PUBLIC (ОБЩЕДОСТУПНО)

Платформа SAP BusinessObjects Business Intelligence

Версия документа: 4.3 Support Package 4 – 2023-12-07

Руководство администратора платформы Business Intelligence

© SAP SE или аффилированная компания SAP, 2024. Все права защищены.

THE BEST RUN SAP

Содержание

1 История документа. 21

2 Начало работы. 23

2.1 О данном руководстве. 23

Для кого предназначено данное руководство?. 23

Общие сведения о платформе Business Intelligence. 23

Переменные. 24

Терминология. 24

2.2 Перед началом работы. 26

Основные понятия. 26

Основные инструменты администрирования. 29

Ключевые задачи. 32

3 Архитектура. 35

3.1 Обзорная информация по архитектуре. 35

Диаграмма компонентов. 36

Уровни архитектуры. 37

Базы данных. 38

Серверы, хосты и кластеры. 39

Серверы веб-приложений. 40

Software Development Kit. 45

Источники данных. 47

Аутентификация и единый вход. 48

Интеграция SAP. 50

Интегрированное управление версиями. 50

3.2 Серверы, службы, узлы и хосты. 51

Изменения сервера с версии XI 3.1. 53

Службы. 55

Категории служб. 62

Типы серверов. 64

Серверы. 69

3.3 Клиентские приложения. 70

Устанавливаемые со средствами клиента платформы SAP BusinessObjects Business Intelligence. 71

Устанавливаемые с платформой SAP BusinessObjects Business Intelligence. 74

Доступно отдельно. 75

Клиенты веб-приложений. 76

3.4 Рабочие процессы. 78
Запуск и аутентификация. 79
Объекты программ. 80
Crystal Reports. 82
Web Intelligence. 86
Анализ. 88
3.5 Интеграция со стартовой панелью Fiori на портале SAP Enterprise Portal. 89

4 Мастер настройки системы. 91
4.1 Вводные сведения о мастере настройки системы. 91
4.2 Указание используемых продуктов. 91
4.3 Выбор шаблона развертывания. 93
4.4 Местоположение каталогов данных. 95
4.5 Просмотр изменений. 97
4.6 Файлы журнала и файлы ответов. 97
Использование файла ответов. 98

5 Управление лицензиями. 102
5.1 Управление лицензионными ключами. 102
Просмотр сведений лицензии. 102
Добавление ключа лицензии. 102
Для просмотра текущей деятельности учетной записи. 103

6 Управление пользователями и группами. 104
6.1 Обзор управления учетными записями. 104
Управление пользователями. 104
Управление группами. 105
Доступные типы аутентификации. 106
6.2 Управление Enterprise и общими учетными записями. 107
Создание учетной записи пользователя. 107
Для изменения учетной записи пользователя. 108
Чтобы удалить учетную запись пользователя. 109
Чтобы создать новую группу. 110
Для изменения свойств группы. 110
Просмотр участников групп. 111
Чтобы добавить подгруппы. 111
Задание принадлежности к группе. 111
Удаление группы. 112
Массовое добавление пользователей или групп пользователей. 112
Чтобы включить учетную запись Гостя. 113
Добавление пользователей в группы. 114
Изменение настроек пароля. 115

Предоставление доступа пользователям и группам. 117
Управление доступом к каталогам "Входящие" пользователей. 118
Настройка параметров стартовой панели BI в стиле Fiori. 118
Управление атрибутами системных пользователей 121
Определение приоритетов атрибутов пользователя для нескольких вариантов аутентификации. 123
Добавление нового атрибута пользователя. 123
Редактирование настроенных атрибутов пользователя. 124
6.3 Управление псевдонимами. 125
Чтобы создать пользователя и добавить сторонний псевдоним. 125
Для создания нового псевдонима существующего пользователя. 126
Для присвоения псевдонима пользователю. 127
Для удаления псевдонима. 127
Для отключения псевдонима. 128

7 Установка прав. 129
7.1 Права на платформе BI. 129
Уровни доступа. 130
Параметры расширенных прав. 130
Наследование. 131
Права для конкретных типов объектов. 136
Определение эффективных прав. 137
7.2 Управление настройками безопасности для объектов в CMC. 138
Для просмотра прав принципала на объект. 139
Для назначения принципалов списку управления доступом к объекту. 139
Для изменения безопасности объекта для принципала. 140
Настройка прав на папку верхнего уровня в платформе BI. 141
Проверка настроек безопасности для принципала. 141
7.3 Работа с уровнями доступа. 144
Выбор между уровнями доступа *Просмотр* и *Просмотр по требованию*. 146
Чтобы скопировать существующий уровень доступа. 147
Создание уровня доступа. 147
Переименование уровня доступа. 148
Для удаления уровня доступа. 148
Изменение прав в уровне доступа. 148
Трассировка связи между уровнями доступа и объектами. 149
Управление уровнями доступа по сайтам. 150
7.4 Отключение наследования. 151
Отключение наследования. 152
7.5 Использование прав передачи административных полномочий. 153
Выбор параметров «*Изменить права пользователей на объекты*». 155
Права владельца. 156

7.6 Сводка рекомендаций по управлению правами . . . 156

8 Обеспечение безопасности платформы BI . . . 158

8.1 Обзор вопросов безопасности . . . 158

8.2 Безопасное использование программных объектов . . . 158

8.3 Планирование аварийного восстановления . . . 159

8.4 Общие рекомендации по обеспечению безопасности развертывания . . . 160

8.5 Настройка безопасности для связанных серверов сторонних производителей . . . 161

8.6 Активные доверительные отношения . . . 161

Маркеры входа . . . 161

Механизм билетов для распределенной безопасности . . . 162

8.7 Сеансы и отслеживание сеансов . . . 163

Отслеживание сеансов центральным сервером управления . . . 163

Управление сеансами . . . 164

Скрипт для очистки устаревших сеансов . . . 165

8.8 Защита среды . . . 165

Веб-браузер с веб-сервером . . . 166

Веб-сервер – платформа BI . . . 166

Защита от попыток выполнения входа злоумышленником . . . 166

Ограничения для пароля . . . 167

Ограничения на вход . . . 167

Ограничения для пользователя . . . 167

Ограничения учетной записи гостя . . . 168

8.9 Аудит изменений параметров безопасности . . . 168

8.10 Расширения обработки . . . 168

8.11 Интерфейс сканирования на наличие вирусов . . . 169

Включение сканирования на вирусы . . . 169

8.12 Безопасность данных платформы BI . . . 170

Защищенные режимы обработки данных . . . 170

Учетные записи администратора . . . 173

Права соединений . . . 173

8.13 Шифрование на платформе BI . . . 174

Работа с ключами кластера . . . 175

Специалисты по шифрованию . . . 177

Управление криптографическими ключами с помощью CMC . . . 178

8.14 Защита и конфиденциальность данных . . . 182

Глоссарий . . . 183

Согласие пользователя . . . 185

Отчет о сведениях . . . 185

Запись доступов чтения в журнал . . . 186

Удаление личных данных . . . 186

Журнал изменений . . . 188

8.15 Настройка внутренних серверов для SSL. 188
Создание файла конфигурации по умолчанию. 189
Создание файлов ключей и сертификатов. 190
Настройка SSL, когда сертификатом управляет центр сертификации. 192
Настройка протокола SSL. 194
8.16 Основные сведения об обмене данными между компонентами платформы BI. 199
Обзор серверов платформы BI и портов обмена данными. 199
Взаимодействие между компонентами платформы BI 202
8.17 Настройка платформы BI для брандмауэров. 213
Настройка системы для использования брандмауэров. 213
Отладка развертывания брандмауэра. 216
8.18 Примеры типовых сценариев развертывания брандмауэров. 218
Пример: уровень приложений развернут в отдельной сети. 218
Пример: толстый клиент и уровень БД отделены брандмауэром от платформы BI 221
8.19 Настройки брандмауэра для интегрированных сред. 223
Рекомендации по настройке брандмауэра для интеграции SAP. 224
Настройка брандмауэра для интеграции с JD Edwards EnterpriseOne. 225
Конкретные рекомендации по настройке брандмауэра для Oracle EBS. 227
Настройка брандмауэра для интеграции с PeopleSoft Enterprise. 228
Настройка брандмауэра для интеграции с Siebel. 229
8.20 Платформа BI и обратные прокси-серверы 230
Понимание механизма развертывания веб-приложений. 231
8.21 Настройка обратных прокси-серверов для веб-приложений платформы BI 231
Подробные инструкции по настройке обратных прокси-серверов. 232
Настройка обратного прокси-сервера. 233
Настройка обратного прокси-сервера Apache 2.2 для платформы BI 233
Настройка обратного прокси-сервера WebSEAL 6.0 для платформы BI 233
Настройка Microsoft ISA 2006 для платформы BI 234
8.22 Специальная настройка для платформы BI при развертывании с обратным прокси-сервером. 236
Включение обратного прокси-сервера для веб-служб 236
Включение пути к корневому каталогу для файлов cookie сеанса для ISA 2006. 239
Включение обратного прокси-сервера для приложения SAP BusinessObjects Live Office 241

9 Аутентификация. 243
9.1 Параметры аутентификации платформы BI. 243
Основная аутентификация. 243
Подключаемые модули безопасности. 244
Единый вход на платформу BI. 245
9.2 Аутентификация Enterprise. 248
Общая информация об аутентификации Enterprise. 248

Настройки аутентификации Enterprise. 249
Изменение параметров Enterprise. 250
Аутентификация SAML 2.0. 252
Установление доверительной аутентификации между сервером приложений Java для SAP NetWeaver и платформой BI. 265
Использование аутентификации SAML 2.0 с сервером приложений Java для SAP NetWeaver. 269
Включение доверительной аутентификации. 269
Настройка доверительной аутентификации для веб-приложения. 272
9.3 Аутентификация LDAP. 282
Использование аутентификации LDAP. 282
Настройка аутентификации LDAP. 284
Сопоставление групп LDAP. 296
9.4 Аутентификация Windows AD. 306
Использование аутентификации Windows AD. 306
Подготовка контроллера домена. 307
Настройка аутентификации AD в CMC. 309
Настройка сервиса платформы BI для запуска SIA. 317
Настройка сервера веб-приложений для аутентификации AD. 320
Настройка единого входа. 328
Устранение неполадок с аутентификацией Windows AD. 346
9.5 Аутентификация SAP. 348
Настройка аутентификации SAP 348
Создание учетной записи пользователя для платформы BI. 349
Подключение к системам контроля полномочий SAP. 351
Настройка параметров аутентификации SAP. 352
Импорт ролей SAP. 357
Настройка защищенного обмена данными (SNC). 361
Настройка единого входа в систему SAP. 375
Настройка единого входа для SAP Crystal Reports и SAP Netweaver. 379
9.6 Аутентификация PeopleSoft. 380
Обзор. 380
Включение аутентификации PeopleSoft Enterprise. 380
Сопоставление ролей PeopleSoft в платформе BI. 381
Планирование пользовательских обновлений. 384
Использование моста безопасности PeopleSoft. 386
9.7 Аутентификация JD Edwards. 396
Обзор. 396
Включение аутентификации JD Edwards EnterpriseOne. 397
Сопоставление ролей JD Edwards EnterpriseOne в платформе BI. 397
Планирование пользовательских обновлений. 400

9.8 Аутентификация Siebel. . . . 402
Включение аутентификации Siebel. . . . 402
Сопоставление ролей платформе BI. . . . 403
Планирование пользовательских обновлений. . . . 406
9.9 Аутентификация Oracle EBS. . . . 408
Разрешение аутентификации Oracle EBS. . . . 408
Сопоставление ролей Oracle E-Business Suite с платформой BI. . . . 409
Неотображаемые роли 413
Настройка прав для назначенных групп и пользователей Oracle EBS 414
Настройка единого входа (SSO) для SAP Crystal Reports и Oracle EBS. . . . 415
9.10 Аутентификация X.509. . . . 416
Аутентификация X.509 для стартовой панели BI. . . . 416
Аутентификация по стандарту X.509 для веб-служб. . . . 424
Аутентификация X.509 для CMC. . . . 427
9.11 Аутентификация OpenID Connect. . . . 430
Активация аутентификации OpenID Connect. . . . 430

10 Ссылка на источник данных. . . . 431
10.1 Расширенное сопоставление учетных данных. . . . 431
Создать ссылку на источник данных. . . . 432
Определение учетных данных базы данных для ссылки на источник данных для пользователя в CMC. . . . 433
Определение учетных данных базы данных для ссылки на источник данных для пользователя на стартовой панели BI. . . . 433
Определить учетные данные базы данных для ссылки на источник данных для группы 434
Связать ссылку на источник данных с соединением OLAP. . . . 434

11 Администрирование сервера. . . . 436
11.1 Работа с областью управления CMC "Серверы". . . . 436
11.2 Управление серверами с помощью скриптов в Windows 439
11.3 Управление серверами в UNIX 439
11.4 Просмотр и изменение статуса сервера. . . . 440
Просмотр состояний серверов. . . . 440
Запуск, остановка и перезапуск серверов. . . . 441
Остановка центрального сервера управления (CMS). . . . 444
Включение и выключение серверов. . . . 444
11.5 Добавление, клонирование и удаление серверов. . . . 446
Добавление, клонирование и удаление серверов. . . . 446
11.6 Добавление пользовательского интернет-заголовка. . . . 449
11.7 Кластеризация центральных серверов управления (CMS). . . . 450
Кластеризация центральных серверов управления (CMS). . . . 450
11.8 Управление группами серверов. . . . 454

Создание группы серверов. 455
Преобразование исключающей группы серверов в неисключающую и наоборот. 457
Работа с подгруппами серверов. 458
Изменение принадлежности сервера к группе. 460
Административный доступ к серверам и группам серверов для пользователей. 461
Сопоставление группы пользователей с группой серверов. 463
Сопоставление папки с группой серверов. 466
Общие сведения об управлении правами для группы серверов. 468
11.9 Настройка адаптивных серверов обработки для производственных систем. 473
11.10 Оценка производительности системы. 474
Мониторинг серверов платформы BI. 474
Анализ серверных показателей. 474
Просмотр системных показателей. 475
Регистрация деятельности сервера. 475
11.11 Конфигурация настроек серверов. 476
Для изменения свойств сервера. 477
Применение параметров службы к нескольким серверам. 477
Работа с шаблонами конфигурации. 478
11.12 Настройка сетевых параметров сервера. 480
Параметры сетевой среды. 481
Параметры идентификации хоста сервера. 482
Настройка группового компьютера. 483
Настройка номеров портов. 486
11.13 Управление узлами. 489
Использование узлов. 489
Добавление нового узла. 492
Восстановление узла. 496
Удаление узла. 500
Переименование узла. 503
Перемещение узла. 505
Параметры скриптов. 509
Добавление зависимостей сервера Windows. 514
Изменение учетных данных пользователя для узла. 515
11.14 Переименование компьютера в развертывании платформы BI. 515
Изменение имен кластеров. 515
Изменение IP-адресов. 516
Переименование компьютеров. 518
11.15 Использование 32-битных и 64-битных сторонних библиотек вместе с платформой BI. 521
11.16 Управление заполнителями сервера и узла. 521
Просмотр заполнителей для сервера. 521
Просмотр и изменение заполнителей для узла. 522

12 Управление базами данных Центрального сервера управления (CMS). 523
12.1 Управление соединением с системной базой данных центрального сервера управления 523
Выбор SAP HANA в качестве базы данных CMS. 523
Выбор SAP HANA в качестве базы данных CMS. 524
12.2 Выбор новой или существующей базы данных центрального сервера управления. 525
Выбор новой или существующей базы данных CMS в Windows. 527
Выбор новой или существующей базы данных центрального сервера управления в UNIX 527
12.3 Повторное создание базы данных системы центрального сервера управления. 528
Восстановление системной базы данных CMS в ОС Windows. 529
Восстановление системной базы данных CMS в ОС UNIX. 529
12.4 Копирование данных из одной базы данных CMS в другую.. 530
Подготовка к копированию системной базы данных CMS. 531
Копирование системной базы данных CMS в Windows. 532
Для копирования данных из базы данных системы центрального сервера управления на UNIX. 532
12.5 Драйвер базы данных Центрального сервера управления. 533

13 Управление серверами контейнера веб-приложений (WACS). 534
13.1 WACS. 534
Сервер контейнера веб-приложений (WACS). 534
Добавление дополнительных серверов WACS в систему и их удаление. 537
Добавление или удаление служб на сервере WACS. 540
Настройка HTTPS/SSL. 541
Поддерживаемые методы аутентификации. 545
Настройка Kerberos AD для WACS 546
Настройка единого входа в AD Kerberos 553
Настройка веб-служб RESTful. 556
Сервер контейнера веб-приложений (WACS) и ваша IT-среда. 566
Настройка свойств веб-приложений. 568
Устранение неполадок. 569
Свойства WACS. 573

14 Резервное копирование и восстановление системы. 575
14.1 Обзор резервного копирования и восстановления. 575
14.2 Терминология. 575
14.3 Случаи использования резервного копирования и восстановления. 577
14.4 Резервные копии. 578
Резервное копирование всей системы. 579
Резервное копирование настроек сервера. 583
Резервное копирование платформы BI. 586
14.5 Восстановление системы. 586

Восстановление всей системы. . . . 587
Восстановление настроек сервера. . . . 594
Восстановление содержимого BI. . . . 597
14.6 Скрипты BackupCluster и RestoreCluster. . . . 597

15 Копирование развертывания платформы BI. . . . 601
15.1 Обзор копирования системы. . . . 601
15.2 Терминология. . . . 601
15.3 Ситуации, в которых может потребоваться копирование системы. . . . 602
15.4 Планирование копирования системы. . . . 602
15.5 Рекомендации и ограничения. . . . 604
15.6 Процедура копирования системы. . . . 605
Экспорт из исходной системы. . . . 606
Импорт в целевую систему. . . . 609

16 Управление повышением. . . . 613
16.1 Введение в управление переносом объектов. . . . 613
Обзор. . . . 613
Функции. . . . 613
Права доступа к приложению. . . . 614
Поддержка WinAD в управлении переносами. . . . 615
16.2 Начало работы со средством "Диспетчер переноса объектов". . . . 615
Запуск Диспетчера переноса объектов. . . . 615
Компоненты пользовательского интерфейса. . . . 616
Использование параметра настройки. . . . 618
16.3 Использование Диспетчера переноса объектов. . . . 625
Создание и удаление папок. . . . 626
Создание задания. . . . 628
Создание нового задания путем копирования существующего. . . . 630
Поиск задания. . . . 631
Редактирование задания. . . . 632
Добавление объекта InfoObject в задание. . . . 632
Управление зависимостями задания. . . . 633
Поиск зависимых объектов. . . . 635
Повышение задания при соединении с репозиториями. . . . 635
Перенос задания с помощью файла LCMBIAR. . . . 638
Планирование переноса задания. . . . 642
Просмотр журнала заданий. . . . 644
Откат задания. . . . 644
16.4 Перенос всего содержимого репозитория с помощью Диспетчера переноса объектов. . . . 647
Подготовка исходной и целевой систем. . . . 647
Стратегии миграции. . . . 649

16.5 Шаги полного переноса системы. . . . 650
Перенос пользователей и групп пользователей (задание 1). . . . 651
Перенос зависимых объектов (задание 2). . . . 651
Перенос основных объектов (задание 3). . . . 652
После переноса. . . . 653
16.6 Использование опции "Командная строка". . . . 654
Запуск программы командной строки в Windows. . . . 654
Запуск командной строки в Unix. . . . 655
Параметры командной строки. . . . 655
Образец файла свойств. . . . 680
16.7 Использование Enhanced Change and Transport System. . . . 681
Предварительные требования. . . . 682
Настройка платформы BI и интеграции с CTS+. . . . 682
Перенос заданий с помощью CTS. . . . 689
16.8 Использование мастера диспетчера переноса объектов 692
Исключение объектов из переноса. . . . 693
Когда используется мастер диспетчера переноса объектов. . . . 694
Сценарий. . . . 695
Объекты. . . . 697
Зависимости. . . . 701
Общие сведения. . . . 702
(необязательно) Файл свойств. . . . 703
Мастер диспетчера переноса объектов в Linux. . . . 706

17 Управление версиями. . . . 707
17.1 Управление различными версиями объекта InfoObject. . . . 707
Права доступа к приложению управления версиями. . . . 707
Резервное копирование и восстановление файлов Subversion. . . . 708
17.2 Управление разными версиями ресурсов BI. . . . 709
17.3 Запуск и остановка Subversion вручную в Unix. . . . 711
17.4 Необходимые файлы для Subversion в Solaris 10 и RedHat Linux 5. . . . 711
17.5 Использование Apache Subversion в качестве системы управления версиями. . . . 712
17.6 Использование Git в качестве системы управления версиями. . . . 713
17.7 Параметры системы управления версиями по умолчанию. . . . 714
17.8 Сравнение разных версий одного задания. . . . 714
17.9 Обновление содержимого Subversion. . . . 715
17.10 Настройка Subversion для кластеризованных серверов обработки заданий. . . . 715
Вариант А: настройка основного компьютера Subversion до любых операций системы управления версиями. . . . 715
Вариант Б: настройка Subversion после создания каталога рабочих копий системой управления версиями. . . . 716
Настройка других компьютеров с Subversion. . . . 717

18 Управление приложениями. 718
18.1 Выключение всплывающего сообщения GDPR. 718
18.2 Управление приложениями с помощью CMC. 720
Обзор. 720
Общие настройки приложений. 721
Настройки, зависящие от приложения. 723
18.3 Управление приложениями с помощью свойств семантического уровня. 783
18.4 Управление приложениями с помощью свойств BOE.war. 784
Файл BOE.war. 784
18.5 Настройка точек входа в систему для стартовой панели BI и OpenDocument. 802
Местоположения файлов стартовой панели BI и OpenDocument. 803
Определение пользовательской страницы входа в систему. 804
Добавление доверительной аутентификации при входе в систему. 805
18.6 Настройка пользовательских интерфейсов приложений. 806
Web Intelligence. 806
Стартовая панель BI. 812
18.7 Настройка веб-служб RESTful платформы BI на веб-сервере. 813
18.8 Гибридное управление пользователями. 817
18.9 Провизионирование локальных пользователей в SAP Analytics Cloud. 817
Установить соединение между локальной системой и облаком. 818
18.10 Создание учетных данных клиента OAuth в SAP Analytics Cloud. 819
18.11 Настроить исходную систему. 820
18.12 Настроить целевую систему. 821
18.13 Провизионирование пользователей и групп пользователей в SAP Analytics Cloud. 822
18.14 Просмотр провизионированных пользователей в SAP Analytics Cloud. 822
18.15 Образцы шаблонов. 823

19 Управление соединениями и юниверсами. 827
19.1 Управление соединениями. 827
Для удаления соединения юниверса. 827
19.2 Управление Юниверсами. 828
Удаление юниверсов. 829

20 BI Admin Studio. 830
20.1 Рабочее место администратора. 831
Рабочее место администратора. 831
Бизнес-аналитическая информация о серверах. 832
BI в экземплярах документов. 833
BI – пользователи и сеансы. 834
Бизнес-аналитическая информация об использовании контента. 834
Бизнес-аналитическая информация о приложениях. 835
20.2 Мониторинг. 836

Термины мониторинга. . . . 837
Настройка поддержки баз данных в приложении мониторинга. . . . 840
Свойства конфигурации. . . . 848
Интеграция с другими приложениями. . . . 855
Поддержка кластеров для сервера мониторинга. . . . 855
Устранение неполадок. . . . 856
20.3 Визуальное отличие. . . . 859
Сравнение объектов и файлов с использованием функции визуального отличия. . . . 860
Сравнение объектов и файлов с помощью системы управления версиями. . . . 861
20.4 Авторизация элементов HTML. . . . 862
Изменение списка авторизованных элементов HTML. . . . 864

21 Отчетность CMS. . . . 866
21.1 Отчетность CMS. . . . 866
Архитектура платформы SAP BusinessObjects. . . . 866
Структура базы данных системы CMS. . . . 867
Об объектах InfoObject. . . . 869
21.2 Обзор системы отчетности CMS. . . . 872
21.3 Соединение с базой данных CMS. . . . 873
21.4 Образец комплекта отчетности CMS. . . . 874
Импорт образца комплекта отчетности CMS с помощью диспетчера переноса объектов . . . 874
Образец юниверса CMS . . . 875
Расширение образца юниверса CMS. . . . 875
21.5 Создание отчета в CMS. . . . 876

22 Workflow Assistant. . . . 877
22.1 Целевая аудитория. . . . 878
22.2 Общие сведения об архитектуре. . . . 878
22.3 Глоссарий. . . . 879
22.4 Об установке и обновлении. . . . 882
22.5 Настройка Workflow Assistant. . . . 883
Базовая конфигурация. . . . 883
22.6 Управление правами Workflow Assistant через Central Management Console. . . . 886
22.7 Работа с Workflow Assistant. . . . 891
О стандартных шаблонах задач. . . . 891
О стандартных моделях потока операций. . . . 901
О пользовательских шаблонах задач. . . . 902
Управление моделями потока операций. . . . 902
Управление сценариями и просмотр результатов. . . . 904
Общие сведения о состояниях шаблонов задач, моделей потока операций и сценариев . . . 910

Работа с системами. . . . 911
Непрерывное выполнение Workflow Assistant. . . . 914
22.8 Проверка файлов журналов. . . . 915

23 Корзина. . . . 916
23.1 Корзина. . . . 916
Восстановление элементов из корзины. . . . 916
Удаление элементов из корзины без возможности восстановления. . . . 917
Включение автоматической очистки корзины. . . . 917

24 Аудит. . . . 919
24.1 Обзор. . . . 919
24.2 Страница "Аудит CMC". . . . 925
Состояние аудита. . . . 926
Настройка аудита событий. . . . 927
Параметры конфигурации хранилища данных аудита. . . . 932
24.3 События аудита. . . . 933
Audit events and details. . . . 942

25 События. . . . 965
25.1 Общие сведения о событиях. . . . 965
Уведомления пользователей. . . . 966

26 Поиск по платформе. . . . 970
26.1 Описание поиска по платформе. . . . 970
Platform Search SDK. . . . 970
Кластеризованная среда. . . . 970
26.2 Настройка поиска по платформе. . . . 971
Развертывание OpenSearch. . . . 971
Настройка обратного прокси. . . . 973
Настройка свойств приложения в CMC. . . . 973
26.3 Работа с поиском по платформе. . . . 981
Индексация содержимого в репозитории CMS. . . . 981
Список сбоев индексации. . . . 982
Результаты поиска. . . . 983
26.4 Интеграция поиска по платформе с SAP NetWeaver Enterprise Search. . . . 989
Создание соединителя в SAP NetWeaver Enterprise Search . . . 990
Импорт роли пользователя на платформу BI. . . . 990
26.5 Поиск из SAP NetWeaver Enterprise Search. . . . 991
26.6 Выполнение аудита. . . . 991
26.7 Устранение неполадок. . . . 993
Самовосстановление. . . . 993
Проблемные сценарии. . . . 993

27 Интеграция. 996
27.1 Интеграция. 996
27.2 Термины для функции интеграции. 997
27.3 Управление правами безопасности. 999
Права, необходимые на сайте-источнике. 999
Права, необходимые на сайте-адресате. 1000
Права, характерные для интеграции. 1001
Тиражирование безопасности объекта. 1002
Тиражирование параметров безопасности с использованием уровней доступа. 1003
27.4 Параметры типов и режимов тиражирования. 1004
Однонаправленное тиражирование 1004
Двунаправленное тиражирование 1004
"Обновлять из источника" или "Обновлять из адресата". 1005
27.5 Тиражирование сторонних пользователей и групп. 1006
27.6 Тиражирование юниверсов и соединений юниверсов. 1008
27.7 Управление списками тиражирования. 1009
Создание списков тиражирования. 1010
Изменение списков тиражирования. 1012
27.8 Управление удаленными соединениями. 1013
Создание удаленных соединений. 1013
Изменение удаленных соединений. 1015
27.9 Управление заданиями тиражирования. 1015
Создание заданий тиражирования. 1016
Планирование заданий тиражирования. 1018
Изменение заданий тиражирования. 1018
Просмотр журнала после выполнения задания тиражирования. 1019
27.10 Управление очисткой объектов. 1019
Способ использования очистки объектов. 1020
Ограничения очистки объектов. 1020
Частота очистки объектов. 1021
27.11 Управление обнаружением и разрешением конфликтов. 1022
Разрешение конфликтов однонаправленного тиражирования. 1022
Разрешение конфликта двунаправленного тиражирования. 1024
27.12 Использование веб-служб в функции интеграции. 1028
Переменные сеанса 1028
Кэширование файлов 1029
Настраиваемое развертывание 1029
27.13 Удаленное планирование и экземпляры, выполняемые локально. 1030
Удаленное планирование. 1030
Экземпляры, выполняемые локально. 1032
Совместное использование экземпляров. 1033

27.14 Импорт и перенос тиражированного содержимого. . . . 1034
Импорт тиражированного содержимого. . . . 1034
Импорт тиражированного содержимого и продолжение тиражирования 1034
Перенос содержимого из тестовой среды. . . . 1035
Повторное назначение сайта-адресата. . . . 1036
27.15 Оптимальные методы работы. . . . 1036
Текущие ограничения выпуска. . . . 1040
Устранение неисправностей: сообщения об ошибках. . . . 1041

28 Дополнительные конфигурации для сред ERP. . . . 1046
28.1 Конфигурации для интеграции с SAP NetWeaver. . . . 1046
Интеграция с SAP Business Warehouse (BW). . . . 1046
28.2 Настройка для интеграции с JD Edwards. . . . 1092
Настройка единого входа (SSO) для SAP Crystal Reports. . . . 1092
Настройка протокола SSL для интеграции с JD Edwards. . . . 1093
28.3 Настройка для интеграции с PeopleSoft Enterprise. . . . 1095
Настройка единого входа (SSO) для SAP Crystal Reports и PeopleSoft Enterprise. . . . 1095
Настройка соединений по протоколу SSL. . . . 1096
Настройка производительности для систем PeopleSoft. . . . 1097
28.4 Настройка для интеграции с Siebel. . . . 1099
Настройка Siebel для интеграции с платформой SAP BI. . . . 1099
Создание пункта меню "Crystal Reports". . . . 1100
Контекстуальная зависимость. . . . 1101
Настройка единого входа (SSO) для SAP Crystal Reports и Siebel. . . . 1104
Настройка соединений по протоколу SSL. . . . 1104

29 Управление журналами и их настройка. . . . 1107
29.1 Ведение журнала трассировок компонентов. . . . 1107
29.2 Уровни журнала трассировки. . . . 1107
29.3 Настройка трассировки для серверов. . . . 1108
Настройка уровня журнала в CMC. . . . 1109
Установка уровня журнала для нескольких серверов в CMC. . . . 1109
Настройка серверной трассировки с использованием файла BO_trace.ini. . . . 1110
29.4 Настройка трассировки для веб-приложений. . . . 1112
Настройка уровня журнала трассировки веб-приложения в CMC. . . . 1113
Настройка параметров трассировки с использованием файла `BO_trace.ini`. . . . 1114
29.5 Настройка трассировки для клиентских приложений платформы BI. . . . 1119
29.6 Настройка расширенной трассировки сообщений об ошибках. . . . 1120
29.7 Включение файлов журнала с подробной информацией о сообщениях об ошибках. . . . 1120

30 Интеграция с SAP Solution Manager. . . . 1122
30.1 Обзор интеграции. . . . 1122

30.2 Контрольный список по интеграции SAP Solution Manager. 1122
30.3 Управление регистрацией System Landscape Directory. 1123
Регистрация платформы BI в System Landscape. 1123
Точки запуска SLD. 1125
Очистка SLD перед установкой исправлений. 1125
Ведение журнала SLD-соединения 1126
Имя виртуального хоста. 1126
30.4 Управление агентами Solution Management Diagnostics. 1127
Обзор Solution Manager Diagnostics (SMD). 1127
Работа с SMD-агентами. 1127
Учетная запись пользователя SMAdmin. 1128
30.5 Инструментальные средства управления производительностью. 1129
Настройка инструментов мониторинга производительности для платформы BI. 1129
Настройка инструментальных средств мониторинга производительности для платформы BI. 1129
Настройка конфигурации производительности для веб-уровня. 1131
Файлы журнала настройки конфигурации 1131
30.6 Трассировка с использованием SAP Passport. 1131

31 Администрирование в командной строке. 1133
31.1 Скрипты UNIX. 1133
Утилиты скриптов. 1133
Шаблоны скриптов. 1139
Скрипты, используемые платформой BI. 1139
31.2 Скрипты Windows. 1141
ccm.exe. 1141
31.3 Командные строки сервера. 1144
Обзор командных строк. 1144
Стандартные параметры для всех серверов. 1145
Центральный сервер управления. 1145
Сервер обработки Crystal Reports и кэш-сервер Crystal Reports. 1147
Серверы заданий. 1148
Адаптивный сервер обработки. 1149
Сервер приложений отчетов. 1149
Сервер обработки Web Intelligence. 1152
Серверы репозитория входящих и исходящих файлов. 1153
Сервер событий. 1156

32 Repository Diagnostic Tool. 1157
32.1 Обзор инструмента Repository Diagnostic Tool. 1157
32.2 Использование Repository Diagnostic Tool. 1158
Использование Repository Diagnostic Tool. 1158

Параметры Repository Diagnostic Tool. 1159
32.3 Несоответствия между CMS и FRS. 1169
32.4 Несоответствия в метаданных CMS. 1170
32.5 Управление SDK Restful в веб-приложении BOE. 1173

33 HTTP Strict Transport Security (HSTS). 1175
33.1 Настройка HTTP Strict Transport Security (HSTS). 1175

34 Приложение "Права". 1176
34.1 О приложении "Права". 1176
34.2 Общие права. 1176
Права назначения. 1180
34.3 Права для определенных типов объектов. 1181
Права доступа к папке. 1181
Категории. 1181
Отчеты Crystal. 1182
Документы Web Intelligence. 1182
Пользователи и группы. 1183
Уровни доступа. 1185
Права юниверсов (.unv). 1185
Права юниверсов (.unx). 1187
Уровни доступа к объектам для юниверсов. 1188
Права соединений. 1190
Приложения. 1191

35 Приложение "Свойства серверов". 1200
35.1 О приложении "Свойства серверов". 1200
Общие свойства сервера. 1200
Свойства основных служб. 1202
Свойства служб соединения. 1215
Свойства служб Crystal Reports. 1219
Свойства служб Analysis. 1229
Свойства служб объединения данных. 1230
Свойства служб Web Intelligence. 1231

36 Приложение "Показатели сервера". 1240
36.1 О приложении "Показатели сервера". 1240
Общие показатели сервера. 1240
Показатели центрального сервера управления. 1242
Показатели сервера соединений. 1246
Показатели сервера событий. 1246
Показатели сервера репозитория файлов. 1247
Показатели адаптивного сервера обработки. 1247

Показатели сервера контейнера веб-приложений. 1252
Показатели адаптивного сервера заданий. 1253
Показатели Crystal Reports Server. 1254
Показатели сервера Web Intelligence. 1257

37 Приложение заполнителя сервера и узла. 1259
37.1 Заполнители сервера и узлов. 1259

38 Приложение выполнения аудита схемы хранилища данных. 1269
38.1 Обзор. 1269
38.2 Диаграмма схемы. 1269
38.3 Auditing Data Store Tables. 1269

39 Приложение "Схема базы данных мониторинга". 1277
39.1 Схема базы данных тенденций. 1277

40 Приложение "Рабочая таблица системной копии". 1280
40.1 Рабочая таблица системной копии. 1280

1 История документа

В следующей таблице описываются наиболее важные изменения документа.

Версия	Дата	Описание
Платформа SAP BusinessObjects Business Intelligence 4.3 SP3	Декабрь 2022 г.	В следующих разделах добавлено новое поле максимальной длины пароля для аутентификации Enterprise: • Настройки аутентификации Enterprise [страница 249] • Создание учетной записи пользователя [страница 107] • Изменение общих настроек пароля [страница 116] • Изменение общих настроек пароля [страница 251] • Добавлен активируемый параметр "Использовать относительный путь URL", чтобы использовать относительный URL-адрес браузера.
Платформа SAP BusinessObjects Business Intelligence 4.3 SP2	Декабрь 2021 г.	Добавлен раздел Конфигурация сервера авторизации [страница 778]. Обновлен раздел Пользовательская настройка элементов интерфейса Web Intelligence по группам пользователей и папкам [страница 806].

Платформа SAP BusinessObjects Business Intelligence 4.3 SP1	Декабрь 2020 г.	• Добавлены следующие новые разделы:
		  • Раздел о настройке пользовательского интерфейса Web Intelligence. См. Пользовательская настройка элементов интерфейса Web Intelligence по группам пользователей и папкам [страница 806].
		  • Скрипт для очистки устаревших сеансов [страница 165].
		  • Определение учетных данных базы данных для ссылки на источник данных для пользователя на стартовой панели BI [страница 433]
		  • Конфигурация JMX SSL [страница 852]
		• Обновлены два раздела:
		  • Варианты обновления [страница 30].
		  • Права назначения [страница 1180] для *Параметров места назначения* и *Свойств места назначения электронной почты* с новым введенным полем *Ответить кому* для всех сценариев публикации.

Версия	Дата	Описание
Платформа SAP BusinessObjects Business Intelligence 4.3	Июнь 2020 г.	• SAP BusinessObjects Explorer, SAP BusinessObjects Dashboards, средство преобразования отчетов, средство управления обновлением и виджеты BI были исключены из версии 4.3. • Добавлен новый раздел Workflow Assistant [страница 877].

2 Начало работы

2.1 О данном руководстве

В этом руководстве описываются процедуры развертывания и настройки платформы SAP BusinessObjects Business Intelligence (платформа «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 предназначено данное руководство?

В этом руководстве описываются развертывание и настройка платформы BI. Используйте его при выполнении следующих задач:

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

Руководство предназначено для системных администраторов, выполняющих настройку и обслуживание платформы BI, а также управляющих ею. Администраторам пригодится знание операционной системы и сетевой среды, а также общее 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 Общие сведения о платформе Business Intelligence

Платформа Business Intelligence (BI) – это гибкое и масштабируемое решение для предоставления конечным пользователям информации различного вида, включая инструментальные панели и интерактивные отчеты, посредством сетевых приложений – локальных сетей, Интернета или корпоративного портала.

Платформа предоставляет интегрированный пакет функций отчетности, анализа и получения информации в рамках всей организации и за ее пределами.

Кроме того, она позволяет повысить эффективность работы конечных пользователей и сократить объемы действий административного характера.

Например, платформа используется для рассылки еженедельных отчетов о продажах, предоставления клиентам персонализированных предложений услуг и интеграции критически важной информации на корпоративные порталы.

2.1.3 Переменные

В настоящем руководстве используются перечисленные ниже переменные.

Переменная	Описание
`<INSTALLDIR>`	Каталог установки платформы BI. На компьютере под управлением Windows каталог по умолчанию – `C:\Program Files (x86)\SAP BusinessObjects`.
`<PLATFORM64DIR>`	Имя операционной системы Unix. Допустимы следующие значения: • aix_rs6000_64 • linux_x64 • solaris_sparcv9 • hpux_ia64
`<SCRIPTDIR>`	Каталог, где расположены скрипты администрирования платформы BI. На компьютере под управлением ОС Windows это каталог`<КАТАЛОГ_УСТАНОВКИ>`\SAP `BusinessObjects Enterprise XI 4.0\win64_x64\scripts`. На компьютере под управлением Unix это каталог `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj/enterprise_xi40/<PLATFORM64DIR>/scripts`.

2.1.4 Терминология

В документации по платформе BI используются следующие термины:

Термин	Определение
Дополнительные компоненты	Продукты, которые работают с платформой BI, но имеют собственную программу установки.
Хранилище данных аудита (ADS)	База данных, используемая для хранения данных аудита

Термин	Определение
Платформа BI	Сокращение для "платформа SAP BusinessObjects Business Intelligence"
Связанная база данных; связанный сервер веб-приложений	База данных или сервер веб-приложений, входящие в комплект поставки платформы BI
Кластер	Два или несколько Центральных серверов управления (CMS), которые работают совместно и используют одну базу данных CMS
Кластеризация	Создание кластера: 1. Установите Центральный сервер управления и базу данных CMS на компьютер A. 2. Установите Центральный сервер управления на компьютер Б. 3. Привяжите Центральный сервер управления на компьютере Б к базе данных CMS на компьютере A.
Ключ кластера	Используется для расшифровки ключей в базе данных CMS. Ключ кластера можно изменить в CCM, но нельзя сбросить, как пароль. Он содержит зашифрованное содержимое, и его важно не терять.
CMS	Сокращение для "Центральный сервер управления"
база данных CMS	База данных, используемая Центральным сервером управления для хранения информации о платформе BI
Развертывание	Программное обеспечение платформы BI, установленное, настроенное и выполняющееся на одном или нескольких компьютерах
Установка	Экземпляр файлов платформы BI на компьютере, созданный с помощью программы установки
Компьютер	Компьютер, где установлено программное обеспечение платформы BI
Основная версия	Полная версия программного обеспечения
Отладочная версия	Выпуск некоторых компонентов программного обеспечения
Узел	Группа серверов платформы BI, которая выполняется на одном компьютере и управляется одним агентом SIA

Термин	Определение
Исправление	Небольшое обновление для конкретной версии пакета поддержки
Перенос объектов	Процесс переноса содержимого BI между развертываниями с одинаковыми основными версиями (например, из версии 4.3 в 4.3) с использованием приложения "Диспетчер переноса объектов"
Сервер	Процесс платформы BI. На сервере размещаются одна или несколько служб
Server Intelligence Agent (SIA)	Процесс, управляющий группой серверов, включая остановку, запуск и перезапуск серверов
Пакет поддержки	Обновление ПО для отладочной или основной версии
Сервер веб-приложений	Сервер, обеспечивающий обработку динамического содержимого
Обновление	Операции планирования, подготовки, миграции и последующей обработки, необходимые для выполнения процесса миграции
ЕДИНЫЙ установщик	ЕДИНЫЙ установщик – это отдельный пакет установки, который поддерживает несколько сценариев установки BI, например новую установку сервисного пакета или исправления, любой переход с одного исправления на другое или любой переход с сервисного пакета на исправление.

2.2 Перед началом работы

2.2.1 Основные понятия

2.2.1.1 Server Intelligence

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

На Центральном сервере управления хранится информация о серверах в базе данных системы CMS, с помощью которой можно легко восстановить их настройки по умолчанию. SIA периодически запрашивает в CMS информацию об управляемых серверах, поэтому имеет сведения о необходимых серверах состояния и требуемых действиях.

> ⓘ Примечание
>
> 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. Поддержка нескольких установок программного обеспечения на одном компьютере возможна только для платформ Unix. Если каждая установка выполняется под уникальной учетной записью пользователя и помещается в отдельную папку, то у этих установок нет совместно используемых файлов. Следует помнить, что все компьютеры в кластере должны иметь одинаковые версии и уровни пакетов исправлений.

Связанные сведения

Серверы, хосты и кластеры [страница 39]

2.2.1.2 Серверы, службы, узлы и хосты

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

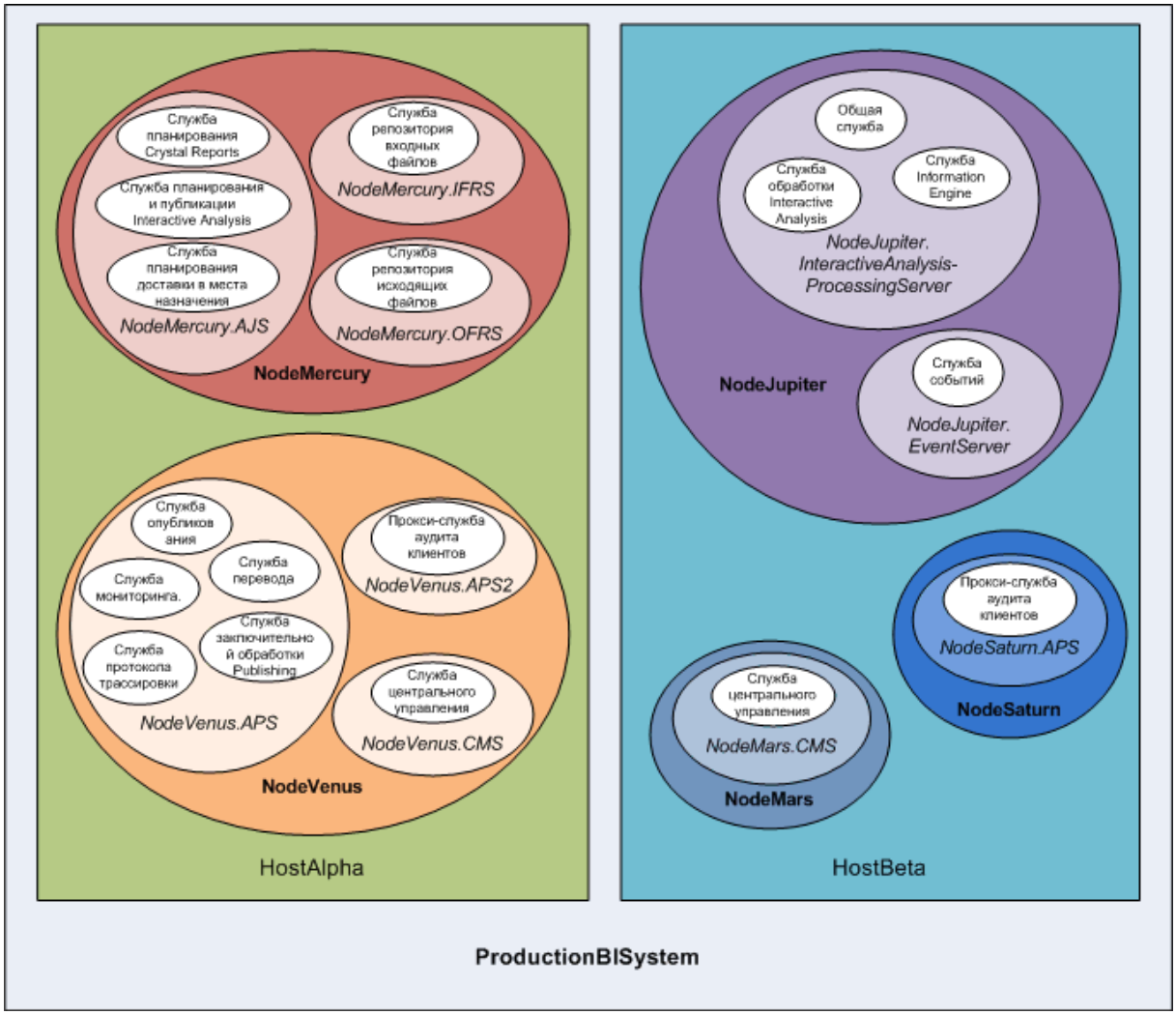
Термином «сервер» обозначается процесс уровня операционной системы (в некоторых системах он носит название демон), в котором размещаются одна или несколько служб. В качестве примера подобного сервера можно привести Центральный сервер управления (CMS) и адаптивный сервер обработки. Сервер запускается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

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.

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).

На следующем рисунке 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 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.

2.2.2 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 продуктов 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.

> ⓘ Примечание
>
> В продуктивных системах рекомендуется не настраивать автоматический запуск мастера, чтобы избежать случайных изменений конфигурации.

> ⓘ Примечание
>
> Рекомендуется выполнить полное резервное копирование, прежде чем использовать мастер для внесения изменений в существующую систему.

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.

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.

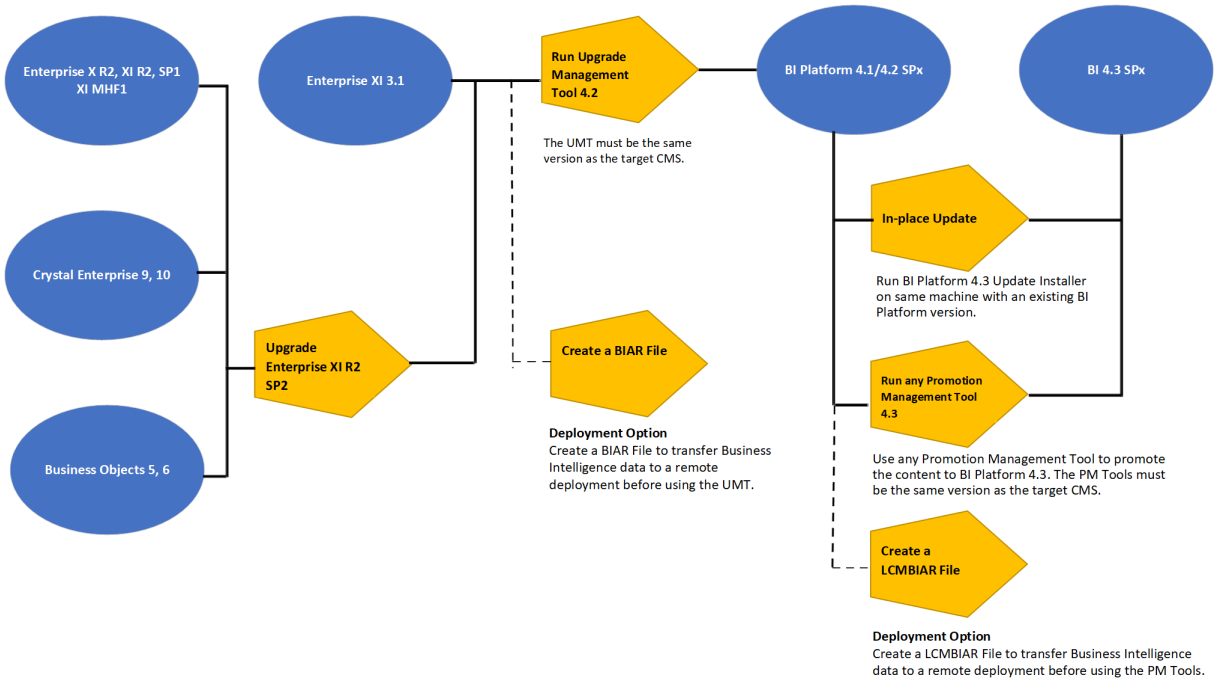
> ⓘ Примечание
>
> В продуктивных системах рекомендуется регулярно выполнять RDT, отключив при этом опцию «исправление», для поиска ошибок в системе. Выполняйте RDT с включенным параметром исправления, только если требуется внести исправления в систему.

2.2.2.5 Средство управления апгрейдом

Не рекомендуется использовать средство UMT в версии BI 4.3, так как оно устарело. Для получения дополнительных сведений см. 2801797

2.2.2.6 Варианты обновления

Можно выполнить миграцию данных системы и контента Business Intelligence из предыдущих версий BI 4.x в платформу SAP BusinessObjects Business Intelligence 4.3.



Средство управления обновлением не рекомендуется использовать в платформе SAP BusinessObjects Business Intelligence 4.3, однако можно перейти на версию 4.3 с помощью указанных ниже вариантов обновления.

При наличии развертывания более ранней версии используйте следующие правила его обновления до платформы BI 4.3:

1. Если текущее развертывание – XI R2, XI MHF1, XI R2 SP1, BusinessObjects 5/6 или Crystal Enterprise 9/10, необходимо сначала выполнить обновление до версии XI R2 SP2 (или более поздней) и затем перейти к шагу 3.
2. Если текущее развертывание – XI 3.x, можно сразу перейти к обновлению, описанному в шаге 3.
3. Установите BI 4.1/4.2 SPx на отдельном компьютере и запустите инструмент управления обновлениями из версии 4.1/4.2 SPx, чтобы выполнить миграцию контента из вышеупомянутых версий на уровень BI 4.1/4.2 SPx.
4. После миграции контента на уровень BI 4.1/4.2 SPx, можно перейти к версии 4.3, используя один из следующих способов:
   1. Запустите программное обеспечение для установки обновлений BI 4.3.x на компьютере на уровне 4.1/4.2 SPx или
   2. Установите BI 4.3 на отдельном компьютере и используйте Диспетчер переноса объектов на BI 4.3.x для переноса контента с уровня BI 4.1/4.2 SPx на уровень BI 4.3.x.

ⓘ Примечание

1. Чтобы перенести контент с уровня BI 4.1/4.2 SPx на уровень BI 4.3.x, версии Диспетчера переноса объектов и целевого сервера CMS должны совпадать.
2. Дополнительные сведения об обновлении BusinessObjects 5/6 до версии XI 3.1 см. в Руководстве по миграции и Руководстве по установке платформы BI соответствующей версии, которые доступны по адресу https://help.sap.com/viewer/product/SAP_BUSINESSOBJECTS_ENTERPRISE_BUSINESS_INTELLIGENCE_PLATFORM/XI.3.1/en-US.

3. С помощью средства управления обновлением (UMT) можно обновить в развертывании только функции сервера и веб-уровня. Для получения дополнительной информации об UMT см. Руководство по обновлению платформы Business Intelligence соответствующей версии, которое доступно по адресу https://help.sap.com/viewer/product/SAP_BUSINESSOBJECTS_BUSINESS_INTELLIGENCE_PLATFORM/4.2/en-US.

2.2.3 Ключевые задачи

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

Связанные сведения

Планирование или выполнение первого развертывания системы [страница 32]
Настройка развертывания [страница 33]
Повышение производительности системы [страница 33]
Central Management Console (CMC) [страница 29]

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:

- Сведения о компонентах платформы BI см. в разделе «Обзор архитектуры».
- «Обмен данными между компонентами платформы BI»
- «Настройки 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 CMC»

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

Связанные сведения

Обзорная информация по архитектуре [страница 35]
Взаимодействие между компонентами платформы BI [страница 202]
Обзор вопросов безопасности [страница 158]
Параметры аутентификации платформы BI [страница 243]
Работа с областью управления CMC "Серверы" [страница 436]

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:

Связанные сведения

Вводные сведения о мастере настройки системы [страница 91]
Взаимодействие между компонентами платформы BI [страница 202]
Обзор вопросов безопасности [страница 158]
Мониторинг [страница 836]

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:

- Дополнительные сведения о настройке системы на основе шаблона развертывания см. в разделе «Вводные сведения о мастере настройки системы».
- 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 CMC, ознакомьтесь с разделом «Работа с областью управления серверами в среде CMC».

Связанные сведения

Вводные сведения о мастере настройки системы [страница 91]
Мониторинг [страница 836]

Работа с областью управления CMC "Серверы" [страница 436]

2.2.3.4 Работа с объектами в CMC

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 CMC, прочтите следующие разделы:

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

Связанные сведения

Обзор управления учетными записями [страница 104]
Права на платформе BI [страница 129]

3 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
>
> Список поддерживаемых платформ, языков, баз данных, серверов веб-приложений, веб-серверов и других систем, поддерживаемых в данном выпуске, см. в *матрице доступности продуктов* (PAM), доступной по адресу http://service.sap.com/sap/support/pam?hash=pvnr%3D67837800100900006540.

> ⓘ Примечание
>
> Поскольку PAM постоянно обновляется, всегда смотрите онлайн-версию PAM, а не загруженную копию.

Платформа Business Intelligence (BI) рассчитана на высокую производительность при использовании различными пользователями и в различных сценариях развертывания. 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 с другими технологическими системами 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 создания юниверсов
  - Query as a Web Service
  - Средство дизайна информации (ранее "Дизайнер информации")
  - Средство управления переводами (ранее "Диспетчер переводов")
- Клиенты, доступные отдельно:
  - SAP Crystal Reports
  - SAP BusinessObjects Analysis (ранее Voyager)

- Рабочие пространства BI (ранее Dashboard Builder)

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

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

Для обеспечения гибкости, надежности и расширяемости компоненты платформы BI можно установить на один или несколько компьютеров. В некоторых случаях можно установить две различные версии платформы BI 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 – это платформа Business Intelligence (BI), которая предоставляет средства анализа данных и создания отчетов на корпоративном уровне для более эффективного предоставления информации. 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 диаграмме архитектуры 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. Диаграмма архитектуры BI 4.3.

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 BI, 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 решение SAP Crystal Reports (доступное и установленное отдельно).

Начиная с SAP BI 4.3, приложения настольного клиента (Web Intelligence Rich Client, средство дизайна информации, средство создания юниверсов и т. д.) являются 64-разрядными. Они больше не являются 32-разрядными приложениями.

Веб-уровень

Веб-уровень содержит веб-приложения, развернутые на сервере приложений Java. Веб-приложения предоставляют конечным пользователям функции платформы BI через веб-браузер. К примерам веб-приложений относятся веб-интерфейс администрирования консоли CMC и стартовая панель BI.

Веб-уровень включает также веб-службы. Веб-службы предоставляют программным средствам через сервер веб-приложений функции платформы BI, такие 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 BI с продуктами Microsoft Office.

Уровень управления

Уровень управления (уровень обработки данных) координирует и контролирует все компоненты, составляющие платформу BI. Он состоит из Центрального сервера управления (CMS) и сервера событий, а также связанных служб. CMS выполняет ведение данных безопасности и конфигурации, отправляет служебные запросы на серверы, управляет аудитом и ведет системную базу данных CMS. Сервер событий управляет событиями на основе файлов, которые возникают на 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`, `.unx`.

> **Примечание**
>
> Размер хранилища файлов репозитория входных файлов не регулируется системой, поэтому администратор должен управлять планом мониторинга и обслуживания.

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

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

Уровень обработки

На уровне обработки анализируются данные и составляются отчеты, а также создаются другие виды вывода. Это единственный уровень, который обращается к базам данных, содержащим данные отчетов. Этот уровень состоит из адаптивного сервера заданий, сервера соединений (64-разрядного) 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 BI используется несколько различных баз данных.

- База данных отчетов
  Используется для хранения данных организации. Это исходные данные, используемые для анализа и отчетов 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
  База данных системы CMS используется для хранения данных платформы BI, таких как сведения о пользователе, сервере, папке, документе, конфигурации и аутентификации. 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 на платформе BI. Эти сведения могут использоваться для мониторинга использования системных компонентов, активности пользователей и других параметров ежедневных операций.
- База данных мониторинга
  Приложение мониторинга использует хранилище данных аудита (ADS) для хранения сведений о системной конфигурации и компонентах, предназначенных для обеспечения поддержки SAP.
- База данных Commentary
  BI Commentary — это новое приложение в CMC. Оно позволяет пользователям совместно комментировать данные и статистику в документе.
  База данных Commentary конфигурируется в той же базе данных, что и база данных аудита. Она создается по умолчанию в базе данных аудита.

Если сервер для работы с базами данных системы CMS и хранилища данных аудита отсутствует, он может автоматически создаваться и настраиваться программой установки платформы BI. Рекомендуется проанализировать сведения, предоставляемые поставщиком сервера базы данных, чтобы определить базу данных, которая лучше всего отвечает требованиям организации.

> ⓘ Примечание
>
> Базу данных SQL Anywhere по умолчанию не рекомендуется использовать для продуктивных систем. Она входит в состав пакетов серверов платформы BI, которые поддерживают быстрое развертывание и тестирование платформы BI, но имеют ограниченные возможности для управления базой данных. Рекомендуется использовать полную форму SQL Anywhere или существующий поддерживаемый экземпляр базы данных для продуктивной системы, поскольку важно, чтобы база данных CMS находилась в центре обработки данных. Она управляется администраторами баз данных с использованием соответствующих процессов, установленных для безопасности данных и доступности серверов.

3.1.4 Серверы, хосты и кластеры

Платформа BI 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 в кластере совместно. Например, если в организации большое количество пользователей SAP Crystal Reports, можно создать несколько серверов обработки Crystal Reports на нескольких хостах серверов платформы BI, что обеспечивает достаточный объем 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.
- Балансировка нагрузки
  При высокой нагрузке на сервер CMS автоматически направляет новые задания на другие серверы в кластере.
- Повышение доступности
  При возникновении непредвиденной ситуации на сервере CMS автоматически перенаправляет задания на другие серверы 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 BI. 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://support.sap.com/home.html.

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 Включение кластеризации в веб-приложении стартовой панели BI для масштабируемости и поддержки восстановления сеанса после отказа

В этом разделе описывается включение кластеризации в веб-приложении стартовой панели BI для масштабируемости и поддержки восстановления сеанса после отказа. В нем также описываются шаги по настройке серверов приложений Apache Tomcat и WebSphere для реализации тех же целей.

Чтобы включить кластеризацию для сервера приложений, такого как Tomcat или WebSphere, требуется наличие следующих компонентов:

- HTTP-сервер;
- совместимый балансировщик нагрузки;
- не менее двух экземпляров сервера приложений с установленным веб-приложением;
- завершенная установка BOE (репозиторий).

> **Примечание**
>
> Шаги, описанные в этом разделе, являются родовыми и могут использоваться для включения кластеризации в любом другом приложении. Потребуется изменить только дескриптор развертывания веб-приложения (web.xml). Рекомендуется узнать у поставщика сервера веб-приложений, как настроить балансировку нагрузки на веб-уровне.

3.1.5.1.1 Установка Apache Tomcat

Чтобы установить сервер Apache Tomcat, выполните следующие действия:

1. Установите HTTP-сервер Apache.
2. Установите сервер Apache Tomcat Server на компьютерах.
3. Загрузите mod_jk (балансировщик нагрузки) из http://tomcat.apache.org/download-connectors.cgi и сохраните его в каталоге "modules" на HTTPD-сервере Apache.
4. Запустите агент SI на компьютере, где уже выполнена полная установка BOE.

   > **Примечание**
   >
   > Чтобы проверить совместимость с mod_jk, запустите HTTP-сервер. Если загруженная версия mod_jk не совместима с версией HTTP-сервера, на консоли появится сообщение об ошибке.

Настройка Apache Tomcat

Чтобы настроить конфигурацию Apache Tomcat, выполните следующие действия:

1. Настройте HTTP-сервер Apache.
   a. Настройте httpd.conf (балансировщик нагрузки, веб-приложение загрузки, мониторинг, путь к файлу worker.properties).
   b. Настройте файл workers.properties и сохраните его в библиотеке Apache\Conf.

```
# If specified, ensure that no two invocations of Apache share the same
# scoreboard file. The scoreboard file MUST BE STORED ON A LOCAL DISK.
#
#ScoreBoardFile logs/apache_runtime_status

# Used for clustering

# Specify path to worker configuration file
#
JkWorkersFile C:\Server\Apache2\Apache2\conf\workers.properties
# Configure logging and memory
JkShmFile logs/mod_jk.shm
JkLogFile logs/mod_jk.log
JkLogLevel info

# Configure monitoring
JKMount /jkmanager jkstatus
JkMount /jkmanager/* jkstatus
<Location /jkmanager>
Order deny,allow
Deny from all
Allow from localhost
</Location>

# Configure applications
# JkMount /webapp-directory/* loadBalancer
JKMount /clusterjsp loadBalancer
JKMount /clusterjsp/* loadBalancer
JKMount /login loadBalancer
JKMount /login/* loadBalancer
JKMount /boe loadBalancer
JKMount /boe/* loadBalancer
#JKMount /BOE loadBalancer
#JKMount /BOE/* loadBalancer
JKMount /docs loadBalancer
JKMount /docs/* loadBalancer

LoadModule env_module modules/mod_env.so
#LoadModule expires_module modules/mod_expires.so
#LoadModule file_cache_module modules/mod_file_cache.so
#LoadModule headers_module modules/mod_headers.so
LoadModule imap_module modules/mod_imap.so
LoadModule include_module modules/mod_include.so
#LoadModule info_module modules/mod_info.so
LoadModule isapi_module modules/mod_isapi.so

# Used for clustering
#LoadModule for clustering

LoadModule jk_module modules/mod_jk.so

LoadModule log_config_module modules/mod_log_config.so
LoadModule mime_module modules/mod_mime.so
```

Load Tomcat Connector (mod_jk)

2. Настройте файл server.xml на сервере Tomcat (добавьте теги кластеризации).
   a. В файле server.xml атрибут jvmRoute должен соответствовать имени, которое использовалось в файле workers.properties.
   b. Если используется версия Tomcat 8 и выше, удалите JvmRouteSessionIDBinderListener (устарел).
3. Добавьте тег <distributable> в файл web.xml (дескриптор развертывания) веб-приложения, которое должно поддерживать кластеризацию.

Ниже описан пользовательский "клапан", вызывающий "клапан" по умолчанию для каждого запроса. Если используется Tomcat 8, во всех файлах server.xml Tomcat замените:

```
<Interceptor
className="org.apache.catalina.tribes.group.interceptors.MessageDispatch15Inte
rceptor"/>
```

на

```
<Interceptor
className="org.apache.catalina.tribes.group.interceptors.MessageDispatchInterc
eptor"/>
```

```
    <Sender className="org.apache.catalina.tribes.transport.ReplicationTransmitter">
      <Transport className="org.apache.catalina.tribes.transport.nio.PooledParallelSender"/>
    </Sender>
    <Interceptor className="org.apache.catalina.tribes.group.interceptors.TcpFailureDetector"/>
    <Interceptor className="org.apache.catalina.tribes.group.interceptors.MessageDispatch15Interceptor"/>
  </Channel>

  <Valve className="com.sap.customvalve.ForceReplicationValve"/>
   <Valve className="org.apache.catalina.ha.tcp.ReplicationValve" filter=".*\.gif;.*\.jpg;.*\.png;.*\.js;.*\.htm
  <Valve className="org.apache.catalina.ha.session.JvmRouteBinderValve"/>

  <Deployer className="org.apache.catalina.ha.deploy.FarmWarDeployer" deployDir="/tmp/war-deploy/" tempDir="/tmp
```

4. Экспортируйте файл .jar для пользовательского "клапана" из кода (если требуются изменения). Скопируйте файл `forcereplicationvalve.jar` в каталоге `<BOEInstallDir>/SAP BusinessObjects XI 4.0/java/lib` и вставьте его в `<TomcatInstallDir>/tomcat/lib` (во всех узлах Tomcat).
5. Сохраните этот файл .jar в папке `tomcat/lib` для каждого экземпляра.
6. Перезапустите все серверы.

> ⓘ Примечание
>
> - В качестве лучшей методики рекомендуем поочередную перезагрузку серверов: подождите, пока один сервер полностью запустится, прежде чем перезагружать другой.
> - Не используйте localhost:6400 в качестве системного имени на экране входа в систему для стартовой панели.. Укажите имя (или IP) компьютера, с которого осуществляется установка BOE. Убедитесь, что на этом компьютере запущен агент SI
> - Выберите подходящую опцию с помощью атрибута channelSendOptions. Он используется для настройки опций синхронного ответа, асинхронного ответа и т.д.
> - При экспорте файла .jar для пользовательского "клапана" из кода не забудьте создать подходящую иерархию пакетов для файла jar и включить эту иерархию в server.xml.

3.1.5.1.2 Установка WebSphere

Настройка WebSphere

Чтобы настроить WebSphere, выполните следующие действия:

1. Добавьте тег <distributable> в файл web.xml веб-приложения BOE для обоих экземпляров сервера приложений WebSphere.
2. В консоли IBM перейдите к *Все серверы* > *элемент1* > *Управление сеансами*.
   a. Проверьте и включите cookies.
   b. Установите *Разрешить последовательный доступ* и задайте время ожидания, составляющее 10 секунд.
3. Перейдите к *Параметры среды распределения* > *Копирование память-память*.
   a. Создайте домен тиражирования и выберите его.
   b. Выберите режим тиражирования для клиента и сервера.
4. В меню *Все серверы* для каждого экземпляра выберите один и тот же домен тиражирования, как указано на предыдущем этапе.
5. Перейдите к *Параметры среды распределения* > *Пользовательские параметры настройки*.
   a. Для восстановления после отказа выберите *Низкий* уровень настройки.
6. Перезапустите все серверы.

3.1.5.2 Сервер контейнера веб-приложений (WACS)

Сервер веб-приложения служит для размещения веб-приложений платформы BI.

Опытный администратор серверов веб-приложений Java с расширенными потребностями в отношении администрирования может использовать для размещения веб-приложений платформы BI поддерживаемый сервер веб-приложений Java. Если для размещения платформы BI используется поддерживаемая операционная система Windows и важна простота процесса установки сервера веб-приложений, или отсутствуют ресурсы для администрирования сервера веб-приложений Java, можно при установке платформы BI установить сервер контейнера веб-приложений (WACS).

WACS представляет собой сервер платформы BI, который позволяет выполнять веб-приложения платформы BI, такие как консоль CMC, стартовая панель BI и веб-службы, без необходимости предварительно устанавливать сервер веб-приложений Java.

Преимущества использования сервера WACS:

- Установка, обслуживание и настройка WACS требуют минимальных усилий. Он устанавливается и настраивается с помощью программы установки платформы BI; 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 BI.
- Как и другие серверы платформы BI, 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 BI.
> - 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 CMC и другие веб-приложения платформы BI находятся 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.

В состав платформы BI входят SDK для разработки программного обеспечения на платформах Java и .NET.

> **Примечание**
>
> Пакеты SDK BI для платформы .NET не устанавливаются по умолчанию и должны быть загружены с портала SAP Service Marketplace.

Платформа BI поддерживает следующие пакеты SDK:

- Java SDK и .NET SDK для платформы Business Intelligence
  Пакеты SDK для платформы BI позволяют выполнять в приложениях такие задачи, как аутентификация, управление сеансами, 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.

- SDK веб-службы RESTful для платформы Business Intelligence
  Пакет SDK веб-службы RESTful для платформы BI 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 для платформы 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 BI используют такие стандарты, как XML, SOAP, AXIS 2.0 и WSDL. Платформа соответствует спецификациям веб-служб WS-Interoperability Basic Profile 1.0

> **Примечание**
>
> В настоящее время приложения веб-служб поддерживаются в следующих конфигурациях распределителя нагрузки:
>
> 1. Постоянство IP-адреса источника.
> 2. Постоянство порта назначения и IP-адреса источника (доступно только в коммутаторах Cisco Content Services Switch).
> 3. Постоянное использование SSL.
> 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.
- Пакет SDK Java семантического уровня
  Пакет SDK Java семантического уровня 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 платформы BI, которые обеспечивают интеграцию платформы BI, 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. 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 Web Intelligence. Пользователи могут изменять документы посредством добавления, удаления и изменения таких объектов, как таблицы, диаграммы, условия и фильтры.

- Platform Search SDK. 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 разработчиков и справочники по API-интерфейсам, см. на странице продукта Платформа SAP BusinessObjects Business Intelligence.

3.1.7 Источники данных

3.1.7.1 Юниверсы

Юниверс – это семантический уровень, позволяющий абстрагироваться от сложности данных посредством использования бизнес-лексики вместо языка данных при доступе к данным, их обработке и организации. Этот бизнес-язык хранится в файле юниверса в виде объектов. В Web Intelligence, Crystal Reports и других приложениях юниверсы используются для того, чтобы упростить для конечного пользователя процесс создания, необходимый для выполнения простых и сложных запросов и анализа.

Юниверсы – это основные компоненты платформы BI. Все объекты юниверса и соединения защищены и хранятся в центральном репозитории сервера соединений. Для доступа к системе и создания юниверсов клиентским средствам создания юниверсов требуется выполнить вход на платформу BI. Доступом к юниверсам и безопасностью на уровне строк и столбцов можно управлять на уровне групп и отдельных пользователей в среде проектирования.

Семантический уровень позволяет 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. Платформа BI обеспечивает полную поддержку средства Business Views.

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 BI, 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 использовать ее данные как источник для отчетов. 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 BI. 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 LDAP или Windows Active Directory (AD) с платформой 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 CMC аутентификацию Windows AD для платформы BI и пользовательских приложений, CMC и стартовая панель BI непосредственно не поддерживают аутентификацию Windows AD с NTLM. Единственными методами аутентификации, поддерживаемыми CMC 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 реальном времени информацию, связанную с повседневными операциями. Платформа BI поддерживает функции единого входа и ведения отчетности следующих систем планирования ресурсов предприятия:

- 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 BI , см. документ *Поддерживаемые платформы/PAR*, доступный по адресу https://support.sap.com/home.html.

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

3.1.9 Интеграция SAP

Платформа BI интегрируется с существующей инфраструктурой SAP с помощью следующих средств:

- SAP System Landscape Directory (SLD)
  Каталог System Landscape Directory в SAP NetWeaver является центральным источником сведений System Landscape, связанных с управлением 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 BI регистрирует имена производителей 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».
- Система изменений и переносов (CTS+)
  Система изменений и переносов (CTS) помогает организовать проекты разработок в инструментальных средствах ABAP и в пользовательской настройке, а затем перенести 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 предоставляет 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 BI 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.

3.2 Серверы, службы, узлы и хосты

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

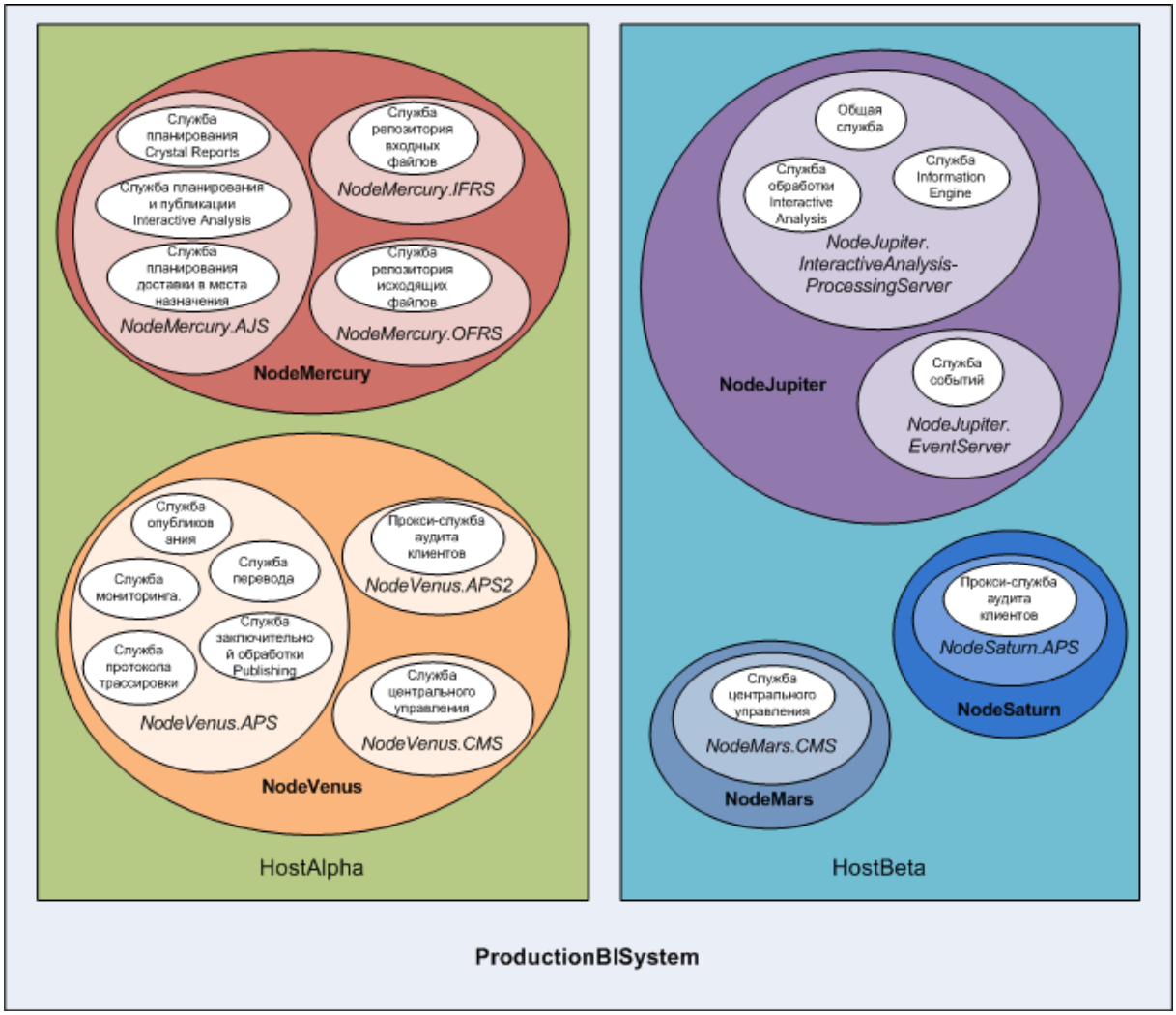
Термином «сервер» обозначается процесс уровня операционной системы (в некоторых системах он носит название демон), в котором размещаются одна или несколько служб. В качестве примера подобного сервера можно привести Центральный сервер управления (CMS) и адаптивный сервер обработки. Сервер запускается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

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.

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).

На следующем рисунке 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 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 по сравнению с версией XI 3.1. К типам изменений относятся:

- 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 адаптивный сервер заданий с версии 4.0.
- Новые серверы

Изменения серверов

XI 3.1	4.0	4.0 с пакетом компонентов 3	4.1	4.2	4,3
Сервер соединений [1]	Сервер соединений Сервер соединений 32	Сервер соединений Сервер соединений 32	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	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 2013 Сервер обработки Crystal Reports (для отчетов SAP Crystal Reports для Enterprise)	Сервер обработки Crystal Reports 2016 Сервер обработки Crystal Reports (для отчетов SAP Crystal Reports для Enterprise)	Сервер обработки Crystal Reports 2020 Сервер обработки Crystal Reports (для отчетов SAP Crystal Reports для Enterprise)
Сервер информационных панелей (Dashboard Builder) [2]	Сервер информационных панелей (рабочие пространства BI)	Недоступно для версии 4.0 с пакетом компонентов 3	Недоступно в версии 4.1	Недоступно в версии 4.2	Недоступно в версии 4.3
Сервер аналитики информационных панелей (Dashboard Builder) [2]	Сервер аналитики информационных панелей (рабочие пространства BI)	Недоступно с версии 4.0 с пакетом компонентов 3	Недоступно в версии 4.1	Недоступно в версии 4.2	Недоступно в версии 4.3

XI 3.1	4.0	4.0 с пакетом компонентов 3	4.1	4.2	4,3
Сервер кэширования Desktop Intelligence [3]	Недоступно для версии 4.0	Недоступно с версии 4.0	Недоступно в версии 4.1 [3]	Недоступно в версии 4.2 [3]	Недоступно в версии 4.3 [3]
Сервер заданий Desktop Intelligence [3]	Недоступно с версии 4.0	Недоступно с версии 4.0	Недоступно в версии 4.1 [3]	Недоступно в версии 4.2 [3]	Недоступно в версии 4.3 [3]
Сервер обработки Desktop Intelligence [3]	Недоступно с версии 4.0	Недоступно с версии 4.0	Недоступно в версии 4.1 [3]	Недоступно в версии 4.2 [3]	Недоступно в версии 4.3 [3]
Сервер заданий для адресатов	Адаптивный сервер заданий	Адаптивный сервер заданий	Адаптивный сервер заданий	Адаптивный сервер заданий	Адаптивный сервер заданий
Сервер многомерного анализа	Адаптивный сервер обработки	Адаптивный сервер обработки	Адаптивный сервер обработки	Адаптивный сервер обработки	Адаптивный сервер обработки
Сервер выполнения программы	Адаптивный сервер заданий	Адаптивный сервер заданий	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 2013 Report Application Server (RAS)	Crystal Reports 2016 Report Application Server (RAS)	Crystal Reports 2020 Report Application Server (RAS)
Сервер выполнения Web Intelligence	Адаптивный сервер заданий	Адаптивный сервер заданий	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)	Кэш-сервер Dashboards (Xcelsius)	Недоступно в версии 4.7 [3]
Сервер обработки Xcelsius [4]	Сервер обработки Dashboard Design (Xcelsius) [5]	Сервер обработки Dashboards (Xcelsius)	Сервер обработки Dashboards (Xcelsius)	Сервер обработки Dashboards (Xcelsius)	Недоступно в версии 4.7 [3]
Определенные веб-части [6]	Средство просмотра отчетов Crystal, средство просмотра Xcelsius и средство просмотра аналитических отчетов	Средство просмотра отчетов Crystal, средство просмотра Xcelsius и средство просмотра аналитических отчетов	Средство просмотра отчетов Crystal, средство просмотра Xcelsius и средство просмотра аналитических отчетов	Средство просмотра отчетов Crystal, средство просмотра Xcelsius и средство просмотра аналитических отчетов	Использование некоторых веб-частей в версии 4.3 не рекомендовано, так как они устарели

- [1] В версии 4.0 сервер соединений 32 является 32-битным и выполняет подключения к источникам данных, которые не поддерживают работу с 64-битным компонентом доступа. Сервер соединений является 64-битным 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 больше не требуется для функционирования рабочих пространств BI (ранее 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 «Dashboards» в версии 4.0 с пакетом компонентов 3, чтобы привести их в соответствие с изменением названия продукта на SAP BusinessObjects Dashboards.
- [6] Не рекомендовано использование следующих веб-частей в версии 4.3:
  - Средство просмотра отчетов Crystal
  - Средство просмотра Xcelsius
  - Средство просмотра аналитических отчетов
- [7] Не рекомендуется использовать сервер обработки Dashboards (Xcelsius) и кэш-сервер Dashboards (Xcelsius), так как они устарели.

3.2.2 Службы

При добавлении серверов необходимо включить также некоторые службы на адаптивном сервере заданий. Например, службу планирования доставки в места назначения.

> ⓘ Примечание
>
> - В дальнейшем в выпуски могут быть добавлены новые типы служб и серверов.
> - Образец службы планирования Java используется только для внутренних целей разработки и недоступен внешним пользователям.

Служба	Категория службы	Тип сервера	Описание службы
Служба адаптивного соединения	Службы соединения	Адаптивный сервер обработки	Предоставляет службы соединений для драйверов на основе Java
Служба Analytics Hub	Основные службы	Адаптивный сервер обработки	Эта служба выполняется на адаптивном сервере обработки и взаимодействует с системами SAP Analytics Cloud и SAP Analytics Hub.

Служба	Категория службы	Тип сервера	Описание службы
Служба планирования обновления аутентификации	Основные службы	Адаптивный сервер заданий	Обеспечивает синхронизацию обновлений подключаемых модулей безопасности сторонних разработчиков.
Служба веб-приложений BEx	Службы Analysis Services	Адаптивный сервер обработки	Обеспечивает интеграцию веб-приложений SAP Business Warehouse (BW) Business Explorer (BEx) и стартовой панели BI.
BIMobileService(OCA)	Основные службы	Адаптивный сервер обработки	Обеспечивает push-уведомления на мобильных устройствах.
Служба контейнера веб-приложений	Основные службы	Сервер контейнера веб-приложений	Предоставляет веб-приложения для WACS: включает CMC, стартовую панель BI и OpenDocument.
Центральная служба управления	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 Commentary	Основные службы	Адаптивный сервер обработки	Обеспечивает операции комментирования в документах.
Служба обработки Crystal Reports 2020	Службы Crystal Reports	Сервер обработки Crystal Reports	Принимает и обрабатывает отчеты Crystal Reports 2020; может объединять данные разных отчетов, что сокращает число обращений к базе данных.
Служба планирования Crystal Reports 2020	Службы Crystal Reports	Адаптивный сервер заданий	Выполняет запланированные прежние задания Crystal Reports и публикует результаты в заданном местоположении.

Служба	Категория службы	Тип сервера	Описание службы
Служба просмотра и изменения Crystal Reports 2020	Службы Crystal Reports	Сервер приложений отчетов (RAS)	Обрабатывает запросы на просмотр и изменение для отчетов Crystal Reports 2020.
Служба кэша Crystal Reports	Службы Crystal Reports	Кэш-сервер Crystal Reports	Ограничивает число обращений к базе данных из отчетов Crystal и ускоряет создание отчетов посредством управления кэшем отчетов.
Служба обработки Crystal Reports	Службы Crystal Reports	Сервер обработки Crystal Reports	Принимает и обрабатывает отчеты Crystal; может объединять данные для разных отчетов, что сокращает число обращений к базе данных.
Служба планирования Crystal Reports	Службы Crystal Reports	Адаптивный сервер заданий	Выполняет запланированные новые задания Crystal Reports и публикует результаты в заданном местоположении.
Служба доступа к пользовательским данным	Службы Web Intelligence	Адаптивный сервер обработки	Обеспечивает динамическое подключение к источникам данных, для которого не требуется сервер соединений. Эта служба обеспечивает доступ и обновление отчетов, созданных с помощью поставщиков персональных данных (например, CSV-файлов). См. *Руководство пользователя SAP BusinessObjects Web Intelligence Rich Client* для получения дополнительных сведений о создании запроса или обновлении документа на основе текстового файла.
Служба объединения данных	Службы объединения данных	Адаптивный сервер обработки	Запрос и обработка базовых источников данных для юниверса с несколькими источниками

Служба	Категория службы	Тип сервера	Описание службы
Служба планирования доставки в места назначения	Основные службы	Адаптивный сервер заданий	Выполняет запланированные задания и публикует результаты в заданное местоположение, такое как файловая система, FTP-сервер, SFTP-сервер, адрес электронной почты или папка входящей почты пользователя. **Примечание** При добавлении серверов необходимо включить некоторые службы адаптивного сервера заданий, в том числе эту службу.
Служба восстановления документов	Службы Web Intelligence	Адаптивный сервер обработки	Автоматическое сохранение и восстановление документа Web Intelligence
Служба DSL Bridge	Службы Web Intelligence	Адаптивный сервер 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 доступа к данным Excel	Службы Web Intelligence	Адаптивный сервер обработки	Поддерживает в качестве источников данных файлы Excel, загруженные в платформу BI. См. раздел *Руководство пользователя SAP BusinessObjects Web Intelligence Rich Client* 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	Категория службы	Тип сервера	Описание службы
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 Диспетчера переноса объектов	Службы Диспетчера переноса объектов	Адаптивный сервер обработки	Обеспечивает поддержку ClearCase для управления жизненным циклом
Служба планирования Диспетчера переноса объектов	Службы Диспетчера переноса объектов	Адаптивный сервер заданий	Выполняет запланированные задания Диспетчера переноса объектов
Служба Диспетчера переноса объектов	Службы Диспетчера переноса объектов	Адаптивный сервер обработки	Основная служба Диспетчера переноса объектов
Служба мониторинга	Основные службы	Адаптивный сервер обработки	Обеспечивает функции мониторинга
Multi-Dimensional analysis service	Службы Analysis Services	Адаптивный сервер обработки	Обеспечивает доступ к многомерным OLAP-данным; преобразует необработанные данные в формат XML, который можно затем перенести в кросс-таблицы и диаграммы Excel, PDF и Analysis (ранее Voyager).
Служба прямого соединения	Службы соединений	Сервер соединений	Предоставляет службы прямого соединения для 64-разрядной архитектуры
Служба прямого соединения (32-разрядная)	Службы соединений	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-сервере, SFTP-сервере, 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 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	Категория службы	Тип сервера	Описание службы
Служба маркера безопасности	Основные службы	Адаптивный сервер обработки	Поддержка единого входа для SAP
Служба материализации наборов	Основные службы	Адаптивный сервер обработки	Управляет материализацией наборов и групп наборов.
Служба планирования материализации наборов	Основные службы	Адаптивный сервер заданий	Позволяет планировать наборы и группы наборов для материализации.
Служба преобразований	Основные службы	Адаптивный сервер обработки	Переводит объекты InfoObject с входными данными из клиента диспетчера переводов
Служба планирования импорта пользователей и групп	Основные службы	Адаптивный сервер заданий	Позволяет планировать импорт файлов принципалов
Служба планирования Visual Difference	Службы Диспетчера переноса объектов	Адаптивный сервер заданий	Выполняет запланированные задания Visual Difference (Диспетчер переноса объектов) и публикует результаты в заданном выходном местоположении.
Служба Visual Difference	Службы Диспетчера переноса объектов	Адаптивный сервер обработки	Определяет, являются ли документы визуально идентичными для перевода документа на уровень выше и управления переносом объектов
Служба визуализации	Службы Web Intelligence	Адаптивный сервер обработки	Служба Common Visualization Object Model, используемая приложением Web Intelligence.
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

Служба	Категория службы	Тип сервера	Описание службы
Служба управления версиями	Службы Диспетчера переноса объектов	Адаптивный сервер обработки	Управляет несколькими версиями ресурсов BI с использованием IBM Rational ClearCase или Apache Subversion.

3.2.3 Категории служб

> ⓘ Примечание
>
> В дальнейшем в выпуски могут быть добавлены новые типы служб и серверов.

Категория службы	Служба	Тип сервера
Службы Analysis Services	Служба веб-приложений BEx	Адаптивный сервер обработки
Службы Analysis Services	Multi-Dimensional analysis service	Адаптивный сервер обработки
Службы соединений	Служба адаптивного соединения	Адаптивный сервер обработки
Службы соединений	Служба прямого соединения	Сервер соединений
Службы соединений	Служба прямого соединения (32-разрядная)	Сервер соединений
Основные службы	Служба Analytics Hub	Адаптивный сервер обработки
Основные службы	Служба планирования обновления аутентификации	Адаптивный сервер заданий
Основные службы	BIMobileService(OCA)	Адаптивный сервер обработки
Основные службы	Central Management Service	Центральный сервер управления
Основные службы	Прокси-служба аудита клиента	Адаптивный сервер обработки
Основные службы	Служба Commentary	Адаптивный сервер обработки
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

Категория службы	Служба	Тип сервера
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	Веб-служба RESTful	Сервер контейнера веб-приложений
Основные службы	Служба тиражирования	Адаптивный сервер заданий
Основные службы	Служба планирования запросов безопасности	Адаптивный сервер заданий
Основные службы	Служба маркера безопасности	Адаптивный сервер обработки
Основные службы	Служба материализации наборов	Адаптивный сервер обработки
Основные службы	Служба планирования материализации наборов	Адаптивный сервер обработки
Основные службы	Служба единого входа*	Центральный сервер управления, сервер соединений, сервер обработки Crystal Reports, RAS 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 2020	Сервер обработки Crystal Reports
Службы Crystal Reports	Служба планирования Crystal Reports 2020	Адаптивный сервер заданий
Службы Crystal Reports	Служба просмотра и изменения Crystal Reports 2020	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 объединения данных	Служба объединения данных	Адаптивный сервер обработки
Службы управления жизненным циклом	Служба ClearCase Диспетчера переноса объектов	Адаптивный сервер обработки
Службы управления жизненным циклом	Служба планирования Диспетчера переноса объектов	Адаптивный сервер заданий

Категория службы	Служба	Тип сервера
Службы управления жизненным циклом	Служба Диспетчера переноса объектов	Адаптивный сервер обработки
Службы управления жизненным циклом	Служба планирования Visual Difference	Адаптивный сервер заданий
Службы управления жизненным циклом	Служба Visual Difference	Адаптивный сервер обработки
Службы Web Intelligence	Служба 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
Службы Диспетчера переноса объектов	Служба управления версиями	Адаптивный сервер обработки

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

Тип сервера	Служба	Категория службы
Адаптивный сервер заданий	Служба планирования Crystal Reports 2020	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 Диспетчера переноса объектов	Службы Диспетчера переноса объектов
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	Службы планирования материализации наборов	Основные службы
Адаптивный сервер заданий	Служба планирования импорта пользователей и групп*	Основные службы
Адаптивный сервер заданий	Служба планирования Visual Difference	Службы Диспетчера переноса объектов
Адаптивный сервер заданий	Служба планирования Web Intelligence	Службы Web Intelligence
Адаптивный сервер обработки	Служба адаптивного соединения	Службы соединения
Адаптивный сервер обработки	Службы Analytical Hub	Основные 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 Диспетчера переноса объектов	Службы Диспетчера переноса объектов

Тип сервера	Служба	Категория службы
Адаптивный сервер обработки	Служба Диспетчера переноса объектов	Службы Диспетчера переноса объектов
Адаптивный сервер обработки	Служба мониторинга	Основные службы
Адаптивный сервер обработки	Multi-Dimensional analysis service	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 материализации наборов	Основные службы
Адаптивный сервер обработки	Служба преобразований	Основные службы
Адаптивный сервер обработки	Служба Visual Difference	Службы Диспетчера переноса объектов
Адаптивный сервер обработки	Служба визуализации	Службы Web Intelligence
Адаптивный сервер обработки	Служба мониторинга Web Intelligence*	Службы Web Intelligence
Центральный сервер управления	Central Management Service	Основные службы
Центральный сервер управления	Служба единого входа*	Основные службы
Сервер соединений	Служба прямого соединения	Службы соединений
Сервер соединений	Служба прямого соединения (32-битная)	Службы соединений
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 2020	Службы Crystal Reports
Сервер обработки Crystal Reports	Служба обработки Crystal Reports	Службы Crystal Reports
Сервер обработки Crystal Reports	Служба единого входа*	Основные службы
Сервер событий	Служба событий	Основные службы
Сервер репозитория входных файлов	Служба хранилища входных файлов	Основные службы
Сервер репозитория выходных файлов	Служба хранилища выходных файлов	Основные службы
Сервер приложений отчетов (RAS)	Служба просмотра и изменения Crystal Reports 2020	Службы Crystal Reports
RAS	Служба единого входа*	Основные службы
Сервер контейнера веб-приложений	Веб-служба RESTful	Основные службы

Тип сервера	Служба	Категория службы
Сервер контейнера веб-приложений	Служба контейнера веб-приложений*	Основные 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 2020	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 Диспетчера переноса объектов	Службы Диспетчера переноса объектов
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 Visual Difference	Службы Диспетчера переноса объектов
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

Тип сервера	Служба	Категория службы
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 Диспетчера переноса объектов	Службы Диспетчера переноса объектов
Адаптивный сервер обработки	Служба Диспетчера переноса объектов	Службы Диспетчера переноса объектов
Адаптивный сервер обработки	Служба мониторинга	Основные службы
Адаптивный сервер обработки	Multi-Dimensional analysis service	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 Диспетчера переноса объектов
Адаптивный сервер обработки	Служба визуализации	Службы Web Intelligence
Центральный сервер управления	Central Management Service	Основные службы
Сервер соединений	Служба прямого соединения	Службы соединений
Сервер соединений	Служба прямого соединения (32-битная)	Службы соединений
Кэш-сервер Crystal Reports	Служба кэша Crystal Reports	Службы Crystal Reports
Сервер обработки Crystal Reports	Служба обработки Crystal Reports 2020	Службы Crystal Reports
Сервер обработки Crystal Reports	Служба обработки Crystal Reports	Службы Crystal Reports
Сервер событий	Служба событий	Основные службы
Сервер репозитория входных файлов	Служба хранилища входных файлов	Основные службы
Сервер репозитория выходных файлов	Служба хранилища выходных файлов	Основные службы
Сервер приложений отчетов (RAS)	Служба просмотра и изменения Crystal Reports 2020	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
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	Универсальный сервер, обеспечивающий обработку запланированных заданий. При добавлении сервера заданий на платформу BI можно настроить на нем обработку отчетов, документов, программ или публикаций, а также отправку результатов в различные целевые компоненты.
Адаптивный сервер обработки	Общий сервер, на котором находятся службы, отвечающие за обработку запросов из различных источников. Программа установки устанавливает по одному адаптивному серверу обработки (APS) на каждый хост. 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. В производственных и тестовых системах рекомендуется создавать дополнительные адаптивные серверы обработки и настраивать их в соответствии с бизнес-требованиями. Дополнительные сведения см. в Вводные сведения о мастере настройки системы [страница 91] и Настройка адаптивных серверов обработки для производственных систем [страница 473].
Центральный сервер управления (CMS)	Обслуживает базу данных о системе платформы BI (в системной базе данных CMS) и проверенных 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.

Сервер	Описание
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 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 BI 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 BI более не выполняет установку приложений для настольных систем. Для установки таких 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 ПК, а обмен данными с экземпляром развертывания платформы BI осуществляет с использованием архитектуры CORBA или CORBA с шифрованием SSL.
Примеры приложений этого типа: Crystal Reports и Live Office.

> **ⓘ Примечание**
>
> Хотя Live Office является полнофункциональным приложением, обмен данными с веб-службами платформы BI 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 Устанавливаемые со средствами клиента платформы SAP BusinessObjects Business Intelligence

3.3.1.1 Web Intelligence Rich Client

Web Intelligence Rich Client – это специальное средство анализа и составления отчетов для бизнес-пользователей с доступом или без доступа к платформе BI.

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).

> **ⓘ Примечание**
>
> - Не рекомендуется устанавливать Web Intelligence Rich Client на том же компьютере, что и серверы платформы BI. Web Intelligence Rich Client и серверы платформы BI имеют общие двоичные файлы, что может привести к проблемам с развертыванием при обновлении

установки (клиента или сервера). Рекомендуется устанавливать Web Intelligence Rich Client на отдельный компьютер.

- Если выполняется обновление версии 4.2 до 4.3, убедитесь, что предыдущая версия остановлена и закрыта. Проверьте область задач Windows, так как, возможно, значок Rich Client свернут, но приложение по-прежнему работает.

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 RCT исключено в версии BI 4.3 как устаревшее. Для получения дополнительных сведений см. 2801797

3.3.1.4 Средство создания юниверсов

Средство создания юниверсов (ранее Universe Designer) позволяет разработчикам данных объединять данные из нескольких источников на семантическом уровне, скрывающем 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 формирования юниверса на конечном этапе процесса создания.

3.3.1.5 Средство дизайна информации

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

3.3.1.6 Средство управления переводами

Платформа BI поддерживает работу с многоязычными документами и юниверсами. 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.

3.3.1.7 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 BI 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.

3.3.2 Устанавливаемые 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 апгрейдом

Не рекомендуется использовать средство UMT в версии BI 4.3, так как оно устарело. Для получения дополнительных сведений см. 2801797

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 оперативного 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 BI. 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 Lumira

Приложение SAP Lumira помогает визуализировать данные и создавать журналы с данными. С помощью SAP Lumira можно управлять, изменять, форматировать и настраивать данные, создавать визуализации для графического представления данных и публиковать визуализации, используя журналы.

SAP Lumira теперь фигурирует в CMC как приложение, что позволяет управлять правами, связанными с функциями SAP Lumira по импорту данных и совместному использованию объектов, для каждого пользователя или группы пользователей.

> **Примечание**
>
> Все события, связанные с приложением SAP Lumira, регистрируются без ид. клиента в базе данных аудита.

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 развертываются автоматически при установке платформы BI.

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.

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).

3.3.4.2 Стартовая панель BI в стиле Fiori

Стартовая панель BI в стиле Fiori (ранее InfoView) представляет собой веб-интерфейс, используемый конечными пользователями для просмотра, планирования и отслеживания опубликованных отчетов BI. Стартовая панель BI в стиле Fiori позволяет просматривать, использовать и экспортировать бизнес-аналитику любого типа (включая отчеты, аналитические данные и информационные панели).

Стартовая панель BI поддерживает следующие возможности:

- 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 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 корректировки бизнес-правил в соответствии с изменениями условий. Это позволяет отслеживать и анализировать ключевые бизнес-данные посредством управления рабочими пространствами BI и модулями. Это также обеспечивает поддержку группового принятия решений и анализа посредством возможностей интегрированного сотрудничества и рабочих процессов. В рабочих пространствах BI доступны следующие функции:

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

> ⓘ Примечание
>
> Документы Design Studio не поддерживают связывание содержимого.

3.3.4.4 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.

3.3.4.5 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.

3.3.4.6 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 BI

Данный рабочий процесс описывает вход пользователя в веб-приложение платформы BI 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.

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 2020 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 2020

Этот рабочий процесс описывает запрос пользователем из отчета SAP Crystal Reports 2020 (например, из средства просмотра отчетов на стартовой панели BI) страницы, которая еще не существует на кэш-сервере.

> **Примечание**
>
> Для данного рабочего процесса требуется, чтобы CMS, кэш-сервер Crystal Reports, сервер обработки Crystal Reports 2020 и сервер репозитория выходных файлов выполнялись.

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 2020.
8. Сервер обработки Crystal Reports 2020 запрашивает на сервере репозитория выходных файлов запрошенный экземпляр отчета, и сервер репозитория выходных файлов отправляет запрошенный экземпляр отчета на сервер обработки Crystal Reports 2020.

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

9. Сервер обработки Crystal Reports 2020 открывает экземпляр отчета и проверяет отчет на наличие в нем данных.

   Сервер обработки Crystal Reports 2020 определяет, что отчет содержит данные, и создает файл `.epf` запрошенной страницы отчета, не подключаясь к производственной базе данных.
10. Сервер обработки Crystal Reports 2020 отправляет файл `.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 2020 по требованию

Этот рабочий процесс описывает запрос пользователем страницы отчета SAP Crystal Reports 2020 по требованию для просмотра последних данных, например из средства просмотра отчетов или со стартовой панели BI.

> **Примечание**
>
> Для данного рабочего процесса требуется выполнение CMS, кэш-сервера Crystal Reports, сервера обработки Crystal Reports 2020 и сервера репозитория входных файлов.

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 `.epf`).
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 2020 запрос на создание страницы.
7. Сервер обработки Crystal Reports 2020 запрашивает объект отчета на сервере репозитория входных файлов. Сервер репозитория входных файлов направляет копию объекта на сервер обработки Crystal Reports 2020.

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

8. Сервер обработки Crystal Reports 2020 открывает отчет в собственной памяти и проверяет его на наличие данных. В этом примере отчет не содержит данных, поэтому сервер обработки Crystal Reports 2020 подключается к источнику данных для получения информации и создания отчета.
9. Сервер обработки Crystal Reports 2020 направляет страницу (файл `.epf`) на кэш-сервер Crystal Reports. Кэш-сервер Crystal Reports сохраняет копию файла `.epf` 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 2020 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 2020

Этот рабочий процесс описывает процесс выполнения запланированного отчета SAP Crystal Reports 2020 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 2020 на адаптивном сервере заданий (на основе значения *Максимально допустимое число задач*, настроенного для каждого адаптивного сервера заданий). CMS отправляет информацию о задании (идентификатор отчета, формат, место назначения, сведения о входе в систему, параметры и формулы выбора) в службу планирования Crystal Reports 2020.
3. Служба планирования Crystal Reports 2020 обращается к серверу репозитория входных файлов 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 2020 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.
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 2020 периодически обновляет в CMS информацию о состоянии выполнения задания. Текущее состояние имеет значение "Обработка".
9. После компиляции отчета в памяти службы планирования Crystal Reports 2020 его можно экспортировать 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 2020 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 сервер 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, SFTP, 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 Анализ

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.

3.5 Интеграция со стартовой панелью Fiori на портале SAP Enterprise Portal

Обзор

Интеграция SAP BusinessObjects BI с платформами стартовой панели Fiori позволяет конечным пользователям портала SAP Enterprise Portal просматривать отчеты BI на сервере CMS SAP BusinessObjects. На вкладке «Меню пользователя» конечные пользователи могут осуществлять доступ к отчетам BI, иерархия папок которых соответствует иерархии на сервере CMS SAP BusinessObjects.

Предварительные условия

- Business Intelligence 4.2 SP4
- Web Dispatcher 7.49 для установки соединения
- NetWeaver 7.5 SP7
- Аутентификация Active Directory и конфигурация SSO на основе Kerberos, как описано в SAP-ноте 1631734

Процедура

Администратор содержимого стартовой панели Fiori и администратор портала Enterprise Portal могут интегрировать SAP BusinessObjects Enterprise со стартовой панелью Fiori.

Полные указания по настройке см. в разделе Интеграция SAP BusinessObjects Enterprise документации по порталу SAP NetWeaver 7.5.

> ⓘ Примечание
>
> - Платформа BI поддерживает службы OData для интеграции панели запуска Fiori и SAP Enterprise Portal.
> - Платформа BI поддерживает службы OData на сервере приложений NetWeaver.
> - После успешной интеграции из SAP Enterprise Portal можно войти в Общие папки, Личные папки и в папку Входящие BI.

4 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 (CMC), 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 CMC 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".

> ⓘ Примечание
>
> Чтобы не допустить автоматического выполнения мастера, пользователь с правами «администратора» может установить флажок *Не показывать этот мастер, когда запущена CMC* на первой странице мастера.

> ⓘ Примечание
>
> 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 станице *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*.

> **Примечание**
>
> Чтобы упростить развертывание, конфигурацию с этой страницы не нужно повторно создавать для каждого узла – конфигурация применяется к целому кластеру.

> **Примечание**
>
> Если какие-либо настройки были ранее изменены в CMC, в мастере отображается сообщение, информирующее о том, что параметры были изменены вне мастера. Можно сохранить существующую конфигурацию или перезаписать текущие параметры.

> **Примечание**
>
> 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.

> ⓘ Примечание
>
> Требуемый объем ОЗУ – это минимальный объем ОЗУ, необходимый для серверов платформы BI. Например, если на машине установлено 16 ГБ ОЗУ, из которых ОС использует только 1 ГБ, 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.

> ⓘ Примечание
>
> 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 CMC 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.

> ⓘ Примечание
>
> Чтобы упростить развертывание, выбранная конфигурация APS применяется к каждому узлу (если на этих узлах установлен APS), поэтому чем больше узлов, тем больше емкость кластера.

> ⓘ Примечание
>
> 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 самого малого на средний 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 скопирует 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. Кода мастер завершает свою работу, отображается страница *Выполнено* со списком дальнейших шагов, которые требуется выполнить вручную.

Связанные сведения

Файлы журнала и файлы ответов [страница 97]

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 CMC. 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.

Связанные сведения

Использование файла ответов [страница 98]

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 CMC. Имена файлов имеют метки времени в формате `год_месяц_день_час_минута_секунда` и расширение `.ini`. На консоли CMC 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.

> **Примечание**
>
> В целях безопасности поддерживается только аутентификация Enterprise (аутентификации Windows AD, LDAP и SAP не поддерживаются).

> **Примечание**
>
> Если нужно отложить перезапуск каких-либо узлов до следующего планового перезапуска, выполните скрипт непосредственно перед плановым простоем системы.

5 Управление лицензиями

5.1 Управление лицензионными ключами

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

Связанные сведения

Просмотр сведений лицензии [страница 102]
Добавление ключа лицензии [страница 102]
Для просмотра текущей деятельности учетной записи [страница 103]

5.1.1 Просмотр сведений лицензии

В области управления CMC*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 CMC.
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.

Связанные сведения

Добавление ключа лицензии [страница 102]
Для просмотра текущей деятельности учетной записи [страница 103]

5.1.2 Добавление 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.

> **Примечание**
>
> При обновлении до платформы SAP BusinessObjects Business Intelligence 4.2 с пакетом поддержки 2 или выше и более ранних выпусков существующие лицензии будут считаться истекшими.
> При этом необходимо сгенерировать и использовать новый ключ лицензии для платформы SAP BusinessObjects Business Intelligence 4.2.

1. Перейдите в область управления *Ключи лицензий* в CMC.
2. Введите ключ в поле *Добавить ключ*.
3. Нажмите кнопку *Добавить*.

Ключ добавится в список.

Связанные сведения

Просмотр сведений лицензии [страница 102]
Для просмотра текущей деятельности учетной записи [страница 103]

5.1.3 Для просмотра текущей деятельности учетной записи

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

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

Связанные сведения

Добавление ключа лицензии [страница 102]
Просмотр сведений лицензии [страница 102]

6 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».

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.
SMAdmin	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 позволить 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 CMC, нажмите *Список групп* на панели *Дерево*. В качестве альтернативы, можно нажать *Иерархия групп* для отображения иерархического списка всех доступных групп.

Учетные записи групп по умолчанию

Имя учетной записи	Описание
Администраторы	Участники этой группы могут выполнять все задачи во всех приложениях платформы BI (CMC, CCM, мастер публикаций и стартовая панель BI). По умолчанию, группа *Администраторы* содержит только пользователей-администраторов.
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.

Связанные сведения

Права на платформе BI [страница 129]
Предоставление доступа пользователям и группам [страница 117]

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 аутентификации, доступные для вас в зависимости от инструментов безопасности, используемых вашей организацией.

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.
Siebel	Можно сопоставить существующие роли Siebel с учетными записями в платформе BI. После сопоставления ролей Siebel пользователи смогут входить в приложения платформы BI со своими учетными данными Siebel. Это устраняет необходимость повторного создания пользователей и групп в платформе BI.

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

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, а также управлении ими платформа 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 CMC.
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 информацию о пароле и настройки в соответствии с критериями паролей, определенными для аутентификации Enterprise.

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 BI):
   - 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. Пользовательские лицензии удобны для людей, которым необходим доступ к платформе BI независимо от числа других подключенных пользователей в данный момент.

   > ⓘ Примечание
   >
   > Число параллельных сеансов входа для именованного пользователя, созданного с использованием пользовательской лицензии, ограничивается 10 сеансами. Если такой именованный пользователь попытается войти в 11-й параллельный сеанс входа, будет выдано соответствующее сообщение об ошибке. Для входа необходимо будет завершить один из текущих сеансов.
   >
   > Однако число параллельных сеансов входа для именованных пользователей, созданных с использованием лицензии на процессор и лицензии на публичные документы, не ограничено.

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.

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 CMC.
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*.

Связанные сведения

Для создания нового псевдонима существующего пользователя [страница 126]

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 пользователя не обязательно не обязательно приведет к тому, что пользователь не сможет выполнить вход 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 CMC.
2. Выберите пользователя, которого нужно удалить.
3. Выберите *Управление* > *Удалить*.

   Появится диалоговое окно подтверждения удаления, которое уведомляет, является ли выбранный пользователь владельцем одного или нескольких объектов.
4. Нажмите кнопку *OK*.
   Учетная запись пользователя будет удалена.

Связанные сведения

Для изменения учетной записи пользователя [страница 108]

Для отключения псевдонима [страница 128]

6.2.4 Чтобы создать новую группу

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

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 BI.

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 CMC *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 CMC.
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 CMC 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 *OK*.

Связанные сведения

Задание принадлежности к группе [страница 111]

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 CMC 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 *OK*.
   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.

> ⓘ Примечание
>
> 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 CMC.

1. Перейдите в область управления *Пользователи и группы* консоли CMC.
2. Выберите группу, которую необходимо удалить.
3. Выберите *Управление* > *Удалить*.
   Появится диалоговое окно с запросом на подтверждение удаления.
4. Нажмите кнопку *OK*.
   Группа удалена.

6.2.10 Массовое добавление пользователей или групп пользователей

Для массового добавления пользователей или групп пользователей к CMC 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.

> **Примечание**
>
> Выполнять массовое добавление пользователей могут лишь те пользователи, которые являются членами группы "Администраторы", существующей по умолчанию. Для делегированных администраторов эта функция не поддерживается.

1. В области управления CMC *Пользователи и группы* 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 CMC выполнит проверку файла импорта.
3. Нажмите кнопку *Импорт*.

Пользователи или группы пользователей импортируются в CMC.

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 CMC.
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

Группы пользователей позволяют администраторам выполнять задачи стартовой панели BI для пакетов пользователей (например, можно настроить предпочтения или запланировать публикации для определенных групп пользователей).

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*.

Можно добавить пользователя в несколько групп. Однако если пользователь входит в две или несколько групп, на стартовой панели BI отображаются предпочтения только для одной из них.

Связанные сведения

Задание принадлежности к группе [страница 111]

6.2.12.1 Добавление пользователя в одну или несколько групп пользователей

Можно добавить пользователя в несколько групп. Однако на стартовой панели BI будут отображаться предпочтения только для одной из них.

1. В области управления CMC *Пользователи и группы* выберите пользователя, которого требуется добавить в группу.
2. Выберите *Действия* > *Присоединиться к группе*.

   > ⓘ Примечание
   >
   > Все пользователи платформы BI в системе являются частью группы "Все".

3. В диалоговом окне *Присоединиться к группе* переместите группу, в которую нужно добавить пользователя, из списка *Доступные группы* в список *Группы-места назначения*.

   > → Совет
   >
   > Используйте сочетание `SHIFT`+`щелчок мышью` или `CTRL`+`щелчок мышью` для выбора нескольких групп.

4. Нажмите кнопку *OK*.

6.2.12.2 Добавление одного или нескольких пользователей в группу пользователей

В группу пользователей можно добавить несколько пользователей.

Предпочтения, заданные для группы пользователей, применяются ко всем пользователям в группе. На стартовой панели BI выводятся предпочтения только для одной группы пользователей одновременно.

1. В области управления CMC *Пользователи и группы* выберите группу пользователей.
2. Выберите *Действия* > *Добавить участников в группу*.
3. В диалоговом окне *Добавить* нажмите *Список пользователей*.
   Список *Доступные пользователи/группы* будет обновлен, и в нем отобразятся все учетные записи пользователей в системе.
4. Переместите одного или нескольких пользователей в группу (из списка *Доступные пользователи/группы* в список *Выбранные пользователи/группы*).

   > → Совет
   >
   > Чтобы выбрать несколько пользователей, используйте сочетание `SHIFT`+`щелчок мышью` или `CTRL`+`щелчок мышью`. Чтобы найти определенного пользователя, введите его имя в поле *поиска*.

   > → Совет
   >
   > Если в системе много пользователей, используйте кнопки *Назад* и *Далее* для навигации по списку пользователей.

5. Нажмите кнопку *OK*.

6.2.13 Изменение настроек пароля

В CMC 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 CMC.
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*.

> ⓘ Примечание
>
> При изменении пароля пользователя будет осуществлен выход этого пользователя из всех существующих сеансов, и он будет направлен на домашнюю страницу, чтобы снова выполнить вход в систему.

6.2.13.2 Изменение общих настроек пароля

> ⓘ Примечание
>
> Неактивные учетные записи пользователей не отключаются автоматически.

1. Перейдите в область управления CMC *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.

   Настройки пароля

Настройка пароля	По умолчанию	Минимум	Рекомендованный максимум
Должен содержать не менее N символов	8 символов	6 символа	255 символов
Не может превышать N символов	255 символов	13 символов	255 символов
Должен изменять пароль каждые N дн.	30 дн.	2 дн.	100 дней
Не может повторно использовать N последних паролей	3 пароля	1 пароль	100 паролей
Должен ждать N мин. для изменения пароля	0 минут	0 минут	100 минут

Настройка пароля	По умолчанию	Минимум	Рекомендованный максимум
Отключать учетную запись после N неудачных попыток входа	10 неудачная попытка	1 неудачная попытка	100 неудачных попыток
Сбрасывать счетчик неудачных попыток через N мин.	5 минут	1 минута	100 минут
Повторно включать учетную запись через N мин.	5 минут	0 минут	100 минут

> ⓘ Примечание
>
> При обновлении более ранней версии платформы SAP BusinessObjects Business Intelligence с заменой на более новую версию или при выполнении расширенной установки необходимо установить для параметра *Отключать учетную запись после N неудачных попыток входа* значение по умолчанию.

> ⓘ Примечание
>
> Вышеупомянутые правила применимы только к пользователям Enterprise и не предназначены для других типов аутентификации сторонних поставщиков.

4. Нажмите кнопку *Обновить*.

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 IT доступ к редактированию и удалению объектов.

Связанные сведения

Для назначения принципалов списку управления доступом к объекту [страница 139]

6.2.15 Управление доступом к каталогам "Входящие" пользователей

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

Связанные сведения

Управление настройками безопасности для объектов в CMC [страница 138]

6.2.16 Настройка параметров стартовой панели BI в стиле Fiori

В CMC администраторы могут настроить предпочтительные параметры стартовой панели BI в стиле Fiori для групп пользователей.

> ⓘ Примечание
>
> Если пользователь входит в две или несколько групп, на стартовой панели BI в стиле Fiori отображаются предпочтения, настроенные только для одной из них.

6.2.16.1 Настройка экрана входа в систему стартовой панели BI в стиле Fiori

По умолчанию на экране входа в систему стартовой панели BI в стиле Fiori содержится запрос на ввод имени пользователя и пароля. Можно также настроить приглашение пользователей на ввод имени CMS и типа аутентификации. Чтобы изменить эту настройку, необходимо отредактировать свойства стартовой панели BI в стиле Fiori для файла BOE.war.

6.2.16.1.1 Настройка экрана входа в систему стартовой панели BI в стиле Fiori

Чтобы изменить настройки по умолчанию стартовой панели BI в стиле Fiori, необходимо задать пользовательские свойства 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:

```
<INSTALLDIR>\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:

   `FioriBI.properties`
4. Чтобы включить параметры аутентификации на экране входа в систему стартовой панели BI в стиле Fiori, 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 в стиле Fiori, 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 предпочтений стартовой панели BI в стиле Fiori для групп пользователей в CMC

Администраторы настраивают стандартные предпочтения стартовой панели BI в стиле Fiori для групп пользователей в CMC.

Настроенные администратором предпочтения для группы пользователей применяются ко всем пользователям в группе. Если пользователь входит в две или несколько групп, на стартовой панели BI в стиле Fiori отображаются предпочтения, настроенные только для одной из них.

Пользователи могут настраивать собственные предпочтения на стартовой панели BI в стиле Fiori, и эти предпочтения будут иметь приоритет перед значениями по умолчанию. Они также могут снова переключиться на предпочтения по умолчанию в любое указанное время. См. раздел *Установка*

предпочтений страницы для *Руководства пользователя стартовой панели Business Intelligence в стиле Fiori*.

Однако если администратор изменяет в CMC стандартные предпочтения стартовой панели BI в стиле Fiori, эти значения по умолчанию имеют приоритет перед значениями, определенными пользователями.

6.2.16.2.1 Настройка предпочтений стартовой панели BI в стиле Fiori для группы пользователей

1. Перейдите в область *Управление пользователями и группами* консоли CMC.
2. В *Списке групп* выберите группу пользователей, для которой требуется задать предпочтения стартовой панели BI в стиле Fiori.
3. Щелкните правой кнопкой мыши и выберите *Предпочтения стартовой панели BI в стиле Fiori*.
4. Снимите флажок *Предпочтения не определены*.
5. Для настройки вкладки *Домашняя страница* выполните одно из следующих действий для выбора требуемой домашней страницы для вкладки:

Опция вкладки домашней страницы	Действие
Просмотр вкладки домашней страницы стартовой панели BI в стиле Fiori по умолчанию	Выберите *Вкладка "Домашняя страница по умолчанию"*
Просмотр специфической вкладки домашней страницы	Выберите *Вкладка "Выбор домашней страницы"*, затем: 1. В поле *Начальная страница* выберите начальную страницу: • *Моя домашняя страница* • *Расписание* • *Входящие* • *Папки* • *Корзина* 2. В поле *Представление документов* выберите представление: *Плитки* (по умолчанию) или *Список*. 3. В поле *Начальный фильтр* выберите начальный фильтр: • *Показать все* • *Мои документы* • *Все категории* • *Мое избранное* • *Мои недавно просмотренные* • *Мои недавно запущенные* Можно выбрать объект из *Мои папки*, *Общие папки* *Личные категории* и *Корпоративные категории* для от-

Опция вкладки домашней страницы	Действие
	ображения в качестве начальной страницы по умолчанию.
Просмотр специфического отчета в качестве домашней страницы	Выберите *Выбрать отчет*, затем щелкните *Обзор документов*, чтобы выбрать документ из *Моих папок* или *Общих папок*.
Просмотр категории в качестве домашней страницы	Выберите *Выбрать категорию*, затем щелкните *Обзор категорий*, чтобы выбрать категорию из *Личных категорий* или *Корпоративных категорий*.

6. В поле *Выбрать столбец для отображения на вкладке "Документы"* выберите предпочтения для столбца:
   - *Тип*
   - *Дата последнего запуска*
   - *Экземпляры*
   - *Описание*
   - *Автор*
   - *Последнее обновление*
   - *Дата создания*
   - *Расположение (категории)*
   - *Избранное (домашняя страница)*
   - *Состояние (расписание)*
   - *Время создания экземпляра (расписание)*
   - *Путь к папке*

   > **Примечание**
   >
   > По умолчанию выбираются столбцы *Тип*, *Описание*, *Последнее обновление*, *Избранное (домашняя страница)*, *Состояние (расписание)* и *Время создания экземпляра (расписание)*. Набор отображаемых столбцов можно изменить.

7. Нажмите *Сохранить и закрыть*.

Чтобы определенные администратором предпочтения отражались в интерфейсе, пользователи должны выполнить вход на стартовую панель BI в стиле Fiori, выбрать *Настройки* > *Предпочтения учетной записи* > *Предпочтения страницы* и включить *Использовать предоставленные администратором настройки*.

6.2.17 Управление атрибутами системных пользователей

Администраторы платформы BI определяют и добавляют атрибуты системных пользователей в области *Управление пользовательскими атрибутами* консоли Central Management Console (CMC). Можно расширять атрибуты и управлять ими для следующих пользовательских каталогов:

- Enterprise
- SAP
- LDAP
- Windows AD

При импорте пользователей из таких внешних каталогов, как SAP, LDAP и Windows AD, для учетных записей пользователей, как правило, доступны следующие атрибуты:

- Полное имя
- Адрес электронной почты

Имена атрибутов

Все атрибуты пользователей, добавляемые в систему, должны содержать следующие свойства:

- *Имя*
- *Внутреннее имя*

Свойство «Имя» — это дружественный идентификатор атрибута, который используется для запроса фильтров при работе с семантическим уровнем юниверса. Для получения дополнительных сведений см. документацию по средству создания юниверсов. «Внутреннее имя» используется разработчиками, работающими с SDK платформы Business Intelligence. Это свойство — автоматически сформированное имя.

Имена атрибутов должны содержать не более 256 символов и только буквенно-цифровые символы и символы подчеркивания.

> → Совет
>
> Если в атрибуте "Имя" использованы недопустимые символы, внутреннее имя в платформе BI создано не будет. Внутренние имена нельзя изменить после их добавления в систему. Рекомендуется тщательно выбрать соответствующие имена атрибутов с буквенно-цифровыми символами и подчеркиваниями.

Предварительные требования для развертывания сопоставленных пользователем атрибутов

Чтобы добавить атрибуты пользователей в систему, во всех используемых подключаемых модулях аутентификации для внешних каталогов пользователей необходимо настроить возможность сопоставлять и импортировать пользователей. Кроме того, потребуется ознакомиться со схемой внешних каталогов, в частности с именами, используемыми для целевых атрибутов.

> ⓘ Примечание
>
> Для подключаемого модуля аутентификации SAP можно указать только атрибуты, которые содержатся в структуре BAPIADDR3.

Когда на платформе BI будет настроена возможность сопоставления новых атрибутов пользователя, значения подставятся автоматически после следующего запланированного обновления. Все атрибуты пользователя отобразятся в области управления *Пользователи и группы* консоли CMC.

6.2.18 Определение приоритетов атрибутов пользователя для нескольких вариантов аутентификации

При настройке подключаемых модулей аутентификации для SAP, LDAP и AD можно указать уровни приоритетов каждого подключаемого модуля относительно двух других. Например, в области аутентификации LDAP используйте параметр *Установка приоритета для привязки атрибута LDAP относительно других привязок атрибутов*, чтобы указать приоритет LDAP относительно SAP и AD. По умолчанию значение атрибута Enterprise имеет более высокий приоритет, чем любое значение из внешнего каталога. Приоритеты привязки атрибутов устанавливаются на уровне подключаемого модуля аутентификации, а не отдельно для какого-либо атрибута.

Связанные сведения

Настройка хоста LDAP [страница 284]
Чтобы выполнить импорт ролей SAP [страница 358]

6.2.19 Добавление нового атрибута пользователя

Перед добавлением нового атрибута пользователя в платформу Business Intelligence необходимо настроить подключаемый модуль аутентификации для внешнего каталога, из которого выполняется отображение учетных записей пользователей. Это относится к SAP, LDAP и Windows AD. Конкретно, следует проверить параметр *Импорт полного имени, адреса электронной почты и других атрибутов* для всех требуемых подключаемых модулей.

> ⓘ Примечание
>
> Для распространения атрибутов на учетные записи пользователей Enterprise выполнение предварительных задач не требуется.

> → Совет
>
> Если один атрибут планируется распространить на несколько подключаемых модулей, рекомендуется установить для атрибута уровень приоритета привязки, соответствующий требованиям организации.

1. Перейдите к области *Управление атрибутами пользователя* консоли CMC.
2. Щелкните значок *Добавить новый сопоставленный пользователем атрибут*.

Откроется диалоговое окно *Добавить атрибут*.

3. В поле *Имя* укажите имя нового атрибута.

   В рамках платформы BI введенное имя будет использоваться в качестве понятного имени для нового атрибута.

   Когда дружественное имя будет введено, в поле *Внутреннее имя* автоматически подставится значение в следующем формате: `SI_[Дружественное_имя]`. После того как системный администратор укажет "дружественное" имя, на платформе Business Intelligence будет автоматически создано "внутреннее" имя.

4. При необходимости измените поле *Внутреннее имя*; допускается использование букв, цифр и знаков подчеркивания.

   > → Совет
   >
   > Значение поля *Внутреннее имя* можно изменить только на этом этапе. После сохранения нового атрибута изменить это значение невозможно.

   Если новый атрибут предназначен для учетных записей Enterprise, перейдите к шагу 8.

5. Выберите необходимый параметр *Добавить новый источник для* из списка и щелкните значок *Добавить*. Доступны следующие параметры:

   - *SAP*
   - *LDAP*
   - *AD*

   Для указанного источника атрибута создается строка таблицы.

6. В столбце *Имя источника атрибута* укажите имя атрибута в каталоге источника.

   В рамках платформы BI механизм автоматической проверки существования указанного имени атрибута во внешнем каталоге не предусмотрен. Убедитесь, что указано правильное и действительное имя.

7. Повторите шаги 5-6, если для нового атрибута требуются дополнительные источники.

8. Нажмите кнопку *OK*, чтобы сохранить новый атрибут и отправить его в платформу BI. "Имя", "Внутреннее имя", "Источник" и "Имя источника атрибута" для нового атрибута отобразятся в области *Управление атрибутами пользователя* консоли CMC.

Новый атрибут и его соответствующее значение для каждой задействованной учетной записи пользователя после следующего запланированного обновления появятся в области управления *Пользователи и группы*.

Если для нового атрибута используется несколько источников, убедитесь, что для каждого подключаемого модуля аутентификации указан правильный приоритет привязки атрибута.

6.2.20 Редактирование настроенных атрибутов пользователя

Используйте следующую процедуру для редактирования атрибутов пользователя, созданных в платформе BI. Можно изменить следующие элементы:

- Имя атрибута в платформе BI.

> **Примечание**
>
> Это не "Внутреннее имя" атрибута. После создания атрибута и его добавления в платформу BI внутреннее имя изменить невозможно. Чтобы удалить внутреннее имя, администраторы должны удалить связанный атрибут.

- Имя источника атрибута
- Дополнительные источники атрибута

1. Перейдите к области *Управление атрибутами пользователя* консоли CMC.
2. Выберите атрибут, который требуется изменить.
3. Щелкните значок *Изменить выбранный атрибут*.
   Откроется диалоговое окно *Правка*.
4. Измените "Имя" атрибута или данные источника.
5. Нажмите кнопку *OK*, чтобы сохранить изменения и передать их в платформу BI.
   Измененные значения отобразятся в области *Управление атрибутами пользователя* консоли CMC.

Имя и значения измененного атрибута отобразятся после следующего запланированного обновления в области управления *Пользователи и группы*.

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 CMC 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 CMC 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 CMC.
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 CMC 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 CMC.
2. Выберите пользователя, которому будет присвоен псевдоним.
3. Выберите команду *Управление* > *Свойства*.
   Откроется 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 CMC 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 CMC.
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 *OK*.

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, сопоставленной 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 CMC *Аутентификация*.

1. Перейдите в область управления *Пользователи и группы* консоли CMC.
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 *OK*.
   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 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. 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 CMC.
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.

Связанные сведения

Для удаления псевдонима [страница 127]

7 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.

Связанные сведения

Переопределение прав [страница 133]

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 потребуется 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.

Связанные сведения

Работа с уровнями доступа [страница 144]

7.1.2 Параметры расширенных прав

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

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

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

Параметры прав

Значок	Параметр прав	Описание
	Предоставлено	Право предоставлено принципалу.

Значок	Параметр прав	Описание
	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*.

Связанные сведения

Права для конкретных типов объектов [страница 136]

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.

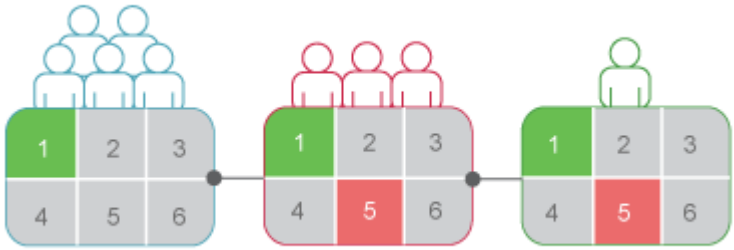
По умолчанию пользователи или группы, которые имеют права на папку, унаследуют те же права на любой объект, который в последствии будет опубликован в эту папку. Следовательно, лучшей стратегией является установка соответствующих прав для пользователей и групп сначала на уровне папки, а потом публиковать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

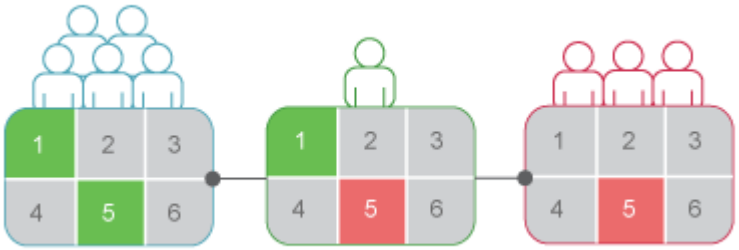
В «первом примере наследования группы» можно увидеть принципы работы наследования группы. Красная группа является группой, вложенной в синюю группу, поэтому она наследует права синей группы. В этом случае она наследует право 1 как предоставленное и остальные права как неопределенные. Каждый элемент красной 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.



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.



Пример наследования группы 2

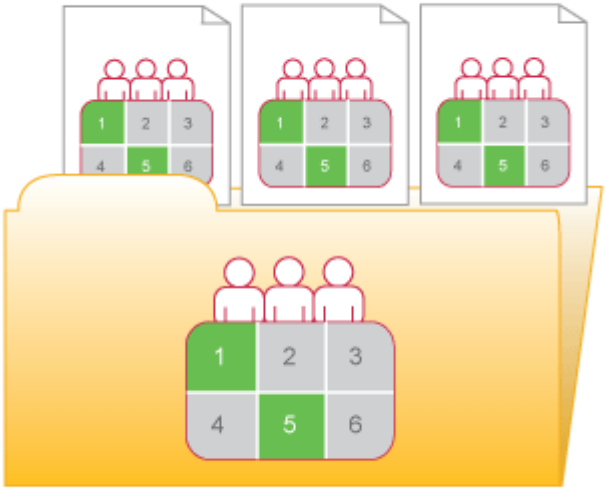
Связанные сведения

Переопределение прав [страница 133]

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.



Пример наследования папок

Связанные сведения

Переопределение прав [страница 133]

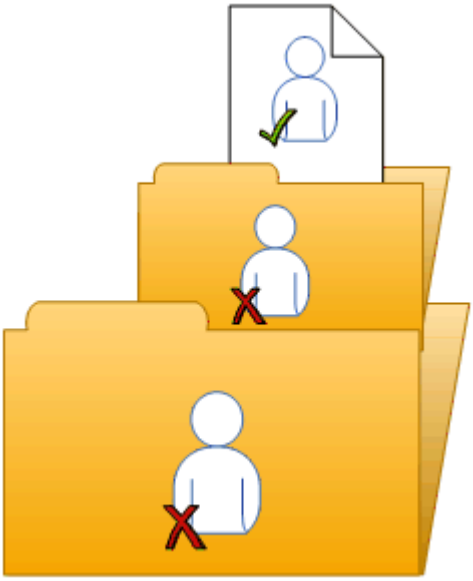
7.1.3.3 Переопределение прав

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.

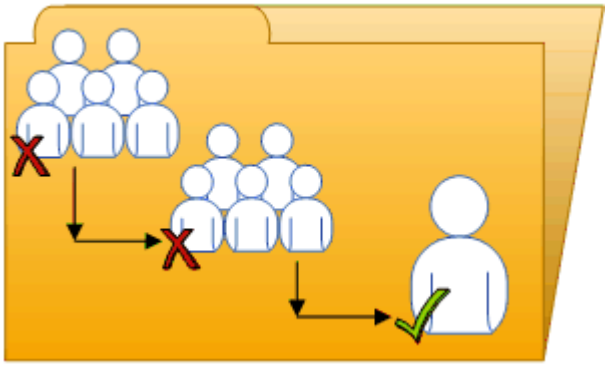
Вам не нужно блокировать наследование для установки настраиваемых прав на объект. Дочерний объект наследует настройки прав родительского объекта и содержит права, которые явно установлены на дочерний объект. Кроме того, любые изменения настроек прав родительского объекта применяются и к дочернему.

«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.



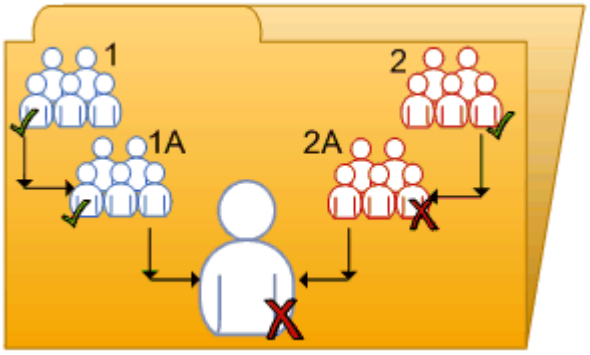
Пример переопределения прав 1

«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.



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.



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 менеджеру по продажам нужно просмотреть конфиденциальные отчеты в папке "Конфиденциально". Менеджер по продажа 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".

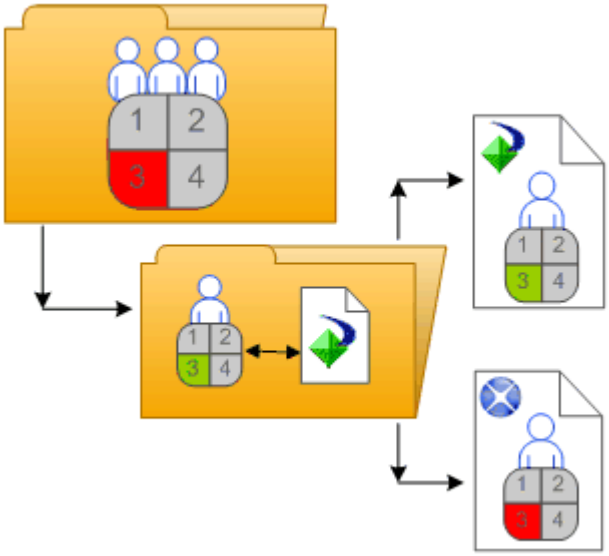
Области действия прав также могут сокращать эффективные права делегированного администратора. Например, делегированный администратор может иметь права *Редактирование* и *Защищенное изменение прав* по отношению к папке, но область действия этих прав ограничивается только этой папкой и не применима к 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.



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:

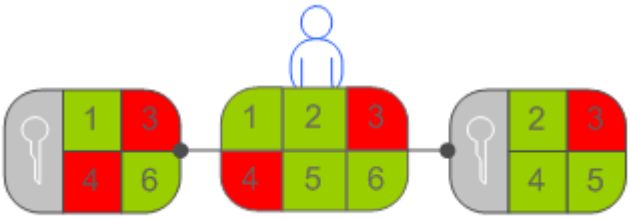
- *Общие*
  Эти права влияют на все объекты.
- *Содержимое*
  Эти права делятся в зависимости от типа содержимого объектов. Примерами типов объектов являются отчеты Crystal и Adobe Acrobat PDF.
- *Приложение*
  Эти права делятся в зависимости от того, на какое приложение платформы BI они влияют. Примерами приложений являются CMC 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.



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 CMC

Можно управлять настройками безопасности большинства объектов в CMC, 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.

Связанные сведения

Для изменения безопасности объекта для принципала [страница 140]

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"*.

Связанные сведения

Для назначения принципалов списку управления доступом к объекту [страница 139]

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 CMC, 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 *OK*.

   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.

Связанные сведения

Для назначения принципалов списку управления доступом к объекту [страница 139]
Для изменения безопасности объекта для принципала [страница 140]

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.

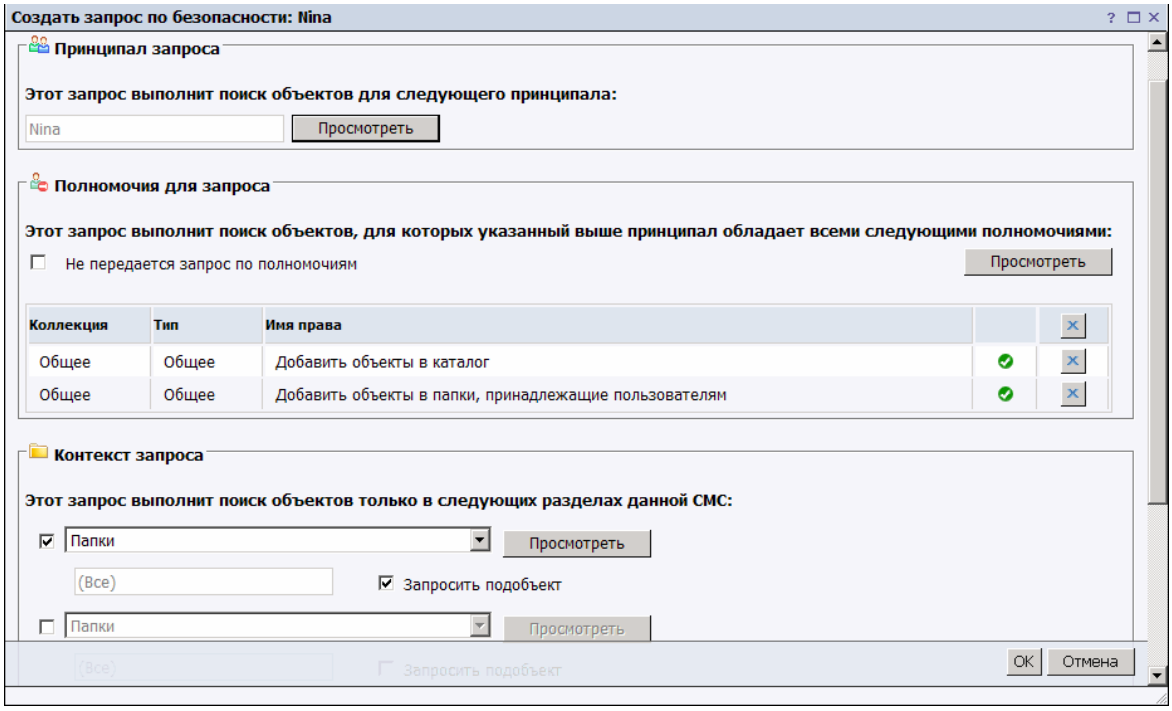
- Контекст запроса
  Укажите области CMC, по которым запрос безопасности будет выполнять поиск. Для каждой области можно выбрать, включать или не включать в запрос безопасности подобъекты. В запрос безопасности можно включить максимум четыре области.

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*.



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 *OK* 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 *OK*.

     > → 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 контроля доступа, независимо от полномочий принципала на доступ к объекту.

5. В области *содержание запроса* укажите области СМС, которые хотите запросить.
   a. Установите флажок рядом в 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 *OK*. 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 CMC, которую хотите запросить.

> ⓘ Примечание
>
> Запрос может включать максимум 4 области.

6. Нажмите кнопку *OK*.
   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 предопределенных уровней доступа в платформе BI, чтобы быстро и единообразно установить права для многих принципалов.

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

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.	• Просмотр объектов • Просмотр экземпляров документа
Запланировать	Принципал может создавать экземпляры, планируя запуск объекта в соответствии с указанным источником данных один раз или периодически. Принципал может просматривать, удалять и приостанавливать расписание экземпляров, которыми владеет. Принципалы могут также составлять расписание для различных форматов и адресатов, настраивать параметры и информацию о подключении к базе данных, выбирать серверы для обработки заданий, добавлять содержимое в папку, а также копировать объект или папку.	Права уровня доступа *Просмотр*, плюс: • 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: • Обновить данные отчета
Полное управление	Принципал может осуществлять полное управление объектом.	Все доступные права, включая: • 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	Права на *Добавление* для папки верхнего уровня *Уровней доступа*
Просмотр конкретных прав в уровне доступа	Права на *Просмотр* для уровня доступа.

Задача, связанная с уровнем доступа	Необходимые права
Назначить принципалу уровень доступа к объекту	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 **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.
Изменить уровень доступа	Права на *Просмотр* и *Редактирование* для уровня доступа
Удалить уровень доступа	Права на *Просмотр* и *Удаление* для уровня доступа
Клонировать уровень доступа	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 менеджерам 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 периодичные 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 *OK*.
   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*.

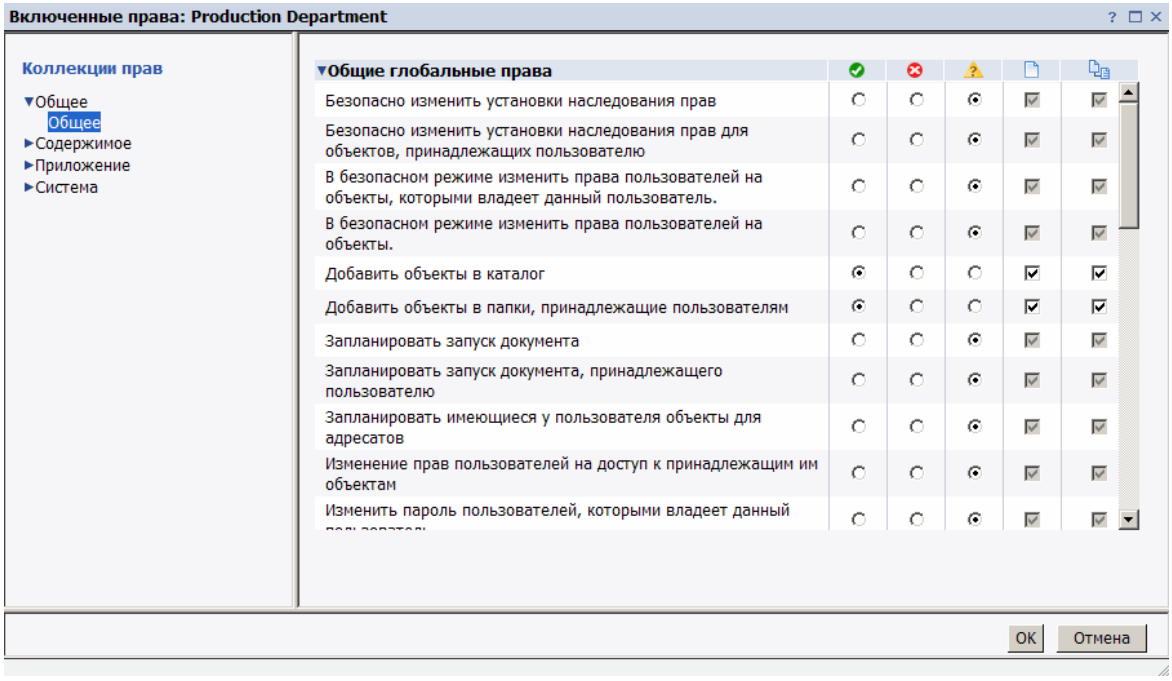
   > **Примечание**
   >
   > Предварительно определенные уровни доступа удалить нельзя.

   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 *OK*.
   Вы вернетесь к списку действующих прав.

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 CMC. 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 A и подразделение B, в подразделение C. Администратор решает удалить все уровни доступа для подразделений A и B, 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 CMC 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.

> **ⓘ Примечание**
>
> 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 A к отчету Crystal, и этот отчет тиражируется по сайтам, уровень доступа A 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.

Связанные сведения

Интеграция [страница 996]
Трассировка связи между уровнями доступа и объектами [страница 149]

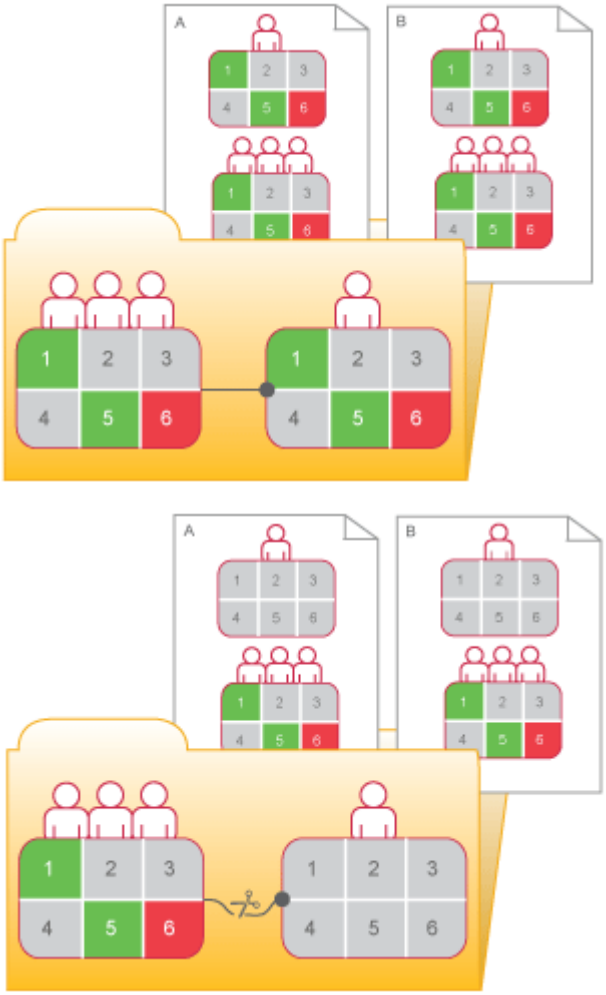
7.4 Отключение наследования

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.



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 принципалом 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 *OK*.

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 ИТ-подразделения.

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

> ⓘ 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.

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

Действия делегированных администраторов	Права, необходимые делегированному администратору
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
Изменение паролей только для принципалов, созданных данным делегированным администратором	*Право владельца на изменение пароля* в отношении папки *Пользователи* высшего уровня, или соответствующих групп **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.
Изменение имен пользователей, описания, других атрибутов, а также перераспределение пользователей по другим группам	*Право на изменение* в отношении соответствующих групп
Изменение имен пользователей, описания, других атрибутов, а также перераспределение пользователей по другим группам, но только в отношении пользователей, созданных данным делегированным администратором	*Право владельца на изменение* в отношении папки *Пользователи* высшего уровня, или соответствующих групп **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.

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 A 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 A 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 A может изменять только права пользователей на объекты, в отношении которых он имеет *право на безопасное изменение прав*.

Пользователь A может изменять права пользователя B на объект O при наличии следующих условий:

- Пользователь A имеет *право на безопасное изменение прав* в отношении объекта O.
- Каждое право или уровень доступа, изменяемые пользователем A для пользователя B, предоставлены пользователю A.
- Пользователь A имеет *право на безопасное изменение прав* пользователя B.
- Если назначается уровень доступа, пользователь A имеет право на *присвоение уровня доступа* пользователю B, 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. На 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 позволят 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.

8 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 Enterprise, 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 Безопасное использование программных объектов

Если у пользователя есть права на расписания для программных объектов, он имеет право на их запуск.

Для программ Java пользователи могут выполнять следующие действия:

- Пользователи могут указывать основной класс. Автор программы должен убедиться, что никакой вторичный/тестовый основной класс непреднамеренно не оставлен в программе.
- Пользователи могут указывать путь к классу. У них не должно быть права загружать JAR-файлы в систему. Его можно использовать для выполнения специально сформированного кода.

Общие рекомендации по обеспечению безопасности программных объектов

- Не предоставляйте пользователю учетные данные для входа на сервер.
- Предоставьте учетной записи пользователя, выполняющего программу на сервере, минимальные права. В особенности запретите доступ к каталогу установки платформы SAP BusinessObjects Business Intelligence.
- Рекомендуется выбрать параметр *Не выполнять задание* в разделе *Приложения* > *Central Management Console* > *Права на программные объекты*.
- Для контроля доступа рекомендуется использовать папки. Программные объекты с разными уровнями безопасности следует размещать в разных папках.

8.3 Планирование аварийного восстановления

Для защиты инвестиций организации в платформу 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. Кроме того, дополнительную информацию см. в этой SAP-ноте.

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 на серверах репозитория файлов: включает в себя патентованное содержимое, например 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 все важнейшие метаданные для развертывания, такие как сведения о пользователе, отчеты и другую информацию повышенной важности для организации.
- Файл ключа информации базы данных (файл .dbinfo): этот ресурс содержит основной ключ для системной базы 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.

8.4 Общие рекомендации по обеспечению безопасности развертывания

Ниже приведены рекомендации по безопасности развертывания платформы BI.

- Используйте брандмауэры для защиты обмена данными между CMS и другими компонентами системы. Если возможно, всегда скрывайте CMS за брандмауэром. По крайней мере следует убедиться, что системная база данных защищена брандмауэром.
- Добавьте дополнительное шифрование для серверов репозитория файлов. Когда система будет в состоянии готовности, патентованное содержимое будет сохраняться на этих серверах. Добавьте дополнительное шифрование через ОС или воспользуйтесь средством стороннего разработчика.
- Обратный прокси-сервер развертывается перед серверами веб-приложений, чтобы скрыть их за одним IP-адресом. При данной конфигурации весь Интернет-трафик, адресованный частным серверам веб-приложений, таким образом направляется через обратный прокси-сервер, скрывая частные IP-адреса.
- Следует строго придерживаться корпоративной политики относительно паролей. Убедитесь, что пользовательские пароли регулярно изменяются.
- Если была выбрана установка системной базы данных и сервера веб-приложений, поставляемого с платформой BI, требуется обратиться к соответствующей документации, чтобы убедиться, что эти компоненты будут развернуты с учетом необходимых настроек безопасности.
- Используйте протокол Secure Sockets Layer (SSL) для сетевого обмена данными между клиентами и серверами в развертывании.
- Убедитесь, что каталог установки платформы и его вложенные каталоги надежно защищены (в процессе эксплуатации системы в них могут храниться временные 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*.
- По умолчанию сообщения об ошибках Web Intelligence включают информацию о схеме базы данных. Чтобы сообщения об ошибках отображались без информации о схеме базы данных, выполните следующие действия:
  1. Откройте файл конфигурации `WebIContainer_ServerDescriptor.xml` для редактирования. По умолчанию он расположен в следующем каталоге `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64config`.
  2. Измените значение указанного параметра на False: `WebiParamDetailedDbErrorsEnabled = False`.

> ⚠ Предупреждение
>
> Заполнители, отличные от предназначенных для редактирования, не следует изменять ни в коем случае. Системный администратор должен обеспечить, чтобы права на редактирование в узле были только у соответствующих лиц из группы администраторов (которые предназначены для управления узлом). Для всех остальных пользователей, включая других членов группы

администраторов, должны быть установлены ограничения на просмотр объектов узла или управление ими путем применения соответствующих прав безопасности. Если какое-либо значение заполнителя случайно повреждено и CMS не появляется, см. SAP-ноту 3269127.

ⓘ Примечание

См. статью 3278916 в базе знаний SAP, чтобы узнать, как ограничить изменяемые заполнители, чтобы избежать возможного вредоносного вмешательства в ландшафт BI.

Связанные сведения

Настройка протокола SSL [страница 194]
Ограничения для пароля [страница 167]
Настройка безопасности для связанных серверов сторонних производителей [страница 161]

8.5 Настройка безопасности для связанных серверов сторонних производителей

Если была выбрана установка компонентов сервера сторонних производителей, связанных с платформой BI, рекомендуется обратиться к разделам, посвященным безопасности, официальной документации для SAP SQL Anywhere и Apache Tomcat .

8.6 Активные доверительные отношения

В сетевой среде доверительное отношение между двумя доменами, как правило, представляет собой соединение, которое позволяет одному домену 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.

8.6.1 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.

8.6.2 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 квитанция 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.

8.7 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 платформа BI 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.

8.7.1 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 удается подключиться к CMS в течении десяти минут, центральный сервер управления удаляет сеанс CMS. Таким образом обрабатываются сеансы, где компоненты клиентской стороны беспорядочно завершают работу.

8.7.2 Управление сеансами

Можно просматривать и завершать сеансы в CMC.

Можно просматривать и завершать сеансы пользователей в Central Management Console (CMC). Например, может потребоваться узнать, какие пользователи используют несколько сеансов. Или может потребоваться завершить сеансы, потребляющие слишком много системных ресурсов, или очень старые сеансы. Также может потребоваться завершить сеансы при подготовке системы к простою или обновлению.

8.7.2.1 Просмотр списка сеансов

Просмотр сеансов осуществляется в CMC.

Можно просмотреть список сеансов в Central Management Console (CMC).

1. Войдите в CMC как администратор.
2. В области *Управление* щелкните *Сеансы*.

Будет выведен список сеансов пользователей для кластера. Можно щелкать заголовки столбцов для сортировки списка по имени пользователя, по числу открытых сеансов или по времени входа в систему. Также можно щелкнуть имя пользователя, число сеансов или время входа в систему, чтобы просмотреть подробные сведения о сеансах пользователя на нижней панели.

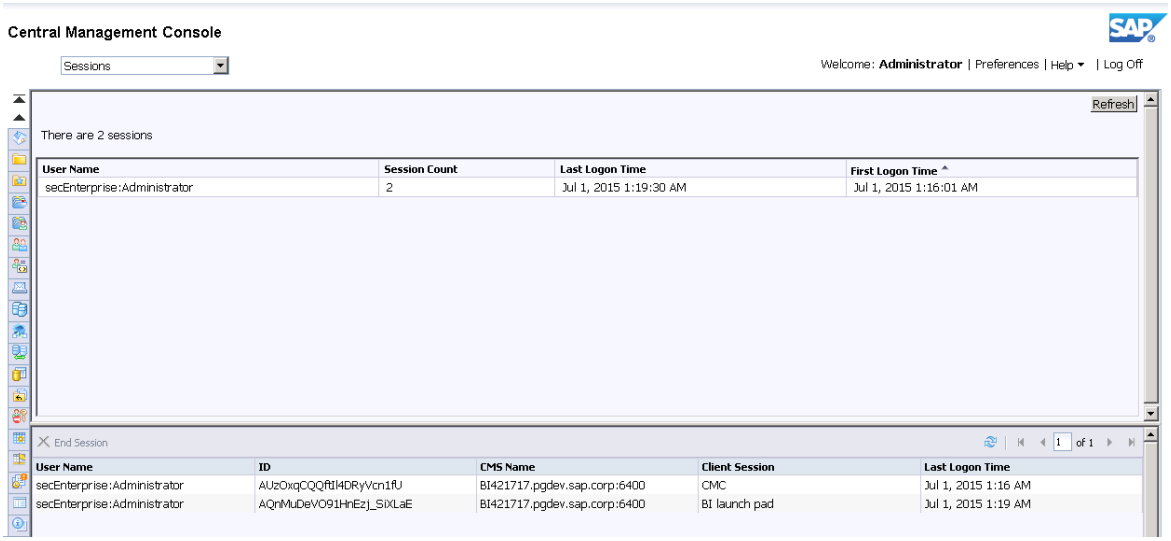
8.7.2.2 Завершение сеансов

Завершение сеансов осуществляется в CMC.

Можно завершить один или несколько сеансов.

1. Войдите в CMC как администратор.
2. В области *Управление* щелкните *Сеансы*.

   Будет выведен список сеансов пользователей для кластера.



3. Щелкните имя пользователя, число сеансов или время входа в систему, чтобы вывести сеансы пользователя на нижней панели.
4. Щелкните сеанс, чтобы выбрать его (для выбора нескольких сеансов используйте CTRL + щелчок).
5. Нажмите *Завершить сеанс*.

> **Примечание**
>
> Сеанс пользователя будет закрыт, как только пользователь закроет браузер.

> **Примечание**
>
> Для завершения сеансов требуется право «Изменить объекты» по отношению к объекту CMS.

> **Примечание**
>
> Нельзя завершить свой текущий сеанс администратора.

8.7.3 Скрипт для очистки устаревших сеансов

Скрипт

Введен скрипт для очистки устаревших сеансов и освобождения неиспользуемых лицензий, чтобы сделать их доступными для пользователей, ожидающих входа в систему. Этот скрипт продолжает выполняться до тех пор, пока не будет закрыт вручную. Он проверяет наличие устаревших сеансов и прекращает их с интервалом в 10 минут.

- Скрипт для Windows можно найти здесь: `<Каталог_установки_BI>\SAP BusinessObjects Enterprise XI 4.0\java\lib\StaleSessionCleaner.jar`
- Скрипт для Unix можно найти здесь: `<Каталог_установки_BI>/sap_bobj/enterprise_xi40/java/lib/StaleSessionCleaner.jar`

Синтаксис, используемый для скрипта:

> **Синтаксис кода**

