Модуль веб-страниц Модуль "Список навигации" Модуль "Средство просмотра" Индексируются заголовок и описание составного модуля. Индексируется только заголовок модуля шаблона рабочего пространства. Для модуля группы индексируются заголовки и метаданные входящих в него модулей. Индексируются заголовок, описание и CUID модулей InfoObject в BIW. <p>Примечание: Поскольку для встроенного модуля InfoObject индексируются только заголовок и описание, при попытке поиска содержимого InfoObject не возвращаются ссылки на этот модуль. Например, если в BIW вставлен компонент CR, индексируются его заголовки и описание. При попытке поиска содержимого этого компонента CR ссылки на встроенный модуль не возвращаются.</p> <ul style="list-style-type: none"> Если в BIW присутствует несколько родительских и дочерних вкладок, также индексируются их заголовки и содержимое.

Тип объекта	Индексируемое содержимое
CR Next Gen	<p>Заголовок, описание, формула выбора, сохраненные данные, текстовые поля любого раздела, значения параметров и подотчеты.</p> <p>Не поддерживаются следующие объекты в отчетах CR Next Gen:</p> <ul style="list-style-type: none"> • Отчет кросс-таблицы • Извлечение данных диаграммы • Извлечение изображений и связанных метаданных • Встроенные OLE-объекты (например, встроенный в компонент CR документ Word) • Извлечение объекта Flash <p>Кроме того, постраничное считывание данных из отчета CR Next Gen невозможно.</p>
Юниверс	<p>Содержимое данных доступно для поиска.</p> <p>Примечание: По умолчанию возможность индексации юниверсов включена. Если запросы, используемые Platform Search для индексации содержимого юниверса, выполняются слишком долго и влияют на производительность сервера БД, то рекомендуется отключить параметр индексации юниверсов в СМС. Пример запроса, используемого Platform Search при индексации содержимого юниверса: Select distinct SampleColumnName from SampleTableName LIMIT 1000</p> <p>Выполните указанные ниже действия, что отключить индексацию юниверсов.</p> <ol style="list-style-type: none"> 1. Выполните вход в консоль Central Management Console (CMC). 2. Выберите Приложения. 3. Перейдите к приложениям поиска по платформе и выберите Свойства. 4. Перейдите к типам содержимого и снимите флажок Юниверс. 5. Нажмите кнопку Сохранить и закрыть.

Примечание:

Максимальный поддерживаемый размер документов Agnostic (MS Office 2003 и 2007, а также документы PDF) составляет 15 МБ.

22.3.3.2 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.

22.3.3.3 Заключительный поиск

22.3.3.3.1 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 аспекты 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 Reports, Microsoft Word (2003 и 2007), Microsoft Excel (2003 и 2007) и Dashboards.
- Универс и соединения: 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.

22.3.3.3.2 Упорядочение ранжирования результатов поиска.

Поиск по платформе учитывает расположение искомого термина при ранжировании документа. Группировка содержимого происходит на основе вхождения содержимого в документ по следующим категориям:

1. Метаданные платформы
2. Метаданные документа
3. Метаданные содержимого
4. Содержимое

Вес для указанных выше категорий можно настроить в СМС.

Настройка веса для ранжирования результатов поиска

Поиск по платформе позволяет установить веса для содержимого, сгруппированного по категориям, основанного на вхождении содержимого в документ таким образом, что можно задать высшее значение для требуемой категории для более быстрого получения соответствующих результатов поиска.

Для настройки веса выполните описанные ниже действия.

1. В области СМС «Управление» щелкните элемент **Приложения**.
2. Откройте приложение **Platform Search**.
3. Выберите **Рейтинг**.
Отобразится вес различных категорий содержимого, например метаданных платформы, документа, содержимого, а также самого содержимого. Параметр «Языковой стандарт пользователя» - это стандарт, установленный в параметрах стартовой панели BI.
4. Установите вес в соответствии с требованиями.
5. Выберите **Сохранить**.

Если при обновлении к уже индексированным документам необходимо применить ранжирование, то потребуются повторно создать индекс. Дополнительные сведения см. в разделе о повторном создании индекса [Настройка свойств приложения в СМС](#).

22.3.3.3.3 Многоязыковая поддержка

Поиск по платформе реализует поддержку многих языков, позволяя индексировать содержимое, извлекать результаты поиска и получать предложения вариантов на необходимом языке. Для индексации всех нелокализованных документов платформы BI используется языковой стандарт, установленный в поле СМС **Языковой стандарт индекса по умолчанию**.

После локализации информационного объекта при поиске по платформе используется соответствующий языковой анализатор для индексации документа.

Поиск основан на языковом стандарте, установленном как языковой стандарт продукта клиента. Поиск по платформе Platform Search придает больше веса языковому стандарту продукта клиента при получении результатов поиска. Вес настраивается в СМС.

22.3.3.3.4 Предложения

Platform Search 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.

При наличии нескольких терминов, которые могут совпадать с исходным запросом, функция поиска предложит три наиболее подходящих варианта на языке, выбранном в поле СМС **Языковой стандарт индекса по умолчанию**.

Примечание:

Поиск Platform Search не создает предложения в следующих случаях:

- 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

22.3.3.3.5 Объединение результатов поиска из SAP BusinessObjects Explorer

Поиск по платформе объединяет поисковый запрос из SAP BusinessObjects Explorer и поверхности InfoSpaces с содержимым 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.

22.4 Интеграция поиска по платформе 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" платформы SAP BusinessObjects Business Intelligence.

22.4.1 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**.

22.4.2 Импорт роли пользователя в аутентификации SAP BusinessObjects Business Intelligence

Выполните следующие действия, чтобы импортировать роль пользователя в аутентификацию 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.

22.5 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.

22.6 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 отправки событий аудита служба Platform Search должна работать на одном сервере со службой прокси аудита клиента.

Для Platform Search выделен идентификатор типа события 1009 и четыре идентификатора элементов сведений события для Platform Search:

- 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 стандартные элементы 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:

- Идентификатор типа события: 1009
- Ид. 19 типа сведений события со значением "продажи"
- Ид. 63 типа сведений события со значением 5
- 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 созданы фасеты и выбраны одна или несколько из них, аудит применяется к следующим событиям:

- Идентификатор типа события: 1009
- Ид. 19 типа сведений события со значением "продажи"
- Ид. 63 типа сведений события со значением 5
- Ид. 20 типа сведений события с 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:

- Идентификатор типа события: 1009
- Ид. 19 типа сведений события со значением "продажи"
- Ид. 63 типа сведений события со значением 0
- Ид. 1 типа сведений события с 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

22.7 Устранение неполадок

22.7.1 Самовосстановление

В приложении поиска по платформе предусмотрен механизм самовосстановления. Он 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.

22.7.2 Проблемные сценарии

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. Перейдите в папку `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging\`, которая содержит 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 Crystal Reports

Поиск по платформе индексирует содержимое отчетов Crystal Reports 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, например, заголовка, описания и ключевых слов, которые являются свойствами 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 информационные пространства InfoSpaces из SAP BusinessObjects Explorer

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 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 платформа BI, 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 в платформу BI с предоставлением соответствующих прав. Для проверки прав пользователя перейдите в раздел **Аутентификация** в CMC и выберите **SAP**.

См. также

- [Список сбоев индексации](#)
- [Настройка свойств приложения в CMC](#)
- [Типы содержимого, доступного для поиска](#)

Интеграция

23.1 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.

Функция интеграции 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	Диспетчер Business View, DataConnection, списки значений, основание 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.

23.2 Термины для функции интеграции

В следующем списке терминов представлены слова и фразы, которые относятся к функции интеграции и могут облегчить его использование.

Выполняемые локально завершённые экземпляры

Экземпляры, обрабатываемые на сайте-адресате и передаваемые обратно на сайт-источник.

Двунаправленное тиражирование

Действие равнозначно действию однонаправленного тиражирования, но при двунаправленном 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.

Задание тиражирования

Объект, в котором содержится информация о планировании содержимого, содержанием, подлежащем тиражированию, и любых специальных условиях, которые должны выполняться при тиражировании содержимого.

Локальный

Локальная система, к которой подключен пользователь или администратор. Например, администратор сайта-адресата считается «локальным» на сайте-адресате.

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.

Обновление тиражирования

Все объекты в списке тиражирования обновляются вне зависимости от последней измененной версии.

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.

Однонаправленное тиражирование

Объекты тиражируются только в одном направлении: с сайта-источника на сайт-адресат. Любые обновления на сайте-адресате остаются на сайте-адресате.

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).

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.

Сайт-адресат

Система платформы BI, извлекающая реплицированное содержимое платформы BI с исходного сайта.

Сайт-источник

Система платформы BI, из которой поступает содержимое.

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.

Тиражирование

Процесс копирования содержимого из одной системы платформы BI в другую.

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.

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.

Удаленный

Система, которая не является локальной для пользователя. Например, сайт-источник считается «удаленным» для пользователей и администраторов сайта-адресата.

23.3 Управление правами безопасности

Однако, поскольку функция интеграции тиражирует содержимое между отдельными системами, и требуется взаимодействие с другими администраторами, необходимо знать механизм работы безопасности перед использованием этого модуля.

Перед включением функции интеграции 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 функции интеграции
- Сценарии интеграции

Совет:

Перед началом использования функции интеграции рекомендуется прочитать этот раздел.

23.3.1 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
Двунаправленное 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](#)

23.3.2 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](#)

23.3.3 Права, характерные для интеграции

В этом разделе подробно описаны сценарии, которые встречаются при использовании функции интеграции.

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>	

23.3.4 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.

23.3.5 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.

23.4 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.

23.4.1 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

23.4.2 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](#)

23.4.3 "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 функции интеграции 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 функцию интеграции 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.

23.5 Тиражирование сторонних пользователей и групп

В функции интеграции 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 функции интеграции.
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 функция интеграции не сможет сопоставить пользователя или группы.

Пример:

Администратор сопоставляет группу A и пользователя A на сайте-источнике и сайте-адресате. Для группы A и пользователя A созданы различные уникальные идентификаторы на сайте-источнике и сайте-адресате. Во время тиражирования функции интеграции не удастся сопоставить их, и группа A или пользователь A 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 функции интеграции.

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 функция интеграции не сможет правильно выполнить тиражирование.

Примечание:

Важно создать учетную запись на одном сайте, а затем тиражировать ее на другой сайт.

23.6 Тиражирование юниверсов и соединений юниверсов

При использовании модуля "Интеграция" для тиражирования юниверсов между развертываниями платформы VI 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 соединения 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».

23.7 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 Dashboards. 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

23.7.1 Создание списков тиражирования

Списки тиражирования располагаются в области "Списки тиражирования" консоли СМС. Для упорядочения списков тиражирования можно создавать папки и вложенные папки.

23.7.1.1 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.

23.7.1.2 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», функция интеграции 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 **Объекты репозитория** в разделе «Тиражировать все» для тиражирования всех объектов Business View, бизнес-элементов, оснований данных, соединений для передачи данных, списков 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**.

23.7.2 Изменение списков тиражирования

После создания списка тиражирования можно изменить его свойства или объекты.

23.7.2.1 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](#)

23.7.2.2 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](#)

23.8 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.

23.8.1 Создание удаленных соединений

Удаленное соединение в функции интеграции 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.

23.8.1.1 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.

23.8.1.2 Создание удаленного соединения

Чтобы подключиться к удаленному развертыванию платформы BI, необходимо создать удаленное соединение в функции интеграции.

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 функции интеграции, которые автоматически развертываются на сервере Java-приложений. Можно использовать любые веб-службы функции интеграции в платформе BI, в которой они являются сайтом-источником или сайтом-адресатом, или другое развертывание. Используйте следующий формат: <code>http://имя_компьютера_сервера_приложений:порт/dswsbobje</code> Пример: <code>http://mymachine.mydomain.com:8080/dswsbobje</code>
CMS удаленной системы	Имя сервера CMS, к которому необходимо подключиться и который доступен через веб-службы функции интеграции. Он будет использоваться как сервер CMS для сайта-источника. Используется следующий формат: <code>имя_CMS:порт</code> Пример: <code>mymachine:6400</code> 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](#)

23.8.2 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**.

23.9 Управление заданиями тиражирования

Задание тиражирования – это тип объекта, который выполняется по расписанию и используется для тиражирования содержимого между двумя развертываниями платформы BI в функции интеграции.

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.

23.9.1 Создание заданий тиражирования

Задание тиражирования требуется для тиражирования содержимого между двумя развертываниями платформы BI в функции интеграции. Для каждого задания тиражирования должно быть создано только одно удаленное соединение и установлена связь с одним списком тиражирования.

23.9.1.1 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](#)

23.9.2 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.

23.9.2.1 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.

23.9.3 Изменение заданий тиражирования

После создания задания тиражирования в функции интеграции можно изменить его свойства.

23.9.3.1 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.

23.9.4 Просмотр журнала после выполнения задания тиражирования

При каждом выполнении задания тиражирования функция интеграции 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

23.10 Управление очисткой объектов

В функции интеграции 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.

23.10.1 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.

23.10.2 Ограничения очистки объектов

В объекте удаленного соединения можно указать число объектов, которые будут одновременно очищаться при выполнении задания тиражирования. В функции интеграции 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.

23.10.3 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](#)

23.11 Управление обнаружением и разрешением конфликтов

В функции интеграции 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.

23.11.1 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 интеграции 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. 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 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.

23.11.2 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.

23.12 Использование веб-служб в функции интеграции

В функции интеграции веб-службы используются для передачи объектов и их изменений между сайтом-источником и сайтом-адресатом. Веб-службы функции интеграции 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 функции интеграции.

23.12.1 Переменные сеанса

Если в одном задании тиражирования передается большое число файлов содержимого, может потребоваться увеличение времени ожидания сеанса веб-служб в функции интеграции.

Это свойство находится в файле `dsws.properties`:

<Каталог установки сервера приложений>\dswsobje\Web-INF\classes

Например:

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI  
4.0\warfiles\webapps\dswsobje\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.

Новые свойства вступают в силу только после повторного развертывания измененного веб-приложения на компьютере, на котором запущен сервер веб-приложений. Воспользуйтесь WDeploy для повторного развертывания WAR-файла на сервере веб-приложений. Для получения сведений об использовании WDeploy см. *Руководство по развертыванию веб-приложений платформы BusinessObjects Business Intelligence*.

23.12.2 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\SAP BusinessObjects Enterprise XI 4.0\warfiles\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.

Новые свойства вступают в силу только после повторного развертывания измененного веб-приложения на компьютере, на котором запущен сервер веб-приложений. Воспользуйтесь WDeploy для повторного развертывания WAR-файла на сервере веб-приложений. Для получения сведений об использовании WDeploy см. *Руководство по развертыванию веб-приложений платформы BusinessObjects Business Intelligence*.

23.12.3 Настраиваемое развертывание

Веб-службы функции интеграции можно развернуть автоматически, необходимо включить службы «federation», «biplatform» и «session». Чтобы отключить функцию интеграции 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\SAP BusinessObjects Enterprise XI 4.0\warfiles\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 интеграции:

Файл `services.xml` расположен в каталоге:

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\dswebobje\WEB-INF\services\federator\META-INF
```

Измените имя службы с

```
<service name="Federator">
```

на

```
<service name="Federator" activate="false">
```

Новые свойства вступают в силу только после повторного развертывания измененного веб-приложения на компьютере, на котором запущен сервер веб-приложений. Воспользуйтесь WDeploy для повторного развертывания WAR-файла на сервере веб-приложений. Для получения сведений об использовании WDeploy см. *Руководство по развертыванию веб-приложений платформы BusinessObjects Business Intelligence*.

23.13 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.

23.13.1 Удаленное планирование

При использовании функции интеграции 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](#)

23.13.2 Экземпляры, выполняемые локально

Экземпляры, выполняемые локально, – это экземпляры отчета, которые обрабатываются из отчетов на сайте-адресате. При использовании функции 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.

23.13.3 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](#)

23.14 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 интеграции.

Примечание:

Миграции объектов лучше всего выполняются участниками группы "Администраторы", в частности владельцами учетной записи "Администратор". Чтобы перенести объект, может потребоваться также перенести большое количество связанных объектов. Получение требуемых прав безопасности для всех объектов может оказаться невозможным для делегированной учетной записи администратора.

23.14.1 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 А – это сайт-адресат в процессе интеграции. Отчет А, тиражированный отчет в системе А, импортируется из системы А в систему Б платформы BI с помощью LifeCycle Manager.

Результат. После копирования отчета А в систему Б платформы BI в нем не содержатся тиражированные данные. Отчет А больше не отмечен значком тиражирования. Если объект находился в состоянии конфликта в системе А платформы BI, состояние конфликта будет отсутствовать в системе Б. Фактически объект воспринимается как объект, созданный в системе Б.

Примечание:

Идентификатор CUID может различаться в зависимости от параметров импорта, настроенных в LifeCycle Manager.

23.14.2 Импорт тиражированного содержимого и продолжение тиражирования

После импорта тиражированного содержимого может потребоваться включение импортированных объектов в процесс интеграции. 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 функцию интеграции 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 функции интеграции для тиражирования объекта.

Пример:

Отчет А был создан в системе А платформы BI. В системе Х функция интеграции использовалась для тиражирования отчета А из системы А в систему Х. Затем LifeCycle Manager использовался для импорта отчета А из системы Х в систему Y.

План. В системе Y необходимо настроить функцию интеграции для использования в системе А и сохранить отчет А в качестве части задания тиражирования. Система Y является адресатом, а система А – 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 функцию интеграции 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.

23.14.3 Перенос содержимого из тестовой среды

В любой организации проверка часто выполняется перед размещением любого компонента в среду производства. Обычно перед настройкой функции интеграции 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 соединения и соответствующих заданий тиражирования на производственных компьютерах в среде производства, которые будут выступать в роли сайтов-адресатов.
 - Б) Использование LifeCycle Manager для импорта удаленного соединения и заданий тиражирования с сайта-адресата в среде Dev/QA на производственные компьютеры, которые будут выступать в роли сайтов-адресатов. Затем измените импортированные удаленные соединения, чтобы они указывали на компьютер в среде производства, который будет выступать в роли сайта-источника.

23.14.4 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.

23.15 Оптимальные методы работы

С помощью интеграции 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 "$SOFTWARE" = "Linux" ];
then
  JAVA_OPTS="$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 функции интеграции 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 функции интеграции 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
-Dobj.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 "$SOFTWARE" = "Linux" ]; then
  JAVA_OPTS="$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 Central Management Console (CMC)
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 функции интеграции](#)
- [Текущие ограничения выпуска](#)

23.15.1 Текущие ограничения выпуска

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 функции интеграции.

- 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 функции интеграции поддерживается тиражирование не более 100 000 объектов.

- **Права**

В функции интеграции 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](#)

23.15.2 Устранение неисправностей: сообщения об ошибках

В этом разделе описаны сообщения об ошибках, которые появляются в редких случаях при использовании функции интеграции. 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_GUID 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 функции интеграции 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 функция интеграции 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 функция интеграции 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 функцией интеграции 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 адаптивного сервера обработки добавьте следующую строку:
`-javaArgs "XX:MaxPermSize=256m".`
2. Добавьте указанные ниже параметры в Java-сервер приложений, который подключается к функции интеграции, 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 функцией интеграции, 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 адаптивного 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 соединение с юниверсом и повторно использовать его.

См. также

- [Оптимальные методы работы](#)
- [Текущие ограничения выпуска](#)

Дополнительные конфигурации для сред ERP

24.1 Конфигурации для интеграции с SAP NetWeaver

24.1.1 Интеграция с SAP Netweaver Business Warehouse (BW)

24.1.1.1 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](#)

24.1.1.1.1 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 CMC:

- 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](#)

24.1.1.1.2 Работа с шаблонами безопасности для папок по умолчанию

При публикации содержимого из SAP на платформе BI платформа автоматически создает остальные компоненты иерархии ролей, папок и отчетов. Система организует отчеты, размещая их в папках с именами, состоящими из идентификатора системы, номера клиента и имени роли.

- При определении системы контроля полномочий система создает папки верхнего уровня: папки SAP, 2.0 и системные папки (*SID*).
- Система создает папки ролей автоматически (импортируя их как группы в 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 элементами различных ролей. Приложение "Content Administration Workbench" используется для управления функциональностью создания отчетов в SAP BW. Вы можете соотносить роли в системе SAP BW с отдельными системами платформы BI, публиковать отчеты, а также синхронизировать их между SAP BW и платформой BI.

Папки содержимого

Платформа BI импортирует группу для каждой роли, добавляемой в систему контроля полномочий в соответствии с определением в CMC.

Чтобы гарантировать предоставление соответствующих прав по умолчанию всем элементам роли носителей содержимого, необходимо предоставить соответствующие права в Content

Administration Workbench для каждой системы контроля полномочий, определенной на платформе BI. Чтобы запустить Content Administration Workbench, выполните операцию /CRYSTAL/RPTADMIN:

1. В Content Administration Workbench раскройте **Система предприятия**, затем раскройте **Доступные системы**.
2. Дважды щелкните требуемую систему.
3. Щелкните вкладку **Компоновка**.
4. Настройте **Стандартная политика безопасности для отчетов на Ракурс**.
5. Настройте **Стандартная политика безопасности для папок ролей на Ракурс**.
6. Нажмите кнопку **ОК**.

Эти настройки отображаются на платформе BI для всех ролей содержимого. Т.е. ролей с опубликованным содержимым. Участники 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 участников обычных ролей.

24.1.1.2 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 с помощью службы на компьютере, где размещена платформа 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.

24.1.1.3 Настройка службы BW Publisher

В этом разделе объясняется, как активировать публикацию отчетов из BW на платформе BI, используя BW Publisher в качестве службы. Выполните следующую процедуру.

24.1.1.3.1 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, создаваемую функцией публикации из BW, установив службы BW Publisher на двух разных компьютерах в одной системе платформы BI.

При установке BW Publisher на компьютерах, на которых размещена платформа BI, необходимо настроить каждый из них для использования одного и того же идентификатора программы, шлюзового хоста и шлюзовой службы SAP. После создания адресата RFC, использующего указанный идентификатор программы, BW выравнивает нагрузку, создаваемую функцией 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 SDK платформы BI и подсистеме печати SAP Crystal Reports. Таким образом, если BW Publisher и локальный шлюз SAP устанавливаются на специальном компьютере, необходимо также установить сервер SIA.

24.1.1.3.2 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 службы BW Publisher она устанавливает соединение со службой шлюза SAP, указанной при выполнении программы установки платформы BI.

24.1.1.3.3 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.

24.1.1.3.4 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.

Если требуется выполнять публикацию из BW в несколько систем платформ BI, следует создать отдельный адресат RFC для службы BW Publisher в каждом развертывании платформы BI. Для каждого адресата необходимо использовать уникальный идентификатор программы, но одинаковый шлюз хоста и службу шлюза.

24.1.1.3.5 Настройка BW Publisher с локальным шлюзом SAP

Примечание:

Не используйте эту конфигурацию, если платформа BI установлена в системе 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](#).

24.1.1.3.6 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 проверенных сред для BusinessObjects XI Integration для SAP можно найти в файле `platforms_EN.txt`, который включен в дистрибутив вашего 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.

24.1.1.4 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.

24.1.1.5 Настройка опубликования в рабочем месте управления содержимым Content Administration Workbench

Приложение "Content Administration Workbench" используется для управления функциональностью создания отчетов в SAP BW. Можно идентифицировать роли из системы SAP BW с определенными системами платформ BI, опубликовать отчеты и синхронизировать отчеты между SAP BW и платформой BI. После настройки проверки подлинности SAP и настройки BW Publisher выполните функции, описанные в этом разделе, чтобы включить функцию публикации. Данные инструкции позволят:

- Задавать необходимые авторизации для различных пользователей рабочего места управления содержимым Content Administration Workbench.
- Настраивать соединения с платформой BI, на которой публикуется содержимое.
- Указывать, какие роли будут иметь право публикации на каждой из платформ BI.
- Публиковать содержимое из BW на платформе BI.

24.1.1.6 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.

24.1.1.7 Создание ролей в BW для назначенных издателей содержимого

При настройке BW для интеграции с платформой BI проверьте, позволяет ли существующая структура ролей быстро назначать определенных пользователей BW в качестве издателей содержимого или системных администраторов для систем платформы BI.

Рекомендуется снабжать создаваемые роли описательными именами. Примерами описательных имен ролей могут послужить BOE_CONTENT_PUBLISHERS и SBOP_SYSTEM_ADMINISTRATORS.

Совет:

Можно присвоить пользователю-администратору полный набор прав системного администратора либо некоторое подмножество этих прав.

Для изменения прав, предоставленных новым или существующим ролям в платформе BI, необходимо сначала настроить аутентификацию SAP и импортировать роли. Затем можно изменить права каждой из импортированных ролей с помощью консоли Central Management Console.

Сведения по созданию ролей находятся в документации по SAP. Дополнительные сведения по использованию ролей в администрировании содержимого находятся в разделах:

- [Импорт ролей SAP.](#)
- [Настройка папок и безопасности для платформы BI .](#)
- [Работа с шаблонами безопасности для папок по умолчанию.](#)

24.1.1.8 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 24-1: 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
S_TABU_CLI	CLIIDMAINT	X
S_TABU_DIS	ACTVT	Изменение, отображение (02, 03)
	DICBERCLS	&NC&
	JOB ACTION	DELE, RELE
	JOB GROUP	' '
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 24-2: 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 издателей нет достаточных прав для удаления отчетов с платформы, это приведет к ошибке.

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)

24.1.1.9 Определение системы платформы BI

Для каждой системы платформы BI, в которой требуется опубликовать отчеты, необходимо создать определение системы в Content Administration Workbench.

24.1.1.9.1 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** выполните следующие действия.
 - 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 работает CMS BusinessObjects Enterprise. 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 **Адреса RFC** добавьте каждый из адресов RFC, связанный с данной системой. 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. См. раздел «Распространение установки BW Publisher».

7. Установите флажок рядом с добавленным именем адреса назначения и щелкните **Проверить назначение БОЕ**.

При этом проверяется возможность связи BW с указанной службой BW Publisher и возможность входа в эту систему с помощью учетной записи системы контроля полномочий Crystal.

8. На вкладке **HTTP** выполните следующие действия:

- В поле **Протокол** введите http или https, если веб-сервер, подключенный к платформе BI, настроен на использование HTTPS.
- В поле **Узел и порт веб-сервера** введите полное имя домена или IP-адрес веб-сервера, на котором размещена стартовая панель BI. Для установленной системы, использующей сервер приложений Java, включите номер порта. Например, введите bserver01.businessobjects.com:8080.
- В поле **Путь** введите SAP.

Данный путь, по сути, является виртуальным путем, который используется веб-сервером как ссылка на подкаталог `sap` веб-содержимого платформы BI. Введите альтернативное значение, только если выполнена пользовательская настройка веб-среды и местоположения файлов веб-содержимого платформы.

Не указывайте прямую наклонную черту в начале или в конце данной записи.

- В поле **Программа просмотра** введите имя своего приложения – средства просмотра.

Чтобы применять средство просмотра платформы BI по умолчанию, которое использует версию Java стартовой панели BI, введите `openDocument.jsp`.

Если платформа BI была установлена в ОС Windows с использованием конфигурации `ASP.NET` по умолчанию, для использования стандартного браузера введите `report/report_view.aspx`.

9. На вкладке **Языки** выберите языки отчетов, которые будут публиковаться в данной системе.

10. Воспользуйтесь вкладкой **Роли**, чтобы добавить роли с содержимым, которые необходимо связать с данной системой платформы BI.

См. раздел «Импорт ролей SAP».

11. Нажмите кнопку **Вставить строку.**

Отобразится список ролей, доступных для добавления в данную систему.

Примечание:

Каждая из ролей может публиковать данные только в одной системе платформы BI. Если роли, которые необходимо добавить в данную систему платформы BI, не отображаются в списке, нажмите **Отмена**, чтобы вернуться на вкладку **Роли** и нажмите **Повт. присвоить роли**.

12. Выберите роли, которые необходимо опубликовать в этой системе, и нажмите кнопку **ОК.****13. На вкладке **Макет** выберите настройки защиты по умолчанию для папок отчетов и ролей, опубликованных в этой системе платформы BI.****Примечание:**

- На платформе BI автоматически создается папка для каждой роли, опубликованной в этой системе. В 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, удалите папки ролей и ярлыки в системе. (При этом сами отчеты удалены не будут.) Измените здесь параметры безопасности и снова опубликуйте роли и отчеты.

14. 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.

См. также

- [Распространение установки BW Publisher](#)
- [Импорт ролей SAP](#)

24.1.1.10 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 (см. раздел [Создание и применение средств авторизации](#)), может использовать приложение Content Administration Workbench для публикации и обслуживания отчетов.

24.1.1.11 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 выберите одну или несколько систем с содержимым, которое требуется отобразить.

Примечание:

Список 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 организованы в иерархическую структуру: Система платформы BI > Роли в этой системе > Отчеты, сохраненные для 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. Чтобы опубликовать все роли на платформе BI, выберите систему.

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](#)

24.1.1.12 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 с помощью запланированных заданий выполняется синхронизация информации об отчетах между BW и развертыванием 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. Для получения подробной информации см. раздел [Обновление статуса отчетов](#).

24.1.1.13 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.

24.1.1.14 Обслуживание отчетов

Задачи по поддержке отчетов включают в себя синхронизацию информации об отчетах между платформой BI и BW ("Обновить статус"), удаление ненужных отчетов ("Удалить отчеты") и обновление отчетов, перенесенных с предыдущих версий платформы ("После переноса").

24.1.1.14.1 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".

24.1.1.14.2 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.

24.1.1.15 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.

24.1.1.16 Конфигурации для обработки данных SAP

24.1.1.16.1 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_OPENSQLE_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 адаптивным сервером заданий), 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 адаптивного сервера заданий.

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](#)

24.1.1.16.2 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 адаптивного сервера заданий.
3. Войдите в Central Management Console (CMC).
4. Выберите **Серверы**.
5. Разверните узел **Категории служб** и выберите пункт **Analysis Services**.
6. Выберите **Адаптивный сервер обработки**, а затем выберите в контекстном меню команду **Свойства**.
Будет открыта страница «Свойства».
7. На странице «Свойства» найдите поле **Параметры командной строки**.

Это команда запуска для адаптивного сервера заданий. Например:

```
"\\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
```

8. Укажите перед командой по умолчанию полный путь к файлу `jobserver_batchmode.bat`, сохраненному на компьютере адаптивного сервера заданий.

В этом примере файл пакета сохранен на компьютере с именем SERVER01 как:

```
C:\Crystal Scripts\jobserver_batchmode.bat
```

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 адаптивного сервера заданий. Благодаря этому обеспечивается различие переменных среды, доступных адаптивному серверу заданий, и переменных среды, доступных серверу, который отвечает за обработку отчетов по запросу (сервер обработки и сервер приложений отчетов Crystal Reports).

9. Нажмите **Сохранить и закрыть**.
10. Щелкните правой кнопкой на адаптивном сервере заданий и в контекстном меню выберите **Запуск**.

Примечание:

Если происходит сбой запуска адаптивного сервера заданий, проверьте новую команду запуска.

24.1.1.17 Конфигурации для переносов SAP

24.1.1.17.1 Обзор

SAP BusinessObjects Enterprise содержит 8 транспортов: связь Open SQL, связь InfoSet, определение безопасности на уровне строк, определение кластера, инструментарий администрирования содержимого, транспорт персонализации параметров запросов BW, транспорт MDX и транспорт 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.

24.1.1.17.2 Настройка транспорта

Чтобы настроить компоненты Data Access или BW Publisher платформы BI, необходимо импортировать в систему SAP соответствующие транспорты. 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 SAP Business Objects необходимо разрешить пространство имен. Описание процедур, соответствующих вашей версии SAP, см. в документации SAP NetWeaver.

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 транспорта 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 вас должно быть разрешение производить запись файлов на сервер UNIX.

Транспорт

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

24.1.1.18 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.

24.1.1.18.1 Создание и применение средств авторизации

Необходимо создать и применять средства авторизации, требуемые для доступа каждого из пользователей к информации, с помощью Desktop Intelligence Integration для SAP. Конкретные 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](#)

24.1.1.19 Действия в BW

В этом разделе перечислены различные действия в модуле BW.

24.1.1.19.1 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 в BusinessObjects Enterprise

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, можно составить отчеты по запросам, содержащим только конкретные информационные области, кубы и компоненты с указанными идентификаторами.

24.1.1.19.2 Действия в стартовой панели BI

Вход в систему BusinessObjects Enterprise под учетными данными SAP

Объект авторизации	Поле	Значения
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M

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, можно 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

24.1.1.19.3 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	ST0R, ST0M
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

24.1.1.19.4 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	ST0R, ST0M

Настройка местоположения источника данных

Объект авторизации	Поле	Значения
P_ABAP	REPID	AQTGSYSTGENERATESY, SAPDBPNP
	COARS	2

24.1.1.19.5 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	ST0R, ST0M
S_TABU_DIS	ACTVT	03
	GROUP	Имя группы таблиц

Проверка базы данных

Объект авторизации	Поле	Значения
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M
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	ST0R, ST0M
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16
S_TABU_DIS	ACTVT	03
	GROUP	Имя группы таблиц

24.1.1.19.6 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 явно перечислить группы пользователей, элементами которых необходим доступ к SAP BusinessObjects Enterprise.</p>

Запуск и разработка запросов BW BeX

Если при создании отчета с использованием юниверса на основе запроса BW BeX включено измерение даты, системный администратор должен предоставить полномочия S_RS_IOBJ разработчику юниверса и пользователю, запускающему отчет.

Объект авторизации	Поле	Значения
S_RS_IOBJ	ACTVT	03
	RSIOBJ	
	RSIOBJ_CAT	
	RSIOBJ_PART	

24.2 Настройка для интеграции с JD Edwards

24.2.1 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).

24.2.1.1 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 единого входа**.
4. Выберите **crdb_pseone**.

5. Нажмите кнопку **Удалить**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. На странице **Серверы** в консоли СМС выберите **Службы Crystal Reports** и щелкните **Перезапустить сервер**.

24.2.1.2 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 единого входа**.
4. В поле «Использовать контекст единого входа для входа в базу данных со следующими драйверами», введите **crdb_pseone**.
5. Нажмите кнопку **Добавить**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. На странице **Серверы** в консоли СМС выберите **Службы Crystal Reports** и щелкните **Перезапустить сервер**.

24.2.2 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).

24.2.2.1 Включение соединений с данными JD Edwards EnterpriseOne по протоколу SSL

Примечание:

Для всех значений, описанных в следующей процедуре, учитывается регистр.

1. Запустите Central Configuration Manager (CCM).
2. Остановите агент серверной аналитики (SIA).
3. Дважды щелкните SIA, чтобы открыть диалоговое окно «Свойства».
4. Щелкните вкладку **Протокол**.
5. Выберите **Включить SSL**.
6. Для поля «Папка сертификатов SSL» выберите каталог, содержащий сертификаты SSL.
7. Для поля «Файл сертификата сервера SSL» выберите `servercert.der`.
8. Для поля «Файлы надежных сертификатов SSL» выберите `cacert.der`.
9. Для поля «Файл закрытого ключа SSL» выберите `server.key`.
10. Для поля «Файл идентификационной фразы для закрытого ключа SSL» выберите `passphrase.txt`.
11. Нажмите кнопку **Применить**.
12. Запустите агента Server Intelligence.

Чтобы эти изменения вступили в силу, необходимо перезапустить серверы отчетов платформы BI (например, адаптивный сервер заданий).

24.2.2.2 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`.

24.3 Настройка для интеграции с PeopleSoft Enterprise

24.3.1 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).

24.3.1.1 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 единого входа**.
4. Выберите **crdb_psenterprise**.
5. Нажмите кнопку **Удалить**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. На странице **Серверы** CMC выберите **Сервисы Crystal Reports** и нажмите **Перезапустить сервер**.

24.3.1.2 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 единого входа**.
4. В области «Использовать следующие драйверы для входа в базу данных контекст SSO» введите **crdb_psenterprise**.

5. Нажмите кнопку **Добавить**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. На странице **Серверы** СМС выберите **Сервисы Crystal Reports** и нажмите **Перезапустить сервер**.

24.3.2 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).

24.3.2.1 Файл свойств конфигурации SSL

Файл свойств `sslconf.properties` содержит все сведения для обязательных сертификатов, используемых компонентами платформы SAP BI. Например:

```
[default]
businessobjects.ora.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\`.

24.3.2.2 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 запросов, 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 платформы BI (например, адаптивный сервер заданий).

24.3.2.3 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.

24.3.3 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.

24.3.3.1 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.

24.3.3.2 Серверы PeopleSoft

На сервере аналитики PeopleSoft отчеты обновляются и выполняются процессом PSANALYTICSRV. На сервере аналитики 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.

24.4 Настройка для интеграции с Siebel

24.4.1 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 стартовую панель BI 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.

24.4.1.1 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 **BusinessObjects Integration**.

24.4.2 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
 - 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](#).

24.4.2.1 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 версий 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 JavaScripts 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.

24.4.3 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.

24.4.3.1 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.

24.4.3.2 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.

24.4.3.3 Проверка контекстуальной зависимости

1. В средствах Siebel Tools щелкните **Отладка > Запуск**.
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 времени ожидания 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.

24.4.3.4 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: *Общедоступные папки\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 SAP BusinessObjects. 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.

24.4.4 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).

24.4.4.1 Отключение единого входа для Siebel и Crystal Reports

1. В Central Management Console (CMC) выберите элемент **Приложения**.
2. Дважды щелкните элемент **Конфигурация Crystal Reports**.
3. Выберите элемент **Параметры единого входа**.
4. Выберите **crdb_siebel**.
5. Нажмите кнопку **Удалить**.
6. Нажмите кнопку **Сохранить и закрыть**.
7. Перезапустите SAP Crystal Reports.

24.4.4.2 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 Central Management Console (CMC) выберите элемент **Приложения**.
2. Дважды щелкните элемент **Конфигурация Crystal Reports**.
3. Выберите элемент **Параметры единого входа**.
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.

24.4.5 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.ocj.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

25.1 Ведение журнала трассировок компонентов

Журналы

Платформа BI создает сообщения системного уровня и записывает их в файлы журнала. Эти файлы могут использоваться системными администраторами для контроля производительности или отладки ошибок.

Трассировки

Платформа BI также создает трассировки (записи событий, которые происходят во время работы контролируемого компонента) и собирает их в файлах журнала с расширением `.glf`. Диапазон отслеживаемых событий - от сообщений о статусе до серьезных ошибок особых ситуаций. Сотрудники службы поддержки и разработчики SAP могут использовать трассировки для создания отчетов о производительности компонентов платформы BI (серверов и веб-приложений) и работе отслеживаемых компонентов.

При установке уровня журнала трассировки для компонента определяется тип и детальность информации, отправляемой в файл журнала. Уровень журнала трассировки является фильтром, который подавляет трассировки ниже указанного порога. Путем контроля журнала трассировки компонента можно определить, следует ли изменить текущий экземпляр компонента или его конфигурацию для работы при повышенной рабочей нагрузке.

Примечание:

Файлы журнала платформы BI можно просмотреть с использованием любого текстового редактора.

25.2 Уровни журнала трассировки

Для компонентов платформы BI доступны следующие уровни журнала трассировки:

Уровень	Описание
Не определен	Уровень журнала трассировки устанавливается с использованием другого способа, обычно через файл <code>.ini</code> .
Нет	Трассировка не происходит.
Нижняя	Фильтр журнала трассировки позволяет протоколировать сообщения об ошибках, игнорируя предупреждающие сообщения и сообщения о статусе. Протоколируются важные статусные сообщения, относящиеся к запуску компонента, к запросам на запуск, а также к запросам на окончание. Этот уровень не рекомендуется для целей отладки.
Средний	Фильтр журнала трассировки настроен на включение сообщений об ошибках, предупреждениях и большинства сообщений о статусе. Менее важные или слишком детальные статусные сообщения отфильтровываются. Этот уровень не достаточно детальный для использования в целях отладки.
Высокий	<p>Нет отфильтрованных сообщений. Этот уровень рекомендуется для использования в целях отладки.</p> <p>Предупреждение: Этот уровень трассировки оказывает значительное влияние на ресурсы системы, повышая нагрузку на процессор и занимая место на диске.</p>

25.3 Настройка трассировки для серверов

Сообщение журнала является постоянной записью событий и статуса системы ПО. Трассировки отслеживаемого развертывания платформы BI записываются в конкретный файл журнала `.glf` и сохраняются в каталоге записи в журнал.

- В Windows по умолчанию используется каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging`.
- В Unix по умолчанию используется каталог `<INSTALLDIR>/sap_bobj/logging`.

Имя файла журнала `.glf` включает краткий идентификатор, имя сервера и ссылку на номер, например: `aps_mysia.AdaptiveProcessingServer_trace.000012.glf`. Для отслеживаемого сервера создается новый файл журнала трассировки, как только размер файла журнала достигает порога в 10 мегабайт. Кроме того, одновременно осуществляется ведение пяти файлов журнала. После создания новых файлов журнала старые файлы журнала удаляются.

Можно калибровать серьезность и важность трассировок, собранных в файле журнала, путем задания уровня журнала трассировки для конкретных серверов или групп серверов.

Примечание:

Для изменения уровней журнала трассировки для конкретных серверов или групп серверов используется служба журнала трассировок в Central Management Console (CMC). Чтобы изменить

другие параметры, вручную измените уровень журнала трассировки и другие параметры в файле `BO_trace.ini`.

25.3.1 Настройка уровня журнала в СМС

Можно скорректировать уровень трассировки журнала для сервера, не влияя на другие параметры трассировки.

1. В области «Серверы» СМС получите доступ к серверу.
 - Выберите сервер в конкретной категории.
 - Щелкните **Список серверов** в навигационной панели, чтобы получить доступ к полному списку серверов, и выберите сервер.
2. Щелкните выбранный сервер правой кнопкой мыши и выберите команду **Свойства**.
Откроется диалоговое окно «Свойства».
3. В области «Служба журналов трассировки» выберите параметр в списке **Уровень журнала**.
4. Нажмите **Сохранить и закрыть**.

Новый уровень трассировки журнала вступит в силу немедленно.

Чтобы указать другой выходной каталог для файлов журнала, включите параметр `-loggingPath <целевой_каталог>` в область «Параметры командной строки». Перезапустите сервер, чтобы эта настройка вступила в силу.

См. также

- [Уровни журнала трассировки](#)

25.3.2 Установка уровня журнала для нескольких серверов в СМС

1. В области «Серверы» СМС получите доступ к нескольким серверам.
 - Выберите серверы в конкретной категории.
 - Щелкните **Список серверов** в навигационной панели, чтобы получить доступ к полному списку серверов. Нажимая и удерживая клавишу **Ctrl**, выделяйте серверы, чтобы их выбрать.
2. Щелкните правой кнопкой мыши выбранные серверы и выберите пункт **Изменить общие службы**.
Будет открыто диалоговое окно «Изменить общие службы».
3. В области «Служба журналов трассировки» выберите параметр в списке **Уровень журнала**.
4. Нажмите кнопку **ОК**.

Новый уровень трассировки журнала вступит в силу немедленно.

Чтобы указать другой выходной каталог для файлов журнала, включите параметр `-loggingPath <целевой_каталог>` в область «Параметры командной строки». Перезапустите сервер, чтобы эта настройка вступила в силу.

См. также

- [Уровни журнала трассировки](#)

25.3.3 Настройка серверной трассировки с использованием файла `BO_trace.ini`

В файле `BO_trace.ini` по умолчанию регистрируются только ошибки и утверждения.

1. Откройте файл `BO_trace.ini`.
 - В Windows по умолчанию используется каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`.
 - В Unix по умолчанию используется каталог `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`.
2. Удалите комментарии строк в разделе «Синтаксис и параметр трассировки».
3. Измените параметры серверной трассировки. Для настройки серверной трассировки используются следующие параметры:

Параметр	Возможные значения	Описание
sap_log_level	log_information, log_warning, log_error, log_fatal, log_none	<p>Определяет серьезность сообщений журнала. По умолчанию используется серьезность log_error.</p> <p>Серьезность для журнала определяется в иерархической последовательности: на самом высоком уровне log_information и на самом низком - log_none. При выборе уровня серьезности журнала будут отображаться все сообщения этого и нижестоящих уровней. Например, если задан уровень серьезности log_warning, в файл журнала будут записываться сообщения, которые включают log_warning, log_error и log_fatal.</p> <p>Примечание: log_information и log_warning можно сократить до log_info и log_warn.</p>
sap_trace_level	trace_debug, trace_path, trace_information, trace_error, trace_none	<p>Определяет серьезность сообщений трассировки. По умолчанию используется серьезность трассировки trace_error.</p> <p>Серьезность трассировки определяется в иерархической последовательности: на самом высоком уровне trace_debug и на самом низком - trace_none. При выборе уровня серьезности трассировки будут отображаться все сообщения этого и нижестоящих уровней. Например, если задана серьезность трассировки trace_path, в файл журнала будут записываться сообщения, которые включают trace_path, trace_information и trace_error.</p> <p>Примечание: trace_information можно сократить до trace_info.</p>

4. Сохраните и закройте файл BO_trace.ini.

Измененные параметры вступят в силу только после перезапуска всех серверов.

Примечание:

Считывание файла BO_trace.ini происходит часто. Изменения в файле BO_trace.ini вступают в силу в течение пяти минут после сохранения. В случае перезапуска CMS изменения в файле BO_trace.ini вступают в силу немедленно.

Пример:`BO_trace.ini`

```
sap_log_level=log_warning;  
sap_trace_level=trace_path;
```

25.3.3.1 Настройка трассировки для конкретного сервера

Файл `BO_trace.ini` определяет параметры 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.

Предупреждение:

Новые параметры уровня журнала трассировки, указанные в СМС для конкретного сервера, будут перезаписывать все параметры в `BO_trace.ini`.

1. Откройте файл `BO_trace.ini`.

- В Windows по умолчанию используется каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`.
- В Unix по умолчанию используется каталог `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`.

2. Используйте оператор `if`, чтобы указать параметры трассировки для конкретного сервера. Например:

```
if (process == "aps_MySIA.ProcessingServer") {  
    sap_log_level=log_warning;  
    sap_trace_level=trace_path;  
}
```

Совет:

Для параметра трассировки необходимо определить процесс, чтобы применить к конкретному серверу.

3. Сохраните и закройте файл `BO_trace.ini`.

Измененные параметры будут реализованы в течение пяти минут.

25.4 Настройка трассировки для веб-приложений

Трассировки для отслеживаемого развертывания платформы BI записываются в конкретный файл журнала `.glf` и сохраняются в каталоге на компьютере, где находится папка веб-приложений.

- В Windows по умолчанию используется каталог
C:\SBOPWebapp_<APPLICATION>_<IPADDRESS>_<PORT>\ Например,
C:\SBOPWebapp_BIlaunchpad_192.0.2.0_8080\
- В Unix по умолчанию используется каталог
\$userHome/SBOPWebapp_<APPLICATION>_<IPADDRESS>_<PORT>/ Например,
\$userHome/SBOPWebapp_CMC_192.0.2.0_8080/

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

Примечание:

Для изменения уровней журнала трассировки для конкретных серверов или групп серверов используется служба журнала трассировок в Central Management Console (CMC). Чтобы изменить другие параметры, вручную измените уровень журнала трассировки и другие параметры в файле `BO_trace.ini`. Этот файл развертывается вместе с файлами `BOE.war` и `dswebobje.war` на сервере веб-приложений.

Перед настройкой файла `BO_trace.ini` необходимо воспользоваться средством WDeploy, чтобы отменить развертывание существующих веб-приложений на сервере веб-приложений. После настройки файла `BO_trace.ini` его следует 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*.

25.4.1 Настройка уровня журнала трассировки веб-приложения в СМС

Для трассировки других веб-приложений следует вручную сконфигурировать соответствующий файл `BO_trace.ini`.

1. В поле «Приложения» консоли СМС щелкните приложение правой кнопкой мыши и выберите **Настройки журнала трассировки**.

Примечание:

Эти приложения имеют следующие параметры журнала трассировки: Стартовая панель BI, СМС, Open Document, Promotion Management, Управление версиями, Visual Difference, Веб-служба.

Будет открыто диалоговое окно «Настройки журнала трассировки».

2. Выберите параметр в раскрывающемся списке **Уровень журнала**.
3. Нажмите **Сохранить и закрыть**.

Новый уровень журнала трассировки вступит в силу после следующего входа в данное веб-приложение.

См. также

- [Уровни журнала трассировки](#)

25.4.2 Настройка параметров трассировки с использованием файла `BO_trace.ini`

Файл `BO_trace.ini` разворачивается с файлами `.warBOE` и `dswsbobje` на сервере веб-приложений. Файл `BO_trace.ini` можно использовать, чтобы указать параметры трассировки для веб-приложений платформы BI. Поскольку этот файл доступен не всегда, необходимо отменить разворачивание затронутого веб-приложения на сервере веб-приложений.

1. При помощи WDeploy отмените разворачивание веб-приложения с сервера веб-приложений. Для получения дополнительных сведений об использовании Wdeploy для отмены разворачивания веб-приложений см. *Руководство по разворачиванию веб-приложений SAP BusinessObjects Business Intelligence Platform*.
 - Если используется сервер веб-приложений Tomcat, предоставленный вместе с установкой платформы BI, отменять разворачивание веб-приложений не требуется. Возможно непосредственное изменение файлов.
 - Файл конфигурации трассировки для файла `BOE.war` доступен в каталоге `<INSTALLDIR>\Tomcat\webapps\BOE\WEB-INF\TraceLog`.
 - Файл конфигурации трассировки для файла `dswsbobje.war` доступен в каталоге `<INSTALLDIR>\Tomcat\webapps\dswsbobje\WEB-INF\conf`.

Примечание:

Если используется связанный сервер приложений Tomcat, пропустите шаг 2.

2. Получите доступ к предварительно развернутой версии файла `BO_trace.ini`:
 - По умолчанию для предварительно развернутой версии файла конфигурации для файла `BOE.war` используется каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`.
 - По умолчанию для предварительно развернутой версии файла конфигурации для файла `dswsbobje.war` используется каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`.
3. Откройте файл `BO_trace.ini`.
 - В Windows по умолчанию используется каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`.
 - В Unix по умолчанию используется каталог `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`.
4. Измените параметры серверной трассировки. Для настройки серверной трассировки используются следующие параметры:

Параметр	Возможные значения	Описание
sap_log_level	log_information log_warning log_error log_fatal log_none	<p>Определяет серьезность сообщений журнала. По умолчанию используется серьезность log_error.</p> <p>Серьезность для журнала определяется в иерархической последовательности: на самом высоком уровне log_information и на самом низком - log_none. При выборе уровня серьезности журнала будут отображаться все сообщения этого и нижестоящих уровней. Например, если задан уровень серьезности log_warning, в файл журнала будут записываться сообщения, которые включают log_warning, log_error и log_fatal.</p> <p>Примечание: log_information и log_warning можно сократить до log_info и log_warn.</p>
sap_trace_level	trace_debug trace_path trace_info trace_error trace_none	<p>Определяет серьезность сообщений трассировки. По умолчанию используется серьезность трассировки trace_error.</p> <p>Серьезность трассировки определяется в иерархической последовательности: на самом высоком уровне trace_debug и на самом низком - trace_none. При выборе уровня серьезности трассировки будут отображаться все сообщения этого и нижестоящих уровней. Например, если задана серьезность трассировки trace_path, в файл журнала будут записываться сообщения, которые включают trace_path, trace_info и trace_error.</p> <p>Примечание: trace_information можно сократить до trace_info.</p>

5. Сохраните и закройте файл `BO_trace.ini`.
6. При помощи WDeploy разверните файл `.war` на компьютере, где размещен сервер веб-приложений.

Измененные параметры трассировки вступят в силу после следующего входа в веб-приложение.

25.4.2.1 Настройка трассировки для конкретного веб-приложения

Файл `BO_trace.ini` развертывается вместе с файлами `.warBOE` и `dswsbobje` на сервере веб-приложений. Файл `BO_trace.ini` можно использовать, чтобы указать параметры трассировки для веб-приложений платформы BI. Поскольку этот файл доступен не всегда, необходимо отменить развертывание затронутого веб-приложения на сервере веб-приложений. Ниже перечислены 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	dswsbobje.war	<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\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*.

- Если используется сервер веб-приложений Tomcat, предоставленный вместе с установкой платформы BI, отменять развертывание веб-приложений не требуется. Доступно непосредственное изменение файла.
 - Файл конфигурации трассировки для файла `BOE.war` доступен в каталоге `<INSTALLDIR>\Tomcat\webapps\BOE\WEB-INF\TraceLog`.
 - Файл конфигурации трассировки для файла `dswsbobje.war` доступен в каталоге `<INSTALLDIR>\Tomcat\webapps\dswsbobje\WEB-INF\conf`.

Примечание:

Если используется связанный сервер приложений Tomcat, пропустите шаг 2.

2. Получите доступ к предварительно развернутой версии файла `BO_trace.ini`:

- По умолчанию для предварительно развернутой версии файла конфигурации для файла `BOE.war` используется каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`.
- По умолчанию для предварительно развернутой версии файла конфигурации для файла `dswsbobje.war` используется каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`.

3. Откройте файл `BO_trace.ini`.

- В Windows по умолчанию используется каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`.

- В Unix по умолчанию используется каталог
<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/.

4. Используйте оператор `if`, чтобы указать параметры трассировки для конкретного веб-приложения. Например:

```
if (device_name == "Webapp_opendocument_trace") {  
    sap_log_level=log_warning;  
    sap_trace_level=trace_path;  
}
```

Для параметра трассировки необходимо определить процесс, чтобы применить его к конкретному веб-приложению. После начальной установки доступны следующие веб-приложения:

Веб-приложение	Имя устройства
Стартовая панель BI	WebApp_BIlaunchpad
Центральный сервер управления	WebApp_CMC
OpenDocument	WebApp_OpenDocument

Для настройки трассировки сервера веб-приложений используются следующие параметры:

Параметр	Возможные значения	Описание
sap_log_level	log_information log_warning log_error log_fatal log_none	<p>Определяет серьезность сообщений журнала. По умолчанию используется серьезность log_error.</p> <p>Серьезность для журнала определяется в иерархической последовательности: на самом высоком уровне log_information и на самом низком - log_none. При выборе уровня серьезности журнала будут отображаться все сообщения этого и нижестоящих уровней. Например, если задан уровень серьезности log_warning, в файл журнала будут записываться сообщения, которые включают log_warning, log_error и log_fatal.</p> <p>Примечание: log_information и log_warning можно сократить до log_info и log_warn.</p>
sap_trace_level	trace_debug trace_path trace_info trace_error trace_none	<p>Определяет серьезность сообщений трассировки. По умолчанию используется серьезность трассировки trace_error.</p> <p>Серьезность трассировки определяется в иерархической последовательности: на самом высоком уровне trace_debug и на самом низком - trace_none. При выборе уровня серьезности трассировки будут отображаться все сообщения этого и нижестоящих уровней. Например, если задана серьезность трассировки trace_path, в файл журнала будут записываться сообщения, которые включают trace_path, trace_info и trace_error.</p> <p>Примечание: trace_information можно сократить до trace_info.</p>

5. Сохраните и закройте файл BO_trace.ini.
6. При помощи WDeploy разверните файл .war на компьютере, где размещен сервер веб-приложений.

25.5 Настройка трассировки для средства управления обновлением

Трассировку конфигурации для средства управления обновлением невозможно выполнить с использованием СМС. Трассировку для средства управления обновлением необходимо выполнить с помощью файла `BO_trace.ini`.

- В Windows по умолчанию используется каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`.
- В Unix по умолчанию используется каталог `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`.

25.5.1 Настройка трассировки для средства управления обновлениями

1. Откройте файл `BO_trace.ini`.
 - В Windows по умолчанию используется каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`.
 - В Unix по умолчанию используется каталог `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`.
2. Удалите комментарии обязательных строк в разделе «Синтаксис и параметр трассировки».
3. Для определения параметров трассировки используйте оператор `if`. Например:

```
if (process == "upgrademanagementtool") {
    sap_log_level=log_warning;
    sap_trace_level=trace_path;
}
```

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 реализованы в течение пяти минут.

25.6 Настройка трассировки для клиентских приложений платформы BI

Трассировку можно активировать для следующих клиентов:

- Средство создания универсов
- Средство дизайна информации
- Web Intelligence Rich Client

Трассировку этих компонентов можно настроить редактированием INI-файлов для каждого типа клиента. Эти INI-файлы функционируют так же, как файл `BO_trace.ini`, описанный в других разделах этой главы. Подробные сведения об изменении INI-файла см. в разделе [Настройка серверной трассировки с использованием файла BO_trace.ini](#).

Файлы должны находиться в рабочих каталогах, настроенных для этих приложений (по умолчанию <INSTALLDIR>\SAP BusinessObjects). Если они еще не существуют, необходимо создать их. Эти файлы имеют следующие имена:

- Средство создания юниверсов: `designer_trace.ini`.
- Средство разработки информации: `BO_Trace.ini`
- Web Intelligence Rich Client: `WebIRichClient_trace.ini`

Для получения дополнительных сведений см. документацию по этим продуктам.

Интеграция с SAP Solution Manager

26.1 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>

26.2 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. (Необязательно) Для регистрации SLD на сервере Apache Tomcat требуется установка SLDREG на каждом сервере Tomcat. Дополнительные сведения см. в SAP-ноте 1508421.
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.

Поддержка в SAP Solution Manager	Требуется для платформы BI
SAP Passport	<ul style="list-style-type: none"> Необходимо загрузить и установить средство клиента SAP Passport.

26.3 Управление регистрацией System Landscape Directory

26.3.1 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 SLD 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*.

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.

26.3.1.1 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.

26.3.2 Точки запуска SLD

Процесс регистрации в SLD инициируется поставщиком данных, создающим отчетность по обслуживаемым 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. Чтобы обновить SLD-сервер, когда удаляется сервер или узел, удалите систему из SLD и повторите ее отправку, перезапустив платформу BI.

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.

26.3.3 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.

26.4 Управление агентами Solution Management Diagnostics

26.4.1 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.

26.4.2 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 Central Management Console (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 SAdmin.

26.4.3 Учетная запись пользователя SAdmin

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 SMAAdmin по умолчанию неактивна.

26.4.3.1 Активация учетной записи пользователя SMAAdmin

1. В области управления СМС «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**.

26.5 Инструментальные средства управления производительностью

26.5.1 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.

26.5.2 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.
2. После установки платформы SAP BusinessObjects Business Intelligence можно предоставить данные конфигурации для SMD-агента при помощи заполнителей в свойствах узла в Central Management Console (CMC).

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](#)

26.5.2.1 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.

1. Перейдите в область «Серверы» консоли CMC.
2. В области навигации щелкните **Узлы**.
Будут отображены все доступные узлы.
3. Щелкните правой кнопкой мыши узел, на котором нужно выполнить настройку конфигурации, и выберите команду **Заполните**.
Отобразится диалоговое окно "Заполнители".
4. Измените значения для следующих заполнителей.

Заполнитель	Описание
%IntroscopeAgentEnableInstrumentation%	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.
%IntroscopeAgentEnterpriseManagerHost%	Имя хоста для компьютера, на котором установлено приложение Enterprise Manager.
%IntroscopeAgentEnterpriseManagerPort%	Порт прослушивания, используемый Enterprise Manager.
%IntroscopeAgentEnterpriseManagerTransport%	Протокол обмена данными, используемый Enterprise Manager. К поддерживаемым протоколам относятся TCP, SSL, HTTP Tunnel и HTTPS.
%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.

26.5.3 Настройка конфигурации производительности для веб-уровня

Данные инструментов мониторинга для компонентов веб-уровня не включены в платформу BI.

26.5.4 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: <INSTALLDIR>/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: <INSTALLDIR>/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: <INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/wily/webapp/logs. В этой папке доступно два типа файлов журнала: Introscope.log и Autoprobe.log.

26.6 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 CMC и файле конфигурации BO_trace.ini, используются в том случае, если они выше уровней, заданных в клиентском инструменте SAP Passport – SAPClientPlugin.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

27.1 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.

27.1.1 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.

27.1.1.1 ccm.sh

Скрипт `ccm.sh` устанавливается в каталог `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj` установки. 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></i> [другая информация для аутентификации]	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 <code>-password</code> вы должны также указать аргумент <code>-username</code> .

ССМ прочитывает строки запуска и другие значения конфигурации из файла `ccm.config`.

См. также

- [ccm.config](#)

27.1.1.1.1 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. CCM активирует все сервера в кластере, в на которых CMS выполняется на компьютере MACHINE01 и доступен через порт 6701:

```
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 указанной административной учетной записи SysAdmin и заданного пароля:

```
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 для отключения адаптивного сервера заданий, запущенного на втором компьютере:

```
ccm.sh -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

27.1.1.1.2 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 вы обычно редактируете только этот файл. Настоятельно рекомендуется перед редактированием этого файла вручную создать его резервную копию.

См. также

- [Обзор командных строк](#)

27.1.1.2 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 предлагает ввести имя агента Server Intelligence Agent (SIA). Для проверки имени агента SIA просмотрите его свойство команды в файле `ccm.config`. Текущее имя агента SIA отображается после параметра `-name`. Также можно воспользоваться параметром 8 в файле `serverconfig.sh`.

См. также

- [Кластеризация центральных серверов управления \(CMS\)](#)
- [Обзор резервного копирования и восстановления](#)

27.1.1.3 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
- Изменение конфигурации веб-уровня
- Перечисление всех узлов

27.1.1.3.1 Для добавления, удаления, изменения или перечисления узлов в UNIX

1. Перейдите в каталог `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj` установки.
2. Вызовите следующую команду:

```
./serverconfig.sh
```

Скрипт предлагает список вариантов:

- a. Добавить узел
- b. Удалить узел
- c. Изменить узел
- d. Переместить узел

- e. Резервное копирование конфигурации сервера
 - f. Восстановление конфигурации сервера
 - g. Изменение конфигурации веб-уровня
 - h. Перечисление всех узлов
3. Введите число, соответствующее действию, которое вы хотите выполнить.
 4. Если выполняется добавление, удаление или изменение сервера, предоставьте скрипту дополнительные запрашиваемые сведения.

27.1.2 Шаблоны скриптов

27.1.2.1 startservers

Скрипт `startservers` устанавливается в каталог `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj` установки. 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.

27.1.2.2 stopservers

Скрипт `stopservers` устанавливается в каталог `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj` установки. 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.

27.1.3 Скрипты, используемые платформой BI

Эти дополнительные скрипты часто запускаются в фоновом режиме при использовании главных утилит скриптов платформы BI, так что запускать их самостоятельно нет необходимости.

bobjrestart.sh

Этот скрипт запускается внутренними средствами CCM для управления узлами Server Intelligence Agent. Не запускайте этот скрипт самостоятельно.

env.sh

Скрипт `env.sh` устанавливается в каталог установки `sap_bobj/setup`. Этот скрипт устанавливает переменные среды платформы BI, которые необходимы некоторым другим скриптам. `env.sh` запускается при необходимости скриптами платформы BI. Для получения дополнительных сведений см. *Руководство по установке платформы SAP BusinessObjects Business Intelligence*.

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.

initlaunch.sh

Скрипт `initlaunch.sh` запускает скрипт `env.sh` для установки переменных среды платформы BI, а затем запускает любую команду, добавленную к этому скрипту в форме аргумента командной строки. Этот скрипт предназначен в первую очередь для использования SAP Business Objects в качестве средства отладки.

postinstall.sh

Скрипт `postinstall.sh` устанавливается в каталог установки `<SCRIPTDIR>`. Запускать его самостоятельно не следует.

setup.sh

Скрипт `setup.sh` устанавливается в корневой каталог установки. Этот скрипт содержит программу с текстовым интерфейсом, которая позволяет настроить установку платформы BI. Он запускается автоматически при установке платформы BI. Скрипт предлагает ввести информацию, необходимую для первой установки платформы BI.

Для получения дополнительных сведений об ответах на вопросы скрипта установки при установке установке платформы BI см. *Руководство по установке платформы SAP BusinessObjects Business Intelligence*.

setupinit.sh

Скрипт `setupinit.sh` устанавливается в каталог установки `sap_bobj/init`. Этот скрипт копирует скрипты управления выполнением в каталоги `rc#` для автоматического запуска. Если требуется, чтобы серверы платформы BI запускались и останавливались одновременно с компьютером, на котором они установлены, запустите этот скрипт после завершения работы скрипта `setup.sh`.

Примечание:

Для запуска этого скрипта необходимы привилегии суперпользователя (root).

27.2 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.

27.2.1 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
<code>-help</code>	недоступно	Отображает справку по командной строке.
<code>-managedstart</code>	<code>all</code> или <code><полное имя сервера></code> [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`.

27.2.1.1 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 (NODENAME)"
```

SIA можно также остановить при помощи команды `net stop "Server Intelligence Agent (ИМЯ_УЗЛА)"`.

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
```

27.3 Командные строки сервера

27.3.1 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 СМС 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 СМС. 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.

27.3.1.1 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.

27.3.2 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>	<code>port</code>	<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>

Параметр	Допустимые аргументы	Поведение
-loggingPath	<i>абсолютный путь</i>	Укажите путь, в котором будут создаваться файлы журнала.

27.3.2.1 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).

27.3.3 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
-threads	<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.

Параметр	Допустимые аргументы	Поведение
<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> .
<code>-receiverPool</code>	<i>number</i>	Задаёт количество потоков, создаваемых CMS для получения запросов клиентов. Клиентом может быть другой сервер Business Objects, Мастер публикации отчетов, 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.

Параметр	Допустимые аргументы	Поведение
<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 объемов базы данных. В большинстве случаев максимально допустимым значением является 20.
<code>-oobthreads</code>	<i>number</i>	Если в кластере находится более восьми участников 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.

См. также

- [Стандартные параметры для всех серверов](#)

27.3.4 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](#)

27.3.5 Сервер обработки и кэш-сервер Dashboards

Управление сервером обработки и кэш-сервером Dashboards 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\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](#)

27.3.6 Серверы заданий

В этом разделе содержатся сведения о параметрах командной строки для адаптивных серверов заданий.

Путь по умолчанию к серверу в ОС Windows – `<INSTALLEDIR>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\JobServer.exe`.

Путь по умолчанию к серверу в ОС UNIX -
`<INSTALLEDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/boe_jobsd`.

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](#)

27.3.7 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.

27.3.8 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>	<code>mask</code>	<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](#)

27.3.9 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
<code>-ConnectionTimeout</code> Минуты	<i>minutes</i>	Определяет количество минут, по истечении которых сервер переходит в режим ожидания.
<code>-MaxConnections</code>	<i>number</i>	Определяет максимальное количество одновременных соединений, разрешенных сервером.
<code>-DocExpressEnable</code>		Активирует кэширование документов Web Intelligence при их просмотре.
<code>-DocExpressRealTime CachingEnable</code>		Активирует кэширование документов Web Intelligence в режиме реального времени.
<code>-DocExpressCache DurationMinutes</code>	<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](#)

27.3.10 Серверы репозитория входящих и исходящих файлов

В этом разделе содержится информация об особых параметрах командной строки, относящимся только к серверу репозитория входящих файлов.

Путь по умолчанию к серверам в ОС Windows – `<INSTALLDIR>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\fileserver.exe`.

Путь по умолчанию к программе, предоставляющей оба сервера в ОС UNIX - `<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_filesd`. По умолчанию Server Intelligence Agent будет запускать один экземпляр `boe_filesd` для сервера репозитория входных файлов и другой экземпляр для сервера репозитория выходных файлов.

Параметр	Допустимые аргументы	Поведение
<code>-rootDir</code>	<i>absolutePath</i>	<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>	<p>Определяет количество минут, по истечении которого выполняется очистка бездействующего сеанса.</p>

См. также

- [Стандартные параметры для всех серверов](#)

27.3.11 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/<platform>/boe_eventsd`.

Параметр	Допустимые аргументы	Процедура
<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 пять минут.

См. также

- [Стандартные параметры для всех серверов](#)

Repository Diagnostic Tool

28.1 Обзор инструмента Repository Diagnostic Tool

Инструмент Repository Diagnostic Tool (RDT) — это инструмент командной строки, который производит сканирование, диагностику и устраняет возможные несоответствия между системной базой данных центрального сервера управления (CMS) и файловым хранилищем серверов репозитория файлов (FRS), а также несоответствия в метаданных объектов InfoObject, хранимых в базе данных CMS.

При нормальной работе несоответствия в системной базе данных CMS возникать не должны. Однако несоответствия могут возникнуть во время неожиданных событий, например восстановления в аварийных ситуациях, резервного восстановления или в случае перебоев в работе сети. При возникновении этих событий выполнение задачи в базе данных системы CMS может быть прервано. Это может привести к возникновению несоответствий объектов в системной базе данных CMS.

Repository Diagnostic Tool сканирует системную базу данных CMS на наличие несоответствий в таких объектах, как отчеты, пользователи, группы пользователей, папки, серверы, юниверсы, соединения юниверсов и в других объектах.

Repository Diagnostic Tool определяет два типа несоответствий.

- Несоответствия между объектами и файлами.

Это несоответствия между объектами InfoObjects в базе данных CMS и соответствующими файлами в репозиториях файлов. Например, для файла, хранящегося в FRS, может отсутствовать соответствующий объект в системной базе данных CMS.

- Несоответствия метаданных InfoObject.

Это несоответствия, которые могут существовать в определении объекта InfoObject (метаданных) в базе данных CMS. Например, объект InfoObject может ссылаться на несуществующий в базе данных CMS объект InfoObject.

Repository Diagnostic Tool выполняет две функции, в зависимости от заданных при запуске инструмента параметров:

- Он сканирует системную базу данных CMS и файловое хранилище FRS, выдает отчет о несоответствиях и файл журнала в формате XML, выполняя указанные действия по устранению несоответствий.
- Он сканирует и устраняет несоответствия, обнаруженные в системной базе данных CMS и FRS, а также сообщает о предпринятых действиях в XML-файле журнала.

28.2 Использование Repository Diagnostic Tool

Repository Diagnostic Tool (RDT) доступен на любом компьютере, на котором установлен диспетчер ССМ. Этот инструмент командной строки просматривает, диагностирует и исправляет несоответствия, которые могут возникнуть между системной базой данных центрального сервера управления (CMS) и хранилищем файлов сервера репозитория файлов (FRS), а также возможные несоответствия в метаданных объектов InfoObject.

Рекомендуется выполнить резервное копирование базы данных CMS и хранилища файлов FRS, а затем запустить средство RDT в резервной копии, пока все службы платформы SAP BusinessObjects Business Intelligence остановлены. Если это невозможно, средство RDT можно запускать в активной базе данных.

Если требуется запустить средство RDT в активной базе данных, учитывайте следующие соображения.

- При работе средства RDT используется одно соединение с базой данных.
- Средство RDT проверяет целостность базы данных на момент своего запуска. Любые несогласованности, возникшие уже после запуска средства RDT, не заносятся в журнал и не исправляются.
- Для обработки транзакций RDT на компьютере, на котором выполняется это средство, рекомендуется установить объем памяти, превышающий стандартные требования к системе:
 - Для обработки базы данных, содержащей до 50 000 объектов InfoObject, требуется дополнительно 350 МБ свободной памяти
 - Для обработки базы данных, содержащей от 50 000 до 400 000 объектов InfoObject, требуется дополнительно 1,7 ГБ свободной памяти
 - Для обработки базы данных, содержащей от 400 000 до 1 000 000 объектов InfoObject, требуется дополнительно 4 ГБ свободной памяти
- Средство RDT не обязательно запускать с сервера CMS. Запустив его с отдельного компьютера, можно уменьшить падение производительности системы.
- Во время работы это средство оказывает умеренное влияние на производительность базы данных.

Для работы средства RDT не требуется запускать службу CMS, поскольку оно обращается напрямую к базе данных CMS.

28.2.1 Использование Repository Diagnostic Tool

1. Если инструмент запущен в системе Windows, откройте окно командной строки и выполните следующую команду.

`<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\reposcan.exe<arguments>`, где `<arguments>` – это список параметров, которые необходимо задать.

2. Если инструмент запущен в системе UNIX, откройте совместимую оболочку `/usr/bin/sh` и выполните следующую команду.

`./<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_reposcan.sh <arguments>`, где `<platform>` – это «linux_x64», «solaris_sparcv9», «hpux_ia64» или «aix_rs6000_64», а `<arguments>` – это список параметров, которые необходимо задать.

Repository Diagnostic Tool сканирует репозиторий на наличие несоответствий. В зависимости от указанных параметров инструмент либо диагностирует несоответствия и записывает их в журнал, либо исправляет несоответствия и записывает в журнал предпринятые действия.

`Repo_Scan_YYYY_MM_DD_HH_MM_SS.xml` – список всех найденных инструментом несоответствий. Если инструмент исправляет найденные различия, он также создает файл `Repo_Repair_YYYY_MM_DD_HH_MM_SS.xml`. В этом файле содержатся сведения об исправленных объектах и удаленных файлах с утраченными связями. Также здесь приводятся любые обнаруженные несогласованности, которые не удалось исправить.

Путь к файлам журналов можно также указать в параметре `outputdir`. Если параметр не указан, по умолчанию для файлов журналов используется каталог `<INSTALLDIR>\BusinessObjects Enterprise XI 4.0\reposcan` в системе Windows и `./sap_bobj/enterprise_xi40/reposcan` в системе Unix.

Примечание:

В приложении также предоставлен файл XSL по умолчанию, который наряду с файлом XML используется для создания страницы HTML. Файл XSL сохраняется в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\reposcan` в системе Windows и в каталоге `./sap_bobj/enterprisexi_40/reposcan` в системе Unix.

Список предупреждающих сообщений и рекомендуемых действий, предпринимаемых инструментом RDT при обнаружении несоответствий, можно просмотреть в разделах *Противоречия в метаданных CMS* и *Противоречия CMS и FRS*.

См. также

- [Несоответствия в метаданных CMS](#)
- [Несоответствия между CMS и FRS](#)

28.2.2 Параметры Repository Diagnostic Tool

Repository Diagnostic Tool принимает параметры, указанные в следующей таблице:

Примечание:

Аргументы командной строки переопределяют любые записи файла параметров при выполнении.

Таблица 28-1: Общие параметры

Параметр	Дополнительный или обязательный	Описание
dbdriver	Обязательный	<p>Тип драйвера, используемого для подключения к базе данных CMS. Допустимы следующие значения:</p> <ul style="list-style-type: none"> • db2databasesubsystem • maxdbdatabasesubsystem • mysqldatabasesubsystem • oracledatabasesubsystem • sqlserverdatabasesubsystem • sybasedatabasesubsystem • sqlanywheredatabasesubsystem
connect	Обязательный	<p>Сведения о соединении, которые используются для подключения к базе данных CMS.</p> <p>Например: <code>-connect "UID=root;PWD=<пароль>;DSN=<dsn>;HOSTNAME=<имя_хоста>;PORT=<номер_порта>"</code></p>

Параметр	Дополнительный или обязательный	Описание
dbkey	Принудительный	<p>Введите ключ кластера для развертывания платформы BI.</p> <p>Если ключ кластера неизвестен, его можно сбросить, выполнив следующие операции:</p> <p>Примечание:</p> <p>Если компьютер принадлежит кластеру, то указанные шаги должны быть выполнены для каждого члена кластера. Перед продолжением создайте резервную копию базы данных CMS и файлового хранилища.</p> <ol style="list-style-type: none"> 1. Запустите Central Configuration Manager (CCM). 2. В CCM щелкните правой кнопкой мыши Server Intelligence Agent (SIA) и выберите команду Остановить. Не переходите к шагу 3, пока статус агента SIA не сменится на «Остановлен». 3. Щелкните SIA правой кнопкой мыши и выберите команду Свойства. 4. На панели конфигурации нажмите кнопку Изменить в разделе «Конфигурация ключа кластера CMS». 5. Появится сообщение с предупреждением. Нажмите кнопку "Да" для продолжения. 6. В диалоговом окне «Изменение ключа кластера» введите одинаковое значение ключа из восьми символов в полях «Новый ключ кластера» и «Подтвердите новый ключ кластера». <p>Примечание:</p> <ul style="list-style-type: none"> • Средство RDT не будет запущено, если не указать параметр dbkey, или если указан неверный ключ кластера. • Ключ кластера отображается в CCM в зашифрованном виде и он не может использоваться в качестве параметра dbkey. <p>Для получения подробных сведений о ключах кластера см. «Безопасность платформы BI» в <i>Руководстве администратора платформы SAP BusinessObjects Business Intelligence</i>.</p>

Параметр	Дополнительный или обязательный	Описание
inputfrsdir	Обязательный	<p>Путь к файлу сервера репозитория входящих файлов.</p> <p>Примечание: Для выполнения инструмента командной строки используется учетная запись пользователя, под которой выполнен вход в систему. Учетная запись должна иметь права полного контроля для местоположения файла.</p>
outputfrsdir	Обязательный	<p>Путь к файлу сервера репозитория исходящих файлов.</p> <p>Примечание: Для выполнения инструмента командной строки используется учетная запись пользователя, под которой выполнен вход в систему. Учетная запись должна иметь права полного контроля для местоположения файла.</p>
outputdir	Дополнительный	<p>Путь к файлу, в который Repository Diagnostic Tool записывает файлы журнала.</p> <p>По умолчанию используется значение <code><INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\reposcan</code> в системе Windows и <code>./sap_bobj/enterprise_xi40/reposcan</code> в системе Unix.</p>
count	Дополнительно	<p>Количество примерных ошибок для сканирования. Это помогает обеспечить оптимальную производительность. Верхним пределом является $2e31 - 1$. Значение 0 интерпретируется как весь репозиторий.</p> <p>По умолчанию это значение равно 0.</p>

Параметр	Дополнительный или обязательный	Описание
repair	Дополнительно	<p>Предписывает Repository Diagnostic Tool устранить любые обнаруженные несоответствия. Поведением по умолчанию является лишь создание отчета о несоответствиях, без выполнения каких-либо исправлений. Если в командной строке указан параметр -repair, RDT сообщает о всех несоответствиях и исправляет их.</p> <p>Предупреждение: В рамках этого процесса из базы данных репозитория удаляются любые объекты или файлы с утраченными связями.</p>
scanfrs	Дополнительно	<p>Указывает на то, следует ли Repository Diagnostic Tool выполнять сканирование CMS и FRS на наличие несоответствий. Допустимыми значениями являются True и False.</p> <p>Значением по умолчанию является True.</p>
scancms	Дополнительно	<p>Указывает на то, следует ли Repository Diagnostic Tool выполнять сканирование CMS на наличие несоответствий между объектами InfoObjects. Допустимыми значениями являются True и False.</p> <p>Значением по умолчанию является True.</p>
submitterid	Дополнительно	<p>Указывает идентификатор пользователя для замены отсутствующих или недействительных идентификаторов для запланированных объектов. Если значение не указано, Repository Diagnostic Tool не заменяет недействительный идентификатор. Если указанный идентификатор пользователя не существует в CMS, Repository Diagnostic Tool запрашивает действительный идентификатор.</p> <p>Этот параметр используется только при работе Repository Diagnostic Tool в режиме исправления.</p>

Параметр	Дополнительный или обязательный	Описание
startid	Дополнительно	<p>Указывает на объект базы данных CMS, с которого следует начать сканирование. Например, если уже просканированы первые 500 объектов в репозитории, можно установить значение -startid=501, чтобы начать новое сканирование с 501-го объекта.</p> <p>Значением по умолчанию является 1.</p>
optionsfile	Дополнительно	<p>Указывает путь к файлу параметров. Файл параметров является текстовым файлом, в котором перечислены параметры командной строки и их значения. В этом файле каждый параметр должен находиться на отдельной строке.</p> <p>Примечание: Используя данную опцию можно задать все параметры в текстовом файле, как описано выше. Используйте данный параметр для указания на файл параметров, не вводя параметры в командную строку.</p>
syscopy	Дополнительно	<p>Данный параметр используется при копировании базы данных репозитория. Необходимо запустить средство для созданной копии, чтобы обновить ее в целях предотвращения кластеризации исходными системными серверами. Это делать не обязательно, если копия не сможет связываться с исходной системой. Это может быть использовано только с базовыми параметрами и не должно объединяться с другими дополнительными параметрами в данном списке.</p> <p>Примечание: Не запускайте средство Repository Diagnostic Tool с параметром syscopy для исходной системы.</p>

Следующие параметры используются, если в активном кластеризованном CMS выполняется средство Repository Diagnostic Tool.

Таблица 28-2: Использование Repository Diagnostic Tool в кластеризованной системе CMS

Параметр	Дополнительный или обязательный	Описание
requestport	Дополнительно	Номер порта, который использует Repository Diagnostic Tool для связи с CMS. Принимает целые положительные числа. По умолчанию инструмент использует значение, установленное в операционной системе машины, на которой выполняется Repository Diagnostic Tool.
numericip	Дополнительно	Использует ли Repository Diagnostic Tool числовой IP-адрес вместо имени хоста для связи между CMS и компьютером, на котором выполняется этот инструмент. Допустимыми значениями являются True и False. Значением по умолчанию является False.
ipv6	Дополнительно	ipv6-имя машины, на которой выполняется Repository Diagnostic Tool. Принимает строковое значение. Значением по умолчанию является имя хоста машины, на которой выполняется Repository Diagnostic Tool.
port	Дополнительно	ipv4-имя машины, на которой выполняется инструмент диагностики репозитория. Принимает строковое значение. Значением по умолчанию является имя хоста машины, на которой выполняется Repository Diagnostic Tool.
threads	Дополнительно	Количество потоков, которое нужно использовать. Принимает целые положительные числа. Значением по умолчанию является 12.

Когда Repository Diagnostic Tool использует SSL для связи со сканируемой базой данных CMS, применяются следующие параметры.

Таблица 28-3: Использование Repository Diagnostic Tool с SSL

Параметр	Дополнительный или обязательный	Описание
protocol	Дополнительно	Указывает, должен ли инструмент работать в режиме SSL. Единственным допустимым значением является ssl.
ssl_certdir	Дополнительно	Каталог, содержащий сертификаты SSL.
ssl_trustedcertificate	Дополнительно	Имя файла сертификата.
ssl_mycertificate	Дополнительно	Имя подписанного сертификата.
ssl_mykey	Дополнительно	Имя файла, содержащего частный ключ SSL.
ssl_mykey_passphrase	Дополнительно	Имя файла, содержащего идентификационную фразу SSL.

Пример:

Ниже приведен пример сканирования CMS и FRS на наличие обоих видов несоответствий и исправления обнаруженных несоответствий.