```
java -jar StaleSessionCleaner.jar <username> <password>
<machine:port><authentication> <logdir>
```

8.8 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".

8.8.1 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 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.

8.8.2 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.

8.8.3 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.

8.8.4 Ограничения для пароля

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

1. Принудительно устанавливать пароли с символами в разных регистрах
   Этот параметр гарантирует, что пароль будет содержать по крайней мере один символ в верхнем и один в нижнем регистре. По умолчанию он установлен, но это может быть изменено администратором.
2. Обязательное использование цифр в пароле
   Этот параметр гарантирует, что пароль содержит по крайней мере один цифровой символ.
3. Обязательное использование специальных символов в пароле
   Если этот параметр выбран, пароль должен содержать минимум один специальный символ.

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

8.8.5 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

8.8.6 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.

8.8.7 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.

8.9 Аудит изменений параметров безопасности

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

- 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 CMC. Это также справедливо в отношении изменений, выполняемых в CCM. Изменения, фиксируемые с использованием CMC, могут подвергаться аудиту.

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 определят 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 Интерфейс сканирования на наличие вирусов

Разные типы файлов (Adobe Acrobat, Microsoft Excel, Microsoft Word, Microsoft PowerPoint, Lumira, Crystal Reports, Web Intelligence и т. д.) можно фиксировать на платформе BI с помощью консоли CMC, стартовой панели BI, веб-служб REST и пользовательских приложений SDK. В каталоге-адресате эти файлы проходят проверку размера (чтобы убедиться, что файл имеет ненулевой размер) и проверку разрешений. После появления в BI 4.2 SP4 интерфейса сканирования на наличие вирусов файлы, которые вы фиксируете на платформе BI, также фиксируются в системе сканирования на вирусы, чтобы убедиться, что содержимое таких файлов не заражено и не содержит вирусов.

Файлы проходят сканирование на вирусы, когда вы:

- добавляете новый файл;
- нажимаете кнопку "Сохранить как" для документа;
- копируете документ;
- нажимаете кнопку "Отправить в каталог входящих" для документа;
- создаете экземпляр документа;
- выполняете любую операцию, которая фиксирует новый файл на серверах репозитория файлов.

> ⓘ Примечание
>
> Сканирование на вирусы проходят только вновь фиксируемые на платформе BI в BI 4.2 SP4 файлы (то есть после включения сканирования на вирусы).

8.11.1 Включение сканирования на вирусы

Можно включить сканирование на вирусы для файлов, зафиксированных на платформе BI, для серверов репозиториев входных и выходных файлов.

Вы загрузили библиотеку адаптеров для сканирования на вирусы (VSA) от сертифицированного SAP поставщика. Список сертифицированных SAP поставщиков см. на сайте http://global.sap.com/community/ebook/2013_09_adpd/enEN/search.html#search=NW-VSI.

> ⓘ Примечание
>
> Если вам требуется поддержка в работе с новой платформой или поставщиком, обратитесь к соответствующим поставщикам.

Чтобы включить сканирование на вирусы на сервере репозитория входных файлов, выполните следующие действия:

1. Войдите на консоль CMC.

2. Перейдите в раздел *Серверы* > *Список серверов*.
3. Щелкните правой кнопкой мыши сервер репозитория входных файлов и в раскрывающемся списке выберите *Свойства*.

   Откроется окно *Свойства*.
4. В разделе *Служба хранилища входных файлов* установите флажок *Включить сканирование на вирусы*.
5. В поле *Расположение файла адаптера для сканирования на вирусы* введите абсолютный путь к файлу библиотеки адаптеров для сканирования на вирусы.
6. Нажмите кнопку *Сохранить и закрыть*.

> **Примечание**
>
> - По умолчанию сканирование на вирусы отключено для всех файлов, зафиксированных на платформе BI 4.2 SP4.
> - Включить сканирование на вирусы можно с помощью графического интерфейса пользователя или интерфейса командной строки. Аргумент командной строки, который требуется предоставить на серверах репозиториев файлов для включения сканирования на вирусы, – `vsaFileLoc`.
> - Выполните аналогичные действия, чтобы включить сканирование на вирусы на сервере репозитория выходных файлов. При наличии нескольких серверов репозиториев входных и выходных файлов не забудьте включить сканирование на вирусы на каждом из серверов.
> - После включения сканирования на вирусы необходимо перезапустить серверы репозиториев файлов, чтобы изменения вступили в силу.

8.12 Безопасность 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.

8.12.1 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 BI 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 BI 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.

8.12.1.1 Для включения FIPS-совместимого режима в Windows

По умолчанию FIPS-совместимый режим включается при установке платформы BI.

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 *OK*, 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.

8.12.1.2 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.

8.12.1.3 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 и выберите *Свойства*.
   Отобразится диалоговое окно *Свойства* с вкладкой *Свойства*.
3. Удалите `-FIPS` из поля *Команда* и щелкните *Применить*.
4. Нажмите кнопку *OK*, чтобы закрыть диалоговое окно *Свойства*.
5. Перезапустите SIA.

8.12.2 Учетные записи администратора

Платформа BI автоматически создает начальную учетную запись администратора. Рекомендуется создать учетную запись в группе "Администраторы" для каждого лица.

Пользователю-администратору автоматически предоставляется право *Изменение прав пользователей на объекты*. После создания учетной записи администратора не забудьте отключить начальную учетную запись администратора.

8.12.3 Права соединений

По умолчанию администраторы имеют доступ к сведениям о соединениях, включая пароли, если соединения определены с учетными данными.

В этом разделе объясняется, как применять принцип наименьших привилегий для соединений, если доступ к источникам данных администраторов не предполагается.

Ограничение права "Загрузить соединение локально"

Право *Загрузить соединение локально* строго необходимо только для пользователей, управляющих соединениями (см. Права соединений [страница 1190]). Оно должно предоставляться только отдельным пользователям, а не группам. Если группа имеет соответствующее право, любой добавленный пользователь может получить доступ к сведениям о соединениях.

Чтобы полностью защитить соединения, выполните следующие действия:

1. Предоставьте право *Загрузить соединение локально* пользователям, управляющим соединениями.
2. Запретите *Загрузить соединение локально* в верхней папке соединений для групп "Администраторы" и "Пользователи Universe Designer".

Чтобы пользователи не могли предоставить себе право самостоятельно, см. следующий раздел.

Обеспечение права "Изменение прав пользователей на объекты"

Право по умолчанию *Изменение прав пользователей на объекты* позволяет пользователям предоставлять право, даже если они сами его не имеют. Для соединений оно должно быть заменено правом *Безопасное изменение прав пользователей на объекты*. Если у администраторов нет права *Загрузить соединение локально*, они не должны иметь права предоставлять его другим пользователям.

В папке "Соединения" верхнего уровня выполните следующие действия:

1. Предоставьте группам "Администраторы" и "Universe Designer" право *Безопасное изменение прав пользователей на объекты*.

2. Предоставьте право *Безопасное изменение прав пользователей на объекты* пользователям, управляющим соединениями, как определено в предыдущем разделе. Они будут иметь право предоставлять право *Загрузить соединение локально*.
3. Запретите группам "Администраторы" и "Universe Designer" право *Изменение прав пользователей на объекты*.

8.13 Шифрование на платформе BI

Секретные данные

Функция шифрования 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 необходимые ресурсы шифрования (включая систему шифрования и библиотеки RSA) по умолчанию устанавливаются в каждом развертывании платформы BI.

Система платформы BI использует систему двухключевого шифрования.

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 для шифрования и дешифрования секретных данных используются симметричные ключи шифрования, известные как криптографические ключи. 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.

8.13.1 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	`<INSTALLDIR>/sap_bobj/enterprise_xi40/aix_rs6000_64/`
Solaris	`<INSTALLDIR>/sap_bobj/enterprise_xi40/solaris_sparcv9/`
Linux	`<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64/`

> **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.

8.13.1.1 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 *OK* , 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.

8.13.1.2 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 и нажмите клавишу *Enter*.

   > **Примечание**
   >
   > Убедитесь, что ключ содержит не менее шести символов и сочетает два из следующих типов символов: прописные буквы, строчные буквы, цифры или знаки пунктуации. Например, можно использовать один символ в нижнем регистре с цифрой, символ в верхнем регистре с символом пунктуации и т. д.

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.

8.13.2 Специалисты по шифрованию

Для управления криптографическими ключами в CMC 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.

8.13.2.1 Для добавления пользователя в группу специалистов по шифрованию

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

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

1. В области управления *Пользователи и группы* в CMC, 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 *OK*.

Добавленный участник группы специалистов по шифрованию получит доступ к области управления *Криптографические ключи* в CMC.

8.13.2.2 Просмотр криптографических ключей на консоли CMC

В приложении CMC 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 CMC перейдите по пути *Программы* > *SAP Business Intelligence* > *Платформа SAP BusinessObjects BI 4* > *SAP BusinessObjects BI platform Central Management Console*.
   Появится домашняя страница CMC.
2. Перейдите на вкладку *Криптографические ключи*.
   Отобразится область управления *Криптографические ключи*.
3. Дважды щелкните криптографический ключ, подробные сведения о котором нужно просмотреть.

Связанные сведения

Для просмотра объектов, связанных с криптографическим ключом [страница 180]

8.13.3 Управление криптографическими ключами с помощью CMC

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 CMS.

В области управления *Криптографические ключи* отображается список всех определенных в системе криптографических ключей. Основные данные по каждому ключу приводится 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

Связанные сведения

Статус криптографического ключа [страница 179]
Создание криптографических ключей [страница 180]

Удаление криптографических ключей из системы [страница 182]
Отзыв криптографических ключей [страница 181]
Для просмотра объектов, связанных с криптографическим ключом [страница 180]
Обозначение криптографических ключей как рассекреченных [страница 181]

8.13.3.1 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, помеченный как *Деактивированный*, невозможно удалить 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.
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

Статус	Описание
	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.

8.13.3.2 Для просмотра объектов, связанных с криптографическим ключом

1. Выберите ключ в области управления *Криптографические ключи* в CMC.
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.

8.13.3.3 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 CMC 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 *OK*, 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.

8.13.3.4 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 CMC.
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.

Связанные сведения

Отзыв криптографических ключей [страница 181]
Статус криптографического ключа [страница 179]
Для просмотра объектов, связанных с криптографическим ключом [страница 180]

8.13.3.5 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 *OK*.
   Начнется шифрование всех объектов, связанных с отозванных ключом, с помощью текущего активного ключа. Если ключ связан с большим количеством объектов данных, он будет помечен как *Неактивно – выполняется повторное шифрование*, пока шифрование не завершится.

Отозванный криптографический ключ можно безопасно удалить из системы, поскольку в системе не останется конфиденциальных объектов данных, для шифрования которых необходим этот ключ.

8.13.3.6 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 CMC.
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 CMC.

> ⓘ Примечание
>
> Удаленный из системы криптографический ключ восстановить невозможно.

Связанные сведения

Отзыв криптографических ключей [страница 181]
Статус криптографического ключа [страница 179]

8.14 Защита и конфиденциальность данных

Защита данных связана с различными законодательными требованиями и задачами обеспечения конфиденциальности. Помимо соблюдения соответствующих правил сохранения

конфиденциальности данных необходимо учитывать соблюдение отраслевых законодательств в разных странах. SAP обеспечивает различные возможности и функции для поддержки соблюдения законодательных требований, включая защиту данных. SAP не делает никаких заключений о том, являются ли эти возможности и функции лучшим методом поддержки конкретных требований компании, отрасли, региона или страны. Более того, в этих сведениях отсутствуют рекомендации относительно дополнительных функций, которые могут потребоваться в конкретной ИТ-среде. Решения, связанные с защитой данных, должны приниматься на индивидуальной основе с учетом определенного системного ландшафта и применимых законодательных требований.

> ⓘ Примечание
>
> В большинстве случаев функция продукта не сможет обеспечить соблюдение применимых законов о защите и конфиденциальности данных. Программное обеспечение SAP поддерживает выполнение требований по защите данных благодаря предоставлению возможностей обеспечения безопасности и определенных функций, релевантных для защиты данных, таких как упрощенные блокировка и удаление личных данных. SAP не дает правовых рекомендаций ни в какой форме. Определения и другие термины, используемые в этом документе, не взяты из какого-либо определенного источника нормативных данных.

8.14.1 Глоссарий

Термин	Определение
Личные данные	Любая информация, касающаяся идентифицированного или доступного для идентификации физического лица ("субъекта данных"). Доступным для идентификации физическим лицом является лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на идентификатор, такой как имя, идентификационный номер, данные расположения, онлайн-идентификатор, или на один или несколько факторов, специфичных для физической, физиологической, генетической, ментальной, экономической, культурной или социальной идентификации этого физического лица.
Цель	Установленная законом, основанная на договоре или в другой форме правомерная причина обработки **личных данных**. Предполагается, что любая цель имеет конечный результат, который обычно уже определен при постановке цели.
Блокировка	Способ ограничения доступа к данным, для которых достигнута основная **бизнес-цель**.
Удаление	Необратимое уничтожение **личных данных**.

Термин	Определение
Период хранения	Период времени между моментом достижения цели (EoP) для набора данных и моментом удаления этого набора данных в соответствии с применимыми законами. Является комбинацией периода удержания и периода блокировки.
Достижение цели (EoP)	Способ идентификации момента времени для набора данных, когда обработка **личных данных** больше не требуется для основной **бизнес-цели**. После достижения **EoP** данные **блокируются** и могут быть доступны только пользователям с особыми полномочиями (например, аудиторам).
Уязвимые личные данные	Категория личных данных, обычно включающая сведения следующего типа: • Особые категории личных данных, такие как данные, раскрывающие расовое или этническое происхождение, политические убеждения, религиозные верования или философские взгляды либо участие в профсоюзах и результаты обработки генетических и биометрических данных, данных, касающихся здоровья и сексуальной жизни или ориентации • Личные данные, обусловленные профессиональной тайной • Личные данные, связанные с уголовными преступлениями или административными правонарушениями • Личные данные, касающиеся страхования и банковских счетов и кредитных карт
Период удержания	Период времени с момента достижения цели (EoP) для набора данных, в течение которого данные остаются в базе данных и могут использоваться в случае последующих процессов, связанных с исходной целью. По окончании самого длинного периода удержания, который был настроен, данные блокируются или удаляются. Период удержания является частью общего периода удержания.

Термин	Определение
Проверка использования (WUC)	Процесс, предназначенный для обеспечения целостности данных в случае возможной блокировки данных делового партнера. Проверка использования (WUC) приложения определяет, существуют ли в базе данных какие-либо зависимые данные для конкретного делового партнера. Если зависимые данные существуют, это означает, что эти данные еще требуются для бизнес-операций. Поэтому блокировка деловых партнеров, упомянутых в этих данных, запрещается.
Согласие	Действие субъекта данных, подтверждающее разрешение на использование его личных данных для указанной цели. Функция согласия позволяет хранение записи согласия в отношении определенной цели и показывает, дал ли субъект данных согласие, отклонил ли предложение о согласии или отозвал свое согласие.

8.14.2 Согласие пользователя

Прежде чем собирать персональные данные пользователя, приложения SAP запрашивают его согласие. Платформа SAP BusinessObjects Business Intelligence предоставляет функцию, которая позволяет субъектам данных давать согласие на сбор и обработку личных данных. SAP предполагает, что пользователь, например клиент SAP, собирающий данные, получил согласие на сбор или передачу данных в решение от своего субъекта данных (физического лица, например клиента, контакта или учетной записи).

> ⓘ Примечание
>
> *Сообщение о согласии пользователя*
>
> Этот продукт содержит открытые или свободно настраиваемые поля ввода, не предназначенные для хранения личных данных без дополнительных технических и организационных мер по обеспечению безопасности и конфиденциальности данных

8.14.3 Отчет о сведениях

Каждый человек имеет право получить подтверждение, касающееся того, обрабатываются ли его персональные данные. В платформе SAP BusinessObjects Business Intelligence можно просмотреть все сохраненные сведения об определенном субъекте данных.

Дополнительные сведения о получении пользователем доступа к сохраненной информации о субъекте данных см. в разделе 'Доступ к личной информации' в *Руководстве пользователя стартовой панели Business Intelligence в стиле Fiori* на SAP Help Portal.

> **Примечание**
>
> Платформа SAP BusinessObjects Business Intelligence не обеспечивает защиту документов, сохраненных локально. Защиту необходимо предоставить с помощью соответствующих возможностей управления устройством (например, контроля доступа, шифрования и т. д.).

8.14.4 Запись доступов чтения в журнал

Запись доступов чтения в журнал (RAL) используется для контроля и записи доступа для чтения к уязвимым данным. Данные можно определить как уязвимые согласно законодательству, а также внешней или внутренней политике компании. Для приложения, в котором используется запись доступов чтения в журнал, могут представлять интерес следующие общие вопросы:

- Кто получал доступ к данным указанного бизнес-объекта, например банковского счета?
- Кто получал доступ к личным данным, например, делового партнера?
- Какой работник получал доступ к личным сведениям, например, о вероисповедании?
- К каким учетным записям или деловым партнерам получали доступ пользователи и кто из них?

На эти вопросы можно получить ответы, используя сведения о том, кто получал доступ к конкретным данным в указанный интервал времени. Технически это означает, что всем удаленным информационным структурам интерфейсов API и пользователя (которые получают доступ к данным) должна быть разрешена запись в журнал.

Плаформа SAP BusinessObjects BI не предназначена для идентификации, обработки или хранения конфиденциальных персональных данных. Поэтому, чтобы получить доступ для чтения, выполнять вход в систему на платформе BI не требуется.

8.14.5 Удаление личных данных

- Упрощенные блокировка и удаление. Помимо выполнения соответствующих правил сохранения конфиденциальности данных необходимо учитывать соблюдение отраслевых законодательств в разных странах. Обычным возможным сценарием в некоторых странах является удаление личных данных по достижении указанной, явной и законной цели обработки личных данных, но только если в законодательстве не определены другие периоды хранения, например периоды хранения финансовых документов. Установленные законом требования в некоторых сценариях или странах также часто предписывают блокировать данные в случаях, когда указанные, явные и законные цели обработки этих данных достигнуты, но эти данные должны сохраняться в базе данных по причине определения в законодательстве других периодов хранения. В некоторых сценариях личные данные также включают ссылочные данные. Поэтому задача удаления и блокировки заключается в том, чтобы сначала обработать ссылочные данные и в конце остальные данные, например данные делового партнера.
- Удаление личных данных. Обработка личных данных подчиняется применимым законам, связанным с удалением подобных данных по достижении цели (EoP). Если законная цель, которая требует использования личных данных, больше не существует, они должны быть удалены. При удалении данных в наборе данных также должны быть удалены все ссылочные объекты, связанные с набором

данных. Также помимо общих законов о защите персональных данных необходимо учитывать отраслевые законодательства в различных странах. После окончания самого длинного периода хранения данные должны быть удалены.

Удаление данных в платформе SAP BusinessObjects BI

Платформа SAP BusinessObjects BI и ее клиенты не предназначены для идентификации или классификации данных (полученных из источников данных для анализа и отчетности) в качестве персональных данных. Для таких данных управлять требованиями к извлечению и прозрачности сведений должна система-владелец данных. Удаление данных является стандартной функцией системы-владельца данных. Дополнительно платформа SAP BusinessObjects BI и ее клиенты предоставляют функции (соединение с источниками данных в реальном времени) для обеспечения синхронизации с системой-владельцем данных.

Однако данные пользователей, ведение которых осуществляется в системе, могут быть доступны самим пользователям или пользователям с полномочиями на управление этими данными. Пользователи, импортированные из поставщиков удостоверений (например, Windows AD, LDAP и т. д.), сохраняют синхронизацию с ними, и их ведение должно выполняться непосредственно в поставщике удостоверений.

Корпоративные пользователей, созданные на платформе SAP BusinessObjects BI, могут быть удалены или отключены пользователями, имеющими полномочия на управление этими данными. В этом случае пользователи могут быть сначала просто деактивированы в системе, а по истечении периода хранения удалены из системы вручную пользователями, имеющими полномочия на управление этими данными.

При удалении учетной записи пользователя удаляются также папка "Избранное", личные категории и папка "Входящие" этого пользователя. Права собственности на артефакты в общей папке перейдут от удаленных пользователей к администратору. Обратите внимание, что, если пользователь деактивирован, это должны сделать вручную пользователи, имеющие полномочия на управление этими данными.

Идентификатор объекта пользователя хранится как в базе данных аудита, так и в базе данных комментариев. При этом он не удаляется при удалении пользователей, поскольку идентификатор пользователя в журналах аудита необходим для соблюдения законодательных требований и требований безопасности. Комментарии пользователя важны с точки зрения бизнеса и поэтому должны быть сохранены в истории диалогов. Предполагается, что комментарии не содержат личных данных, поскольку пользователя заранее предупреждают не выполнять ведение личных данных в открытых полях.

Кроме того, записи базы данных аудита и базы данных комментариев могут быть удалены вручную авторизованными пользователями.

Для получения дополнительных сведений о деактивации пользователя см. Для изменения учетной записи пользователя [страница 108].

Для получения дополнительных сведений об удалении записей комментариев, сделанных пользователем, см. Управление настройками приложения BI Commentary [страница 751]

8.14.6 Журнал изменений

Журнал изменений в платформе SAP BusinessObjects Business Intelligence обрабатывает личные данные деловых партнеров, задействованных в запросах на изменение и соответствующих операциях. Если произошли изменения, касающиеся делового партнера, система записывает в журнал следующую информацию, связанную с личными данными, согласно запросу на изменение и операции:

- Пользователь, изменивший данные
- Дата и время изменения
- Тип изменения (обновление, вставка, удаление, документация к отдельному полю)
- Идентификационные ключи и их значения для записей данных
- Старое и новое значение атрибута, который был изменен
- Имя заголовка измененного атрибута

Поля, подлежащие записи в журнал, можно определить.

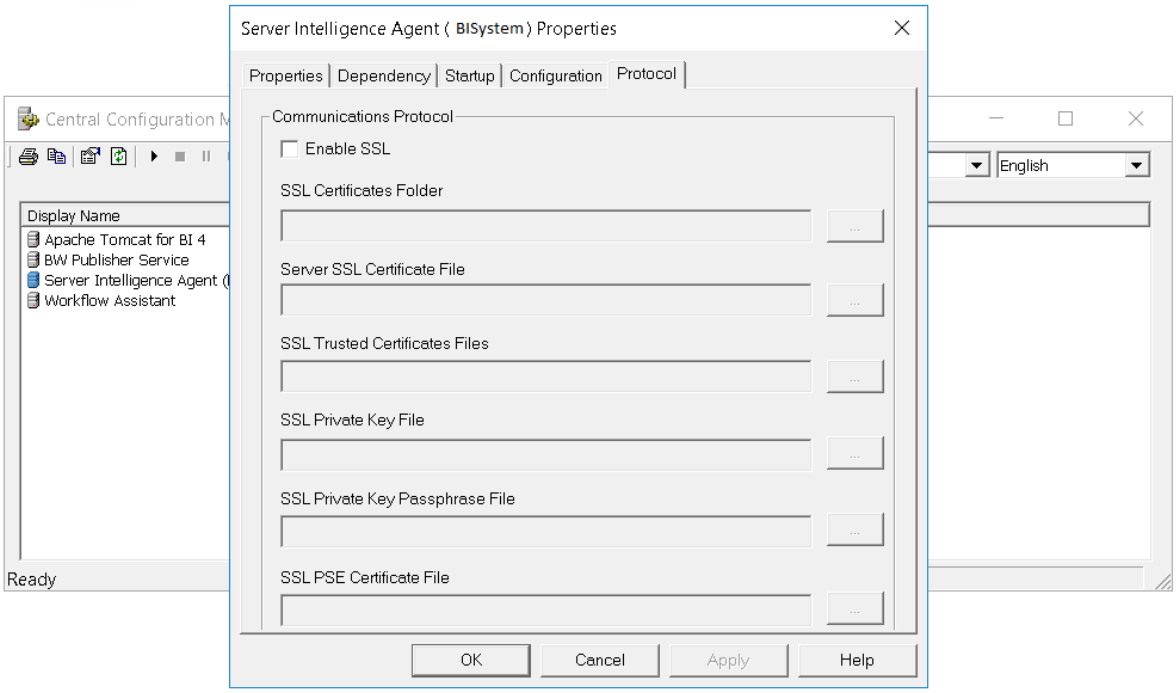
Для получения подробной информации о журналах обновления учетной записи пользователя см. ид типа события: 1007 в Audit events and details [страница 942].

8.15 Настройка внутренних серверов для SSL

Можно использовать протокол SSL для сетевого обмена данными между клиентами и серверами BI в 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.
- Также можно настроить SSL для сертификатов, которые подписываются самостоятельно или управляются через центр сертификации.



> ⓘ Примечание
>
> Если используются "толстые" клиенты, такие как Crystal Reports, их также следует настроить для SSL в случае подключения к CMS. В противном случае при попытке подключения к серверу CMS, настроенному для использования SSL, с "толстого" клиента, который не был настроен соответствующим образом, будут возникать ошибки.

8.15.1 Создание файла конфигурации по умолчанию

Во избежание повторного добавления значений во время создания сертификата или запроса на подпись сертификата можно создать файл конфигурации по умолчанию.

> ⓘ Примечание
>
> При создании файла конфигурации по умолчанию необходимо следовать указанным ниже правилам.
>
> - Следует добавить значения с левой стороны точно так, как указано ниже.
> - Значения с левой стороны необходимо добавлять с учетом регистра.
> - Между значением и знаком "равно" (=) должен быть только один пробел. Например, между значением *CA_Common_Name* и знаком "равно" имеется только один пробел.
> - Необходимо убедиться в отсутствии пробелов после значений с правой стороны.

Для создания файла конфигурации по умолчанию с именем **Name.cnf** выполните следующие шаги:

1. Откройте новый документ в текстовом редакторе.

2. Добавьте значения, как указано ниже:

```
CA_Common_Name = rootnm
CA_Country = DE
CA_State = BW
CA_Locality = RRR
CA_Email = example@example.com
CA_Unit = root_u
CA_Expiration[YYMMDD] = yymmdd
User_Expiration[YYMMDD] = yymmdd
User_Country = IN
User_State = KA
User_Locality = BLR
User_Organization = SSS
User_Unit = Unit
User_Common_Name = UserName
```

3. Сохраните файл с именем **Name.cnf** в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64` в среде Windows и в каталоге `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` в среде Unix.

8.15.2 Создание файлов ключей и сертификатов

Чтобы установить протокол SSL для обмена данными между серверами, используйте инструмент командной строки GENPSE для создания файла ключа и файла сертификата для каждой машины в развертывании.

> ⓘ Примечание
>
> Необходимо повторно создать сертификаты для всех машин развертывания, включая машины, на которых выполняются компоненты толстых клиентов, такие как Crystal Reports. Для конфигурации таких клиентских компьютеров используйте инструмент командной строки `sslconfig`.

> ⓘ Примечание
>
> Для максимальной безопасности все секретные ключи должны быть защищены и не должны передаваться по незащищенным каналам.

8.15.2.1 Создание файлов ключа и сертификата для компьютера

В этом разделе описано создание самостоятельно подписанного ключа и сертификатов, которые необходимы для обеспечения безопасности коммуникаций между серверами или сервером и клиентом. Для создания сертификатов можно использовать средство GENPSE, средство командной строки для выполнения множества задач, связанных с инфраструктурой открытого ключа. Средство GENPSE используется для создания сертификатов X.509, запросов подписи сертификатов и PSE-файлов, используемых в потоке операций CORBA SSL. Оно основано на библиотеке шифрования SAP **CommonCryptoLib** и поддерживает механизм SHA-2.

Для создания необходимых сертификатов для безопасной коммуникации выполните следующие шаги:

> **Примечание**
>
> Можно создать файл конфигурации по умолчанию **Name.cnf** со значениями по умолчанию для сведений, запрашиваемых при создании сертификатов. Файл конфигурации по умолчанию делает ненужным повторное добавление сведений для каждого сертификата. Для получения дополнительных сведений см. Создание файла конфигурации по умолчанию [страница 189].

1. Перейдите в каталог `<INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\win64_x64` в ОС Windows и `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` в ОС Unix.
2. Выполните следующую команду:
   - В ОС Windows: `GenPSE.exe selfsigned <Name.pse> <Name.der> <root Cert.der> <Name.key> <private key password.txt> <path to Name.cnf>`
   - В ОС Unix: `GenPSE.sh selfsigned <Name.pse> <Name.der> <root Cert.der> <Name.key> <private key password.txt> <path to Name.cnf>`

   Для получения представления о команде см. следующую таблицу.

Команда	Функция
GenPSE.exe или GenPSE.sh	Запуск средства криптографии
selfsigned	Для создания самостоятельно подписанных сертификатов
<Name.pse>	Имя файла сервера PSE
<Name.der>	Имя файла сертификата сервера
<root Cert.der>	Имя сертификата центра сертификации
<Name.key>	Имя файла личного ключа сервера
<private key password.txt>	Фраза-пароль для личного ключа сервера
< path to Name.cnf >	Путь к файлу конфигурации по умолчанию

3. Для создания корневого центра сертификации, сервера и сертификата клиента введите следующие сведения.
   - *Название страны*
   - *Название региона*
   - *Название района*
   - *Имя организации*
   - *Имя организационной единицы*
   - *Введите свое имя*
   - *Стандартное имя*
   - *Адрес электронной почты*
   - *Введите дату окончания срока действия в формате ГГММДД*

4. PSE-файл и сертификаты создаются и сохраняются в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64` в ОС Windows и `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` в ОС Unix.

> → Совет
>
> При создании сертификата пользователя дополнительный параметр *Тип сертификата пользователя* позволяет средству идентифицировать и создать сертификат для аутентификации сервера или клиента. В данный момент любой вариант, выбранный для этого параметра, не влияет на настройку CORBA SSL.

> ⓘ Примечание
>
> - PSE сервера и файл сертификата центра сертификации должны иметь разные имена.
> - Поддерживается дата окончания срока действия до 2049 г.

8.15.3 Настройка SSL, когда сертификатом управляет центр сертификации

Вам следует создать запрос подписи сертификата для стороннего центра сертификации, чтобы подписать сертификаты. Средство GenPSE создает запрос подписи сертификата, выполнив простые команды и предоставив необходимые сведения при появлении соответствующих запросов.

Для создания запроса подписи сертификата выполните следующие шаги:

> ⓘ Примечание
>
> Можно создать файл конфигурации по умолчанию `Name.cnf` со значениями по умолчанию для сведений, запрашиваемых при создании сертификатов. Файл конфигурации по умолчанию делает ненужным повторное добавление сведений для каждого сертификата. Для получения дополнительных сведений см. Создание файла конфигурации по умолчанию [страница 189].

1. Перейдите в каталог `<INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\win64_x64` в ОС Windows и `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` в ОС Unix.
2. Выполните следующую команду:
   - В ОС Windows: `GenPSE.exe gencsr <csrname.p10> <Name.key> <private key password.txt> <path to Name.cnf>`
   - В ОС Unix: `GenPSE.sh gencsr <csrname.p10> <Name.key> <private key password.txt> <path to Name.cnf>`

Команда	Функция
GenPSE.exe или GenPSE.sh	Запуск средства криптографии
gencsr	Для создания запроса подписи сертификата

Команда	Функция
<csrname.p10>	Имя файла запроса подписи сертификата
<Name.key>	Имя файла личного ключа сервера
<private key password.txt>	Фраза-пароль для личного ключа сервера
<path to Name.cnf>	Путь к файлу конфигурации по умолчанию

3. Введите следующие сведения:
   - *Введите фразу-пароль личного ключа для настройки*
   - *Введите еще раз фразу-пароль личного ключа для подтверждения*
   - *Название страны*
   - *Название региона*
   - *Название района*
   - *Имя организационной единицы*
   - *Стандартное имя*
   - *Адрес электронной почты*
4. Файл CSR в формате p10, личный ключ сервера и файл фразы-пароля создаются и сохраняются в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64` в ОС Windows и `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` в ОС Unix. Созданный файл CSR отправляется в центр сертификации для создания подписанного сертификата.

8.15.3.1 Создание PSE-файла

Если управление вашими сертификатами осуществляется внешним центром сертификации, необходимо создать PSE-файл. Для создания PSE-файла выполните следующие шаги:

1. Откройте каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
2. Запустите консоль командной строки и выполните команду `set SECUDIR=.` для Windows и `export SECUDIR=.` для Linux.
3. Выполните команду `sapgenpse import_p8 -p <file_path_PSE> -c <file_path_server_certificate> -r <file_path_CA_certificate> -z <file_path_passphrase_text_file> <file_path_server_key>`.

   Для получения более глубокого представления о команде см. следующую таблицу.

Команда	Описание
sapgenpse	Запуск средства криптографии

Команда	Описание
import_p8	Создание нового PSE-файла из личного ключа в формате PKCS#8 (при необходимости защищенного шифрованием на основе пароля PKCS#5) вместе со всеми необходимыми сертификатами X.509
-p <file_path_PSE>	Путь к созданному новому PSE-файлу
-c <file_path_server_certificate>	Путь к файлу сертификата сервера
-r <file_path_CA_certificate>	Путь к файлу сертификата CA
-z <file_path_passphrase_text_file>	Путь к текстовому файлу фразы-пароля
<file_path_server_key>	Путь к файлу личного ключа сервера

Пример

sapgenpse import_p8 -p C:\SSL\cert.pse -c C:\SSL\servercert.der -r C:\SSL\cacert.der -z C:\SSL\passphrase.txt C:\SSL\server.key

4. Укажите пустой пароль, нажав клавишу Enter при запросе пароля.
5. Добавьте в созданный PSE-файл учетные данные пользователя.

Совет

Если SIA работает с учетной записью LocalSystem, необходимо выполнить команду `sapgenpse seclogin -p C:\SSL\cert.pse -O SYSTEM`, чтобы добавить учетные данные пользователя в PSE-файл.

Примечание

Для PSE-файла можно выбрать любое имя по своему усмотрению.

8.15.4 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.

Активация FIPS на платформе на базе Unix для настройки SSL

FIPS активируется по умолчанию для полной установки 4.2 SP04 или выше, однако в следующих сценариях стандарт необходимо активировать вручную:

- Обновление исправлений с 4.1 SPXX до 4.2 SP04
- Обновление исправлений с 4.1 SPXX до 4.2 SP02 или с SP03 и выше до 4.2 SP04

> **Примечание**
>
> В Windows CORBA SSL работает, даже если FIPS не активирован, в то время как на платформах на базе Unix необходимо убедиться в том, что FIPS активирован для серверов, прежде чем настраивать CORBA SSL.

Процедура активации FIPS:

- Перейдите в каталог `<INSTALLDIR>/sap_bobj.`
- Запустите `./stopservers`
- Откройте файл ccm.config.
- Добавьте текст "-FIPS" из списка свойств узла SIA.
- Запустите `./startservers`

8.15.4.1 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, `d:\ssl`
Файл сертификата SSL сервера	Имя файла для хранения сертификата SSL сервера. По умолчанию используется имя `servercert.der`
Файл надежных сертификатов SSL	Имя файла с надежным сертификатом SSL. По умолчанию используется имя `cacert.der`
Файл личного ключа SSL	Имя файла личного ключа SSL, используемого для доступа к сертификату. По умолчанию используется имя `server.key`
Файл фразы-пароля личного ключа SSL	Имя текстового файла, содержащего фразу-пароль для доступа к личному ключу. По умолчанию используется имя `passphrase.txt`

Поле	Описание
Файл сертификатов PSE SSL	Имя PSE-файла, который содержит сведения о доверенных сертификатах и сертификатах сервера.

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

8.15.4.2 Настройка протокола SSL в ОС UNIX

Для настройки протокола SSL для SIA нужно использовать скрипт `serverconfig.sh`. Этот сценарий запускает текстовую программу, которая позволяет вам просматривать информацию сервера, добавлять и удалять серверы из вашей установки. Скрипт `serverconfig.sh` устанавливается в каталог установки `sap_bobj`.

1. Используйте скрипт `ccm.sh` для остановки SIA и всех серверов SAP BusinessObjects.
2. Выполните скрипт `serverconfig.sh`.
3. Выберите пункт *3 – Изменить 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 `ccm.sh` и дождитесь, пока запустятся серверы.

8.15.4.3 Настройка протокола SSL для сервера веб-приложений

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

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

   В следующей таблице приводятся описания, соответствующие этим примерам:

Пример	Описание
`<DcertDir>=d:\ssl`	Каталог для хранения всех сертификатов и ключей.

Пример	Описание
`<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 ключевой фразы (passphrase) секретного ключа.
`<Dpsecert>=cert.pse`	PSE – это репозиторий, который содержит ключи и сертификаты, используемые для защиты коммуникации. Для получения дополнительных сведений см. SAP-ноту 3026364

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

8.15.4.4 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 личного ключа SSL	`server.key`
Файл, содержащий контрольную фразу для доступа к личному ключу SSL	`passphrase.txt`
Имя файла сертификатов PSE SSL	cert.pse

После создания перечисленных выше ресурсов настройте приложения "толстых" клиентов, такие как CCM, выполнив следующие указания.

1. Убедитесь, что в приложении "толстого" клиента в данный момент не выполняются операции.

> **Примечание**
>
> Убедитесь, что задан каталог для компьютера, на котором выполняется сервер.

2. Запустите инструмент `sslconfig.exe` из командной строки. В зависимости от конфигурации используйте инструмент из win32_x86 для 32-разрядных клиентов и из win64_x64 для 64-разрядных клиентов.

   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 -psecert cert.pse -protocol ssl
```

4. Повторно запустите приложение толстого клиента.

Связанные сведения

Создание файлов ключа и сертификата для компьютера [страница 190]

8.15.4.4.1 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 каталоге `<КАТАЛОГ_УСТАНОВКИ>\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.

8.15.4.4.2 Настройка SSL для средства преобразования отчетов

Не рекомендуется использовать средство RCT в версии BI 4.3, так как оно устарело. Для получения дополнительных сведений см. 2801797

8.16 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 межу серверами платформы BI, толстыми клиентами и сервером веб-приложений, на котором размещен пакет SAP BusinessObjects Enterprise SDK, перед настройкой системы для работы с брандмауэрами.

Связанные сведения

Настройка платформы BI для брандмауэров [страница 213]
Примеры типовых сценариев развертывания брандмауэров [страница 218]

8.16.1 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.

8.16.1.1 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.

8.16.1.2 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.

8.16.1.3 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™).

8.16.1.4 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.

Связанные сведения

Взаимодействие между компонентами платформы BI [страница 202]

8.16.1.5 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.

8.16.1.6 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_номер_порта>-<наибольший_номер_порта>` и `-requestPort <номер_порта>` 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.

Связанные сведения

Обзор командных строк [страница 1144]

8.16.2 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.

8.16.2.1 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, SFTP-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.

Связанные сведения

Платформа BI: требования к портам [страница 203]

8.16.2.2 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.

8.16.2.2.1 Требования к портам для приложений платформы BI

В этой таблице перечислены серверы и номера портов, используемых приложениями платформы BI.

Продукт	Клиентское приложение	Связанный сервер	Необходимые порты для сервера
Crystal Reports	Конструктор SAP Crystal Reports 2020	CMS	Порт сервера имен CMS (по умолчанию 6400)
		Сервер репозитория входных файлов	Порт запросов CMS
		Сервер репозитория выходных файлов	Порт запросов сервера репозитория входных файлов
		Crystal Reports 2020 Report Application Server (RAS)	Порт запросов сервера репозитория выходных файлов
		Сервер обработки Crystal Reports 2020	Порт запросов сервера Crystal Reports 2020 Report Application Server
		Кэш-сервер Crystal Reports	Порт запросов сервера обработки Crystal Reports 2020
			Порт запросов кэш-сервера Crystal Reports

Продукт	Клиентское приложение	Связанный сервер	Необходимые порты для сервера
Crystal Reports	Конструктор SAP Crystal Reports для Enterprise	CMS Сервер репозитория входных файлов Сервер репозитория выходных файлов Сервер обработки Crystal Reports Кэш-сервер Crystal Reports	Порт сервера имен CMS (по умолчанию 6400) Порт запросов CMS Порт запросов сервера репозитория входных файлов Порт запросов сервера репозитория выходных файлов Порт запросов сервера обработки Crystal Reports Порт запросов кэш-сервера Crystal Reports
Live Office	Клиент Live Office	Приложение поставщика веб-служб (`dswsbobje.war`), в котором размещается веб-служба Live Office	Порт HTTP (по умолчанию 80)
SAP Analysis для Microsoft Office	SAP Analysis для Microsoft Office	CMS Адаптивный сервер обработки, на котором размещена служба Multi-Dimensional analysis service Сервер репозитория входных файлов Сервер репозитория выходных файлов	Порт сервера имен CMS (по умолчанию 6400) Порт запросов CMS Порт запросов настраиваемого сервера обработки Порт запросов сервера репозитория входных файлов Порт запросов сервера репозитория выходных файлов
Платформа BI	SAP BusinessObjects Web Intelligence Rich Client	CMS Сервер репозитория входных файлов	Порт сервера имен CMS (по умолчанию 6400) Порт запросов CMS Порт запросов сервера репозитория входных файлов
Платформа BI	Средство создания юниверсов	CMS Сервер репозитория входных файлов Сервер соединений	Порт сервера имен CMS (по умолчанию 6400) Порт запросов CMS Порт запросов сервера репозитория входных файлов Порт сервера соединений

Продукт	Клиентское приложение	Связанный сервер	Необходимые порты для сервера
Платформа BI	Диспетчер Business View	CMS Сервер репозитория входных файлов	Порт сервера имен CMS (по умолчанию 6400) Порт запросов CMS Порт запросов сервера репозитория входных файлов
Платформа BI	Central Configuration Manager (CCM)	CMS Server Intelligence Agent (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)
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	Repository Diagnostic Tool	CMS Сервер репозитория входных файлов Сервер репозитория выходных файлов	Порт сервера имен CMS (по умолчанию 6400) Порт запросов CMS Порт запросов сервера репозитория входных файлов Порт запросов сервера репозитория выходных файлов

Продукт	Клиентское приложение	Связанный сервер	Необходимые порты для сервера
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 2020 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 необходимого сервера. Например, порт запросов сервера обработки Crystal Reports 2020.
Платформа BI	Поставщик веб-служб (`dswsbobje.war`)	Все серверы платформы BI, необходимые для доступа продуктов к веб-службам. 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.	Порт сервера имен CMS (по умолчанию 6400) Порт запросов CMS Порт запросов для каждого необходимого сервера. Например, порты запросов кэш-сервера и сервера обработки Dashboards.
Платформа BI	SAP BusinessObjects Analysis, выпуск для OLAP	CMS Адаптивный сервер обработки, на котором размещена служба Multi-Dimensional analysis service Сервер репозитория входных файлов Сервер репозитория выходных файлов	Порт сервера имен CMS (по умолчанию 6400) Порт запросов CMS Порт запросов настраиваемого сервера обработки Порт запросов сервера репозитория входных файлов Порт запросов сервера репозитория выходных файлов

8.16.2.2.2 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 базы данных	Эти серверы получают данные из базы данных отчетов.
сервер веб-приложений	Все веб-службы SAP BusinessObjects и все веб-приложения, включая стартовую панель BI и CMC	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*.

Стороннее приложение	Компонент SAP Business Objects, использующий сторонний продукт	Требование к порту стороннего приложения	Описание
SFTP-сервер	Каждый сервер заданий	SMTP (порт 22)	На сервере заданий порты SFTP используются для разрешения *отправки на SFTP*. **Примечание** Отпечаток ключа хоста используется для защиты соединения SSH и предотвращения атак через посредника. Это обязательно для определенных параметров, требуемых при настройке SFTP. Процесс создания отпечатка ключа хоста отличается в зависимости от используемого сервера SFTP. Администратор/пользователь должен настроить отпечаток SHA-2 для включения SFTP. Для создания отпечатка SHA-2 администратор/пользователь может обратиться к документации по продукту, относящейся к внедрению сервера SSH/SFTP. **Пример** Основные SFTP-клиенты, такие как PuTTY и WinSCP, используют отпечатки MD5 для однозначной идентификации SFTP-серверов. Отпечатки MD5 не работают. Инструкции о том, как получить отпечатки SHA-2, приводятся в документации по SFTP-серверу. Пример методики при наличии файла открытого ключа и инструментов OpenSSH Unix приведен ниже. Дан файл открытого ключа с именем RSAKey.pub, содержащий: `ssh-rsa <base64 encoded key>`. Выполните следующую команду: `cut -d`

Стороннее приложение	Компонент SAP Business Objects, использующий сторонний продукт	Требование к порту стороннего приложения	Описание
			`' ' -f 2 < RSAKey.pub | base64 -d | openssl dgst -c -sha256`. Будет выдан результат вида: `(stdin)= 00:93:1e:cc:bd:cc:43:05:41:89:5f:5c:c7:91:1d:11:a0:1e:58:e8`, где 20-значная хеш-сумма зависит от значения зашифрованного открытого ключа base64. Используйте 20-значное значение `00:93:1e:cc:bd:cc:43:05:41:89:5f:5c:c7:91:1d:11:a0:1e:58:e8` для отпечатка ключа хоста. → Рекомендация Наилучший рекомендуемый способ состоит в том, чтобы разрешить конфигурацию SFTP на странице серверов CMC в BOE и использовать значения по умолчанию при отправке на SFTP-серверы.

Стороннее приложение	Компонент SAP Business Objects, использующий сторонний продукт	Требование к порту стороннего приложения	Описание
Сервер электронной почты	Каждый сервер заданий	SMTP (порт на каждый SMTP-сервер)	Можно использовать один и тот же порт для SMTPS и SMTP. Однако для SMTPS необходимо убедиться, что на сервере включен SSL/TLS, с помощью команды STARTTLS smtp. На сервере заданий порт SMTP используется для разрешения *отправки электронной почты*. **Настройка адаптивного сервера заданий:** Чтобы настроить адаптивный сервер заданий, выполните следующие действия: 1. Запустите Central Management Console (CMC). 2. Выберите пункт *Серверы* в раскрывающемся меню. 3. Щелкните правой кнопкой мыши элемент **AdaptiveJobServer** и выберите *Адресат* 4. Выберите пункт *Электронная почта* в раскрывающемся меню. Если вы еще не добавили сервер электронной почты в качестве целевого местоположения, необходимо сделать это, прежде чем продолжать. 5. Введите необходимые данные. 6. При необходимости выберите параметр *Включить SSL*. 7. Нажмите *Сохранить и закрыть*. **Настройка SMTP по протоколу SSL:** Для настройки SMTP по протоколу SSL необходимо, чтобы сертификат сервера SMTP присутствовал в системах сервера и BOE.

Стороннее приложение	Компонент SAP Business Objects, использующий сторонний продукт	Требование к порту стороннего приложения	Описание
			Для настройки SMTP по протоколу SSL выполните описанные ниже шаги. 1. Создание сертификата сервера с сервера SMTP. 2. В окне *Место назначения* установите флажок *Включить SSL*. 3. Введите абсолютный путь к сертификату SMTP. **Примечание** Введите абсолютный путь к сертификату SMTP. Если не указывается абсолютный путь к сертификату SMTP, можно ввести заполнитель (%SI_DEFAULT_CERT_LOC%) и система прочитает это как местоположение по умолчанию, то есть `\SAP BusinessObjects Enterprise XI 4.0\win64_x64\` или `\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`, и выполнит поиск сертификата (имя сертификата по умолчанию – .crt). 4. Выберите необходимое значение для *безопасности соединения*. **Примечание** По умолчанию выбран параметр *StartTLS*. Можно

Стороннее приложение	Компонент SAP Business Objects, использующий сторонний продукт	Требование к порту стороннего приложения	Описание
			выбрать параметр *SSL/TLS*. 5. Выберите нужную версию TLS. **Примечание** По умолчанию выбрана TLS v1.0. Можно выбрать TLS v1.1 или TLS v1.2. 6. Нажмите кнопку *Сохранить и закрыть*. Теперь SMTP по каналу SSL настроен. **Примечание** При обновлении исправления BI 4.1 SP6 до любой более поздней версии параметр StartTLS и TLS 1.0 выбираются по умолчанию. **Примечание** • Когда пользователь устанавливает флажок *Включить SSL*, открывается защищенный канал. Это позволяет осуществлять защищенный обмен данными SMTP по каналу SSL. • Для одного адаптивного сервера заданий можно настроить только один сертификат SMTP. Для одного сервера заданий настройка нескольких сертификатов невозможна. • Параметр *Включить SSL* доступен только на адаптивном сервере заданий, а не на уровне документа.

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 rexec (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 определяется пользователем 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.

8.17 Настройка платформы BI для брандмауэров

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

8.17.1 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_номер_порта>-<наибольший_номер_порта>` и `<номер_порта>` 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.

Связанные сведения

Взаимодействие между компонентами платформы BI [страница 202]
Настройка номеров портов [страница 486]
Обзор командных строк [страница 1144]
Определение правил брандмауэра [страница 214]
Настройка файла хостов для брандмауэров с NAT [страница 215]

8.17.1.1 Определение правил брандмауэра

Необходимо настроить брандмауэр, чтобы разрешить передачу требуемых данных между компонентами платформы BI. Обратитесь к документации по брандмауэру для получения сведений об определении этих правил.

Укажите по одному правилу входящего доступа для каждого пути соединения через брандмауэр. Возможно, правила доступа следует определять не для каждого из серверов платформы BI за брандмауэром.

Используйте номер порта, указанный в поле сервера *Порт запросов* на странице свойств сервера CMC. 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 развертывание 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 CMC 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

Связанные сведения

Взаимодействие между компонентами платформы BI [страница 202]

8.17.1.2 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 доменных имен (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.

8.17.1.2.1 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`.

8.17.1.2.2 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 выполняется 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`.

8.17.2 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
```

8.17.2.1 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 удается*

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.

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 CMC. 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.

Связанные сведения

Настройка номеров портов [страница 486]

8.18 Примеры типовых сценариев развертывания брандмауэров

В этом разделе приводятся примеры типовых сценариев развертывания брандмауэров.

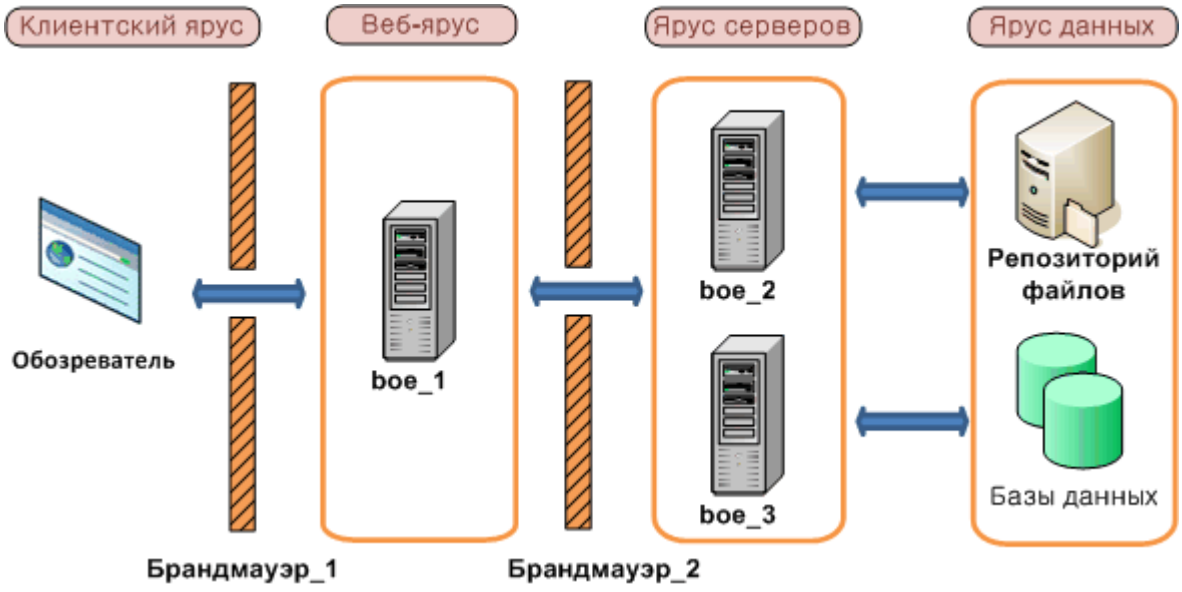
8.18.1 Пример: уровень приложений развернут в отдельной сети

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.

Уровень приложений развернут в отдельной сети



8.18.1.1 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	Номер порта
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.

   Конфигурация для Firewall_1

Порт	Целевой компьютер	Порт	Действие
Любой	boe_1	8080	Разрешить

   Конфигурация для Firewall_2

Исходный компьютер	Порт	Целевой компьютер	Порт	Действие
boe_1	Любой	boe_2	6400	Разрешить
boe_1	Любой	boe_2	6411	Разрешить
boe_1	Любой	boe_2	6415	Разрешить
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.

Связанные сведения

Настройка номеров портов [страница 486]
Основные сведения об обмене данными между компонентами платформы BI [страница 199]

8.18.2 Пример: толстый клиент и уровень БД отделены брандмауэром от платформы BI

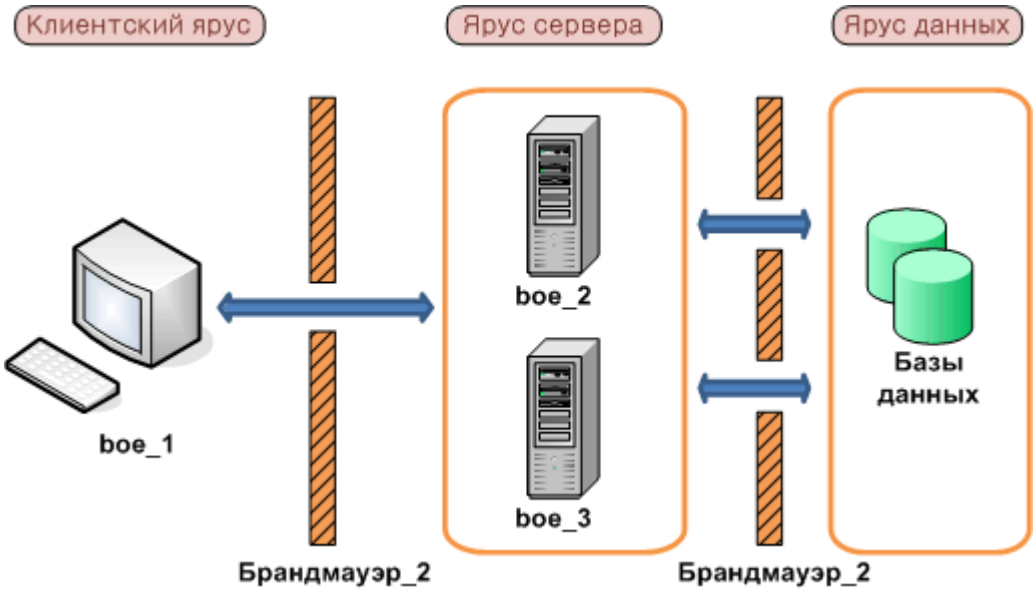
В этом примере показан способ настройки брандмауэра и платформы BI для совместной работы в сценарии развертывания, в котором:

- 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.

Толстый клиент и уровень базы данных развернуты в отдельных сетях



8.18.2.1 Настройка уровней, отделенных брандмауэром от серверов платформы BI

Ниже приводятся действия по настройке, которые необходимо выполнить в этом примере.

1. В этом примере примените следующие требования к обмену данными:
   - Мастер публикаций должен иметь возможность инициировать обмен данными с сервером CMS™ через оба порта.
   - Мастер публикация должен иметь возможность инициировать обмен данными с сервером репозитория входящих файлов и сервером репозитория исходящих файлов.
   - Сервер соединений, каждый дочерний процесс сервера заданий и каждый сервер обработки должны иметь доступ к порту прослушивания на сервере отчетов базы данных.
   - Сервер CMS™ должен иметь доступ к порту прослушивания базы данных на сервере баз данных CMS™.
2. Настройте определенный порт для сервера CMS™, сервера репозитория входящих файлов и сервера репозитория исходящих файлов. Обратите внимание на то, что использовать можно любой свободный порт в пределах 1025-65535.
   Номера портов, выбранных для этого примера, перечислены в следующей таблице:

Сервер	Номер порта
Центральный сервер управления™	6411
Сервер репозитория входящих файлов	6415
Сервер репозитория исходящих файлов	6416

3. 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.
4. 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

5. В этом брандмауэре не поддерживается NAT, поэтому настраивать файл `hosts` не требуется.

Связанные сведения

Основные сведения об обмене данными между компонентами платформы BI [страница 199]
Настройка платформы BI для брандмауэров [страница 213]

8.19 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
• 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

8.19.1 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.

Связанные сведения

установка локального шлюза SAP [страница 1054]

8.19.1.1 Подробное описание требований к настройке портов

Требования, предъявляемые к портам SAP

В платформе BI для обмена данными с SAP NetWeaver используется средство подключения SAP Java Connector (SAP JCO). Необходимо настроить следующие порты и обеспечить их доступность.

- Порт службы шлюза SAP (например, 3300).
- Порт службы диспетчера SAP (например, 3200).

В следующей таблицы 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

8.19.2 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	Необходимые порты для сервера
Платформа SAP BusinessObjects Business Intelligence	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.

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

Исходный компьютер	Порт	Целевой компьютер	Порт	Действие
Сервер веб-приложений	Любой	JD Edwards EnterpriseOne	Любой	Разрешить

8.19.3 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.

8.19.3.1 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

8.19.4 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	Необходимые порты для сервера
Платформа SAP BI	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 веб-службы HTTP/HTTPS	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 Intellignece*.

Помимо настройки брандмауэра для платформы BI требуется также ряд дополнительных настроек.

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	HTTP/HTTPS-порт для веб-служб PeopleSoft	Разрешить
CrystalReports с компонентом "Подключение к данным" на стороне клиента для PeopleSoft	Любой	PeopleSoft	HTTP/HTTPS-порт для веб-служб PeopleSoft	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	Порт сервера репозитория входящих файлов	Разрешить
Мост EPM	Любой	PeopleSoft	Порт базы данных PeopleSoft	Разрешить

8.19.5 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.

Требования, предъявляемые к портам серверов платформы BI

Продукт	Необходимые порты для сервера
Платформа SAP BI	Порт для запросов сервера регистрации BusinessObjects Enterprise

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 для Siebel	Любой	Разрешить
Платформа BI – сервер регистрации для 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

8.20 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.

8.20.1 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 распложены 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.

8.21 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.

8.21.1 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.

8.21.2 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.

8.21.3 Настройка обратного прокси-сервера Apache 2.2 для платформы BI

В этом разделе представлен рабочий процесс по настройке платформы BI для совместной работы с веб-сервером Apache 2.2.

1. Платформа BI и Apache 2.2 должны быть установлены на разных компьютерах.
2. Apache 2.2 должен быть установлен и настроен как обратный прокси-сервер в соответствии с документацией поставщика.
3. Настройте `ProxyPass` для каждого WAR-файла, развернутого за обратным прокси-сервером.
4. Откройте файл *httpd.conf* в папке установки обратного прокси-сервера Apache.
5. Настройте `ProxyPassReverseCookiePath` для каждого веб-приложения, развернутого за обратным прокси-сервером. Например:

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

8.21.4 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
```

8.21.5 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*

      > **→ Напоминание**
      >
      > 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.
   a. Введите имя в поле *Имя веб-средства прослушивания* и нажмите *Далее*.
   b. Выберите тип соединения между сервером ISA и публикуемым веб-узлом и нажмите *Далее*.

      Например, выберите *SSL-подключение к клиентам не требуется*.
   c. 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.
   d. 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 *OK*.
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 CMC. 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.

8.22 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.

8.22.1 Включение обратного прокси-сервера для веб-служб

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

8.22.1.1 Активация обратного прокси на Tomcat

Для включения обратного прокси-сервера на сервере веб-приложений Tomcat, необходимо изменить файл `server.xml`. В числе необходимых изменений следует выполнить настройку параметра `proxyPort` в качестве порта прослушивания обратного прокси-сервера и добавление нового 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 каталоге: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf`

   В ОС Unix `server.xml` находится в каталоге `<CATALINA_HOME>/conf`. Значением по умолчанию для `<CATALINA_HOME>` является `<INSTALLDIR>/sap_bobj/tomcat`.
3. Найдите этот раздел в файле server.xml:

```
<!-- A "Connector" represents an endpoint by which requests are received
         and responses are returned. Documentation at :
         Java HTTP Connector: /docs/config/http.html (blocking & non-blocking)
         Java AJP  Connector: /docs/config/ajp.html
         APR (HTTP/AJP) Connector: /docs/apr.html
         Define a non-SSL/TLS HTTP/1.1 Connector on port 8080
    -->
    <Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000"
redirectPort="8443" compression="on" URIEncoding="UTF-8"
compressionMinSize="2048" noCompressionUserAgents="gozilla,
traviata" compressableMimeType="text/html,text/xml,text/plain,text/css,text/
javascript,text/json,application/javascript,application/json"/>
```

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 `my_reverse_proxy_server.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 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 BusinessObjects™ 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.

8.22.1.2 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.

8.22.2 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.

8.22.2.1 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.

8.22.2.2 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.

8.22.2.3 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. Выберите *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.

8.22.2.4 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.

8.22.3 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.

8.22.3.1 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:ПортОбратногоПроксиСервера/BOE/OpenDocument.jsp?
sIDType=CUID&iDocID=%SI_CUID%
```

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

9 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.

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.

  > ⓘ Примечание
  >
  > По умолчанию пароль проверяется только на выполнение условия об использовании разных регистров. Параметры проверки других условий может настроить администратор. Это гарантирует, что пароль будет содержать по крайней мере один символ в верхнем и один в

нижнем регистре. При необходимости администратор может сделать обязательными другие условия и параметры пароля.

- 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 отключить. Однако при этом будет отключено восстановление 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 безопасности 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 CMC.

> ⓘ 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.

Режим аутентификации	Сервер CMS	Параметры	Примечания
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.

9.1.3.1.1 Включение единого входа для CMC

Для настройки SSO для CMC выполните описанные ниже шаги.

На стороне клиента перед начальной установкой CMC необходимо очистить кэш. Иначе метода аутентификации Enterprise будет кэширован.

На сервере Tomcat выполните следующие шаги.

1. В системе с уже настроенным SSO для BILP перейдите по пути `C:\Program Files (x86)\SAP BusinessObjects\tomcat\webapps\BOE\WEB-INF\config\custom`.
2. Создайте файл CmcApp.properties и запишите в него
   - sso.supported.types=vintela, trustedIIS, trustedHeader, trustedParameter, trustedCookie, trustedSession, trustedUserPrincipal, trustedVintela, trustedX509, sapSSO, siteminder
   - authentication.default=secWinAD

   .
3. Перезапустите Tomcat.

   SSO для CMC активирован.

> ⓘ Примечание
>
> После тайм-аута сеанса панели запуска BI или CMC, если SSO активирован (в обоих случаях), пользователю будет предложено войти в систему. При обновлении страницы будет выполнен повторный вход в систему без ввода пароля. Во время этого процесса не следует деактивировать средство ping.

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 данных. 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 как к платформе BI 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 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 для платформы BI методом аутентификации по умолчанию. Она автоматически активируется при первой установке системы (ее невозможно деактивировать). При добавлении пользователей и групп, а также управлении ими платформа хранит сведения о пользователях и группах 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 на 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 аутентификации 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 будет содержать по крайней мере один символ в верхнем и один в нижнем регистре. **Примечание** Этот параметр выбран по умолчанию. При необходимости администратор может отменить выбор данного параметра.
	Обязательное использование цифр в пароле	Этот параметр гарантирует, что пароль содержит по крайней мере один цифровой символ.
	Обязательное использование специальных символов в пароле	Этот параметр гарантирует, что пароль содержит по крайней мере один специальный символ.
	Должно содержать N символов, где N:	Этот параметр обеспечивает длину паролей не менее N символов.
	Не может превышать N символов, где N:	Этот параметр гарантирует, что длина пароля не может превышать N символов.
	Не должно содержать следующую последовательность символов:	Этот параметр гарантирует, что пароль не может содержать ограниченные последовательности символов. По умолчанию используется следующее значение: "Password 12345678 administrator".
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.
	Должен изменить пароль через N дней неактивности:	Этот параметр обеспечивает смену пароля через N дней бездействия.
	Должен изменить начальный пароль через N дней:	Этот параметр обеспечивает смену начального пароля через N дней.
Ограничения на вход	*Отключать учетную запись после N неудачных попыток входа*	В этом параметре безопасности указывается количество попыток входа в систему, которое может

Настройки	Параметры	Описание
		сделать пользователь, прежде чем его учетная запись будет отключена.
	Сбрасывать счетчик неудачных попыток через N мин.	В этом параметре указывается промежуток времени, по истечении которого сбрасывается счетчик попыток входа в систему.
	Повторно включать учетную запись через N мин.	В этом параметре указывается время, в течение которого учетная запись остается заблокированной после N неудачных попыток входа в систему.
Синхронизовать учетные данные для входа в систему и источник данных	*Разрешить и обновить учетные данные пользователя для входа в источник данных при входе в систему*	Этот параметр включает учетные данные пользователя для входа в источник данных после выполнения пользователем входа в систему.
Доверительная аутентификация	*Доверительная аутентификация включена*	Позволяет использовать параметры для настройки доверительной аутентификации.
Аутентификация OpenID Connect	*Аутентификация OpenID Connect активирована*	Чтобы активировать настройку *Аутентификация OpenID Connect*, установите флажок *Аутентификация OpenID Connect активирована*. При аутентификации через OpenID Connect на платформе BI создается внутренний сеанс Enterprise.

9.2.3 Изменение параметров Enterprise

1. Перейдите в область управления CMC *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 CMC *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	По умолчанию	Минимум	Рекомендованный максимум
Не должно содержать следующую последовательность символов:	password 12345678 administrator	1 символ	25550 символов
Должен содержать не менее N символов	8 символов	6 символа	255 символов
Не может превышать N символов	255 символов	13 символов	255 символов
Должен изменять пароль каждые N дн.	30 дн.	2 дн.	100 дней
Не может повторно использовать N последних паролей	3 пароля	1 пароль	100 паролей
Должен ждать N мин. для изменения пароля	0 минут	0 минут	100 минут
Должен изменить пароль через N дней неактивности:	20 дней	2 дня	365 дней
Должен изменить начальный пароль через N дней:	7 дней	2 дня	15 дней
Отключать учетную запись после N неудачных попыток входа	10 неудачная попытка	1 неудачная попытка	100 неудачных попыток

Настройка пароля	По умолчанию	Минимум	Рекомендованный максимум
Сбрасывать счетчик неудачных попыток через N мин.	5 минут	1 минута	100 минут
Повторно включать учетную запись через N мин.	5 минут	0 минут	100 минут

4. Нажмите кнопку *Обновить*.

9.2.4 Аутентификация SAML 2.0

9.2.4.1 Обеспечение единого входа через SAML 2.0

Платформа Business Intelligence теперь может быть интегрирована с любыми порталами или приложениями с поддержкой SAML в качестве механизма аутентификации для единого входа. Это означает, что теперь можно войти в облачное приложение, например Analytics Hub или SAP Analytics Cloud, и получить доступ к ресурсам в приложениях BI, таких как стартовая панель BI в стиле Fiori и OpenDocument, в одном сеансе входа.

Чтобы обеспечить единый вход через SAML 2.0, необходимо настроить сервер приложений.

> **Примечание**
>
> Задайте следующие настройки, чтобы использовать функцию аутентификации SAML функцию для входа в систему через адрес электронной почты:
>
> - Сторонние пользователи
> Чтобы активировать импорт адресов электронной почты из внешней системы, используйте параметр командной строки `"-importtpemailduringsync"`:
> 1. Добавьте параметр `"-importtpemailduringsync"` в *CMS* > *Свойства* > *Параметры командной строки*.
> 2. Перезапустите CMS.
> 3. Обновите аутентификацию стороннего пользователя, электронную почту которого требуется использовать для входа в систему.
>
> Поддерживаемые типы аутентификации сторонних пользователей для этой функции: SAP, LDAP и WinAD.
> - Корпоративные пользователи
> См. SAP-ноту 2642247.

9.2.4.2 Настройка платформы BI в качестве поставщика услуг SAML

Чтобы использовать платформу BI в качестве поставщика услуг SAML, необходимо настроить ее для аутентификации SAML 2.0.

В этой версии упрощена настройка сервера приложений в качестве поставщика услуг SAML. В целях упрощения настройки удалены следующие шаги:

- Копирование файлов JAR SAML в каталог установки платформы BI
- Редактирование файла securitycontext.xml
- Редактирование файла web.xml

Это означает, что файлы JAR SAML, теги XML для каждого веб-приложения в файле securitycontext.xml и фильтры в файле web.xml доступны по умолчанию. Поэтому после выполнения перечисленных ниже шагов можно включить или отключить аутентификацию SAML 2.0 для каждого веб-приложения с помощью файла свойств каждого веб-приложения.

> **Примечание**
>
> В качестве поставщика удостоверений по умолчанию используйте SAP Cloud Identity Provider.

> **Примечание**
>
> В качестве поставщика услуг SAML можно использовать сервер приложений Tomcat, WebSphere и Jboss.

1. Выполните процедуру, описанную в Настройка доверительной аутентификации с использованием веб-сеансов [страница 255].
2. Если используется поставщик удостоверений SAP Cloud Platform, экспортируйте всех пользователей и затем импортируйте их в платформу BI. См. раздел Массовый импорт пользователей из Central Management Console.

   Для получения сведений об экспорте пользователей SAP Cloud Platform в CSV см. раздел Экспорт существующих пользователей арендатора службы SAP Cloud Platform Identity Authentication.
3. Отредактируйте файл свойств, изменив `logon.webssoauthnetication.framework=None` на `logon.webssoauthnetication.framework=SAML`.
   - Для стартовой панели BI в стиле Fiori: перейдите в каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` и отредактируйте файл `fioriBI.properties`.
   - Для Open Document: перейдите в каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` и отредактируйте файл `OpenDocument.properties`.
   - Для CMC: перейдите в каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` и отредактируйте файл `CMCApp.properties`.

> **Примечание**
>
> Помимо добавления `saml.enabled=true` задайте свойство `sso.supported.types = trustedSession` в файлах свойств `CMC\FioriBI\OpenDocument`.

4. Чтобы обновить метаданные IDP в SP, сначала выгрузите метаданные IDP из соответствующих поставщиков услуг IDP, затем скопируйте файл метаданных в каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF` и переименуйте его в `idp-meta-downloaded.xml`.

   Для получения дополнительных сведений о выгрузке метаданных IDP см. раздел Конфигурация SAML 2.0 арендатора.

   > **Примечание**
   >
   > Если платформа BI развернута на компьютере с ОС, отличной от Windows, необходимо изменить разделители пути в пути к файлу метаданных IDP в bean **FilesystemMetadataProvider** в файле `securityContext.xml` в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`.
   >
   > Например, измените `<value type="java.io.File">/WEB-INF/idp-meta-downloaded.xml</value>` на `<value type="java.io.File">\WEB-INF\idp-meta-downloaded.xml</value>`.

   Для получения сведений о создании хранилища ключей для включения SAML 2.0 см. Создание хранилища ключей SAML 2.0 [страница 256].

5. (Необязательно) В качестве атрибута утверждения SAML можно использовать адрес электронной почты. Подробную информацию см. в разделе Использование адреса электронной почты как атрибута утверждения SAML [страница 258].
6. (Необязательно) Если используется балансировщик нагрузки или обратный прокси-сервер, для получения дополнительных сведений см. 2621904.
7. Создайте файл WAR, используя средство WDeploy.
   a. Перейдите по пути `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\wdeploy`.
   b. Используйте соответствующую команду развертывания, чтобы создать файл WAR для версий, специфических для приложения.

   - Для Windows: `wdeploy.bat <App_Server_Name><Version_Name> -DAPP=BOE predeploy`
   - Для UNIX: `wdeploy.sh <App_Server_Name><Version_Name> -DAPP=BOE predeploy`

   > **Примечание**
   >
   > Следует заменить <App_Server><Version_Name> на тип сервера приложений и его версию. Например, для сервера приложений Tomcat 8.0 можно использовать tomcat8. Аналогичным образом jboss7 для сервера приложений JBoss 7.0 и websphere9 для сервера приложений WebSphere 9.0.

8. После создания файла WAR скопируйте и разверните его на сервере приложений.
9. Создайте и загрузите метаданные поставщика услуг.

> **ⓘ Примечание**
>
> В файле securitycontext.xml можно определить свойство entitybase URL на основе объекта, чтобы сгенерировать метаданные поставщика услуг с использованием URL-адреса конечной точки. По умолчанию имя хоста и номер порта, указанные в URL-адресе, учитываются при загрузке метаданных поставщика услуг.

a. Перейдите на `http(s)://host:port/BOE/saml/metadata`.

   Файл XML будет автоматически выгружен.

b. Загрузите файл XML в поставщик удостоверений. Если в качестве поставщика удостоверений используется Microsoft Active Directory Federation Services, для получения дополнительных сведений см. Создание отношений доверия с проверяющей стороной [страница 259].

> **ⓘ Примечание**
>
> Можно использовать файл метаданных поставщика услуг по умолчанию `spring_saml_metadata.xml`, который находится в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`, а не создавать его вручную. Тег XML`<replace_withip>` необходимо заменить IP-адресом или именем хоста компьютера на основе вашей сети, а `<replace_withport>` – номером порта сервера приложений. Замените HTTP на HTTPS, если на сервере приложений включен HTTPS.

10. Если используется SAP Cloud Identity, сведения о создании приложения SAML в IDP и загрузке файла `metadata.xml` SP в IDP для настройки SSO SAML для платформы BI см. в разделе Настройка доверенного поставщика услуг.

> **ⓘ Примечание**
>
> После изменения файла хранилища ключей необходимо создать метаданные последнего поставщика услуг.

> **→ Совет**
>
> Чтобы можно было проверить успешность интеграции SAML, после того как вы запустите приложение с настройкой SAML (стартовую панель BI, стартовую панель BI в стиле Fiori или OpenDocument), вы будете перенаправлены в IDP.

9.2.4.2.1 Настройка доверительной аутентификации с использованием веб-сеансов

Необходимо настроить доверительную аутентификацию с использованием веб-сеансов в рамках настройки сервера приложений в качестве поставщика услуг SAML.

> **ⓘ Примечание**
>
> По соображениям безопасности доверительную аутентификацию не следует включать без HTTPS. Если доверительная аутентификация включена без HTTPS, это считается нарушением безопасности, поскольку URL-адрес отображается для неавторизованных пользователей. Во

избежание нарушения безопасности информация пользователя может быть проверена с помощью действительного сертификата. Для получения дополнительных сведений см. 1388240.

1. Создайте файл `global.properties` в пользовательской папке `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.
2. В качестве содержимого файла `global.properties` введите следующее:

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

> **Примечание**
>
> Ведение значений параметров `trusted.auth.user.param` и `trusted.auth.shared.secret` следует выполнить в соответствии с обновлением в файле *custom.jsp*.

3. Выберите *CMC* > *Аутентификация* > *Enterprise*.
4. Установите значение от 0 до 365 (в *днях*) в качестве *срока действия*.
5. Выберите *Новый общий секретный ключ*.
6. Чтобы загрузить созданный общий секретный ключ, выберите *Загрузить общий секретный ключ*.

   Файл `TrustedPrincipal.conf` загружается.
7. Скопируйте и вставьте файл `TrustedPrincipal.conf file` в `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` и `\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
8. Выберите *CMC* > *Аутентификация* > *Enterprise* и нажмите *Обновить*.
9. Обновите в файле custom.jsp значение общего секретного ключа для классической стартовой панели BI и стартовой панели BI в стиле Fiori. Для получения более подробной информации см. Редактирование файла custom.jsp [страница 421].

> **Примечание**
>
> Необходимо обновить файл custom.jsp, если в качестве поставщика удостоверений используются Microsoft ADFS и Microsoft Azure.

9.2.4.2.2 Создание хранилища ключей SAML 2.0

Чтобы использовать собственный файл хранилища ключей для SAML 2.0, необходимо создать его.

При обменах SAML для подписания и шифрования данных используется криптография. Образец файла самоподписанного хранилища ключей `sampletestKeystore.jks` поставляется в пакете с продуктом и действителен до 18 октября 2019 г. `sampletestKeystore.jks` имеет псевдоним **Testkey** и пароль **Password1**.

Теперь можно создать файл самоподписанного хранилища ключей с использованием утилиты keytool JAVA.

1. Перейдите в каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`.
2. Выполните команду: `keytool -genkeypair -alias aliasname -keypass password -keystore samplekeystore.jks -validity numberofdays`

Команда	Описание
-alias	Ввод псевдонима сертификата
-keypass	Ввод пароля сертификата
-keystore	Имя файла хранилища ключей
-validity	Срок действия сертификата
numberofdays	Число дней, в течение которых действителен самостоятельно подписанный сертификат

После выполнения команды ответьте на предлагаемые следующие вопросы:

- Введите пароль хранилища ключей: *****
- Введите еще раз новый пароль: *****
- Ваши имя и фамилия? : **MY_FIRST_AND_LAST_NAME**
- Название вашей организационной единицы? : **MY_ORGANIZATIONAL_UNIT**
- Название вашей организации? : **MY_ORGANIZATION**
- Название вашего города или места жительства? : **MY_CITY**
- Название вашей области или края? : **MY_STATE**
- Двухбуквенный код страны для этой единицы? : **COUNTRY_CODE**

Файл хранилища ключей генерируется в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`.

3. Переместите файл хранилища ключей в каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`
4. Отредактируйте файл `securityContext.xml`, находящийся в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`, с использованием новых псевдонима, пароля и имени файла хранилища ключей.

   См. следующий код XML:

   {·} Пример кода

```
<bean id="keyManager"
class="org.springframework.security.saml.key.JKSKeyManager">
<constructor-arg value="/WEB-INF/sampleKeystore.jks"/>
<constructor-arg type="java.lang.String" value="Password1"/>
<constructor-arg>
<map>
<entry key="aliasname" value="password"/>
</map>
</constructor-arg>
```

```
<constructor-arg type="java.lang.String" value="Testkey"/>
</bean>
```

Для получения представления об аргументах см. следующую таблицу.

Тег XML	Описание
`<constructor-arg value="/WEB-INF/sampleKeystore.jks"/>`	Определяет местоположение файла хранилища ключей
`<constructor-arg type="java.lang.String" value="Password1"/>`	Пароль для файла хранилища ключей
`<entry key="aliasname" value="password"/>`	Пароль псевдонима
`<constructor-arg type="java.lang.String" value="Testkey"/>`	Псевдоним сертификата по умолчанию

9.2.4.2.3 Использование адреса электронной почты как атрибута утверждения SAML

Можно включить аутентификацию электронной почты в SAML для стартовой панели BI в стиле Fiori, OpenDocument и Central Management Console (CMC).

1. В зависимости от приложения, с которым вы работаете, отредактируйте соответствующие свойства файла, добавив две строки:

```
saml.enabled=true
saml.isUseEmailAddress=true
saml.authType=secEnterprise
```

> **Примечание**
>
> `saml.isUseEmailAddress` принимает логические значения, а `saml.authType` соответствует типу аутентификации сведений о пользователе или псевдониме, с которыми будет происходить вход в систему. Функцию электронной почты можно настроить отдельно для каждого приложения, указанного выше. Если для `saml.isUseEmailAddress` установлено значение `false`, вход выполняется на основе параметра имени. Если установлено значение `true`, вход выполняется на основе параметра электронной почты. `saml.authType` проверяет наличие возможных дубликатов и гарантирует, что два псевдонима с одинаковым типом аутентификации не будут иметь один и тот же адрес электронной почты.

- Для стартовой панели BI в стиле Fiori: `fioriBI.properties` в `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`

- Для OpenDocument: `OpenDocument.properties` в `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`
- Для CMC: `CMCApp.properties` в `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`

> **Примечание**
>
> Для CMC задайте в файле `CMCApp.properties` свойство `sso.supported.types = trustedSession`.

2. Настройте IDP для поддержки электронной почты. Также можно обратиться к Руководству по службе SAP Cloud Platform Identity Authentication за дополнительными сведениями, если используется поставщик удостоверений SAP Cloud Identity Provider.
   a. Перейдите в консоль администрирования арендатора для службы SAP Cloud Platform Identity Authentication с помощью URL консоли.

   > **Примечание**
   >
   > URL имеет следующую форму: `https://<tenant ID>.accounts.ondemand.com/admin`. Ид. арендатора создается системой автоматически. Первый администратор, созданный для арендатора, получает электронное сообщение об активации, в котором указан URL, содержащий ид. арендатора.

   b. Выберите *Приложения*.
   c. Выберите приложение.
   d. На вкладке *доверия* в разделе *SAML 2.0* щелкните *Атрибут ид. имени*.
   e. Выберите *Электронная почта*.
   f. Нажмите кнопку *Сохранить*.

9.2.4.2.4 Создание отношений доверия с проверяющей стороной

Для обновления метаданных поставщика услуг необходимо создать отношения доверия с проверяющей стороной и правило утверждения в средстве Microsoft ADFS Management.

1. Запустите *Server Manager* (Диспетчер сервера).
2. Выберите *Tools (Инструменты)* > *AD FS Management (Управление AD FS)*.
3. Разверните *Trust Relationships* (Отношения доверия).
4. Щелкните правой кнопкой мыши *Relying Trust Party* (Отношения доверия с проверяющей стороной) и выберите *Add Relying Trust Party* (Добавить отношения доверия с проверяющей стороной).
5. В мастере *Add Relying Trust Party* выберите *Start* (Пуск).
6. Выберите *Import data about the relying party from a file* (Импортировать данные о проверяющей стороне из файла) и нажмите *Browse* (Обзор).
7. Найдите выгруженный файл метаданных поставщика услуг и выберите его.
8. Нажмите кнопку *Next* (Далее).
9. Введите *Display Name* (Выводимое имя) и нажмите *Next*.

10. На шаге *Configure Multi-factor Authentication Now?* (Настроить многофакторную проверку подлинности сейчас?) нажмите *Next*.
11. Выберите *Permit all users to access this relying party* (Разрешить всем пользователям доступ к этой проверяющей стороне) и нажмите *Next*.
12. Просмотрите информацию на экране *Ready to Add Trust* (Готово к добавлению отношений доверия) и нажмите *Next*.
13. Нажмите кнопку *Finish* (Готово).
    Появится диалоговое окно *Edit Claim Rules* (Редактировать правила утверждений). Можно создать правила утверждений с именем пользователя или адресом электронной почты в качестве атрибута.

Отношения доверия с проверяющей стороной успешно созданы.

9.2.4.2.4.1 Создание правила утверждения с именем пользователя в качестве атрибута

Можно создать правило утверждения с именем пользователя в качестве атрибута утверждения SAML.

Должны быть доступны отношения доверия с проверяющей стороной.

1. В диалоговом окне *Edit Claim Rules* (Редактировать правила утверждений) выберите *Add Rule* (Добавить правило).
2. В окне *Add Transform Claim Rule Wizard* (Мастер добавления правила преобразования утверждения) выберите *Send LDAP Attributes as Claims* (Отправить атрибуты LDAP как утверждения) и нажмите *Next* (Далее).
3. Введите *Claim rule name* (Имя правила утверждения) и выберите *Active Directory* в качестве *Attribute store* (Хранилище атрибутов).
4. В разделе *LDAP Attribute* (Атрибут LDAP) выберите *SAM-Account Name* (Имя входа пользователя пред-Windows 2000).
5. В разделе *Outgoing Claim Type* (Тип исходящего утверждения) выберите *Name ID* (Ид. имени).
6. Нажмите кнопку *Finish* (Готово).

Правило утверждения создано для имени пользователя в качестве атрибута.

9.2.4.2.4.2 Создание правила утверждения с адресом электронной почты в качестве атрибута

Чтобы использовать адрес электронной почты как атрибут утверждения SAML, необходимо создать два правила утверждений.

1. В диалоговом окне *Edit Claim Rules* (Редактировать правила утверждений) выберите *Add Rule* (Добавить правило).
2. В окне *Add Transform Claim Rule Wizard* (Мастер добавления правила преобразования утверждения) выберите *Send LDAP Attributes as Claims* (Отправить атрибуты LDAP как утверждения) и нажмите *Next* (Далее).

3. Введите *Claim rule name* (Имя правила утверждения) и выберите *Active Directory* в качестве *Attribute store* (Хранилище атрибутов).
4. В разделе *LDAP Attribute* (Атрибут LDAP) выберите *E-Mail-Addresses* (Адреса электронной почты) и затем в разделе *Outgoing Claim Type* (Тип исходящего утверждения) выберите *E-Mail Address* (Адрес электронной почты).
5. Во второй записи в разделе *LDAP Attribute* (Атрибут LDAP) выберите *Given Name* (Собственное имя) и затем в разделе *Outgoing Claim Type* (Тип исходящего утверждения) введите *FirstName* (Имя).
6. Нажмите кнопку *Finish* (Готово).

   Первое правило создано. Для создания второго правила утверждения выполните следующие шаги.
7. В диалоговом окне *Edit Claim Rules* (Редактировать правила утверждений) выберите *Add Rule* (Добавить правило).
8. В окне *Add Transform Claim Rule Wizard* (Мастер добавления правила преобразования утверждения) выберите *Transfer an Incoming Claim* (Передать входящее утверждение) и нажмите *Next* (Далее).
9. Введите *Claim rule name* (Имя правила утверждения), выберите *E-mail Address* (Адрес электронной почты) в качестве *Incoming claim type* (Тип входящего утверждения), *Name ID* (Ид. имени) в качестве *Outgoing claim type* (Тип исходящего утверждения) и *Email* (Электронная почта) в качестве *Outgoing name format* (Иисходящий формат имени).
10. Нажмите кнопку *Finish* (Готово).

9.2.4.3 Использование сервера приложений WebSphere в качестве поставщика услуг SAML

Этот раздел содержит инструкции по настройке сервера приложений WebSphere для аутентификации SAML 2.0.

> ⓘ Примечание
>
> В перечисленных ниже шагах в качестве поставщика удостоверений по умолчанию используется поставщик удостоверений SAP Cloud Identity.

Выполните следующие шаги:

1. Скопируйте файлы JAR SAML из `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\SAMLJARS` в `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Profile_Name>\installedApps\<Node_Name>\BOE.ear\BOE.war\WEB-INF\lib`.
2. Чтобы настроить доверительную аутентификацию с использованием веб-сеанса, выполните следующие шаги:
   1. Добавьте файл global.properties в папку custom: `<WebSphere_InstallDir>\WebSphere\\AppServer\profiles\<Profile_Name>\installedApps\<Node_Name>\BOE.ear\BOE.war\WEB-INF\config\custom`. Ниже представлено содержимое файла global.properties:
      ```
      sso.enabled=true
      trusted.auth.user.retrieval=WEB_SESSION
      trusted.auth.user.param=UserName
      ```

2. Выберите *CMC* > *Аутентификация* > *Enterprise* .
3. Включите *доверительную аутентификацию*.
4. Укажите *срок действия*.
5. Выберите *Новый общий секретный ключ*.
6. Чтобы загрузить созданный общий секретный ключ, выберите *Загрузить общий секретный ключ*.
   <Файл `TrustedPrincipal.conf` загружается.
7. Вставьте файл TrustedPrincipal.conf в каталоги `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` и `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
8. Выберите *CMC* > *Аутентификация* > *Enterprise* и нажмите *Обновить*.
9. Перезапустите сервер приложений WebSphere.

3. Если используется поставщик удостоверений SAP Cloud Platform, экспортируйте всех пользователей и затем импортируйте их в платформу BI. См. раздел Массовый импорт пользователей из Central Management Console

   Для получения сведений об экспорте пользователей SAP Cloud Platform в CSV см. раздел Экспорт существующих пользователей арендатора службы SAP Cloud Platform Identity Authentication

4. Отредактируйте файл свойств, добавив `saml.enabled=true`. См. имена файлов и каталоги ниже:
   1. Для стартовой панели BI в стиле Fiori: перейдите в каталог `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Profile_Name>\installedApps\<Node_Name>\BOE.ear\BOE.war\WEB-INF\config\custom` и отредактируйте файл *fioriBI.properties*.
   2. Для Open Document: перейдите в каталог `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Profile_Name>\installedApps\<Node_Name>\BOE.ear\BOE.war\WEB-INF\config\custom` и отредактируйте файл *OpenDocument.properties*.
   3. Для CMC: перейдите в каталог `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Profile_Name>\installedApps\<Node_Name>\BOE.ear\BOE.war\WEB-INF\config\custom` и отредактируйте файл *CMCApp.properties*.

      > **Примечание**
      >
      > Для CMC: задайте еще одно свойство `sso.supported.types = trustedSession` в файле *CMCApp.properties*.

   > **Примечание**
   >
   > Если приложение не содержит файл пользовательских свойств, создайте новый файл.

5. Чтобы обновить метаданные IDP в SP, загрузите метаданные из соответствующих поставщиков услуг IDP. Скопируйте файл метаданных в каталог `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Profile_Name>\installedApps\<Node_Name>\BOE.ear\BOE.war\WEB-INF` и переименуйте его в **idp-meta-downloaded.xml**. Для получения дополнительных сведений о загрузке метаданных IDP см. раздел Конфигурация SAML 2.0 арендатора

> **Примечание**
>
> Новый алгоритм SHA-256 теперь поддерживается для интеграции SAML.

6. Перезапустите сервер приложений WebSphere.

> **Примечание**
>
> В случае развертывания BOE на компьютере не под управлением Windows разделители пути к файлу метаданных IDP в bean **FilesystemMetadataProvider** следует изменить в файле `securityContext.xml` в каталоге `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Profile_Name>\installedApps\<Node_Name>\BOE.ear\BOE.war\WEB-INF`.
>
> Т. е. `<value type="java.io.File">/WEB-INF/idp-meta-downloaded.xml</value>` следует изменить на `<value type="java.io.File">\WEB-INF\idp-meta-downloaded.xml</value>`.

Создание хранилища ключей для включения SAML 2.0 (необязательно)

Этот шаг применим, только если вы хотите использовать собственный файл хранилища ключей.

При обмене данными SAML для подписания и шифрования данных используется криптография. Образец самостоятельно подписанного хранилища ключей `sampletestKeystore.jks` поставляется в пакете с продуктом и действителен до 18 октября 2019 г. `sampletestKeystore.jks` имеет псевдоним `Testkey` и пароль `Password1`. Теперь можно создать файл самоподписанного хранилища ключей с использованием утилиты keytool JAVA. Для создания файла хранилища ключей выполните следующие шаги:

1. Перейдите в каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`.
2. Выполните команду: `keytool -genkeypair -alias aliasname -keypass password -keystore samplekeystore.jks -validity numberofdays`

Команда	Описание
-alias	Ввод псевдонима сертификата
-keypass	Ввод пароля сертификата
-keystore	Имя файла хранилища ключей
-validity	Срок действия сертификата
numberofdays	Число дней, в течение которых действителен самостоятельно подписанный сертификат

После выполнения команды потребуется ответить на следующие вопросы:

- Введите пароль хранилища ключей: *****
- Введите еще раз новый пароль: *****
- Ваши имя и фамилия? : <Имя и фамилия>
- Название организационной единицы? : <Название отдела>

- Название организации? : <Название компании>
- Название города и района? : <Город>
- Название области и края? : <Регион>
- Двухбуквенный код страны для этой единицы? : <Страна или код ISO>

3. Остановите сервер приложений WebSphere.
   Файл хранилища ключей создается в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`.
4. Переместите файл хранилища ключей в каталог `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Profile_Name>\installedApps\<Node_Name>\BOE.ear\BOE.war\WEB-INF`.
5. Отредактируйте файл `securityContext.xml` , расположенный в `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Profile_Name>\installedApps\<Node_Name>\BOE.ear\BOE.war\WEB-INF`, указав новые сведения о псевдониме, пароле и имени файла хранилища ключей. См. следующий код XML:

   Пример кода

   ```
   <bean id="keyManager"
   class="org.springframework.security.saml.key.JKSKeyManager">
   <constructor-arg value="/WEB-INF/sampleKeystore.jks"/>
   <constructor-arg type="java.lang.String" value="Password1"/>
   <constructor-arg>
   <map>
   <entry key="aliasname" value="password"/>
   </map>
   </constructor-arg>
   <constructor-arg type="java.lang.String" value="Testkey"/>
   </bean>
   ```

   Для получения представления об аргументах см. следующую таблицу.

Тег XML	Описание
`<constructor-arg value="/WEB-INF/sampleKeystore.jks"/>`	Определяет место файла хранилища ключей
`<constructor-arg type="java.lang.String" value="Password1"/>`	Пароль для файла хранилища ключей
`<entry key="aliasname" value="password"/>`	Пароль псевдонима
`<constructor-arg type="java.lang.String" value="Testkey"/>`	Псевдоним сертификата по умолчанию

7. Создайте и загрузите метаданные поставщика услуг.
   1. Перейдите в http(s)://host:port/BOE/saml/metadata. Файл XML автоматически загружается после перехода по указанному URL-адресу.

2. Загрузите файл XML в поставщик удостоверений.

> ⓘ Примечание
>
> Можно использовать файл метаданных поставщика услуг по умолчанию `spring_saml_metadata.xml`, который находится в каталоге `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Profile_Name>\installedApps\<Node_Name>\BOE.ear\BOE.war\biprws\WEB-INF`, а не создавать его вручную. Тег XML `<replace_withip>` необходимо заменить IP-адресом или именем хоста компьютера на основе вашей сети, а `<replace_withport>` – номером порта сервера приложений WebSphere. Замените HTTP на HTTPS, если в WebSphere включен HTTPS.

8. Если используется SAP Cloud Identity, сведения о создании приложения SAML в IDP и загрузке файла `metadata.xml` SP в IDP для настройки SAML SSO для платформы BI см. в разделе Настройка доверенного поставщика услуг.
9. Перезапустите сервер приложений WebSphere.

> ⓘ Примечание
>
> Последние метаданные поставщика услуг необходимо создать после изменения файла хранилища ключей.

> → Совет
>
> Для проверки успешности интеграции SAML, после того как вы запустите приложение с настройкой SAML (стартовую панель BI, стартовую панель BI в стиле Fiori или OpenDocument), вы будете перенаправлены в IDP.

9.2.5 Установление доверительной аутентификации между сервером приложений Java для SAP NetWeaver и платформой BI

- Сервер приложений Java для SAP NetWeaver настроен для аутентификации SAML 2.0 как поставщик услуг.
- Пользователь должен существовать на сервере приложений Java для SAP NetWeaver.
- Сертификаты SAML 2.0 поставщика услуг и поставщика удостоверений заменены для установления отношений доверия между ними.
  Тот же пользователь должен быть импортирован как пользователь Enterprise в платформу BI.

Для установления доверительной аутентификации между сервером приложений Java для SAP NetWeaver и платформой BI выполните следующие шаги:

> ⓘ Примечание
>
> - Для извлечения данных пользователя при включении доверительной аутентификации для веб-приложений следует использовать метод `USER_PRINCIPAL`.
> - По соображениям безопасности доверительную аутентификацию не следует включать без HTTPS. Если доверительная аутентификация включена без HTTPS, это считается нарушением

безопасности, поскольку URL-адрес отображается для неавторизованных пользователей. Во избежание нарушения безопасности информация пользователя может быть проверена с помощью действительного сертификата. Для получения дополнительных сведений см. 1388240.

1. Создайте веб-приложение BI с использованием WDeploy.
   a. Откройте каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\wdeploy`.
   b. Выполните команду для создания файла `BOE.sca`: `wdeploy.bat sapappsvr73 -DAPP=BOE predeploy`

      `BOE.sca` создается в каталоге `<INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\wdeploy\workdir\sapappsvr73\application`.
2. Включите доверительную аутентификацию, отредактировав файл `web.xml`.
   a. Извлеките файл `BOE.sca` в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\workdir\sapappsvr73\application` с помощью таких средств, как winrar или winzip.
   b. Прежде чем вносить изменения, сделайте копию файла `BOE.sca`. В `BOE.sca` выберите *DEPLOYARCHIVES* > *BOE.ear* > *BOE.war* > *WEB-INF* >.
   c. Отредактируйте файл `web.xml`, добавив нижеприведенные теги XML перед `</web-app>`.

   Примечание

   Необходимо добавить роли (указанные в коде XML ниже) в сервер приложений Java для SAP NetWeaver и назначить их группе пользователей или пользователю.

   - j2ee-admin
   - j2ee-guest
   - j2ee-special

   Пример кода

```
<security-constraint>
<web-resource-collection>
 <web-resource-name>InfoView</web-resource-name>
<url-pattern>*</url-pattern>
<http-method>DELETE</http-method>
<http-method>GET</http-method>
<http-method>POST</http-method>
<http-method>PUT</http-method>
</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>BASIC</auth-method>
<realm-name>InfoView</realm-name>
</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>
```

d. Создайте новый файл XML `web-j2ee-engine.xml` с указанными ниже тегами XML и сохраните его в каталоге `<INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\wdeploy\workdir\sapappsvr73\application\BOE.sca\DEPLOYARCHIVES\BOE.ear\BOE.war\WEB-INF`.

Пример кода

```
<?xml version="1.0" encoding="UTF-8"?>
<web-j2ee-engine xsi:noNamespaceSchemaLocation="web-j2ee-engine.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<security-role-map>
    <role-name>j2ee-admin</role-name>
    <server-role-name>administrators</server-role-name>
</security-role-map>
<security-role-map>
      <role-name>j2ee-guest</role-name>
      <server-role-name>guests</server-role-name>
</security-role-map>
<security-role-map>
      <role-name>j2ee-special</role-name>
      <server-role-name>all</server-role-name>
</security-role-map>
 <login-module-configuration>
      <security-policy-domain>/irj</security-policy-domain>
 </login-module-configuration>
</web-j2ee-engine>
```

e. Сохраните файл `web-j2ee-engine.xml`.

f. Перетащите файл в папку `WEB-INF` архива `BOE.war`.

Включение SSO в BIP - USER PRINCIPAL, общий секретный ключ – `Trustedprincipal.conf`

Включение SSO осуществляется с использованием метода USER PRINCIPAL (Принципал пользователя) для передачи имени пользователя NW и файла `Trustedprincipal.conf` для передачи общего секретного ключа.

Чтобы включить доверительную аутентификацию и создать общий секретный ключ, выполните следующие шаги:

1. Выберите *CMC* > *Аутентификация* > *Enterprise* >.
2. Включите *доверительную аутентификацию*.
3. Выберите *Создать новый общий секретный ключ*.
4. Выберите *Загрузить общий секретный ключ* и сохраните его на компьютере BOE.
5. Нажмите *Обновить*.
6. В папке `BOE.war/web-inf/config/default/folder`, извлеките следующий файл в папку `BOE.war/web-inf/config/custom/folder`:
   - `global.properties`
7. Добавьте в `global.properties` следующее:

- `sso.enabled=true`
- `trusted.auth.user.retrieval=USER_PRINCIPAL`
- `trusted.auth.user.namespace.enabled=true`
- `trusted.auth.shared.secret=MySecret`

> **Примечание**
>
> Задано trusted.auth.user.namespace.enabled=true

При первой попытке вы должны получить сообщение об ошибке: "Отказано во входе: пользователь "secExternal:samltest" не найден (FWB 00007)". Имеется функция автоматической привязки, которая отображает `secExternal: samltest` на пользователя BOE как псевдоним. Войдите, как обычно, через форму входа InfoView. Учетные данные BOE, которые вы используете, имеют псевдоним `secExternal: samltest`, созданный для них. Например, если вы используете учетную запись пользователя samltest, в ее свойствах пользователя можно увидеть, что `secExternal: samltest` присвоен как псевдоним.

8. Перейдите в каталог `<INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\wdeploy\workdir\sapappsvr73\application\ BOE.sca\DEPLOYARCHIVES\BOE.ear\BOE.war\ WEB-INF\ Eclipse\plugins\webpath.InfoView\web\custom.jsp`
9. Добавьте указанные ниже теги XML в файл `custom.jsp`.
   Блок кода:

   > **Пример кода**
   >
   > ```
   > <%@ page language="java" contentType="text/html;charset=utf-8"%>
   > <%@ page
   > import="com.businessobjects.bip.core.web.appcontext.RequestInfo"%>
   > <%
   > request.getSession().setAttribute("MySecret","Your generated shared
   > secret content");
   > %>
   > <html>
   > <head>
   > <title></title>
   > </head>
   > <body>
   > <script type="text/javascript" src="noCacheCustomResources/
   > custom.js"></script>
   > <script type="text/javascript">
   > window.location = "logon.faces";
   > </script>
   > </body>
   > </html>
   > ```

10. Сохраните файл.

3. Обновите и закройте архивный файл.
4. После выполнения перечисленных выше шагов в файле `BOE.sca` разверните его в NetWeaver.
5. После успешного развертывания BOE.sca запустите его для проверки (http://<hostname>:<port_number>/nwa).
6. При объявлении базовой аутентификации в `web.xml` вы можете увидеть всплывающее окно браузера для аутентификации.

   Теперь доверительная аутентификация между сервером приложений Java для SAP NetWeaver и платформой BI установлена.

> **Примечание**
>
> Если вы увидели всплывающее окно браузера для аутентификации, выполните следующие шаги:
>
> 1. Войдите на сервер приложений Java для SAP NetWeaver по адресу http://<hostname>:<port_number>/nwa.
> 2. Выберите *Конфигурация* > *Безопасность* > *Аутентификация* > *SSO*
> 3. Определите настройки безопасности приложения BI.
> 4. Включите режим *редактирования*.
> 5. На вкладке *Стек аутентификации* оставьте поле *Используемый шаблон* незаполненным и добавьте *SAML2LoginModule* в стек сверху с флагом *SUFFICIENT*.
> 6. Сохраните изменения и закройте приложение.

9.2.6 Использование аутентификации SAML 2.0 с сервером приложений Java для SAP NetWeaver

Чтобы обеспечить пользователям SAP Web Application Server Java доступ к содержимому платформы SAP Business Intelligence с помощью единого входа (SSO), необходимо установить механизм для авторизации доступа к этим приложениям. Следующие шаги описывают, как можно установить доверительную аутентификацию между SAP Web Application Server Java и Business Intelligence.

Область действия. Область действия этих шагов не предназначена для настройки аутентификации SAML, поскольку IDP для разных поставщиков может отличаться. Сведения о настройке аутентификации SAML см. в документах для конкретных поставщиков.

Настройка включает следующее:

1. Настройка аутентификации SAML на сервере приложений Java для SAP NetWeaver.
2. Настройка доверительной аутентификации для платформы BI.

Для получения дополнительных сведений о включении аутентификации SAML на сервере приложений Java для SAP NetWeaver см. раздел Использование SAML 2.0.

9.2.7 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 входить в систему однократно, 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 (CMC), 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 требуется вход в платформу BI.
> - По соображениям безопасности доверительную аутентификацию не следует включать без HTTPS. Если доверительная аутентификация включена без HTTPS, это считается нарушением безопасности, поскольку URL-адрес отображается для неавторизованных пользователей. Во избежание нарушения безопасности информация пользователя может быть проверена с помощью действительного сертификата. Для получения дополнительных сведений см. 1388240.

Связанные сведения

Настройка сервера на использование доверительной аутентификации [страница 271]
Настройка доверительной аутентификации для веб-приложения [страница 276]

9.2.7.1 Доверительная аутентификация для веб-служб RESTful на веб-сервере

В этом разделе даны инструкции по включению доверительной аутентификации для веб-служб RESTful на веб-сервере.

> ⓘ Примечание
>
> По соображениям безопасности доверительную аутентификацию не следует включать без HTTPS. Если доверительная аутентификация включена без HTTPS, это считается нарушением безопасности, поскольку URL-адрес отображается для неавторизованных пользователей. Во избежание нарушения безопасности информация пользователя может быть проверена с помощью действительного сертификата. Для получения дополнительных сведений см. 1388240.

Чтобы включить доверительную аутентификацию, выполните следующие шаги:

1. Сгенерируйте общий секретный ключ. Для получения дополнительных сведений см. Создание значения общего секретного ключа [страница 425].
2. Сохраните общий секретный ключ в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container\bin` в ОС Windows.

3. Откройте общий секретный ключ в текстовом редакторе.
4. Скопируйте общий секретный ключ.
5. 5. Скопируйте файл biprws.properties из каталога `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps` и вставьте его в каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps \biprws\WEB-INF\config\custom`.
6. Откройте файл *biprws.properties* в текстовом редакторе.
7. Вставьте общий секретный ключ рядом со значением *Trusted_Auth_Shared_Secret=*.
8. Добавьте *Метод извлечения* и *Параметр имени пользователя*. Сведения о добавлении метода извлечения и параметра имени пользователя см. в следующей таблице.

Веб-служба RESTful – свойства конфигурации доверительной аутентификации

Свойство	Описание	Значение по умолчанию
Метод извлечения	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`. • *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	Это метка, использующаяся для идентификации доверенного пользователя при извлечении маркера входа.	**X-SAP-TRUSTED-USER**

9. Сохраните файл *biprws.properties*.
10. Перезапустите веб-сервер.

9.2.7.2 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.

> **Примечание**
>
> По соображениям безопасности доверительную аутентификацию не следует включать без HTTPS. Если доверительная аутентификация включена без HTTPS, это считается нарушением безопасности, поскольку URL-адрес отображается для неавторизованных пользователей. Во избежание нарушения безопасности информация пользователя может быть проверена с помощью действительного сертификата. Для получения дополнительных сведений см. 1388240.

1. Выполните вход в CMC.
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*.

      Клиентом и CMS используется общий секретный ключ для установки доверительных отношений. Сначала следует 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:

      > ⚠ 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.
   g. Если планируется совместно использовать общий секретный ключ посредством файла TrustedPrincipal.conf, а не веб-сеанса, скопируйте этот файл в один из следующих каталогов:
      - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\`
      - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`
5. Нажмите кнопку *Обновить*, чтобы передать в систему общий секретный ключ.

Платформа BI не проверяет все изменения параметров доверительной аутентификации. Необходимо 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.

9.2.8 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`.

> **Примечание**
>
> По соображениям безопасности доверительную аутентификацию не следует включать без HTTPS. Если доверительная аутентификация включена без HTTPS, это считается нарушением безопасности, поскольку URL-адрес отображается для неавторизованных пользователей. Во избежание нарушения безопасности информация пользователя может быть проверена с помощью действительного сертификата. Для получения дополнительных сведений см. 1388240.

9.2.8.1 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.

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**
>
> Пользователи должны либо быть импортированы в платформу BI, либо иметь учетные записи Enterprise.

> **Примечание**
>
> Чтобы этот механизм работал, необходимо включить определенное свойство для WAR-файла BOE: `trusted.auth.user.namespace.enabled`.

9.2.8.2 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`.

> **Примечание**
>
> По соображениям безопасности доверительную аутентификацию не следует включать без HTTPS. Если доверительная аутентификация включена без HTTPS, это считается нарушением безопасности, поскольку URL-адрес отображается для неавторизованных пользователей. Во избежание нарушения безопасности информация пользователя может быть проверена с помощью действительного сертификата. Для получения дополнительных сведений см. 1388240.

Свойство	Значение по умолчанию	Описание
`sso.enabled=true`	`sso.enabled=false`	Включает или отключает единый вход в платформу BI. Чтобы включить доверительную аутентификацию, установите значение `true`.
`trusted.auth.shared.secret`	Нет	Имя переменной сеанса, используемой для извлечения секретного ключа для доверительной аутентификации. Применяется только случае использования веб-сеанса для передачи общего секретного ключа.
`trusted.auth.user.param`	Нет	Задает переменную, используемую для извлечения имени пользователя для доверительной аутентификации.
`trusted.auth.user.retrieval`	Нет	Задает метод, используемый для извлечения имени пользователя для доверительной аутентификации: • `REMOTE_USER` • `HTTP_HEADER` • `COOKIE` • `QUERY_STRING` • `WEB_SESSION` • `USER_PRINCIPAL` Чтобы отключить доверительную аутентификацию, установите пустое значение.

Свойство	Значение по умолчанию	Описание
`trusted.auth.user.namespace.enabled`	Нет	Включает и отключает динамическую привязку псевдонимов к существующим учетным записям. Если этому свойству присвоено значение `true`, 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 свойство пустое, в доверительной аутентификации будет использоваться сопоставление имен при аутентификации пользователей.

9.2.8.3 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 TrustedPrincipal.conf
ОС Windows, каталог установки по умолчанию	• `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\` • `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\`
AIX	`<INSTALLDIR>/sap_bobj/enterprise_xi40/ aix_rs6000/`
Solaris	`<INSTALLDIR>/sap_bobj/enterprise_xi40/ solaris_sparc/`
Linux	`<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x86`

Поддерживаются различные механизмы заполнения переменной имени пользователя, которая используется при настройке доверительной аутентификации для клиента, на котором размещаются веб-приложения. Настройте или установите сервер веб-приложений таким образом, чтобы имена пользователей были доступны перед использованием этих методов извлечения имен пользователей.

Для получения дополнительной информации см. 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:

   `<INSTALLDIR>\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=<User Variable>
trusted.auth.shared.secret=<Secret Variable>
```

   Для свойства `trusted.auth.user.retrieval` выберите один из следующих параметров для извлечения 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 `trusted.auth.user.param`.
`QUERY_STRING`	Имя пользователя извлекается из параметра URL-адреса запроса. Необходимо указать строку запроса, которая будет использоваться в свойстве `trusted.auth.user.param`.
`COOKIE`	Имя пользователя извлекается из указанного cookie-файла. Необходимо указать cookie-файл, который будет использоваться в свойстве `trusted.auth.user.param`.

Параметр	Способ получения имени пользователя
`WEB_SESSION`	Имя пользователя извлекается из содержимого указанной переменной сеанса. Необходимо указать переменную веб-сеанса, которая будет использоваться в свойстве `trusted.auth.user.param` в файле `global.properties`.
`REMOTE_USER`	Имя пользователя извлекается из вызова `HttpServletRequest.getRemoteUser()`.
`USER_PRINCIPAL`	Имя пользователя извлекается путем обращения к методу `getUserPrincipal().getName()` в объекте `HttpServletRequest` для текущего запроса в сервлете или JSP.

→ Рекомендация

При использовании единого входа на базе HTTP_HEADER или QUERY_STRING убедитесь, что конечные пользователи (браузеры) не устанавливают для аутентификации прямое соединение с BOE. Вместо этого SAP рекомендует доступ к BOE для конечных пользователей (браузеров) только черех портал или пользовательское приложение.

ⓘ 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`.

ⓘ Примечание

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*.

9.2.8.3.1 Примеры конфигурации

9.2.8.3.1.1 Передача общего секретного ключа с помощью файла TrustedPrincipal.conf

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\win64_x64`. Пакетная версия Tomcat представляет собой сервер веб-приложений.

1. Создайте новый файл в каталоге `<КАТАЛОГ_УСТАНОВКИ>\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=<Method for user ID retrieval>
trusted.auth.user.param=<User Variable>
```

3. Сохраните файл с именем **`global.properties`**.
4. Найдите файл `custom.jsp` в папке `web` в файле `com.businessobjects.webpath.InfoView.jar`, расположенном по пути `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins`.
5. Вставьте следующий пользовательский JAVA-код в файл `custom.jsp` в файле `com.businessobjects.webpath.InfoView.jar`:

```
<%
//custom Java code
request.getSession().setAttribute("MyUser","<Username>");
%>
```

> ⓘ Примечание
>
> В приведенном выше фрагменте кода переменная <Имя пользователя> должна быть действительным пользователем Enterprise в платформе BI.

6. Перезапустите сервер веб-приложений.
7. 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. Запрос на ввод имени пользователя и пароля отображается только в первый раз. После успешной аутентификации будет автоматически выполнено перенаправление на стартовую панель BI.

9.2.8.3.1.2 Передача общего секретного ключа с использованием переменной веб-сеанса

И сведения о пользователе, и общий секретный ключ хранятся и передаются с помощью переменной веб-сеанса. Откройте сохраненный ранее файл TrustedPrincipal.conf и просмотрите его содержимое. В этом примере конфигурации предполагается использование следующего общего секретного ключа:

```
9ecb0778edcff048edae0fcdde1a5db8211293486774a127ec949c1bdb98dae8e0ea388979edc6577
3841c8ae5d1f675a6bf5d7c66038b6a3f1345285b55a0a7
```

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 в текстовом редакторе новый файл.
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:

   Классическая стартовая панель BI: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp`

   Стартовая панель BI в стиле Fiori: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.FioriBI\web\custom.jsp`

6. Измените содержимое файла и включите в него следующие атрибуты:

   ```
   <%
   //custom Java code
   request.getSession().setAttribute("MySecret","9ecb0778edcff048edae0fcdde1a5db8
   211293486774a127ec949c1bdb98dae8e0ea388979edc65773841c8ae5d1f675a6bf5d7c66038b
   6a3f1345285b55a0a7");
   request.getSession().setAttribute("MyUser","<Username>");
   %>
   ```

   > ⓘ Примечание
   >
   > В приведенном выше фрагменте кода переменная <Имя пользователя> должна быть действительным пользователем Enterprise в платформе BI.

7. Перезапустите сервер веб-приложений.
8. 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://`

`[cmsname]:8080/BOE/BI/custom.jsp`, где [cmsname] – это имя компьютера, где установлен CMS. Запрос на ввод имени пользователя и пароля отображается только в первый раз. После успешной аутентификации будет автоматически выполнено перенаправление на стартовую панель BI.

9.2.8.3.1.3 Передача имени пользователя с использованием принципала

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

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.
2. Откройте файл `server.xml` для Tomcat, по умолчанию находящийся в каталоге `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf\`.
3. Найдите `<Realm className="org.apache.catalina.realm.UserDatabaseRealm"..../>` и измените на следующее значение:

   ```
   Realm className=" org.apache.catalina.realm.UserDatabaseRealm".../
   ```

4. Откройте файл `tomcat-users.xml`, по умолчанию находящийся в каталоге `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf\`.
5. В теге `<tomcat-users>` измените следующее значение:

   ```
   <user name=«JohnDoe» password=«password»
   roles=«onjavauser»/>
   ```

6. Откройте файл `web.xml` в каталоге `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`.
7. 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.

8. 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 платформы BI.

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*.

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 безопасности LDAP, поставляемый с платформой BI, может взаимодействовать с сервером LDAP по протоколу SSL с использованием аутентификации сервера или обоюдной аутентификации. При аутентификации сервера платформа BI использует для подтверждения подлинности сервера имеющийся у сервера LDAP сертификат безопасности; при этом сервер LDAP разрешает подключения от анонимных клиентов. При обоюдной аутентификации используются сертификаты безопасности сервера LDAP и платформы BI, и перед установлением соединения сервер LDAP также обязательно проверяет сертификат клиента.

Подключаемый модуль безопасности LDAP, поставляемый с платформой BI, можно настроить таким образом, чтобы взаимодействие с сервером LDAP осуществлялось по протоколу SSL, а для проверки учетных данных пользователей применялась базовая аутентификация. Перед тем как развертывать 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 .

Связанные сведения

Настройка аутентификации LDAP [страница 284]
Сопоставление групп LDAP [страница 296]

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.

Связанные сведения

Настройка параметров SSL для LDAP-сервера или взаимной аутентификации [страница 288]
Сопоставление LDAP и Windows AD [страница 298]
Настройка подключаемого модуля LDAP для SiteMinder [страница 293]

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 *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 сервер LDAP позволяет выполнять анонимную привязку, оставьте это поле пустым. Серверы и клиенты платформы BI будут выполнять привязку к основному хосту с использованием анонимного входа.
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 хоста, на который настроены ссылки, будет сопоставлена платформе BI.

    > ⓘ Примечание
    >
    > Хотя можно сопоставлять группы с нескольких хостов, настроить можно только один набор учетных данных для ссылок. Поэтому при наличии нескольких хостов для ссылок необходимо создать на каждом хосте учетную запись пользователя с одинаковым характерным именем и паролем.

> **Примечание**
>
> Если параметру *Максимальное количество ссылочных узлов маршрутизации* присвоено значение 0, ссылочные переходы осуществляться не будут.

11. Нажмите *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*
         Данный вариант используется для автоматического создания псевдонима для каждого пользователя LDAP, сопоставленного платформе BI. Новые учетные записи LDAP добавляются для пользователей без учетных записей платформы BI или для всех пользователей, если выбран вариант *Создавать новую учетную запись для каждого добавленного псевдонима LDAP*.
       - *Создавать новые псевдонимы только при входе пользователя в систему*
         Данный вариант используется в случае, когда сопоставляемый каталог LDAP содержит много пользователей, но только некоторые из них будут использовать платформу BI. Система не будет автоматически создавать псевдонимы и учетные записи Enterprise ни для каких пользователей. Вместо этого программа создает псевдонимы (и учетные записи, при необходимости) только для пользователей, которые входят в платформу BI.

    c. 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 человек уже подключено к ней. Для каждой учетной записи, созданной с использованием данного параметра, должна существовать именованная пользовательская лицензия.

  > ⓘ Примечание
  >
  > Число параллельных сеансов входа для именованного пользователя, созданного с использованием пользовательской лицензии, ограничивается 10 сеансами. Если такой именованный пользователь попытается войти в 11-й параллельный сеанс входа, будет выдано соответствующее сообщение об ошибке. Для входа необходимо будет завершить один из текущих сеансов.
  >
  > Однако число параллельных сеансов входа для именованных пользователей, созданных с использованием лицензии на процессор и лицензии на публичные документы, не ограничено.

- *Новые пользователи создаются как параллельные пользователи*
  Новые учетные записи пользователей настраиваются для использования 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 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:
    a. 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.
    b. 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*.

Связанные сведения

Настройка параметров SSL для LDAP-сервера или взаимной аутентификации [страница 288]

Настройка подключаемого модуля LDAP для SiteMinder [страница 293]

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.

> ⓘ Примечание
>
> 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").

Связанные сведения

Настройка аутентификации LDAP [страница 284]

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.

Для систем Windows коммуникация по протоколу SSL по умолчанию осуществляется через TLS 1.2. Для систем Linux – см. в SAP-ноте. 2623529

Связанные сведения

Настройка хоста LDAP [страница 284]

9.3.2.3.1 Настройка аутентификации LDAP-сервера или взаимной аутентификации

Ресурс	Выполните это действие перед переходом к данному заданию.
Сертификат CA	Это действие необходимо как для аутентификации сервера, так и для взаимной аутентификации при использовании SSL. 1. Нужно, чтобы центр сертификации создал сертификат CA. 2. Добавьте сертификат на сервер LDAP. Дополнительные сведения см. в документации поставщика LDAP.
Сертификат сервера	Это действие необходимо как для аутентификации сервера, так и для взаимной аутентификации при использовании SSL. 1. Запросите, а затем создайте сертификат сервера. 2. Авторизовать сертификат и затем добавить его на LDAP-сервер.
cert7.db или cert8.db, key3.db	Эти файлы необходимы как для аутентификации сервера, так и для взаимной аутентификации при использовании SSL. 1. Загрузите приложение certutil, которое создает файл `cert7.db` или `cert8.db` (в зависимости от требований) на основе https://developer.mozilla.org/en-US/docs/NSS/tools . 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`: `certutil -N -d .`

Ресурс	Выполните это действие перед переходом к данному заданию.
	4. Используйте следующую команду, чтобы добавить сертификат CA в файл `cert7.db` или `cert8.db`: `certutil -A -n <CA_alias_name> -t CT -d . -I cacert.cer` 5. Сохраните эти три файла в каталоге на компьютере, где размещена платформа BI.
cacerts	Этот файл необходим для взаимной аутентификации с использованием SSL для приложений Java, таких как стартовая панель BI. 1. Перейдите к своему файлу `keytool` в каталоге `bin` Java. 2. Воспользуйтесь следующей командой для создания файла `cacerts`: `keytool -import -v -alias <CA_alias_name> -file <CA_certificate_name> -trustcacerts -keystore` 3. Сохраните файл `cacerts` в тот же каталог, в котором хранятся файлы `cert8.db` или `cert8.db`, а также файлы `key3.db`.
Сертификат клиента	1. Создайте отдельные клиентские запросы для файла `cert7.db` или `cert8.db` и файлов `.keystore`: • Чтобы настроить подключаемый модуль LDAP, используйте приложение certutil для создания запроса клиентского сертификата. • Используйте следующую команду для создания запроса клиентского сертификата: `certutil -R -s "<client_dn>" -a -o <certificate_request_name> -d .` `<client_dn>` содержит такую информацию, как "CN=`<имя_клиента>`, OU=`<организационное_подразделение>`, O=`<название_компании>`, L=`<город>`, ST=`<регион>`, C=`<страна>`. 2. Используйте CA для аутентификации запроса сертификата. Используйте следующую команду,

Ресурс	Выполните это действие перед переходом к данному заданию.

	чтобы извлечь сертификат и вставить его в файл `cert7.db` или `cert8.db`:
	`certutil -A -n <client_name> -t Pu -d . -I <client_certificate_name>`
	3. Реализация аутентификации Java с помощью SSL:
	• Используйте утилиту keytool в каталоге `bin` Java, чтобы создать запрос клиентского сертификата.
	• Используйте следующую команду, чтобы создать пару ключей:
	`keytool -genkey -keystore .keystore`
	4. После указания сведений о клиенте воспользуйтесь такой командой для создания запроса сертификата клиента:
	`keytool -certreq -file <certificate_request_name> -keystore .keystore`
	5. После аутентификации запроса клиентского сертификата центром сертификации используйте следующую команду, чтобы добавить сертификат CA в файл `.keystore`:
	`keytool -import -v -alias <CA_alias_name> -file <ca_certificate_name> -trustcacerts -keystore .keystore`
	6. Извлеките запрос клиентского сертификата из CA и с помощью следующей команды добавьте его в файл `.keystore`:
	`keytool -import -v -file <client_certificate_name> -trustcacerts -keystore .keystore`
	7. Сохраните файл `.keystore` в тот же каталог, в котором хранится файл `cert7.db` или `cert8.db`, а также файл `cacerts` 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 CMC *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 хостом LDAP (для аутентификации пользователей и групп LDAP), она должна принять сертификат безопасности от хоста LDAP 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 хостом LDAP (для аутентификации пользователей и групп LDAP), она должна принять сертификат безопасности от хоста LDAP и проверить его. Чтобы проверить сертификат, платформа BI должна найти выдавший его центр сертификации 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 в формате **`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. Нажмите кнопку *Готово*.

Связанные сведения

Настройка подключаемого модуля LDAP для SiteMinder [страница 293]

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 CMC *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 пользователей от стороннего производителя, которое можно использовать с подключаемым модулем безопасности LDAP для организации 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.

Связанные сведения

Настройка хоста LDAP [страница 284]

9.3.2.5.1 Установка библиотек ETPKI

Вам следует установить библиотеки ETPKI, чтобы защитить информацию, обмен которой происходит между сервером политик CA Single Sign-on и платформой BI.

Перед установкой библиотек ETPKI необходимо загрузить и установить CA Single Sign-On SDK.

Платформа BI поддерживает только CA Single Sign-on 12.x. Если установлена более ранняя версия CA Single Sign-On, ранее называвшегося CA Siteminder, следует выполнить обновление до версии 12.x.

1. Перейдите к `<CA Single Sign-On_INSTALLDIR>\CA\sdk\etpki-install-64` для 64-разрядной и `<CA Single Sign-On_INSTALLDIR>\CA\sdk\etpki-install` для 32-разрядной операционной системы.

   > ⓘ Примечание
   >
   > Если установка CA Single Sign-On не выполнена на компьютере, где установлена платформа BI, скопируйте библиотеки ETPKI на тот же компьютер.

2. Установите библиотеки ETPKI в среде Linux:
   a. Войдите с правом доступа к корневым каталогам и выполните команду `./setup install caller=sdk veryverbose`.
      Сообщение об успешной установке отображается в конце консоли или установки.
   b. Выполните команды `export CAPKIHOME=/opt/CA/SharedComponents/CAPKI` и `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<BOE_INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64/`, чтобы задать путь как каталог установки с пользователем платформы BI.
   c. Перезапустите *Server Intelligence Agent*.
3. Установите библиотеки ETPKI в среде Windows:
   a. Запустите командную строку с полномочиями администратора из местоположения библиотеки ETPKI.

b. Выполните команду `setup.exe install caller=sdk veryverbose`.
c. Проверьте наличие сообщения об успешной установке в файле *capki_install.log* в папке *%temp%*.
d. Перезапустите *Server Intelligence Agent*.

Библиотеки ETPKI успешно установлены.

9.3.2.5.2 Настройка LDAP на использование единого входа с SiteMinder

1. Откройте окно *Задайте 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.

9.3.2.5.3 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 с группами 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 с платформой BI.

> ⓘ Примечание
>
> Также можно назначить группы Windows AD таким образом, чтобы аутентификация в платформе BI выполнялась через подключаемый модуль безопасности LDAP.

> ⓘ Примечание
>
> В ходе настройки LDAP с AD процедура выполнит сопоставление групп AD.

9.3.3.1 Сопоставление групп LDAP с использованием платформы BI

1. Перейдите в область управления CMC *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.

     > **Примечание**
     >
     > Число параллельных сеансов входа для именованного пользователя, созданного с использованием пользовательской лицензии, ограничивается 10 сеансами. Если такой именованный пользователь попытается войти в 11-й параллельный сеанс входа, будет выдано соответствующее сообщение об ошибке. Для входа необходимо будет завершить один из текущих сеансов.
     >
     > Однако число параллельных сеансов входа для именованных пользователей, созданных с использованием лицензии на процессор и лицензии на публичные документы, не ограничено.

   - *Новые пользователи создаются как параллельные пользователи*
     Новые учетные записи пользователей настраиваются для использования 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 системой, лицензия на одновременный доступ для 100 пользователей может поддерживать 250, 500 или 700 пользователей.

7. Нажмите кнопку *Обновить*.

9.3.3.2 Отмена сопоставления групп LDAP с использованием платформы BI

1. Перейдите в область управления CMC *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 доверительная 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	Сопоставление можно осуществлять со следующими элементами: • Универсальные группы в дочернем домене • Группы в этом же домене, которые содержат универсальные группы из дочернего домена • Универсальные группы в кросс-домене Сопоставление нельзя осуществлять со следующими элементами: • Глобальные группы в дочернем домене • Локальные группы в дочернем домене • Группы из того же домена, который содержит глобальную группу дочернего домена • Междоменные глобальные группы 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.
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 `bin` и `lib` в переменные среды `PATH` и `LD_LIBRARY_PATH`.
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 <username>base.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 <sianame>, 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.
`-pass`	Задает пароль, используемый учетной записью службы.

Параметр	Описание
`-ptype`	Задает тип администратора доступа: `-ptype KRB5_NT_PRINCIPAL`
`-crypto`	Задает используемый для учетной 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/kerb5.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 principal08/10/11 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 CMC *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

`<sianame>`	Имя агента Server Intelligence
`<служба>`	Имя учетной записи службы, используемой для работы платформы BI
ИМЯ_СФЕРЫ_DNS	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 принципала 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.

Связанные сведения

Настройка аутентификации LDAP [страница 284]

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 в другом месте. Однако при этом его местоположение 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="<имя принципала>";
};
```

> **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="<имя принципала>";
> };
> ```

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.

Связанные сведения

Настройка аутентификации LDAP [страница 284]
Сопоставление групп LDAP [страница 296]

9.4 Аутентификация Windows AD

9.4.1 Использование аутентификации Windows AD

9.4.1.1 Требования к поддержке Windows AD и начальная 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.

> **Примечание**
>
> Дополнительную информацию о настройке аутентификации Windows AD см. в базе знаний SAP KBA 1631734 по адресу https://service.sap.com/sap/support/notes/1631734.

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.
- 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 пользовательскую аутентификацию AD на платформе BI, воспользуйтесь следующим рабочим процессом:

1. Настройте контроллер домена.
2. Настройте аутентификацию AD в CMC.
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 -s`, 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 –s BICMS/service_account_name.domain.com serviceaccountname
   setspn -s HTTP/<servername> <servicename>
   setspn -s HTTP/<servername.domain.com> <servicename>
   setspn -s HTTP/<ip address of server> <servicename>
   ```

   `BICMS`— это имя компьютера, на котором запущен SIA, `<имя_сервера>`— имя сервера, на котором развернута стартовая панель BI, а `<имя_сервера.домен>`— 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>.@example.com
   HTTP/<servername>
   <servername>/<servicename>@example.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@example.com
           HTTP/Tomcat HTTP/Tomcat@example.com
           HTTP/Load_Balancer.@example.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 CMC

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 Windows AD функционирует, 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.

  > ⓘ Примечание
  >
  > Настройка проведена и проверена с использованием только SUSE linux Enterprise 11.

- Подключаемый модуль Windows AD для платформы BI поддерживает домены в нескольких лесах.

9.4.3.2 Сопоставление пользователей и групп Windows 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.

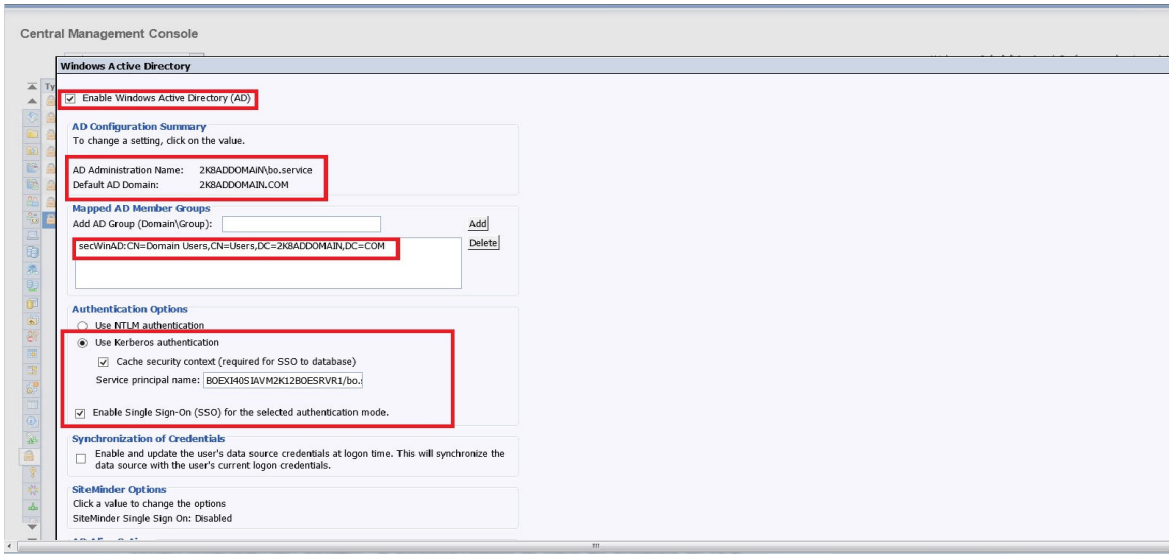
  > ⓘ Примечание
  >
  > Чтобы реализовать аутентификацию AD с функцией единого входа Vintela (SSO), необходимо предоставить специально настроенное для этой цели имя администратора доступа к службе (SPN). Далее приведены шаги по настройке пользовательской аутентификации AD для платформы BI. После настройки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

Чтобы импортировать группы AD на платформу BI, необходимо выполнить шаги с 1 по 11.

1. Перейдите в область управления CMC *Аутентификация*.
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 Керберос, 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=GroupName, ....., dc=DomainName, dc=com`)

   > ⓘ Примечание
   >
   > Если требуется сопоставить локальную группу, можно использовать только формат имени NT: `\\<имя_сервера>\<имя_группы>`. 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. Выберите *Добавить*.

   Группа добавлена в список в разделе *Сопоставленные группы-участники AD*

9. В области *Отображенные группы элементов AD* введите домен/группу AD в поле *Поиск в группе AD (домен\группа)*.

   Нужная группа будет найдена в списке. Также можно выбрать *Показать*, чтобы просмотреть полный список групп AD в отдельном диалоговом окне.

10. В пункте *Параметры аутентификации* выберите *Использовать аутентификацию Kerberos*.
11. В поле *Имя администратора доступа к службе* введите имя принципала 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 принципала службы. Пример: `BICMS/bossosvcacct.domain.com`.

12. Нажмите кнопку *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 обновления групп AD, то шаги с 12 по 19 можно пропустить. Эти необязательные параметры можно настроить после успешной настройки неавтоматической аутентификации AD с использованием Kerberos.

13. 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.

14. Если для текущей настройки аутентификации AD требуется SSO, то выберите *Включить единый вход для выбранного режима аутентификации*.

15. 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.

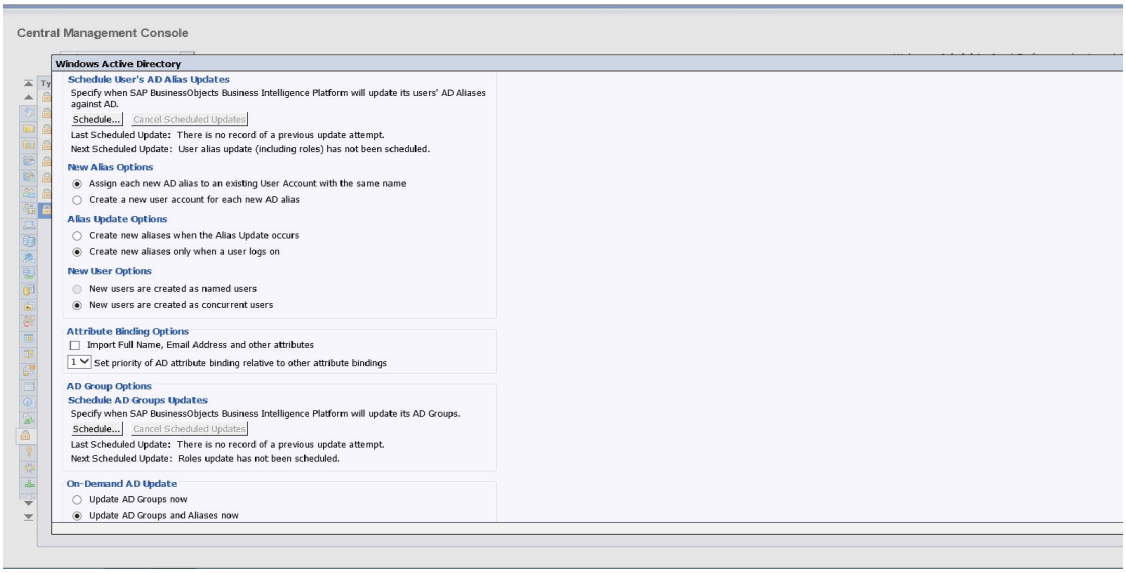
16. В области *Параметры псевдонима AD*укажите способ добавления и обновления новых псевдонимов в платформе BI.

    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 параметр 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*
         Этот параметр используется в том случае, когда сопоставляемый каталог AD содержит много пользователей, но только некоторые из них будут 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. 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.

  > **Примечание**
  >
  > Число параллельных сеансов входа для именованного пользователя, созданного с использованием пользовательской лицензии, ограничивается 10 сеансами. Если такой именованный пользователь попытается войти в 11-й параллельный сеанс входа, будет выдано соответствующее сообщение об ошибке. Для входа необходимо будет завершить один из текущих сеансов.
  >
  > Однако число параллельных сеансов входа для именованных пользователей, созданных с использованием лицензии на процессор и лицензии на публичные документы, не ограничено.

- *Новые пользователи создаются как параллельные пользователи*
  Новые учетные записи пользователей настраиваются для использования 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 системой, лицензия на одновременный доступ для 100 пользователей может поддерживать 250, 500 или 700 пользователей.

17. Для настройки способа обновления псевдонимов AD щелкните *Запланировать*.
    a. В диалоговом окне *Расписание* выберите в списке *Запустить объект* тип повторения.
    b. Задайте оставшиеся необходимые параметры планирования.

c. Нажмите кнопку *Расписание*.
   При обновлении псевдонимов также обновляются данные групп.

18. В области *Параметры привязки атрибутов* можно указать приоритет привязки атрибутов для подключаемого модуля AD:
    a. 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.
    b. 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. Для привязок следует установить разные значения. Одно значение привязки для нескольких подключаемых модулей аутентификации может привести к нежелательным результатам.
19. В области *Параметры групп AD* настройте обновления групп AD:
    a. Нажмите кнопку *Расписание*.
       Откроется диалоговое окно *Расписание*.
    b. В списке *Запустить объект* выберите тип повторения.
    c. Задайте другие необходимые параметры планирования.
    d. Нажмите кнопку *Расписание*.

    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.
20. 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.
21. Нажмите кнопку *Обновить*, а затем нажмите *OK*.

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

Связанные сведения

Создание файла конфигурации Kerberos [страница 320]

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. CMC 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. Указывается время начала, а также дата начала и дата 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 выполняться 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-й день N-й 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 CMC. 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 входит в систему.
- Администратор выбирает параметр *Обновить группы и псевдонимы AD сейчас* в области CMC *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:

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

Чтобы предоставить пользователю определенные права, выполните следующие шаги:

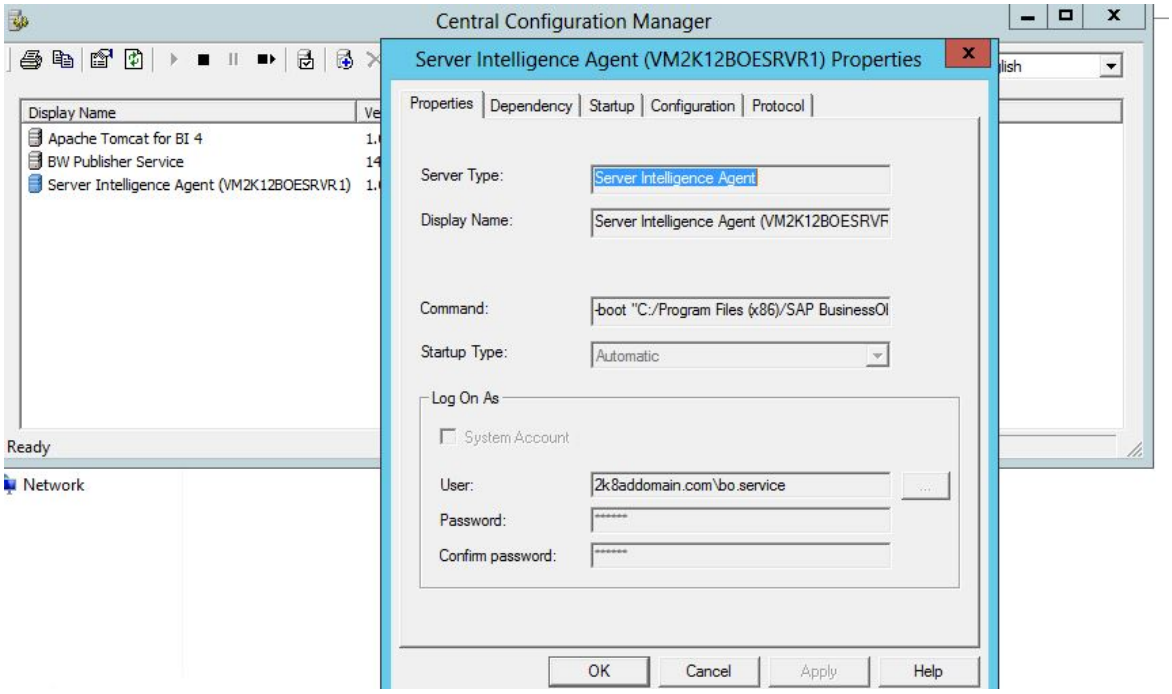
1. Выберите *Пуск > Панель управления > Администрирование > Локальная политика безопасности*.
2. Разверните узел *Локальные политики*, а затем выберите *Назначение прав пользователя*.
3. Дважды щелкните пункт *Работа в режиме операционной системы*.
4. Щелкните *Добавить* и введите имя созданной учетной записи службы, а затем нажмите кнопку *OK*.

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 *Остановить*.

   > **Примечание**
   >
   > При остановке агента SIA останавливаются все службы, которыми он управляет.

3. Щелкните SIA правой кнопкой мыши и выберите *Свойства*.



4. Снимите флажок *Системная учетная запись*.
5. Введите данные учетной записи службы (`<ИМЯ_ДОМЕНА>\<имя_службы>`) и нажмите кнопку *OK*.

   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 систему в качестве службы».
   - Права полного доступа к папке, в которой установлена платформа BI.
   - Права полного доступа к разделу «HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects» в системном реестре.
6. 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.
7. Перезапустите SIA.
8. При необходимости повторите шаги 1 – 5 для каждого агента SIA, управляющего службой, которую требуется настроить.

После этого получите 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* > *CMC* > *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

9.4.5.1.1.1 Создание файла конфигурации Kerberos

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

- Создать учетную запись службы для платформы BI на контроллере домена.
- Убедитесь, что имена принципалов службы (SPN) добавлены в учетную запись службы.
- Сопоставить группы пользователей AD с платформой 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`

   > **Примечание**
   >
   > Этот файл можно сохранить в другом месте. Однако его местоположение необходимо будет указать в параметрах java. Для получения дополнительной информации о `krb5.ini` см. 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 хоста 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]` значение `default_realm` может соответствовать любому 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 CMC. Как и в приведенном примере, имена всех доменов должны быть введены в верхнем регистре.

9.4.5.1.2 Создание файла конфигурации входа JAAS

9.4.5.1.2.1 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.

9.4.5.1.2.2 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`.

9.4.5.1.2.3 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.

9.4.5.1.2.4 Добавление LoginModule для SAP NetWeaver AS

Для использования единого входа Kerberos и SAP NetWeaver AS 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 AS 7.3.

Для правильного сопоставления `com.sun.security.auth.module.Krb5LoginModule` и `com.businessobjects.security.jgss.initiate` нужно вручную добавить LoginModule в SAP NetWeaver AS 7.3.

1. Откройте "Администратор" SAP NetWeaver с помощью ввода следующего адреса в веб-браузере: `http://<имя_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*.
   SAP 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 "Администратора" SAP NetWeaver.

9.4.5.1.3 Изменение настроек Java сервера приложений для загрузки файлов конфигурации

9.4.5.1.3.1 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.

9.4.5.1.3.2 Изменение параметров Java для SAP NetWeaver AS 7.3

1. Перейдите к инструменту конфигурации Java (по умолчанию расположен в каталоге `C:\usr\sap\<идентификатор_NetWeaver>\<экземпляр>\j2ee\configtool\`) и дважды щелкните файл `configtool.bat`.
   Открывается инструмент конфигурации.
2. Нажмите *Вид* > *Экспертный режим*.
3. Разверните *Данные кластера* > *Шаблон*.
4. Выберите экземпляр, соответствующий серверу SAP NetWeaver AS (например, *Instance* - `<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 krb5.ini 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 SAP NetWeaver AS.

9.4.5.1.3.3 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.

9.4.5.1.3.4 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.
   1. Прокрутите страницу сервера вниз до пункта *Process Definition* (определение процесса) в столбце *Additional Properties* (дополнительные свойства).
   2. Щелкните *Process Definition* (определение процесса).
   3. Прокрутите окно вниз и щелкните *Java Virtual Machine* (виртуальная Java-машина).

   Если используется WebSphere 6.0, для перехода на страницу *JVM* выполните следующие шаги.
   1. На странице сервера выберите *Java and Process Management* (управление Java и процессами).
   2. Выберите *Process Definition* (определение процесса).
   3. 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 <имя пользователя>`.
3. Нажмите клавишу `Enter`.
4. Введите пароль.

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0
\win64_x64\jdk\bin>kinit sfredell
Password for sfredell@VTIAUTH08.COM: password
New ticket is stored in cache file C:\Users\Administrator\krb5cc_Administrator
```

   Если файл `krb5.ini` настроен правильно и модуль входа Java загружен, 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 контроллере домена 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 каталог `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.

   > ⓘ 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 необходимо вручную войти в стартовую панель BI, получить доступ к приложению и выбрать Windows AD в списке параметров аутентификации.

> ⓘ 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 единого входа

9.4.6.1 SSO в платформу BI с аутентификацией AD

Параметры SSO при использовании Windows AD

На платформе BI поддерживается три 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 авторизированным 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 базам 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 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 CMC параметры аутентификации Windows AD с использованием функции единого входа.
4. Настроить общие 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 принципала 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 принципала 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 принципала, используемого для учетной записи службы, в формате SPN:`<MYSIAMYSERVER>/<sbo.service.domain.com>@<DOMAIN>.COM`, где `<MYSIAMYSERVER>` — 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 `Ldp.exe`.
`-pass`	Задает пароль, используемый учетной записью службы.

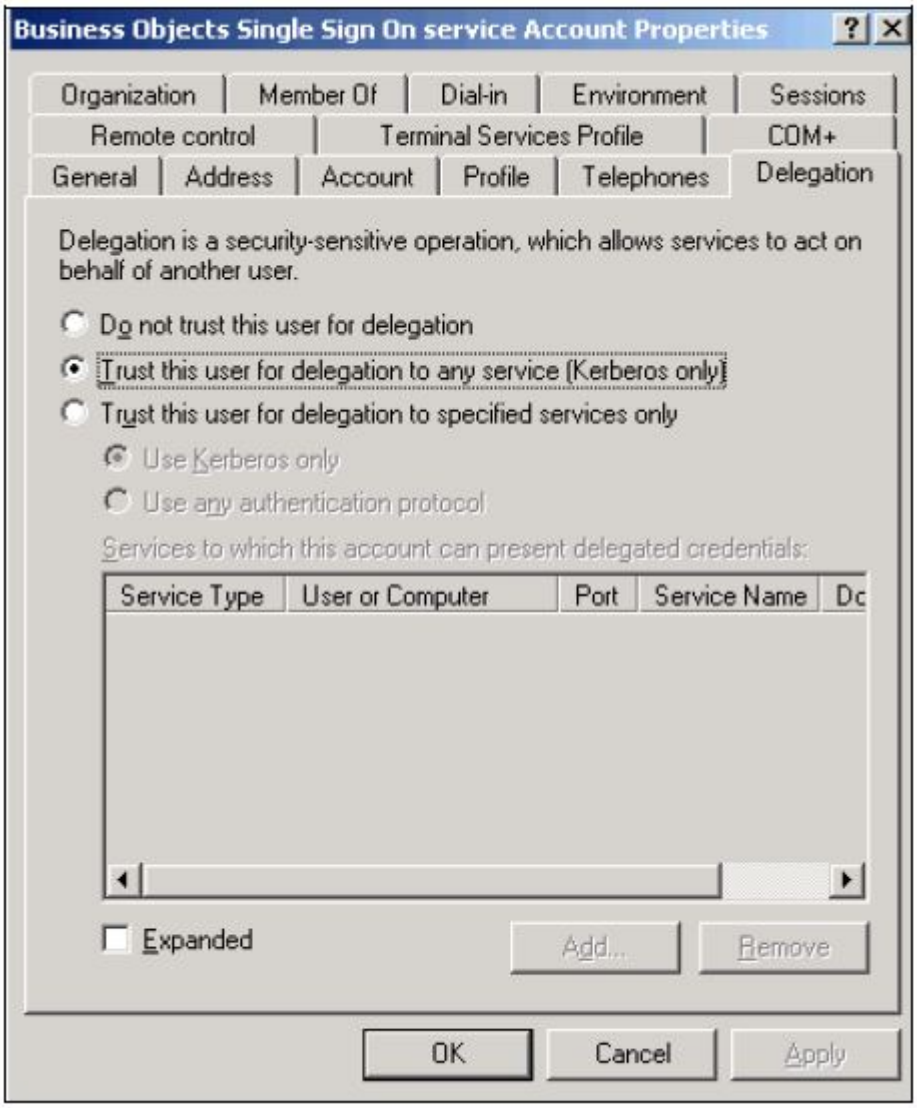
Параметр	Описание
`-ptype`	Задает тип администратора доступа: `-ptype KRB5_NT_PRINCIPAL`
`-crypto`	Задает используемый для учетной записи службы тип шифрования: `-crypto RC4-HMAC-NT`

Пример:

```
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 *OK*, 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.

> ⓘ Примечание
>
> Применимо для сквозного единого входа или для единого входа в базу данных с помощью сценариев файла ярлыков ключей.
>
> В случае сбоев, исправленных заменой KVNO в файле ярлыков ключей, значение атрибута KVNO в учетной записи службы может превышать значение KVNO, использованное при создании файла ярлыков ключей (с помощью ktpass). Для получения сведений о том, как исправить KVNO, см. http://service.sap.com/sap/support/notes/1853668

9.4.6.2.2.1 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 *OK*.
   Отображается список служб.
7. Выберите следующие службы и нажмите кнопку *OK*.
   - 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 приступать 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 выполнять в каталоге `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.

> **Примечание**
>
> 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.

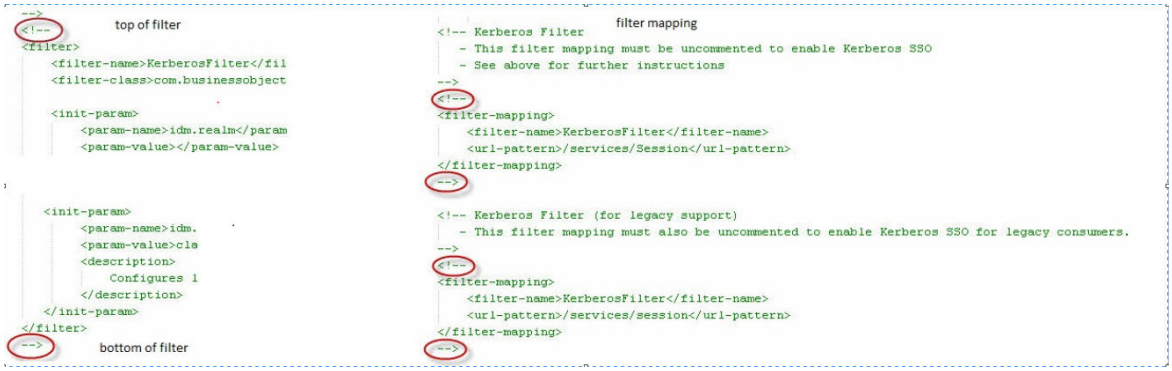
Новые свойства вступают в силу только после повторного развертывания веб-приложения BOE на компьютере, на котором запущен сервер веб-приложений. Воспользуйтесь WDeploy для повторного развертывания BOE на сервере веб-приложений. Для получения дополнительных сведений об использовании Wdeploy для отмены 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. Подробную информацию см. в соответствующей SAP-ноте по адресу: http://service.sap.com/sap/support/notes/1646920

1. Создайте резервную копию этого файла: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\web.xml`, затем откройте его для редактирования.
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 `<КАТАЛОГ_УСТАНОВКИ>\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 `<КАТАЛОГ_УСТАНОВКИ>\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 этого файла: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\classes\dsws.properties`, затем откройте его для редактирования
5. Установите для параметра kerberos.sso значение **`true`** и сохраните файл.