```

reposcan.exe
-dbdriver mysqldatabasesubsystem
-connect «UID=root;PWD=Password1;DSN=myDsn;HOSTNAME=myHostname;PORT=3306»
-inputfrsdir«C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\FileStore\Input»
-outputfrsdir «C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\FileStore\Output»
-dbkey <cluster key>
-repair

```

28.3 Несоответствия между CMS и FRS

В следующей таблице приведены несоответствия, которые могут возникнуть между базой данных центрального сервера управления (CMS) и серверами репозитория файлов (FRS) и которые распознаются инструментом Repository Diagnostic Tool. Таблица состоит из 4 столбцов:

- Предупреждающее сообщение

Предупреждающее сообщение, записываемое в файлы журнала сканирования и исправлений.

- Несоответствие

Описание несоответствия, обнаруженного инструментом диагностики репозитория по отношению к объекту.

- Рекомендация

Действие, рекомендуемое средством Repository Diagnostic Tool при обнаружении несоответствия. Это действие обозначено в файле журнала сканирования.

- Действие

Действие Repository Diagnostic Tool по исправлению несоответствия. Это действие обозначено в файле журнала исправлений.

Предупреждающее сообщение	Несоответствие	Рекомендация	Действие
Объект <Имя объекта><Тип объекта> (идентификатор объекта = <ID>) ссылается на несуществующие в FRS файлы (<Имя файла>)	Объект существует в базе данных CMS, но в FRS соответствующий файл отсутствует.	Разрешить приложению удалить объект. Также будут удалены все потомки этого объекта.	Объект удален из репозитория.
Файл <Имя файла> существует на сервере FRS входящих или исходящих файлов, но в репозитории отсутствует соответствующий объект InfoObject.	Файл существует на сервере FRS, но соответствующий файл отсутствует в базе данных CMS.	Разрешить приложению удалить файл, на который отсутствуют ссылки.	Действия не предпринимаются.
Объект <Тип объекта><Имя объекта> (Идентификатор объекта = <ID>) содержит файл <File Name>. Размер хранимого файла (<Размер> байт) не совпадает с фактическим размером файла <Размер>.	Размер файла не совпадает с размером файла объекта InfoObject.	Разрешить приложению обновить объект, указав правильный размер файла.	Объект обновлен, указан правильный размер файла.
Этот каталог не содержит файлов.	Папка FRS пуста.	Разрешить приложению удалить каталог.	Пустая папка удалена.

28.4 Несоответствия в метаданных CMS

В следующей таблице приведены распознаваемые Repository Diagnostic Tool несоответствия, которые могут возникнуть в метаданных объектов, размещенных в системной базе данных центрального сервера управления (CMS). Таблица состоит из 4 столбцов:

- Предупреждающее сообщение

Предупреждающее сообщение, записываемое в файлы журнала сканирования и исправлений.

- Несоответствие

Описание несоответствия, обнаруженного инструментом диагностики репозитория по отношению к объекту.

- Рекомендация

Действие, рекомендуемое средством Repository Diagnostic Tool при обнаружении несоответствия. Это действие обозначено в файле журнала сканирования.

- Действие

Действие Repository Diagnostic Tool по исправлению несоответствия. Это действие обозначено в файле журнала исправлений.

Предупреждающее сообщение	Несоответствие	Рекомендация	Действие
<Тип объекта> Для объекта <Имя объекта> (Идентификатор объекта: <ID>) отсутствует родительский объект (Идентификатор родительского объекта = <ID>).	У объекта отсутствует идентификатор родительского объекта, или идентификатор недействителен.	Разрешить приложению переместить объект в папку "BOE Repair".	Объект и его дочерние объекты перемещены в папку "BOE Repair".
<Object Type> Для объекта <Object Name> (идентификатор объекта: <ID>) отсутствует объект-владелец (идентификатор объекта-владельца = <ID>).	Для объекта отсутствует идентификатор объекта-владельца или идентификатор недействителен.	Разрешить приложению назначить объект администратору.	Объект назначен администратору.
<Object Type> Для объекта <Object Name> (идентификатор объекта: <ID>) отсутствует объект-предъявитель (идентификатор объекта-предъявителя = <ID>).	Для объекта отсутствует идентификатор объекта-предъявителя или идентификатор недействителен.	<p>Рекомендация, отображаемая Repository Diagnostic Tool, зависит от того, заданы ли значения для параметра -submitterid.</p> <ul style="list-style-type: none"> Если значение задано, рекомендация звучит как «Разрешить приложению обновить объект с учетом предоставленного идентификатора предъявителя». Если значение для параметра не задано, выдается рекомендация «Повторно запланируйте объект или воспользуйтесь ключом командной строки -submitterid для замены недействительного идентификатора предъявителя». 	<p>Если значение параметра -submitterid указано, Repository Diagnostic Tool использует это значение в качестве идентификатора предъявителя объекта.</p> <p>Если значение параметра не указано, Repository Diagnostic Tool не выполняет никаких действий. При перепланировании объекта CMS использует новый идентификатор.</p>

Предупреждающее сообщение	Несоответствие	Рекомендация	Действие
<Тип объекта>Свойство последнего успешного экземпляра объекта "<Имя объекта>" (идентификатор объекта = <ID>) ссылается на отсутствующий объект (идентификатор последнего успешного экземпляра объекта = <ID>).	Последний успешный экземпляр объекта отсутствует или недействителен.	Разрешить приложению повторно вычислить свойство.	Свойство вычислено повторно.
<Тип объекта> Для объекта "<Имя объекта>" (идентификатор объекта = <ID>) отсутствует объект-календарь (идентификатор объекта календаря = <ID>).	Объект ссылается на несуществующий календарь.	Перезапланировать объект с использованием существующего календаря. Приложение не может выполнить какие-либо действия.	Действия не предпринимаются.
<Тип объекта> Для объекта "<Имя объекта>" (идентификатор объекта = <ID>) отсутствует требуемая группа серверов планирования (идентификатор объекта группы серверов = <ID>).	Указанный сервер не существует.	Перезапланировать объект и выбрать существующую группу серверов. Приложение не может выполнить какие-либо действия.	Действия не предпринимаются.
<Тип объекта> Список ожидающих событий объекта "<Имя объекта>" (идентификатор объекта = <ID>) содержит отсутствующие объекты (идентификаторы объектов = <ID>).	Одно или несколько ожидаемых объектом событий не существуют.	Перезапланируйте объект, чтобы он ожидал существующих объектов событий. Приложение не может выполнить какие-либо действия.	Действия не предпринимаются.

Предупреждающее сообщение	Несоответствие	Рекомендация	Действие
<Тип объекта> Список инициируемых событий объекта "<Имя объекта>" (идентификатор объекта = <ID>) содержит отсутствующие объекты (идентификаторы объектов = <ID>).	Объект инициирует несуществующее событие.	Разрешить приложению удалить отсутствующие события из списка инициируемых событий.	Отсутствующие события удалены из списка инициируемых событий приложения.
<Тип объекта> Список контроля доступа объекта "<Имя объекта>" (идентификатор объекта = <ID>) ссылается на отсутствующего принципала (идентификатор объекта = <ID>).	Для записи управления доступом отсутствует уровень доступа.	Разрешить приложению удалить отсутствующие принципалы из списка контроля доступа объекта.	Отсутствующий принципал удален из списка контроля доступа объекта.
<Тип объекта> Список контроля доступа объекта "<Имя объекта>" (идентификатор объекта = <ID>) ссылается на отсутствующий уровень доступа (идентификатор объекта уровня доступа = <ID>).	Для записи управления доступом отсутствует уровень доступа.	Разрешить приложению удалить отсутствующий уровень доступа из списка контроля доступа объекта.	Отсутствующий уровень доступа удален из списка контроля доступа объекта.
<Тип объекта> Объект <Имя объекта> (Идентификатор объекта = <ID>) имеет несколько папок "Избранное".	Указанная учетная запись пользователя имеет несколько папок "Избранное".	Разрешить приложению объединить несколько папок "Избранное" в одну.	Все папки "Избранное" объединены в одну папку.
<Тип объекта> Объект <Имя объекта> (Идентификатор объекта = <ID>) содержит недопустимые записи входных файлов (Files).	В списке входных файлов объекта содержатся недопустимые записи.	Разрешить инструменту удалить недопустимые записи объекта из его списка входных файлов.	Недопустимые записи удалены из списка входных файлов объекта.

Предупреждающее сообщение	Несоответствие	Рекомендация	Действие
<Тип объекта> Объект <Имя объекта> (Идентификатор объекта = <ID>) содержит недопустимые записи выходных файлов (Files).	В списке выходных файлов объекта содержатся недопустимые записи.	Разрешить инструменту удалить недопустимые записи объекта из его списка выходных файлов.	Недопустимые записи удалены из списка выходных файлов объекта.
<Тип объекта> Для объекта "<Имя объекта>" (идентификатор объекта = <ID>) отсутствует требуемая группа серверов кэширования (идентификатор объекта группы серверов = <ID>).	У объекта отсутствует требуемая группа серверов кэширования.	Перезапланировать объект и выбрать существующую группу серверов.	Действия не предпринимаются.
<Тип объекта> Для объекта "<Имя объекта>" (идентификатор объекта = <ID>) отсутствует требуемая группа серверов обработки (идентификатор объекта группы серверов = <ID>).	У объекта отсутствует требуемая группа серверов обработки.	Перезапланировать объект и выбрать существующую группу серверов.	Действия не предпринимаются.
<Тип объекта> Список профилей объекта "<Имя объекта>" (идентификатор объекта = <ID>) содержит отсутствующие объекты (идентификаторы объектов = <ID>).	В списке профилей объекта содержатся отсутствующие объекты.	Обновите публикацию с использованием существующих профилей. Приложение не может выполнить какие-либо действия.	Действия не предпринимаются.

Приложение "Права"

29.1 О 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*.

29.2 Общие права

Права, рассмотренные в данном разделе, применимы к различным типам объектов. 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. Дополнительные сведения об этом праве см. в главе «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](#)

29.3 Права для определенных типов объектов

29.3.1 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](#)

29.3.2 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.
«Изменить 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.

29.3.3 Документы Desktop Intelligence

Права в этом разделе применимы только к документам Desktop Intelligence.

Право	Описание
«Использовать списки значений»	Позволяет использовать списки значений.
«Загрузка файла, связанного с объектом»	Позволяет загружать файл, связанный с объектом.
«Экспорт данных отчета»	Позволяет экспортировать данные документа 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.
«Просмотр SQL»	Позволяет просматривать созданный для запроса SQL.
«Обновление данных отчета»	Позволяет обновлять данные документа.
«Обновление списка значений»	Позволяет обновлять списки значений для подсказок при создании подсказки или просмотре документа. Для этого также необходимо иметь право «Использовать списки значений» по отношению к документу.

Права на документы в формате PDF, XLS, Rich Text и текстовом формате:

Право	Описание
«Добавление объектов в каталог»	Позволяет добавлять объекты в папку. Это право также применимо к объектам, которые ведут себя как каталог (например, папки "Входящие", "Избранное" или пакеты объектов).
«Копирование объектов в другой каталог»	Позволяет создавать копии объектов в других каталогах CMS. Для этого также требуется право "Добавление объектов в каталог" в соответствующей папке назначения.
«Удаление экземпляров»	Позволяет удалять только экземпляры объектов. При наличии права "Удаление объектов" для удаления экземпляров данное право не требуется.
«Удаление объектов»	Позволяет удалить эту категорию.

Право	Описание
«Изменение объектов»	Позволяет изменять свойства категорий, перемещать категорию в другую категорию в виде вложенной категории, добавлять объекты в категорию и удалять объекты из категории.
«Изменение прав пользователей на объекты»	Позволяет изменить любое право любого пользователя на данный объект.
«Приостановка и возобновление выполнения экземпляров документа»	Позволяет приостанавливать и возобновлять выполняемые экземпляры объектов.
«Тиражирование содержимого»	Позволяет тиражировать объекты в другую систему объединенного развертывания.
«Повторное планирование экземпляров»	Позволяет повторно планировать выполнение экземпляров объектов.
«Безопасное изменение прав пользователей в отношении объектов»	Позволяет предоставлять, отзывать или возвращать в состояние "Не задано" только права, которые уже были предоставлены пользователю.
«Просмотр экземпляров документа»	Позволяет просматривать экземпляры объектов. Это право является базовым и требуется для выполнения всех задач в отношении экземпляров объектов.
«Просмотр объектов»	Позволяет просматривать категории и содержащиеся в них вложенные категории.

29.3.4 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.

29.3.5 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 отказаться 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.

29.3.6 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 – включить 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 подсказок при создании подсказки 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 Web Intelligence Rich Client возможность отправлять документы в виде вложений электронной почты.

29.3.7 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 универсов 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.
«Добавить или изменить атрибуты пользователя»	<p>Позволяет изменять значение адреса электронной почты пользователя или настраиваемые атрибуты пользователя.</p> <p>Это право применяется к пользователям.</p>
«Добавить или изменить атрибуты пользователя (право владельца)»	

Право	Описание
	<p>Позволяет владельцу объекта пользователя изменять адрес электронной почты пользователя или настраиваемые атрибуты пользователя.</p> <p>Это право применяется к пользователям.</p>

29.3.8 Уровни доступа

Права, рассмотренные в данном разделе, применимы только к уровням доступа.

Право	Описание
«Использовать уровень доступа для назначения защиты»	<p>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.</p>

См. также

- [Выбор параметров Изменить права пользователей на объекты](#)

29.3.9 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
«Добавление объектов 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>
«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.

Право	Описание
«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»	<p>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 соединению юниверса.</p>
«Создание и редактирование запросов на основе юниверса»	<p>Позволяет создавать документы и редактировать запросы, основанные на юниверсе.</p>

29.3.10 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».

29.3.11 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 универсе.

Примечание:

- Настройки безопасности на уровне доступа к объекту переопределяют все наследуемые универсом настройки безопасности.
- Для универсов .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 универсов](#)

29.3.11.1 Назначение уровней доступа к объектам для универсов

Для установки защиты на уровне доступа к объектам для универсов вам необходимо иметь право **Изменение прав пользователей на объекты** по отношению к универсу.

1. Выберите универс в области «Юниверсы» центрального сервера управления.
2. Выберите **Действие > Безопасность универса**.
3. В диалоговом окне «Безопасность универса» для пользователя или группы выберите уровень доступа к объектам в списке **Уровень безопасности объектов**.

29.3.12 Права соединений

В данном разделе рассматриваются права, которые применимы только к соединениям универсов, или общие права, которые имеют особое значение в контексте соединений универсов. Эти права применяются к соединениям, опубликованным в репозитории.

Права реляционного соединения

Право	Описание
«Просмотр объектов»	Позволяет просмотреть соединение.
«Изменить объекты»	Позволяет изменять параметры соединения.
«Загрузить соединение локально»	<p>Позволяет использовать юниверсы, созданные для соединений в Web Intelligence Rich Client в автономном режиме.</p> <p>Позволяет использовать драйвер локального ПО среднего яруса в средстве дизайна информации. Для этого выберите параметр локального ПО среднего яруса в предпочтениях средства дизайна информации. В противном случае для обработки запросов к базе данных будет использоваться серверное ПО среднего яруса.</p> <p>Это право также требуется для редактирования защищенного соединения в средстве дизайна информации.</p>
«Удалить объекты»	Позволяет удалить соединение.

Право	Описание
«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.

29.3.13 Приложения

29.3.13.1 СМС

Права, рассмотренные в данном разделе, применимы только к СМС.

Право	Описание
«Входить в систему СМС и выполнять просмотр объекта в СМС»	Позволяет выполнить вход 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.

29.3.13.2 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.

29.3.13.2.1 Права на приложения сотрудничества

Права, описываемые в этом разделе, применяются к приложениям SAP Jam и SAP StreamWork, настроенным на платформе BI.

Право	Описание
Комментарии к документам	Добавление комментариев к документам и экземплярам
Комментарии к документам, правами на которые владеет пользователь	Добавление комментариев к документам и экземплярам, принадлежащим пользователю
Просмотр комментариев к документам, правами на которые владеет пользователь	Просмотр комментариев к документам и экземплярам, принадлежащим пользователю
Просмотр комментариев к документам	Просмотр комментариев к документам и экземплярам

29.3.13.3 Рабочие пространства BI

Права, рассмотренные в данном разделе, применимы только к рабочим пространствам BI.

Право	Описание
«Создание и редактирование рабочих пространств BI»	Разрешает пользователю создавать новые рабочие пространства BI и изменять существующие рабочие пространства BI.
«Создание и редактирование модулей»	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.

29.3.13.4 Desktop Intelligence

Права в этом разделе применимы к SAP BusinessObjects Desktop Intelligence.

Право	Описание
«Создание и изменение соединений»	Позволяет создавать новое соединение или редактировать существующее.
«Манипулирование источником данных»	Позволяет изменять запрос или юниверс, на котором основан запрос.
«Изменение произвольного SQL»	Позволяет редактировать запрос, в качестве источника данных которого используются рукописные SQL-скрипты. Для выполнения этого действия необходимо предоставить разрешение «Использовать рукописный SQL».
«Использование произвольного SQL»	Позволяет создавать запрос с использованием скриптов с рукописным SQL в качестве источника данных.
«Обновление списка и категорий документов»	Позволяет обновлять список документов.
«Отправка документов в репозиторий»	Позволяет публиковать документ в CMS, общих папках или личных папках пользователя.
«Отправка документов по почте»	Позволяет отправлять документы из Desktop Intelligence в виде электронного сообщения.

Право	Описание
«Извлечение документов»	Позволяет импортировать документ из CMS.
«Выполнение кода VBA»	Позволяет запустить и выполнить код VBA.
«Установка модулей расширения»	Позволяет устанавливать или удалять надстройки VBA.
«Управление всеми корпоративными категориями»	Позволяет создавать, редактировать и удалять любые документы в категории.
«Управление своими корпоративными категориями»	Позволяет создавать, изменять и удалять корпоративные категории из приложения Desktop Intelligence.
«Изменение области анализа»	Позволяет изменять область анализа
«Работа в режиме детализации»	Позволяет выполнять развертку до содержащих больше подробных сведений уровней анализа в отчетах.
«Работа в режиме "Срезы"»	Позволяет работать с панелью "Срезы".
«Изменение кода VBA»	Позволяет изменять используемые в отчетах макросы VBA.
«Конвертер евро»	Позволяет преобразовывать валюту в отчетах в/из евро.
«Копирование в буфер»	Позволяет вырезать или копировать содержимое документа.
«Детализация»	Позволяет выполнять более глубокую детализацию отчета и извлекать новые данные.
«Изменение курса конвертации евро»	Позволяет изменять обменные курсы евро, используемые функцией "Конвертер евро".
«Взаимосвязь отчетов Desktop Intelligence»	Позволяет выбирать отдельные элементы отчета для вырезания, копирования, очистки, дублирования или удаления.
«Взаимосвязь документов Desktop Intelligence»	Позволяет переименовывать, дублировать, вставлять или удалять отчет в документ.
«Печать документов»	Позволяет печатать документы.

Право	Описание
«Обновление содержимого Desktop Intelligence»	Позволяет обновлять содержимое Desktop Intelligence.
«Использование шаблонов»	Позволяет создавать отчеты с шаблонами или применять шаблоны к имеющемуся содержимому.
«Создание шаблонов»	Позволяет сохранять документы в качестве шаблонов.
«Сохранение документов для всех пользователей»	Позволяет сохранять документы без ограничений безопасности для использования в автономном режиме (чтобы все пользователи смогли просматривать документ, сохраненный локально).
«Создание документов Desktop Intelligence»	Позволяет создавать новый документ.
«Сохранение документов Desktop Intelligence»	Позволяет сохранять документы локально.
«Отправка документов в папку "Входящие"»	Позволяет отправлять документы в папку "Входящие" стартовой панели BI.
«Использование пользовательских объектов»	Позволяет создавать, редактировать или удалять пользовательские объекты.
«Обновление списка значений»	Позволяет обновлять списки значений.
«Использование списка значений»	Позволяет использовать и обновлять списки значений в документе.
«Изменение списка значений»	Позволяет редактировать списки значений, определенные в юниверсах.
«Использование запросов»	Позволяет создавать новые запросы на основе юниверса.
«Редактирование запросов»	Позволяет редактировать запросы на основе юниверса.
«Просмотр SQL»	Позволяет просматривать созданный для запроса SQL.
«Изменение SQL запроса»	Позволяет изменять SQL запросов.

Право	Описание
«Постоянное воссоздание SQL»	Позволяет воссоздавать запросы после каждого обновления.
«Использование хранимых процедур»	Позволяет создавать запрос, используя хранимую процедуру в качестве источника данных.
«Изменение хранимых процедур»	Позволяет изменять параметры хранимых процедур.
«Использование файла персональных данных»	Позволяет создавать отчет с использованием текстовых файлов Excel, dBase или ASCII в качестве поставщика данных.
«Изменение файла персональных данных»	Позволяет редактировать поставщик персональных данных.
«Безопасное изменение прав пользователей на объект»	Позволяет предоставлять, отзываться или возвращать в состояние "Не задано" только права, которые уже были предоставлены пользователю.
«Изменение прав пользователей на данный объект»	Позволяет изменить любое право любого пользователя на данный объект.
«Редактирование этого объекта»	Позволяет изменять свойства приложения в СМС.
«Вход в Desktop Intelligence и просмотр данного объекта в СМС»	Позволяет выполнять вход в Desktop Intelligence и просматривать объект в СМС.

29.3.13.5 Web Intelligence

Права в этом разделе применимы только к SAP BusinessObjects Web Intelligence (включая интерфейс Rich Client) 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 Rich Client – включить Web Intelligence Rich Client»	Разрешает использование интерфейса Rich Client.
«Интерфейс Rich Client – включить локальные поставщики данных»	Разрешает использовать личные поставщики данных в интерфейсе Rich Client.
«Интерфейс Rich Client – экспорт документов»	Позволяет экспортировать документы в CMS в интерфейсе Rich Client.
«Интерфейс Rich Client – импорт документов»	Позволяет импортировать документы из CMS в интерфейсе Rich Client.
«Интерфейс Rich Client – установка со стартовой панели BI»	Позволяет загружать интерфейс Rich Client со стартовой панели BI.
«Интерфейс Rich Client – печать документов»	Позволяет печатать документы из интерфейса Rich Client.
«Интерфейс Rich Client – удаление защиты документов»	Позволяет снимать защиту документа из интерфейса Rich Client.
«Интерфейс Rich Client – сохранение документов для всех пользователей»	Разрешает сохранение документов для всех пользователей из интерфейса Rich Client.
«Интерфейс Rich Client – локальное сохранение документов»	Разрешает сохранение документов на локальный диск в интерфейсе Rich Client.
«Интерфейс Rich Client - отправка по электронной почте»	Разрешает отправку документов по электронной почте в интерфейсе Rich Client.
«Интерфейс Rich Client - включить локальные поставщики данных»	Разрешает использовать личные поставщики данных в интерфейсе Rich Client.
«Документы – отключить автоматическое обновление при открытии»	Отключает автоматическое обновление документов при их открытии.

Право	Описание
«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 CMS.
«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).
«Скрипт запроса – включить просмотр (SQL, MDX...)»	Разрешает просмотр скриптов запросов (SQL и MDX).

Право	Описание
«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.
«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).

29.3.13.6 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.
«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.

29.3.13.7 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.

29.3.13.8 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.

29.3.13.9 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 ВІ при помощи проводника списка документов.
«Использовать папку "Входящие" для предупреждений»	(Не рекомендуется) Позволяет использовать папку "Входящие" для предупреждений.
«Использовать поиск»	Позволяет пользователям выполнять поиск сразу по всем подключенным репозиториям платформы ВІ, используя контекстный поиск.

29.3.13.10 Предупреждение

Права, рассмотренные в данном разделе, применимы только к приложению Предупреждение.

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

29.3.13.11 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»

29.3.13.12 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"

30.1 0 приложении "Свойства серверов"

В приложении "Свойства серверов" перечислены и описаны свойства, которые можно задать для каждого сервера платформы SAP BusinessObjects Business Intelligence.

30.1.1 Общие свойства сервера

Представленные в этом разделе свойства серверов применимы к серверам любого типа.

Таблица 30-1: 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 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 30-2: 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 30-3: 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 30-4: 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 30-5: 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](#)

30.1.2 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 30-6: 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 30-7: 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>	5
Максимальное число запросов дочерних объектов	Указывает количество заданий, которые дочерний объект обрабатывает перед повторным запуском.	100

Свойства сервера адаптивной обработки

Таблица 30-8: 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>	1200

Таблица 30-9: Свойства службы прокси аудита клиента

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Таблица 30-10: Свойства службы маркера безопасности

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Таблица 30-11: Свойства службы аналитических действий

Показатель	Описание	
Максимальное число активных соединений на сеанс пользователя	Максимальное число доступных пользователю на заданный момент времени соединений с сервером SAP. При открытии пользователем отчета или информационной панелью с поддержкой RRI устанавливается соединение с сервером SAP, с помощью которого определяются целевые идентификаторы RRI.	20
Максимальное число неиспользуемых соединений на сеанс пользователя	Число неиспользуемых соединений, которые остаются открытыми и используются последующими запросами RRI. Увеличение значения этого параметра повлечет за собой дополнительные затраты ресурсов системы.	20
Максимальное время ожидания соединения (в секундах)	Период времени, в течение которого платформа представления службы действий ожидает ответа от сервера SAP (в секундах).	30

Таблица 30-12: Свойства службы публикации

Свойство	Описание	Значение по умолчанию
Размер пула потока	Указывает, сколько потоков обработки для пакета области можно запустить одновременно. Если для этого свойства установлено значение «0», размер пула потока определяется с помощью формулы на основе числа ядер ЦП на используемом компьютере.	0

Таблица 30-13: Свойства службы преобразований

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Таблица 30-14: Свойства службы мониторинга

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Таблица 30-15: Свойства службы поиска по платформе

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Таблица 30-16: Свойства службы заключительной обработки публикаций

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Свойства центрального сервера управления**Примечание:**

При изменении любого из этих свойств сервера необходимо перезапустить сервер, чтобы изменения вступили в силу.

Таблица 30-17: Свойства Central Management Service

Свойство	Описание	По умолчанию
Порт сервера имен	Определяет порт, на котором CMS прослушивает начальные запросы к службе имен.	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>	14
Автоматическое повторное подключение к системной базе данных	<p>Определяет, будет ли CMS автоматически предпринимать попытки восстановления соединения с базой 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 соединения с базой данных потребуется перезапуск CMS.</p>	ИСТИНА

Таблица 30-18: 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>	86400

Свойства сервера событий

Таблица 30-19: Свойства службы событий

Свойство	Описание	Значение по умолчанию
Интервал опроса событий (в секундах)	Определяет периодичность, с которой сервер опрашивает файл, инициирующий события (в секундах).	10 Допускаются значения в диапазоне от 1 до 1200.
Интервал очистки (мин)	Определяет периодичность запуска служебной программы для очистки в минутах.	20

Свойства сервера репозитория входящих файлов

Таблица 30-20: Свойства службы хранилища входящих файлов

Свойство	Описание	Значение по умолчанию
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%
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 хранилища файлов .	%DefaultInputFRSDirTemp%

Свойство	Описание	Значение по умолчанию
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.	10
Максимальное число повторных попыток доступа к файлам	Определяет количество попыток сервера получить доступ к определенному файлу.	1

Свойства сервера репозитория исходящих файлов

Таблица 30-21: Свойства службы хранилища исходящих файлов

Свойство	Описание	Значение по умолчанию
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.	%DefaultOutputFSDir%
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.	%DefaultOutputFSDirTemp%

Свойство	Описание	Значение по умолчанию
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.	10
Максимальное число повторных попыток доступа к файлам	Определяет количество попыток сервера получить доступ к определенному файлу.	1

Свойства сервера контейнера веб-приложений

Таблица 30-22: 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 службы, которые еще не были запущены. 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>	1200

Таблица 30-23: Свойства службы протокола трассировки

Свойство	Описание	Значение по умолчанию
Уровень журнала	<p>Позволяет включить регистрацию в журнале и присвоить уровню важности и детализации значение "Нет" (регистрация только критических событий), "Низкий" (запуск, завершение работы, сообщения о начале и завершении запроса), "Средний" (сообщения об ошибках, предупреждениях и большинство сообщений о статусе) или "Высокий" (регистрация всех событий без исключений; Используется только для отладки. загрузка ЦП повышается и может снизиться производительность).</p> <p>Доступны следующие пункты меню:</p> <ul style="list-style-type: none"> • Не определен • Нет • Низкий • Средний • Высокий 	Не определен