```
68  allowedOrderBy = SI_CREATION_TIME,SI_KIND,SI_LAST_RUN_TIME,SI_SCHEDULEINFO.SI_SUBMITTER,SI_OWNER
69
70  ##############################
71  # Kerberos SSO Properties #
72  ##############################
73  #Set this value to true and activate the Vintela Authentication Filter (in web.xml) to enable SSO via Kerberos
74  kerberos.sso=true
75
76  #Setting this value to true if user wants trusted authentication
77  trustedAuthentication.enabled = false
```

kerberos SSO setting

6. Используйте Wdeploy, чтобы повторно развернуть WAR-файл 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>/dswsbobje/services/Session`.

    Пример: `http://BI4:8080/dswsbobje/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 *OK*.

9.4.6.2.6 Включение единого входа Vintela для веб-служб RESTful

Некоторые клиентские инструменты требуют аутентификации через веб-службы RESTful. Выполните следующие действия, чтобы включить единый вход (SSO) для веб-служб.

1. Скопируйте файл `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\biprws.properties` в `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps \biprws\WEB-INF\config\custom\biprws.properties` и откройте его для редактирования.
2. Чтобы включить Kerberos SSO для аутентификации Windows Active Directory (secWinAD), задайте для параметра `sso.enabled` значение `true`. См. следующий снимок экрана:

```
# ------------------------------------------------------ SSO Related Default Global Core Web Properties ------------------------------------------------------
# Vintela single sign on properties
sso.enabled=
idm.realm=
idm.princ=
idm.keytab=
idm.allowUnsecured=
idm.allowNTLM=
idm.logger.name=
idm.logger.props=
```

   Укажите следующие обязательные параметры:
   - `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 `<КАТАЛОГ_УСТАНОВКИ>\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 `<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).
   - Если SSL не используется с сервером приложения Java, для параметра `idm.allowUnsecured` должно быть задано значение `true`. Дополнительные сведения о Tomcat SSL см. в *статье базы знаний с идентификатором 1484802*
3. 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*.
4. Перезапустите Tomcat.
5. Чтобы протестировать настройки, на компьютере клиента откройте любой браузер и запустите URL-адрес: http://<WebAppServer>:<portnumber>/biprws/v1/logon/adsso.
   Как реакция на API должен появиться маркер REST.

9.4.6.2.7 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.

9.4.6.2.8 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.

9.4.6.2.8.1 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 *OK*, 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.

9.4.6.2.8.2 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.

9.4.6.2.9 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 развертываемой 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.

9.4.6.2.10 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.

9.4.6.2.10.1 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 пользователей от стороннего производителя, которое можно использовать с подключаемым модулем безопасности LDAP для организации 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.

9.4.6.3.1.1 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*.

9.4.6.3.1.2 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 CMC *Аутентификация*.
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 принципала 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 *OK*.
   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 параметр 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*
        Этот параметр используется в том случае, когда сопоставляемый каталог AD содержит много пользователей, но только некоторые из них будут 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 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.

        > **Примечание**
        >
        > Число параллельных сеансов входа для именованного пользователя, созданного с использованием пользовательской лицензии, ограничивается 10 сеансами. Если такой именованный пользователь попытается войти в 11-й параллельный сеанс входа,

> будет выдано соответствующее сообщение об ошибке. Для входа необходимо будет завершить один из текущих сеансов.
>
> Однако число параллельных сеансов входа для именованных пользователей, созданных с использованием лицензии на процессор и лицензии на публичные документы, не ограничено.

- *Новые пользователи создаются как параллельные пользователи*
  Новые учетные записи пользователей настраиваются для использования 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 системой, лицензия на одновременный доступ для 100 пользователей может поддерживать 250, 500 или 700 пользователей.

10. Для настройки способа обновления псевдонимов AD щелкните *Запланировать*.
    a. В диалоговом окне *Расписание* выберите в списке *Запустить объект* тип повторения.
    b. Задайте оставшиеся необходимые параметры планирования.
    c. Нажмите кнопку *Расписание*.
    При обновлении псевдонимов также обновляются данные групп.
11. В области *Параметры привязки атрибутов* можно указать приоритет привязки атрибутов для подключаемого модуля AD:
    a. 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.
    b. 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. Для привязок следует установить разные значения. Одно значение привязки для нескольких подключаемых модулей аутентификации может привести к нежелательным результатам.
12. В области *Параметры групп AD* настройте обновления групп AD:
    a. Нажмите кнопку *Расписание*.
    Откроется диалоговое окно *Расписание*.
    b. В списке *Запустить объект* выберите тип повторения.
    c. Задайте другие необходимые параметры планирования.
    d. Нажмите кнопку *Расписание*.

    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 *OK*.

9.4.6.3.1.3 Отключение SiteMinder

Если требуется запретить настройку SiteMinder или отключить его после настройки в CMC, измените файл конфигурации сети для стартовой панели BI.

9.4.6.3.1.3.1 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).

```
<Каталог_установки>\SAP BusinessObjects Enterprise XI
4.0\win64_64\jdk\bin\servact@TESTM03.COM Password
```

Например:

```
C:\Program Files\SAP BusinessObjects\
 SAP BusinessObjects 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 удается успешно выполнить вход в CMC 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 выполнять 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 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 квитанции входа Enterprise Portal в системах SAP.
- Это облегчает создание учетной записи, так как позволяет сопоставлять роли в SAP группам пользователей в платформе BI, а также облегчает управление учетными записями, за счет согласованного назначения пользователям и группам прав 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 нужны для подключения платформы BI к вашей 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

Объект авторизации	Поле	Значение
	Имя защищаемого RFC (RFC_NAME)	BDCH, STPA, SUSO, BDL5, SUUS, SU_USER, SYST, SUNI, RFC1, SDIFRUNTIME, PRGN_J2EE, /CRYSTAL/SECURITY
	Тип защищаемого объекта RFC (RFC_TYPE)	Группа функций (FUGR)
Поддержка основной записи пользователя: Группы пользователей (S_USER_GRP)	Действие (ACTVT)	Создать или сгенерировать, затем отобразить (03)
	Группа пользователей на экране поддержки основной записи пользователя (CLASS)	* **Примечание** В целях повышения безопасности можно непосредственно перечислить группы пользователей, членам которых необходим доступ к платформе BI.

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.

Примечание

Если в среде ABAP активированы определенные расширения производительности, могут потребоваться дополнительные полномочия для объекта S_RFC. Эти ошибки будут отображаться на странице "Импорт роли" с указанием функции, для которой не удалось найти полномочия.

Пример: Нет полномочий RFC для функционального модуля RFC_METADATA_GET.

Объект авторизации	Поле	Значение
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 и RFC_METADATA
	Тип защищаемого объекта RFC (RFC_TYPE)	Группа функций (FUGR)

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 выполняет аутентификацию пользователей SAP.

9.5.3.1 Добавление системы контроля полномочий SAP

1. Перейдите в область управления CMC *Аутентификация*.
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 SAP-систему.
   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 конфигурация балансировка загрузки, при которой платформа BI должна подключаться через сервер сообщений.

   > ⓘ Примечание
   >
   > Необходимо сделать соответствующие записи в файле **Службы** на компьютере с платформой 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 настроена (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. Нажмите кнопку *Обновить*.

Если добавлено несколько систем контроля полномочий, откройте 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).

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 полномочий 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 ссылку *SAP* и затем выберите вкладку *Параметры*.
3. Просмотрите и при необходимости измените следующие параметры:

Параметр	Описание
Включить аутентификацию SAP	Снимите этот флажок, чтобы отключить аутентификацию SAP. **Примечание** Чтобы отключить аутентификацию SAP для конкретной системы SAP, установите соответствующий этой системе флажок *Отключена* на вкладке *Системы контроля полномочий*.
Корневая папка содержимого	Укажите место, с которого платформа BI должна начинать тиражирование структуры папки BW, в консоли CMC и на стартовой панели BI. По умолчанию это `/SAP/2.0`, однако можно указать и другую папку. Если требуется изменить значение, это нужно сделать и на центральной консоли управления, и на рабочей панели администрирования содержимого.
Система по умолчанию	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 SAP-систему. **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

Параметр	Описание
	выполнить вход как пользователь user1 при использовании аутентификации SAP.
Макс. число неудачных попыток доступа к системе контроля полномочий	Укажите, сколько раз платформа BI должна предпринимать попытки связаться с системой SAP для выполнения запросов аутентификации. 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. **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.
Отключить систему контроля полномочий [сек]	Укажите, сколько секунд платформа BI должна подождать, прежде чем возобновлять попытки выполнить аутентификацию пользователей в SAP-системе. 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 SAP-системе. Если четвертая попытка также завершается неудачей, система делает перерыв в попытках аутентифицировать пользователей в этой системе на указанное время.
Макс. число параллельных соединений на систему	Укажите, сколько открытых соединений необходимо одновременно оставлять открытыми в системе SAP. Например, если указать значение 2, платформа BI оставляет для SAP открытыми 2 соединения.
Число использований на соединение	Укажите, сколько операций можно разрешить выполнять системе SAP на одно соединение. Например, если в качестве значения параметра *Макс. число параллельных соединений на систему* указано 2, а параметра *Число пользователей на соединение* – значение 3, то по достижении трех попыток входа

Параметр	Описание
	по одному соединению платформа BI закрывает и перезапускает это соединение.
Параллельные пользователи и *Зарегистрированные пользователи*	Укажите, какой тип лицензий будет использоваться для новых учетных записей пользователей: лицензии на одновременный доступ или пользовательские лицензии. 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 системой, лицензия на одновременный доступ для 100 пользователей может поддерживать 250, 500 или 700 пользователей. Пользовательские лицензии связаны с пользователями. Они позволяют осуществлять доступ в систему с использованием имени пользователя и пароля. Это дает зарегистрированным пользователям право доступа к системе независимо от того, сколько человек уже подключено к ней. **ⓘ Примечание** Число параллельных сеансов входа для именованного пользователя, созданного с использованием пользовательской лицензии, ограничивается 10 сеансами. Если такой именованный пользователь попытается войти в 11-й параллельный сеанс входа, будет выдано соответствующее сообщение об ошибке. Для входа необходимо будет завершить один из текущих сеансов. Однако число параллельных сеансов входа для именованных пользователей, созданных с использованием лицензии на процессор и лицензии на публичные документы, не ограничено. **ⓘ Примечание** Выбираемый вариант не меняет число или тип лицензий, установленных на платформе BI. В

Параметр	Описание
	системе должны быть доступны подходящие лицензии.
Импорт полного имени, адреса электронной почты и других атрибутов	Укажите уровень приоритетности подключаемого модуля аутентификации SAP. Полные имена и описания, используемые в учетных записях SAP, импортируются и сохраняются в пользовательских объектах в платформе BI.
Установка приоритета для привязки атрибута SAP относительно других привязок атрибутов	Задает приоритет для привязки атрибутов пользователя SAP (полное имя и адрес электронной почты). Если задано значение 1, в сценариях, в которых включены SAP и другие подключаемые модули (Windows AD и LDAP), приоритет имеют атрибуты SAP. Если задано значение 3, приоритет имеют атрибуты из других подключаемых модулей. Для привязок следует установить разные значения. Одно значение привязки для нескольких подключаемых модулей аутентификации может привести к нежелательным результатам.

Задайте значения следующих параметров, чтобы настроить службу единого входа SAP:

Параметр	Описание
Идентификатор системы	Системный идентификатор, предоставляемый платформой BI в SAP-систему при выполнении службы единого входа SAP.
Обзор	Щелкните, чтобы отправить файл `keystore`, 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 `keystore`.
Пароль личного ключа	Укажите пароль, необходимый для доступа к сертификату, соответствующему файлу `keystore`. Этот сертификат хранится в SAP-системе.
Псевдоним личного ключа	Укажите псевдоним, необходимый для доступа к файлу `keystore`.

4. Нажмите кнопку *Обновить*.

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 узел *Доступные системы* и двойным щелчком мыши выберите систему, к которой подключена платформа BI.
7. Откройте вкладку *Макет*, затем в разделе *Базовая папка 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 участникам 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* CMC. Эти группы можно также использовать для определения параметров 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.

9.5.5.1 Чтобы выполнить импорт ролей SAP

1. Перейдите в область управления *Аутентификация* CMC.
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 приступать к выполнению этой задачи, запомните или запишите имя пользователя и пароль пользователя SAP, который относится к одной из ролей, сопоставленных платформе BI.

1. Для стартовой панели BI Java перейдите по ссылке **`http://<веб-сервер>:<номер_порта>/BOE/BI`**.

   Замените `<webserver>` именем веб-сервера, а `<portnumber>` – номером порта для 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 SAP 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:

- Обновить 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 имеются проблемы с использованием системных ресурсов. Если обновляются только роли SAP, новых учетных записей создано не будет.
- Обновить роли и псевдонимы: этот вариант позволяет обновить не только ссылки между ролями, но также создать 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 этом разделе описывается процесс настройки SNC в рамках процесса настройки аутентификации SAP для платформы BI.

Подробнее см. SAP-ноту 1396213.

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.

Связанные сведения

Общие сведения о настройке доверительных параметров сервера SAP [страница 361]

9.5.6.1 Общие сведения о настройке доверительных параметров сервера SAP

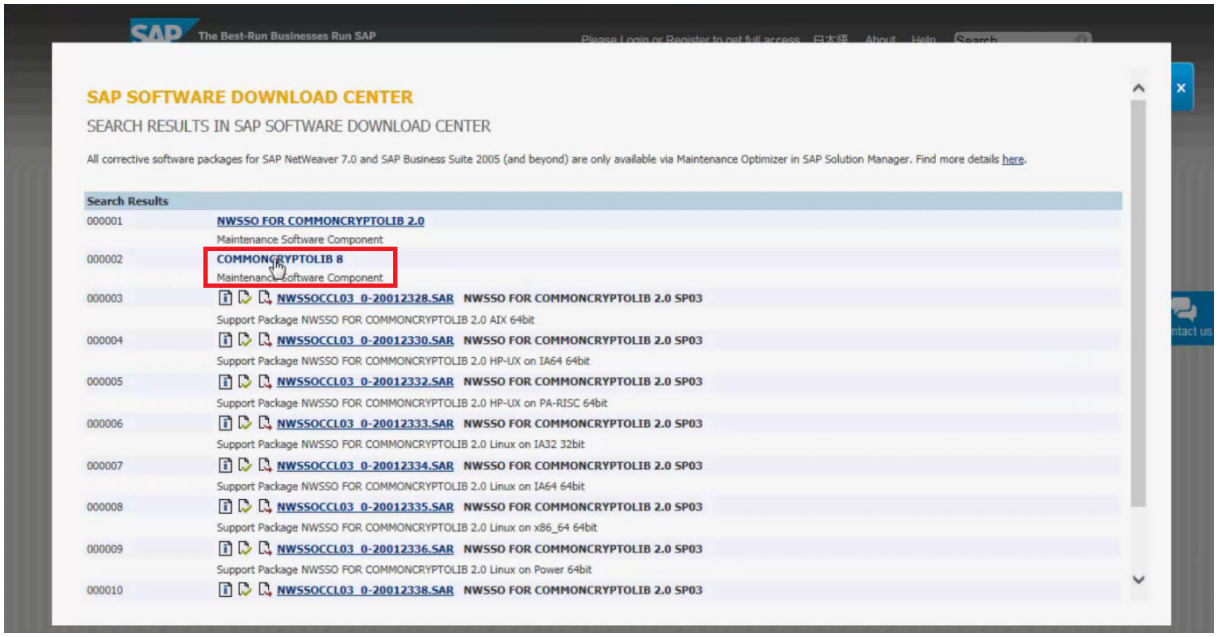
В этом разделе описан процесс настройки параметров доверия между серверами веб-приложений SAP (версии 6.20 и выше) и платформой SAP BusinessObjects Business Intelligence. Настраивать доверительные параметры со стороны сервера нужно в случае использования многопроходной пакетной передачи отчета (для публикаций, где запрос отчета зависит от контекста пользователя).

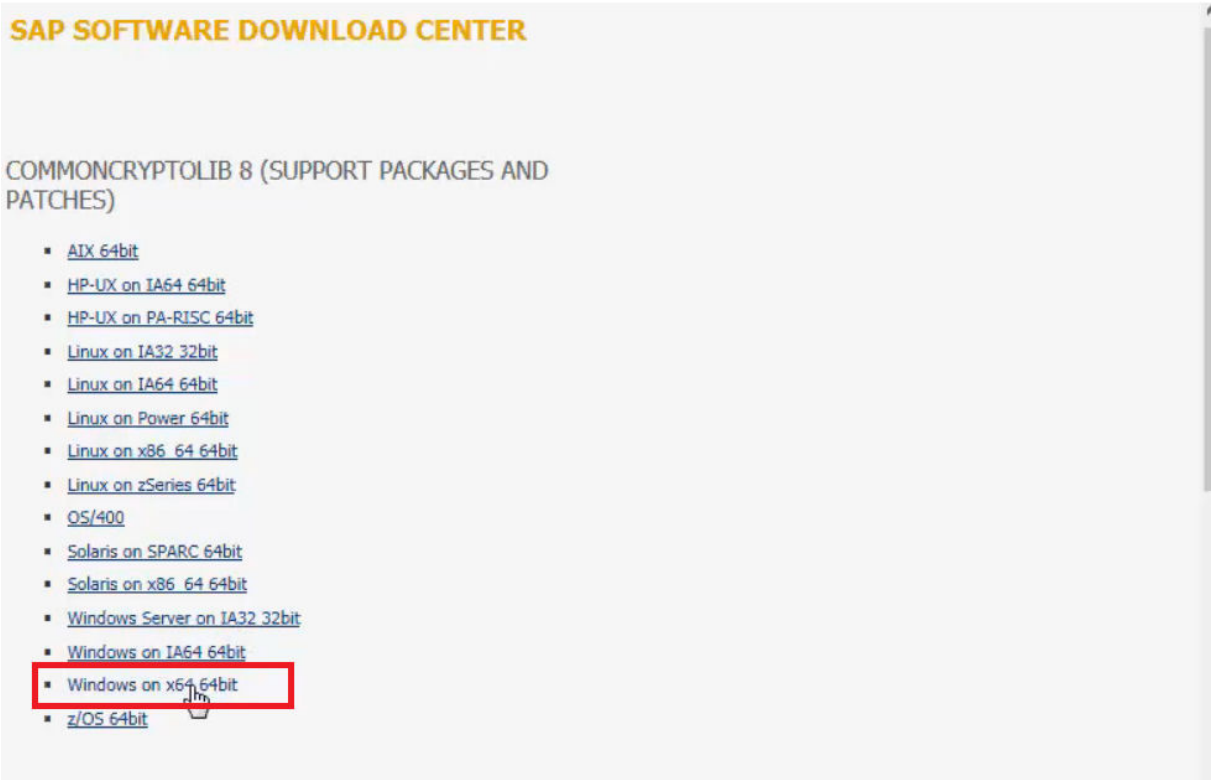
Доверительные параметры со стороны сервера подразумевают использование беспарольного заимствование прав. Для осуществления заимствования прав пользователя SAP без предоставления пароля пользователь должен пройти идентификацию на SAP с использованием более защищенного метода, чем обычный ввод имени и 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 параметров доверия на стороне сервера для платформы BI с использованием библиотеки шифрования SAP нужно запустить соответствующие серверы с использованием учетных данных, прошедших проверку зарегистрированного провайдера защищенного сетевого обмена данными (SNC). Эти данные настраиваются в SAP и используются для заимствования прав без ввода пароля. В платформе 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 шифрования SAP устанавливается на компьютер с платформой BI. Обратите внимание, эта библиотека может использоваться только для настройки доверительных параметров со стороны сервера. Библиотека шифрования доступна для систем Windows и Unix.


SAP SOFTWARE DOWNLOAD CENTER
SEARCH RESULTS IN SAP SOFTWARE DOWNLOAD CENTER
All corrective software packages for SAP NetWeaver 7.0 and SAP Business Suite 2005 (and beyond) are only available via Maintenance Optimizer in SAP Solution Manager. Find more details here.
Search Results
000001 NWSSO FOR COMMONCRYPTOLIB 2.0
Maintenance Software Component
000002 COMMONCRYPTOLIB 8
Maintenance Software Component
000003 NWSSOCCL03_0-20012328.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 AIX 64bit
000004 NWSSOCCL03_0-20012330.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 HP-UX on IA64 64bit
000005 NWSSOCCL03_0-20012332.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 HP-UX on PA-RISC 64bit
000006 NWSSOCCL03_0-20012333.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 Linux on IA32 32bit
000007 NWSSOCCL03_0-20012334.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 Linux on IA64 64bit
000008 NWSSOCCL03_0-20012335.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 Linux on x86_64 64bit
000009 NWSSOCCL03_0-20012336.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 Linux on Power 64bit
000010 NWSSOCCL03_0-20012338.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03


SAP SOFTWARE DOWNLOAD CENTER
COMMONCRYPTOLIB 8 (SUPPORT PACKAGES AND PATCHES)
AIX 64bit
HP-UX on IA64 64bit
HP-UX on PA-RISC 64bit
Linux on IA32 32bit
Linux on IA64 64bit
Linux on Power 64bit
Linux on x86_64 64bit
Linux on zSeries 64bit
OS/400
Solaris on SPARC 64bit
Solaris on x86_64 64bit
Windows Server on IA32 32bit
Windows on IA64 64bit
Windows on x64 64bit
z/OS 64bit

Для получения подробной информации о библиотеке шифрования см. SAP-ноты 711093, 597059 и 397175 на сайте SAP.

Серверу SAP и платформе BI необходимо назначить сертификаты, чтобы они могли подтвердить друг другу свою подлинность. У каждого сервера будет свой собственный сертификат и список сертификатов для доверенных сторон. Для настройки параметров доверия на стороне сервера между SAP и платформой BI требуется создать набор сертификатов, защищенных паролем, который называется средой персональной безопасности (PSE). В этом разделе описывается процесс настройки и обслуживания сред персональной безопасности, а также перечисляются способы безопасной привязки PSE к серверам обработки платформы BI.

Задачи сервера платформа SAP BusinessObjects BI

Определенные серверы платформы BI обеспечивают интеграцию SAP в рамках единого входа (SSO). Эти серверы и области ответственности перечислены в следующей таблице.

Сервер	Области ответственности
Сервер веб-приложений	список ролей для аутентификации SAP
Служба BW Publisher	Списки выбора динамических параметров Crystal Reports и персонализация
CMS	Пароль, билет, проверка принадлежности к роли и списки пользователей
Сервер страниц	Просмотр отчетов Crystal по требованию
Сервер заданий	Планирование отчетов Crystal
Сервер обработки Web Intelligence	Просмотр и планирование отчетов и подсказок в виде списков значений (LOV) для сервера Web Intelligence
Multi-Dimensional analysis service	Анализ

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 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 SAP в системе SAP и на компьютере, на котором выполняется система, а также идентификационных данных администратора для платформы BI и компьютера (или компьютеров), на которых она выполняется.
2. На компьютере с SAP-системой проверьте наличие библиотеки шифрования SAP 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 *OK*.
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_cpic`	`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_cpic`, 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 BI.

9.5.6.3 Настройка доверия к платформе BI на стороне сервера

Чтобы настроить доверие к платформе BI на стороне сервера, необходимо выполнить следующие действия. Обратите внимание, что эти шаги основаны на Windows, но поскольку инструмент SAP является инструментом командной строки, эти шаги очень схожи с действиями в UNIX.

1. Настройка среды
2. Создание среды личной безопасности (PSE)
3. Настройка серверов платформы BI
4. Настройка PSE-доступа
5. Настройка параметров SNC для аутентификации SAP
6. Настройка выделенных групп серверов SAP

Связанные сведения

Установка среды [страница 366]
Для генерации PSE [страница 367]
Настройка серверов платформы BI [страница 368]
Настройка доступа PSE [страница 369]
Для настройки SNC аутентификации SAP [страница 370]
Использование групп серверов [страница 371]

9.5.6.3.1 Установка среды

Платформа BI включает библиотеку шифрования SAP по умолчанию. Если используется библиотека по умолчанию, необходимо выполнить только два последних шага: создать подпапку 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: `<INSTALLDIR>\sap\sapcrypto.dll`
- Unix: `<INSTALLDIR>/sap/libsapcrypto.so`

Перед началом убедитесь в следующем:

- Библиотека шифрования SAP загружена и развернута на хосте, на котором выполняются серверы обработки платформы BI.
- Соответствующие системы SAP были настроены на работу с Криптографической библиотекой SAP в качестве провайдера SNC.

Перед началом обслуживания PSE необходимо установить библиотеку, вспомогательный инструмент и среду, в которой хранятся PSE.

1. Скопируйте библиотеку шифрования SAP (включая средство обслуживания среды персональной безопасности) в папку на компьютере с платформой BI.

   Например: `C:\Program Files\SAP\Crypto`.
2. Добавьте папку в переменную среды `<PATH>`.
3. Добавьте общесистемную переменную среды `<SNC_LIB>`, которая указывает на Криптографическую библиотеку.

   Например: `C:\Program Files\SAP\Crypto\sapcrypto.dll`

   > ⓘ 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`**.

Связанные сведения

Настройка доверительных параметров SAP со стороны сервера [страница 364]

9.5.6.3.2 Для генерации PSE

SAP принимает сервер платформы BI как доверенный объект, если соответствующие серверы платформы BI имеют среду личной безопасности, которая связана с SAP. «Доверие» между компонентами SAP и платформы BI устанавливается благодаря совместному использованию публичной версии сертификатов друг друга. Первым шагом является создание для платформы BI среды персональной безопасности, которая автоматически создает собственный сертификат.

1. Откройте командную строку и запустите файл **`sapgenpse.exe gen_pse -a sha256WithRsaEncryption -s 2048 -v -p BOE.pse`**, находящийся в папке Cryptographic Library.
2. Выберите PIN-код и отличительное имя для системы платформы BI.

   Например, **`CN=MyBOE01, OU=PG, O=BOBJ, C=CA`**.

   Теперь у вас есть PSE по умолчанию, со своим собственным сертификатом.
3. Для экспорт сертификата в PSE используйте следующую команду:

   ```
   sapgenpse.exe export_own_cert -v -p BOE.pse -o <MyBOECert.crt>
   ```

4. В пользовательском интерфейсе SAP перейдите к транзакции STRUST и откройте среду персональной безопасности системы, связанную с SAP-системой.

   Если среде персональной безопасности был назначен пароль, появится запрос на его ввод.

5. Импортируйте ранее созданный файл `<MyBOECert.crt>`. Для этого нажмите кнопку «Импортировать сертификат» в нижнем левом углу экрана транзакции STRUST.

   Сертификаты SAPGENPSE представлены в кодировке Base64. Убедитесь, что при импорте выбрана кодировка Base64:

6. Для добавления сертификата платформы BI к списку PSE-сертификатов на сервере SAP нажмите кнопку *Добавить в список сертификатов*.
7. Сохраните изменения в транзакции STRUST.
8. Нажмите кнопку *Экспорт* и введите имя файла для сертификата.

   Например, **`MySAPCert.crt`**.

   > ⓘ Примечание
   >
   > Кодировка должна оставаться в формате Base64.

9. Выполните транзакцию SNC0.
10. Введите новую запись, где:
    - Идентификатор системы является произвольным, однако он отражает используемую систему платформы BI.
    - Именем SNC должно быть отличительное имя (с префиксом **`p:`**), указанное при создании PSE платформы BI (шаг 2).
    - Флажки *Запись для RFC активирована* и *Запись для вн. идентификатора активирована* установлены.
11. Для добавления экспортированного сертификата к PSE платформы BI выполните в командной строке следующую команду:

    ```
    sapgenpse.exe maintain_pk -v -a <MySAPCert.crt> -p BOE.pse
    ```

Библиотека SAP Cryptographic Library установлена на компьютере с платформой BI. Создана среда PSE, которая будет использоваться серверами платформы BI для идентификации на серверах SAP. Среды PSE системы SAP и платформы BI обменялись сертификатами. SAP разрешает сущностям с доступом к PSE платформы BI выполнять вызовы RFC и в анонимном режиме без пароля.

Связанные сведения

Настройка серверов платформы BI [страница 368]

9.5.6.3.3 Настройка серверов платформы BI

После создания среды персональной безопасности для платформы 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 BI серверы больше не настраиваются в Central Configuration Manager (CCM). Вместо этого необходимо создать новый агент Server Intelligence Agent (SIA).

1. В CCM создайте новый узел для серверов обработки SAP.

   Присвойте узлу подходящее имя, такое как **`SAPProcessor`**.
2. В CMC добавьте серверы обработки в новый узел, затем запустите новые серверы.

9.5.6.3.4 Настройка доступа PSE

После настройки узла и серверов платформы BI необходимо настроить доступ PSE с использованием инструмента SAPGENPSE.

1. Выполните следующую команду в командной строке:

   `sapgenpse.exe seclogin -p SBOE.pse`

   > ⓘ Примечание
   >
   > Появится подсказка для ввода PIN-кода PSE. Если инструмент запущен с учетными данными, совпадающими с теми, которые используются серверами обработки SAP платформы BI, имя пользователя указывать не нужно.

2. Чтобы убедиться в том, что ссылка для единого входа (SSO) установлена, просмотрите содержимое PSE с помощью следующих команд.

   `sapgenpse.exe maintain_pk -l`

   Результаты должны иметь следующий вид:

   ```
   C:\Documents and
   Settings\username\Desktop\sapcrypto.x86\ntintel>sapgenpse.exe
   maintain_pk -l
    maintain_pk for PSE "C:\Documents and Settings\username\My
   Documents\snc\sec\bobjsapproc.pse"
   *** Object <PKList> is of the type <PKList_OID> ***
   1. ------------------------------------------------------------
              Version:                  0 (X.509v1-1988)
              SubjectName:              CN=R21Again, OU=PG, O=BOBJ, C=CA
              IssuerName:               CN=R21Again, OU=PG, O=BOBJ, C=CA
              SerialNumber:             00
              Validity  -  NotBefore:   Wed Nov 28 16:23:53 2007 (071129002353Z)
                                                                   NotAfter:
   Thu Dec 31 16:00:01 2037 (380101000001Z)
              Public Key Fingerprint:   851C 225D 1789 8974 21DB 9E9B 2AE8 9E9E
              SubjectKey:               Algorithm RSA (OID
   1.2.840.113549.1.1.1), NULL
   C:\Documents and Settings\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 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 CMC *Аутентификация*.
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.
   >
   > *Качество защиты* относится только к обработке на стороне платформы. Например, указанному уровню соответствует средство просмотра Web Intelligence DHTML. Однако коммуникацию с SAP Business Warehouse (BW) на стороне клиента следует считать незащищенной. Например, коммуникация экземпляра Web Intelligence Rich Client или средства дизайна информации всегда является незашифрованной.

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 `p:` в качестве префикса.

9. Убедитесь, что SNC-имя учетных данных, под которыми работают серверы платформы BI, отображается в поле *SNC-имя системы Enterprise*.

   При настройке нескольких имен SNC данное поле должно оставаться пустым.

10. Укажите отличительные имена сред персональной безопасности для системы SAP и платформы 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 дополнительных сведений и описаний разных серверов платформы BI см. главу «Архитектура».

Существует три варианта настройки серверов обработки содержимого SAP.

1. Поддерживайте один SIA, включая все серверы платформы BI, выполняемый с учетными данными, которые обеспечивают доступ к PSE. Это самый простой вариант – нет необходимости создавать группы серверов. Данный подход является наименее безопасным, так как доступ к PSE будет у излишнего количества серверов.
2. Создайте второй SIA с доступом к PSE и добавьте его к серверам обработки Crystal 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 защищенного сетевого обмена данными (SNC) для аутентификации и шифрования данных компонентов SAP. Если выполнялось внедрение криптографической библиотеки SAP (или другого продукта защиты, использующего 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.

Связанные сведения

Импорт ролей SAP [страница 357]

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, убедиться, что файл библиотеки SNC находится в известном каталоге, 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 веб-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*.

9. Нажмите кнопку *Обновить.*

Связанные сведения

Подключение к системам контроля полномочий SAP [страница 351]

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 2 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 SAP 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 SAP NetWeaver ABAP.

Подробнее см. в ноте 1670073.

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

В этом разделе содержатся инструкции по использованию Java Keytool для создания файлов хранилища ключей. В следующей таблице перечислены расположения Java Keytool по умолчанию.

Платформа	Местоположение по умолчанию
Windows	`<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\ win64_x64\sapjvm\bin`
Linux	`sap_bobj/enterprise_xi40/linux_x64/sapjvm/bin/keytool`

1. Перейдите в расположение Java Keytool по умолчанию и запустите командную строку.
2. Запустите Java Keytool для создания хранилища ключей.
   a. Перейдите в каталог <INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin.
   b. Выполните следующую команду:
      - Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin\keytool" -genkey -alias mywin -keystore keystore.p12 -storepass admin1 -dname CN=palmtree -validity 365 -keyalg DSA -keysize 1024 -storetype pkcs12`
      - Linux: `*/sap_bobj/enterprise_xi40/java/lib>/sap_bobj/enterprise_xi40/linux_x64/sapjvm/bin/keytool" -genkey -alias mywin -keystore keystore.p12 -storepass admin1 -dname CN=palmtree -validity 365 -keyalg DSA -keysize 1024 -storetype pkcs12`

→ Совет

Для переопределения значений по умолчанию запустите средство вместе с параметром -?. На экран выводится следующее сообщение.

{·} Пример кода

```
Usage: keytool -genkey <options>
        -keystore <filename(keystore.p12)>
        -alias <key entry alias(mywin)>
        -storepass <keystore password (admin1)>
        -dname <certificate subject DN(CN=palmtree)>
        -validity <number of days (365)>
        -cert <filename (cert.der)>
         (No certificate is generated when importing a keystore)
        -importkeystore <filename>
```

Для переопределения значений по умолчанию можно использовать параметры.

ⓘ Примечание

Java Keytool необходимо использовать как замену для средства PKCS12 для создания хранилища ключей. Для получения дополнительных сведений см. 2524775.

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.

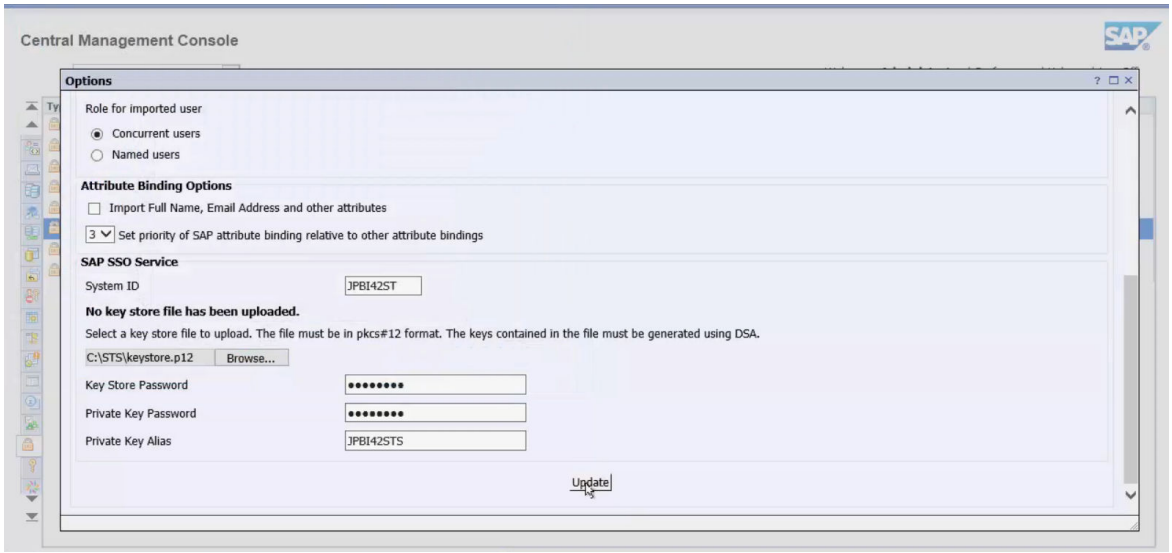
   Идентификатор системы должен совпадать с тем, который используется для идентификации платформы BI в SAP BW.

   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 CMC

Для выполнения этого алгоритма нужен доступ к подключаемому модулю безопасности SAP под учетной записью администратора.

1. Перейдите в область управления CMC *Аутентификация*.
2. Дважды щелкните на ссылку *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 CMC.
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 *OK*.
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 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 Infoset	*crb_infoset*
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 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 "raquino"), а с PeopleSoft Financials 8.4 работаете под учетной записью пользователя Raoul Aquino (имя пользователя "raquino"), 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 `<КАТАЛОГ_УСТАНОВКИ>\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. Войдите в консоль Central Management Console с 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 "A", введите *A%*. При поиске также учитывается регистр слов.

   > **Примечание**
   >
   > 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:

- *Назначить каждый добавленный псевдоним учетной записи с тем 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 человек уже подключено к ней. Для каждой учетной записи, созданной с использованием данного параметра, должна существовать именованная пользовательская лицензия.

     > **Примечание**
     >
     > Число параллельных сеансов входа для именованного пользователя, созданного с использованием пользовательской лицензии, ограничивается 10 сеансами. Если такой именованный пользователь попытается войти в 11-й параллельный сеанс входа, будет выдано соответствующее сообщение об ошибке. Для входа необходимо будет завершить один из текущих сеансов.
     >
     > Однако число параллельных сеансов входа для именованных пользователей, созданных с использованием лицензии на процессор и лицензии на публичные документы, не ограничено.
   - *Новые пользователи создаются как параллельные пользователи.*
     Новые учетные записи пользователей настраиваются для использования 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 *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:

- Обновить 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.
- Обновить 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 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*.

9.6.5 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 [страница 390].

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 членами 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`.

   > ⓘ Примечание
   >
   > 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.

> **Примечание**
>
> 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 исполнителей 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 пакетный файл `crpsepmsecuritybridge.bat` (в ОС Windows) или `crpsempsecuritybridge.sh` (в ОС Unix) и в качестве аргумента укажите созданный ранее файл ответа. Например, введите **`crpsepmsecuritybridge.bat myresponsefile.properties`** (ОС Windows) или **`crpsempsecuritybridge.sh myresponsefile.properties`** (ОС Unix).

Запустится приложение моста безопасности. Оно создаст пользователей в платформе BI для исполнителей 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 исполнителя 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 безопасности PeopleSoft.

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 исполнителем 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 исполнителей 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 безопасности PeopleSoft.
- Для исполнителей управляемых ролей PeopleSoft, которые также являются исполнителями управляемой группы платформы BI, мост безопасности изменяет настройки безопасности, применяемые к этим пользователям, предоставляя им доступ к соответствующим данным из управляемых юниверсов.

Если у исполнителя управляемой роли PeopleSoft имеется учетная запись в платформе BI, но он *не является* исполнителем 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 исполнитель управляемой группы платформы BI *не является* членом управляемой роли PeopleSoft, то мост безопасности *не предоставляет* ему доступ к управляемым юниверсам. Как правило, такая ситуация возникает только в том случае, если администратор PeopleSoft удаляет пользователей, для которых ранее было выполнено сопоставление в платформе BI с помощью моста безопасности из управляемой роли PeopleSoft.

> ⓘ Примечание
>
> Это еще один метод управления безопасностью: удаляя пользователей из управляемых ролей PeopleSoft, вы гарантировано лишаете их доступа к данным из PeopleSoft.

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 моста 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	Путь класса для загрузки необходимых файлов .jar. Если указывается несколько путей классов, в качестве разделителя используется ';' (как в Windows, так и в UNIX). Пути классов, необходимые для файлов `com.peoplesoft.epm.pf.jar` и файлов .jar драйвера JDBC.

Параметр	Описание
db.driver.name	Имя драйвера JDBC, используемое для подключения базы данных PeopleSoft (например, `com.microsoft.jdbc.sqlserver.SQLServerDriver`).
db.connect.str	Строка подключения JDBC, используемая для подключения к базе данных PeopleSoft (например, `jdbc:microsoft:sqlserver:// vanrdpsft01:1433;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.
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. Подробную информацию см. в разделе Определение управляемых объектов [страница 387].
enterprise.license	Определяет тип лицензии при импорте пользователей из Peoplesoft. "0" задает лицензию для именованных пользователей, а "1" – лицензию на одновременный доступ.

Параметр	Описание
peoplesoft.role.n	Список управляемых ролей PeopleSoft. Подробную информацию см. в разделе Определение управляемых объектов [страница 387]. **<n>** – целое число, и каждой записи присваивается свойство с помощью префикса "peoplesoft.role". **Примечание** **<n>** не должно быть менее 1. Символом "*" можно обозначить все доступные роли PeopleSoft (при условии, что n=1, и что это единственное свойство, имеющее префикс "peoplesoft.role" в файле ответов).
mapped.universe.n	Список юниверсов, которые мост безопасности должен обновить. Подробную информацию см. в разделе Определение управляемых объектов [страница 387]. **<n>** – целое число, и каждой записи присваивается свойство с помощью префикса "mapped.universe". **Примечание** **<n>** не должно быть менее 1. Символом "*" можно обозначить все доступные юниверсы (при условии, что n=1, и оно является единственным свойством, имеющим префикс "mapped.universe" в файле ответа).
log4j.appender.file.File	Файл журнала, создаваемый мостом безопасности.

Параметр	Описание
log4j.*	Свойства log4j по умолчанию, необходимые для надлежащей работы log4j: log4j.rootLogger=INFO, file, stdout log4j.appender.file=org.apache.log4j.RollingFile Appender log4j.appender.file.layout=org.apache.log4j.PatternLayout log4j.appender.file.MaxFileSize=5000KB log4j.appender.file.MaxBackupIndex=100 log4j.appender.file.layout.ConversionPattern=%d [%-5] %c{1} – %m%n log4j.appender.stdout=org.apache.log4j.ConsoleAppender log4j.appender.stdout.layout=org.apache.log4j.PatternLayout log4j.appender.stdout.layout.ConversionPattern=%d [%-5] %c{1} – %m%n
peoplesoft classpath	Путь класса к файлам .jar PeopleSoft EPM API. Это необязательный параметр.
enterprise.classpath	Путь класса к JAR-файлам 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.

Параметр	Описание
sql.db.class.location sql.db.host sql.db.port sql.db.database	Местоположение файлов .jar драйвера JDB 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.
db2.db.class.location db2.db.host db2.db.port db2.db.sid	Местоположение файлов .jar драйвера JDBC DB2, хост базы данных DB2, порт базы данных DB2 и SID базы данных DB2. Эти параметры можно использовать, только если параметр "db.driver.type" имеет значение "DB2 UDB 8.2 Fixpack 7" Это необязательные параметры.
custom.db.class.location custom.db.drivername custom.db.connectStr	Местоположение, имя и строка соединения нестандартного драйвера JDBC. Эти параметры можно использовать, только если параметр "db.driver.type" имеет значение "Custom". Это необязательные параметры.

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. Войдите в систему Central Management Console под учетной записью администратора.
2. В области "Управление" щелкните *Аутентификация*.
3. Дважды щелкните *JD Edwards EnterpriseOne*.
   На экране будет отображена страница *JD Edwards EnterpriseOne*.
4. На вкладке *Параметры* установите флажок *Включить аутентификацию JD Edwards EnterpriseOne*.
5. Внесите необходимые изменения в разделы *Новый псевдоним*, *Параметры обновления* и *Параметры нового пользователя* в соответствии с имеющимся развертыванием платформы BI. Нажмите кнопку *Обновить* для сохранения изменений перед переходом на вкладку *Системы*.
6. Нажмите вкладку *Серверы*.
7. 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 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.
11. Введите имя среды и нажмите кнопку *Добавить*.
12. 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 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 "raquino"), а в производственной среде – учетная запись пользователя Raoul Aquino (имя пользователя "raquino"), 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 консоль Central Management Console с 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:
   - *Назначить каждый добавленный псевдоним учетной записи с тем 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*
     Этот параметр используется для создания нового псевдонима для каждого пользователя, для которого устанавливается соответствие в платформе BI. Новые учетные записи создаются для пользователей, у которых нет учетных записей платформы BI, или для всех пользователей, если выбран параметр "Создать новую учетную запись для каждого добавляемого псевдонима".
   - *Новые псевдонимы не будут добавлены, и новые пользователи не будут созданы*
     Этот параметр используется в том случае, если роль, для которой устанавливается соответствие, содержит много пользователей, но только некоторые из них будут использовать платформу BI. Система 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.
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 человек уже подключено к ней. Для каждой учетной записи, созданной с использованием данного параметра, должна существовать именованная пользовательская лицензия.

> **Примечание**
>
> Число параллельных сеансов входа для именованного пользователя, созданного с использованием пользовательской лицензии, ограничивается 10 сеансами. Если такой именованный пользователь попытается войти в 11-й параллельный сеанс входа, будет выдано соответствующее сообщение об ошибке. Для входа необходимо будет завершить один из текущих сеансов.
>
> Однако число параллельных сеансов входа для именованных пользователей, созданных с использованием лицензии на процессор и лицензии на публичные документы, не ограничено.

- *Новые пользователи создаются как параллельные пользователи.*
  Новые учетные записи пользователей настраиваются для использования 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.

7. Перейдите на вкладку *Роли*.
8. В *списке доменов* выберите сервер JD Edwards, содержащий роли, которые нужно сопоставить.
9. В разделе *Доступные роли* выберите роли, которые требуется сопоставить платформе BI, и нажмите кнопку <.
10. Нажмите кнопку *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 *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:

- Обновить 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.
- Обновить 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 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.
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.

Тип повтора	Описание
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 "raquino"), а в производственной среде – учетная запись пользователя Raoul Aquino (имя пользователя "raquino"), 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. Войдите в консоль Central Management Console с 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:
   - *Назначить каждый добавленный псевдоним учетной записи с тем 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 человек уже подключено к ней. Для каждой учетной записи, созданной с использованием данного параметра, должна существовать именованная пользовательская лицензия.

     > **Примечание**
     >
     > Число параллельных сеансов входа для именованного пользователя, созданного с использованием пользовательской лицензии, ограничивается 10 сеансами. Если такой именованный пользователь попытается войти в 11-й параллельный сеанс входа, будет выдано соответствующее сообщение об ошибке. Для входа необходимо будет завершить один из текущих сеансов.
     >
     > Однако число параллельных сеансов входа для именованных пользователей, созданных с использованием лицензии на процессор и лицензии на публичные документы, не ограничено.
   - *Новые пользователи создаются как параллельные пользователи*
     Новые учетные записи пользователей настраиваются для использования 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.
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**
>
> Используя поле *Поиск ролей, начинающихся с:*, можно сузить круг поиска в случае большого числа ролей. Введите символы, с которых начинается роль или роли, затем символ шаблона (%) и щелкните *Поиск*.

> **Примечание**
>
> Чтобы функция поиска работала, JAR-файл подключаемого модуля Siebel должен быть развернут в каталоге lib Tomcat: `<КАТАЛОГ_УСТАНОВКИ>\tomcat\webapps\BOE\WEB-INF\lib` и в каталоге `<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\java\lib\siebel\default\siebel`. После этого перезапустите сервер Tomcat и Server Intelligence Agent.

11. Нажмите кнопку *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:

- Обновить 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.
- Обновить 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 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.
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 DLL и JAR Oracle 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.

Связанные сведения

Сопоставление ролей Oracle E-Business Suite [страница 409]

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 в 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 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 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 "raquino"), а в производственной среде – учетная запись пользователя Raoul Aquino (имя пользователя "raquino"), 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. Войдите в консоль Central Management Console с 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*
     Этот параметр используется для создания нового псевдонима 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*
     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.
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 человек уже подключено к ней. Для каждой учетной записи, созданной с использованием данного параметра, должна существовать именованная пользовательская лицензия.

     > **Примечание**
     >
     > Число параллельных сеансов входа для именованного пользователя, созданного с использованием пользовательской лицензии, ограничивается 10 сеансами. Если такой именованный пользователь попытается войти в 11-й параллельный сеанс входа, будет выдано соответствующее сообщение об ошибке. Для входа необходимо будет завершить один из текущих сеансов.
     >
     > Однако число параллельных сеансов входа для именованных пользователей, созданных с использованием лицензии на процессор и лицензии на публичные документы, не ограничено.

   - *Новые пользователи создаются как параллельные пользователи.*
     Новые учетные записи пользователей настраиваются для использования 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, 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. Нажмите кнопку *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:

- Обновить 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 имеются проблемы с использованием системных ресурсов. Если обновляются только роли Oracle EBS
- Обновить роли и псевдонимы: этот вариант позволяет обновить не только ссылки между ролями, но также создать 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.
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.

Тип повтора	Описание
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

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. Нажмите *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.

9.9.4 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 представлена 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 *OK*.

Исполнители 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 исполнителям 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 *OK*.

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 CMC 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 (CMC) 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 CMC и выберите *Службы отчетов Crystal Reports*.
8. Нажмите кнопку *Перезапустить сервер*.

9.10 Аутентификация X.509

9.10.1 Аутентификация X.509 для стартовой панели BI

9.10.1.1 Создание и настройка сертификатов и хранилищ ключей

> **Примечание**
>
> Для обеспечения единого входа (SSO) с помощью аутентификации X.509 пользователь должен существовать в платформе BI.

> **Примечание**
>
> Загрузите и установите инструментарий OpenSSL, чтобы выполнить описанные ниже шаги.

> **Примечание**
>
> Выполните все следующие шаги, если требуется создать сертификат центра сертификации (CA) и самостоятельно подписать его.

> **Примечание**
>
> Если у вас имеется доверенный центр сертификации, см. инструкции по созданию и настройке сертификатов и хранилищ ключей в разделе С доверенным центром сертификации [страница 418].

1. Выполните команду для создания файлов ключа центра сертификации (ca.key) и запроса сертификата (ca.csr). `Openssl.exe req -newkey rsa:2048 -nodes -out c:\ssl\ca.csr -keyout c:\ssl\ca.key`
2. Выполните команду, чтобы создать подписанный сертификат ca.pem. `Openssl.exe x509 -req -trustout -signkey c:\ssl\ca.key -days 365 -in c:\ssl\ca.csr -out c:\ssl\ca.pem`
3. Создайте пару ключей сервера, сертификат и хранилище ключей.
   a. Создайте файл для хранения серийных номеров CA, выполнив следующий код: `Echo 02 >c:\ssl\ca.srl`

b. Перейдите в каталог `C:\Program Files\Java\jre7\bin` и с помощью keytool.exe создайте хранилище ключей сервера, сертификат и личный ключ.

> ⓘ Примечание
>
> В расположении Java keytool.exe значение jre7 может варьироваться в зависимости от версии Java.

```
Keytool.exe -genkey -alias server -keyalg RSA -keysize 2048 -keystore
c:\ssl\serverkeystore.jks -storetype JKS
Keytool.exe -certreq -keyalg RSA -alias server -file c:\ssl\server.csr -
keystore c:\ssl\serverkeystore.jks
```

> → Напоминание
>
> При создании сертификата введите имя хоста сервера, когда появится подсказка. В противном случае при подключении возникнет ошибка сертификата на клиенте.

c. Введите пароль хранилища ключей.

> → Напоминание
>
> Необходимо отредактировать файл запроса server.csr в текстовом редакторе и изменить New Begin Certificate Request на Begin Certificate Request и New End Certificate Request на End Certificate Request.

4. Выполните команду, чтобы создать подписанный сертификат server.crt. `Openssl.exe x509 -CA c:\ssl\ca.pem -cakey c:\ssl\ca.key -CAserial c:\ssl\ca.srl -req -in c:\ssl\server.csr -out c:\ssl\server.crt -days 365`
5. Импортируйте сертификат центра сертификации и сертификат сервера в хранилище ключей сервера.

```
Keytool.exe -import -alias ca -keystore c:\ssl\serverkeystore.jks -
trustcacerts -file c:\ssl\ca.pem
Keytool.exe -import -alias server -keystore c:\ssl\serverkeystore.jks -
trustcacerts -file c:\ssl\server.crt
```

6. Выполните команду для создания сертификатов клиента client.req и client.key. `Openssl.exe -newkey rsa:2048 -nodes -out c:\ssl\client.req -keyout c:\ssl\client.key -config c:\ssl\sslc.cnf`

> ⓘ Примечание
>
> Скопируйте файл sslc.cnf из расположения `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` в C:\SSL и измените следующие параметры:
>
> Dir=c:/ssl # расположение для всех элементов
>
> Certificate= $dir/ca.pem # сертификат CA
>
> Private_key= $dir/ca.key # личный ключ
>
> RANDFILE= $dir/.rand # личный файл с произвольным номером

7. Выполните команду, чтобы подписать сертификат клиента. `Openssl.exe x509 -CA c:\ssl\ca.pem -CAkey c:\ssl\ca.key -CAserial c:\ssl\ca.srl -req -in c:\ssl\client.req -out c:\ssl\client.pem -days 365`

8. Импортируйте сертификат CA и сертификат клиента в хранилище ключей, выполнив команду, указанную ниже. Эта команда позволяет создать файл trustkeystore.jks.

```
Keytool.exe –import –alias ca –keystore c:\ssl\trustkeystore.jks –
trustcacerts –file c:\ssl\ca.pem
Keytool.exe –import –alias client –keystore c:\ssl\trustkeystore.jks –
trustcacerts –file c:\ssl\client.pem
```

9. Экспортируйте сертификат клиента с личным ключом клиента в формате PKCS12. `Openssl.exe pkcs12 –export –clcerts –in c:\ssl\client.pem –inkey c:\ssl\client.key –out c:\ssl\client.p12 –name “client certificate”`. Эта команда позволяет создать файл client.p12.
10. Выполните команду, чтобы экспортировать сертификат CA и создать файл ca.crt. `Openssl.exe x509 –in c:\ssl\ca.pem –inform PEM –out c:\ssl\ca.crt –outform DER`
11. Скопируйте файлы .p12 и ca.crt на клиентский компьютер, чтобы установить сертификат клиента и сертификат CA.

> ⓘ Примечание
>
> Для установки сертификатов в Mozilla Firefox перейдите в раздел *Сервис* > *Параметры* > *Дополнительно* > и выберите «Просмотр сертификатов» на вкладке «Шифрование», чтобы импортировать файл client.p12 с вкладки «Ваши сертификаты» и файл ca.crt с вкладки «Центры сертификации».

9.10.1.1.1 С доверенным центром сертификации

1. Создайте пару ключей сервера, сертификат и хранилище ключей.
   a. Создайте файл для хранения серийных номеров CA, выполнив следующий код: `Echo 02 >c:\ssl\ca.srl`
   b. Перейдите в каталог `C:\Program Files\Java\jre7\bin` и с помощью keytool.exe создайте хранилище ключей сервера, сертификат и личный ключ.

   > ⓘ Примечание
   >
   > В расположении keytool.exe значение jre7 может варьироваться в зависимости от версии Java.

   ```
   Keytool.exe –genkey –alias server –keyalg RSA –keysize 2048 –keystore
   c:\ssl\serverkeystore.jks –storetype JKS
   Keytool.exe –certreq –keyalg RSA –alias server –file c:\ssl\server.csr –
   keystore c:\ssl\serverkeystore.jks
   ```

   > → Напоминание
   >
   > При создании сертификата введите имя хоста сервера, когда появится подсказка. В противном случае при подключении возникнет ошибка сертификата на клиенте.

   c. Введите пароль хранилища ключей.

> → Напоминание
>
> Необходимо отредактировать файл запроса server.csr в текстовом редакторе и изменить New Begin Certificate Request на Begin Certificate Request и New End Certificate Request на End Certificate Request.

2. Выполните команду, чтобы создать подписанный сертификат server.crt. `Openssl.exe x509 –CA c:\ssl\ca.pem –cakey c:\ssl\ca.key –CAserial c:\ssl\ca.srl –req –in c:\ssl\server.csr –out c:\ssl\server.crt –days 365`
3. Импортируйте сертификат сервера в хранилище ключей сервера.

```
Keytool.exe –import –alias server –keystore c:\ssl\serverkeystore.jks –
trustcacerts –file c:\ssl\server.crt
```

4. Выполните команду, чтобы создать сертификаты клиента client.req и client.key. `Openssl.exe –newkey rsa:2048 –nodes –out c:\ssl\client.req –keyout c:\ssl\client.key –config c:\ssl\sslc.cnf`

> ⓘ Примечание
>
> Скопируйте файл sslc.cnf из расположения `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` в C:\SSL и измените следующие параметры:
>
> Dir=c:/ssl # расположение для всех элементов
>
> Certificate= $dir/ca.pem # сертификат CA
>
> Private_key= $dir/ca.key # личный ключ
>
> RANDFILE= $dir/.rand # личный файл с произвольным номером

5. Выполните команду, чтобы подписать сертификат клиента. `Openssl.exe x509 –CA c:\ssl\ca.pem –CAkey c:\ssl\ca.key –CAserial c:\ssl\ca.srl –req –in c:\ssl\client.req –out c:\ssl\client.pem –days 365`
6. Импортируйте сертификат клиента в доверенное хранилище ключей, выполнив команду, указанную ниже. Эта команда позволяет создать файл trustkeystore.jks.

```
Keytool.exe –import –alias client –keystore c:\ssl\trustkeystore.jks –
trustcacerts –file c:\ssl\client.pem
```

7. Экспортируйте сертификат клиента с личным ключом клиента в формате PKCS12. `Openssl.exe pkcs12 –export –clcerts –in c:\ssl\client.pem –inkey c:\ssl\client.key –out c:\ssl\client.p12 –name “client certificate”`. Эта команда позволяет создать файл client.p12.
8. Скопируйте файл .p12 на клиентский компьютер, чтобы установить его.

> ⓘ Примечание
>
> Для установки сертификатов в Mozilla Firefox перейдите в раздел *Сервис* > *Параметры* > *Дополнительно* и выберите «Просмотр сертификатов» на вкладке «Шифрование», чтобы импортировать файл client.p12 с вкладки «Ваши сертификаты» и файл ca.crt с вкладки «Центры сертификации».

9.10.1.2 Настройка сервера Tomcat с SSL

9.10.1.2.1 Настройка одностороннего SSL

1. Перейдите в каталог `<INSTALLDIR>\tomcat\conf\server.xml`
2. Отредактируйте тег XML:
```
<Connector port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="200"
SSLEnabled="true" scheme="https" secure="true">
<SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/
myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></
Connector>
```

   > ⓘ Примечание
   >
   > Пароль (Password1) и расположение (C:\ssl\serverkeystore.jks) файла хранилища ключей, используемые в теге XML выше, приводятся исключительно в качестве примеров. Можно использовать любой собственный пароль и расположение.

3. Сохраните файл и перезапустите сервер Tomcat.

9.10.1.2.2 Настройка двухстороннего SSL

На сервере Tomcat настройте запрос аутентификации клиента, выполнив описанные ниже шаги.

1. Перейдите в каталог `<INSTALLDIR>\tomcat\conf\server.xml`
2. Отредактируйте файл server.xml, используя тег XML, указанный ниже:
```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="200" SSLEnabled="true" scheme="https" secure="true">
<SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/
myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></
Connector>
```

   > ⓘ Примечание
   >
   > Пароль (Password1) и расположение (C:\ssl\serverkeystore.jks или C:\ssl\trustkeystore.jks) файла хранилища ключей сервера и доверенного хранилища ключей, используемые в теге XML выше, приводятся исключительно в качестве примеров. Можно использовать любой собственный пароль и расположение.

3. Сохраните файл и перезапустите сервер Tomcat.

   > ⓘ Примечание
   >
   > В Internet Explorer отключите параметр «Не запрашивать сертификат клиента, когда имеется только один сертификат», щелкнув *Свойства браузера* > *Безопасность* > *Местная интрасеть* > *Другой* > *Разное* >.

9.10.1.3 Настройка стартовой панели BI

9.10.1.3.1 Создание общего секретного ключа

Общий секретный ключ используется, чтобы установить доверительные отношения между клиентом и CMS. Для доверительной аутентификации необходимо настроить сначала сервер, а затем клиент.

1. Войдите в систему CMC.
2. Перейдите в раздел «Аутентификация» и выберите Enterprise.
3. Включите доверительную аутентификацию.
4. Выберите «Новый общий секретный ключ».

   > ⓘ Примечание
   >
   > Будет создан общий секретный ключ, и появится сообщение о загрузке.

5. Выберите «Загрузить общий секретный ключ».
6. Нажмите кнопку «Сохранить» в диалоговом окне загрузки и выберите один из следующих каталогов:
   - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\`
   - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`

9.10.1.3.2 Передача общего секретного ключа с помощью файла TrustedPrincipal.conf

1. Создайте новый текстовый файл в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEBINF\config\custom\directory`.
2. Добавьте в новый файл приведенный ниже текст.

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

3. Сохраните файл и назовите его global.properties.

9.10.1.3.3 Редактирование файла custom.jsp

> ⓘ Примечание
>
> Прежде чем редактировать файл custom.jsp, создайте пользователя с именем компьютера в CMC.

1. Перейдите в каталог

a. *<INSTALLDIR>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.InfoView* > *web* > *custom.jsp* в *com.businessobjects.webpath.InfoView.jar* для классической стартовой панели BI.

b. *<INSTALLDIR>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.fioriBI* > *web* > *custom.jsp* в *com.businessobjects.webpath.fioriBI.jar* стартовой панели BI в стиле Fiori.

2. Отредактируйте файл custom.jsp.

```
<\!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","<Shared_Secret_Key>")
request.getSession().setAttribute("MyUser", "John Doe");
%>
<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>
```

> **Примечание**
>
> Следует заменить <Shared_Secret_Key> новым ключом, доступным в файле *TrustedPrincipal.conf*. Сведения о создании общего секретного ключа см. в Создание общего секретного ключа [страница 421].

9.10.1.3.4 Создание файла myScript.js

1. Перейдите в каталог *<INSTALLDIR>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.InfoView* > *web* > *noCacheCustomResources* и создайте файл myScript.js.
2. Добавьте в файл myScript.js следующий код:

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

3. Перезапустите сервер Tomcat.

9.10.1.3.5 Настройка внутренних файлов и файлов пользовательских свойств BOE

1. Перейдите в каталог *<INSTALLDIR>* > *Tomcat* > *webapps* > *BOE* > *WEB-INF* > *internal*
2. Откройте файл bilaunchpad.properties и измените следующие свойства:

```
redirection.iframe.1.incoming.url=property.ref.app.url.name
redirection.iframe.1.application=InfoView
redirection.iframe.1.bundle.path=/InfoView
redirection.iframe.1.redirectto.url=/custom.jsp
redirection.iframe.2.incoming.url=property.ref.app.url.name
redirection.iframe.2.incoming.url.suffix=/index.html
redirection.iframe.2.application=InfoView
redirection.iframe.2.bundle.path=/InfoView
redirection.iframe.2.redirectto.url=/custom.jsp
redirection.iframe.9.incoming.url=/InfoView/index.html
redirection.iframe.9.application=InfoView
redirection.iframe.9.bundle.path=/InfoView
redirection.iframe.9.redirectto.url=/custom.jsp
```

3. Перезапустите сервер Tomcat.

9.10.1.3.6 Настройка файлов Web.xml в BOE

1. Перейдите в каталог `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF`.
2. Отредактируйте файл web.xml в этом расположении, используя приведенный ниже код:

```
<init-param>
<param-name>extendedFrameworkExports</param-name>
<param-
value>com.businessobjects.servletbridge.listener,com.businessobjects.servletbr
idge.customconfig,com.businessobjects.servletbridge.external,com.businessobjec
ts.servletbridge.session,com.businessobjects.resource,oracle.jdbc.pool,com.sie
bel.data,com.jdedwards.system.xml,org.ietf.jgss,com.sap.security.api</param-
value>
</init-param>
```

3. Добавьте в файл web.xml параметры, выполнив следующие шаги:
   a. Перейдите в каталог `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\eclipse\plugins\webpath.BIPCoreWeb\web\WEB-INF`
   b. Добавьте параметры, указанные ниже:

```
<init-param>
<param-name>trusted.auth.shared.secret</param-name>
<param-value>New_Shared_Secret_Key</param-value>
</init-param>
```

   c. Повторите шаги, перейдя в каталог `<INSTALLDIR>\tomcat\work\Catalina\localhost\BOE\eclipse\plugins\webpath.BIPCoreWeb\web\WEB-INF`

> → Совет
>
> Чтобы проверить правильность настройки доверительной аутентификации, воспользуйтесь следующим URL-адресом для доступа к приложению стартовой панели BI:

> https://[имя_cms]:8443/BOE/BI/logon.jsp, где [имя_cms] — это имя компьютера, на котором размещена система CMS.

9.10.2 Аутентификация по стандарту X.509 для веб-служб

9.10.2.1 Веб-службы SOAP

9.10.2.1.1 Настройка SSL в Tomcat

Когда используются веб-службы, прежде чем приступать к настройке платформы SAP Business Intelligence, необходимо настроить SSL в Tomcat.

> ⓘ Примечание
>
> Для обеспечения единого входа (SSO) с помощью аутентификации X.509 пользователь должен существовать в платформе BI.

1. Перейдите в каталог `<INSTALLDIR>\tomcat\conf`.
2. Откройте файл server.xml в редакторе XML и отредактируйте тег XML:

   ```
   <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
   maxThreads="200" SSLEnabled="true" scheme="https" secure="true">
   <SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/
   myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></
   Connector>
   ```
3. Сохраните файл.

   > ⓘ Примечание
   >
   > Упомянутые выше пароль и расположение файлов приводятся исключительно в качестве примеров. Можно использовать любой собственный пароль и расположение.

   > ⓘ Примечание
   >
   > Дополнительные сведения о создании и настройке файлов хранилища ключей см. в разделе Создание и настройка сертификатов и хранилищ ключей [страница 416].

9.10.2.1.2 Настройка файла axis2.xml

> ⓘ Примечание
>
> Перед выполнением нижеописанных шагов убедитесь, что в системе Linux или Unix у пользователя, устанавливающего BI в этой ОС, имеются рекурсивные права 755 на каталог `<INSTALLDIR>\SAP`

`BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje`. Эти права могут быть предоставлены с помощью команды `chmod -R 755`

1. Перейдите в каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`
2. Откройте файл axis2.xml в любом редакторе XML.
3. Обновите тег XML, указав новый номер порта для защищенного соединения.

```
<transportReceiver name="http"
class="org.apache.axis2.transport.http.AxisServletListener">
<parameter name="port">8080</parameter>
</transportReceiver>
<transportReceiver name="https"
class="org.apache.axis2.transport.http.AxisServletListener">
<parameter name="port">8443</parameter>
</transportReceiver>
```

> **Примечание**
>
> Конфигурация по умолчанию основана на допущении, что AxisServlet получает запросы только через HTTP. Чтобы разрешить связь по протоколу HTTPS, необходимо настроить прослушиватель AxisServletListener, указав имя https и параметр порта на обоих приемниках. Кроме того, можно добавить или удалить несколько номеров портов путем обновления тегов XML.

4. Сохраните файл axis2.xml.
5. Перезапустите сервер Tomcat.
6. Запустите любой браузер и перейдите по пути https://<IP-адрес>:<порт HTTPS>/dswsbobje/services/listServices, чтобы проверить защищенное соединение. После перехода по ссылке на вкладке сеанса отобразится trustedLoginWithX509.

9.10.2.1.3 Создание значения общего секретного ключа

1. Запустите консоль Central Management Console.
2. Перейдите в раздел *Аутентификация* > *Предприятие.*
3. В разделе *Доверительная аутентификация* установите флажок *Доверительная аутентификация включена*.
4. Выберите *Новый общий секретный ключ*. В результате будет создан общий секретный ключ.
5. Выберите *Загрузить общий секретный ключ* и затем *Обновить*.
6. Скопируйте загруженный файл TrustedPrincipal.conf в каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container\bin` в ОС Windows.

> **Примечание**
>
> Значение общего секретного ключа можно просмотреть, открыв файл TrustedPrincipal.conf в любом редакторе XML.

9.10.2.1.4 Настройка файла web.xml

1. Перейдите в каталог `<INSTALLDIR>\tomcat\webapps\dswsbobje\WEB-INF.`
2. Откройте файл web.xml в редакторе XML и обновите тег XML, добавив имя компьютера хоста CMS:

```
<context-param>
        <param-name>cms.default</param-name>
        <param-value>EnterHostMachineName</param-value>
    </context-param>
```

3. Добавьте приведенный ниже тег XML со значением общего секретного ключа. Дополнительные сведения о создании значения общего секретного ключа см. в разделе Создание значения общего секретного ключа [страница 425].

```
<context-param>
<param-name>trusted.auth.shared.secret</param-name>
<param-value>shared secret value</param-value>
</context-param>
```

4. Сохраните файл web.xml.

> **Примечание**
>
> Конфигурации, созданные в файле axis2.xml, будут отклонены, если выполняется обновление с версии ниже BI 4.2 SP04.

9.10.2.2 Веб-службы RESTful

> **Примечание**
>
> Для обеспечения единого входа (SSO) с помощью аутентификации X.509 пользователь должен существовать в платформе BI.

Ознакомьтесь с разделом "Настройка HTTPS/SSL" в *Руководстве администратора платформы Business Intelligence*, чтобы установить доверительную аутентификацию для веб-служб RESTful.

Чтобы установить доверительную аутентификацию с использованием сертификатов X.509, необходимо сгенерировать общий секретный ключ. Для получения дополнительных сведений см. раздел "Создание значения общего секретного ключа" в *Руководстве администратора платформы Business Intelligence*.

Кроме того, дополнительные сведения о конечной точке пакета SDK для служб REST см. по пути *Справочник по API-интерфейсу* > *Аутентификация* > */v1//logon/trustedx509* в *Руководстве разработчика по использованию веб-служб RESTful платформы Business Intelligence*.

9.10.2.2.1 Аутентификация X.509 для веб-служб RESTful на сервере Tomcat

В криптографии открытого ключа X.509 является стандартом, определяющим требования для безопасного цифрового сертификата. Сертификат X.509 проверяет владение открытым ключом пользователем или удостоверением службы.

Теперь можно включить аутентификацию X.509 для веб-служб RESTful на сервере приложений Tomcat, выполнив следующие шаги:

1. Включите SSL на Tomcat. Для получения дополнительных сведений см. Настройка SSL в Tomcat [страница 424].
2. Сгенерируйте общий секретный ключ. Для получения дополнительных сведений см. Создание значения общего секретного ключа [страница 425].
3. Откройте файл общего секретного ключа в текстовом редакторе.
4. Скопируйте общий секретный ключ.
5. Отредактируйте файл *biprws.properties*.
   a. Перейдите в каталог `<INSTALLDIR>/tomcat/webapps/biprws/WEB-INF/config/default`.
   b. Откройте файл *biprws.properties* в текстовом редакторе.
   c. Найдите *Trusted_Auth_Shared_Secret=*.
   d. Вставьте общий секретный ключ рядом со значением *Trusted_Auth_Shared_Secret=*.
   e. Сохраните файл *biprws.properties*.

9.10.3 Аутентификация X.509 для CMC

> **Примечание**
>
> Для обеспечения единого входа (SSO) с помощью аутентификации X.509 пользователь должен существовать в платформе BI.

Единый вход через аутентификацию X.509 можно обеспечить, выполнив следующие шаги:

1. Создание и настройка сертификатов и хранилищ ключей [страница 416]
2. Настройка одностороннего SSL [страница 420]
3. Настройка двухстороннего SSL [страница 420]
4. Создание общего секретного ключа [страница 421]
5. Передача общего секретного ключа с помощью файла TrustedPrincipal.conf [страница 421]
6. Редактирование файла Custom.jsp (для CMC) [страница 428]
7. Создание файла myScript.js (для CMC) [страница 428]
8. Настройка внутренних файлов и файлов пользовательских свойств BOE (для CMC) [страница 429]
9. Настройка файла Web.xml в BOE (для CMC) [страница 429]

9.10.3.1 Редактирование файла Custom.jsp (для CMC)

> ⓘ Примечание
>
> Прежде чем редактировать файл custom.jsp, создайте пользователя с именем компьютера в CMC. Если пользователь существует, на компьютере можно сразу перейти к выполнению следующих шагов:

1. Перейдите в каталог `<INSTALLDIR>\tomcat\webapps\BOE\WEBINF\eclipse\plugins\webpath.CmcApp\web\cutom.jsp` в com.businessobjects.webpath.InfoView.jar.
2. Отредактируйте файл custom.jsp

```
<\!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","Shared
Secret Key")
request.getSession().setAttribute("MyUser", "John Doe");
%>
<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>
```

> ⓘ Примечание
>
> Следует заменить значение общего секретного ключа, которое содержится в этом коде, новым ключом, а пользователя – именем компьютера, созданным в CMC.

9.10.3.2 Создание файла myScript.js (для CMC)

1. Перейдите в каталог `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\eclipse\plugins\webpath.CmcApp\web\noCacheCustomResources and create myScript.js`.
2. Добавьте в файл myScript.js следующий код:

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

3. Перезапустите сервер Tomcat.

9.10.3.3 Настройка внутренних файлов и файлов пользовательских свойств BOE (для CMC)

1. Перейдите в каталог `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\internal\CmcApp.properties`.
2. Откройте файл CmcApp.properties и добавьте параметры:

   ```
   sso.supported.types=vintela, trustedIIS, trustedHeader, trustedParameter,
   trustedCookie, trustedSession, trustedUserPrincipal, trustedVintela,
   trustedX509, sapSSO, sitemindera
   ```
3. Перезапустите сервер Tomcat.

9.10.3.4 Настройка файла Web.xml в BOE (для CMC)

1. Перейдите в каталог `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF`.
2. Отредактируйте файл web.xml в этом расположении, используя приведенный ниже код:

   ```
   <init-param>
   <param-name>extendedFrameworkExports</param-name>
   <param-
   value>com.businessobjects.servletbridge.listener,com.businessobjects.servletbr
   idge.customconfig,com.businessobjects.servletbridge.external,com.businessobjec
   ts.servletbridge.session,com.businessobjects.resource,oracle.jdbc.pool,com.sie
   bel.data,com.jdedwards.system.xml,org.ietf.jgss,com.sap.security.api</param-
   value>
   </init-param>
   ```
3. Добавьте в файл web.xml параметры, выполнив следующие шаги:
   a. Перейдите в каталог `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\eclipse\plugins\webpath.CmcApp\web\WEB-INF\web.xml`
   b. Добавьте параметры, указанные ниже:

      ```
      <init-param>
      <param-name>trusted.auth.shared.secret</param-name>
      <param-value>Shared_Secret_Key</param-value>
      </init-param>
      ```
   c. Повторите шаги, перейдя в каталог `<INSTALLDIR>\tomcat\work\Catalina\localhost\BOE\eclipse\plugins\webpath.CmcApp\web\WEB-INF\web.xml`

> **Примечание**
>
> Чтобы проверить правильность настройки доверительной аутентификации, воспользуйтесь следующим URL-адресом для доступа к приложению стартовой панели BI: https://[имя_cms]:8443/BOE/BI/logon.jsp, где [имя_cms] — это имя компьютера, на котором размещена система CMS.

9.11 Аутентификация OpenID Connect

Можно включить аутентификацию OpenID Connect.

Аутентификация OpenID Connect работает на основе сервера аутентификации (OAuth). Как и в случае поддержки облачного диска, аутентификация OpenID Connect также основана на конфигурации сервера аутентификации. Для получения дополнительных сведений о конфигурации сервера аутентификации см. Конфигурация сервера авторизации [страница 778].

Аутентификация OpenID Connect разработана на основе аутентификации Enterprise.

Как и в случае аутентификации SAML, пользователей необходимо заранее импортировать на платформу BI как пользователей Enterprise (secEnterprise).

> ⓘ Примечание
>
> При импорте пользователей необходимо убедиться, что также включен ид. электронной почты пользователя.

В отличие от аутентификации SAML, для аутентификации OpenID Connect применяется следующее:

- Все настройки должны быть выполнены в бэкэнде платформы BI, а не на уровне сервера приложений.
- Она не зависит от доверительной аутентификации.

Аутентификация OpenID Connect поддерживается только для стартовой панели BI и OpenDocument.

9.11.1 Активация аутентификации OpenID Connect

Аутентификация OpenID Connect поддерживается только для стартовой панели BI и OpenDocument.

Для получения сведений о том, как включить аутентификацию OpenID Connect, см. Настройки аутентификации Enterprise [страница 249]. После включения аутентификации OpenID Connect в подключаемом модуле аутентификации Enterprise в бэкэнде необходимо активировать тот же уровень приложения для поддерживаемых приложений (например, файл `FioriBI.properties` для стартовой панели BI и файл `OpenDocument.properties` для приложений OpenDocument в папке `WEB-INF/config/custom`).

Для включения рабочего процесса веб-аутентификации SSO установите `logon.webssoauthentication.framework` на `OpenId`.

Установите `openid.restful.url` на URL-адрес веб-служб RESTful ландшафта (например, `https://<server>:8443/biprws`).

Можно выполнить вход в стартовую панель BI через OpenID с использованием URL-адреса `…/BO/BI`. Однако после входа с помощью аутентификации OpenID Connect на стартовую панель BI можно обнаружить, что к URL-адресу будет добавлен путь контекста заполнителя "WEBSSO". Он останется в пути URL-адреса даже после выхода. Если вам потребуется снова войти в систему из этого же окна с использованием того же самого URL-адреса, вам будет необходимо удалить "WEBSSO" из URL-адреса браузера.

10 Ссылка на источник данных

10.1 Расширенное сопоставление учетных данных

В BI 4.2.X и более ранних версиях для каждого пользователя в CMC администратор мог сохранить только один набор учетных данных базы данных.

Эта функция требует, чтобы администратор выполнил ведение одинаковых учетных данных для всех баз данных. Начиная с BI 4.3 для каждого пользователя можно сохранить несколько наборов учетных данных баз данных с помощью ссылок на источники данных.

> ⓘ Примечание
>
> Функция расширенного сопоставления учетных данных, введенная в платформе SAP BusinessObjects Business Intelligence 4.3, поддерживается только в средстве дизайна информации. Расширенное сопоставление учетных данных не поддерживается в средстве создания юниверсов.

Ссылка на источник данных в CMC

В CMC администратор создает ссылку на источник данных на платформе BI. Затем эта ссылка на источник данных используется в свойствах пользователя, где администратор определяет для него один набор учетных данных базы данных. Затем эта ссылка на источник данных используется как часть сопоставления учетных данных, представляющего собой режим аутентификации, доступный для соединений.

Администратор получает возможность выбрать нужную ссылку на источник данных, когда в качестве режима аутентификации выбрано сопоставление учетных данных. Точно так же администратор может создать несколько ссылок на источники данных, если к платформе BI подключено несколько баз данных, и определить уникальные учетные данные для каждого пользователя.

> ⓘ Примечание
>
> При импорте пользователей с помощью CSV-файла, переносе пользователей с использованием диспетчера переноса объектов или синхронизации учетных данных источника данных при входе в систему для типов аутентификации Enterprise, LDAP, Windows AD платформа BI присваивает учетные данные ссылке на источник данных по умолчанию.

Ссылка на источник данных на стартовой панели BI

Использование ссылок на источники данных доступно также на стартовой панели BI, где вы можете обновлять и сопоставлять свои учетные данные пользователя.

> **Примечание**
>
> Вы не можете редактировать сведения о *ссылке на источник данных*, но можете редактировать поля *Имя учетной записи*, *Пароль* и *Подтверждение пароля*.

Принцип работы

Предположим, что:

- В платформе BI доступны две ссылки на источники данных, например DSR1 для вашей базы данных продаж и DSR2 для базы данных финансов
- Для каждой ссылки на источник данных в свойствах пользователя A определены учетные данные базы данных
- Существует два соединения, CN1 и CN2, которые настроены для использования в качестве режима аутентификации сопоставления учетных данных
- DSR1 связана с соединением CN1, а DSR2 аналогично связана с CN2

Теперь, если пользователь A пытается обновить отчет, для которого требуется доступ к базе данных продаж, платформа BI выполняет поиск DSR1 в свойствах пользователя и использует учетные данные базы данных, определенные для DSR1, для установки соединения.

Чтобы использовать ссылку на источник данных, необходимо выполнить следующие задачи.

1. Создать ссылку на источник данных [страница 432]
2. Определение учетных данных базы данных для ссылки на источник данных для пользователя в CMC [страница 433]
3. Связать ссылку на источник данных с соединением OLAP [страница 434]

> **Примечание**
>
> Также можно настроить сопоставление учетных данных для реляционных соединений и соединений OLAP в средстве дизайна информации.

10.1.1 Создать ссылку на источник данных

Ссылка на источник данных выступает в качестве переменной, которую администратор создает на платформе BI для сохранения уникального набора учетных данных для каждого пользователя. Для создания ссылки на источник данных выполните следующие шаги:

1. Войдите в CMC.
2. В разделе "Определение" выберите "Ссылки на источники данных".
3. Выберите значок (Создать новую ссылку на источник данных).
4. Добавьте заголовок ссылки на источник данных и описание.
5. Нажмите "OK".

Вы успешно создали ссылку на источник данных.

10.1.2 Определение учетных данных базы данных для ссылки на источник данных для пользователя в CMC

Чтобы пользователь мог подключиться к базе данных, для ссылки на источник данных в свойствах пользователя должны быть определены учетные данные базы данных. Чтобы определить учетные данные базы данных в CMC, выполните следующие шаги.

1. Войдите в CMC.
2. Выберите *Пользователи и группы*.
3. Откройте контекстное меню пользователя в *Списке пользователей*.
4. Выберите *Свойства* и нажмите *Добавить* в разделе *Учетные данные источника данных*.
5. Выберите предпочтительную ссылку на источник данных.
6. Введите значения в поля *Имя учетной записи*, *Пароль* и *Подтверждение пароля*.
7. Повторите процесс с шага 4, чтобы добавить другую ссылку на источник данных.
8. Нажмите *Сохранить и закрыть*.

   Учетные данные базы данных для ссылки на источник данных успешно определены.

10.1.3 Определение учетных данных базы данных для ссылки на источник данных для пользователя на стартовой панели BI

Чтобы пользователь мог подключиться к базе данных, для ссылки на источник данных в свойствах пользователя должны быть определены учетные данные базы данных.

Использование ссылок на источники данных теперь доступно на стартовой панели BI, где вы можете обновлять и сопоставлять свои учетные данные пользователя. Учетные данные базы данных синхронизированы между CMC и стартовой панелью BI.

Чтобы определить учетные данные базы данных на стартовой панели BI, выполните следующие шаги.

1. Выполните вход на стартовую панель BI.
2. Выберите (Настройки пользователя), щелкните опцию (*Настройки*) в раскрывающемся списке.

   Будет открыто окно *Параметры*.
3. Щелкните *Учетная запись пользователя (администратор)*.

   Откроется страница "Учетная запись пользователя" с тремя вкладками: *Информация учетной записи*, *Учетные данные базы данных* и *Токены авторизации*.
4. Щелкните *Учетные данные базы данных*.

   Можно просмотреть синхронизированные данные пользователя из CMC, отображаемые здесь.

   > **Примечание**
   >
   > Вы не можете редактировать сведения *ссылки на источник данных*.

> Однако можно редактировать поля *Имя учетной записи*, *Пароль* и *Подтверждение пароля*.

При изменении пароля на экране появится всплывающее сообщение *Изменения некоторых параметров вступят в силу после перезагрузки страницы*.

5. Нажмите *Сохранить* и *Закрыть*, чтобы сохранить сопоставленные изменения учетных данных.

10.1.4 Определить учетные данные базы данных для ссылки на источник данных для группы

Чтобы пользователь мог подключиться к базе данных, для ссылки на источник данных в свойствах пользователя должны быть определены учетные данные базы данных.

> ⓘ Примечание
>
> Эта задача не служит для обновления ссылок на источники данных для членов подгрупп. Те же самые шаги можно выполнить для подгруппы, чтобы обновить ссылки на источники данных для ее членов.

Чтобы определить учетные данные базы данных, выполните следующие шаги:

1. Войдите в CMC.
2. Выберите *Пользователи и группы*.
3. Откройте контекстное меню группы пользователей и выберите *Диспетчер учетных записей*.
4. Установите флажок *Учетные данные базы данных* и выберите *Добавить*.
5. Введите значения в обязательные поля.
6. Нажмите *Сохранить и закрыть*.

Вы успешно определили новую ссылку на источник данных с учетными данными базы данных для членов группы пользователей. Вы можете перейти к *Свойствам* любого пользователя этой группы, чтобы проверить ссылку на источник данных, которую вы обновили сейчас.

10.1.5 Связать ссылку на источник данных с соединением OLAP

Администратор получает возможность выбрать нужную ссылку на источник данных, когда в качестве режима аутентификации для соединения выбрано сопоставление учетных данных.

Чтобы связать ссылку на источник данных с соединением, выполните следующие шаги:

1. Войдите в CMC.
2. Выберите *Соединения OLAP*.
3. Откройте существующее соединение или создайте новое.
4. В поле *Аутентификация* выберите *Сопоставление учетных данных*.
   Появится поле *Ссылка на источник данных*.

5. Выберите ссылку на источник данных.
6. Введите другие необходимые данные и выберите *Сохранить*.

Вы успешно связали ссылку на источник данных с соединением OLAP.

11 Администрирование сервера

11.1 Работа с областью управления CMC "Серверы"

Область управления серверами CMC – 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 CCM. Можно выбрать узел, щелкнув его, с целью просмотра серверов для узла или управления ими.

Параметр дерева навигации	Описание
Категории служб	Выводит список типов служб, которые могут быть в вашем развертывании. Категории служб подразделяются на корневые службы платформы BI и службы, связанные с конкретными компонентами SAP BusinessObjects. Категории служб включают в себя: • *Службы соединений* • *Корневые службы* • *Службы Crystal Reports* • *Службы объединения данных* • *Службы Диспетчера переноса объектов* • *Службы Analysis Services* • *Службы Web Intelligence* Выберите категорию службы в списке навигации для просмотра серверов категории или управления ими. **Примечание** На сервере могут размещаться службы, принадлежащие нескольким категориям служб. Следовательно, один сервер может быть в нескольких категориях служб.
Состояние сервера	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: • *Остановлено* • *Запуск* • *Инициализация* • *Выполнение* • *Остановка* • *Выполнение с ошибками* • *Сбой* • *Ожидание ресурсов*

О панели "Сведения"

В зависимости от параметров, выбранных в дереве навигации, на панели *Сведения* в правой части области управления "Серверы" отображается список серверов, серверных групп, состояний, категорий или узлов. В таблице ниже перечислены данные по серверам, отображаемые на панели *Сведения*.

> **Примечание**
>
> На панели *Сведения* обычно отображаются имена и описания узлов, серверных групп, категорий и состояний.

Столбец панели "Сведения"	Описание
Имя сервера или *Имя*	Отображает имя сервера.
Состояние	Отображает текущее состояние сервера С помощью списка *Состояние сервера* в дереве навигации можно выполнить упорядочивание по состоянию сервера. Возможны следующие состояния сервера: • *Остановлено* • *Запуск* • *Инициализация* • *Выполнение* • *Остановка* • *Выполнение 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.
Тип	Отображает тип сервера.
Имя хоста	Отображает имя хоста для данного сервера.
Работоспособность	Показывает общую работоспособность сервера. Возможны следующие состояния сервера: • *Зеленый* (Работает нормально) • *Янтарный* (Внимание) • *Красный* (Осторожно) Состояние работоспособности сервера напрямую зависит от статуса наблюдения сервера. Например, состояние работоспособности центрального сервера управления зависит от статуса `<NODENAME>.CentralManagementServerWatch`. Доступ к подробным сведениям наблюдений можно получить на странице *Мониторинг* в CMC: на вкладке *Список наблюдений* выберите наблюдение и нажмите *Редактировать*. Отобразятся *Правило для состояния "Внимание"* и *Правило для состояния "Осторожно"* для просматриваемого наблюдения, соответствующие желтому и красному состояниям работоспособности соответственно.

Столбец панели "Сведения"	Описание
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.

11.2 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.

Связанные сведения

ccm.exe [страница 1141]

11.3 Управление серверами в UNIX

Исполняемый файл `ccm.sh` позволяет запускать, останавливать, перезапускать, включать и отключать сервера в существующем развертывании UNIX в командной строке.

Связанные сведения

ccm.sh [страница 1133]

11.4 Просмотр и изменение статуса сервера

11.4.1 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 сервер мог отвечать на запросы платформы BI, его нужно запустить и включить. Выключенный сервер все еще работает как процесс; однако он не принимает запросы от платформы BI. Если сервер остановлен, его процесс не выполняется.

В этом разделе описывается изменение состояния серверов из CMC.

Связанные сведения

Просмотр статуса сервера [страница 440]
Просмотр состояния служб [страница 441]
Запуск, остановка и перезапуск серверов [страница 441]
Включение и выключение серверов [страница 444]
Остановка центрального сервера управления (CMS) [страница 444]
Автоматический запуск сервера [страница 443]

11.4.1.1 Просмотр статуса сервера

1. Перейдите в область управления CMC *Серверы*.

   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 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 вам нужно быстро просмотреть список серверов, которые неправильно запускаются или неожиданно остановились.

11.4.1.2 Просмотр состояния служб

В случае сбоя какой-либо службы для хост-сервера устанавливается состояние *Выполнение с ошибками* (означает, что по крайней мере одна служба запущена успешно) или *Сбой* (означает, что не удалось запустить ни одну службу). Состояния сервера можно просмотреть в CMC и CCM. Однако также можно просмотреть статус отдельных служб на странице *Свойства* сервера в CMC.

1. Перейдите в область управления CMC *Серверы*.

   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.

Связанные сведения

Просмотр состояний серверов [страница 440]

11.4.2 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 CMC выдаст подсказку для перезапуска 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 определенных свойств и параметров необходимо остановить серверы платформы BI.
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, CMC 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 удается, 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*.

Связанные сведения

Включение и выключение серверов [страница 444]

11.4.2.1 Запуск, остановка или перезапуск серверов при помощи CMC

1. Перейдите в область управления CMC *Серверы*.

   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*.

11.4.2.2 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 *Закрыть*, чтобы вернуться в CCM.

11.4.2.3 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 *OK*, чтобы закрыть страницу свойств сервера, и снова нажмите кнопку *OK*. 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.

11.4.3 Остановка центрального сервера управления (CMS)

Если в вашей установке платформы BI имеется более одного Центрального сервера управления (CMS), вы можете 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 BI без обслуживания.

Однако, если в развертывании платформы BI имеется только один CMS, то его выключение сделает платформу 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 BI, так как все другие серверы в узле также будут остановлены.

> ⓘ Примечание
>
> Можно столкнуться с ситуацией, когда CMS остановился, и возникла необходимо 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 *OK*, чтобы закрыть страницу свойств сервера, и снова нажмите кнопку *OK*. 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.

Связанные сведения

Использование узлов [страница 489]
Клонирование серверов [страница 447]
Кластеризация центральных серверов управления (CMS) [страница 450]

11.4.4 Включение и выключение серверов

При отключении сервера платформы BI допускается получение им новых запросов и отправка ответов, однако, выполняемые им 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.

> ⓘ Примечание
>
> CMS нельзя включить или выключить.

11.4.4.1 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*.

11.4.4.2 Включение или отключение сервера Windows в CCM

1. В CCM выберите *Управление серверами*.
2. При отображении соответствующей подсказки войдите в CMS под учетными данными пользователя платформы BI с правами администратора.
3. В диалоговом окне *Управление серверами* выберите сервер, который нужно включить или выключить.
4. Нажмите кнопку *Включить* или *Выключить*.
5. Щелкните *Закрыть*, чтобы вернуться в CCM.

11.5 Добавление, клонирование и удаление серверов

11.5.1 Добавление, клонирование и удаление серверов

Чтобы добавить новое оборудование для платформы BI путем установки компонентов сервера на дополнительные компьютеры, запустите на нужных компьютерах программу установки платформы BI. 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 BI*.

11.5.1.1 Добавление сервера

Можно запускать несколько экземпляров одного и того же сервера платформы BI на одном и том же компьютере. Чтобы добавить сервер, выполните следующие действия.

1. Перейдите в область управления CMC *Серверы*.
2. В меню *Управление* щелкните *Создать* > *Новый сервер*.
   Появится диалоговое окно *Создать новый сервер*.
3. Выберите пункт *Категория службы*.
4. Выберите тип службы из списка *Выбрать службу*, затем нажмите кнопку *Далее*.
5. Для добавления дополнительной службы к серверу выберите службу в списке *Доступные дополнительные службы* и нажмите кнопку >.

   > **Примечание**
   >
   > Дополнительные службы доступны не для всех типов серверов.

6. После добавления необходимых дополнительных служб нажмите кнопку *Далее*.
7. Если архитектура платформы BI состоит из нескольких узлов, в списке *Узел* выберите узел, на который требуется добавить новый сервер.
8. В поле *Имя сервера* введите имя для сервера.

   Каждый сервер на системе, должен иметь уникальное имя. Соглашение по присвоению имен по умолчанию: `<ИМЯ_УЗЛА>.<тип_сервера>` (если на компьютере есть более одного сервера определенного 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 CMC, но при этом он не запускается и не включается.
12. Используйте CMC для включения и запуска нового сервера, если требуется, чтобы он начал отвечать на запросы платформы BI.

11.5.1.2 Клонирование серверов

Если необходимо добавить новый экземпляр сервера к развертыванию, можно клонировать существующий сервер. Клонированный сервер сохраняет параметры конфигурации исходного сервера, за исключением общих параметров и параметров командной строки. Это особенного 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 CMS в другой узел, можно клонировать его в новом узле. Клонированный сервер CMS появляется в новом узле с такими же параметрами конфигурации, что и у исходного сервера CMS, за исключением общих параметров и параметров командной строки.

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.

> ⓘ Примечание
>
> Перед клонированием серверов убедитесь, что на всех компьютерах в развертывании установлена одинаковая версия платформы BI (и всех обновлений, если имеются).

> ⓘ Примечание
>
> Можно клонировать серверы с любого компьютера. Однако серверы можно клонировать только на компьютеры, на которых установлены необходимые двоичные файлы.

> ⓘ Примечание
>
> 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.

11.5.1.2.1 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 А с несколькими дисками 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 компьютере Б 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 А на компьютер Б, если заполнители используются для временного каталога Auditing, заполнители будут разрешаться и сервер событий будет функционировать правильно. Если заполнители не используются, будет происходить сбой сервера событий, пока параметр временного каталога Auditing не будет перезаписан вручную.

11.5.1.2.2 Порядок клонирования сервера

1. На компьютере, где необходимо добавить клонированный сервер, войдите в область управления CMC *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 *OK*.
   В области управления CMC *Серверы* добавится новый сервер.

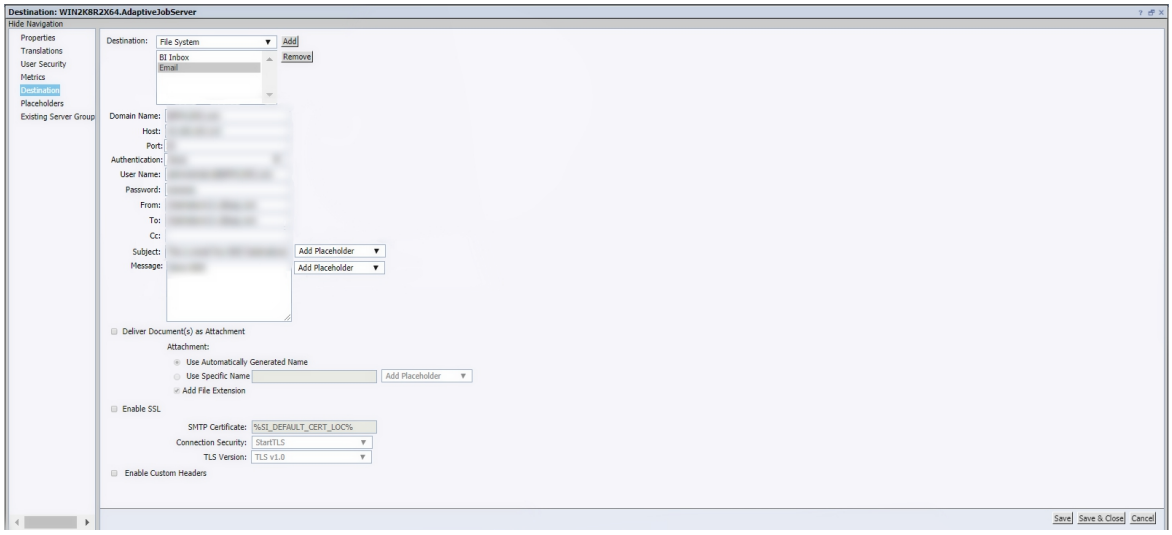
11.5.1.3 Удаление сервера

1. Перейдите в область управления *Серверы* в CMC.
2. Остановите сервер, который хотите удалить.
3. Щелкните сервер правой кнопкой мыши и выберите команду *Удалить*.
4. При запросе подтверждения нажмите кнопку *OK*.

11.6 Добавление пользовательского интернет-заголовка

Интернет-заголовок сообщения электронной почты включает сведения о составителе сообщения, сервере электронной почты, через который отправлено сообщение, и средстве или ПО, использованном для составления сообщения. Теперь можно добавить пользовательские интернет-заголовки в сообщения электронной почты, запланированные из платформы SAP BusinessObjects BI. Для добавления пользовательских заголовков выполните следующие шаги:

1. Войдите в *CMC*.
2. Выберите *Серверы* и затем *Список серверов*.
3. Нажмите *Адаптивный сервер заданий*, чтобы открыть контекстное меню, и выберите *Места назначения*.
4. В мастере *мест назначения* выберите *Электронная почта* и добавьте необходимые сведения для каждого поля, как указано ниже:



5. Установите флажок *Включить пользовательские заголовки* и добавьте интернет-заголовки в пустое поле, как указано ниже:

6. Нажмите *Сохранить и закрыть*.

Сообщения электронной почты с запланированными документами теперь содержат интернет-заголовки.

> **Примечание**
>
> - При планировании выберите *Использовать настройки по умолчанию*, чтобы добавить пользовательские интернет-заголовки в запланированные сообщения электронной почты.
> - Каждый *адаптивный сервер заданий* необходимо настроить, чтобы обеспечить добавление пользовательских заголовков в каждое сообщение электронной почты.

11.7 Кластеризация центральных серверов управления (CMS)

11.7.1 Кластеризация центральных серверов управления (CMS)

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 BI. Такая высокая доступность позволяет убедиться в том, что пользователи платформы BI 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* CMC.

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 удается вовремя обработать эти запросы, то производительность платформы BI 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 BI (включая исправления, если они доступны).
  - Убедитесь, что все CMS подключены к базе данных системы CMS одинаковым способом (с использованием собственных драйверов или драйверов 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 развертывании WAR-файла см. в *руководстве по установке платформы SAP BusinessObjects Business Intelligence*.
- Убедитесь, что все CMS в кластере работают в одной и той же локальной сети.
- 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*.
- Включение аудита на одном CMS будет действовать как настройка в кластеризованной среде. Также можно изменить сведения аудита базы данных на странице настроек в CMC. 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.

Связанные сведения

Изменение имени кластера CMS [страница 453]

11.7.1.1 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 репозиториев входящих и исходящих файлов. При необходимости обратитесь к администратору базы данных.

Связанные сведения

Добавление нового узла в кластер [страница 452]
Добавление сервера [страница 446]
Клонирование серверов [страница 447]
Обзор резервного копирования и восстановления [страница 575]

11.7.1.2 Добавление нового узла в кластер

При добавлении узла (узел – это коллекция серверов платформы BI, управляемых одним SIA) выводится подсказка на создание нового CMS или на кластеризацию узла в существующий CMS.

Для добавления узла в существующий кластер CMS, можно использовать программу установки. Запустите установку платформы BI и настройте программу на машине, где требуется установить новый член 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 добавить 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.

> **Примечание**
>
> Лицензии Edge BI и Crystal Server не поддерживают кластеризацию или развертывание с несколькими узлами. Однако начиная с версии Edge BI 4.3 SP2 и Crystal Server 2020 SP2, если Edge BI и Crystal Server развернуты в Linux, для служб Crystal Reports 2020 разрешен ОДИН узел Windows. Для получения дополнительной информации см. раздел Распределение служб SAP Crystal Reports 2020 на сервер Windows.

Связанные сведения

Использование узлов [страница 489]

11.7.1.3 Добавление кластеров в файлы свойств веб-приложений

Если вы добавили в развертывание дополнительные системы CMS, эта информация фиксируется в файле `clusterinfo.1400.properties`, который доступен в папке `C:/Users/<имя_пользователя>/.businessobjects`. Этот файл создается или обновляется при перезапуске SIA.

> ⓘ Примечание
>
> В автономном развертывании Tomcat файл `clusterinfo.1400.properties` создается, только если вход в систему выполняется с одним из имен CMS. При обновлении кластера файл в автономном развертывании Tomcat не обновляется. Необходимо скопировать файл из CMS на свой компьютер Tomcat.

11.7.1.4 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
>
> Опытный администратор платформы BI должен обратить внимание, что дальнейшее использование параметра `-ns` в командной строке сервера для настройки, в которой выполняется регистрация сервера CMS, будет невозможно. Теперь этот выбор автоматически выполняется SIA.

11.7.1.4.1 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 *OK*, 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.

11.7.1.4.2 Изменение имени кластера в ОС UNIX

Используйте скрипт `cmsdbsetup.sh`. Для получения информации см. раздел «Скрипты Unix» главы "Администрирование в командной строке" *Руководства администратора платформы BI*.

Связанные сведения

Скрипты UNIX [страница 1133]

11.8 Управление группами серверов

Группы серверов служат для организации серверов платформы BI и помощи в управлении ими в системе. Можно выбрать определенный сервер или группу серверов для публикации (не для пользователя). Также можно группировать серверы по регионам или типам.

При группировке серверов по региону легко задать параметры обработки по умолчанию, расписания для повторного выполнения и места назначения планирования для пользователей, которые работают в том или ином региональном офисе. Можно связать объект отчета (такой как отчет Crystal или документ Web Intelligence) с отдельной группой серверов, чтобы его всегда обрабатывали одни и те же серверы. Запланированные объекты отчетов можно связать с определенной группой серверов, чтобы они всегда отправлялись на соответствующие принтеры, серверы файлов и т. д. Группы серверов особенно полезны при работе с системами, охватывающими несколько местоположений и часовых поясов.

Группы серверов особенно полезны при работе с системами, охватывающими несколько местоположений и часовых поясов. Например, используйте группы серверов для настройки системы платформы BI для отчетов, просматриваемых из различных местоположений, и для разных типов отчетов. При организации серверов по регионам можно выполнить для групп серверов следующие действия:

- Настроить параметры обработки по умолчанию
- Настроить расписания с повторением
- Настроить места назначения планирования для пользователей, работающих в определенном региональном офисе

- Связать объект отчета (такой как отчет Crystal или документ Web Intelligence) с отдельной группой серверов, чтобы его всегда обрабатывали одни и те же серверы
- Связать запланированные объекты отчетов с определенной группой серверов, чтобы они всегда отправлялись на соответствующие принтеры, серверы файлов и т. д.

Сгруппируйте серверы по типам при настройке объектов, которые требуется обрабатывать на серверах, которые оптимизированы для этих объектов.

После создания групп серверов настройте объекты для использования определенных групп серверов для планирования, просмотра и изменения отчетов. Для просмотра групп серверов используйте дерево навигации в области управления CMC *Серверы*. Параметр *Список групп серверов* отображает список групп серверов на панели *Сведения*, а параметр *Группы серверов* позволяет просматривать серверы, включенные в группу.

Пример: Группировка серверов обработки по типам

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 на основе базы данных DB2, можно создать группу серверов обработки для обработки отчетов только для сервера базы данных DB2. Для повышения производительности системы при просмотре отчетов можно настроить для отчетов постоянное использование данной группы серверов обработки для просмотра.

11.8.1 Создание группы серверов

Чтобы создать группу серверов, необходимо ввести имя и описание группы, а затем добавить в нее серверы.

11.8.1.1 Создание неисключающей группы серверов

Неисключающие группы серверов могут содержать серверы или группы серверов, которые входят в любую другую неисключающую группу серверов или общий пул серверов.

1. Перейдите в область управления CMC *Серверы*.
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 *OK*.
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.

> ⓘ Примечание
>
> В списке указываются только серверы, которые не входят ни в какую другую исключающую группу серверов.

9. Нажмите кнопку *OK*.

   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.

11.8.1.2 Создание исключающей группы серверов

Исключающие группы серверов содержат серверы и группы серверов, не входящие в какую-либо другую группу серверов или в общий пул серверов. Когда группа серверов создается как исключающая группа серверов, серверы, входящие в эту группу, не могут быть назначены любой другой группе серверов (исключающей или неисключающей), и серверы, добавленные в исключающую группу серверов, исключаются из общего пула. Это позволяет создавать группы серверов, отделенные от общей нагрузки системы BI.

1. Перейдите в область управления компонента CMC *Серверы*.
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. Установите флажок *Исключающая группа серверов*.

> ⓘ Примечание
>
> Исключающую группу серверов можно создать только на корневом уровне. Исключающую группу серверов для дочернего узла можно создать только в том случае, если корневая или родительская группа серверов является исключающей.
>
> > Пример
> >
> > Рассмотрим следующий сценарий, чтобы получить более ясное представление об исключающих группах серверов.
> >
> > Два сервера заданий JS1 и JS2 входят в общий пул серверов.
> >
> > Вы создаете исключающую группу серверов SG1.
> >
> > Вы добавляете JS1 в SG1.

> Вы планируете документ (D), выбрав опцию *Использовать только серверы, принадлежащие к выбранной группе*.
>
> Предположим, что и на JS1, и на JS2 уже выполняется несколько заданий.
>
> **Результат:** JS1 уже нагружен некоторыми заданиями, который должны быть обработаны. Однако поскольку JS1 теперь является частью SG1, JS1 получает только запросы на обработку потоков операций, назначенных SG1. То есть JS1 освобожден от общей системной нагрузки.

6. Нажмите кнопку *OK*.
7. В области управления *Серверы* в дереве навигации щелкните *Группы серверов* и выберите новую группу серверов.
8. Выберите *Добавить элементы* в меню *Действия*.
9. Выберите серверы, которые требуется добавить в группу, и нажмите кнопку >.

   > → Совет
   >
   > Удерживая нажатой клавишу `CTRL` + `, щелкните кнопкой мыши`, чтобы выбрать несколько серверов.

   > ⓘ Примечание
   >
   > В перечисленные серверы включены только те, которые еще не входят в другие группы серверов или в обший пул серверов.

10. Нажмите кнопку *OK*.

    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.

11.8.2 Преобразование исключающей группы серверов в неисключающую и наоборот

11.8.2.1 Преобразование исключающей группы серверов в неисключающую

Вы можете преобразовать существующую исключающую группу серверов в неисключающую.

Чтобы преобразовать исключающую группу серверов корневого уровня в неисключающую, выполните следующие действия:

1. Щелкните правой кнопкой мыши исключающую группу серверов, которую требуется преобразовать, и выберите *Свойства* в раскрывающемся списке.

Открывается диалоговое окно *Свойства*. Обратите внимание, что флажок *Исключающая группа серверов* установлен.

2. Снимите флажок *Исключающая группа серверов*.

   Появится предупреждающее сообщение.

3. Нажмите кнопку *OK*, чтобы подтвердить преобразование.
4. Нажмите кнопку *Сохранить и закрыть*.

   Исключающая группа серверов успешно преобразована в неисключающую.

> ⓘ Примечание
>
> В неисключающие можно преобразовывать только исключающие группы серверов корневого уровня.

11.8.2.2 Преобразование неисключающей группы серверов в исключающую

Вы можете преобразовать существующую неисключающую группу серверов в исключающую.

Чтобы преобразовать неисключающую группу серверов, которая содержит **независимые** серверы и группы серверов, выполните следующие действия:

1. Щелкните правой кнопкой мыши неисключающую группу серверов, которую требуется преобразовать, и выберите *Свойства* в раскрывающемся списке.

   Открывается диалоговое окно *Свойства*. Обратите внимание, что флажок *Исключающая группа серверов* не установлен.

2. Установите флажок *Исключающая группа серверов*.

   Появится сообщение об успешном выполнении.

3. Нажмите кнопку *OK*.
4. Нажмите кнопку *Сохранить и закрыть*.

   Неисключающая группа серверов успешно преобразована в исключающую.

> ⓘ Примечание
>
> Это можно сделать только для неисключающих групп серверов, которые содержат независимые серверы и группы серверов. Независимыми серверами и группами серверов называются серверы и группы серверов, не входящие в какую-либо другую группу серверов.

11.8.3 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.

11.8.3.1 Чтобы добавить подгруппы в группу серверов

1. Перейдите в область управления *Серверы* в CMC.
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 *OK*.

   Вы вернетесь в область управления *Серверы*, в которой будут перечислены все группы серверов, добавленные вами в родительскую группу.

11.8.3.2 Чтобы сделать одну группу серверов элементом другой

1. Перейдите в область управления CMC *Серверы*.
2. Выберите группу, которую нужно добавить в другую группу.

   > ⓘ Примечание
   >
   > Для исключающих групп серверов корневого уровня все исключающие группы серверов перечислены в разделе *Доступные группы серверов*. Поскольку исключающая группа серверов может иметь только одну родительскую группу серверов, вы можете выбрать только одну исключающую группу серверов и переместить ее в список *Элемент групп серверов*.
   >
   > Исключающие группы серверов дочернего уровня могут иметь только одну родительскую группу, в связи с чем в списке *Доступные группы серверов* у них отсутствуют группы серверов.

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 *OK*.

11.8.4 Изменение принадлежности сервера к группе

Принадлежность сервера к группе можно изменить, чтобы быстро добавить сервер в любую группу или подгруппу, созданную в системе (или удалить из нее).

Приведем пример: предположим, вы создали группы серверов для разных регионов. Вам нужно использовать единый центральный сервер управления (CMS) для нескольких регионов. Вместо того чтобы добавлять сервер CMS отдельно в группу каждого региона, можно воспользоваться ссылкой *Элемент* для данного сервера и добавить его сразу во все три региона.

11.8.4.1 Чтобы изменить принадлежность сервера к группе

1. Перейдите в область управления CMC *Серверы*.
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.

   > ⓘ Примечание
   >
   > Для групп серверов корневого уровня все исключающие группы серверов перечислены в разделе *Доступные группы серверов*. Поскольку исключающая группа серверов может иметь только одну родительскую группу серверов, вы можете выбрать только одну исключающую группу серверов и переместить ее в список *Элемент групп серверов*. После того, как вы выберете исключающую группу серверов в списке *Доступные группы серверов* и переместите ее в список *Элемент групп серверов*, исключающая группа серверов переносится из своей группы корневого уровня в новую группу серверов, с которой она сопоставляется.
   >
   > Для групп серверов дочернего уровня существующие родительские группы отображаются в списке *Элемент групп серверов*, а остальные исключающие группы серверов – в разделе *Доступные группы серверов*. При необходимости вы можете сопоставить дочернюю группу серверов с другой исключающей группой серверов.

3. Чтобы изменить принадлежность сервера к группам, стрелками переместите соответствующие группы серверов из одного списка в другой и нажмите кнопку *OK*.

> **Примечание**
>
> Параметр *Удалить из группы серверов* отображается только для исключающих групп серверов дочернего уровня. Исключающая группа серверов дочернего уровня, удаленная из родительской группы, по-прежнему остается исключающей и переносится на корневой уровень.
>
> Группы серверов отображаются на стартовой панели BI, если администратором из CMC предоставлены права безопасности пользователя для конкретных групп серверов.

11.8.5 Административный доступ к серверам и группам серверов для пользователей

Предоставление административных прав пользователям позволяет им выполнять задачи для серверов и групп серверов, такие как запуск и остановка серверов.

Исходя из конфигурации вашей системы и соображений безопасности, можно ограничить возможность управления серверами для администратора платформы BI или предоставить административный доступ 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 ее участникам административные права доступа к серверам. Также может потребоваться делегировать административные задачи серверов платформы BI другим лицам или передать каким-либо группам в организации управление собственными серверами.

> **Примечание**
>
> Можно выбрать сервер или группу серверов для публикации (не для определенного пользователя). Однако можно присвоить пользователям или группам пользователей административные права для определенного сервера или группы серверов.

11.8.5.1 Предоставление административных прав доступа к серверу или группе серверов

Можно присвоить пользователям или группам пользователей административные права для определенного сервера или группы серверов.

> **Примечание**
>
> Можно выбрать сервер или группу серверов для публикации (не для пользователя).

1. Перейдите в область управления CMC *Серверы*.
2. Щелкните правой кнопкой мыши сервер или группу серверов, для которых требуется предоставить административные права доступа, и выберите пункт *Безопасность пользователя*.

3. Нажмите кнопку *Добавить принципалов*, чтобы добавить пользователей или группы, которым требуется предоставить административные права доступа к серверу или группе серверов.
4. В диалоговом окне *Добавить принципалов*, выберите пользователя или группу для предоставления прав администратора для сервера или группы серверов и нажмите кнопку >.
5. Щелкните *Добавить и назначить безопасность*.
6. На экране *Назначение безопасности* выберите параметры безопасности для пользователя или группы и нажмите кнопку *OK*.

Связанные сведения

Права на платформе BI [страница 129]

11.8.5.2 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

Пользователь должен иметь разрешение на добавление объектов как минимум в одну папку до того, как он сможет сохранять отчеты в платформе BI.

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.

11.8.6 Сопоставление группы пользователей с группой серверов

Благодаря новой опции *Параметры по умолчанию* вы можете сопоставить группу пользователей с определенной группой серверов.

Чтобы сопоставить группу пользователей с группой серверов, выполните следующие шаги:

1. Войдите в CMC.
2. Выберите *Пользователи и группы*.
3. На странице *Пользователи и группы* щелкните правой кнопкой мыши группу пользователей (которую требуется сопоставить с группой серверов).
4. Щелкните *Параметры по умолчанию*.
5. На странице *Планирование группы серверов* укажите серверы, которые будут по умолчанию использоваться для планирования группы пользователей.

   Можно выбрать один из следующих вариантов:

   - (По умолчанию) Выберите *Использовать первый доступный сервер* для выполнения объекта на сервере, на котором в момент планирования доступно больше всего свободных ресурсов.
   - Выберите *Отдавать предпочтение серверам из выбранной группы*, чтобы выполнить объект на серверах определенной группы серверов. Затем выберите нужную группу серверов из раскрывающегося списка, чтобы указать предпочтение определенной группы серверов. Если в выбранной группе нет доступных серверов, объект будет выполнен на следующем доступном сервере из общего пула серверов.
   - Выберите *Использовать только серверы из выбранной группы*, чтобы выполнять объект только на серверах определенной группы серверов, и выберите требуемую группу серверов из раскрывающегося списка, чтобы использовать только эту группу. Если в выбранной группе нет доступных серверов, объект обрабатываться не будет. Кроме того, если сервер заданий отсутствует в назначенной группе серверов, задание остается в состоянии ожидания.

> ⓘ Примечание
>
> Чтобы сопоставить с группой пользователей исключающую или неисключающую группу серверов, нужно выбрать один из двух переключателей: *Отдавать предпочтение серверам, принадлежащим к выбранной группе* или *Использовать только серверы, принадлежащие к выбранной группе*.
>
> Аналогично можно назначить группы серверов для просмотра или обработки документов Crystal Reports и Web Intelligence, перейдя в раздел *Параметры по умолчанию* и выбрав *Параметры обработки Crystal Reports* и *Параметры обработки Web Intelligence*, соответственно.
>
> Если группа серверов привязана как обязательная, это означает, что используются **только** серверы из данной группы. Серверы из общего пула не используются. Если группа серверов привязана как предпочтительная, то, когда серверы в ней заняты, используются серверы из общего пула. Общий пул серверов включает все серверы, которые не являются частью какой-либо исключающей группы серверов. Для получения дополнительных сведений об исключающих группах серверов см. Создание исключающей группы серверов [страница 456].
>
> Присвоение группы серверов группе пользователей может быть сложной процедурой, так как один пользователь может входить одновременно в несколько групп пользователей. Кроме

того, каждую группу пользователей можно сопоставить с разными группами серверов. Каждую группу серверов можно присваивать как "обязательную" или как "предпочтительную".

Пример

Рассмотрим следующий сценарий.

Пользователь (U) входит в две группы пользователей, UG1 и UG2. Каждая группа пользователей сопоставляется с разной группой серверов, SG1 и SG2. Тогда возможны следующие результаты различных сценариев.

Сценарий	Результат
Вы планируете документ (D). Группа серверов 1 (SG1) задана на уровне UG1, группа серверов 2 (UG2) задана на уровне UG2. SG1 задается как обязательная (R). SG2 также задается как обязательная (R). На уровне документа (D) группа серверов не назначена.	Комбинация двух групп серверов (SG1 и SG2) выступает в роли обязательной (R) группы серверов. Поскольку обе группы серверов (SG1 и SG2) указаны как обязательные, серверы из общего пула НЕ используются.
Вы планируете документ (D). Группа серверов 1 (SG1) задана на уровне UG1, группа серверов 2 (UG2) задана на уровне UG2. SG1 задана как предпочтительная (P). SG2 также задана как предпочтительная (P). На уровне документа (D) группа серверов не назначена.	Комбинация двух групп серверов (SG1 и SG2) выступает в роли предпочтительной (P) группы серверов. Поскольку обе группы серверов (SG1 и SG2) указаны как предпочтительные, то, если в выбранных группах серверы недоступны, используются серверы из общего пула.
Вы планируете документ (D). Группа серверов 1 (SG1) задана в UG1, группа серверов 2 (UG2) задана в UG2. SG1 задается как обязательная (R). SG2 задана как предпочтительная (P). На уровне документа (D) группа серверов не назначена.	Комбинация двух групп серверов (SG1 и SG2) выступает в роли обязательной (R) группы серверов. Поскольку комбинация (SG1 и SG2) выступает в роли обязательной группы серверов, серверы из общего пула НЕ используются.

6. Нажмите кнопку *Сохранить и закрыть*.

   Вы успешно сопоставили группу пользователей с группой серверов.

Примечание

- Пользователь может входить в одну или несколько групп пользователей, и каждая из этих групп может входить в другие группы пользователей. Если группа серверов не связана с близлежащей группой пользователей, к которой относится пользователь, программа проверяет, связана ли группа серверов со следующим уровнем групп пользователей. Этот процесс длится до тех пор, пока программа не найдет группу пользователей,

которой назначена группа серверов. Когда программа находит группу серверов, связанную на уровне группы пользователей, она прекращает проверку. Если на уровне группы пользователей связано несколько групп серверов, рассматривается поведение комбинации двух групп серверов (описанное в вышеприведенной таблице). Рассмотрим следующий сценарий, чтобы лучше понять принципы назначения групп серверов.

> **Пример**
>
> **Сценарий.** Вы планируете документ (D).
>
> Пользователь (U) входит в две группы пользователей (UG1 и UG2). Однако на уровне UG1 и UG2 нет назначенной группы серверов.
>
> UG1 относится к группе пользователей 3 (UG3) , а UG2 – к группе пользователей 4 (UG4).
>
> Группа серверов 3 (SG3) задается на уровне UG3.
>
> SG3 задается как обязательная (R).
>
> **Результат.** Поскольку нет групп серверов, заданных на первом уровне (UG1 и UG2), программа проверяет, есть ли группы серверов, заданные на следующем уровне (UG3 и UG4). Поскольку SG3 задана на уровне UG3 и SG3 задана как обязательная, только серверы в SG3 используются для обработки объекта, а серверы из общего пула использовать невозможно.
>
> Это подразумевает, что если нет групп серверов, заданных на уровне группы пользователей, то программа проверяет, не заданы ли какие-либо группы серверов для ближайшего следующего уровня. Если программа обнаруживает, что группа серверов задана на уровне какой-либо группы пользователей, она прекращает поиск групп серверов на следующем уровне.

- На уровне документа может быть только одна назначаемая группа серверов, и назначить ее можно как обязательную (R) или предпочтительную (P). Однако пользователь может относиться к одной или нескольким группам пользователей, и в результате этого пользователю может быть назначено несколько групп серверов. Если группа серверов задается и на уровне документа (D), и на уровне группы пользователей (UG), то связь группы серверов на уровне документа всегда является приоритетной по сравнению со связью группы серверов на уровне группы пользователей. Рассмотрим следующий сценарий, чтобы лучше понять принципы назначения групп серверов.

  > **Пример**
  >
  > **Сценарий.** Вы планируете документ (D).
  >
  > Группа серверов 1 (SG1) задана на уровне D, и SG1 задана как обязательная.
  >
  > Группа серверов 2 (SG2) задана на уровне UG, и SG2 задана как предпочтительная.
  >
  > **Результат.** Используется SG1. Поскольку SG1 задана как обязательная, серверы из общего пула использоваться не могут.
  >
  > Так как группа серверов (SG1) уже задана на уровне документа (D), программа игнорирует назначение группы серверов на уровне группы пользователей. Это подразумевает, что назначение группы серверов на уровне документа считается предпочтительнее уровня группы пользователей.

- Вам необходимо убедиться, что все требуемые серверы входят в нужную группу серверов.

- Чтобы лучше разобраться в назначении групп серверов на уровне папок и групп пользователей, см. https://blogs.sap.com/2016/11/07/servergroup-enhancements-for-scheduling-in-4.2sp03/.

11.8.7 Сопоставление папки с группой серверов

Благодаря появлению опции *Параметры по умолчанию* теперь можно сопоставить папку с определенной группой серверов.

Чтобы сопоставить папку с группой серверов, выполните следующие шаги:

1. Выполните вход на консоль CMC.
2. Перейдите в раздел *Папки* и щелкните правой кнопкой мыши нужную папку (которую требуется сопоставить группе серверов).
3. Щелкните *Параметры по умолчанию*.
4. На странице *Планирование группы серверов* укажите серверы, которые будут по умолчанию использоваться для планирования на уровне папок.

   Можно выбрать один из следующих вариантов:

   - (По умолчанию) Выберите *Использовать первый доступный сервер* для выполнения объекта на сервере, на котором в момент планирования доступно больше всего свободных ресурсов.
   - Выберите *Отдавать предпочтение серверам из выбранной группы*, чтобы выполнить объект на серверах определенной группы серверов. Затем выберите нужную группу серверов из раскрывающегося списка, чтобы указать предпочтение определенной группы серверов. Если в выбранной группе нет доступных серверов, объект будет выполнен на следующем доступном сервере из общего пула серверов.
   - Выберите *Использовать только серверы из выбранной группы*, чтобы выполнять объект только на серверах определенной группы серверов, и выберите требуемую группу серверов из раскрывающегося списка, чтобы использовать только эту группу. Если в выбранной группе нет доступных серверов, объект обрабатываться не будет.

   ⓘ Примечание

   Чтобы сопоставить с папкой исключающую или неисключающую группу серверов, нужно выбрать один из двух переключателей: *Отдавать предпочтение серверам, принадлежащим к выбранной группе* или *Использовать только серверы из выбранной группы*.

   Аналогично можно назначить группы серверов для просмотра или обработки документов Crystal Reports и Web Intelligence, перейдя в раздел *Параметры по умолчанию* и выбрав *Параметры обработки Crystal Reports* и *Параметры обработки Web Intelligence*, соответственно.

   Если группа серверов привязана как обязательная, это означает, что используются **только** серверы из данной группы. Серверы из общего пула не используются. Если группа серверов привязана как предпочтительная, то, когда серверы в ней заняты, используются серверы из общего пула. Общий пул серверов включает все серверы, которые не являются частью какой-либо исключающей группы серверов. Для получения дополнительных сведений об исключающих группах серверов см. Создание исключающей группы серверов [страница 456].

5. Нажмите кнопку *Сохранить и закрыть*.

Вы успешно сопоставили папку с группой серверов.

ⓘ Примечание

- На уровне папки или документа может быть только одна назначаемая группа серверов, и назначить ее можно как обязательную (R) или предпочтительную (P). Если группа серверов задается на уровне папки (F), документа (D) и группы пользователей (UG), то назначение группы серверов на уровне документа всегда является приоритетным по сравнению с назначением на уровне папки, за которым следует назначение на уровне группы пользователей. Следовательно, при назначении группы серверов используется следующий порядок приоритетности:
  Документ > Папка > Группа пользователей
- Документ может относиться к папке, которая, в свою очередь, может относиться к другой родительской папке. Учитывая, что на уровне документа нет назначенной группы серверов, если с промежуточной папкой, в которой хранится документ, не связана ни одна группа серверов, программа проверяет, связана ли группа серверов со следующей родительской папкой. Этот процесс длится до тех пор, пока программа не найдет родительскую папку, которой назначена группа серверов. Когда программа находит группу серверов, привязанную на уровне папки, она прекращает проверку. Рассмотрим следующий сценарий, чтобы лучше понять принципы назначения групп серверов.

  #### Пример

  Сценарий. Вы планируете документ (D).

  Однако на уровне документа нет назначенной группы серверов.

  Документ (D) относится к папке (F). Однако на уровне F нет назначенной группы серверов.

  Папка (F), в свою очередь, является частью другой папки: родительской папки (PF). Группа серверов (SG) задается на уровне PF.

  SG задается как обязательная (R).

  Результат. Поскольку нет групп серверов, заданных на уровне документа (D), программа проверяет, есть ли группы серверов, заданные на уровне папки (F). Поскольку, опять же, нет групп серверов, заданных на уровне F, программа проверяет, есть ли группы серверов, заданные на следующем уровне – уровне родительской папки (PF). Поскольку SG задана на уровне PF как обязательная, только серверы в SG используются для обработки объекта, а серверы из общего пула использовать невозможно.

  Это подразумевает, что если нет групп серверов, заданных на уровне документа, то программа проверяет, не заданы ли какие-либо группы серверов для следующей папки. Если программа обнаруживает, что группа серверов задана на уровне какой-либо папки, она прекращает поиск групп серверов на следующем уровне.

  Аналогично, если ни одна группа серверов не задана ни на уровне документа, ни на уровне папок, программа ищет назначение группы серверов на уровне группы пользователей.
- Вам необходимо убедиться, что все требуемые серверы входят в нужную группу серверов.

- Чтобы лучше разобраться в назначении групп серверов на уровне папок и групп пользователей, см. https://blogs.sap.com/2016/11/07/servergroup-enhancements-for-scheduling-in-4.2sp03/.

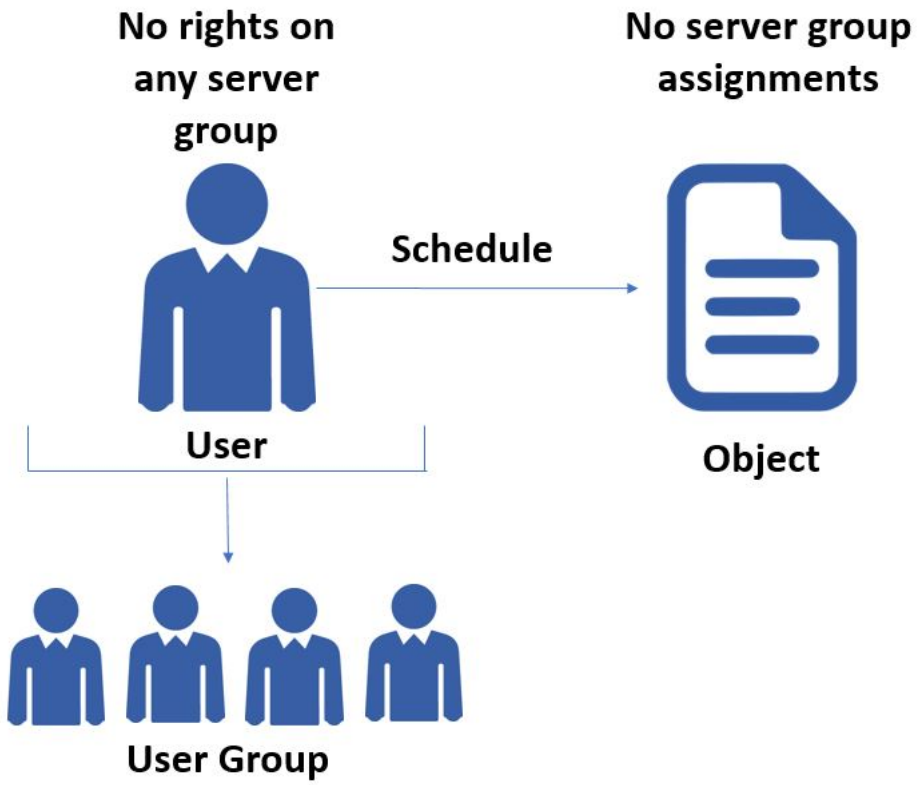
11.8.8 Общие сведения об управлении правами для группы серверов

Вы можете включить права доступа для группы серверов на уровне пользователя или группы пользователей. Это означает, что вы можете управлять доступом к группам серверов каждого пользователя или группы пользователей.

> **Примечание**
>
> - В следующих сценариях в качестве процесса для пояснения управления правами для группы серверов использовалось планирование. Аналогичным образом общие сведения об управлении правами для группы серверов можно использовать для просмотра и кэширования.
> - Планирование объекта может быть успешным, если серверы доступны в группе серверов или в комбинации групп серверов. Если доступные серверы отсутствуют, выполнить планирование не удастся.

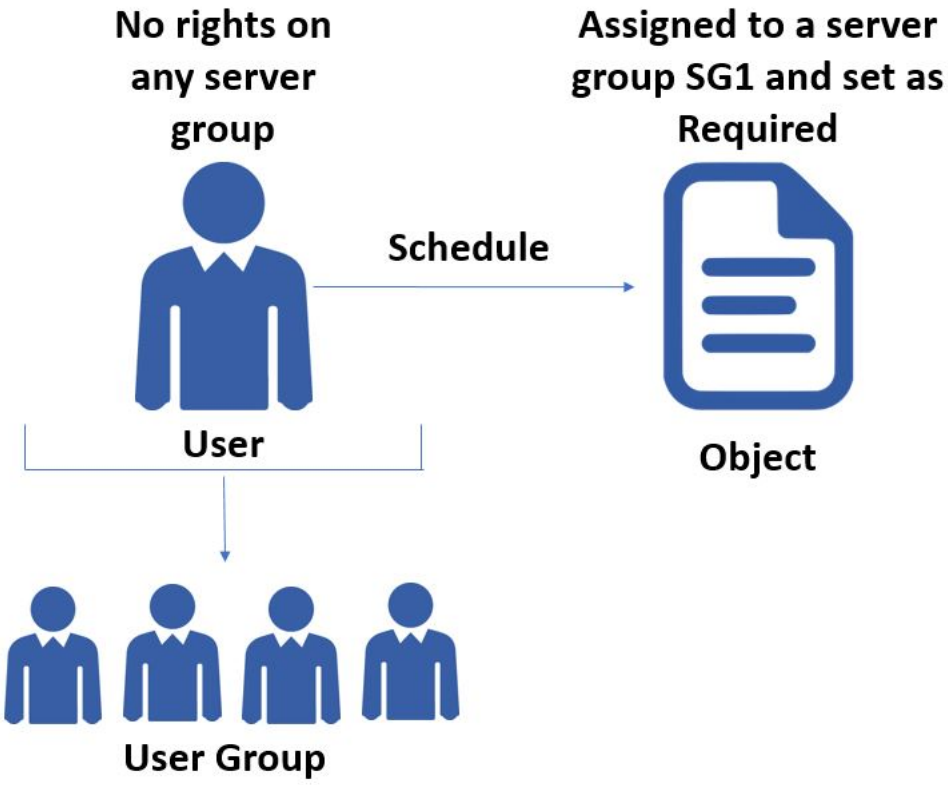
Сценарий 1:

Рассмотрим идеальный сценарий, где пользователь входит в группу пользователей в платформе Business Intelligence. У пользователя и связанной с ним группы пользователей нет прав ни в одной из групп серверов. Сейчас пользователю нужно запланировать объект, который также не назначен ни одной группе серверов.



Сценарий 2:

Когда вы изменяете вышеприведенный сценарий, назначая группу серверов объекту, планирование объекта выполнить не удается.



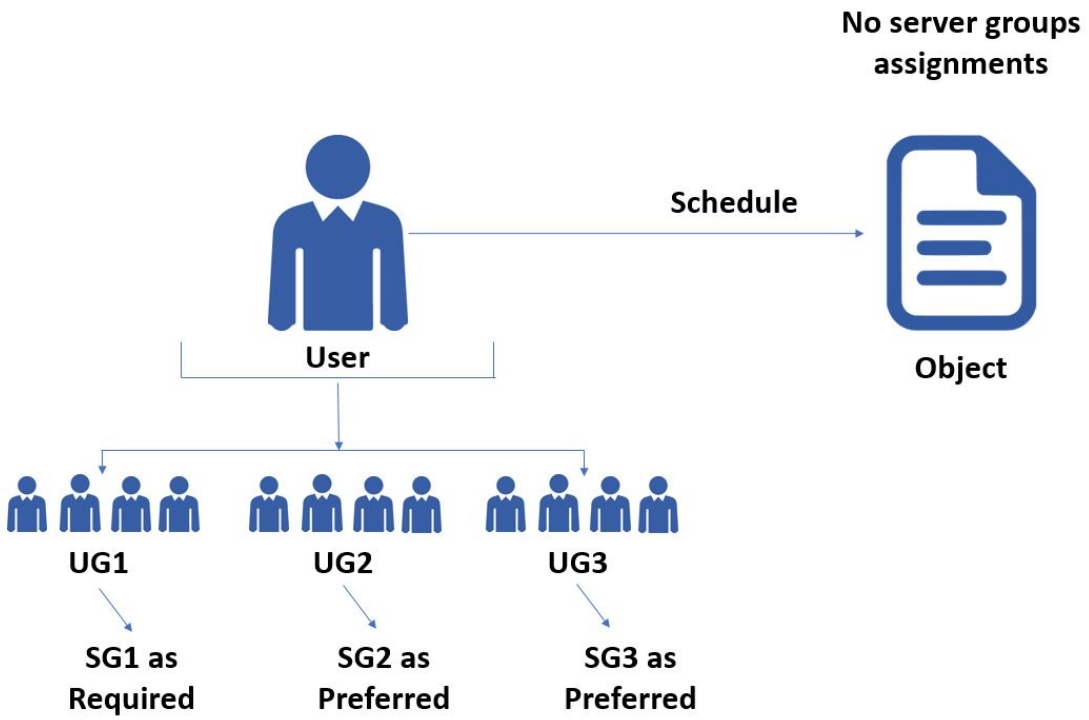
Когда пользователь планирует объект, платформа проверяет назначения групп серверов объекту. Если группа серверов назначена объекту, платформа проверяет, имеет ли пользователь права на просмотр в группе серверов.

Во втором сценарии ни у пользователя, ни у связанной с ним группы пользователей нет прав в SG1. Это приводит к сбою задания планирования. Если вы хотите, чтобы пользователь успешно запланировал объект в этом сценарии, убедитесь, что пользователь или любые связанные группы пользователей имели права на просмотр для SG1.

Сценарий 3:

> ⓘ Примечание
>
> Для сценариев 3 и 4 предполагается, что пользователь наследует права от связанных с ним групп пользователей.

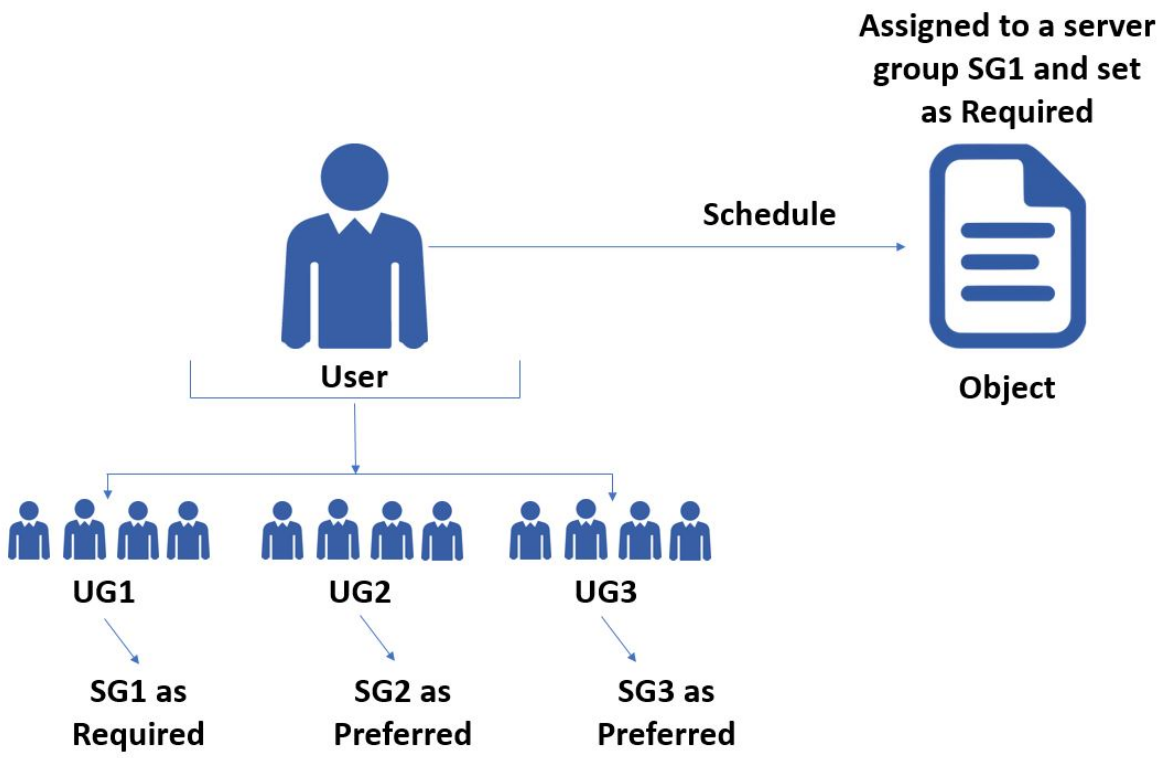
Пользователь входит в три группы пользователей UG1, UG2 и UG3, и каждая группа пользователей сопоставлена с группами серверов SG1, SG2 и SG3 соответственно. Однако SG1 настроена как обязательная группа серверов, а SG2 и SG3 – как предпочтительные группы серверов. Для получения дополнительных сведений о настройке группы серверов как обязательной или предпочтительной см. раздел *Сопоставление группы пользователей с группой серверов* в *Руководстве администратора платформы Business Intelligence*.



Когда пользователь связан с несколькими группами пользователей и каждая группа пользователей сопоставлена с другой группой серверов, платформа вычисляет доступную группу серверов. В вышеупомянутом сценарии задание планирования успешно выполняется, поскольку у объекта отсутствуют назначения групп серверов и доступной группой серверов для планирования объекта является комбинация SG1, SG2 и SG3.

Сценарий 4:

В дополнение к сценарию 3, объект назначен SG1 и группа серверов SG1 настроена как обязательная. Для получения дополнительных сведений о настройке группы серверов как обязательной или предпочтительной см. раздел *Сопоставление группы пользователей с группой серверов* в *Руководстве администратора платформы Business Intelligence*.



Когда группа серверов назначена объекту, платформа проверяет, предоставлены ли пользователю права на просмотр в группе серверов. В этом сценарии платформа не вычисляет доступную группу серверов, так как назначение группы серверов на уровне объекта имеет наивысший приоритет. В сценарии 4 объект успешно запланирован, поскольку группа пользователей UG1 имеет права в SG1, и пользователь наследует эти права от UG1.

> → Напоминание
>
> - Перед планированием объекта проверьте назначения групп серверов всем группам пользователей, связанным с пользователем, и вычислите доступную группу серверов.
> - Задание планирования выполняется успешно, когда доступная группа серверов для пользователя включает группу серверов, назначенную объекту.

См. следующую таблицу:

> ⓘ Примечание
>
> Рассмотрим SG1 и SG2, присвоенные группам пользователей UG1 и UG2 соответственно.

Уровень доступа	Комбинация групп серверов (SG1 + SG2)	Поиск серверов в общем пуле
Пользователь обладает правами во всех группах серверов	Обязательно + Обязательно	False

Уровень доступа	Комбинация групп серверов (SG1 + SG2)	Поиск серверов в общем пуле
Пользователь обладает правами во всех группах серверов	Обязательно + Предпочтительно	False
Пользователь обладает правами во всех группах серверов	Предпочтительно + Предпочтительно	True
Пользователь не обладает правами ни в одной группе серверов	Обязательно + Обязательно	False
Пользователь не обладает правами ни в одной группе серверов	Обязательно + Предпочтительно	False
Пользователь не обладает правами ни в одной группе серверов	Предпочтительно + Предпочтительно	True
Пользователь обладает правами в нескольких группах серверов	Обязательно (нет) + Обязательно (да)	False
Пользователь обладает правами в нескольких группах серверов	Обязательно (нет) + Обязательно (да)	False
Пользователь обладает правами в нескольких группах серверов	Обязательно (да) + Предпочтительно (нет)	False
Пользователь обладает правами в нескольких группах серверов	Предпочтительно (нет) + Предпочтительно (да)	True

11.9 Настройка адаптивных серверов обработки для производственных систем

Программа установки устанавливает по одному адаптивному серверу обработки (APS) на каждый хост. В зависимости от состава установленных компонентов на этом APS может размещаться большое количество служб, в том числе служба мониторинга, служба Диспетчера переноса объектов, служба многомерного анализа 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.

- Создание и настройка дополнительных адаптивных серверов обработки вручную при помощи консоли CMC.

Дополнительные сведения о конфигурировании серверов адаптивной обработки для продуктивных систем см. в следующей статье KBA по адресу: 1694041.

> → Напоминание
>
> 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.

11.10 Оценка производительности системы

11.10.1 Мониторинг серверов платформы BI

Приложение мониторинга позволяет фиксировать оперативные и исторические показатели серверов платформы BI 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.

Связанные сведения

Мониторинг [страница 836]

11.10.2 Анализ серверных показателей

Консоль Central Management Console (CMC) позволяет просматривать показатели для серверов в составе системы. Эти показатели включают общую информацию о каждом компьютере, а также сведения, относящиеся к каждому типу сервера. Также CMC позволяет вам просматривать системные показатели, которые включают информацию о версии продукта, CMS и текущей деятельности системы.

> ⓘ Примечание
>
> Для просмотра доступны показатели только для серверов, запущенных в настоящее время.

11.10.2.1 Просмотр показателей сервера

1. Перейдите в область управления *Серверы* в CMC.
2. Щелкните правой кнопкой мыши сервер, показатели которого требуется просмотреть, и выберите команду *Показатели*.

На вкладке *Показатели* отображается список показателей для сервера.

Связанные сведения

Для изменения свойств сервера [страница 477]
О приложении "Показатели сервера" [страница 1240]

11.10.3 Просмотр системных показателей

Область управления CMC *Настройки* отображает системные показатели, которые предоставляют общую информацию о данном внедрении платформы BI. 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.

11.10.3.1 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*.

11.10.4 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 хранятся в каталоге `<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\logging`.
- В UNIX по умолчанию журналы хранятся в каталоге `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj/logging` 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.

11.11 Конфигурация настроек серверов

В этом разделе вы найдете техническую информацию и процедуры, которые покажут вам, как изменять настройки серверов платформы BI.

Большинство настроек, описанных в данном разделе, позволит вам более эффективно интегрировать платформу BI 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**
>
> Информации о том, как настроить сервер веб-приложений для развертывания приложений платформы BI, в этом разделе нет. Эта задача обычно выполняется при установке продукта.

Для получения дополнительной информации см. *Руководство по установке платформы SAP BusinessObjects Business Intelligence*.

Связанные сведения

Настройка номеров портов [страница 486]
Для изменения свойств сервера [страница 477]
Повторное создание базы данных системы центрального сервера управления [страница 528]
Выбор новой или существующей базы данных центрального сервера управления [страница 525]

11.11.1 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.

11.11.2 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 CMC.
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 *OK*.

> **Примечание**
>
> Перенаправление в область управления CMC *Серверы*. Если требуется перезагрузить сервер, он отмечается как устаревший. После перезапуска сервера он применяет новые настройки, а флаг "Устаревший" удаляется.

11.11.3 Работа с шаблонами конфигурации

С помощью шаблонов конфигурации можно с легкостью настроить несколько экземпляров серверов. В шаблонах конфигурации сохраняется список настроек каждого типа службы, который можно использовать для настройки дополнительных экземпляров сервера. Например, если нужно ввести одинаковые настройки для двенадцати серверов обработки Web Intelligence, потребуется задать настройки только для одного из них. Затем можно будет сохранить введенные настройки службы в шаблоне конфигурации для серверов обработки Web Intelligence и применить данный шаблон к оставшимся 11 серверам.

Для каждого типа службы платформы BI используется особый 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 (CMC).

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.

Связанные сведения

Определение шаблона конфигурации [страница 479]
Применение шаблона конфигурации к серверу [страница 479]

11.11.3.1 Определение шаблона конфигурации

Шаблон конфигурации можно задать для каждого типа службы. Однако для одной службы нельзя задать несколько шаблонов конфигурации. Используйте страницу *Свойства* любого сервера для введения настроек, которые будут применяться шаблоном конфигурации к службе определенного типа, размещенной на сервере.

1. Перейдите в область управления *Серверы* в CMC.
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.

Связанные сведения

Применение шаблона конфигурации к серверу [страница 479]

11.11.3.2 Применение шаблона конфигурации к серверу

Перед применением шаблона убедитесь в том, что вы задали настройки шаблона конфигурации для соответствующего типа сервера. Если параметры шаблона конфигурации явно не заданы, для службы используются параметры по умолчанию.

> ⓘ Примечание
>
> Серверы, на которых не активирована настройка "Использовать шаблон конфигурации", не будут обновляться при изменении шаблона конфигурации.

1. Перейдите в область управления *Серверы* в CMC.
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.

Связанные сведения

Определение шаблона конфигурации [страница 479]

11.11.3.3 Восстановление настроек системы по умолчанию

Возможно, вам потребуется восстановить конфигурацию службы до состояния на момент изначальной инициализации (например, если для серверов будут заданы неверные настройки или возникнут проблемы с работоспособностью системы).

1. Перейдите в область управления *Серверы* в CMC.
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.

11.12 Настройка сетевых параметров сервера

Управление сетевыми параметрами серверов платформы BI осуществляется посредством CMC. 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 CMS по умолчанию: 6400. Другие серверы платформы BI динамически устанавливают связь с доступными портами. Платформа BI управляет номерами портов автоматически, однако их также можно задать в CMC.

11.12.1 Параметры сетевой среды

Платформа BI поддерживает передачу сетевого трафика по протоколам IPv4 и смешанной среды IPv4/IPv6. Серверные и клиентские компоненты можно использовать в любой из следующих сред:

- Сеть IPv4: все серверные и клиентские компоненты работают только по протоколу IPv4.
- Смешанная сеть IPv6/IPv4: серверные и клиентские компоненты могут работать по протоколам IPv6 и IPv4.
  То есть хосты
  - только IPv6 (стек IPv6 включен, стек IPv4 установлен и стек IPv4 отключен),
  - смешанная среда IPv6/IPv4 (стеки IPv6 и IPv4 включены),
  - только IPv4 (стек IPv4 включен, стек IPv6 отключен или удален).

> ⓘ Примечание
>
> - Настройка сети является обязанностью системного и сетевого администратора. Платформа BI не обеспечивает механизм для определения сетевой среды. С помощью CMC определенный IP-адрес IPv6 или IPv4 можно связать с любым сервером платформы BI.
> - Отдельный стек IPv6 (установлен и включен только протокол IPV6) не поддерживается. Тем не менее, поддерживается смешанная среда IPv6.

11.12.1.1 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 IPv4 или в качестве узлов IPv6/IPv4.

Смешанный режим может быть особенно полезен в следующих ситуациях:

- Вы переходите от узла среды IPv4 к узлу смешанной среды 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.

11.12.2 Параметры идентификации хоста сервера

В консоли CMC можно задать параметры идентификации хоста для всех серверов платформы BI. В следующей таблице перечислены все параметры, доступные в области *Общие параметры*.

Действие	Описание
Назначать автоматически	Это установка по умолчанию для всех серверов. Если установлен этот флажок, сервер автоматически связывает свой порт запросов с первым сетевым интерфейсом устройства. **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. *руководство администратора платформы SAP BusinessObjects Business Intelligence* .
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 CMC.

> **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.

Связанные сведения

Настройка системы для использования брандмауэров [страница 213]
Настройка группового компьютера [страница 483]
Устранение неполадок при наличии нескольких сетевых интерфейсов [страница 485]

11.12.2.1 Изменение идентификации хоста сервера

1. Перейдите в область управления *Серверы* в CMC.
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.

11.12.3 Настройка группового компьютера

Групповой компьютер – это компьютер с несколькими сетевыми адресами. Такую конфигурацию можно создавать в нескольких сетевых интерфейсах, для каждого из которых предусмотрен один или несколько IP-адресов, или в одном сетевом интерфейсе, который назначен нескольким IP-адресам.

При наличии нескольких сетевых интерфейсов, для каждого из которых предусмотрен один IP-адрес, измените порядок привязки, чтобы сетевой интерфейс на верхнем уровне привязки

использовался для связи с серверами платформы BI. Если для интерфейса предусмотрено несколько IP-адресов, используйте параметр "Идентификаторы хоста" в консоли CMC для определения сетевой интерфейсной платы для сервера платформы BI. 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 BI. В этом примере DNS должен маршрутизировать подключения других серверов платформы BI к личному адресу сервера репозитория файлов.

Связанные сведения

Устранение неполадок при наличии нескольких сетевых интерфейсов [страница 485]

11.12.3.1 Настройка привязки сервера CMS к сетевому адресу

> ⓘ Примечание
>
> На многосетевом компьютере необходимо задать параметр "Идентификатор хоста" для полного определенного имени домена или IP-адреса интерфейса, с которым необходимо связать сервер.

1. Перейдите в область управления *Серверы* в CMC.
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.

11.12.3.2 Настройка остальных серверов для привязки к сетевому адресу

На остальных серверах платформы BI 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».

Связанные сведения

Изменение порта, который используется сервером для приема запросов [страница 489]

11.12.3.3 Устранение неполадок при наличии нескольких сетевых интерфейсов

На многосетевом компьютере CMS может автоматически выполнить привязку к неверному сетевому интерфейсу. Чтобы предотвратить подобное, убедитесь, что сетевые интерфейсы на компьютере хоста перечислены в правильном порядке (используя инструменты операционной системы данного компьютера) и в CMC заданы параметры имени хоста CMS. Если маршрутизация основного сетевого интерфейса невозможна, выполните нижеуказанные инструкции для привязки платформы BI к дополнительному сетевому интерфейсу, пригодному для маршрутизации. Выполните данные действия сразу же после установки платформы BI на локальном компьютере перед установкой платформы 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 *OK* 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 *OK*.
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.

11.12.4 Настройка номеров портов

Во время установки CMS настраивается на использование номеров портов по умолчанию. Номер порта CMS по умолчанию: 6400. Этот порт попадает в диапазон портов, зарезервированных продуктом SAP BusinessObjects (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 BI, через который CMS слушает запросы службы имен. По умолчанию это порт 6400.	Не применимо.

11.12.4.1 Для изменения порта CMS по умолчанию в CMC

Если в кластере уже выполняется CMS, можно использовать CMC для изменения номера порта CMS по умолчанию. Если в кластере нет запущенных серверов CMS, для изменения номера порта необходимо использовать CCM в Windows или скрипт `serverconfig.sh` в UNIX.

> ⓘ Примечание
>
> CMS использует одну и ту же сетевую интерфейсную плату для порта запросов и порта сервера имен.

1. Перейдите в область управления *Серверы* в CMC.
2. В списке серверов дважды щелкните CMS.
3. Замените номер *порта сервера имен* на порт, на котором вы хотите, чтобы CMS выполнял прослушивание. (Порт по умолчанию: 6400).
4. Нажмите кнопку *Сохранить и закрыть*.
5. Перезапустите CMS.

   CMS начинает прослушивание на порте, который вы указали. Server Intelligence Agent динамически распространяет новые параметры на остальные серверы на узле, если на этих серверах для порта запросов выбран параметр *Назначать автоматически*. (Чтобы внесенные изменения появились в параметрах меню "Свойства" для всех членов узла, потребуется несколько минут).

   Параметры, выбранные на странице *Свойства*, отражаются в командной строке сервера, которая также отображается на странице *Свойства*.

11.12.4.2 Изменение порта CMS по умолчанию на сервере CCM в операционной системе Windows

Если в кластере отсутствуют доступные CMS, и нужно изменить порт CMS по умолчанию для части CMS в развертывании, это делается с помощью CCM.

1. Откройте CCM и остановите SIA для данного узла.
2. Щелкните SIA правой кнопкой мыши и выберите команду *Свойства*.
3. В диалоговом окне *Свойства* выберите вкладку *Запуск*.
4. В списке *Локальные серверы CMS* выберите CMS, для которого нужно изменить номер порта, и щелкните пункт *Свойства*.
5. Чтобы привязать CMS к определенному порту, введите номер порта в поле *Порт*.
6. Чтобы применить новые параметры, нажмите кнопку *OK*.
7. Запустите SIA и подождите, пока не запустятся серверы.

11.12.4.3 Изменение порта CMS по умолчанию на сервере CCM в операционной системе UNIX

Если в кластере нет доступных CMS и требуется изменить порт CMS по умолчанию для одного или нескольких серверов CMS в развертывании, для изменения порта CMS необходимо использовать скрипт `serverconfig.sh`.

1. Используйте скрипт `ccm.sh` для остановки SIA (Server Intelligence Agent), на котором размещается сервер CMS, номер порта которого требуется изменить.
2. Выполните скрипт `serverconfig.sh`.

   По умолчанию этот скрипт находится в каталоге `<InstallDir>/sap_bobj`.
3. Выберите пункт *3 – 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.

11.12.4.4 Изменение порта, который используется сервером CMS для приема запросов

1. Перейдите в область управления *Серверы* в CMC.
2. Выберите сервер CMS, затем выберите пункт *Свойства* в меню *Управление*.
3. В меню *Общие параметры* снимите флажок *Назначать автоматически* для *Порта запроса*, затем введите номер порта, на котором сервер должен выполнять прослушивание.

4. Нажмите кнопку *Сохранить* или *Сохранить и закрыть*.
5. Перезапустите CMS.

Сервер CMS установит связь с новым портом и начнет прослушивание запросов от других серверов.

11.12.4.5 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 CMC.
2. Выберите сервер, а затем выберите пункт *Остановка сервера* в меню *Действия*.
3. Дважды щелкните на сервер.
   Откроется окно *Свойства*.
4. В меню *Общие параметры* снимите флажок *Назначать автоматически* для *Порта запроса*, затем введите номер порта, на котором сервер должен выполнять прослушивание.
5. Нажмите кнопку *Сохранить* или *Сохранить и закрыть*.
6. Запустите и включите сервер.

Сервер устанавливает связь с новым портом, регистрирует его в CMS и начинает прослушивание запросов платформы BI на новом порте.

11.13 Управление узлами

11.13.1 Использование узлов

Узел – это группа серверов платформы BI, 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).

11.13.1.1 Переменные

Переменная	Описание
`<INSTALLDIR>`	Каталог установки SAP BusinessObjects Business Intelligence. В Windows: `C:\Program Files (x86)\SAP BusinessObjects`
`<SCRIPTDIR>`	Каталог, в котором размещаются скрипты управления узлами. • В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts` • В Unix: `<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM64>/scripts`
`<PLATFORM32>`	Имя операционной системы Unix. Допустимы следующие значения: • `aix_rs6000` • `linux_x86` • `solaris_sparc` • `win32_x86`
`<PLATFORM64>`	Имя операционной системы Unix. Допустимы следующие значения: • `aix_rs6000_64` • `linux_x64` • `solaris_sparcv9` • `win64_x64`

11.13.1.2 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 `<КАТАЛОГ_УСТАНОВКИ>/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=tcpip(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
```

Связанные сведения

Переменные [страница 490]

11.13.2 Добавление нового узла

Программа установки создает один узел при первой установке платформы BI.

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 поддерживается 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.

> → Рекомендация
>
> Для добавления узлов в развертывание платформы BI с активированным FIPS и сконфигурированным CORBA SSL рекомендуется использовать опцию "Запуск нового временного CMS".
>
> Для добавления узлов в развертывание платформы BI с неактивированным FIPS и сконфигурированным CORBA SSL рекомендуется использовать опцию "Запуск нового временного CMS".
>
> Для добавления узлов в развертывание платформы BI с активированным FIPS и несконфигурированным CORBA SSL рекомендуется использовать существующий CMS.

11.13.2.1 Добавление узла на новый компьютер в существующем развертывании

При добавлении нового компьютера в существующее развертывание с помощью программы установки можно автоматически создать на этом компьютере первый узел.

> → Совет
>
> В процессе установки нажмите кнопку *Развернуть* и укажите существующий центральный сервер управления.

Для создания дополнительных узлов используйте Central Configuration Manager или скрипт `serverconfig.sh`.

Для получения дополнительных сведений об установке см. *Руководство по установке платформы SAP BI*.

11.13.2.2 Добавление узла в Windows

> ⚠ Предупреждение
>
> Перед добавлением узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

1. В панели инструментов Central Configuration Manager (CCM) выберите команду *Добавить узел*.
2. В окне *Мастер добавления узлов* введите имя узла и номер порта для нового агента Server Intelligence (SIA).
3. Укажите, требуется ли создавать серверы в новом узле.
   - *Добавить узел без серверов*
   - *Добавить узел с CMS*
   - *Добавить узел с серверами по умолчанию*
     При выборе этого параметра создаются только серверы, установленные на этом компьютере. При этом не включаются все возможные серверы.
4. Выберите CMS.
   - Если развертывание работает, выберите пункт *Использование существующего выполняющегося CMS* и нажмите кнопку *Далее*.
     При появлении соответствующего запроса введите имя хоста и 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 CCM создает узел. При возникновении любых ошибок см. сведения о них в файле журнала.

После этого можно запустить новый узел с помощью CCM.

11.13.2.2.1 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 дополнительных 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.

Связанные сведения

Переменные [страница 490]
Параметры скрипта для добавления, восстановления и удаления узлов [страница 509]

11.13.2.3 Добавление узла в Unix

> ⚠ Предупреждение
>
> Перед добавлением узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

1. Выполните скрипт `<КАТАЛОГ_УСТАНОВКИ>/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 CCM создает узел. При возникновении любых ошибок см. сведения о них в файле журнала.

После этого можно выполнить команду `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj/ccm.sh -start <имя_узла>` для запуска нового узла.

11.13.2.3.1 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`. Для получения дополнительных сведений 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
```

Связанные сведения

Переменные [страница 490]
Параметры скрипта для добавления, восстановления и удаления узлов [страница 509]

11.13.3 Восстановление узла

Можно восстановить узел с помощью Central Configuration Manager (CCM) или скрипта управления узлами после восстановление 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.

> ⓘ Примечание
>
> Все серверы кроме CMS должны быть остановлены перед повторным созданием узла.

> → Напоминание
>
> Восстановление узла возможно только на том компьютере, на котором он расположен.

11.13.3.1 Восстановление узла в Windows

1. В панели инструментов Central Configuration Manager (CCM) выберите команду *Добавить узел*.
2. В окне *Мастер добавления узлов* введите имя узла и номер порта для восстановленного Server Intelligence Agent (SIA).

   > ⓘ Примечание
   >
   > Имена исходного и восстановленного узлов должны совпадать.

3. Выберите команду *Повторно создать узел* и нажмите кнопку *Далее*.
   - Если узел существует в системной базе данных 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*.
   CCM восстанавливает узел и добавляет сведения о нем на локальный компьютер. При возникновении любых ошибок см. сведения о них в файле журнала.

После этого можно запустить восстановленный узел с помощью CCM.

11.13.3.1.1 Восстановление узла в Windows с помощью скрипта

Для восстановления узла на компьютере под управлением Windows можно использовать скрипт `AddNode.bat`. Для получения дополнительных 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 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.

Связанные сведения

Переменные [страница 490]
Параметры скрипта для добавления, восстановления и удаления узлов [страница 509]

11.13.3.2 Восстановление узла в Unix

1. Выполните скрипт `<КАТАЛОГ_УСТАНОВКИ>/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 <имя_узла>` для запуска восстановленного узла.

11.13.3.2.1 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
        -siaport 6415
        -cms mycms:6400
        -username Administrator
        -password Password1
  -cmsport 7400
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=BusinessObjects CMS
140;UID=Administrator;PWD=Password1;HOSTNAME=database;PORT=3306"
        -dbkey abc1234
        -adopt
```

Связанные сведения

Переменные [страница 490]
Параметры скрипта для добавления, восстановления и удаления узлов [страница 509]

11.13.4 Удаление узла

Для удаления остановленного узла можно использовать Central Configuration Manager (CCM) или скрипт управления узлами. Придерживайтесь следующих рекомендаций:

- При удалении узла также безвозвратно удаляются серверы этого узла.
- Если кластер содержит несколько компьютеров, узлы следует удалять перед удалением компьютера из кластера и удалением с него программного обеспечения. Если компьютер удаляется из кластера до удаления узла, а также в случае сбоя файловой системы на компьютере, необходимо восстановить узел на другом компьютере с теми же серверами и в том же кластере, после чего удалить узел.

> → Напоминание
>
> Удаление узла возможно только на том компьютере, на котором он расположен.

Связанные сведения

Восстановление узла [страница 496]

11.13.4.1 Удаление узла в Windows

> ⚠ Предупреждение
>
> Перед удалением узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

1. Запустите Central Configuration Manager (CCM).
2. В диспетчере CCM остановите узел, который требуется удалить.
3. Выберите узел и затем выберите команду *Удалить узел* на панели инструментов.
4. Если потребуется, введите имя хоста, номер порта и учетные данные администратора для CMS.

Диспетчер CCM удаляет узел и все присутствующие в нем серверы.

> ⓘ Примечание
>
> Новый добавленный узел можно удалить после конфигурации следующими способами:
>
> - удалить параметры SSL из нового созданного узла и из узла SIA, к серверам CMS которого выполняется подключение;
> - добавить следующие параметры SSL в RemoveNode.bat перед объявлением основного класса и запустить их: -Dbusinessobjects.orb.oci.protocol=ssl -DcertDir="Путь к каталогу сертификатов SSL" -DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key -Dpassphrase=passphrase.txt -Dpsecert=cert.pse

11.13.4.1.1 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
```

Связанные сведения

Переменные [страница 490]
Параметры скрипта для добавления, восстановления и удаления узлов [страница 509]

11.13.4.2 Удаление узла в Unix

До и после удаления узла создайте резервную копию конфигурации сервера для всего кластера.

1. Выполните команду `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj/ccm.sh -stop <имя_узла>`, чтобы остановить узел, который требуется удалить.
2. Выполните скрипт `<КАТАЛОГ_УСТАНОВКИ>/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.

> ⓘ Примечание
>
> Новый добавленный узел можно удалить после конфигурации следующими способами:
>
> - удалить параметры SSL из нового созданного узла и из узла SIA, к серверам CMS которого выполняется подключение;
> - добавить следующие параметры SSL в RemoveNode.bat перед объявлением основного класса и запустить их: -Dbusinessobjects.orb.oci.protocol=ssl -DcertDir="Путь к каталогу сертификатов SSL" -DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key -Dpassphrase=passphrase.txt -Dpsecert=cert.pse

11.13.4.2.1 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
```

Связанные сведения

Переменные [страница 490]
Параметры скрипта для добавления, восстановления и удаления узлов [страница 509]

11.13.5 Переименование узла

Можно переименовать узел с помощью Central Configuration Manager (CCM). Чтобы переименовать узел, необходимо создать новый узел с нужным именем, клонировать серверы исходного узла на новый узел, а затем удалить исходный узел. Придерживайтесь следующих рекомендаций:

- При переименовании компьютера, на котором располагается узел, не требуется переименовывать сам узел. Можно использовать существующее имя узла.
- Если используется брандмауэр, убедитесь, что порты Server Intelligence Agent (SIA) и Центрального сервера управления (CMS) открыты.

> → Напоминание
>
> Выполнить переименование узла возможно только на том компьютере, на котором он расположен.

Связанные сведения

Добавление нового узла [страница 492]
Удаление узла [страница 500]

11.13.5.1 Переименование узла в Windows

> ⚠ Предупреждение
>
> Перед переименованием узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

1. Запустите Central Configuration Manager (CCM).
2. В панели инструментов Central Configuration Manager (CCM) выберите команду *Добавить узел*.
3. В окне *Мастер добавления узлов* введите имя узла и номера порта для нового Server Intelligence Agent (SIA), учетные данные администратора, сведения о соединении с базой данных, учетные данные для системной базы данных и ключ кластера.
4. Выберите команду *Добавить узел без серверов*.
5. После создания узла на странице *Управление серверами* 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.

Связанные сведения

Добавление нового узла [страница 492]
Удаление узла [страница 500]

11.13.5.2 Переименование узла в Unix

> ⚠ Предупреждение
>
> Перед переименованием узла следует выполнить резервное копирование конфигурации серверов для всего кластера.

1. Выполните скрипт `<КАТАЛОГ_УСТАНОВКИ>/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 `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj/ccm.sh -start <имя_узла>` для запуска нового узла.
9. После того как новый узел проработает пять минут, удалите старый узел с помощью скрипта `serverconfig.sh`.

Связанные сведения

Добавление нового узла [страница 492]
Клонирование серверов [страница 447]
Удаление узла [страница 500]

11.13.6 Перемещение узла

Можно переместить остановленный узел из одного кластера в другой с помощью Central Configuration Manager (CCM) или скрипта управления узлами. Придерживайтесь следующих рекомендаций:

- Убедитесь, что в целевом кластере отсутствует узел с таким же именем.
- Удостоверьтесь, что серверы всех типов, установленных на компьютере с исходным узлом, также установлены в целевом кластере.
- Чтобы добавить новый компьютер в рабочий кластер и запретить его использование до тех пор, пока не будет завершено тестирование, установите платформу BI на автономный компьютер, протестируйте компьютер, а затем переместите узел в продуктивный кластер.
- Версия платформы BI и уровень пакета обновления для этого компьютера должны соответствовать остальной части кластера.

> → Напоминание
>
> Перемещение узла возможно только на том компьютере, на котором он расположен.

11.13.6.1 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.

11.13.6.1.1 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=database1;PORT=3306"
        -dbkey abc1234
        -destcms destinationMachine:6401
        -destusername Administrator
        -destpassword Password2
        -destdbdriver sybasedatabasesubsystem
        -destconnect "DSN=Destin BOEXI40;UID=username;PWD=Password2;"
        -destdbkey def5678
```

> ⓘ Примечание
>
> Чтобы избежать использования символа крышки в длинных строках, можно записать имя скрипта и все его параметры во временный файл `response.bat` и затем выполнить этот файл `response.bat` без параметров.

Связанные сведения

Переменные [страница 490]
Параметры скриптов для перемещения узлов [страница 512]

11.13.6.2 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 `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj/ccm.sh -stop <имя_узла>`, чтобы остановить узел.

2. Выполните скрипт `<КАТАЛОГ_УСТАНОВКИ>/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 `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj/ccm.sh -start <имя_узла>` для запуска перемещенного узла.

11.13.6.2.1 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
```

Связанные сведения

Переменные [страница 490]
Параметры скриптов для перемещения узлов [страница 512]

11.13.7 Параметры скриптов

11.13.7.1 Параметры скрипта для добавления, восстановления и удаления узлов

Параметр	Описание	Пример
`-adopt`	Восстанавливает узел, если он уже существует в CMS.	**`-adopt`**
`-cms`	Имя и номер порта центрального сервера управления (CMS) **⚠ Предупреждение** Не используйте этот параметр, если используется `-usetempcms` **ⓘ Примечание** Необходимо указать номер порта, если CMS запущен не на порте по умолчанию 6400.	**`-cms mycms:6409`**

Параметр	Описание	Пример
`-cmsport`	• Номер порта CMS при запуске временной системы CMS. **⚠ Ограничение** Также необходимо использовать параметры `-usetempcms`, `-dbdriver`, `-connect`, и `-dbkey`. • Номер порта CMS при создании новой системы CMS. **⚠ Ограничение** Также необходимо использовать параметры `-dbdriver`, `-connect`, и `-dbkey`.	**`-cmsport 6401`**
`-connect`	Строка соединения для системной базы данных CMS (или временной системы CMS). **ⓘ Примечание** Пропустите атрибуты `HOSTNAME` и `PORT` при соединении с базами данных DB2, Oracle, SQL Anywhere, SQL Server или Sybase.	**`-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=password;HOSTNAME=database;PORT=3306"`**
`-dbdriver`	Драйвер базы данных CMS. Допустимые значения: • **`db2databasesubsystem`** • **`mysqldatabasesubsystem`** • **`oracledatabasesubsystem`** • **`sqlanywheredatabasesubsystem`** • **`sqlserverdatabasesubsystem`** • **`sybasedatabasesubsystem`** • **`newdbdatabasesubsystem`**	**`-dbdriver mysqldatabasesubsystem`**
`-dbkey`	Ключ кластера.	**`-dbkey abc1234`**
`-name`	Имя узла	**`-name mynode2`**
`-noservers`	Создается узел без серверов. **ⓘ Примечание** Дополнительный параметр `-createcms` создает узел с CMS, но без остальных серверов. Пропустите эти параметры для создания узла с серверами по умолчанию.	**`-noservers`**

Параметр	Описание	Пример
`-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`**

Связанные сведения

Добавление узла в Windows с помощью скрипта [страница 494]
Добавление узла в Unix с помощью скрипта [страница 496]
Восстановление узла в Windows с помощью скрипта [страница 498]
Восстановление узла в Unix с помощью скрипта [страница 500]
Удаление узла в Windows с помощью скрипта [страница 501]
Удаление узла в Unix с помощью скрипта [страница 502]

11.13.7.2 Параметры скриптов для перемещения узлов

Параметр	Описание	Пример
`-cms`	Имя исходного центрального сервера управления (CMS). **⚠ Предупреждение** Не используйте этот параметр, если используется `-usetempcms` **ⓘ Примечание** Необходимо указать номер порта, если CMS запущен не на порте по умолчанию 6400.	`-cms sourceMachine:6409`
`-cmsport`	• Номер порта CMS при запуске временной системы CMS. **⚠ Ограничение** Также необходимо использовать параметры `-usetempcms`, `-dbdriver`, `-connect`, и `-dbkey`. • Номер порта CMS при создании новой системы CMS. **⚠ Ограничение** Также необходимо использовать параметры `-dbdriver`, `-connect`, и `-dbkey`.	`-cmsport 6401`
`-connect`	Строка соединения исходного CMS или временной системной базы данных CMS. **ⓘ Примечание** Пропустите атрибуты HOSTNAME и PORT при соединении с базами данных DB2, Oracle, SQL Anywhere, SQL Server или Sybase.	`-connect "DSN=Source BOEXI40;UID=username;PWD=password;HOSTNAME=database;PORT=3306"`

Параметр	Описание	Пример
`-dbdriver`	Драйвер базы данных исходного CMS. Допустимые значения: • **`db2databasesubsystem`** • **`mysqldatabasesubsystem`** • **`oracledatabasesubsystem`** • **`sqlanywheredatabasesubsystem`** • **`sqlserverdatabasesubsystem`** • **`sybasedatabasesubsystem`** • **`newdbdatabasesubsystem`**	**`-dbdriver mysqldatabasesubsystem`**
`-dbkey`	Исходный ключ кластера.	**`-dbkey abc1234`**
`-destcms`	Имя CMS назначения. **Примечание** Необходимо указать номер порта, если CMS запущен не на порте по умолчанию 6400.	**`-destcms destinationMachine:6401`**
`-destconnect`	Строка соединения конечной системной базы данных CMS. **Примечание** Пропустите атрибуты `HOSTNAME` и `PORT` при соединении с базами данных DB2, Oracle, SQL Anywhere, SQL Server или Sybase.	**`-destconnect "DSN=Destin BOEXI40;UID=username;PWD=passwor d;HOSTNAME=database;PORT=3306"`**
`-destdbdriver`	Драйвер базы данных конечного CMS Допустимые значения: • **`db2databasesubsystem`** • **`mysqldatabasesubsystem`** • **`oracledatabasesubsystem`** • **`sqlanywheredatabasesubsystem`** • **`sybasedatabasesubsystem`** • **`newdbdatabasesubsystem`**	**`-destdbdriver sybasedatabasesubsystem`**
`-destdbkey`	Ключ кластера назначения.	**`-destdbkey def5678`**
`-destpassword`	Пароль учетной записи администратора в целевом CMS.	**`-destpassword Password2`**
`-destusername`	Имя пользователя учетной записи администратора на целевом CMS.	**`-destusername Administrator`**

Параметр	Описание	Пример
`-password`	Пароль учетной записи администратора в исходном CMS.	`-password Password1`
`-username`	Имя пользователя учетной записи администратора на исходном CMS.	`-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`

Связанные сведения

Перемещение узла в Windows с помощью скрипта [страница 506]
Перемещение узла в Unix с помощью скрипта [страница 508]

11.13.8 Добавление зависимостей сервера Windows

В среде Windows каждый экземпляр Server Intelligence Agent (SIA) зависит от служб журнала событий и вызова удаленной процедуры (RPC).

При возникновении ошибок в работе агента SIA убедитесь, что обе эти службы отображаются на вкладке *Зависимость* агента SIA.

11.13.8.1 Добавление зависимостей сервера Windows

1. Откройте Central Configuration Manager (CCM) и остановите Server Intelligence (SIA).
2. Щелкните SIA правой кнопкой мыши и выберите команду *Свойства*.
3. Выберите вкладку *Зависимость*.
4. Нажмите кнопку *Добавить*.
   Открывается диалоговое окно *Добавление зависимости*, в котором отображается список всех доступных зависимостей.
5. Выберите зависимость и нажмите кнопку *Добавить*.
6. Нажмите кнопку *OK*.

7. С помощью диспетчера CCM перезапустите агент SIA.

11.13.9 Изменение учетных данных пользователя для узла

С помощью Central Configuration Manager (CCM) можно установить или обновить учетные данные пользователя для агента Server Intelligence (SIA) при изменении пароля операционной системы, а также в тех случаях, когда требуется запускать все серверы в узле под разными учетными записями.

Все серверы, управляемые агентом SIA, запускаются под одной учетной записью. Чтобы запустить сервер с использованием несистемной учетной записи, убедитесь, что эта учетная запись входит в группу "Локальные администраторы" на сервере, и ей назначено право «Замена маркера уровня процесса».

> ⚠ Ограничение
>
> На компьютере под управлением Unix запуск платформы BI должен осуществляться с использованием той же учетной записи, под которой эта система была установлена. Чтобы использовать иную учетную запись, следует переустановить систему с необходимой записью.

11.13.9.1 Изменение учетных данных пользователя для узла в Windows

1. Откройте Central Configuration Manager (CCM) и остановите агент Server Intelligence (SIA).
2. Щелкните SIA правой кнопкой мыши и выберите команду *Свойства*.
3. Очистите флажок *Системная учетная запись*.
4. Введите имя пользователя и пароль и нажмите кнопку *OK*.
5. С помощью диспетчера CCM перезапустите агент SIA.

Агент SIA и сервер выполняют вход в систему локального компьютера с использованием новой учетной записи пользователя.

11.14 Переименование компьютера в развертывании платформы BI

11.14.1 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 `<имя_хоста>:<порт>`). Обновите имя кластера в файлах свойств всех серверов веб-приложений на веб-уровне.
Вы устанавливаете другую версию платформы BI на компьютере, на котором ранее выполнялся сервер CMS, или добавляете компьютер в другой кластер.	• Убедитесь в том, что новый сервер CMS запущен на другом порте. • Используйте разные пароли для различных кластеров, чтобы предотвратить вход пользователей на неверный кластер.

11.14.2 Изменение IP-адресов

Чтобы избежать внесения в конфигурацию изменений, ведущих изменение IP-адреса компьютера, выберите команду *Свойства сервера* на вкладке CMC *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.
Вы используете другой тип соединения с базой данных CMS или базой данных аудита.	Используйте CCM, 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 `localhost` в качестве имени компьютера.
URL используется для веб-приложений платформы BI, к которым пользователи обращаются с помощью веб-браузера (например CMC).	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 CMC, 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.

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* CMC, 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 CMC, чтобы убедиться в работоспособности платформы BI.

> → Напоминание
>
> Перезапустите компьютер после выполнения этого действия.

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 CMC *Приложения*.
Пользователи обращаются к веб-приложениям платформы BI (например к CMC) 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.

Связанные сведения

Выбор новой или существующей базы данных центрального сервера управления [страница 525]

11.14.3 Переименование компьютеров

Компьютер в развертывании платформы BI 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.

11.14.3.1 Уровень сервера

> ⓘ Примечание
>
> Перед переименованием компьютера CMS следует ознакомиться с конфигурацией всех серверов на изменяемом компьютере на вкладке CMC «Управление серверами». Если свойство *Имя хоста* использует старое имя хоста CMS, измените его на новое имя хоста CMS.

> → Напоминание
>
> 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 `cms.default`.	Измените имя компьютера CMS в свойстве `cms.default` во всех настраиваемых файлах свойств на всех компьютерах веб-уровня. В Tomcat созданные файлы свойств по умолчанию размещаются в папке `<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`. ⓘ 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 `cms.default`.

Условие	Действие
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: • 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».

→ Напоминание

Перезапустите веб-приложение или сервер приложений после выполнения этого действия.

Связанные сведения

Восстановление узла [страница 496]

11.14.3.2 Веб-уровень

При переименовании компьютера с сервером веб-приложений платформы 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*.
Вы изменяете имя компьютера с сервером веб-приложений платформы BI, а пользователи обращаются к веб-приложениям платформы BI с помощью URL-адреса, который содержит 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.

11.14.3.3 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 `localhost` 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 CMC *Аудит*.

11.14.3.4 Серверы репозитория файлов

При переименовании компьютера, на котором размещено хранилище файлов FRS, необходимо обновить серверы *репозитария входящих файлов* и *репозитария исходящих файлов* на странице CMC «Управление сервером» и убедиться в том, что свойства *Каталог хранилища файлов* и *Временный каталог* содержат новый путь к хранилищу, а затем перезапустить серверы.

11.15 Использование 32-битных и 64-битных сторонних библиотек вместе с платформой BI

На серверах платформы BI сочетаются 32- и 64-разрядные процессы. На некоторых серверах дополнительно запускаются 32-битные и 64-битные дочерние процессы. Чтобы использовать правильную версию сторонних библиотек (32-битную или 64-битную) с процессами платформы BI, необходимо задать на компьютерах с платформой BI отдельные 32-битные и 64-битные переменные среды. 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-разрядными процессами платформы BI.
- `<FIRST_ENV_VAR32>`=значение, которое должно использоваться для 32-разрядных процессов.
- `<SECOND_ENV_VAR>`=значение, которое должно использоваться для 64-разрядных процессов.
- `<SECOND_ENV_VAR32>`=значение, которое должно использоваться для 32-разрядных процессов.
- BOE_USE_32BIT_ENV_FOR=`<FIRST_ENV_VAR>`,`<SECOND_ENV_VAR>`

Например, если платформа BI установлена на компьютере AIX наряду с 32- и 64-разрядными клиентами Oracle, и требуется задать переменную LIBPATH, укажите следующие переменные:

- ORACLE_HOME=`<домашний каталог 64-битной версии клиента Oracle>`
- ORACLE_HOME32=`<домашний каталог 32-битной версии>`
- LIBPATH=`<путь к библиотеке 64-битной версии>`
- LIBPATH32=`<путь к библиотеке 32-битной версии>`
- 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.

11.16 Управление заполнителями сервера и узла

11.16.1 Просмотр заполнителей для сервера

В области управления *Серверы* консоли CMC 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.

Связанные сведения

Заполнители сервера и узлов [страница 1259]

11.16.2 Просмотр и изменение заполнителей для узла

1. В области управления *Серверы* Central Management Console щелкните правой кнопкой мыши узел, для которого необходимо изменить заполнители, и выберите команду *Заполнители*.
2. Внесите требуемые изменения параметров заполнителей и щелкните *Сохранить* для продолжения.

> ⚠ Предупреждение
>
> Заполнители, отличные от предназначенных для редактирования, не следует изменять ни в коем случае. Системный администратор должен обеспечить, чтобы права на редактирование в узле были только у соответствующих лиц из группы администраторов (которые предназначены для управления узлом). Для всех остальных пользователей, включая других членов группы администраторов, должны быть установлены ограничения на просмотр объектов узла или управление ими путем применения соответствующих прав безопасности. Если какое-либо значение заполнителя случайно повреждено и CMS не появляется, см. SAP-ноту 3269127.

> ⓘ Примечание
>
> См. статью 3278916 в базе знаний SAP, чтобы узнать, как ограничить изменяемые заполнители, чтобы избежать возможного вредоносного вмешательства в ландшафт BI.

Связанные сведения

Заполнители сервера и узлов [страница 1259]

12 Управление базами данных Центрального сервера управления (CMS)

12.1 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 развертывании платформы BI содержится несколько Центральных серверов управления, последующие запросы с других серверов перенаправляются на любой Центральный сервер управления в кластере, имеющий активное подключение к системной базе данных. Пока CMS находится в состоянии «Ожидание ресурсов», любой текущий запрос, не требующий доступа к базе данных, продолжает успешно обрабатываться, однако при обработке запросов, требующих обращения к базе данных центрального сервера управления, происходит сбой.

По умолчанию центральный сервер управления в состоянии «Ожидание ресурсов» периодически выполняет определенное количество попыток подключения в соответствии с настройками свойства «Запросы соединений с системной БД». Сразу после установления по меньшей мере одного 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*.

Связанные сведения

Для изменения свойств сервера [страница 477]

12.1.1 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).

Связанные сведения

Копирование данных из одной базы данных CMS в другую. [страница 530]
Выбор новой или существующей базы данных центрального сервера управления [страница 525]

12.1.2 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]
     DRIVER=<HANA CLIENT PATH>/libodbcHDB.so
     SERVERNODE=<HANA Server IP address>:<HANA server port #>
     DATABASENAME=<DBNAME>
     DESCRIPTION=<DESCRIPTION>
     ```

     `<New_DB_version>` – версия SAP HANA; например, «NewDB 1.0», `<HANA Server IP address>` – IP-адрес сервера SAP HANA, а `<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=<INSTALLDIR>/sap_bobj/enterprise_xi40/odbc.ini
     ```

Убедитесь, что переменная среды ODBCINI задана в профиле пользователя, запускающего серверы BI.

- 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* > *Администрирование* > *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>/odbcreg <SERVER>:<HDBINDEXSERVERPORT> <SYSTEMID>
<NONADMINUSER> <NONADMINPASSWORD>
```

   - В ОС Windows можно использовать администратор источников данных ODBC для тестирования соединения ODBC с SAP HANA.
5. В Unix убедитесь, что переменные среды `LD_LIBRARY_PATH` или `LIBPATH` содержат путь к `libodbcHDB.so`. Для получения дополнительных сведений см. 2792543, 1886746 и 2721890.
6. Установите продукт, следуя указаниям ассистента, и выберите SAP HANA в качестве базы данных CMS/аудита.
7. Убедитесь в том, что развертывание работает (например, войдите в CMC и просмотрите отчет).

> **Примечание**
>
> Эта процедура не применяется при перемещении базы данных из существующей базы данных в базу данных SAP HANA. В этом случае используйте процедуру копирования источника данных. Для получения дополнительной информации см. Копирование данных из одной базы данных CMS в другую. [страница 530].

Связанные сведения

Копирование данных из одной базы данных CMS в другую. [страница 530]
Выбор новой или существующей базы данных центрального сервера управления [страница 525]

12.2 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 BI, эти шаги позволят вам выбрать 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).

> **ⓘ Примечание**
>
> Не настраивайте установленную платформу BI на использование базы данных системы CMS, относящейся к другому кластеру, если не выполняется рабочий процесс копирования 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.

> **ⓘ Примечание**
>
> Платформа Business Intelligence поддерживает обмен данными по протоколу SSL между CMS и базами данных, такими как база данных CMS и база данных аудита. Для коммуникации по протоколу SSL:
>
> - Для безопасной коммуникации с CMS следует использовать базы данных SQL Anywhere, SQL Server и SAP HANA, такие как база данных CMS или аудита.
> - Следует включить SSL на соответствующих серверах баз данных. Обратитесь к документации по вашей базе данных.
> - Необходимо создать соединение ODBC и передать через это соединение сертификат сервера БД.
> - Для подключения к базе данных CMS и базе данных аудита следует использовать одно и то же соединение ODBC.

12.2.1 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 *OK*.
4. Выберите драйвер базы данных и щелкните *OK*.
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 *OK*. (Щелкните *Создать*, чтобы настроить новое DSN.) Система пригласит вас ввести учетные данные, после чего необходимо нажать *OK*.
   - Если вы выбрали собственный драйвер, необходимо будет ввести имя сервера базы данных, ваши логин и пароль. После ввода этой информации нажмите *OK*.
6. Укажите ключ кластера.
7. Перезапустите агент Server Intelligence.

12.2.2 Выбор новой или существующей базы данных центрального сервера управления в UNIX

Используйте скрипт `cmsdbsetup.sh`. Для получения информации см. раздел «Скрипты Unix» главы "Администрирование в командной строке" *Руководства администратора платформы BI*.

1. Выполните скрипт `cmsdbsetup.sh` (расположение по умолчанию: `<КАТАЛОГ_УСТАНОВКИ>/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 подсказка на восстановление Server Intelligence (SIA), укажите пароль администратора и необходимый номер порта, через который будет устанавливать связь центральный сервер управления.

   > **Примечание**
   >
   > Эта подсказка появится, только если назначение выполняется в пустой базе данных центрального сервера управления.

Связанные сведения

Скрипты UNIX [страница 1133]

12.3 Повторное создание базы данных системы центрального сервера управления

В этой процедуре описаны способы повторного создания (повторной инициализации) текущей системной базы данных центрального сервера управления. При выполнении этой задачи уничтожаются все данные, содержащиеся в базе данных. Эта процедура необходима, например, если платформа BI 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 CMS. 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 CMC 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 CMS все данные в текущей системной базе данных CMS будут уничтожены. Перед началом операции рассмотрите возможность создания резервных копий текущей базы данных. При необходимости обратитесь к администратору базы данных.

Связанные сведения

Резервное копирование настроек сервера [страница 583]

12.3.1 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 *OK* и при появлении запроса на подтверждения нажмите кнопку *Да*.
6. Укажите пароль для базы данных системы CMS, а затем нажмите кнопку *OK*.

   > ⓘ 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 *OK*.

   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.

12.3.2 Восстановление системной базы данных CMS в ОС UNIX

Используйте скрипт `cmsdbsetup.sh`. Для получения информации см. раздел «Скрипты Unix» главы "Администрирование в командной строке" *Руководства администратора платформы BI*.

1. Выполните файл `cmsdbsetup.sh` (расположение по умолчанию: `<КАТАЛОГ_УСТАНОВКИ>/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 устанавливать связь центральный сервер управления.

   > ⓘ Примечание
   >
   > Эта подсказка появится, только если назначение выполняется в пустой базе данных центрального сервера управления.

7. В каталоге `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj/` выполните следующую команду, чтобы запустить узел.

   ```
   ccm.sh -start <имя_узла>
   ```

8. Для включения служб используйте следующую команду:

   ```
   ccm.sh -enable all -cms <ИМЯ_CMS:ПОРТ> -username administrator -password
   <пароль>
   ```

   > ⓘ Примечание
   >
   > Поскольку база данных CMS только что восстановлена, пароль администратора не задан.

Связанные сведения

Скрипты UNIX [страница 1133]

12.4 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.

База данных адресата инициализируется до переноса в нее новых данных, поэтому ее содержимое будет временно удалено (все таблицы платформы BI будут временно удалены, а затем пересозданы).

После завершения копирования данных целевая база данных устанавливается в качестве текущей базы данных для CMS.

> ⚠ Предупреждение
>
> Никогда не пытайтесь использовать базу данных CMS из другого кластера платформы BI. Перед запуском этого рабочего процесса всегда убеждайтесь, что исходная база данных CMS использовалась с этим кластером платформы BI, а не с каким-то другим.

> ⚠ Предупреждение
>
> Никогда не пытайтесь выполнить обновление с помощью рабочего процесса копирования базы данных CMS. Рабочий процесс копирования базы данных CMS предназначен для перемещения базы данных CMS с одного сервера базы данных на другой. Он не предназначен для обновления базы данных CMS. Перед запуском этого рабочего процесса всегда убеждайтесь, что исходная база данных CMS использовалась с этим кластером платформы BI и что у нее та же версия и уровень пакета поддержки, что и у текущей установки платформы BI.

12.4.1 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 база данных назначения не содержит системных таблиц платформы BI, то эти таблицы будут созданы. Если системные таблицы платформы BI содержатся в целевой базе данных, то эти таблицы будут удалены навсегда, после чего будут созданы новые системные таблицы, а данные из исходной базы данных будут скопированы в новые таблицы. Остальные таблицы в базе данных не изменяются.

> **Примечание**
>
> 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`.

12.4.2 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 *OK*.
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 *OK*.

12.4.3 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 <имя_узла>
   ```

2. Выполните файл `cmsdbsetup.sh` (расположение по умолчанию: `<КАТАЛОГ_УСТАНОВКИ>/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.

12.5 Драйвер базы данных Центрального сервера управления

Теперь вы можете получать доступ к базе данных репозитория CMS платформы BI для анализа отчетности с помощью компонентов и функций, доступных на платформе (Сервер соединений, анализ на семантическом уровне, клиенты системы отчетности). Драйвер доступа к данным SAP BusinessObjects позволяет использовать юниверс для выполнения запросов к базе данных CMS. Для получения дополнительных сведений см. раздел http://scn.sap.com/docs/DOC-74580.

13 Управление серверами контейнера веб-приложений (WACS)

13.1 WACS

13.1.1 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 ручное или с использованием WDeploy развертывание платформы BI или внешних веб-приложений.

13.1.1.1 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 приложений Java для развертывания веб-приложений платформы BI, или если установка платформы BI выполняется в системе UNIX, установка и использование WACS не требуется.

13.1.1.2 Какие преимущества дает использование WACS?

При использовании WACS для размещения CMC вы получаете ряд преимуществ:

- Установка, обслуживание и конфигурация WACS требует минимальных усилий.
- Все размещаемые приложения предварительно развертываются на WACS, поэтому выполнять дополнительные действия вручную не требуется.
- WACS поддерживается SAP.
- Благодаря WACS не требуются особые навыки администрирования и обслуживания серверов Java-приложений.
- WACS предоставляет интерфейс администрирования, согласованный с другими серверами платформы BI.

13.1.1.3 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.	• Добавление дополнительных серверов WACS в систему и их удаление [страница 537] • Клонирование сервера контейнера веб-приложений [страница 539]
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 [страница 537]
Как создать среду, в которой можно легко устранить последствия неверной настройки CMC?	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 [страница 537]
Как повысить безопасность связи между клиентами и WACS?	Настройте HTTPS на WACS.	• Настройка HTTPS/SSL [страница 541] • Использование WACS с брандмауэрами [страница 568]
Как повысить безопасность связи между WACS и другими серверами платформы BI в моем развертывании?	Настройте связь SSL между WACS и другими серверами платформы BI в своем развертывании.	• Настройка внутренних серверов для SSL [страница 188] • Использование WACS с брандмауэрами [страница 568]
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 [страница 567]
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.	• Использование WACS с другими веб-серверами [страница 566] • Использование WACS с балансировщиком нагрузки [страница 566]

Задача	Описание	Раздел
		• Использование WACS с обратным прокси [страница 567] • Использование WACS с брандмауэрами [страница 568]
Можно ли использовать WACS в развертывании с балансировщиком нагрузки?	Вы можете использовать WACS с развертывании с балансировщиком нагрузки аппаратного обеспечения. Сам сервер WACS не может использоваться для балансировки нагрузки.	Использование WACS с балансировщиком нагрузки [страница 566]
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 [страница 567]
Как устранять неисправности на серверах WACS?	При необходимости определения причин низкой производительности серверов WACS можно просмотреть файлы журнала и параметры системы.	• Настройка трассировки на WACS [страница 569] • Для просмотра серверных показателей [страница 570]
Я не получаю никаких обработанных для меня страниц на конкретном порту. В чем проблема?	Имеются несколько причин, почему вы не можете подключиться к WACS. Убедитесь, что: • 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.	• Разрешение конфликтов порта HTTP [страница 571] • Изменение параметров памяти [страница 571] • Изменение количества параллельных запросов [страница 572] • Восстановление настроек системы по умолчанию [страница 572]
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 [страница 568]

Задача	Описание	Раздел
Где можно найти список свойств WACS?	В приложении «Свойства сервера» данного руководства содержится список свойств WACS.	Свойства основных служб [страница 1202]

13.1.2 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.

13.1.2.1 Установка WACS

Установка WACS на отдельных компьютерах может повысить производительность и улучшить распределение нагрузки в развертывании, а также увеличить доступность сервера. Если в вашем развертывании содержится два или несколько серверов WACS на разных компьютерах, доступность веб-приложений и веб-служб не будет зависеть от аппаратных или программных сбоев на конкретной машине, так как другие серверы WACS по-прежнему будут предоставлять службы.

С помощью программы установки платформы BI можно установить сервер контейнера веб-приложений. Существует два способа установки WACS:

- При полной установке на экране *Выберите сервер веб-приложений Java* выберите *Установить сервер контейнера веб-приложений и автоматически развернуть веб-приложения*.
  При выборе сервера Java-приложений в новой установке WACS не устанавливается.
- При пользовательской/расширенной установке существует возможность выбора установки WACS на экране *Выбор компонентов*. Это можно сделать, развернув узлы ▶ *Серверы* ▶ *Службы платформы* ▶ и выбрав *Сервер контейнера веб-приложений*.

При установке WACS программа установки автоматически создает сервер с именем `<NODE>.WebApplicationContainerServer`, где `<NODE>` – имя узла. Веб-приложения и веб-службы платформы BI будут развернуты на этом сервере. Вмешательство пользователя для развертывания или настройки 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. Номер порта по умолчанию – 6405. Если предполагается разрешить пользователям подключаться к WACS с внешней стороны брандмауэра, необходимо, чтобы на брандмауэре был открыт порт HTTP сервера.

> **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 получат 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.

13.1.2.2 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.

13.1.2.3 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 *OK*.

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.

Связанные сведения

Разрешение конфликтов порта HTTP [страница 571]

13.1.2.4 Удаление серверов WACS из развертывания

Удаление WACS возможно только в том случае, если сервер в данный момент не обеспечивает службу CMC. 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 CMC, невозможно.

1. Перейдите в область управления *Серверы* в CMC.
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 *OK*.

13.1.3 Добавление или удаление служб на сервере WACS

13.1.3.1 Добавление веб-приложения или веб-службы к WACS

Для добавления дополнительных веб-приложений или веб-служб платформы BI к WACS требуется остановить WACS. Поэтому необходимо оставить хотя бы одну дополнительную CMC 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 CMC.
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 CMC, 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 *OK*, 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 – *OK*.
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.

13.1.3.2 Удаление веб-приложения или веб-службы с WACS

Для удаления веб-приложения или веб-службы с WACS требуется выполнить вход для CMC на другом WACS или на сервере приложений Java. Остановка WACS, с которого в данный момент запущена служба CMC, 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 CMC.
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 CMC, 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 *OK*, 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 *OK*.
7. Запустите сервер WACS, щелкнув его правой кнопкой мыши и выбрав команду *Запустить сервер*.

Служба удалена с WACS.

13.1.4 Настройка HTTPS/SSL

Можно использовать протокол SSL и HTTP для сетевого обмена данными между клиентами и WACS в вашем развертывании платформы BI. 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 дополнительной

информации об использовании SSL между серверами платформы BI в развертывании см. раздел «Основные сведения об обмене данными между компонентами платформы BI» главы «Работа с брандмауэрами» в *Руководстве 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 сертификаты и личные ключи. Вы можете использовать Microsoft Internet Information Service (IIS) и Microsoft Management Console (MMC) для генерации файла PCKS12, 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.

Связанные сведения

Основные сведения об обмене данными между компонентами платформы BI [страница 199]
Использование WACS с обратным прокси [страница 567]

13.1.4.1 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 *OK*.

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 *OK*.

   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.

13.1.4.2 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 *OK*.
      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 .

13.1.4.3 Настройка HTTPS/SSL

Перед началом настройки HTTPS/SSL на сервере WACS убедитесь, что вы уже создали файл PCKS12 или хранилище ключей JKS и скопировали или переместили его на компьютер, на котором установлен сервер WACS.

1. Перейдите в область управления компонента CMC *Серверы*.
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 файлов сертификатов или хранилище ключей, в котором содержится более одного сертификата, и этот сертификат в хранилище файлов 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 PCKS12 или хранилища ключей JKS, в котором содержится файл списка надежных сертификатов.

> **Примечание**
>
> Тип списка надежных сертификатов должен быть таким же, как тип Хранилища сертификатов.

> **Примечание**
>
> Для получения дополнительных сведений об установке доверительной аутентификации с использованием сертификатов X.509 см. Веб-службы RESTful [страница 426].

> **Примечание**
>
> Вы можете импортировать сертификат системы ABAP в платформу BI, выполнив команду: `keytool -import -trustcacerts -alias <Alias_Name> -file <CA_certificate_path> -keystore <trust_keystore_path>` . Для получения представления о команде см. следующую таблицу.
>
> | Команда | Описание |
> | --- | --- |
> | -alias | Псевдоним |
> | -file | Путь к файлу сертификата для системы ABAP |
> | -keystore | Путь к файлу доверенного хранилища ключей |

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.

13.1.5 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

13.1.6 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.

Связанные сведения

Подключаемый модуль безопасности Windows AD [страница 309]
Сопоставление пользователей и групп Windows AD [страница 310]
Настройка учетной записи службы для аутентификации AD с Kerberos [страница 307]
Запуск SIA под учетной записью службы платформы BI [страница 317]
Включение аутентификации Kerberos в подключаемом модуле Windows AD для WACS [страница 546]
Создание файлов конфигурации. [страница 548]
Конфигурация WACS для AD Kerberos [страница 551]
Настройка единого входа в AD Kerberos [страница 553]

13.1.6.1 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.

13.1.6.1.1 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 [страница 307]
- Запуск SIA под учетной записью службы платформы BI [страница 317]
- Сопоставление пользователей и групп Windows AD [страница 310]

13.1.6.1.2 Настройка подключаемого модуля безопасности Windows AD для Kerberos

1. Перейдите в область управления *Аутентификация* в CMC.
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 BI или имя 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.

Связанные сведения

Настройка единого входа в AD Kerberos [страница 553]

13.1.6.2 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).

13.1.6.2.1 Создание файла конфигурации Kerberos

Чтобы создать файл конфигурации Kerberos, выполните указанные ниже шаги.

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

   > ⓘ Примечание
   >
   > Этот файл можно сохранить в другом месте. Однако если это сделать, необходимо будет указать его местоположение в поле *Расположение файла Krb5.ini* на странице *Свойства* для сервера WACS в CMC.

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` – это DNS-имя домена, которое необходимо ввести заглавными буквами в формате FQDN.

> ⓘ Примечание
>
> `kdc` – имя хоста контроллера домена.

> ⓘ Примечание
>
> 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 [страница 550].

> ⓘ Примечание
>
> 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.

13.1.6.2.2 Создание файла конфигурации входа JAAS

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

13.1.6.2.3 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
        }
```

13.1.6.3 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).

13.1.6.3.1 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.

13.1.6.4 Устранение неполадок с Kerberos

Описанные ниже шаги могут помочь при возникновении проблем с настройкой Kerberos.

- Включение регистрации событий
- Тестирование конфигурации Kerberos

13.1.6.4.1 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 *OK*.
7. Запустите WACS в экране *Управление серверами*.

13.1.6.4.2 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).

```
<INSTALLDIR>\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.

13.1.6.4.3 Сопоставленному пользователю AD не удается войти в платформу BI в WACS

Несмотря на то, что пользователи сопоставлены платформе BI, могут возникать две проблемы.

13.1.6.4.3.1 Ошибка входа в результате различия имен AD UPN и SAM

Идентификаторы пользователей Active Directory успешно сопоставлены платформе BI. Несмотря на это им не удается успешно выполнить вход в CMC с использованием аутентификации AD и Kerberos в следующем формате: `DOMAIN\ABC123`

Эта проблема может возникать в случае, когда пользователь настроен в Active Directory с использованием несовпадающих UPN- и SAM-имен (несовпадение регистров или по иной причине). Ниже приведено два примера, из-за которых могут возникать проблемы:

- UPN – abc123@company.com, а SAM-имя – DOMAIN\ABC123.
- UPN – jsmith@company, а SAM-имя – DOMAIN\johnsmith.

Эту проблему можно устранить двумя способами:

- Пользователи должны выполнять вход с использованием UPN-имени, а не SAM-имени.
- SAM-имя учетной записи и UPN-имя должны совпадать.

13.1.6.4.3.2 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.

13.1.7 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.

Связанные сведения

Обзор вопросов безопасности [страница 158]
Настройка Kerberos AD для WACS [страница 546]
Настройка компьютера для единого входа AD Kerberos [страница 554]
Настройка WACS для единого входа AD Kerberos [страница 554]

13.1.7.1 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 [страница 333]
- Настройка учетной записи службы для функции единого входа Vintela [страница 330]
- Настройка нескольких SPN-имен [страница 554]
- Увеличение лимита размера заголовка WACS [страница 554]

В разделах ниже описано выполнение каждого из этих шагов.

13.1.7.1.1 Настройка нескольких SPN-имен

Использование нескольких SPN не поддерживается.

13.1.7.1.2 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 CMC.
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.

13.1.7.2 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 CMC.
2. Дважды щелкните сервер контейнера веб-приложений, который требуется настроить. Откроется окно *Свойства*.

3. Установите флажок *Включить единый вход в Active Directory с Kerberos*.
4. Укажите значения свойств "Домен AD по умолчанию", "Имя принципала службы" и "Файл ярлыков ключей", после чего выберите команду *Сохранить и закрыть* .
5. Перезапустите WACS.

Служба единого входа Active Directory готова к использованию.

13.1.7.3 Настройка модуля Kerberos и режима единого входа в базе данных

Единый вход в базу данных поддерживается для систем, удовлетворяющих следующим требованиям:

- Развертывание платформы BI выполнено на сервере 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 CMC 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 [страница 553].

13.1.7.3.1 Включение режима единого входа в базе данных

1. Откройте файл `krb5.ini`, используемый в развертывании платформы BI.

   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.

13.1.8 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 администрирования веб-служб RESTful. Подробнее о веб-службах RESTful см. в *Руководстве разработчика веб-служб RESTful платформы Business Intelligence*.

13.1.8.1 Приложения

13.1.8.1.1 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-служб 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-служб RESTful на нужные сервер и порт. Базовый URL-адрес также используется в ответах веб-служб RESTful, определяя гиперссылки на другие ресурсы RESTful.

> **Примечание**
>
> В установке платформы BI, используемой 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 (CMC) в качестве администратора.
2. В CMC щелкните пункт *Приложения*.
   Откроется список приложений.
3. Щелкните правой кнопкой мыши *Веб-служба RESTful* > *Свойства*.
   Откроется страница *Свойства: веб-служба RESTful*. Теперь на странице введен флажок *Использовать относительный путь в URL-адресе*, чтобы учитывать URL-адрес браузера для запуска веб-службы RESTful. Дополнительные сведения см. в SAP-ноте 3048101.
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 выполняется прослушивание запросов веб-служб RESTful.

> ⚠ Предупреждение
>
> - Для интерфейсов API веб-служб RESTful **поддерживаются серверы Tomcat, WACS и WebSphere, а также JBoss и SAP NetWeaver**.
> - В поле *URL-адрес доступа* **по умолчанию** отображается URL-адрес WACS. Если требуется использовать интерфейсы API веб-служб RESTful на веб-сервере Tomcat, измените необходимые значения `<server>` и `<port>` должным образом.

5. Нажмите *Сохранить и закрыть*.

> ⓘ Примечание
>
> Если активировать параметр *Использовать относительный путь URL*, используется относительный URL-адрес браузера.

13.1.8.2 Свойства WACS

13.1.8.2.1 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 сервер контейнера веб-приложений (WACS), 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*.

13.1.8.2.2 Настройка системных свойств

13.1.8.2.2.1 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 (WACS), 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.

13.1.8.2.2.2 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 (WACS), 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*.

13.1.8.2.2.3 Настройка времени ожидания для маркера входа в систему

Срок действия маркера входа в систему истекает, если он не используется в течение заданного периода времени. Можно 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 (WACS), 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*.

13.1.8.2.2.4 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 (WACS), 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*.

13.1.8.2.2.5 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 (WACS), 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*.

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 `:`.

Связанные сведения

Настройка параметров пула сеансов [страница 559]

13.1.8.2.3 Совместное использование ресурсов из различных источников

13.1.8.2.3.1 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 CMC 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 (WACS), 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*.

13.1.8.2.4 Аутентификация

13.1.8.2.4.1 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 CMC 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`.

13.1.8.2.4.2 Включение и настройка доверительной аутентификации

Доверительная аутентификация включается и настраивается через Central Management Console (CMC) в разделах: *Аутентификация > Enterprise*, где разрешена доверительная аутентификация и генерируется файл общего секретного ключа; *Пользователи и группы > Список пользователей*, где создается учетная запись для доверенного пользователя по следующему пути; *Серверы > Список серверов > WACS > Свойства*, где выбирается параметр *Метод извлечения* для запросов маркера входа в систему API `/logon/trusted`.

> **Примечание**
>
> По соображениям безопасности доверительную аутентификацию не следует включать без HTTPS. Если доверительная аутентификация включена без HTTPS, это считается нарушением безопасности, поскольку URL-адрес отображается для неавторизованных пользователей. Во избежание нарушения безопасности информация пользователя может быть проверена с помощью действительного сертификата. Для получения дополнительных сведений см. 1388240.

1. Войдите в Central Management Console в качестве пользователя с правами администратора.
2. Перейдите к разделу *Аутентификация* > *Enterprise*, затем щелкните *Доверительная аутентификация включена*.
3. Щелкните *Новый общий секретный ключ*, затем выберите *Загрузить общий секретный ключ*.
4. Щелкните *Сохранить* и поместите файл `TrustedPrincipal.conf` в местоположение по умолчанию: `<EnterpriseDir>\<platform>`.
   Пример местоположения:

   ```
   "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjectsEnterprise XI
   4.0\win64_x64\"
   ```

   > **Примечание**
   >
   > Можно изменить местоположение файла общего секретного ключа `TrustedPrincipal.conf` по умолчанию, добавив запись командной строки в CMC в разделе *Серверы > Список серверов > WACS > Свойства > Параметры командной строки* и затем перезапустив службу WACS. Например, запись командной строки, включающая `-Dbobj.trustedauth.home=` и папку `SharedSecrets`, расположенную в корневом каталоге диска `C:\` сервера платформы BI, будет выглядеть следующим образом:
   >
   > ```
   > "-Dbobj.trustedauth.home=C:\SharedSecrets"
   > ```

   > **Примечание**
   >
   > Можно оставить для параметра *Период действия общего секретного ключа (в днях)* значение по умолчанию, равное нулю (0); в этом случае действие ключа будет бессрочным. 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 команды *Управление > Создать > Создать пользователя*. Снимите флажок *Пользователю следует изменить пароль при следующем входе в систему*, 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 *Создать* > *Создать пользователя*.

7. Выберите *Серверы* > *Основные службы* > *WACS* > *Свойства*, выполните прокрутку до раздела *Конфигурация доверительной аутентификации* и используйте меню *Метод извлечения* для выбора *HTTP_HEADER*, *QUERY_STRING* или *COOKIE*.

   > **Примечание**
   >
   > При необходимости можно сменить значение по умолчанию `X-SAP-TRUSTED-USER` *Параметра имени пользователя* на любое другое более удобное значение (например, `UserName`, `bankteller` или `nurse`), 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. Убедитесь, что можно извлечь маркер входа в систему с помощью API `.../biprsw/logon/trusted/` и отправки запроса `GET` с ярлыком заголовка по умолчанию `X-SAP-TRUSTED-USER` и указанием имени пользователя, созданного в шаге 6.

13.1.8.2.4.3 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, создаваемый в CMC: выберите *Аутентификация* и дважды щелкните *Enterprise*. Выберите *Доверительная аутентификация включена* и нажмите кнопку *Новый общий секретный ключ*. Сохраните файл, нажав *Загрузить общий секретный ключ* и выбрав расположение файла 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*.

13.1.9 Сервер контейнера веб-приложений (WACS) и ваша IT-среда

В этом разделе содержится информация о настройках WACS в сложной среде.

13.1.9.1 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.

13.1.9.2 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.

Связанные сведения

Настройка HTTPS/SSL [страница 541]

13.1.9.3 Использование WACS с обратным прокси

WACS можно использовать в развертывании с прямым или обратным прокси-сервером. Использовать WACS в качестве прокси-сервера нельзя.

13.1.9.3.1 Настройка WACS для поддержки HTTP с обратным прокси

Для использования WACS в развертывании с обратным прокси следует настроить WACS таким образом, чтобы порт HTTP использовался для связи в пределах брандмауэра (например, в защищенной сети), а порт HTTP через прокси – для связи за пределами брандмауэра (например, в сети Интернет).

1. Перейдите в область управления CMC *Серверы*.
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. Щелкните *Сохранить и закрыть*.

13.1.9.3.2 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.

13.1.9.4 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 использовать брандмауэр между сервером WACS и другими серверами платформы SAP BI в развертывании, см. раздел «Основные сведения об обмене данными между компонентами платформы BI» в *Руководстве администратора платформы SAP BusinessObjects Business Intelligence*.

Связанные сведения

Основные сведения об обмене данными между компонентами платформы BI [страница 199]

13.1.9.5 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 CMC.
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 затем задайте имя хоста или IP-адрес сетевого адаптера, используемого для обмена данными между WACS и другими серверами платформы BI в данном развертывании.
6. Нажмите кнопку *Сохранить и закрыть*.
7. Перезапустите WACS.

13.1.10 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 `<имя_веб_приложения>_web_xml.ino`, где переменная `<имя_веб_приложения>` 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 `<каталог_Enterprise>/warfile/webapps/<имя_веб_приложения>`, где переменная `<имя_веб_приложения>` 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 с помощью свойств BOE.war» в *Руководстве администратора платформы SAP BI*.

> **Примечание**
>
> Не изменяйте файлы `web.xml`, `web_xml.ino`, или `.properties` в каталоге `<каталог_Enterprise>/java/pjs/container/work/<понятное_имя_сервера>`, поскольку изменения будут переопределяться при каждом запуске или перезапуске WACS.

> **Примечание**
>
> После изменения свойств для WACS необходимо перезапустить сервер.

Связанные сведения

Для изменения свойств сервера [страница 477]
Файл BOE.war [страница 784]

13.1.11 Устранение неполадок

13.1.11.1 Настройка трассировки на WACS

Чтобы настроить трассировку для WACS, см. раздел Ведение журнала трассировок компонентов [страница 1107]

13.1.11.2 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*.

Связанные сведения

Показатели сервера контейнера веб-приложений [страница 1252]

13.1.11.3 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 «Выполнение 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.

13.1.11.4 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 удается 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.

13.1.11.4.1 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 *OK*.
6. Запустите WACS в экране *Управление серверами*.

13.1.11.4.2 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*.

13.1.11.5 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 *OK*.
6. Запустите WACS в экране *Управление серверами*.

13.1.11.6 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*.

13.1.11.7 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 *OK*.
7. В окне *Управление серверами* запустите WACS.

13.1.11.8 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 CMC.
2. Дважды щелкните по WACS, который требуется изменить.
   Откроется окно *Свойства*.
3. В разделе *Служба контейнеров веб-приложений* снимите флажок *Привязка ко всем IP-адресам*.
4. В поле *Связать с именем хоста или IP-адресом* введите **`127.0.0.1`** и нажмите кнопку *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.

13.1.12 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».

Связанные сведения

Свойства основных служб [страница 1202]

14 Резервное копирование и восстановление системы

14.1 Обзор резервного копирования и восстановления

В этой главе описывается, как выполнить резервное копирование платформы BI 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.

Связанные сведения

Резервное копирование всей системы [страница 579]
Резервное копирование платформы BI [страница 586]
Резервное копирование параметров сервера с помощью CCM в Windows [страница 583]
Резервное копирование параметров сервера в ОС Unix [страница 584]
Обзор копирования системы [страница 601]

14.2 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	Средство создания версий формирует несколько версий определенного файла или файлов в системе. В данном случае можно вернуть систему в более раннее состояние. 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.
Аппаратное резервное копирование системы	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. 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.
Сравнение аппаратного резервного копирования системы с резервным копированием приложения	Аппаратное резервное копирование системы создает копию всей файловой системы, включая операционную систему. Аппаратное резервное копирование позволяет восстановить систему в целом до более ранней версии. При резервном копировании приложения создаются резервные копии файлов, относящихся к отдельным приложениям. Платформой BI поддерживается аппаратное резервное копирование системы и не поддерживается резервное копирование приложения. 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. Полное резервная копия системы платформы BI называется набором резервного копирования.
Набор резервного копирования	Набор резервного копирования включает следующие отдельные резервные копии, созданные одновременно: • 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 репозиториев 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.

Термин	Определение
Сравнение "холодного" и оперативного резервного копирования	"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. Платформой BI поддерживается как "холодное", так и оперативное резервное копирование. Оперативное резервное копирование называется также «резервированием онлайн».

14.3 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
Цель: восстановление системы 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.	• Целевая система с аппаратной конфигурацией, аналогичной исходной системе И • Резервные копии исходной системы	Используйте рабочий процесс резервного копирования и восстановления системы, описанный в этом руководстве. См. процедуру Резервное копирование всей системы [страница 579]. Воссоздайте целевую систему из резервных копий исходной системы.
Цель: восстановление объектов Требуется восстановление документа или другого объекта, который был случайно удален.	• Резервные копии баз данных и файлов исходной системы И • Подробные сведения о системе, описанные в Экспорт из исходной системы [страница 606]	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 [страница 602] и следуйте инструкциям, указанным в остальной части главы.

Цель	Необходимые ресурсы	Решение
		ⓘ 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.
Цель: восстановление объектов 2 Требуется восстановление документа или другого объекта, который был случайно удален.	Система, в которой используется управление версиями Promotion Management	Воспользуйтесь приложением Promotion Management для восстановления более ранней версии документа. Подробные сведения см. в соответствующей теме для Promotion Management.

ⓘ Примечание

Резервное копирование системы до и после обновления программного обеспечения:

CMS связан с "версией" продукта. Нельзя использовать систему платформы SAP BusinessObjectsBusiness Intelligence с CMS и FRS из другой версии. Перед любыми обновлениями программного обеспечения необходимо делать резервные копии и CMS, и файлового хранилища FRS. Если вы выполняете "восстановление" для отката обновления программного обеспечения, необходимо убедиться, что CMS, FRS и программное обеспечение имеют одну и ту же версию.

Связанные сведения

Резервные копии [страница 578]
Планирование копирования системы [страница 602]
Обзор [страница 613]

14.4 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. Дополнительные сведения

о реконструкции платформы BI вместо ее восстановления из резервной копии см. в соответствующей теме 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.

> → Совет
>
> Можно создать резервную копию системы платформы BI и затем восстановить ее на том же или другом хост-компьютере для создания копии системы.

Связанные сведения

Резервное копирование всей системы [страница 579]
Резервное копирование настроек сервера [страница 583]
Резервное копирование платформы BI [страница 586]
Обзор копирования системы [страница 601]

14.4.1 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.

> ⓘ Примечание
>
> 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.

14.4.1.1 Оперативное резервное копирование

Функция оперативного резервного копирования позволяет выполнять копирование платформы BI, 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 завысить 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
>
> - При оперативном резервном копировании по сути не выполняется резервное копирование, а откладывается удаление файлов. Если файлы изменяются или обновляются, то сохраняется несколько копий. Это означает, что CMS и FRS всегда поддерживают корректные отношения, позволяя выполнять резервное копирование в разное время. Однако оно должно происходить в определенный интервал оперативного резервного копирования.
> - При восстановлении системы в FRS находится много ненужных файлов, которые средству Repository Diagnostic Tool необходимо удалить.
> - Всегда запускайте резервное копирование CMS перед резервным копированием файлового хранилища FRS.
>
> 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).

> **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.

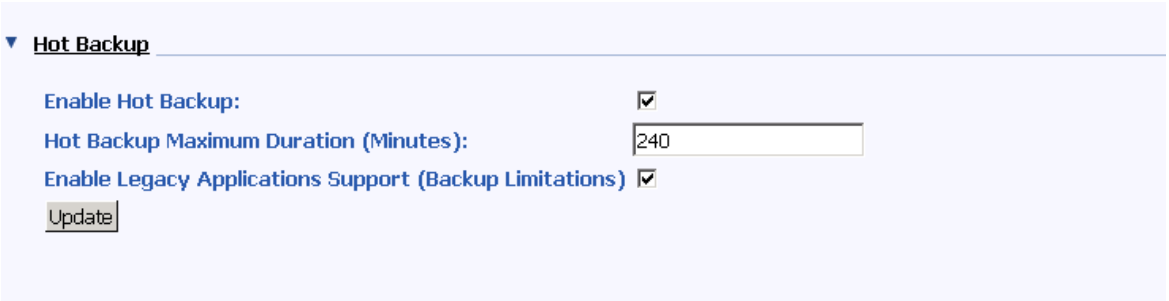
14.4.1.1.1 Включение оперативного резервного копирования

1. Откройте Central Management Console (CMC).
2. В области *Управление* откройте страницу *Настройки*.
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 завысить ожидаемое время.

5. Нажмите кнопку *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.

14.4.1.2 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. Для компьютеров с ОС Unix выполните резервное копирование каталога установки и домашнего каталога учетной записи установки.
   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.

Связанные сведения

Оперативное резервное копирование [страница 580]

14.4.2 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, репозиториев 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.

> ⓘ Примечание
>
> Резервное копирование настроек сервера не является отдельной задачей резервного копирования CMS и файлового хранилища FRS, т. е. при восстановление CMS/FRS автоматически приведет к восстановлению настроек сервера. Резервное копирование настроек сервера — это небольшая часть полного резервного копирования базы данных CMS. Если восстановление CMS выполнено, дополнительно восстанавливать настройки сервера не требуется.

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 `<КАТАЛОГ_УСТАНОВКИ>\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`.

14.4.2.1 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.
   CCM выполняет резервное копирование параметров конфигурации сервера для всего кластера в указанный файл BIAR. Подробные сведения о процедуре резервного копирования записываются в файл журнала. Имя файла журнала и путь к нему отображаются в диалоговом окне.
9. Если во время операции резервного копирования произошел сбой, проверьте файл журнала для установления причины.
10. Нажмите кнопку *OK*, чтобы закрыть мастер.

14.4.2.2 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.

```
-----------------------------------------------------------

            SAP BusinessObjects

What do you want to do?

1 - Add node
2 - Delete node
3 - Modify node
4 - Move node
5 - Back up server configuration
6 - Restore server configuration
7 - Modify web tier configuration
8 - List all nodes


[quit(0)]
-----------------------------------------------------------

[8]5
```

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.

14.4.2.3 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 `<КАТАЛОГ_УСТАНОВКИ>\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`.

Связанные сведения

Скрипты BackupCluster и RestoreCluster [страница 597]

14.4.3 Резервное копирование платформы BI

Рекомендуется использовать стандартные средства и процедуры резервного копирования баз данных и файлов, чтобы регулярно создавать следующие резервные копии:

- База данных CMS
- Хранилища файлов репозиториев входящих и исходящих файлов

Наличие актуальных копий содержимого позволяет восстановить систему Business Intelligence без восстановления параметров всей системы или сервера.

Для получения дополнительных сведений о резервном копировании системы см. Выполнение оперативного и "холодного" резервного копирования системы [страница 582]

14.5 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.

Связанные сведения

Восстановление всей системы [страница 587]
Восстановление настроек сервера [страница 594]
Восстановление содержимого BI [страница 597]

14.5.1 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 произошел сбой службы базы данных, можно перезапустить службу, не восстанавливая систему целиком.

- Хранилище сервера репозитория файлов
- Файловая система компьютера

> ⓘ Примечание
>
> Для полного восстановления системы не требуется установленная в целевой системе платформа BI.

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.

Связанные сведения

Восстановление всей системы [страница 588]
Восстановление только базы данных аудита [страница 590]
Восстановление содержимого веб-уровня [страница 590]
Восстановление только базы данных CMS [страница 590]

14.5.1.1 Восстановление всей системы

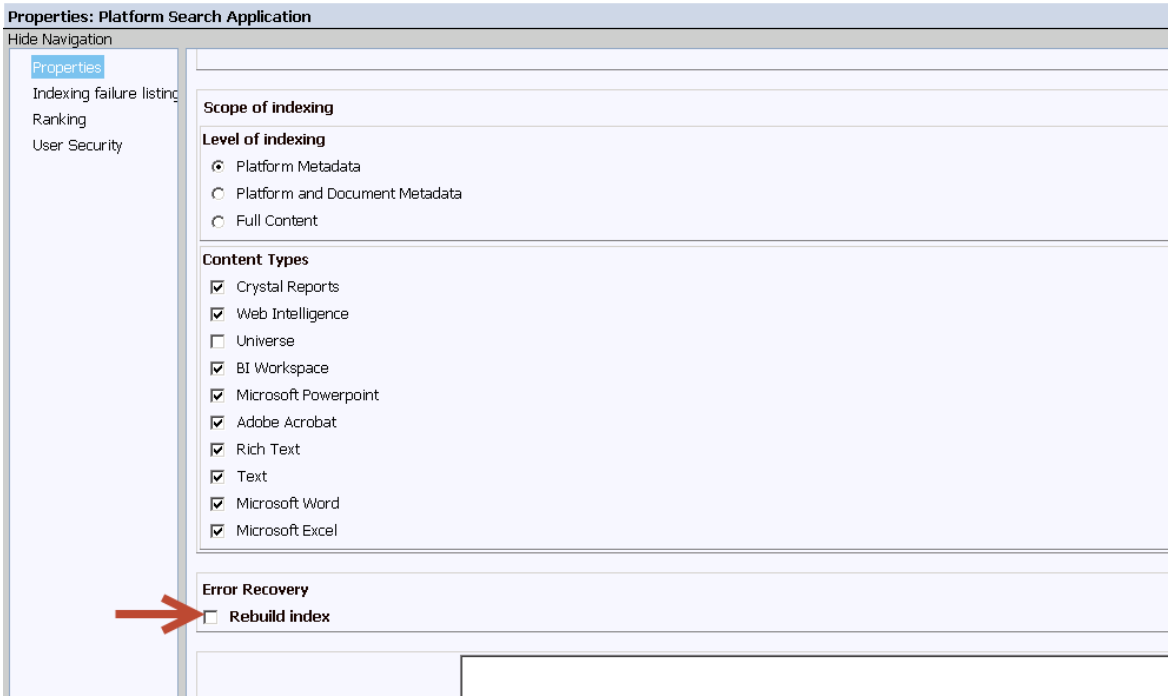
Перед восстановлением системы необходимо использовать Central Configuration Manager (CCM), чтобы остановить все узлы в развертывании платформы BI, после чего также требуется выбрать время для восстановления системы.

> ⓘ 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 репозиториев 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.
   > - При выполнении резервного копирования и восстановления CMS и FRS считаются одним целым. При восстановлении одного из них потребуется восстановить и другой.
   > - 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 репозиториев 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 вы используете функцию аудита, используйте средства базы данных для восстановления базы данных аудита.
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 [страница 593]. 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 [DB_NAME].ADS_EVENT where Start_Time > '<[time of DB failure]>' and Start_Time < '<[time of DB restoration]>'`

Связанные сведения

Индексация содержимого в репозитории CMS [страница 981]

14.5.1.2 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.

С помощью средств управления базой данных восстановите БД аудита.

Связанные сведения

Восстановление всей системы [страница 588]

14.5.1.3 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.

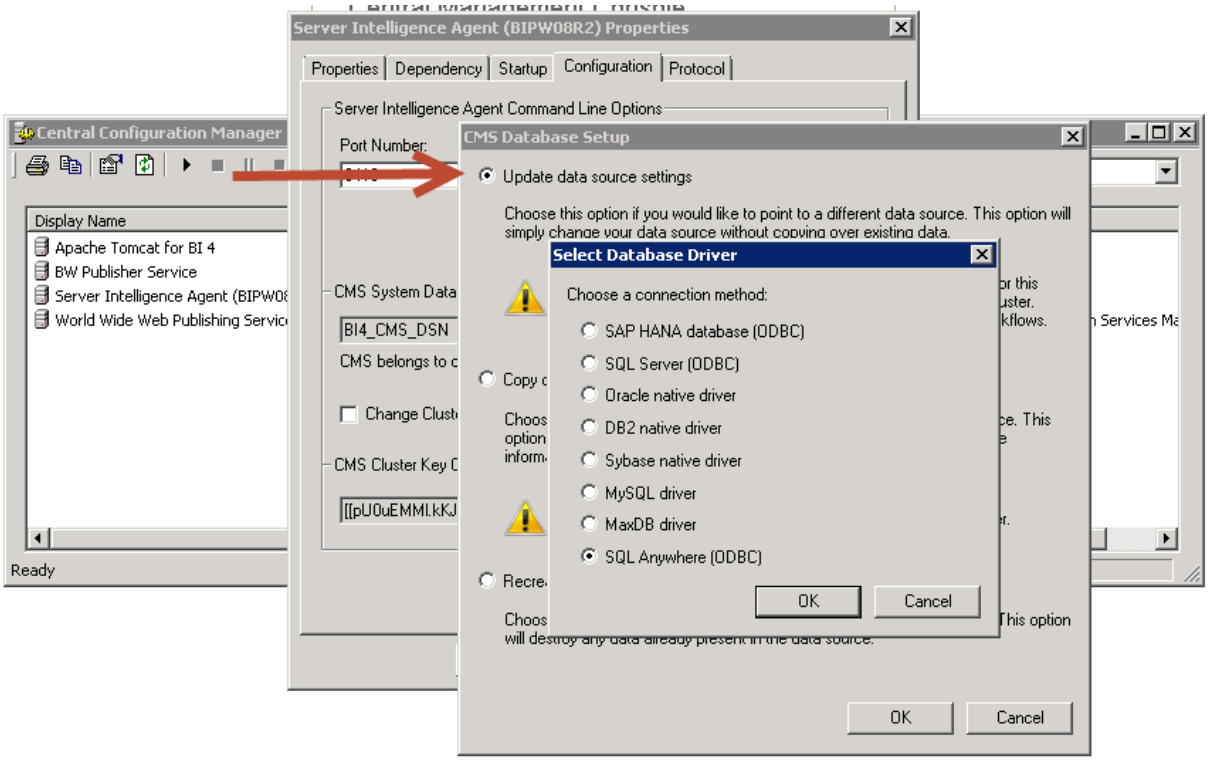
14.5.1.4 Восстановление только базы данных CMS

> ⓘ Примечание
>
> Если произошел сбой службы базы данных, можно перезапустить службу, не восстанавливая систему целиком. 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.

Для ОС Windows:



Для ОС Unix: Выполните cmsdbsetup.sh, введите в подсказку имя узла, затем выберите вариант 6 `update`.

```
-----------------------------------------------------------

           SAP BusinessObjects


Current CMS Data Source: BI4_CMS_DSN_1381344842

Current cluster name: LRHEL57x64:6400

Current cluster key: [[pU0uEMM1.kKJPezTK002bw]]


update (Update Data Source Settings)
reinitialize (Recreate the current data surce)
copy (Copy data from another Data Source)
change cluster (Change current cluster name)
change cluster key (Change current cluster key)


[update(6)/reinitialize(5)/copy(4)/change cluster(3)/change cluster key(2)/back(1)/quit(0)]
-----------------------------------------------------------

[update]6
```

1. Остановите все узлы платформы BI с помощью ССМ.
2. С помощью средств управления базой данных восстановите БД аудита.
3. Запустите узлы платформы BI с помощью ССМ.

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.

Связанные сведения

Индексация содержимого в репозитории CMS [страница 981]

14.5.1.5 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, 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`.

Связанные сведения

Индексация содержимого в репозитории CMS [страница 981]

14.5.1.5.1 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 BuinsessObjects 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 *Enter*.
4. При появлении соответствующей подсказки введите следующие данные и нажмите клавишу *ВВОД*:
   - Папка установки платформы BI (например, `<Перейдите в каталог >/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`	Должен использоваться для развертываний с одним сервером или (в развертываниях с несколькими серверами) для первого хост-компьютера сервера APS со службой поиска: В системе с несколькими серверами поиска APS при первом запуске скрипта используйте вариант `-Both` (обновляет базу данных и хранилище содержимого). Когда скрипт запускается для всех прочих серверов поиска APS, используйте вариант `-ContentStore` (обновляет только хранилище содержимого).
`-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).

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0
\java\lib>java  -jar platformsearchOnlineHotbackupRestore.jar
Enter the BOE install location :
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0

Enter the CMS Credentials:
CMS NAME: BIPW08R2
USER NAME: Administrator
PASSWORD:
AUTHENTICATION: secEnterprise
BOE Install Location = C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessOb
jects Enterprise XI 4.0 CMS = BIPW08R2  User = Administrator    Authentication =
 secEnterprise

Please verify if the details given above are correct(y/n)...Press 'e' if you wan
t to exit  :y
 What would you like to restore?
 1. Index ?
 2. Content Store ?
 3. Both Index and Content Store (Choose this option only when index and content
 store are present on one node) ?
 4. Exit ?
3_
```

14.5.2 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.

> **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.

14.5.2.1 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. Чтобы запустить мастер, 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. Для продолжения нажмите кнопку *Далее*.
   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 *OK*, 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.

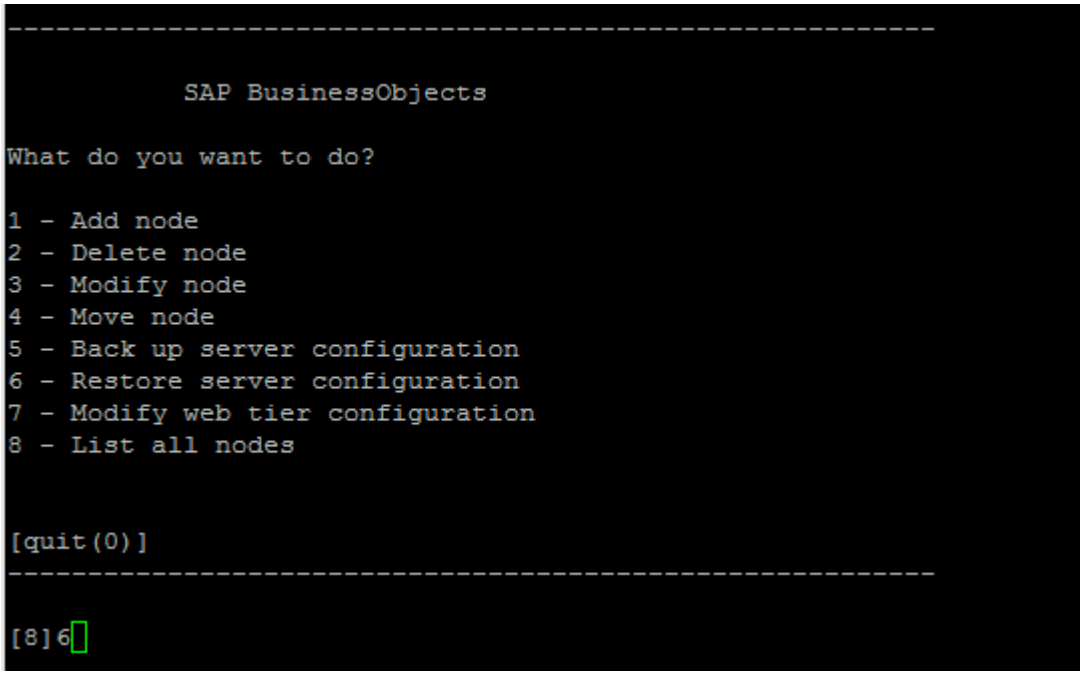
Связанные сведения

Использование узлов [страница 489]

14.5.2.2 Восстановление параметров сервера в ОС 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.

14.5.2.3 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 `RestoreCluster.bat` расположен в каталоге `<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.

В Unix файл `restorecluster.sh` расположен в каталоге `/<КАТАЛОГ_УСТАНОВКИ>/sap_bobj/enterprise_xi40/<PLATFORM64>/scripts`.

Связанные сведения

Скрипты BackupCluster и RestoreCluster [страница 597]

14.5.3 Восстановление содержимого BI

Если создана резервная копия содержимого Business Intelligence (BI) в файлах LCMBIAR, можно использовать Диспетчер переноса объектов для восстановления содержимого BI, не восстанавливая при этом всю систему. Дополнительные сведения см. в разделе «Диспетчер переноса объектов».

14.6 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.

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`
`-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`.

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.

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: • **`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 140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"`**
`-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
```

15 Копирование развертывания платформы BI

15.1 Обзор копирования системы

В этой главе описывается создание копии развертывания платформы BI для тестирования, резервирования и других целей.

Дополнительные сведения см. в SAP-ноте 1275068.

Связанные сведения

Обзор резервного копирования и восстановления [страница 575]

15.2 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.

15.3 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	Необходимые ресурсы	Решение
Цель: идентичная копия Создание дублирующей системы для резервирования или тестирования с идентичной аппаратной конфигурацией и теми же IP-адресами и именами компьютеров.	• Целевая система с аппаратной конфигурацией, аналогичной исходной системе и • Резервные копии исходной системы или доступ к исходной системе для создания резервной копии.	Используйте рабочий процесс резервного копирования и восстановления системы, описанный в этом руководстве. См. процедуру Резервное копирование всей системы [страница 579]. Воссоздайте целевую систему из резервных копий исходной системы.
Цель: копирование Создание дублирующей системы для резервирования, тестирования или обучения с аппаратной конфигурацией или IP-адресами и именами компьютеров, отличными от исходной системы.	• 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 [страница 606]	Используйте рабочий процесс копирования системы, начиная с Планирование копирования системы [страница 602], и следуйте указаниям, приведенным в остальной части главы. **Примечание** 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.

Связанные сведения

Резервные копии [страница 578]
Планирование копирования системы [страница 602]

15.4 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? Используйте функцию *Добавить/Удалить* > *Изменить* в программе установки, чтобы 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 Subversion для Диспетчера переноса объектов (необязательно).

15.5 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 копированию SAP-системы. Руководства по созданию копии системы доступны по адресу 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	Скопировать исходную систему можно только целиком. Невозможно выбрать для копирования отдельные элементы содержимого или настройки конфигурации системы.
Путь установки	Путь установки в расположениях исходной и целевой систем должен в точности совпадать: например, если исходная система установлена по адресу `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 `.properties` в папке `custom`), необходимо вручную применить эти настройки к целевому объекту.

Диаграмма с областями	Рекомендация
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 версиями. (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 [страница 38] 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 [страница 609].

- Не устанавливайте все узлы, установите только первый узел с CMS и базой данных.
- Не устанавливайте базы данных аудита, Диспетчера переноса объектов и мониторинга.
- Не воссоздавайте соединения с базамм данных аудита и отчетов.

Используйте LCM для перемещения объекта, который вы хотите восстановить из целевой системы в исходной системе.

15.6 Процедура копирования системы

Далее описываются две стадии копирования платформы BI.

15.6.1 Экспорт из исходной системы

Необходимо собрать следующие сведения об исходной системе. Если требуется записать эту информацию, то в Рабочая таблица системной копии [страница 1280] 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* CMC и разверните в левом дереве *Узлы*.
Имя компьютера и папка установки платформы BI для каждого компьютера в развертывании.	Откройте вкладку *Серверы* в CMC, 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.
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. **Примечание** Если вы копируете базу данных аудита, вам также необходимы имена и учетные данные соединения с базой данных аудита.	Откройте вкладку *Серверы* CMC, щелкните CMS правой кнопкой и выберите *Метрики*. Найдите следующие метрики: • *Имя соединения с системной базой 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 2020 или SAP Crystal Reports для 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.	В Windows это можно определить, используя средство *Удаление или изменение программ*. В ОС Unix можно воспользоваться утилитой `modifyOrRemoveProducts.sh` в каталоге установки платформы BI.

Свойство	Местоположение
Расположения хранения файлов для каждого репозитория входящих и исходящих файлов FRS в развертывании.	Откройте вкладку *Серверы* в CMC, щелкните правой кнопкой репозиторий входящих или исходящих файлов FRS и выберите *Свойства*. Найдите свойство *Каталог хранилища файлов*. **Примечание** Если значение начинается с символа "%", это заполнитель, и вам потребуется щелкнуть *Заполнители* и записать каталог, указанный для этого заполнителя.
Если планируется копировать Диспетчер переноса объектов, сохраните местоположение папки базы данных Управления жизненным цилком и папок Subversion.	Папка по умолчанию для базы данных Диспетчера переноса объектов в установках на основе Windows -`<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Data\LCM\LCMOverride`; на основе Unix - `<INSTALLDIR>/sap_bobj/data/LCM/LCMOverride`. Местонахождение по умолчанию для файлов Subversion в установках на основе Windows: • `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\CheckOut` • `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository` , а в ОС UNIX – следующие: • `<INSTALLDIR>/check_out` (этот каталог создается только после использования Subversion для извлечения файлов). • `$HOME/LCM_Repository`
Если вы планируете копирование базы данных мониторинга, сохраните местоположение папки базы данных мониторинга.	Она устанавливается в CMC. Перейдите в область управления *Приложения* в CMC, выберите *Приложение мониторинга* > *Свойства* и найдите *Каталог резервного копирования базы данных тренда*. 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`.
Путь к папке семантического уровня.	Папка по умолчанию в Windows: `<КАТАЛОГ_УСТАНОВКИ>\SAP`

Свойство	Местоположение
	`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 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 `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB`. В Unix: `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj/Data/TrendingDB`.
   - База данных Subversion для Диспетчера переноса объектов (необязательно). Для этого можно создать резервную копию файлов из папок Subversion, как указано в рабочей таблице. По умолчанию в Windows это следующие каталоги:
     - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\CheckOut`
     - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository`.

     В ОС UNIX это следующие каталоги:
     - `<INSTALLDIR>/check_out` (этот каталог создается только после использования Subversion для извлечения файлов).
     - `$HOME/LCM_Repository`
   - Файлы конфигурации из папки семантического уровня: файл `cs.cfg` в папке `connectionServer`, а также любые файлы `.sbo` и `.prm` во всех вложенных папках.

     > **Примечание**
     >
     > Сведения об ограничениях и подробное описание этой процедуры см. в разделе Оперативное резервное копирование [страница 580].
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
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/conf`
   - `clientSDKOptions.xml`, установленный в каталоге:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/java/lib`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/win32_x86`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/win64_x64`
   - `CRConfig.xml`, устанавливается в папку:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/java`
   - `mdas.properties`, устанавливается в папку:

    - `[INSTALLDIR]/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.sapappsvr75`
    - `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`, установленный в каталоге:
    - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/BOE/WEB-INF/TraceLog`
    - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/conf`
  - `clientaccesspolicy.xml`, устанавливается в папку:
    - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT`
  - `clientSDKOptions.xml`, установленный в каталоге:
    - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/clientapi/WEB-INF/lib`
    - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/lib`
  - `crossdomain.xml`, устанавливается в папку:
    - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT`
    - `[INSTALLDIR]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.

15.6.2 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

сведения (например, ключ кластера и учетные данные базы данных), определенные в разделе «Экспорт 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 [страница 586].

3. Если платформа BI уже установлена на целевом хосте, перейдите к шагу 4. Если платформа BI не установлена, установите ее на целевом хосте, не забывая о следующих шагах:
   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.

   e. 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 входящих и исходящих файлов FRS 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 Диспетчера переноса объектов (если требуется скопировать данные Диспетчера переноса объектов) в ту же папку, что использовалась в исходной системе.
9. Восстановите файлы Subversion (если требуется скопировать данные Диспетчера переноса объектов) в ту же папку, что использовалась 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. [страница 530], указав нужную базу данных.
15. Восстановите все настраиваемые пользователем файлы, резервные копии которых были созданы на шаге 3 процедуры «Экспорт из исходной системы».
16. Восстановите все файлы веб-уровня, резервные копии которых были созданы на шаге 4 процедуры «Экспорт 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 из исходной системы».

После завершения 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.

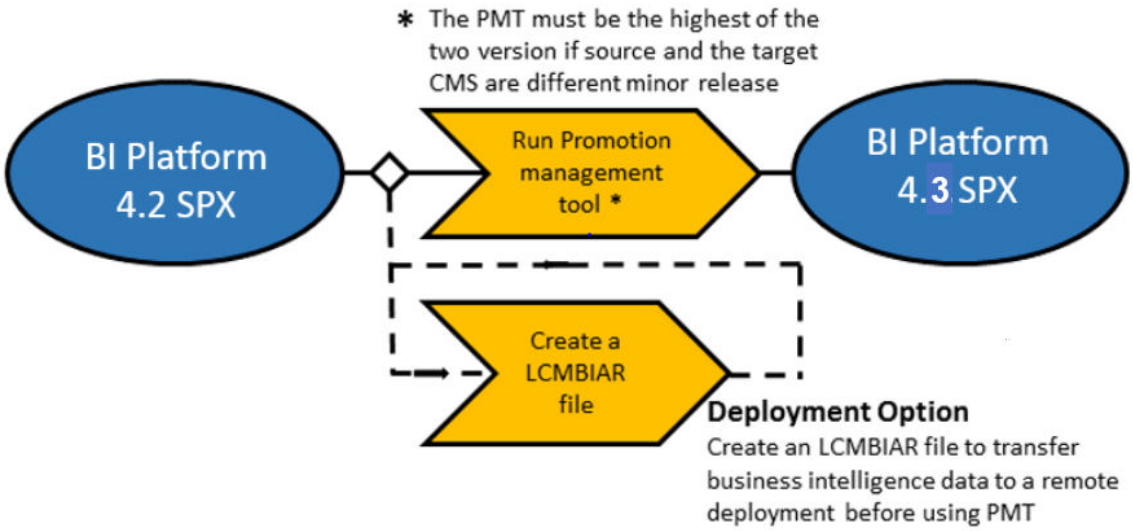
   > → Напоминание
   >
   > Если исходная система не удалена (или если она используется параллельно целевой системе), рекомендуется переименовать кластер целевой системы.

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 [страница 328].
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.

16 Управление повышением

16.1 Введение в управление переносом объектов

16.1.1 Обзор



Диспетчер переноса объектов позволяет:

- перемещать или переносить ресурсы Business Intelligence (BI) из одного репозитория в другой;
- управлять зависимостями ресурсов;
- выполнять откат перенесенных ресурсов в целевой системе в случае необходимости.

Также диспетчер переноса объектов поддерживает управление различными версиями одного ресурса BI.

Диспетчер переноса объектов интегрирован с Central Management Console. Можно перенести ресурс BI из одной системы в другую только в том случае, если и в исходной, и в целевой системе установлена одна и та же версия платформы BI.

16.1.2 Функции

Диспетчер переноса объектов позволяет выполнять следующие действия с объектами InfoObject в целевом развертывании:

- Создать новое задание
- Скопировать существующее задание
- Изменить задание
- Планировать задание для переноса
- Просмотреть журнал задания
- Экспортировать как LCMBIAR
- Импортировать BIAR и LCMBIAR

Поток операций переноса также включает следующие задачи:

- *Управление зависимостями* – эта функция позволяет выбирать, фильтровать зависимые элементы InfoObject и управлять ими в задании, которое требуется перенести.
- *Планирование* – эта функция позволяет указать время переноса задания вместо переноса задания сразу после создания. Можно задать однократное или периодическое выполнение переноса заданий.
- *Безопасность* – эта функция позволяет переносить объекты InfoObject вместе с соответствующими правами безопасности и при необходимости переносит объекты InfoObject, связанные с правами приложения.
- *Проверка переноса* – с помощью этой функции можно проверять или тестировать перенос с целью убедиться, что все защитные меры приняты до фактического переноса объектов InfoObject.
- *Откат* – эта функция позволяет после переноса задания восстановить целевую систему в ее предшествующем состоянии. Можно выполнить откат всего задания или его части.
- *Аудит* – события, сгенерированные Диспетчером переноса объектов, сохраняются в базе данных аудита. Эта функция позволяет контролировать события, записанные в базу данных аудита.
- *Параметры переопределения Диспетчера переноса объектов* – эта функция позволяет сканировать и переносить переопределения с помощью переноса заданий.

16.1.3 Права доступа к приложению

В этом разделе описаны права доступа к приложению для Диспетчера переноса объектов.

- Права доступа к Диспетчеру переноса объектов можно задать в CMC.
- Для разных функций Диспетчера переноса объектов можно задать разные права доступа.

Чтобы задать отдельные права доступа в Диспетчере переноса объектов, выполните следующие действия:

1. Выполните вход в систему на CMC и выберите *Приложения*.
2. Дважды щелкните *Диспетчер переноса объектов*.
3. Щелкните *Безопасность пользователя* и выберите пользователя. Можно просмотреть или назначить права безопасности пользователю.
4. Доступны следующие права безопасности на управление переносом:
   - Права на доступ к изменению переопределений
   - Права на доступ к включению безопасности
   - Права на доступ к администрированию
   - Права на доступ к управлению зависимостями

- Создание задания
- Удаление задания
- Изменение задания
- Изменение LCMBIAR
- Экспорт как LCMBIAR
- Импорт LCMBIAR
- Перенос задания
- Откат задания
- 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 юниверсов

5. Если необходимо назначить права выбранному пользователю, выберите соответствующее право и нажмите кнопку *Назначить безопасность*.

Права доступа к Диспетчеру переноса объектов задаются в CMC.

16.1.4 Поддержка WinAD в управлении переносами

Чтобы Диспетчер переноса объектов функционировал корректно, необходимо добавить следующее ко всем аргументам `javaargs` для всех адаптивных серверов заданий:

```
Djava.security.auth.login.config=<путь>\bsclogin.conf,Djava.security.krb5.conf=<
путь>\krb5.ini
```

> → Напоминание
>
> Укажите верный путь к `bsclogin.conf` и `krb5.ini` в своем развертывании.

16.2 Начало работы со средством "Диспетчер переноса объектов"

16.2.1 Запуск Диспетчера переноса объектов

Для запуска Диспетчера переноса объектов выберите *Диспетчер переноса объектов* на домашней странице CMC.

Любой пользователь с правами на просмотр папки *Задания для переноса* может запустить Диспетчер переноса объектов. 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 Диспетчера переноса объектов.

- Панель инструментов рабочего пространства Диспетчера переноса объектов
- Панель рабочего пространства
- Панель дерева
- Панель сведений
- Корзина покупок и страница средства просмотра заданий

Панель инструментов рабочего пространства Диспетчера переноса объектов

В следующей таблице приведен список параметров, входящих в панель инструментов рабочего пространства Диспетчера переноса объектов, и описаны задачи, которые можно выполнять с помощью этих параметров:

Параметр	Описание
	Позволяет создать новую папку. Новая папка создается как вложенная папка в папке *Задания для переноса*.
	Позволяет скопировать и удалить выбранное задание или папку из текущего местоположения.
	Позволяет скопировать задание или папку из текущего местоположения.
	Позволяет вставить скопированное задание или папку в новое местоположение.
	Позволяет удалить существующее задание или папку.
	Позволяет обновить домашнюю страницу для отображения обновленного списка заданий или папок.
Свойства	Позволяет изменить свойства выбранного задания. Можно изменять заголовок, описание и ключевые слова выбранного задания.
Журнал	Позволяет просмотреть журнал выбранного задания.
Создать задание	Позволяет создать новое задание.
Импорт	Позволяет импортировать файлы BIAR и LCMBIAR, а также файлы переопределения.

Параметр	Описание
Изменить	Позволяет изменить выбранное задание.
Перенести	Позволяет перенести выбранное задание.
Откат	Позволяет отменить перенос задания в целевой системе. **Примечание** Если задание переносит объекты в целевую систему, при откате эти объекты удаляются. Если задание обновляет объекты в целевой системе, при откате восстанавливается предыдущая версия объектов.
1	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 для переноса	Позволяет просматривать задания и папки.
Состояние переноса	Показывает перенесенные задания в соответствии с их состоянием, например, "Выполнено успешно", "Сбой" или "Выполнено частично".

Панель рабочего пространства

На панели рабочего пространства, доступной на домашней странице Диспетчера переноса объектов, выводится список заданий. Эту панель можно использовать для просмотра имени задания, его статуса, времени создания и времени последнего выполнения, исходной и целевой систем и лица, создавшего задание.

Панель дерева

На панели дерева, доступной на домашней странице Диспетчера переноса объектов, выводится древовидная структура, включающая папки *Задания для переноса* и *Состояние переноса*. Задания отображаются в иерархической структуре в папке *Задания для переноса*. В папке *Состояние переноса* отображаются перенесенные задания в соответствии с их состоянием.

Страница средства просмотра заданий

Страница «Средство просмотра заданий» выводится при создании пользователем нового здания или изменении существующего. Она содержит динамически создаваемый список объектов InfoObject для переноса и панель сведений. Объекты в списке делятся по группам пользователей, юниверсам и соединениям. На панели сведений выводится содержимое узла, выбранного в списке.

16.2.3 Использование параметра настройки

Параметр "Настройки" позволяет настраивать параметры до переноса объектов InfoObject из одного развертывания платформы BI в другое развертывание платформы BI и развертывание SAP. В этом разделе описано, как использовать параметры настройки.

Выберите раскрывающийся список *Настройки* на экране *Задания для переноса*. В этом раскрывающемся списке представлены следующие элементы:

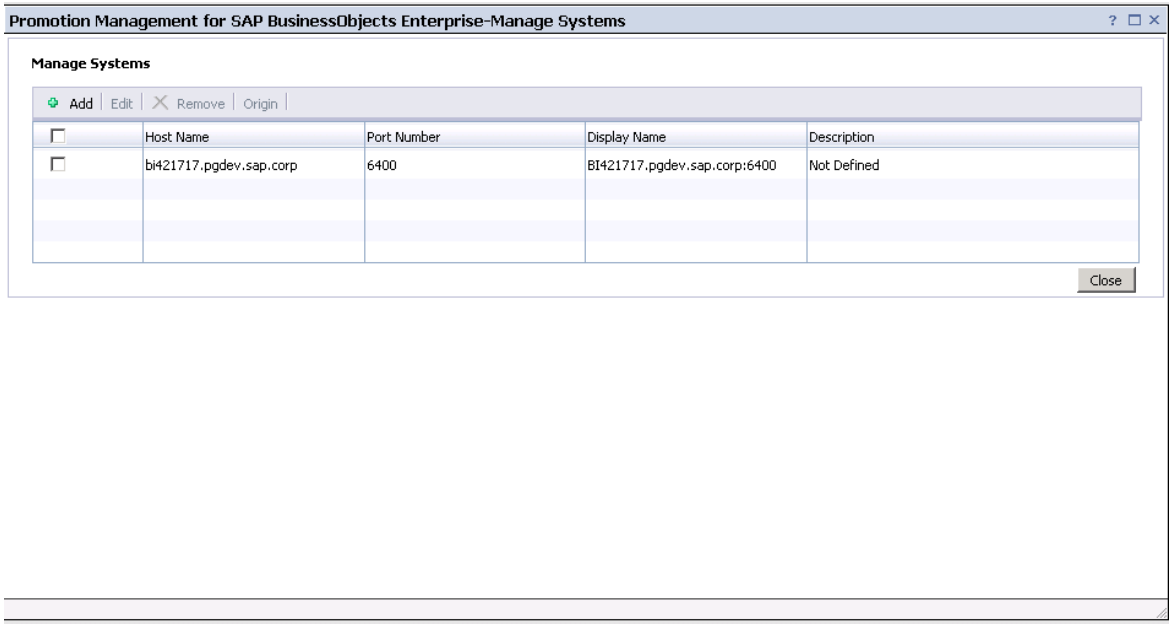
- *Управление системами* – позволяет добавить все системы, необходимые для операций Диспетчера переноса объектов.
- *Настройки отката* – позволяет выбрать систему, для которой включен откат.
- *Настройки задания* – позволяет просматривать выполненные экземпляры на странице "Зависимости" и управлять операциями очистки экземпляров задания. Здесь также можно выполнить фильтрацию по дате создания задания.
- *Настройки CTS* – позволяет добавить информацию о веб-службах и системе SAP BW для интеграции усовершенствованной системы изменений и переносов (CTS+).

16.2.3.1 Использование параметра "Управление системами"

В этом разделе описывается использование параметра "Управление системами". С помощью этого параметра можно добавлять и удалять хост-системы.

Чтобы добавить хост-систему, выполните следующие шаги:

1. На панели инструментов рабочего пространства Диспетчера переноса объектов щелкните *Настройки* и выберите *Управление системами*.
   Откроется окно *Управление системами*. В этом окне содержится список систем с указанием имени хоста, номера порта, отображаемого имени и описания.



2. Нажмите кнопку *Добавить*.
   Откроется диалоговое окно *Добавить систему*.
3. Добавьте имя хоста, номер порта, отображаемое имя и описание в соответствующие поля.

   > ⓘ Примечание
   >
   > Выберите *Пометить как источник*, чтобы определить систему как исходную, то есть систему, из которой исходит информация о соединении. Этот параметр полезен при работе с переопределениями.

4. Нажмите кнопку *OK*, чтобы добавить систему.
   Хост-система добавляется в список.

> ⓘ Примечание
>
> Чтобы удалить или изменить хост-систему, выберите ее в списке и нажмите кнопку *Удалить* или *Изменить*.

Связанные сведения

Использование параметра "Настройки отката" [страница 619]
Использование параметра "Настройки задания" [страница 619]

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.

Связанные сведения

Использование параметра "Настройки задания" [страница 619]

16.2.3.3 Использование параметра "Настройки задания"

Параметр "Настройки задания" позволяет указать, требуется ли показывать завершенные экземпляры на странице «Управление зависимостями», и число экземпляров задания, которые могут существовать в системе. Можно выбрать один из следующих параметров:

- *Показать завершенные экземпляры на странице управления зависимостями* – этот параметр позволяет просматривать завершенные экземпляры на странице «Управление зависимостями», которую можно добавить к заданию.
- *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 для задания* – этот параметр позволяет задать удаление экземпляров задания, созданных раньше, чем указанное число дней назад.
- В списке *Показать созданные задания* можно выбрать интервал времени для просмотра заданий, созданных в этом периоде.

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 *Закрыть*, чтобы закрыть окно.

> ⓘ Примечание
>
> Старые экземпляры задания удаляются только при следующем выполнении задания.

Связанные сведения

Использование Apache Subversion в качестве системы управления версиями [страница 712]

16.2.3.4 Использование опции "Параметры переопределения"

Опция "Параметры переопределения" позволяет переносить переопределения с помощью переноса заданий или файла LCMBIAR. Она позволяет сканировать, переносить и изменять информацию о соединении с базой данных для подключений Crystal Reports и юниверсов. Также ее можно использовать для изменения URL QAAWA.

> ⓘ Примечание
>
> Для использования опции "Параметры переопределения" следует установить Adobe Flash Viewer.

В следующих процедурах используется термин *система*. Существует три типа систем:

- *Источник данных*: исходная система для информации о соединении.
- *Центральный диспетчер переноса объектов*: система, где выполняется "Диспетчер переноса объектов".
- *Место назначения*: конечная система, в которую переносятся ресурсы BI.

16.2.3.4.1 Перенос переопределений

Добавьте базисную систему перед переносом переопределений. Для получения дополнительных сведений о добавлении базисных систем см. раздел Использование параметра "Управление системами" [страница 618].

Для переноса переопределений выполните следующие шаги.

1. На панели инструментов рабочего пространства Диспетчера переноса объектов выберите опцию *Параметры переопределения*.
   Будет открыто окно *Параметры переопределения*.
2. В области *Источник* выберите в раскрывающемся меню нужную исходную систему.

   > ⓘ Примечание
   >
   > Вы также можете войти в *новую систему*. Чтобы выбрать в качестве исходной системы новую систему, выполните следующие действия:
   > 1. Выберите пункт *Новая система* в раскрывающемся меню.
   > Откроется диалоговое окно Вход в источник.
   > 2. Введите действительные значения в поля *Система*, *Имя пользователя*, *Пароль* и *Аутентификация*.
   > 3. Выберите *Вход в систему*.

3. Выберите *Вход в систему*.
4. Выберите *Сканировать*.

   Начнется процесс сканирования. Откроется *список уникальных соединений*.

   > ⓘ Примечание
   >
   > Чтобы запланировать повторное сканирование, выберите *Параметры повторения*.

5. В списке переопределений установите флажок напротив каждого переопределения, которое требуется перенести.

   > ⓘ Примечание
   >
   > Можно найти нужные переопределения по имени, дате последнего обновления и другим ключевым словам.
   >
   > Вы также можете отфильтровать переопределения по следующим параметрам: все, соединение, Qwaas, Crystal Report.
   >
   > Кроме того, переопределения можно отсортировать в алфавитном порядке.

6. В области *Место назначения* выберите в раскрывающемся меню требуемую целевую систему. Можно указать несколько систем назначения.

   > ⓘ Примечание
   >
   > Вы также можете войти в *новую систему*. Чтобы выбрать в качестве целевой системы новую систему, выполните следующие действия:
   > 1. Выберите пункт *Новая система* в раскрывающемся меню.
   > Откроется диалоговое окно Вход в целевую систему.

2. Введите действительные значения в поля *Система*, *Имя пользователя*, *Пароль* и *Аутентификация*.
3. Выберите *Вход в систему*.

Чтобы экспортировать переопределения в формате LCMBIAR, выполните следующие действия:

1. Выберите команду Экспорт в файл LCMBIAR в раскрывающемся меню.
2. Выберите *Экспортировать*
   Откроется диалоговое окно *Параметры экспорта*.
3. Введите действительные значения в соответствующие поля.
4. Нажмите *Готово*.

7. Выберите *Перенести*.

   Откроется диалоговое окно Переопределения для нескольких целевых систем.

   > ⓘ Примечание
   >
   > По умолчанию выбраны все целевые системы, в которые выполнен вход. Можно выбрать отдельные целевые системы, в которые требуется перенести переопределения, установив соответствующие флажки.

8. Нажмите *Готово*.

   Перенос переопределений завершен.

9. Войдите в одну из целевых систем, используя действительные идентификационные данные.

   Все перенесенные объекты отображаются в списке уникальных соединений. Эти задания имеют статус "Неактивное".

10. Выберите *Обновить* для объектов, которые нужно изменить.

    Откроется диалоговое окно *Изменение общих свойств соединения*.

11. Обновите требуемые значения и выберите *Готово*.

    Измененные объекты станут активными.

    > ⓘ Примечание
    >
    > Также можно активировать соединение, выбрав *Неактивно*. В этом случае изменять свойства соединения в целевой системе не требуется.

12. Нажмите *Сохранить*.

16.2.3.4.2 Перенос переопределений с использованием BIAR-файлов

Добавьте базисную систему перед переносом переопределений. Для получения дополнительных сведений о добавлении базисных систем см. раздел Использование параметра "Управление системами" [страница 618].

Чтобы перенести переопределения с помощью файлов BIAR, выполните следующие действия:

1. На панели инструментов рабочего пространства Диспетчера переноса объектов выберите опцию *Параметры переопределения*.
   Будет открыто окно *Параметры переопределения*.
2. Если вы находитесь в Центральном диспетчере переноса объектов, выйдите из него.
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 запланировать повторение сканирования, выберите в раскрывающемся списке опцию *Параметры повторения*.

6. В списке переопределений измените состояние требуемых объектов на "Активен", а затем щелкните *Сохранить*.
7. Нажмите кнопку *Перенести переопределения*.
   В месте отображения списка целевых систем откроется экран *Перенести переопределения*.
8. Чтобы защитить файл BIAR паролем, отметьте флажок *Шифрование пароля*.
   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 целевую систему через CMC и выберите в Диспетчере переноса объектов *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 *OK*. Перенос переопределений завершен.
15. Выйдите из исходной системы.
16. На экране *Переопределение параметров* нажмите кнопку *Вход*.
    Откроется окно *Вход в систему*.
17. Выполните вход в целевую систему, 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*.
    Измененные объекты станут активными.
20. Нажмите кнопку *Сохранить*.

16.2.3.4.3 Перенос переопределений с использованием CTS+

Добавьте базисную систему перед переносом переопределений. Для получения дополнительных сведений о добавлении базисных систем см. раздел Использование параметра "Управление системами" [страница 618].

Чтобы перенести переопределения через CTS+, выполните следующие шаги:

> ⓘ Примечание
>
> Чтобы этот параметр стал доступным, запустите Диспетчер переноса объектов с использованием аутентификации SAP.

1. На панели инструментов рабочего пространства Диспетчера переноса объектов выберите опцию *Параметры переопределения*.
   Будет открыто окно *Параметры переопределения*.
2. Если вы находитесь в Центральном диспетчере переноса объектов, выйдите из него.
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 запланировать повторение сканирования, выберите в раскрывающемся списке опцию *Параметры повторения*.

6. В списке переопределений измените состояние объектов, которые нужно повысить, на "Активен", а затем щелкните *Сохранить*.
7. Нажмите кнопку *Перенести переопределения*.
   В месте отображения списка целевых систем откроется экран *Перенести переопределения*.
8. В раскрывающемся списке *Параметры переноса* выберите значение *Перенести с помощью CTS+*.
9. Нажмите кнопку *Перенести*.
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. раздел Веб-интерфейс организатора переносов.
    b. Если запрос имеет статус *Изменяемый*, нажмите кнопку *Выпустить*, чтобы выпустить запрос на перенос переопределений. Для получения дополнительных сведений об освобождении запросов на перенос, содержащих объекты, не относящиеся к ABAP, см. раздел Освобождение запросов на перенос с объектами, не относящимися к ABAP.

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 идентификатор целевой системы Диспетчера переноса объектов.
       Можно просмотреть список запросов на перенос, которые можно импортировать в систему.
    e. Нажмите кнопку *Обновить*.
    f. Импортируйте соответствующие запросы на перенос. Дополнительную информацию см. в документе Импорт запросов.
12. Перенос переопределений завершен.
13. Войдите в одну из целевых систем, используя действительные идентификационные данные.
    Список всех перенесенных 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*.
    Измененные объекты станут активными.
16. 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. раздел Настройка параметров CTS+ в Диспетчере переноса объектов [страница 684] для получения дополнительной информации об использовании параметра "Настройки CTS" и настройке CTS для использования с Диспетчером переноса объектов.

16.3 Использование Диспетчера переноса объектов

При запуске Диспетчера переноса объектов по умолчанию открывается страница *Задания для переноса*.

> ⓘ Примечание
>
> В диспетчере переноса объектов реализованы усовершенствования безопасности, что приводит к изменениям в определенном поведении при выполнении действий. Дополнительные сведения см. в SAP-ноте 3350454.

Экран домашней страницы *Задания для переноса* содержит различные вкладки, которые позволяют выполнять следующие задачи:

- Щелкните *Новое задание*, чтобы создать новое задание. Также можно щелкнуть правой кнопкой мыши экран домашней страницы и выбрать *Новое задание* из списка.
- Выберите *Импорт* > *Файл импорта*, чтобы импортировать файл BIAR или LCMBIAR напрямую из файловой системы и не выполнять полную процедуру создания нового задания.
- Для импорта переопределений выберите *Импорт* > *Переопределить файл*.
- Выберите существующее задание из списка и щелкните *Изменить*, чтобы изменить выбранное задание.
- Выберите существующее задание из списка и щелкните *Перенести*, чтобы перенести задание из исходной системы в целевую систему или экспортировать задание в файл LCMBIAR.
- Выберите существующее выполненное ранее задание из списка и щелкните *Откат*, чтобы отменить изменения в целевой системе.
- Выберите существующее выполненное ранее задание из списка и щелкните *Журнал*, чтобы просмотреть предыдущие экземпляры переноса выбранного задания.
- Выберите существующее задание из списка и щелкните *Свойства*, чтобы просмотреть свойства выбранного задания, такие как заголовок, идентификатор, имя файла и описание.

Прикладная область *Задания для переноса* содержит список заданий и папок, существующих в системе, вместе со следующей информацией о каждом задании или папке:

- *Имя:* имя созданного задания или папки.
- *Статус:* статус задания, например, "Создано", "Успешно", "Частично успешно", "Выполняется" или "Сбой".
- *Создано:* дата и время создания задания или папки.
- *Последний запуск:* дата и время последнего переноса задания.
- *Исходная система:* имя системы, откуда переносится задание.
- *Целевая система:* имя системы, куда переносится задание.
- *Автор:* имя пользователя, создавшего конкретное задание или папку.

> **Примечание**
>
> Диспетчер переноса объектов использует для всех операций SDK платформы BI.

16.3.1 Создание и удаление папок

Этот раздел описывает процесс создания и удаления папки на домашней странице заданий для переноса.

> **Примечание**
>
> В диспетчере переноса объектов реализованы усовершенствования безопасности, что приводит к изменениям в определенном поведении при выполнении действий. Дополнительные сведения см. в SAP-ноте 3350454.

16.3.1.1 Создание папки

Этот раздел описывает процесс создания папки.

Чтобы создать папку, выполните следующие шаги:

1. На панели инструментов управления переносом нажмите .
2. В диалоговом окне *Создать папку* введите имя папки.
3. Нажмите кнопку *OK*.

Создана новая папка.

Связанные сведения

Создание задания [страница 628]
Удаление папки [страница 627]

16.3.1.2 Удаление папки

Этот раздел описывает процесс удаления папки.

> ⓘ Примечание
>
> В диспетчере переноса объектов реализованы усовершенствования безопасности, что приводит к изменениям в определенном поведении при выполнении действий. Дополнительные сведения см. в SAP-ноте 3350454.

Для удаления папки выполните следующие шаги:

1. Выберите папку на домашней странице *Задания для переноса*.
2. Щелкните .
   Откроется диалоговое окно подтверждения.
3. Нажмите кнопку *OK*.

Выбранная папка удалена.

Связанные сведения

Создание задания [страница 628]

16.3.2 Создание задания

В этом разделе описывается процесс создания нового задания с использованием Диспетчера переноса объектов.

В следующей таблице представлены элементы GUI и поля, которые можно использовать для создания нового задания:

> **Примечание**
>
> В диспетчере переноса объектов реализованы усовершенствования безопасности, что приводит к изменениям в определенном поведении при выполнении действий. Дополнительные сведения см. в SAP-ноте 3350454.

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 BI, из которой требуется перенести задание.
Целевая система	Имя системы платформы BI, в которую требуется перенести 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	Тип аутентификации, используемый для входа в исходную или целевую систему. Диспетчер переноса объектов поддерживает следующие типы аутентификации: • Enterprise • Windows AD • LDAP • 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 Диспетчер переноса объектов выполните следующие действия:

1. Запустите Диспетчер переноса объектов.
2. На домашней странице *Задания для переноса* выберите *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. 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.
6. Нажмите кнопку *Создать*.
   Будет открыто окно «Добавить объекты».
7. Выберите объекты из исходной системы, которые требуется добавить в задание, а затем нажмите кнопку *Добавить и закрыть*.
8. Нажмите кнопку *Сохранить*.

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.

Связанные сведения

Использование опции "Параметры переопределения" [страница 620]

16.3.2.1 Вход в новую систему CMS

Этот раздел описывает, как войти в новый CMS.

> ⓘ Примечание
>
> В диспетчере переноса объектов реализованы усовершенствования безопасности, что приводит к изменениям в определенном поведении при выполнении действий. Дополнительные сведения см. в SAP-ноте 3350454.

Чтобы войти в новый CMS, выполните следующие шаги:

1. Запустите Диспетчер переноса объектов.
2. Создайте новое задание.

   Для получения дополнительных сведений о создании нового задания см. Создание задания [страница 628]
3. В раскрывающемся списке *Исходная система* выберите *Выполнить вход в новую CMS*.
   Будет открыто диалоговое окно *Вход в систему*.
4. Выберите систему в раскрывающемся списке или введите новое имя системы.
5. Введите реквизиты пользователя, выберите соответствующий тип аутентификации и нажмите кнопку *Вход в систему*.
6. В раскрывающемся списке *Целевая система* выберите *Вход в новую CMS*.
7. Выберите систему в раскрывающемся списке или введите новое имя системы.
8. Введите учетные данные пользователя, выберите соответствующий тип аутентификации и нажмите кнопку *Вход в систему*.

Связанные сведения

Редактирование задания [страница 632]
Добавление объекта InfoObject в задание [страница 632]
Повышение задания при соединении с репозиториями [страница 635]
Планирование переноса задания [страница 642]

16.3.3 Создание нового задания путем копирования существующего

В этом разделе описан процесс создания нового задания путем копирования существующего.

> **Примечание**
>
> В диспетчере переноса объектов реализованы усовершенствования безопасности, что приводит к изменениям в определенном поведении при выполнении действий. Дополнительные сведения см. в SAP-ноте 3350454.

Для создания нового задания путем копирования существующего выполните следующие шаги:

1. Запустите Диспетчер переноса объектов.
2. На домашней странице *Задания переноса* выберите *Создать задание*.
3. Нажмите параметр *Копировать существующее задание*.
   Появится окно *Копировать существующее задание*, где отображается список заданий в папке *Задания для переноса*.
4. Выберите в списке требуемое задание и нажмите кнопку *Создать*.
   Отображаются имя, ключевые слова и описание задания, а также поля *Сохранить задание в* и *Место назначения*. При необходимости эти поля можно изменить.

5. В поле *Сохранить задание в* найдите и выберите папку, в которой требуется сохранить задание, и выберите *Сохранить*.

Создано новое задание, открывается окно *Добавить объекты*.

Связанные сведения

Добавление объекта InfoObject в задание [страница 632]
Редактирование задания [страница 632]
Повышение задания при соединении с репозиториями [страница 635]

16.3.4 Поиск задания

Функция поиска Диспетчера переноса объектов используется для поиска задания, которое доступно в репозитории.

> ⓘ Примечание
>
> В диспетчере переноса объектов реализованы усовершенствования безопасности, что приводит к изменениям в определенном поведении при выполнении действий. Дополнительные сведения см. в SAP-ноте 3350454.

Для поиска задания выполните следующие действия:

1. В поле *Поиск* на домашней странице введите текст, который требуется найти.
2. Щелкните список, открывающийся рядом с полем *Поиск*, чтобы указать параметры поиска. Можно указать следующие параметры поиска:
   - *Поиск по названию* – этот параметр позволяет искать задание по имени.
   - *Поиск по ключевым словам*– этот параметр позволяет искать задание по ключевым словам.
   - *Поиск по описанию*– этот параметр позволяет искать задание по описанию.
   - *Поиск по всем полям* – этот параметр позволяет искать задание по заголовку, ключевым словам и описанию.
3. Щелкните значок поиска.

Связанные сведения

Добавление объекта InfoObject в задание [страница 632]
Редактирование задания [страница 632]

16.3.5 Редактирование задания

В этом разделе описывается процесс изменения задания.

> ⓘ Примечание
>
> - В диспетчере переноса объектов реализованы усовершенствования безопасности, что приводит к изменениям в определенном поведении при выполнении действий. Дополнительные сведения см. в SAP-ноте 3350454.
> - Изменение задания не является созданием нового задания.

Чтобы изменить задание, выполните следующие шаги:

1. Запустите Диспетчер переноса объектов.
2. На домашней странице *Задания для переноса* выберите задание, которое требуется изменить.
3. Щелкните *Изменить*.
   Появится подробная информация о выбранном задании. В зависимости от необходимости можно добавлять или удалять объекты InfoObject, управлять зависимостями и переносить задание.

Во время изменения задания имя исходной системы не может быть изменено.

Связанные сведения

Добавление объекта InfoObject в задание [страница 632]
Повышение задания при соединении с репозиториями [страница 635]
Планирование переноса задания [страница 642]

16.3.6 Добавление объекта InfoObject в задание

Каждое задание должно содержать набор объектов InfoObject. Поэтому следует добавлять объекты InfoObject в задание до передачи его в целевую систему.

> ⓘ Примечание
>
> - При переносе 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.
> - В диспетчере переноса объектов реализованы усовершенствования безопасности, что приводит к изменениям в определенном поведении при выполнении действий. Дополнительные сведения см. в SAP-ноте 3350454.

Для добавления информационного объекта в задание выполните следующие шаги:

1. Запустите Диспетчер переноса объектов.
2. Создайте новое задание или измените существующее.

Для получения сведений о создании нового задания см. Создание задания [страница 628] и Редактирование задания [страница 632].

3. В случае изменения задания выберите *Добавить объекты*.

   > ⓘ Примечание
   >
   > При создании нового задания открывается диалоговое окно *Добавить объекты*.

4. Перейдите к папке, в которой требуется выбрать InfoObject.
   В выбранной папке появится список объектов InfoObject.
5. Выберите объект InfoObject, который требуется добавить в задание, и нажмите кнопку *Добавить*.

   Если требуется добавить инфо-объект и выйти из диалогового окна «Добавить объекты из системы: `<ИМЯ>`», нажмите кнопку *Добавить и закрыть*. Объект InfoObject будет добавлен к заданию, и диалоговое окно закроется.

После добавления объекта InfoObject в задание можно щелкнуть правой кнопкой мыши страницу *Средство просмотра заданий* и выбрать процессы переноса для задания. Можно управлять объектами, зависимыми от выбранного объекта InfoObject, с помощью параметра *Управление зависимостями* на странице *Средство просмотра заданий*.

> ⓘ Примечание
>
> - В корзине покупок, которая отображается на левой панели страницы *Средство просмотра заданий*, выводится задание вместе с зависимыми элементами в виде простой древовидной структуры.
> - Для сохранения изменений нажмите кнопку *Сохранить* после добавления объектов InfoObject. В противном случае пользователю предлагается сохранить задание при закрытии вкладки.

Рекомендация. Для оптимальной производительности Диспетчера переноса объектов SAP BusinessObjects рекомендует выбирать для переноса небольшое количество объектов InfoObject, не более 100 одновременно.

Связанные сведения

Управление зависимостями задания [страница 633]
Повышение задания при соединении с репозиториями [страница 635]
Планирование переноса задания [страница 642]

16.3.7 Управление зависимостями задания

Этот раздел описывает процесс управления зависимыми объектами объекта InfoObject.

> ⓘ Примечание
>
> В диспетчере переноса объектов реализованы усовершенствования безопасности, что приводит к изменениям в определенном поведении при выполнении действий. Дополнительные сведения см. в SAP-ноте 3350454.

Чтобы управлять зависимыми объектами объекта InfoObject, выполните следующие шаги:

1. Запустите Диспетчер переноса объектов.
2. Создайте новое задание или измените существующее.
   Для получения сведений о создании нового задания см. Создание задания [страница 628] и Редактирование задания [страница 632].
3. Добавьте требуемые объекты InfoObject в задание и закройте диалоговое окно *Добавить объекты*, чтобы вернуться к окну *Средство просмотра заданий*.
4. Нажмите кнопку *Управление зависимостями*.
   Откроется окно *Управление зависимостями*. В этом окне представлен список объектов InfoObject 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 для добавления сгруппированных зависимых объектов в задание. Зависимые объекты не выбираются по умолчанию; необходимо явно выбрать зависимые элементы, которые требуется повысить.

   Например, при выборе *Все юниверсы* в раскрывающемся списке *Выбор зависимых объектов*, будут выбраны все юниверсы, включенные в список зависимых объектов. Также можно выбирать зависимые объекты по отдельности.

   Для просмотра поддерживаемых параметров фильтрации объектов InfoObject можно щелкнуть

   Тип. Откроется раскрывающийся список. Этот список содержит поддерживаемые параметры фильтрации. Выберите параметр фильтрации и нажмите кнопку *OK*. Появятся отфильтрованные объекты InfoObject.

   При выборе зависимых объектов в столбце *Зависимые объекты* и нажатии *Применить изменения* 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. вПоиск зависимых объектов [страница 635].
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 объектов InfoObject или свойств объектов InfoObject. 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.

Связанные сведения

Повышение задания при соединении с репозиториями [страница 635]

16.3.8 Поиск зависимых объектов

Функция расширенного поиска в Диспетчере переноса объектов позволяет находить зависимые объекты объектов InfoObject, доступных в репозитории.

> ⓘ Примечание
>
> В диспетчере переноса объектов реализованы усовершенствования безопасности, что приводит к изменениям в определенном поведении при выполнении действий. Дополнительные сведения см. в SAP-ноте 3350454.

Для поиска зависимых объектов объекта InfoObject выполните следующие действия:

1. Запустите Диспетчер переноса объектов.
2. Создайте новое задание или измените существующее.
   Если создано новое задание, добавьте в него объекты InfoObject. 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.

Связанные сведения

Управление зависимостями задания [страница 633]

16.3.9 Повышение задания при соединении с репозиториями

В этом разделе описывается процесс переноса задания из исходной системы в целевую, если обе они являются продуктивными.

> ⓘ Примечание
>
> В диспетчере переноса объектов реализованы усовершенствования безопасности, что приводит к изменениям в определенном поведении при выполнении действий. Дополнительные сведения см. в SAP-ноте 3350454.

В следующей таблице содержится список типов объектов InfoObject, которые можно переносить с помощью Диспетчера переноса объектов:

Категория	Типы объектов, которые можно повысить
Отчеты	Отчеты Crystal, Web Intelligence, QaaWS, Lumira

Категория	Типы объектов, которые можно повысить
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, документ папки "Входящие", персональная папка и папка "Избранное"
Юниверс, рабочее пространство, наборы	Юниверсы (UNV), соединения, наборы
Информационная панель EPM	Юниверсы, соединения, отчеты и аналитика
Бизнес-представление	Фонд данных
Интеграция • Список тиражирования • Задания на тиражирование	Список тиражирования обеспечивает повышение следующих объектов: Flash, .txt, дискуссии, .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, юниверс DSL (UNX), бизнес-уровень (BLX), соединение (CNX), основание данных (DFX), WebI, Data Federator, Data Steward, рабочее пространство BI и т. д.
Манданты	Диспетчер переноса объектов поддерживает перенос арендаторов вместе с объектами, от которых они зависят, из исходной системы в целевую, предоставляя возможности выбора и добавления арендаторов и соответствующих им объектов в задание. Также Диспетчер устанавливает связь между мандантами и соответствующими объектами мандантов в виде зависимостей. Эта функция работает в режимах графического интерфейса пользователя (GUI) и интерфейса командной строки (CLI) Диспетчера переноса объектов.

В Диспетчере переноса объектов поддерживается сервис комментирования BI Commentary. При переносе документа, к которому есть комментарии, они также переносятся из исходной системы в целевую (в сценариях Live to Live, Live to BIAR, BIAR to Live). Чтобы перенести документ с комментариями выберите *Повысить* > *Настройки комментариев* и установите флажок *Включить комментарии*.

> **Примечание**
>
> По умолчанию флажок *Включить комментарии* не установлен.

При переносе тиражированных объектов специфичные для тиражирования сведения, связанные с объектами, также переносятся из исходной системы в целевую (в сценариях Live to Live, Live to BIAR, BIAR to Live).. Чтобы перенести документ без специфичных для тиражирования сведений, выберите *Перенести* > *Настройки заданий объединения* и снимите флажок *Включить отношение заданий объединения*.

> **ⓘ Примечание**
>
> По умолчанию флажок *Включить отношение заданий объединения* установлен.

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 списке *Место назначения* выберите другую целевую систему, если это необходимо.

   > **ⓘ 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 и журнале заданий. Диспетчер переноса объектов позволяет сопоставить каждый экземпляр создания задания с идентификатором управления изменениями. Идентификатор управления изменениями – это атрибут, который 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 возможные действия:
   - *Не переносить безопасность* – это параметр по умолчанию.
   - *Перенести безопасность* – используйте этот параметр для переноса заданий вместе с соответствующими правами безопасности.
   - *Перенести безопасность объекта* – используйте этот параметр для переноса безопасности объектов и папок.
   - *Перенести безопасность пользователя* – позволяет перенести права пользователей, участвующих в задании.
   - *Включить права приложения* – этот параметр можно выбрать, только если выбран параметр *Перенести безопасность пользователя*. Если объекты задания наследуют какие-либо права приложения, задание повышается вместе с этими правами.
   - *Перенести безопасность верхнего уровня* – используйте этот параметр для переноса прав безопасности верхнего уровня.

     > **⚠ Предупреждение**
     >
     > Параметр *Перенести безопасность верхнего уровня* перезаписывает права безопасности верхнего уровня, определенные в целевой системе.

   Также можно выбрать *Права просмотра* для просмотра зависимостей безопасности информационных объектов задания.

> **ⓘ Примечание**
>
> Кнопка *Права просмотра* неактивна, пока вы не сохраните новое задание.

6. Нажмите *Сохранить*.

   Кнопка *Права просмотра* станет активной. Теперь можно просматривать зависимости безопасности.

7. Выберите *Проверить повышение*, чтобы убедиться в отсутствии конфликтов между идентификаторами CUID информационных объектов исходной и целевой системах. Сведения о переносе отображаются на вкладках *Успешно*, *Сбой* и *Предупреждение*. В первом столбце отображаются объекты для повышения, а во втором – состояние повышения каждого информационного объекта. В Диспетчере переноса объектов 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:

   - `Перезаписано` – объект InfoObject в целевой системе перезаписан объектом InfoObject из исходной системы.
   - `Скопировано` – объект InfoObject из исходной системы скопирован в целевую систему.
   - `Удалено` – объект InfoObject не перенесен из исходной системы в целевую.
   - `Предупреждение` – объект InfoObject в целевой системе имеет более новую версию и может удалить объект InfoObject из задания. Однако если требуется, информационный объект будет повышен.
   - `Сопоставлено`– объект InfoObject сопоставлен с объектом InfoObject в целевой системе.

8. Нажмите *Расписание*, чтобы задать выполнение переноса в определенное время или периодически по расписанию.
9. Нажмите кнопку *Перенести*.
   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 Перенос задания с помощью файла LCMBIAR

Перенос относится к действию передачи источника BI из одного репозитория в другой. Если исходная и целевая системы находятся в одной сети, Диспетчер переноса объектов передает объект InfoObject через локальную или глобальную сеть. Однако Диспетчер переноса объектов поддерживает перенос объектов InfoObject, даже если исходная и целевая системы не находятся в одной сети.

На случай отсутствия соединения между исходной и целевой системами Диспетчер переноса объектов поддерживает перенос заданий в целевую систему путем экспорта задания из исходной системы в файл LCMBIAR и последующего импорта этого задания из файла BIAR в целевую систему.

В этом разделе описывается выполнение экспорта задания в файл LCMBIAR и импорт задания из файла BIAR в целевую систему.

> **Примечание**
>
> - В диспетчере переноса объектов реализованы усовершенствования безопасности, что приводит к изменениям в определенном поведении при выполнении действий. Дополнительные сведения см. в SAP-ноте 3350454.
> - В диспетчере переноса объектов реализованы усовершенствования безопасности, что приводит к изменениям в определенном поведении при выполнении действий. Для получения дополнительных сведений см. SAP-ноту 3350454.

Связанные сведения

Экспорт задания в файл LCMBIAR [страница 639]
Импорт задания из файла LCMBIAR [страница 640]

16.3.10.1 Экспорт задания в файл LCMBIAR

Этот раздел описывает экспорт задания в файл LCMBIAR.

Чтобы экспортировать задание в файл LCMBIAR, выполните следующие шаги:

1. Запустите Диспетчер переноса объектов и создайте новое задание.

   Дополнительные сведения о создании нового задания см. в Создание задания [страница 628]
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. Чтобы защитить файл LCMBIAR паролем, установите флажок *Шифрование паролем*.
5. Введите пароль в поле *Пароль*.
6. Повторно введите пароль в поле *Подтверждение пароля*.
7. Нажмите кнопку *Повысить*.
   Будет открыто окно *Перенести*.
8. Измените параметры безопасности в соответствии с необходимостью и нажмите кнопку *Экспорт*.
   Создан файл LCMBIAR. Можно сохранить файл LCMBIAR в файловой системе.
9. (Необязательно.) Щелкните *Место назначения файла LCMBiar* и выберите *FTP* или *SFTP*, чтобы экспортировать файл LCMBIAR на сервер FTP или SFTP. Введите имя хоста, порт, имя пользователя, пароль, каталог и имя файла и нажмите *Экспорт*.

   > **Примечание**
   >
   > Если выбрать *SFTP* в качестве *места назначения файла LCMBiar*, потребуется также ввести отпечаток SFTP.

10. В раскрывающемся списке *Место назначения* выберите пункт *В файл LCMBIAR* и нажмите кнопку *Место назначения файла LCMBIAR*.

Можно запланировать экспорт задания в файл LCMBIAR. Для получения дополнительных сведений см. раздел Планирование переноса задания [страница 642].

Связанные сведения

Добавление объекта InfoObject в задание [страница 632]
Управление зависимостями задания [страница 633]

16.3.10.2 Импорт задания из файла LCMBIAR

Можно импортировать задание из файла LCMBIAR. Файл LCMBIAR копируется с устройства хранения в целевую систему.

Чтобы импортировать файл LCMBIAR, выполните следующие действия:

1. Запустите Диспетчер переноса объектов.
2. На домашней странице *Задания для переноса* выберите *Импорт* > *Файл импорта*. Откроется окно *Импорт из файла*.
3. Файл BIAR можно импортировать из файловой системы либо с сервера FTP или SFTP.
   - Для импорта файла BIAR из файловой системы выполните следующие действия:
     1. Выберите *файловую систему*.
     2. Нажмите кнопку *Обзор* и выберите файл LCMBIAR в файловой системе.
     3. В поле *Пароль* введите пароль для файла LCMBIAR.

        > **Примечание**
        > Поле "Пароль" отображается только в случае, если файл LCMBIAR защищен паролем.

     4. Нажмите кнопку *Создать*. Задание создано.

        > **Примечание**
        > Если существует задание с этим именем, появится всплывающее окно подтверждения сохранения. Для перезаписи существующего задания нажмите "Да". Для создания задания с новым именем `Имя_задания_копия<ТЕКУЩИЕ_ДАТА_И_ВРЕМЯ>` нажмите "Нет".

   - Чтобы импортировать файл LCMBIAR с сервера FTP, выполните следующие действия:
     1. Выберите *FTP*.
     2. Введите в соответствующие поля информацию о хосте, порте, имени пользователя, пароле, каталоге и имени файла и нажмите *OK*.
   - Чтобы импортировать файл LCMBIAR с сервера SFTP, выполните следующие действия:
     1. Выберите *SFTP*.

2. Введите в соответствующие поля информацию о хосте, порте, имени пользователя, пароле, каталоге, отпечатке и имени файла и нажмите *OK*.

4. Нажмите кнопку *Перенести*.
   Появится окно *Перенести – 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 *Перенести*, чтобы перенести содержимое в целевую систему.

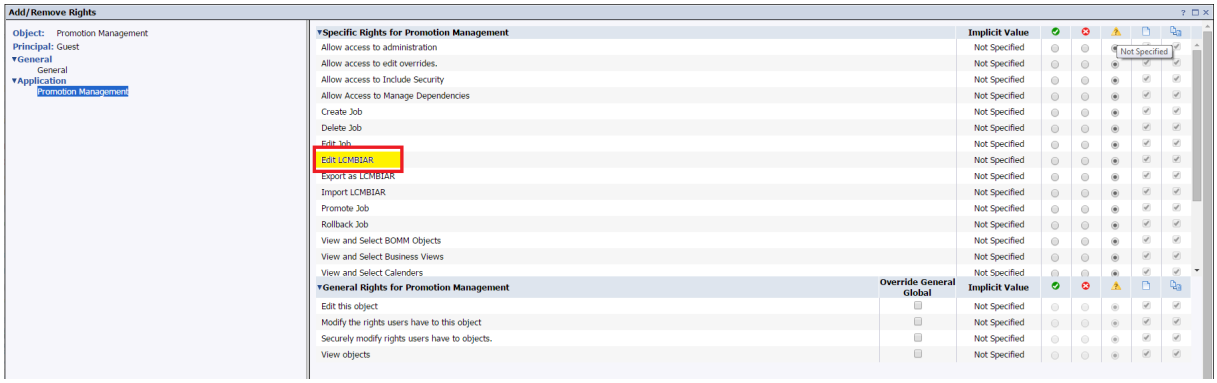
   Также можно нажать параметр *Выполнить проверку переноса*, чтобы просмотреть объекты для переноса и состояние переноса.
7. **Необязательно:** При импорте документа Web Intelligence, использующего настройку, на вкладке *Предпочтения группы пользователей BI* установите флажок *Перезаписать предпочтения группы пользователей BI*, чтобы импортировать настройку.

Связанные сведения

Управление зависимостями задания [страница 633]

16.3.10.2.1 Выборочное извлечение объектов из файла LCMBIAR

Для извлечения отдельных объектов из файла LCMBIAR необходимо, чтобы у пользователя было право *Изменить LCMBIAR*.



Чтобы извлечь отдельные объекты из файла LCMBIAR, выполните следующие действия:

1. Выберите объекты, которые нужно перенести.
2. Нажмите кнопку *Перенести*.

> ⓘ Примечание
>
> - Будет создано новое задание с выбранными объектами.

- Эту операцию также можно выполнить с помощью командной строки. Дополнительные сведения см. в разделе Параметры командной строки [страница 655].
- Выборочный перенос не поддерживается в сценарии Live to Live.

16.3.11 Планирование переноса задания

Этот раздел описывает процесс планирования переноса задания. В нем также описано, как указать параметры периодичности.

> ⓘ Примечание
>
> В диспетчере переноса объектов реализованы усовершенствования безопасности, что приводит к изменениям в определенном поведении при выполнении действий. Дополнительные сведения см. в SAP-ноте 3350454.

Чтобы спланировать перенос экземпляра задания, выполните следующие шаги:

1. В диалоговом окне *Перенос* выберите параметр *Расписание*.
2. Установите требуемое значение параметра планирования и нажмите *Запланировать*.

Если добавить объекты InfoObject в папку, которая содержится в задании, после планирования переноса задания, эти объекты также будут перенесены в место назначения в установленное время. Однако при попытке запланировать перенос задания с помощью файла LCMBIAR это не так, поскольку LCMBIAR не рассматривается как "действительное" место назначения.

> → Совет
>
> После переноса задания можно просмотреть все экземпляры этого задания, выбрав его на странице *Задания для переноса* и щелкнув *Журнал* на панели инструментов.

Перенос задания может также произойти на основе триггеров событий.

Для каждого статуса переноса 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".

Связанные сведения

Экспорт задания в файл LCMBIAR [страница 639]

16.3.11.1 Обновление повторяющихся и ожидающих экземпляров заданий для переноса

Диспетчер переноса объектов позволяет отслеживать статус экземпляров заданий переноса и изменять их расписание с помощью параметра *Повторяющиеся и ожидающие экземпляры*.

Для отслеживания статуса и изменения расписания экземпляров задания переноса выполните следующие шаги:

1. Запустите Диспетчер переноса объектов.
2. На домашней странице *Задания для переноса* выберите задание.
3. Нажмите кнопку *Журнал*.
   Будет открыто окно *Журнал заданий*.
4. Выберите *Повторяющиеся и ожидающие экземпляры*.
   Откроется окно *Журнал повторяющихся заданий и ожидающих обработки экземпляров*. В этом окне отображается список повторяющихся и ожидающих экземпляров задания переноса.

   Можно использовать следующие опции:

   - Выберите *Перенесенные экземпляры*, чтобы просмотреть список перенесенных экземпляров задания.
   - Выберите *Приостановить*, чтобы приостановить выбранный ожидающий или повторяющийся экземпляр.
   - Выберите *Возобновить*, чтобы возобновить приостановленный запланированный экземпляр задания переноса.
   - Выберите *Изменить расписание*, чтобы повторно запланировать выбранный экземпляр задания переноса.
   - Выберите , чтобы удалить запланированный экземпляр задания переноса.
   - Выберите , чтобы обновить статус запланированного экземпляра задания переноса.
   - 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 задания переноса, например, повторяющийся, ожидающий и т. д.

Связанные сведения

Откат задания [страница 644]

16.3.12 Просмотр журнала заданий

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

> **Примечание**
>
> В диспетчере переноса объектов реализованы усовершенствования безопасности, что приводит к изменениям в определенном поведении при выполнении действий. Дополнительные сведения см. в SAP-ноте 3350454.

Чтобы просмотреть журнал задания, выполните следующие шаги:

1. Запустите Диспетчер переноса объектов.
   Откроется домашняя страница *Задания для переноса*.
2. Выберите задание, историю которого требуется просмотреть, и нажмите на вкладку *История*.

   Появится следующая информация: время экземпляра задания, имя задания, имена исходной и целевой систем, идентификатор пользователя, выполнившего перенос задания, и статус ("Успешно", "Сбой" или "Частично успешно").

   Подробный 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 переноса задания.

> **Примечание**
>
> В диспетчере переноса объектов реализованы усовершенствования безопасности, что приводит к изменениям в определенном поведении при выполнении действий. Дополнительные сведения см. в SAP-ноте 3350454.

Чтобы откатить задание, выполните следующие шаги:

1. Запустите Диспетчер переноса объектов.
   Откроется домашняя страница *Задания для переноса*.
2. Выполните любую из следующих операций:
   - Щелкните правой кнопкой мыши задание, откат которого требуется выполнить, и выберите *Откат*.

- Выберите задание, откат которого требуется выполнить, и щелкните вкладку *Откат*.

Будет открыто окно *Откат*.

3. Выберите экземпляр, откат которого требуется выполнить, и нажмите кнопку *Полный откат*.
   Будет выполнен откат экземпляра.

Можно выполнить откат только самого последнего экземпляра задания. Нельзя выполнить откат нескольких экземпляров задания одновременно.

16.3.13.1 Использование параметра "Частичный откат"

Диспетчер переноса объектов позволяет выполнить полный или частичный откат объектов InfoObject в задании в целевой системе.

Чтобы выполнить частичный откат объектов infoobject, выполните следующие шаги:

1. Запустите Диспетчер переноса объектов.
   Откроется домашняя страница *Задания для переноса*.
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*.

   Будет открыто окно *Откат*.
3. Выберите экземпляр из списка и нажмите кнопку *Частичный откат*.

   Список объектов infoobject в выбранном задании появится на странице *Средство просмотра заданий*.
4. Выберите объекты infoobject, для которых требуется выполнить откат, и нажмите кнопку *Откат*.

> ⓘ Примечание
>
> Убедитесь, что выполнен откат всех объектов InfoObject в экземпляре, прежде чем выполнять откат объектов в следующем экземпляре.

> ⚠ Предупреждение
>
> Если задание переносится с применением настроек безопасности, то в процессе частичного отката информационных объектов InfoObject выбранные зависимые информационные объекты InfoObject могут не получить предшествующего состояния безопасности, которое было до осуществления отката.

Связанные сведения

Управление разными версиями ресурсов BI [страница 709]

16.3.13.2 Откат задания по истечении срока действия пароля

В этом разделе описывается процесс отката задания после того, как истек срок действия пароля, использованного для переноса.

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, перенесенные с использованием учетных данных исходной или целевой системы, обновляются автоматически.

Связанные сведения

Частичный откат объектов InfoObject по истечении срока действия пароля [страница 646]
Использование параметра "Частичный откат" [страница 645]

16.3.13.2.1 Частичный откат объектов InfoObject по истечении срока действия пароля

В этом разделе описывается процесс частичного отката объектов InfoObject после того, как истек срок действия пароля исходной или целевой системы.

Чтобы осуществить частичный откат объектов InfoObject по истечении срока действия пароля, выполните следующие шаги:

1. Выберите задание, которое требуется откатить, и нажмите кнопку *Откат*.
   Будет открыто окно *Откат*.
2. Выберите параметр *Частичный откат*.
   Появится сообщение об ошибке. Это сообщение говорит о том, что откат объектов InfoObject 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 заданий*. На этой странице представлен список объектов InfoObject.
4. Выберите требуемые объекты InfoObject и нажмите кнопку *Откат*.

> **Примечание**
>
> Задания, перенесенные с использованием учетных данных исходной или целевой системы, обновляются автоматически.

Связанные сведения

Откат задания [страница 644]
Использование параметра "Частичный откат" [страница 645]
Откат задания по истечении срока действия пароля [страница 646]

16.4 Перенос всего содержимого репозитория с помощью Диспетчера переноса объектов

Перенос содержимого репозитория требует планирования, подготовки и достаточного времени. В этом разделе описаны действия, необходимые для успешного переноса содержимого из одного развертывания в другое.

16.4.1 Подготовка исходной и целевой систем

Перед переносом содержимого необходимо убедиться, что исходная и целевая системы настроены оптимальным образом.

1. В исходной системе:
   a. Используйте Repository Diagnostic Tool (RDT) для сканирования исходной системы и исправления ошибок. Устраните любые несоответствия в репозитории и FRS. Для получения дополнительных сведений об RDT см. *Руководство пользователя Repository Diagnostic Tool платформы Business Intelligence*.
   b. Минимизируйте использование исходной системы, чтобы обеспечить минимальные изменения во время переноса. Активность системы может привести к сбоям в объектах.

   > **Примечание**
   >
   > При возникновении ошибок проверьте статус задания для их исправления.

2. В целевой системе:
   a. Используйте ключ лицензии, чтобы убедиться, что в целевой системе установлена правильная и достаточная лицензия.

   > **Примечание**
   >
   > Чтобы избежать сбоя переноса содержимого из-за недостаточности лицензии, используйте одинаковые лицензии в обеих системах.

b. При использовании сторонней аутентификации необходимо настроить и включить ее в целевой системе, прежде чем переносить содержимое.

> **Примечание**
>
> Не сопоставляйте пользователей или группы пользователей. Это приведет к созданию в целевой системе пользователей и групп пользователей с другими CUID. Процесс переноса использует CUID для определения и сопоставления объектов между исходной и целевой системами. Сопоставление пользователей и групп пользователей приведет к несоответствиям в содержимом и сбою переноса.

c. Убедитесь, что все необходимые дополнительные компоненты в исходной системе установлены также в целевой системе.

> **Примечание**
>
> Для обеспечения успешной миграции необходимо установить в исходной системе дополнительные компоненты, такие как Analysis или Design Studio.

d. При наличии содержимого с использованием соединений QaaWS необходимо включить переопределения, чтобы эти соединения указывали на правильные веб-службы. Дополнительные сведения о настройке переопределений см. в разделе «Переопределения».

e. Если требуется перенести все выполненные запланированные экземпляры, необходимо щелкнуть *Показать завершенные экземпляры на странице управления зависимостями* в *Настройках задания* в Диспетчере переноса объектов.

3. В центральной системе:

a. Можно назначить исходную, целевую или отдельную систему центральной системой, где выполняются задания Диспетчера переноса объектов. При переносе всего репозитория необходимо обработать большое количество содержимого, что требует дополнительных системных ресурсов в центральной системе. Используйте следующую справочную информацию для настройки центральной системы для 10 000 объектов:

	Временное выделение памяти	Выделение памяти	Дополнительная настройка
`LCM_CLI`	2 ГБ	2 ГБ	Обновите `LCM_CLI.bat` и измените параметр `-Xmx`.
Сервер заданий Диспетчера переноса объектов	3 ГБ	3 ГБ	В CMC обновите свойство запуска сервера заданий Диспетчера переноса объектов, добавив параметр `-javaargs Xmx3g`. Дополнительные сведения см. в SAP-ноте 2286419.

Например, если задание будет содержать порядка 50 000 объектов:

- Выделите 10 ГБ памяти для `LCM_CLI` (50 000 ÷ 10 000 × 2)
- Выделите 15 ГБ памяти для сервера заданий (50 000 ÷ 10 000 × 3)

> **Примечание**
>
> Эти инструкции по оценке размеров применимы для большинства сред. Однако размер документов может повлиять на потребность в ресурсах.

16.4.2 Стратегии миграции

- Используйте для переноса всех заданий интерфейс командной строки, а не веб-средство CMC.
  - Интерфейс командной строки позволяет обойти 20-минутный лимит веб-сеанса во время выполнения задания переноса, которое включает больше 1000 объектов.

    > **Примечание**
    >
    > Ограничение на число объектов зависит от достаточности системных ресурсов.

  - Интерфейс командной строки обеспечивает точный контроль над переносом содержимого за счет использования языка запросов для выбора содержимого для миграции. Можно выбрать содержимое одного типа или содержимое, находящееся в одном каталоге.
  - Из интерфейса командной строки возможно пакетное выполнение, а задания переноса могут запускаться другими средствами создания скриптов.
- Обеспечьте безопасность, сначала выполнив перенос принципалов (пользователей и групп пользователей).
  - Перенос в первую очередь пользователей и групп пользователей сохраняет модель безопасности в целевой системе и обеспечивает успех последующей миграции личного содержимого пользователей (такого как папки "Входящие", избранное и личные категории).

    > **Примечание**
    >
    > Важно сначала выполнить эту задачу, чтобы CUID пользователей и групп пользователей в целевой системе совпадали с CUID в исходной системе.

- Отключите вычисление зависимостей.
  - Вычисление зависимостей – это одна из наиболее ресурсоемких задач в процессе создания задания. При полной миграции репозитория переносятся все объекты, что делает это вычисление ненужным.

    > **Примечание**
    >
    > Эта функция полезна, только если нет уверенности в том, какие зависимые объекты необходимы.

- По возможности избегайте включения вычисления безопасности.
  - Вычисление безопасности – это вторая по ресурсоемкости задача в процессе создания задания. Разбейте перенос на два задания, если у вас много документов в разных каталогах, а безопасность задана только для каталогов. Первое задание должно содержать только объекты с включенной защитой, а второе – только документы с отключенной защитой. Это позволит вычислять безопасность только для каталогов, не вычисляя ее для всех документов.

> **Примечание**
>
> Безопасность объектов при этом сохранится, поскольку она наследуется из безопасности папок.