Таблица 30-24: Свойства службы бизнес-процессов VI

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Таблица 30-25: Свойства службы построителя запросов

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Таблица 30-26: Веб-служба RESTful – Свойства конфигурации свойств системы

Свойство	Описание	Значение по умолчанию
Показать стек ошибок	Если это свойство включено, в журнал ошибок вносятся сообщения об ошибках веб-службы RESTful для целей отладки. Это свойство не следует использовать для других целей или в ситуации, когда встает вопрос обеспечения безопасности в связи с раскрытием данных платформы BI.	Не выбрано
Число объектов по умолчанию на одной странице	Число записей на странице. Разработчики могут переопределить эту настройку с помощью параметра "&pageSize=<m>" в пакете SDK веб-служб RESTful.	50
Время ожидания маркера сеанса Enterprise (мин)	Время срока действия для маркера входа. По истечении этого времени необходимо сгенерировать новый маркер входа.	60
Размер пула сеанса	Число одновременно кэшируемых сеансов, которое используется для повышения производительности сервера. В пуле сеанса кэшируются активные сеансы веб-службы RESTful, что позволяет повторно использовать их при отправке пользователем другого запроса, содержащего такой же маркер входа в систему в заголовке запроса HTTP.	1000
Время ожидания пула сеанса (мин)	Срок действия кэшированных сеансов (в минутах).	2

Свойство	Описание	Значение по умолчанию
Включить базовую аутентификацию HTTP	Если эта настройка не включена, в запросах веб-службы RESTful должен использоваться маркер входа. Если эта настройка включена, пользователи должны ввести свои имя и пароль только при первом выполнении запроса веб-службы RESTful. При включенной настройке появляется раскрывающийся список Схема аутентификации по умолчанию для базового HTTP .	Не выбрано
Схема аутентификации по умолчанию для базового HTTP	<p>Если установлен флажок Включить базовую аутентификацию HTTP, можно выбрать один из четырех типов аутентификации. Обратите внимание, что имена и пароли передаются как текст, если не используются параметры HTTPS.</p> <p>Допустимы следующие значения:</p> <ul style="list-style-type: none"> • secEnterprise • secDAP • SAPR3 • secWinAD 	Пустая. Однако если выбрано значение Включить базовую аутентификацию HTTP , по умолчанию используется параметр secEnterprise .

Таблица 30-27: Веб-служба RESTful – Свойства конфигурации совместного использования ресурсов по всем источникам

Свойство	Описание	Значение по умолчанию
Разрешение источников	Этот параметр позволяет пользователям, работающим в браузерах с поддержкой CORS, осуществлять доступ к страницам с Javascript, которые должны осуществлять доступ к нескольким доменным именам. Добавьте имена доменов, разделенные запятыми. Например, <code>http://origin1.server.com:8080, http://origin2.server.com:8080</code> . По умолчанию браузеры имеют доступ ко всем доменам (*).	* (звездочка)
Максимальный срок (минуты)	Это максимальный срок кэширования HTTP-запросов браузерами.	1440

Таблица 30-28: Веб-служба – свойства конфигурации доверительной аутентификации

Свойство	Описание	Значение по умолчанию
Метод извлечения	<p>Эта настройка представляет собой меню, позволяющее указать, какой метод запроса будет использоваться для извлечения маркеров входа доверительной аутентификации при использовании API-интерфейса веб-службы RESTful /logon/trusted.</p> <ul style="list-style-type: none"> • HTTP_HEADER используется для запросов GET с заголовком запроса accept=application/xml (или application/json). • QUERY_STRING используется для добавления имени входа в систему в конец запроса URL-адреса, отправляемого с помощью API-интерфейса веб-службы RESTful, например /logon/trusted/?user=johndoe. • COOKIE используется, если имя входа в систему извлечено из cookie-файла веб-браузера. Домен, имя, значение и путь должны сохраняться в cookie-файле. 	HTTP_HEADER
Параметр имени пользователя	<p>Это метка, использующаяся для идентификации доверенного пользователя при извлечении маркера входа.</p>	X-SAP-TRUSTED-USER

Таблица 30-29: Свойства службы веб-приложения BOE

Тип свойства	Описание	Значение по умолчанию
Тип аутентификации	<p>Тип аутентификации, который используется при входе пользователей в стартовую панель BI платформы SAP BusinessObjects Business Intelligence.</p> <p>Допустимы следующие значения:</p> <ul style="list-style-type: none"> • AD Kerberos • Служба SSO AD Kerberos • Enterprise • LDAP 	Enterprise
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».	(пустой)
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.	(пустой)
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.	(пустой)

Таблица 30-30: SDK для веб-служб и свойства 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.	ЛОЖЬ
Домен AD по умолчанию	Используется домен Active Directory по умолчанию, чтобы пользователям не нужно было указывать домен при входе в систему.	(пустой)
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.	(пустой)
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.	(пустой)

Таблица 30-31: 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.	ИСТИНА

Свойство	Описание	По умолчанию
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 .	localhost
Порт HTTP	Порт, через который предоставляется служба HTTP.	6405 Допускаются значения в диапазоне от 1 до 65535.
Максимальный размер заголовка HTTP	Максимальный допустимый размер (в байтах) запроса и ответа заголовка HTTP.	32768

Таблица 30-32: Конфигурация HTTP через свойства прокси-сервера

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.	ЛОЖЬ
Привязка ко всем IP-адресам	Привязывать ли порт HTTP через прокси ко всем сетевым интерфейсам.	ИСТИНА
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 .	localhost

Свойство	Описание	По умолчанию
Порт HTTP	Порт, через который предоставляется служба HTTP в развертываниях с обратным прокси. Для указания значения поставьте флажок в поле Включить HTTP через прокси .	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 .	(пустой)
Порт прокси	Порт прямого или обратного прокси-сервера. Для указания значения поставьте флажок в поле Включить HTTP через прокси .	0 Допускаются значения в диапазоне от 1 до 65535.
Максимальный размер заголовка HTTP	Максимальный допустимый размер (в байтах) запроса и ответа заголовка HTTP.	32768

Таблица 30-33: Свойства конфигурации HTTPS

Свойство	Описание	По умолчанию
Включить HTTPS	Включать ли связь HTTPS/SSL.	ЛОЖЬ
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 .	localhost
Порт HTTPS	Порт, через который предоставляется служба HTTPS. Для указания значения поставьте флажок в поле Включить HTTPS .	443 Допускаются значения в диапазоне от 1 до 65535.

Свойство	Описание	По умолчанию
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 .	(пустой)
Порт прокси	Порт прямого или обратного прокси-сервера. Для указания значения поставьте флажок в поле Включить HTTPS .	0 Допускаются значения в диапазоне от 1 до 65535.
Протокол	Используемый протокол шифрования. Для указания значения поставьте флажок в поле Включить HTTPS .	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 .	PKCS12 Допускаются значения PKCS12 или JKS.
Местоположение файла хранилища сертификатов	Полный путь к файлу сертификатов. Для указания значения поставьте флажок в поле Включить HTTPS .	(пустой)
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 .	(пустой)

Свойство	Описание	По умолчанию
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 .	(пустой)
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 .	ЛОЖЬ
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 .	(пустой)
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 .	(пустой)
Максимальный размер заголовка HTTP	Максимальный допустимый размер (в байтах) запроса и ответа заголовка HTTP.	32768

Таблица 30-34: Свойства параллельной работы (по коннекторам)

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.	150 Допускаются значения в диапазоне от 1 до 1000.

Таблица 30-35: Свойства 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.	(пустой)
Расположение файла bscLogin.conf	Полный путь к файлу <code>bscLogin.conf</code> .	(пустой)

30.1.3 Свойства служб соединения

Категория службы 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 30-36: Свойства службы доступа к данным Excel

Свойство	Описание	Значение по умолчанию
Время ожидания очистки доступа к данным Excel (сек)	Задаёт время (в секундах) ожидания службой неактивного клиента перед выполнением очистки сеанса клиента.	По умолчанию используется значение 1200 секунд.

Свойство	Описание	Значение по умолчанию
Время ожидания замены доступа к данным Excel (всек)	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 доступа к данным Excel (сек) .	По умолчанию используется значение 600 секунд.

Таблица 30-37: 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

Свойство	Описание	Значение по умолчанию
Время ожидания пула подключений	<p>Задаёт максимальное время простоя для соединений в пуле (в минутах).</p> <p>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>.</p>	60
Время простоя неактивности переходных объектов (мин)	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 30-38: Свойства отслеживания низкого уровня

Свойство	Описание	Значение по умолчанию
Помните: Нет необходимости перезапускать сервер после изменения следующих свойств отслеживания низкого уровня.		
Включение отслеживания заданий	Включает отслеживание заданий сервера соединений. Примечание: Для отслеживания необходимо, чтобы свойство Уровень журнала было установлено в значение Высокий .	Отменено
Включить отслеживание программного обеспечения среднего яруса	Включает трассировку всего промежуточного ПО. Для трассировки конкретного промежуточного ПО необходимо настроить файл <code>cs.cfg</code> и перезапустить сервер. Примечание: Для отслеживания необходимо, чтобы свойство Уровень журнала было установлено в значение Высокий .	Отменено

Таблица 30-39: Свойства источников данных Active Data

Свойство	Описание	Значение по умолчанию
Предупреждение: После изменения следующих свойств источников данных Active Data необходимо перезапустить сервер.		

Свойство	Описание	Значение по умолчанию
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
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

Свойство	Описание	Значение по умолчанию
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> 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.

Таблица 30-40: Свойства службы доступа к пользовательским данным

Свойство	Описание	Значение по умолчанию
Время ожидания очистки доступа к пользовательским данным (сек)	Задаёт время (в секундах) ожидания службой неактивного клиента перед выполнением очистки сеанса клиента.	По умолчанию используется значение 1200 секунд.
Время ожидания замены доступа к пользовательским данным (сек)	<p>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 доступа к пользовательским данным (сек).</p>	По умолчанию используется значение 600 секунд.

Таблица 30-41: 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.

Таблица 30-42: Свойства службы управления жизненным циклом

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Таблица 30-43: Свойства службы ClearCase управления жизненным циклом

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Таблица 30-44: Свойства службы Visual Difference

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

См. также

- [Общие свойства сервера](#)

30.1.4 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 2013
- Сервер обработки Crystal Reports 2013

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 30-45: 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>	Значением по умолчанию является FALSE.
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.
Время 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.
Время ожидания кэша безопасности (мин)	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.
Имя DLL		rasprocReport

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 30-46: 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 20 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>	Значением по умолчанию является FALSE.
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
Время 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 -Xms128m -Djava.class.path=%CommondH%\ocr.jar

Таблица 30-47: 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 2013

Примечание:

При изменении любого из этих свойств необходимо перезапустить сервер, чтобы изменения вступили в силу.

Таблица 30-48: Свойства службы просмотра и изменений Crystal Reports 2013

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.
Время 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 30-49: 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 2013**Примечание:**

При изменении любого из этих свойств необходимо перезапустить сервер, чтобы изменения вступили в силу.

Таблица 30-50: Свойства службы обработки Crystal Reports 2013

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 20 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>	Значением по умолчанию является FALSE.
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
Время 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.	<code>%TEMP%</code> <code>C:\Temp</code>
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.
Число считываемых записей БД при предварительном просмотре или обновлении (0 – не ограничено)	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 30-51: 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.

30.1.5 Свойства служб Analysis

Категория служб Analysis включает адаптивный сервер обработки:

Таблица 30-52: Свойства службы Multi-Dimensional analysis service

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 чрезмерно 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 100000 элементов.

Таблица 30-53: 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 SAP BusinessObjects Business Intelligence.	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.

30.1.6 Свойства служб объединения данных

Категория служб объединения данных включает адаптивный сервер обработки:

Таблица 30-54: 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 10800 секунд.
Время ожидания неактивного оператора	Задаёт время (в секундах), по истечении которого неактивный оператор запроса закрывается.	По умолчанию используется значение 600 секунд.

30.1.7 Свойства служб Web Intelligence

К категории служб Web Intelligence относятся следующие серверы:

- Адаптивный сервер обработки
- Сервер обработки Web Intelligence

Параметры адаптивного сервера обработки

Таблица 30-55: Параметры командной строки

Свойство	Описание	Значение по умолчанию
Развертывание до уровня	<p>Указывает уровень извлечения данных из запросов BEx.</p> <p>По умолчанию иерархии не развертываются до заданного уровня. В качестве уровня по умолчанию всегда используется Level00. Это поведение можно изменить, добавив данный параметр в командную строку, однако если значение слишком велико, Web Intelligence извлекает все данные иерархии, что может негативно сказаться на производительности и стабильности системы.</p>	<p>-Dsap.sl.bics.expandToLevel=n</p> <p>n — это любое целое число от 0 до 99. Если n=0 или этот параметр не указан, иерархии не будут использовать параметр "Развертывание до уровня".</p>

Таблица 30-56: Свойства службы мониторинга Web Intelligence

Свойство	Описание	Значение по умолчанию
Включить мониторинг	Определяет, включен ли мониторинг для службы.	ИСТИНА
Задержка цикла потока мониторинга (секунды)	Указывает длительность интервалов между попытками службы направлять проверочные запросы клиентам, в секундах.	300
Время ожидания очистки отслеживаемых ресурсов по умолчанию (сек)	Задаёт время (в секундах) ожидания службой неактивного клиента перед выполнением очистки сеанса клиента.	1200
Время ожидания очистки отслеживаемых ресурсов по умолчанию (сек)	Задаёт время (в секундах) ожидания службой неактивного клиента перед выгрузкой сеанса клиента на жесткий диск. Рекомендуется, чтобы это значение было меньше значения свойства "Время ожидания очистки отслеживаемых ресурсов по умолчанию (сек)".	600
Включить профилирование службы		ИСТИНА
Включить мониторинг активности службы		ИСТИНА

Таблица 30-57: Свойства службы визуализации

Свойство	Описание	Значение по умолчанию
Время ожидания очистки подсистемы визуализации(сек)	Задаёт время (в секундах) ожидания службой неактивного клиента перед выполнением очистки сеанса клиента.	1200

Свойство	Описание	Значение по умолчанию
Время ожидания замены подсистемы 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 подсистемы визуализации (сек) .	600

Таблица 30-58: Свойства службы Rebean

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Таблица 30-59: Свойства службы восстановления документов

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Таблица 30-60: Свойства службы моста DSL

Свойство	Описание	Значение по умолчанию
Время ожидания очистки подсистемы моста DSL (сек)	Задаёт время (в секундах) ожидания службой неактивного клиента перед выполнением очистки сеанса клиента.	1200

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 30-61: Свойства службы Information Engine

Свойство	Описание	По умолчанию
Включить список значений кэша	Определяет необходимость включения кэширования списка значений на сервере обработки Web Intelligence.	ИСТИНА
Размер пакета списка значений (записи)	Определяет максимальное число записей (или значений) для каждого пакета списка значений.	1000
Макс. размер пользовательской сортировки (элементы)	Определяет максимальное число элементов при пользовательской сортировке.	100
Макс. размер кэша юниверсов (юниверсы)	Определяет число Юниверсов, которые могут быть кэшированы на сервере обработки Web Intelligence.	20
Максимальный размер списка значений (записи)	Определяет максимальное число записей (или значений) для каждого списка значений.	50000

Таблица 30-62: Свойства основной службы Web Intelligence

Свойство	Описание	Значение по умолчанию
Время ожидания перед повторным использованием (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 .	1200

Свойство	Описание	Значение по умолчанию
Предельное 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.	300 Допустимый диапазон: от 100 до 10000 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.	120
Максимальное число документов на одного пользователя	Определяет максимальное число активных сеансов (документов Web Intelligence), которые могут быть связаны с пользователем в любое заданное время. Следовательно, если задано значение 5, пользователь может одновременно использовать до 5 активных сеансов.	5 Можно задать значение в диапазоне 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 Время ожидания перед повторным использованием .	50
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.	ИСТИНА
Время 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.	20

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>	<p>50</p> <p>Допустимым диапазоном является от 5 до 65535.</p>
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>	<p>ИСТИНА</p>

Свойство	Описание	Значение по умолчанию
Нижний порог памяти (Мбайт)	Определяет нижнее пороговое значение использования памяти.	3500
Верхний порог памяти (Мбайт)	Определяет верхнее пороговое значение использования памяти.	4500
Макс. порог памяти (Мбайт)	Определяет максимальное пороговое значение использования памяти.	6000
Включить мониторинг службы APS	Включает мониторинг сервера службой APS, размещаемой на адаптивном сервере обработки.	ИСТИНА
Число повторов тестового опроса службы APS	Указывает количество выполняемых сервером попыток установить связь со службой APS перед решением о невозможности выполнения этой задачи.	3
Период потока мониторинга службы APS	Указывает период задержки между попытками достижения службы APS.	300
Включить протоколы текущей активности	Указывает необходимость создания полных трассировок в файлах журнала сервера. Примечание: Это свойство следует включать только для отладки при диагностике ошибок. В нормальном режиме работы необходимо установить значение равным FALSE.	ЛОЖЬ

Таблица 30-63: Свойства службы обработки Web Intelligence

Свойство	Описание	Значение по умолчанию
Включить использование HTTP URL	Указывает, может ли сервер получать доступ к файлам, сохраненным удаленно.	ИСТИНА

Свойство	Описание	Значение по умолчанию
Значение прокси	Задаёт адрес прокси-сервера данной сети. Это значение необходимо задавать только в случае, если в сети имеется прокси-сервер и выполняется попытка доступа к файлам, сохранённым удалённо.	(пустой)

Таблица 30-64: Свойства общей службы Web Intelligence

Свойство	Описание	Значение по умолчанию
Время ожидания кэша без-опасности (мин)	Определяет период времени (в минутах) перед выполнением очистки содержимого кэша документов. Время ожидания зависит от даты последнего доступа к каждому документу.	4370
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> .	120
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.	ЛОЖЬ

Свойство	Описание	Значение по умолчанию
Включить кэш документов	Определяет необходимость включения кэша документов. Если свойство включено, в кэш можно загрузить предварительно запланированные документы Web Intelligence.	ИСТИНА
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.	ИСТИНА
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> .	1000000
Максимальное пространство уменьшения кэша документа (в процентах)	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.	70

Свойство	Описание	Значение по умолчанию
Макс. размер символьного потока (Мбайт)	<p>Определяет максимальный размер символьного потока, переданного клиенту Web Intelligence.</p> <p>Примечание: Если значение свойства Макс. размер символьного потока превышено, документ Web Intelligence создан не будет и клиент получит сообщение об ошибке.</p>	<p>5</p> <p>Допустимым диапазоном является от 1 до 65535 Мбайт.</p>
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>	<p>50</p> <p>Допустимым диапазоном является от 1 до 65535 Мбайт.</p>
Каталог изображений	Определяет расположение каталога изображений.	(пустой)
Выходной каталог кэша	Определяет расположение кэша.	(пустой)

Таблица 30-65: 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.	86400

См. также

- [Параметры пороговых значений серверной памяти Web Intelligence](#)

30.1.7.1 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 соединений 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:

$$4500\text{МБ} - .20 \times 4500\text{МБ} = 3600\text{МБ}$$

- 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.

30.1.8 Свойства служб Dashboards**Свойства кэш-сервера Dashboards**

Таблица 30-66: Свойства службы кэша Dashboards

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.
Время простоя соединения (мин)	Определяет период времени (в минутах), в течение которого кэш-сервер Dashboards 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
Время ожидания кэша безопасности (мин)	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.	Xmx858M

Свойства сервера обработки Dashboards

Таблица 30-67: Свойства службы обработки Dashboards

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 10000.

2013-07-02

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"

31.1 0 приложении "Показатели сервера"

Если не указано иное, в этом приложении термин "сервер" обозначает сервер SAP BusinessObjects, а не компьютер, на котором установлена или выполняется платформа SAP BusinessObjects Business Intelligence .

Показатели сервера недоступны на серверах, которые не работают.

Приложение мониторинга поддерживает показатели, описываемые в этом приложении, а также отслеживание следующих состояний сервера:

Состояние сервера	Описание
Состояние работоспособности	Состояние работоспособности указывает общую работоспособность сервера. Возможные значения: <ul style="list-style-type: none"> • 0 = красный (Осторожно) • 1 = янтарный (Внимание) • 2 = зеленый (Работает нормально)
Состояние включения сервера	Это состояние указывает, включен или выключен сервер. Возможные значения: <ul style="list-style-type: none"> • 0 = отключено • 1 = включено
Состояние работы сервера	Это состояние указывает состояние работы сервера. Возможные значения: <ul style="list-style-type: none"> • 0 = ОСТАНОВЛЕНО • 1 = ЗАПУСК • 2 = ИНИЦИАЛИЗАЦИЯ • 3 = ВЫПОЛНЕНИЕ • 4 = ОСТАНОВКА • 5 = СБОЙ • 6 = ВЫПОЛНЕНИЕ С ОШИБКАМИ • 7 = ВЫПОЛНЕНИЕ С ПРЕДУПРЕЖДЕНИЯМИ

См. также

- [Анализ серверных показателей](#)

31.1.1 Общие показатели сервера

Приведенные ниже показатели относятся к компьютеру, на котором работает указанный сервер.

Таблица 31-2: 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).
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 SAP BusinessObjects Business Intelligence. 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 SAP BusinessObjects Business Intelligence. Учитывается пространство, которое занимает сама платформа SAP BusinessObjects Business Intelligence 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 31-3: 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.
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 31-4: 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 31-5: Регистрация показателей службы

Показатель	Описание
Каталог протоколирования	Файлы журналов для сервера, доступные в этом местоположении.

31.1.2 Показатели центрального сервера управления

В таблице ниже приведены показатели сервера, которые отображаются на экране «Показатели» центральных серверов управления (CMS).

Таблица 31-6: Показатели центрального сервера управления

Показатель	Описание
Соединение с базой данных аудита установлено	<p>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.</p>

Показатель	Описание
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 экрана «Показатели». Если это значение приходится на время, более чем на два часа раньше времени загрузки страницы, возможно, это признак неправильной работы аудита.
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>

Показатель	Описание
Кластеризованные серверы CMS	Разделяемый точками с запятыми список имен хостов и номеров портов выполняющихся центральных серверов управления 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	Общее 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.
Число сеансов, установленных серверами	Число параллельных сеансов, созданных серверами платформы SAP BusinessObjects Business Intelligence с 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	Число невыполненных заданий в системе.
Отложенные задания	Количество заданий, которые запланированы, но не готовы к запуску, так как запланированное время не наступило или не произошло нужное событие.
Выполняющиеся задания	Количество заданий, запущенных в настоящее время.
Завершенные задания	Число выполненных заданий в системе.
Ожидающие задания	Число заданий в системе, которые были запланированы и ожидают свободных 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 соединения с системной базой 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.

Показатель	Описание
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.
Номер построения	Номер построения CMS. С помощью этого номера можно определить установленную версию платформы SAP BusinessObjects Business Intelligence.
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	Общее 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 подключений к базе данных стабильно ниже, чем число системных подключений к базе данных, указанное в свойстве Запросы соединений с системной БД (область «Central Management Service» на экране «Свойства»), это может говорить о том, что службе CMS не удастся получить дополнительные подключения, а значит, система не функционирует в оптимальном режиме. 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	Общее текущее число объектов, которые содержатся в системном кэше CMS.
Число объектов в системной БД CMS	Общее текущее число объектов, которые содержатся в системной базе данных CMS.
Существующие учетные записи пользователей с лицензиями на параллельный доступ	Общее число существующих в кластере пользователей с лицензиями на параллельный доступ.
Существующие учетные записи именованных пользователей	Общее число имеющихся в кластере пользователей с именованными лицензиями на параллельный доступ.

31.1.3 Показатели сервера соединений

Для сервера соединений характерны следующие показатели.

Таблица 31-7: 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>

31.1.4 Показатели сервера событий

В следующей таблице приведены показатели сервера, которые отображаются на экране «Показатели» серверов событий.

Таблица 31-8: 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	Общее число файлов, которые отслеживаются сервером событий.

31.1.5 Показатели сервера репозитория файлов

В следующей таблице приведены показатели сервера, которые отображаются на экране «Показатели» серверов репозитория входных и выходных файлов.

Таблица 31-9: Показатели службы хранилища файлов

Показатель	Описание
Активные файлы	Число файлов на сервере репозитория файлов, к которым в данный момент осуществляется доступ.
Записано данных (Мбайт)	Общее количество мегабайтов, записанных в файлы на сервере.
Передано данных (Мбайт)	Общее 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	Общее 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).
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).

31.1.6 Показатели адаптивного сервера обработки

В следующей таблице приведены показатели сервера, которые отображаются на экране «Показатели» адаптивного сервера обработки.

Таблица 31-10: 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.
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.

Показатель	Описание
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 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>
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 свидетельствовать 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.

Показатель	Описание
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 31-11: 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 31-12: Показатели службы прокси аудита клиента

Показатель	Описание
Число событий аудита, полученных с момента запуска сервера	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 31-13: 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.
Метка времени последнего обновления индекса	Дата и время последнего обновления индекса.
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.
Выполняемая индексация	TRUE, если выполняется индексация. В противном случае – значение FALSE.
Число индексируемых документов	Отображений числа документов, индексируемых с момента запуска службы.

Таблица 31-14: Показатели службы Multi-Dimensional analysis service

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 31-15: Показатели службы объединения данных

Показатель	Описание
Число выполняющихся запросов	Число выполняющихся запросов (использующих или не использующих память).
Число соединений	Общее число соединений пользователей к подсистеме запросов объединения данных.

Показатель	Описание
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).
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 соединений	Общее число блоков соединений, загруженных в службу.

Показатель	Описание
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».

Таблица 31-16: Показатели службы соединений

Показатель	Описание
Источники данных	<p>Списки в таблице являются источниками данных, активируемыми на странице «Свойства». Выводится следующая информация для каждой пары сетевого уровня и базы данных:</p> <ul style="list-style-type: none"> • Состояние («Загружено» или «Сбой»): текущий статус драйвера • Доступные соединения: число соединений пула, которые могут использоваться • Задания (CORBA): число обрабатываемых заданий (развертывание 2-го уровня) • Задания (HTTP): число обрабатываемых заданий (развертывание веб-уровня) <p>Для получения дополнительных сведений о пулах соединений см. <i>руководство по доступу к данным</i>.</p>