16.5 Шаги полного переноса системы

Полный перенос системы требует выполнения трех отдельных заданий переноса по очереди. Каждое задание переносит определенный тип содержимого. Дополнительные сведения о переносе нескольких объектов см. в статье базы знаний 1969259.

В следующей таблице перечислены типы содержимого и настройки параметров для каждого задания переноса.

Задание переноса	Тип содержимого	`exportDependencies`	`includeSecurity`
1	Все пользователи и группы пользователей	false	true
2	Все зависимые объекты	false	true
3	Все основные объекты	false	true

Используйте интерфейс командной строки для создания и выполнения каждого задания. Дополнительные сведения об интерфейсе командной строки см. в разделе Использование опции "Командная строка" [страница 654].

Общие параметры

Используйте следующие параметры для всех трех заданий переноса:

> **→ Напоминание**
>
> Убедитесь, что каждый параметр введен в отдельной строке.

```
action=promote
Source_CMS=<SourceSystem>
Source_userName=Administrator
Source_password=<AdministratorPassword>
LCM_CMS=<NameOfCentralSystem>
LCM_userName=Administrator
LCM_password=<AdministratorPassword>
Destination_CMS=<TargetSystem>
Destination_userName=Administrator
Destination_password=<AdministratorPassword>
exportDependencies=false
includeSecurity=true
stacktrace=true
consolelog=true
```

16.5.1 Перенос пользователей и групп пользователей (задание 1)

Для обеспечения идентичности моделей безопасности в исходной и целевой системах и совпадения CUID объектов пользователей и групп пользователей сначала перенесите пользователей и группы пользователей.

1. Создайте файл `usersandgroups.properties` с общими параметрами и добавьте в него следующие параметры, чтобы выбрать всех пользователей и все группы пользователей:

```
exportQuery1=SELECT TOP 10000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
(SI_KIND='User' OR SI_KIND='UserGroup') AND NOT (SI_ID in (11,12, 501, 1, 2,
3))
```

2. Для выполнения задания перейдите в каталог `<INSTALLDIR>\win64x64\scripts` и выполните следующую команду:

```
Lcm_cli.bat –lcmproperties=usersandgroups.properties
```

16.5.2 Перенос зависимых объектов (задание 2)

Зависимые объекты – это объекты, которые зависят от основных объектов в общей папке и папках избранного пользователей. Чтобы не устанавливать для параметра `includeDependencies` значение `true` для всех других заданий, переносите зависимые объекты во вторую очередь. К зависимым объектам относятся:

- Уровни доступа
- Приложения
- Бизнес-представления
- Календари
- Категории
- Соединения
- События
- Соединения OLAP
- Профили
- Проекты
- QaaWS
- Удаленные соединения
- Списки тиражирования
- Группы серверов
- Юниверсы

1. Создайте файл dependencies.properties с общими параметрами и добавьте в него следующие параметры, чтобы выбрать все зависимые объекты:

```
#total number of queries (if > 1)
exportQueriesTotal=12
```

```
#Projects, Universes, Connections, OLAP Connects: SI_ID=95
exportQuery1=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (95)")
#QaaWS: SI_CUID='AcTDjF_lm8dElXVCUgHI2Ps'
#-need to ensure Overrides are scanned at the source, promoted to the target
and set to active
exportQuery2=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID='AcTDjF_lm8dElXVCUgHI2Ps'")
#Events: SI_ID=21
exportQuery3=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS
WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (21)") and
si_specific_kind != 'MON.MonitoringEvent'
#Calendars: SI_ID=22
exportQuery4=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (22)")
#Categories: SI_ID=45
exportQuery5=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID IN (45)")
#Access Levels: SI_ID=57
exportQuery6=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (57)")
#Server Groups: SI_ID=17
exportQuery7=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (17)")
#Profiles: SI_ID=50
exportQuery8=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (50)")
#Applications: SI_ID=99
exportQuery9=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (99)")
#Remote Connections:  SI_CUID = 'AVwSekNrtFxGqJ6Jp2rLwrI'
exportQuery10=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS
WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID =
'AVwSekNrtFxGqJ6Jp2rLwrI'")
#Replication Lists:  SI_CUID = 'ASOr8wap3MJOgdWV5HLcZ1M'
exportQuery11=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID='ASOr8wap3MJOgdWV5HLcZ1M'")
#BusinessViews: SI_ID=98
exportQuery12=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (98)")
```

2. Для выполнения задания перейдите в каталог `<INSTALLDIR>\win64x64\scripts` и выполните следующую команду:

```
Lcm_cli.bat –lcmproperties=dependencies.properties
```

16.5.3 Перенос основных объектов (задание 3)

Основные объекты – это основные документы BI, находящиеся в общей папке и папках избранного пользователей. Если второе задание переноса (миграция всех зависимых объектов) уже было

выполнено, при переносе после этого основных объектов повторно создаются их отношения с зависимыми объектами.

1. Создайте файл `primaryobjects.properties` с общими параметрами и добавьте в него следующие параметры, чтобы выбрать всех пользователей и все группы пользователей:

```
#total number of queries (if > 1)
exportQueriesTotal=4
#All Public Folders
exportQuery1=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)")
#All user collaterals (Inbox, FavoriteFolder, PersonalCategory)
exportQuery2=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='Inbox')")
exportQuery3=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='FavoritesFolder')")
exportQuery4=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='PersonalCategory')")
```

   При повторном выполнении того же задания исключите задание LCM с помощью следующего запроса:

```
SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)") and SI_KIND not in
('LCMJob')
```

2. Для выполнения задания перейдите в каталог `<INSTALLDIR>\win64x64\scripts` и выполните следующую команду:

```
Lcm_cli.bat –lcmproperties=primaryobjects.properties
```

> **ⓘ Примечание**
>
> Если в общей папке и папках избранного пользователей содержится больше 50 000 объектов, может потребоваться разбить это последнее задание на несколько заданий.

> **ⓘ Примечание**
>
> Убедитесь, что на компьютерах, где выполняется команда интерфейса командной строки и запущен сервер заданий Диспетчера переноса объектов, выполняются требования по оценке размеров. Для получения дополнительной информации см. раздел «Оценка размеров».

16.5.4 После переноса

Диспетчер переноса объектов переносит только группы серверов, но не серверы. Чтобы убедиться, что отчеты с назначенными серверами будут продолжать работать, необходимо повторно создать и назначить серверы правильным группам серверов.

16.6 Использование опции "Командная строка"

Опция "Командная строка" средства Диспетчер переноса объектов позволяет переносить объекты из одного развертывания платформы BI в другое. Можно создать пакетный скрипт для нескольких заданий.

> → Совет
>
> Используйте опцию "Командная строка" для заданий, содержащих большое количество объектов.

Диспетчер переноса объектов поддерживает следующие виды переноса заданий из командной строки:

- Экспорт существующего шаблона задания для переноса в LCMBIAR с использованием шифрования пароля
- Экспорт существующего шаблона задания для переноса в LCMBIAR без шифрования пароля
- Экспорт одного/нескольких запросов платформы
- Перенос нескольких запросов платформы
- Перенос с существующим шаблоном задания
- Импорт и перенос существующего файла LCMBIAR
- Выполнение переноса между продуктивными системами

16.6.1 Запуск программы командной строки в 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 из каталога `C:\Program Files (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts\lcm_cli.bat`
     Команда: `lcm_cli.bat -lcmproperty <файл свойств>`

     > ⓘ Примечание
     >
     > При появлении подсказки введите действительный пароль.

Средство командной строки для управления переносом принимает файл `<свойств>` в качестве параметра. Файл `<свойств>` содержит требуемые параметры для взаимодействия с Диспетчером переноса объектов, касающегося выполняемых действий, выбора развертывания платформы BI для выполнения соединения, методов соединения, переносимых объектов и пр.

Файл должен иметь форму `<FILENAME>.properties`

Например: `<Myproperties.properties>`

16.6.2 Запуск 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_xi40/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>`
   - Выполните файл BAT из `<installdir_path>\sap_bobj\lcm_cli.sh`
     Команда: `lcm_cli.sh -lcmproperty <файл свойств>`

> ⓘ Примечание
>
> При появлении подсказки введите действительный пароль.

16.6.3 Параметры командной строки

Параметры командной строки для диспетчера переноса объектов организуются в соответствии с типом переноса. Существует три основных типа переноса:

- Перенос объектов из файла LCMBIAR на рабочий сервер CMS
- Перенос объектов с исходного рабочего сервера CMS на конечный рабочий сервер CMS
- Экспорт объектов с рабочего сервера CMS в файл LCMBIAR

Помимо параметров, относящихся к этим трем типам переноса, существуют также параметры общих команд, которые могут использоваться во всех сценариях переноса.

> → Напоминание
>
> Не заключайте параметры командной строки в кавычки.

> ⓘ 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>`.
> - Откат задания возможен только из Диспетчера переноса объектов. Командная строка не поддерживает откат заданий.

- При работе с большим количеством объектов рекомендуется увеличить максимальный размер динамической памяти Java, задав параметр `-Xmx=8g` в скрипте `LCMCLI`.

Связанные сведения

Перенос объектов из файла LCMBIAR на рабочий сервер CMS [страница 660]
Перенос с исходного рабочего сервера CMS на конечный рабочий сервер CMS [страница 667]
Перенос с рабочего сервера CMS в файл LCMBIAR [страница 663]
Список всех параметров командной строки [страница 670]

16.6.3.1 Параметры командной строки для различных сценариев переноса

Параметры командной строки представлены в порядке, рекомендованном для каждого сценария переноса. В данной таблице указаны все доступные параметры и их статус для каждого сценария переноса (обязательный или необязательный). Каждый обязательный параметр описывается в применении к соответствующему сценарию переноса. Необязательные параметры описываются в разделе «Список всех параметров командной строки». Сведения о всех параметрах для тех или иных сценариев и о доступных необязательных параметрах см. по ссылкам ниже.

Группа параметров	Параметр	Из LCMBIAR на рабочий сервер	С рабочего сервера в LCMBIAR	С сервера на сервер	Откат
Файл свойств	`lcmproperty`	Необязательный	Рекомендуется	Рекомендуется	Рекомендуется
Тип действия	`action`	Обязательный action=promote	Обязательный action=export	Обязательный action=promote	Обязательный action=rollback
Узел LCM	`LCM_CMS`	Обязательный			
	`LCM_userName`	Обязательный			
	`LCM_Password`	Обязательный Если значение здесь не указано, его необходимо будет задавать на консоли			
	`LCM_authentication`	Необязательный По умолчанию `secEnterprise`			

Группа параметров	Параметр	Из LCMBIAR на рабочий сервер	С рабочего сервера в LCMBIAR	С сервера на сервер	Откат
	`LCM_SystemID`	Обязательный только для аутентификации SAP			
	`LCM_ClientID`	Обязательный только для аутентификации SAP			
Источник (рабочий сервер или LCMBIAR)	`importLocation`	Обязательный	Неприменимо	Неприменимо	Неприменимо
	`lcmbiarpassword`	Обязательный (может быть пустым)	Неприменимо	Неприменимо	Неприменимо
	`Source_CMS`	Неприменимо	Обязательный	Обязательный	Неприменимо
	`Source_UserName`	Неприменимо	Обязательный	Обязательный	Неприменимо
	`Source_password`	Неприменимо	Обязательный Если значение здесь не указано, его необходимо будет задавать на консоли	Обязательный Если значение здесь не указано, его необходимо будет задавать на консоли	Неприменимо
	`Source_authentication`	Неприменимо	Необязательный По умолчанию `secEnterprise`	Необязательный По умолчанию `secEnterprise`	Неприменимо
	`Source_systemID`	Неприменимо	Обязательный только для аутентификации SAP	Обязательный только для аутентификации SAP	Неприменимо
	`Source_clientID`	Неприменимо	Обязательный только для аутентификации SAP	Обязательный только для аутентификации SAP	Неприменимо
Место назначения (рабочий сервер или LCMBIAR)	`Destination_CMS`	Обязательный	Неприменимо	Обязательный	Неприменимо
	`Destination_username`	Обязательный	Неприменимо	Обязательный	Неприменимо
	`Destination_password`	Обязательный	Неприменимо	Обязательный	Неприменимо

Группа параметров	Параметр	Из LCMBIAR на рабочий сервер	С рабочего сервера в LCMBIAR	С сервера на сервер	Откат
	`Destination_authentication`	Необязательный По умолчанию `secEnterprise`	Неприменимо	Необязательный По умолчанию `secEnterprise`	Неприменимо
	`Destination_systemID`	Обязательный только для аутентификации SAP	Неприменимо	Обязательный только для аутентификации SAP	Неприменимо
	`Destination_clientID`	Обязательный только для аутентификации SAP	Неприменимо	Обязательный только для аутентификации SAP	Неприменимо
	`ExportLocation`	Неприменимо	Обязательный	Неприменимо	Неприменимо
	`lcmbiarpassword`	Неприменимо	Обязательный (может быть пустым)	Неприменимо	Неприменимо
Связанные с заданием	`JOB_CUID`	Неприменимо	Необязательный	Необязательный	Обязательный
	`Override`	Необязательный	Неприменимо	Неприменимо	Неприменимо
	`forceOverride` Доступно в SP4	Необязательный	Неприменимо	Неприменимо	Неприменимо
	`Timeout` Доступно в SP4	Необязательный	Неприменимо	Необязательный	Неприменимо
Связанные с экспортом	`ExportDependencies`	Неприменимо	Необязательный По умолчанию `False`	Необязательный По умолчанию `False`	Неприменимо
	`ExportQuery`	Неприменимо	Обязательный	Обязательный	Неприменимо
	`ExportQueriesTotal`	Неприменимо	Необязательный: Используется при наличии более одного запроса экспорта	Необязательный: Используется при наличии более одного запроса экспорта	Неприменимо
	`BatchJobQuery`	Неприменимо	Необязательный: Используется вместе с параметром Exportquery	Необязательный: Используется вместе с параметром Exportquery	Неприменимо

Группа параметров	Параметр	Из LCMBIAR на рабочий сервер	С рабочего сервера в LCMBIAR	С сервера на сервер	Откат
	`LimitQueryBatchSize`	Неприменимо	Необязательный	Необязательный	Неприменимо
Связанные с журналом	`Consolelog`	Необязательный По умолчанию `False`	Необязательный По умолчанию `False`	Необязательный По умолчанию `False`	Неприменимо
	`ResultFileName`	Необязательный	Необязательный	Необязательный	Неприменимо
	`LogFileName` Доступно в SP4	Необязательный	Необязательный	Необязательный	Неприменимо
Выбор объектов	`Selected_CUIDS`	Необязательный	Неприменимо	Неприменимо	Неприменимо
	`selectUser` Доступно в SP4	Неприменимо	Необязательный По умолчанию `All`	Необязательный По умолчанию `All`	Неприменимо
	`selectGroup` Доступно в SP4	Неприменимо	Необязательный По умолчанию `All`	Необязательный По умолчанию `All`	Неприменимо
Безопасность	`IncludeApplicationSecurity`	Необязательный По умолчанию `False`	Необязательный По умолчанию `False`	Необязательный По умолчанию `False`	Неприменимо
	`IncludeSecurity`	Необязательный По умолчанию `False`	Необязательный По умолчанию `False`	Необязательный По умолчанию `False`	Неприменимо
	`IncludeTopLevelSecurity`	Необязательный По умолчанию `False`	Необязательный По умолчанию `False`	Необязательный По умолчанию `False`	Неприменимо
Комментарии	`IncludeComments`	Необязательный По умолчанию `False`	Необязательный По умолчанию `False`	Необязательный По умолчанию `False`	Неприменимо
Задания объединения	`IncludeFederationJobsRelationship`	Необязательный По умолчанию `True`	Неприменимо	Необязательный По умолчанию `True`	Неприменимо

Связанные сведения

Перенос объектов из файла LCMBIAR на рабочий сервер CMS [страница 660]
Перенос с рабочего сервера CMS в файл LCMBIAR [страница 663]
Перенос с исходного рабочего сервера CMS на конечный рабочий сервер CMS [страница 667]
Список всех параметров командной строки [страница 670]

16.6.3.2 Перенос объектов из файла LCMBIAR на рабочий сервер CMS

При переносе объектов из файла LCMBIAR на рабочий сервер CMS в командной строке указывается файл свойств, в котором задается порядок переноса:

- Расположение для импорта и тип действия переноса.
- Учетные данные для входа на сервер CMS, на котором размещен диспетчер переноса объектов (ранее называвшийся инструментом управления жизненным циклом, LCM).
- Учетные данные для входа на целевой сервер CMS.
- Другие параметры, необходимые для успешного переноса на CMS, например пароль LCMBIAR или настройки переопределения, позволяющие при необходимости перезаписывать существующие объекты.

Можно включить другие дополнительные параметры, в зависимости от конкретных требований переноса. Такие дополнительные параметры описываются в разделе Список всех параметров командной строки [страница 670].

В следующем примере показан перенос файла LCMBIAR на рабочий сервер CMS без указания файла свойств в командной строке:

```
Go to
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\win64_x64\scripts>
Type
lcm_cli.bat -action promote -LCM_CMS myCMS.mydomain.sap:6400 -LCM_userName
adminLCM -LCM_password my_adminpassword1 -
Destination_CMS myCMS.mydomain.sap:6400 -Destination_userName adminLCM
-Destination_password my_adminpassword1 -
importLocation "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\Samples\webi\WebISamples.lcmbiar" -
lcmbiarpassword
```

В следующем примере показан перенос файла LCMBIAR на рабочий сервер CMS с указанием файла свойств в командной строке:

```
Go to
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\win64_x64\scripts>
Type
lcm_cli.bat -lcmproperty C:\LCMTEST\MyPropertyFile.properties
#
LCM command line property file
#
action=promote
```

```
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
#
importLocation=C:\Backup\CR.lcmbiar
lcmbiarpassword=validlcmbiarpassword
#
Destination_CMS=myCMS.mydomain.sap:6400
Destination_userName=adminLCM
Destination_password=my_adminpassword1
#
```

В следующей таблице перечислены обязательные параметры, которые следует включить в файл свойств для переноса из файла LCMBIAR на рабочий сервер CMS:

Группа параметров	Параметр	Описание
Тип действия	`action`	Операция, выполняемая в CLI. Значение: export Пример: `action=export`
Узел LCM	`LCM_CMS`	CMS для диспетчера переноса объектов. Значение: текст произвольной формы Пример: `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Имя пользователя учетной записи, используемое для подключения к CMS диспетчера переноса объектов. Значение: текст произвольной формы Пример: `LCM_userName=adminLCM`
	`LCM_password`	Пароль учетной записи пользователя. Значение: текст произвольной формы Пример: `LCM_password=my_adminpassword1`

Группа параметров	Параметр	Описание
Источник:файл LCMBIAR	`importLocation`	Расположение файла LCMBIAR, в котором содержатся объекты, подлежащие переносу. Значение: текст произвольной формы. Должен иметь расширение `<.lcmbiar>` Пример: `importLocation=C:\Backup\New.lcmbiar`
	`lcmbiarpassword`	Включает шифрование и дешифровку файлов BIAR с использованием пароля. Значение: текст произвольной формы Пример: `lcmbiar=validlcmbiarpassword`
Место назначения:рабочий сервер CMS	`Destination_CMS`	Сервер CMS, к которому должен подключаться инструмент. Значение: допустимое имя CMS Пример: `Destination_CMS=myCMS.mydomain.sap:6400`
	`Destination_username`	Учетная запись пользователя, которую следует использовать для подключения к CMS платформы BI. Значение: допустимое имя пользователя Пример: `Destination_username=adminLCM`
	`Destination_password`	Пароль, связанный с учетной записью пользователя. Значение: допустимый пароль Пример: `Destination_password=my_adminpassword1`

Связанные сведения

Перенос с рабочего сервера CMS в файл LCMBIAR [страница 663]
Перенос с исходного рабочего сервера CMS на конечный рабочий сервер CMS [страница 667]
Список всех параметров командной строки [страница 670]

16.6.3.3 Перенос с рабочего сервера CMS в файл LCMBIAR

При переносе объектов с рабочего сервера CMS в файл LCMBIAR в командной строке указывается файл свойств, в котором задается порядок переноса:

- Тип действия переноса: export
- Учетные данные для входа на сервер CMS, на котором размещен диспетчер переноса объектов (ранее называвшийся инструментом управления жизненным циклом, LCM).
- Учетные данные для входа в исходный сервер CMS.
- Каталог назначения для файла LCMBIAR.
- Другие параметры, необходимые для успешного переноса из CMS, например пароль LCMBIAR или настройки безопасности.

Можно включить и другие, необязательные параметры, в зависимости от конкретных потребностей переноса. Такие дополнительные параметры описываются в разделе Список всех параметров командной строки [страница 670].

Далее приводится пример типичного файла свойств для переноса с рабочего сервера CMS в файл LCMBIAR:

```
Go to
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\win64_x64\scripts>
Type
lcm_cli.bat -lcmproperty C:\LCMTEST\MyPropertyFile.properties
#
#action=export
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
#
Source_CMS=myCMS.mydomain.sap:6400
Source_userName=adminLCM
Source_password=my_adminpassword1
#
exportLocation=E:\LCMTEST\
lcmbiarpassword=
#
#Queries
#
exportQuery1=SELECT TOP 10000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM
CI_INFOOBJECTS, CI_APPOBJECTS, CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID in (23)")
#
#When applicable...
```

```
#
exportDependencies=true
includeSecurity=true
#
#Options
#
consolelog=true
```

В следующей таблице перечислены обязательные параметры, которые следует включить в файл свойств для переноса из файла LCMBIAR на рабочий сервер CMS:

Группа параметров	Параметр	Описание
Тип действия	`action`	Операция, выполняемая в CLI. Значение: export Пример: `action=export`
Узел LCM	`LCM_CMS`	CMS для диспетчера переноса объектов. Значение: текст произвольной формы Пример: `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Имя пользователя учетной записи, используемое для подключения к CMS диспетчера переноса объектов. Значение: текст произвольной формы Пример: `LCM_userName=adminLCM`
	`LCM_password`	Пароль учетной записи пользователя. Значение: текст произвольной формы Пример: `LCM_password=my_adminpassword1`

Группа параметров	Параметр	Описание
Источник:рабочий сервер CMS	`Source_CMS`	Сервер CMS, к которому должен подключаться диспетчер переноса объектов. Значение: текст произвольной формы Пример: `Source_CMS=myCMS.mydomain.sap:6400`
	`Source_userName`	Учетная запись пользователя, которую должен использовать диспетчер переноса объектов для подключения к CMS платформы BI. Значение: текст произвольной формы Пример: `Source_username=adminLCM`
	`Source_password`	Пароль учетной записи пользователя. Значение: текст произвольной формы Пример: `Source_password=my_adminpassword1`
Место назначения:файл LCMBIAR	`exportLocation`	Указывает место для размещения файла LCMBIAR после экспорта и упаковки объектов. Значение: текст произвольной формы. Должен иметь расширение `<.lcmbiar>` Пример: `exportLocation=C:\Backup\New.lcmbiar`

Группа параметров	Параметр	Описание
	`lcmbiarpassword`	Включает шифрование и дешифровку файлов BIAR с использованием пароля. Значение: текст произвольной формы Пример: `lcmbiarpassword=validlcmbiarpassword`
Связанные с экспортом	`exportQuery`	Запрос к исходному серверу CMS для получения объектов, которые требуется экспортировать в файл LCMBIAR. Значение: текст произвольной формы. Используйте формат языка запросов CMS. Пример: `SELECT TOP 3000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE SI_NAME='Xtreme Employees' AND SI_KIND='Webi'` **Примечание** В одном файле свойств может содержаться любое количество запросов, однако они должны именоваться следующим образом: exportQuery1, exportQuery2 и т. д.

Связанные сведения

Перенос объектов из файла LCMBIAR на рабочий сервер CMS [страница 660]
Перенос с исходного рабочего сервера CMS на конечный рабочий сервер CMS [страница 667]
Список всех параметров командной строки [страница 670]

16.6.3.4 Перенос с исходного рабочего сервера CMS на конечный рабочий сервер CMS

При переносе объектов с исходного на конечный рабочий сервер CMS в командной строке указывается файл свойств, в котором задается порядок переноса:

- Тип действия переноса: promote
- Учетные данные для входа на сервер CMS, на котором размещен диспетчер переноса объектов (ранее называвшийся инструментом управления жизненным циклом, LCM).
- Учетные данные для входа в исходный сервер CMS.
- Учетные данные для входа в конечный сервер CMS.
- Другие параметры, необходимые для успешного переноса из CMS, например зависимости или настройки безопасности.

Можно включить и другие, необязательные параметры, в зависимости от конкретных потребностей переноса. Такие дополнительные параметры описываются в разделе Список всех параметров командной строки [страница 670].

Далее приводится пример типичного файла свойств для переноса с исходного сервера CMS на конечный сервер CMS:

```
#
action=promote
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
LCM_authentication=secEnterprise
#
Source_CMS=myCMS1:myCMS2
Source_userName=adminLCM
Source_password=my_adminpassword1
Source_authentication=secEnterprise
#
Destination_CMS=myCMS1:myCMS2
Destination_userName=adminLCM
Destination_password=my_adminpassword1
Destination_authentication=secEnterprise
#
exportQuery1select*from CI_INFOOBJECTS where SI_NAME='Charting Samples' and
SI_KIND='Webi'
#
includeSecurity=false
#
exportDependencies=false
#
```

В следующей таблице перечислены обязательные параметры, которые следует включить в файл свойств для переноса с исходного сервера CMS на конечный сервер CMS:

Группа параметров	Параметр	Описание
Тип действия	`action`	Операция, выполняемая командной строкой. Значение: promote Пример: `action=promote`
Узел LCM	`LCM_CMS`	CMS для диспетчера переноса объектов. Значение: текст произвольной формы Пример: `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Имя пользователя учетной записи, используемое для подключения к CMS диспетчера переноса объектов. Значение: текст произвольной формы Пример: `LCM_userName=adminLCM`
	`LCM_password`	Пароль учетной записи пользователя. Значение: текст произвольной формы Пример: `LCM_password=my_adminpassword1`
Источник: рабочий сервер CMS	`source_CMS`	Сервер CMS, к которому должен подключаться диспетчер переноса объектов. Значение: текст произвольной формы Пример: `Source_CMS=myCMS.mydomain.sap:6400`

Группа параметров	Параметр	Описание
	`Source_username`	Учетная запись пользователя, которую должен использовать диспетчер переноса объектов для подключения к CMS платформы BI. Значение: текст произвольной формы Пример: `Source_username=adminLCM`
	`Source_password`	Пароль учетной записи пользователя. Значение: текст произвольной формы Пример: `Source_password=my_adminpassword1`
Место назначения: рабочий сервер CMS	`Destination_CMS`	Сервер CMS, к которому должен подключаться инструмент. Значение: текст произвольной формы Пример: `Destination_CMS=myCMS1:myCMS2`
	`Destination_username`	Учетная запись пользователя, которую следует использовать для подключения к CMS платформы BI. Значение: текст произвольной формы Пример: `Destination_username=adminLCM`
	`Destination_password`	Пароль, связанный с учетной записью пользователя. Значение: текст произвольной формы Пример: `Destination_password=my_adminpassword1`

Группа параметров	Параметр	Описание
Связанные с экспортом	`exportQuery`	Запросы, выполняемые инструментом LCM для получения объектов, которые требуется экспортировать на конечный сервер CMS. Значение: текст произвольной формы. Используйте формат языка запросов CMS. Пример: `SELECT TOP 3000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE SI_NAME='Xtreme Employees' AND SI_KIND='Webi'` **Примечание** В одном файле свойств может содержаться любое количество запросов, однако они должны именоваться следующим образом: exportQuery1, exportQuery2 и т. д.

Связанные сведения

Перенос объектов из файла LCMBIAR на рабочий сервер CMS [страница 660]
Перенос с рабочего сервера CMS в файл LCMBIAR [страница 663]
Список всех параметров командной строки [страница 670]

16.6.3.5 Список всех параметров командной строки

В следующей таблице описываются все параметры командной строки.

Примечание

В командной строке параметры вводятся с использованием следующего синтаксиса: `-<parameterName><space><parameterValue>`. В файле свойств параметры задаются с использованием следующего синтаксиса:`<parameterName>=<parameterValue>`.

Группа параметров	Параметр	Описание
Файл свойств	`lcmproperty`	Указывает значения, необходимые для выполнения команды, которые сохранены в файле. Значение: полный путь к расположению, в котором сохранен файл свойств Пример: `-lcmproperty C:\MyPropertyFile.properties`
Тип действия	`action`	Операция, выполняемая в CLI. Значение: promote или export Пример: `action=promote`
Узел LCM	`LCM_CMS`	CMS для диспетчера переноса объектов. Значение: текст произвольной формы Пример: `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Имя пользователя учетной записи, используемое для подключения к CMS диспетчера переноса объектов. Значение: текст произвольной формы Пример: `LCM_userName=adminLCM`
	`LCM_Password`	Пароль учетной записи пользователя. Если он здесь не указан, его необходимо будет задавать на консоли. Значение: текст произвольной формы Пример: `LCM_password=my_adminpassword1`
	`LCM_authentication`	Определяет используемый тип аутентификации. Значение: secEnterprise, secWinAD, secLDAP, secSAPR3. Если значение не указано, используется `secEnterprise`. Пример: `LCM_authentication=secEnterprise`
	`LCM_systemID` **Примечание** Обязательный параметр для аутентификации SAP.	Требуется только для аутентификации SAP. Значение: идентификатор системы Пример: `LCM_systemID=systemID`

Группа параметров	Параметр	Описание
	`LCM_clientID` **Примечание** Обязательный параметр для аутентификации SAP.	Требуется только для аутентификации SAP. Значение: идентификатор клиента Пример: `LCM_clientID=clientID`
Источник:файл LCMBIAR	`importLocation`	Расположение файла LCMBIAR, в котором содержатся объекты, подлежащие переносу. Значение: текст произвольной формы. Должен иметь расширение `<.lcmbiar>` Пример: `importLocation=C:\Backup\New.lcmbiar`
	`lcmbiarpassword`	Включает шифрование и дешифровку файлов BIAR с использованием пароля. Значение: текст произвольной формы Пример: `lcmbiar=validlcmbiarpassword`
Источник:рабочий сервер CMS	`Source_CMS`	Сервер CMS, к которому должен подключаться диспетчер переноса объектов. Значение: текст произвольной формы Пример: `Source_CMS=myCMS.mydomain.sap:6400`
	`Source_UserName`	Учетная запись пользователя, которую должен использовать диспетчер переноса объектов для подключения к CMS платформы BI. Значение: текст произвольной формы Пример: `Source_username=adminLCM`
	`Source_password`	Пароль учетной записи пользователя. Значение: текст произвольной формы Пример: `Source_password=my_adminpassword1`
	`Source_authentication`	Определяет используемый тип аутентификации. Значение: secEnterprise, secWinAD, secLDAP, secSAPR3. Если значение не указано, используется `secEnterprise`. Пример: `Source_authentication=secEnterprise`

Группа параметров	Параметр	Описание
	`Source_systemID` **Примечание** Обязательный параметр для аутентификации SAP.	Требуется только для аутентификации SAP. Значение: идентификатор системы Пример: `Source_systemID=systemID`
	`Source_clientID` **Примечание** Обязательный параметр для аутентификации SAP.	Требуется только для аутентификации SAP. Значение: идентификатор системы Пример: `Source_clientID=clientID`
Место назначения:файл LCMBIAR	`exportLocation`	Указывает место для размещения файла LCMBIAR после экспорта и упаковки объектов. Значение: текст произвольной формы. Должен иметь расширение `<.lcmbiar>` Пример: `exportLocation=C:\Backup\New.lcmbiar`
	`lcmbiarpassword`	Включает шифрование и дешифровку файлов BIAR с использованием пароля. Значение: текст произвольной формы Пример: `lcmbiarpassword=validlcmbiarpassword`
Место назначения:рабочий сервер CMS	`Destination_CMS`	Сервер CMS, к которому должен подключаться инструмент. Значение: допустимое имя CMS Пример: `Destination_CMS=myCMS.mydomain.sap:6400`
	`Destination_username`	Учетная запись пользователя, которую следует использовать для подключения к CMS платформы BI. Значение: допустимое имя пользователя Пример: `Destination_username=adminLCM`
	`Destination_password`	Пароль, связанный с учетной записью пользователя. Значение: допустимый пароль Пример: `Destination_password=my_adminpassword1`

Группа параметров	Параметр	Описание
	`Destination_authentication`	Определяет используемый тип аутентификации. Значение: secEnterprise, secWinAD, secLDAP, secSAPR3. Если значение не указано, используется `secEnterprise`. Пример: `Destination_authentication=secEnterprise`
	`Destination_systemID` **Примечание** Обязательный параметр для аутентификации SAP.	Требуется только для аутентификации SAP. Значение: идентификатор системы Пример: `Destination_systemID=systemID`
	`Destination_clientID` **Примечание** Обязательный параметр для аутентификации SAP.	Требуется только для аутентификации SAP. Значение: идентификатор клиента Пример: `Destination_clientID=clientID`
Связанные с заданием	`JOB_CUID`	Задает экспорт всех объектов задания в файл LCMBIAR. Значение: CUID сохраненного задания диспетчера.
	`Override`	Используется для выборочного переноса объектов из файла LCMBIAR. В случае значения `true`: позволяет пользователю переопределить существующее задание. В случае значения `false`: позволяет пользователю создать новое задание с именем `<JOB_NAME>_<TIME_STAMP>` . Значение: true или false Пример: `Override=true`
	`forceOverride` Доступно в SP4	Используется для переопределения задания с тем же именем, но другим CUID. Значение: true или false Пример: `forceOverride=true`

Группа параметров	Параметр	Описание
	`Timeout` Доступно в SP4	Задает время ожидания для действия переноса. Значение: время в секундах Пример: `timeout=30`
Связанные с экспортом	`ExportDependencies`	Указывает зависимости объекта, собираемые инструментом для экспорта. Применяется только совместно с флагом `Source_CMS`. Значение: true или false. Если значение не указано, по умолчанию принимается `false`. Пример: `ExportDependencies=false`
	`ExportQuery`	Запросы, выполняемые инструментом LCM для получения объектов, которые требуется экспортировать на конечный сервер CMS. Значение: текст произвольной формы. Используйте формат языка запроса CMS. Пример: `SELECT TOP 3000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE SI_NAME='Xtreme Employees' AND SI_KIND='Webi'` **Примечание** В одном файле свойств может содержаться любое количество запросов, однако они должны именоваться следующим образом: exportQuery1, exportQuery2 и т. д.

	`ExportQueriesTotal`	Используется для указания числа выполняемых запросов экспорта. Если имеется x запросов экспорта и требуется выполнить все эти запросы, данному параметру следует присвоить значение x.
		Значение: целое положительное число. Если значение не указано, по умолчанию принимается 1.
		Пример: `ExportQuery1=<your sql statement>`
		`ExportQuery2=<your sql statement>`
		`ExportQueriesTotal=2`

Группа параметров	Параметр	Описание
	`BatchJobQuery`	Используется совместно с параметром `ExportQuery`. Создает и запускает задание для каждой строки, возвращаемой запросом задания. В запросах экспорта для задания могут использоваться заполнители для обозначения свойств, инициируемых в запросе задания. Заполнители вводятся в формате $b:PPTY$ (без учета регистра символов в имени свойства). Допустимые значения <PPTY>: - "cuid" - "name" - "id" Если заполнитель не распознается или инициируется запросом задания, возвращается ошибка. Значение: текст произвольной формы Пример: `batchJobQuery=SELECT si_cuid,si_name FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)") AND SI_KIND='Folder' AND SI_NAME LIKE '%sample%' and SI_PARENTID=0` `exportQuery1= SELECT TOP 10000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'" ,"SI_CUID='$b:CUID$'")`
	`LimitQueryBatchSize`	Ограничивает число возвращаемых объектов значением, по умолчанию равным 1000. Если параметр имеет значение false, возвращаются все запрошенные объекты. **Примечание** Можно в явном виде задать новый лимит числа объектов, возвращаемых запросом, указав `select TOP <number>` Значение: true или false. Если значение не указано, по умолчанию принимается true. Пример: `LimitQueryBatchSize=true`

Группа параметров	Параметр	Описание
Связанные с журналом	`consolelog`	Используется для вывода полного журнала команды, выполненной пользователем, в журнале команд. Значение: true или false. Если значение не указано, по умолчанию принимается `false`. Пример: `consolelog=true`
	`ResultFileName`	Имя файла локальной файловой системы в случае использования параметра `consolelog`. Значение: путь к файлу результатов задания Пример: `ResultFileName=C:\Logs\ResultFile.txt`
	`LogFileName` Доступно в SP4	Позволяет пользователю указать фиксированный путь к файлу журнала. Значение: путь к файлу журнала Пример: `LogFileName=C:\Logs\LogFile.log`
Выбор объектов	`Selected_CUIDS`	Позволяет пользователю выборочно переносить объекты (отчеты, пользователей, юниверсы и т. д.) вместе с их зависимостями из файла LCMBIAR, а не переносить весь файл полностью. Значение: идентификаторы CUID выборочно переносимых объектов в файле LCMBIAR
	`selectUser` Доступно в SP4	Задает фильтрацию пользователей на основе данных сторонней аутентификации (LDAP, SAPR3, WindowsAD...). Значение: all, none, excludeTP, onlyTP. Если значение не указано, по умолчанию принимается `all`. Пример: `selectUser=excludeTP`
	`selectGroup` Доступно в SP4	Задает фильтрацию групп пользователей на основе данных сторонней аутентификации (LDAP, SAPR3, WindowsAD...). Значение: all, none, excludeTP, onlyTP. Если значение не указано, по умолчанию принимается `all`. Пример: `selectGroup=onlyTP`

Группа параметров	Параметр	Описание
Безопасность	`IncludeApplicationSecurity`	Задает экспорт или импорт параметров безопасности, связанных с выбранными приложениями. Значение: true или false. Если значение не указано, по умолчанию принимается `false`. Пример: `IncludeApplicationSecurity=true`
	`IncludeSecurity`	Задает экспорт или импорт параметров безопасности, связанных с выбранными объектами и пользователями. Если используются уровни доступа, они также будут экспортированы/импортированы. Значение: true или false. Если значение не указано, по умолчанию принимается `false`. Пример: `IncludeSecurity=true`
Комментарии	`IncludeComments`	Задает экспорт или импорт комментариев, связанных с выбранными объектами. Значение: true или false. Если значение не указано, по умолчанию принимается `false`. Пример: `IncludeComments=true`
Задания объединения	`IncludeFederationJobsRelationship`	Задает сохранение отношений заданий объединения (списков тиражирования и удаленных соединений). Если установлено значение false, тиражированные объекты становятся обычными объектами, а флаг объединения будет снят. Это может быть полезно, когда тиражированный объект является единственным доступным объектом, а исходный объект больше недоступен. Значение: true или false. Если значение не указано, по умолчанию принимается `true`. Пример: `IncludeFederationJobsRelationship=false`

16.6.3.6 Откат

С помощью *Диспетчера переноса объектов* можно откатить перенесенное задание в целевой системе.

Если задание было перенесено с помощью *Диспетчера переноса объектов* , например, для обновления BI 4.2 SP07 до BI 4.3, а теперь требуется откатить это изменение, можно использовать параметры командной строки, определенные в Параметры командной строки для различных сценариев переноса [страница 656] и выполнить операцию отката.

При выполнении операции отката необходимо предоставить файл свойств, который определяет порядок переноса следующим образом:

- Тип действия переноса: rollback
- Учетные данные для входа на сервер CMS, на котором размещен диспетчер переноса объектов (ранее называвшийся инструментом управления жизненным циклом, LCM).
- Учетные данные для входа в исходный сервер CMS.
- Учетные данные для входа на целевой сервер CMS.
- Другие параметры, необходимые для успешного переноса из CMS, например зависимости или настройки безопасности.

Можно включить другие дополнительные параметры, в зависимости от конкретных требований переноса. Такие дополнительные параметры описываются в разделе Список всех параметров командной строки [страница 670].

Для выполнения операции отката можно ориентироваться на приведенный ниже образец файла свойств:

```
#
action=rollback
job_cuid=AWWxyVk5fkFKjtQnRAygAYg
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
LCM_authentication=secEnterprise
```

> **Примечание**
>
> Идентификатор `job_cuid` перенесенного задания можно найти в разделе *Домашняя страница CMC* > *Диспетчер переноса объектов* > *Свойства*.

В следующей таблице перечислены обязательные параметры, которые следует включить в файл свойств для переноса из файла LCMBIAR на рабочий сервер CMS:

Группа параметров	Параметр	Описание
Тип действия	`action`	Операция, выполняемая в CLI. Значение: rollback Пример: `action=rollback`
Связанное задание	`job_cuid`	Задает экспорт всех объектов задания в файл LCMBIAR. Значение: CUID сохраненного задания диспетчера. Пример: `job_cuid=AWWxyVk5fkFKjtQnRAygAYg`

Группа параметров	Параметр	Описание
Узел LCM	`LCM_CMS`	CMS для диспетчера переноса объектов. Значение: текст произвольной формы Пример: `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Имя пользователя учетной записи, используемое для подключения к CMS диспетчера переноса объектов. Значение: текст произвольной формы Пример: `LCM_userName=adminLCM`
	`LCM_password`	Пароль учетной записи пользователя. Значение: текст произвольной формы Пример: `LCM_password=my_adminpassword1`
	`LCM_authentication`	Тип аутентификации для учетной записи пользователя Значение: Тип аутентификации Пример: `secEnterprise`

16.6.4 Образец файла свойств

Ниже приведен образец файла `свойств`:

Пример

```
importLocation=C:/Backup/CR.lcmbiar
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>

lcmbiarpassword=<password>
```

> **Примечание**
>
> Если в файле `свойств` отсутствует личная информация, в интерфейсе командной строки LCM в консоли будет выдана подсказка ввести такую информацию.

16.7 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+.

Информационные объекты InfoObject платформы BI могут использовать содержимое SAP Business Warehouse в качестве источника данных. Интеграция CTS+ с Диспетчером переноса объектов обеспечивает обработку репозитория платформы BI аналогично репозиторию SAP Business Warehouse (BW) посредством использования запросов транспорта CTS для переноса заданий. CTS+ обеспечивает возможность переноса 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 об Организаторе изменений и переносов см. Организатор изменений и переносов - Обзор (BC-CTS)

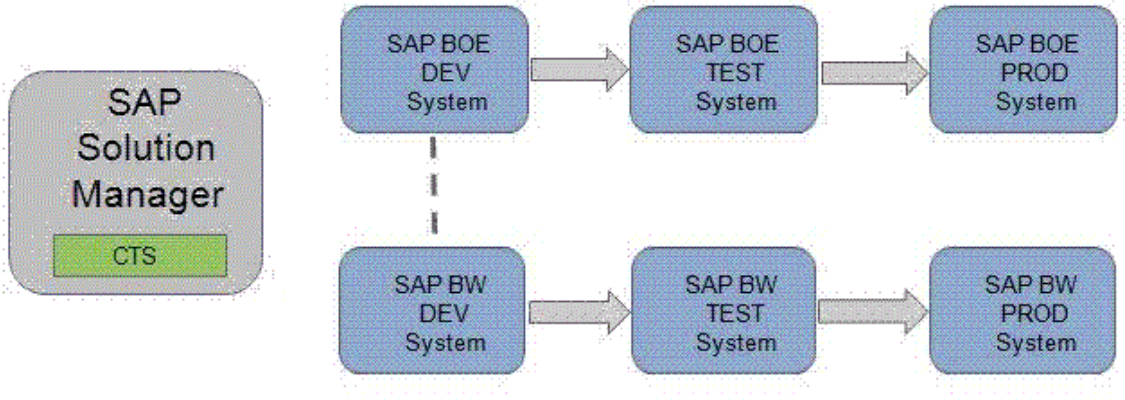
Для получения дополнительных сведений о CTS+ и переносах, не относящихся к ABAP см. Перенос объектов, не относящихся к ABAP, в Организаторе изменений и переносов

16.7.1 Предварительные требования

Пункты, перечисленные ниже, являются предварительными условиями для передачи содержимого Business Intelligence из одной системы в другую с помощью CTS+:

1. Установлена платформа BI 4.0 (или выше).
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 переноса см. раздел Настройка домена переноса.
3. Подключаемый модуль CTS для SAP Solution Manager установлен (модуль CTS взят из SL Toolset 1.0 SP02. Рекомендуется использовать последнюю доступную версию подключаемого модуля CTS).
   Для получения дополнительных сведений об установке необходимого подключаемого модуля CTS см. SAP-ноту 1533059.
4. Установлены системы *SAP Business Warehouse 7.0* (SPS 24 или более новая версия).
   Дополнительные сведения см. в SAP-ноте 1369301.
5. Настроен ландшафт транспорта SAP Business Warehouse (SAP BW) в системе настройки и транспортировки (CTS).
6. На компьютере с CTS Deploy Web Service реализованы SAP-ноты 1692417 и 1860594.

16.7.2 Настройка платформы BI и интеграции с 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 подробных сведений о системе управления переносами см. Система управления переносами (BC-CTS-TMS)

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 подробных сведений см. Система управления переносами (BC-CTS-TMS)

При помощи запросов на перенос CTS Диспетчер переноса объектов платформы BI можно интегрировать с CTS+ и SAP BW.

> ⓘ Примечание
>
> Для активации интеграции платформы BI 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 Диспетчера переноса объектов.
3. Выполните настройку системы импорта платформы Business Intelligence в SAP Solution Manager

Связанные сведения

Активация веб-службы экспорта в CTS [страница 683]
Настройка параметров CTS+ в Диспетчере переноса объектов [страница 684]
Настройка платформы BI и интеграции с CTS+ [страница 682]

16.7.2.1 Активация веб-службы экспорта в CTS

Для настройки 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 SAP Solution Manager. После выполнения входа в веб-браузере будет открыта консоль управления SOA.

   Для получения дополнительной информации о SOA Management и настройке конечной точки службы с помощью SAP Solution Manager 7.0 см. Настройка поставщика службы. Для SAP Solution Manager 7.1 см. Настройка поставщика службы.
2. На вкладке *Коммуникация между приложением и сценарием* нажмите *Настройка отдельной 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.

16.7.2.2 Настройка параметров CTS+ в Диспетчере переноса объектов

В следующем разделе описываются шаги по настройке, которые должны быть выполнены в приложении CMC для настройки использования CTS+ совместно с Диспетчером переноса объектов.

1. На странице *Задания переноса* 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:
   - *Хост BW SID*: укажите идентификатор системы (SID) компьютера SAP BW/ABAP, выполняющего функцию хоста.
   - *Имя хоста*: укажите IP-адрес компьютера, выполняющего функцию хоста.
   - *Номер системы*: введите номер системы хоста.
   - *Клиент*: указываются 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 *OK*, 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 переноса* 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 *Закрыть*, чтобы завершить добавление настроек веб-службы.
8. Создайте файл сопоставления для системы CMS Диспетчера переноса объектов платформы BI.

   Выполните следующие действия в системе разработки платформы BI для создания текстового файла со сведениями о соединении для обеспечения возможности сопоставления:

   a. В CMS Диспетчера переноса объектов платформы BI перейдите в корневой каталог и создайте папку с именем **LCM** по пути `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/`.

   b. Создайте текстовый файл с именем `LCM_SOURCE_CMS_SID_MAPPING.properties` и введите в него следующие данные:

      - `<Полное имя исходной системы платформы SAP BI с доменом>@<номер порта CMS> = <логическое имя исходной системы, используемое в конфигурации CTS >`
      - `<IP-номер исходной системы платформы SAP BI>@<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 файл `LCM_SOURCE_CMS_SID_MAPPING.properties` в систему, где запущен адаптивный сервер обработки.

Для получения дополнительных сведений о выполнении шагов по настройке для систем, не основанных на ABAP, см. Установка настроек переноса в приложении.

16.7.2.3 Настройка системы импорта платформы BI 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 *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 *Перейти* > *Преобразование*.
   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 *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 BI в качестве системы экспорта.

   > **Примечание**
   >
   > Для получения дополнительных сведений о создании системы, не основанной на ABAP, в качестве исходной, см. раздел Определение и настройка систем, не основанных на ABAP.

6. В CTS+ настройте систему импорта платформы BI, выполнив следующие шаги:

   > **Примечание**
   >
   > Можно определить идентификатор системы (SID) как ссылку на систему импорта платформы BI.

a. Создайте систему, отличную от ABAP, в качестве системы импорта.

   Дополнительную информацию см. в разделе Определение и настройка систем, не основанных на ABAP.

b. Укажите метод развертывания *Другие* и отмените выбор всех прочих параметров.

c. Выберите *Сохранить*.

d. Подтвердите выбор в диалоговом окне..
   Откроется табличное представление для настройки параметров системы импорта.

e. Выберите *Изменить* > *Новые 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 web server name>:<Webserver port>/BOE/LCM/CTSServlet?&cmsName=<BOE destination name>:<CMSport>&authType=<BOE authentication type>`**
      где
      - "BOE web server name" – это имя или IP-адрес компьютера, на котором установлен веб-сервер платформы BI.
      - "Web server port" – это номер порта веб-сервера платформы BI.
      - "BOE destination name" – это имя компьютера, на котором установлен целевой Центральный сервер управления (CMS) платформы BI.
      - "CMS port" – это номер порта целевого CMS.
      - "BOE authentication type" – тип аутентификации пользователя для импорта контента платформы BI. Поддерживаемые виды аутентификации: secEnterprise, secLDAP, secWinAD и secSAPR3.
   3. В поле *Пользователь* введите имя пользователя платформы BI.
   4. В поле *Пароль* введите пароль для платформы BI.
   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. в разделе Настройка маршрутов переноса.

16.7.2.4 Экспорт с платформы BI в CTS+ с использованием SSL

16.7.2.4.1 Настройка SSL для CTS+

Чтобы настроить SSL для CTS+, необходимо настроить SSL для ABAP сервера приложений. Для получения дополнительных сведений см. Настройка SAP Web AS для поддержки SSL.

16.7.2.4.2 Настройка SSL-сертификата на стороне клиента

Чтобы настроить SSL-сертификат на стороне клиента, необходимо импортировать сертификат сервера или доверенного центра сертификации в хранилище ключей виртуальной машины Java.

1. Создайте резервные копии файлов `cacerts` из каталога `<INSTALLDIR>\win64_x64\sapjvm\jre\lib\security`.
2. Импортируйте сертификат в Tomcat JVM, где содержится файл `BOE.war`, используя следующие параметры:

```
<INSTALLDIR>\win64_x64\sapjvm\jre\bin\keytool.exe -import -file server.cer
-keystore cacerts
```

3. Перезапустите Tomcat.

16.7.2.4.3 Настройка веб-службы экспорта в CTS+

Для настройки веб-службы экспорта с использованием HTTPS в CTS+ (`EXPORT_CTS_WS`) можно создать новую конечную точку HTTPS.

> ⓘ Примечание
>
> Также можно переключить существующую конечную точку HTTP на использование HTTPS.

1. Используйте код транзакции **`soamanager`**. Затем на вкладке *Безопасность поставщика* в разделе *Безопасность соединения* выберите *SSL по протоколу HTTP (безопасность канала переносов)*, а в разделе *Аутентификация канала переносов* выберите *Идентификатор пользователя/пароль*.
2. На вкладке *Настройки переноса* в разделе *Привязка переноса* присвойте значение *HTTPS* параметру *Вычисляемый протокол*.

16.7.2.4.4 Настройка управления переносом для SSL

> → Напоминание
>
> Импортируйте сертификат сервера или доверенного центра сертификации в хранилище ключей виртуальной машины Java.

1. В CMC на вкладке *Диспетчер переноса объектов* выберите *Настройки* > *Настройки CTS* > *Настройки веб-службы*.
2. Убедитесь, что параметр *URL веб-службы* включает `https://` и номер порта, настроенный выше.

> **Примечание**
>
> *Перенос через CTS* не выводится в списке *Место назначения задания* или в диалоговом окне *Переопределения*, если указанный URL недоступен. В случае неудачи SSL-квитирования между Диспетчером переноса объектов и CTS+ в файл журнала CMC будет записана ошибка.

16.7.2.5 Импорт из CTS+ на платформу BI с использованием SSL

16.7.2.5.1 Настройка сервера Tomcat платформы BI для использования протокола HTTPS

Чтобы настроить сервер Tomcat платформы BI для использования протокола HTTPS, необходимо выполнить следующие шаги на компьютере, где установлена платформа BI.

1. Создайте пару ключа сервера и сертификата, а также хранилище ключей.
   a. Запустите программу `<INSTALLDIR>\win64_x64\sapjvm\jre\bin\keytool.exe` со следующими параметрами:

   ```
   keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore
   serverkeystore.jks -storetype JKS
   keytool -certreq -keyalg RSA -alias server -file server.csr -keystore
   serverkeystore.jks
   ```

   b. При появлении запроса введите следующую информацию:
      - Ваши имя и фамилия.
      - Название вашего подразделения.
      - Название вашей организации.
      - Название вашего города или района.
      - Название вашего региона.
      - Двухбуквенный код страны.

      Отобразится форматированная строка следующего вида: `CN=John Smith, OU=Accounting, O=SAP, L=Vancouver, ST=BC, C=CA`). Введите **yes** и нажмите клавишу `ВВОД`, чтобы подтвердить введенные данные.
2. Отправьте запрос сертификата сервера в центр сертификации.
3. Импортируйте подписанный сертификат сервера в хранилище ключей сервера с использованием следующих параметров:

   ```
   keytool -import -alias server -keystore serverkeystore.jks -trustcacerts
   -file server.crt
   ```

4. Выполните настройку файла конфигурации Tomcat `server.xml`, чтобы использовать протокол HTTPS и созданное вами хранилище ключей сервера.
5. Перезапустите Tomcat и проверьте соединение, перейдя по следующему URL в браузере: `https://<SERVERNAME>:<SSLPORTNUMBER>`

Связанные сведения

Настройка SSL для CTS+ [страница 686]

16.7.2.5.2 Настройка CTS+ для SSL

Чтобы настроить CTS+ для SSL, необходимо создать PSE SSL-клиента и импортировать туда сертификат.

Связанные сведения

Настройка SSL для CTS+ [страница 686]

16.7.2.5.3 Обновление тестовых и продуктивных систем в CTS+ для использования HTTPS

Для включения HTTPS в тестовых и продуктивных системах выполните следующие действия:

1. Используйте код транзакции STMS.
2. Щелкните *Обзор системы*.
3. Выберите тестовую или продуктивную систему и щелкните *Перейти* > *Типы приложений* > *Метод развертывания*.
4. Убедитесь, что параметр *URI развертывания* включает `https://` и настроенный номер порта HTTPS.

16.7.3 Перенос заданий с помощью CTS

В этом разделе описывается рабочий процесс, поддерживаемый Диспетчером переноса объектов для переноса объектов Центрального сервера управления (CMS) платформы BI из исходной системы в целевую систему с использованием системы изменений и переносов (CTS). Чтобы выполнить повышение задания с использованием CTS, выполните следующие шаги:

1. Запустите Диспетчер переноса объектов 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 пункт *Перенести 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 InfoObject.
5. Выберите объект InfoObject, который требуется добавить в задание, и нажмите кнопку *Добавить*.
   Если требуется добавить объект InfoObject и уйти с экрана *Добавить объекты*, выберите *Добавить и закрыть*.
   Объект InfoObject прикреплен к заданию, появится окно *Задания для переноса*.

   > ⓘ Примечание
   >
   > Окно "Задания для переноса" используется для выполнения следующих действий:
   > - Используйте вариант *Добавить объекты* для добавления объектов InfoObject к заданию. Для получения подробных сведений см. раздел "Добавление объекта InfoObject к заданию".
   > - При помощи параметра *Управление зависимостями* доступно управление зависимостями выбранного объекта InfoObject. Зависимости объекта SAP BW отображаются в интерфейсе пользователя и могут быть там выбраны.
   > Более подробные сведения можно получить в разделе "Управление зависимыми объектами задания".

6. Нажмите кнопку *Перенести*.
   Откроется окно *Перенести*, на котором отображены индикатор, владелец и краткое описание заданного в текущий момент запроса на перенос по умолчанию.
7. Гиперссылку *Запросы переносов* можно использовать для выполнения следующих действий:
   - Просмотр сведений о запросе переноса
   - Изменение параметров запроса переноса по умолчанию.
   - Выбор другого запроса переноса.
   - Создание запроса переноса.

   1. Щелкните ссылку *Запросы на перенос*, чтобы открыть веб-интерфейс пользователя *организатора переносов*.
   2. При запросе учетных данных для входа в систему выполните вход с использованием допустимых учетных данных системы контроллера домена CTS.
   3. Обновите экран *Перенести*, чтобы просмотреть обновления.

   Для получения дополнительных сведений об использовании веб-интерфейса *организатора переносов* см. раздел Веб-интерфейс организатора переносов.

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 *Перенести*.
10. Закройте задание.
    Появится главный экран Диспетчера переноса объектов. Теперь созданное задание имеет статус *Экспортировано в CTS*.
11. Выпустите объект платформы BI в систему назначения, выполнив следующие шаги.
    a. Щелкните по ссылке, отображенной в столбце "состояние" задания, которое нужно перенести. Откроется окно *Состояние переноса*.
    b. Нажмите *Состояние запроса*.
    Откроется веб-интерфейс пользователя *организатора переносов*.
    c. Если запрос имеет статус *Изменяемый*, нажмите кнопку *Деблокировать*, чтобы деблокировать запрос на перенос объекта платформы BI. Для получения дополнительных сведений об освобождении запросов на перенос, содержащих объекты, не относящиеся к ABAP, см. раздел Освобождение запросов на перенос с объектами, не относящимися к ABAP.
    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 переноса*.
14. Импортируйте объект платформы BI в систему назначения, выполнив следующие шаги.
    a. Войдите в контроллер домена CTS+.
    b. Вызовите транзакцию **STMS**, чтобы выполнить вход в систему управления переносами.
    c. Щелкните значок *Обзор импорта*.
    Откроется окно *Обзор импорта*, и можно будет просмотреть элементы в очереди на импорт из всех систем.
    d. Выберите идентификатор целевой системы Диспетчера переноса объектов.
    Можно просмотреть список запросов на перенос, которые можно импортировать в систему.
    e. Нажмите кнопку *Обновить*.
    f. Импортируйте соответствующие запросы на перенос. Дополнительную информацию см. в разделе Импорт запросов.

    Для получения общих сведений об импорте запросов на перенос с содержимым BOLM см. раздел Импорт запросов на перенос с объектами, не относящимися к ABAP
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 деблокировать все задачи, связанные отдельно с каждым зависимым объектом.
6. Правой кнопкой мыши щелкните по запросу, связанному с основным объектом BW и выберите *Деблокировать напрямую*.
7. Обновляйте экран, пока не будут деблокированы все запросы.

> **Примечание**
>
> Можно просмотреть журналы запроса, дважды щелкнув его.

b. Импортируйте 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. Дополнительную информацию см. в разделе Импорт запросов.
      Для получения дополнительных сведений о переносах с использованием очередей импорта см. раздел Переносы с использованием очередей импорта

16. Для просмотра статуса задания для переноса войдите в целевую систему.

Для получения информации об общей системе изменений и переносов (CTS) см. раздел Настройка целевых систем для других приложений.

Связанные сведения

Создание задания [страница 628]
Управление зависимостями задания [страница 633]

16.8 Использование мастера диспетчера переноса объектов

Мастер диспетчера переноса объектов позволяет без труда копировать ресурсы BI из одного репозитория в другой несколькими щелчками мыши.

Мастер диспетчера переноса объектов поддерживает следующие сценарии переноса объектов:

- Экспорт ресурса BI из исходной системы в файл LCMBIAR.
- Тиражирование ресурса BI из исходной системы в целевую систему.
- Импорт файла LCMBIAR в целевую систему.

С помощью мастера диспетчера переноса объектов теперь можно перенести все или только выборочное содержимое репозитория без использования командной строки. Удобный графический интерфейс мастера диспетчера переноса объектов облегчает работу администратора.

Для получения дополнительных сведений, касающихся рекомендаций для мастера диспетчера переноса объектов, см. SAP-ноту 2531264.

> ⚠ Предупреждение
>
> Мастер диспетчера переноса объектов не поддерживает откат. Это означает, что после переноса ресурсов BI нельзя будет восстановить предыдущее состояние целевой системы.

> ⓘ Примечание
>
> Прежде чем начать перенос объектов, просмотрите значение параметра памяти. Значение Xms не должно быть больше значения Xmx.

> ⓘ Примечание
>
> При наличии объектов QaaWs необходимо должным образом настроить целевую систему.

> → Совет
>
> Для повышения производительности отключите аудит и мониторинг в CMC целевой системы. Дополнительные сведения см. в разделе "Аудит" руководства администратора платформы Business Intelligence.

16.8.1 Исключение объектов из переноса

Можно выбрать объекты из приведенного ниже списка и исключить их из задания переноса для экономии дискового пространства и сокращения время миграции.

Задание переноса выполняет миграцию каждого объекта BI из исходной системы в целевую. В результате переносятся также переносятся объекты, специфичные для исходной системы и не используемые в целевой системе. Чтобы исключить из переноса объекты BI, выполните следующие действия.

1. Перейдите в папку `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
2. Откройте файл *PromotionManagementWizard.ini* в текстовом редакторе.
3. С помощью средства поиска найдите строку *# List of kinds to exclude automatically from full/selective export* (список типов для автоматического исключения из полного/выборочного экспорта).
   Под этой строкой отображается код `-Dcom.sap.businessobjects.pmw.exclude.kind={}`.
4. Ориентируясь на приведенный ниже список объектов, добавьте объекты для исключения между скобок `{}`.

5. Сохраните файл.

Объекты, указанные в коде, будут исключены при выполнении задания переноса.

Список объектов, которые можно исключить из задания переноса, см. в таблице ниже.

CustomMapped Attributes	DFS.Parameter	Discussions	GDPR Object
LCM JOBS	LCM Overrides	LCM Scan History	LCM Settings
LANDSCAPE	LANDSCAPE Connection	LIVE Office	MoN.MBEAN Config
MON.ManagedEntity Status	MON.MonAppDataStore	Mon.Probe	Mon.Subscription
NotificationScheduleObject	Override entry	PlatformSearchApplication Status	PlatformSearchContentExtractor
PlatformSearchContentStore	PlatformSearchIndexEngine	PlatformSearchQueue	PlatformSearchScheduling
PlatformSearchSearchAgent	PlatformSearchServiceSession	TaskTemplate	VisualDifferenceComprator
XL.XcelsiusApllication	busobjectreporter	Explorer	Lumira Extensions

16.8.2 Когда используется мастер диспетчера переноса объектов

Для мастера диспетчера переноса объектов вам доступно несколько различных параметров. Эта таблица помогает определить, является ли мастер диспетчера переноса объектов наиболее подходящим решением для ваших потребностей.

Различные параметры для диспетчера переноса объектов

	Мастер диспетчера переноса объектов	**Диспетчер переноса объектов с использованием параметра командной строки**	**Диспетчер переноса объектов в Central Management Console**
Назначение	Перенос объектов за один раз	Автоматизация	Проект
Область переноса объектов	Значительное число ресурсов BI	Значительное число ресурсов BI	Небольшое количество ресурсов BI
Задание	Нет возможности создать задание, которое может быть выполнено повторно сервером заданий	Возможно создание прогона задания сервером заданий	Возможно создание прогона задания сервером заданий

> **Примечание**
>
> Файлы LCMBIAR совместимы с каждым параметром диспетчера переноса объектов независимо от выбранного параметра диспетчера.

16.8.2.1 Определение параметров диспетчера переноса объектов

1. Укажите необходимые параметры диспетчера переноса объектов. Справочная информация содержится здесь:

Параметр	Описание
Временная папка	ⓘ Примечание Убедитесь, что выделено достаточно места во временной папке. Объем свободного места должен превышать необходимый объем по крайней мере в два раза.
Расположение журнала	Расположение журнала определено по умолчанию. Его можно изменить позднее. Изменения сразу учитываются в параметрах диспетчера переноса объектов.
Уровень журнала	Для уровня журнала можно указать следующие значения: • По умолчанию • Низкий • Средний • Высокий Установлен уровень журнала "По умолчанию", пока он не будет изменен.
Язык	Для мастера диспетчера переноса объектов можно указать предпочитаемый язык.

2. Нажмите кнопку *Далее*

16.8.3 Сценарий

Мастер диспетчера переноса объектов поддерживает сценарии переноса объектов трех типов:

- Из продуктивной системы в LCMBIAR: копирование объектов с рабочего сервера CMS в файл LCMBIAR.
- С рабочего сервера CMS в продуктивную систему переноса объектов: копирование объектов из продуктивной исходной системы CMS в продуктивную целевую систему CMS.
- Из LCMBIAR в продуктивную систему: импорт объектов из файла LCMBIAR в продуктивную целевую систему CMS.

16.8.3.1 Перенос объектов из рабочей исходной системы CMS в файл LCMBIAR

Чтобы перенести объекты с рабочего сервера CMS в файл LCMBIAR:

1. Нажмите кнопку *Экспорт*.
2. Чтобы определить исходный CMS, выполните одно из следующих действий:
   - Чтобы использовать центральный сервер CMS в качестве исходного CMS, установите флажок *Сделать центральный CMS исходным CMS*.
   - В разделе "Источник" введите следующие данные:
     - Имя CMS
     - Пользователь
     - Пароль
     - Аутентификация
3. В поле *Место назначения* щелкните *Выбрать*, чтобы выбрать расположение файла LCMBIAR.
4. (Необязательно) Введите пароль, чтобы зашифровать файл LCMBIAR.

   > **Примечание**
   >
   > В случае шифрования файла LCMBIAR процесс переноса занимает больше времени.

5. Нажмите кнопку *Далее*, чтобы выбрать объекты для экспорта.

16.8.3.2 Перенос объектов из рабочей исходной системы CMS в рабочую целевую систему CMS

Для переноса объектов из рабочей исходной системы CMS в рабочую целевую систему CMS:

1. Выберите *Перенести*.
2. Чтобы определить исходный CMS, выполните одно из следующих действий:
   - Чтобы использовать центральный сервер CMS в качестве исходного CMS, установите флажок *Сделать центральный CMS исходным CMS*.
   - В разделе "Источник" введите следующие данные:
     - Имя CMS
     - Пользователь
     - Пароль
     - Аутентификация
3. Чтобы определить целевой CMS, выполните одно из следующих действий:
   - Чтобы использовать центральный сервер CMS в качестве целевого CMS, установите флажок *Сделать центральный CMS целевым CMS*.
   - В разделе *Место назначения* введите следующие данные:
     - Имя CMS

    - Пользователь
    - Пароль
    - Аутентификация
4. Нажмите кнопку *Далее*, чтобы выбрать объекты, которые требуется скопировать из исходной системы в целевую.

16.8.3.3 Перенос объектов из файла LCMBIAR в рабочую целевую систему CMS

Чтобы перенести объекты из файла LCMBIAR на рабочий сервер CMS:

1. Нажмите кнопку *Импорт*.
2. Чтобы определить целевой CMS, выполните одно из следующих действий:
    - В разделе *Место назначения* установите флажок *Сделать центральный CMS целевым CMS*.
    - В разделе *Место назначения* введите следующие данные:
        - Имя CMS
        - Пользователь
        - Пароль
        - Аутентификация
3. В разделе *Источник* нажмите кнопку *Выбрать*, чтобы выбрать файл LCMBIAR, который требуется импортировать.
4. (Необязательно) Введите пароль, чтобы зашифровать файл LCMBIAR.

    > ⓘ Примечание
    >
    > В случае шифрования файла LCMBIAR процесс переноса занимает больше времени.

5. Нажмите кнопку *Далее*, чтобы выбрать объекты для импорта.

16.8.4 Объекты

Мастер диспетчера переноса объектов поддерживает перенос содержимого двух типов:

- Полный перенос содержимого
- Перенос выборочного содержимого

В следующей таблице дано пояснение каждого типа.

Типы переноса содержимого	Перенесенное содержимое	Зависимости содержимого
Полный перенос содержимого	Все следующее содержимое переносится из исходной системы в целевую: • Объекты (пользователи, документы, юниверсы, соединения и т. д.) • Экземпляры • Отношения между объектами • Защита объектов	Поскольку выполнено ведение всех отношений, оценка зависимостей не требуется. С текущего шага объектов вы переходите сразу на итоговый шаг.
Перенос выборочного содержимого	Содержимое, выбранное в исходной системе, переносится в целевую систему. Содержимое может быть следующим: • Объекты (пользователи, документы, юниверсы, соединения и т. д.) • Экземпляры • Отношения между объектами • Защита объектов	Поскольку из исходной системы в целевую переносится не все содержимое, необходимо выполнить оценку зависимостей.

16.8.4.1 Перенос всего содержимого

Чтобы перенести все содержимое из исходной системы в целевую:

1. Выберите *Полный перенос содержимого*.

   Для переноса будут выбраны все объекты.
2. Нажмите кнопку *Далее*, чтобы просмотреть выбранное содержимое.

16.8.4.2 О переносе выборочного содержимого

Прежде чем перенести выборочное содержимое из исходной системы в целевую, необходимо определить параметры экспорта. Определение параметров экспорта позволяет извлекать настройки, указанные в исходной системе, которые требуется перенести в целевую систему.

16.8.4.2.1 О параметрах экспорта

Если необходимо извлечь настройки, указанные в исходной системе, и перенести их в целевую систему, в параметрах экспорта нужно определить следующие параметры:

- Экземпляры объектов
- Зависимости объектов
- Безопасность
- Комментирование
- Задания объединения
- Разрешение конфликта имен

Экземпляры объектов

Экземпляры объектов	Описание
Экспорт всех экземпляров объекта, когда объект выбран	Выбранные объекты экспортируются вместе со всеми экземплярами этих объектов.
Экспорт только повторяющихся экземпляров объекта, когда объект выбран	Выбранные объекты экспортируются только вместе с повторяющимися экземплярами этих объектов. Например, если запланировано еженедельное и ежемесячное обновление документа, в процессе экспорта будут экспортированы этот документ и два повторяющихся экземпляра данного документа.
Не экспортировать экземпляры объекта	Экспортируются только выбранные объекты. Их экземпляры не экспортируются.

Зависимости объектов

Зависимости объектов	Описание
Включить зависимости при выборе объектов	Выбранные объекты экспортируются вместе со всеми зависимостями этих объектов. **Примечание** Этот параметр установлен по умолчанию.
Исключить зависимости при выборе объектов	Выбранные объекты экспортируются без зависимостей этих объектов.

Безопасность

Безопасность	Описание
Включить безопасность объекта	Выбранные объекты экспортируются с настройками безопасности этих объектов.

Безопасность	Описание
Включить безопасность пользователей	Выбранные объекты экспортируются с настройками безопасности пользователей этих объектов.
Включить безопасность приложений	Выбранные объекты экспортируются с настройками безопасности приложений этих объектов.
Включить безопасность верхнего уровня	Экспортируются настройки безопасности, определенные в корневой папке. **⚠ Предупреждение** Этот параметр перезаписывает настройки безопасности, определенные в целевой системе. Его следует использовать осмотрительно.

Комментирование

Комментирование	Описание
Включить комментарии	Выбранные объекты экспортируются вместе со всеми комментариями этих объектов.
Предпочтения стартовой панели BI группы пользователей	Если этот флажок установлен, настройки группы пользователей стартовой панели BI исходной системы и предпочтения по умолчанию устанавливаются в целевой системе.

Предпочтения группы пользователей BI

Предпочтения группы пользователей BI	Описание
Перезапись предпочтений групп пользователей BI	Если этот флажок установлен, настройки группы пользователей стартовой панели BI исходной системы и предпочтения по умолчанию устанавливаются в целевой системе. **ⓘ Примечание** При переносе документа Web Intelligence, использующего пользовательскую настройку, с помощью файла BIAR обязательно включите этот параметр для импорта пользовательской настройки.

Задания объединения

Задания объединения	Описание
Включить отношение заданий объединения	Выбранные объекты импортируются вместе с отношениями заданий объединения этих объектов, ведение которых выполнено.

Разрешение конфликта имен

Разрешение конфликта имен	Описание
Разрешение конфликта имен	Если выбранный объект имеет такое же имя, как объект в целевой системе, но другой CUID, в целевой системе будет создана копия выбранного объекта. Если этот параметр не активирован, выбранный объект с именем, совпадающим с именем объекта в целевой системе, но другим CUID, не будет скопирован в целевую систему.

16.8.4.2.2 Перенос выборочного содержимого

Чтобы перенести выборочное содержимое из исходной системы в целевую:

1. Выберите *Перенос выборочного содержимого*.
2. Чтобы определить *параметры экспорта*, щелкните *Параметры*.
3. (Необязательно) Установите флажок *Применить фильтр времени*, чтобы отфильтровать объекты в соответствии с диапазоном дат и времени.
4. Выберите объекты для экспорта.
5. Чтобы оценить зависимости объекта, установите соответствующий флажок под значком зависимостей.

   > **Примечание**
   >
   > По умолчанию все флажки зависимостей установлены. Если оценка зависимостей объекта не требуется, снимите флажок.

6. Щелкните *Далее*, чтобы оценить зависимости.

16.8.5 Зависимости

Если выбран перенос выборочного содержимого из исходной системы в целевую, можно оценить зависимости выборочного содержимого. Шаг *Зависимости* предоставляет обзор выбранных объектов, определенных как зависимости.

О зависимостях выбранных объектов можно просмотреть следующие сведения:

- Название
- CUID
- Дата

Вы можете выбрать объекты, определенные как зависимости:

1. В зависимости от уровня детализации просмотра выполните одно из следующих действий:
   - Щелкните *Развернуть*, чтобы просмотреть подробные сведения о каждой зависимости.
   - Щелкните *Свернуть все*, чтобы просмотреть только зависимые объекты.
2. Выберите зависимости для переноса.

   > ⓘ Примечание
   >
   > По умолчанию все флажки зависимостей установлены. Если перенос зависимостей объекта не требуется, снимите флажок.

3. Нажмите кнопку *Далее*, чтобы просмотреть объекты, выбранные для переноса.

16.8.6 Общие сведения

Прежде чем выполнить перенос, необходимо просмотреть объекты, выбранные для переноса.

Вы можете просмотреть о каждом объекте следующие сведения:

- Название
- CUID
- Дата

> ⚠ Предупреждение
>
> Убедитесь, что включены все объекты, которые вы хотите скопировать, поскольку после начала переноса объектов этот процесс нельзя будет отменить. Мастер диспетчера переноса объектов не поддерживает откат.

Объекты можно просмотреть:

1. В зависимости от уровня детализации просмотра выполните одно из следующих действий:
   - Щелкните *Развернуть*, чтобы просмотреть подробные сведения о каждом объекте.
   - Щелкните *Свернуть*, чтобы просмотреть родительский объект каждого объекта.

   > ⓘ Примечание
   >
   > Уровень детализации в файле CSV результатов переноса меняется в зависимости от того, нажата ли кнопка *Развернуть* или *Свернуть*.

2. Чтобы убедиться, что на жестком диске достаточно места для переноса объектов, просмотрите *Минимальное требуемое временное пространство*.
3. Щелкните *Пуск*, чтобы перенести объекты.

   После начала переноса этот процесс отменить невозможно.

16.8.7 (необязательно) Файл свойств

Следующие параметры можно настроить в файле свойств мастера диспетчера переноса объектов:

- Параметры SSL
- Параметры

Файл свойств мастера диспетчера переноса объектов находится в каталоге:`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\PromotionManagementWizard`

16.8.7.1 Настройка параметров SSL

Если используется SSL, необходимо настроить параметры SSL мастера диспетчера переноса объектов в каталоге

`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\PromotionManagementWizard`

1. Откройте файл `PromotionManagementWizard.ini` в текстовом редакторе.
2. Для активации режима SSL снимите метку комментария в строках, которые начинаются с "-D".
3. Введите значение для каждого из параметров.

Параметр	Значение
`-Dbusinessobjects.orb.oci.protocol`	Значение: ssl **Примечание** Это значение позволяет осуществлять обмен данными по SSL.
`-DcertDir`	Расположение ключей и сертификатов
`-DtrustedCert`	Имя файла доверительного сертификата **Примечание** Чтобы указать несколько файлов, следует разделить записи точкой с запятой (например, файлA; файлB).
`-DsslCert`	Сертификат SDK
`-DsslKey`	Секретный ключ сертификата SDK

Параметр	Значение
`-Dpassphrase`	Расположение файла, содержащего пароль для секретного ключа
`-Dpsecert`	Файл сертификата PSE

> ⚠ Предупреждение
>
> Не добавляйте и не изменяйте другие параметры или значения.

4. Сохраните `PromotionManagementWizard.ini`

Пример: Параметры SSL в файле `PromotionManagementWizard.ini`

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir=C:/SSL
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
-Dpsecert=temp.pse
```

16.8.7.2 Настройка параметров

Можно выполнить настройку параметров в зависимости от собственных потребностей в файле свойств мастера диспетчера переноса объектов, который находится в каталоге:

`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\PromotionManagementWizard`

1. Откройте файл `PromotionManagementWizard.ini` в текстовом редакторе.
2. Для активации параметров снимите метку комментария в строках, которые начинаются с "-D".
3. Введите значение для каждого из параметров.

Параметр	Значение
`-Dbusinessobjects.connectivity.directory`	Расположение каталога сервера соединений.
`-Dcom.businessobjects.mds.cs.ImplementationID`	`csEX` ⓘ Примечание Не изменяйте это значение.

Параметр	Значение
`-Xms8g`	По умолчанию указан объем памяти 8 ГБ. Значение Xms не должно быть больше значения Xmx.
`-Xmx10g`	По умолчанию указан объем памяти 10 ГБ. Для репозитория, включающего 65000 объектов, достаточен объем памяти 10 ГБ.
`-Dbobj.biar.suggestSplit=512`	Значение по умолчанию (рекомендуется) Рекомендуется использовать параметр `-Dbobj.biar.suggestSplit`. При переносе объектов с рабочего сервера CMS в файл LCMBIAR эта настройка позволяет разделить файл LCMBIAR на несколько файлов LCMBIAR.
`-Dbobj.biar.forceSplit=768`	Значение по умолчанию (рекомендуется) Если параметр `-Dbobj.biar.suggestSplit` невозможно применить, в качестве альтернативного решения применяется параметр `-Dbobj.biar.forceSplit`.
`-Dcom.businessobjects.lcm.commit`	• KEEP_TS. Значение по умолчанию. Это значение позволяет сохранить даты изменения источника. • LEGACY. Даты изменения соответствуют дате выполнения в целевой системе. Это существующее поведение до версии 4.2 SP5.
`-Dcom.sap.businessobjects.pmw.exclude.list`	Данный параметр позволяет окончательно исключить объекты при переносе объектов из исходной системы в целевую или при экспорте исходной системы в файл LCMBIAR. Значением (CUID) может быть объект (документ, папка и т. д.). Если указана папка, будут исключены все дочерние элементы папки.

4. Сохраните `PromotionManagementWizard.ini`.

Пример: Параметры мастера диспетчера переноса объектов в `PromotionManagementWizard.ini`

```
-Dbusinessobjects.connectivity.directory=C:\Program Files (x86)\SAP
BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer
-Dcom.businessobjects.mds.cs.ImplementationID=csEX
-Xms2g
-Xmx10g
-Dbobj.biar.suggestSplit=512
```

```
-Dcom.businessobjects.lcm.commit=KEEP_TS
-Dcom.sap.businessobjects.pmw.exclude.list="c:/
PromotionManagementWizardExcludedItems.txt"
# Exclusion List AY2ygq4hFJhJmZMQNlQh8OI # Report Samples
AeN4lEu0h_tAtnPEjFYxwi8 # WebIntelligence Samples
```

16.8.8 Мастер диспетчера переноса объектов в Linux

Мастер диспетчера переноса объектов можно запустить в Linux.

Прежде чем запустить мастер диспетчера переноса объектов в Linux, убедитесь, что в системной переменной `PATH` настроено время выполнения Java.

Чтобы запустить мастер диспетчера переноса объектов в Linux, выполните следующие шаги:

1. Откройте оболочку и перейдите в каталог установки, например следующий:

   ```
   /usr/sap_bobj/enterprise_xi40
   ```

2. Выполните следующую команду:

   ```
   ./PromotionManagementWizard
   ```

   Мастер диспетчера переноса объектов запустится.

   Для получения дополнительных сведений об использовании перенаправления X11 и SSH см. документацию по ОС.

17 Управление версиями

17.1 Управление различными версиями объекта InfoObject

Приложение управления версиями позволяет управлять версиями ресурсов BI, которые находятся в репозитории платформы BI. Оно поддерживает системы управления версиями Subversion и GIT. В этом разделе описывается использование функции управления версиями в Диспетчере переноса объектов.

Для создания версий объекта InfoObject и управления ими выполните следующие действия:

1. Запустите Диспетчер переноса объектов.
2. Щелкните задание правой кнопкой мыши, выберите *Действия VMS* и щелкните *Добавить в систему управления версиями (VM)*. (Также можно выбрать вкладку *Действия VMS*, а затем щелкнуть *Добавить в систему управления версиями (VM)*.)

   > ⓘ Примечание
   >
   > Нажатие *Добавить в систему управления версиями (VM)* приведет к созданию базовой версии объекта в репозитории VMS. Базовая версия требуется для последующей регистрации.

3. Нажмите кнопку *Возврат*, чтобы обновить документ, существующий в репозитории VMS. Откроется диалоговое окно *Комментарии к возврату*.
4. Введите свои комментарии и нажмите кнопку *OK*.
   Изменение номера версии выбранного объекта InfoObject отображается в столбцах VMS и CMS.
5. Чтобы получить последнюю версию документа из VMS, выберите требуемый объект InfoObject и щелкните *Получить последнюю версию*.
6. Чтобы создать копию последней версии, нажмите кнопку *Создать копию*.
   Создана копия выбранной версии.
7. Выберите *Журнал*, чтобы просмотреть все версии, доступные в выбранном ресурсе.
   Будет открыто 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.
   - *Экспортировать копию версии*– позволяет получить копию выбранной версии и сохранить ее в локальной системе.

17.1.1 Права доступа к приложению управления версиями

В этом разделе описаны права доступа к приложению управления версиями.

- Консоль CMC 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 CMC и выберите *Приложения*.
2. Дважды щелкните *Управление версиями*.
3. Щелкните *Безопасность пользователя* и выберите пользователя. Можно просмотреть или назначить права безопасности выбранному пользователю.
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 юниверсов
   - Просмотр удаленных ресурсов
5. Если необходимо назначить права выбранному пользователю, выберите соответствующее право и нажмите кнопку *Назначить безопасность*.

17.1.2 Резервное копирование и восстановление файлов Subversion

В этом разделе описываются предлагаемые процедуры по выполнению резервного копирования и восстановления файлов Subversion. План резервного копирования и восстановления состоит из мер предосторожности, предпринимаемых при системном сбое в результате стихийного бедствия или катастрофы.

17.1.2.1 Резервное копирование файлов Subversion

Для резервного копирования файлов Subversion выполните следующие шаги:

1. В Windows перейдите в `<INSTALLDIR>\SAP BusinessObjects Enterprise 4.0\CheckOut` или в Unix перейдите в `<INSTALLDIR>/sap_bobj/enterprise_40/Subversion/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.

17.1.2.2 Восстановление файлов Subversion

Для восстановления файлов Subversion выполните следующие шаги:

1. Восстановите папку "CheckOut" из местоположения, в которое ранее было выполнено резервное копирование.

   > ⓘ Примечание
   >
   > В консоли CMC выберите *Приложения* > *Управление версиями* > *Настройки VMS* и убедитесь, что в поле *Каталог рабочего пространства* введен правильный путь извлечения.

2. Восстановите репозиторий "LCM_Repository" из местоположения, в которое ранее было выполнено резервное копирование.

   > ⓘ Примечание
   >
   > В консоли CMC выберите *Приложения* > *Управление версиями* > *Настройки VMS* и убедитесь, что в поле *Путь установки* введен правильный путь извлечения.

17.2 Управление разными версиями ресурсов BI

Приложение управления версиями позволяет выполнять ведение разных версий ресурсов BI, которые существуют в репозитории платформы BI. Для поддержки этой функции в средство включена система контроля версий Subversion.

Для управления разными версиями заданий или других объектов InfoObject выполните следующие шаги:

1. Войдите в приложение CMC и выберите *Управление версиями*.
2. На левой панели окна *Управление версиями* выберите папку для просмотра задания или других объектов InfoObject, для которых требуется выполнять 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 к возврату*.

5. Введите свои комментарии и нажмите кнопку *OK*.
   Изменение номера версии выбранного объекта InfoObject отображается в столбцах *Версия системы управления версиями* и *Версия CMS* (Центрального сервера управления).
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 репозиториях VMS и CMS будет создана копия выбранной версии.
8. Выберите *Журнал*, чтобы просмотреть все версии, доступные для выбранного инфо-объекта.
   Будет открыто 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 в локальной системе.
   - *Сравнить* – позволяет сравнить метаданные двух версий задания. Дополнительные сведения см. в разделе «Сравнение разных версий одного задания».
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 новая, чем версия в VMS, рядом с обновленным инфо-объектом появляется индикатор. Если поместить курсор на этот индикатор, появится всплывающая подсказка `CMS имеет более новую версию`.
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 полного удаления объекта из репозитория VMS нажмите *Удалить*.

    > **Примечание**
    >
    > При использовании *Получить версию* ресурс перемещается из списка отсутствующих файлов VMS в CMS.

12. Выберите информационный объект и нажмите кнопку , чтобы просмотреть свойства информационного объекта.

    Вместо этого также можно щелкнуть инфо-объект правой кнопкой мыши и выполнить шаги с 3 по 12.
13. В приложении *Управление версиями* можно выполнить поиск активов BI. Можно использовать такие параметры, как *Найти все поля*, *Найти название*, *Найти ключевое слово*и *Найти описание*, чтобы выполнить поиск и быстрее получить результаты.

> **Примечание**
>
> Функции поиска в приложении *Управление версиями* зависят от контекста. Это означает, что если выбрана папка *Аудит* и введена строка для поиска документа, то платформа BI выполнит поиск документа только в папке *Аудит*. Точно так же, если выбрать *Все папки* и выполнить поиск, то на платформе BI выполняется поиск информационного объекта в каждой из папок.

17.3 Запуск и остановка Subversion вручную в Unix

В Unix Subversion не может запускаться автоматически после перезагрузки компьютера. Начиная с версии платформы BI 4.1 с пакетом поддержки 2 можно выполнить `<INSTALLDIR>/svn_startup.sh` для запуска Subversion и `<INSTALLDIR>/svn_shutdown.sh` для остановки.

> **Примечание**
>
> `svn_shutdown.sh` работает, только если запустить `svnserve` с помощью `svn_startup.sh`.

> **Ограничение**
>
> Если процесс Subversion выполнялся перед установкой исправления пакета поддержки 2, `svn_shutdown.sh` не будет работать после установки исправления. Для перезапуска Subversion необходимо вручную остановить процесс `svnserve`, а затем выполнить `svn_startup.sh`.

17.4 Необходимые файлы для Subversion в Solaris 10 и RedHat Linux 5

Для работы Subversion необходимы следующие файлы.

> **Примечание**
>
> Если какие-либо из следующих двоичных файлов отсутствовали перед установкой платформы BI 4.1 с пакетом поддержки 1, следует выполнить `<INSTALLDIR>/sap_bobj/lcm_installer.sh <SUBVERSION_PASSWORD> <CMS_PASSWORD>`, а затем перезапустить адаптивный сервер обработки, чтобы управление версиями работало правильно.

- В Solaris 10 необходимо установить пакеты `CSWlibiconv2` и `CSWlibgcc-s1`, содержащие `libiconv.so.2` и `libgcc_s.so.1`.

  > **→ Напоминание**
  >
  > После установки пакетов убедитесь, что путь к этим библиотекам включен в переменную среды `LD_LIBRARY_PATH` пользователя.

- В RedHat Linux 5 необходимо развернуть `libexpat.so.1`.

17.5 Использование Apache Subversion в качестве системы управления версиями

Можно установить Apache Subversion в качестве Системы управления версиями и выполнить настройки из Central Management Console.

1. В CMC выберите *Приложения*.
2. Дважды щелкните *VMS*.
   Появится экран "Настройки системы управления версиями".
3. Выберите *Настройки VMS*.
4. В раскрывающемся списке *Системы управления версиями* выберите *Subversion*.
   В соответствующих полях появятся номер порта сервера, пароль, имя репозитория, имя сервера, имя пользователя, имя каталога рабочего пространства и имя каталога установки, указанные в процессе установки средства Диспетчер переноса объектов.
5. Измените поля по необходимости.

   > ⓘ Примечание
   >
   > Убедитесь, что вводите путь установки, содержащий файл `.exe`.

   В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Subversion`

   В Unix: `<INSTALLDIR>/sap_bobj/enterprise_40/subversion/bin`
6. Выберите *SVN*, *HTTP* или *HTTPS*.

   > ⓘ Примечание
   >
   > Дополнительную информацию о подключении к Subversion с использованием HTTPS см. в *документации по Apache Subversion*.

7. (Необязательно) Нажмите кнопку *Проверить VMS*, чтобы проверить настройки системы управления версиями.
8. Нажмите кнопку *Сохранить*.

   > ⓘ Примечание
   >
   > - Если требуется назначить Subversion системой управления версиями по умолчанию, выберите *Использовать в качестве системы управления версиями по умолчанию*.
   > - Если поля были изменены, перезапустите адаптивный сервер обработки.

17.6 Использование Git в качестве системы управления версиями

Можно установить Git в качестве Системы управления версиями и выполнить настройки из Central Management Console.

1. На домашней странице CMC выберите *Приложения*.
2. Щелкните дважды *Управление версиями*.
   Настройки системы управления версиями появятся на экране *Настройки управления версиями*.
3. В списке *Системы управления версиями* выберите *Git*.
   Отображаются *Настройки Git* и необходимые параметры.
4. Выберите протокол и введите значения в пустые поля. Дополнительные сведения о каждом поле см. в следующей таблице.

Термины UI	Описание
Протокол	Выберите "Локальн." в случае установки Git в локальной системе или "HTTP(s)" в случае установки Git на удаленном сервере.
Имя пользователя	Введите имя пользователя сервера, где установлена система Git.
Пароль	Введите пароль для доступа к серверу, где установлена система Git.
URL-адрес сервера	Введите ссылку на сервер, в котором установлена система Git.
Каталог рабочего пространства	Введите путь к файлу, в котором необходимо сохранить рабочее пространство.
Имя репозитория сервера	Введите имя репозитория сервера.
Путь к каталогу установки GIT	Введите каталог установки Git.

> ⓘ Примечание
>
> Если требуется назначить Git системой управления версиями по умолчанию, выберите *Использовать в качестве системы управления версиями по умолчанию*.

5. (Необязательно) Нажмите *Проверить VMS*, чтобы проверить настройки системы управления версиями.
6. Нажмите кнопку *Сохранить*.
7. Выберите *Серверы* > *Список серверов* и в контекстном меню *адаптивного сервера обработки* выберите *Перезапустить сервер*.

Настройка Git в качестве системы управления версиями выполнена успешно.

17.7 Параметры системы управления версиями по умолчанию

При повторной инициализации CMS все настройки приложения удаляются. Ниже перечислены параметры системы управления версиями по умолчанию:

Параметр	Значение
Имя сервера	`localhost`
Порт сервера	`3690`
Имя пользователя	`LCM`
Пароль	Указывается при установке
Путь установки	В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Subversion` В Unix: `<INSTALLDIR>/sap_bobj/enterprise_xi40/subversion/bin`
Имя репозитория	В Windows: `svn_repository` В Unix: `LCM_repository`
Каталог рабочего пространства	В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\CheckOut` В Unix: `<INSTALLDIR>/sap_bobj/enterprise_xi40/CheckOut`
Протокол	`SVN`

17.8 Сравнение разных версий одного задания

Для просмотра различий между двумя версиями одного задания выполните следующие действия:

1. Войдите в приложение CMC.
2. На домашней странице CMC выберите *Управление версиями*.
3. На экране управления версиями выберите задание, 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.

17.9 Обновление содержимого Subversion

При наличии старого содержимого Subversion, созданного с помощью предыдущей версии платформы BI, его можно обновить до последней версии, выполнив следующие действия:

1. Войдите в VMS на компьютере с SAP BusinessObjects Enterprise 4.2.
2. Выполните возврат любого объекта. Например, дважды выполните возврат объектов администратора и гостя.
3. В CMC выберите *Пользователи* и убедитесь, что в качестве номера версии VMS и CMS указано 2.
4. Выйдите из VMS.
5. Из командной строки перейдите в `C:\Program Files\Subversion\bin` и выполните команду экспорта: `svnadmin dump c:/LCM_repository/svn_repository > dumrepo`
6. Скопируйте файл `dumrepo` на компьютер, на котором установлена платформа BI.
7. В командной строке на компьютере, на котором установлена платформа BI, наберите `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 CMC 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.

    Для получения дополнительных сведений об обновлении Apache Subversion см. Примечания к выпуску Apache Subversion 1.10 .

17.10 Настройка Subversion для кластеризованных серверов обработки заданий

17.10.1 Вариант A: настройка основного компьютера Subversion до любых операций системы управления версиями

1. Убедитесь, что каталог рабочих копий не был создан в `<INSTALLDIR>\CheckOut`.

2. Создайте каталог для файлов рабочих копий Subversion и сделайте возможным его совместное использование, задав для него возможность записи с других компьютеров.
3. В CMC на странице параметров системы управления версиями измените *Имя сервера* с **`localhost`** на адрес своего основного компьютера.
4. Измените *Каталог рабочего пространства* на общий каталог рабочих копий, используя следующий формат: `\\<HOSTNAME>\<SHARENAME>`
5. Остановите Server Intelligence Agent (SIA) и смените учетную запись с LocalSystem на администратора операционной системы.

   > **Примечание**
   >
   > LocalSystem не дает права сетевого доступа к общему каталогу.

6. Запустите SIA.

   > **Примечание**
   >
   > Если SIA уже выполнялся под учетной записью с сетевым доступом к общему каталогу, нужно только перезапустить все серверы обработки заданий, где находится система управления версиями, чтобы шаги 3 и 4 вступили в силу.

17.10.2 Вариант Б: настройка Subversion после создания каталога рабочих копий системой управления версиями

1. Убедитесь, что система Subversion не была установлена в рамках платформы BI.
2. Сделайте возможным совместное использование каталога рабочих копий в `<INSTALLDIR>\CheckOut` и задайте для него возможность записи с других компьютеров.
3. Установите имя рабочего пространства одним из следующих способов:
   - Выполните операцию системы управления версиями (VMS) с помощью основного компьютера. Затем просмотрите каталог рабочих копий Subversion, чтобы определить имя рабочего пространства.
   - Вычислите имя рабочего пространства путем удаления символа @ и замены всех двоеточий символом *B*. Например, если кластер имеет имя `ABCD-LCM:6400`, VMS будет использовать `ABCD-LCMB6400` в качестве имени рабочего пространства.

> **Примечание**
>
> Репозиторий Subversion хранится в каталоге рабочих копий.

4. Измените URL по умолчанию с **`localhost`** на тот, который смогут использовать все компьютеры, выполнив следующую команду:

```
svn switch --relocate svn://localhost:3690/
svn_repository svn://<SUBVERSION_MACHINE>:3690/svn_repository \
\<SUBVERSION_SHARE>\CheckOut\<WORKSPACE_NAME>-LCMB6400\WORKSPACE
```

5. При запросе введите пароль администратора операционной системы, пользователя и пароль.

> **Примечание**
>
> По умолчанию используются пользователь LCM и пароль, заданный при установке.

6. В CMC на странице параметров системы управления версиями измените *Имя сервера* с **`localhost`** на адрес своего основного компьютера.
7. Измените *Каталог рабочего пространства* с **`localhost`** на общий каталог рабочих копий: `\\<SUBVERSION_SHARE>\CheckOut`
8. Остановите Server Intelligence Agent (SIA) и смените учетную запись с LocalSystem на администратора операционной системы.
9. Запустите SIA.

> **Примечание**
>
> Если SIA уже был запущен под учетной записью с сетевым доступом к общему каталогу, нужно только перезапустить все серверы обработки заданий, где находится система управления версиями.

17.10.3 Настройка других компьютеров с Subversion

Для настройки других компьютеров с Subversion остановите Server Intelligence Agent (SIA) и смените учетную запись с LocalSystem на учетную запись, имеющую сетевой доступ, чтобы сервер обработки заданий имел доступ к общему каталогу (например, выберите учетную запись администратора операционной системы). Затем перезапустите SIA.

> **Примечание**
>
> Если SIA уже был запущен под учетной записью с сетевым доступом к общему каталогу, нужно только перезапустить все серверы обработки заданий, где находится система управления версиями.

18 Управление приложениями

18.1 Выключение всплывающего сообщения GDPR

Начиная с версии 4.2 SP5 платформы SAP BusinessObjects Business Intelligence всплывающее сообщение GDPR (Общего регламента по защите данных) об отказе от ответственности обязательно появляется у каждого пользователя при входе в веб-приложения платформы BI, такие как:

- Панель запуска BI
- CMC
- Панель запуска Fiori BI
- Открыть документ

Зная, что сообщение GDPR об отказе от ответственности является обязательным, вы можете отключить просмотр этого сообщения.

> ⚠ Предупреждение
>
> Всплывающее сообщение GDPR об отказе от ответственности **не должно** и **не может** быть отключено без участия пользователя. С целью соблюдения Общего регламента ЕС по защите данных все пользователи для продолжения работы должны выразить согласие с содержанием этого сообщения.

Выключение появления сообщения GDPR при входе пользователей в панель запуска BI

1. При стандартной установке Tomcat перейдите к файлу свойств:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`
   Пример: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\default`
2. Создайте новый файл с именем `<Infoview.properties>` и укажите `<файл свойств>` в пользовательском пути:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`
   Пример: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
3. Создайте новую запись свойства для `<disclaimer.enabled>` и задайте для нее значение `<false>`:
   `disclaimer.enabled=false`
4. Сохраните файл.
5. Перезапустите Tomcat.

Выключение появления сообщения GDPR при входе пользователей в CMC

1. При стандартной установке Tomcat перейдите к файлу свойств:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`
   Пример: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
2. Создайте новый файл с именем `<CMCApp.properties>` и укажите `<файл свойств>` в пользовательском пути:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`
   Пример: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
3. Создайте новую запись свойства для `<disclaimer.enabled>` и задайте для него значение `<false>`:
   `disclaimer.enabled=false`
4. Сохраните файл.
5. Перезапустите Tomcat.

Выключение появления сообщения GDPR при входе пользователей в панель запуска Fiori BI

1. При стандартной установке Tomcat перейдите к файлу свойств:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`
   Пример: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\default`
2. Создайте новый файл с именем `<FioriBI.properties>` и укажите `<файл свойств>` в пользовательском пути:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`
   Пример: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
3. Создайте новую запись свойства для `<disclaimer.enabled>` и задайте для него значение `<false>`:
   `disclaimer.enabled=false`
4. Сохраните файл.
5. Перезапустите Tomcat.

Выключение появления сообщения GDPR для приложения "Открыть документ"

1. При стандартной установке Tomcat перейдите к файлу свойств:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`

Пример: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\default`

2. Создайте новый файл с именем `<OpenDocument.properties>` и укажите `<файл свойств>` в пользовательском пути:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`
   Пример: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
3. Создайте новую запись свойства для `<disclaimer.enabled>` и задайте для него значение `<false>`:
   `disclaimer.enabled=false`
4. Сохраните файл.
5. Перезапустите Tomcat.

18.2 Управление приложениями с помощью CMC

18.2.1 Обзор

Область CMC *Приложения* позволяет без программирования изменять внешний вид и функциональность веб-приложений, таких, как CMC и стартовая панель BI. Также вы сможете изменить доступ к этим приложениям для пользователей, групп и администраторов, изменяя права, связанные с каждым приложением.

В этом разделе содержится информация, процедуры и инструкции о выполнении различных настроек. Настройки следующих приложений можно изменить с помощью CMC:

- *Приложение-источник предупреждения*
- *Analysis, выпуск для OLAP*
- *Среда выполнения Analysis Office*
- *Конфигурация сервера авторизации*
- *Веб-приложения BEx*
- *Пульт администрирования BI*
- *Стартовая панель BI*
- *Рабочие пространства BI*
- *Центральная консоль управления*
- *Совместная работа*
- *Приложение комментариев BI*.
- *Конфигурация Crystal Reports*
- *Аутентификация HANA*
- *Средство дизайна информации*
- *Приложение Information Steward*
- *BI Admin Studio*
- *Средство управления несколькими организациями*
- *Open Document*

- *Приложение поиска по платформе*
- *Диспетчер переноса объектов*
- *Приложение Корзина*
- *Веб-служба RESTful*
- *SAP BusinessObjects Mobile*
- *SAP Analytics Cloud*
- *Средство управления переводами*
- *Средство создания юниверсов*
- *Управление версиями*
- *Управление версиями*
- *Visual Difference*
- *Web Intelligence*
- *Веб-служба*
- *Workflow Assistant*

18.2.2 Общие настройки приложений

18.2.2.1 Настройка пользовательских прав на приложения

Для контроля доступа пользователей к некоторым функциям приложений можно использовать права. Область *Приложения* в CMC 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 BI*.

18.2.2.2 Настройка уровня журнала трассировки веб-приложения в CMC

Для трассировки других веб-приложений следует вручную сконфигурировать соответствующий файл `BO_trace.ini`.

1. В поле *Приложения* консоли CMC щелкните приложение правой кнопкой мыши и выберите *Настройки журнала трассировки*.

   > ⓘ Примечание
   >
   > Эти приложения имеют следующие параметры журнала трассировки: Стартовая панель BI в стиле Fiori, CMC, Открыть документ, Диспетчер переноса объектов, Управление версиями, Visual Difference и Веб-служба.

   Будет открыто диалоговое окно *Настройки журнала трассировки*.

2. Выберите параметр в раскрывающемся списке *Уровень журнала*.
3. Нажмите кнопку *Сохранить и закрыть*.
4. Перезапустите сервер веб-приложений.

Новый уровень журнала трассировки вступит в силу после следующего входа в данное веб-приложение.

Связанные сведения

Уровни журнала трассировки [страница 722]

18.2.2.2.1 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 `.ini`.
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	Нет отфильтрованных сообщений. Этот уровень рекомендуется для использования в целях отладки. ⚠ Предупреждение Этот уровень трассировки оказывает значительное влияние на ресурсы системы, повышая нагрузку на процессор и занимая место на диске.

18.2.3 Настройки, зависящие от приложения

18.2.3.1 Управление настройками приложения CMC

18.2.3.1.1 Аутентификация и программные объекты

Можно управлять типами программных объектов, которые могут запускать пользователи, и настраивать реквизиты пользователей, необходимые для запуска программных объектов.

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.

Включение и выключение типов программных объектов

В качестве первого уровня безопасности можно настроить доступные программные объекты.

Аутентификация на всех платформах

В области управления *Папки* консоли CMC 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.

Либо пользователи, которые добавляют программные объекты в службы информационной платформы, 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 удается выполнить, если не указаны реквизиты. Для предоставления реквизитов по умолчанию выберите *CMC* в области управления *Программные приложения*. В меню *Действия* выберите *Права для программного объекта*. Щелкните *Запланировать со следующими реквизитами операционной системы* и введите имя пользователя и пароль по умолчанию.

Аутентификация для программ Java

Службы информационной платформы позволяют настроить безопасность для всех программных объектов. Для программ Java службы информационной платформы обеспечивают 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 SAP BusinessObjects Enterprise Java SDK и предоставляет полные права доступа ко всем JAR-файлам SAP BusinessObjects Enterprise. Вторая запись на основе кодов применяется для всех локальных файлов. Она использует те же параметры безопасности для незащищенного кода, что и параметр по умолчанию для незащищенного кода.

> ⓘ Примечание
>
> Параметры политики Java являются общими для всех серверов выполнения программы, выполняющихся на одном компьютере.

> ⓘ Примечание
>
> По умолчанию файл политики Java устанавливается в каталог Java SDK в корневом каталоге установки служб информационной платформы. Например, типичное расположение в системе Windows: `C:\Program Files\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\conf\crystal-program.policy`

18.2.3.1.1.1 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 службы информационной платформы.
4. Нажмите кнопку *Сохранить и закрыть*.

> ⓘ Примечание
>
> При обновлении до платформы SAP BusinessObjects Business Intelligence 4.3 с пакетом поддержки 3 права на программные объекты по умолчанию отклоняются для всех пользователей. Их может активировать пользователь-администратор (или любой пользователь в группе администраторов).

В разделе *Выполнять программы Java* установлен флажок *Использовать анонимный режим*. В версии 4.3 с пакетом поддержки 3 флажок *Использовать анонимный режим* удален.

18.2.3.1.2 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, сервере обработки и сервере приложений отчетов (RAS). 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\win64_x64\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 группе серверов, необходимо только скопировать библиотеку на каждый сервер обработки в группе.

18.2.3.1.2.1 Регистрация расширения обработки в системе

1. Перейдите в область управления *Приложения* в CMC.
2. Выберите *Central Management Console*.
3. Выберите ▶ *Действия* ▶ *Расширения обработки* ▶.
   Появится диалоговое окно *Расширения обработки: CMC*.

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 CMC.

Теперь вы можете выбрать его, чтобы применить его логику к каким-либо объектам.

18.2.3.1.2.2 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 CMC, 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 CMC. Затем откройте "Свойства" сервера и введите необходимые данные в командной строке. По окончании снова запустите сервер.

18.2.3.1.3 Управление доступом к вкладкам CMC

18.2.3.1.3.1 Делегированное администрирование и доступ к вкладкам CMC

Системный администратор платформы BI 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 CMC. Системный администратор может управлять видимостью вкладок CMC 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 CMC, доступ к которым делегированному администратору не требуется.

> ⚠ Предупреждение
>
> Управление доступом к вкладкам CMC влияет только на внешний вид пользовательского интерфейса CMC. Скрытие вкладок CMC не может рассматриваться как мера 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).

Связанные сведения

Управление доступом других пользователей к вкладкам CMC [страница 729]

Управление разрешениями на настройку доступа других пользователей и групп к вкладкам CMC [страница 731]

18.2.3.1.3.2 Доступ к вкладкам CMC

18.2.3.1.3.2.1 Управление доступом к вкладкам CMC для других пользователей

Системный администратор обладает полным доступом ко всем вкладкам CMC. В следующем списке приводятся рекомендации по администрированию вкладок CMC, доступных принципалам:

- Чтобы упростить процесс управления и снизить частоту проведения процедур по обслуживанию и устранению неполадок, администраторам рекомендуется настраивать управление доступом к вкладкам CMC на уровне групп пользователей, а не отдельных пользователей.
- Для вкладок CMC, содержащих папки верхнего уровня, администратор должен предоставлять права на доступ к вкладкам и *Просмотр* непосредственно на папку верхнего уровня. Следующие вкладки CMC 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 CMC имеют только пользователи из группы "Администраторы": Пользователи из группы "Администраторы", которые по сути являются системными администраторами, имеют доступ к любой вкладке CMC независимо от установленных разрешений на доступ к вкладкам CMC. Разрешения на доступ к вкладкам CMC призваны контролировать доступ назначенных администраторов (то есть пользователей, не являющихся участниками группы "Администраторы") к вкладкам CMC.
  - *Аудит*

- *Аутентификации*
- *Криптографические ключи*
- *Лицензионные ключи*
- *Мониторинг*
- *Сеансы*
- *Параметры*
- *Управление пользовательскими атрибутами*

> ⚠ Предупреждение
>
> Управление доступом к вкладкам CMC влияет только на внешний вид пользовательского интерфейса CMC. Скрытие вкладок CMC не может рассматриваться как мера 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).

18.2.3.1.3.2.1.1 Управление доступом других пользователей к вкладкам CMC

1. Выполните вход в CMC.
2. На вкладке *Пользователи и группы* щелкните правой кнопкой мыши принципала и выберите пункт *Конфигурация вкладок CMC*.

   > ⓘ Примечание
   >
   > Если доступ к вкладкам CMC не ограничен, отображается следующее сообщение: `Предупреждение. Доступ к вкладке CMC не ограничен. Чтобы ограничить доступ к CMC, перейдите к вкладке "Приложение", выберите "CMC" и установите ограниченный доступ к вкладке CMC. Приведенные ниже настройки не будут применены, пока доступ к вкладке CMC не будет ограничен:` Права доступа к вкладкам CMC можно настраивать. Тем не менее, внесенные изменения вступят в силу только после того, как будет ограничен доступ к вкладкам CMC.

   В диалоговом окне *Конфигурация доступа к вкладкам CMC* отображается таблица:

   - Значки □ или □ обозначают вкладки CMC, к которым принципал 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 принципала.
3. Проверьте права доступа к вкладкам CMC. 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 принципала вступают в силу немедленно.

4. По окончании внесения изменений нажмите *Закрыть*.

В столбце *Разрешение* таблицы отображается действующее право доступа к вкладкам.

Связанные сведения

Ограничение доступа к вкладкам CMC [страница 733]

18.2.3.1.3.2.1.2 Наследование прав доступа к вкладкам CMC

Права на доступ к вкладкам CMC 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 BI. Например, если в одной из групп пользователю предоставляются права доступа к вкладкам CMC, а в другой – нет, пользователь соответствующие права не получает.

> ⓘ Примечание
>
> - Изменение прав доступа к вкладкам CMC 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.

18.2.3.1.3.2.1.3 Группы делегированных администраторов

Чтобы упростить управления вкладками CMC, модно создать набор групп делегированных администраторов. Назначив существующих пользователя или группу пользователя участником группы делегированных администраторов, вы сможете избежать необходимости настраивать доступ к отдельным вкладкам CMC. 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 *Юниверсы*. Всем остальным вкладкам присвойте атрибут *Унаследовано*.
Администраторы серверов	Доступ к вкладкам *Серверы* и *Приложения.* Всем остальным вкладкам присвойте атрибут *Унаследовано*.

18.2.3.1.3.2.1.4 Управление разрешениями на настройку доступа других пользователей и групп к вкладкам CMC

В крупных корпоративных средах у системного администратора может возникнуть необходимость делегировать функции управления доступом к вкладкам CMC 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 CMC.

1. Выполните вход в CMC.
2. На вкладке *Пользователи и группы* щелкните правой кнопкой мыши принципала и выберите пункт *Конфигурация вкладок CMC*.
   В диалоговом окне *Конфигурация доступа к вкладкам CMC* для принципала отображается *Разрешение на конфигурацию доступа к вкладке CMC для других пользователей или групп пользователей*.

   > **Примечание**
   >
   > Если это разрешение предоставлено, принципал имеет право на управление доступом к вкладкам CMC (распространяется только на доступные принципалу вкладки) для пользователей, на которых принципалу назначено право *Изменение прав в безопасном режиме*. Кроме того, такой принципал может делегировать права на управление доступом к вкладкам CMC другим пользователям. Для этого требуется предоставить *Разрешение на конфигурацию доступа к вкладке CMC для других пользователей или групп пользователей* пользователям, на которых принципалу назначено право *Изменение прав в безопасном режиме*.

   - Значки □ или □ указывают на наличие у принципала разрешений на конфигурацию доступа к вкладкам CMC для других пользователей или групп пользователей.

- *Унаследовано* – разрешение было унаследовано от родительской группы пользователей.
- *В явном виде* – разрешение было предоставлено явно на уровне принципала.

3. Проверьте разрешения на настройку доступа других пользователей и групп к вкладкам CMC. Чтобы изменить разрешения, выберите один из следующих параметров в списке:
   - Выберите *Предоставить*, чтобы явно предоставить разрешение на конфигурацию доступа к вкладкам CMC для других пользователей или групп пользователей.
   - Выберите *Запретить*, чтобы явно отозвать разрешение на конфигурацию доступа к вкладкам CMC для других пользователей или групп пользователей.
   - Выберите *Унаследовать*, чтобы унаследовать разрешение на конфигурацию доступа к вкладкам CMC для других пользователей или групп пользователей.

   > ⓘ Примечание
   >
   > Изменения разрешений принципала, выбранные в списке, вступают в силу немедленно.

4. По окончании внесения изменений нажмите *Закрыть*.

Отображается действующее на данный момент разрешение.

Связанные сведения

Делегированное администрирование и доступ к вкладкам CMC [страница 727]
Наследование прав доступа к вкладкам CMC [страница 730]

18.2.3.1.3.2.1.5 Добавление вкладки "Настройка" для пользователя или группы пользователей

Доступ к вкладке CMC должен быть «Ограничен» – только после этого можно будет добавить вкладку *Настройка* для определенного пользователя или группы пользователей.

1. В CMC перейдите в область управления *Пользователи и группы*.
2. Щелкните пользователя или группу пользователей правой кнопкой мыши и выберите *Конфигурация вкладок CMC*.

   Отобразится диалоговое окно *Конфигурация вкладок CMC*, на которой будет указано название каждой вкладки CMC и ее уровень разрешений для группы пользователей.

   Если вверху диалогового окна отобразится следующее предупреждение красным шрифтом, необходимо задать статус доступа к вкладке CMC "Ограничен" – только после этого можно добавить вкладку *Настройка*:

   ```
   Предупреждение. Доступ к вкладке CMC не ограничен. Чтобы ограничить доступ к
   CMC, перейдите к вкладке "Приложение", выберите "CMC" и установите ограниченный
   доступ к вкладке CMC. Приведенные ниже настройки не будут применены, пока доступ
   к вкладке CMC не будет ограничен:
   ```

3. (При необходимости) Ограничение доступа к вкладке CMC:

a. В области управления CMC *Приложения* щелкните правой кнопкой мыши *Central Management Console* и выберите *Конфигурация доступа к вкладкам CMC*.
b. В разделе *Доступ к вкладкам CMC* выберите *Ограничен* и щелкните *Сохранить и закрыть*.

4. В диалоговом окне *Настройка вкладок CMC* для соответствующей группы пользователей выберите для каждой вкладки CMC одно из следующих значений из списка: *Предоставлен*, *Запрещен* или *Унаследован*.
   Всякий раз при изменении разрешения для вкладки в диалоговом окне "Настройка вкладок CMC" обновляется разрешение группы пользователей на настройку доступа к вкладке других пользователей или групп пользователей.
5. Нажмите кнопку *Закрыть*.

18.2.3.1.3.2.2 Ограничение доступа к вкладкам CMC

Рекомендуется ограничить доступ к вкладкам CMC после того, как будут настроены права доступа к вкладкам CMC для принципалов. Если ограничить доступ к вкладкам до того, как он будет настроен, пользователи не смогут работать с любыми вкладками CMC, пока администратор не предоставит им соответствующие права.

Чтобы обеспечить согласованность конфигурации с предыдущими версиями платформы BI, доступ к вкладкам CMC после установки платформы BI изначально не ограничен, в связи с чем пользователи с правами доступа к CMC 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 CMC.

Ограничение на доступ к вкладкам CMC рекомендуется снимать только в экстренном случае или для устранения неполадок с конфигурацией доступа (например, если делегированному администратору не удается получить доступ к важной вкладке CMC).

1. Выполните вход в CMC.
2. На вкладке *Приложения* щелкните правой кнопкой мыши элемент *Central Management Console* и выберите пункт *Конфигурация доступа к вкладкам CMC*.
   Откроется диалоговое окно *Доступ к вкладке CMC*.
3. Настройте правила доступа к вкладкам CMC.
   - 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 CMC применяется к системе.

Связанные сведения

Устранение неполадок с доступом к вкладкам CMC [страница 734]

18.2.3.1.3.2.3 Устранение неполадок с доступом к вкладкам CMC

Чтобы запретить несанкционированный доступ или устранить неполадки, связанные с ограничением доступа пользователей к вкладкам CMC, можно изменить права доступа пользователей к вкладкам CMC.

1. Войдите в консоль CMC 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 CMC*.
   Откроется окно *Конфигурация доступа к вкладкам CMC*.
3. Проверьте действующие права доступа к вкладкам CMC. При необходимости вы можете явно предоставить или отозвать права доступа к доступным вкладкам.

   Если права доступа к вкладкам CMC 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 CMC на уровне принципала или ниже уровня группы.

   > ⓘ Примечание
   >
   > Выполнение этой задачи на уровне группы повлияет на права доступа к вкладкам CMC для всех пользователей, являющихся участниками этой группы, а также всех унаследованных от нее групп (если для этих пользователей настроен параметр прав доступа к вкладкам CMC *Унаследовано*).

4. По окончании внесения изменений нажмите *Закрыть*.

Связанные сведения

Управление доступом других пользователей к вкладкам CMC [страница 729]
Наследование прав доступа к вкладкам CMC [страница 730]

18.2.3.2 Управление настройками стартовой панели BI

В этом разделе описывается процесс управления следующими настройками на стартовой панели BI:

- Изменение настроек просмотра стартовой панели BI.
- Конфигурирование сведений URL-адреса службы RESTful в Central Management Console для входа на стартовую панель BI.
- Настройка видимости вкладки аутентификации и CMS на стартовой панели BI.
- Конфигурирование ссылки на электронную почту для параметра *Обратитесь к администратору* на стартовой панели BI.

18.2.3.2.1 Конфигурирование сведений URL-адреса службы RESTful в CMC для входа на стартовую панель BI в стиле Fiori

После установки или обновления BI 4.2 SP4 необходимо сконфигурировать URL-адрес веб-службы RESTful для пользователя, чтобы он мог входить на стартовую панель BI в стиле Fiori.

Чтобы сконфигурировать URL-адрес веб-службы RESTful в CMC, выполните следующие шаги:

1. Войдите в CMC как администратор.
2. Перейдите в *Управление* > *Приложения* > *Веб-службы RESTful* > *Свойства*.
3. Укажите WACS URL (имя хоста или полное имя места развертывания сервера WACS).

18.2.3.2.2 Настройка параметров прокси для включения Web Assistant на стартовой панели BI в стиле Fiori

После установки или обновления до BI 4.2 SP5 необходимо настроить параметры прокси для пользователя, чтобы он мог получить доступ к встроенной справке приложения Web Assistant на стартовой панели BI в стиле Fiori.

Чтобы настроить параметры прокси для Web Assistant на стартовой панели BI в стиле Fiori, выполните следующие шаги:

Предпосылки:

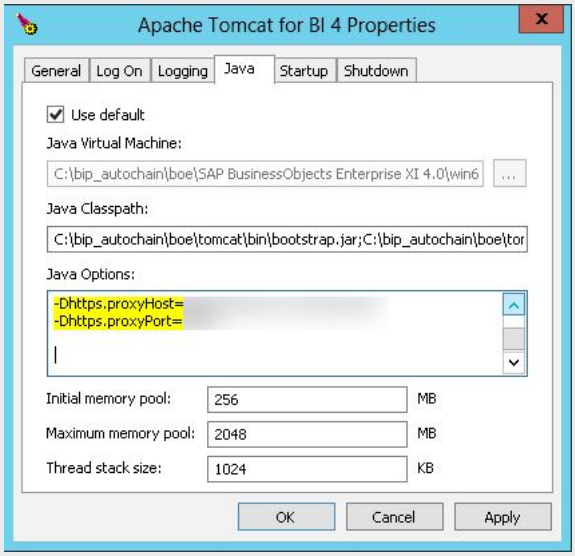
Наличие подключения к Интернету.

1. Перейдите к системным свойствам веб-сервера.
2. Добавьте свойства `https.proxyHost` и `https.proxyPort`.

> Пример
>
> ОС: Windows, Web Server: Tomcat 8.5
>
> 1. Выберите *Windows* > *Tomcat*.
> Откроется окно *Свойства Apache Tomcat для BI 4*.
> 2. Откройте вкладку *Java*.
> 3. В поле параметров Java добавьте в список следующие свойства:

```
-Dhttps.proxyHost=<proxy_host>
-Dhttps.proxyPort=<proxy_port>
```

4. Перезапустите Tomcat.



18.2.3.2.3 Конфигурирование ссылки на электронную почту для параметра "Обратитесь к администратору" на стартовой панели BI в стиле Fiori

Чтобы сконфигурировать ссылку на электронную почту для параметра *Обратитесь к администратору* на стартовой панели BI в стиле Fiori, выполните следующее:

1. Перейдите в папку `<INSTALLDIR>\SAP BusinessObjects Enterprise XI4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Если используется версия Tomcat, установленная на платформе BI, то можно осуществлять доступ к следующему каталогу: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEBINF\config\custom`.
2. Создайте новый файл с помощью программы "Блокнот" и сохраните его с именем: FioriBI.properties.
3. Измените в файле следующее свойство: `admin.user.email=administrator@bilp.com`, чтобы включить идентификатор электронной почты администратора.

18.2.3.2.4 Настройка видимости вкладки аутентификации и CMS на стартовой панели BI в стиле Fiori

Чтобы настроить видимость вкладки аутентификации и CMS на стартовой панели BI в стиле Fiori, выполните следующее:

1. Перейдите в папку `<INSTALLDIR>\SAP BusinessObjects Enterprise XI4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Если используется версия Tomcat, установленная на платформе BI, то можно осуществлять доступ к следующему каталогу: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEBINF\config\custom`.
2. Создайте новый файл с помощью программы "Блокнот" и сохраните его с именем: FioriBI.properties.
3. Чтобы включить в экран входа в систему стартовой панели BI параметры аутентификации, добавьте следующее: `authentication.visible=true`.

   Замените <authentication> на типы аутентификации по умолчанию: “secEnterprise, secLDAP, secWinAD, secSAPR3”.
4. Чтобы изменить тип аутентификации по умолчанию, добавьте следующее: `authentication.default=<authentication>`.
5. Чтобы запрашивать у пользователей имя CMS на экране входа на стартовую панель BI, добавьте следующую строку: `cms.visible=true`.
6. Сохраните и закройте файл.
7. Перезапустите сервер веб-приложений.

18.2.3.2.5 Для изменения параметров отображения стартовой панели BI

1. Перейдите к области *Приложения* в CMC и дважды щелкните *Стартовая панель BI*. Откроется диалоговое окно *Свойства стартовой панели BI*.
2. 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.
3. Щелкните *Сохранить и закрыть*.

18.2.3.3 Управление настройками Web Intelligence

Для документов Web Intelligence можно определить, к каким функциям будут иметь доступ пользователи, задав свойства для приложения Web Intelligence.

18.2.3.3.1 Изменение параметров отображения для Web Intelligence

1. Перейдите в область *Программные приложения* в CMC и выберите пункт *Web Intelligence*.
2. Щелкните ▶ *Управление* > *Свойства* ▶.
   Отобразится диалоговое окно *Свойства*.
3. Определите любой из следующих параметров отображения:

Параметр	Описание
▶ *Параметры отображения измененных данных* > ▶▶ *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 *OK*.
▶ *Параметры отображения измененных данных* > ▶▶ *Колеблющиеся значения (числовые показатели)* ▶	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 *OK*.
Свойства внедренного изображения	Введите максимальный размер внедренного изображения.
Поддержка географических карт	Включение или отключение поддержки географических карт в Web Intelligence.
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 закрытии документа вручную автоматически сохраненная копия документа удаляется.
Автоматическое обновление	Активирует автоматическое обновление документов Web Intelligence, если выбрано свойство документа Web Intelligence *Автоматическое обновление*. Для получения подробных сведений см. *Руководство пользователя SAP BusinessObjects Web Intelligence*.
Автоматическое слияние	Включение автоматического объединения измерений, если выбрано свойство документа Web Intelligence *Автоматическое объединение измерений*. Для получения подробных сведений см. *Руководство пользователя SAP BusinessObjects Web Intelligence*.
Автоматическое обновление документов в настройке права на открытие системы безопасности	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*.

Параметр	Описание
Smart View	Этот параметр определяет, какая версия документа будет отображаться, когда пользователи открывают документы в Web Intelligence. • Просмотреть последний экземпляр 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. • Просмотр объекта Документ открывается в том же состоянии, в котором он был сохранен в последний раз, независимо от выполненных запланированных обновлений.
JavaScript	Ваш выбор определяет визуализацию ячеек с параметром "Считывать содержимое как HTML" или "Считывать содержимое как гиперссылку" в документах Web Intelligence: • *Отключить JavaScript и включить гиперссылки и только элементы HTML, используемые Web Intelligence* Этот параметр по умолчанию включает гиперссылки и ограниченный набор элементов HTML, которые требуются для функций Web Intelligence. JavaScript и другие элементы HTML удаляются из документов. • *Включить только элементы HTML, определенные на странице "Разрешенные элементы HTML"* Этот параметр включает только элементы HTML и атрибуты, указанные на странице *Разрешенные элементы HTML*. • *Включить JavaScript, элементы HTML и гиперссылки* Этот параметр включает и JavaScript, и элементы HTML, и гиперссылки. Всякий раз, когда вы изменяете этот параметр, чтобы просмотреть изменения в Web Intelligence, выйдите из приложения и снова войдите в него. ⚠ Предупреждение • Web Intelligence активирует встроенный код JavaScript/HTML в ячейках документов с использованием формул. Этот код можно активировать и деактивировать в Central Management Console. Однако разрешая использование JavaScript, HTML и гиперссылки, вы признаете, что подвергаете себя риску межсайтового скриптинга. Межсайтовый скриптинг позволяет злоумышленникам изменять веб-сайты или выполнять код на других системах. Эта уязвимость затрагивает такие продукты, как интернет-браузеры, когда они выполняют скрипты. Большинство атак межсайтового скриптинга являются результатом небезопасного программирования на целевой системе. • Для точной настройки кода необходимо авторизовать теги HTML и атрибуты, выбрав *BI Admin Studio* > *Приложения* > *Элементы HTML*. Обратите внимание, что компания SAP не несет ответственности за совместимость этого кода и возможные побочные эффекты. Например, может потребоваться адаптировать код из-за обновлений браузера, поддержки версий JavaScript или способа динамического встраивания кода в веб-стра-

Параметр	Описание
	ницу. Для выполнения в этом новом контексте может потребоваться корректировка кода.
Выравнивание содержимого для новых документов	Используйте эти параметры, чтобы определить, необходимо ли выравнивание содержимого нового документа справа налево, слева направо либо в зависимости от предпочтительного языкового стандарта просмотра пользователя и/или языкового стандарта программного продукта.
Переключатель функций	Это текстовое поле используется для ввода переключателей для активации функций предварительного просмотра. Эти переключатели также можно использовать в SAP-нотах для изменения поведения по умолчанию. Этот список переключателей необходимо вводить как список формата JSON.

4. Нажмите кнопку *Сохранить и закрыть*.

> ⓘ Примечание
>
> Чтобы вернуть значения отображения по умолчанию, нажмите кнопку *Сброс*.

18.2.3.3.2 Сервисы пользовательских элементов

Пользовательские элементы – это визуализации, построение которых Web Intelligence делегирует внешним службам визуализации.

В документах Web Intelligence пользовательские элементы интегрируются и отображаются как любые другие элементы отчетов (диаграммы, таблицы и т. д.). Сервисы пользовательских элементов необходимо настроить на консоли CMC. До этого момента конечные пользователи не смогут визуализировать пользовательские элементы в документах Web Intelligence.

Так как данные будут перемещаться между сервером BOE и внешним сервером для пользовательских элементов, рекомендуется поднимать сервер пользовательских элементов во внутренней сети. Если это невозможно, для доступа к серверу пользовательских элементов рекомендуется использовать исключительно HTTPS.

> ⚠ Предупреждение
>
> Разворачиваемая служба пользовательских элементов добавляет код для Web Intelligence и может сгенерировать потенциальные проблемы безопасности, например, межсайтовый скриптинг. Межсайтовый скриптинг позволяет злоумышленникам выполнять коды и скрипты на ПК других пользователей. Предупреждение безопасности требует вашего прямого согласия перед развертыванием службы пользовательских элементов. Ваше согласие является обязательным для развертывания службы пользовательских элементов.

Миграция

При переносе документа Web Intelligence из одного CMS в другой, необходимо повторно создать сервис пользовательских элементов, использовавшийся для создания контента в этом документе, в

новом CMS под тем же именем. Если сервис не был воссоздан под тем же именем или вообще, пользовательские элементы в перенесенном документе будет невозможно изменить.

18.2.3.3.2.1 Добавление сервиса пользовательских элементов

Чтобы разрешить конечным пользователям работу с пользовательскими элементами, администратор сначала должен указать внешний сервис обработки визуализации. По умолчанию активированных сервисов пользовательских элементов нет. Эта настройка является необязательной и должна быть включена в CMC.

URL-адрес пользовательского сервиса уже добавлен в список доверенных URL-адресов. В противном случае обратитесь к разделу Добавление доверенных URL-адресов в список авторизованных URL-адресов [страница 746].

1. Откройте Central Management Console.
2. Нажмите *Приложения*.
3. Правой кнопкой мыши щелкните *Web Intelligence*.
4. Нажмите *Свойства*.
5. Нажмите *Пользовательские элементы*.
6. Нажмите кнопку *Добавить элемент*.
7. Укажите имя сервиса.

   > ⚠ Предупреждение
   >
   > Имя сервиса будет отображаться в клиентах Web Intelligence и должно быть уникальным. Нельзя использовать имена уже существующих сервисов. Если имя сервиса будет изменено, то изменение пользовательских элементов, созданных с помощью этого сервиса в документах Web Intelligence, станет невозможно.

8. Укажите адрес URL с номером порта.
9. Нажмите *Проверить*.
10. Выберите *Тип носителя*.

    В качестве типов носителя Web Intelligence поддерживает HTML и растровые изображения. Предпочтительным типом является HTML (text/html), который в клиентах Web Intelligence является интерактивным и обеспечен более удобным интерфейсом. Растровые носители должны быть представлены в формате .PNG (image/png), .JPG (image/JPG) или .GIF (image/gif).

11. Укажите *DPI изображения*.

    > ⓘ Примечание
    >
    > Это разрешение растрового изображения, генерируемого сервисом. Использование растрового формата необходимо для публикации отчетов Web Intelligence в виде файлов PDF и Excel, в которых пользовательские элементы представлены как рисунки. Если элементы представлены в другом формате (не растровом), вместо них в файле отображается пустое пространство.

12. Нажмите кнопку *OK*.

> **Примечание**
>
> Одновременно можно использовать несколько сервисов пользовательских элементов. Каждый сервис может поддерживать несколько пользовательских элементов.

Связанные сведения

Авторизация URL [страница 745]

18.2.3.3.3 Параллельное обновление поставщиков данных

Функция параллельного обновления поставщиков данных помогает эффективнее обновлять данные в документах Web Intelligence, содержащих несколько поставщиков данных.

Для параллельного обновления запросов Web Intelligence распределяет все поставщики данных по нескольким потокам. Эта функция активирована по умолчанию. Web Intelligence поддерживает параллельное обновление до 64 запросов. Поддерживаются поставщики данных, основанные на реляционных соединениях, соединениях OLAP и BICS, а также поставщики персональных данных (текстовые файлы, FHSQL).

> **Ограничение**
>
> Поставщики данных Excel не поддерживаются.

Если оборудование, на котором запущен Web Intelligence, не справляется, рекомендуется уменьшить это значение в Central Management Console. Для эффективной работы при такой нагрузке нужно проверить, что оборудование ее выдержит.

В Central Mangement Console представлено два глобальных параметра:

- *Максимальное количество параллельных запросов на документ*. Задает максимальное число поставщиков данных, которое Web Intelligence может обновлять параллельно для одного документа. По умолчанию задано значение 64.
- *Разрешить параллельные запросы при планировании*. Включает или отключает параллельную обработку запросов при планировании документов. Этот параметр установлен по умолчанию.

Кроме того, рекомендуется настроить соединение с базой данных с использованием параметра, который позволяет задавать максимальное число параллельно выполняемых запросов. Этот параметр называется "Максимальное количество параллельных запросов" и доступен в следующих местах:

- В Central Management Console или средстве дизайна информации для соединений OLAP и BICS.
- В средстве дизайна информации или средстве создания юниверсов для реляционных соединений.

Для каждого соединения по умолчанию настроено параллельное обновление до 4 поставщиков данных. Администратор базы данных может изменить это значение в соответствии с возможностями используемого оборудования. Для текстовых файлов этому параметру присваивается значение 1.

Пример

В этом примере используются значения по умолчанию, то есть каждое соединение поддерживает не более 4 параллельных заданий обновления.

Соединение	Число обновляемых поставщиков данных
2 соединения OLAP	6 (5 для соединения 1, 1 для соединения 2)
1 реляционное соединение	2
1 соединение BICS	2
Файл Excel из поставщика персональных данных	2

Оба файла Excel обновляются последовательно, поскольку функция параллельного обновления поставщиков данных не поддерживает их.

Четыре поставщика данных первого соединения OLAP обновляются параллельно в потоках 1, 2, 3 и 4. Пятый поставщик помещается в очередь и обрабатывается после того, как завершается обновление любого из поставщиков данных любого соединения. При этом поставщик из второго соединения OLAP обновляется отдельно в потоке 5, поскольку он принадлежит другому соединению.

4 поставщика данных для реляционного соединения и соединения BICS обновляются параллельно в потоках 5, 6, 7 и 8.

> ⓘ Примечание
>
> В случае, если число поставщиков данных одного типа превышает заданное значение, они ставятся в очередь и обновляются по завершении обновления других поставщиков.

Связанные сведения

Изменение количества параллельно обновляемых поставщиков данных для документа [страница 743]
Изменение количества параллельно обновляемых поставщиков данных для отдельного соединения OLAP [страница 744]

18.2.3.3.3.1 Изменение количества параллельно обновляемых поставщиков данных для документа

1. Выберите *Серверы* на домашней странице CMC.
2. Выберите *Службы Web Intelligence*.
3. Щелкните правой кнопкой мыши *Сервер обработки Web Intelligence* и выберите *Свойства*.
4. Введите значение в поле *Максимальное количество параллельных запросов*.

Допускаются значения в диапазоне от 0 до 64.

> ⓘ Примечание
>
> Если ввести значение 0, функция параллельного обновления поставщиков данных будет отключена.

18.2.3.3.3.2 Отключение параллельной обработки запросов при планировании

1. Выберите *Серверы* на домашней странице CMC.
2. Выберите *Службы Web Intelligence*.
3. Щелкните правой кнопкой мыши *Сервер обработки Web Intelligence* и выберите *Свойства*.
4. Снимите флажок *Разрешить параллельные запросы при планировании*.

18.2.3.3.3.3 Изменение количества параллельно обновляемых поставщиков данных для отдельного соединения OLAP

1. На домашней странице выберите *Соединения OLAP*.
2. Перейдите к соединению, которое требуется настроить, и щелкните его правой кнопкой мыши.
3. Выберите *Организовать* > *Изменить*.
4. Введите значение в поле *Максимальное количество параллельных запросов*.

   Допускаются значения в диапазоне от 1 до 64.

   > ⓘ Примечание
   >
   > Если ввести значение 1, поставщики данных будут обновляться последовательно.

18.2.3.3.4 Защита экспорта в CSV

Web Intelligence обеспечивает меры защиты во избежание ввода команды, когда пользователи открывают CSV-файл, созданный из документа в Microsoft Excel. Защиту для экспорта в CSV можно отключить.

При экспорте в CSV или архив CSV Web Intelligence по умолчанию добавляет пробел перед следующими символами :

- = (равно)

- + (плюс)
- - (минус)
- @ (в)

Дополнительный пробел не позволяет выполнять значения с такими символами как команды, которые вызовут проблемы с безопасностью в системе.

Связанные сведения

Отключение защиты для экспорта в CSV [страница 745]

18.2.3.3.4.1 Отключение защиты для экспорта в CSV

Если необходимо отключить в Web Intelligence защиту по умолчанию, которая препятствует вводу команды, когда пользователи открывают экспортированный файл CSV в Microsoft Excel, измените соответствующий ключ реестра.

Задайте для ключа реестра `EscapeCharactersForCSVExport` значение false, чтобы отключить защиту. По умолчанию этот ключ реестра отсутствует и для него установлено значение true, так что может потребоваться создать его, чтобы задать для него значение false.

Изменение вступит в силу, после того как пользователи Web Intelligence закроют и снова откроют приложение.

Измените ключ реестра, как указано ниже:

- В ОС Windows на компьютерах сервера и клиента задайте для ключа системного реестра значение false: `HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects\Suite XI 4.0\default\WebIntelligence\EscapeCharactersForCSVExport`.
- В ОС UNIX на компьютерах сервера в каталоге `$installdir/setup/boconfig.cfg` задайте для объявления ключа реестра значение false: `HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects\Suite XI 4.0\default\WebIntelligence\EscapeCharactersForCSVExport`.

18.2.3.3.5 Авторизация URL

В Web Intelligence URL-адреса используются в следующих случаях:

- Гиперссылки в документе
- Гиперссылки в указаниях подсказок
- Фоновое изображение
- Источник данных OData
- Пользовательские элементы или внешние расширения

Эти URL-адреса потенциально могут создавать угрозы безопасности.

Администратор должен создать в Central Management Console список доверенных URL-адресов, которые могут использовать пользователи. Данный список определяет использование этих URL-адресов в Web Intelligence.

18.2.3.3.5.1 Добавление доверенных URL-адресов в список авторизованных URL-адресов

Если требуется использовать URL-адрес в Web Intelligence в качестве гиперссылки в документе или указании подсказки, фоновом изображении, источнике данных OData либо новом пользовательском сервисе или внешнем расширении, сначала необходимо авторизовать его.

1. На начальном экране консоли Central Management Console щелкните элемент *Приложения*.
2. Выберите *Web Intelligence*.
3. В контекстном меню выберите *Свойства*.
4. Выберите раздел *Категория авторизованных URL*.
5. Нажмите кнопку *Добавить новый URL*, чтобы добавить доверенный URL-адрес.
6. В поле *Авторизованный URL* укажите уникальный URL-адрес с протоколом, именем хоста и портом.

   > → Совет
   >
   > Можно ввести символ *, чтобы авторизовать любой URL-адрес для гиперссылки, фонового изображения или источника данных OData. Затем необходимо установить флажок *Я принимаю риск*, чтобы подтвердить, что вы понимаете потенциальный риск активации всех URL-адресов.

7. Если введенный URL-адрес является URL-адресом для расширения или сервиса пользовательского элемента, к которому можно получить доступ через прокси, можно установить флажок *Если этот URL используется для пользовательского элемента или расширения, для которого требуется прокси, введите его сервер и порт*, чтобы задать этот прокси-сервер и порт.
8. Нажмите кнопку *OK*.

18.2.3.4 Управление настройками Crystal Reports

18.2.3.4.1 Включение Smart View в Crystal Reports

1. Перейдите к области *Приложения* в CMC и выберите пункт *Crystal Reports*.
2. Выберите *Управление* > *Свойства*
   Отобразится диалоговое окно *Свойства*.
3. Выберите *Стартовая панель BI*.
4. Задайте следующий параметр отображения:

Параметр	Описание
Smart View	Этот параметр определяет, какая версия документа будет отображаться, когда пользователи открывают Crystal Report. • Просмотреть последний экземпляр Будет открыт последний успешно выполненный экземпляр объекта. Например, если для документа запланировано обновление с периодичностью раз в час, а документ был сохранен и закрыт пять часов назад, открывается последний успешно выполненный экземпляр. • Просмотреть объект Документ открывается в том же состоянии, в котором он был сохранен в последний раз, независимо от выполненных запланированных обновлений.

18.2.3.4.2 Включение библиотеки пользовательских функций Java для Crystal Reports для Enterprise

Можно просмотреть и запланировать отчет, содержащий библиотеку пользовательских функций (UFL) Java. Выполните следующие шаги:

1. Войдите на консоль CMC.
2. В раскрывающемся списке выберите *Приложения*.
3. Выберите *Конфигурация Crystal Reports*.
4. На левой панели в разделе *Свойства* выберите *Crystal Reports для Enterprise*.
5. Выберите опцию *Добавить новый* и введите следующие свойства:

Свойство	Значение	Дополнительная информация
classpath	Путь класса к библиотекам UFL Java.	• В качестве разделителя нескольких JAR-файлов используйте точку с запятой. • Используйте двойную обратную косую черту (\\) или обычную косую черту (/). • Пример: C:\\Program Files (x86)\\SAP BusinessObjects\\SAP BusinessObjects Enterprise XI 4.0\\java\\lib\\MyFirstUFL.jar

Свойство	Значение	Дополнительная информация
ExternalFunctionLibraryClassNames.classname	Полное имя UFL.	Пример: samples.ufl.InternationalizationLibrary

6. Перезапустите службы, связанные с Crystal Reports.
   Теперь вы можете просматривать и планировать потоки операций.

18.2.3.4.3 Включение библиотеки пользовательских функций .NET/COM для Crystal Reports для Enterprise

Можно просмотреть и запланировать отчет, содержащий библиотеку пользовательских функций (UFL) .NET/COM. Выполните следующие шаги:

1. Скопируйте 64-разрядную версию .Net UFL в каталог `<Install Directory>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.

   > ⓘ Примечание
   >
   > Конструктор Crystal Reports для Enterprise является 64-разрядным и, следовательно, требует 64-разрядной библиотеки .NET UFL, при этом службы Crystal Reports для Enterprise на платформе Business Intelligence являются 64-разрядными и, следовательно, требуют 64-разрядной библиотеки .NET UFL.

2. Зарегистрируйте и добавьте в глобальный кэш сборок (GAC) 64-разрядную библиотеку dll, используя "regasm <dll>" и "gacutil /if <dll>".
3. Войдите на консоль CMC.
4. В раскрывающемся списке выберите *Приложения*.
5. Выберите *Конфигурация Crystal Reports*.
6. На левой панели в разделе *Свойства* выберите *Crystal Reports для Enterprise*.
7. Выберите опцию *Добавить новый* и введите следующее свойство:

Категория	Свойство	Значение
Оставьте этот столбец незаполненным.	NonJavaExternalFunctionLibraries.managerDirectory	Путь к 64-разрядному файлу UFL. • Используйте двойную обратную косую черту (\\) или обычную косую черту (/). • Пример: C:\\Program Files (x86)\\SAP BusinessObjects\\SAP BusinessObjects Enterprise XI 4.0\\win64_x64).

8. Перезапустите службы, связанные с Crystal Reports.
   Теперь вы можете просматривать и планировать потоки операций.

18.2.3.5 Управление настройками предупреждений

В области *Приложения* CMC платформы BI можно задать для оповещений 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

Связанные сведения

Настройка пользовательских прав на приложения [страница 721]

18.2.3.5.1 Изменение свойств места назначения предупреждений

1. В области *Приложения* в CMC дважды щелкните *Приложение предупреждения*.
2. Выберите команду *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 BI.
   - 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. Щелкните *Сохранить и закрыть*.

Связанные сведения

Настройка пользовательских прав на приложения [страница 721]
Управление настройками предупреждений [страница 749]

18.2.3.5.2 Изменение свойств предупреждений по умолчанию

1. Перейдите к области *Приложения* в CMC 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*.

Связанные сведения

Управление настройками предупреждений [страница 749]

18.2.3.6 Управление настройками приложения BI Commentary

BI Commentary — это новое приложение в CMC. Оно позволяет пользователям совместно комментировать любые данные или статистику в документе.

Благодаря BI Commentary пользователи могут оставлять комментарии к данным или статистике в отчетах.

→ Рекомендация

По умолчанию BI Commentary создает и ведет свои таблицы в базе данных аудита.

ⓘ Примечание

Чтобы использовать BI Commentary с БД аудита на платформах не на базе ОС Windows, см. Руководство по доступу к данным. для конфигурации драйверов ODBC.

Однако SAP рекомендует настроить новую базу данных для хранения комментариев из приложения BI Commentary. BI Commentary поддерживает работу с теми же базами данных которые поддерживаются для аудита. Поддерживаемые базы данных и соответствующие сертифицированные JAR-файлы JDBC для комментариев BI (неполный список):

- IBM DB2 Workgroup Edition - db2jcc4.jar
- Microsoft SQL Server - sqljdbc4.jar
- MySQL - com.mysql.jdbc_5.1.5.jar
- Oracle - ojdbc6.jar
- SAP HANA - ngdbc.jar
- Sybase Adaptive Server Enterprise - jconn4.jar
- Sybase SQL Anywhere - jconn4.jar

ⓘ Примечание

Независимо от того, выбрана ли конфигурация BI Commentary с базой данных аудита или другой поддерживаемой базой данных, для работы BI Commentary с базой данных MySQL необходимо поместить JAR-файл JDBC MySQL в следующее местоположение: `<КАТАЛОГ_УСТАНОВКИ\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\BICommentaryService\lib>`.

Для настройки BI Commentary с использованием IBM DB2 требуется следующий размер страниц для временного табличного пространства: 8K, 16K или 32K. Размер страницы по умолчанию — 4K.

ⓘ Примечание

Если база данных аудита по умолчанию не настроена или не включена, то приложение BI Commentary не будет работать, пока вы вручную не настроите для него новую базу данных.

Если BI Commentary настраивается с базой данных аудита и база данных аудита удаляется, все комментарии, сохраненные в базе данных аудита, также будут удалены.

При работе с базой данных для аудита используются ODBC или собственные драйверы базы данных. Чтобы настроить новую базу данных Commentary, требуется драйвер JDBC.

> ⓘ Примечание
>
> Размер комментария не может превышать 2000 символьных разрядов в кодировке UTF-8 или 666 символьных разрядов в кодировке UTF-16.

> ⓘ Примечание
>
> Перенести комментарии с помощью средства объединения данных невозможно.

> ⓘ Примечание
>
> BI Commentary не поддерживается для соединений MaxDB.

> ⓘ Примечание
>
> Чтобы удалить записи комментариев, сделанные пользователем, используйте следующий запрос:
>
> `DELETE from dba.COMMENTARY_MASTER where UserName ='<User Name>'`

18.2.3.6.1 Настройка новой базы данных для BI Commentary

Создано соединение JDBC.

> ⓘ Примечание
>
> При настройке новой базы данных для BI Commentary за запись информации из Commentary в базу данных отвечает сервис Commentary, расположенный на адаптивном сервере обработки. Для каждого компьютера в кластере, где выполняется сервис Commentary, необходимо предпринять следующие шаги.

Чтобы создать новое соединение JDBC, выполните следующее:

1. Поместите JDBC-файл .jar для настраиваемой базы данных в следующее местоположение: `<INSTALL_DIR\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\BICommentaryService\lib>`.

   > ⓘ Примечание
   >
   > Если выполняется обновление до версии SAP BusinessObjects Business Intelligence Platform 4.2 с пакетом поддержки 2 и уже сконфигурирована новая база данных BI Commentary из ранних версий, переместите файл драйвера для базы данных из папки ‘jdbc’ folder по адресу `<INSTALL_DIR\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib\external>` в папку `<INSTALL_DIR\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\BICommentaryService\lib>`.

2. Перезапустите SIA.

Чтобы настроить новую базу данных для BI Commentary, выполните следующие действия:

1. Войдите в CMC.
2. В раскрывающемся меню на главной странице CMC выберите *Приложения*.
3. В списке *Имя приложения* выберите *Приложение BI Commentary*.

   Появится всплывающее окно *BI Commentary*. По умолчанию выбран переключатель *Использовать базу данных аудита*.
4. Выберите переключатель *Использовать другую поддерживаемую базу данных*.
5. Заполните поля *Тип*, *Имя базы данных*, *Хост*, *Порт*, *Имя пользователя* и *Пароль* на панели *Настройка базы данных для комментариев*.
6. Нажмите кнопку *Сохранить и закрыть*.
7. Перезапустите APS.

   Все изменения в конфигурации БД BI Commentary будут применены только при перезапуске Adaptive Processing Server (APS).

   Чтобы выполнить проверку соединения, нажмите *Проверить соединение*.

   > ⓘ Примечание
   >
   > Если выполняется обновление более ранних версий до версии платформы SAP BusinessObjects Business Intelligence 4.3 с пакетом поддержки 3 и уже настроена база данных для BI Commentary для JDBC, то при выборе *Проверить соединение*, *Сохранить и закрыть* или *Сохранить* поле пароля теперь станет пустым.

   Вы можете удалить или очистить старые комментарии, установив флажок *Удалить все комментарии старше* и указав нужное количество дней.

   > ⓘ Примечание
   >
   > Чтобы изменения вступили в силу, необходимо перезапустить все серверы APS, на которых размещается служба BI Commentary.

Новая база данных для хранения комментариев из приложения BI Commentary настроена.

18.2.3.7 Управление настройками приложения BI Admin Studio

> ⓘ Примечание
>
> Правом доступа к BI Admin Studio обладают пользователи, входящие в группу администраторов.

При отсутствии у пользователя определенных прав доступа, таких как: *Разрешить доступ к рабочему месту администратора BI*, *Разрешить доступ к мониторингу* и *Разрешить доступ к Visual Difference*, доступ к конкретному приложению в BI Admin Studio может быть запрещен.

Specific Rights for BI Admin Studio	Implicit Value
Allow access to BI Admin Cockpit	Granted
Allow access to Monitoring	Granted
Allow access to Visual Difference	Granted
Visual Difference - Create comparison	Granted
Visual Difference - Delete comparison	Granted
Visual Difference - Rerun comparison	Granted
Visual Difference - View comparison	Granted

При отсутствии прав доступа к *Visual Difference* можно также ограничить использование приложения VD.

18.2.3.8 Управление интеграцией приложений сотрудничества

Это руководство предназначено для администраторов платформы BI, отвечающих за ее интеграцию с приложением сотрудничества SAP Jam.

Для включения и настройки сотрудничества используйте область *Приложения* в Central Management Console (CMC) платформы BI.

В агенте Enterprise Agent приложения сотрудничества необходимо выполнить следующую дополнительную настройку:

- Установить соединение HTTPS с поставщиком услуг.
- Выполнить предварительные требования для аутентификации.

После настройки SAP Jam каналы из приложения сотрудничества будут доступны в приложении стартовой панели BI.

SAP Jam не поддерживает Microsoft Internet Explorer 11.

18.2.3.8.1 Предварительные условия для сотрудничества

Перед интеграцией платформы BI с приложением сотрудничества должны быть выполнены предварительные требования для сотрудничества.

- Установлена платформа BI как минимум с одним Центральным сервером управления (CMS).
- Приложение сотрудничества (SAP Jam) настроено в компоненте Central Management Console (CMC).
- Определена организация Enterprise для приложения сотрудничества (SAP Jam).
- В организацию Enterprise добавлены пользователи SAP Jam.
- Агент Enterprise Agent для SAP Jam необходим для подготовки среды для пользователей, использующих локальную службу каталогов LDAP/AD.

18.2.3.8.2 Конфигурация платформы BI

18.2.3.8.2.1 Параметры настройки сотрудничества

Параметры настройки сотрудничества выводятся в диалоговом окне *Свойства: сотрудничество* в Central Management Console (CMC) платформы BI.

Чтобы открыть диалоговое окно *Свойства: сотрудничество*,, на вкладке *Приложения* в CMC щелкните *Сотрудничество* и выберите *Управление* > *Свойства*.

Параметр	Описание
Включить сотрудничество	Установите этот флажок и выберите приложение *SAP Jam*.
URL соединения	Введите URL приложения сотрудничества.
Уникальный идентификатор поставщика сущности	Введите уникальное значение для развертывания платформы BI. Это значение будет связано с сертификатом, используемым для настройки интеграции в консоли администрирования приложения сотрудничества. Приложение, добавляющее сущность для единого входа, должно быть настроено как приложение администрирования OAuth.
Сертификат Base64 поставщика сущности	После нажатия кнопки *Сгенерировать* в этом поле создается сертификат. Используйте этот сертификат в консоли администрирования приложения сотрудничества для создания ключа потребителя OAuth. 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	Введите ключ потребителя OAuth, созданный в консоли администрирования приложения сотрудничества.
Подключение через прокси	Установите этот флажок, чтобы включить соединение через прокси, и введите информацию о хосте прокси-сервера в поля *Хост прокси HTTP* и *Порт*. Чтобы разрешить входящие соединения от серверов приложений сотрудничества с корпоративной сетью, требуется обратный прокси в демилитаризованной зоне (DMZ). Для добавления доверенного сертификата от поставщика сертификатов SSL на обратный прокси вам потребуется имя домена или поддомена для обратного прокси.

Параметр	Описание	
	Хост прокси HTTP	В настройках обратного прокси введите внешний адрес, доступный для приложения сотрудничества. Например, введите `https://<ReverseProxy>/`, где `<ReverseProxy>` – это имя домена или поддомена обратного прокси. 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.
	Порт	Агент Enterprise Agent приложения сотрудничества настраивается для прослушивания порта 8443.

18.2.3.8.2.2 Включение и настройка сотрудничества в CMC

Для выполнения этой задачи требуется действующее соединение с консолью администрирования приложения сотрудничества (SAP Jam). Потребуется передавать в консоль данные о безопасности и извлекать их оттуда.

В целях безопасности следующим учетным записям по умолчанию запрещено отправлять или планировать содержимое в SAP Jam:

- Гость
- SMAdmin
- Администратор
- WaaWSServletPrincipal

1. В консоли CMC 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*.
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 выведен сертификат. Этот сертификат будет использоваться для настройки приложения сотрудничества.
6. В поле *Ключ потребителя OAuth* введите действительный ключ потребителя OAuth.
7. Если соединение с сервером SAP Jam осуществляется через прокси-сервер, 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 сервера.

8. Нажмите кнопку *Сохранить и закрыть*.

18.2.3.8.3 Конфигурация SAP Jam

18.2.3.8.3.1 Регистрация нового доверенного IDP SAML для SAP

Каждый пользователь должен быть зарегистрирован с использованием уникального адреса электронной почты, соответствующего адресу Enterprise пользователя в стартовой панели BI. Адреса электронной почты платформы BI и SAP Jam сопоставляются.

Перед регистрацией нового доверенного IDP SAML:

- Необходимо добавить и настроить компанию в SAP.
- Необходимо создать действительную учетную запись пользователя SAP, связанную с вашей компанией в SAP.
- Необходимо получить права администратора компании в SAP и полные права администратора платформы BI и стартовой панели BI.
- Стартовая панель BI должна быть зарегистрирована в качестве клиента OAuth, который является ее представлением в SAP.

SAP Jam не поддерживает Microsoft Internet Explorer 11.

1. В правом верхнем углу Central Management Console (CMC) платформы BI выберите *Администратор*, а затем выберите *Администрирование*.
   На экран будут выведены сведения о вашей компании, включая лицензию SAP. Запишите или иначе сохраните эту информацию.
2. В меню *Администрирование* выберите *Доверенные ИД SAML*, а затем выберите *Регистрация поставщика удостоверений*.
   Необходимо зарегистрировать IDP, созданный в стартовой панели BI.
3. В поле *ИД IDP* введите уникальное значение поставщика удостоверений, созданное при настройке SAP на 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.
   SAP использует этот URL для единого входа с помощью уникального поставщика удостоверений.
5. В поле *URL для единого выхода* введите URL, который будет отображаться при выходе из SAP.
   SAP использует этот URL для единого выхода с помощью 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 принципала службы для идентификатора имени по умолчанию* введите квалификатор имени принципала, который будет использоваться в запросах аутентификации.

8. В списке *Разрешенный объем утверждений* выберите *Пользователи в моей компании*.

   Этот параметр определяет набор пользователей, для которых SAP будет принимать утверждения от IDP.

9. В поле *Сертификат X509 (Base64)* введите значение сертификата Base64, созданное при настройке SAP на платформе BI.

   Если это значение неизвестно, обратитесь к администратору внешних приложений.

10. Нажмите кнопку *Зарегистрировать*.

18.2.3.8.3.2 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 иметь 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.
- Каждый пользователь должен быть зарегистрирован в SAP Jam с использованием уникального адреса электронной почты, соответствующего адресу Enterprise пользователя в стартовой панели BI. Адреса электронной почты в платформе BI и SAP Jam сопоставляются.

SAP Jam не поддерживает Microsoft Internet Explorer 11.

1. В верхнем правом углу в меню *Администратор* SAP Jam выберите пункт *Администратор*.
   На экран будут выведены сведения о вашей компании, включая лицензию SAP Jam.
2. В меню *Администрирование* выберите *Клиенты OAuth*, а затем выберите *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 для стартовой панели BI.

   При выполнении действий от имени пользователя в SAP Jam имя приложения отображается в виде гиперссылки на 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.

18.2.3.9 Управление сервисом push-уведомлений в SAP BusinessObjects Mobile

Сервер SAP BusinessObjects Mobile отправляет push-уведомления на устройства iOS пользователей приложения SAP BusinessObjects Mobile. Уведомления используются в следующих случаях:

- Когда документы BI, загруженные на пользовательское устройство, обновляются или на сервере доступен новый экземпляр документа.
- Когда в папку входящих BI поступает новый документ.
- Когда платформа BI или администратор BOE рассылает сообщение.

Уведомления автоматически направляются на устройство с сервера Mobile через сервер уведомлений Apple Push Notification Server (APNS). Для получения push-уведомлений подключение к серверу не требуется. Пользователь получит push-уведомление даже в том случае, если приложение не запущено. В приложении необходимо включить "Настройки уведомлений". Для получения дополнительной информации о настройке push-уведомлений см. *Руководство по развертыванию и конфигурированию сервера Mobile* для Mobile Server 4.2.

> ⓘ Примечание
>
> Чтобы разрешить получение push-уведомлений на мобильное устройство, нужно запустить BIMobileService в APS.
>
> Во время работы BIMobileService не занимает большой объем памяти, так что его можно запускать одновременно с другими сервисами в APS.

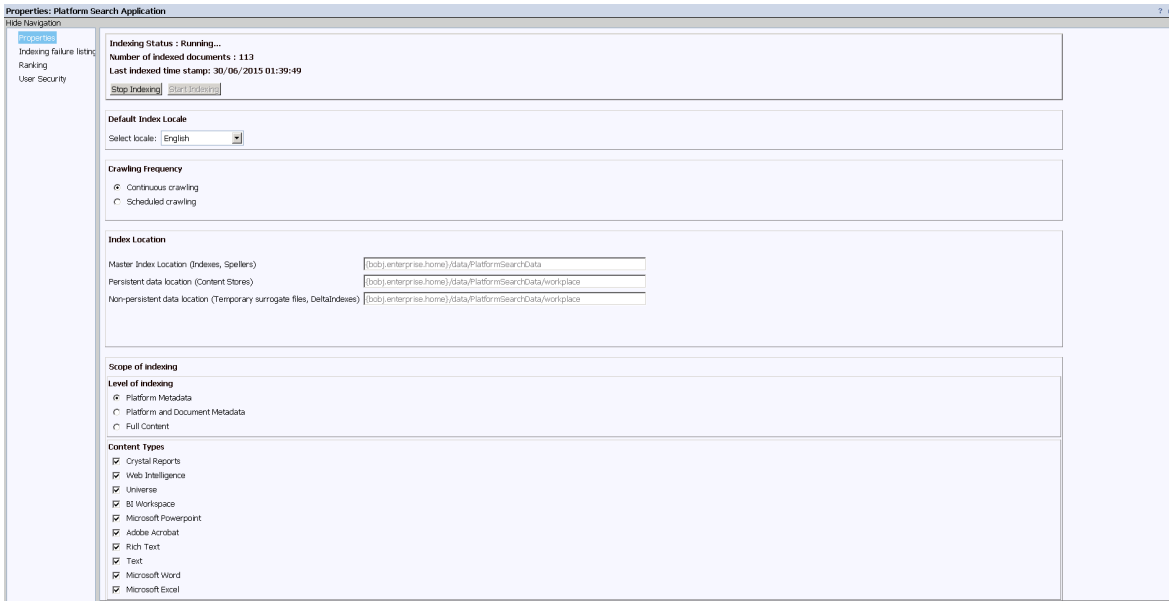
18.2.3.10 Управление настройками поиска по платформе

В области *Приложения* CMC платформы BI можно задать настройки на уровне системы для приложения поиска по платформе.

18.2.3.10.1 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:

Параметр	Описание
Статистика поиска	Поиск по платформе предлагает следующие статистики поиска: • Состояние индексации — состояние процесса индексации • Число проиндексированных документов — число документов, для которых индексация выполнена. • Метка времени последней индексации — метка 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 CMC 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 CMC.

Параметр	Описание
Периодичность поиска	Индексацию всего репозитория платформы BI можно выполнить, используя следующие параметры: • 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 для индексирования документа. • Плановый обход: при выборе этого варианта индексация выполняется на основании расписания, задаваемого настройками "Расписание". Для получения дополнительных сведений о включении объектов в расписание см. раздел *Планирование объекта* справки по поиску по платформе в *Интерактивной справке CMC по платформе SAP BusinessObjects Business Intelligence*. **Примечание** • 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.

Параметр	Описание
Расположение индекса	Индексы хранятся в общих папках в следующих местах: • 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. 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. 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: 1. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Имя сервера>\ContentStores. 2. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Имя сервера 1>\ContentStores. • 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. **Примечание** • Расположение основного индекса должно быть общим каталогом. • 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.

Параметр	Описание
	> • В индексных файлах может содержаться личная и конфиденциальная информация, особенно когда вы выбираете индексацию содержимого документа. Доступ к общей папке необходимо разрешить только системному пользователю, и во избежание хищения данных общие папки следует хранить в зашифрованной среде.

Уровень индексации	Можно выполнить настройку содержимого поиска, задав уровень индексации следующим образом:
	• Метаданные платформы: индекс создается только для метаданных платформы, таких, как заголовки, ключевые слова и описания документов. Этот параметр выбран по умолчанию.
	• Метаданные платформы и документов: этот индекс включает метаданные платформы и метаданные 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:
	  • Фактическое содержимое документа
	  • Содержимое подсказок и списков значений
	  • Диаграммы, графики и метки
	> **Примечание**
	> Полное индексирование содержимого не поддерживается для документов Analysis Office и Lumira. Полное индексирование содержимого не поддерживается для документов Analysis Office и Lumira.
	> **Примечание**
	> При изменении уровня индексации процесс индексации инициализируется заново для всего репозитория платформы BI.

Параметр	Описание
Типы содержимого	Для индексирования могут быть заданы следующие типы содержимого. • Crystal Reports • Web Intelligence • Юниверс • Рабочее пространство BI • Analysis Office • Lumira • Microsoft PowerPoint • Adobe Acrobat • Формат RTF • Текст • Microsoft Word • Microsoft Excel Фильтр типа содержимого не применяется для индексирования метаданных платформы. Независимо от выбранных типов содержимого индексирование метаданных платформы выполняется для всех поддерживаемых типов объектов и результаты поиска на стартовой панели BI возвращают по ключевому слову все объекты, связанные с метаданными платформы. Фильтр типа содержимого релевантен для индексирования метаданных документов (автор документа, заголовок документа, нижний колонтитул документа и т. д.) и индексирования содержимого (графики, диаграммы, таблица с отчетом). В зависимости от выбранного уровня индексирования и типов содержимого поиск на платформе индексирует метаданные и содержимое документов для выбранных типов объектов из репозитория и только эти объекты отображаются в результатах поиска на стартовой панели BI при поиске по ключевому слову, связанному с метаданными и содержимым документа.
Перестроить индекс	Эта функция удаляет все существующие индексы и повторно индексирует весь репозиторий. 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. Чтобы отказаться от повторной индексации документов, снимите флажок *Перестроить индекс* перед нажатием кнопки *Начать индексацию*.

Параметр	Описание
Документы, исключенные из индексации	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. 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. 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*: • Права просмотра и редактирования категории • Непосредственное редактирование документа
Другая конфигурация – Пропуск экземпляра	По умолчанию экземпляры документов выбраны для индексирования. Это увеличивает размер индекса и повышает использование дискового пространства. Размер папки "Lucene Index Engine" в папке PlatformSearchData разрастается из-за индексирования огромного количества экземпляров в репозитории. При наличии в системе миллионов документов (или больше), многие из которых также имеют огромное число существующих экземпляров (наряду с плановым генерированием экземпляров с регулярным интервалом) размер папки "Lucene Index Engine" чрезмерно разрастается даже при установленном уровне индексирования "Метаданные платформы". Функция поиска по платформе "Пропуск экземпляра" позволяет включать и выключать индексирование экземпляров с помощью флажка в разделе "Другая конфигурация – Пропуск экземпляра" на странице свойств приложения поиска по платформев CMC. **Примечание** • В случае включения/отключения пропуска экземпляра необходимо перезапустить адаптивный сервер обработки поиска по платформе. Это изменение влияет на все уровни индексирования. • Если при изменении пропуска экземпляра требуется применить изменения ко всем существующим экземплярам (т. е. подлежащим выбору для индексирования), необходимо перестроить индекс.

Параметр	Описание
Исключенные из индексирования объекты	Параметр *Исключенные из индексирования объекты* позволяет исключить из индексирования некоторые объекты. Например, чтобы избежать перегрузки сервера приложений отчета, может потребоваться отключение функции поиска в некоторых объектах. Исключение конкретных объектов позволяет заблокировать доступ к ним при поиске по платформе. Важно отметить, что объект, проиндексированный до того, как был отнесен к данной группе, все еще может быть доступен для поиска. Чтобы объекты, отнесенные к категории *Исключенные из индексирования объекты*, были гарантированно недоступны для поиска, необходимо перестроить индекс. Список объектов, которые можно исключить из индексирования: • CrystalReport • Webi • LCMJob • Universe • Excel • PDF • PowerPoint • RTF • TXT • Word • AFDashboardPage • ObjectPackage • QaaWS • Profile • Event • Discussions • InformationDesigner • MDAnalysis • Publication • Agnostic • Analytics • Hyperlink • Program • pQuery • DSL.MetaDataFile • Shortcut • DataDiscoveryAlbum • AO.Workbook • VISI.Story

Параметр	Описание
	• VISI.Dataset • VISI.Lums • VISILums • User • UserGroup

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.

18.2.3.11 Настройка веб-интеграции BEx

Веб-приложения BEx представляют собой веб-приложения Business Explorer (BEx) для SAP Business Warehouse (BW) и предназначаются для анализа данных, отчетности и аналитических приложений в Интернете.

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 BI. Авторы веб-приложений BEx могут выполнять веб-приложения непосредственно в стартовой панели BI в конструкторе веб-приложений BEx.

Для интеграции веб-приложений BEx с платформой BI выполните следующие действия по настройке:

1. Настройте сервер для веб-приложений BEx в Central Management Console (CMC).

   Для веб-приложений BEx можно использовать общий или отдельный сервер.

   > **→ Совет**
   >
   > Рекомендуется настроить для веб-приложений BEx отдельный сервер, поскольку на общем сервере, как правило, выполняются многие другие службы.

2. Настройте параметры сервера.
3. Проверьте 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 BI пользователи смогут открывать веб-приложения BEx в стартовой панели BI. Здесь они могут переходить к данным и сохранять веб-приложения BEx как избранные страницы в веб-браузере.

> **⚠ Ограничение**
>
> 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 BI, могут содержать только такие источники данных, которые хранятся в главной системе BW. В параметрах администрирования системы определяется, какая система будет выбрана в качестве главной системы BW в платформе BI.
> Единый вход для платформы BI и SAP NetWeaver BW не включен. Для каждого сеанса работы в платформе BI пользователям веб-приложений BEx необходимо выполнить вход в соответствующую главную систему BW.
> Интерфейс "отчет-отчет" из веб-приложений BEx и в веб-приложения BEx не поддерживается. Соответствующие команды не будут выполняться.
> Инструментальные панели на основе запросов или представлений запросов BEx, созданные в SAP BusinessObjects Dashboards, не поддерживаются.

Подробнее о возможностях веб-приложений BEx см. на портале SAP Help Portal по адресу 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.

Связанные сведения

Запуск сервера для веб-приложений BEx [страница 769]
Запуск отдельного сервера для веб-приложений BEx [страница 769]
Настройка параметров сервера [страница 769]
Проверка соединения с системой BW [страница 770]
Настройка соединения между конструктором веб-приложений BEx и платформой BI [страница 771]

18.2.3.11.1 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 BEx* из списка *доступных служб* в список служб справа.
6. Перезапустите службу веб-приложений BEx, перезапустив настраиваемый сервер обработки.

18.2.3.11.2 Запуск отдельного сервера для веб-приложений BEx

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 BEx* в списке *доступных служб* и переместите ее в список служб справа.
8. Запустите службу веб-приложений BEx, запустив новый настраиваемый сервер обработки.

18.2.3.11.3 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 BEx, а затем в контекстном меню выберите команду *Свойства*.
5. В разделе *Конфигурация службы веб-приложений BEx* в области *Служба веб-приложений BEx* настройте следующие параметры:
   a. Проверьте (и при необходимости измените) максимальное число сеансов работы клиентов.
   b. В разделе *Главная система SAP BW* введите имя соединения OLAP с системе BW, созданной в платформе BI. Имя по умолчанию – *SAP_BW*.

c. В поле *RFC-адресат JCo-сервера* введите имя, которое было введено в системе BW в разделе *Конфигурация RFC-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 BEx, а затем в контекстном меню выберите команду *Перезапустить сервер*.

   Для применения выбранных параметров требуется перезапустить сервер.

> ⓘ Примечание
>
> Перед перезапуском сервера необходимо убедиться, что создан RFC-адресат в системе ABAP.

Связанные сведения

Создание RFC-адресата в системе ABAP [страница 771]

18.2.3.11.4 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-адресата 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.
>
> 1. Для этого щелкните соединение с системой BW правой кнопкой мыши (по умолчанию его имя – **SAP_BW**) и выберите в контекстном меню команду *Безопасность пользователя*.
> 2. Настройте требуемые параметры безопасности, по возможности предоставляя права доступа только администраторам.

18.2.3.11.5 Настройка соединения между конструктором веб-приложений BEx и платформой BI

Чтобы обеспечить авторам возможность выполнять веб-приложения BEx непосредственно в стартовой панели BI из конструктора веб-приложений BEx, необходимо настроить соответствующие параметры в таблице *Подключенные порталы* (**RSPOR_T_PORTAL**) в системе BW.

1. В системе BW вызовите транзакцию **SM30** (*Сопровождение табличного представления*).
2. В поле *Таблица/Представление* введите значение **RSPOR_T_PORTAL**.
3. Нажмите кнопку *Сохранить*.
4. Чтобы создать новую запись, нажмите кнопку *Новые записи*.
5. Настройте следующие параметры:
   a. Чтобы обеспечить интеграцию между системой BW и платформой BI, нужно создать RFC-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 BI.
   c. В поле *Префикс URL* введите URL-адрес сервера WACS, включая протокол, имя хоста и порт, например **http://<wacs><домен>:<порт>**.
   d. В поле *Платформа* выберите значение *BOE*.
   e. Выберите значение *Использовать экспортную библиотеку SAP (PDF)*, чтобы включить экспортную библиотеку для SAP Business Explorer, что позволит экспортировать файлы PDF, PostScript и PCL из веб-приложений BEx.
6. Сохраните введенные сведения.

Связанные сведения

Создание RFC-адресата в системе ABAP [страница 771]

18.2.3.11.5.1 Создание RFC-адресата в системе ABAP

Для интеграции системы BW и платформы BI требуется RFC-адресат. RFC-адресат обеспечивает взаимодействие между системой BW и платформой BI.

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 *T для подключения TCP/IP*.
   c. Введите краткое описание.

      Позже можно изменить описание RFC-адресата на соответствующем языке.
   d. В разделе *Технические настройки* выберите в качестве типа активации *Зарегистрированная серверная программа*.

e. В разделе *Технические настройки* введите код программы.

   Код программы должен совпадать с кодом программы (RFC-адрес сервера JCo), указанным при создании места назначения для данной системы BW на сервере платформы BI.

f. В разделе *Технические настройки* в подразделе *Параметры шлюза* введите хост шлюза и службу шлюза, которые используются сервером платформы BI для взаимодействия с системой BW.

4. На вкладке *Вход и безопасность* выберите параметр *Отправить квитанцию на вход в SAP*.
5. Сохраните введенные сведения.

Связанные сведения

Настройка параметров сервера [страница 769]

18.2.3.12 Настройка единого входа в SAP HANA

В области *Приложения* консоли CMC 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 квитанцию SAML, которую 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 CMC.
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.

18.2.3.12.1 Настройки соединения SAP HANA

В следующей ниже таблице представлены общие сведения о параметрах, доступных в CMC 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 `trust.pem` в развертывании SAP HANA. Этот сертификат устанавливает отношения доверия между SAP HANA и платформой BI. Сам внешний поставщик сущности определяется сертификатом X509, который используется для подписания всех утверждений сущностей. Сертификат должен быть закодирован в формате Base64.
Номер экземпляра HANA	Номер экземпляра базы данных SAP HANA.
База данных арендатора HANA	Имя базы данных арендатора SAP HANA.

18.2.3.12.2 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 хоста, номер порта, номер экземпляра и имя базы данных арендатора.

      Эти данные потребуются на шаге 2.
2. Настройте соединение SAP HANA на платформе BI.
   a. Перейдите в область *Приложения* на CMC и дважды щелкните *Аутентификация HANA*.
   b. В диалоговом окне *Аутентификация HANA* нажмите кнопку *Создать соединение*. Откроется диалоговое окно *Создание соединения для аутентификации HANA*.
   c. Выберите *Тип соединения*.

      > ⓘ Примечание
      >
      > Необходимо выбрать *SAP HANA* для соединения JDBC и *SAP HANA HTTP* для соединения HTTP.

   d. Введите номер порта, имя хоста, номер экземпляра и имя базы данных, записанные на шаге 1.
   e. В поле *Уникальный идентификатор поставщика удостоверений* введите значение, которое будет использоваться для развертывания платформы BI.
   f. Введите *имя поставщика услуг*.

      > ⓘ Примечание
      >
      > Проверить настройку имени поставщика услуг в HANA можно в `indexserver.ini -> Authentication -> saml_service_provider_name`. Кроме

того, можно изменить это значение в HANA, введя указанный ниже код. `ALTER SYSTEM ALTER CONFIGURATION ('indexserver.ini', 'SYSTEM') SET ('authentication', 'saml_service_provider_name') = 'DEV00' WITH RECONFIGURE;` В этом коде DEV 00 – это имя поставщика услуг, которое можно задать по своему усмотрению. Рекомендуется объединять в имени поставщика услуг ИД системы (DEV) и номер экземпляра (00).

g. Выберите *Защищенное соединение*.

> **Примечание**
>
> Необходимо выбрать *Защищенное соединение*, чтобы установить защищенное соединение JDBC или HTTPS.
>
> - Для установки соединения HTTPS необходимо выбрать *SAP HANA HTTP* в качестве *типа соединения* и выбрать *Защищенное соединение*.
> - Для установки защищенного соединения JDBC необходимо выбрать *SAP HANA* в качестве *типа соединения* и выбрать *Защищенное соединение*.

h. Нажмите кнопку *Сгенерировать*.
В поле *Сертификат Base64 поставщика удостоверений* будет создан сертификат.

3. Настройте развертывание SAP HANA.
   a. Войдите в систему HANA.
   b. Разверните узел *SSL and Trust Configuration* и выберите *PSE Management*.
   c. Выберите файл PSE из раскрывающегося списка *Управления PSE*.
   d. Выберите *Импортировать сертификаты*.
   e. Вставьте сертификат, созданный в предыдущем шаге в платформе BI.
   f. Нажмите кнопку *Импорт*.
   g. Запустите SAP HANA Studio.
   h. В представлении *Системы* разверните систему SAP HANA. См. Руководство по администрированию SAP HANA One.
   i. Откройте (Редактор безопасности) папки "Безопасность".
   j. Выберите (Импорт провайдера идентичности SAML для файла сертификата).
   k. Выберите провайдер идентичности из списка *Провайдеры идентичности SAML*.
   l. Выберите (Развернуть).
   m. Перейдите в поле пользователя в HANA в представлении *Системы*.
   n. Откройте пользователя HANA в области "Редакторы".
   o. На вкладке *Пользователь* в качестве аутентификации отметьте *SAML* и нажмите *Настроить*.
   p. В ассистенте *Настройка внешних идентичностей SAML* нажмите кнопку *Добавить*.
   q. Выберите провайдер идентичности.
   r. Нажмите OK.
   s. Выберите провайдер идентичности и введите имя пользователя платформы BI, которому присвоен пользователь HANA.
   t. Нажмите OK.
   u. Выберите (Развернуть).
   v. Перезапустите систему SAP HANA.
      1. Откройте контекстное меню системы SAP HANA.

2. Выберите *Конфигурация и мониторинг*.
3. Нажмите *Перезапуск системы*.

4. Проверьте конфигурацию SAP HANA.
   a. Перейдите в область *Приложения* на CMC и дважды щелкните *Аутентификация HANA*.
   b. В диалоговом окне *Аутентификация HANA* откройте соединение, созданное на 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, отобразится сообщение об ошибке. Для устранения неполадки можно попробовать следующие шаги:

      - Убедитесь, что другие сертификаты в файле `trust.pem` не содержат субъекта или издателя с таким же значением свойства CN. Чтобы просмотреть компоненты сертификата, найдите в Интернете декодер сертификата по фразе «декодер сертификата x509».
      - Для проверки конфигурации на стороне HANA попробуйте следующие команды:

        ```
        select * from "SAML_PROVIDERS"
        select user_name, is_saml_enabled from users where user_name =
        '<UserName>'
        select * from "PUBLIC"."SAML_USER_MAPPINGS"
        ```

      - Если при настройке единого входа (SSO) в SAP HANA отобразится ошибка аутентификации SAML, попробуйте следующие шаги:
        1. В файле `indexserver.ini` установите для параметра `sslCreateSelfSignedCertificate` значение **`false`**.
        2. В этом же файле задайте для параметров `sslKeyStore` и `sslTrustStore` использование абсолютных путей.
        3. Повторно создайте файлы `key.pem` и `trust.pem`.

Если в каталоге `.ssl` отсутствует файл `key.pem`, в SAP HANA неверно настроено использование SSL.

18.2.3.12.3 Настройка HTTPS-подключения к SAP HANA

Настройка HTTPS-подключения к SAP HANA включает добавление сервера HANA и сертификата CA сервера HANA в хранилище TrustStore или любое расположение по вашему выбору.

> ⓘ Примечание
>
> Экспортируйте сертификат сервера SAP HANA из системы SAP HANA перд тем, как добавить сертификат в TrustStore или в другое хранилище.

Добавление сертификата в хранилище TrustStore

1. Перейдите в каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security`.

2. Выполните следующую команду: `..\..\bin\keytool -importcert -file "<absolute path of the certificate>" -alias CertifcateAliasName -keystore cacerts -storepass changeit`.
3. Сервер HANA и сертификат CA сервера HANA сохранены в хранилище TrustStore.

> **Примечание**
>
> Если файл хранилища ключей находится в каталоге по умолчанию `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security`, после обновления SAP Business Intelligence Platform с пакетом поддержки 4 на версию с пакетом поддержки 5 изменения, внесенные в файл хранилища ключей, будут потеряны. Поэтому рекомендуется добавить сертификат в другое расположение.

Добавление сертификата в другое расположение

1. Перейдите в каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\bin`.
2. Выполните следующую команду: `keytool -importcert -file "C:\certificate\HANASERVERCertificate " -alias CertificateAliasName -keystore C:\certificate\cacerts -storepass changeit`.

   > **Примечание**
   >
   > Расположение, определенное выше, указано только в качестве примера. Можно добавить любое расположение по своему выбору.

3. Чтобы сервер APS мог идентифицировать расположение файла, выполните следующую команду:

   ```
   -Djavax.net.ssl.trustStore= cacerts_PATH
   -Djavax.net.ssl.trustStorePassword= Password
   ```

   > **Примечание**
   >
   > cacerts_PATH и Password - просто примеры пути к хранилищу ключей и пароля для сертификата. Можно добавить любой собственный путь и пароль.

18.2.3.13 Управление настройками SAP Lumira

В области CMC "Приложения" можно управлять правами, связанными с функциями SAP Lumira по импорту данных и совместному использованию объектов, для каждого пользователя или группы пользователей.

Для управления правами, относящимися к SAP Lumira, выполните следующие шаги:

1. На домашней странице CMC выберите *Приложения* > *SAP Lumira* > *Безопасность пользователя*.
2. Выберите пользователя или группу, для которых нужно задать правила.

3. Выберите *Назначить безопасность*.
4. Выберите *Дополнительно*.
5. Выберите *Добавить/Удалить права*.
6. Определите права, необходимые пользователю для SAP Lumira.
7. Нажмите кнопку *Применить*.

18.2.3.14 Управление настройками SAP Analytics Cloud

18.2.3.14.1 Перенос основных средств Hub в SAP Analytics Hub

Активы BI можно добавить в новую категорию *Основное средство Hub* и получить к ним доступ из SAP Analytics Hub.

Создайте *клиент OAuth* в SAP Analytics Cloud и запишите значения таких параметров, как *URL клиента SAP Analytics Cloud*, *URL-адрес маркера*, *Ид. клиента OAuth* и *Секретный ключ*. Сведения о том, как создать клиент OAuth, см. в разделе *Управление клиентом OAuth* в Справке SAP Analytics Cloud на портале SAP Help Portal.

SAP Analytics Hub предоставляет переводчикам доступ к локальным и облачным активам BI на единой платформе. Вам необходимо установить доверие между платформой BI и SAP Analytics Cloud, которое служит в качестве поставщика удостоверений для SAP Analytics Hub, чтобы разрешить платформе BI загружать активы BI в SAP Analytics Hub.

> **Примечание**
>
> В категории *Основное средство Hub* не поддерживаются публикации.

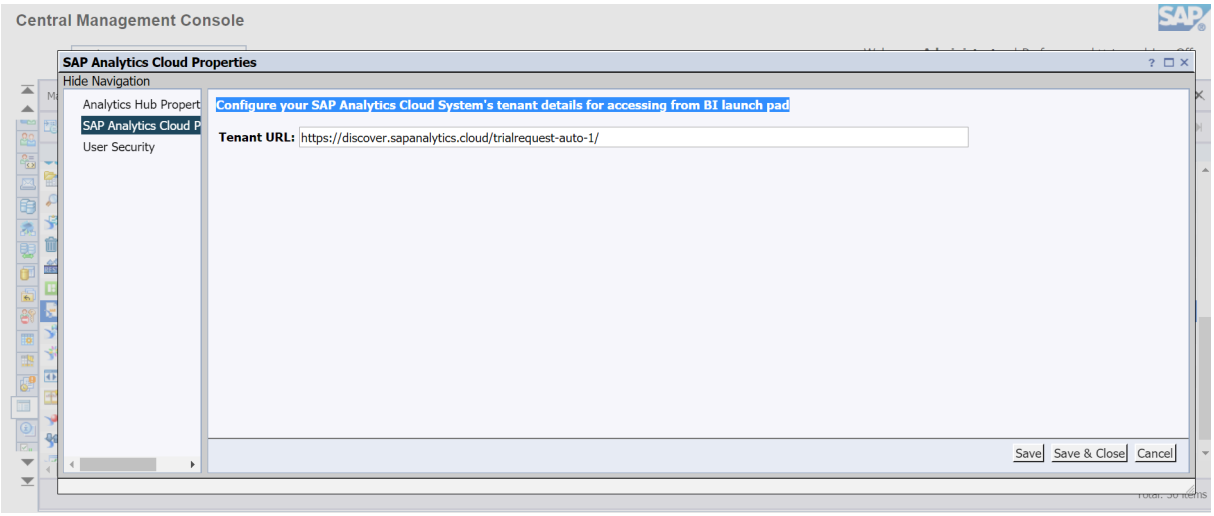
1. Войдите в систему CMC и перейдите в раздел *Приложения* > *SAP Analytics Cloud*.
2. Выберите *Разрешить платформе BI доставку активов BI в Analytics Hub*.
3. Введите следующие параметры:
   - *URL клиента SAP Analytics Cloud*
   - *URL-адрес маркера*
   - *Ид. клиента OAuth*
   - *Секретный ключ*
4. Нажмите *Сохранить и закрыть*.

Настройка параметров SAP Analytics Cloud на платформе BI для загрузки ресурсов BI категории *Основное средство Hub* в SAP Analytics Hub успешно завершена.

18.2.3.14.2 Конфигурирование настроек URL-адреса арендатора SAP Analytics Cloud

Теперь можно конфигурировать подробные данные арендатора системы SAP Analytics Cloud для доступа к нему из плитки SAC в приложениях стартовой панели BI.

> **Примечание**
>
> По умолчанию указывается URL-адрес пробной учетной записи SAP Analytics.



18.2.3.15 Конфигурация сервера авторизации

Приложение "Конфигурация сервера авторизации" предназначено для доступа к любым ресурсам базы данных через механизм или протокол сервера авторизации.

Поддержка сквозного единого входа (SSO) OAuth и поддержка одного и нескольких серверов OAuth

В Central Management Console приложение *Конфигурация сервера авторизации* позволяет настраивать серверы авторизации и управлять ими на платформе BI. В приложении администратор отвечает за регистрацию конфигураций и управление ими через ссылочные объекты полномочий. Каждая конфигурация сервера авторизации имеет ссылочный объект авторизации. Можно создать конфигурации сервера авторизации для независимых ресурсов, Google Диска, Microsoft Drive или OData.

Чтобы создать конфигурацию сервера авторизации, заполните обязательные поля в разделе *Ввод информации конфигурации для сервера авторизации*.

Объем авторизации можно определить в зависимости от ваших потребностей, чтобы контролировать, к чему у конечных пользователей есть доступ (онлайн или офлайн).

18.2.3.15.1 Настройка сервера авторизации

Можно настроить сервер авторизации.

1. Запустите Central Management Console и войдите в нее как администратор.
2. На домашней странице выберите *Приложения* в столбце *Управление*.
3. На странице *Приложения* щелкните дважды *Конфигурация сервера авторизации*.
4. В диалоговом окне *Конфигурации сервера авторизации* выполните одно из следующих действий:
   - Выберите *Управление* > *Новая конфигурация сервера авторизации*.
   - Выберите значок панели инструментов *Создать новую конфигурацию сервера авторизации*.
5. В диалоговом окне *Создать новую конфигурацию сервера авторизации* введите следующие параметры:
   - *Имя ссылки*
     Выберите уникальную произвольную строку и введите то же самое для идентификации конфигурации, чтобы распознавать и выбирать эту конфигурацию в различных рабочих процессах для обеспечения единого входа на основе авторизации.
   - *Описание* (необязательно).
     Введите любой оператор или ключевое слово для описания и простой идентификации конфигурации из списка доступных конфигураций.
   - **Поля, специфичные для OpenID Connect**
     Следующие поля специфичны для аутентификации OpenID Connect и не требуются для SSO на основе авторизации:
     - Флажок *Активировано для аутентификации OpenID Connect*
     - *URI отправителя*
     - *URI наборов веб-ключей JSON (jwks_uri)*
     - *Алгоритм подписания ид. токена*
   - *Конечная точка авторизации*
     Введите URL-адрес сервера авторизации, с помощью которого можно получить авторизацию.
   - *Конечная точка токена*
     Введите URL-адрес сервера авторизации, по которому можно запросить маркер доступа путем обмена кода авторизации.
   - *Идентификатор клиента*
     Введите имя приложения, которое используется для регистрации ландшафта BI на сервере авторизации.
   - *Секрет клиента*
     Введите специальный секретный код, соответствующий приложению, которое используется при регистрации ландшафта BI на сервере авторизации.
   - *URL переадресации*
     Введите URL-адрес конечной точки ландшафта BI, на который сервер авторизации должен отправить код авторизации после успешной проверки авторизации.
   - *Конечная точка отмены* (необязательно)
     Введите URL-адрес сервера авторизации, с помощью которого приложение может запросить отмену всех ранее выданных маркеров доступа посредством определенного маркера обновления.
   - *Объем авторизации*

Введите поддерживаемые сервером авторизации объемы авторизации, чтобы определить ограничения для доступа приложения (ландшафта BI) к различным доступным ресурсам API.

> **Примечание**
>
> Реализация единого входа OAuth платформы BI основана на автономном доступе. Если целью настройки сервера авторизации на платформе BI является обновление данных или доступ к ресурсам без задачи каждый раз выполнять подтверждение авторизации, то необходимо настроить это поле с требуемым параметром объема вместе с одним обязательным параметром (например, refresh_token или offline_access) на основе поставщика сервера авторизации.

- *Тип ресурса*
  Выберите нужный тип ресурса в списке доступных типов ресурсов, поддерживаемых платформой BI. Ниже приведен текущий список типов ресурсов, которые поддерживаются платформой BI для настройки и доступа через соответствующий сервер авторизации:
  - *Независимый* (значение по умолчанию)
    Не специфичен для какого-либо поставщика или протокола, чтобы указать любой ресурс, к которому можно получить доступ при успешной авторизации сервером авторизации.
  - *Google Диск*
    Указывает, что конфигурация относится к серверу авторизации Google, который можно использовать для доступа к Google Диску в различных сценариях платформы BI. В любой момент времени в системе может существовать только одна конфигурация типа Google Диск.
  - *Microsoft Drive*
    Указывает, что конфигурация относится к серверу авторизации Microsoft, который можно использовать для доступа к Microsoft Drive в различных сценариях платформы BI. В любой момент времени в системе может существовать только одна конфигурация типа Microsoft Drive.
  - *OData*
    Не специфичен для какого-либо поставщика, но указывает, что конфигурация связана с ресурсом, доступ к которому можно получить по протоколу OData с авторизацией на сервере авторизации. Как и в случае Google Диск, в любой момент времени в системе может существовать только одна конфигурация типа OData.

> **Примечание**
>
> Параметр *Тип ресурса* не имеет ничего общего со стандартом OAuth 2.0. Однако он введен в конфигурацию, чтобы избежать возможной двусмысленности при идентификации определенных ресурсов на платформе BI. Поэтому соответствующие конфигурации можно легко выбрать и использовать в определенных сценариях для обеспечения авторизации.

- *Тип доступа*
  Этот параметр специфичен для конфигурации авторизации типа *Google Диск*. Это поле будет заполнено автоматически, если поле *Тип ресурса* имеет значение *Google Диск*.
- *Пользовательские параметры* (необязательно)
  Введите любые пользовательские параметры, необходимые для отправки при запросе авторизации. Это зависит от пользовательских требований (в случае необходимости) настраиваемого сервера авторизации.

> **Примечание**
>
> Имя пользовательского параметра должно быть уникальным в конфигурации.
>
> В любой конфигурации авторизации разрешается настраивать не более пяти пользовательских параметров.

6. После ввода всех обязательных параметров нажмите *OK*, чтобы подтвердить сведения и сохранить конфигурацию.

   Конфигурация будет сохранена как системный объект в репозитории с типом *AuthorizationReference*. На эту конфигурацию можно ссылаться во всех поддерживаемых сценариях с использованием ее *имени ссылки*.

18.2.3.15.2 Тестирование конфигурации сервера авторизации

Можно протестировать конфигурацию сервера авторизации.

1. После успешного сохранения конфигурации сервера авторизации откройте стартовую панель BI и выполните вход, чтобы протестировать конфигурацию.

   > **Примечание**
   >
   > В настоящее время невозможно протестировать конфигурацию из CMC.
   >
   > Войдите в систему в качестве администратора или с любой учетной записью пользователя платформы BI, у которой нет ограничений на использование конфигурации авторизации, сохраненной выше.
   >
   > Используйте текущий метод входа, настроенный для стартовой панели BI (например, Enterprise или любой метод аутентификации).

2. Выберите значок пользователя.
3. В появившемся раскрывающемся меню выберите *Настройки*.
4. В диалоговом окне *Настройки* выберите *Токены авторизации* в разделе *Учетная запись пользователя*.
5. Выберите *Сгенерировать* в столбце *Управление токенами*.
6. В соответствии с политикой вашей организации на основе конфигурации авторизации на сервере авторизации либо будет выполняться проверка учетной записи на основе сертификатов, сконфигурированных в системе, либо у вас будут запрошены имя пользователя, пароль и/или многофакторная аутентификация на основе настроек конфигурации.
7. После успешной проверки учетных данных или сертификата платформа BI должна получить маркер обновления. Он должен быть надежно сохранен в репозитории платформы BI. После этого на вкладке *Токены авторизации* должны появиться следующие изменения:
   - В столбце *Срок действия истекает* должно отображаться значение истечения срока действия маркера, выданного сервером авторизации. Если сервер авторизации выдает маркер без срока действия, значение столбца будет обновлено на *Нет срока действия*.
   - В столбце *Управление токенами* рядом с кнопкой *Сгенерировать* должна появиться кнопка *Удалить*.

- Кнопка *Удалить* предназначена для удаления маркера, выданного сервером авторизации. Удаление не ограничивается только удалением маркера из хранилища репозитория платформы BI. Его также можно распространить на сервер авторизации на основе конфигурации и поддержки.
- Если необязательный параметр *Конечная точка отмены* заполнен соответствующим URL-адресом, основанным на соответствующей поддержке сервера авторизации, то выданный маркер также будет удален на уровне сервера авторизации вместе с очисткой из хранилища репозитория платформы BI.

8. Если маркер выдан и столбец *Срок действия истекает* обновляется в соответствии с истечением срока действия выданного маркера, то конфигурация успешно работает и готова к использованию разработчиком BI и конечным пользователем BI.

18.2.3.16 Конфигурация классификации информации

На платформе BI можно сконфигурировать сервер политик Azure организации, чтобы активировать для ландшафта BI возможность классифицировать BI-контент. Эти возможности классификации могут применяться по меткам чувствительности, определенным администратором сервера политик Azure вашей организации.

> ⓘ Примечание
>
> Эта опция интеграции для конфигурирования сервера политик поддерживается только для платформы защиты информации Microsoft Azure.
>
> Версия SAP BusinessObjects BI 4.3 SP04 включает опцию интеграции для платформы защиты информации Microsoft Azure. Однако важно отметить, что приложение для конфигурирования сведений сервера политик Azure на платформе BI не активировано по умолчанию; оно поставляется как скрытая функция. Чтобы сделать эту скрытую функцию видимой, см. SAP-ноту 3409349.

Эта функция доступна только на платформе Windows.

18.2.3.16.1 Чтобы сконфигурировать классификацию информации

1. Войдите в *Central Management Console* как администратор.
2. Перейдите к узлу *Приложения*.
3. Щелкните правой кнопкой мыши приложение *Конфигурация классификации информации*.
4. Выберите *Конфигурация для классификации информации*.
5. Установите флажок *Активировать классификацию информации*, чтобы активировать конфигурацию и поля.
6. Введите URL-адрес маркера сервера политик Azure в поле *URL-адрес сервера политик*.
   URL-адрес должен иметь формат `https://login.microsoftonline.com/<tenant-id>/oauth2/v2.0/token`.

7. Введите значения *Ид. клиента* и *Секрет клиента* из клиентского приложения в Azure.
   Они активированы для режима потока учетных данных клиента авторизации для доступа к серверу политик Azure вашей организации.
8. Нажмите *Сохранить и тестировать конфигурацию*, чтобы проверить соединение.
9. Если тест конфигурации выполнен успешно, нажмите *Сохранить* или *Сохранить и закрыть*.

> **Примечание**
>
> Не устанавливайте флажок *Активировано для аутентификации сертификата*, так как этот режим конфигурации аутентификации не поддерживается.

18.3 Управление приложениями с помощью свойств семантического уровня

Параметры конфигурации многомерного семантического слоя (DSL) устанавливаются при выполнении для изменения поведения HANA Direct Access и BW Direct Access через соединения BICS в таких средствах BI, как Web Intelligence, средство дизайна информации, Dashboards и Crystal Reports для Enterprise. Эти параметры определяются параметрами командной строки Java в форме:

-DoptionName=optionValue

Сохранение и модификация параметров может представлять определенную сложность:

- Параметры командной строки требуется определить для каждого процесса Java при запуске DSL. Единого местоположения для внесения изменений не существует.
- Каждый процесс DSL Java нужно перезапускать для внесения изменений. Изменения не начинают действовать "на лету".

Чтобы упростить работу администратора при поддержании параметров конфигурации DSL-BICS, был разработан механизм, позволяющий сохранять параметры в файл. Внесенные в файл изменения распространятся на новые настройки параметров всех процессов DSL, которые читают данный файл.

Имя и значение параметра сохраняются в файле как допустимый XML-код для java.util.Propertes в соответствии с http://java.sun.com/dtd/properties.dtd

При первом запуске механизма в DSL автоматически генерируются два файла:

- DSLBICSConfiguration.xml или DSLConfiguration.xml – файл, содержащий все доступные параметры со значениями по умолчанию. Этот файл не следует изменять.
- DSLBICSConfiguration_custom.xml или DSLConfiguration_custom.xml – файл, содержащий все параметры со значениями, заданными администратором.

> **Примечание**
>
> - Файлы DSLBICSConfiguration.xml и DSLBICSConfiguration_custom.xml используются для управления поведением BW Direct Access через соединения BICS.
> - Файлы DSLConfiguration.xml и DSLconfiguration_custom.xml используются для управления поведением HANA Direct Access.

Сгенерированный файл `DSLBICSConfiguration_custom.xml` или `DSLConfiguration_custom.xml` содержит все настройки параметров, определенные через командную строку, а также настройки по умолчанию для других параметров. После первичной генерации файл `DSLBICSConfiguration_custom.xml` или `DSLConfiguration.xml` можно изменить, добавляя или изменяя значения параметров. Механизм не обновляет этот файл после первичной генерации. Обновляется файл `DSLBICSConfiguration.xml`: в него вносятся новые параметры и изменяются значения по умолчанию.

Чтобы изменить одно из свойств по умолчанию, используйте файл пользовательской конфигурации для сохранения новых настроек, как для глобальных свойств, так и свойств приложения. По умолчанию файл хранятся в папке `SAP BusinessObjects Enterprise XI 4.0\java\lib`

Не изменяйте свойства в файле настроек по умолчанию.

18.4 Управление приложениями с помощью свойств BOE.war

18.4.1 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*.

18.4.1.1 Глобальные свойства файла BOE.war

В следующей таблице перечислены параметры, которые входят в состав установленного по умолчанию файла `global.properties` для BOE.war.

Чтобы перезаписать какие-либо 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
`persistentcookies.enabled`	`persistentcookies.enabled=true`	Включает или отключает сохранение cookie-файлов на странице входа в приложение.
`siteminder.authentication`	`siteminder.authentication=secLDAP`	Указывает метод аутентификации, используемый в SiteMinder. Допустимые параметры: secLDAP и secwinAD.
`siteminder.enabled`	`siteminder.enabled=false`	Включает или отключает аутентификацию в SiteMinder.
`sso.enabled`	`sso.enabled=false`	Включает или отключает единый вход в платформу BI.
`sso.sap.primary`	`sso.sap.primary=false`	Присвойте этому параметру значение `true`, 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.
`max.tree.children.threshold`	`max.tree.children.threshold=200`	Устанавливает пороговое значение, при достижении которого в иерархических списках вместо отображения всех узлов будет отображаться сообщение "слишком много дочерних узлов".
`trusted.auth.shared.secret`	Нет	Задает имя переменной сеанса, используемой для извлечения секретного ключа для доверительной аутентификации. Применяется только случае использования веб-сеанса для передачи общего секретного ключа.
`trusted.auth.user.param`	Нет	Задает переменную, используемую для извлечения имени пользователя для доверительной аутентификации, и может иметь одно из следующих значений: • `Header` • `URL Parameter` • `Cookie` • `Session`
`trusted.auth.user.retrieval`	Нет	Задает метод, используемый для извлечения имени пользователя для доверительной аутентификации, и может иметь одно из следующих значений:

Параметр	Значения по умолчанию	Описание
		• "REMOTE_USER" • "HTTP_HEADER" • "COOKIE" • "QUERY_STRING" • "WEB_SESSION" • "USER_PRINCIPAL" Чтобы отключить доверительную аутентификацию, установите пустое значение.
trusted.auth.user.namespace.enabled	trusted.auth.user.namespace.enabled=false	Включает и отключает динамическую привязку псевдонимов к существующим учетным записям. Если этому свойству присвоено значение true, 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 false, для аутентификации пользователей при доверительной аутентификации используется сопоставление имен.
vintela.enabled	vintela.enabled=false idm.realm=YOUR_REALM idm.princ=YOUR_PRINCIPAL idm.allowUnsecured=true idm.allowNTLM=false idm.logger.name=simple idm.logger.props=error-log.properties	Используется для включения или отключения параметров Vintela для аутентификации Windows AD.
pinger.showWarningDialog.cmc	pinger.showWarningDialog.cmc=true	Указывает, отображается или нет диалоговое окно предупреждения с сообщением о скором истечении срока действия сеанса в CMC.
pinger.showWarningDialog.bilaunchpad	pinger.showWarningDialog.bilaunchpad=true	Указывает, отображается или нет диалоговое окно предупреждения с сообщением о скором истечении срока действия сеанса в стартовой панели BI.
pinger.warningPeriod.pingIncrementsInSeconds	pinger.warningPeriod.pingIncrementsInSeconds=15	Указывает частоту отправки запросов веб-сервера во время отображения предупреждающего сообщения об истечении срока действия сеанса. Этот параметр важен для синхронизации диалоговых окон предупреждения между приложениями.

Параметр	Значения по умолчанию	Описание
pinger.warningPeriod.lengthInMinutes	pinger.warningPeriod.lengthInMinutes=5	Указывает, за какое время до истечения срока действия сеанса отображается предупреждение.
logoff.on.websession.expiry	logoff.on.websession.expiry=true	Указывает необходимость выхода из системы для всех сеансов приложений в случае истечения срока действия веб-сеанса.
pinger.enabled	pinger.enabled=true	Включает или отключает механизм отображения предупреждающих сообщений об истечении срока действия сеанса.
system.com.sap.bip.jcomanager.destinations.maxsize	system.com.sap.bip.jcomanager.destinations.maxsize=1000	Указывает максимальное число кэшируемых соединений Java.
httpproxy.username	httpproxy.username=myusername	Указывает имя пользователя для входа на прокси-сервер HTTP.
httpproxy.password	httpproxy.password=mypassword	Указывает пароль для входа на прокси-сервер HTTP.
logon.embed.secret	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.
logon.embed.timeout	logon.embed.timeout=300	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.
iview.autologoff	iview.autologoff=true	При значении `true` включен незамедлительный автоматический выход для iViews на технологической платформе SAP NetWeaver.
pinger.showWarningDialog	pinger.showWarningDialog=true	Указывает, должно ли отображаться диалоговое окно предупреждения с сообщением о скором истечении срока действия сеанса. Не применяется для CMC и стартовой панели BI.
ure.request.queue.timeout.seconds	ure.request.queue.timeout.seconds=20	Количество секунд ожидания запросом предыдущих ожидаемых запросов, прежде чем произойдет тайм-аут Когда пользователи выполняют действия навигации и развертывания папок в древовидном списке на стартовой панели BI, создается очередь запросов AJAX для

Параметр	Значения по умолчанию	Описание
		этих действий. Пользовательский интерфейс ожидает выполнения этих запросов перед передачей управления пользователю. Этот параметр определяет количество секунд ожидания пользовательским интерфейсом каждого запроса при возникновении неожиданных задержек в запросе бэкэнда.
`enable.safe.html`	`enable.safe.html=true`	Активирует использование безопасных URL-адресов веб-страниц в URL-адресах модуля веб-страниц для рабочей области BI.
`upload.file.maxsize.in MB`	`upload.file.maxsize.in MB = 0`	Указывает максимальный размер загружаемого файла (в мегабайтах). Если установлено значение по умолчанию (0), допускается загрузка файлов любого размера.
`upload.file.allowed.fo rmats`	Нет	Указывает разрешенные форматы загружаемых файлов. Дополнительные сведения см. в SAP-ноте 2296060.
`upload.file.maxsize.in MB=0`	Нет	Максимальный размер файла для загрузки локальных документов в мегабайтах; должен быть целым числом, например: 10 и т. д.
`upload.file.allowed.fo rmats=`	Нет	Это свойство служит для контроля различных типов файлов, разрешенных для загрузки локальных документов. Список поддерживаемых форматов файлов см. в SAP-ноте 2296060. Если вы определяете несколько форматов файлов, разделите их запятыми, например, txt,doc,xls.
`offlinehelp.enabled=fa lse`	Нет	Для включения офлайн-справки установите для флага offlineHelp значение true. По умолчанию этому свойству присваивается значение false.
`offlinehelp.url=`	Нет	URL offlinehelp.url будет использоваться, пока пользователь установил флаг офлайн на true

18.4.1.2 Свойства стартовой панели BI

В следующей таблице перечислены параметры доверительной аутентификации, которые входят в состав установленного по умолчанию файла `bilaunchpad.properties` для WAR-файла BOE. Чтобы

перезаписать какие-либо настройки, 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=BI launch pad`
`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=BI launch pad`
`app.url.name`	Задает URL-имя приложения, предваряемое символом «/»". По умолчанию: `app.url.name=/BI`
`authentication.default`	Задает метод аутентификации по умолчанию, используемый для аутентификации пользователей в приложении. Для этого параметра доступны любые из следующих параметров: **Аутентификация** / **Значение параметра** Enterprise — `secEnterprise` LDAP — `secLDAP` Windows AD — `secWinAD` SAP — `secSAPR3` PeopleSoft — `secpsenterprise` JD Edwards — `secPSE1` Siebel — `secSiebel7` Oracles EBS — `secOraApps` По умолчанию: `authentication.default=secEnterprise`
`authentication.visible`	Указывает возможность просмотра и изменения метода аутентификации пользователем, выполняющим вход в стартовую панель BI. По умолчанию: `authentication.visible=false`
`Authentication.VisibleList`	Определяет видимость списка доступных типов аутентификации на экране входа. Ниже представлен список доступных типов аутентификации: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`. В списке можно включить или отключить типы аутентификации, включив требуемые типы в файл `Authentication.VisibleList` или исключив их из него. По умолчанию:

Параметр	Описание
	`Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`

`sap.system.client.visible`
`authentication.sapSystem`
`authentication.sapClient`
	Определяет видимость полей *SAP-система* и *Клиент SAP* при выборе типа аутентификации "SAP". По умолчанию: `sap.system.client.visible=true`. Когда для `sap.system.client.visible` задано значение `sap.system.client.visible=false`, можно указать значения для SAP-системы и клиента SAP в файле свойств, используя параметры `authentication.sapSystem` и `authentication.sapClient` соответственно.

`cms.default`	Задает имя CMS по умолчанию. По умолчанию: `cms.default=[name of host machine]`
`cms.visible`	Указывает возможность просмотра и изменения имени CMS пользователем, выполняющим вход в стартовую панель BI. По умолчанию: `cms.visible=true`
`dialogue.prompt.enabled`	Указывает необходимость запроса пользователя при переходе со страницы ввода в диалоговом окне. По умолчанию: `dialogue.prompt.enabled=false`
`logontoken.enabled`	Указывает, требуется ли включать создание маркеров для сеанса после входа пользователя в стартовую панель BI. Маркер будет храниться в cookie-файле. По умолчанию: `logontoken.enabled=false`
`SMTPFrom`	Включает или отключает поле *От кого* при планировании объекта для адресата. По умолчанию: `SMTPFrom=true` Если значение задано как `false`, поле *От* не будет отображаться, а система попытается получить значение *От* следующим образом: 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.
`url.exit`	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.
`disable.locale.preference`	Разрешает или запрещает просмотр и изменение пользователями локальных параметров просмотра

Параметр	Описание
	для стартовой панели BI. По умолчанию: `disable.locale.preference=false`
`extlogon.allow.logoff`	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 false. По умолчанию: `extlogon.allow.logoff=true`
`logon.allowInsecureEmbedding`	Указывает, разрешено ли другим приложениям встраивать это приложение (в качестве кадра) без допустимого маркера встраивания. По умолчанию: `logon.allowInsecureEmbedding=false`
`sso.types.and.order`	Указывает разделенный запятыми список типов единого входа, которые будут включены, а также порядок их выполнения. Пустой список указывает, что должен использоваться прежний порядок. Если список указан, прежние параметры игнорируются. Допустимые параметры: `vintela`, `trustedIIS`, `trustedHeader`, `trustedParameter`, `trustedCookie`, `trustedSession`, `trustedUserPrincipal`, `trustedVintela`, `trustedX509`, `sapSSO` и `siteminder`. Если ничего не требуется, укажите: `none`
`allowed.cms`	Чтобы обеспечить безопасный вход и избежать фальсификации запросов на стороне сервера, можно создать белый список допустимых имен или IP-адресов CMS вместе с номерами портов. Вы входите в приложение, только если значение, введенное при входе в систему, в точности соответствует значению в белом списке. Введите список имен или IP-адресов CMS вместе с номером порта в свойстве allowed.cms. Например, `allowed.cms =<cms name or IP>:<port number>.` При наличии нескольких CMS для подключения введите значения через запятую (,): `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>`

Параметр	Описание
	Примечание • Чтобы войти в систему с использованием или имени CMS, или IP-адреса, добавьте их в свойство `allowed.cms`. • Поскольку номер порта необязателен на экране входа, его можно не включать в белый список. Тогда вы будет входить в порт по умолчанию. Однако если номер порта присутствует в белом списке и не будет введен при входе в систему, вход выполнить не удастся. Ниже представлены сценарии, не требующие использования белого списка: • Если для `cms.visible` задано значение false и для `cms.default` задано значение CMS. • если CMS кластеризован и вы входите в систему с использованием имени кластера. Если вы пытаетесь войти в определенный кластер(CMS), имя CMS должно быть указано в свойстве `allowed.cms`; • если вход осуществляется через SSO.

18.4.1.3 Свойства стартовой панели BI в стиле Fiori

В следующей таблице перечислены настройки, включенные в файл `FioriBI.properties` по умолчанию для WAR-файла BOE. Чтобы перезаписать какие-либо настройки, создайте новый файл в каталоге `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Примечание

В BI 4.2 SP5 файл Bing.properties переименован в файл FioriBI.properties. При обновлении любой версии на BI 4.2 SP5 необходимо вручную изменить имя файла свойств стартовой панели BI в стиле Fiori с Bing.properties на FioriBI.properties, чтобы сохранить существующие конфигурации для стартовой панели BI в стиле Fiori.

Настройка	Описание
`app.name`	Задает отображаемое имя приложения. Это имя отображается на странице заголовка веб-приложения и экране входа в систему. По умолчанию: `app.name=BI launch pad`

Настройка	Описание
`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=BI launch pad`
`app.url.name`	Задает URL-имя приложения, предваряемое символом «/»". По умолчанию: `app.url.name=/BILaunchpad`
`authentication.default`	Задает метод аутентификации по умолчанию, используемый для аутентификации пользователей в приложении. Для этого параметра доступны любые из следующих параметров: **Аутентификация** — **Значение параметра** Enterprise — `secEnterprise` LDAP — `secLDAP` Windows AD — `secWinAD` SAP — `secSAPR3` PeopleSoft — `secpsenterprise` JD Edwards — `secPSE1` Siebel — `secSiebel7` Oracles EBS — `secOraApps` По умолчанию: `authentication.default=secEnterprise`
`authentication.visible`	Указывает возможность просмотра и изменения метода аутентификации пользователем, выполняющим вход в стартовую панель BI в стиле Fiori. По умолчанию: `authentication.visible=false`
`Authentication.VisibleList`	Определяет видимость списка доступных типов аутентификации на экране входа. Ниже представлен список доступных типов аутентификации: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`. В списке можно включить или отключить типы аутентификации, включив требуемые типы в файл `Authentication.VisibleList` или исключив их из него. По умолчанию: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`

`sap.system.client.visible`
 	
`authentication.sapSystem`
	Определяет видимость полей *SAP-система* и *Клиент SAP* при выборе типа аутентификации "SAP". По умолчанию: `sap.system.client.visible=true`. Когда для `sap.system.client.visible` задано

Настройка	Описание
`authentication.sapClient`	значение `sap.system.client.visible=false`, можно указать значения для SAP-системы и клиента SAP в файле свойств, используя параметры `authentication.sapSystem=` и `authentication.sapClient=` соответственно.
`cms.default`	Задает имя CMS по умолчанию. По умолчанию: `cms.default=[name of host machine]`
`cms.visible`	Указывает возможность просмотра и изменения имени CMS пользователем, выполняющим вход в стартовую панель BI в стиле Fiori. По умолчанию: `cms.visible=true`
`dialogue.prompt.enabled`	Указывает необходимость запроса пользователя при переходе со страницы ввода в диалоговом окне. По умолчанию: `dialogue.prompt.enabled=false`
`logontoken.enabled`	Указывает, требуется ли включать создание маркеров для сеанса после входа пользователя в стартовую панель BI. Маркер будет храниться в cookie-файле. По умолчанию: `logontoken.enabled=false`
`SMTPFrom`	Включает или отключает поле *От кого* при планировании объекта для адресата. По умолчанию: `SMTPFrom=true` Если значение задано как `false`, поле *От* не будет отображаться, а система попытается получить значение *От* следующим образом: 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.
`url.exit`	Задает URL-адрес, на который перенаправляются пользователи после завершения сеанса стартовой панели BI в стиле Fiori. Эта настройка применяется только для тех пользователей, которые выполнили вход в приложение с использованием внешнего процесса проверки.
`disable.locale.preference`	Разрешает или запрещает просмотр и изменение пользователями локальных параметров просмотра для стартовой панели BI в стиле Fiori. По умолчанию: `disable.locale.preference=false`
`extlogon.allow.logoff`	Включает или отключает автоматический выход из системы для сеансов пользователей после закрытия соответствующих сеансов стартовой панели BI в стиле Fiori. Чтобы отключить автоматическое завершение

Настройка	Описание
	сеансов при выходе пользователей из стартовой панели BI, присвойте этому параметру значение false. По умолчанию: `extlogon.allow.logoff=true`
`logon.allowInsecureEmbedding`	Указывает, разрешено ли другим приложениям встраивать это приложение (в качестве кадра) без допустимого маркера встраивания. По умолчанию: `logon.allowInsecureEmbedding=false`
`sso.types.and.order`	Указывает разделенный запятыми список типов единого входа, которые будут включены, а также порядок их выполнения. Пустой список указывает, что должен использоваться прежний порядок. Если список указан, прежние параметры игнорируются. Допустимые параметры: `vintela`, `trustedIIS`, `trustedHeader`, `trustedParameter`, `trustedCookie`, `trustedSession`, `trustedUserPrincipal`, `trustedVintela`, `trustedX509`, `sapSSO` и `siteminder`. Если ничего не требуется, укажите: `none`
`allowed.cms`	Чтобы обеспечить безопасный вход и избежать фальсификации запросов на стороне сервера, можно создать белый список допустимых имен или IP-адресов CMS вместе с номерами портов. Вы входите в приложение, только если значение, введенное при входе в систему, в точности соответствует значению в белом списке. Введите список имен или IP-адресов CMS вместе с номером порта в свойстве allowed.cms. Например, `allowed.cms =<cms name or IP>:<port number>.` При наличии нескольких CMS для подключения введите значения через запятую (,): `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>` **Примечание** • Чтобы войти в систему с использованием или имени CMS, или IP-адреса, добавьте их в свойство `allowed.cms`. • Поскольку номер порта необязателен на экране входа, его можно не включать в белый список. Тогда вы будет входить в порт по умолчанию.

Настройка	Описание
	> Однако если номер порта присутствует в белом списке и не будет введен при входе в систему, вход выполнить не удастся. Ниже представлены сценарии, не требующие использования белого списка: • если для `cms.visible` задано значение false и для `cms.default` задано значение CMS. • если CMS кластеризован и вы входите в систему с использованием имени кластера. Если вы пытаетесь войти в определенный кластер(CMS), имя CMS должно быть указано в свойстве `allowed.cms`; • если вход осуществляется через SSO.
upload.file.maxsize.inMB=0	Максимальный размер файла для загрузки локальных документов в мегабайтах; должен быть целым числом, например: 10 и т. д.
upload.file.allowed.formats=	Это свойство служит для контроля различных типов файлов, разрешенных для загрузки локальных документов. Список поддерживаемых форматов файлов см. в SAP-ноте 2296060. Если вы определяете несколько форматов файлов, разделите их запятыми, например, txt,doc,xls.
app.custom.banner.message	Определяет баннерное сообщение на стартовой панели BI.
logon.webssoauthnetication.framework=Нет	Это свойство используется для включения рабочего процесса веб-аутентификации SSO. Возможные значения: Нет, OpenId и SAML.
openid.restful.url=	Это свойство используется для установки URL-адреса Restful, предоставляемого в CMC. Например: `http://<hostname>:<portNo>/biprws`

18.4.1.4 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`	Задает метод аутентификации по умолчанию, используемый для аутентификации пользователей в приложении. Для этого параметра доступны любые из следующих параметров: **Аутентификация** / **Значение параметра** Enterprise: `secEnterprise` LDAP: `secLDAP` Windows AD: `secWinAD` SAP: `secSAPR3` PeopleSoft: `secpsenterprise` JD Edwards: `secPSE1` Siebel: `secSiebel7` Oracles EBS: `secOraApps` По умолчанию: `authentication.default=secEnterprise`
`authentication.visible`	Указывает возможность просмотра и изменения режима аутентификации пользователем, выполняющим вход в OpenDocument. По умолчанию: `authentication.visible=false`
`Authentication.VisibleList`	Определяет видимость списка доступных типов аутентификации на экране входа. Ниже представлен список доступных типов аутентификации: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`. В списке можно включить или отключить типы аутентификации, включив требуемые типы в файл `Authentication.VisibleList` или исключив их из него. По умолчанию: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`

Параметр	Описание

`sap.system.client.visible`
`authentication.sapSystem`
`authentication.sapClient`
	Определяет видимость полей *SAP-система* и *Клиент SAP* при выборе типа аутентификации "SAP". По умолчанию: `sap.system.client.visible=true`. Когда для `sap.system.client.visible` задано значение `sap.system.client.visible=false`, можно указать значения для SAP-системы и клиента SAP в файле свойств, используя параметры `authentication.sapSystem=` и `authentication.sapClient=` соответственно.

`cms.default`	Задает имя CMS по умолчанию. По умолчанию: `cms.default=[name of host machine]`
`cms.visible`	Указывает возможность просмотра и изменения имени CMC пользователем, выполняющим вход в OpenDocument. По умолчанию: `cms.visible=true`
`logontoken.enabled`	Указывает, требуется ли включать создание маркеров для сеанса после входа пользователя в OpenDocument. Маркер будет храниться в cookie-файле. По умолчанию: `logontoken.enabled=false`
`extlogon.allow.logoff`	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 false. По умолчанию: `extlogon.allow.logoff=true`
`SAPLogonToken.enabled`	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: `SAPLogonToken.enabled=true`
`logon.allowInsecureEmbedding=false`	Указывает, разрешено ли другим приложениям встраивать это приложение (в качестве кадра) без допустимого маркера встраивания. По умолчанию: `logon.allowInsecureEmbedding=false`
`sso.types.and.order`	Указывает разделенный запятыми список типов единого входа, которые будут включены, а также порядок их выполнения. Пустой список указывает, что должен использоваться прежний порядок. Если список указан, прежние параметры игнорируются. Допустимые параметры: `serializedSession`, `sapLogonToken`, `trustedIIS`, `trustedHeader`, `trustedParameter`, `trustedCookie`,

Параметр	Описание
	`trustedSession`, `trustedUserPrincipal`, `trustedVintela`, `vintela`, `infoview`, `trustedX509`, `sapSSO` и `siteminder`. Если ничего не требуется, укажите: `none`
`allowed.cms`	Чтобы обеспечить безопасный вход и избежать фальсификации запросов на стороне сервера, можно создать белый список допустимых имен или IP-адресов CMS вместе с номерами портов. Вы входите в приложение, только если значение, введенное при входе в систему, в точности соответствует значению в белом списке. Введите список имен или IP-адресов CMS вместе с номером порта в свойстве allowed.cms. Например, `allowed.cms =<cms name or IP>:<port number>.` При наличии нескольких CMS для подключения введите значения через запятую (,): `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>` **Примечание** • Чтобы войти в систему с использованием или имени CMS, или IP-адреса, добавьте их в свойство `allowed.cms`. • Поскольку номер порта необязателен на экране входа, его можно не включать в белый список. Тогда вы будет входить в порт по умолчанию. Однако если номер порта присутствует в белом списке и не будет введен при входе в систему, вход выполнить не удастся. Ниже представлены сценарии, не требующие использования белого списка: • Если для `cms.visible` задано значение false и для `cms.default` задано значение CMS. • если CMS кластеризован и вы входите в систему с использованием имени кластера. Если вы пытаетесь войти в определенный кластер(CMS), имя CMS должно быть указано в свойстве `allowed.cms`; • если вход осуществляется через SSO.

18.4.1.5 Свойства CMC

В следующей таблице перечислены параметры доверительной аутентификации, которые входят в состав установленного по умолчанию файла `cmc.properties` для файла BOE.war. Чтобы перезаписать какие-либо параметры, создайте новый файл в каталоге `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Параметр	Описание
`app.url.name`	Задает URL-имя приложения, предваряемое символом «/»". По умолчанию: `app.url.name=/CMC`
`authentication.default`	Задает метод аутентификации по умолчанию, используемый для аутентификации пользователей в приложении. Для этого параметра доступны любые из следующих параметров: **Аутентификация** / **Значение параметра** Enterprise — `secEnterprise` LDAP — `secLDAP` Windows AD — `secWinAD` SAP — `secSAPR3` PeopleSoft — `secpsenterprise` JD Edwards — `secPSE1` Siebel — `secSiebel7` Oracles EBS — `secOraApps` По умолчанию: `authentication.default=secEnterprise`
`authentication.visible`	Указывает возможность просмотра и изменения режима аутентификации пользователем, выполняющим вход в CMC. По умолчанию: `authentication.visible=false`
`Authentication.VisibleList`	Определяет видимость списка доступных типов аутентификации на экране входа. Ниже представлен список доступных типов аутентификации: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`. В списке можно включить или отключить типы аутентификации, включив требуемые типы в файл `Authentication.VisibleList` или исключив их из него. По умолчанию: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`

Параметр	Описание

`sap.system.client.visible`
`authentication.sapSystem`
`authentication.sapClient`
	Определяет видимость полей *SAP-система* и *Клиент SAP* при выборе типа аутентификации "SAP". По умолчанию: `sap.system.client.visible=true`. Когда для `sap.system.client.visible` задано значение `sap.system.client.visible=false`, можно указать значения для SAP-системы и клиента SAP в файле свойств, используя параметры `authentication.sapSystem=` и `authentication.sapClient=` соответственно.

`cms.default`	Задает имя CMS по умолчанию. По умолчанию: `cms.default=[name of host machine]`
`cms.visible`	Указывает возможность просмотра и изменения имени CMC пользователем, выполняющим вход в CMC. По умолчанию: `cms.visible=true`
`dialogue.prompt.enabled`	Указывает необходимость запроса пользователя при переходе со страницы ввода в диалоговом окне. По умолчанию: `dialogue.prompt.enabled=false`
`logontoken.enabled`	Указывает, требуется ли включать создание маркеров для сеанса после входа пользователя в CMC. Маркер будет храниться в cookie-файле. По умолчанию: `logontoken.enabled=false`
`SMTPFrom`	Включает или отключает поле *От кого* при планировании объекта для адресата. По умолчанию: `SMTPFrom=true` Если значение задано как `false`, поле *От* не будет отображаться, а система попытается получить значение *От* следующим образом: 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.
`ulr.exit`	Задает URL-адрес, на который перенаправляются пользователи после завершения сеанса CMC. Этот параметр применяется только для тех пользователей, которые выполнили вход в приложение с использованием внешнего процесса проверки.
`allowed.cms`	Чтобы обеспечить безопасный вход и избежать фальсификации запросов на стороне сервера, можно создать белый список допустимых имен или IP-адресов CMS вместе с номерами портов. Вы входите в приложение, только если значение, введенное при

Параметр	Описание
	входе в систему, в точности соответствует значению в белом списке. Введите список имен или IP-адресов CMS вместе с номером порта в свойстве allowed.cms. Например, `allowed.cms =<cms name or IP>:<port number>.` При наличии нескольких CMS для подключения введите значения через запятую (,): `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>` **Примечание** • Чтобы войти в систему с использованием или имени CMS, или IP-адреса, добавьте их в свойство `allowed.cms`. • Поскольку номер порта необязателен на экране входа, его можно не включать в белый список. Тогда вы будет входить в порт по умолчанию. Однако если номер порта присутствует в белом списке и не будет введен при входе в систему, вход выполнить не удастся. Ниже представлены сценарии, не требующие использования белого списка: • если для `cms.visible` задано значение false и для `cms.default` задано значение CMS; • если CMS кластеризован и вы входите в систему с использованием имени кластера. Если вы пытаетесь войти в определенный кластер(CMS), имя CMS должно быть указано в свойстве `allowed.cms`; • если вход осуществляется через SSO.

18.5 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*.

18.5.1 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:

- `<КАТАЛОГ_УСТАНОВКИ_BOE>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf\apps\BOE.properties`

В системах UNIX файл `BOE.properties` располагается в следующей папке:

- `<КАТАЛОГ_УСТАНОВКИ_BOE>/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.

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`

Местоположения файлов OpenDocument

Тип файла	Местоположение
Пользовательский скрипт входа в систему	`WEB-INF\eclipse\plugins\webpath.OpenDocument\web\opendoc\custom.jsp`

Тип файла	Местоположение
Каталог для дополнительных файлов	`WEB-INF\eclipse\plugins\webpath.OpenDocument\web\noCacheCustomResources`
Пользовательский URL-адрес для входа в систему	`http://<servername>:<port>/BOE/OpenDocument/opendoc/custom.jsp`

18.5.2 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.faces`.

   ```
   function load() {window.location =  "logon.faces";}
   ```

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.

18.5.3 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.

> **Примечание**
>
> По соображениям безопасности доверительную аутентификацию не следует включать без HTTPS. Если доверительная аутентификация включена без HTTPS, это считается нарушением безопасности, поскольку URL-адрес отображается для неавторизованных пользователей. Во избежание нарушения безопасности информация пользователя может быть проверена с помощью действительного сертификата. Для получения дополнительных сведений см. 1388240.

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 CMC.

   На вкладке *Аутентификация* дважды щелкните *Enterprise* и установите флажок *Доверительная аутентификация включена*.

Связанные сведения

Включение доверительной аутентификации [страница 269]

Настройка доверительной аутентификации для веб-приложения [страница 276]

18.6 Настройка пользовательских интерфейсов приложений

Пользовательские интерфейсы некоторых приложений можно настраивать с помощью CMC.

В Central Management Console можно настраивать внешний вид некоторых приложений. Например, можно переключать элементы пользовательских интерфейсов.

18.6.1 Web Intelligence

18.6.1.1 Пользовательская настройка элементов интерфейса Web Intelligence по группам пользователей и папкам

Персонализация позволяет скрывать несколько элементов интерфейса, чтобы упростить взаимодействие конечных пользователей с приложением, в зависимости от групп пользователей и папок, содержащих документы Web Intelligence. Можно скрыть типы источников данных, переключить режим редактирования, отключить функцию автоматического обновления и многое другое.

По умолчанию каждый элемент интерфейса активирован. Чтобы скрыть их, используйте Central Management Console. В следующей таблице перечислены элементы пользовательского интерфейса, которые можно скрыть.

Список функций	Описание
Режим	Скрывает доступные режимы в списке раскрывающейся кнопки. • Чтение Скрыть режим чтения в списке раскрывающейся кнопки. • Разработка Скрыть режимы разработки и структуры из списка раскрывающейся кнопки. • Данные Скрыть режим данных в списке раскрывающейся кнопки. Если все режимы отключены, документы могут быть открыты только в режиме чтения.

Список функций	Описание
Местоположение	Скрывает целую категорию источников данных. Можно деактивировать следующие категории: • Репозиторий платформы BI • Локальные (доступные только в Rich Client) • Веб-службы • Google Диск • Microsoft OneDrive
Источник данных	В режиме разработки можно ограничить источники данных, доступные в диалоговых окнах *Выбрать источник данных* и *Изменить источник*. Можно отключить следующие источники данных: • Юниверсы • Документы Web Intelligence • Файлы Excel • Текстовые файлы • SAP BW • Представления SAP HANA • Запросы рукописного SQL • OData • Google Таблицы
Запрос	• Обновление В режиме чтения скрывает раздел *Данные* на панели инструментов. В режиме разработки скрывает раскрывающееся меню *Обновить*, команду *Обновить все*, кнопку *Выполнить* и раскрывающееся меню панели запросов. • Расширенное обновление В режиме разработки скрывает команду *Расширенное обновление* в раскрывающемся меню *Обновить*. • Автообновление Скрывает параметр *Автообновление* в режиме презентации. • Изменить источник В режиме разработки скрывает возможность изменения источников данных документа.
Данные	В режиме данных скрывает функции объединения кубов.

Список функций	Описание
Анализ	• Детализация В режимах чтения и разработки скрывает флажок *Детализация* в разделе "Анализ" панели инструментов и фильтры детализации на *панели фильтров*. Кроме того, в отчете значения, которые можно детализировать, не отображаются в виде гиперссылок, а действия детализации и значки, доступные для этих значений, скрыты. В режиме разработки скрывает фильтры детализации на панели *Построение* в области *Фильтры данных*. • Отслеживать изменение данных В режимах чтения и разработки скрывает кнопки *Отслеживать изменения данных* и *Показать изменения* на панели инструментов.
Документы	• *Создать*, *Открыть*, *Сохранить*, *Избранное*, *Режим презентации*. Скрывает соответствующие кнопки на панели инструментов. • Комментарии В режимах чтения и разработки скрывает вкладку *Комментарии* на боковой панели и команду *Комментарии* в контекстном меню. • Совместно используемые элементы В режиме разработки скрывает вкладку *Совместно используемые элементы* на боковой панели и команду *Совместно используемые элементы* в разделе *Вставка* панели инструментов.
Экспорт в	В любом режиме скрывает возможность экспорта документов отчета и кубов в: • Excel • PDF • HTML • TXT • CSV
Сгенерировать ссылку	В режиме разработки скрывает в контекстных меню возможность создания ссылок OpenDocument и генерирования ссылок OData для запросов и отдельных элементов отчетов.
Планирование и публикация	Скрывает возможность планирования и публикации документов в форматах TXT, XLS, PDF, HTML, MHTML и CSV.

18.6.1.1.1 Интерфейс настройки

Можно выбрать отдельные папки, чтобы к содержащимся в них документам автоматически применялись настройки. Просто выберите одну или несколько папок в области *Настраиваемые папки* и перейдите на вкладку *Функции*, чтобы начать настройку. По умолчанию настройка применяется ко всем документам в выбранной папке.

На вкладке *Функции* перечислены все функции, которые можно активировать или деактивировать. Используйте соответствующие флажки, чтобы включить или выключить их.

18.6.1.1.2 Правила настройки

При определении настроек, применяемых к пользователям, действуют следующие правила:

- Если пользователь принадлежит к нескольким группам, применяется только настройка для группы, чей идентификатор ниже. Настройка, определенная для других групп, в которые входит пользователь, не применяется.
- Если используется структура вложенных папок, непосредственная родительская папка документа, добавленная в список настраиваемых папок, определяет настройки документа, касающиеся элементов пользовательского интерфейса, функций и расширений.
- Настройка, определенная для папки Default Folders, применяется к документам, хранимым в папках "Персональные документы" и "Входящие", и к документам, для которых родительская папка не настроена.
- Настройка, определенная для элементов пользовательского интерфейса, имеет приоритет над настройкой для функций, так как функция играет лишь роль своеобразного ярлыка для включения всех элементов пользовательского интерфейса.
- Сценарий. Когда элементы пользовательской настройки отображаются в виде древовидного списка и вы отключаете узел в системе. Здесь при обновлении этой системы на новую версию продукта, имеющего новые позиции в узлах, эти позиции по умолчанию активируются, даже если верхний узел деактивирован.

18.6.1.1.3 Настройка внешнего вида интерфейса Web Intelligence

Внешний вид пользовательского интерфейса Web Intelligence можно настраивать, скрывая основные и дополнительные элементы меню, а также функции для выбранной группы пользователей и папки документов.

1. Войдите в консоль CMC с правами администратора.
2. В списке *Организовать* выберите *Пользователи и группы*.
3. В списке *Иерархия группы* выберите пользовательскую группу.
4. В списке *Действия* выберите *Настройка*.
5. В разделе *Настраиваемые папки* выполните одно из следующих действий:

Параметр	Описание
Определение настройки по умолчанию	1. Выберите *Default Folders* в области *Настраиваемые папки*.
Добавление папок документов, к которым необходимо применить настройку для выбранной группы пользователей	1. Нажмите *Добавить папку*. 2. Выберите папки. Папки будут добавлены в область *Настраиваемые папки*.
Автоматическое применение такой же настройки к другим папкам	1. В области *Настраиваемые папки* выберите папку, настройку которой необходимо скопировать.

Параметр	Описание
	2. В раскрывающемся списке выберите *Дублировать настройку*. 3. Выберите папку, к которой необходимо применить настройку. 4. Нажмите *Вставить настройку*. 5. Перейдите к шагу 7.
Удаление настройки для отдельной папки	1. В области *Настраиваемые папки* выберите папку. 2. В раскрывающемся списке выберите *Удалить папку*. 3. Перейдите к шагу 7. ⓘ Примечание Невозможно удалить *папки по умолчанию*.

6. Выберите или отмените выбор элементов на вкладке *Функции*, чтобы отобразить или скрыть их в Web Intelligence.

   Если отменить выбор всех дочерних элементов родительского элемента, выбор родительского элемента также будет отменен и скрыт в Web Intelligence. Для получения дополнительной информации см. Пользовательская настройка элементов интерфейса Web Intelligence по группам пользователей и папкам [страница 806].
7. Нажмите кнопку *Сохранить и закрыть*.

При сохранении настройки все пользователи выбранной группы увидят эти изменения, когда в следующий раз войдут в Стартовую панель BI и откроют Web Intelligence.

> ⓘ Примечание
>
> Рекомендуется войти в Стартовую панель BI под именем пользователя из только что настроенной группы, запустить Web Intelligence и удостовериться, что интерфейс изменен в соответствии с параметрами настройки.

18.6.1.2 Выравнивание содержимого Web Intelligence

Выберите способ отображения содержимого документа (слева направо или справа налево) при создании документов Web Intelligence пользователями.

Для интерфейса Rich Client выравнивание содержимого определяется языковыми стандартами, заданными в предпочтениях стартовой панели BI:

- Система использует выравнивание справа налево только в том случае, если предпочтительный языковой стандарт просмотра и языковой стандарт продукта задают языки с соответствующим направлением чтения.
- Во всех прочих случаях используется выравнивание слева направо.

> ⓘ Примечание
>
> Дополнительные сведения о настройке языковых параметров см. в *Руководстве пользователя стартовой панели Business Intelligence*.

> **Примечание**
>
> Выравнивание содержимого применяется только при создании документа и не влияет на существующие документы.

18.6.1.3 Включение точек расширения пользовательского интерфейса Web Intelligence для определенных групп пользователей

Можно настроить права Web Intelligence, чтобы разрешить выбранным группам пользователей получать доступ к пользовательским расширениям интерфейса. Для получения дополнительной информации о доступных пакетах расширений и вызовах API веб-служб REST см. *Руководство разработчика SAP BusinessObjects BI для Web Intelligence и семантического уровня BI*.

18.6.1.3.1 Включение точек расширения пользовательского интерфейса Web Intelligence

- В установке создано и развернуто соответствующее расширение. Разверните по одному расширению для каждой функции расширения (например, "Пользовательская кнопка" или "Сохранить как HTML").
- Расширение добавлено в список доверенных URL-адресов. В противном случае обратитесь к разделу Добавление доверенных URL-адресов в список авторизованных URL-адресов [страница 746].

1. Войдите в CMC как администратор.
2. В списке *Организовать* выберите *Пользователи и группы*.
3. В списке *Иерархия группы* выберите группу пользователей.
4. В списке *Действия* выберите *Настройка*.
5. Перейдите на вкладку *Расширения* и выполните одно из следующих действий:

Параметр	Описание
Добавление расширения OSGi, развертываемого на платформе BI и соответствующем сервере приложений	Выберите пользовательские расширения, которые вы хотите сделать доступными для пользователей.
Добавление расширения, отличного от OSGi, которое развертывается на сервере приложений платформы BI или на внешнем сервере приложений	1. Нажмите кнопку *Добавить*. 2. Введите URL-адрес расширения. Это URL-адрес файла JSON.

Параметр	Описание

	> **Примечание**
	> Замените все пробелы в URL-адресе символами `%20`.
	Примеры.
	• Сервер приложений Apache Tomcat:
	`http://myserver/webiextension/extension/SAP/RayLight_Embedded/extension.json`
	• Внешний сервер приложений:
	`http://www.mysite.org/documents/web/extension/Custom%20Button/extension.json`
	3. Если этого требует сервер приложений, выберите *Задать сведения о прокси-сервере* и введите имя сервера и номер порта.
	4. Выберите *Без аутентификации* или, если этого требует сервер приложений, выберите *Стандартная аутентификация* и введите имя пользователя и пароль.
	5. Нажмите кнопку *OK* и выберите расширение.
	6. Нажмите кнопку *Сохранить*.

Изменение сведений о расширении	Нажмите *Изменить*.
Удаление расширения из CMC	Выберите *Удалить*.

6. Нажмите кнопку *Сохранить и закрыть*.

Включенные расширения станут доступны выбранной группе пользователей при открытии документа, расположенного в выбранной папке. Точки расширения доступны всем клиентам приложений Web Intelligence: веб-клиентам, микроприложениям Java и Rich Client.

18.6.2 Стартовая панель BI

18.6.2.1 Включение очистки" значений подсказок в диалоговом окне "Расписание"

При планировании документа Web Intelligence на основе запроса BEx, который содержит подсказки SAP BW, пользователи стартовой панели BI могут очистить значение подсказки для того, чтобы оно было получено из переменной источника данных SAP BW во время выполнения документа, или исправить его перед выполнением задания планирования.

Следующая процедура позволяет отобразить в пользовательском интерфейсе два переключателя:

- *Использовать динамическое значение*: предоставьте источнику данных SAP BW возможность обработать значение.
- *Использовать постоянное значение*: введите фиксированное значение.

1. Выполните одно из следующих действий в папке `<InstallDir>\<WebAppServer>\webapps\BOE\WEB-INF\config\custom`:

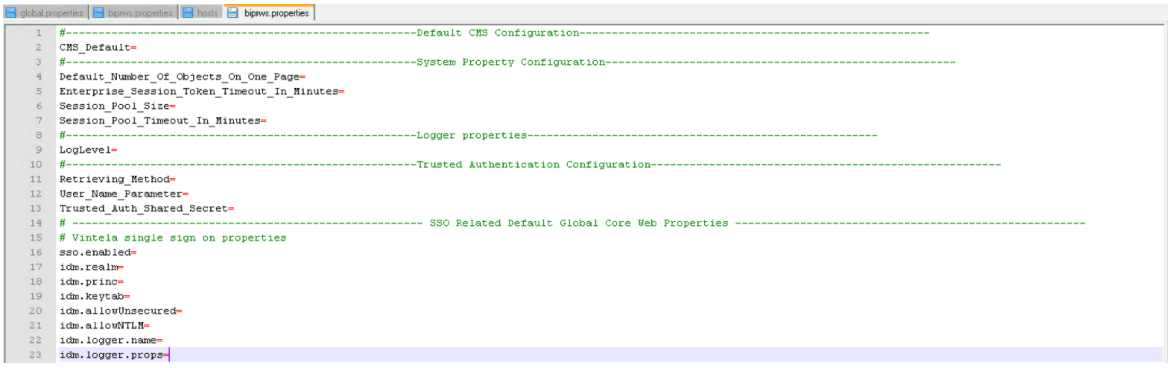
- Если файл `AnalyticalReporting.properties` расположен в папке, откройте файл в текстовом редакторе.
- Если файл `AnalyticalReporting.properties` отсутствует в папке, создайте файл с таким именем и откройте его в текстовом редакторе.

2. Выполните одно из следующих действий в файле `AnalyticalReporting.properties`:
   - Если файл уже существует, найдите свойство `bex.dynamic_variable.schedule` в файле и убедитесь, что для свойства установлено значение `true`.
   - Если файл `AnalyticalReporting.properties` создается, добавьте `bex.dynamic_variable.schedule=true` в конце файла.
3. Сохраните и закройте файл, перезапустите сервер веб-приложений.

18.7 Настройка веб-служб RESTful платформы BI на веб-сервере

Чтобы настроить конфигурацию для веб-служб RESTful, выполните следующие шаги:

1. Скопируйте файл: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps \biprws\WEB-INF\config\default\biprws.properties` to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps \biprws\WEB-INF\config\custom\biprws.properties` и откройте его для редактирования.
   Измените параметры.



   Ниже представлена таблица с описанием свойств, показанных на снимке экрана.

Свойство	Описание	Значение по умолчанию

`CMS_Default`	Пользователь может предоставить имя CMS и номер порта, а также имя кластера.
	Пример:
	`CMS_HOST_NAME:CMS_PORT_NUMBER`
	Или
	`@CMS_CLUSTER_NAME`
		0

`Default_Number_Of_Objects_On _One_Page`	Число записей на странице. Эту настройку можно переопределить с помощью параметра `&pageSize=<m>` в пакете SDK веб-служб RESTful.	50
`Enterprise_Session_Token_Timeout_In_Minutes)`	Время срока действия для маркера входа. По истечении этого времени потребуется создать новый маркер входа.	60
`Session_Pool_Size`	Число кэшированных сеансов, которое может быть сохранено в любой момент времени. 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
`Session_Pool_Timeout_In_Minutes`	Время в минутах, по истечении которого заканчивается срок действия кэшированных сеансов.	2

Свойство	Описание	Значение по умолчанию
`LogLevel`	Позволяет включить запись в журнал и присвоить уровню важности и детализации значение *Нет* (запись 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* (запись в журнал всех событий без исключения; используется только для отладки; использование ЦП может повыситься, что сказывается на производительности). Доступны следующие пункты меню: • `Unspecified` • `None` • `Low` • `Medium` • `High`	Не указано
Log_Location	Местоположение файла журнала, в котором зарегистрированы записи журналов использования для компьютера, где размещена платформа BI. **Примечание** • Если указан путь к несуществующей папке, будет создана новая папка. • Если в файле biprws.properties местоположение не указано, местоположение файла журнала становится местоположением по умолчанию.	Не указано

Свойство	Описание	Значение по умолчанию
`Retrieving_Method`	Меню, указывающее, какой метод запроса будет использоваться для извлечения маркеров входа доверительной аутентификации при использовании API /logon/trusted веб-службы RESTful. • `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`
`User_Name_Parameter`	Это метка, использующаяся для идентификации доверенного пользователя при извлечении маркера входа.	`X-SAP-TRUSTEDUSER`
`Trusted_Auth_Shared_Secret`	Строковое значение, создаваемое с помощью шагов, указанных в разделе Создание значения общего секретного ключа [страница 425].	Не указано
`Basic_Auth_Supported`	Активация базовой аутентификации на веб-сервере Tomcat. Возможные значения: `True` и `False`.	Не указано
`Basic_Auth_Type`	Установка типа аутентификации `secEnterprise`, `secLDAP`, `secSAPR3`, или `secWinAD` для поддержки базовой аутентификации.	`secEnterprise`

2. Перезапустите Tomcat.

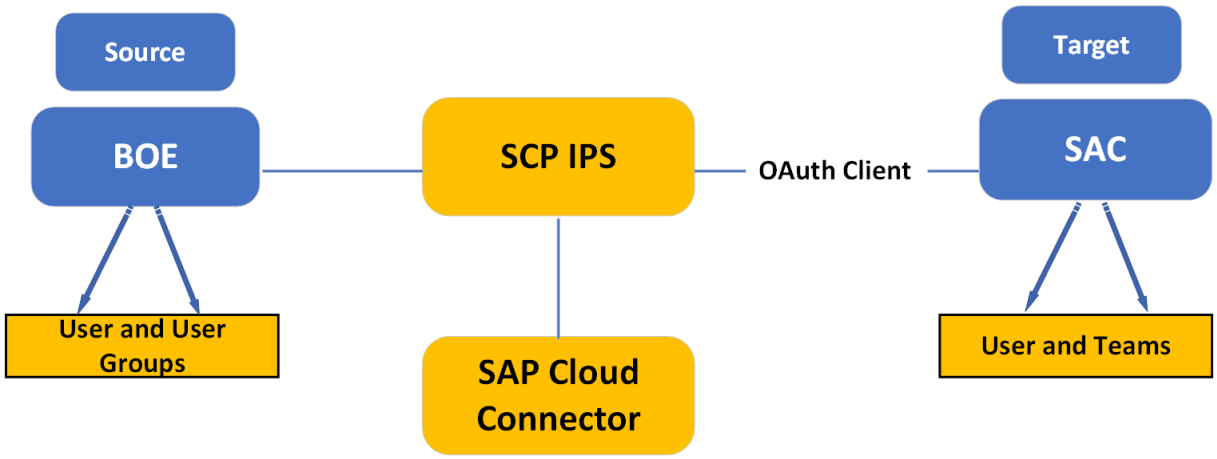
18.8 Гибридное управление пользователями

Компания SAP уделяет особое внимание стратегии "облако в приоритете", и клиенты также быстрее переходят к гибридным решениям, где они управляют активами между локальной средой и облаком. Первостепенная задача SAP – предоставить службы из платформы SAP BusinessObjects BI, которые позволяют это сделать.

Это достигается благодаря представлению системы для API-интерфейсов (внутренних) провизионирования пользователей на основе междоменного управления идентичностью (SCIM), которые могут использоваться службой SAP Cloud Platform Identity Provisioning (SCP IPS) для провизионирования пользователей Enterprise платформы BI в любую другую поддерживаемую систему SCIM с использованием службы Identity Provisioning (IPS) (главным образом, SAP Analytics Cloud).

С использованием SCP IPS и платформы SAP BusinessObjects BI 4.2 SP06 или выше пользователей Enterprise платформы BI теперь можно провизионировать в любую поддерживаемую целевую систему SCIM.

На следующем рисунке представлен гибридный сценарий и показано, как включить службы между локальными и облачными системами.



18.9 Провизионирование локальных пользователей в SAP Analytics Cloud

Для провизионирования сущностей (пользователей, групп, ролей) из одной системы в другую на предприятии сначала необходимо добавить и настроить эти системы в качестве исходной и целевой систем в интерфейсе пользователя Identity Provisioning.

Можно провизионировать пользователей локальной системы (BOE) в SAP Analytics Cloud через службу SAP Cloud Platform Identity Provisioning (PVS IPS), выполнив несколько простых шагов.

1. Установить соединение между локальной системой и облаком
2. Создать учетные данные OAuthClient в SAP Analytics Cloud
3. Настроить исходную систему

4. Настроить целевую систему
5. Провизионировать пользователей и группы пользователей в SAP Analytics Cloud
6. Просмотреть провизионированных пользователей и группы пользователей

18.9.1 Установить соединение между локальной системой и облаком

Можно установить соединение между локальной системой и облаком (системой Identity Provisioning) с помощью облачного коннектора SAP (системы IPS).

Установлен облачный коннектор.

1. Запустите страницу администрирования облачного коннектора SAP и войдите в: `https://<HCC HOST>:8443`.

   > ⓘ Примечание
   >
   > Замените `<HCC HOST>` именем хоста системы, в которой установлен облачный коннектор.

2.
3. На панели навигации выберите *Коннектор*, затем щелкните значок + (*Добавить подчиненную учетную запись*).

   Появится диалоговое окно *Добавить подчиненную учетную запись*.

4. Введите следующие данные для своей учетной записи IPS:

   > ⓘ Примечание
   >
   > Для пользователя подчиненной учетной записи в IPS требуются полномочия *Управление локальными соединениями*. *Хост региона* и *имя подчиненной учетной записи* можно найти в разделе *Поддержка – Информация учетной записи* в IPS.

   a. *Хост региона*: в списке выберите хост региона.
   b. *Имя подчиненной учетной записи*: добавьте имя своей учетной записи. Например, dd00bb33.
   c. (Необязательно) *Отображаемое имя*: добавьте имя для учетной записи.
   d. *Пользователь подчиненной учетной записи*: добавьте имя пользователя подчиненной учетной записи (S-пользователя).
   e. *Пароль*: добавьте пароль S-пользователя.
   f. *Ид. местоположения*: оставьте пустым, чтобы использовать местоположение по умолчанию.
   g. (Необязательно) *Описание*: добавьте описание облачного коннектора.

5. Нажмите кнопку *Сохранить*.
6. На панели навигации в разделе *DisplayName* выберите *Облако для локальной системы*.

   DisplayName – имя арендатора облачного коннектора.

7. На вкладке *Контроль доступа* щелкните значок + (Добавить).

   Откроется диалоговое окно *Редактировать сопоставление системы*.

8. Добавьте запрашиваемую информацию о сопоставлении системы для системы платформы BI, сервера веб-приложений (например, Tomcat), на котором размещается biprws:

a. *Тип бэкэнда*: в раскрывающемся списке выберите другую систему SAP.
b. *Протокол*: в раскрывающемся списке выберите HTTP.
c. (Необязательно) *Виртуальный хост*: хостом и портом по умолчанию являются внутренние хост и порт. Можно переименовать хост и порт, чтобы имя и порт внутреннего хоста не отображались.
d. (Необязательно) *Виртуальный порт*: это номер порта, используемый виртуальным хостом.
e. *Внутренний хост*: это имя хоста для WAS (например, Tomcat), на котором размещается веб-служба Restful (biprws).
f. *Внутренний порт*: это номер порта, используемый внутренним хостом. (Порт, где развернуты веб-службы RESTful BIP, например biprws.)
g. *SAProuter*: оставьте это поле незаполненным.
h. *Тип принципала*: в раскрывающемся списке выберите "Нет".
i. *Имя партнера SNC*: оставьте это поле незаполненным.
j. (Необязательно) *Описание*: добавьте описание системы.

9. Установите флажок *Проверить внутренний хост* и нажмите *Сохранить*.
10. Выберите систему, добавленную в список *Сопоставление виртуальной системы с внутренней системой*.
11. В области *Доступные ресурсы* щелкните значок + (Добавить).

    Откроется диалоговое окно *Добавить ресурс*.
12. Добавьте следующие сведения о ресурсах для своей учетной записи:
    a. *Путь URL*: /biprws/sbop/internal/v2/scim.
    b. *Включено*: убедитесь, что флажок установлен.
    c. *Политика доступа*: выберите переключатель *Путь и все под-пути*.
    d. (Необязательно) *Описание*: добавьте описание ресурса.
13. Нажмите кнопку *Сохранить*.

> ⓘ Примечание
>
> Статус рядом с виртуальным хостом должен быть зеленым.

18.10 Создание учетных данных клиента OAuth в SAP Analytics Cloud

Чтобы создать учетные данные клиента OAuth в SAP Analytics Cloud, выполните следующие шаги:

1. Войдите в SAP Analytics Cloud.
2. В главном меню выберите *Система > Администрирование > Интеграция приложений*.
3. Выберите *Новый клиент OAuth*.
4. Укажите нужное имя.
5. В качестве *Цели* выберите *Доступ к API*.
6. В разделе "Доступ" выберите *Провизионирование пользователя*.
7. Нажмите *Добавить*.

   В списке *Настроенные клиенты* выберите клиента, который был только что добавлен.

> **Примечание**
>
> Щелкните значок ✎ (Редактировать), чтобы просмотреть сгенерированные идентификатор клиента OAuth и секретный ключ (пароль). Эти учетные данные необходимы при настройке целевой системы.
>
> Идентификатор клиента OAuth соответствует вашему имени пользователя в сведениях о конфигурации целевой системы в PSP IPS, а секретный ключ – вашему паролю.

18.11 Настроить исходную систему

Необходимо настроить сведения исходной системы, из которой требуется провизионировать пользователей и группы пользователей в службе SAP Cloud Platform Identity Provisioning (SDP IPS).

1. Войдите в SDP IPS.
2. На домашней странице выберите плитку *Исходные системы*.
3. Щелкните значок + (Добавить) в нижней части левой панели.
4. В комбинированном списке *Тип* выберите тип системы, который требуется использовать.
5. Добавьте имя системы. (Убедитесь, что не дублируется имя другой системы.)
6. (Необязательно) Введите описание системы, чтобы в дальнейшем было легко отличить ее в списке.
7. Нажмите кнопку *Сохранить*.

   Новая система отображается на левой панели.

   Внимание: если не сохранить систему на этом этапе, то преобразования и свойства по умолчанию не будут отображаться.
8. Теперь щелкните значок ✎ (Редактировать), чтобы просмотреть преобразования и добавить свойства конфигурации.
9. Добавьте следующие сведения:
   a. *Аутентификация*: BasicAuthentication.
   b. *Хост*: <имя хоста и порт BOE>.
   c. *ips.delta.read*: включено.
   d. *ips.full.read.force.count*: 2.
   e. *ips.trace.failed.entity.content*: true.
   f. *Пароль*: <пароль пользователя-администратора BOE>.
   g. *Тип прокси*: OnPremise.
   h. *scim.group.filter*: <ид. или CUID группы пользователей>.

      Например, `scim.group.filter: groupId eq "4214"`.
   i. *scim.user.filter*: <ид. или CUID пользователя>.

      Например, `scim.filter.filter: userId in "8077"` или `scim.user.filter: userCuid in "AQ.rQ1V1FR9JmQoQa0xYfII"`.
   j. *Тип*: HTTP.
   k. *URL*: http://имя хоста: порт/biprws/sbop/internal/v2/scim.

l. *Пользователь*: администратор.

> ⓘ Примечание
>
> - Можно предоставить подробные сведения о локальной системе с нуля или путем импорта существующего файла с информацией о конфигурации.
> - С помощью преобразований можно указать определенные ограничения или условия, касающиеся исходной системы.
> - Выбираемое место назначения соединения должно соответствовать релевантному типу системы. Место назначения должно указывать все настройки соединения, необходимые для сценария Identity Provisioning.
> - Имя хоста/порт, указанные в поле URL, должны совпадать с именем виртуального хоста/портом, указанными в облачном коннекторе.

10. Если поле *Имя адресата* пропускается, можно открыть вкладку *Свойства*, чтобы ввести все свойства соединения и конфигурации, необходимые для сценария провизионирования.
11. При необходимости преобразование системы по умолчанию можно изменить.
12. Сохраните изменения.

> ⓘ Примечание
>
> В конце URL-адреса Identity Provisioning отображается строка, разделенная дефисами. Это автоматически сгенерированный уникальный идентификатор созданной новой системы.

18.12 Настроить целевую систему

Сначала убедитесь, что в SAP Analytics Cloud созданы учетные данные клиента OAuth.

1. На домашней странице откройте вкладку *Целевая система*.
2. На вкладке *Сведения* укажите имя системы SAP Analytics Cloud, URL-адрес SAP Analytics Cloud и исходные системы.

> ⓘ Примечание
>
> По умолчанию здесь отображаются исходные системы, которые уже настроены.

3. Откройте вкладку *Свойства*.
4. Добавьте следующие сведения:
   a. *Аутентификация*: BasicAuthentication.
   b. *csrf.token.path*: api/v1/scim/Users?count=1.
   c. *ips.trace.failed.entity.content*: true.
   d. *URL-адрес OAuth2TokenService*: <OAuthClientTokenURL>.
   e. *Пароль*: <секрет, сгенерированный в ходе конфигурации OAuthClient>.
   f. *Тип прокси*: Интернет.
   g. *scim.api.csrf.protection*: активировано.
   h. *Тип*: HTTP.

i. *URL-адрес*: URL-адрес SAP Analytics Cloud.
j. *Пользователь*: <ид. клиента OAuth>.

18.13 Провизионирование пользователей и групп пользователей в SAP Analytics Cloud

После настройки исходной и целевой систем с помощью службы SAP Cloud Platform Identity Provisioning можно провизионировать их с вкладки *Задания* в окне *Сведения об исходной системе*.

Для пользователей платформы BI, которые будут провизионированы, должны быть настроены адреса электронной почты.

1. Щелкните плитку *Исходная система*.
2. Нажмите *Задания*.
3. В разделе *Задания* для *Типа задания*: *задание чтения* выберите действие *Выполнить сейчас*.

   > ⓘ Примечание
   >
   > Если вы изменили пользователей или группы пользователей в BOE, выберите *Задание повторной синхронизации*, чтобы обеспечить обновление изменений в SAP Analytics Cloud.

4. Чтобы просмотреть динамику, на левой панели выберите *Журналы заданий* и просмотрите *Статус* инициированных заданий.
5. Чтобы просмотреть сведения о выполнении задания, щелкните соответствующую строку.

   Откроется окно *Сведения о выполнении задания* со статусом действий.

18.14 Просмотр провизионированных пользователей в SAP Analytics Cloud

1. Перейдите в главное меню > *Безопасность* > *Группы*.
2. Перейдите к странице *Группы*.
3. Выберите группу пользователей BOE.
4. Щелкните *Члены группы*, чтобы просмотреть список пользователей, провизионированных из BOE в SAP Analytics Cloud.

   > ⓘ Примечание
   >
   > Также можно просмотреть список пользователей из меню *Пользователи* в разделе *Безопасность*.

18.15 Образцы шаблонов

Для провизионирования пользователя или группы пользователей можно использовать следующие шаблоны.

Образец конфигурации исходной системы

```
{ "connectorTypeString": "SCIM", "accessMode": "READ",
"alias": "SBOP_10.47.228.194",
"relatedSystems": [
],
"gitAllowedExpressions": [
],
"gitDisallowedExpressions": [
],
"emailSubscribers": [
],
"name": "SBOP_43",
"state": "ENABLED",
"transformation": {
"user": {
"condition": "($.memberOf contains '7741') || ($.memberOf contains '7962') ||
($.id contains '8077') || ($.id contains '8081')",
"mappings": [
{
"sourcePath": "$",
"targetPath": "$"
},
{
"sourcePath": "$.id",
"targetVariable": "entityIdSourceSystem"
},
{
"targetPath": "$.id",
"type": "remove"
},
{
"targetPath": "$.meta",
"type": "remove"
}
]
},
"group": {
"condition": "$.id contains '7741' || $.id contains '7962'",
"mappings": [
{
"sourcePath": "$",
"targetPath": "$"
},
{
"sourcePath": "$.id",
"targetVariable": "entityIdSourceSystem"
},
{
"targetPath": "$.id",
"type": "remove"
},
{
"targetPath": "$.meta",
"type": "remove"
}
]
}
},
"properties": {
```

```
"Type": "HTTP",
"User": "Administrator",
"ips.full.read.force.count": "2",
"Authentication": "BasicAuthentication",
"host": "adept6991435:6400",
"scim.group.filter": "groupId eq \"7741,7962\" or groupCuid eq
\"ATKZxWcAGfhOnHwu_A_uyAc,AYIbS.o1pSlDmjcUS107aCQ\"",
"ProxyType": "OnPremise",
"ips.delta.read": "enabled",
"ips.trace.failed.entity.content": "true",
"URL": "http://adept6991435:6405/biprws/sbop/internal/v2/scim",
"Password": "Password1",
"scim.user.filter": "groupId eq \"7741\" and groupCuid eq
\"ATKZxWcAGfhOnHwu_A_uyAc,AYIbS.o1pSlDmjcUS107aCQ\" and userId in \"8077\" or
userCuid in \"AQ.rQ1V1FR9JmQoQa0xYfII\""
},
"encryptedProperties": {
},
"gitFetchAllowed": false
}
```


Образец преобразования


```
{
"connectorTypeString": "SAP_ANALYTICS_CLOUD",
"accessMode": "WRITE",
"destinationName": " ",
"alias": "https://idcsac.jp1.sapanalytics.cloud",
"relatedSystems": [
"SBOP_43"
],
"gitAllowedExpressions": [
],
"gitDisallowedExpressions": [
],
"emailSubscribers": [
],
"name": "SAC-Machine",
"state": "ENABLED",
"transformation": {
"user": {
"mappings": [
{
"sourcePath": "$.schemas",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.schemas"
},
{
"sourceVariable": "entityIdTargetSystem",
"targetPath": "$.id"
},
{
"sourcePath": "$.userName",
"targetPath": "$.userName"
},
{
"sourcePath": "$.name",
"targetPath": "$.name"
},
{
"sourcePath": "$.displayName",
"optional": true,
"targetPath": "$.displayName"
},
{
"sourcePath": "$.active",
```

```
"optional": true,
"targetPath": "$.active"
},
{
"sourcePath": "$.emails",
"preserveArrayWithSingleElement": true,
"targetPath": "$.emails"
},
{
"condition": "$.emails[0].length() > 0",
"constant": true,
"targetPath": "$.emails[0].primary"
},
{
"constant": [
"PROFILE:sap.epm:BI_Admin"
],
"preserveArrayWithSingleElement": true,
"targetPath": "$.roles"
},
{
"sourcePath": "$.groups",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.groups"
},
{
"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['value']",
"optional": true,
"targetPath": "$['urn:scim:schemas:extension:enterprise:1.0']['manager']
['managerId']",
"functions": [
{
"type": "resolveEntityIds"
}
]
}
]
},
"group": {
"mappings": [
{
"sourcePath": "$.schemas",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.schemas"
},
{
"condition": "$.displayName EMPTY false",
"sourcePath": "$.displayName",
"targetPath": "$.id"
},
{
"condition": "$.id EMPTY false",
"sourcePath": "$.id",
"targetPath": "$.id"
},
{
"sourcePath": "$.displayName",
"optional": true,
"targetPath": "$.displayName"
},
{
"sourcePath": "$.roles",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.roles"
```

```
},
{
"sourcePath": "$.members[*].value",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.members[?(@.value)]",
"functions": [
{
"type": "resolveEntityIds"
}
]
}
]
}
},
"properties": {
"Type": "HTTP",
"User": "<exampleusername>",
"Authentication": "BasicAuthentication",
"OAuth2TokenServiceURL": "https://oauthasservices-
gf097393f.jp1.hana.ondemand.com/oauth2/api/v1/token",
"csrf.token.path": "/api/v1/scim/Users?count=1",
"ProxyType": "Internet",
"ips.trace.failed.entity.content": "true",
"URL": "https://idcsac.jp1.sapanalytics.cloud",
"scim.api.csrf.protection": "enabled",
"Password": "<examplepassword>"
},
"encryptedProperties": {
},
"gitFetchAllowed": false
}
```

19 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 платформы BI в папке "Соединения".

Дизайнеры определяют юниверсы на основании соединений. Пользователи приложений запросов, анализа и отчетности получают доступ к базе данных с помощью юниверса, что избавляет их от необходимости знать о расположенных в основе базы данных структурах данных.

Соединения могут быть созданы с помощью следующих приложений:

- Средство создания юниверсов: соединения сохраняются в репозитории.
- Средство дизайна информации: соединения можно создавать локально и публиковать в репозитории, а также создавать и редактировать 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.

Связанные сведения

Управление настройками безопасности для объектов в CMC [страница 138]
Права соединений [страница 1190]

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.

Связанные сведения

Управление настройками безопасности для объектов в CMC [страница 138]
Средство создания юниверсов [страница 1195]
Права юниверсов (.unv) [страница 1185]
Средство дизайна информации [страница 1196]
Права юниверсов (.unx) [страница 1187]

19.2.1 Удаление юниверсов

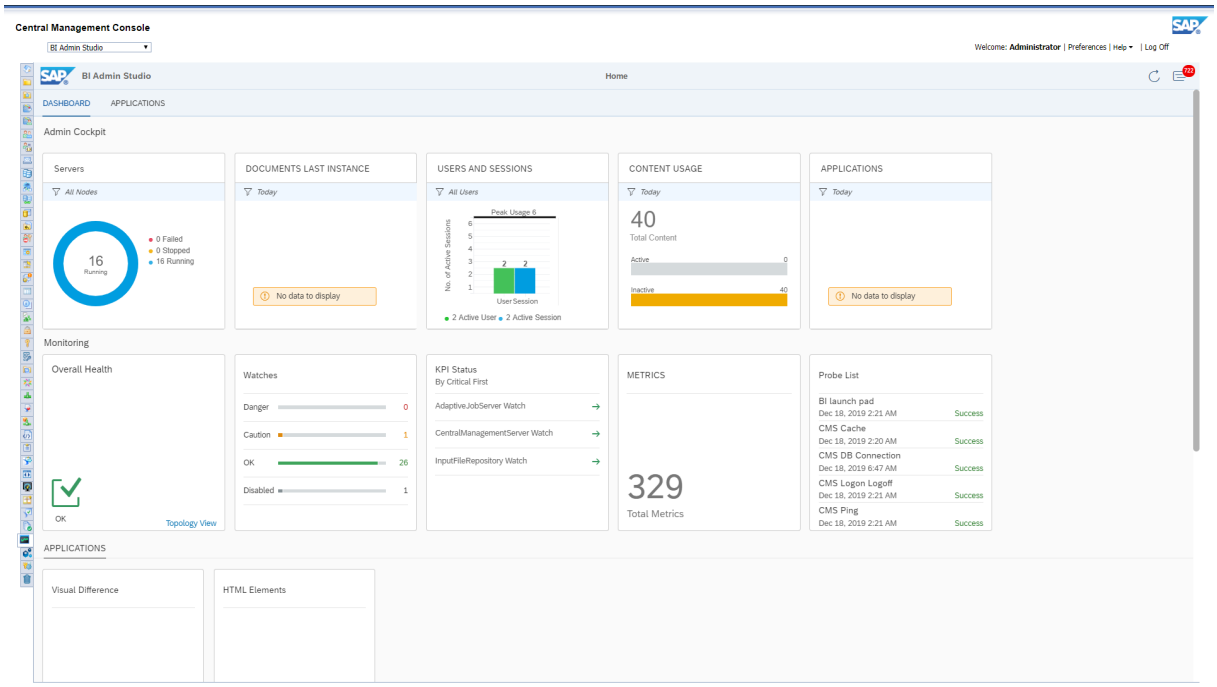
> → Совет
>
> Юниверсы также можно удалять с помощью средства дизайна информации.

1. В области CMC *Юниверсы* выберите в списке юниверс.
2. Выберите *Управление* > *Удалить*.
3. При запросе подтверждения нажмите кнопку *OK*.

20 BI Admin Studio

BI Admin Studio – приложение в CMC, включающее мониторинг, предупреждения и рабочее место администратора, ранее известное как пульт администрирования BI.

Приложение содержит две вкладки, *Инструментальная панель* и *Приложения*.



Инструментальная панель

На вкладке *Инструментальная панель* содержится одно представление инструментальных панелей, доступных в *Рабочем месте администратора* и *Мониторинге*. Каждую инструментальную панель можно щелкнуть, чтобы получить подробную информацию о ней. Например, можно выбрать инструментальную панель *Серверы*, чтобы получить список серверов, имеющих *статус Выполняется*, *Остановлено* и *Сбой*, а также такие сведения, как *Имя сервера*, *PID* и *Тип*. Для получения дополнительных сведений о рабочем месте администратора см. Рабочее место администратора [страница 831], о мониторинге см. Мониторинг [страница 836].

Приложения

Visual Difference и *Авторизованные элементы HTML* доступны на вкладке *Приложения*. Для получения дополнительных сведений о *Visual Difference* см. Визуальное отличие [страница 859], об *элементах HTML* см. Авторизация элементов HTML [страница 862].

Предупреждения

Для получения доступа к области уведомлений для предупреждений можно выбрать . В области уведомлений можно выбрать параметр *На страницу предупреждений*, чтобы получить дополнительные сведения о созданных предупреждениях.

20.1 Рабочее место администратора

Рабочее место администратора — это новое приложение, добавленное в CMC. Он позволяет администратору собирать базовые данные о среде BI. Это означает извлечение бизнес-аналитики из данных в среде BI. С помощью рабочего места администратора можно получать информацию о серверах, запланированных заданиях, пользователях и сеансах, а также об использовании контента и приложениях.

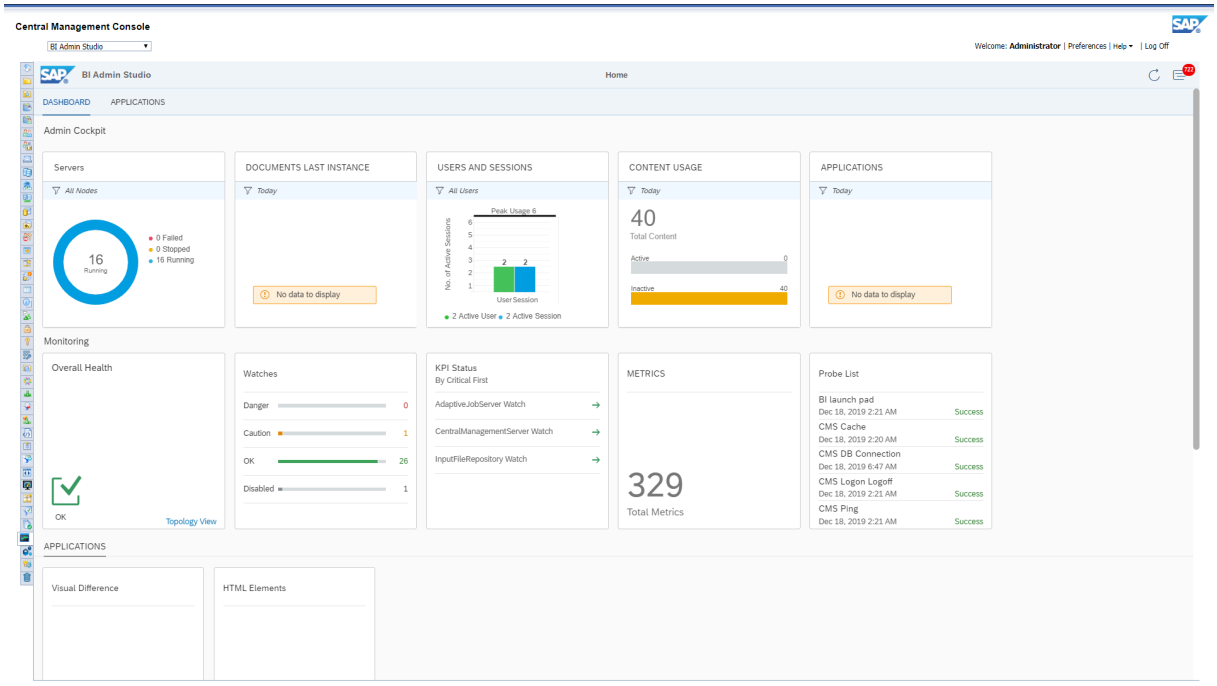
> **Примечание**
>
> Для успешного использования рабочего места администратора необходимо соблюдение следующих требований:
>
> - Должна быть активна служба мониторинга.
> - Необходимо включить аудит и соответствующее событие для извлечения правильных данных.
> - Веб-служба RESTful в платформе BI должна быть доступна для клиентов.
> - Должен быть запущен WACS, если веб-служба RESTful не развернута на Tomcat.
> - Если настраивается SSL для CMC, также необходимо настроить SSL для WACS, если веб-служба RESTful не развернута на Tomcat.
> - Требуется междоменный доступ.
> - Для доступа к рабочему месту администратора пользователи должны входить в группу администраторов или любую ее подгруппу.

20.1.1 Рабочее место администратора

В рабочем месте администратора отображается комплексный анализ данных, связанных со следующими компонентами графической визуализации:

- Серверы
- Последний экземпляр документа
- Пользователи и сеансы
- Использование контента
- Приложение

> **Примечание**
>
> Для просмотра анализа компонентов *Использование контента* и *Приложение* должна быть включена база данных аудита.



Чтобы обновить данные на каждой странице рабочего места администратора, щелкните значок в правом верхнем углу главной страницы.

20.1.2 Бизнес-аналитическая информация о серверах

В рабочем месте администратора можно просмотреть данные реального времени о статусе и связанные сведения для всех серверов в среде BI.

На домашней странице содержатся следующие сведения:

- Общее число серверов
- Число серверов с ошибками
- Число остановленных серверов

Можно фильтровать данные, представленные на плитке *Серверы*, выбирая нужный кластер серверов.

После выбора плитки *Серверы* откроется страница "Серверы" с детальной информацией об общем числе серверов, серверах, вызывающих ошибки, и остановленных серверах. Для каждого сервера, вызывающего ошибки, на странице "Серверы" также приводятся следующие данные: *Статус*, *Имя сервера*, *PID* (идентификатор процесса), *Тип*, *Состояние* и *Время последнего изменения*.

На странице *Серверы* можно фильтровать данные по конкретным кластерам серверов, выбирая нужные кластеры.

Для просмотра более подробной информации о сервере, вызывающем ошибки, нужно выбрать соответствующую строку. Откроется следующая страница с детальным описанием причины ошибки. Чтобы снова запустить сервер, вызывающий ошибки, нужно выбрать на этой странице команду *ЗАПУСК*.

20.1.3 BI в экземплярах документов

В рабочем месте администратора можно просматривать данные о статусе и связанные сведения для всех экземпляров запланированных документов в среде BI.

На домашней странице содержится следующая информация:

- Общее число последних экземпляров всех запланированных документов.
- Число последних запущенных экземпляров всех запланированных документов.
- Число последних вызывающих ошибки экземпляров всех запланированных документов.
- Число последних ожидающих обработки экземпляров всех запланированных документов.

На плитке *Последний экземпляр документа* можно отфильтровать данные по определенному временному диапазону, выбрав нужный диапазон времени в раскрывающемся меню. Доступные диапазоны времени:

- Текущая дата
- Последние 7 дней
- Последние 30 дней
- Квартал
- Год

Щелкнув плитку *Последний экземпляр документа*, можно перейти на страницу последних экземпляров, где содержатся сведения об общем числе последних экземпляров всех запланированных документов с разбивкой по статусу: "Выполняется", "Ошибка", "Ожидание". На вкладке *Статистика* содержатся сведения, которые можно просмотреть в разделах *Документы с наибольшим числом экземпляров* и *Экземпляры с наиболее длительным временем выполнения*. Также на странице экземпляров документов для каждого экземпляра со статусом ошибки указывается *Имя экземпляра*, *Статус*, *Тип*, *Владелец* и *Время окончания*.

Данные, отображаемые на странице *Последние экземпляры*, можно экспортировать в виде CSV-файла, нажав кнопку ссылки экспорта. Кроме того, можно экспортировать выбранные экземпляры, установив соответствующие флажки и выбрав команду *Экспортировать выбранные* в раскрывающемся меню экспорта.

Для просмотра более подробной информации о вызывающем ошибку экземпляре нужно выбрать соответствующую строку. Можно повторно запустить задание на странице, выбрав команду *ВЫПОЛНИТЬ*.

На вкладке статистики активирован новый фильтр диаграмм, позволяющий фильтровать и просматривать первые 5, 10, 15 или 20 документов.

20.1.4 BI – пользователи и сеансы

В рабочем месте администратора можно просмотреть данные о пользователях и сеансах в среде BI.

Например, на домашней странице содержатся следующие сведения:

- Число активных пользователей
- Число активных сеансов

На плитке *Пользователи и сеансы* можно фильтровать данные по следующим категориям:

- Все пользователи
- Зарегистрированные пользователи
- Параллельные пользователи

При щелчке на плитке *Пользователи и сеансы* вы переходите на одноименную страницу, на которой представлены разделы "Все пользователи", "Первые пользователи" и "Статистика". На вкладке "Статистика" представлены подробные сведения о самых активных и неактивных пользователях.

Кроме того, на странице "Пользователи и сеансы" представлены следующие сведения: *Имя пользователя*, *Общее количество сеансов*, *Время последнего входа в систему* и *Самый длинный активный сеанс*.

Для просмотра более подробной информации о конкретном пользователе нужно выбрать соответствующую строку. При этом откроется новая страница с детальным описанием первых сеансов указанного пользователя. С этой страницы вы можете завершить любой сеанс этого пользователя, выбрав нужный сеанс и щелкнув *ЗАВЕРШИТЬ СЕАНС*.

20.1.5 Бизнес-аналитическая информация об использовании контента

В рабочем месте администратора можно просмотреть данные об использовании контента в среде BI.

Например, на домашней странице содержатся следующие сведения:

- Число активных документов
- Число неактивных документов

На плитке *Использование контента* можно отфильтровать данные по определенному временному диапазону, выбрав нужный диапазон времени в раскрывающемся меню.

> **Примечание**
>
> Если какой-либо активный контент удален и данные фильтруются по определенному временному диапазону, удаленный элемент будет по-прежнему указан в активном контенте, если он был активным в выбранном временном диапазоне.

Доступные диапазоны времени:

- Текущая дата
- Последние 7 дней
- Последние 30 дней
- Квартал
- Год

После выбора плитки *Использование контента* откроется страница использования контента с детальной информацией об активном контенте, неактивном контенте и статистике. На вкладке Статистика приводятся сведения, относящиеся к папкам входящей почты с наибольшим количеством неактивного контента, юниверсам и папкам с наибольшим количеством содержимого.

Вы можете экспортировать данные, отображаемые на странице *Использование контента*, в CSV-файл, нажав соответствующую кнопку для экспорта ссылки. Кроме того, вы можете экспортировать выбранные задания, установив соответствующий флажок и выбрав команду *Экспортировать выбранные* в раскрывающемся меню экспорта.

На странице использования контента также приводятся следующие сведения: *Имя контента*, *Тип* и *Время выполнения*.

На вкладке статистики активирован новый фильтр диаграмм, позволяющий фильтровать и просматривать первые 5, 10, 15 или 20 документов.

20.1.6 Бизнес-аналитическая информация о приложениях

В рабочем месте администратора можно просмотреть данные о числе приложений с сортировкой по именам приложений в среде BI.

На плитке *Приложение* можно отфильтровать данные по определенному диапазону времени, выбрав нужный диапазон в раскрывающемся меню. Доступные диапазоны времени:

- Текущая дата
- Последние 7 дней
- Последние 30 дней
- Квартал
- Год

После выбора плитки *Приложения* откроется страница приложений с детальной информацией о *Всех приложениях* и *Популярных приложениях*.

На вкладке *Популярные приложения* приводится список пяти самых популярных приложений с наибольшим числом документов, созданных за указанный диапазон времени. Также на странице

приложений содержатся следующие сведения: *Имя приложения*, *Число пользователей* и *Число артефактов*.

20.2 Мониторинг

Приложение мониторинга позволяет фиксировать оперативные и исторические показатели серверов платформы BI для ведения отчетности и создания уведомлений. Приложение мониторинга помогает администраторам системы 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.

Приложение мониторинга поддерживает выполнение следующих задач:

- Проверка производительности каждого сервера: возможна благодаря использованию наблюдений, которые показывают состояние каждого сервера в виде цветовых индикаторов. Администратор системы может задавать пороговые значения для этих наблюдений и получать предупреждения в случае превышения пороговых значений, а также принимать соответствующие меры при возникновении 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 (в графическом и табличном виде) по группам серверов, категориям служб и узлам Enterprise.
- 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 серверов и 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.
- Отслеживание значения показателя *Уровень аудита* на *центральном сервере управления*, когда для параметра *Установить события* выбрано значение *Выкл.* (значение показателя 1). Предусмотрена возможность создания списка наблюдений; если значение показателя равно 1, в списке наблюдений отправляется тестовое предупреждение, а также предупреждение по электронной почте.

Дополнительную информацию об использовании приложения мониторинга, включая сведения о зондах и наблюдениях, см. в *Интерактивной справке по CMC платформы SAP BusinessObjects Business Intelligence*.

Связанные сведения

О приложении "Показатели сервера" [страница 1240]

20.2.1 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.

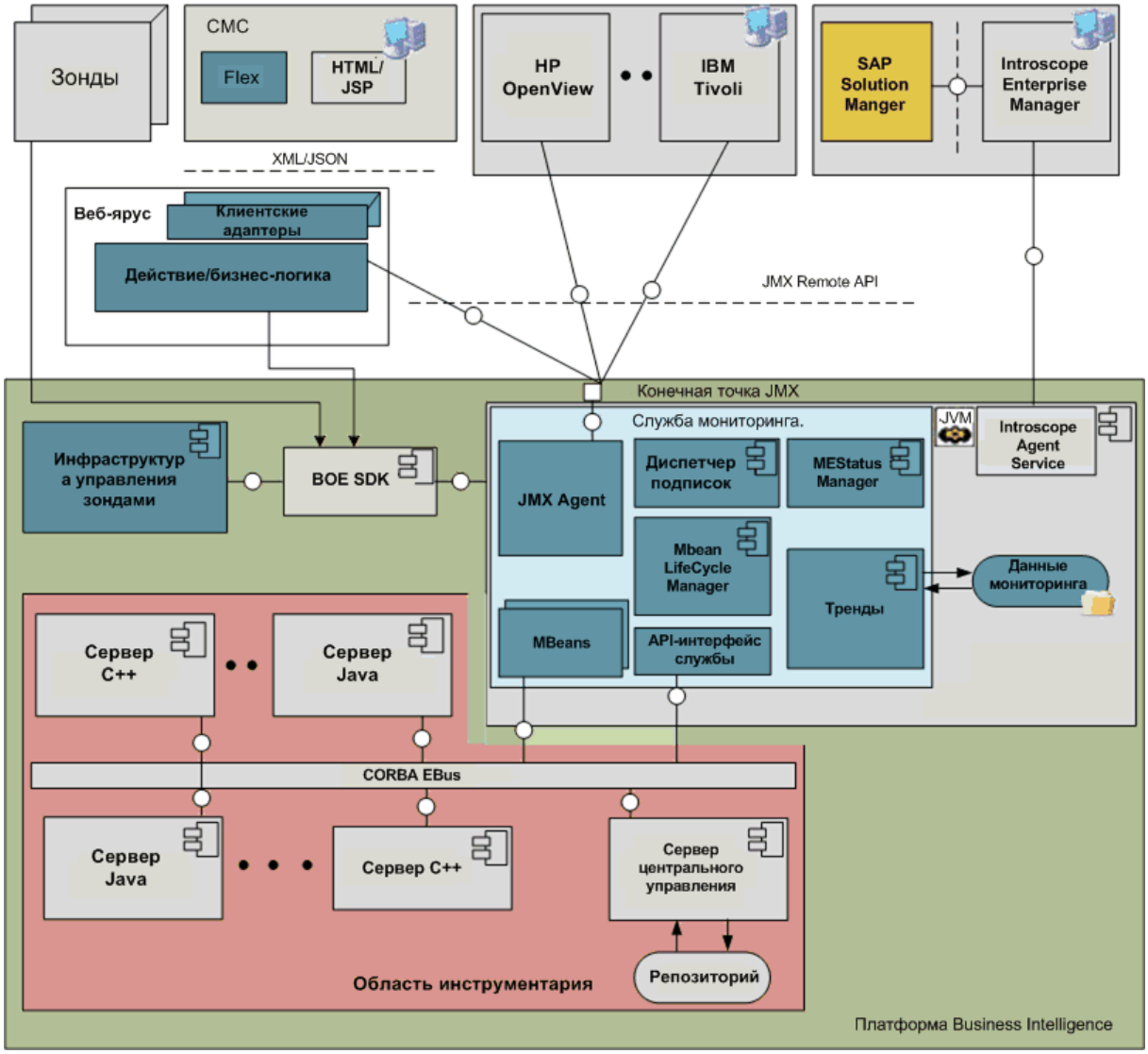
Предупреждение

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*.

20.2.1.1 Архитектура

В этом разделе представлен общий обзор архитектуры мониторинга и кратко поясняются роли, выполняемые ее компонентами. Ниже архитектура мониторинга представлена графически:



Ниже перечислены компоненты архитектуры верхнего 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 в приложении мониторинга используется база данных хранилища данных аудита (ADS). Сведения о схеме базы данных тенденций см. в разделе Схема базы данных тенденций [страница 1277].

20.2.2 Настройка поддержки баз данных в приложении мониторинга

В этом разделе описывается настройка мониторинга и отчетности по данным мониторинга.

> ⓘ Примечание
>
> Сведения мониторинга заносятся в базу данных трендов только по показателям, для которых установлен флажок *Запись в базу данных трендинга*.

Для записи сведений мониторинга доступно два параметра базы данных: запись сведений с помощью хранилища данных аудита (ADS) или любой другой базы данных, поддерживаемой платформой, посредством драйвера JDBC.

> ⓘ Примечание
>
> Использование базы данных Apache Derby прекращается, начиная с версии BI 4.3. Для получения дополнительных сведений о переносе и резервном копировании данных см. 2912759.

Можно использовать хранилище данных аудита (ADS) по умолчанию, часто именуемое базой данных аудита. Это реляционная база данных, в которой CMS хранит данные аудита. В качестве базы

данных аудита можно использовать хранилище ADS, включенное в платформу BI, или любую другую поддерживаемую базу данных, настроенную в качестве базы данных аудита.

Поддерживаемые базы данных:

- DB2
- SQL Server
- My SQL
- Oracle
- База данных SAP HANA
- SQL Anywhere
- Sybase

С помощью базы данных аудита пользователи могут включать в отчеты данные аудита в дополнение к информации мониторинга. Хранение данных в реляционной базе данных обеспечивает возможности резервного копирования и восстановления, а также доступность данных в режиме реального времени.

Связанные сведения

Настройка для использования базы данных аудита [страница 841]

20.2.2.1 Настройка для использования базы данных аудита

Чтобы использовать базу данных аудита для данных мониторинга, потребуется выполнить дополнительные шаги настройки:

- В версиях, предшествующих BI 4.3, если база данных трендов Derby содержит данные, требуется перенести базу данных Derby в базу данных аудита, а затем настроить для платформы BI запись 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 трендов 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 потребуется 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.

Связанные сведения

Настройка SBO-файлов [страница 843]
Добавление псевдонимов в SBO-файл [страница 846]
Переход на базу данных аудита [страница 847]
Создание таблиц мониторинга в ADS [страница 842]

20.2.2.1.1 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.

20.2.2.1.2 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:

   1. `MOT_TREND_DETAILS`
   2. `MOT_TREND_DATA`
   3. `MOT_MES_DETAILS`
   4. `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.

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.

20.2.2.1.3 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.

> ⓘ Примечание
>
> Приложение "Мониторинг" ссылается на имя соединения с базой данных аудита и использует JDBC, если используется `<имя_хоста>.<номер_порта>.<имя_БД>`, или ODBC (в противном случае). Чтобы приложение "Мониторинг" могло подключаться к базе данных аудита, SBO-файлы сервера соединений должны быть настроены соответствующим образом.

> **Примечание**
>
> Для баз данных Oracle поддерживаются только соединения JDBC.

Пример

- Если в поле имени соединения на странице "Аудит CMC" установлено значение `<имя_хоста>.<номер_порта>.<имя_БД>`, JAR-файл драйвера необходимо настроить в файле `dataAccess\connectionServer\jdbc\<тип_БД>.sbo`.
- Если в поле имени соединения на странице "Аудит CMC" задано имя источника данных (DSN) ODBC, драйвер необходимо настроить в файле `<каталог_установки>\dataAccess\connectionServer\odbc\<тип_БД>.sbo`.
- Если для аудита используется база данных SAP HANA, драйвер следует настроить в файле `<каталог_установки>\dataAccess\connectionServer\odbc\newdb.sbo`.
- Если для аудита используется база данных MS SQL Server, драйвер следует настроить в файле `<каталог_установки>\dataAccess\connectionServer\odbc\sqlsrv.sbo`.
- Если база данных используется для сервера DB2, сервер соединений не содержит файл поддержки `db2iseries.sbo`.
  По умолчанию приложение мониторинга использует режим соединения ODBC для подключения к базе данных аудита DB2. Для работы в этом режиме следует добавить и настроить системный DSN (для сервера DB2) на компьютере, где выполняется приложение мониторинга. Для получения сведений о добавлении и настройке соединения ODBC для DB2 см. следующие ссылки:
  - http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=%2Fcom.ibm.db2.udb.apdv.cli.doc%2Fdoc%2Ft0024166.htm
  - http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=%2Fcom.ibm.db2.udb.apdv.cli.doc%2Fdoc%2Ft0024200.htm

  > **Примечание**
  >
  > Если системный DSN для DB2 не настроены, произойдет сбой мониторинга трендов.

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>
```

- id="li_9D4EB94F9752458BB21A940C0A892C6D">Если для версии базы данных используется версия MySQL 5, SBO должен содержать эту запись:

```
<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>
```

- Если для аудита используется версия базы данных Oracle, SBO-файл должен иметь следующую конфигурацию:

```
<DataBase Active="Yes" Name="Oracle 11">
        <Aliases>
           <Alias>Oracle</Alias>
        </Aliases>
      <JDBCDriver>
            <ClassPath>

<Path>C:\app\Administrator\product\11.2.0\client_64\jdbc\lib\ojdbc6.jar</Path>
             </ClassPath>
                <Parameter Name="JDBC Class">oracle.jdbc.OracleDriver</
Parameter>
                <Parameter Name="URL Format">jdbc:oracle:thin:@//$DATASOURCE$/
$DATABASE$</Parameter>
```

```
        </JDBCDriver>
        <Parameter Name="Extensions">oracle11,oracle,jdbc</Parameter>
         <Parameter Name="Escape Character">/</Parameter>
          <Parameter Name="Force Execute">Always</Parameter>
          <Parameter Name="Catalog Separator">.</Parameter>
</DataBase>
```

Дополнительные сведения о настройке драйвера в SBO-файлах см. в *руководстве по доступу к данным*.

20.2.2.1.4 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>
```

20.2.2.1.5 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 CMC щелкните *Приложения*.
2. Нажмите *BI Admin Studio*.
3. Затем щелкните *Свойства мониторинга*.
4. Дважды щелкните *Приложение мониторинга*, чтобы открыть страницу свойств.
5. В области *Настройки базы данных тенденций* выберите *Использовать базу данных аудита*.

> **Примечание**
>
> Если для аудита используется база данных Oracle, для параметра *Имя соединения с базой данных ADS* на странице "Аудит" в консоли CMC необходимо указать соединение JDBC. Укажите имя соединения следующим образом: `<server_name>,<port>,<service_name>`.

> **Примечание**
>
> Чтобы таблицы мониторинга были созданы корректно, учетной записи пользователя в базе данных необходимы следующие разрешения:
>
> ВЫПОЛНИТЬ
> СОЗДАТЬ ПОСЛЕДОВАТЕЛЬНОСТЬ
> СОЗДАТЬ ТРИГГЕР

20.2.2.2 Настройка базы данных мониторинга с использованием JDBC

Создано соединение JDBC. Чтобы создать новое соединение JDBC, выполните следующие действия:

1. Поместите файл драйвера JDBC .jar для настраиваемой базы данных в следующее местоположение: `<INSTALL_DIR\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\MON.MonitoringService\lib>`.

   > **Примечание**
   >
   > Для кластеризованных развертываний необходимо скопировать драйвер JDBC в систему, в которой размещены службы мониторинга.

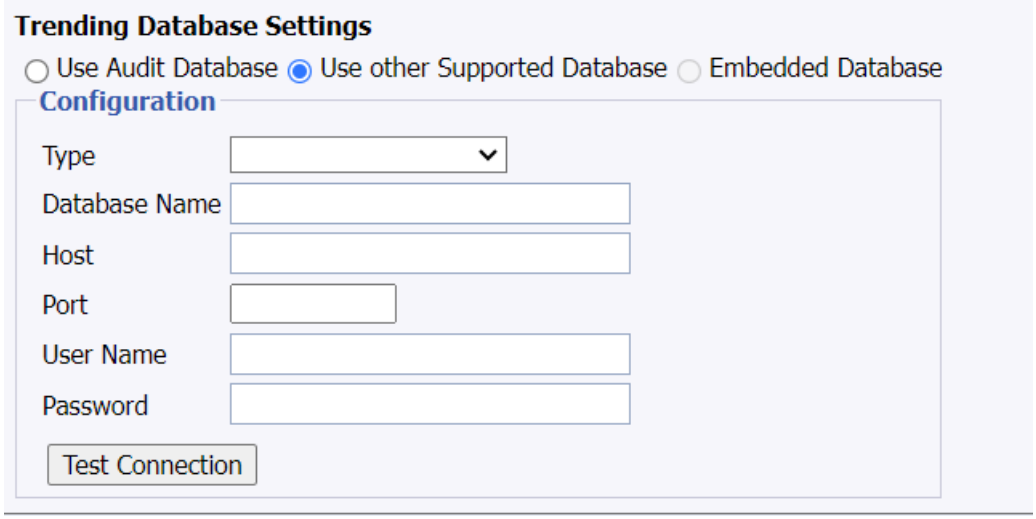
2. Перезапустите SIA.

Чтобы настроить новую базу данных для мониторинга BI, выполните следующие действия:

1. Войдите в консоль CMC.
2. В раскрывающемся меню на главной странице CMC выберите *Приложения*.
3. Щелкните правой кнопкой *BI Admin Studio* и выберите *Свойства мониторинга*.

Открывается всплывающее окно *Свойства приложения мониторинга*. По умолчанию установлен переключатель *Использовать базу данных аудита*.

4. Выберите переключатель *Использовать другую поддерживаемую базу данных*.
5. Введите *тип*, *имя базы данных*, *хост*, *порт*, *имя пользователя* и *пароль*.



6. **Необязательно:** С помощью свойства *Удалить всю историю старше X дней* добавьте число дней, по истечении которых данные истории мониторинга должны удаляться платформой.
7. Нажмите кнопку *Сохранить и закрыть*.
8. Перезапустите адаптивный сервер обработки.

   Чтобы выполнить проверку соединения, нажмите *Проверить соединение*.

> ⓘ Примечание
>
> Чтобы изменения вступили в силу, необходимо перезапустить все серверы APS, на которых размещается служба мониторинга BI.

Новая база данных для хранения комментариев из приложения мониторинга BI настроена.

20.2.3 Свойства конфигурации

В этом разделе описаны свойства приложения мониторинга и способы их изменения.

Чтобы просмотреть свойства конфигурации приложения мониторинга, выполните следующие действия:

1. Выберите *Приложение* на домашней странице CMC.
2. Щелкните правой кнопкой *BI Admin Studio* и выберите *Свойства мониторинга*. Ниже приводятся настраиваемые свойства.

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-адрес 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.
RMI	*Включить протокол RMI для JMX*	По умолчанию данный параметр отключен. При включении параметра необходимо указать номер порта RMI. Этот порт будет использоваться как записью RMI в реестре, так и коннектором порта RMI. Этот порт должен быть доступен службе, в противном случае запуск службы будет невозможен. Указав номер порта RMI, перезапустите сервер. После перезагрузки сервера создается URL-адрес конечной точки агента RMI JMX. Это свойство доступно только для чтения и содержит URL-адрес конечной точки агента JMX, использующего протокол RMI. Используйте этот URL-адрес, чтобы подключить к процессу мониторинга другие клиенты.
Показатели хоста	*Включить показатели хоста*	По умолчанию данный параметр отключен. При включении этого параметра необходимо указать путь к каталогу установки двоичного файла SAPOSCOL. Для включения показателей хоста необходимо установить SAPOSCOL. Для получения дополнительной информации об установке SAPOSCOL см. раздел «Установка SAPOSCOL».
Параметры базы данных тренда	*Использовать базу данных аудита*	Выберите этот параметр, чтобы хранить журнал трендов показателей в базе данных аудита для хранилища данных аудита (ADS). **Примечание** Для этого требуется настроить хранилище данных аудита.
	Использовать другую поддерживаемую базу данных	Выберите этот параметр, чтобы хранить журнал трендов показателей/наблюдения в настроенной поддерживаемой базе данных.
	Удалить всю историю старше X дней	Срок хранения данных истории в днях.

Раздел	Поле	Описание
Другие настройки	*Интервал обновления метрики (в секундах)*	Минимальный интервал, который можно указать, – 15 секунд. Этот интервал управляет следующими аспектами: • Расчет подписки наблюдений: правила предостережения и опасности постоянно рассчитываются с указанным интервалом времени. • Расчет состояния наблюдения: состояние наблюдения вычисляется постоянно с указанным интервалом, если настройка "Событие" наблюдения выбрана с параметром *Изменять статус наблюдения каждый раз, когда правило "Опасно" или "Внимание" принимает значение true*. • Период трендинга: режим журнала для графиков всегда анализируется с указанным здесь интервалом.
	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 предупреждений (дн.)	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` с 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`.

20.2.3.1 URL-адрес конечной точки JMX

Приложение мониторинга предоставляет URL-адрес конечной точки JMX, через которую могут подключиться другие клиенты, использовав 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
cecore.jar;
celib.jar;
cesession.jar
commons-logging-1.1.jar
corbaidl.jar
ebus405.jar
log4j.jar;
logging.jar.
monitoring-plugins.jar
monitoring-sdk.jar
stax-api-1.0.1.jar
wsdl4j-1.6.2.jar
wstx-asl-3.2.1.jar
XmlSchema-1.3.2.jar
TraceLog.jar
ceaspect.jar
aspectjrt.jar

Другой вариант подключения – через порт RMI по умолчанию. Для получения дополнительных сведений о подключении через порт RMI см. раздел Свойства конфигурации [страница 848].

20.2.3.2 Конфигурация JMX SSL

Теперь можно осуществлять защищенную коммуникацию между JConsole и BOE через конфигурацию JMX SSL.

1. Войдите в CMC.
2. Перейдите в раздел *Приложения* > *BI Admin Studio* > *Свойства мониторинга*.
3. В разделе *RMI* активируйте параметр *Активировать протокол RMI для JMX*.
4. Введите номер порта RMI.

   7777
5. Активируйте параметр *Активировать SSL для протокола RMI для JMX*.
6. Нажмите кнопки *Сохранить* и *Закрыть*.
7. Перезапустите *адаптивный сервер обработки*.

> ⓘ Примечание
>
> Сервер, на котором размещена служба мониторинга, будет перезапущен.

20.2.3.2.1 Создание сертификата

1. Откройте командную строку в режиме администратора или в сеансе терминала и перейдите к следующей папке:

   Windows:

   ```
   INSTALLDIR\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin
   ```

   Linux/Unix:

   ```
   INSTALLDIR/sap_bobj/enterprise_xi40/<PLATFORM>_x64/sapjvm/bin
   ```
2. Выполните команду для создания сертификата: `keytool -genkeypair -alias serverkey -keyalg RSA -keysize 2048 -keystore serverkeystore`
3. Введите всю необходимую информацию для создания сертификата.
4. 4. При успешном выполнении будет создан файл сертификата по имени в том же каталоге sapjvm bin: `serverkeystore`

20.2.3.2.2 Добавление файла хранилища сертификатов в службу мониторинга

1. В CMC выберите *Серверы* > *Список серверов*.
2. Выберите *Адаптивный сервер обработки* (сервер, где установлена служба мониторинга).
3. Выберите *Свойства*.

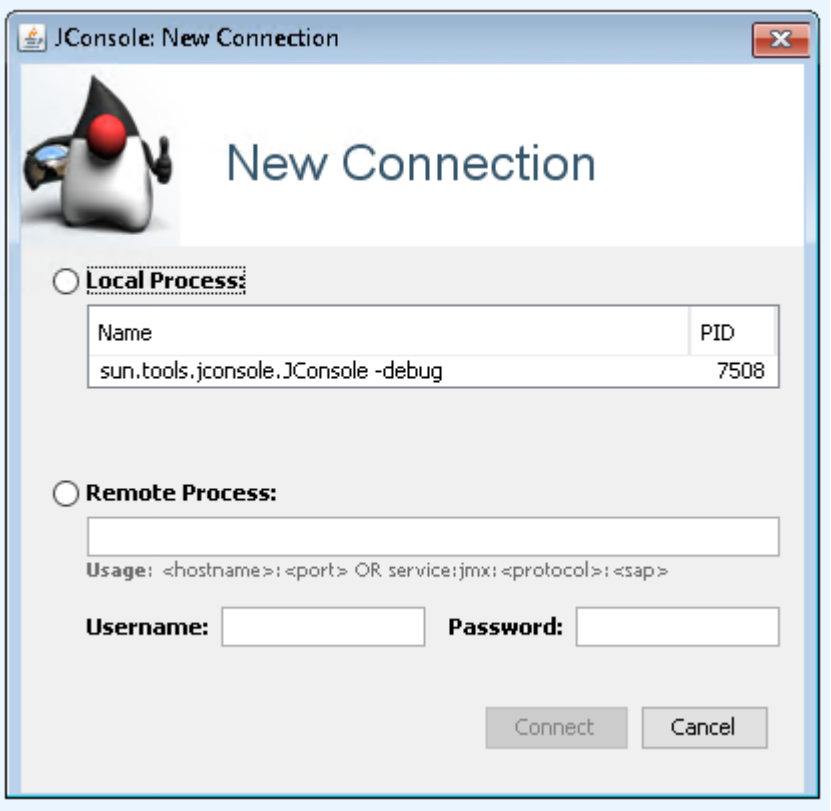
4. Перейдите в раздел *Конфигурация JMX SSL*.
5. В поле *Местоположение файла хранилища сертификатов* введите путь к *местоположению файла хранилища ключей сертификатов*.
6. Введите информацию о *пароле доступа к секретным ключам*.

   Password1

20.2.3.2.3 Подключение к JConsole

1. Выполните команду для запуска `JCONSOLE.exe` в командной строке (`jconsole.exe -J-Djavax.net.ssl.trustStore="<Path of Certificate Keystore file location >" -J-Djavax.net.ssl.trustStorePassword=<PasswordDetail>`)

   ```
   jconsole.exe -J-Djavax.net.ssl.trustStore="C:\Program Files
   (x86)\SAP BusinessObjects\SAP BusinessObjects
   Enterprise XI 4.0\win64_x64\sapjvm\bin\serverkeystore" -J-
   Djavax.net.ssl.trustStorePassword=Password1
   ```
2. После выполнения этой команды запускается средство просмотра JConsole, как показано ниже.

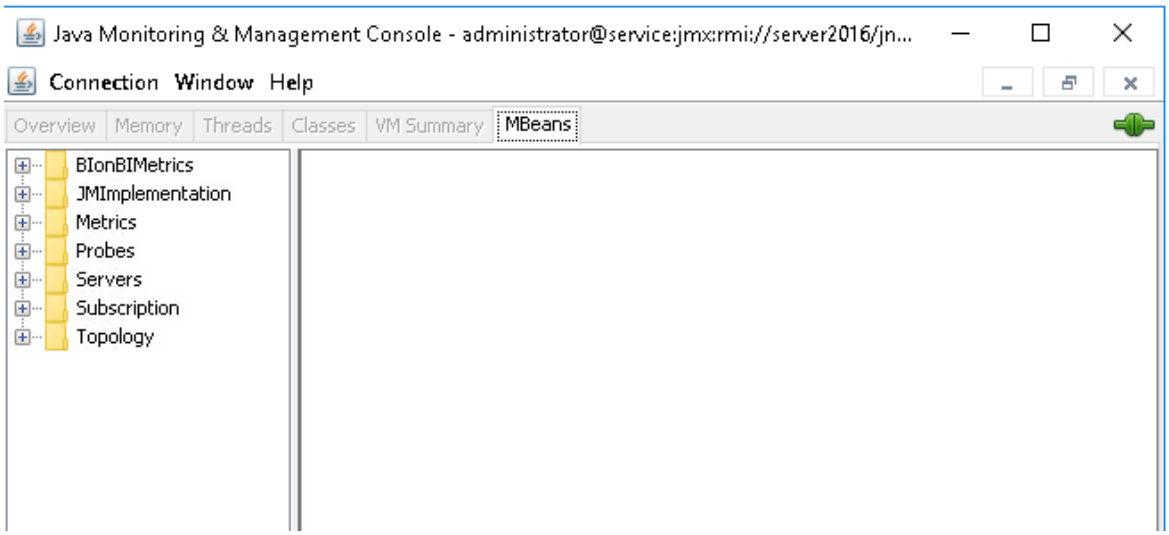


3. Щелкните переключатель *Удаленный процесс*, чтобы активировать поле.
4. Введите *URL-адрес конечной точки агента RMI JMX* и связанные *Имя пользователя* и *Пароль*.

   URL-адрес конечной точки агента RMI JMX имеет следующий формат: `service:jmx:rmi://<HostName>/jndi/rmi://<HostName>:<RMI Port Number>/<hostname>:<CMS Port>`.

   `service:jmx:rmi://server2016/jndi/rmi://server2016:7777/server2016:6400`.

5. Нажмите *Соединить*.
6. Будет запущена *Консоль управления и мониторинга Java* средства просмотра JConsole.



7. В средстве просмотра JConsole можно перейти к различным разделам, таким как "BIonBIMetrics", "Показатели", "Зонды", "Серверы" и "Топология", чтобы извлечь связанные данные.

20.2.3.3 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.

20.2.3.4 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 CMC.

20.2.4 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.

20.2.4.1 Интеграция приложения мониторинга с SAP Solution Manager

Чтобы интегрировать приложение мониторинга с SAP Solution Manager, в системе 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 «настройки связи с Wily Introscope Enterprise Manager» укажите имя хоста и порт. При установке платформы BI агент Introscope устанавливается в каталоге `C:\Program Files (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\java\Wily`.
2. Запустите рабочую станцию Wily 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 Wily Introscope (IS), выбрав *CMC* > *Серверы* > *Узел сервера* > *Заполнители*. Здесь также указываются хост и порт IS Enterprise Manager для связи агента IS с приложением мониторинга. Дополнительные сведения см. в разделе *Управление серверами* справки по CMC.
>
> 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.

20.2.5 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 удается, 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.

20.2.6 Устранение неполадок

В этом разделе приводятся пошаговые инструкции для решения широкого диапазона проблем, которые могут возникать при работе с приложением мониторинга.

20.2.6.1 Инструментальная панель

На странице CMC 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 *Свойства сервера CMS* > *Показатели*.
- Убедитесь, что ответ центрального сервера управления соответствует ожиданиям.

20.2.6.2 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.

20.2.6.3 Список наблюдений

Не удается извлечь данные журнала для наблюдений

- Проверьте интервал опроса на странице *Свойства* приложения мониторинга.
- Проверьте файл трассировки в папке журнала.
- 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.

20.2.6.4 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

20.2.6.5 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

20.2.6.6 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.

20.3 Визуальное отличие

Функция визуального отличия позволяет просматривать различия между двумя версиями LCMBIAR, объектов и других элементов. Эту функцию можно использовать, чтобы обнаруживать различия между файлами или объектами для разработки и ведения разных типов 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 файлы, чтобы точно определить проблему.

Домашняя страница

Домашняя страница функции 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
- Панель "Сравнения" - эта панель содержит вкладки фильтров и отличий
- Сравнения: Панель "Отличия" - эта панель содержит список сравненных объекты с указанием имени сравнения, даты/времени и статуса отличий

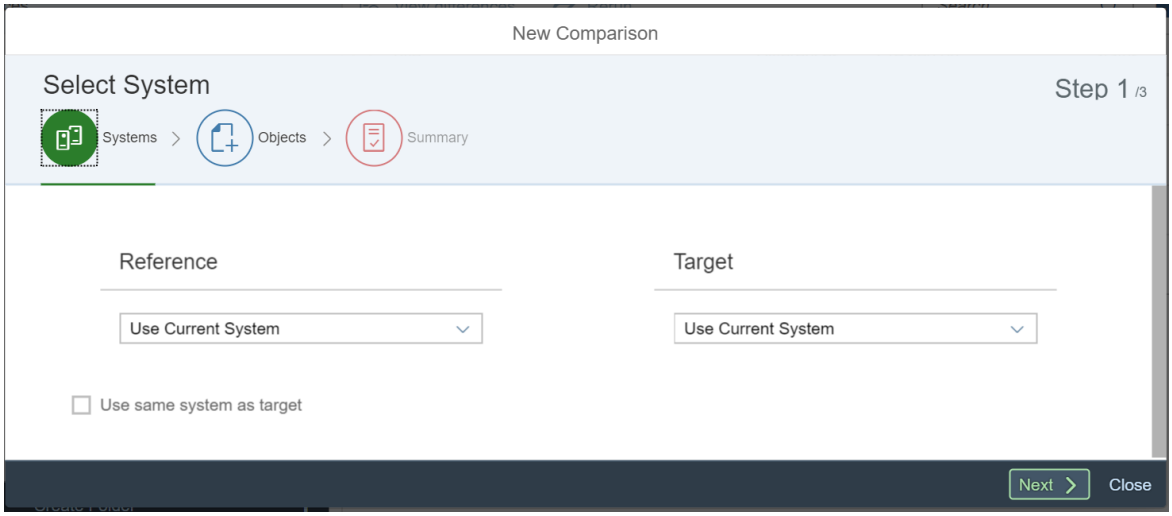
20.3.1 Сравнение объектов и файлов с использованием функции визуального отличия

Для сравнения файлов с использованием визуального отличия выполните следующие шаги.

1. Войдите в приложение CMC.
2. На главной странице CMC на вкладке *Управление* щелкните ссылку *Визуальное отличие*. Отобразится страница "Визуальное отличие". Сравниваемые файлы хранятся в папке "Отличия" или в любой созданной пользователем подпапке.

   > **Примечание**
   >
   > Чтобы создать новую вложенную папку, выберите Create Folder +.

3. Выберите +, чтобы создать новое сравнение.
   Отображается ассистент *Новое сравнение*



.

4. Выберите *ссылочную* и *целевую* систему из раскрывающегося списка.

   Можно подключиться к любой из следующих ссылочных и целевых систем:

> ⓘ Примечание
>
> Если объект добавляется в систему управления версиями (VMS), вы получите возможность выбрать версию на следующем шаге.

- CMS
- Локальная файловая система

5. На экране *Выбор объектов* выполнте поиск и выберите объект или файл в *ссылочной* и *целевой* системе.
6. При необходимости измените *Имя сравнения*.
7. Нажмите *Сравнить*, чтобы сравнить объекты.

> ⓘ Примечание
>
> - Можно проверить различия, сначала выбрав сравнение, затем нажав *Просмотреть различия*. Отличия выделяются оранжевым цветом, а отсутствующие объекты – красным.
> - Можно выполнить сравнение повторно, сначала выбрав сравнение, а затем нажав *Выполнить повторно*.

Процесс сравнения начнется немедленно.

При помощи фильтра можно также просмотреть сравниваемые объекты по типу, а также с отличиями или с общими атрибутами.

20.3.2 Сравнение объектов и файлов с помощью системы управления версиями

Объекты или файлы можно сравнивать в системе управления версиями с помощью параметра визуального отличия.

Чтобы сравнить объекты в системе управления версиями, выполните следующие шаги.

1. Выполните вход в приложение CMC.
2. На главной странице CMC на вкладке *Управление* щелкните ссылку *Визуальное отличие*.
   Отобразится страница "Визуальное отличие". Сравниваемые файлы хранятся в папке "Отличия" или в любой созданной пользователем подпапке.

   > ⓘ Примечание
   >
   > Чтобы создать новую вложенную папку, щелкните значок "Папка".

3. Выберите *Новое сравнение*.
   Отобразится экран *Визуальное отличие - 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*.
   Откроется 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.
9. Нажмите кнопку *Сравнить*, чтобы сравнить задания 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 *OK*.

20.4 Авторизация элементов HTML

Чтобы предоставить пользователям возможности использования надежных элементов HTML и не допустить использования в организации других элементов, укажите список авторизованных элементов HTML.

Когда пользователь открывает документ, который содержит ячейку со свойством "Прочесть как HTML" или "Прочитать как гиперссылку", в средстве просмотра HTML или интерактивном средстве просмотра Web Intelligence, средство просмотра может интерпретировать HTML. Его поведение зависит от того, как вы определили визуализацию ячеек в свойствах отображения Web Intelligence, и элементов HTML, которые вы авторизуете.

Когда указаны авторизованные элементы HTML и документ в режиме чтения содержит неавторизованный элемент, сохраняется только текст из этого элемента, но не тег элемента и не его атрибуты. В документе, содержащем авторизованный элемент и авторизованные и неавторизованные атрибуты, сохраняются только этот элемент и авторизованные атрибуты.

Чтобы авторизовать только определенные элементы HTML, в свойствах отображения Web Intelligence для JavaScript выберите *Включить только элементы HTML, определенные на странице авторизованных элементов HTML* и укажите элементы HTML на странице *Авторизованные элементы HTML*.

По умолчанию авторизованы только элементы HTML, необходимые для правильного функционирования Web Intelligence. Элементы можно добавить в список по умолчанию или удалить из списка.

⚠ Предупреждение

- Web Intelligence активирует встроенный код JavaScript/HTML в ячейках документов с использованием формул.
  Этот код можно активировать и деактивировать в Central Management Console. Однако разрешая использование JavaScript, HTML и гиперссылки, вы признаете, что подвергаете себя риску межсайтового скриптинга. Межсайтовый скриптинг позволяет злоумышленникам изменять веб-сайты или выполнять код на других системах. Эта уязвимость затрагивает такие продукты, как интернет-браузеры, когда они выполняют скрипты. Большинство атак

межсайтового скриптинга являются результатом небезопасного программирования на целевой системе.

- Код можно настроить с помощью списка авторизованных тегов HTML и атрибутов. Обратите внимание, что компания SAP не несет ответственности за совместимость этого кода и возможные побочные эффекты. Например, может потребоваться адаптировать код из-за обновлений браузера, поддержки версий JavaScript или способа динамического встраивания кода в веб-страницу. С технической точки зрения, приложение, начиная с версии 4.3, выполняется в виде одностраничного приложения. То есть между отчетом и общей веб-страницей нет технического разделения. Для выполнения в этом новом контексте может потребоваться корректировка кода.
- При удалении элементов из списка по умолчанию функционирование Web Intelligence ухудшится, и рекомендуется об этом помнить.

Вы можете авторизовать:

- Элемент `<a>` с атрибутом `href` для добавления ссылки.
- Набор атрибутов для всех элементов в списке, связав элемент * со списком атрибутов.
  Все атрибуты, связанные с элементом, авторизовать нельзя .
- Элементы, которые могут содержать JavaScript, например `<script>`, `<onClick>` и `<onMouseEnter>`.
  Ключевые слова JavaScript авторизовать нельзя.

Пример

Авторизованные элементы HTML

Элемент	Атрибуты
*	style, class, id
img	src
link	ref

В следующей таблице показано, как в результате авторизации Web Intelligence отображает элементы HTML в документах.

Влияние авторизации элементов HTML

Исходный HTML	Конечный HTML	Пояснение
`<link title="SAP" ref="www.sap.com">`	`<link ref="www.sap.com">`	Элемент `<link>` и атрибут `ref` авторизованы, поэтому в документе ссылка отображается как активная. Атрибут `title` не авторизован, поэтому он удаляется из документа.

Исходный HTML	Конечный HTML	Пояснение
`<img src="datasource" id="I1">`	`<img src="datasource" id="I1">`	Элемент `<img>` и связанный атрибут `src` авторизованы, и атрибут `id` авторизован для всех элементов, поэтому исходный HTML сохраняется.
`<div title="datasource" id="D1">`	Удалено.	Элемент `<div>` не авторизован, поэтому этот элемент и связанные атрибуты удаляются из документа.
`<p> ...as shown in the picture below: <img src="../picture.jpg" alt="Mountain"> </p>`	`...as shown in the picture below:<img src="../picture.jpg">`	Элемент `<p>` не авторизован, поэтому он удаляется. Остается только текст, содержащийся в элементе `<p>`. Элемент `<img>` и связанный атрибут `src` авторизованы, поэтому они сохраняются. Атрибут `alt` не авторизован, поэтому он удаляется из документа.

Изменение параметров отображения для Web Intelligence [страница 738]Изменение списка авторизованных элементов HTML [страница 864]

20.4.1 Изменение списка авторизованных элементов HTML

Укажите надежные элементы HTML, которые требуется авторизовать, чтобы предоставить защиту от потенциально злонамеренных элементов, изменив список авторизованных элементов HTML.

Web Intelligence авторизует только элементы, определенные на странице *Авторизованные элементы HTML*, когда свойство отображения JavaScript *Включить только элементы HTML, определенные на странице авторизованных элементов HTML* активно в свойствах Web Intelligence.

1. Перейдите в CMC и выберите *BI Admin Studio*.
2. На *домашней странице Central Management Console* выполните прокрутку вниз до *элементов HTML*.
3. Измените список, как описано в следующей таблице:

Изменение	Шаги
Для добавления элемента	Щелкните *Добавить новый элемент* и введите элементы и связанные атрибуты для авторизации.

Изменение	Шаги
	Примечание • Чтобы авторизовать определенные атрибуты для всех элементов HTML, введите в качестве элемента звездочку (*) и добавьте атрибуты. • При попытке добавить элемент HTML, который уже есть в списке, в список добавляются только новые атрибуты для этого элемента.
Для изменения элемента	Щелкните элемент и выберите *Изменить выбранный элемент*.
Для удаления элемента	Щелкните элемент и выберите *Удалить выбранный элемент*.
Для восстановления списка авторизованных элементов HTML по умолчанию	Нажмите *Сброс*. Список по умолчанию содержит только элементы, необходимые для правильной работы Web Intelligence.

21 Отчетность CMS

21.1 Отчетность CMS

Прежде чем приступить к работе с отчетностью CMS, необходимо получить базовое представление о следующих понятиях:

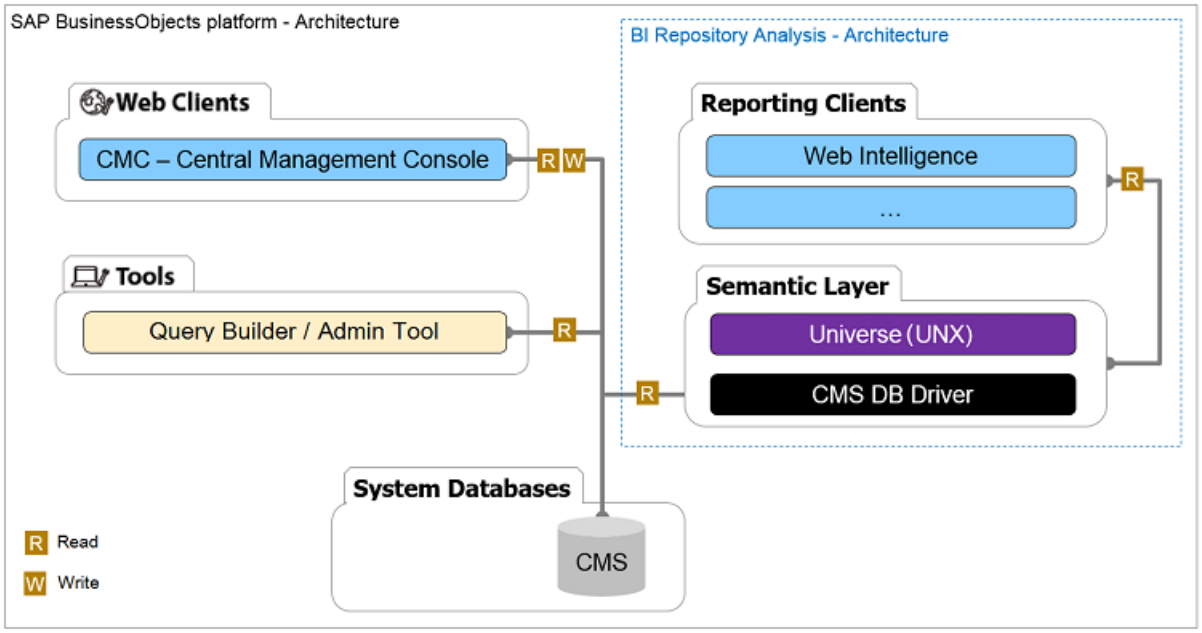
- Архитектура платформы SAP BusinessObjects
- Структура базы данных системы CMS
- Свойства и отношения объектов InfoObject

Связанные сведения

Архитектура платформы SAP BusinessObjects [страница 866]
Структура базы данных системы CMS [страница 867]

21.1.1 Архитектура платформы SAP BusinessObjects

Эта схема позволяет лучше понять архитектуру платформы SAP BusinessObjects.



В следующей таблице приводятся дополнительные сведения о компонентах платформы SAP BusinessObjects.

Компоненты платформы SAP BusinessObjects

Компоненты	Описание
CMC – Central Management Console	Веб-инструмент, используемый для настройки параметров безопасности и управления следующими элементами: • Пользователь • Контент • Сервер
База данных системы CMS	База данных, в которой хранятся следующие данные платформы BI: • Пользователь • Сервер • Документ • Конфигурация • Аутентификация Ведение системной базы данных CMS осуществляется на центральном сервере управления (CMS); иногда она также называется системным репозиторием.
Построитель запросов (также называемый средством администрирования)	Веб-инструмент, используемый для запроса данных в репозитории BusinessObjects и получения информации, недоступной в CMC.
BI Repository Analysis	Это решение использует семантический уровень платформы BI, юниверс (UNX) и драйвер БД CMS для запроса данных CMS.

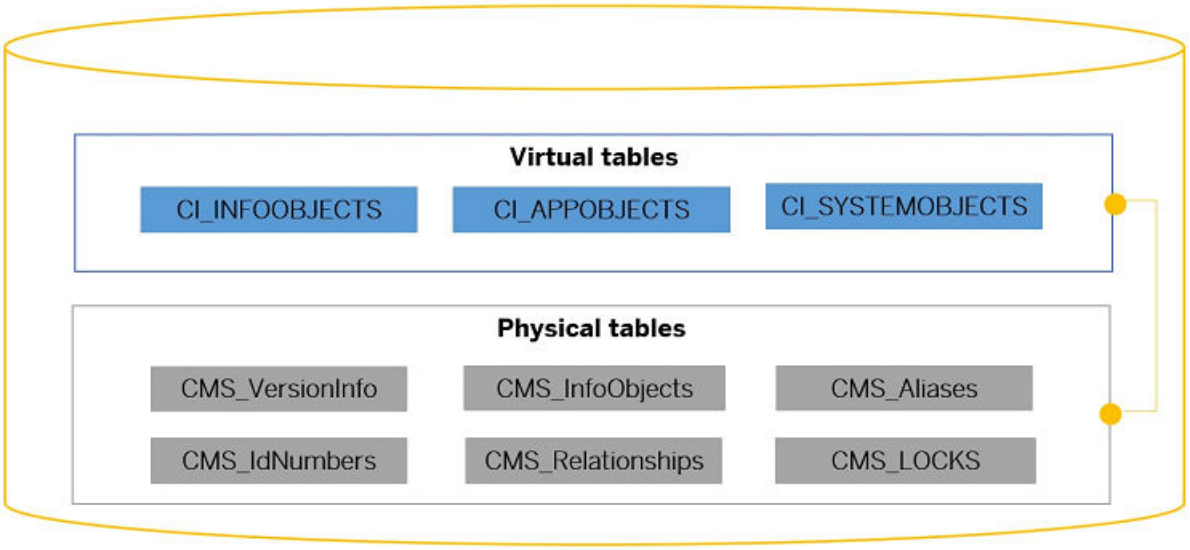
21.1.2 Структура базы данных системы CMS

База данных системы CMS ведется на центральном сервере управления (CMS); иногда она также называется системным репозиторием. Система CMS — это база данных, которая хранит сведения о платформе BI в форме объектов InfoObject.

База данных системы CMS включает два вида таблиц:

- Физическая таблица базы данных: в физических таблицах базы данных хранятся метаданные CMS.
- Виртуальная таблица: в виртуальных таблицах сервер CMS выполняет поиск объектов InfoObject.

На следующей схеме представлен обзор структуры базы данных системы CMS.



Дополнительные сведения о структуре базы данных системы CMS см. в связанных разделах.

Связанные сведения

Физические таблицы базы данных [страница 868]
Виртуальные таблицы [страница 869]

21.1.2.1 Физические таблицы базы данных

Метаданные CMS хранятся в шести физических таблицах базы данных.

Физические таблицы базы данных

Физическая таблица	Описание
CMS_VersionInfo	Включает текущую версию BusinessObjects Enterprise (BOE)
CMS_InfoObjects	Основная таблица в системном репозитории. В каждой строке хранится по одному объекту InfoObject.
CMS_Aliases	Сопоставляет псевдонимы пользователя с соответствующим идентификатором пользователя. Пользователь имеет псевдоним для каждого домена безопасности, участником которого он является. Однако пользователь имеет только один идентификатор.

Физическая таблица	Описание
CMS_IdNumbers	Создает уникальные идентификаторы объектов и типов.
CMS_Relationships	Хранит отношения между объектами InfoObject.
CMS_LOCKS	Дополнительная таблица CMS_RELATIONS

21.1.2.2 Виртуальные таблицы

Сервер CMS выполняет поиск объектов InfoObject в трех виртуальных таблицах.

Виртуальные таблицы

Виртуальная таблица	Описание
Таблица объектов InfoObject	Включает доступные для просмотра конечным пользователем объекты InfoObject, такие как: • Документы отчетов • Программы • Ярлыки • Папки • Категории • Входящая почта
Таблица объектов приложений	Включает объекты InfoObject, используемые документами, такие как: • Юниверсы • Соединения • Перегрузки
Таблица системных объектов	Включает объекты InfoObject, используемые платформой BI для работы, такие как: • Пользователи • Группы • Лицензионные ключи

21.1.3 Об объектах InfoObject

Перед запросом метаданных InfoObject необходимо получить четкое представление о следующих понятиях:

- Свойства объектов InfoObject

- Отношения между объектами InfoObject

Если вы поймете, как организованы объекты InfoObject в репозитории CMS, вы сможете легко и быстро выполнять поиск в этом репозитории и исправлять связанные с ним ошибки.

Связанные сведения

Свойства объектов InfoObject [страница 870]
Отношения между объектами InfoObject [страница 870]

21.1.3.1 Свойства объектов InfoObject

В следующей таблице перечислены важнейшие свойства объектов InfoObject с описаниями.

Свойства объектов InfoObject

Свойства объектов InfoObject	Описание
SI_NAME	Имя объекта
SI_KIND	Вид объекта
SI_OWNER	Имя пользователя для владельца объекта
SI_OWNERID	Идентификатор пользователя для владельца
SI_CHILDREN	Число дочерних объектов
SI_CUID	CUID для InfoObject – уникальный идентификатор объекта в кластере
SI_UNIVERSE	Юниверсы (UNV), используемые документом

21.1.3.2 Отношения между объектами InfoObject

Объекты InfoObject упорядочены по трем иерархиям:

- Иерархия папок
- Иерархия пользователей или групп пользователей
- Иерархия серверов или групп серверов

Приложения CMS и клиентские приложения используют иерархию папок для навигации по объектам InfoObject.

Дополнительные сведения об отношениях между объектами InfoObject см. в связанных разделах.

Связанные сведения

Иерархия папок [страница 871]
Корневые папки [страница 871]

21.1.3.2.1 Иерархия папок

Иерархия папок — это простой список, созданный из родительского объекта InfoObject. Все объекты InfoObject должны иметь один определенный в свойстве SI_PARENTID родительский объект.

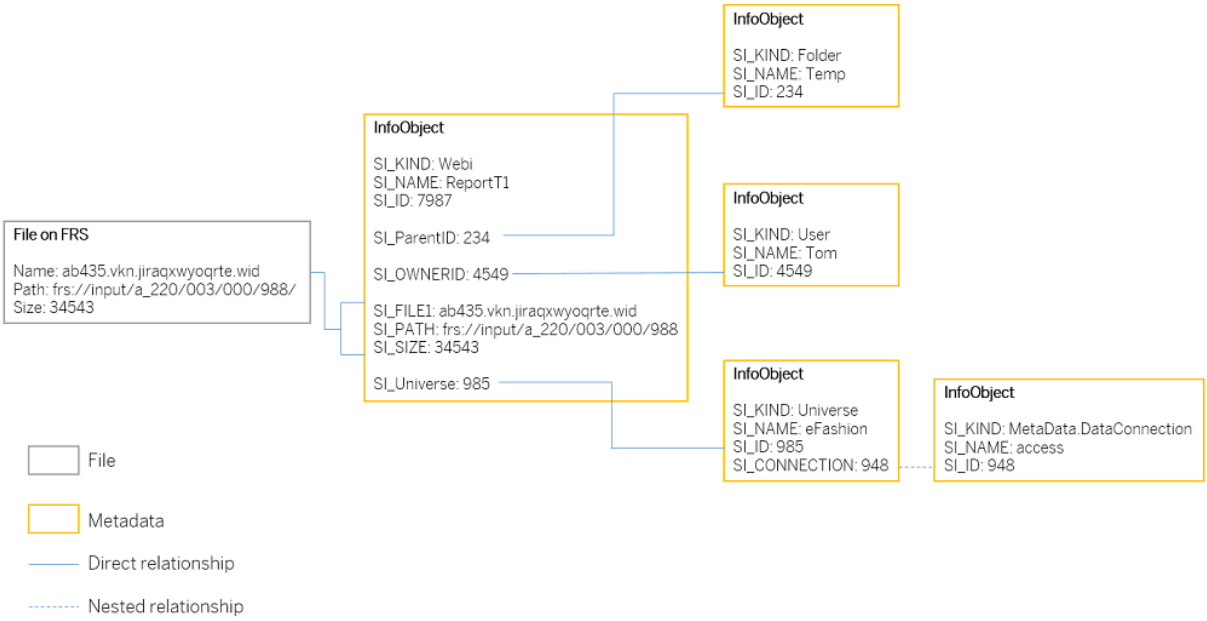
CMS использует свойство «идентификатор родительского элемента» для создания виртуальной иерархии папок. На самом деле эта иерархия не соответствует расположению объектов InfoObject в репозитории.

21.1.3.2.2 Корневые папки

Папка верхнего уровня в иерархии репозитория CMS — это папка кластера CMS. Корневые папки находятся на один уровень ниже папки кластера CMS. Это виртуальные папки, не соответствующие никаким объектам файловой системы.

Объекты InfoObject упорядочены в корневых папках, чтобы приложения CMS и клиентские приложения могли легко и быстро их найти. Например, клиентские приложения могут осуществлять навигацию по коллекции объектов InfoObject в таком порядке: корневая папка объекта, свойство «идентификатор родительского элемента» и свойства «идентификатор дочернего элемента». Объекты InfoObject одного вида, как правило, можно найти в одной корневой папке.

Следующая диаграмма поможет разобраться в отношениях между объектами InfoObject.



Как видите, структура объектов InfoObject позволяет им иметь неограниченное количество отношений и вложенных отношений.

21.2 Обзор системы отчетности CMS

Каждый администратор должен разбираться в методах использования платформы Business Intelligence и уметь их оптимизировать. Образец комплекта отчетности CMS включает драйвер базы данных CMS, который позволяет визуализировать объекты метаданных базы данных CMS и составлять по ним отчеты. Используя юниверс и встроенные клиенты системы отчетности, можно запрашивать объекты метаданных из базы данных репозитория CMS. Эти объекты метаданных включают информацию с платформы Business Intelligence, например:

- Соединения
- Документы
- Расписания
- Юниверсы
- Пользователи

Импортировав образец комплекта отчетности CMS, содержащий предварительно определенные объекты, можно создавать отчеты и информационные панели с помощью следующих приложений анализа данных и ведения отчетности SAP BusinessObjects:

- SAP BusinessObjects Web Intelligence
- SAP Crystal Reports для Enterprise

Чтобы быстро начать создавать отчеты в CMS, можно воспользоваться образцом комплекта отчетности CMS. Основные этапы создания отчета CMS:

- Импорт образца комплекта отчетности CMS: Для импорта образца комплекта отчетности CMS используется Диспетчер переноса объектов на консоли CMC.
- Создание отчета CMS: С помощью SAP BusinessObjects Web Intelligence можно создать отчет CMS, используя образец юниверса CMS в качестве источника данных.

Описание всей процедуры, дающее более детальное представление о процессе создания отчета, см. по ссылке, указанной ниже.

Связанные сведения

Образец комплекта отчетности CMS
Создание отчета CMS
Импорт образца комплекта отчетности CMS с помощью диспетчера переноса объектов [страница 874]

21.3 Соединение с базой данных CMS

Для создания защищенного соединения с базой данных CMS используется драйвер базы данных CMS. Можно использовать стандартное соединение из образца комплекта отчетности CMS или создать собственное соединение с базой данных CMS.

В качестве соединения с базой данных CMS необходимо использовать реляционное соединение. Параметры реляционного соединения описываются в следующей таблице.

Параметры реляционного соединения

Параметр	Описание
Режим аутентификации	Метод аутентификации учетных данных пользователей при обращении к источнику данных: • *Использовать указанные имя пользователя, пароль и ИД системы*: используются параметры *Имя пользователя* и *Пароль*, определенные для соединения. Доступ к источнику данных может производиться как из локальной системы, так и из удаленной. **Примечание** Убедитесь, что пользователь обладает правами на просмотр контента этого сеанса. • *Использовать токен сеанса*: Используется текущий сеанс пользователя. Вы можете видеть только контент, который вам разрешено просматривать и обрабатывать. Источник данных доступен только из локальной системы. **Примечание** По соображениям безопасности рекомендуется использовать именно этот режим аутентификации.
Идентификатор системы	Имя CMS, если параметр *Режим аутентификации* имеет значение *Использовать указанные имя пользователя и пароль*.
Имя пользователя	Имя пользователя для доступа к источнику данных в случае, если параметр *Режим аутентификации* имеет значение *Использовать указанные имя пользователя и пароль*.
Пароль	Пароль для доступа к источнику данных в случае, если параметр *Режим аутентификации* имеет значение *Использовать указанные имя пользователя и пароль*.

21.4 Образец комплекта отчетности CMS

Используйте образец комплекта отчетности CMS, чтобы начать создавать документы для ведения отчетности CMS. Драйвер базы данных CMS интегрирован в платформу Business Intelligence, а сам образец комплекта отчетности CMS находится в следующей папке:

`<INSTALLDIR>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\BI on BI`.

В этот образец входит следующее:

- Соединение (BI platform CMS system database.cns)
- Юниверс (BI platform CMS system database.unx)
- Образцы Web Intelligence

Подробнее об отчетах CMS см. в сети SAP Community Network.

Связанные сведения

Импорт образца комплекта отчетности CMS с помощью диспетчера переноса объектов [страница 874]

21.4.1 Импорт образца комплекта отчетности CMS с помощью диспетчера переноса объектов

Прежде чем приступать к процедуре, проверьте наличие прав доступа к образцу комплекта отчетности CMS, находящемуся в следующей папке:

`<INSTALLDIR>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\BI on BI`

Для импорта образца комплекта отчетности CMS используется диспетчер переноса объектов на консоли Central Management Console (CMC).

1. Откройте Central Management Console и щелкните *Диспетчер переноса объектов*.
2. Выберите *Импорт* > *Файл импорта*.
3. Выберите *Файловая система*
4. Щелкните *Выбрать файл* для выбора образца.
5. В поле области *Новое задание* выберите *Вход в новую систему CMS* для поля *Место назначения*.
6. Введите параметры входа и выберите *Вход в систему* > *Создать*.
7. В области *Задания переноса* щелкните образец правой кнопкой мыши и выберите *Перенести*.
8. В диалоговом окне *Перенос* щелкните *Перенести*.

Когда *Состояние переноса* образца комплекта отчетности CMS примет значение *Успешно*, это будет означать, что образец успешно импортирован в систему Business Intelligence 4.2. Об использовании образца юниверса для отчетности CMS см. соответствующий раздел.

Связанные сведения

Образец комплекта отчетности CMS [страница 874]

21.4.2 Образец юниверса CMS

Образец юниверса CMS – это предварительно определенный юниверс, поддерживающий типичные сценарии составления отчетов.. Этот юниверс можно изменять и расширять в соответствии с конкретными потребностями анализа и отчетности. Кроме того, в области *Запросы* приводится список предварительно определенных запросов. Эти запросы можно использовать в учебных целях при знакомстве с функциями юниверса.

В следующей таблице перечислены наиболее полезные запросы и указано, что они означают.

Полезные запросы для использования в юниверсе CMS

Запрос	Описание
Sample-User-Relationship-Detail	Позволяет узнать, к какой группе принадлежит пользователь.
Sample-FolderPath (юниверс)	Позволяет найти расположение юниверса.
Sample-ScheduleInfo-Relationships	Позволяет визуализировать действия, выполняемые пользователями.
Sample-QT-Properties с фильтром (сервер)	Позволяет визуализировать свойства InfoObject.

21.4.3 Расширение образца юниверса CMS

Для расширения образца юниверса CMS можно создать связанный юниверс. Связанный юниверс – это юниверс .UNX, который содержит ссылку на предварительно назначенный главный юниверс в CMS.

В данном случае образец юниверса CMS выступает в качестве главного юниверса, т. е. связанный юниверс сможет использовать основание данных и бизнес-уровень образца как готовые структурные блоки. Создав связанный юниверс, можно сохранить его основание данных и бизнес-уровень, унаследованные из образца юниверса CMS, как новые файлы, чтобы их жизненный цикл не зависел от образца.

Можно использовать соединение с базой данных CMS из образца юниверса CMS или другое соединение, совместимое с базой данных CMS.

Также можно добавлять таблицы, создавать объединения, связывающие таблицы главного основания данных с новыми таблицами, и добавлять в бизнес-уровень новые компоненты – точно так же, как при работе с любым другим юниверсом. Любые изменения в главных компонентах автоматически переносятся в связанный юниверс при его возврате в CMS.

21.5 Создание отчета в CMS

С помощью SAP BusinessObjects Web Intelligence можно создать отчет в CMS, используя образец юниверса CMS в качестве источника данных.

1. Откройте приложение Web Intelligence и щелкните значок *Создать* на панели инструментов *Файл*.
2. Выберите образец юниверса CMS.

   Если используется клиент Web Intelligence Rich Client, щелкните *Выбрать*.

   Откроется *Панель запросов*.
3. Выберите показатели и измерения, которые необходимо включить в запрос, и перетащите их на панель *Объекты результатов*.
4. Выберите объекты, которые требуется использовать для определения фильтров запроса, и перетащите их на панель *Фильтры запроса*. Чтобы создать быстрый фильтр для объекта, выберите объект в области *Объекты результатов*, а затем щелкните значок *Добавить быструю фильтрацию* на панели инструментов *Объекты результатов*.
5. Нажмите кнопку *Выполнить запрос*.

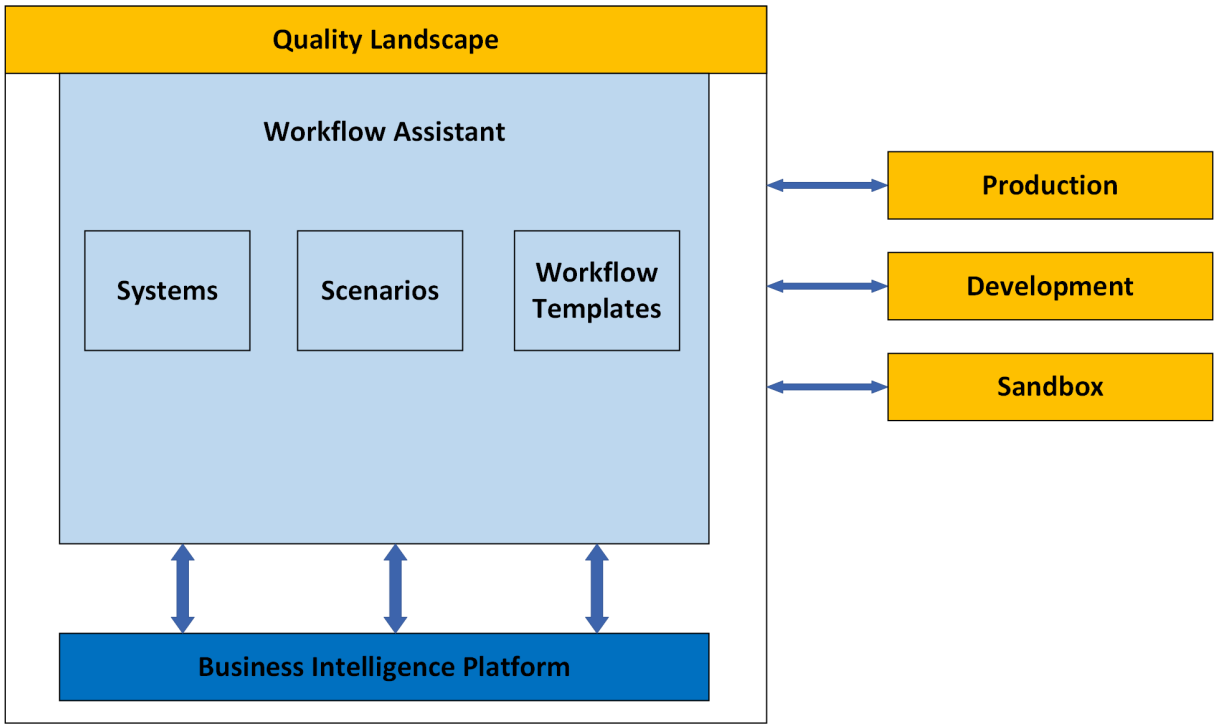
22 Workflow Assistant

Службы Automation Framework и "Агент" теперь объединены в одну службу, которая называется службой Workflow Assistant. Workflow Assistant – это приложение в Central Management Console (CMC) для администрирования систем BI и автоматизации задач BI.

> **Примечание**
>
> Функции Automation Framework в консоли администрирования BI теперь обеспечиваются через Workflow Assistant. URL-адрес консоли администрирования BI (`http://<systemName>:<portNo>/BOE/BIAdminConsole`) и служба очереди сообщений теперь устарели.

Workflow Assistant отображает содержимое в виде вкладок: *Сценарии*, *Модели потока операций* и *Системы*. На этих вкладках можно выполнить детализацию до соответствующего раздела для получения более подробной информации и функций.

Workflow Assistant реализует концепцию на основе ролей, чтобы пользователи имели доступ только к тем вкладкам, для которых у них есть полномочия.



О системах

Термин Система относится к одному или нескольким компьютерам BI, к которым у вас есть доступ. Приложение "Управление системой" предоставляет возможности централизованного доступа

к ландшафтам BI и управления ими. Чтобы использовать возможности Workflow Assistant, необходимо сначала зарегистрировать ландшафты BI с помощью приложения "Управление системой".

О Workflow Assistant

Workflow Assistant позволяет упростить сложные и повторяющиеся задачи BI.

> Пример
>
> Обратите внимание, что необходимо выполнить следующие задачи BI по порядку:
>
> 1. Войдите в платформу BI.
> 2. Измените источник некоторых документов Web Intelligence с `.unv` на `.unx`.
> 3. Обновите эти документы Web Intelligence.
> 4. Выйдите из платформы BI.

Workflow Assistant позволяет сократить объем операций, выполняемых вручную. Можно создать сценарий с помощью шаблонов задач и моделей потока операций, сохранить этот сценарий, выполнить его и просмотреть результаты.

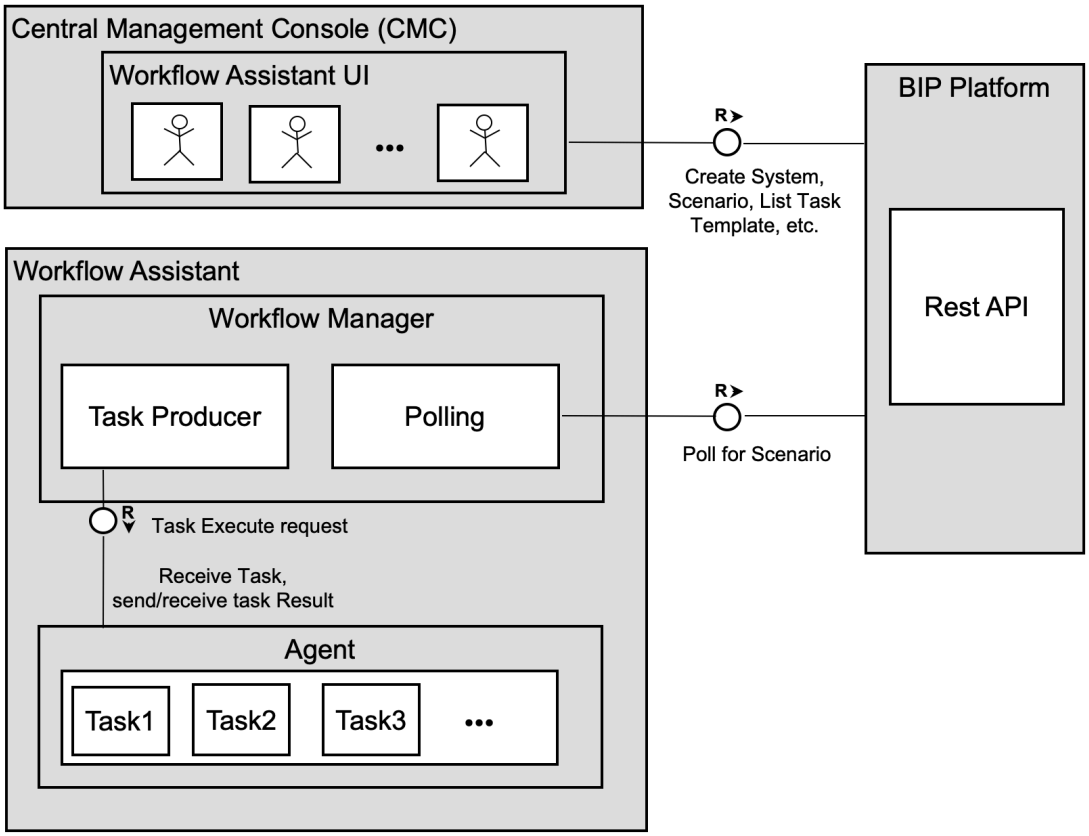
22.1 Целевая аудитория

Это руководство предназначено для определенных пользователей платформы Business Intelligence (BI) и определенных разработчиков платформы BI.

- Пользователи платформы BI, использующие данное руководство, должны иметь права доступа к Central Management Console (CMC) и Workflow Assistant. Эти пользователи имеют роль администраторов или делегированных администраторов.
- Разработчики платформы BI, которые используют это руководство, должны уметь работать с пакетами средств разработки Java и могут создавать схемы JSON для пользовательских требований с помощью SDK шаблонов задач.

22.2 Общие сведения об архитектуре

Следующая диаграмма поможет получить представление об архитектуре Workflow Assistant и соединениях между его компонентами.



Глоссарий терминов, используемых в вышеприведенной диаграмме:

Термин	Определение
Интерфейс пользователя Workflow Assistant	Интерфейс пользователя для создания моделей потока операций и сценариев, которые могут выполняться в любой указанной системе.
Диспетчер потока операций	Диспетчер потока операций выполняет опрос сценариев из платформы, управляет выполнением сценариев и сохраняет результаты.
Агент	Это упрощенный процесс для выполнения задач в сценариях.

22.3 Глоссарий

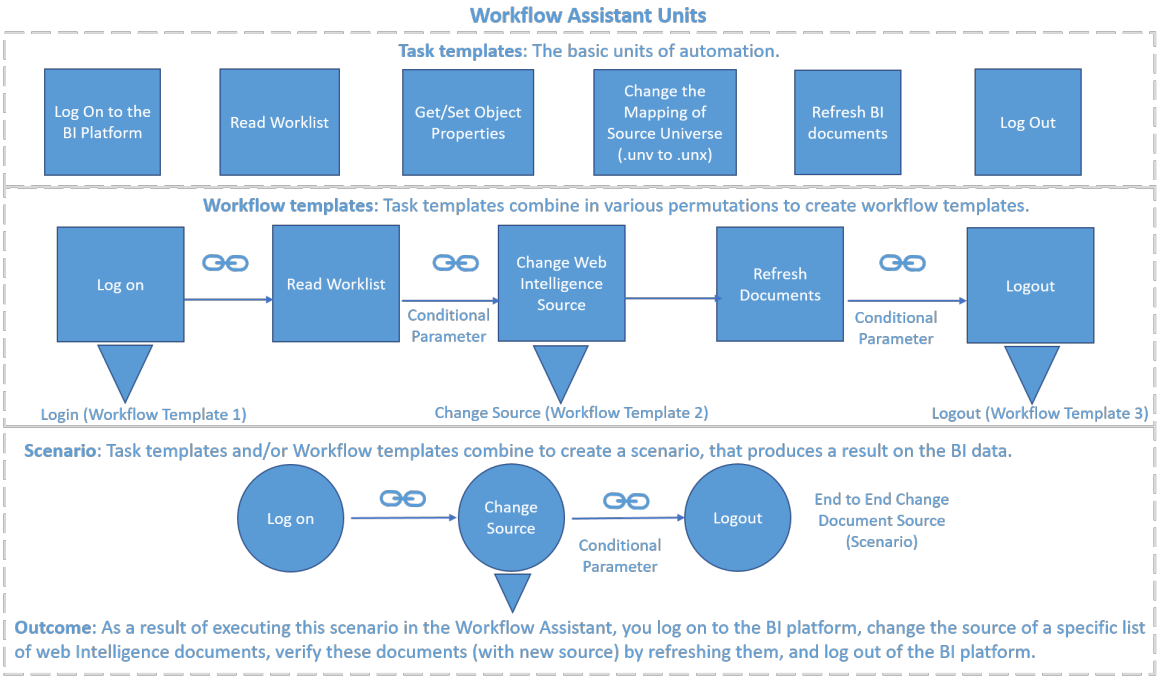
Для Workflow Assistant существует собственный специальный словарь.

Термины, часто используемые в Workflow Assistant

Термин	Определение
Стандартный шаблон задачи	Базовая единица автоматизации, предоставляемая в приложении по умолчанию. Эти единицы можно использовать в сценариях и моделях потока операций. Например, простая задача, такая как вход в платформу BI, обновление документов BI, чтение данных, изменение сопоставления исходного юниверса документов Web Intelligence (с `unv` на `unx`), добавление пользователей в ландшафт или выход из системы.
Пользовательский шаблон задачи	Шаблон задачи (базовая единица автоматизации), созданный разработчиками для пользовательских требований. **⚠ Ограничение** Создать пользовательский шаблон задачи с помощью интерфейса пользователя Workflow Assistant невозможно. Для этого требуется SDK шаблонов задач.
Модель потока операций	Логическая группа шаблонов задач, упорядоченных в требуемой последовательности для достижения результата потока операций.
Стандартная модель потока операций	Модели потока операций, предоставляемые в готовом виде в Workflow Assistant. Администраторы могут использовать стандартные модели потока операций при создании сценариев для различных требований автоматизации BI.
Пользовательская модель потока операций	Модель потока операций, созданная администратором в соответствии с пользовательскими требованиями. Она создается в Workflow Assistant путем группирования стандартных или пользовательских шаблонов задач.
Сценарий	Выполняемая сущность, создаваемая с помощью шаблонов задач или моделей потока операций в требуемой последовательности.

Термин	Определение
Условный параметр	Соединительное звено между шаблонами задач или моделями потока операций, которое направляет поток управления, основано на одном из следующих условий: • Продолжить (по умолчанию) • После успешного выполнения • После сбоя • При частичном успехе **Примечание** Условный параметр также позволяет вставить *задержку времени* (в секундах), чтобы следующая задача сценария начиналась только по истечении определенного времени после завершения предыдущей задачи. **Напоминание** Workflow Assistant учитывает значение условного параметра: "Продолжить", только если предыдущая задача завершена с одним из трех следующих статусов: "Успешно", "Частично успешно" или "Сбой". Если предыдущая задача имеет статус "Ошибка" или "Не выполнено", статус следующего узла автоматически устанавливается на "Не выполнено".

Эта иллюстрация поможет получить представление о взаимосвязи между некоторыми из указанных выше терминов:



22.4 Об установке и обновлении

В зависимости от того, выполняется ли новая установка или обновляется существующая, доступ к функциям бэкэнда может отличаться.

При выполнении **новой установки** платформы SAP BusinessObjects BI (установка по умолчанию) вам предоставляется полный доступ к Workflow Assistant на компьютерах, на которых установлена и сконфигурирована платформа BI. Сюда входит доступ к приложению Workflow Assistant в CMC и функциям бэкэнда (службе Workflow Assistant).

Однако при обновлении платформы BI SP5 или более поздней версии до версии 4.3 доступны все функции Workflow Assistant, но вам еще потребуется просмотреть SAP-ноту, указанную в разделе "Ограничения". После установки обновления запустите поток операций установки "Изменить" для вызова бэкэнд-служб. Для получения дополнительных сведений об изменении установки см. *Руководство по обновлению пакета поддержки*, опубликованное на странице платформы SAP Business Intelligence справочного портала.

> ⓘ Примечание
>
> Workflow Assistant входит в файл BOE.war. После обновления платформы BI 4.2 SP4 или более ранней версии до версии 4.2 SP5 и выше веб-приложение развертывается только в том случае, если во время установки существующей версии была выбрана функция *Веб-приложения Java*.

> ⚠ Предупреждение
>
> Не следует устанавливать Workflow Assistant на нескольких компьютерах в системах, так как кластеризация Workflow Assistant не поддерживается.

Workflow Assistant теперь поддерживает операционные системы AIX и Solaris.

> ⚠ Ограничение
>
> - Для платформ AIX и Solaris: при установке версии BI 4.3 на версии 4.2 SP05 или выше Workflow Assistant устанавливается по умолчанию. Однако для вызова бэкэнд-служб требуется исправление.
> - При обновлении платформы BI 4.2 SP4 или более ранней до версии 4.2 SP5 или выше можно увидеть, что некоторые папки не указаны в Workflow Assistant. Для получения дополнительных сведений см. 2882649.

22.5 Настройка Workflow Assistant

При установке Workflow Assistant в составе установки платформы BI эту службу вы получите по умолчанию.

Затем, чтобы начать использование Workflow Assistant, можно настроить доверительную аутентификацию.

22.5.1 Базовая конфигурация

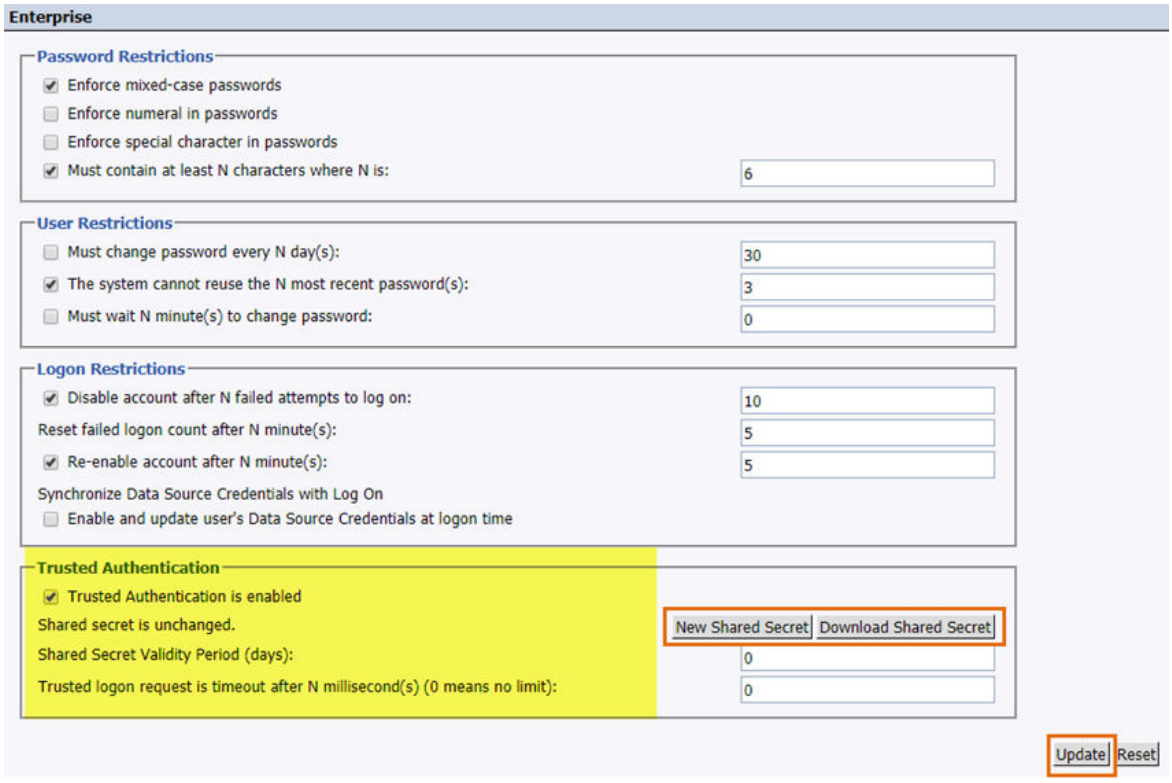
22.5.1.1 Настройка аутентификации Enterprise для Workflow Assistant

Workflow Assistant установлен в рамках установки платформы BI.

Чтобы настроить доверительную аутентификацию (Enterprise) для Workflow Assistant, выполните следующую процедуру.

1. Войдите в Central Management Console (CMC), установив соединение с CMS основного узла.
2. В раскрывающемся списке выберите *Аутентификация* и щелкните дважды *Enterprise*.

Появится диалоговое окно "Enterprise", как показано ниже:



3. Убедитесь, что в разделе "Доверительная аутентификация" включен параметр *Доверительная аутентификация*.
4. Выберите *Новый общий секретный ключ*.
   Общий секретный ключ генерируется.
5. Нажмите *Загрузить общий секретный ключ*.
6. Выберите *Обновить*.
7. Сохраните сгенерированный общий секретный ключ (TrustedPrincipal.conf):
   a. В Windows в каталоге `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0\win64_x64/`.
   b. В Linux в каталоге `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64/`.
   c. В AIX в каталоге `<INSTALLDIR>/sap_bobj/enterprise_xi40/aix_rs6000_64/`.
   d. В Solaris в каталоге `<INSTALLDIR>/sap_bobj/enterprise_xi40/solaris_sparcv9/`.

> **Примечание**
>
> Для получения дополнительных сведений о создании сертификатов доверительной аутентификации с различными параметрами см. раздел Включение доверительной аутентификации [страница 269].

22.5.1.2 Создание пользователя по умолчанию для бэкэнд-службы Workflow Assistant

1. Создайте нового пользователя в Workflow Assistant с именем **WAUser**.
2. Назначьте соответствующие права, перейдя к папке `Workflow Assistant` и предоставьте полный контроль учетной записи **WAUser**.

   Бэкэнд-служба Workflow Assistant запускается с использованием учетной записи **WAUser**.

   Если учетная запись **WAuser** не существует, Workflow Assistant запускается с использованием учетной записи *Администратор*.

   > ⓘ Примечание
   >
   > Новый пользователь не обязательно должен входить в группу пользователей *Администратор*.

22.5.1.3 Запуск службы Workflow Assistant

В этом разделе приводятся инструкции по запуску *службы Workflow Assistant*.

1. Настройте аутентификацию Enterprise для Workflow Assistant. Для получения дополнительных сведений см. Настройка аутентификации Enterprise для Workflow Assistant [страница 883].
2. Для запуска *службы Workflow Assistant*:
   a. В Windows запустите *Central Configuration Manager* (CCM) и *службу Workflow Assistant*.
   b. В Unix перейдите в каталог `<INSTALLDIR>/AdminConsole/WorkflowAssistant/startWfAssistant.sh`.

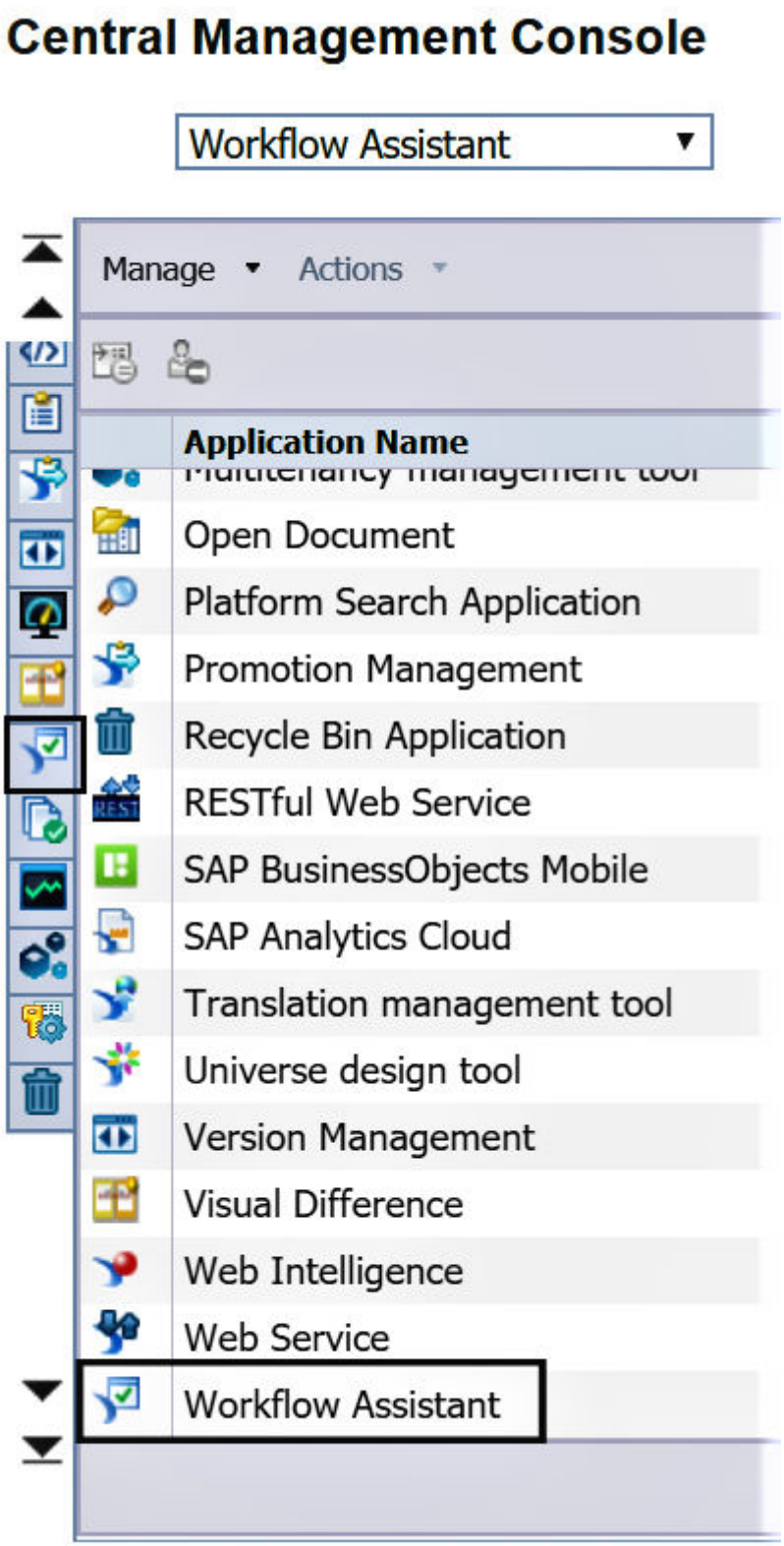
   Теперь можно использовать *Workflow Assistant* и выполнить сценарии.

   > ⓘ Примечание
   >
   > Чтобы убедиться в успешном запуске Workflow Assistant, проверьте содержимое файла `message.properties` в каталоге `<BOE-Install-Directory>\AdminConsole\WorkflowAssistant\service-logs`. Содержимое `message.properties` должно быть следующим:
   >
   > ```
   > STATUS_WFM=success
   >
   > MESSAGE_AGENT=Agent - Started\!\!
   >
   > STATUS_AGENT=success
   >
   > MESSAGE_WFM=Workflow Assistant - Started\!\!
   > ```

22.6 Управление правами Workflow Assistant через Central Management Console

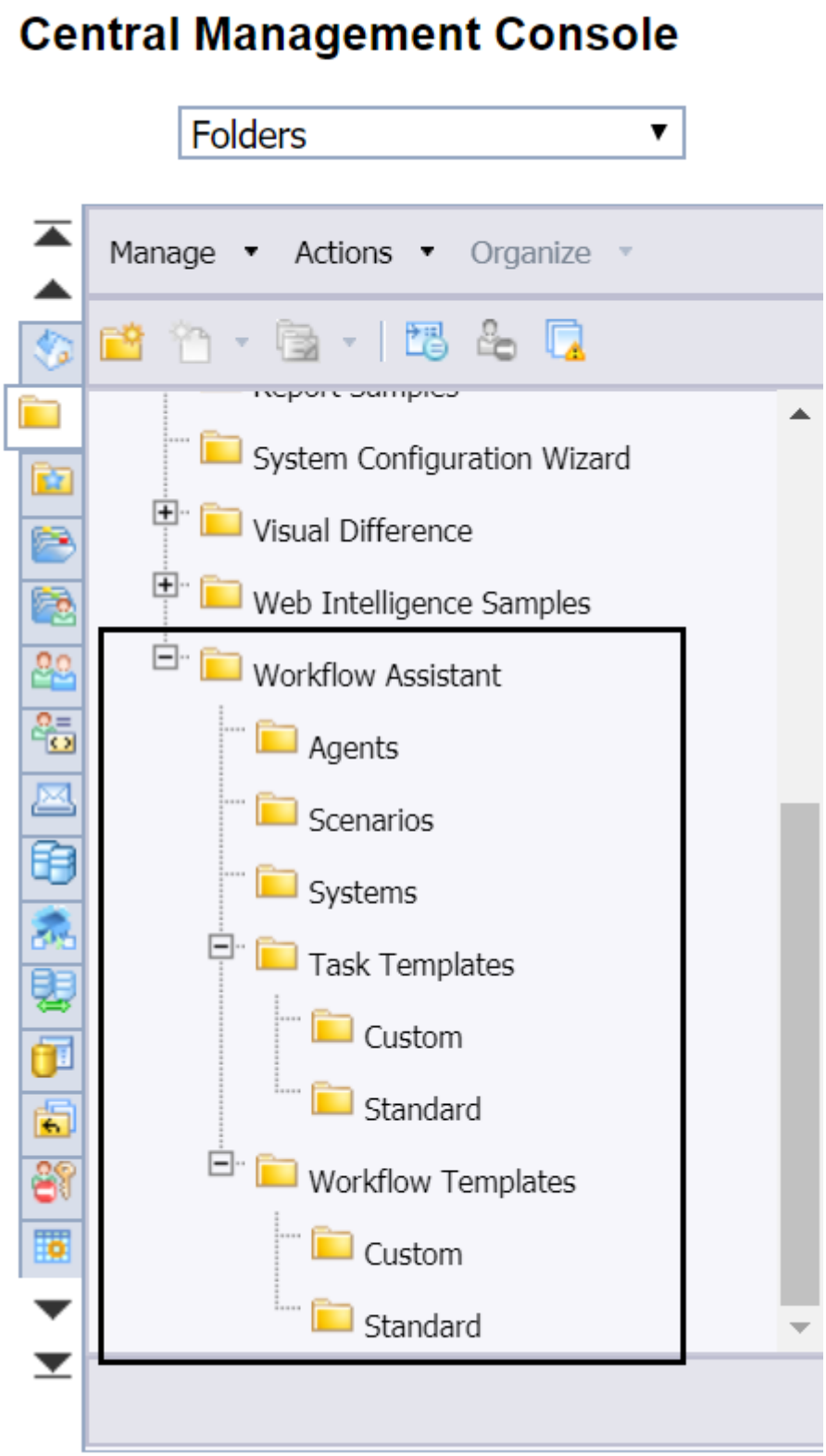
Управление безопасностью Workflow Assistant осуществляется через Central Management Console.

Workflow Assistant отображается в разделе *Приложения Central Management Console*.



В Workflow Assistant вы можете просматривать права доступа и общие настройки безопасности, а также управлять ими для следующих сущностей:

- Системы
- Сценарии
- Шаблоны задач
- Модели потоков операций



Для получения сведений об управлении настройками безопасности для объектов в CMC см. Управление настройками безопасности для объектов в CMC.

> **Примечание**
>
> - Вы можете управлять доступом к функциям в Workflow Assistant, таким как *Системы*, *Сценарии*, *Шаблоны задач* и *Модели потоков операций*, предоставляя пользователю права на уровне папки или объекта, однако отсутствие прав не будет влиять на пользовательский интерфейс. Это означает, что для создания сценария пользователь должен иметь право *Добавить объекты в папку* в папке *Сценарий*.
> - Например, пользователь сможет видеть параметр для создания сценария в Workflow Assistant, даже если у него нет прав на папку *Сценарий* в CMC. Если пользователь попытается создать и сохранить сценарий в папке *Сценарий*, будет выведено сообщение об ошибке.

Управление правами приложений

С помощью соответствующих специфичных для приложения прав в Workflow Assistant можно отклонить или выполнить следующие задачи:

- Чтобы отклонить задачу *Создать шаблон задачи*, перейдите в папку "Шаблон задачи" и отмените право *Добавить объекты в папку*.
- Чтобы отклонить задачу *Создать модель потока операций*, перейдите в папку "Модель потока операций" и отмените право *Добавить объекты в папку*.
- Чтобы отклонить задачу *Создать сценарий*, перейдите в папку "Сценарий" и отмените право *Добавить объекты в папку*.
- Чтобы отклонить задачу *Редактировать шаблон задачи*, перейдите в папку "Шаблон задачи" и отмените право *Редактировать объекты*.
- Чтобы отклонить задачу *Редактировать шаблон задачи, которым владеет пользователь*, перейдите в папку "Шаблон задачи" и отмените право *Редактировать объекты, которыми владеет пользователь*.
- Чтобы отклонить задачу *Редактировать модель потока операций*, перейдите в папку "Модель потока операций" и отмените право *Редактировать объекты*.
- Чтобы отклонить задачу *Редактировать модель потока операций, которой владеет пользователь*, перейдите в папку "Модель потока операций" и отмените право *Редактировать объекты, которыми владеет пользователь*.
- Чтобы отклонить задачу *Редактировать сценарий*, перейдите в папку "Сценарий" и отмените право *Редактировать объекты*.
- Чтобы отклонить задачу *Редактировать сценарий, которым владеет пользователь*, перейдите в папку "Сценарий" и отмените право *Редактировать объекты, которыми владеет пользователь*.
- Чтобы отклонить задачу *Просмотреть шаблон задачи*, перейдите в папку "Шаблон задачи" и отмените право *Просмотр объектов*.
- Чтобы отклонить задачу *Просмотреть шаблон задачи, которым владеет пользователь*, перейдите в папку "Шаблон задачи" и отмените право *Просмотреть объекты, которыми владеет пользователь*.
- Чтобы отклонить задачу *Просмотреть модель потока операций*, перейдите в папку "Модель потока операций" и отмените право *Просмотр объектов*.
- Чтобы отклонить задачу *Просмотреть модель потока операций, которой владеет пользователь*, перейдите в папку "Модель потока операций" и отмените право *Просмотреть объекты, которыми владеет пользователь*.
- Чтобы отклонить задачу *Просмотреть сценарий*, перейдите в папку "Сценарий" и отмените право *Просмотр объектов*.

- Чтобы отклонить задачу *Просмотреть сценарий, которым владеет пользователь*, перейдите в папку "Сценарий" и отмените право *Просмотреть объекты, которыми владеет пользователь*.
- Чтобы отклонить задачу *Удалить шаблон задачи*, перейдите в папку "Шаблон задачи" и отмените право *Удалить объекты*.
- Чтобы отклонить задачу *Удалить шаблон задачи, которым владеет пользователь*, перейдите в папку "Шаблон задачи" и отмените право *Удалить объекты, которыми владеет пользователь*.
- Чтобы отклонить задачу *Удалить модель потока операций*, перейдите в папку "Модель потока операций" и отмените право *Удалить объекты*.
- Чтобы отклонить задачу *Удалить модель потока операций, которой владеет пользователь*, перейдите в папку "Модель потока операций" и отмените право *Удалить объекты, которыми владеет пользователь*.
- Чтобы отклонить задачу *Удалить сценарий*, перейдите в папку "Сценарий" и отмените право *Удалить объекты*.
- Чтобы отклонить задачу *Удалить сценарий, которым владеет пользователь*, перейдите в папку "Сценарий" и отмените право *Удалить объекты, которыми владеет пользователь*.
- Чтобы отклонить задачу *Выполнить сценарий для всех комбинаций*, перейдите к сценарию и отмените право *Добавить объекты в папку*.
- Чтобы отклонить задачу *Выполнить сценарий, которым владеет пользователь, для всех комбинаций*, перейдите к сценарию и отмените право *Добавить объекты в папку, которой владеет пользователь*.
- Чтобы отклонить задачу *Создать ландшафт*, перейдите в папку "Ландшафт" и отмените право *Добавить объекты в папку*.
- Чтобы отклонить задачу *Редактировать и просмотреть ландшафт*, перейдите в папку "Ландшафт" и отмените права *Редактировать объекты* и *Просмотр объектов*.
- Чтобы отклонить задачу *Удалить ландшафт*, перейдите в папку "Ландшафт" и отмените право *Удалить объекты*.
- Чтобы отклонить задачу *Добавить учетные данные пользователя в ландшафт*, перейдите в папку "Ландшафт" и отмените право *Добавить объекты в папку*.

> ⓘ Примечание
>
> Все вышеупомянутые права могут быть применены к отдельному шаблону задачи/модели потока операций/сценарию.

22.7 Работа с Workflow Assistant

Workflow Assistant – это приложение в CMC, позволяющее автоматизировать повторяющиеся и сложные задачи администрирования BI. В следующих разделах описывается, как можно автоматизировать задачи администрирования BI.

22.7.1 О стандартных шаблонах задач

Поставляемые стандартные шаблоны задач встроены (готовы к использованию) в Workflow Assistant. Эти шаблоны задач можно использовать при создании сценариев или моделей потока операций.

Стандартный шаблон задачи	Описание
Вход в систему	Создает сеанс с целевым сервером платформы BI.
Обновить документ	Открывает и обновляет список предоставленных документов с помощью операции `<Поставить в расписание сейчас>`. **Примечание** Для документов с подсказками значения по умолчанию должны быть указаны в документах до выполнения.
Изменить источник Web Intelligence	Изменяет сопоставление исходного юниверса для списка документов с .unv на .unx, .unx на .unx или .unv на .bex.
Добавить/удалить пользователя и группу пользователей	Добавляет или удаляет пользователей и группы пользователей в ландшафте BI. **Примечание** Этот шаблон задачи соответствует `<функции импорта>` на платформе BI. Информацию о функции импорта см. в разделе Массовое добавление пользователей или групп пользователей.
Вызвать свойства	Возвращает значения определенных свойств для запрашиваемых инфо-объектов.
Установить свойства	Устанавливает значения определенных свойств для указанных инфо-объектов в CMS.
Считать рабочий список	Считывает CSV-файлы в качестве ввода и возвращает разделенные запятыми значения, которые могут использоваться в последующих задачах. Используйте этот шаблон задачи, когда в моделях потока операций в сценарии должно использоваться большое количество значений (массовые данные) и невозможно вручную предоставить значения с помощью панели ввода Workflow Assistant.
Запросить рабочий список	Запрашивает таблицы CMS и предоставляет вывод в формате CSV.
Сохранить выходные данные	Сохраняет значения, полученные из *Параметра вывода* задачи, в CSV-файле в CMS.
Установить свойства сервера	Устанавливает значения определенных свойств для указанных серверов.
Выход из системы	Завершает сеанс задачи с целевым сервером платформы BI.

22.7.1.1 Вход в систему

Параметры для шаблона задачи входа в систему

Входные параметры

Имя	Тип	Описание
Система	Строка	Имя зарегистрированного ландшафта в Workflow Assistant

22.7.1.2 Обновить документ

Параметры для обновления документов

Входной параметр

Имя	Тип	Описание
*Документы	CSV	Идентификаторы (id/cuid) для документов, которые требуется обновить. Пользователь также может выбрать документы в Repository Explorer через справку по вводу. Формат CSV: id или cuid

Выходные параметры

Имя	Тип	Описание
SuccessfullyRefreshedDocuments	CSV	Документы, которые успешно обновлены. Формат CSV: id, cuid
UnsuccessfullyRefreshedDocuments	CSV	Документы, которые не были обновлены успешно. Формат CSV: id, cuid
Все	CSV	Список обработанных документов. Формат CSV: id, cuid

22.7.1.3 Изменить источник Web Intelligence

Параметры для изменения источника Web Intelligence

Входные параметры

Имя	Тип	Описание
*Документ	CSV	Укажите cuid документа Web Intelligence, для которого необходимо заменить UNV на UNX, UNX на UNX или UNV на BEx. Пользователь также может выбрать документы в Repository Explorer с помощью справки по вводу или сопоставления вывода одной задачи с другой. Формат CSV: id или cuid
*Сопоставление юниверсов	CSV	Сопоставление юниверсов (UNV, UNX, BEx) на основе id или cuid. Также можно сопоставить юниверсы с помощью экрана "Сопоставление юниверсов" в справке по вводу. Формат CSV (для UNV-UNX): unv_tuid, unx_cuid или unv_id, une_id Формат CSV (для UNX-UNX): src_cuid,dest_cuid,type Формат CSV (для UNV-BEx): src_cuid,dest_cuid,type,technicalical_name
Действие с документом	Строка	Чтобы изменить источник без сохранения документа, присвойте значение: "Тест" Чтобы изменить источник и сохранить документ, присвойте значение: "Изменить"

Выходные параметры

Имя	Тип	Описание
Успешно	CSV	Документы, для которых источник успешно изменен. Формат CSV: id, cuid
Сбой	CSV	Документы, для которых не удалось изменить источник. Формат CSV: id, cuid
Все	CSV	Список документов ввода. Формат CSV: id, cuid

Ограничение

- Только .UNX, созданный на базе запроса .BEx, может быть заменен другим запросом .BEx.
- Запросы BEx с подсказками не поддерживаются.
- Сопоставление происходит только в том случае, если объекты юниверса имеют схожий тип и имена, точно соответствующие объектам запроса BEx.
- Объекты юниверса, созданные с метками, не сопоставляются.

22.7.1.4 Добавить/удалить пользователя и группу пользователей

Параметры для добавления/удаления пользователя и группы пользователей

Входные параметры

Имя	Тип	Описание

*Данные	CSV	Информация, специфичная для пользователя.
		
		См. приведенный ниже образец данных CSV. Для получения дополнительных сведений о данных CSV см. раздел *Массовое добавление пользователей или групп пользователей* в *Руководстве администратора платформы Business Intelligence*.
		
		`command,group,user,fullname,password,mail,profileName,profileValue`
		`Add,MyGroup,MyUser1,MyFullName,Password1,My1@example.com,ProfileName,ProfileValue`

> **Примечание**
>
> Также можно создать CSV-файл без заголовка CSV и использовать его в качестве входных данных в сценарии.
>
> Пароль, выбранный в CSV-файле, должен соответствовать политике паролей.

> **→ Совет**
>
> Для пропуска поля ввода можно использовать последовательные запятые.

22.7.1.5 Вызвать свойства

Параметры для вызова свойств

Входные параметры

Имя	Тип	Описание
*InfoObject	CSV	Значения CSV для инфо-объектов. Префикс "si_" не следует указывать для использования свойств. Формат CSV: id или cuid
Свойство	CSV	Значения CSV свойств. Префикс "si_" не следует указывать для использования свойств. Для инфо-объектов пользователя поддерживается свойство "property;data".

Выходные параметры

Имя	Тип	Описание
Успешно	CSV	Список инфо-объектов, для которых успешно выполнен поиск или присвоение значения свойства. Формат CSV: id или <искомое свойство>
Сбой	CSV	Список инфо-объектов, для которых не удалось выполнить поиск или присвоение значения свойства. Формат CSV: id, cuid
Все	CSV	Список всех обработанных инфо-объектов. Формат CSV: id, cuid

22.7.1.6 Установить свойства

Параметры для установки свойств

Входные параметры

Имя	Тип	Описание
*InfoObject	CSV	Значения CSV для инфо-объектов. Префикс "si_" не следует указывать для использования свойств. Формат CSV: id или cuid
*Свойство	CSV	Значения CSV свойств. Для инфо-объектов пользователя поддерживается свойство "property;data".

Выходные параметры

Имя	Тип	Описание
Успешно	CSV	Список инфо-объектов, для которых значение свойства было успешно вызвано или установлено. Формат CSV: id или <искомое свойство>
Сбой	CSV	Список инфо-объектов, для которых не удалось успешно вызвать или установить значение свойства Формат CSV: id, cuid
Все	CSV	Список всех обработанных инфо-объектов. Формат CSV: id, cuid

22.7.1.7 Установить свойства сервера

Параметры для установки свойств сервера

Входные параметры

Имя	Тип	Описание
*Сервер	CSV	Идентификаторы (id/cuid) для серверов, которые требуется изменить. Пользователь также может выбрать серверы в Repository Explorer через справку по вводу. Формат CSV: id или cuid
*Свойство	CSV	Значения CSV со свойством и значением. Например: `hostname;new value`. Поддерживаемые свойства: hostname

Выходные параметры

Имя	Тип	Описание
Успешно	CSV	Список серверов, для которых значение свойства было успешно установлено. Формат CSV: id
Сбой	CSV	Список серверов, для которых не удалось успешно установить значение свойства. Формат CSV: id
Все	CSV	Список всех обработанных серверов. Формат CSV: id

22.7.1.8 Считать рабочий список

Параметры для чтения рабочего списка

Входные параметры

Имя	Тип	Описание
*Файл	CSV	CSV-файл с необходимыми данными для чтения. Пользователь также может выбрать CSV-файл в Repository Explorer через справку по вводу. Формат CSV: <Заголовок1>, <Заголовок2>, ..<ЗаголовокN> **Примечание** Для получения дополнительных сведений о форматах данных и разделителях в CSV см. Работа с CSV-файлами [страница 906].

Выходные параметры

Имя	Тип	Описание
Значения	CSV	Список значений, считанных из входного файла, которые возвращаются в формате значений, разделяемых запятыми.

22.7.1.9 Сохранить выходные данные

Параметры для задачи сохранения выходных данных

Входные параметры

Имя	Тип	Описание
*Параметр	CSV	Сопоставление выходных данных, полученных из предыдущей задачи.
*Имя файла	Строка	Указание имени файла для сохранения выходных данных.
*Выбрать папку назначения	Строка	Выбор папки, в которой следует сохранить файл.

Имя	Тип	Описание
*Параметры сохранения	Строка	Чтобы перезаписать существующий файл с тем же именем, выберите значение: *Перезаписать* Чтобы переименовать существующий файл с тем же именем с суффиксом _1, _2, выберите значение: *Переименовать*

> ⓘ Примечание
>
> **Выходной параметр:**
>
> Полученные выходные данные – это файл в CMS. Поэтому нет доступного параметра для использования.

22.7.1.10 Выход из системы

Параметры для задачи выхода из системы

Входной параметр

Имя	Тип	Описание
SessionToken	Строка	Маркер сеанса (сгенерирован вследствие входа в систему)

22.7.2 О стандартных моделях потока операций

Поставляемые стандартные модели потока операций встроены (готовы к использованию) в Workflow Assistant. Эти модели потока операций можно использовать при создании сценариев.

Стандартные модели потока операций, доступные в Workflow Assistant

Имя модели	Описание
Вход в систему	Создает сеанс с целевым сервером платформы BI.
Обновить документ	Обновляет указанный список документов Web Intelligence.

Имя модели	Описание
Изменить владение документом	Запрашивает владельца документа и присваивает этого владельца другому документу.
Изменить тип лицензии пользователя	Запрашивает список пользователей на основе специфичных для пользователя условий и изменяет тип лицензии.
Изменить источник Web Intelligence и проверить документы	Массово изменяет сопоставление исходного юниверса с .unv на .unx, .unx на .unx или .unv на .bex и выполняет проверку документов Web Intelligence.
Добавить/удалить пользователей	Позволяет администратору добавлять и удалять пользователей и группы.
Выход из системы	Завершает сеанс задачи с целевым сервером платформы BI.

22.7.3 О пользовательских шаблонах задач

Для создания моделей потока операций и выполнения сценариев можно использовать стандартные шаблоны задач в Workflow Assistant. Если для удовлетворения существующих потребностей стандартных шаблонов недостаточно, можно разработать собственный шаблон задачи и подключаемый модуль для Workflow Assistant.

Создайте собственный пользовательский шаблон задачи с помощью SDK пользовательских шаблонов задач, который предоставляет разработчикам API для внедрения новых шаблонов задач. Для получения дополнительных сведений см. Как создать пользовательский шаблон задачи в BI Automation Framework.

22.7.4 Управление моделями потока операций

Пользовательские модели потока операций можно создавать, изменять и удалять в Workflow Assistant.

22.7.4.1 Создание пользовательских моделей потока операций

Пользовательские модели потока операций создаются с помощью стандартных или пользовательских шаблонов задач.

1. На домашней странице выберите *Workflow Assistant*.

2. На странице *Workflow Assistant* откройте вкладку *Модели потока операций*.
3. Щелкните значок + (*Добавить*) вверху справа на вкладке *Модели потока операций*.
4. На основе *Создать модель потока операций* выберите значок > (*Развернуть*), который отображается перед категориями *Стандартная* и *Пользовательская* шаблонов задач на левой панели.
5. Перетащите нужные шаблоны задач в основу в правой части страницы.
6. Переименуйте эти шаблоны задач в основе.
7. (Необязательно) Выберите значок (*Ссылка*), который отображается между двумя шаблонами задач, и в появившемся списке выберите необходимое значение для условных параметров.

   Здесь также можно вставить требуемую `<задержку времени>` (в секундах).
8. (Необязательно) Установите значения для входных параметров. Они будут использоваться по умолчанию, когда эта модель потока операций будет использоваться в сценарии.
9. Нажмите *Сохранить*.
10. В диалоговом окне *Сохранить модель потока операций* введите имя (обязательно) для модели потока операций и при необходимости добавьте описание.
11. Нажмите *Сохранить* в диалоговом окне *Сохранить модель потока операций*.

    Новая модель потока операций появится в списке в представлении *Модели потока операций* Workflow Assistant.

    > **Примечание**
    >
    > Никакие изменения существующих моделей потока операций не влияют на имеющиеся сценарии.

22.7.4.2 Редактирование пользовательских моделей потока операций

Пользовательские модели потока операций редактируются в Workflow Assistant.

1. На вкладке *Модели потока операций* Workflow Assistant нажмите (*Дополнительно*) и выберите *Редактировать*.
2. На экране *Редактирование модели потока операций* внесите необходимые изменения в модель потока операций, добавив/удалив шаблоны задач, изменив значения входных параметров или изменив условные параметры между шаблонами задач.
3. Нажмите *Сохранить как*.
4. В диалоговом окне *Сохранить модель потока операций* измените имя модели потока операций в соответствии необходимостью.
5. Нажмите *Сохранить*.

   Изменения модели потока операций сохраняются, и снова открывается домашняя страница Workflow Assistant.

22.7.4.3 Удаление пользовательских моделей потока операций

Пользовательские модели потока операций удаляются в Workflow Assistant.

1. На вкладке *Модели потока операций* Workflow Assistant нажмите (*Дополнительно*) и выберите *Удалить*.
2. Нажмите *Удалить* в появившемся предупреждении.

   Удаленная модель потока операций больше не отображается на вкладке *Модели потока операций* Workflow Assistant.

22.7.5 Управление сценариями и просмотр результатов

Сценарии создаются путем соединения шаблонов задач и моделей потока операций. Для управления сценариями и просмотра результатов используется Workflow Assistant.

22.7.5.1 Создание сценариев

В этом разделе объясняется, как можно создавать сценарии в Workflow Assistant.

1. На домашней странице CMC выберите *Workflow Assistant*.

   Доступные сценарии представлены на отображающейся странице.
2. Щелкните значок + (*Создать папку или сценарий*) и выберите *Сценарий*.
3. На странице *Создание сценария* выберите значок > (*Развернуть*), который отображается перед категориями *Стандартная* и *Пользовательская* шаблонов задач на левой панели.

   > **Примечание**
   >
   > Чтобы просмотреть описание задачи, наведите указатель мыши на имя шаблона задачи.
4. Перетащите требуемые модели потока операций в основу в правой части страницы.
5. (Необязательно) Выберите значок (*Ссылка*), который отображается между двумя шаблонами задач, и в появившемся списке выберите необходимое значение для условных параметров.

   Здесь также можно вставить требуемую `<задержку времени>` (в секундах).
6. Щелкните модель потока операций в основе.

   С правой стороны основы откроется панель ввода.
7. На панели ввода справа выберите > (*Развернуть*), чтобы просмотреть поля входных параметров для каждого шаблона задачи и выбрать необходимые значения в этих полях.

   > **Предупреждение**
   >
   > - Убедитесь, что значения ввода, указанные для параметров шаблона, не содержат персональных данных и соответствуют требованиям Общего регламента по защите

данных (GDPR). Для получения дополнительных сведений о GDPR см. раздел Защита и конфиденциальность данных [страница 182].

> **ⓘ Примечание**
>
> Дополнительную информацию о параметрах можно получить, используя "Сведения о параметре". Для получения дополнительной информации по сведениям о параметрах см. Сведения о параметре [страница 907].

8. Нажмите *Сохранить*.

> **→ Напоминание**
>
> Перед выполнением сценария необходимо указать входные данные для каждого шаблона задачи в сценарии. Но также, чтобы указать входные данные, можно использовать параметр *Выполнить с параметром*.

9. В диалоговом окне *Сохранить сценарий* введите необходимые сведения на вкладках *Сохранить сценарий* и *Уведомить по электронной почте*.
   a. На вкладке *Сохранить сценарий* введите имя сценария (обязательно), добавьте описание и выберите расположение, в котором будет сохранен сценарий.
   b. На вкладке *Уведомить по электронной почте* установите переключатель включения. Отображаются параметры, показанные на следующем

   Only On ☐ Success ☐ Partial Success ☐ Failure

   рисунке.
   c. Выберите один или несколько параметров. Выбор служит критерием инициирования уведомления по электронной почте.
   d. Можно включить или выключить *Использовать настройку по умолчанию* с помощью переключателя. Настройки по умолчанию определяются в CMC. Сведения об определении настроек по умолчанию для адресатов электронной почты см. в *Руководстве администратора Business Intelligence*.
   e. В случае отмены выбора *Использовать настройку по умолчанию* укажите адреса в полях *От*, *Кому*, *Копия* (необязательно) и *Скрытая копия* (необязательно), а также сведения в полях *Тема* и *Сообщение*. В каждое поле также можно добавить метку-заполнитель.
10. Нажмите *Сохранить* или *Сохранить и выполнить*.

    Новый сценарий отображается в представлении *Сценарии Workflow Assistant*, и на основании критериев, выбранных на вкладке *Уведомить по электронной почте*, будет инициировано сообщение электронной почты.

22.7.5.1.1 Предоставление входных параметров

При создании моделей потока операций в *Workflow Assistant* можно добавить значения ввода во время разработки и выполнения. Это означает, что можно добавить значения ввода при создании и выполнении сценария. Существует два способа добавления значений ввода в *сценарий*:

1. Справка по вводу

2. Присвоение выходных данных задачи в качестве входных данных другой задачи

Справка по вводу

Можно выбрать объект, такой как документ или рабочий список, в проводнике репозитория с помощью *справки по вводу*. Например, в сценарии для обновления документа можно выбрать документ, нажав значок *Справка по вводу* в поле *Документы*.

Присвоение выходных данных задачи в качестве входных данных другой задачи

При выполнении сценария можно предоставить выходные данные первой задачи в качестве входных данных для второй задачи. В поле ввода необходимо ввести @ для просмотра списка значений, полученных из первой задачи.

- Формат значения ввода: **@<Модель потока операций>.<Шаблон задачи>.<Выходной параметр>**.
- В списке значений ввода отображаются только совместимые значения, полученные из первой задачи. Например, если поле ввода принимает CSV в качестве типа данных, то отображаются значения ввода в формате CSV из предыдущей задачи.

> ⓘ Примечание
>
> Входные параметры поддерживают CSV-файл в качестве входных данных. Для получения дополнительных сведений см. Работа с CSV-файлами [страница 906].

22.7.5.1.2 Работа с CSV-файлами

Большинство стандартных шаблонов задач поддерживают значения параметров ввода в формате CSV. Например, шаблон задачи *Обновление документа* поддерживает формат CSV для поля ввода *Документы*. Это означает, что можно выбрать CSV-файл, состоящий из данных в формате **name, cuid и status**, в качестве ввода для поля *Документы*.

> ⓘ Примечание
>
> Если поле ввода задачи принимает **cuid** и вы выбираете CSV-файл, который содержит другие параметры, включающие **cuid**, то поле ввода использует только значения столбца **cuid** из CSV-файла. Например, см. следующие данные CSV:
>
> name, cuid, status;
>
> Charting, AW4AVT1AUhVAogA6P7OQv9c, success;
>
> SalesReport, BW3AVT1AUhVAogA743QCDsD, success;

В этом примере поле ввода использует AW4AVT1AUhVAogA6P7OQv9c и BW3AVT1AUhVAogA743QCDsD и игнорирует другие значения.

Разделитель столбцов и строк

Поддерживаемый разделитель столбцов: **,**. Разделитель строк: **;**. Разделитель строк и столбцов в поле ввода разделяет данные в формате строк и столбцов. Например, см. следующие данные CSV:

name, cuid, status;

Charting, AW4AVT1AUhVAogA6P7OQv9c, success;

SalesReport, BW3AVT1AUhVAogA743QCDsD, success;

Здесь запятая указывает, что **name, cuid и status** – это столбцы, тогда как точка с запятой обозначает конец строки.

> ⓘ Примечание
>
> Если CSV-файл является вводом для шаблона задачи *Считать рабочий список*, то разделителем столбцов является **,**. Разделителем строк является **;** или новая строка.

> ⚠ Предупреждение
>
> Значение в данных CSV не должно содержать ни запятую, ни точку с запятой.

22.7.5.1.3 Сведения о параметре

Сведения о параметрах можно просмотреть после развертывания и выбора любого параметра на панели ввода сценария. Например, в шаблоне задачи "Обновить документ" есть поле ввода "Документы". Если выбрать поле ввода документа, отобразятся сведения о параметре.

Сведения о параметре включают два раздела:

1. Входной параметр

2. Выходной параметр

Входной параметр

Входной параметр поясняет тип ввода для выбранного поля. Он специфичен для поля ввода в шаблоне задачи.

Выходные параметры

Выходные параметры поясняют различные выходные данные, полученные из задачи. Они являются специфичными для всей задачи, а не только для одного поля ввода.

22.7.5.2 Изменение сценариев

Для изменения сценариев используется Workflow Assistant.

1. На вкладке *Сценарии* Workflow Assistant нажмите ⋯ (*Дополнительно*) и выберите *Редактировать*.

   Появится экран "Изменить сценарий".
2. На экране *Изменить сценарий* внесите необходимые изменения в сценарий, добавив/удалив шаблоны задач или модели потока операций либо изменив значения входных параметров шаблонов.
3. Нажмите *Сохранить*.

   Появится диалоговое окно "Сохранить сценарий".
4. В диалоговом окне *Сохранить сценарий* измените имя сценария на необходимое и нажмите *Сохранить*.

   Изменения сценария сохраняются, и снова открывается домашняя страница Workflow Assistant.

22.7.5.3 Удаление сценариев

Для удаления сценариев используется Workflow Assistant.

1. На вкладке *Сценарии* Workflow Assistant нажмите ⋯ (*Дополнительно*) и выберите *Удалить*.
2. Нажмите *Удалить* в появившемся предупреждении.

   Удаленный сценарий больше не отображается на вкладке *Сценарии* Workflow Assistant.

22.7.5.4 Выполнение сценариев и просмотр результатов

Для выполнения сценариев по данным BI и просмотра результатов используется Workflow Assistant.

1. В представлении *Сценарии* Workflow Assistant нажмите ⋯ (*Дополнительно*) и выберите *Выполнить* или *Выполнить с параметром*.

   Выполнить с параметром позволяет открыть диалоговое окно, в котором отображаются все входные параметры сценария, и изменить значения или указать отсутствующие значения.

> **Примечание**
>
> Значения, заданные в этом диалоговом окне параметров, не сохраняются в сценарии и используются только для выполняемого экземпляра.

Сценарий (плитка или элемент в списке) начинает отображать новый статус "Выполнение" или "В ожидании". После завершения выполнения статус обновляется, чтобы отображалось релевантное значение (`<Успешно/Частично успешно/Сбой/В ожидании/Ошибка/Выполнение с ошибками>`).

2. Чтобы просмотреть результаты сценария (во время выполнения или после успешного завершения), нажмите ⋯ (*Дополнительно*) и выберите *Просмотр результатов*.

> **Примечание**
>
> Можно выбрать параметр "Просмотр истории", чтобы просмотреть результаты предыдущих выполнений сценария.

3. На странице *Результаты* разверните результаты, чтобы просмотреть подробные данные выполнения и завершения для каждой модели потока операций и шаблона задачи в сценарии. После просмотра результатов можно вернуться к главному экрану, нажав кнопку < (*Назад*).

> **Примечание**
>
> Можно выбрать параметр "Экспорт", чтобы сохранить результаты сценария в формате PDF.

> **Примечание**
>
> 1. Для задачи можно установить максимальное время ответа агенту, добавив время (в секундах) для значения ключа task_time_out в файле wfmanager_conf.properties. По умолчанию значение ключа task_time_out имеет значение 86400, т. е. один день.
>
> 2. Значение task_time_out устанавливается для всех агентов в Workflow Assistant.

22.7.5.5 Остановка сценариев

Сценарий можно остановить во время выполнения задачи.

Предварительные условия:

Действия, описанные ниже, можно выполнить, только если сценарий имеет статус "Выполнение" или "В ожидании".

- В представлении "Сценарии" выберите *Дополнительно* для сценария.
- Нажмите "Остановить".

> **Примечание**
>
> Параметр "Остановить" не останавливает сценарий немедленно. После выбора параметра "Остановить" сначала завершается текущая задача, которая выполняется, затем останавливается сценарий. Это означает, что в этом сценарии не будут выполнены только задачи, которые находятся в ожидании.

22.7.6 Общие сведения о состояниях шаблонов задач, моделей потока операций и сценариев

Возможные состояния артефакта (шаблона задачи/модели потока операций/сценария) с описаниями

Состояние	Описание
Создано (C)	Когда артефакт создан, но еще не выполнен даже один раз.
В ожидании (P)	Когда артефакт инициирован для выполнения и ожидает выполнения в очереди.
Выполнение (R)	Артефакт выполняется.
Успешно (S)	После успешного выполнения всех обработанных элементов. Например, обработанные документы успешно обновлены после выполнения задачи "Обновить документ". **Примечание** Если хотя бы одна модель потока операций в сценарии не выполнена успешно, общий сценарий не достигает состояния "Успешно".
Частично успешно (PS)	После успешного выполнения только нескольких обработанных элементов. Например, если после выполнения задачи "Обновить документ" не удалось обновить несколько документов, состояние изменяется на "Частично успешно".
Сбой (F)	После того как не выполнены все элементы.
Ошибка (E)	Когда во время выполнения артефакта возникает ошибка или исключение.
Выполнение с ошибками (RE)	Когда при выполнении артефакта возникает ошибка на сервере, но выполнение продолжается.
Не выполнено	После того как шаблон задачи или модель потока операций в сценарии не выполняется из-за настроек условного параметра. Например, если администратор задает условие <При успехе> между двумя моделями потока операций, вследствие чего поток выполнения не достигает следующей модели потока операций, если не выполнена предыдущая модель потока операций. В этом случае следующая и последующие модели потока операций остаются в состоянии <Не выполнено>.

Примечание

Ниже перечислены условные обозначения для таблиц:

- TTS: статус шаблона задачи
- WFTS: статус модели потока операций
- SS: статус сценария

Матрица статусов: статус шаблона задачи и результирующий статус модели потока операций

TTS1	TTS2	TTS3	TTS4	TTS5	WFTS
S	S	S	E	NE	E (ошибка)
S	S	S	PS	NE	PS (частично успешно)
S	S	PS	F	NE	F (сбой)
S	PS	F	R	NE	R (выполнение)
S	E	NE	NE	NE	E (ошибка)
S	E	RE	NE	NE	RE (выполнение с ошибками)

Следующая матрица поясняет, как статус каждой модели потока операций влияет на общий статус сценария.

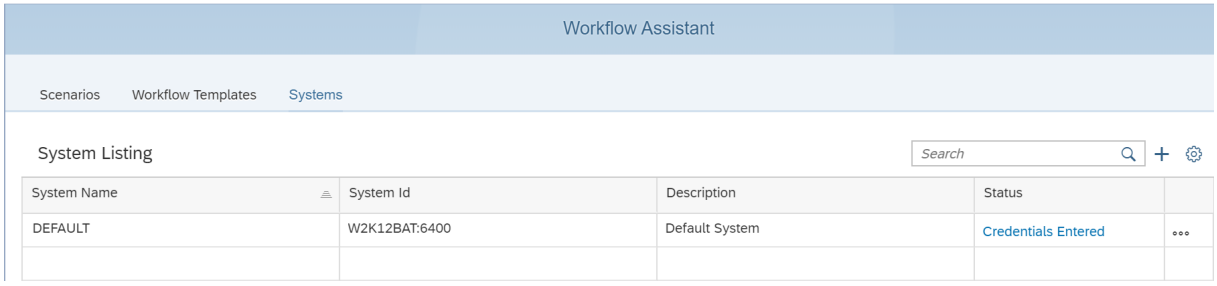
Матрица статусов: статус модели потока операций и результирующий статус сценария

WFTS1	WFTS2	WFTS3	WFTS4	WFTS5	SS
S	S	S	E	NE	E (ошибка)
S	S	S	PS	NE	PS (частично успешно)
S	S	PS	F	NE	F (сбой)
S	PS	F	R	NE	R (выполнение)
S	E	NE	NE	NE	E (ошибка)
S	E	RE	NE	NE	RE (выполнение с ошибками)

22.7.7 Работа с системами

Вкладка *Системы* позволяет зарегистрировать несколько ландшафтов BI. Вкладка *Системы* предоставляет доступ к зарегистрированным ландшафтам BI.

Снимок вкладки *Системы*



На вкладке *Системы* можно выполнить следующие действия:

- Добавить (зарегистрировать) новую систему

  > → Напоминание
  >
  > Регистрация систем на этой вкладке является обязательной, чтобы можно было использовать эти системы в других представлениях, таких как *Сценарии* и *Модели потока операций*.

- Изменить (отредактировать или удалить) существующую систему
- Подключиться к системе (или отключиться от нее), введя свои учетные данные (`User Name, Password, Authentication`)

  > ⓘ Примечание
  >
  > Система, где установлен Workflow Assistant, отображается в списке на вкладке *Системы* как система по умолчанию. Однако для соединения с этим ландшафтом необходимо ввести свои учетные данные.

- Настроить столбцы, отображаемые в представлении Системы

22.7.7.1 Регистрация новой системы BI

Чтобы подключиться к авторизованной системе BI и использовать функции Workflow Assistant, сначала необходимо зарегистрировать (добавить) системы BI в Workflow Assistant.

Для регистрации систем следуйте описанной ниже процедуре:

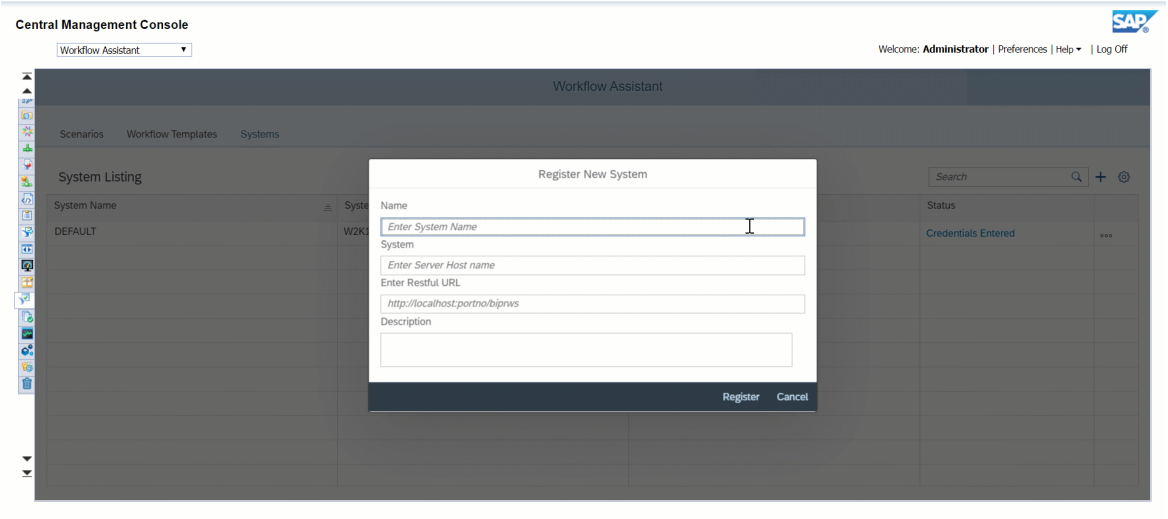
1. Выполните вход в Workflow Assistant.
2. На *домашней* странице перейдите на вкладку *Системы*.

   В этом представлении перечислены доступные зарегистрированные системы.
3. Нажмите значок + (*Добавить*).

   Появится диалоговое окно "Зарегистрировать новую систему".
4. В поле `<Имя>` введите псевдоним, по которому можно найти систему.
5. В поле `<Система>` введите имя хоста сервера или IP-адрес, идентифицирующий компьютер или кластер компьютеров.
6. В поле `<URL-адрес RestFull>` введите URL-адрес веб-служб RESTful для сервера платформы BI. Также в поле `<Описание>` можно добавить описание системы.
7. Нажмите *Зарегистрировать*.

   > ⓘ Примечание
   >
   > Одну и ту же систему BI можно зарегистрировать под разными именами, но рекомендуется, чтобы в представлении "Системы" система BI была зарегистрирована только один раз.

   Зарегистрированная система добавляется в список в таблице "Список систем".



22.7.7.2 Изменение существующих систем BI

Представление "Системы" позволяет изменять зарегистрированные системы.

Чтобы изменить существующую систему, выполните описанную ниже процедуру.

1. Выполните вход в Workflow Assistant и перейдите на вкладку *Системы*.
2. В представлении "Системы" выберите ⋯ (*Дополнительно*) → *Редактировать* для указанной в списке системы, которую требуется изменить.

   Откроется диалоговое окно *Изменить систему*.
3. В соответствии с необходимостью измените значения в полях `<Имя>` (псевдоним), `<Система>`, `<URL-адрес RestFull>` и `<Описание>` и нажмите *Готово*.

   Изменения отражаются в таблице "Список систем".

> ⓘ Примечание
>
> Чтобы удалить систему, выберите (*Дополнительно*) → *Удалить* для указанной в списке системы, которую требуется удалить, и в появившемся диалоговом окне подтвердите удаление.

22.7.7.3 Соединение с зарегистрированными системами BI

Вы можете подключиться к своим зарегистрированным системам, используя поле `<Статус>` в таблице "Список систем". Соединение с системой BI имеет важное значение для использования систем в сценариях в Workflow Assistant.

Чтобы подключиться к добавленной системе BI, следуйте описанной ниже процедуре.

1. Выполните вход в Workflow Assistant и перейдите на вкладку *Системы*.
2. Выберите строку флага (*Учетные данные не введены*) в поле `<Статус>` зарегистрированных систем, с которыми еще не установлено соединение.

   Появится диалоговое окно "Введите учетные данные".
3. Введите свои учетные данные для системы BI (на основе полномочий, предоставленных администратором платформы): `<Имя пользователя>`, `<Пароль>` и `<Аутентификация>`. Затем нажмите *Сохранить*.

   Workflow Assistant проверяет учетные данные и, если проверка выполнена успешно, обновляет `<Статус>` вашего ландшафта BI на *Учетные данные введены*. В противном случае выводится сообщение об ошибке, и `<Статус>` не изменяется.

22.7.7.4 Пользовательская настройка представления "Системы"

Внешний вид представления "Список систем" можно настроить, изменив видимость полей (столбцов) в представлении.

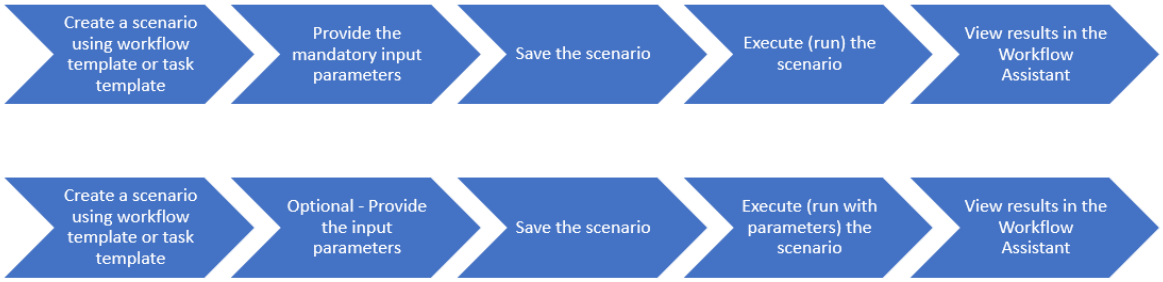
Чтобы скрыть/показать определенные столбцы представления "Системы", выполните следующие действия.

1. Выполните вход в Workflow Assistant и перейдите на вкладку *Системы*.
2. Выберите (*Настройки*) и отмените выбор столбцов (заголовков полей), которые необходимо скрыть в таблице "Список систем".

   Эти столбцы больше не будут отображаться в таблице "Список систем".
3. Чтобы снова включить скрытый столбец в представление, нажмите *Настройки* и вновь выберите нужные заголовки полей.

22.7.8 Непрерывное выполнение Workflow Assistant

См. визуальное представление.



22.8 Проверка файлов журналов

В этом разделе описана проверка файлов журналов Workflow Assistant.

Workflow Assistant

Для Workflow Assistant следует выбрать уровень трассировки в файле *WorkflowAssignant_Trace.ini* в каталоге `<INSTALLDIR>\AdminConsole\WorkflowAssistant`. Файлы трассировки также можно настроить с помощью файла **_Trace.ini**, задав следующие переменные среды:

- `BO_TRACE_CONFIGDIR`, чтобы задать имя папки файлов конфигурации для журналов, например: `C:\BOTraces\config`
- `BO_TRACE_CONFIGFILE`, чтобы задать имя файла конфигурации, например `BO_Trace.ini`
- `BO_TRACE_LOGDIR`, чтобы задать имя папки для журналов, например: `C:\BOTraces`

> **Примечание**
>
> Имя файла `INI` следует вводить с учетом регистра.

Создайте файл конфигурации `BO_Trace.ini` следующим образом:

```
sap_log_level = log_info;
sap_trace_level = trace_debug;
```

Можно проверить журналы по умолчанию в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging`.

23 Корзина

23.1 Корзина

Общие сведения о корзине

Корзина — это новое приложение в CMC. Удаляемые пользователем элементы из системы BOE перемещаются в корзину, где хранятся до тех пор, пока она не будет очищена. Благодаря корзине пользователь может восстановить случайно удаленные отчеты и папки в их исходном расположении.

Корзина позволяет администратору:

- инициировать восстановление любого удаленного элемента (например, отчетов и папок),
- удалить элементы из корзины без возможности восстановления,
- выполнить автоматическую очистку корзины.

Если корзина включена, в нее можно переносит инфо-объекты следующих типов:

- Содержимое личных папок
- События
- Календари
- Содержимое общих папок
- Юниверсы
- Соединения
- Общие категории
- Персональные категории
- Входящая почта
- Профили
- Пользовательские роли

23.1.1 Восстановление элементов из корзины

В корзине отображается список удаленных элементов. Чтобы восстановить элемент из корзины, выполните следующие действия:

1. Войдите в CMC.
2. На панели *Управление* на главной странице CMC выберите *Корзина*.
3. Щелкните правой кнопкой мыши элемент, который требуется восстановить, и выберите в контекстном меню команду *Восстановить*.

4. Нажмите кнопку *OK*.

   Чтобы убедиться, что операция восстановления выполнена, можно перейти в папку восстановленного элемента.

   > ⓘ Примечание
   >
   > Если при восстановлении элемента из корзины в папке восстановления существует другой элемент с таким же именем, то восстанавливаемый элемент сохранится в этой папке со следующем именем: "<имя_элемента> restored(1, 2...)".
   >
   > Если родительская папка элемента из корзины была удалена, то при восстановлении элемента она будет создана заново. Однако в ней будут содержаться только элементы, восстановленные из корзины.
   >
   > Из корзины невозможно открыть элемент или перейти к нему.
   >
   > Если вы удаляете элемент из папки, а впоследствии администратор ограничивает права на изменение этой папки, будет возможно восстановить такой элемент в исходную папку.

Элемент восстановлен из корзины.

23.1.2 Удаление элементов из корзины без возможности восстановления

Администратор может удалить из корзины отдельные элементы или очистить ее полностью.

Чтобы удалить элементы из корзины без возможности восстановления, выполните следующие действия:

1. Войдите в CMC.
2. На панели *Управление* на главной странице CMC выберите *Корзина*.
3. Щелкните правой кнопкой мыши элемент, который требуется удалить, и выберите в контекстном меню команду *Удалить*.
4. Выберите *OK*.

Элемент удален из корзины.

23.1.3 Включение автоматической очистки корзины

Можно периодически выполнять автоматическую очистку корзины.

Чтобы включить автоматическую очистку корзины, выполните следующие действия:

1. Войдите в CMC.
2. На панели *Управление* на главной странице CMC выберите *Приложения*.
3. На странице *Приложения* выберите приложение *Корзина*.

   Откроется диалоговое окно *Свойства: корзина*.

4. Установите флажок и укажите, через сколько дней элементы в корзине будут удаляться без возможности восстановления.
5. Нажмите кнопку *Сохранить и закрыть*.

Автоматическая очистка корзины настроена.

24 Аудит

24.1 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 юниверсов и отчетов можно просмотреть в сети сообщества SAP http://community.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

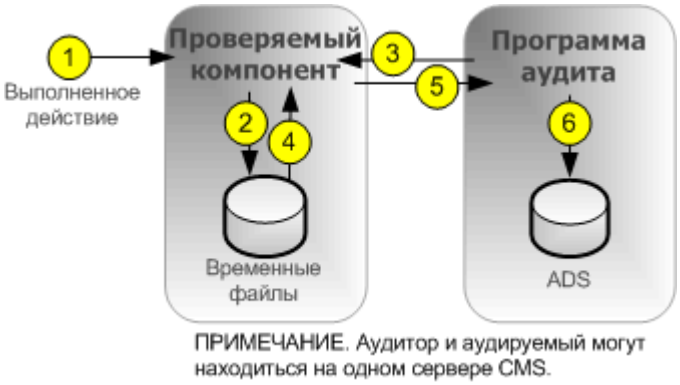
Центральный сервер управления (CMS) выполняет роль аудитора системы, а сервер или приложение, инициирующее проверяемое событие, выполняют роль проверяемого компонента. Если происходит событие, подлежащее аудиту, в проверяемом компоненте создается запись, которая сохраняется в локальном временном файле. 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

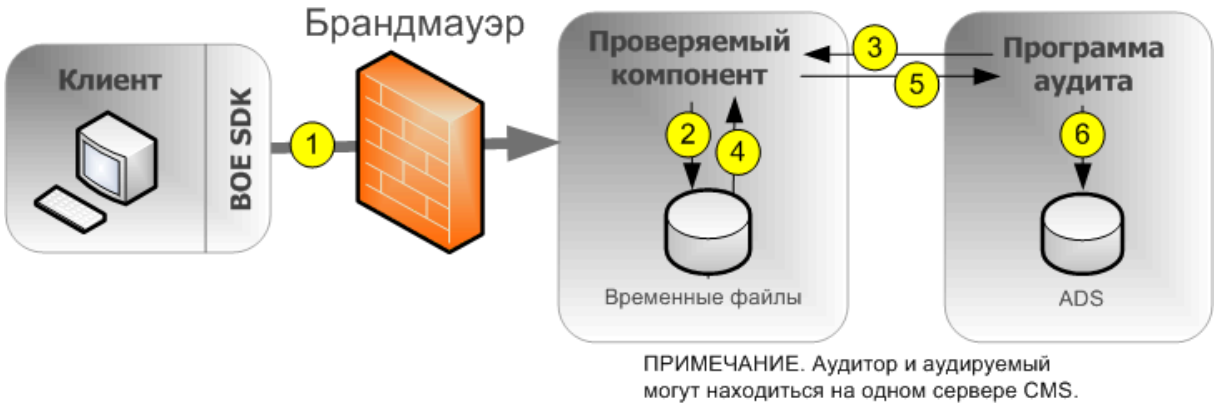
При возникновении событий, созданных сервером, CMS может выступать в роли аудитора и проверяемого.



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.



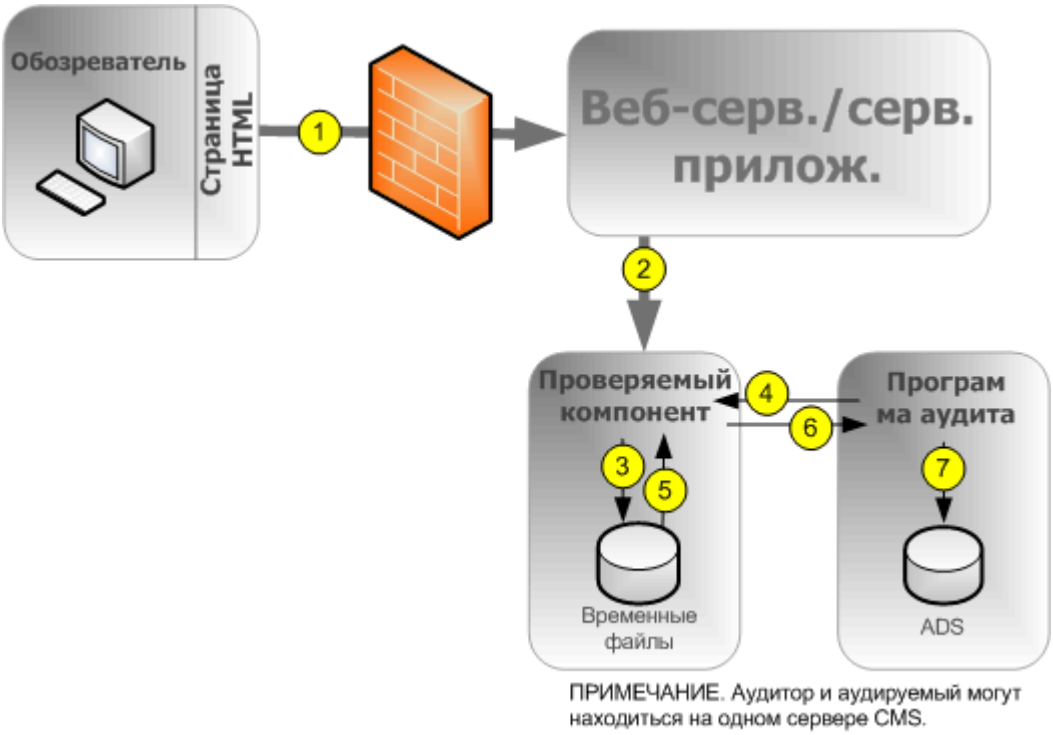
1. Клиент подключается к CMS, который выполняет роль проверяемого компонента. Клиент предоставляет IP-адрес и имя компьютера, а проверяемый компонент проверяет эти данные.

> ⓘ 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.

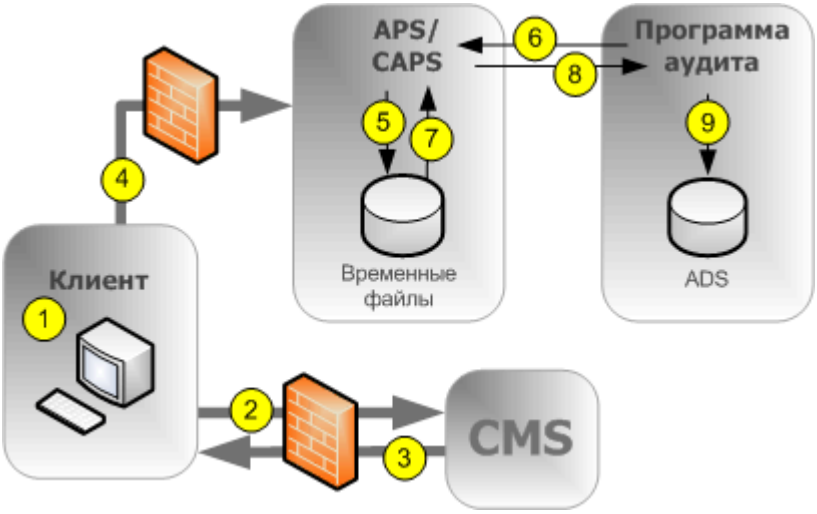


1. Браузер подключается к серверу веб-приложения, и на него передаются данные входа в систему.
2. SDK платформы BI отправляет проверяемому компоненту (CMS) запрос входа, а также IP-адрес и имя компьютера, на котором установлен браузер.
3. Проверяемый компонент записывает события во временный файл. Шаги 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.



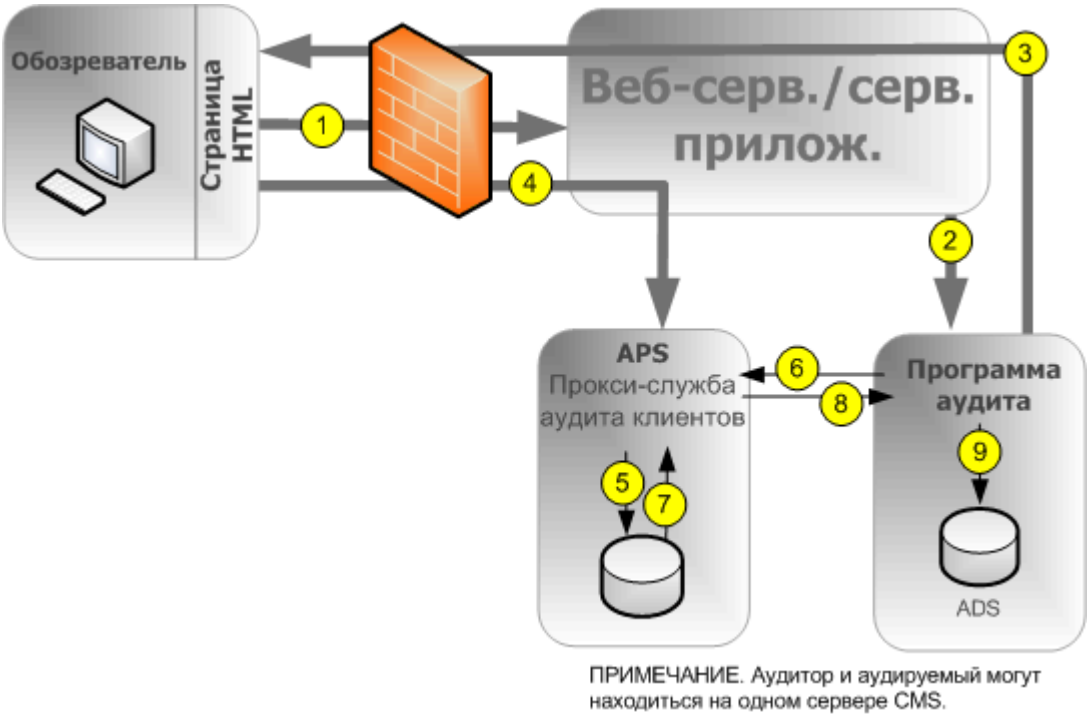
1. Пользователь выполняет операцию, которая подлежит аудиту.
2. Клиент устанавливает связь с CMS для проверки, настроена ли операция на аудит.
3. Если для действия назначен аудит, CMS сообщает эту информацию клиенту.
4. Клиент отправляет сведения о событии прокси-службе аудита клиента (CAPS), размещенной 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.



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:

- Analysis, выпуск для OLAP (AOLAP)
- Стартовая панель BI (BILP)
- Диспетчер Business View (BVM)
- Central Configuration Manager (CCM)
- Central Management Console (CMC)
- OpenDocument
- Средство дизайна информации (IDT)
- Live Office (LO)
- SAP BusinessObjects Mobile
- Средство управления переводами (TMT)
- Web Intelligence Rich Client (WIRC)
- Приложение Lumira Desktop (Discovery)
- Приложение Lumira Designer

> ⓘ 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.

> ⓘ Примечание
>
> 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".

> ⓘ Примечание
>
> 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 [страница 1259]

24.2 Страница "Аудит CMC"

Страница *Аудит* в консоли CMC содержит следующие области:

- *Сводка состояния*
- *Установить события*
- *Установить сведения о событии*
- *Настройка*

24.2.1 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	Процентная доля цикла опроса, которую CMS затрачивает на сбор данных о проверяемых объектах. Остаток – это время в состоянии покоя между опросами. 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. 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 соединений или более мощного аппаратного обеспечения базы данных), либо уменьшить число событий аудита, отслеживаемых системой.

Показатель	Сведения
Последний цикл опроса: продолжительность	Длительность последнего цикла опроса в секундах. Указывает максимальную задержку доставки данных о событии в базу данных аудита в течение предыдущего цикла опроса. • 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. 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 соединений или более мощного аппаратного обеспечения базы данных), либо уменьшить число событий аудита, отслеживаемых системой.
Аудитор CMS	Имя CMS, функционирующего в данный момент в качестве аудитора.
Имя соединения с базой данных ADS	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 соединения, за которыми следует имя сервера.
Имя пользователя базы данных ADS	Имя пользователя проверяющего CMS. используемое для входа в базу данных ADS.

24.2.2 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
>
> События аудита отправляются в базу данных аудита в пакетном режиме, а не по одному. Установленный в настоящее время размер пакета – 1000 событий аудита.

> **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.*

24.2.2.1 Настройка событий аудита

Чтобы настроить события аудита, выполните следующие действия:

1. В Central Management Console откройте вкладку *Аудит*.
   Откроется страница *Аудит*.
2. Установите ползунок *Установить события* на требуемый уровень аудита, где каждый уровень аудита соответствует определеному значению показателя.
   - *Выкл.* – 1
   - *Минимальный* – 2
   - *По умолчанию* – 3
   - *Завершено* – 4
   - *Пользовательский* – 0

   В следующей таблице показаны различные параметры настройки для ползунка и события, собираемые на каждом уровне.

Уровень аудита	Собираемые события
Выкл.	Нет
Минимальный	• Вход в систему • Выход из системы • Изменение прав • Пользовательский уровень доступа изменен • Изменение аудита
По умолчанию	*Минимальные* события, плюс: • Просмотр • Обновить • Подсказка • Создание • Удаление • Изменение • Сохранение • Поиск • Изменить • Выполнение • Доставка

Уровень аудита	Собираемые события
Завершено	*Минимальные* события и события *По умолчанию*, плюс: • Инициация • Детализация за пределами области действия • Страница извлечена • Конфигурация Диспетчера переноса объектов • Откат • Добавление VMS • Извлечение VMS • Возврат VMS • Изъятие VMS • Экспорт VMS • Блокировка VMS • Разблокирование VMS • Удаление VMS • Соединение с кубом • Сеанс MDAS **Примечание** Если установлены дополнительные компоненты, можно просматривать больше событий.
Пользовательский	Выбор пользовательского набора событий.

Примечание

Если *Установить события* установлено на *По умолчанию*, то значение *Уровень аудита* будет равно 3.

При установке параметра *Установить события* на *Выкл.* значение *Уровень аудита* изменится с 3 на 1.

3. Выберите значение *Пользовательский*, щелкните события для внесения в список под ползунком *Установить события*.
4. Под *Установить сведения о событии* щелкните дополнительные сведения, которые вы хотите записать вместе с событиями. Чем меньше записывается сведений, тем лучше 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: • *Путь к папке объекта (идентификатор сведений 71)*

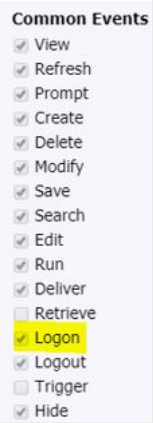
Сведения	Описание
	• *Имя верхней папки (идентификатор сведений 72)* • *Путь к каталогу контейнера (идентификатор сведений 64)*
Сведения о правах	При выборе этого параметра будут собираться следующие сведения: • *Право добавлено (идентификатор сведений 55)* • *Право удалено (идентификатор сведений 56)* • *Право изменено (идентификатор сведений 57)*
Сведения о группе пользователей	При выборе этого параметра будут собираться следующие сведения: • *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 CMC, стартовой панели BI или событий SharePoint.

5. Нажмите кнопку *Сохранить*.

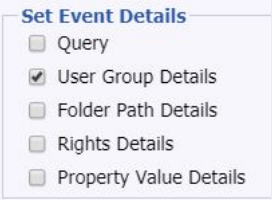
> ⓘ Примечание
>
> При аудите клиента после внесения изменений системе потребуется около двух минут, чтобы начать запись данных для каких-либо новых событий. При внесении изменений в систему убедитесь, что эта задержка допустима.

24.2.2.2 Расширенная запись сведений о событии в таблице подробных данных аудита

> ⓘ Примечание
>
> • Чтобы усвоить информацию, которая представлена ниже, вы должны обладать достаточными знаниями в отношении Страница "Аудит CMC" [страница 925], особенно касательно *общих событий, установки сведений о событии, сведений о группе пользователей* и *входа в систему*.
> • *Вход в систему* - событие, обеспечивающее сведения о пользователе, получающем доступ к приложению.



- *Сведения о группе пользователей* позволяют получить информацию о группах пользователей, связанных с пользователем, для каждого события.



Запись сведений о группе пользователей в таблице AUDIT_EVENT_DETAIL частично зависит от выбора, произведенного в разделах *Общие события* и *Установить сведения о событии* на странице аудита. Рассмотрим сценарий, в котором вы выбрали *Вход в систему*, но не выбрали *Сведения о группе пользователей* на странице *Аудит*. В этом сценарии сведения о группе пользователей по-прежнему записываются для события *Вход в систему* в таблице AUDIT_EVENT_DETAIL. Чтобы понять поведение в BI 4.2 с пакетом поддержки 5, см. следующую таблицу.

Вход в систему	Сведения о группе пользователей	Поведение
Выбрано	Выбрано	Сведения о группе пользователей записываются для всех событий, выбранных в разделе "Общее событие".
Выбрано	Не выбрано	Сведения о группе пользователей записываются только для событий входа в систему.
Не выбрано	Не выбрано	Сведения о группе пользователей не записываются.
Не выбрано	Выбрано	Сведения о группе пользователей записываются для всех выбранных событий, за исключением событий входа в систему.

24.2.3 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.

24.2.3.1 Настройка параметров базы данных ADS (хранилища данных аудита)

1. В консоли 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 данных	Имя соединения
IBM DB2	имя службы
Microsoft SQL Server	ODBC DSN
MySQL	`<serverhostname>,<port>,<databasename>`
Oracle	Имя службы TNS
SAP HANA	ODBC DSN
SAP MaxDB	`<serverhostname>,<port>,<databasename>`
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.

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 109 200.)

> ⚠ 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.

24.3 События аудита

В следующей таблице представлены все события аудита в системе с кратким описанием. Список типов служб, создающих события.

Событие	
Описание изменения аудита, а также серверы и клиенты, создающие тип события	Настройки аудита системы изменены. • Центральная служба управления
Создание	В систему добавлен новый объект. • Службы BI Commentary • Центральная служба управления • Служба просмотра и изменения Crystal Reports • Desktop Intelligence • Служба Information Engine • Управление жизненным циклом • Web Intelligence • Общая служба Web Intelligence

Событие	
	• Описание, а также серверы и клиенты, генерирующие основную службу Web Intelligence • Служба обработки Web Intelligence
Соединение с кубом	Выполняется операция соединения с кубом OLAP. • Multi-Dimensional Analysis Service • Аналитические приложения
Пользовательский уровень доступа изменен	Изменена информация по привилегиям. • Центральная служба управления
Удаление	Объект удален из системы. • Службы BI Commentary • Центральная служба управления • Служба управления жизненным циклом
Доставка	Объект отправлен/назначен по месту назначения. • Служба планирования обновления аутентификации • Центральная служба управления • Служба 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
Детализация за пределами области действия	Пользователем документа Web Intelligence выполнен переход по иерархии до уровня детализации, находящегося за пределами предварительно загруженных данных отчета. • Web Intelligence • Служба обработки Web Intelligence • Общие службы Web Intelligence • Основные службы Web Intelligence • Служба Information Engine
Правка	Содержимое объекта изменено. • Приложение "Рабочие пространства BI"

Событие	
	• Desktop Intelligence • Служба Information Engine • Web Intelligence • Общая служба Web Intelligence • Основная служба Web Intelligence • Служба обработки Web Intelligence
Конфигурация LCM	Сведения конфигурации консоли управления жизненным циклом (LCM) изменены. • Управление жизненным циклом
Вход в систему	Пользователь входит в систему. • Центральная служба управления
Выход из системы	Пользователь выходит из системы • Центральная служба управления
Изменение	Свойства файла объекта изменены • Web Intelligence • Управление жизненным циклом • Центральная служба управления • Службы BI Commentary
Сеанс MDAS	Выполняется операция службы многомерного анализа. • Multi-Dimensional Analysis Service
Страница извлечена	Клиент SAP BusinessObjects Web Intelligence извлекает дополнительную информацию из репозитория. • Служба обработки Web Intelligence • Общие службы Web Intelligence • Основные службы Web Intelligence • Служба Information Engine
Подсказка	Для подсказки объекта введена информация. • Служба кэша Crystal Reports • Служба планирования Crystal Reports для Enterprise • Служба планирования Crystal Reports • Desktop Intelligence • Служба Information Engine • Live Office • Web Intelligence • Общая служба Web Intelligence • Основная служба Web Intelligence • Служба обработки Web Intelligence
Обновление	Данные в объекте обновлены из базы данных по запросу пользователя.

Событие	
	• Служба кэша Crystal Reports • Служба планирования Crystal Reports для Enterprise • Служба планирования Crystal Reports • Desktop Intelligence • Служба Information Engine • Live Office • Web Intelligence • Общая служба Web Intelligence • Основная служба Web Intelligence • Служба обработки Web Intelligence
Извлечение	Объект извлечен из репозитория. • Центральная служба управления • Desktop Intelligence
Изменение прав	Для пользователя, группы или объекта изменены параметры безопасности. • Центральная служба управления
Откат	LifeCycle Manager используется для восстановления предыдущей версии объекта. • Управление жизненным циклом
Выполнение	Задание выполняется. • Служба планирования обновления аутентификации • Служба 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

Событие	
Сохранение	Объект сохранен после обновления или изменения. • Выпуск Analysis для OLAP • Служба кэша Crystal Reports • Служба планирования Crystal Reports для Enterprise • Служба планирования Crystal Reports • Служба просмотра и изменения Crystal Reports • 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	Выполнен поиск. • Служба поиска • Explorer • Управление жизненным циклом
Инициация	Запущено событие файла. • Служба событий • Центральная служба управления
Просмотр	Объект просматривается. • Аналитические приложения • Выпуск Analysis для OLAP • Стартовая панель BI • Приложение "Рабочие пространства BI" • Службы BI Commentary • CMC • Служба кэша Crystal Reports • Служба просмотра и изменения Crystal Reports • Desktop Intelligence • Служба Information Engine • Open Document • SAP BusinessObjects Mobile • Web Intelligence • Общая служба Web Intelligence • Основная служба Web Intelligence • Служба обработки Web Intelligence
Добавление VMS	Объект добавляется к системе контроля версий LCM.

Событие	
	• Управление жизненным циклом
Возврат VMS	Объект возвращен в систему контроля версий LCM. • Управление жизненным циклом
Изъятие VMS	Объект изъят из системы контроля версий LCM. • Управление жизненным циклом
Экспорт VMS	Ресурс экспортирован из VMS. • Управление жизненным циклом
Блокировка VMS	Ресурс в VMS заблокирован. • Управление жизненным циклом
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
Аналитические приложения	• Просмотр • Соединение с кубом
Служба планирования обновления аутентификации	• Доставка • Выполнение
Стартовая панель BI в стиле Fiori	Просмотр
Службы BI Commentary	• Создание • Удаление • Просмотр • Изменение • Скрыть
Центральная служба управления	• Изменение аудита • Создание • Пользовательский уровень доступа изменен • Удаление • Доставка

Тип службы	Создаются типы событий
	• Вход в систему • Выход из системы • Изменение • Извлечение • Изменение прав • Инициирование
Центральная консоль управления	Просмотр
Служба планирования Crystal Reports	• Доставка • Запрос на ввод • Обновление • Выполнение • Сохранение
Служба кэша Crystal Reports	• Запрос на ввод • Обновление • Сохранение • Просмотр
Служба планирования Crystal Reports для Enterprise	• Доставка • Запрос на ввод • Обновление • Выполнение • Сохранение
Служба планирования Crystal Reports	• Доставка • Запрос на ввод • Обновление • Выполнение • Сохранение
Служба просмотра и изменения Crystal Reports	• Создание • Сохранение • Просмотр
Desktop Intelligence (клиент)	• Доставка • Запрос на ввод • Извлечение • Выполнение
Процесс планировщика Desktop Intelligence	• Доставка • Выполнение
Служба планирования доставки в места назначения	• Доставка • Выполнение
Служба событий	Инициирование

Тип службы	Создаются типы событий
Служба Information Engine	• Создание • Детализация за пределами области действия • Правка • Страница извлечена • Запрос на ввод • Обновление • Сохранение • Просмотр
Служба планирования LCM	Выполнение
Служба LCM	• Создание • Удаление • Конфигурация LCM • Изменение • Откат • Выполнение • Сохранение • Добавление VMS • Возврат VMS • Изъятие VMS • Удаление VMS • Экспорт VMS • Блокировка VMS • Извлечение VMS • Разблокирование VMS • Поиск
Live Office	• Запрос на ввод • Обновление
Служба многомерного анализа	• Соединение с кубом • Сеанс MDAS • Сохранение
OpenDocument	Просмотр
Служба планирования поиска по платформе	• Доставка • Выполнение
Служба поиска по платформе	Поиск
Служба планирования зонда	• Доставка • Выполнение
Служба планирования программ	• Доставка • Выполнение
Служба планирования публикаций	Выполнение

Тип службы	Создаются типы событий
Служба тиражирования	Выполнение
SAP BusinessObjects Design Studio версии 1.3 и выше	• Вход в систему • Выход из системы
Служба планирования запросов безопасности	• Выполнение • Доставка
Служба планирования импорта пользователей и групп	• Выполнение • Доставка
Служба планирования Visual Difference	Выполнение
Приложение Web Intelligence	• Создание • Детализация за пределами области действия • Правка • Изменение • Запрос на ввод • Обновление • Сохранение • Просмотр
Общая служба Web Intelligence	• Создание • Детализация за пределами области действия • Правка • Страница извлечена • Запрос на ввод • Обновление • Сохранение • Просмотр
Основная служба Web Intelligence	• Создание • Детализация за пределами области действия • Правка • Страница извлечена • Запрос на ввод • Обновление • Сохранение • Просмотр
Служба обработки Web Intelligence	• Создание • Детализация за пределами области действия • Правка • Страница извлечена • Запрос на ввод • Обновление • Сохранение

Тип службы	Создаются типы событий
	• Просмотр
Служба планирования и публикаций Web Intelligence	• Доставка • Выполнение

Свойства и сведения о событии

Каждое событие, записываемое платформой BI, включает набор свойств и сведений.

Свойства события всегда создаются с событием, однако, если информация неприменима к определенному событию, некоторые свойства могут не иметь значений. В ADS свойства события включены в таблицу, хранящую событие, что позволяет использовать их для сортирования или группирования событий при создании отчетов.

Сведения о событии содержат дополнительную информацию по событию, которая не включена в свойства события. Если сведения о событии нерелевантны определенному событию, данные сведения о событии не создаются. Существует набор общих сведений о событии, которые могут быть созданы для всех релевантных типов событий. Также существуют наборы дополнительных сведений о событии, которые создаются для событий определенного типа. Например, события для 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 объектов или папок) будут записаны на локальном языке аудитора CMS по умолчанию.

Связанные сведения

Auditing Data Store Tables [страница 1269]

24.3.1 Audit events and details

The following sections list all of the event types, followed by a description of any properties and event details that are unique to those events. At the beginning of the section is a list of the properties and details that are common to all event types.

> **Примечание**
>
> Some client programs do not have their own unique events, and rely on the common and platform events to capture relevant information about their operations.

Universal event Properties and Details

The following tables show what properties and event details are recorded for all events.

> **Примечание**
>
> The properties in this table are columns in the ADS_EVENT table in the Auditing Data Store.

Event Property	Description
Event_ID	A unique identifier for the event.
Client_Type_ID	Identifier for the type of application that performed the event
Service_Type_ID	Shows the ID of the type of service or application that triggered the event.
Start_Time	The start date and time when the event started (in GMT).
Duration	Duration of the event in milliseconds. Value may be zero (0) for certain events. For Example: with View event type, if the document gets loaded quickly, the value will be `0`.
Session_ID	ID of the session during which the event was triggered.
Event_Type_ID	Type of event (for example, 1002 for view).
Status_ID	Records if the action succeeds or fails ("0" = succeeded, "1" = failed). Some events will have additional status types, these are detailed with the descriptions of those events.
Object_ID	CUID of the object affected (if applicable). CUID of the alerting event for Trigger events. **Примечание** All objects not saved in the CMS repository will have an ID of 0. These objects could be documents that have not yet been saved to the CMS database, or are stored locally on a client machine for example. You will need to use the Object_Name property to differentiate these objects.
User_ID	CUID of the User that performed the event.
User_Name	The user-name of the user the performed the event.

Event Property	Description
Object_Name	Name of the affected object (if applicable). Name of the alerting event for Trigger events.
Object_Type_ID	CUID of object type (for example document, folder, and so on).
Object_Folder_Path	Full folder path to where the affected object is located in the CMS repository. For example, `Sales/North America/East Coast`
Folder_ID	The CUID of the folder where the object is stored.
Top_Folder_Name	Name of the top level folder the affected object is stored in. For example, if object is located in `Sales/North America/East Coast` then the value would be `Sales`.
Top_Folder_ID	The CUID of the top level folder where the affected object is located. For example, if object is located in `Sales/North America/East Coast` then the value would be the CUID of the folder `Sales`.
Cluster ID	The CUID of the CMS cluster that recorded the event.
Action_ID	A unique identifier that can be used to tie together a sequence of events initiated by a single user action.

> **Примечание**
>
> The properties in this table are columns in the ADS_EVENT_DETAIL_TYPE_STR table in the Auditing Data Store.

Event Detail	ID	Description
Error	1	Only recorded if the action fails; the text of any error messages that result from the attempt.
Element ID	2	Name of an object that resides in a container object (Live Office document or Dashboard for example).
Element Name	3	ID generated for an object that resides in a container object (Live Office document or Dashboard for example).
Element Type ID	5	The type of object in a container object that is being viewed or modified. Only generated if applicable.
Parent Document ID	12	• For a document instance: the CUID of the parent document. • For parent documents: its own CUID.
Universe ID	13	CUID of the Universe used by the document or object. An event detail will

Event Detail	ID	Description
		be generated for each Universe if more than one is used.
Universe Name	14	The name of the Universe used by the document/object. An event detail will be generated for each Universe if more than one is used.
User Group Name	15	The user group name that the user performing the action belongs to. If the user belongs to multiple groups. An event detail will be generated for each group.
User Group ID	16	The user group ID that the user performing the action belongs to. If the user belongs to multiple groups. An event detail will be generated for each group.

Common Events

The following event types are common to all SAP BusinessObjects servers and clients.

View

User viewed a document / object.

- Event Type ID: 1002

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.
Container ID	32	The CUID of the container object (a dashboard, for example) that the object resides in (if applicable).
Container Type	33	The application type of the container for the object (if applicable).

> **Примечание**
>
> If you are using a search service then during document indexing you may notice a large number of View events generated by the "System Account" user. This is caused by the search indexing service opening documents in order to build the search index.

Refresh

An object was refreshed from the database.

- Event Type ID: 1003

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event. **Примечание** For View on Demand Crystal Reports this will be set to 0.
Number of Rows	63	The number of records the database server returned. **Примечание** For View on Demand Crystal Reports this will be set to 0.
Query	25	Records the SQL query used to refresh the data (optional, set in CMC).
Universe Object Name	31	The name of the universe the document or object uses. An event detail will be generated for each universe accessed by the document or object.
Document Scope	36	Records information on the intended scope of the document from its publishing settings (for example: Country=USA, Role=Manager). Only applicable to publishing workflows.
Publication Instance ID	37	ID of this instance of the publication. Only applicable to publishing workflows.
Live Office Object Type	10701	Identifies the type of object that is being refreshed in a Live Office document (a Crystal report for example). This will only be generated for Live Office documents.

Prompt

A value was entered for a prompt.

- Event Type ID: 1004

Event Detail	ID	Description
Prompt name	26	The name assigned to the prompt ("Date" for example). A separate detail will be generated for each prompt in a document or object, and they will be grouped.
Prompt value	27	The value entered for a prompt. A separate detail will be generated for

Event Detail	ID	Description
		each value entered. These can be grouped together and related back to the prompt name.
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager).
Publication Instance ID	37	ID of this instance of the publication. Only applies to publishing workflows.
Name at Design Time	90	The name of the Dashboards document at the time it was designed. This is only generated for Dashboards refreshes, or a Dashboards or Live Office document that includes a prompt.
Live Office Object Type	10701	Identifies the type of object that is being refreshed in a Live Office document (a Crystal report for example). This will only be generated for Live Office documents where the embedded object includes a prompt.

Create

User created an object.

- Event Type ID: 1005

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.
Overwrite	21	Records if the document or object is new or overwrites an existing object (0=New document or object, 1=overwrite of existing document or object).
Refresh on Open	23	Records if the document or object is set to be automatically refreshed on open (0=No refresh, 1=Refresh on open). Only generated if applicable.
Description	24	Records any information in the document or object's description field.

Delete

User deleted an object.

- Event Type ID: 1006

Modify

User modified a file property or the file properties of an object.

- Event Type ID: 1007

Event Detail	ID	Description
Property Name	28	The name of the property that was modified. An event detail will be generated for each modified property.
Property Value	29	The new value for any modified property of the document or object. An event detail will be generated for each modified property.
Old Property Value	120	A user's old email address.
New Property Value	121	The same user's new email address.

Save

Saving or exporting a document or object locally, remotely, or to the CMS repository, in either its existing format or a different format.

- Event Type ID: 1008
- Statuses:
  - "0" indicates the object was successfully saved locally
  - "1" indicates the attempt failed
  - "2" indicates the object was successfully saved or exported to a repository
  - "3" indicates the object was successfully saved or exported to a new format

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that was saved or exported.
File Name	18	The full name the document or object was saved under. If the file is saved locally by a client application, the name will also include the file path.
Overwrite	21	Records if the document or object is new or overwrites an existing file. "0"=New document or object, "1"=overwrite of existing document or object.
Format	22	Specifies the format of the document saved/exported, displayed as the common three-letter file extension ("doc" for a Microsoft Word file, or "pdf" for an Adobe PDF file, for example).
Refresh on Open	23	Records if the document or object is set to be automatically refreshed on open ("0"=No refresh, "1"=Refresh on open). Only recorded if applicable.

Search

A search was conducted.

- Event Type ID: 1009

Event Detail	ID	Description
Keyword	19	The keywords of the conducted search.
Category	20	Category used in the search (if applicable).
Number of Rows	63	The number of rows returned by the search.

Edit

User edited the content of an object.

- Event Type ID: 1010

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.
Query	25	If the edit modifies an SQL query, records the new query. (This setting is optional and can be selected in the CMC Auditing page.)
Universe Object Name	31	The name of the universe the document or object uses. A separate detail will be generated for each universe accessed by the document or object.
Container ID	32	The CUID of the container (a dashboard for example) that uses the object (if applicable).
Container Type	34	The application type of the container for the object (if applicable).
Container Folder Path	64	Folder path for the container of the object (if applicable).

Run

A job was run.

- Event Type ID: 1011
- Statuses:
  - "0" indicates the job was successful
  - "1" indicates the job failed
  - "2" indicates the job failed but will be reattempted
  - "3" indicates the job was cancelled

Event Detail	ID	Description
Size	17	Size of the document (in bytes) that was run.

Event Detail	ID	Description
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager).

Deliver

An object was delivered.

- Event Type ID: 1012

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that was delivered.
Destination Type	35	The destination of the document or object instance. For example, email, FTP, unmanaged disk, inbox, or printer.
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager)
Publication Instance ID	37	ID of this instance of the document or object.
Domain	38	Records the SMTP server domain name for documents/objects distributed by email (if applicable).
Host Name	39	Records the name of the SMTP or FTP host for documents/objects distributed by email or FTP (if applicable).
Port	40	Records the SMTP or FTP server domain port for documents/objects distributed by email or FTP (if applicable).
From address	41	Records the sender's address for documents/objects distributed by email (if applicable).
To address	42	Records the recipient's address for documents/objects distributed by email (if applicable). Will also specify if the address is included in the To, CC, or BCC fields. An event detail will be generated for each intended recipient.
File Name	18	Records the file name of documents/objects distributed by email or FTP, or written directly to a disk that is not part of the Business Objects deployment.
Account Name	45	This records one of the following:

Event Detail	ID	Description
		• For *Inbox* delivered objects, a list of BusinessObjects user account names. • For *FTP* delivered objects, the FTP account name. • For *Unmanaged Disk* delivered objects, the login account used. • For *SMTP* delivered objects, the login account used for the SMTP server.
Printer Name	46	The name of the printer the document or object was delivered to (if applicable).
Number of copies	47	The number of copies of the document or object printed (if applicable).
Recipient Name	48	User name or names of the recipient or recipients of the document or object. An event detail will be generated for each intended recipient.
Alerting Event ID	92	The CUID of the Alerting event. This is generated only if the event was prompted by an alert.
Alerting Event Name	93	The name of the alerting event. This is generated only if the event was prompted by an alert.
Delivery Type	75	Indicates how the delivery was initiated: • "0" indicates scheduled • "1" indicates sent to a destination • "2" indicates published • "3" indicates an alert was triggered

Retrieve

An object is retrieved from the CMS.

- Event Type ID: 1013

Logon

A user logs on.

- Event Type ID: 1014
- Statuses:
  - "0" indicates a concurrent-user license logon was successful
  - "1" indicates a failed logon attempt
  - "2" indicates a named-user license logon was successful
  - "3" indicates a non-user (system) login was successful

- Event Type ID: 123
- Statuses:
  - "0" indicates a concurrent-user license logon was successful
  - "2" indicates a named-user license logon was successful

Event Detail	ID	Description
Concurrent User Count	50	The number of users on the system at the time the event was triggered.
Client hostname reported by client	51	Hostname of client as reported by client.
Client hostname resolved by server	52	Hostname of client as resolved by server. If the client hostname cannot be resolved, no value is recorded.
Client IP address reported by client	53	IP address of client as reported by the client.
Client IP address resolved by server	54	IP address of client as resolved by the server. If the client IP cannot be resolved, no value is recorded.
Authentication Type	122	Authentication type is valid for the vlaues secEnterprise, secLDAP, secWinAD, secSAPR3
User Type	123	Type of the user.
Session Count	125	Count of the session is recorded.
Tenant ID	126	The ID of the tenant is recorded.
Concurrent Tenant Session	127	The count of the concurrent session of the tenant is recorded.

Logout

A user logs off.

- Event Type ID: 1015

Event Detail	ID	Description
Concurrent User Count	50	The number of concurrent users on the system at the time the event was triggered.

Trigger

A file event is triggered.

- Event Type ID: 1016

Event Detail	ID	Description
File Name	18	The name of the file that was being monitored and triggered the event.

24.3.1.1 События платформы

Для платформы BI характерны следующие события.

Изменение прав

Право или права для объекта были изменены.

- Идентификатор типа события: 10003

Сведения о событии	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: `added right=Export; new value=Granted; scope=Current object; applicable object type=all object types`.
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: `removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types`.
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: `modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types`.
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

Сведения о событии	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: `added right=Export; new value=Granted; scope=Current object; applicable object type=all object types`
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: `removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types`.
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: `modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types`.
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

Сведения о событии	Идентификатор	Описание
Идентификатор типа события	58	Записывает идентификатор типа события аудита, которое было включено или отключено. Если одновременно включается или отключается несколько типов событий, сведения о событии 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).
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 каждых 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,DB Восстановить соединение=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 `*`.

Сведения о событии	Идентификатор	Описание
Интервал автоматического удаления	105	Для этих подробностей будут записываться изменения в поле *Удалить события старше, чем* на странице CMC аудита. Это определяет, сколько дней будут сохраняться данные аудита в ADS.

24.3.1.2 События для комментариев

Следующие права специфичны для **BI Commentary** на платформе Business Intelligence.

Добавление комментария

Это событие создается при добавлении нового комментария, при дублировании комментария и при массовом добавлении комментариев. При добавлении комментария записывается только идентификатор родительского документа. В случае дублирования или массового добавления комментариев записываются все сведения о событии, указанные в таблице ниже.

Идентификатор типа события: 11001

Сведения о событии	Идентификатор	Описание
Идентификатор родительского документа	12	Записывается идентификатор объекта.
Описание	24	Записывается любая дополнительная информация в событии.
Размер	17	Размер (в байтах) объекта, являющегося субъектом события.
Имя файла	18	Записывается имя файла объекта.

Вызов комментария

Это событие создается при просмотре комментария.

Идентификатор типа события: 11002

Сведения о событии	Идентификатор	Описание
Идентификатор родительского документа	12	Записывается идентификатор объекта.
Размер	17	Размер (в байтах) объекта, являющегося субъектом события.

Изменение комментария

Это событие создается при редактировании существующего комментария.

Идентификатор типа события: 11003

Сведения о событии	Идентификатор	Описание
Идентификатор родительского документа	12	Записывается идентификатор объекта.

Удаление комментария

Это событие создается при удалении существующего комментария.

Идентификатор типа события: 11004

Сведения о событии	Идентификатор	Описание
Идентификатор родительского документа	12	Записывается идентификатор объекта.

Скрытие комментария

Это событие создается при скрытии комментария.

Идентификатор типа события: 11005

Сведения о событии	Идентификатор	Описание
Идентификатор родительского документа	12	Записывается идентификатор объекта.

24.3.1.3 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

Сведения о событии	Идентификатор	Описание
Экземпляр задания	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 CMC).
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

Сведения о событии	Идентификатор	Описание
Имя отчета WebIntelligence	10220	Запись имени просматриваемого отчета WebIntelligence.
Тип вывода	10221	Формат вывода просматриваемого документа, например:

Сведения о событии	Идентификатор	Описание
		• `xml.ro` для WebIntelligence • `pdf` для Adobe Acrobat • `xls` для Microsoft Excel • `text/xml` в неизвестном случае
Номер страницы	10222	Запись номера просматриваемой страницы отчета WebIntelligence. NB: • "0", когда извлечение невозможно (например, PDF) • "-1" в случае ошибки

Статистика BW

> **Примечание**
>
> Эти события аудита отправляются непосредственно в SAP BW. Они перечислены ниже для ссылки как события Web Intelligence, но не сохраняются в хранилище данных аудита платформы BI. Эти события доступны с версии 4.2 SP03.

Параметр	Возможные значения	Описание

Длинное имя
`sap.sal.bics.postBWstatistics`
Короткое имя
`postBWstatistics`
Значение по умолчанию: `false`
	`true`
	`false`
		Активирует следующие элементы статистики BW:
		• 20100: извлекает элементы характеристики BEx
		• 20101: извлекает результаты запроса BEx
		• 20102: отправляет переменные BEx
		• 20103: открывает запрос BEx с использованием BICS API
		• 20104: синхронизирует с BEx
		• 20105: задает строку ввода переменной

24.3.1.4 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.

24.3.1.5 События консоли Диспетчера переноса объектов SAP BusinessObjects

Следующие события являются уникальными для компонента Диспетчер переноса объектов для SAP BusinessObjects.

Общие сведения Диспетчера переноса объектов SAP BusinessObjects

Для всех событий Диспетчера переноса объектов имеются следующие дополнительные сведения.

Сведения о событии	Идентификатор	Описание
Кластер элементов	6	CUID затронутых кластеров, если Диспетчер переноса объектов выполняет операцию для объектов, 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 Диспетчера переноса объектов SAP BusinessObjects

Конфигурация Диспетчера переноса объектов изменилась.

- Идентификатор типа события: 10900

Сведения о событии	Идентификатор	Описание
Конфигурация	100	Пользователь просматривает конфигурацию Диспетчера переноса объектов. Конфигурация отображается в виде разделяемых запятыми пар значений, например: настройки отката=включено, порт=900.
Конфигурация до	101	Если настройки Диспетчера переноса объектов для объекта изменены, записывает предыдущие настройки конфигурации. Использует такой же формат, что и конфигурация.
Конфигурация после	102	Если настройки Диспетчера переноса объектов для объекта изменены, записывает новые настройки конфигурации. Использует такой же формат, что и конфигурация.

Сведения о событии	Идентификатор	Описание
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 VMS

Ресурс добавлен в VMS.

- Идентификатор типа события: 10902

Сведения о событии	Идентификатор	Описание
Версия	104	Записывает номер версии документа в системе управления версиями.

Извлечение VMS

Ресурс извлекается из VMS.

- Идентификатор типа события: 10903

Сведения о событии	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

Сведения о событии	Идентификатор	Описание
Версия	104	Записывает номер версии документа в VMS.

Экспорт VMS

Ресурс экспортирован из VMS.

- Идентификатор типа события: 10906

Сведения о событии	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

Сведения о событии	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

Сведения о событии	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

Сведения о событии	Идентификатор	Описание
Версия	104	Записывает номер версии документа в системе управления версиями.

25 События

25.1 Общие сведения о событиях

События аналогичны флагам или контрольным точкам, которые предоставляют информацию о том, какие действия или события происходят на сервере. Планирование событий предоставляет дополнительные возможности управления запланированными объектами: можно настраивать события, чтобы объекты обрабатывались только после возникновения определенного события.

Ниже приведен список доступных объектов в CMC.

События Crystal Reports

События Crystal Reports запускают ожидающий события отчет только в том случае, если он уже запланирован и готов к выполнению. Событием Crystal Reports может стать появление нового файла, и запуск отчетов можно запланировать на основе таких событий.

Пользовательские события

Пользовательские события также называют событиями, запускаемыми вручную. Каждое пользовательское событие имеет два свойства: имя события и его описание. С помощью пользовательских событий можно инициировать отправку предупреждений в папку входящих BI и на адрес электронной почты пользователя. Пользовательские события также позволяют выбирать условия для планирования объектов на основе событий.

События мониторинга

События мониторинга — это создаваемые системой события, связанные с работоспособностью служб. Приложение мониторинга встроено в CMC и позволяет администраторам контролировать состояние системы. Самыми важными компонентами мониторинга являются наблюдения и зонды.

Наблюдения позволяют устанавливать в системе пороговые значения для более чем 250 метрик и уведомляют пользователя при их превышении.

> Пример
>
> Если в системе установлено наблюдение за дисковым пространством, потребляемым сервером репозитория выходных файлов (FRS), то при достижении указанного объема дискового пространства будет отправлено уведомление.

Системные события

Системные события бывают двух типов:

- **События на основе файлов**
  События на основе файлов возникают при размещении файла по определенному пути. Например, если файл расположен в одной из папок на сервере, то можно запланировать запуск отчета на основе пути к этому файлу. С точки зрения бизнеса можно рассмотреть загрузку необходимых для отчетов таблиц на ежемесячной, еженедельной или ежедневной основе. Размещение текстового файла по определенному пути после загрузки отчетов вызовет событие на основе файла.
- **События на основе расписания**
  События на основе расписания используются для последовательного запуска отчетов или объектов BI. Определение таких событий включает три состояния: "Успех", "Сбой" и "Успех или сбой". Это связано с тем, что статус выполняющегося объекта в любой момент времени может быть либо "Успех", либо "Сбой".

Уведомления пользователей

Уведомления пользователей применяются администраторами для информирования конечных пользователей BI, использующих стартовую панель BI, о важных событиях. Администраторы могут передавать отдельным пользователям критически важные сообщения, а также другую плановую информацию (например, о недоступности систем). Такие сообщения отображаются во всплывающем окне уведомлений на экране стартовой панели BI при входе пользователя в систему.

События BW

В системе BW *начальное событие BOE*, тип процесса в цепочке процессов BW, инициирует события BW для платформы BI. Каждое событие BW включает имя события и его описание. События BW используются для настройки графика на основе событий для отчетов, которые основаны на источнике данных BW. Система BW инициирует событие BW, когда в системе изменяются данные. С помощью событий BW также можно инициировать отправку предупреждений в папку входящих BI и на адрес электронной почты пользователя.

25.1.1 Уведомления пользователей

Функция отправки уведомлений позволяет администратору отправлять пользователям оповещения из CMC. С ее помощью администраторы могут передавать отдельным пользователям критически важные сообщения, а также другую информацию (например, о недоступности систем). Такие сообщения отображаются во всплывающем окне уведомлений в правом верхнем углу экрана стартовой панели BI при входе пользователя в систему.

25.1.1.1 Создание события уведомления

Событие уведомления – это подключаемый модуль с поддержкой планирования. При создании события уведомления администратор должен указать даты и время начала и окончания. Когда наступает время начала, заданное для уведомления, адаптивный сервер заданий, на котором осуществляется планирование, создает экземпляр планирования. Адаптивный сервер заданий затем отправляет предупреждение в папку входящих предупреждений на стартовой панели. Эти уведомления отображаются в правом верхнем углу экрана стартовой панели BI.

Чтобы создать событие уведомления, выполните следующие действия:

1. Войдите в CMC.
2. В раскрывающемся меню на главной странице CMC выберите *События*.
3. На панели *События* слева щелкните правой кнопкой мыши *Уведомления пользователей* и последовательно выберите *Создать* > *Новое уведомление*.

   Откроется окно *Новое уведомление*.
4. Чтобы запланировать уведомление, выполните следующие действия:
   a. Выберите часовой пояс в раскрывающемся меню *Часовой пояс*.
   b. Задайте *дату/время начала*.
   c. Задайте *дату/время окончания*.

   > ⓘ Примечание
   >
   > - Время *окончания* не может предшествовать времени *начала*.
   > - Разница между временем *начала* и временем *окончания* не может превышать 14 дней.
   > - Независимо от выбранного часового пояса время *начала* не может быть раньше времени сервера CMS. Если время *начала* предшествует времени севера CMS, то уведомление не будет активировано.

   d. В поле *Заголовок уведомления* введите заголовок уведомления.

   > ⓘ Примечание
   >
   > Длина текста в поле *Заголовок уведомления* не может превышать 256 символов.

   e. Введите описание уведомления в поле *Описание*.

   > ⓘ Примечание
   >
   > Длина текста в поле *Описание* не может превышать 1024 символа.

   > ⓘ Примечание
   >
   > Также можно настроить отправку уведомления на адрес электронной почты пользователя, установив флажок *Отправить это уведомление на адрес электронной почты пользователя*.
5. Нажмите кнопку *OK*.

Событие уведомления создано.

> **Примечание**
>
> На странице "Свойства уведомлений" время создания и изменения указываются по времени центрального сервера управления (CMS).
>
> Администратор может отключить автоматическое отображение всплывающих уведомлений в стартовой панели BI, изменив файл `BIlaunchpad.properties`, а также отключить опросы, изменив значение в поле `Notification.enabled` на `false`. Чтобы опросы уведомлений работали по умолчанию, необходимо включить свойство `pinger.enabled` в файле `global.properties`. Если опросы и средство проверки связи отключены, всплывающее уведомление отображается только при обновлении страницы, первом входе в систему или повторном входе в систему в момент, когда уведомление активно.
>
> Опрос выполняется каждые 3 минуты на стартовой панели BI.

25.1.1.2 Выбор получателей уведомления

Функция отправки уведомлений позволяет выбирать получателей для каждого создаваемого уведомления.

Чтобы выбрать получателей уведомления, выполните следующие действия:

1. Щелкните правой кнопкой мыши созданное уведомление и выберите в контекстном меню пункт *Управление подписчиками*.

   Откроется окно *Управление подписчиками*.
2. На панели *Список подписчиков* выберите *Добавить*.

   Появится всплывающее окно *Добавление подписчиков*.
3. Выберите пользователей или группы пользователей, которых требуется уведомить.
4. Выберите *Добавить подписки по умолчанию*.

   Всплывающее окно *Добавление подписчиков* исчезнет.
5. В окне *Управление подписчиками* выберите *Сохранить и закрыть*.

Получатели уведомления выбраны.

> **Примечание**
>
> - После срабатывания уведомления изменить список подписчиков невозможно.
> - Теперь можно отправлять уведомления пользователям OpenDocument.

25.1.1.3 Изменение события уведомления

Чтобы изменить событие уведомления, выполните следующие действия:

1. Войдите в CMC.

2. В раскрывающемся меню на главной странице CMC выберите *События*.
3. В области *События* слева выберите *Уведомления пользователей*.
4. Щелкните правой кнопкой мыши уведомление, которое требуется изменить, и выберите в контекстном меню команду *Изменить событие*.

   Откроется диалоговое окно *Изменение события*.
5. Измените необходимые параметры события уведомления.

   > **Примечание**
   >
   > Можно изменить следующие параметры события уведомления:
   > - Часовой пояс
   > - Дата/время начала
   > - Дата/время окончания
   > - Заголовок уведомления
   > - Описание
   > - Управление подписчиками
6. Выберите *OK*.

Событие уведомления изменено.

> **Примечание**
>
> При изменении события с помощью меню *Событя* > *Уведомления пользователей* > *Свойства* > уведомление не будет срабатывать, пока вы не нажмете кнопку *OK* на странице *Изменение события*.

26 Поиск по платформе

26.1 Описание поиска по платформе

Поиск по платформе позволяет выполнять поиск содержимого внутри репозитория платформы BI. Результаты поиска уточняются, группируются в категории и ранжируются с учетом значимости.

В этой версии платформы BI поиск по платформе имеет следующие функции:

- Поиск содержимого платформы BI.
- Выдача запроса о создании документа в случае, если найти существующий документ не удается.
- 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.

26.1.1 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.

Дополнительные сведения об интерфейсе API поиска по платформе см. в *справочнике по API Java платформы SAP BusinessObjects Business Intelligence*.

26.1.2 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.

Для получения дополнительных сведений о настройке расположения индекса поиска по платформе в кластеризованной среде см. SAP-ноту.

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.

26.2 Настройка поиска по платформе

26.2.1 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 или с помощью средства WDeploy. Этот файл копируется программой установки в каталог `<КАТАЛОГ_УСТАНОВКИ>\warfiles\OpenSearch`.

> **Примечание**
>
> Для обмена данными с поиском по платформе программы-клиенты должны поддерживать стандарты OpenSearch.

> **Примечание**
>
> При установке платформы BI по умолчанию устанавливается сервер приложений Tomcat.

26.2.1.1 Развертывание вручную

Чтобы развернуть OpenSearch в среде платформы BI, выполните следующие действия:

1. Перейдите в каталог `<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\`.
2. Скопируйте папку OpenSearch в `<УСТАНОВКИ>\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://<tomcathost>:<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.

26.2.1.2 Развертывание с помощью WDeploy

Для Windows команды описываются как `wdeploy.bat <parameters>`. Для UNIX команды описываются как `wdeploy.sh <parameters>`.

1. Обновите файл `config.<ApplicationServer>`, расположенный в папке `<InstallDir>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf` с обновленными параметрами сервера веб-приложений (например каталог установки, имя экземпляра, порт администратора, имя пользователя администратора и пароль администратора).
2. Измените параметры конфигурации в файле `<InstallDir>\SAP BusinessObjects Enterprise XI 4.0\warfiles\OpenSearch\WEB-INF\config.properties`:
   a. Для параметра `CMS` введите `<CMSName>:<Port>`.
   b. Для параметра `OpenDocURL` введите URL-адрес приложения OpenDocument.

      URL-адрес должен быть `http://<WebApplicationServerHost>:<ConnectorPort>/BOE/OpenDocument/opendoc/openDocument.jsp`.
   c. (Требуется для обратного прокси) для параметра прокси `Proxy.rpurl` введите имя обратного прокси-сервера.
   d. (Требуется для обратного прокси) для параметра прокси `Proxy.opendoc.rpurl` введите имя обратного прокси-сервера приложения OpenDocument.
3. Выполните команду развертывания `wdeploy.bat <WebApplicationServer> -Dapp_source_tree=<ParentFolderOpenSearchWebApp> -DAPP=OpenSearch deploy` из `<InstallDir>\SAP BusinessObjects Enterprise XI 4.0\wdeploy`.
   Например, с помощью следующей команды OpenSearch развертывается 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 веб-приложений.

26.2.2 Настройка обратного прокси

Для развертывания веб-приложений на сервере веб-приложений, расположенном за обратным прокси-сервером, необходимо настроить обратный прокси-сервер на сопоставление входящих URL-запросов с верным WAR-файлом.

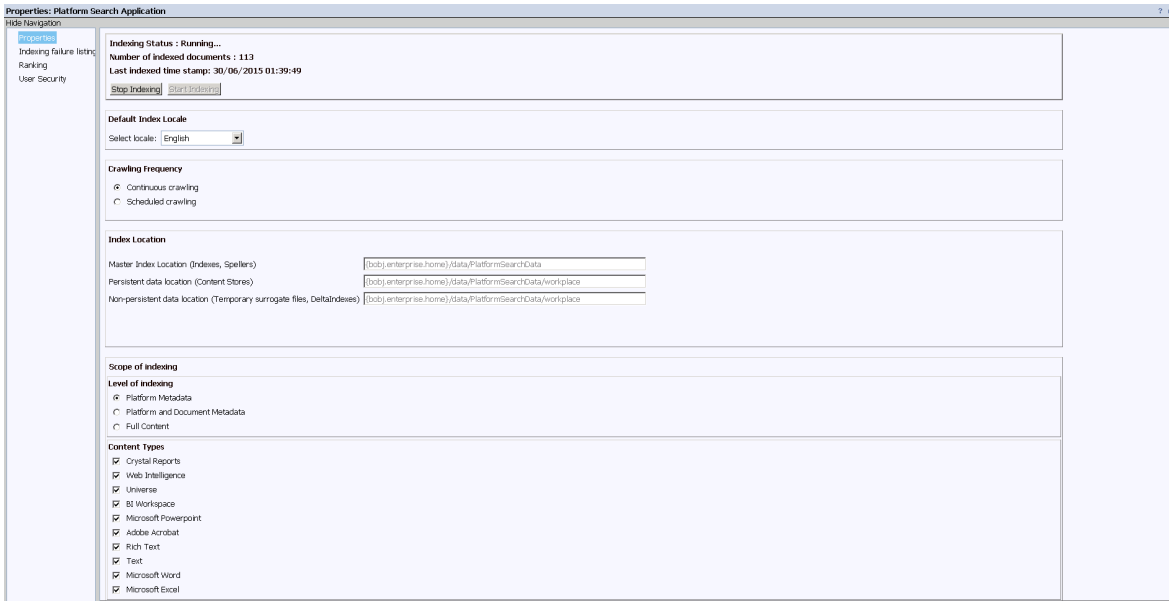
Для наглядного представления шагов конфигурации в качестве примера используется обратный прокси-сервер Apache 2.2. Настройка обратного прокси-сервера Apache 2.2 для системы OpenSearch

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 соединителя>/BOE/OpenDocument/`
   - `ProxyPass /RP/OpenSearchRP/ http://<хост Tomcat>:<порт соединителя>/OpenSearch/`
   - `ProxyPassReverseCookiePath /BOE /RP/BOE`
   - `ProxyPassReverseCookiePath /OpenSearchRP /RP/OpenSearchRP`
4. Перезапустите обратный прокси-сервер Apache 2.2.

26.2.3 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:

Параметр	Описание
Статистика поиска	Поиск по платформе предлагает следующие статистики поиска: • Состояние индексации — состояние процесса индексации • Число проиндексированных документов — число документов, для которых индексация выполнена. • Метка времени последней индексации — метка 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 CMC 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 CMC.

Параметр	Описание
Периодичность поиска	Индексацию всего репозитория платформы BI можно выполнить, используя следующие параметры: • 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 для индексирования документа. • Плановый обход: при выборе этого варианта индексация выполняется на основании расписания, задаваемого настройками "Расписание". Для получения дополнительных сведений о включении объектов в расписание см. раздел *Планирование объекта* справки по поиску по платформе в *Интерактивной справке CMC по платформе SAP BusinessObjects Business Intelligence*. **Примечание** • 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.

Параметр	Описание
Расположение индекса	Индексы хранятся в общих папках в следующих местах: • 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. 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. 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: 1. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Имя сервера>\ContentStores. 2. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Имя сервера 1>\ContentStores. • 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. **Примечание** • Расположение основного индекса должно быть общим каталогом. • 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.

Параметр	Описание
	> • В индексных файлах может содержаться личная и конфиденциальная информация, особенно когда вы выбираете индексацию содержимого документа. Доступ к общей папке необходимо разрешить только системному пользователю, и во избежание хищения данных общие папки следует хранить в зашифрованной среде.

Уровень индексации	Можно выполнить настройку содержимого поиска, задав уровень индексации следующим образом:
	• Метаданные платформы: индекс создается только для метаданных платформы, таких, как заголовки, ключевые слова и описания документов. Этот параметр выбран по умолчанию.
	• Метаданные платформы и документов: этот индекс включает метаданные платформы и метаданные 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:
	  • Фактическое содержимое документа
	  • Содержимое подсказок и списков значений
	  • Диаграммы, графики и метки
	> **Примечание**
	> Полное индексирование содержимого не поддерживается для документов Analysis Office и Lumira. Полное индексирование содержимого не поддерживается для документов Analysis Office и Lumira.
	> **Примечание**
	> При изменении уровня индексации процесс индексации инициализируется заново для всего репозитория платформы BI.

Параметр	Описание
Типы содержимого	Для индексирования могут быть заданы следующие типы содержимого. • Crystal Reports • Web Intelligence • Юниверс • Рабочее пространство BI • Analysis Office • Lumira • Microsoft PowerPoint • Adobe Acrobat • Формат RTF • Текст • Microsoft Word • Microsoft Excel Фильтр типа содержимого не применяется для индексирования метаданных платформы. Независимо от выбранных типов содержимого индексирование метаданных платформы выполняется для всех поддерживаемых типов объектов и результаты поиска на стартовой панели BI возвращают по ключевому слову все объекты, связанные с метаданными платформы. Фильтр типа содержимого релевантен для индексирования метаданных документов (автор документа, заголовок документа, нижний колонтитул документа и т. д.) и индексирования содержимого (графики, диаграммы, таблица с отчетом). В зависимости от выбранного уровня индексирования и типов содержимого поиск на платформе индексирует метаданные и содержимое документов для выбранных типов объектов из репозитория и только эти объекты отображаются в результатах поиска на стартовой панели BI при поиске по ключевому слову, связанному с метаданными и содержимым документа.
Перестроить индекс	Эта функция удаляет все существующие индексы и повторно индексирует весь репозиторий. 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. Чтобы отказаться от повторной индексации документов, снимите флажок *Перестроить индекс* перед нажатием кнопки *Начать индексацию*.

Параметр	Описание
Документы, исключенные из индексации	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. 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. 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*: • Права просмотра и редактирования категории • Непосредственное редактирование документа
Другая конфигурация – Пропуск экземпляра	По умолчанию экземпляры документов выбраны для индексирования. Это увеличивает размер индекса и повышает использование дискового пространства. Размер папки "Lucene Index Engine" в папке PlatformSearchData разрастается из-за индексирования огромного количества экземпляров в репозитории. При наличии в системе миллионов документов (или больше), многие из которых также имеют огромное число существующих экземпляров (наряду с плановым генерированием экземпляров с регулярным интервалом) размер папки "Lucene Index Engine" чрезмерно разрастается даже при установленном уровне индексирования "Метаданные платформы". Функция поиска по платформе "Пропуск экземпляра" позволяет включать и выключать индексирование экземпляров с помощью флажка в разделе "Другая конфигурация – Пропуск экземпляра" на странице свойств приложения поиска по платформев CMC. **Примечание** • В случае включения/отключения пропуска экземпляра необходимо перезапустить адаптивный сервер обработки поиска по платформе. Это изменение влияет на все уровни индексирования. • Если при изменении пропуска экземпляра требуется применить изменения ко всем существующим экземплярам (т. е. подлежащим выбору для индексирования), необходимо перестроить индекс.

Параметр	Описание
Исключенные из индексирования объекты	Параметр *Исключенные из индексирования объекты* позволяет исключить из индексирования некоторые объекты. Например, чтобы избежать перегрузки сервера приложений отчета, может потребоваться отключение функции поиска в некоторых объектах. Исключение конкретных объектов позволяет заблокировать доступ к ним при поиске по платформе. Важно отметить, что объект, проиндексированный до того, как был отнесен к данной группе, все еще может быть доступен для поиска. Чтобы объекты, отнесенные к категории *Исключенные из индексирования объекты*, были гарантированно недоступны для поиска, необходимо перестроить индекс. Список объектов, которые можно исключить из индексирования: • CrystalReport • Webi • LCMJob • Universe • Excel • PDF • PowerPoint • RTF • TXT • Word • AFDashboardPage • ObjectPackage • QaaWS • Profile • Event • Discussions • InformationDesigner • MDAnalysis • Publication • Agnostic • Analytics • Hyperlink • Program • pQuery • DSL.MetaDataFile • Shortcut • DataDiscoveryAlbum • AO.Workbook • VISI.Story

Параметр	Описание
	• VISI.Dataset • VISI.Lums • VISILums • User • UserGroup

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.

26.3 Работа с поиском по платформе

26.3.1 Индексация содержимого в репозитории CMS

Индексирование – это непрерывный процесс, включающий следующие последовательные задачи:

1. Обход: Обход – это механизм опроса репозитория CMS и идентификации объектов, которые были опубликованы, изменены или удалены. Возможны два типа обхода: планируемый и непрерывный. Для получения дополнительных сведений о непрерывном и планируемом обходе см. главу *Настройка свойств приложения* в разделе ссылок.
2. Извлечение: Извлечение – это механизм вызова средств извлечения, основанных на типе документа. У каждого типа документов, доступных в репозитории, есть свой собственный процесс извлечения. Новые типы документов можно сделать доступными для поиска, если определить новые подключаемые модули средств извлечения. Масштабируемость каждого из этих средств 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: 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. Хранилище содержимого: 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.

Связанные сведения

Настройка свойств приложения в CMC [страница 973]
Типы содержимого, доступного для поиска [страница 984]

26.3.2 Список сбоев индексации

Список сбоев индексации содержит список документов, которые не удалось индексировать. Поиск по платформе обеспечивает три попытки индексации документа. Если индексировать документ не удается, он указывается в списке случаев сбоя индексации.

Для просмотра списка ошибок индексирования выполните следующие действия:

1. Перейдите в область CMC "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.

26.3.3 Результаты поиска

26.3.3.1 Предварительный поиск

26.3.3.1.1 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 платформы BI.

Проанализировав структуру юниверсов и существующих отчетов в репозитории 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 Web Intelligence:

- Показатели в юниверсах, которые соответствуют словам в строке поиска.
  Если значение соответствует одному из критериев поиска, показатель будет использоваться в результирующем документе Web Intelligence.
- Имена измерений в юниверсах, которые соответствуют словам в строке поиска.
  Если имя измерения соответствует одному из критериев поиска, результирующий документ Web Intelligence проанализирует информацию этого измерения.
- Фильтры запроса могут использоваться при фокусировании на определенных данных документа. Эти фильтры запроса генерируются при анализе строки поиска.
  - Если имя условия юниверса соответствует критерию поиска, это условие используется в качестве фильтра.
  - Если в существующих документах 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.

26.3.3.1.2 Типы содержимого, доступного для поиска

Содержимое, опубликованное в платформе BI, доступно для поиска с помощью поиска по платформе. Ниже перечислены типы объектов и соответствующее им индексируемое содержимое:

Тип объекта	Индексируемое содержимое
Crystal Reports 2020	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, локально определенном 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 доступен для поиска.
LCMJob, ObjectPackage, запрос веб-службы (QaaWS), профиль, обсуждения, InformationDesigner, виджеты для платформы SAP BusinessObjects BI, MDAnalysis, публикации, аналитика и гиперссылка	Содержимое метаданных доступно для поиска.
События	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 источник вместе с событием. **Примечание** Поиск по платформе поддерживает события для Crystal Reports для Enterprise.

Тип объекта	Индексируемое содержимое

Рабочее пространство BI	• Заголовок, описание и содержимое индексируются для следующих модулей BIW:
	  • Текстовый модуль
	  • Модуль веб-страниц
	  • Модуль списка навигации
	  • Модуль средства просмотра
	• Индексируются заголовок и описание составного модуля.
	• Индексируется только заголовок модуля шаблона рабочего пространства.
	• Для модуля группы индексируются заголовок и метаданные входящих в него модулей.
	• Индексируются заголовок, описание и CUID модулей InfoObject в BIW.
	  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 заголовок и описание. При попытке поиска содержимого этого компонента CR ссылки на встроенный модуль не возвращаются.
	• Если в BIW присутствует несколько родительских и дочерних вкладок, также индексируются их заголовки и содержимое.

CR Next Gen	Заголовок, описание, формула выбора, сохраненные данные, текстовые поля любого раздела, значения параметров и подотчеты. Не поддерживаются следующие объекты в отчетах CR Next Gen: • Отчет в виде кросс-таблицы • Извлечение данных диаграммы • Извлечение изображений и связанных метаданных • Встроенные OLE-объекты (например, встроенный в компонент CR документ Word) Кроме того, постраничное считывание данных из отчета CR Next Gen невозможно.

Тип объекта	Индексируемое содержимое
Юниверс	Содержимое данных доступно для поиска. **Примечание** По умолчанию возможность индексации юниверсов включена. Если запросы, используемые поиском по платформе для индексации содержимого юниверса, выполняются слишком долго и влияют на производительность сервера БД, то рекомендуется отключить параметр индексации юниверсов в Central Management Console (CMC). Пример запроса, используемого при выполнении поиска по платформе при индексации содержимого юниверса: `Select distinct SampleColumnName from SampleTableName LIMIT 1000`. Выполните следующие шаги, чтобы отключить индексацию юниверсов: 1. Выполните вход в 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*.
Документ Lumira	Только содержимое метаданных доступно для поиска.
Документ Analysis Office	Только содержимое метаданных доступно для поиска.

Примечание

Максимальный поддерживаемый размер документов Agnostic (MS Office 2003 и 2007, а также документы PDF) составляет 15 МБ.

26.3.3.2 Поиск

Когда пользователь производит поиск по ключевому слову в стартовой панели BI или любом другом приложении, использующем SDK Platform Search, проверяется наличие условий поиска в основном индексе. В поисковой системе отображаются только те документы, на которые у пользователя есть права доступа.

> **Примечание**
>
> Если поиск выполняется в CMC в среде с большой базой данных CMS, поиск может завершиться неудачно. Для получения дополнительных сведений см. SAP-ноту 2156647 Поиск в CMC осуществляется медленно или не возвращает результаты.

26.3.3.3 Заключительный поиск

26.3.3.3.1 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 выводятся динамически на основе документов, соответствующих поисковому запросу, и сортируются по количеству документов.

Документы группируются по следующим общим фасетам или категориям:

- Персональные или общие (например, HR, корпоративные и финансовые): на основе категорий документов платформы BI.
- Тип документа: на основе типа документа, например Web Intelligence, Crystal Reports, Microsoft Word (2003 и 2007) и Microsoft Excel (2003 и 2007).
- Юниверс и соединения: на основе источника содержимого.
- Дата: дата последнего обновления: (год, квартал и месяц).
- Время: время последнего обновления, например последние 24 часа или прошлая неделя.
- Автор: имя пользователя, создавшего документ.

> **Примечание**
>
> Если выполнить поиск содержимого в стартовой панели BI, работая на иврите или арабском языке, результаты поиска не будут отображать фасеты.

26.3.3.3.2 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 этих категорий можно настроить в CMC.

26.3.3.3.2.1 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 CMC *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 потребуется повторно создать индекс. Дополнительные сведения см. в разделе о повторном создании индекса Настройка свойств приложения в CMC [страница 973].

26.3.3.3.3 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 CMC *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, установленным как языковой стандарт продукта клиента. Поиск по платформе Platform Search придает больше веса языковому стандарту продукта клиента при получении результатов поиска. Вес настраивается в CMC.

26.3.3.3.4 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 CMC *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

26.4 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, SAP 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 на платформу BI.

26.4.1 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*.

26.4.2 Импорт роли пользователя на платформу BI

Чтобы импортировать роль пользователя на платформу BI, выполните следующие действия:

> **Примечание**
>
> Администратор должен располагать подробными данными пользователя, сведениями по системе, информацией о хосте приложения и учетными данными пользователя.

1. Перейдите в область CMC *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 CMC пункт меню *Управление* > *Безопасность пользователя*, чтобы назначить соответствующие права пользователя.

26.5 Поиск из SAP 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.

26.6 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 и несколько стандартных элементов сведений события, например sessionCuid и userCuid, которые поддерживаются любым аудитом в любом модуле платформы BI.

Работа аудита в поиске по платформе поясняется далее на примере.

При поиске по ключевому слову, такому как "Продажи", общее число результатов может быть равно 5. В этом случае аудит применяется к следующим событиям:

- 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

26.7 Устранение неполадок

26.7.1 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.

26.7.2 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 отметка времени документа в репозитории платформы BI, что инициирует повторную индексацию документа.

Дополнительные сведения о документе, индексирование которого завершилось неудачно, см. в разделе *Список случаев сбоев индексации* в списке связанных тем ниже.

- Проверьте журналы трассировки адаптивного сервера обработки, содержащие данные о сбое индексирования.
  1. Перейдите в каталог `<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\logging\`, который 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 Crystal Reports 2020. 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*.

Приложение SAP NetWeaver Enterprise Search не может получить результаты из репозитория платформы BI

- 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*.

Связанные сведения

Список сбоев индексации [страница 982]
Настройка свойств приложения в CMC [страница 973]
Типы содержимого, доступного для поиска [страница 984]

27 Интеграция

27.1 Интеграция

Приложение для интеграции – 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.

Интеграция позволяет создавать отдельные модели безопасности и жизненные циклы, определять различное время тестирования и развертывания, а также иметь разных владельцев организации и администраторов. 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
Представления 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, Word, TXT, RTF и Shockwave	

Категория	Типы объектов, которые можно тиражировать	Дополнительные примечания
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 выполнят 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.

27.2 Термины для функции интеграции

В следующем списке терминов представлены слова и фразы, которые относятся к функции интеграции и могут облегчить его использование.

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 безопасности, жизненный цикл, сроки тестирования и развертывания, а также отдельные владельцы организации и администраторы.

Сайт-адресат	Система платформы BI, извлекающая реплицированное содержимое платформы BI с исходного сайта.
Локальный	Локальная система, к которой подключен пользователь или администратор. Например, администратор сайта-адресата считается «локальным» на сайте-адресате.
Выполняемые локально завершенные экземпляры	Экземпляры, обрабатываемые на сайте-адресате и передаваемые обратно на сайт-источник.
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.
Однонаправленное тиражирование	Объекты тиражируются только в одном направлении: с сайта-источника на сайт-адресат. Любые обновления на сайте-адресате остаются на сайте-адресате.
Сайт-источник	Система платформы BI, из которой поступает содержимое.
Удаленный	Система, которая не является локальной для пользователя. Например, сайт-источник считается «удаленным» для пользователей и администраторов сайта-адресата.
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.
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.
Тиражирование	Процесс копирования содержимого из одной системы платформы BI в другую.
Задание тиражирования	Объект, в котором содержится информация о планировании содержимого, содержимом, подлежащем тиражированию, и любых специальных условиях, которые должны выполняться при тиражировании содержимого.
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.
Объект тиражирования	Объект, тиражируемый с сайта-источника на сайт-адресат. Все тиражированные объекты на сайте-адресате будут помечены значком тиражирования. При наличии конфликта объекты будут помечены значком конфликта.
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 содержатся

	подмножество списка тиражирования, если объекты изменяются нечасто по сравнению с планированием задания тиражирования. Пакет тиражирования выполняется как файл BIAR (программный ресурс BI).
Обновление тиражирования	Все объекты в списке тиражирования обновляются вне зависимости от последней измененной версии.
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.

27.3 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.

27.3.1 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.	• Права «просмотра» и «тиражирования» всех тиражируемых объектов

Действие	Описание	Необходимые права
	ⓘ Примечание Права «просмотра» и «тиражирования» требуются для всех тиражируемых объектов, включая объекты, которые тиражируются автоматически путем вычислений зависимостей.	• Право «просмотра» списка тиражирования
Двунаправленное тиражирование	Выполнение тиражирования с сайта-источника на сайт-адресат и с сайта-адресата на сайт-источник.	• 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.	• Право «планирования» для всех объектов, планируемых удаленно

Связанные сведения

Права, необходимые на сайте-адресате [страница 1000]

27.3.2 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.	• Права «просмотра», «добавления»,« правки» и«изменения» для всех объектов

Действие	Описание	Необходимые права
		• 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.	• Права «просмотра», «добавления», «редактирования» и «изменения прав» во всех папках верхнего уровня и объектах по умолчанию.

Связанные сведения

Права, необходимые на сайте-источнике [страница 999]

27.3.3 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.	• Учетная запись, под которой выполняется задание тиражирования, требует наличия прав «удаления» для всех объектов, которые могут быть удалены.
Отключение очистки для определенных объектов	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.	• Запретите права «удаления» пользовательской учетной записи, под которой выполняется задание тиражирования, для объектов, которые необходимо сохранить.

Действие	Описание	Необходимые права
	Пример. Может потребоваться сохранение тиражированного юниверса, в котором пользователи на сайте-адресате создают собственные локальные отчеты, если юниверс удален с сайта-источника.	
Двунаправленное тиражирование при отсутствии изменений на исходном сайте	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. **ⓘ 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.	• Запретите права «изменения» пользовательской учетной записи, используемой для подключения в объекте удаленного соединения.

27.3.4 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.

27.3.5 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.

27.4 Параметры типов и режимов тиражирования

В зависимости от выбранных типа и режима тиражирования можно создавать один из четырех видов заданий тиражирования:

- Однонаправленное тиражирование,
- Двунаправленное тиражирование
- Обновлять из источника
- Обновлять из адресата.

27.4.1 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

27.4.2 Двунаправленное тиражирование

При двунаправленном тиражирование 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 двунаправленного тиражирования.

При наличии нескольких платформ BI, в которых содержимое создается, изменяется, администрируется и используется в обоих местоположениях, самым эффективным вариантом является двунаправленное тиражирование. Оно также позволяет синхронизировать системы.

Для создания двунаправленного тиражирования выберите следующие параметры:

- Тип тиражирования = Двунаправленное тиражирование
- Режим тиражирования = Обычное тиражирование

Связанные сведения

Удаленное планирование и экземпляры, выполняемые локально [страница 1030]

27.4.3 "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.

> ⓘ Примечание
>
> 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.

27.5 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 удается 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.

> ⓘ Примечание
>
> 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 CMC *Аутентификация*, дважды щелкните *Windows AD* или *LDAP* и щелкните *Обновить*.

> ⓘ Примечание
>
> Будьте осторожны при тиражировании сторонних групп. При добавлении новых пользователей в группу на сервере каталогов они получат 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 CMC, учетная запись пользователя создается на обоих сайтах. Учетным записям будут назначены различные идентификаторы, и функция интеграции не сможет правильно выполнить тиражирование.
>
> Важно создать учетную запись на одном сайте, а затем тиражировать ее на другой сайт.

27.6 Тиражирование юниверсов и соединений юниверсов

При использовании модуля "Интеграция" для тиражирования юниверсов между развертываниями платформы BI 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».

27.7 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 CMC.

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, Word, TXT, RTF, Shockwave
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.

- Представления Business View
- Бизнес-элементы
- Основания данных
- Соединения данных
- Список значений
- Переопределения юниверсов

27.7.1 Создание списков тиражирования

Списки тиражирования располагаются в области "Списки тиражирования" консоли CMC. Для упорядочения списков тиражирования можно создавать папки и вложенные папки.

27.7.1.1 Создание папки списка тиражирования

1. Перейдите в область *Списки тиражирования* консоли CMC.
2. Выберите *Списки тиражирования*.
3. Выберите команду *Управление* > *Создать* > *Папка*.
   Открывается диалоговое окно *Создать папку*.
4. Введите имя папки и нажмите кнопку *OK*.
   После этого в данной папке можно создавать списки тиражирования.

27.7.1.2 Создание списка тиражирования

1. Перейдите в область *Списки тиражирования* консоли CMC.
2. Выберите папку, в которой необходимо сохранить новый список тиражирования.
3. Щелкните *Управление* > *Создать* > *Новый список тиражирования*.
   Откроется 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.

Параметры объекта зависимости	Определение
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.
Включить папки "Входящие" выбранных пользователей	Тиражирует папку "Входящие" выбранного пользователя и ее содержимое.
Включить группы пользователей для выбранных юниверсов	Тиражирует группы пользователей, связанные с переопределениями юниверса.
Включить уровня 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 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 *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. Щелкните *Сохранить и закрыть*.

27.7.2 Изменение списков тиражирования

После создания списка тиражирования можно изменить его свойства или объекты.

27.7.2.1 Изменение свойств списка тиражирования

1. Перейдите в область *Списки тиражирования* консоли CMC.
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*.

Связанные сведения

Создание списков тиражирования [страница 1010]

27.7.2.2 Изменение объектов в списке тиражирования

1. Перейдите в область *Списки тиражирования* консоли CMC.
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*.

Связанные сведения

Создание списков тиражирования [страница 1010]

27.8 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 CMC.

27.8.1 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.

27.8.1.1 Создание папки удаленных соединений

1. Перейдите к области *Интеграция* консоли CMC.
2. Выберите *Удаленные соединения*.
3. Выберите команду *Управление* > *Создать* > *Папка*.
   Открывается диалоговое окно *Создать папку*.
4. Введите имя папки и нажмите кнопку *OK*.
   После этого в данной папке можно создавать удаленные соединения.

27.8.1.2 Создание удаленного соединения

Чтобы подключиться к удаленному развертыванию платформы BI, необходимо создать удаленное соединение в функции интеграции.

1. Перейдите к области *Интеграция* консоли CMC.
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
Заголовок	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 модуля "Интеграция" в платформе BI, в которой они являются сайтом-источником или сайтом-адресатом, а также в другом развертывании. Используйте следующий формат: **`http://<имя_компьютера_сервера_приложений>:<порт>/dswsbobje`**. Пример: **`http://<mymachine.mydomain.com>:<8080>/dswsbobje`**
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: **`имя_сервера_CMS:порт`** Пример: **`<mymachine>:6400`** **Примечание** Если используется порт по умолчанию 6400, номер порта можно не указывать.
Имя пользователя	Имя пользователя, которое будет использоваться для подключения к сайту-источнику. **Примечание** Убедитесь, что для используемой учетной записи настроены права на просмотр списка тиражирования в системе на сайте-источнике.
Пароль	Пароль учетной записи пользователя, используемой для подключения к сайту-источнику.
Аутентификация	Тип аутентификации учетной записи, используемой для подключения к сайту-источнику. Доступные параметры: Enterprise, AD и LDAP.
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.

Поле	Описание
Ограничить число объектов очистки до	Число объектов, очистка которых выполняется заданием тиражирования. (Не обязательно)

5. Нажмите кнопку *OK*.

27.8.2 Изменение удаленных соединений

После создания удаленного соединения можно изменить его свойства и параметры безопасности.

Изменение удаленного соединения:

1. Перейдите к области *Интеграция* консоли CMC.
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*.

27.9 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 CMC.

27.9.1 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.

27.9.1.1 Создание задания тиражирования

1. Перейдите к области *Интеграция* консоли CMC.
2. Выберите *Удаленные соединения*.
3. Выберите *Удаленное соединение*, в котором будет содержаться новое задание тиражирования.

   > ⚠ Предупреждение
   >
   > Сервер CMC 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.

Параметр	Описание
Включить очистку объектов для места назначения	Принудительное удаление заданием тиражирования всех тиражированных объектов на сайте-адресате, если исходный объект был удален с сайта-источника. ⓘ Примечание При очистке объектов не будут удаляться объекты, тиражированные с использованием зависимостей, или объектов, выбранных в списке тиражирования.
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

Параметр	Описание
	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.
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 *OK*.

27.9.2 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.

27.9.2.1 Планирование задания тиражирования

1. Перейдите к области *Интеграция* консоли CMC.
2. Выберите *задание тиражирования*, которое необходимо запланировать.
3. Выберите *Действия* > *Расписания*.
4. Выберите необходимые параметры планирования.

27.9.3 Изменение заданий тиражирования

После создания задания тиражирования в функции интеграции можно изменить его свойства.

27.9.3.1 Изменение задания тиражирования

1. Перейдите к области *Интеграция* консоли CMC.
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.

27.9.4 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 CMC.
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:

   - В ОС Windows: `<каталог_установки>\SAP BusinessObjects XI 4.0\logging`
   - В ОС Unix: `<каталог_установки>/sap_bobj/logging`

27.10 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.

27.10.1 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.

27.10.2 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.

27.10.3 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.

Связанные сведения

Ограничения очистки объектов [страница 1020]

27.11 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.

27.11.1 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 CMC. Конфликтующие объекты группируются на основе удаленного соединения с сайтом-источником. Для получения доступа к этому списку в области интеграции консоли CMC 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 завершении выполнения задания тиражирования, использующего удаленное соединение. В нем содержатся все конфликтующие объекты для всех заданий тиражирования, в которых используется данное удаленное соединение.

> ⓘ Примечание
>
> Любой пользователь, который имеет доступ к консоли CMC 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 A 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.

27.11.2 Разрешение конфликта двунаправленного тиражирования

При возникновении конфликта двунаправленного тиражирования предусмотрены три варианта обнаружения конфликта:

- Сайт-источник имеет приоритет
- Сайт-адресат имеет приоритет
- Без автоматического разрешения 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.

Без автоматического разрешения 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.

> **Примечание**
>
> 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 CMC 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 CMC. Конфликтующие объекты группируются на основе удаленного соединения с сайтом-источником. Для получения доступа к этим спискам выберите *CMC* > *Интеграция* > *Ошибки тиражирования* > *Удаленное соединение*.

> **Примечание**
>
> Этот список обновляется после завершении 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 помечены значком тиражирования. При наличии конфликта объекты будут помечены значком конфликта.

Пример

Михаил изменяет отчет A 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.

> **Примечание**
>
> Любой пользователь, который имеет доступ к консоли CMC 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 CMC. Конфликтующие объекты группируются на основе удаленного соединения с сайтом-источником. Для получения доступа к этим спискам выберите *CMC* > *Интеграция* > *Ошибки тиражирования* > *Удаленное соединение*.

> **Примечание**
>
> Этот список обновляется после завершении 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 помечены значком тиражирования. При наличии конфликта объекты будут помечены 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 на сайте-адресате задайте для автоматического разрешения конфликтов значение «Сайт-адресат имеет приоритет», а для типа тиражирования – значение «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.

27.12 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.

27.12.1 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>\dswsbobje\Web-INF\classes
```