Таблица 31-17: Показатели службы мониторинга

Показатель	Описание
Среднее время вычисления состояния наблюдения для последних 15 циклов (мс)	Среднее время, затрачиваемое на вычисление состояния наблюдения за последние 15 циклов для заданного экземпляра службы мониторинга.
Число показателей, созданных пользователем	Общее число созданных всеми пользователями показателей в кластере.
Число наблюдений	Общее число наблюдений, в том числе отключенных и включенных, в кластере.
serviceBean.monitoringAppPropEnabled	Принимает значение TRUE, если приложение мониторинга включено. В противном случае – значение FALSE. Этот показатель совпадает с настройкой на странице "Свойства приложения мониторинга" в консоли СМС.

Показатель	Описание
Интервал обновления показателей мониторинга (секунды)	Интервал обновления, заданный для текущего экземпляра службы мониторинга. При запуске службы этому показателю присваивается значение, установленное на странице "Свойства приложения мониторинга" в консоли СМС в соответствующий момент времени. В другие моменты значение показателя может отличаться от настройки, установленной на странице СМС.
Доступная служба	Принимает значение TRUE, если эта служба мониторинга активна. В противном случае – значение FALSE. В кластере одновременно может быть активна только одна служба мониторинга.
Число показателей тренда	Общее число показателей, записываемых в базу данных мониторинга.

Таблица 31-18: Показатели службы веб-приложений ВЕх

Показатель	Описание
Число сеансов	Общее число активных сеансов в службе веб-приложений ВЕх.

31.1.7 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 31-19: 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

Показатель	Описание
Ошибка запуска одного или нескольких соединителей WACS	Показывает, имеются ли отказавшие соединители. При значении 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](#)

31.1.8 Показатели адаптивного сервера заданий

Таблица 31-20: 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.
Создания заданий, завершившиеся сбоем	Количество заданий на сервере, в которых возникали 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».

Показатель	Описание
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.
Установка по умолчанию адресатов SAP StreamWork допустима	Принимает значение «TRUE», если сервер может отправлять объекты в целевую папку SAP StreamWork, указанную в окне «Адресат» сервера. В противном случае этот параметр имеет значение «FALSE».

В следующей таблице описываются показатели для каждой из служб планирования, выполняющихся на сервере.

Таблица 31-21: Показатели службы планирования

Показатель	Описание
Служба планирования	Имя службы.
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.

Показатель	Описание
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 31-22: 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.
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».

31.1.9 Показатели Crystal Reports Server

В следующей таблице приведены показатели сервера, которые отображаются на экране «Показатели» для серверов Crystal Reports Processing и Crystal Reports 2013 Processing.

Таблица 31-23: 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.
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.

Показатель	Описание
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.
Максимальное 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 31-24: 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.

Показатель	Описание
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.
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 2013.

Таблица 31-25: Показатели сервера приложений отчетов Crystal Reports 2013

Показатель	Описание
metric_currentdoccount Примечание: Этот показатель отображается на странице "Мониторинг" консоли СМС как «document_s_».	Количество документов, обрабатываемых в настоящий момент сервером.
metric_totaldoccount Примечание: Этот показатель отображается на странице "Мониторинг" консоли СМС как «document_s_».	Количество документов, обработанных сервером с момента его запуска.
metric_currentagentthreadcount Примечание: Этот показатель отображается на странице "Мониторинг" консоли СМС как «agent thread_s_».	Количество потоков, обрабатываемых в настоящий момент сервером.
metric_totalagentthreadcount Примечание: Этот показатель отображается на странице "Мониторинг" консоли СМС как «agent thread_s_».	Количество потоков, обработанных сервером с момента его запуска.

31.1.10 Показатели сервера Web Intelligence

Таблица 31-26: 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.
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.
Число удаленных ошибок расширения	Количество неудачных попыток соединения с удаленной службой расширения, расположенной на адаптивном сервере обработки.
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.

Показатель	Описание
Текущее число активных сеансов	Текущее число сеансов, которые могут принять запросы от клиентов.
Число документов, открытых из кэша	Число документов, для которых результат последнего запроса считан напрямую из кэша.
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 истечений времени ожидания сеансов	Число сеансов, для которых истекло время ожидания с момента запуска сервера.
Общее число сеансов	Число сеансов, созданных на сервере с момента его запуска.
Число пользователей	Общее число пользователей, подключенных к серверу.
Число активных потоков	Число потоков, обслуживающих запросы, которые получены сервером (пул асинхронных потоков).
Общее число потоков	Общее число потоков, созданных с момента запуска сервера (пул асинхронных потоков).

31.1.11 Показатели сервера Dashboards

Таблица 31-27: Показатели сервера обработки Dashboards

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.

Показатель	Описание
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.
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.
Максимальное число дочерних процессов	Максимальное число параллельных дочерних процессов, разрешенное на сервере.

Таблица 31-28: 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 Dashboards в данной системе. 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.
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

32.1 Заполнители сервера и узлов

За исключением «%SERVER_FRIENDLY_NAME%» и «%SERVER_NAME%», эти заполнители относятся ко всем серверам на одном узле.

Таблица 32-1: Заполнители

Заполнитель	Описание	Значения по умолчанию
%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, в которой расположены двоичные файлы 64-битной версии платформы SAP BusinessObjects Business Intelligence.	В Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64 В UNIX: <INSTALLDIR/sap_bj/enterprise_xi40/platform/
%BINDIR32%	Папка, в которой расположены двоичные файлы 32-битной версии платформы SAP BusinessObjects Business Intelligence.	В Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86. В UNIX: <INSTALLDIR/sap_bj/enterprise_xi40/platform/
%CACHESERVER_EXE%	Имя исполняемого файла кэш-сервера Crystal Reports.	В ОС Windows это crcache.exe. В ОС Unix: boe_crcached.bin.
%CMS_EXE%	Имя выполняемого файла центрального сервера управления.	В ОС Windows это cms.exe. В ОС UNIX это boe_cmds.
%CONNECTIONSERVER32_EXE%	Имя выполняемого файла для 32-битного сервера соединений.	В Windows, ConnectionServer32.exe. В UNIX, ConnectionServer32.

Заполнитель	Описание	Значения по умолчанию
%CONNECTIONSERVER_DIR%	Корневая папка сервера соединений.	В Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer. В UNIX: <INSTALLDIR>/sapobj/enterprise_xi4/dataAccess/connectionServer
%CONNECTIONSERVER_EXE%	Имя выполняемого файла для 64-битного сервера соединений.	В OC Windows это ConnectionServer.exe. В UNIX это ConnectionServer.
%CR2011_BINDIR%	Каталог, где расположены двоичные файлы сервера Crystal Reports 2011.	В Windows: <INSTALLDIR>\SAP BusinessObjectsEnterprise XI 4.0\win32_x86. В UNIX каталог будет аналогичным следующему: <INSTALLDIR>/sapobj/enterprise_xi4/dataAccess/bin/sapcr00
%CR2011_DefaultWorkingDir%	Рабочий каталог по умолчанию для серверов Crystal Reports 2011.	В Windows: <INSTALLDIR>\SAP BusinessObjectsEnterprise XI 4.0\win32_x86. В UNIX каталог будет аналогичным следующему: <INSTALLDIR>/sapobj/enterprise_xi4/dataAccess/bin/sapcr00
%CRYSTALRAS_EXE%	Имя выполняемого файла сервера Report Application Server.	В OC Windows это crystalras.exe. В OC UNIX это boe_crystalrasd.
%CR_ODBCINI%	Полное имя (включая путь) файла .odbc.ini. **	В UNIX, <INSTALLDIR>/sapobj/odbc.ini. Для Windows это пустая строка.
%CommonJavaBundlesDir%	Папка, где находится OSGI.	В OC Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bundles. В Unix: <INSTALLDIR>/sapobj/enterprise_xi4/java/lib/bundles
%CommonJavaLibDir%	Папка, где находятся общие библиотеки Java.	В Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib. В Unix: <INSTALLDIR>/sapobj/enterprise_xi4/java/lib
%DLLEXT%	Расширение по умолчанию DLL-или SO-файла.	В OC Windows это .dll. В OC UNIX это .so.

Заполнитель	Описание	Значения по умолчанию
%DLLPATH%	На компьютере с установленной платформой SAP BusinessObjects Business Intelligence это имя переменной среды, обозначающей каталоги, в которых интерпретатором будет выполняться поиск исполняемых файлов.	В ОС Windows это «Path». В ОС UNIX это «LD_LIBRARY_PATH».
%DLLPATH32%	В 32-битных системах Solaris, на компьютере с установленной платформой SAP BusinessObjects Business Intelligence, это имя переменной среды, обозначающей каталоги, в которых интерпретатором будет выполняться поиск исполняемых файлов.	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 SAP BusinessObjects Business Intelligence, это имя переменной среды, обозначающей каталоги, в которых интерпретатором будет выполняться поиск исполняемых файлов.	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.
%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 «:».

Заполнитель	Описание	Значения по умолчанию
%DefaultAuditingDir%	Каталог, куда записываются временные файлы аудита. Для оптимизации производительности это местоположение должно быть на локальном диске сервера.	В Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Auditing. В UNIX это <INSTALLDIR>/sap_bobj/data/Auditing/.
%DefaultDataDir%	Временный каталог, используемый сервером заданий.	В Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Data. В UNIX это <INSTALLDIR>/sap_bobj/data/.
%DefaultInputFRSDir%	Корневая папка на сервере репозитория входных файлов.	В Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\FileStore\Input. В UNIX это <INSTALLDIR>/sap_bobj/data/frsinput.
%DefaultLoggingDir%	Местоположение, где хранятся файлы журнала.	В Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging. В UNIX это <INSTALLDIR>/sap_bobj/logging.
%DefaultOutputFRSDir%	Корневая папка на сервере репозитория выходных файлов.	В Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\FileStore\Output. В UNIX это <INSTALLDIR>/sap_bobj/data/frsoutput.
%DefaultWorkingDir%	Рабочий каталог для 64-битных серверов.	В Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64 В UNIX это <INSTALLDIR>/sap_bobj/enterprise_xi40/platform
%DefaultWorkingDir32%	Рабочий каталог для 32-битных серверов.	В Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 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 ОС Windows это EventServer.exe. В ОС UNIX это boe_eventsd.

Заполнитель	Описание	Значения по умолчанию
%EXEEXT%	Расширение по умолчанию исполняемых файлов.	В ОС Windows это .exe. В ОС UNIX этот заполнитель не используется.
%EXEPATH%	На компьютере с установленной платформой SAP BusinessObjects Business Intelligence, это имя переменной среды, обозначающей каталоги, в которых интерпретатором будет выполняться поиск исполняемых файлов.	В ОС Windows это «Path». В ОС UNIX это «PATH».
%EnterpriseDir%	Местоположение, в котором установлена 64-битная версия платформы SAP BusinessObjects Business Intelligence platform.	В Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\ . В UNIX это <INSTALLDIR>/sap_bobj/enterprise_xi40.
%EnterpriseDir32%	Местоположение, в котором установлена 32-битная версия платформы SAP BusinessObjects Business Intelligence platform.	В Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\ . В UNIX, <INSTALLDIR>/sap_bobj/enterprise_xi40.
%ExternalJavaLibDir%	Папка, где находятся внешние библиотеки Java сторонних организаций.	В Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\external. В UNIX: <INSTALLDIR>/sap_bobj/enterprise_xi40/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, в которой установлена 64-битная версия платформы SAP BusinessObjects Business Intelligence.	Это значение задается во время установки.
%INSTALLROOTDIR32%	Папка, в которой установлена 32-битная версия платформы SAP BusinessObjects Business Intelligence.	Это значение задается во время установки.

Заполнитель	Описание	Значения по умолчанию
<code>%IntroscopeAgentEnableInstrumentation%</code>	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 SAP BusinessObjects Business Intelligence.
<code>%IntroscopeAgentEnterpriseManagerHost%</code>	Имя хоста диспетчера Introscope Agent Enterprise, куда отправляются данные инструментальных средств.	Это значение задается во время установки.
<code>%IntroscopeAgentEnterpriseManagerPort%</code>	Имя хоста диспетчера Introscope Agent Enterprise, куда отправляются данные инструментальных средств.	Это значение задается во время установки.
<code>%IntroscopeAgentEnterpriseManagerTransport%</code>	Транспорт, используемый при отправке данных инструментальных средств диспетчеру Introscope Agent Enterprise. Допустимые значения: <ul style="list-style-type: none"> • TCP • HTTP • HTTPS • SSL 	TCP
<code>%IntroscopeAgentEnterpriseManagerTransportHTTP%</code>	Класс, используемый при отправке данных инструментальных средств диспетчеру Introscope Agent Enterprise через HTTP.	<code>com.wily.introscope.agent.transport.http.HttpURLConnectionFactory</code>
<code>%IntroscopeAgentEnterpriseManagerTransportHTTPS%</code>	Класс, используемый при отправке данных инструментальных средств диспетчеру Introscope Agent Enterprise через HTTPS.	<code>com.wily.introscope.agent.transport.https.HttpURLConnectionFactory</code>
<code>%IntroscopeAgentEnterpriseManagerTransportSSL%</code>	Класс, используемый при отправке данных инструментальных средств диспетчеру Introscope Agent Enterprise через SSL.	<code>com.wily.introscope.agent.transport.ssl.SSLURLConnectionFactory</code>
<code>%IntroscopeAgentEnterpriseManagerTransportTCP%</code>	Класс, используемый при отправке данных инструментальных средств диспетчеру Introscope Agent Enterprise через TCP.	<code>com.wily.introscope.agent.transport.tcp.DefaultURLConnectionFactory</code>

Заполнитель	Описание	Значения по умолчанию
%IntroscopeDir%	Папка, в которой установлен Introscope Agent Enterprise Manager.	B Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\wily. B UNIX: <INSTALLDIR>/sap_bobj/enterprise_xi40/java/wily
%JAVAW_EXE%	Имя исполняемого файла для виртуальной машины Java, в которой нет окна консоли.	B OC Windows это javaw.exe. B OC UNIX это java.
%JAVA_EXE%	Имя исполняемого файла для виртуальной машины Java.	B OC Windows это java.exe. B OC UNIX это java.
%JOBSEVERCHILD_EXE%	Имя исполняемого файла дочернего настраиваемого сервера заданий.	B OC Windows это JobServerChild.exe. B OC UNIX это boe_jobcd.
%JOBSEVER_EXE%	Имя исполняемого файла настраиваемого сервера заданий.	B OC Windows это JobServer.exe. B OC UNIX это boe_jobsd.
%JdkBinDir%	Папка, где находятся двоичные файлы JDK.	B Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin. B UNIX: <INSTALLDIR>/sap_bobj/<PLATFORM>/sapjvm/bin
%JreBinDir%	Папка, где находятся двоичные файлы JRE.	B Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\bin. B UNIX: <INSTALLDIR>/sap_bobj/<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.	B OC Windows - Djava.awt.headless=false. B OC UNIX -Djava.awt.headless=true

Заполнитель	Описание	Значения по умолчанию
%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.	B Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Languages. B UNIX: <INSTALLDIR>\sap_bobj\enterprise_xi40\languages/
%LANGUAGEPACKSDIR32%	Папка, в которой установлены языковые пакеты развертывания в 32-битных системах.	. B Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Languages. B UNIX: <INSTALLDIR>\sap_bobj\enterprise_xi40\languages/
%LSTDir%	Папка, в которой хранятся файлы конфигурации LST.	B Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\lst. B UNIX это <INSTALLDIR>\sap_bobj\enterprise_xi40\conf\lst
%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.	По умолчанию используется значение 0.
%PAGESERVER_EXE%	Имя исполняемого файла сервера обработки Crystal Reports 2011.	B OC Windows это crproc.exe. B UNIX это boe_crprocd.bin.
%PJSContainerDir%	Папка, в которой расположены JAR-файлы контейнера APS.	B Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container. B UNIX: <INSTALLDIR>\sap_bobj\enterprise_xi40\java\pjs/container
%PJSServicesDir%	Папка, в которой расположены JAR-файлы службы APS.	B Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services. B UNIX: <INSTALLDIR>\sap_bobj\enterprise_xi40\java\pjs/services

Заполнитель	Описание	Значения по умолчанию
%Platform%	Операционная система компьютера, на котором выполняется платформа SAP BusinessObjects Business Intelligence.	Операционная система компьютера, на котором выполняется платформа SAP BusinessObjects Business Intelligence.
%Platform32%	Операционная система компьютера, на котором выполняется 32-битная версия платформы SAP BusinessObjects Business Intelligence.	Операционная система компьютера, на котором выполняется платформа SAP BusinessObjects Business Intelligence.
%RasBinDir%	Корневая папка сервера приложений отчетов.	В Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86. В UNIX, <INSTALLDIR/sapobj/enterprise_xi40/HAIOM/ras
%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 Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\BO_trace.ini. В UNIX: <INSTALLDIR/sapobj/enterprise_xi40/conf/BO-trace.ini.
%WarFilesDir%	Местоположение файлов веб-приложений.	В Windows: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps. В UNIX: <INSTALLDIR/sapobj/enterprise_xi40/warfiles/webapps
%WEBI_LD_PRELOAD%	Имя переменной среды LD_PRELOAD для платформы.	\$LD_PRELOAD\$
%WEBISERVER_EXE%	Имя исполняемого файла сервера обработки Web Intelligence.	В ОС Windows это wireportserver.exe. В ОС UNIX это WIReportServer.

Заполнитель	Описание	Значения по умолчанию
%WEBI_LD_PRELOAD_ONCE%	Имя переменной среды LD_PRELOAD_ONCE для платформы.	\$LD_PRELOAD_ONCE\$
%XCCACHE_EXE%	Имя исполняемого файла кэш-сервера Dashboards.	В ОС Windows это <code>xccache.exe</code> . В UNIX. <code>boe_xccached</code> .
%XCPROC_EXE%	Имя исполняемого файла для сервера обработки Dashboards.	В ОС Windows это <code>xcproc.exe</code> . В UNIX это <code>boe_xcprocd</code> .

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

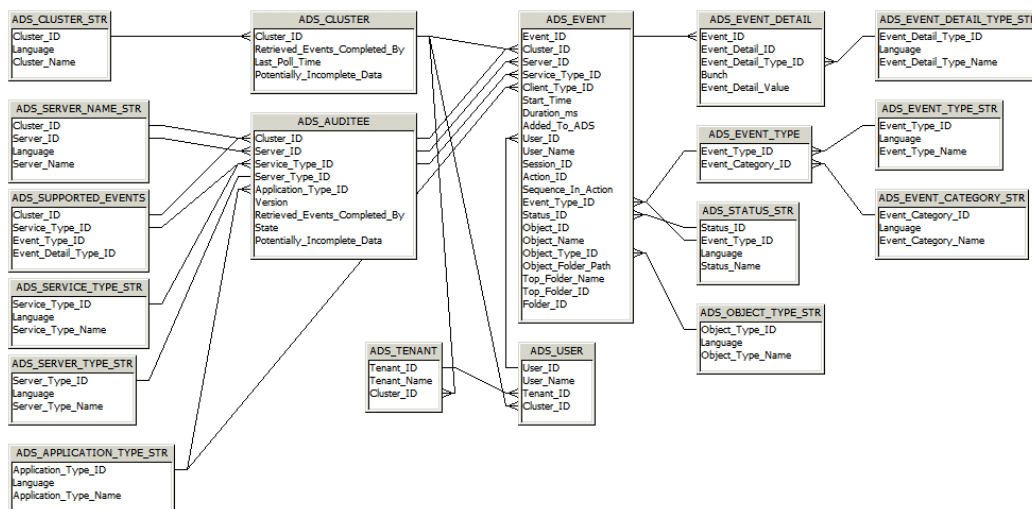
- [Просмотр и изменение заполнителей для узла](#)

Приложение выполнения аудита схемы склада данных

33.1 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.

33.2 Диаграмма схемы



33.3 Таблицы аудита склада данных

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_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.
Server_ID	Символ (64)	<ul style="list-style-type: none"> Основной ключ Внешний ключ (из ADS_SERVER) 	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 Внешний ключ (из ADS_SERVICE) 	CUID типа службы для службы, запустившей событие. События, запущенные клиентом, записывают CUID типа приложения.
Server_Type_ID	Символ (64)	<ul style="list-style-type: none"> Основной ключ Внешний ключ (из ADS_SERVER) 	CUID типа сервера для сервера, запустившего событие.
Код Application_Type_ID	Символ (64)	<ul style="list-style-type: none"> Основной ключ Внешний ключ (из ADS_APPLICATION) 	CUID типа приложения для клиента, запустившего событие. Для событий сервера записывается идентификатор типа службы.

Имя столбца	Тип	Ключ	Описание
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_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 Внешний ключ (из ADS_USERS) 	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)	Основной ключ	Код настройки языка для кластера, например <i>EN</i> или <i>DE</i> .
Cluster_Name	Символ (255)	Нет данных	Имя кластера.

Таблица ADS_EVENT

Данная таблица содержит основные свойства каждого события и является основным моментом 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 (из ADS_CLUSTER)	GUID кластера аудита. Записывается, так как несколько кластеров могут использовать одну ADS.
Server_ID	Символ (64)	Внешний ключ (из ADS_SERVER_NAME)	CUID сервера, запустившего событие.

Имя столбца	Тип поля	Ключ	Описание
Service_Type_ID	Символ (64)	Внешний ключ (из ADS_SERVICE_TYPE)	<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 (из ADS_APPLICATION_TYPE)	Содержит идентификатор типа клиента, который установил сеанс.
Start_Time	Дата и время	Нет данных	Дата и время (UTC) 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 (UTC) 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.
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 (из ADS_EVENT_TYPE)	Тип события (например, Просмотр или Сохранить).

Имя столбца	Тип поля	Ключ	Описание
Status_ID	Целое	Внешний ключ (из 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 (из 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_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 EN или DE.

Имя столбца	Тип	Ключ	Описание
Event_Category_Name	Символ (255)	Нет данных	Имя категории события.

ADS_EVENT_DELETES

Не использовать отчеты из этой таблицы. Предназначено только для внутреннего использования системой и может быть исключено в последующих выпусках.

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)	<ul style="list-style-type: none"> Основной ключ Внешний ключ (из ADS_EVENT) 	GUID родительского события.
Event_Detail_Type_ID	Целое	Внешний ключ (из ADS_EVENT)	Тип сведений события.
Набор	Целое	Нет данных	<p>Если сведения являются частью серии, данный параметр используется для их связи.</p> <p>Например, если отчет содержит подсказки 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 подсказки: Страна Значение подсказки: США <p>Второй набор будет содержать:</p> <ul style="list-style-type: none"> Имя подсказки: Штат Значение подсказки: Калифорния Значение подсказки: Невада

Имя столбца	Тип	Ключ	Описание
Event_Detail_Value	Символ (подробный текст)	Нет данных	Значение сведений о событии.

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_EVENT_TYPE

Данная таблица содержит ссылочную запись для различных категорий событий.

Имя столбца	Тип	Ключ	Описание
Event_Type_ID	Целое	<ul style="list-style-type: none"> Основной ключ Внешний ключ (из ADS_EVENT_TYPE_STR) 	Уникальный идентификатор типа события.
Event_Category_ID	Целое	<ul style="list-style-type: none"> Основной ключ Внешний ключ (из 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.

Имя столбца	Тип	Ключ	Описание
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_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_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_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".

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 (из ADS_EVENT_TYPE)	Идентификатор типа записанного события (например, идентификатор "Сохранить").

Имя столбца	Тип	Ключ	Описание
Event_Detail_Type_ID	Целое	Внешний ключ (из ADS_EVENTS ADS_EVENTS)	CUID, идентифицирующий тип сведений события, собранных для данного события (например, Путь к файлу).

Таблица ADS_TENANT

В этой таблице записаны отношения между именами и идентификаторами абонентов.

Имя столбца	Тип	Ключ	Описание
Cluster_ID	Символ (64)	Основной ключ	GUID кластера.
Tenant_ID	Символ (64)	Основной ключ	CUID абонента.
Tenant_Name	Символ (255)	Нет дан- ных	Имя абонента.

Таблица ADS_USER

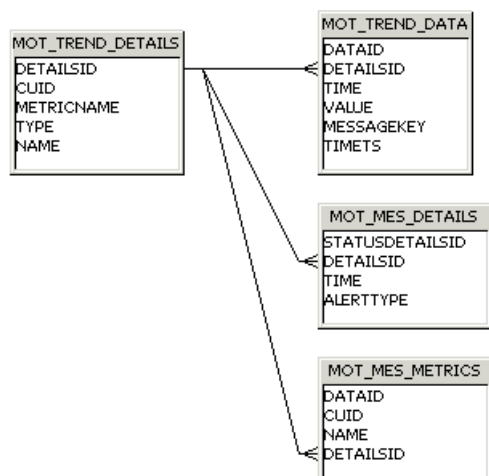
В этой таблице записаны отношения между пользователями и абонентами.

Имя столбца	Тип	Ключ	Описание
Cluster_ID	Символ (64)	Основной ключ	GUID кластера.
User_ID	Символ (64)	Основной ключ	CUID пользователя.
User_Name	Символ (255)	Нет дан- ных	Имя пользователя
Tenant_ID	Символ (64)	Основной ключ	CUID абонента.

Приложение "Мониторинг схемы базы данных"

34.1 Схема базы данных 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.



MOT_TREND_DETAILS

В этой таблице регистрируются сведения об управляемых объектах, тестах и наблюдениях. Например, CUID и имена показателей.

Имя столбца	Тип	Ключ	Описание
DetailsId	INTEGER	Основной ключ Создается автоматически	
CUID	VARCHAR(64)	Нет данных	CUID инфообъекта, который содержит данный показатель или связан с ним
MetricName	VARCHAR(255)	Нет данных	Имя показателя

Имя столбца	Тип	Ключ	Описание
Тип	VARCHAR(32)	Нет данных	"Subscription", "ManagedEntityStatus" или "Probe"
Имя	VARCHAR(255)	Нет данных	Имя наблюдения при типе "ManagedEntityStatus". В обратном случае по умолчанию соответствует строке в поле "Тип", записанной в верхнем регистре, например "PROBE" или "SUBSCRIPTION".

MOT_TREND_DATA

В этой таблице регистрируются данные тенденций из показателей, наблюдений и тестов. Например, значение показателя и время.

Имя столбца	Тип	Ключ	Описание
DataId	INTEGER	Основной ключ Создается автоматически	
DetailsId	INTEGER	Внешний ключ (из MOT_TREND_DETAILS)	
Time или TimeT	BIGINT или NUMBER или FIXED Дата Unix Epoch	Нет данных	Время, когда были собраны данные
Значение	FLOAT или DOUBLE или NUMBER	Нет данных	Значение показателя или подписки
MessageKey	VARCHAR(32)	Нет данных	Ключ сообщения об ошибке либо NULL при успешном завершении. Для наблюдения также доступны значения "watchEnabled" или "watchDisabled". Называется ключом, поскольку в итоге используется для извлечения локализованных сообщений перед отображением ИП.
Метка времени	DATETIME или TIMESTAMP	Нет данных	Время занесения данных в базу

MOT_MES_DETAILS

В этой таблице регистрируются данные о нарушениях подписки и сведения о доставке предупреждений. Например, время нарушения и время доставки предупреждения.

Имя столбца	Тип	Ключ	Описание
StatusDetailsId	INTEGER	Основной ключ Создается автоматически	
DetailsId	INTEGER	Внешний ключ (из MOT_TREND_DETAILS)	
Время	BIGINT или NUMBER Дата Unix Epoch	Нет данных	Время, когда были собраны данные
AlertType	SMALLINT или NUMBER	Нет данных	Тип доставки уведомления о подписке (например, по электронной почте)

MOT_MES_METRICS

В этой таблице записываются данные о метриках, которые принадлежат уравнениям наблюдения. У каждой метрики, которая принадлежит наблюдению, в этой таблице будет одна запись.

Имя столбца	Тип	Ключ	Описание
DataId	INTEGER	Основной ключ Создается автоматически	
DetailsId	INTEGER	Внешний ключ (из MOT_TREND_DETAILS)	
CUID	VARCHAR(64)	Нет данных	CUID наблюдения
Имя	VARCHAR(255)	Нет данных	Имя наблюдения

Приложение "Рабочая таблица системной копии"

35.1 Рабочая таблица системной копии

Свойство	Значение
Ключ кластера.	
Имена узлов.	
Имя компьютера и папка установки платформы BI для каждого компьютера в развертывании.	
Пароль администратора платформы BI.	
Соединения с базой данных CMS, имена пользователей и пароли, связанные с этими соединениями для каждого компьютера в развертывании.	
Соединения с базой данных аудита, имена пользователей и пароли, связанные с этими соединениями для каждого компьютера в развертывании.	
Для каждого компьютера в развертывании — сведения обо всех других клиентских подключениях к базам данных для каждого компьютера в исходной системе, используемого юниверсами и отчетами.	
Для каждого компьютера в развертывании — типы и версии клиентов баз данных.	

Свойство	Значение
Версия, пакет поддержки и уровень исправлений.	
Расположения хранения файлов для каждого репозитория входящих и исходящих файлов FRS в развертывании.	
Если планируется копирование приложения Lifecycle management (LCM), расположение папки базы данных LCM и папок Subversion LCM.	
Если вы планируете копирование базы данных мониторинга, это папка базы данных мониторинга.	
Путь к папке семантического уровня.	

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-sdklibrary
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

"холодное" резервное копирование
525, 529

A

Analysis, выпуск для OLAP 84

B

BackupCluster.bat 536
backupcluster.sh 536
BExWebApplicationsService 672
BIAR файл
 экспорт задания 595
BO_trace.ini
 настройка 928
BOLMT 108
BW
 включение просмотра 874
 интеграция с платформой BI 859
BW Publisher
 настройка в UNIX 862
 настройка в качестве службы 862
 распространение компонентов
 862

C

CA Wily Introscope 45
cacert.der 189, 190
cakey.pem 189, 190
ccm.config 953
ccm.exe 957, 959
ccm.sh 949, 953
 восстановление настроек
 сервера 545
Central Configuration Manager (CCM)
 28, 78
Central Management Console (CMC)
 28, 81
ClearCase 46
CMS 322, 354
 аутентификация 242
 База данных SAP HANA, выбор
 474
 База данных SQL, выбор 473
 вход в систему 586
 добавление в кластер 412

CMS ((продолжение))
 параметры командной строки 962
 переменные сеанса 171
 аутентификация 242
 отслеживание 172
 показатели 422
 распределенная безопасность
 171
 свойства 1034
cmsdbsetup.sh 953
Content Administration Workbench 868
 добавление систем платформы
 BI 868
 обзор публикации отчета 864
 обновление источников данных
 отчетов 873
 определение уровней доступа
 пользователей 865
 публикация отчетов в фоновом
 режиме 873
 синхронизация информации
 отчета 873
 удаление отчетов 874
Crystal Reports
 права 1002
 см. SAP Crystal Reports 80
CTS 582
custom.jsp 693

D

Dashboard Builder 82
Data Access
 обзор установки 877
dumrepo 568

E

env-locale.sh 955
env.sh 955
Explorer 802
 права 1027
 см. SAP BusinessObjects Explorer
 80

F

FIPS-совместимый режим
 Включение UNIX 178
 включение Windows 177

FIPS-совместимый режим
 ((продолжение))
 отключение Windows 178
 параметр безопасности 176
 Федеральный стандарт
 обработки информации 176

G

GWSETUP 863

H

HTTP 171, 242
HTTPS
 настройка серверов контейнера
 веб-приложений (WACS) 492,
 495, 516

I

idm.keytab 511
idm.princ 511
idm.realm 511
InfoView 82
initlaunch.sh 955
INSTALLDIR 24
Introscope 735
IPv6
 настройка адреса в CMC 431
 параметры 428
 CMC 428
ISA 2006
 конфигурация для Oracle 10gR3
 237
 конфигурация для Sun Java 8.2
 237
 конфигурация для Tomcat 5.5 237
 конфигурация для WebSphere
 CE 2.0 237
iView
 включение просмотра 874

J

JAAS, файл конфигурации 299, 300,
 500
Java, Kerberos 302, 303
JD Edwards EnterpriseOne 45
JMX MBeans 732

JMX Remote API 730

K

Kerberos 297, 499

Krb5.ini 500

LDAP 283

единый вход для Java 314, 505

и NetWeaver SSO 300

устранение неполадок 320, 501

файл конфигурации 298, 499

KPI (ключевой показатель
эффективности) 714

Krb5.ini 500

L

LDAP

Secure Sockets Layer (SSL) 262

аутентификация 262

настройка 264

аутентификация Kerberos 283

группы

сопоставление 274

настройка единого входа 273

подключаемый модуль

аутентификации 263

подключаемый модуль

безопасности 263

сопоставление с Windows AD 277

учетные записи 262

устранение неполадок 285

файл конфигурации входа 284

хосты

настройка 264, 269

управление несколькими 267

Live Office

конфигурация для обратных

прокси-серверов 234

logon.csp 242

M

MBean 715

O

ODBC

база данных CMS

взаимодействие 480

odbc.ini

создание для SQL Anywhere 439

OpenDocument

настройка входа в систему 691

OpenSearch 784

OpenSearch с помощью WDeploy 785

Oracle

JAAS 300

Kerberos 298

параметры Java 303

Oracle E-Business Suite 45

сопоставление ролей со

службами информационной

платформы 386

Oracle EBS

обновить псевдонимы 388

обновить роли 388

P

PeopleSoft Enterprise 45

PLATFORM64DIR 24

PlatformServices.properties 413

postinstall.sh 955

PSE

доверительные параметры со

стороны сервера 336

настройка доступа 344

Q

QaaWS 571

Query as a Web Service 75

R

Repository Diagnostic Tool 29

использование

Windows и Unix 978

несогласованность

диагностика и

восстановление 977

объект в файл 977

сценарии 977

обзор 977

параметры 978

таблица несоответствий

рекомендации 986, 988

restart.sh 955

RestoreCluster.bat 545

restorecluster.sh 545

RFC-адресат 863

для локального шлюза SAP 864

для службы BW Publisher 863

S

SAML

SSO 252

SAP

интеграция 45

настройка брандмауэра 220

обновление псевдонимов 334

обновление ролей 334

SAP Business Explorer 671

SAP BusinessObjects Analysis,

выпуск для Microsoft Office 79

SAP BusinessObjects Dashboards 80

SAP BusinessObjects Explorer 80, 655

свойства приложения 655

управление настройками 655

SAP BusinessObjects Mobile 84

SAP BusinessObjects Web Intelligence
83

SAP Crystal Reports 80

SAP ERP 45

SAP HANA

настройка единого входа 278,
676

SAP Jam

права 1015

SAP Jam, интеграция

введение 655

предварительные требования
656

SAP Passport 948

SAP Solution Manager 45

SLD 941

SMD 944

обзор 939

SAP StreamWork

права 1015

SAPGENPSE 344

SCRIPTDIR 24

SDK

Platform Search 783

Secure Network Communication

(SNC), интеграция с

настройки SNC 346

Secure Socket Layer (SSL)

настройка для 910, 913

Secure Sockets Layer (SSL) 172, 189,
193, 194, 195, 262

и LDAP 262

и балансировка нагрузки 171

Server Intelligence Agent 27

зависимости сервера Windows,

добавление 461

узлы 437, 440, 445, 448, 450

воссоздание 445, 446, 447,

448, 449, 450, 456

добавление 441, 442, 443,

444, 456

новый компьютер,

добавление на 441

Server Intelligence Agent
 ((продолжение))
 узлы ((продолжение))
 переименование 451
 перемещение 452, 453, 454,
 455, 458
 удаление 449, 456
 учетные данные
 пользователя, изменение
 для 462
 Server Intelligence Agent (SIA)
 рабочий процесс отключения 87
 serverconfig.sh 954
 узлы
 воссоздание 447
 добавление 443
 переименование 451
 перемещение 454
 удаление 449
 setup.sh 955
 setupinit.sh 955
 Siebel Enterprise 45
 SiteMinder
 Windows AD 315
 настройка WAR-файла BOE 274
 настройка единого входа с
 использованием протокола
 LDAP 273, 315
 настройка подключаемого
 модуля LDAP 273
 ошибка 274
 устранение неполадок 274
 SMD 944
 SMD-агент 944
 SNC
 см. Безопасный сетевой обмен
 данными 336
 Software Development Kit (SDK) 40
 Solution Manager 713
 учетная запись SAdmin 944
 SQL Anywhere
 создание файла odbc.ini 439
 SSL 189, 193, 194, 195
 sslconfig.exe 196
 ключи 189, 190
 конфигурация серверов 189,
 193, 194, 195
 настройка серверов контейнера
 веб-приложений (WACS) 492,
 495
 сертификаты 189, 190
 средство преобразования
 отчетов 197
 средство управления
 переводами 196
 толстые клиенты 196

SSL, настройка для 922
 SSL. См. Secure Sockets Layer (SSL)
 262
 sslc.cnf 189
 sslc.exe 189
 stopservers 955
 Strategy Builder, права 1022
 syslog 423
 System Landscape Directory (SLD) 45
 запуски 942
 проверка регистрации 943
 регистрация 941
 файл connect.key 942

T

Tomcat
 JAAS 299
 Kerberos 298

U

Universe Designer
 см. Средство создания
 юниверсов 74
 UNIX
 syslog 423

V

Voyager 84
 см. SAP BusinessObjects Analysis
 79

W

war-файл BOE 126
 WDeploy 81
 Web Intelligence 650, 967
 настройка интерфейса 694
 права 1019
 права доступа к HTML-запросам
 650
 права приложения 650
 Сервер обработки 971
 Web Intelligence Rich Client 73
 WebLogic
 Kerberos 298
 параметры Java 302
 файл конфигурации JAAS 299
 WebSphere
 JAAS 300
 параметры Java 303
 WinAD 573

Windows
 журнал событий 423
 зависимости сервера,
 добавление 461
 Windows AD
 Vintela 309, 310
 активация Kerberos 497, 498
 аутентификация 285
 единый вход 307, 309, 310
 подключаемый модуль
 безопасности 288
 сопоставление LDAP 277
 учетная запись службы 307
 учетные записи и группы 293
 планирование обновлений
 293

X

Xcelsius. См. SAP BusinessObjects
 Dashboards 80

A

автоматический запуск серверов 97,
 404
 авторизации
 Content Administration Workbench
 865
 для доступа к данным SAP 888
 для служб информационной
 платформы 322
 права на платформе BI 859
 применение 888
 агент Server Intelligence
 автоматический запуск серверов
 404
 Агент Server Intelligence (SIA)
 рабочий процесс запуска 86
 Агент мониторинга 732
 Адаптивный сервер заданий 25, 47,
 1034, 1106
 время ожидания сокета 851
 параметры командной строки 967
 Адаптивный сервер обработки 25,
 47, 715
 администрирование
 входящие 126
 группы 125
 делегирование 160
 назначение прав 391
 пользователи 125
 права 160
 приложения 634
 серверы и группы серверов 419
 CMC 634

администрирование *((продолжение))*
 стартовая панель BI 634
 администрирование веб-служб
 RESTful
 TrustedPrincipal.conf 513
 web.xml 511
 включение стека сообщений об
 ошибках 507
 время ожидания пула сеансов
 509
 настройка базового URL-адреса
 506
 настройка времени ожидания
 маркера сеанса 508
 настройка размера страницы по
 умолчанию 508
 параметры командной строки 507
 параметры командной строки
 для доверительной
 аутентификации 514
 пул сеансов 509
 размер пула сеансов 509
 активные данные 153
 активные доверительные отношения
 169
 анализ 79
 анонимный единый вход 244
 аппаратное резервное копирование
 525, 529
 архитектура 33, 715
 Поиск по платформе 793
 атрибуты, маркеры входа 170
 аудит
 идентификатор сведений о
 событии 764, 774, 777, 778,
 779
 идентификатор типа события
 764, 774, 777, 778, 779
 настройка 747
 общие события 764
 параметры соединения базы
 данных 751
 показатели 747
 сведения о событии 764, 774,
 777, 778, 779
 сводка состояния 747
 свойства события 764, 777, 778,
 779
 события
 настройка 749
 события 753
 сохранение базы данных 751
 список 753
 события Analyzer 778
 события Web Intelligence 777

аудит *((продолжение))*
 события консоли управления
 жизненным циклом 779
 события платформы 774
 Страница CMC 747
 типы событий 764
 Блокировка VMS 779
 Возврат VMS 779
 выход за пределы области
 действия при переходе по
 иерархии 777
 Добавление VMS 779
 Извлечение VMS 779
 изменение аудита 774
 изменение прав 774
 Изъятие VMS 779
 откат 779
 пользовательский уровень
 доступа изменен 774
 Разблокирование VMS 779
 Сеанс MDAS 778
 Соединение с кубом MDAS
 778
 страница извлечена 777
 Экспорт VMS 779
 типы событий:вход в систему 764
 типы событий:выполнение 764
 типы событий:выход из системы
 764
 типы событий:доставка 764
 типы событий:изменение 764
 типы событий:подсказка 764
 типы событий:поиск 764
 типы событий:получение 764
 типы событий:просмотр 764
 типы событий:редактирование
 764
 типы событий:создание 764
 типы событий:сохранение 764
 типы событий:триггер 764
 типы событий:удаление 764
 хранилище данных аудита
 диаграмма схемы 1127
 таблицы схемы 1128
 Аудит 571
 аудит лицензий 108
 процедура 109
 аутентификация 43
 enterprise 246
 LDAP 262, 263
 Windows AD 285
 Доверительная аутентификация
 250
 основная 242
 подключаемые модули
 безопасности 243

аутентификация *((продолжение))*
 Сервер контейнера
 веб-приложений (WACS) 497
 типы 113
 Аутентификация
 Enterprise 573
 LDAP 573
 Windows AD 573
 Аутентификация SAP 322
 параметры CMC 326

Б

база данных Derby, миграция 719
 база данных SAP HANA
 выбор для CMS 474
 База данных SQL Anywhere
 выбор для CMS 473
 база данных аудита 530
 база данных аудита, миграция базы
 Derby 719
 база данных системы CMS 473, 474,
 475, 476, 477
 База данных SAP HANA, выбор
 474
 База данных SQL Anywhere,
 выбор 473
 воссоздание 477, 478, 479
 выбор 475, 476, 477
 изменение пароля 475
 копирование 480, 481
 удаление 477, 478, 479
 база данных системы центрального
 сервера управления
 создание резервной копии 530
 База данных тенденций 715
 база данных тенденций, миграция
 719
 база данных, миграция Derby 719
 базовая аутентификация HTTP 509
 базы данных 37
 база данных SAP HANA 474
 База данных SQL Anywhere 473
 выбор для CMS 475, 476, 477
 доступ с единым входом 245
 инициализация CMS 477, 478,
 479
 представления 43
 юниверс 42
 балансировка загрузки 171
 добавление CMS 412
 и распределенная безопасность
 171
 кластеризация 411
 Серверы контейнера
 веб-приложений (WACS) 515

безопасности
 подключаемые модули 44
 безопасность 43, 361, 391, 860
 активные доверительные отношения 169
 аудит действий через Интернет 173
 брандмауэры 173
 веб-браузер с веб-сервером 172
 веб-серверы 172
 запросы 148, 149
 защита от попыток выполнения входа злоумышленником 174
 защита среды 172
 импорт настроек 361
 на платформе BI 859
 настройка прав 391
 обработка расширений 175
 объекты юниверса 1010
 ограничения 175
 ограничения для пароля 174
 ограничения для пользователя 175
 ограничения на вход 174
 ограничения учетной записи гостя 175
 отслеживание сеансов 171
 папки верхнего уровня 147
 подключаемые модули 44, 243
 применение 365
 распределенный 171
 управление 145
 управление настройками 365
 уровень папок 859
 шаблоны по умолчанию 860
 безопасность данных
 FIPS-совместимый режим 176
 двухключевая криптография 176
 обзор 176
 обратная совместимость 176
 режим обработки данных по умолчанию 176
 безопасность низкого уровня, обработка расширений 175
 безопасность объекта юниверса 1010
 Безопасный сетевой обмен данными
 библиотека шифрования SAP 336
 группы серверов 345
 клиент относительно сервера 336
 конфигурация SAP 338
 конфигурация серверов 343
 многопроходные публикации 346
 настройки CMC 344

Безопасный сетевой обмен данными *((продолжение))*
 рабочий процесс 341
 серверы платформы BI 336
 создание PSE 342
 установка среды 341
 брандмауэры 173
 конфигурация
 Интеграция SAP 220
 настройка 209
 для интеграции с Oracle E-Business 224
 настройка для JD Edwards EnterpriseOne 222
 настройка для PeopleSoft Enterprise 224
 настройка для интеграции с Siebel 226
 обмен данными между серверами, и 198
 отладка 213, 214
 принудительная регистрация серверов по имени 437
 Сервер контейнера веб-приложений (WACS) 516
 сценарии настройки 214

В

веб-клиенты 72
 веб-приложения BEx 671
 веб-серверы
 защита 172
 веб-служба 582
 веб-службы
 добавление на сервер Web Application Container Server 491
 конфигурация для обратных прокси-серверов 234, 236
 кэширование файлов 843, 844
 настраиваемое развертывание 843, 844
 переменная сеанса 843
 удаление с сервера Web Application Container Server 492
 веб-службы RESTful 506
 версии 571
 верхний уровень
 папки, права 147
 виджеты
 права 1025
 управление настройками 655

Виджеты BI
 см. виджеты для платформы SAP BusinessObjects Business Intelligence 77
 виджеты для платформы SAP BusinessObjects Business Intelligence 77
 включение
 серверы 406, 407
 владельцы учетных записей
 назначение прав 146
 назначение расширенных прав 147
 права просмотра для 145
 права, на папки верхнего уровня 147
 проверка прав 148, 149
 войти
 новый CMS 586
 восстановление
 задание 599
 информационный объект 599
 установки системы по умолчанию 428, 522
 восстановление SAP платформы BI
 настройки сервера 544
 восстановление платформы BI
 настройки сервера 543, 545
 временные файлы 101
 время нарушения 1139
 время ожидания сокета 851
 время отклика 713
 Вспомогательная версия 46, 565
 вход в систему
 защита от попыток выполнения злоумышленником 174
 настройка 692
 рабочий процесс 85
 стартовая панель BI 126
 входящие
 контролирование доступа к 126
 выбор зависимых объектов 590
 выбор продуктов 97
 Вызов удаленного метода (RMI) 715
 вызов удаленной процедуры 461
 выполнение аудита
 архитектура 741
 веб-действия 173
 информационный поток 741
 выполнено, мастер настройки системы 103
 выполняется публикация
 в нескольких системах платформы BI 868
 в фоновом режиме 873

выполняется публикация
(*продолжение*)

несколько отчетов с
использованием ролей 870
определения ролей для, в BW
865
отчеты в пакетном режиме 874
отчеты в роли или системе 870
планирование в фоновом
режиме 873
установка 864

Г

глобальные показатели системы 422
график тенденций 714
группы 332

добавление подгрупп 119
добавление пользователей к 122
добавление, массовое 121
изменение 118
назначение прав 146
параметры стартовой панели BI
127
по умолчанию 112
права 1004
на папки высшего уровня 147
нарушение наследования 159
наследование 138
переопределение прав 140
предоставление доступа к 125
проверка прав 148, 149
просмотр
права для 145
участники 119
создание 118
сопоставление 355, 373, 379, 386
специалисты по шифрованию
182
удаление 120
указание принадлежности к
группе 120
управление 112
группы пользователей
делегированное
администрирование 642
группы серверов
доступ к 419
подгруппы 417
подгруппы серверов 415, 418
создание 416
узлы 395

Д

данные
активно 153
сохранено 153
двунаправленное тиражирование
818
действительные права 144
делегированное администрирование
160
группы пользователей 642
обзор 639
демоны, обработка сигналов 962
дерево навигации
серверы 395
диаграмма компонентов 34
диаграмма схемы базы данных
тенденций 1139
диаграмма схемы, база данных
тенденций 1139
диаграмма, компоненты 34
динамически подключаемые
библиотеки, обработка
расширений 175
дискуссии
управление настройками 646
Диспетчер Business View 74
Добавить объекты 595
добавление 411
CMS 412
подгруппы 119
пользователей к группе 122
серверы 407
хост-системы 576
элементы кластера 411
добавление веб-службы 582
добавление информационных
объектов 589
доверие, активные доверительные
отношения 169
доверительная аутентификация 694
пример конфигурации 258
свойства 253
Доверительная аутентификация 250
SAML 252
принципал пользователя 260
документы Desktop Intelligence
права 999
документы Web Intelligence
права 1003
Домашняя страница
Корзина покупок 574
Панель администратора 574
Панель дерева 574
Панель рабочей области 574

Домашняя страница (*продолжение*)

Панель средства просмотра
заданий 574
дополнительный сетевой интерфейс
433
доставка уведомления 1139
доступ 135
входящие 126
группы 125
группы серверов 419
панель HTML-запросов 650
пользователи 125
приложения 634
серверы 419
СМС 634
соединения с юниверсами 709
стартовая панель BI 634
доступ к вкладкам, СМС
Настройка 644
обзор 639
ограничение 645
разрешения, наследование 642
управление для других
пользователей 640, 641
управление разрешениями на
настройку для других 643
устранение неполадок 645

Е

единый вход 43, 244, 315, 322
Kerberos 314, 505
анонимный 244
импорт ролей 332
к базе данных 245
на платформу BI 244
настройка
LDAP 273
SiteMinder 273, 315
сквозной 246
устранение неполадок 274
учетная запись службы 307
единый вход, настройка для JD
Edwards 909
единый вход, настройка для Oracle
EBS 392
единый вход, настройка для
PeopleSoft 912
единый вход, настройка для SAP
Netweaver 353
единый вход, настройка для Siebel
922
емкость, мастер настройки системы
99

Ж

Журнал 582
 журнал заданий
 просмотр 598
 журнал событий 423, 461
 журнал трассировки
 уровни протоколирования 635, 925

З

зависимости 571
 зависимости сервера
 вызов удаленной процедуры 461
 добавление 461
 Журнал событий 461
 задание
 изменение 588
 поиск 587
 Задания тиражирования
 изменение 833
 параметры конфигурации 830
 планирование 832, 833
 просмотр 830
 создание 830
 заполнители 1117
 инструментальные средства 946
 заполнители сервера 1117
 заполнители узлов 1117
 запросы
 безопасность 148, 149
 запросы отношений
 для уровней доступа 157
 запуск серверов 955
 Защита 571
 защита данных
 ключи кластера 179
 ключи шифрования 179
 криптографические ключи 179
 криптография 179
 зеленый флажок, для систем по умолчанию 868

И

изменение задания 588
 изменение размера и настройка 99
 Изменить идентификатор
 управления 592
 Импорт задания
 файл BIAR 596
 индексирование 793
 инициализация базы данных
 системы CMS 477, 478, 479

инструмент Content Administration Workbench
 опубликование отчетов 870
 применение авторизаций 865
 Инструмент определения кластера 877, 882
 инструментальные средства 947
 веб-ярус 947
 заполнители 946
 не Java-серверы 946
 проверка 947
 регистрация 947
 инструменты мониторинга
 обзор 945
 интеграция 809
 SAP 45
 SNC 346
 веб-службы 843, 844
 двунаправленное тиражирование 818, 819
 задания тиражирования 830
 изменение 833
 планирование 832, 833
 создание 830
 импортирование и повышение
 уровня растаженного
 содержимого 848, 849, 850
 локальный запуск экземпляров 845, 847
 обновлять из адресата 818, 819
 обновлять из источника 818, 819
 однаправленное
 тиражирование 818, 819
 очистка объекта 835, 836
 повышение производительности 854
 практический опыт 851
 преимущества 809
 просмотр журналов 834
 режимы репликации 818, 819
 списки тиражирования 823
 папки 823, 824
 создание 823, 824
 управление 826
 сторонние пользователи и
 группы, тиражирование 820
 термины 810
 тиражирование больших
 объектов 851
 удаленное планирование 845, 847, 848
 удаленные соединения 827
 изменение 829
 создание 827
 узлы назначения для отчетов 848, 851

интеграция ((*продолжение*))
 управление безопасностью 812, 813, 814, 816, 817
 уровни доступа 157
 устранение конфликтов 837, 838, 840
 устранение неполадок 856
 Интеграция времени поиска с NWES 802
 интеграция с JD Edwards EnterpriseOne
 настройка брандмауэра 222
 интеграция с Oracle E-Business Suite
 настройка брандмауэра 224
 интеграция с PeopleSoft Enterprise
 настройка брандмауэра 224
 интеграция с SAP Jam
 введение 655
 ключ потребителя OAuth 659, 660
 консоль администрирования SAP Jam 659, 660
 предварительные требования 656
 интеграция с SAP StreamWork
 введение 655
 ключ потребителя OAuth 662
 консоль администрирования SAP StreamWork 662
 предварительные требования 656
 рабочие пространства BI 663
 интеграция с Siebel
 меню "Crystal Reports", создание 918
 настройка брандмауэров 226
 повторная компиляция
 приложения Siebel 918
 проект интеграции 917
 интеграция с приложениями
 сотрудничества
 введение 655
 ключ потребителя OAuth 659, 660, 662
 консоль администрирования
 приложения сотрудничества 659, 660, 662
 предварительные требования 656
 рабочие пространства BI 663
 интеллектуальный ярус 424
 информационная панель 714
 информационный объект
 управление разными версиями 565
 исходное устройство 596

исходные сайты
уровни доступа 157

К

карточки 171
 для распределенной безопасности 171
 маркеры входа 170
каталог установки, расположение 438
категории 128
 права 998
Категории данных мониторинга 732
категории служб 60, 395
кластеры 411, 413
 добавление CMS 412
 изменение имен 414
 просмотр подробностей 422
 узлы 411
клиенты
 Data Federator. См. Data Federation Administration Tool 76
 Query as a Web Service 75
 SAP BusinessObjects Analysis, выпуск для Microsoft Office 79
 SAP BusinessObjects Dashboards 80
 SAP Crystal Reports 80
 Web Intelligence Rich Client 73
 веб 72
 виджеты для платформы SAP BusinessObjects Business Intelligence 77
 Дизайнер информации. См. "Средство дизайна информации" 76
 Диспетчер Business View 74
 настольные 72
 Средство администрирования объединения данных 76
 Средство дизайна информации 76
 Средство преобразования отчетов 74
 Средство создания универсов 74
 Средство управления переводами 76
клиенты на основе браузеров 72
клиенты рабочих станций 72
клиенты, на базе браузера 81
 Analysis, выпуск для OLAP 84
 Central Management Console (CMC) 28, 81

клиенты, на базе браузера *((продолжение))*
 SAP BusinessObjects Mobile 84
 SAP BusinessObjects Web Intelligence 83
 рабочие пространства BI 82
 стартовая панель BI 82
Клиенты, на базе браузера
 Средства просмотра отчетов 83
клиенты, настольные ПК
 Central Configuration Manager (CCM) 28, 78
 Repository Diagnostic Tool 29
 Средство преобразования отчетов 79
 Средство управления обновлением 29, 79
клонирование
 серверы 408, 410
 Серверы контейнера веб-приложений (WACS) 490
ключевые слова 584
ключи кластера 179
 обзор 179
 сброс в UNIX 181
 сброс в Windows 180
 файл dbinfo 179
ключи командной строки 607
ключи командной строки для повышения 607
ключи командной строки для управления повышением уровня 607
ключи реестра 274
количество минут, маркеры входа 170
количество попыток входа, маркеры входа 170
компоненты 877, 882
 Инструмент определения кластера 877, 882
Конструктор агента 732
контекстуальная зависимость 919
 настройка 920, 921
конфигурация 725
конфигурирование
 Secure Sockets Layer 922
 ярус приложений 424
конфликты объектов
 двунаправленное тиражирование 837, 840
 однаправленное тиражирование 837, 838
копирование
 существующее задание 587
 уровни доступа 154

криптографические ключи 179
 обозначение как рассекреченных 187
 просмотр 183
 CMC 183
 список объектов 186
 статус 184
криптографический ключ
 отзыв 188
 создать новый 186
Кэш-сервер 965, 966

Л

лицензионные ключи
 и миграция базы данных CMS 480
лицензионный ключ 108
 добавление 108
 измерение показателей использования 108
 обзор 107
 приобретение 107
 просмотр 107

М

маркеры входа 170
 аутентификация 242
 отслеживание сеансов 171
 распределенная безопасность 171
массовое добавление
 группы 121
 пользователи 121
мастер 27
Мастер импорта
 см. "Средство управления обновлением" 29, 79
мастер настройки системы 27
Мастер настройки системы 97
мастер настройки.См. «Мастер настройки системы» 27
мастер настройки.См. Мастер настройки системы 97
мастер, настройка системы 97
многосетевые компьютеры 431, 432
Сервер контейнера веб-приложений (WACS) 517
Многоязыковая поддержка 801
Мобильные устройства
 права 1029
Мониторинг 713
мониторинг, диаграмма схемы 1139
Мост безопасности PeopleSoft EPM
 файл ответов 362

Н

наблюдение 714
наследование 137
 группа 138
 нарушение 159
 ограничение 142
 папка 139
 переопределение прав 140
 разрешения на доступ к
 вкладкам CMS 642
наследование папок 139
 переопределение прав 140
настройка
 Apache 2.2 230
 ISA 2006 232
 WebSEAL 6.0 231
 база данных CMS 475, 476, 477
 база данных системы CMS 477,
 478, 479
 брандмауэры 209
 Доверительная аутентификация
 250
 интеллектуальный ярус 424
 кластеры 411
 кластеры CMS 414
 несколько серверов 425
 обрабатывающий ярус 424
 обратные прокси-серверы 229,
 230
 узлы 411
 шаблоны настройки 426
Настройка
 процесс отката 577
Настройка OpenSearch 785
настройка аудита, см. аудит 747
Настройка веса для ранжирования
 результатов поиска 801
настройка входа в систему
 OpenDocument 691
 стартовая панель BI 691
настройка и изменение размера 99
настройка обратного прокси 786
настройки SubVersion 566
Настройки задания 577
Настройки отката 577
настройки сервера
 csm.sh
 резервное копирование
 параметров сервера 535
 восстановление 543, 544, 545
 создание резервной копии 533,
 534, 535, 536
настройки управления версиями 566
неотображаемые роли 358, 390
непрерывная трассировка 948

номера портов
 изменение 434, 435, 436
 конфликты 520
Сервер контейнера
 веб-приложений (WACS) 519

О

О показателях сервера
 общие показатели
 IP-адрес хоста 1090
 PID 1090
 Версия 1090
 Занятые потоки на сервере
 1090
 Зарегистрированное имя
 1090
 Имя компьютера 1090
 Имя хоста 1090
 Использованное дисковое
 пространство (Гбайт) 1090
 Каталог протоколирования
 1090
 Местное время 1090
 ОЗУ (Мбайт) 1090
 Операционная система 1090
 Порт запросов 1090
 Размер диска (Гбайт) 1090
 Сервер имен 1090
 Тип ЦПУ 1090
 ЦПУ 1090
 Показатели аудита
 Текущее число проверяемых
 событий, ожидающих
 своей очереди 1090
обеспечение отказоустойчивости
 736
Обзор 783
область действия прав 142
Облегченный протокол доступа к
 каталогам. См. LDAP 262
обмен данными 242
 между браузером и сервером
 веб-приложений 242
 между серверами платформы BI
 198
обновить 588
Обновить содержимое
 вспомогательной версии 568
обновление
 повторяющиеся и ожидающие
 экземпляры задания 597
 статус
 плановое повышение
 задания 597
Обновление 568
Обновление вспомогательной
 версии 568
обновления 47
обрабатывающий ярус 424
обработка расширений 175
 регистрация 637
 совместное использование 638
обработка сигналов 962
обратные прокси-серверы
 Live Office 239
 Tomcat 234
 URL-адрес средства просмотра
 239
 веб-службы 234, 236
использование с серверами
 контейнера веб-приложений
 (WACS) 516
 конфигурация Apache 2.2 230
 конфигурация ISA 2006 232
 конфигурация WebSEAL 6.0 231
настройка на платформе BI 229,
 230
поддерживаемые 228
развертывание на платформе BI
 228, 229
развертывание с помощью
 Сервера контейнера
 веб-приложений (WACS) 516
 специальная конфигурация 234
 файлы cookies сеансов 237
общий доступ к экземпляру 845, 848
объекты
 права 859, 995
 настройка 146
 просмотр 145
объекты отчета
 права 1002
 права на создание/изменение
 420
объекты программы
 аутентификация 635
 включение, отключение 635, 637
ограничение
 область действия прав 142
ограничения 175
 вход в систему 174
 пароль 174
 пользователь 175
 учетная запись гостя 175
однаправленное тиражирование
 818
ОЗУ 99
оперативное резервное копирование
 525, 529, 530
определенные права
 рабочие пространства BI 1015

основная аутентификация 242
 основной сетевой интерфейс 433
 откат
 задание в средстве управления
 повышением 599
 Откат 571
 Откат задания
 по истечении срока действия
 пароля 600
 Откат информационных объектов
 по истечении срока действия
 пароля 601
 отключение
 псевдонимы 133
 серверы 406
 учетные записи гостя 121
 отображаемые пользователи,
 управление псевдонимами 130
 отображение ролей 332, 355, 373,
 379, 386
 отслеживание
 сквозной 948
 отслеживание, сеансы 171
 отфильтрованные информационные
 объекты 590
 отчеты
 выполняется публикация 870
 в пакетном режиме 874
 обновление источников данных
 873
 удаление 874

П

Пакет SDK для SAP BusinessObjects
 175
 панель HTML-запросов, права
 доступа 650
 папка
 создание 583
 папка управления повышением 573
 папки
 права 998
 права объекта
 наследование 139
 папки, мастер настройки системы
 101
 параметр CTS 582
 Параметр настройки CTS 582
 Параметры администрирования 571
 Настройки задания 576
 Настройки отката 576
 Переопределение параметров
 576
 Управление системами 576

параметры командной строки 960,
 961, 971, 975
 CMS 962
 SSL 189
 Адаптивный сервер заданий 967
 все серверы 961
 Кэш-сервер 965, 966
 Сервер обработки 965, 966
 Сервер приложений отчетов 969
 Сервер событий 975
 Серверы репозитория входящих
 и исходящих файлов 972
 параметры памяти
 изменение на Сервере
 контейнера веб-приложений
 (WACS) 521
 параметры повышения 592
 параметры поиска 587
 параметры профиля 346
 параметры режима обновления, для
 интеграции 818, 819
 параметры скриптов, узлы
 воссоздание 456
 добавление 456
 перемещение 458
 удаление 456
 пароли 475, 476, 477
 изменение 123
 для базы данных CMS 475
 параметры 124, 248
 ограничения 174
 перевод доверия 171
 перезагрузка серверов 402, 403, 404
 переименование, уровни доступа
 155
 переменные
 AIX 24
 HP-UX 24
 Linux 24
 Solaris 24
 каталог скриптов 24
 каталог установки 24, 438
 операционная система UNIX 24
 скрипты управления узлами 438
 переменные сеанса 171
 аутентификация 242
 перенос базы данных Derby в базу
 данных аудита 719
 Персональная среда безопасности
 см. PSE 336
 планирование
 повышение задания 597
 Планирование 571
 планирование аварийного
 восстановления 167

Планирование ресурсов
 предприятия (ERP) 45
 платформа BI
 импорт ролей 332
 обмен данными между
 серверами 198
 отображение ролей 379
 папки верхнего уровня, права
 147
 планирование аварийного
 восстановления 167
 права 135
 процесс основной
 аутентификации 242
 развертывание с
 использованием обратных
 прокси-серверов 228, 229
 резервное копирование и
 восстановление 530
 рекомендации по безопасности
 168
 трассировки, ведение журнала
 925
 уровни журнала трассировки
 635, 925
 Платформа SAP BusinessObjects
 Business Intelligence
 Сервер контейнера
 веб-приложений (WACS) 483
 повышение 571
 повышение задания 597
 при соединении с репозиториями
 592
 с помощью файла BIAR 594
 повышение задания при отсутствии
 соединения с репозиториями 594
 подгруппы, добавление 119
 поддерживаемое задание
 статус 598
 поддерживаемые информационные
 объекты 592
 поддержка кластеров 736, 784
 поддержка отчета 873
 подключаемые модули безопасности
 243, 322
 Аутентификация LDAP 263
 аутентификация Windows AD 288
 подключаемые модули безопасности
 третьих производителей 243
 подключаемые модули,
 безопасность 243
 Подключение к Open SQL 877
 поиск 647, 793
 темы дискуссии 647
 поиск зависимых объектов 590, 591

Поиск из NetWeaver Enterprise Search 805	показатели сервера ((продолжение))	показатели сервера ((продолжение))
Поиск по платформе 664, 787	Показатели Central Management Service ((продолжение))	Показатели адаптивного сервера заданий ((продолжение))
показатели	Существующие учетные записи именованных пользователей 1092	Завершение работы 1106
просмотр 422	Существующие учетные записи пользователей с лицензиями на одновременный доступ 1092	Инициализация 1106
показатели сервера 1089	Установленные соединения с системной БД 1092	Максимально разрешенное число заданий 1106
Показатели Central Management Service	Число входов в систему с момента запуска 1092	Максимальное разрешенное количество параллельных заданий 1106
Аудитор CMS 1092	Число запросов с момента запуска 1092	Параллельные задания 1106
Версия продукта 1092	Число объектов в системной БД CMS 1092	Пиковые задания 1106
Версия ресурса 1092	Число объектов в системном кэше CMS 1092	Полученные запросы заданий 1106
Выполняющиеся задания 1092	Число сеансов пользователей с лицензиями на одновременный доступ 1092	СвязьСБои 1106
Дата сборки 1092	Число сеансов, установленных всеми пользователями 1092	Служба планирования 1106
Длительность последнего цикла опроса потока аудита (секунды) 1092	Число сеансов, установленных зарегистрированными пользователями 1092	Службы планирования 1106
Завершенные задания 1092	Число сеансов, установленных серверами 1092	Создания заданий, завершившиеся сбоем 1106
Задания, завершившиеся сбоем 1092	Число фиксаций с момента запуска 1092	Установка по умолчанию адресатов FTP допустима 1106
Имя источника данных 1092	Показатели Crystal Reports Server	Установка по умолчанию адресатов папки "Входящие" допустима 1106
Имя пользователя базы данных аудита 1092	Имя Dll объекта 1108	Установка по умолчанию адресатов файловой системы допустима 1106
Имя пользователя системной базы данных 1092	Макс. число дочерних процессов 1108	Установка по умолчанию адресатов эл. почты допустима 1106
Имя сервера системной базы данных 1092	Максимальное время обработки (мс) 1108	Показатели адаптивного сервера обработки DSLServiceMetrics.activeConnectionCount 1099
Имя соединения с базой данных аудита 1092	Минимальное время обработки (мс) 1108	DSLServiceMetrics.activeOLAPConnectionCount 1099
Имя соединения с системной базой данных 1092	Обслужено запросов 1108	DSLServiceMetrics.activeSessionCount 1099
Использование потока аудита 1092	Объем кэш-памяти 1108	DSLServiceMetrics.queryCount 1099
Кластеризованные серверы CMS 1092	Открытые в данный момент задания отчетов 1108	serviceBean.monitoringAppPropEnabled 1099
Лицензии для именованных пользователей 1092	Открытые в данный момент соединения 1108	Аудит полученных событий 1099
Лицензии на одновременный доступ пользователей 1092	Открытые задания 1108	Всего памяти (Мбайт) 1099
Максимальное время обработки запроса с момента запуска (мсек) 1092	Передано данных (КБ) 1108	Выполняемая индексация 1099
Максимальное время обработки фиксации с момента запуска (мсек) 1092	Среднее время обработки (мс) 1108	Доступная служба 1099
Максимальное число пользовательских сеансов с момента запуска 1092	Тип объекта 1108	Доступные процессоры 1099
Незавершенные запросы в системную БД 1092	Удачных обращений в кэш (%) 1108	Интервал обновления показателей мониторинга (секунды) 1099
Номер построения 1092	Частота сбоев запросов 1108	Количество конфликтов при блокировках JVM 1099
Ожидающие задания 1092	Число запросов в очереди 1108	Количество ошибок страниц в течение GC (последние 15 минут) 1099
Отложенные задания 1092	Число запросов, выполненных с ошибкой 1108	Количество ошибок страниц в течение GC (последние 5 минут) 1099
Параллельно использующиеся соединения с системной БД 1092	Число открытых соединений 1108	Количество полных GC 1099
Последнее использование базы данных аудита 1092	Показатели адаптивного сервера заданий PID 1106	Максимальный объем памяти (Мбайт) 1099
Соединение с базой данных аудита установлено 1092	Временный каталог 1106	Метка времени последнего обновления индекса 1099
Среднее время ответа на запрос с момента запуска (мсек) 1092	дочерние элементы 1106	Метка времени создания последнего хранилища содержимого 1099
Среднее время ответа при фиксации с момента запуска (мсек) 1092		Общее число байтов объема диска, используемого выполнением запроса 1099

показатели сервера ((продолжение))	показатели сервера ((продолжение))	показатели сервера ((продолжение))
Показатели адаптивного сервера обработки ((продолжение))	Показатели адаптивного сервера обработки ((продолжение))	Показатели сервера Web Intelligence ((продолжение))
Общее число байтов памяти, используемых при выполнении запроса 1099	Число наблюдений 1099	Число активных потоков 1112
Общее число байтов памяти, используемых кэшем метаданных 1099	Число неудачных попыток извлечения момента запуска службы 1099	Число документов 1112
Общее число байтов, переданных из источников данных 1099	Число показателей тренда 1099	Число истечений времени ожидания сеансов 1112
Общее число байтов, созданных при выполнении запроса 1099	Число показателей, созданных пользователем 1099	Число операций подкачки документов 1112
Общее число записей, переданных из источников данных 1099	Число сбоев запросов 1099	Число подкачанных документов 1112
Общее число записей, созданных при выполнении запроса 1099	Число сеансов 1099	Число пользователей 1112
Потоки на транспортном уровне 1099	Число соединений 1099	Число удаленных ошибок расширения 1112
Процент использования ЦПУ (последние 15 минут) 1099	Число успешных попыток извлечения с момента запуска службы 1099	Показатели сервера контейнера веб-приложений
Процент использования ЦПУ (последние 5 минут) 1099	Показатели сервера Dashboards	Ошибка запуска одного или нескольких соединителей WACS 1105
Процент остановленной системы в течение GC (последние 15 минут) 1099	Имя Dll объекта 1113	Список выполняющихся средств связи WACS 1105
Процент остановленной системы в течение GC (последние 5 минут) 1099	Макс. число дочерних процессов 1113	Показатели сервера репозитория файлов
Размер пула потоков транспортного уровня 1099	Максимальное время обработки (мс) 1113	Активные файлы 1098
Сведения о версии JVM 1099	Минимальное время обработки (мс) 1113	Активных соединений 1098
Сведения об отладке JVM 1099	Открытые задания 1113	Доступное дисковое пространство в корневом каталоге (%) 1098
Свободная память (Мбайт) 1099	Передано данных (КБ) 1113	Доступное дисковое пространство в корневом каталоге (Гб) 1098
Служба объединения данных доступна 1099	Размер кэша (кбайт) 1113	Записано данных (Мб) 1098
Службы 1099	Среднее время обработки (мс) 1113	Общее дисковое пространство в корневом каталоге (Гб) 1098
Среднее время вычисления состояния наблюдения для последних 15 циклов (мс) 1099	Тип объекта 1113	Передано данных (Мб) 1098
Счетчик заблокированных потоков JVM 1099	Удачных обращений в кэш (%) 1113	Свободное дисковое пространство в корневом каталоге (Гб) 1098
Флаги трассировки JVM 1099	Частота сбоев запросов 1113	Список активных файлов 1098
Число активных потоков 1099	Число запросов в очереди 1113	Показатели сервера событий
Число активных соединений на загруженных блоках соединений 1099	Число запросов, выполненных с ошибкой 1113	Отслеживаемые файлы 1097
Число выполняющихся запросов 1099	Число обслуживаемых запросов 1113	Список отслеживаемых файлов 1097
Число загруженных блоков соединений 1099	Число открытых заданий 1113	Показатели сервера соединений
Число запросов 1099	Число открытых соединений 1113	Источники данных 1097
Число запросов на стадии анализа 1099	Показатели сервера Web Intelligence	Показатели сервера
Число запросов на стадии выполнения запроса 1099	Верхний порог использования памяти 1112	Просмотр 422
Число запросов на стадии оптимизации запроса 1099	Время простоя (сек) 1112	Показатели системы, просмотр 422
Число запросов, использующих диск 1099	Использование ЦП (%) 1112	Сервер контейнера веб-приложений (WACS) 519
Число запросов, использующих память 1099	Максимальное количество документов в кэше 1112	Пользователь 714, 1139
Число запросов, ожидающих ресурсов 1099	Максимальный порог использования памяти 1112	Полный откат 599
Число индексированных документов 1099	Общее время работы ЦП (сек) 1112	Пользователи
Число кубов 1099	Общее число вызовов клиента 1112	Добавление, массовое 121
	Общее число задач 1112	Назначение прав 146
	Общее число потоков 1112	Назначение расширенных прав 147
	Общее число сеансов 1112	Полная права 1004
	Размер виртуальной памяти (Мб) 1112	Права просмотра для 145
	Размер кэша (КБ) 1112	Права, на папки верхнего уровня 147
	Текущее число активных сеансов 1112	Предоставление доступа к 125
	Текущее число вызовов клиента 1112	Проверка прав 148, 149
	Текущее число задач 1112	
	Текущее число сеансов 1112	
	Уровень максимального использования кэша 1112	

- пользователи ((*продолжение*))
 сопоставление 355, 373, 379, 386
 последовательности операций
 назначение расширенных прав 147
 настройка прав доступа к папкам верхнего уровня 147
 права просмотра 145
 списки контроля доступа, назначение владельцев учетных записей 146
 права 135, 391, 995
 Crystal Reports 1002
 Explorer 1027
 Mobile 1029
 Web Intelligence 1019
 администрирование 160, 164
 виджеты 1025
 входящие 126
 группы 125, 1004
 группы серверов 419
 действительные права 144
 документы Desktop Intelligence 999
 документы Web Intelligence 1003
 зависимые от типа 143
 запрос безопасности 148, 149
 категории 998
 назначение владельцам учетных записей 146
 наследование 137
 группа 138
 нарушение 159
 папка 139
 область действия прав 142
 общее 995
 папки 998
 папки верхнего уровня 147
 переопределение прав 140
 пользователи 125, 1004
 Построитель стратегий 1022
 права
 тиражирование 812, 813, 814, 816, 817
 права администрирования 391
 права владельца 164
 права на публикацию 392
 Предупреждение 1026
 приложения 634
 примечания 1001
 просмотр 145
 просмотр и просмотр по запросу 153
 рабочее пространство BI 1015
 расширенные права 136, 147
 Сервер приложений отчетов 420
- права ((*продолжение*))
 серверы 419
 CMC 634, 1014
 соединения с юниверсами 1011
 средство дизайна информации 1024
 средство создания юниверсов 1023
 стартовая панель BI 634, 1014
 управление 145
 управление безопасностью 812, 813, 814, 816, 817
 уровни доступа 136, 1006
 задачи 151
 запросы отношений 157
 изменение включенных прав 156
 тиражированный 157
 управление на уровне нескольких сайтов 157
 юниверсы (.unv) 1006
 юниверсы (.unx) 1008
 права владельца 164
 права для конкретных типов объектов
 виджеты 1025
 права доступа к приложению 572
 права доступа к приложению управления повышением 572
 права, зависимые от типа 143
 Crystal Reports 1002
 Web Intelligence 1019
 группы 1004
 документы Desktop Intelligence 999
 документы Web Intelligence 1003
 категории 998
 папки 998
 пользователи 1004
 Построитель стратегий 1022
 Предупреждение 1026
 примечания 1001
 CMC 1014
 соединения с юниверсами 1011
 средство дизайна информации 1024
 средство создания юниверсов 1023
 стартовая панель BI 1014
 уровни доступа 1006
 юниверсы (.unv) 1006
 юниверсы (.unx) 1008
 Предложения 802
 представления 43
 предупреждение 714
- Предупреждение 653
 права 1026
 свойства места назначения 653
 свойства по умолчанию 654
 управление 653
 управление настройками 653
 преобразование сетевых адресов
 настройка, файл хостов сервера 211
 приложения 633
 Поиск по платформе 664, 787
 свойства 664, 787
 приложения сотрудничества, интеграция
 введение 655
 предварительные требования 656
 примечания, права 1001
 Проверить повышение 571
 продукты, мастер настройки системы 97
 производительность 99, 713
 балансировка нагрузки 171
 кластеры 411
 производный показатель 714
 просмотр
 журнал заданий 598
 подробности кластера CMS 422
 Показатели Сервера контейнера веб-приложений (WACS) 519
 показатели системы 422
 права для владельцев учетных записей 145
 текущие показатели 422
 Просмотр полномочий 145
 просмотр текущей учетной записи 108
 просмотр, мастер настройки системы 102
 протокол RMI 725
 Процесс PSANALYTIC 916
 Процесс PSAPPSRV 916
 процесс отката 600
 псевдонимы
 назначение пользователям 131
 отключение 133
 создание 131
 для новых пользователей 130
 для существующих пользователей 131
 удаление 132
 управление 130
 псевдонимы пользователей 131
 назначение 131
 отключение 133

псевдонимы пользователей
 ((*продолжение*))
 создание 131
 для новых пользователей 130
 для существующих
 пользователей 131
 удаление 132
 публикация, назначение прав на 392

Р

работоспособность 714
 рабочие пространства BI 82
 Рабочие пространства BI, права
 1015
 рабочие процессы 85
 вход пользователя в систему 85
 выполнение запланированного
 объекта программы 88
 выполнение запланированного
 отчета SAP Crystal Reports
 2011 92
 запланированный документ Web
 Intelligence 94
 Запуск узла SIA 86
 настройка расписания для
 программного объекта 87
 Отключение SIA 87
 просмотр документа Web
 Intelligence по требованию 93
 просмотр кэшированной
 страницы отчета Crystal 89
 просмотр некашированной
 страницы Crystal Reports 2011
 89
 просмотр отчета Crystal Reports
 2011 по требованию 90
 просмотр рабочего пространства
 Analysis 95
 установка расписания для
 объекта Web Intelligence 94
 установка расписания для отчета
 Crystal 91
 размещение зависимостей объекта
 591
 распространение
 компоненты BW Publisher 862
 Расширения Java Management (JMX)
 715
 расширения, обработка 175
 расширенные права 136, 144, 147
 регистрация 423, 947
 веб-действия 173
 работа сервера 423
 трассировки 925

регистрация ((*продолжение*))
 уровни, журнал трассировки 635,
 925
 Редактор параметров безопасности
 транспорт 877, 881
 режим выполнения 361
 режим настройки 361
 резервное копирование платформы
 BI 525, 530
 "холодное" резервное
 копирование 529
 настройки сервера 533, 534, 535,
 536
 оперативное резервное
 копирование 525, 529
 оперативное резервное
 копирование:включение 531
 предварительные требования
 для оперативного резервного
 копирования 530
 резервное копирование приложений
 525
 резервное копирование системы
 525, 529
 рекомендации по увеличению
 производительности 915
 Репозиторий входящих файлов 25,
 47, 1034
 Репозиторий исходящих файлов 25,
 47, 1034
 ресурсы BI 571
 роли 355, 373, 379, 386, 865
 импорт 332
 назначение 332, 355, 358, 373,
 375, 379, 386
 назначение прав 391
 неотображаемые 358, 390
 переназначение 381
 создание для
 администрирования 865

С

сайты
 управление правами 812, 813,
 814, 816, 817
 уровни доступа 157
 сайты-адресаты
 уровни доступа 157
 Самовосстановление 806
 светофор 714
 свойства серверов 1031
 связанные с заданием процессы 582
 Связь 735
 сеансы 171
 отслеживание 171

сервер Java-приложений, Kerberos
 297
 Сервер адаптивной обработки 1034
 Сервер аналитики PeopleSoft 916
 Сервер аналитики информационных
 панелей 1034
 Сервер информационных панелей
 1034
 Сервер контейнера веб-приложений
 (WACS) 39, 1034
 AD Kerberos 501
 HTTPS 492, 495, 516
 SSL 492, 495
 балансировка нагрузки 515
 брандмауэры 516
 восстановление установок
 системы по умолчанию 522
 добавление 487
 добавление веб-служб к 491
 изменение параметров памяти
 521
 использование с другими
 веб-серверами 515
 использование с
 прокси-серверами 516
 клонирование 490
 на многосетевых компьютерах
 517
 обзор 483
 общие задания 484
 ошибки сервера 519
 показатели 1105
 показатели системы 519
 свойства 523
 служба СМС 483
 соединители 483
 создание серверов 489
 удаление 487, 491
 удаление веб-служб с 492
 установка 488
 устранение конфликтов портов
 519, 520
 устранение неполадок 518
 файлы JAAS 500
 файлы конфигурации Kerberos
 499
 сервер мониторинга 736
 Сервер обработки
 Web Intelligence 971
 параметры командной строки
 965, 966
 Сервер обработки Crystal Reports
 965
 параметры командной строки 965
 сервер обработки Dashboards 966
 параметры командной строки 966

Сервер обработки Web Intelligence 25, 47
 Сервер приложений отчетов
 необходимые права объекта 420
 параметры командной строки 969
 Сервер событий 1034
 параметры командной строки 975
 серверы 38
 URL агента мониторинга 1034
 Автоматическое повторное подключение к системной базе данных 1034
 адрес IPv6 431
 варианты идентификации узлов 429
 включение 406, 407
 Включить HTTP через прокси 1034
 Включить HTTPS 1034
 Включить аутентификацию клиента 1034
 Временный каталог 1034
 Время ожидания замены подсистемы визуализации (сек) 1034
 Время ожидания запуска службы 1034
 Время ожидания очистки подсистемы визуализации (сек) 1034
 Время ожидания простаивающих временных объектов 1034
 Время простоя соединения 1034
 выполнение входа 423
 группирование 415
 действия, регистрация 423
 дерево навигации 395
 добавление 407
 доступ к 419
 заполнители 409
 Запросы соединений с системной базой данных 1034
 запуск 402, 403, 404
 автоматически 402, 403
 изменение 400
 состояние 400
 статус 401
 изменение принадлежности к группе 418
 имя хоста 431
 Имя хоста прокси 1034
 Интервал опроса событий 1034
 Интервал очистки 1034
 Истечение срока действия единого входа 1034
 Каталог хранилища файлов 1034

серверы ((*продолжение*))
 клонирование 408, 410
 коммуникация 198
 конфигурирование 424
 Максимальное время ожидания соединения (в секундах) 1034
 Максимальное время простоя 1034
 Максимальное число активных соединений на сеанс пользователя 1034
 Максимальное число запросов дочерних объектов 1034
 Максимальное число неиспользуемых соединений на сеанс пользователя 1034
 Максимальное число параллельных заданий 1034
 Максимальное число параллельных запросов 1034
 Максимальное число повторных попыток доступа к файлам 1034
 Максимальное число попыток 1034
 Максимальный размер заголовка HTTP 1034
 Местоположение файла bscLogin.conf 1034
 Местоположение файла Krb5.ini 1034
 Местоположение файла списка надежных сертификатов 1034
 Местоположение файла хранилища сертификатов 1034
 настройка IP-адреса 431
 настройка серверов на использование учетной записи службы 295
 настройка учетной записи службы 286
 настройки производительности 424
 Начальный номер порта 1034
 обработка сигналов UNIX 962
 общие свойства сервера
 Автоматический запуск сервера при запуске SIA 1031
 Восстановить системные значения по умолчанию 1031
 Задать шаблон конфигурации 1031
 Идентификаторы хостов 1031

серверы ((*продолжение*))
 общие свойства сервера ((*продолжение*))
 Использовать шаблон конфигурации 1031
 Назначать автоматически 1031
 Порт запросов 1031
 Уровень журнала 1031
 остановка 402, 403, 404
 отключение 406, 407
 ошибки 401
 Параметры сервера Desktop Intelligence
 Верхний порог памяти 1084
 Максимальный порог памяти 1084
 Нижний порог памяти 1084
 Пароль доступа к секретным ключам 1034
 Пароль доступа к секретным ключам списка надежных сертификатов 1034
 перезагрузка 402, 403, 404
 Порт 1034
 Порт HTTP 1034
 Порт HTTPS 1034
 Порт прокси 1034
 Порт сервера имен 1034
 Привязка к имени хоста или IP-адресу 1034
 Привязка ко всем IP-адресам 1034
 просмотр статуса сервера 401
 Протокол 1034
 Псевдоним сертификата 1034
 регистрация по имени 437
 свойства 424, 425
 Свойства основных служб
 CORS – совместное использование ресурсов по всем источникам 1034
 pageSize 1034
 SAPR3 1034
 secDAP 1034
 secEnterprise 1034
 secWinAD 1034
 URL агента мониторинга 1034
 Автоматическое повторное подключение к системной базе данных 1034
 Базовая аутентификация HTTP, включение 1034
 Включить HTTP через прокси 1034
 Включить HTTPS 1034

серверы ((продолжение))

Свойства основных служб
((продолжение))
Включить аутентификацию
клиента 1034
Временный каталог 1034
Время ожидания замены
подсистемы визуализации
(сек) 1034
Время ожидания запуска
службы 1034
Время ожидания маркера
сеанса Enterprise 1034
Время ожидания очистки
подсистемы визуализации
(сек) 1034
Время ожидания
простаивающих
временных объектов 1034
Время ожидания пула сеанса
1034
Время простоя соединения
1034
Доступ к нескольким
доменам, Javascript 1034
Запросы соединений с
системной базой данных
1034
Имя хоста прокси 1034
Интервал опроса событий
1034
Интервал очистки 1034
Истечение срока действия
единого входа 1034
Каталог хранилища файлов
1034
Максимальное время
ожидания соединения (в
секундах) 1034
Максимальное время простоя
1034
Максимальное число
активных соединений на
сеанс пользователя 1034
Максимальное число
запросов дочерних
объектов 1034
Максимальное число
неиспользуемых
соединений на сеанс
пользователя 1034
Максимальное число
параллельных заданий
1034

серверы ((продолжение))

Свойства основных служб
((продолжение))
Максимальное число
параллельных запросов
1034
Максимальное число
повторных попыток
доступа к файлам 1034
Максимальное число попыток
1034
Максимальный размер
заголовка HTTP 1034
Максимальный срок 1034
Местоположение файла
bscLogin.conf 1034
Местоположение файла
Krb5.ini 1034
Местоположение файла
списка надежных
сертификатов 1034
Местоположение файла
хранилища сертификатов
1034
Начальный номер порта 1034
Пароль доступа к секретным
ключам 1034
Пароль доступа к секретным
ключам списка надежных
сертификатов 1034
Показать стек ошибок 1034
Порт 1034
Порт HTTP 1034
Порт HTTPS 1034
Порт прокси 1034
Порт сервера имен 1034
Привязка к имени хоста или
IP-адресу 1034
Привязка ко всем IP-адресам
1034
Протокол 1034
Псевдоним сертификата 1034
Размер пула потока 1034
Размер пула сеанса 1034
Служба протокола
трассировки 1034
Тип хранилища сертификатов
1034
Уровень журнала 1034
Число объектов по
умолчанию на одной
странице 1034
свойства сервера Crystal Reports
Аргументы Java VM 1060
Аргументы дочерней Java VM
1060

серверы ((продолжение))

свойства сервера Crystal Reports
((продолжение))
Временный каталог 1060
Время ожидания кэша
безопасности (мин) 1060
Время простоя соединения
1060
Истечение срока действия
единого входа 1060
Каталог файлов кэша 1060
Количество записей БД,
прочитываемых для
предварительного
просмотра или
обновления отчета 1060
Максимальное количество
заданий на весь срок
жизни для каждого
дочернего объекта 1060
Максимальное число
параллельных заданий
1060
Максимальное число
предварительно
запущенных дочерних
процессов 1060
Максимальный размер кэша
1060
Максимальный срок хранения
данных, предоставляемых
клиенту 1060
Предельное время простоя
задания 1060
Предоставлять совместный
доступ к данным отчета
для клиентов 1060
При обновлении средства
просмотра всегда
выдаются текущие
данные 1060
Путь к классу Java 1060
Размер данных просмотра
1060
Размер пакета 1060
Разрешить заданиям для
отчетов сохранять
соединение с БД до
закрытия данного задания
для отчета 1060
Число записей,
прочитываемое в базе
данных для
предварительного
просмотра или
обновления 1060

серверы ((продолжение))

Свойства сервера Dashboards
 Аргументы Java VM 1085
 Аргументы дочерней Java VM 1085
 Время ожидания кэша безопасности (мин) 1085
 Время простоя задания 1085
 Время простоя соединения 1085
 Время простоя соединения (мин) 1085
 Максимальное количество заданий на весь срок жизни для каждого дочернего объекта 1085
 Максимальное число параллельных заданий 1085
 Максимальное число предварительно запущенных дочерних процессов 1085
 Максимальный размер кэша (в КБ) 1085
 Разрешить заданиям для отчетов сохранять соединение с БД до закрытия данного задания для отчета 1085
 Самые старые данные, выданные клиентам по запросам (сек) 1085
 Совместный доступ к данным для клиентов 1085
 Число записей, прочитываемое в базе данных для предварительного просмотра или обновления 1085
 Свойства сервера соединений
 Активация источника данных 1054
 База данных 1054
 Включение отслеживания заданий 1054
 Включить образование блоков HTTP 1054
 Включить отслеживание программного обеспечения среднего яруса 1054
 Время ожидания пула соединений 1054

серверы ((продолжение))

Свойства сервера соединений ((продолжение))
 Время простоя неактивности переходных объектов (мин) 1054
 Интервал таймера временных объектов 1054
 Размер блока HTTP 1054
 Сетевой уровень 1054
 Создание пула соединений 1054
 Свойства служб Web Intelligence
 Верхний порог памяти 1073
 Включить анализ памяти 1073
 Включить кэш документов 1073
 Включить кэш реального времени 1073
 Включить мониторинг 1073
 Включить мониторинг службы APS 1073
 Включить протоколы текущей активности 1073
 Включить список значений кэша 1073
 Время ожидания замены отслеживаемых ресурсов по умолчанию (сек) 1073
 Время ожидания замены подсистемы визуализации (сек) 1073
 Время ожидания кэша 1073
 Время ожидания очистки отслеживаемых ресурсов по умолчанию (сек) 1073
 Время ожидания очистки подсистемы визуализации (сек) 1073
 Время ожидания перед повторным использованием 1073
 Время простоя соединения 1073
 Выходной каталог кэша 1073
 Задержка цикла потока мониторинга (секунды) 1073
 Значение прокси 1073
 Интервал опроса сервера 1073
 Интервал очистки кэша документов 1073
 Истечение срока действия единого входа 1073
 Каталог изображений 1073

серверы ((продолжение))

Свойства служб Web Intelligence ((продолжение))
 Макс. размер пользовательской сортировки 1073
 Макс. размер потока двоичных данных 1073
 Макс. размер символического потока 1073
 Максимальное количество документов в кэше 1073
 Максимальное количество документов до утилизации 1073
 Максимальное сжатие кэша документов 1073
 Максимальное число документов на одного пользователя 1073
 Максимальное число соединений 1073
 Максимальный порог памяти 1073
 Максимальный размер кэша документов 1073
 Максимальный размер кэша юниверсов 1073
 Максимальный размер списка значений 1073
 Не удастся использовать HTTP URL 1073
 Нижний порог памяти 1073
 Отключить совместное использование кэша 1073
 Период потока мониторинга службы APS 1073
 Предельное время простоя документа 1073
 Размер пакета списка значений 1073
 Размер пакета списка значений (элементы) 1073
 Разрешить ошибки макс. размера карты документа 1073
 Число повторов тестового опроса службы APS 1073
 Свойства служб веб-приложений VEx
 Главная система SAP BW 1071
 Количество соединений сервера JCo 1071
 Максимальное число сеансов клиентов 1071

серверы ((*продолжение*))

Свойства служб веб-приложений
 BEх ((*продолжение*))
 Назначение RFC сервера JCo
 1071
 Служба шлюза сервера JCo
 1071
 Хост шлюза сервера JCo
 1071
 Свойства службы
 Multi-Dimensional analysis
 service
 Максимальное число сеансов
 клиента 1071
 Максимальное число
 элементов,
 возвращаемых при
 фильтрации 1071
 Максимальное число ячеек,
 возвращаемых запросом
 1071
 Свойства службы объединения
 данных
 Время ожидания неактивного
 оператора 1072
 Время ожидания неактивного
 соединения 1072
 Максимальное число
 соединений 1072
 Размер пула потока
 выполнения 1072
 состояние 400
 список 395
 сравнение со службами 25, 47
 стандартные параметры
 командной строки 961
 статус 395
 строки команд 960, 961
 Тип хранилища сертификатов
 1034
 удаление 410
 узлы 25, 47
 Уровень журнала 1034
 установки по умолчанию 428
 шаблоны настройки 425
 настройка 426
 применение 427
 серверы веб-приложений 38
 аутентификация 242
 серверы каталогов 263
 о протоколе LDAP 262
 подключаемый модуль
 безопасности 263
 серверы платформы BI 732
 настройка Kerberos и браузеров
 297

серверы платформы BI

((*продолжение*))
 настройка файла хостов для
 брандмауэра 211
 серверы платформы SAP
 BusinessObjects Business
 Intelligence
 настройка Kerberos и браузеров
 499
 Серверы репозитория файлов 25,
 47, 1034
 параметры командной строки 972
 Серверы файлового репозитория
 создание резервной копии 530
 сетевой интерфейс
 устранение неполадок
 нескольких 433
 сетевые интерфейсы для
 устранения неполадок 434
 сетевые среды
 IPv4
 двойные узлы IPv4/IPv6 429
 IPv6 429
 синхронизация информации отчета
 873
 синхронизация сведений отчета 873
 система контроля полномочий 324
 Система управления версиями 565
 системная учетная запись 322
 сквозной единый вход 246
 скрипты UNIX, обзор 949
 скрипты Windows, обзор 957
 скрипты управления узлами,
 расположение 438
 скрипты, UNIX 949
 скрипты, Windows 957
 Служба Business Process BI
 добавление на сервер Web
 Application Container Server
 491
 удаление с сервера Web
 Application Container Server
 492
 служба BW Publisher 862
 выполняется настройка 862
 запуск 862
 создание RFC-адресата 863
 служба мониторинга 725
 службы 51
 ошибки 401
 сравнение с серверами 25, 47
 шаблоны настройки 425
 Службы информационной
 платформы
 административные права 391
 отображение ролей 355, 373, 386

Службы информационной

платформы ((*продолжение*))
 права на публикацию 392
 создание учетной записи для 322
 служебная программа SPN 286
 CMS
 включение и отключение других
 серверов 406, 407
 запуск 405
 изменение имени кластера 414
 как сервер имен 434, 435, 436
 кластеризация 411, 413
 требования 411
 установка нового элемента
 кластера 413
 настройка 434, 435, 436, 475,
 476, 477, 478, 479
 остановка 405
 поиск и устранение
 неисправностей 405
 порт по умолчанию 434, 435, 436
 устранение неполадок на
 многосетевых компьютерах
 434
 CMC
 включение и отключение
 серверов 406
 делегированное
 администрирование
 группы пользователей 642
 обзор 639
 Добавление вкладки "Настройка"
 644
 доступ к вкладкам
 обзор 639
 ограничение 645
 разрешения, наследование
 642
 управление для других
 пользователей 640, 641
 управление разрешениями
 на настройку для других
 643
 устранение неполадок 645
 зависимости сервера Windows,
 добавление 461
 запуск, остановка и перезагрузка
 серверов 402, 403
 клонирование серверов 408, 410
 контролирование доступа к 634
 криптографические ключи 183
 права 1014
 удаление сервера 410
 управление серверами 395
 совместная работа
 права 1015

совместно используемые библиотеки, обработка расширений 175
 совместное использование ресурсов из нескольких источников 510
 Содержимое вспомогательной версии 568
 соединения с источниками данных 709
 соединения с юниверсами
 права 1011
 тиражирование 821
 удаление 709
 управление 709
 создание
 группы 118
 задание 584
 новое задание 587
 папка 583
 подгруппы серверов 417
 уровни доступа 155
 учетные записи пользователей 116
 Сопоставление 571
 состояние, просмотр и изменение для серверов 400, 401
 состояния сервера 395
 сохранение
 задание 587
 новое задание 584
 сохраненные данные 153
 специалисты по шифрованию 182
 добавление участников 182
 списки контроля доступа
 добавление владельцев учетных записей к 146
 просмотр 145
 списки надежных сертификатов 494
 списки тиражирования
 изменение 826
 параметры зависимостей 823, 824
 поддерживаемые объекты 823
 создание 823, 824
 управление 826
 Сравнение разных версий 568
 Сравнение разных версий LCM 568
 Средства просмотра отчетов 83
 Средство администрирования объединения данных 76
 Средство дизайна информации 76
 средство дизайна информации, права 1024
 средство преобразования отчетов SSL 197

Средство преобразования отчетов 74, 79
 Средство создания юниверсов 74
 средство создания юниверсов, права 1023
 Средство управления обновлением 29, 79
 средство управления переводами SSL 196
 Средство управления переводами 76
 CCM
 включение и отключение серверов 406, 407
 для UNIX 949, 953
 для Windows 957, 959
 добавление сервера 407
 запуск, остановка и перезагрузка серверов 402, 404
 удаление сервера 410
 узлы 437
 воссоздание 445
 добавление 441
 переименование 451
 перемещение 453
 удаление 449
 учетные данные пользователя, изменение для 462
 стартовая панель BI 82
 вход в систему 126
 контролирование доступа к 634
 настройка 126
 настройка входа в систему 691
 параметры группы 127, 128
 права 1014
 управление 649
 статистика, аудит действий через Интернет 173
 сторонние группы, репликация 820
 сторонние объекты 592
 сторонние пользователи, репликация 820
 Страница задания повышения 582
 сходство, и SSL 171

Т

темы дискуссии 647
 отмена поиска 647
 поиск 647
 сортировка результатов поиска 648
 тенденция, определение 714
 тест 714, 1139
 типы серверов 63, 70

Типы содержимого, доступного для поиска 796
 тиражирование 525
 объекты 809
 сторонние пользователи и группы 820
 топологический показатель 714
 Транспорт CTS (CTS+) 45
 Транспорт InfoSet Connectivity 877
 Транспорт Open SQL Connectivity 877
 транспорт определения кластера 877, 882
 транспорты 877, 878
 Content Administration Workbench 883
 взаимодействие InfoSet 881
 взаимодействие Open SQL 879
 группы функций 876
 импорт 878
 общие сведения 876
 объекты 876
 определение безопасности на уровне строки 881
 определение кластера 882
 Определение кластера 877
 персонализация параметров 877, 886
 Подключение к InfoSet 877
 проверка на конфликты 878
 программы 876
 Редактор параметров безопасности 877
 таблицы 876
 трассировка
 серверы 926
 BO_trace.ini, настройка 928
 требования
 кластеризация 411

У

уведомление 715
 удаление 477, 478, 479, 576
 база данных системы CMS 477, 478, 479
 группы 120
 папка 584
 псевдонимы 132
 серверы 410
 Серверы контейнера веб-приложений (WACS) 491
 соединения с юниверсами 709
 уровни доступа 155
 учетные записи пользователей 117

удаление ((*продолжение*))
экземпляры задания 577
юниверсы 711
удаленное планирование 845, 848
удаленные соединения
безопасность 829
изменение 829
просмотр 827
создание 827
создание папок 827
узлы 25, 47, 437
воссоздание 456
AddNode.bat 446
addnode.sh 448
RemoveNode.bat 449
removenode.sh 450
serverconfig.sh 447
скрипты для 445
CCM 445
добавление 440, 456
AddNode.bat 442
addnode.sh 444
CMS 412
serverconfig.sh 443
в кластер 413
новый компьютер 441
CCM 441
кластеризация 411
переименование 450
serverconfig.sh 451
CCM 451
перемещение 452, 458
MoveNode.bat 454
movenode.sh 455
serverconfig.sh 454
CCM 453
CMC 395
удаление 448, 456
serverconfig.sh 449
CCM 449
указание
периодичность встреч 597
Упорядочение ранжирования
результатов поиска 801
управление версиями 46, 525, 566
Управление версиями 571
управление зависимостями 589, 590
Управление зависимостями 571
управление повышением 574
управление приложениями 633
war-файл BOE 679
темы дискуссии, удаление 649
Управление системами 576
управляемые объекты 362
группа платформы BI 362, 366
роли PeopleSoft 362, 366

управляемые объекты
((*продолжение*))
юниверсы 362, 366
уровень журнала трассировки
CMC-сервер, настройка для 927
уровни архитектуры 35
уровни доступа 136, 144, 160
RAS 420
администрирование 160
задачи, права, требуемые для
151
изменение прав в 156
копирование 154
назначение владельцам учетных
записей 146
Отношения к объектам 157
переименование 155
права 1006
предопределенный 151
просмотр 145
просмотр и просмотр по запросу
153
создание 155
удаление 155
управление на уровне
нескольких сайтов 157
установка
уровни безопасности по
умолчанию 860
шлюза SAP в Windows 863
экземпляры задания 577
установки по умолчанию
порты 434, 435, 436
серверы 428
устранение неполадок 807
Kerberos 501
единый вход 274
настройка Kerberos 320
Серверы контейнера
веб-приложений (WACS) 518
сообщения об ошибках 856
учетные записи LDAP 285
учетная запись SMCAdmin 944
учетная запись службы
делегирование 286
конфигурация серверов 295
установка 286
учетные данные пользователя,
изменение для узлов 462
учетные записи
службы информационной
платформы 322
управление 111, 115
учетные записи гостя
отключение 121

учетные записи пользователей
изменение 117
по умолчанию 111
создание 116
удаление 117
управление 111, 115

Ф

файл BIAR 594
импорт задание 596
Файл kerberos 284
файл ответов 362
применение 365
создание 362
Файл ответов PeopleSoft 367
параметры 367
файл хостов, настройка для
брандмауэра с NAT 211
файловая система
создание резервной копии 530
файлы cookie 171
маркеры входа 170
отслеживание сеансов 171
файлы WAR
BOE 229, 679, 683, 686
dswebobje 229
war-файл BOE
глобальные свойства 679
свойства CMC 689
свойства OpenDocument 686
свойства стартовой панели
BI 683
Веб-приложения для платформы
BI 229
и веб-приложения для
платформы BI 228
файлы аудита 101
файлы данных 101
файлы журнала 101, 102, 103
файлы журнала аудита 530
файлы ключа 189, 190
файлы ответов 102, 103
файлы сертификатов 189, 190, 493
фасеты 800

Х

хост-системы
добавить 576
хосты
настройка LDAP 264, 269
хранилище входящих файлов 101
хранилище исходящих файлов 101

Ц

Центральный сервер управления
25, 47, 573
центральный сервер управления.
См. CMS. 322

Ч

Частичный откат 599

Ш

шаблон развертывания 99
шаблон, развертывание 99
шаблоны безопасности по
умолчанию 860

шаблоны настройки 425
восстановление установок
системы по умолчанию 428
настройка 426
практический опыт 425
применение 427
шифрование, маркеры входа 170
шлюз SAP 346
и SNC 346
публикация с использованием
локального 863
распространение компонентов
862
установка 863

Э

экземпляры задания
удаление 577

экземпляры задания
((продолжение))
установка 577
экспорт задания
файл BIAR 595

Ю

юниверс 42
юниверсы 590
права (.unv) 1006
права (.unx) 1008
тиражирование 821
управление 710

Я

ярус приложений 424