Например:

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\dswsbobje\WEB-INF\classes
```

Для активации переменной сеанса введите:

```
session.timeout = x
```

Где «x »- необходимое время, «x» измеряется в секундах. Если значение не указано, по умолчанию используется 1200 секунд или 20 минут.

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*.

27.12.2 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*.

27.12.3 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\dswsbobje\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*.

27.13 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.

27.13.1 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 экземпляр на сайте-адресате является выполненным.

> **Примечание**
>
> Задание тиражирования должно выполняться дважды для возвращения одного выполненного экземпляра.

Пример

1. Антон составляет расписание отчета A для удаленного планирования.
2. Отчет A создан на сайте-адресате и переводится в состояние ожидания.
3. Выполняется задание тиражирования A. 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 A выполняется повторно. Когда задание выполняет тиражирование содержимого с сайта-источника на сайт-адресат, выбирается выполненный экземпляр отчета A 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.

Связанные сведения

Управление правами безопасности [страница 999]

27.13.2 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.

27.13.3 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 тиражирую 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.

Связанные сведения

Управление правами безопасности [страница 999]

27.14 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.

27.14.1 Импорт тиражированного содержимого

Если для импорта содержимого из одной платформы BI в другую используется LifeCycle Manager, импорт данных, относящихся к тиражированию и связанных с импортируемыми тиражированными объектами, не выполняется. Это означает, что после импорта поведение объектов аналогично их поведению до тиражирования. Этот пример относится к тиражированным объектам на сайте-адресате, его описание приводится в следующем сценарии.

Пример

Платформа BI A – это сайт-адресат в процессе интеграции. Отчет A, тиражированный отчет в системе A, импортируется из системы A в систему Б платформы BI с помощью LifeCycle Manager.

Результат. После копирования отчета A в систему Б платформы BI в нем не содержатся тиражированные данные. Отчет A больше не отмечен значком тиражирования. Если объект находился в состоянии конфликта в системе A платформы BI, состояние конфликта будет отсутствовать в системе Б. Фактически объект воспринимается как объект, созданный в системе Б.

> ⓘ Примечание
>
> Идентификатор CUID может различаться в зависимости от параметров импорта, настроенных в LifeCycle Manager.

27.14.2 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 A был создан в системе A платформы BI. В системе X функция интеграции использовалась для тиражирования отчета A из системы A в систему X. Затем LifeCycle Manager использовался для импорта отчета A из системы X в систему Y.

План. В системе Y необходимо настроить функцию интеграции для использования в системе A и сохранить отчет A в качестве части задания тиражирования. Система Y является адресатом, а система A – источником.

Действия. Во время импорта отчета A из системы X в систему Y необходимо сохранить идентификатор CUID отчета A. Кроме того, при выполнении первого задания тиражирования будет предпринята попытка тиражирования отчета A. 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 A будет выполнено из системы A в систему Y, и не будет необходимости использования LifeCycle Manager для импорта объекта из системы X в систему Y.

27.14.3 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.

27.14.4 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, информация о тиражировании в копии будет отсутствовать.

27.15 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. Большие задания тиражирования могут замедлять работу поставщика веб-служб и быть причиной увеличения времени отклика поставщика на запросы других обслуживаемых им веб-служб и 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).

> ⓘ Примечание
>
> 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 "$BOBJEDIR"/tomcat ]; then
 # set the JAVA_OPTS for Tomcat
 JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120
-Djava.awt.headless=true"
 if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" =
"SunOS" -o "$SOFTWARE" = "Linux" ];
then
 JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxMetaspaceSize=256m"
 fi
 export JAVA_OPTS
```

```
# fi
```

> ⓘ Примечание
>
> В BI 4.2 с пакетом поддержки 5 можно использовать параметр MaxMetaspaceSize для определения размера памяти Metaspace, а не параметр MaxPermSize.
>
> - При обновлении более ранних версий, чем BI 4.2 SP5, на BI 4.2 SP5 необходимо вручную изменить этот параметр для всех существующих серверов.
> - Если выполняется новая установка BI 4.2 с пакетом поддержки 5, параметр заменяется по умолчанию.

3. Увеличьте значение параметра `-Xmx1024m` до необходимого размера.

Пример

Чтобы увеличить объем памяти до 2 ГБ, введите: `-Xmx2048m`

> → Совет
>
> Для получения сведений об увеличении объема памяти на других серверах Java-приложений см. документацию о сервере Java-приложений.

3) Уменьшение размера создаваемых файлов BIAR.

В модуле "Интеграция" веб-службы используются для тиражирования содержимого с сайта-источника на сайт-адресат. Для повышения эффективности переноса объекты группируются и сжимаются в файлы BIAR.

При тиражировании большого числа объектов настройте на сервере Java-приложений создание файлов BIAR меньшего размера. В модуле "Интеграция" выполняются упаковывание и сжатие объектов в несколько файлов BIAR меньшего размера, поэтому число объектов, которые необходимо тиражировать, будет неограниченным.

Для уменьшения размера создаваемых файлов BIAR добавьте следующие параметры Java на сервере Java-приложений:

```
Dbobj.biar.suggestSplit
and
Dbobj.biar.forceSplit
```

Параметр `bobj.biar.suggestSplit`, в котором предлагается подходящий размер файла BIAR, который по возможности будет учитываться. Предлагаемое новое значение равно 90 МБ.

Параметр `bobj.biar.forceSplit` позволяет принудительно остановить создание файла BIAR по достижении заданного размера. Предлагаемое новое значение равно 100 МБ.

> ⓘ Примечание
>
> Изменять настройки размера файла BIAR по умолчанию следует только в том случае, если на сервере приложений недостаточно памяти и дальнейшее увеличение максимального размера кучи невозможно.

Для сервера Tomcat в ОС Windows:

1. Чтобы открыть средство *Конфигурация Tomcat*, выберите *Пуск* > *Программы* > *Tomcat* > *Конфигурация Tomcat* >.
2. Выберите *Java*.
3. В поле *Параметры Java* в конец добавьте следующие строки:

```
                    -Dbobj.biar.suggestSplit=90
                    -Dbobj.biar.forceSplit=100
```

Для сервера Tomcat в системе Unix/Linux:

1. Откройте файл env.sh в необходимом текстовом редакторе. Файл находится в каталоге `<Каталог_установки_BOE>/setup/`
2. Найдите следующие строки:

```
 # if [ -d "$BOBJEDIR"/tomcat ]; then
# set the JAVA_OPTS for tomcat
JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120
-Djava.awt.headless=true"
if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" = "SunOS" -o "$SOFTWARE" = "Linux" ];
then
JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m"
 fi
export JAVA_OPTS
 # fi
```

Добавьте необходимые параметры размера файлов BIAR.

Пример: `JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m` **-Dbobj.biar.suggestSplit=90 -Dbobj.biar.forceSplit=100"**

Для добавления системных свойств на других серверах Java-приложений см. документацию.

4) Увеличьте время ожидания для сокета.

Адаптивный сервер заданий предназначен для выполнения заданий тиражирования. Во время выполнения задания тиражирования настраиваемый сервер заданий устанавливает соединение с сайтом-источником. При получении больших объемов данных с исходного сайта важно, чтобы на сокете, который используется адаптивным сервером заданий для получения данных, не истекло время ожидания.

По умолчанию используется значение 90 минут. При необходимости можно увеличить время ожидания для сокета.

Увеличение времени ожидания для сокета на адаптивном сервере заданий:

1. Откройте Центральную консоль управления (CMC)
2. Перейдите к разделу *Сервер* и выберите *Адаптивный сервер заданий*.
3. Нажмите *Свойства*.
4. Добавьте «параметры командной строки» в конец следующей строки:
   - **Windows:** `-javaArgs Xmx1000m,Xincgc,server,Dbobj.federation.WSTimeout=<timeout in minutes>`
   - **Unix:** `-javaArgs Xmx512m,Dbobj.federation.WSTimeout=<timeout in minutes>`

Связанные сведения

Устранение неисправностей: сообщения об ошибках [страница 1041]
Использование веб-служб в функции интеграции [страница 1028]
Текущие ограничения выпуска [страница 1040]

27.15.1 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.

Связанные сведения

Управление очисткой объектов [страница 1019]

27.15.2 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_CUID в объекте с номером 1285) является недопустимым GUID`.

Эта ошибка означает, что выполняется тиражирование объекта, родительский элемент которого не тиражирован и еще не существует на сайте-адресате. Например, объект тиражируется без папки, в которой он содержится. Тиражирование родительского объекта невозможно, поскольку для учетной записи, под которой тиражируются объекты, не настроены подходящие права в родительском объекте.

2) Crystal Reports не отображают данные на сайте-источнике

Эта ошибка может возникнуть, если в отчете Crystal используется объект Business View, бизнес-элемент, основание данных, соединение для передачи данных или список значений (LOV), которые были изначально созданы на сайте-адресате, а затем тиражированы на сайт-источник.

3) Переопределения юниверса применяются неправильно

Эта ошибка может возникнуть, если в отчете используется юниверс, в котором содержится переопределение юниверса, созданное на сайте-адресате и тиражированное на сайт-источник.

4) Приложению Java не хватает памяти

Пример ошибки: `java.lang.OutOfMemoryError`.

Ошибка может появиться, если во время обработки задания тиражирования на сервере Java-приложений обнаружено недостаточно памяти. Возможно, задание тиражирования является слишком большим, или на сервере Java-приложений недостаточно памяти.

Увеличьте доступную память на сервере Java-приложений путем перемещения веб-служб 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:MaxMetaspaceSize=256m"`.

   > ⓘ Примечание
   >
   > В BI 4.2 с пакетом поддержки 5 можно использовать параметр MaxMetaspaceSize для определения размера памяти Metaspace, а не параметр MaxPermSize.
   >
   > - При обновлении более ранних версий, чем BI 4.2 SP5, на BI 4.2 SP5 необходимо вручную изменить этот параметр для всех существующих серверов.
   > - Если выполняется новая установка BI 4.2 с пакетом поддержки 5, параметр заменяется по умолчанию.

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) Корректировка адаптивных серверов обработки

Новый аргумент Java `-XX:MetaspaceSize` добавлен в командную строку APS в сочетании с существующим `-XX:MaxMetaspaceSize`, чтобы улучшить процесс инициализации и избежать нежелательной и полной очистки памяти в процессе Java, связанном с адаптивными серверами обработки.

Тестирование на VM с минимальными ресурсами RAM, APS по умолчанию и все службы включают эти значения для MetaSpace и MaxMetaSpace, чтобы APS запускался и инициализировался немного быстрее, чем при поставляемых настройках. Сообщается о нулевом количестве полных GC.

Для получения дополнительных сведений о *настройке параметров JAVA для адаптивных серверов обработки для избежания полной очистки памяти (полных GC) с помощью MetaSpace* см. SAP-ноту 3001317.

12) 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 функций 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 настраиваемого сервера обработки следующую строку: `-javaArgs «-Dbobj.tmp.dir=<TempDir>»`.

В приведенных выше примерах `<каталог_временных_файлов>` – это местоположение временного каталога, который требуется использовать.

13) 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.

Связанные сведения

Оптимальные методы работы [страница 1036]
Текущие ограничения выпуска [страница 1040]

28 Дополнительные конфигурации для сред ERP

28.1 Конфигурации для интеграции с SAP NetWeaver

28.1.1 Интеграция с SAP Business Warehouse (BW)

28.1.1.1 Обзор

В этом разделе демонстрируется, как настроить BW для включения и администрирования публикации отчетов из приложения SAP Business Warehouse на платформе BI.

Перед началом ознакомления с разделом убедитесь, что выполнена настройка подключаемого модуля аутентификации SAP в CMC.

Связанные сведения

Настройка аутентификации SAP [страница 348]

28.1.1.1.1 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 импорте 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:

> **Примечание**
>
> Основной издатель недоступен до момента публикации содержимого.
>
> - Добавить объекты в папку
> - Просмотреть объекты
> - 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.

Связанные сведения

Работа с уровнями доступа [страница 144]
Права на платформе BI [страница 129]

28.1.1.1.2 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>`).
- Папки ролей создаются автоматически (импортируются как группы на платформу BI) при необходимости, когда роль публикуется из BW.
- Папка содержимого создается автоматически для каждой из ролей, в которую публикуется содержимое.
- На каждый объект отчета распространяется параметр безопасности, и пользователи могут просматривать только те отчеты, которые относятся к их роли.

Администратор обязан распределять права между 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 элементами 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 *OK*.

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, опубликовать отчет можно, используя роль администратора, но лучше использовать для этого роль издателя. 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.

28.1.1.1.3 Планирование на основе событий BW

Теперь в платформе BI возможно планирование объектов на основе событий BW. Чтобы активировать планирование на основе событий BW, необходимо установить надежный канал связи между системой SAP NetWeaver Business Warehouse (BW) и платформой BI.

28.1.1.1.3.1 Создание и настройка событий BW

Для создания события BW выполните следующие шаги:

1. Войдите в CMC.
2. Выберите *События* > *События BW*.

3. Выберите , чтобы создать новое событие.
4. Введите *имя события* и *описание*.
5. Выберите *Создать*.
   Новое событие BW создано.

28.1.1.1.3.2 Добавление событий BW при планировании отчета

Чтобы добавить событие BW при планировании отчетов, выполните следующие шаги:

1. В **CMC** перейдите в область *Папки* и выберите отчет.
2. В контекстном меню отчета выберите *Запланировать*.
3. В области *Навигация* выберите *События* > *События BW*.
4. В списке *Доступные события* выберите событие.
5. Добавьте его к ожидаемым событиям, используя >>.
6. В области *Навигация* выберите *Повтор*.
7. Укажите параметры *Запустить объект*, *Допустимое число повторных попыток* и *Интервал повторения в секундах*.
8. Нажмите кнопку *Запланировать*.

   После инициирования события статус отчета **Отложено** изменится на **Выполняется**.

   > ⓘ Примечание
   >
   > Статус планирования **Отложено** сохраняется, если одно из событий, определенных как *Ожидаемые события*, не инициировано.

28.1.1.1.3.3 Интеграция платформы BI и системы ABAP

В этом разделе объясняется, как можно активировать планирование на основе события BW.

Выполните следующие шаги:

1. Настройте HTTPS/SSL для любого поддерживаемого сервера приложений на платформе BI и добавьте общий секретный ключ в `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container\bin`. См. раздел Настройка HTTPS/SSL [страница 543] для WACS и Настройка SSL в Tomcat [страница 424] для Tomcat.

   > ⓘ Примечание
   >
   > Для получения дополнительных сведений о поддерживаемых серверах приложений см. матрицу доступности продуктов SAP (PAM).

2. Экспортируйте сертификат сервера платформы BI из браузера в локальную систему. Из браузера Chrome можно выгрузить сертификаты, выполнив следующие шаги.
1. Выполните переход http://<имя_хоста>:<номер_порта>/biprws. Для получения дополнительных сведений о номере порта, специфичном для каждого приложения, см. раздел Настройка базового URL-адреса для веб-служб RESTful [страница 556].
2. Откройте инструменты разработчика браузера Chrome, нажав клавишу F12.
3. Откройте вкладку *Безопасность* и выберите *Просмотреть сертификат*.
   Откроется мастер `Сертификат`.
4. В мастере `Сертификат` откройте вкладку *Состав* и выберите *Копировать в файл*.
   Откроется *Мастер экспорта сертификатов*.
5. Выберите *Далее*.
6. На странице *Формат экспортируемого файла* выберите формат *Файлы X.509 (.CER) в кодировке Base-64* и нажмите *Далее*.
7. Укажите имя файла сертификата и сохраните его локально.
3. Выгрузите сертификат системы SAP NetWeaver BW.
1. Запустите SAP NetWeaver BW.
2. Выполните транзакцию *STRUSTSSO2*.
3. Выберите ▶ *PSE системы* > *Тема* > *Собственный сертификат* ▶.
4. Выберите команду *Загрузить*.
5. Укажите путь к файлу и выберите формат файла *Base64*.
6. Выберите ✔.

Сертификат системы SAP NetWeaver BW загружается в указанную папку.

4. Импортируйте сертификат платформы BI в систему SAP NetWeaver BW.
1. Выполните транзакцию *STRUSTSSO2*.
2. Включите режим *обработки*.
3. Выберите папку *SSL-клиент (стандарт)*.
4. Нажмите кнопку *Импорт*.
5. Загрузите сертификат системы SAP NetWeaver BW и выберите *Добавить в список сертификатов*.
   Сертификат добавляется в *Список сертификатов*.
6. Сохраните транзакцию.
5. Импортируйте сертификат системы SAP NetWeaver BW в платформу BI. Для получения дополнительных сведений об импорте сертификатов см. 12-й шаг в разделе Настройка HTTPS/SSL [страница 543].
6. Создайте пользователя в платформе BI.

> **Примечание**
>
> Необходимо, чтобы имя пользователя в платформе BI совпадало с именем пользователя в системе SAP NetWeaver BW. Например, если в системе SAP NetWeaver BW указано имя MySystem, в платформе BI следует создать пользователя с именем MySystem.

7. Создайте HTTP-адрес в системе SAP NetWeaver BW.
1. Выполните транзакцию *SM59*.
2. Выберите *HTTP-соединения с внешним сервером*.
3. Щелкните 🗋.

4. В окне *RFC-адрес* выберите вкладку "Технические настройки" и в полях *Хост*, *Порт* и *Префикс пути* введите соответственно значения `<hostname>`, `<port_number>` и `/biprws`.
5. Откройте вкладку *Вход и безопасность* и выберите *Активно* рядом с *SSL*.
6. Выберите *SSL-клиент по умолчанию (стандарт)* в качестве *сертификата SSL*.
7. Нажмите кнопку *Сохранить*.
8. Выберите Connection Test (Проверить соединение), чтобы проверить соединение с HTTP-адресом. Отобразится результат проверки соединения и текст статуса "OK".

> **Примечание**
>
> HTTP-соединение между SAP NetWeaver BW и платформой BI невозможно, если не выполнены условия, которые перечислены ниже.
>
> - Система BW должна быть обновлена, чтобы поддерживались версии TLS 1.1 и TLS 1.2.
> - Система BW должна поддерживать те же наборы шифров, которые поддерживает платформа BI.

9. Создайте цепочку процессов в системе SAP NetWeaver BW.
1. Вызовите транзакцию *RSPC*.
2. Откройте контекстное меню *Цепочки процессов* и выберите *Создать компонент отображения*.
3. В окне *Создание группировки* укажите *прикладной компонент* и *длинное описание*.
   Компонент SAP NetWeaver BW создан.
4. В контекстном меню прикладного компонента выберите *Создать цепочку процессов*.
5. Укажите имя и описание и выберите .
   После указания имени новой цепочки процессов откроется диалоговое окно `Вставить триггер`. Оно позволяет вставить триггер для цепочки процессов.
6. Укажите *варианты процессов* и *длинное описание* и выберите .
   Откроется окно ведения триггера.
7. Выберите *Обработать условия* и нажмите *Немедленно*, чтобы выполнить цепочку процессов незамедлительно.
8. Нажмите кнопку *Сохранить* в окне `Время начала`.
9. Нажмите *Сохранить* в окне `Ведение триггера`.
10. В окне `Вставить триггер` выберите .
    Цепочка процессов создана.
10. Настройте тип процесса в цепочке процессов.
1. Выберите цепочку процессов, созданную после предыдущего шага, в столбце *Цепочки процессов*.
2. Разверните папку *Процесс загрузки и постобработка* и выберите *Начальное событие в платформе SAP BOBJ BI для изменений данных BW*.
   Откроется диалоговое окно `Вставить начальное событие в платформе SAP BOBJ BI для изменений данных BW`.
3. В диалоговом окне *Вставить начальное событие в платформе SAP BOBJ BI для изменений данных BW* выберите .
4. Введите *варианты процессов* и *длинное описание*.
5. Выберите .
   Откроется окно `Ведение процесса`.

6. Выберите рядом с полем *Адрес назначения*, чтобы выбрать место назначения.
7. Выберите рядом с полем *Событие*, чтобы выбрать событие.
8. Сохраните изменения.
9. Выберите в диалоговом окне `Вставить начальное событие в платформе SAP BOBJ BI для изменений данных BW`.
   Создается тип процесса.
11. Активируйте цепочку процессов и выполните ее.

Это действие инициирует событие BW, указанное в типе процесса.

28.1.1.2 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.

28.1.1.3 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.

28.1.1.3.1 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 на использование тех же идентификатора программы, хоста шлюза и службы шлюза 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.

28.1.1.3.2 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.

28.1.1.3.3 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.

28.1.1.3.4 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.

28.1.1.3.5 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 публикацию отчетов из BW на платформе BI с использованием локального шлюза SAP, выполните следующие действия:

- установка локального шлюза SAP [страница 1054].
- Настройка назначения для BW Publisher [страница 1054].

28.1.1.3.6 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.

Для ознакомления с подробным списком протестированных сред см. матрицу доступности продуктов (PAM) по адресу http://service.sap.com/sap/support/pam?hash=pvnr%3D67837800100900006540. PAM 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`.

28.1.1.4 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.

28.1.1.5 Настройка опубликования в рабочем месте управления содержимым Content Administration Workbench

Приложение "Content Administration Workbench" используется для управления функциональностью создания отчетов в SAP BW. 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. После настройки аутентификации SAP и BW Publisher выполните действия, описанные в данном разделе, чтобы включить опубликование. Данные инструкции позволят:

- Задавать необходимые авторизации для различных пользователей рабочего места управления содержимым Content Administration Workbench.
- Настраивать 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.

28.1.1.6 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.

28.1.1.7 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 на 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 [страница 357].

- Настройка папок и безопасности для платформы BI [страница 1046].
- Работа с шаблонами безопасности для папок по умолчанию [страница 1047].

28.1.1.8 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.

Средства авторизации для пользователей с правами администратора

Объект авторизации	Поле	Значения
S_RFC	RFC_TYPE	FUGR
S_TCODE	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&
	JOBACTION	DELE, RELE
	JOBGROUP	' '
S_RS_ADMWB	ACTVT	Выполнение (16)
	RSADMWBOBJ	WORKBENCH
	ACTVT	Создание, изменение, отображение, удаление (01, 02, 03, 06)
ZCNTADMJOB	ACTVT	Создание, удаление (01, 06)
ZCNTADMRPT	ACTVT	Отображение, удаление, активация, обслуживание, проверка (03, 06, 07, 23, 39)

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)

Объект авторизации	Поле	Значения
	RSADMWBOBJ	WORKBENCH
	ACTVT	Отображение (03)

28.1.1.9 Определение системы платформы BI

Для каждой системы платформы BI, в которой требуется опубликовать отчеты, необходимо создать определение системы в Content Administration Workbench.

28.1.1.9.1 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 Центральный сервер управления (CMS). Если Центральный сервер управления настроен на прослушивание порта, отличного от порта по умолчанию, введите имя в формате **`ИМЯ_CMS:ПОРТ`**
   - 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 BOE*.

   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 **`boserver01.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 *OK*.
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.

    > ⓘ Примечание
    >
    > 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 *OK* внизу, чтобы сохранить настройки и создать систему платформы BI в Content Administration Workbench.

Теперь из BW можно публиковать отчеты на платформе BI.

Связанные сведения

Распространение установки BW Publisher [страница 1052]
Импорт ролей SAP [страница 357]

28.1.1.10 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 [страница 1076]), может использовать приложение Content Administration Workbench для публикации и обслуживания отчетов.

28.1.1.11 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 "A: активный" отображаются все отчеты, которые можно опубликовать. При выборе пустого значения отображаются все отчеты. (Остальные параметры являются зарезервированными выражениями SAP.)
   - *Статус объекта*
     Выберите "ACT 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 который 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 *OK*.
   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 элементы в иерархии отмечен красной, желтой или зеленой точкой. Элементы, расположенные выше в иерархии, соответствуют состоянию содержащихся в иерархии элементов – наименее благоприятные условия расположены на верхнем уровне иерархии. Например, если один отчет в роли является желтым (активным), но все остальные – зелеными (опубликованными), роль отмечена желтым цветом (активна).
   - Зеленый: элемент полностью опубликован. Если этим элементом является система платформы BI или роль, публикуются все отчеты в этом элементе.
   - Желтый: элемент активен, но не опубликован. Если элемент является отчетом, то он доступен для опубликования. Если этим элементом является роль или система платформы BI, то все содержимое является активным и по крайней мере один элемент в этой роли или системе не опубликован.
   - Красный: элемент является содержимым SAP и недоступен для опубликования с использованием Content Administration Workbench. Содержимое недоступно для опубликования, пока оно не активировано с использованием BW Administration Workbench.
7. Выберите отчеты, которые необходимо опубликовать.
   Для публикации всех отчетов в роли выберите роль. Выберите эту систему, чтобы опубликовать все роли в системе платформы BI.

   > **Примечание**
   >
   > При выборе роли (или системы) выбираются все отчеты, содержащиеся в роли (или системе). Чтобы очистить выделение, снимите флажок роли (или системы), а затем нажмите кнопку "Обновить".

8. Щелкните *Опубликовать*.

   > **Примечание**
   >
   > Отчеты, опубликованные в фоновом режиме, обрабатываются по мере высвобождении 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 *Перезаписать*, чтобы перезаписать опубликованный отчет.

Связанные сведения

Планирование публикации в фоновом режиме [страница 1062]

28.1.1.12 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 [страница 1063].

28.1.1.13 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.

28.1.1.14 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").

28.1.1.14.1 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 [страница 1062]), либо вручную обновлять статус отчета с использованием средства "Обслуживание отчетов".

28.1.1.14.2 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.

28.1.1.15 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.

28.1.1.16 Конфигурации для обработки данных SAP

28.1.1.16.1 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_OPENSQL_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.

Связанные сведения

Планирование отчета в пакетном режиме посредством запроса Open SQL [страница 1091]

28.1.1.16.2 Обработка запланированных отчетов в пакетном режиме SAP

1. Создайте пакетный скрипт (файл `.bat`) в текстовом редакторе, таком как "Блокнот", со следующим содержимым:

   ```
   @echo off
   set CRYSTAL_INFOSET_FORCE_BATCH_MODE=1
   set CRYSTAL_OPENSQL_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 задний. 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.

28.1.1.17 Конфигурации для переносов SAP

28.1.1.17.1 Обзор

Платформа BI содержит следующие транспорты:

- Транспорт Open SQL Connectivity
- Транспорт InfoSet Connectivity
- Транспорт определения безопасности на уровне строки
- Транспорт определения кластера
- Транспорт Content Administration Workbench
- Транспорт персонализации параметров запроса BW
- MDX
- 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 использоваться 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.

28.1.1.17.2 Настройка транспорта

Чтобы задать компоненты Data Access или BW Publisher платформы BI, необходимо импортировать в SAP-систему соответствующие файлы транспорта. Эти компоненты используют содержимое этих файлов транспорта при взаимодействии с системой SAP.

Процедуры установки и настройки, требуемые для системы SAP, должен выполнить специалист по BASIS, знакомый с системой изменений и транспорта, у которого есть права администратора для системы SAP. Точная процедура импорта файлов транспорта зависит от используемой версии BASIS. Точные сведения о процедуре см. в документации SAP.

По умолчанию при первом развертывании компонента Data Access все пользователи могут иметь доступ ко всем таблицам SAP. Чтобы обеспечить безопасность данных SAP, к которым пользователи могут получать доступ, используйте Редактор определения безопасности.

После импорта транспортов необходимо настроить соответствующие уровни доступа пользователей. Создайте нужные средства авторизации и примените их с помощью профилей или ролей к пользователям SAP, которые будут создавать, использовать или планировать отчеты Crystal.

Связанные сведения

Создание и применение средств авторизации [страница 1076]

28.1.1.17.2.1 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 использоваться 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.

Поддерживаемые типы 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.
- 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).
- 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).

28.1.1.17.2.2 Проверка на наличие конфликтов

Содержимое файлов транспорта автоматически регистрируется в пространстве имен SAP BusinessObjects при импорте этих файлов. С этой целью пространство имен SAP BusinessObjects зарезервировано в последних версиях R/3 и MYSAP 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 BusinessObjects необходимо

разрешить пространство имен. Описание процедур, соответствующих вашей версии SAP, см. в документации технологической платформы SAP NetWeaver.

28.1.1.17.2.3 Импорт файлов транспорта

Прочтите файл `transports_EN.txt`, расположенный в следующем каталоге дистрибутивного носителя для продукта: `\Collaterals\Add-Ons\SAP\Transports\`. В этом файле перечислены имена файлов для каждого транспорта. (Папки `cofiles` и `data` в директории `транспорты` соответствуют директориям .../`trans/cofiles` и .../`trans/data` на вашем сервере SAP).

Перед импортом транспортов для определения безопасности на уровне строки или определения кластера следует импортировать транспорт взаимодействия Open SQL Connectivity. Другие транспорты можно импортировать в любом порядке.

> ⓘ Примечание
>
> Скопировав файлы с диска на сервер, перед импортом убедитесь, что все файлы доступны для записи. Если файлы доступны только для чтения, то при импорте произойдет ошибка.

> ⓘ Примечание
>
> 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.

28.1.1.17.2.4 Переносы

28.1.1.17.2.4.1 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

Объект	Тип	Описание
/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
/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

Объект	Тип	Описание
ZSSAUTHREF	Таблица	Прежние метаданные RLS
ZSSAUTH FCN	Таблица	Прежние метаданные RLS

28.1.1.17.2.4.2 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.

28.1.1.17.2.4.3 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
/CRYSTAL/RLS_INCLUDE1	Программа	Включает программу, которая содержит определения модулей

Объект	Тип	Описание
/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.

28.1.1.17.2.4.4 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

28.1.1.17.2.4.5 Транспорт 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
/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

Объект	Тип	Описание
/CRYSTAL/PUBLISH_WORKER_PROC	Программа	Программный компонент
/CRYSTAL/ PUBLISH_WORKER_PROC_I	Программа	Программный компонент
/CRYSTAL/ PUBLISH_WORKER_SCREEN	Программа	Программный компонент
/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

28.1.1.17.2.4.6 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

28.1.1.17.2.4.7 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

28.1.1.17.2.4.8 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
/CRYSTAL/MDX_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

Объект	Тип	Описание
/CRYSTAL/ CX_NO_MORE_PROPERTIES	Класс	Исключение
/CRYSTAL/CX_SAVE_SESSION_STATE	Класс	Исключение
/CRYSTAL/MDX_APPEND_DATA	Класс	Процессор набора данных
/CRYSTAL/MDX_READER_BASE	Класс	Процессор набора данных
/CRYSTAL/MDX_READ_DIMENSIONS	Класс	Процессор набора данных
/CRYSTAL/MDX_READ_MEASURES	Класс	Процессор набора данных
/CRYSTAL/MDX_READ_PROPERTIES	Класс	Процессор набора данных
/CRYSTAL/MDX_PROPERTY_KEYS	Тип таблицы	Структура метаданных
/CRYSTAL/MDX_PROPERTY_KEYS	Тип таблицы	Структура метаданных
/CRYSTAL/MDX_PROPERTY_VALUES	Тип таблицы	Структура метаданных
/CRYSTAL/ MDX_STREAM_LAYOUT_TAB	Тип таблицы	Структура метаданных

28.1.1.18 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 разделе приводится только в целях рекомендации.

> ⓘ Примечание
>
> Объект авторизации ZSEGREPORT принадлежит к классу объектов ZSSI, который устанавливается при импорте файлов переноса SAP Integration, необходимых для поддержки запросов Open SQL.

28.1.1.18.1 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.

Связанные сведения

Настройка опубликования в рабочем месте управления содержимым Content Administration Workbench [страница 1054]

28.1.1.19 Действия в BW

В этом разделе перечислены различные действия в модуле BW.

28.1.1.19.1 Действия в Crystal Reports

28.1.1.19.1.1 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>** **

Объект авторизации	Поле	Значения
	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.

28.1.1.19.1.2 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	**<INFO_AREA>** **
	RSINFOCUBE	**<INFO_CUBE>** **
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** **
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** **

Объект авторизации	Поле	Значения
	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.

28.1.1.19.1.3 Предварительный просмотр или обновление отчета

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 вы укажете конкретное значение, можно составить отчеты по запросам, содержащим только конкретные информационные области, кубы и компоненты с указанными идентификаторами.

28.1.1.19.1.4 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.

28.1.1.19.1.5 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

Объект авторизации	Поле	Значения
	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.

28.1.1.19.1.6 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.

28.1.1.19.1.7 Подготовка отчета к переводу во время сохранения в BW

Объект авторизации	Поле	Значения
S_USER_AGR	ACT_GROUP	**<USER_ROLE>** *
	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.

28.1.1.19.1.8 Сохранение отчета и одновременная публикация на платформе BI

Объект авторизации	Поле	Значения
S_USER_AGR	ACT_GROUP	**<USER_ROLE>** *
	ACTVT	01
S_CTS_ADMI	CTS_ADMFCT	TABL
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** ***
	RSINFOCUBE	**<INFO_CUBE>** ***
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** ***
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** ***
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** **
	ACTVT	16

* **<USER_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.

28.1.1.19.1.9 Запуск BEx Query Designer™

Объект авторизации	Поле	Значения
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****

Объект авторизации	Поле	Значения
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16
S_CTS_ADMI	CST_ADMFCT	TABL

* **<QUERY_OWNER>** обозначает имя владельца запроса, на основе которого создается отчет. Если ввести имя владельца отчета, отчеты можно создавать только с использованием запросов для этого владельца. Введите * для обозначения всех владельцев запросов.

** Чтобы указать для **<INFO_AREA>** (информационной области), **<INFO_CUBE>** (инфо-куба) или **<COMP_ID>** (ид. компонента) любое значение, введите *. Если вы укажете конкретные значения, вы сможете создавать отчеты только по запросам, содержащим указанные информационные области, кубы и идентификаторы компонентов.

28.1.1.19.2 Действия в стартовой панели BI

28.1.1.19.2.1 Вход на платформу BI с учетными данными SAP

Объект авторизации	Поле	Значения
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM

28.1.1.19.2.2 Просмотр отчета SAP BW по запросу

Объект авторизации	Поле	Значения
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB, SUNI

Объект авторизации	Поле	Значения
	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.

28.1.1.19.2.3 Обновление отчета из средства просмотра

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_RS_ODSO	RSINFOAREA	**<INFO_AREA>****
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* **<QUERY_OWNER>** обозначает имя владельца запроса, на основе которого создается отчет. Если ввести имя владельца отчета, отчеты можно создавать только с использованием запросов для этого владельца. Введите * для обозначения всех владельцев запросов.

** Чтобы указать для **<INFO_AREA>** (информационной области), **<INFO_CUBE>** (инфо-куба) или **<COMP_ID>** (ид. компонента) любое значение, введите *. Если вы укажете конкретные значения, вы сможете создавать отчеты только по запросам, содержащим указанные информационные области, кубы и идентификаторы компонентов.

28.1.1.19.2.4 Планирование отчета

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>** **

Объект авторизации	Поле	Значения
	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.

28.1.1.19.2.5 Чтение динамических списков выбора в параметрах отчета

Объект авторизации	Поле	Значения
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB
	ACTVT	16

28.1.1.19.3 Действия в SAP Netweaver (ABAP)

28.1.1.19.3.1 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.

28.1.1.19.3.2 Вход на сервер SAP

Объект авторизации	Поле	Значения
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16

28.1.1.19.3.3 Создание нового отчета

Объект авторизации	Поле	Значения
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	01

28.1.1.19.3.4 Открытие или предварительный просмотра существующего отчета

Объект авторизации	Поле	Значения
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	02

28.1.1.19.3.5 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/OPENSQL
	ACTVT	16

28.1.1.19.3.6 Настройка местоположения источника данных

Объект авторизации	Поле	Значения
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQL
	ACTVT	16

28.1.1.19.4 Действия в Crystal Reports с использованием драйвера InfoSet и отчеты из InfoSet

28.1.1.19.4.1 Вход на сервер SAP

Объект авторизации	Поле	Значения
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

28.1.1.19.4.2 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.

Связанные сведения

Настройка местоположения источника данных [страница 1088]

28.1.1.19.4.3 Проверка базы данных (обновление определений таблицы в отчете)

Объект авторизации	Поле	Значения
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM

28.1.1.19.4.4 Настройка местоположения источника данных

Объект авторизации	Поле	Значения
P_ABAP	REPID	AQTGSYSTGENERATESY, SAPDBPNP
	COARS	2

28.1.1.19.5 Действия в Crystal Reports с использованием драйвера InfoSet и отчеты из запроса ABAP

28.1.1.19.5.1 Вход на сервер SAP

Объект авторизации	Поле	Значения
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

28.1.1.19.5.2 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

28.1.1.19.5.3 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

28.1.1.19.5.4 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

28.1.1.19.6 Действия на платформе BI

28.1.1.19.6.1 Планирование отчета в диалоговом режиме (с запросом Open SQL)

Объект авторизации	Поле	Значения
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	02

> ⓘ Примечание
>
> Значением для CLASS является ПУСТО.

28.1.1.19.6.2 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.

28.1.1.19.6.3 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

Объект авторизации	Поле	Значение
	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)	* **Примечание** В целях повышения безопасности можно непосредственно перечислить группы пользователей, членам которых необходим доступ к платформе BI.

28.1.1.19.6.4 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	

28.2 Настройка для интеграции с JD Edwards

28.2.1 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).

28.2.1.1 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 CMC выберите *Службы Crystal Reports* и щелкните *Перезапустить сервер*.

28.2.1.2 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 CMC выберите *Службы Crystal Reports* и щелкните *Перезапустить сервер*.

28.2.2 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).

28.2.2.1 Включение соединений с данными JD Edwards EnterpriseOne по протоколу SSL

> **Примечание**
>
> Для всех значений, описанных в следующей процедуре, учитывается регистр.

1. Скопируйте сертификаты SSL в каталог `C:\SSLCert`.
2. Запустите Central Configuration Manager (CCM).
3. Остановите агент серверной аналитики (SIA).
4. Дважды щелкните SIA, чтобы открыть диалоговое окно *Свойства*.
5. Щелкните вкладку *Протокол*.
6. Выберите *Включить SSL*.
7. Для поля *Папка сертификатов SSL* выберите каталог, содержащий сертификаты SSL: `C:\SSLCert`.
8. Для поля *Файл сертификата сервера SSL* выберите `servercert.der`.
9. Для поля *Файлы надежных сертификатов SSL* выберите `cacert.der`.
10. Для поля *Файл закрытого ключа SSL* выберите `server.key`.
11. Для поля *Файл идентификационной фразы для закрытого ключа SSL* выберите `passphrase.txt`.
12. Нажмите кнопку *Применить*.
13. Запустите агента Server Intelligence.

Чтобы эти изменения вступили в силу, необходимо перезапустить серверы отчетов платформы BI (например, адаптивный сервер заданий).

28.2.2.2 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`.

28.3 Настройка для интеграции с PeopleSoft Enterprise

28.3.1 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).

28.3.1.1 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*.

28.3.1.2 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* CMC выберите *Сервисы Crystal Reports* и нажмите *Перезапустить сервер*.

28.3.2 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).

28.3.2.1 Файл свойств конфигурации SSL

Файл свойств `sslconf.properties` содержит все сведения для обязательных сертификатов и ключей, используемых компонентами платформы BI. Например:

```
[default]
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

Файл `sslconf.properties` необходимо поместить в папку, в которой установлен продукт платформы BI. По умолчанию это папка `C:\Program Files\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\`.

28.3.2.2 Включение поддержки SSL для сервера запросов PeopleSoft

> **Примечание**
>
> Для всех значений, описанных в следующей процедуре, учитывается регистр.

1. Скопируйте сертификаты SSL в каталог `C:\SSLCert`.
2. Запустите Central Configuration Manager (CCM).
3. Остановите агент серверной аналитики (SIA).
4. Дважды щелкните SIA, чтобы открыть диалоговое окно *Свойства*.
5. Щелкните вкладку *Протокол*.
6. Выберите *Включить SSL*.

7. Для поля *Папка сертификатов SSL* выберите каталог, содержащий сертификаты SSL: `C:\SSLCert`.
8. Для поля *Файл сертификата сервера SSL* выберите `servercert.der`.
9. Для поля *Файлы надежных сертификатов SSL* выберите `cacert.der`.
10. Для поля *Файл закрытого ключа SSL* выберите `server.key`.
11. Для поля *Файл идентификационной фразы для закрытого ключа SSL* выберите `passphrase.txt`.
12. Нажмите кнопку *Применить*.
13. Запустите агента Server Intelligence.

Чтобы эти изменения вступили в силу, необходимо перезапустить серверы отчетов платформы BI (например, адаптивный сервер заданий).

28.3.2.3 Включение моста безопасности с SSL

> **Примечание**
>
> Для всех значений, описанных в следующей процедуре, учитывается регистр.

1. Скопируйте сертификаты SSL в каталог `C:\SSLCert`.
2. Запустите Central Configuration Manager (CCM).
3. Остановите агент серверной аналитики (SIA).
4. Дважды щелкните SIA, чтобы открыть диалоговое окно *Свойства*.
5. Щелкните вкладку *Протокол*.
6. Выберите *Включить SSL*.
7. Для поля *Папка сертификатов SSL* выберите каталог, содержащий сертификаты SSL: `C:\SSLCert`.
8. Для поля *Файл сертификата сервера SSL* выберите `servercert.der`.
9. Для поля *Файлы надежных сертификатов SSL* выберите `cacert.der`.
10. Для поля *Файл закрытого ключа SSL* выберите `server.key`.
11. Для поля *Файл идентификационной фразы для закрытого ключа SSL* выберите `passphrase.txt`.
12. Нажмите кнопку *Применить*.
13. Запустите агента Server Intelligence.

28.3.3 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*.

28.3.3.1 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*.

> ⓘ Примечание
>
> 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.

28.3.3.2 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.

28.4 Настройка для интеграции с Siebel

28.4.1 Настройка Siebel для интеграции с платформой SAP BI

Интеграция с платформой BI обеспечивает связь с Crystal Reports, что позволяет пользователям внедрять содержимое пакета SAP 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 требуемые файлы устанавливаются в следующую папку: `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\siebel\Siebel Files\`.

28.4.1.1 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 `<КАТАЛОГ_УСТАНОВКИ>\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*.

28.4.2 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 [страница 1100].

28.4.2.1 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:

```
ClientBusinessService<NUMBER> = 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.

28.4.3 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 получат отчеты, созданные с использованием данных Siebel.

28.4.3.1 Настройка контекстуальной зависимости

Перед настройкой следует удостовериться, что выполнены следующие действия.

- Установка продукта интеграции с Siebel
- Настройка Siebel для интеграции с платформой BI

1. Откройте Central Management Console (CMC).
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.

28.4.3.2 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.

> **Примечание**
>
> Значение переменной "userDomain" является чувствительным к регистру.

28.4.3.3 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 на ввод имени пользователя и пароля, которые будут использоваться для соединения. Эти данные необходимо вводить только при первом входе в систему до того, как истечет время ожидания сеанса. 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.

28.4.3.4 Добавление папок к платформе BI

Для полноценной контекстной поддержки 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.

28.4.4 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).

28.4.4.1 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.

28.4.4.2 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.

28.4.5 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 компонентом интеграции для компонентов Siebel. Например,

```
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

Файл `sslconf.properties` необходимо поместить в папку, где установлен продукт платформы BI. По умолчанию это папка `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0`.

28.4.5.1 Включение соединений с данными Siebel по протоколу SSL

> **Примечание**
>
> Для всех значений, описанных в следующей процедуре, учитывается регистр.

1. Скопируйте сертификаты SSL в каталог `C:\SSLCert`.
2. Запустите Central Configuration Manager (CCM).
3. Остановите агент серверной аналитики (SIA).
4. Дважды щелкните SIA, чтобы открыть диалоговое окно *Свойства*.
5. Щелкните вкладку *Протокол*.
6. Выберите *Включить SSL*.
7. Для поля *Папка сертификатов SSL* выберите каталог, содержащий сертификаты SSL: `C:\SSLCert`.
8. Для поля *Файл сертификата сервера SSL* выберите `servercert.der`.
9. Для поля *Файлы надежных сертификатов SSL* выберите `cacert.der`.
10. Для поля *Файл закрытого ключа SSL* выберите `server.key`.
11. Для поля *Файл идентификационной фразы для закрытого ключа SSL* выберите `passphrase.txt`.
12. Нажмите кнопку *Применить*.
13. Запустите агента Server Intelligence.

Чтобы эти изменения вступили в силу, необходимо перезапустить серверы отчетов платформы BI (например, адаптивный сервер заданий).

29 Управление журналами и их настройка

29.1 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.

29.2 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 `.ini`.

Уровень	Описание
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	Нет отфильтрованных сообщений. Этот уровень рекомендуется для использования в целях отладки. ⚠ Предупреждение Этот уровень трассировки оказывает значительное влияние на ресурсы системы, повышая нагрузку на процессор и занимая место на диске.

29.3 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 `<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\logging`.
- В Unix по умолчанию используется каталог `<КАТАЛОГ_УСТАНОВКИ>/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`.

29.3.1 Настройка уровня журнала в CMC

Можно скорректировать уровень трассировки журнала для сервера, не влияя на другие параметры трассировки.

1. В области *Серверы* CMC 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 области *Параметры командной строки*. Перезапустите сервер, чтобы эта настройка вступила в силу.

Связанные сведения

Уровни журнала трассировки [страница 722]

29.3.2 Установка уровня журнала для нескольких серверов в CMC

1. В области *Серверы* CMC 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 *OK*.

Новый уровень трассировки журнала вступит в силу немедленно.

Чтобы указать другой выходной каталог для файлов журнала, включите параметр `-loggingPath <целевой_каталог>` в области *Параметры командной строки*. Перезапустите сервер, чтобы эта настройка вступила в силу.

Связанные сведения

Уровни журнала трассировки [страница 722]

29.3.3 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 `<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\conf\`.
   - В Unix по умолчанию используется каталог `<КАТАЛОГ_УСТАНОВКИ>/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**	Определяет серьезность сообщений журнала. По умолчанию используется серьезность **log_error**. 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

Параметр	Возможные значения	Описание
		`log_warning`, `log_error` и `log_fatal`. ⓘ Примечание `log_information` и `log_warning` можно сократить до `log_info` и `log_warn`.
`sap_trace_level`	`trace_debug` `trace_path` `trace_information` `trace_error` `trace_none`	Определяет серьезность сообщений трассировки. По умолчанию используется серьезность трассировки `trace_error`. 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`. ⓘ Примечание `trace_information` можно сократить до `trace_info`.

4. Сохраните и закройте файл `BO_trace.ini`.

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` вступят в силу немедленно.

Пример

Файл `BO_trace.ini`

```
sap_log_level=log_warning;
sap_trace_level=trace_path;
```

29.3.3.1 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 CMC для конкретного сервера, будут перезаписывать все параметры в `BO_trace.ini`.

1. Откройте файл `BO_trace.ini`.
   - В Windows по умолчанию используется каталог `<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\conf\`.
   - В Unix по умолчанию используется каталог `<КАТАЛОГ_УСТАНОВКИ>/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.

29.4 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 расположение по умолчанию – `C:\Windows\System32\config\systemprofile\SBOPWebapp_<APPLICATION>_<IPADDRESS>_<PORT>\` Например, `C:\Windows\System32\config\systemprofile\SBOPWebapp_BIlaunchpad_192.0.2.0_8080\`
- В Unix по умолчанию используется каталог `$userHome/SBOPWebapp_<ПРИЛОЖЕНИЕ>_<IP_АДРЕС>_<ПОРТ>/`. Например, `$userHome/SBOPWebapp_CMC_192.0.2.0_8080/`

По умолчанию для уровня журнала трассировки для веб-приложений в CMC установлено значение *Не определен*. Настройки журнала трассировки доступны для следующих приложений в CMC:

- Central Management Console
- Стартовая панель BI
- Open Document
- 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 `dswsbobje.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*.

29.4.1 Настройка уровня журнала трассировки веб-приложения в CMC

Для трассировки других веб-приложений следует вручную сконфигурировать соответствующий файл `BO_trace.ini`.

1. В поле *Приложения* консоли CMC щелкните приложение правой кнопкой мыши и выберите *Настройки журнала трассировки*.

   > **Примечание**
   >
   > Эти приложения имеют следующие параметры журнала трассировки: Стартовая панель BI в стиле Fiori, CMC, Открыть документ, Диспетчер переноса объектов, Управление версиями, Visual Difference и Веб-служба.

   Будет открыто диалоговое окно *Настройки журнала трассировки*.
2. Выберите параметр в раскрывающемся списке *Уровень журнала*.

3. Нажмите кнопку *Сохранить и закрыть*.
4. Перезапустите сервер веб-приложений.

Новый уровень журнала трассировки вступит в силу после следующего входа в данное веб-приложение.

Связанные сведения

Уровни журнала трассировки [страница 722]

29.4.2 Настройка параметров трассировки с использованием файла `BO_trace.ini`

Файл `BO_trace.ini` развертывается с файлами `.war` `BOE` 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.

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. Возможно непосредственное изменение файлов.
     - Файл конфигурации трассировки для файла `BOE.war` доступен в каталоге `<КАТАЛОГ_УСТАНОВКИ>\Tomcat\webapps\BOE\WEB-INF\TraceLog`.
     - Файл конфигурации трассировки для файла `dswsbobje.war` доступен в каталоге `<КАТАЛОГ_УСТАНОВКИ>\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 `<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`.
   - По умолчанию для предварительно развернутой версии файла конфигурации для файла `dswsbobje.war` каталог `<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`.
3. Откройте файл `BO_trace.ini`.
   - В Windows по умолчанию используется каталог `<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\conf\`.

- В Unix по умолчанию используется каталог `<КАТАЛОГ_УСТАНОВКИ>/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**	Определяет серьезность сообщений журнала. По умолчанию используется серьезность **log_error**. 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**. ⓘ Примечание **log_information** и **log_warning** можно сократить до **log_info** и **log_warn**.
sap_trace_level	**trace_debug** **trace_path** **trace_information** **trace_error** **trace_none**	Определяет серьезность сообщений трассировки. По умолчанию используется серьезность трассировки **trace_error**. 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

Параметр	Возможные значения	Описание
		нижестоящих уровней. Например, если задана серьезность трассировки **trace_path**, в файл журнала будут записываться сообщения, которые включают **trace_path**, **trace_info** и **trace_error**. Примечание **trace_information** можно сократить до **trace_info**.

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.

29.4.2.1 Настройка трассировки для конкретного веб-приложения

Файл `BO_trace.ini` развертывается вместе с файлами `.war` `BOE` 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`	`<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`
Стартовая панель BI	`BOE.war`	`<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`
Открыть документ	`BOE.war`	`<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI`

Веб-приложение	Файл WAR	Предварительно развернутое расположение
		4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
Веб-служба	dswsbobje.war	<КАТАЛОГ_УСТАНОВКИ>\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 <КАТАЛОГ_УСТАНОВКИ>\Tomcat\webapps\BOE\WEB-INF\TraceLog.
     - Файл конфигурации трассировки для файла `dswsbobje.war` доступен в каталоге <КАТАЛОГ_УСТАНОВКИ>\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 <КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog.
   - По умолчанию для предварительно развернутой версии файла конфигурации для файла `dswsbobje.war` каталог <КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf.
3. Откройте файл `BO_trace.ini`.
   - В Windows по умолчанию используется каталог <КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Enterprise XI 4.0\conf\.
   - В Unix по умолчанию используется каталог <КАТАЛОГ_УСТАНОВКИ>/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`	Определяет серьезность сообщений журнала. По умолчанию используется серьезность `log_error`. 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`. ⓘ Примечание `log_information` и `log_warning` можно сократить до `log_info` и `log_warn`.
`sap_trace_level`	`trace_debug` `trace_path` `trace_information` `trace_error` `trace_none`	Определяет серьезность сообщений трассировки. По умолчанию используется серьезность трассировки `trace_error`. Серьезность трассировки определяется в иерархической последовательности: на самом

Параметр	Возможные значения	Описание
		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**. Примечание **trace_information** можно сократить до **trace_info**.

5. Сохраните и закройте файл `BO_trace.ini`.
6. При помощи WDeploy разверните файл `.war` на компьютере, где размещен сервер веб-приложений.

29.5 Настройка трассировки для клиентских приложений платформы BI

Трассировку можно активировать для следующих клиентов:

- Средство создания юниверсов
- 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 [страница 1110].

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.

29.6 Настройка расширенной трассировки сообщений об ошибках

Для некоторых приложений, например SAP BusinessObjects Web Intelligence, можно включить трассировку для создания файлов журнала, которые содержат обширную информацию о любых сообщениях об ошибках, выданных приложением.

> ⓘ Примечание
>
> Эти файлы журнала предназначены для инженеров службы поддержки SAP. Файл журнала имеет формат JSON.

Файлы журнала с подробной информацией о сообщениях об ошибках можно включить, изменив следующий файл в установке SAP BusinessObjects BI: `extended_info.properties`.

29.7 Включение файлов журнала с подробной информацией о сообщениях об ошибках

Вам требуется извлечь подробную информацию о сообщениях об ошибках, выданных приложением. Для этого вам следует включить файлы журнала с подробной информацией о сообщениях об ошибках.

> ⓘ Примечание
>
> В пакете SAP BusinessObjects BI Suite версии 4.2 SP5 эта функция поддерживается только для SAP BusinessObjects Web Intelligence.

1. В установке SAP BusinessObjects BI откройте следующий файл: `extended_info.properties`.

   Расположение по умолчанию:
   - В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`
   - В UNIX: `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`
2. Введите соответствующие значения параметров.

Параметр	Возможные значения	Описание
`output.format`	• Json • none	Управляет форматом созданных файлов. ⓘ Примечание Если установлен формат none, файлы не создаются.

Параметр	Возможные значения	Описание
`output.size`	`<size><unit>`, где `<size>` – положительное целое число, `<unit>` – "g" для гигабайтов, "m" для мегабайтов. **Примечание** Единицей по умолчанию являются килобайты.	Общий размер всех файлов, которые может создать приложение. Если размер превышен, более старые файлы удаляются.

Файлы журнала создаются в той же папке, что и файлы трассировки. Расположение по умолчанию:

- В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging\`
- В UNIX: `<INSTALLDIR>/sap_bobj/logging/`

Файлам присваиваются имена `<application_name>_<error_id>_exinfo.<format>`

Именем приложения является имя приложения, выдавшего ошибку. Идентификатор ошибки создается случайным образом. Форматом файла является формат, указанный в файле конфигурации.

> **Примечание**
>
> Единственным возможным расширением файла является `.json`

Для каждого сообщения, выданного определенным приложением, создается отдельный файл журнала.

30 Интеграция с SAP Solution Manager

30.1 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 порталу поддержки SAP для SAP BusinessObjects перейдите по следующему адресу: https://support.sap.com/home.html

30.2 Контрольный список по интеграции SAP Solution Manager

В следующей таблице приводится сводка компонентов, которые требуются для включения поддержки платформы BI в SAP Solution Manager.

Поддержка в SAP Solution Manager	Обязательно для платформы BI
Регистрация в SLD	• Для включения регистрации на серверах платформы BI должен быть установлен агент SAPHOSTAGENT. **Примечание** Если агент SAPHOSTAGENT установлен, программа установки платформы BI выполнит регистрацию серверов автоматически. • Необходимо создать файл connect.key для поставщика данных, ведущего отчетность по обслуживающим 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	• Необходимо загрузить и установить SMD-агент (DIAGNOSTICS.AGENT) на всех хостах серверов платформы BI. • Необходимо включить учетную запись пользователя SMAdmin в платформе BI.
Настройка конфигурации для производительности	• Для подключения к Enterprise Manager должен быть настроен агент Introscope. Для настройки соединений воспользуйтесь программой установки платформы BI или заполнителями узлов в CMC. • 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 CMC.
SAP Passport	• Необходимо загрузить и установить средство клиента SAP Passport.

30.3 Управление регистрацией System Landscape Directory

30.3.1 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.

30.3.1.1 Создание файла connect.key для поставщика данных SLD

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.

30.3.2 Точки запуска SLD

Процесс регистрации в SLD инициируется поставщиком данных, создающим отчетность по обслуживающим серверам платформы BI, в следующих сценариях:

- Перезапуск узла сервера в развертывании платформы BI.
- Добавление в развертывание нового сервера или узла.
- Удаление сервера или узла

> ⓘ Примечание
>
> При удалении сервера или узла процесс регистрации в SLD не изменяет содержимое SLD-сервера. 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 вызвать 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.

30.3.3 Очистка SLD перед установкой исправлений

Данные из предшествующих версий платформы BI накапливаются на сервере SLD после установки исправления. Это осложняет диагностику продукта с помощью SAP Solution Manager. Во избежание такой проблемы перед установкой любого исправления выполните на базовом компьютере следующие шаги:

> ⓘ Примечание
>
> Эта функция доступна для версии 4.2 SP3 и более поздних версий.

1. Перейдите в каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bobj-sld-ds`.
2. Запустите пакетный файл bobjsldds.bat с параметрами очистки (`-clean`).

   > ⓘ Примечание
   >
   > Система создаст XML-файл (с предварительно определенными параметрами), который будет отправлен на сервер SLD для очистки. Результаты очистки обновятся после перезапуска SIA.

30.3.4 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: `<INSTALLDIR>/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 `<INSTALLDIR>/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: `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/log`. Имена файлов журнала инструмента sldreg не могут изменяться. Они имеют следующий формат: `sldreg_<отметка_времени>.log`.

Каждый раз при вызове инструмента sldreg в поставщике данных создается новый файл журнала.

30.3.5 Имя виртуального хоста

При перезапуске *Server Intelligence Agent* создается файл поставщика данных для каждого узла. Файл передается в System Landscape Directory и далее с использованием SAP Solution Manager. В платформе Business Intelligence версии 4.2 с пакетом поддержки 4 и более ранних версий в файл поставщика данных было добавлено имя физического хоста. В платформе Business Intelligence версии 4.2 с пакетом поддержки 5 можно определить имя виртуального хоста в файле *sldparserconfig.properties*, чтобы обеспечить использование имени виртуального хоста файлом поставщика данных.

> ⓘ Примечание
>
> По умолчанию файл поставщика данных использует имя физического хоста, если файл sldparserconfig.properties не содержит имени виртуального хоста.

Чтобы добавить имя виртуального хоста в файл sldparserconfig.properties, выполните следующие шаги:

1. Перейдите в каталог `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bobj-sld-ds`.
2. Отредактируйте файл sldparserconfig.properties.
3. Добавьте следующий параметр: `virtualHostName = <Virtual Hostname>`.
4. Сохраните файл.
5. Перезапустите *Server Intelligence Agent*, чтобы изменения использовались файлом поставщика данных.

> **Примечание**
>
> Использование изменений также можно обеспечить, выполнив следующую команду:
>
> В ОС Windows: `runbobjsldds.bat -config sldparserconfig.properties -name <Node Name> -clusterlist <Cluster Name with Port Number>` в каталоге `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bobj-sld-ds`.
>
> В ОС Unix: `runbobjsldds.sh -config sldparserconfig.properties -name <Node Name> -clusterlist <Cluster Name with Port Number>` в каталоге `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/lib/bobj-sld-ds`.

30.4 Управление агентами Solution Management Diagnostics

30.4.1 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.

30.4.2 Работа с SMD-агентами

Платформа BI не устанавливает SMD-агент. Агент `DIAGNOSTICS.AGENT` можно загрузить по следующей ссылке: https://support.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 SMAdmin.

30.4.3 Учетная запись пользователя SMAdmin

В каждом развертывании платформы BI существует учетная запись пользователя, созданная специально для обеспечения интеграции с SMD. Эта учетная запись только для чтения используется на SMD-сервере для входа на CMS и сбора параметров конфигурации сервера, а также других сведений о развертывании.

Учетная запись SMAdmin по умолчанию неактивна.

30.4.3.1 Активация учетной записи пользователя SMAdmin

1. В области управления CMC *Пользователи и группы* выберите значение *Список пользователей*. Будет открыт список пользователей.
2. Найдите учетную запись пользователя *SMAdmin* .
3. Выберите команду *Управление* > *Свойства* . Отобразится диалоговое окно *Свойства*.
4. Снимите флажок *Учетная запись отключена*.
5. Нажмите кнопку *Сохранить и закрыть*.

30.5 Инструментальные средства управления производительностью

30.5.1 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 обслуживающих 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.

30.5.2 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 BI можно предоставить данные конфигурации для SMD-агента при помощи заполнителей в свойствах узла в консоли CMC.

> **Примечание**
>
> Для настройки инструментов мониторинга рабочих процессов на серверах, не являющихся Java-серверами, необходимо предварительно установить SMD-агент (`DIAGNOSTICS.AGENT`).

Связанные сведения

Работа с SMD-агентами [страница 1127]

30.5.2.1 Настройка узлов для выполнения инструментальных средств

Если во время установки платформы BI 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 `true`, 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.

30.5.3 Настройка конфигурации производительности для веб-уровня

Данные инструментов мониторинга для компонентов веб-уровня не включены в платформу BI.

30.5.4 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: `<КАТАЛОГ_УСТАНОВКИ>/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`.

30.6 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.

Для получения дополнительных сведений посетите 1861180.

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 https://support.sap.com/swdc.

31 Администрирование в командной строке

31.1 Скрипты UNIX

В этом разделе описываются все инструменты администрирования и скрипты, включенные в дистрибутив платформы BI для UNIX. Основное назначение данного раздела – ссылки. Здесь также изложены основные принципы и процедуры настройки.

> ⓘ Примечание
>
> Право выполнять скрипты оболочки в платформе BI имеет только пользователь, установивший платформу BI.

Дистрибутив платформы BI для UNIX содержит ряд скриптов, которые в совокупности предоставляют все параметры конфигурации, доступные в версии Central Configuration Manager (CCM) для Windows. Также включены другие скрипты, которые предоставляют параметры, доступные только в UNIX, или служат шаблонами для создания собственных скриптов. Также предоставляется несколько дополнительных скриптов, используемых платформой BI. Здесь рассматриваются все эти скрипты, а также применимые параметры командной строки.

> ⓘ Примечание
>
> При вводе параметров командной строки UNIX требуется экранировать специальные символы оболочки (один или несколько раз). Например, если в пароле используется восклицательный знак («!»), необходимо экранировать его следующим образом: `./ccm.sh -display -username Administrator -password Abc\!defgh123 -cms cmsname`.

31.1.1 Утилиты скриптов

В этом разделе описаны административные скрипты, которые помогают вам работать с платформой BI в операционной системе UNIX. В оставшейся части этого раздела обсуждаются основные принципы задач, которые можно выполнять с помощью этих скриптов. В справочном разделе представлены главные параметры командной строки и их аргументы.

31.1.1.1 ccm.sh

Скрипт `ccm.sh` устанавливается в каталог `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj` установки. Этот скрипт создает версию командной строки CCM. В этом разделе перечислены параметры командной строки и приведены некоторые примеры.

> **ⓘ Примечание**
>
> Аргументы в квадратных скобках [ ] являются необязательными.

> **ⓘ Примечание**
>
> Если имя агента Server Intelligence не известно, посмотрите свойства команды в файле `ccm.config` и используйте значение, указанное после параметра `-name`.

> **ⓘ Примечание**
>
> Скрипт `ccm.sh` может быть запущен только пользователем, который выполнял установку платформы BI.

- Аргументы, отмеченные как **`<другая информация для аутентификации>`**, представлены во второй таблице.

Параметр CCM	Допустимые аргументы	Описание
`-help`	недоступно	Отображает справку по командной строке.
`-start`	`all` (все) или **`<имя_SIA>`**	Запускает каждого агента Server Intellegence в качестве процесса. Параметр `all` позволяет запустить все узлы на компьютере, включая узлы, входящие в разные кластеры.
`-stop`	`all` (все) или **`<имя_SIA>`**	Остановка каждого SIA путем удаления ID его процесса. Параметр `all` (все) позволяет запустить все узлы на компьютере, включая узлы, входящие в разные кластеры.
`-restart`	`all` (все) или **`<имя_SIA>`**	Останавливает каждого агента SIA путем удаления ID его процесса; затем каждый SIA запускается заново. Параметр `all` позволяет запустить все узлы на компьютере, включая узлы, входящие в разные кластеры.
`-managedstart`	**`<полное имя сервера><[другая информация для аутентификации]>`**	Запустите сервер.

Параметр CCM	Допустимые аргументы	Описание
`-managedstop`	**`<полное имя сервера><[другая информация для аутентификации]>`**	Остановите сервер.
`-managedrestart`	**`<полное имя сервера><[другая информация для аутентификации]>`**	Остановите сервер, а затем запустите его.
`-managedforceterminate`	**`<полное имя сервера><[другая информация для аутентификации]>`**	Немедленно останавливает сервер без завершения текущей обработки запросов.
`-enable`	**`<полное имя сервера><[другая информация для аутентификации]>`**	Делает доступным запущенный сервер таким образом, что он регистрируется в системе и ожидает данные с подходящего порта. Используйте полную форму имени сервера.
`-disable`	**`<полное имя сервера><[другая информация для аутентификации]>`**	Блокирует сервер таким образом, что он перестает обрабатывать запросы платформы BI, но остается запущенным в качестве процесса. Используйте полную форму имени сервера.
`-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
>
> 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`	**`<имя_CMS:номер_порта>`**	Укажите CMS, в который следует выполнить вход. Если этот параметр не указан, CCM обращается к локальному компьютеру и порту по умолчанию (6400).
`-username`	**`<имя_пользователя>`**	Укажите учетную запись, предоставляющую административные права для платформы BI. Если запись не указана, по умолчанию применяется учетная запись Администратор.
`-password`	**`<пароль>`**	Укажите соответствующий пароль. Если пароль не указан, применяется пустой пароль. **Примечание** Для указания аргумента `-password` вы должны также указать аргумент `-username`.

CCM прочитывает строки запуска и другие значения конфигурации из файла `ccm.config`.

Связанные сведения

ccm.config [страница 1137]

31.1.1.1.1 Примеры

Эти команды запускают и активируют все серверы платформы BI. Центральный сервер управления (CMS) запускается на локальном компьютере и использует порт по умолчанию (6400):

```
ccm.sh -start all
ccm.sh -enable all
```

Эти команды запускают и активируют все серверы платформы BI. 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 BI 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
```

31.1.1.1.2 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 BI. При изменении командной строки агента Server Intelligence вы обычно редактируете только этот файл. Настоятельно рекомендуется перед редактированием этого файла вручную создать его резервную копию.

Связанные сведения

Обзор командных строк [страница 1144]

31.1.1.2 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 репозиториев входных и выходных файлов. Для получения дополнительных сведений см. раздел «Резервное копирование и восстановление системы». Для получения дополнительных сведений о кластерах CMS и настройке базы данных CMS см. раздел "Кластеризация центральных серверов управления" в главе «Сопровождение сервера» *Руководства администратора платформы SAP BI*.

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`.

Связанные сведения

Кластеризация центральных серверов управления (CMS) [страница 450]
Обзор резервного копирования и восстановления [страница 575]

31.1.1.3 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

31.1.1.3.1 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:

   1. Добавить узел
   2. Удалить узел
   3. Изменить узел
   4. Переместить узел
   5. Резервное копирование конфигурации сервера
   6. Восстановление конфигурации сервера
   7. Изменение конфигурации веб-уровня
   8. 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.

31.1.2 Шаблоны скриптов

31.1.2.1 startservers

Скрипт `startservers` устанавливается в каталог `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj` установки. Этот скрипт может использоваться в качестве шаблона для ваших собственных скриптов: он является примером, показывающим вам, каким должен быть скрипт, запускающий серверы BusinessObjects Enterprise путем выполнения последовательности команд CCM. Для получения дополнительной информации о написании CCM-команд для серверов см. описание скрипта ccm.sh [страница 1133].

31.1.2.2 stopservers

Скрипт `stopservers` устанавливается в каталог `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj` установки. Этот скрипт может использоваться в качестве шаблона для ваших собственных скриптов: он является примером, показывающим вам, каким должен быть скрипт, останавливающий серверы BusinessObjects Enterprise путем выполнения последовательности команд CCM. Для получения дополнительной информации о написании CCM-команд для серверов см. описание скрипта ccm.sh [страница 1133].

31.1.3 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 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).

31.2 Скрипты Windows

В этом разделе описываются все инструменты администрирования и скрипты, включенные в дистрибутив платформы BI для Windows. Основное назначение данного раздела – ссылки. Здесь также изложены основные принципы и процедуры настройки.

Дистрибутив платформы BI для Windows содержит версию Central Configuration Manager (CCM) для Windows. Помимо работы в графическом интерфейсе пользователя для управления серверами можно запускать исполняемый файл CCM в командной строке с соответствующими параметрами.

31.2.1 ccm.exe

Исполняемый файл `ccm.exe` устанавливается в папку `<КАТАЛОГ_УСТАНОВКИ>\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.

> ⓘ Примечание
>
> Аргументы в квадратных скобках [ ] являются необязательными.

> ⓘ Примечание
>
> Аргументы, отмеченные как **`<другая информация для аутентификации>`** , представлены во второй таблице.

Параметр CCM	Допустимые аргументы	Описание
`-help`	недоступно	Отображает справку по командной строке.

Параметр CCM	Допустимые аргументы	Описание
`-managedstart`	`all` или **`<полное_имя_сервера> <[другая_информация_для_аутентификации]>`**	Запустите сервер.
`-managedstop`	`all` или **`<полное_имя_сервера> <[другая_информация_для_аутентификации]>`**	Остановите сервер.
`-managedrestart`	`all` или **`<полное_имя_сервера> <[другая_информация_для_аутентификации]>`**	Остановите сервер, а затем запустите его.
`-managedforceterminate`	`all` или **`<полное_имя_сервера> <[другая_информация_для_аутентификации]>`**	Немедленно останавливает сервер без завершения текущей обработки запросов.
`-enable`	`all` или **`<полное_имя_сервера> <[другая_информация_для_аутентификации]>`**	Делает доступным запущенный сервер таким образом, что он регистрируется в системе и ожидает данные с подходящего порта.
`-disable`	`all` или **`<полное_имя_сервера> <[другая_информация_для_аутентификации]>`**	Блокирует сервер таким образом, что он перестает обрабатывать запросы платформы BI, 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`	**`<cmsname:port#>`**	Укажите CMS, в который следует выполнить вход. Если этот параметр не указан, CCM обращается к локальному компьютеру и порту по умолчанию (6400).
`-username`	**`<имя пользователя>`**	Задает учетную запись, предоставляющую административные права на платформу BI. Если запись не указана, по умолчанию применяется учетная запись Администратор.
`-password`	**`<пароль>`**	Укажите соответствующий пароль. Если пароль не указан, применяется пустой пароль. ⓘ Примечание Для указания аргумента `-password` вы должны также указать аргумент `-username`.
`-authentication`	**`<тип аутентификации>`**	Укажите тип аутентификации. Поддерживается только **`secEnterprise`**.

CCM прочитывает строки запуска и другие значения конфигурации из файла `ccm.config`.

31.2.1.1 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 BI:

```
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
```

31.3 Командные строки сервера

31.3.1 Обзор командных строк

В этом разделе содержится информация о параметрах командной строки, контролирующих поведение каждого сервера платформы BI.

При запуске или настройке сервера с помощью CMC 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 CMC. В справочных целях в этом разделе приводится полный список параметров командной строки, поддерживаемых каждым из серверов. Вы можете изменить непосредственно командную строку каждого из серверов, если хотите дополнительно настроить поведение платформы BI.

Значения, которые приведены в квадратных скобках [ ] в различных частях данного раздела, являются необязательными.

> ⓘ Примечание
>
> В следующих таблицах перечислены поддерживаемые параметры командной строки. Серверы платформы BI используют ряд внутренних параметров, не перечисленных в этих таблицах. Изменять эти внутренние параметры не следует.

31.3.1.1 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.

31.3.2 Стандартные параметры для всех серверов

Эти параметры командной строки применяются ко всем серверам платформы BI, если не указано иное. В оставшейся части данного раздела приведены параметры, особые для каждого типа сервера.

Параметр	Допустимые аргументы	Поведение
`-requestPort`	`<port >`	Укажите порт, на котором сервер выполняет прослушивание. Сервер регистрирует этот порт с помощью CMS. Если значение не указано, сервер выбирает любой свободный порт с номером больше 1024. **Примечание** Этот порт используется разными серверами в различных целях. Перед изменением значения ознакомьтесь с разделом *Руководства администратора платформы BI*, посвященным изменению номеров портов сервера по умолчанию.
`-loggingPath`	`<absolute path>`	Укажите путь, в котором будут создаваться файлы журнала.

31.3.2.1 Обработка сигналов UNIX

В UNIX служебные программы платформы BI 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).

31.3.3 Центральный сервер управления

В этом разделе содержится информация по особым параметрам командной строки, относящимся к CMS. Путь по умолчанию к серверу в ОС Windows: `<КАТАЛОГ_УСТАНОВКИ>\BusinessObjects Enterprise XI 4.0\win64_x64\CMS.exe`.

Путь по умолчанию к серверу в ОС UNIX: `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj/enterprise_xi40/<платформа>/boe_cmsd`.

Параметр	Допустимые аргументы	Поведение
`-threads`	**`<number>`**	Определяет количество рабочих потоков, инициализируемых и используемых CMS. Значение можно выбрать в диапазоне от 12 до 150. По умолчанию используется значение 50.
`-reinitializedb`		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.
`-quit`		При выборе этого параметра CMS принудительно завершит работу после обработки параметра `-reinitializedb` .
`-receiverPool`	**`<number>`**	Задает количество потоков, создаваемых CMS для получения запросов клиентов. Клиентом может быть другой сервер SAP BusinessObjects, мастер публикации отчетов, Crystal Reports или произвольное клиентское приложение, созданное вами. Значение по умолчанию – 5. Как правило, увеличивать данное значение требуется только в том случае, если вы создали произвольное приложение с большим количеством клиентов.
`-maxobjectsincache`	**`<number>`**	Задает 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. Значение по умолчанию – 100000.

Параметр	Допустимые аргументы	Поведение
-ndbqthreads	<number>	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.
-oobthreads	<number>	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 выдержать серьезную нагрузку.

Связанные сведения

Стандартные параметры для всех серверов [страница 1145]

31.3.4 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/<PLATFORM>/boe_cachesd.
- <INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/boe_procd.

Параметр	Допустимые аргументы	Поведение
-cache		Активирует функции кэш-сервера.
-deleteCache		Удаляет каталог кэша при каждом запуске и прекращении работы сервера.
-report_ProcessExtPath	**<absolutepath>**	Указывает каталог по умолчанию для расширений обработки.

Связанные сведения

Стандартные параметры для всех серверов [страница 1145]

31.3.5 Серверы заданий

В этом разделе содержатся сведения о параметрах командной строки для адаптивных серверов заданий.

Путь по умолчанию к серверу в ОС Windows: <КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\JobServer.exe.

Путь по умолчанию к серверу в ОС UNIX: <КАТАЛОГ_УСТАНОВКИ>/sap_bobj/enterprise_xi40/<ПЛАТФОРМА>/boe_jobsd.

Параметр	Допустимые аргументы	Поведение
-dir	**<absolutepath>**	Определяет каталог данных для сервера заданий.
-maxJobs	**<number>**	Задает максимальное количество одновременно выполняемых заданий, которое может обработать сервер. По умолчанию используется значение 5.

Параметр	Допустимые аргументы	Поведение
`-requestJSChildPorts`	**`<lowerbound-upperbound>`**	Определяет диапазон портов, которые должны использовать дочерние процессы в среде брандмауэра. Например, значение `6800-6805` задает для дочерних процессов ограничение в шесть портов. **Примечание** Чтобы данный параметр вступил в силу, необходимо также задать параметр `-requestPort`.
`-report_ProcessExtPath`	**`<absolutepath>`**	Указывает каталог по умолчанию для расширений обработки. Для получения дополнительной информации см. *Руководство администратора платформы SAP BusinessObjects Business Intelligence*.

Связанные сведения

Стандартные параметры для всех серверов [страница 1145]

31.3.6 Адаптивный сервер обработки

Адаптивный сервер обработки использует параметры, определенные для виртуальной машины SAP Java (SAP JVM). Для получения дополнительных сведений см. документацию по SAP JVM.

31.3.7 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: `<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Business Intelligence platform 4.0\win32_x86\crystalras.exe`.

Путь по умолчанию к серверу в ОС UNIX: `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj/enterprise_xi40/<ПЛАТФОРМА>/ras/boe_crystalrasd`.

Параметр	Допустимые аргументы	Поведение
`-ipport`	**`<port>`**	Указывает номер порта для приема запросов TCP/IP при работе в автономном режиме (за пределами платформы BI).
`-report_ProcessExtPath`	**`<absolutepath>`**	Указывает каталог по умолчанию для расширений обработки. Для получения дополнительной информации см. *Руководство администратора платформы SAP BusinessObjects Business Intelligence*.

Параметр	Допустимые аргументы	Поведение
`-ProcessAffinityMask`	`<mask>`	Использует маску, чтобы точно определить ЦП, используемый сервером приложений отчетов при выполнении на многопроцессорном устройстве. Данная маска задана в формате `0xffffffff`, где каждый символ `f` представляет процессор, а список процессоров читается справа налево (т.е. последний символ `f` представляет первый процессор). Каждый символ `f` необходимо заменить либо на 0 (использовать ЦП запрещается), либо на `1` (использовать ЦП разрешается). Например, если сервер приложений отчетов запущен на устройстве с 4 процессорами, и вам необходимо использовать 3-й и 4-й процессоры, используйте маску `0x1100`. Чтобы использовать 2-й и 3-й процессоры, используйте маску `0x0110`. **Примечание** Сервер приложений отчетов использует первый разрешенный процессор в строке вплоть до максимального значения, определяемого лицензией. Если вы обладаете лицензией на два процессора, маска `0x1110` будет действовать так же, как и `0x0110`. **Примечание** Значение маски по умолчанию равно `-1`, что равносильно значению `0x1111`.

Связанные сведения

Стандартные параметры для всех серверов [страница 1145]

31.3.8 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: `<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\WIReportServer.exe`.

Путь по умолчанию к серверу в ОС UNIX: `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj/enterprise_xi40/<ПЛАТФОРМА>/WIReportServer`.

Параметр	Допустимые аргументы	Поведение
-ConnectionTimeout Минуты	**<minutes>**	Определяет количество минут, по истечении которых сервер переходит в режим ожидания.
-MaxConnections	**<number>**	Определяет максимальное количество одновременных соединений, разрешенных сервером.
-DocExpressEnable		Активирует кэширование документов Web Intelligence при их просмотре.
-DocExpressRealTime CachingEnable		Активирует кэширование документов Web Intelligence в режиме реального времени.
-DocExpressCache DurationMinutes	**<minutes>**	Определяет количество времени (в минутах), в течение которого содержимое сохраняется в кэше.
-DocExpressMaxCache SizeKB	**<kilobytes>**	Определяет размер кэша для документов.
-EnableListOfValues Cache		Активирует кэширование списка значений для каждого сеанса пользователя.
-ListOfValuesBatchSize	**<number>**	Определяет максимальное количество значений, возвращаемых на пакет списка значений.
-UniverseMaxCacheSize	**<number>**	Определяет максимальное количество юниверсов для сохранения в кэше.

Параметр	Допустимые аргументы	Поведение
-WIDMaxCacheSize	**<number>**	Определяет максимальное количество документов Web Intelligence для сохранения в кэше.

Связанные сведения

Стандартные параметры для всех серверов [страница 1145]

31.3.9 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: `<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\fileserver.exe`

Путь по умолчанию к программе, предоставляющей оба сервера в ОС UNIX: `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj/enterprise_xi40/<платформа>/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
`-rootDir`	**`<absolutepath>`**	Задает корневой каталог для различных каталогов нижележащего уровня и файлов, управляемых сервером. Пути к файлам, используемые для ссылки на файлы на файловом сервере репозитория, интерпретируются по отношению к данному корневому каталогу. **Примечание** Все серверы репозитория входящих файлов должны использовать один и то 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.

Параметр	Допустимые аргументы	Поведение
`-tempDir`	**`<absolutepath>`**	Задает 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). **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.
`-maxidle`	**`<minutes>`**	Определяет количество минут, по истечении которого выполняется очистка бездействующего сеанса.
`-legacymode`		Разрешает полный доступ к платформе BI для более ранних версий SDK или клиентов с версией выпуска ранее 4.0.
`-vsaFileLoc`	**`<absolutepath>`**	Укажите абсолютный путь к файлу библиотеки адаптера для сканирования вирусов. **Примечание** Все серверы репозитория входящих файлов должны использовать один и тот же корневой каталог, и все серверы репозитория исходящих файлов также должны использовать один и тот же корневой каталог (во избежание проблемы противоречивости экземпляров).

Связанные сведения

Стандартные параметры для всех серверов [страница 1145]

31.3.10 Сервер событий

В этом разделе содержится информация по особым параметрам командной строки, относящимся к серверу событий.

Путь по умолчанию к серверу в ОС Windows: `<КАТАЛОГ_УСТАНОВКИ>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\EventServer.exe`.

Путь по умолчанию к серверу в ОС Unix: `<КАТАЛОГ_УСТАНОВКИ>/sap_bobj/enterprise_xi40/<платформа>/boe_eventsd`.

Параметр	Допустимые аргументы	Процедура
`-cleanup`	**`<minutes>`**	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.

Связанные сведения

Стандартные параметры для всех серверов [страница 1145]

32 Repository Diagnostic Tool

32.1 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 три 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.
- Несоответствия в отношениях.
  Несоответствия возникают, когда между двумя инфо-объектами существует отношение, но один из них был удален. Обрабатываются только отношения EnterpriseNode-Server, Service-Server, ServiceContainer-Server.

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.

32.2 Использование Repository Diagnostic Tool

Repository Diagnostic Tool (RDT) доступен на любом компьютере, на котором установлен диспетчер CCM. 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 BI приостановлены. 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.

32.2.1 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>` – список параметров, которые требуется указать.

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>` – «linux64_x64», «solaris_sparcv9», «hpux_ia64» или «aix_rs6000_64» и `<arguments>` – список параметров, которые требуется указать.

> **Примечание**
>
> При вводе параметров командной строки Unix может требоваться экранировать специальные символы оболочки (один или несколько раз). Например, если в пароле используется восклицательный знак («!»), может потребоваться экранировать его следующим образом: `./ccm.sh -display -username Administrator -password Abc\!defgh123 -cms cmsname`.

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>\SAP 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 `./sap_bobj/enterprise_xi40/reposcan` в системе Unix

Для получения списка сообщений с предупреждениями и рекомендуемых действий, предпринимаемых инструментом RDT при нахождении противоречий, см. разделы *Противоречия в метаданных CMS* и *Противоречия CMS и FRS*.

Связанные сведения

Несоответствия в метаданных CMS [страница 1170]
Несоответствия между CMS и FRS [страница 1169]

32.2.2 Параметры Repository Diagnostic Tool

Repository Diagnostic Tool принимает параметры, указанные в следующей таблице:

> **Примечание**
>
> Аргументы командной строки переопределяют любые записи файла параметров при выполнении.

> **Примечание**
>
> Опции параметров базы данных SAP HANA см. в SAP-ноте 1916845.

Общие параметры

Параметр	Дополнительный или обязательный	Описание
`dbdriver`	Обязательный	Тип драйвера, используемого для подключения к базе данных CMS. Допустимы следующие значения: • `db2databasesubsystem` • `maxdbdatabasesubsystem` • `mysqldatabasesubsystem` • `oracledatabasesubsystem` • `sqlserverdatabasesubsystem` • `sybasedatabasesubsystem` • `sqlanywheredatabasesubsystem`
`connect`	Обязательный	Сведения о соединении, которые используются для подключения к базе данных CMS. Например: `-connect "UID=root;PWD=<password>;DSN=<dsn>;HOSTNAME=<hostname>;PORT=<portnumber>"`

Параметр	Дополнительный или обязательный	Описание
`dbkey`	Обязательный	Введите ключ кластера для развертывания платформы BI. Если ключ кластера неизвестен, его можно сбросить, выполнив следующие операции: **Примечание** 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. 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 SIA не изменится на «Остановлен». 3. Щелкните SIA правой кнопкой мыши и выберите команду *Свойства*. 4. На вкладке "Конфигурация" щелкните 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 ключ, состоящий из восьми символов, в поле *Новый ключ кластера*, и повторите ввод в поле *Подтвердить новый ключ кластера*. **Примечание** Средство RDT не будет запущено, если пропущен параметр `dbkey` или если ключ кластера неправильный. **Примечание** Ключ кластера, отображаемый в CCM, зашифрован и не может быть использован в параметре `dbkey`. Дополнительные сведения о ключах кластера см. в разделе «Безопасность платформы BI» в *руководстве администратора платформы SAP BusinessObjects Business Intelligence*.

Параметр	Дополнительный или обязательный	Описание
`inputfrsdir`	Обязательный	Путь к файлу сервера репозитория входящих файлов. **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.
`outputfrsdir`	Обязательный	Путь к файлу сервера репозитория исходящих файлов. **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.
`outputdir`	Дополнительно	Путь к файлу, в который Repository Diagnostic Tool записывает файлы журнала. Значение по умолчанию: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\reposcan` в системе Windows и `./sap_bobj/enterprise_xi40/reposcan` в системе Unix.
`count`	Дополнительно	Количество примерных ошибок для сканирования. Это помогает обеспечить оптимальную производительность. Максимальное значение: 2e31 - 1. Значение, равное 0, указывает на репозиторий целиком. Значением по умолчанию является 1000.

Параметр	Дополнительный или обязательный	Описание
`repair`	Дополнительно	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. ⚠ Предупреждение В рамках этого процесса из базы данных репозитория удаляются любые объекты или файлы с утраченными связями.
`scanfrs`	Дополнительно	Указывает на то, следует ли Repository Diagnostic Tool выполнять сканирование CMS и FRS на наличие несоответствий.
`scancms`	Дополнительно	Указывает на то, следует ли Repository Diagnostic Tool выполнять сканирование CMS на наличие несоответствий между объектами InfoObjects.
`submitterid`	Дополнительно	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. Этот параметр используется только при работе Repository Diagnostic Tool в режиме исправления.
`startid`	Дополнительно	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. Значением по умолчанию является **`1`**.

Параметр	Дополнительный или обязательный	Описание
`optionsfile`	Дополнительно	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. **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.
`syscopy`	Дополнительно	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. Этот может быть использован только с базовыми параметрами и не должен использоваться вместе с другими дополнительными параметрами из данного списка. **Примечание** Не запускайте средство RDT, если в исходной системе указан параметр `syscopy`.
`trace`	Дополнительно	Этот параметр создает трассировки (записи событий, которые происходят во время работы контролируемого компонента) и собирает их в файлах журнала с расширением .glf в следующей папке: `<SAP_BOBJ_INST_DIR>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\logging`

Параметр	Дополнительный или обязательный	Описание
`scankind`	Дополнительно	Введите вид InfoObject, который необходимо сканировать на наличие несоответствий. **Пример** SI_KIND - отчеты Web Intelligence, отчеты Crystal В перечень поддерживаемых InfoObject, которые можно сканировать на наличие несоответствий, входят следующие: • folder (папка) • crystalreport (отчет Crystal) • shortcut (ярлык) • user (пользователь) • usergroup (группа пользователей) • calendar (календарь) • connection (соединение) • category (категория) • objectpackage (пакет объекта) • publication (публикация) • pdf • rtf • txt • note (примечание) • word • excel • tenant (клиент) • profile (профиль) • program (программа) • agnostic (агностический) • universe (юниверс) • hyperlink (гиперссылка) • fullclient • powerpoint • scopebatch • metadata.dataconnection • webi • qaaws • lcmjob

Параметр	Дополнительный или обязательный	Описание
		• overload • xcelsius • biwidgets • mon.probe • liveoffice • mdanalysis • visualdiff • ao.workbook • dsl.metadatafile • afdashboardpage • ao.presentation • ccis.dataconnection • platformsearchqueue • metadata.businessview • platformsearchindex • platformsearchcontentstore • platformsearchcontentsurrogate **Примечание** В файле вывода XML по видам сканирования отображается список несоответствий по InfoObject. Другими словами, затронутые объекты файлов не включаются в список.
`scandays`	Дополнительно	Введите количества дней для выполнения проверки RepoScan на наличие несоответствий. **Пример** Это может быть любое реальное число, кроме 0. **Примечание** Этот параметр зависит от текущего системного времени.

Отношения не сканируются во время частичных сканирований. Частичное сканирование происходит, если используется один из трех следующих параметров:

- startid
- scankind
- scandays

Несоответствия в отношениях

Предупреждающее сообщение	Несоответствие	Рекомендация	Действие
`Relation '<Name>' from object ID <ID> has an invalid target (Object ID = <ID>)`	Граница отношения больше не существует.	Разрешить приложению удалить отношение.	Отношение удалено.

Следующие параметры используются, если в активном кластеризованном CMS выполняется средство Repository Diagnostic Tool.

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.

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 для системы Windows 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
```

Пример

Пример в системе Unix:

```
./boe_reposcan.sh
-dbdriver oracledatabasesubsystem
-connect "UID=<bi_admin>;PWD=<Password1>;DSN=<myDsn>;PORT=<6400>"
-inputfrsdir /apps/frs/bi/frsinput
-outputfrsdir /apps/frs/bi/frsoutput
-dbkey <cluster key>
```

32.3 Несоответствия между CMS и FRS

В следующей таблице приведены несоответствия, которые могут возникнуть между базой данных центрального сервера управления (CMS) и серверами репозиториев файлов (FRS) и которые распознаются инструментом Repository Diagnostic Tool.

- 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 не имеет соответствующего файла на сервере FRS.	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 не имеет соответствующего файла в базе данных CMS.	Разрешить приложению удалить файл, на который отсутствуют ссылки.	Действия не предпринимаются.
<Тип объекта> Объект <Имя объекта>(идентификатор объекта = <Ид.>) содержит файл <Имя файла>. 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.

32.4 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).

- 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.
- Action
  Действие Repository Diagnostic Tool по исправлению несоответствия. Это действие обозначено в файле журнала исправлений.

Предупреждающее сообщение	Несоответствие	Рекомендация	Действие
Для объекта `<Тип объекта> <Имя объекта>` (Идентификатор объекта = `<ID>`) отсутствует родительский объект (Идентификатор родительского объекта = `<ID>`).	Для 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".
Для объекта `<Тип объекта> <Имя объекта>` (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.
Для объекта `<Тип объекта> <Имя объекта>` (Идентификатор объекта = `<ID>`) отсутствует объект-предъявитель (Идентификатор объекта-предъявителя = `<ID>`).	Для объекта отсутствует идентификатор объекта-предъявителя или идентификатор недействителен.	Рекомендация, отображаемая Repository Diagnostic Tool, зависит от того, заданы ли значения для параметра `-submitterid`. • Если значение задано, рекомендация звучит как «Разрешить приложению обновить объект с учетом	Если значение параметра `-submitterid` указано, средство RDT использует это значение в качестве идентификатора предъявителя объекта. Если значение параметра не указано, Repository Diagnostic Tool не выполняет никаких действий. При перепланировании

Предупреждающее сообщение	Несоответствие	Рекомендация	Действие
		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».	объекта CMS использует новый идентификатор.
Свойство последнего успешного экземпляра объекта `<Тип 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.
Для объекта `<Тип 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.
Для объекта `<Тип 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.
Список ожидающих событий объекта `<Тип объекта> <Имя объекта>` (Идентификатор объекта = `<ID>`) содержит	Одно или несколько ожидаемых объектом событий не существуют.	Перезапланируйте объект, чтобы он ожидал существующих объектов событий. Приложение не	Действия не предпринимаются.

Предупреждающее сообщение	Несоответствие	Рекомендация	Действие
отсутствующие объекты (Идентификаторы объектов событий = <ID>).		может выполнить какие-либо действия.	
Список инициируемых событий объекта <Тип объекта> <Имя объекта> (Идентификатор объекта = <ID>) содержит отсутствующие объекты (Идентификаторы объектов событий = <ID>).	Объект инициирует несуществующее событие.	Разрешить приложению удалить отсутствующие события из списка инициируемых событий.	Отсутствующие события удалены из списка инициируемых событий приложения.
Список контроля доступа объекта <Тип объекта> <Имя объекта> (Идентификатор объекта = <ID>) ссылается на отсутствующего принципала (Идентификатор объекта принципала = <ID>).	Для записи управления доступом отсутствует принципал.	Разрешить приложению удалить отсутствующие принципалы из списка контроля доступа объекта.	Отсутствующий принципал удален из списка контроля доступа объекта.
Список контроля доступа объекта <Тип объекта> <Имя объекта> (Идентификатор объекта = <ID>) ссылается на отсутствующий уровень доступа (Идентификатор объекта уровня доступа = <ID>).	Для записи управления доступом отсутствует принципал.	Разрешить приложению удалить отсутствующий уровень доступа из списка контроля доступа объекта.	Отсутствующий уровень доступа удален из списка контроля доступа объекта.
Объект <Тип объекта> <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.
Объект <Тип объекта> <Имя объекта> (Идентификатор объекта = <ID>) содержит недопустимые записи входных файлов (<Файлы>).	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.
Объект <Тип объекта> <Имя объекта> (Идентификатор объекта = <ID>) содержит недопустимые записи выходных файлов (<Файлы>).	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.

Предупреждающее сообщение	Несоответствие	Рекомендация	Действие
Для объекта `<Тип 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.
Для объекта `<Тип 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.
Список профилей объекта `<Тип объекта> <Имя объекта>` (Идентификатор объекта = `<ID>`) содержит отсутствующие объекты (Идентификаторы объектов профиля = `<ID>`).	В списке профилей объекта содержатся отсутствующие объекты.	Обновите публикацию с использованием существующих профилей. Приложение не может выполнить какие-либо действия.	Действия не предпринимаются.

32.5 Управление SDK Restful в веб-приложении BOE

Чтобы активировать веб-приложение BIPRWS веб-приложения BOE в версии 4.3 SP03, установите флажок на *true* в следующем расположении:

```
<BOE_INST_DIR>\SAP BusinessObjects\tomcat\webapps\BOE\WEB-INF\internal\Global.properties
```

Установить `use.boe.internal.biprws=true`

Если этот флаг установлен на true, внутренние приложения не зависят от URL-адреса приложения Restful или флага относительного пути, установленного в CMC.

Эта функция удобна, так как позволяет избежать следующего:

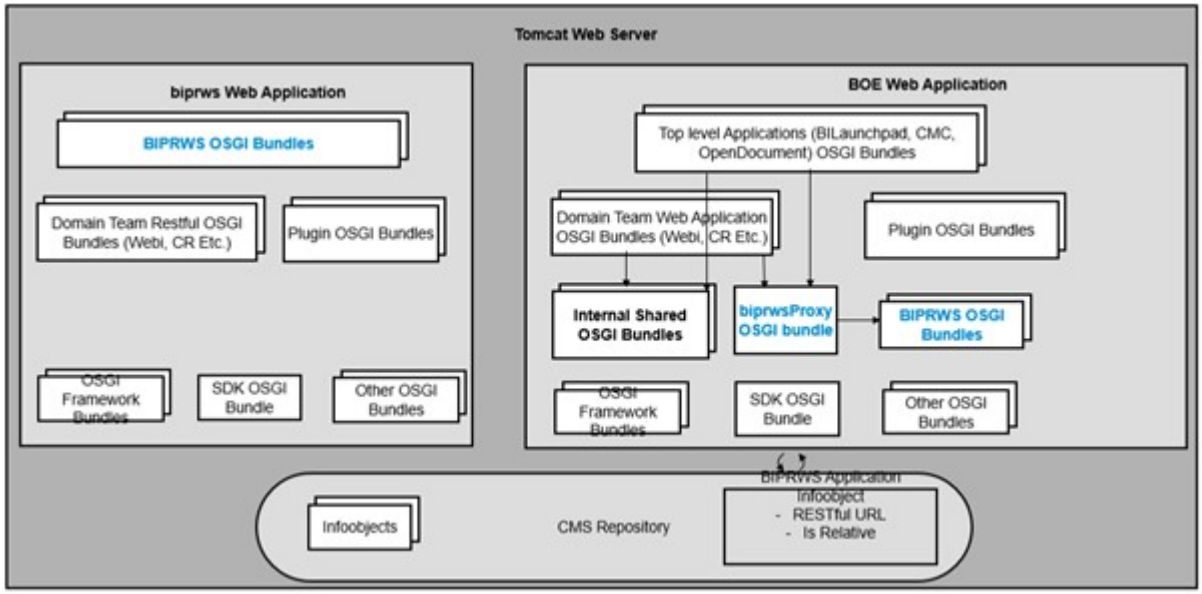
- Проблемы CORS (совместное использование ресурсов из нескольких источников)
- Проблемы с подключением внутренних и внешних систем
- Проверка ping веб-приложения BOE для поддержки соединения в сеансе
- Проблемы, связанные с прокси, поскольку для BIPRWS и BOE нет отдельной конфигурации.
- Проблемы, связанные с кластером веб-приложений.

Существующее развертывание с веб-приложением BOE работает без проблем после обновления.

Регистрация:

После объединения BIPRWS с веб-приложением BOE журналы создаются в рамках расположения журнала стартовой панели BI или приложения CMC.

Архитектура:



33 HTTP Strict Transport Security (HSTS)

33.1 Настройка HTTP Strict Transport Security (HSTS)

HTTP Strict Transport Security (HSTS) – это механизм политики для защиты веб-сайтов от атак через посредника, таких как атаки с понижением версии протокола и перехват файлов cookie.

Он позволяет веб-серверам объявлять, что веб-браузеры (или другие соответствующие агенты пользователей) должны автоматически взаимодействовать с ним только с использованием HTTPS-соединений. Это обеспечивает Transport Layer Security (TLS/SSL), в отличие от небезопасного использования HTTP.

HSTS является протоколом отслеживания стандартов IETF и указан в RFC 6797.

Политика HSTS передается сервером агенту пользователя через поле заголовка ответа HTTP "Strict-Transport-Security".

1. Эта политика определяет период, в течение которого агент пользователя должен осуществлять доступ к серверу только в безопасном режиме.
2. Веб-сайты, использующие HSTS, часто не принимают открытый текст HTTP, либо отклоняя соединения по HTTP, либо систематически перенаправляя пользователей на HTTPS (хотя это не требуется спецификацией).
   Это позволяет гарантировать, что агент пользователя, не способный обеспечить TLS, не сможет соединиться с сайтом.
3. Защита применяется только после того, как пользователь хотя бы один раз посетил сайт, на основании принципа доверия по первому использованию.

Принцип работы

Когда пользователь вводит или выбирает URL-адрес сайта, на котором указан HTTP, URL-адрес автоматически обновляется на HTTPS без запроса HTTP. Это предотвращает возникновение атаки HTTP через посредника.

В версии 4.3 SP03 SAP BOE поддерживает соглашение о поддержке HSTS.

Перед настройкой HSTS необходимо настроить сервер приложений с SSL.

Чтобы включить поддержку HSTS, выполните следующие шаги:

1. Остановите сервер Tomcat.
2. Перейдите к `C:\Program Files (x86)\SAP BusinessObjects\tomcat\webapps\BOE\WEB-INF\config\default`
3. Откройте файл Global.properties и установите следующие параметры.
   1. `hsts.enabled` True/False. По умолчанию установлено значение false.
   2. `hsts.Include.SubDomains` True /False – влияет на все поддомены имени домена.
   3. `hsts.MaxAge.Seconds` = 31536000.
   4. По умолчанию = 365 дней.
4. Сохраните изменения.

34 Приложение "Права"

34.1 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 BI*.

34.2 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.
Добавление объектов 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.
Изменение объектов	Позволяет изменять содержимое объекта и свойства объектов и папок.

Право	Описание
Изменение прав пользователей на объекты	Позволяет изменить настройки безопасности объекта.
Изменение прав пользователей на объекты в безопасном режиме	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» *руководства администратора платформы SAP BusinessObjects Business Intelligence*.
Определить 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.
Удаление объектов	Позволяет удалить объекты и их экземпляры.
Копирование объектов 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.
Тиражирование содержимого	Позволяет тиражировать объекты в другую систему интегрированного развертывания.
Составление расписания для запуска документа	Позволяет планировать объекты.
Планирование от имени других пользователей	Позволяет планировать объекты для других пользователей и групп. Пользователи или группы, для которых выполняется планирование объекта, становятся владельцами экземпляра этого объекта. Для планирования объекта для других пользователей или групп также необходимы следующие права: • Данное право по отношению к пользователю или группе. • Право *Составить расписание для запуска документа* по отношению к объекту.

Право	Описание
Составление расписания для адресатов	*Составление расписания для адресатов* является родительским правом для прав *Расписание для FTP, SMTP, SFTP, каталога входящих* и *Файловая система*. Для планирования объекта для конкретного адресата следует выбрать право *Составление расписания для адресатов* в сочетании с определенным дочерним правом. Например, для планирования объекта для адресата FTP следует выбрать права *Составление расписания для адресатов* и *Расписание для FTP*. Если выполняется обновление ландшафта BI с BI 4.2 SP04 или более ранней версии до BI 4.2 SP05 или выше, для получения дополнительных сведений об устранении неполадок см. 2675734, 2642221, 2626550. Для планирования объекта для адресатов также необходимы следующие права: • 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). **Примечание** Если право *Составление расписания для адресатов* присваивается через *уровень доступа*, например роли *Полный контроль* или *Расписание* в BI 4.2 SP04 или выше, то после обновления до BI 4.2 SP05 с исправлением 03 или выше также предоставляются дочерние права для адресатов, такие как *Расписание для FTP, SMTP, SFTP, каталога входящих* и *Файловая система*. Для *уровней доступа*, таких как *Просмотр по требованию* и существующие *пользовательские* роли в BI 4.2 SP04 или более ранней версии, то после обновления до BI 4.2 SP05 с исправлением 03 или выше дочерние права для назначения по умолчанию не предоставляются. Права следует предоставить вручную. Поэтому периодическое задание планирования, созданное в BI 4.2 SP04 или более ранней версии, будет успешно планировать объекты в BI 4.2 SP05 с исправлением 03 или выше.
Запланировать для FTP	Позволяет планировать отправку объекта в место назначения FTP.

Право	Описание
Запланировать для SFTP	Позволяет планировать отправку объекта в место назначения SFTP.
Запланировать для SMTP	Позволяет планировать отправку объекта в место назначения SMTP.
Запланировать для файловой системы	Позволяет планировать отправку объекта в место назначения "Файловая система".
Запланировать для папки "Входящие"	Позволяет планировать отправку объекта в место назначения "Папка входящих BI".
Просмотр экземпляров документа	Позволяет просматривать экземпляры объекта. Это право является базовым и требуется для выполнения всех задач в отношении экземпляров объектов.
Удаление экземпляров	Позволяет удалять только экземпляры объектов. Если у вас есть право *Удалить объекты*, вам необязательно иметь это право, чтобы удалить экземпляры.
Приостановка и возобновление выполнения экземпляров документа	Позволяет приостановить и возобновить выполнение экземпляров объекта.
Повторное планирование экземпляров	Позволяет повторно составить расписание для экземпляров объекта.
Добавить комментарии — BI Commentary	Позволяет пользователю добавить комментарии в документ, используя BI Commentary.
Удалить комментарии — BI Commentary	Позволяет пользователю удалить комментарии из документа, используя BI Commentary.
Удалить созданные пользователем комментарии — BI Commentary	Позволяет пользователю удалить созданные им комментарии из документа, используя BI Commentary.
Изменить комментарии — BI Commentary	Позволяет пользователю изменить комментарии в документе, используя BI Commentary.
Изменить созданные пользователем комментарии — BI Commentary	Позволяет пользователю изменить созданные им комментарии в документе, используя BI Commentary.
Просмотреть комментарии — BI Commentary	Позволяет пользователю просматривать комментарии в документе, используя BI Commentary.

Право	Описание
Просмотреть созданные пользователем комментарии — BI Commentary	Позволяет пользователю просматривать созданные им комментарии в документе, используя BI Commentary.
Скрыть комментарии – BI Commentary	Позволяет пользователю скрывать комментарии в документе, используя BI Commentary.
Скрыть созданные пользователем комментарии – BI Commentary	Позволяет пользователю скрывать созданные им комментарии в документе, используя BI Commentary.
Массовое добавление комментариев — BI Commentary	Предоставляет пользователю возможность переносить комментарии вместе с документом.

34.2.1 Права назначения

Каждое место назначения связано с определенным правом назначения. Администратор BOE должен убедиться в наличии у пользователей всех требуемых прав назначения.

Ранее пользователь с правом *Расписание по адресатам* мог составить расписание для всех доступных мест назначения. Начиная с версии SP05, пользователям, у которых параметру *Расписание по адресатам* соответствует только *Местоположение Enterprise по умолчанию*, предоставляются права на отдельные места назначения.

В разделе "Общие права" для каждого места назначения теперь предусмотрены новые отдельные права:

- Расписание для файловой системы
- Расписание для FTP
- Расписание для папки "Входящие"
- Расписание для SFTP
- Расписание для SMTP
- Расписание для Google Диск

Для получения дополнительных сведений об *общих правах* см. Общие права [страница 1176].

Для предоставления этих параметров назначения во время планирования администратор должен присвоить соответствующие индивидуальные права для мест назначения. См. 2621878. Если для пользователя установлено только право *Расписание по адресатам*, он не может составлять расписание для FTP, папки "Входящие", SFTP, SMTP и файловой системы.

Если право *Расписание по адресатам* присваивается в более ранней версии через уровень доступа, например в роли "Полный контроль" или "Расписание", то после обновления до версии 4.2 SP05 пользователям также предоставляются дополнительные (недавно введенные) права. Таким образом, предоставляется возможность составлять расписание по всем местам назначения (адресатам).

Если право присваивается через уровень доступа *Просмотр по требованию*, любую пользовательскую роль или напрямую (отдельное право, не через роль), то расписание составляется только для значения *Местоположение Enterprise по умолчанию*, расписание для остальных мест назначения недопустимо.

Для получения дополнительных сведений см. Параметры места назначения и Свойства адресатов электронной почты

34.3 Права для определенных типов объектов

34.3.1 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).

34.3.2 Категории

В данном разделе рассматриваются общие права, которые имеют особое значение в контексте их принадлежности к общим или персональным категориям.

> ⓘ Примечание
>
> Объекты в категориях не наследуют права, заданные для категорий.

Право	Описание
Добавить объекты в каталог	Позволяет создавать в категориях новые категории. Это право не требуется для добавления объектов в категорию.
Редактировать объекты	Позволяет выполнять следующие действия: • Изменять свойства категорий. • Помещать одну категорию в другую в качестве подкатегории. • Добавлять объекты в категорию. • Удалять объекты из категории. Для помещения одной категории в другую в качестве подкатегории требуются также следующие права: • Право *Удалить объекты* по отношению к исходной категории.

Право	Описание
	• Право *Добавить объекты в каталог* по отношению к категории назначения.
Удалить объекты	Позволяет удалить категорию.

34.3.3 Отчеты Crystal

Права, рассмотренные в данном разделе, применимы только к отчетам Crystal.

> ⓘ Примечание
>
> Эти права применимы, только если отчеты Crystal находятся в среде платформы BI. При загрузке отчетов Crystal на локальный диск эти права не действуют. Во избежание таких ситуаций вы можете отказать в праве *Загрузить файлы, связанные с данным объектом* по отношению к отчету Crystal.

Право	Описание
Печать данных отчета	Позволяет распечатать отчет.
Обновить данные отчета	Позволяет обновить данные отчета.
Экспортировать данные отчета	Позволяет экспортировать данные отчета в любой формат при просмотре отчета в Интернете, используя средство просмотра Crystal Reports. Для экспорта данных отчета в формат RPT также необходимо иметь право *Загрузить файлы, связанные с данным объектом*.
Загрузить файлы, связанные с данным объектом	Данное право позволяет выполнять следующие действия: • Экспортировать отчет в формат RPT. • Открывать отчет в конструкторе Crystal Reports. • Планировать отчет формата RPT для внешних адресатов.

34.3.4 Документы Web Intelligence

Права, рассмотренные в данном разделе, применимы только к документам Web Intelligence.

Право	Описание
Использовать списки значений	Позволяет использовать списки значений.

Право	Описание
Экспортировать данные отчета	Позволяет экспортировать данные отчетов в формат TXT, CSV, Excel, PDF или HTML. Эта команда также позволяет использовать команду "Печать", генерирующую PDF-файл, который можно распечатать.
Скрипт запроса – включить просмотр (SQL, MDX...)	Позволяет просматривать скрипты запросов (SQL и MDX).
Скрипт запроса – включить изменение (SQL, MDX...)	Позволяет редактировать скрипты запросов (SQL и MDX). Кроме того, можно редактировать источники данных Free-hand SQL (FHSQL).
Обновить данные отчета	Позволяет обновлять данные документа.
Изменить запрос	Позволяет редактировать запросы в документе.
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.
Отправить	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.

34.3.5 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.

> ⓘ Примечание
>
> Создатель учетной записи пользователя считается ее владельцем. Однако пользователь, для которого создана учетная запись, также считается ее владельцем.

Право	Описание
Изменение объектов	Позволяет выполнять следующие действия: • Изменить свойства пользователя или группы. • Управлять принадлежностью к группе. Для добавления пользователя или группы в другую группу необходимо иметь это право по отношению к пользователю или группе и по отношению к группе-адресату.
Изменить пароль пользователя	Позволяет выполнять следующие действия: • 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. **Примечание** Это право не влияет на следующие настройки пароля пользователя: *Пароль не ограничен по сроку действия* *Пользователю следует изменить пароль при следующем входе в систему* *Пользователь не может изменить пароль* **Примечание** Это право неприменимо к учетным данным для доступа к источнику данных юниверсов SAP BusinessObjects.
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	Позволяет изменять значение адреса электронной почты пользователя или настраиваемые атрибуты пользователя. Это право применяется к пользователям.

Право	Описание
Добавить или изменить атрибуты пользователя (право владельца)	Позволяет владельцу объекта пользователя изменять адрес электронной почты пользователя или настраиваемые атрибуты пользователя. Это право применяется к пользователям.
Изменение предпочтений для объектов, владельцем которых является пользователь	Отображает меню *Предпочтения* в объекте приложения Без этого права доступа пользователь не может выставлять личные предпочтения в приложениях и меню "Предпочтения" не будет отображаться в приложениях. Например, без этого права пользователи не могут выбирать единицы измерения (дюймы или миллиметры), которые следует использовать в отчетах в Web Intelligence или приложении стартовой панели BI.

34.3.6 Уровни доступа

Права, рассмотренные в данном разделе, применимы только к уровням доступа.

Право	Описание
Использовать уровень доступа для назначения защиты	Позволяет установить уровень доступа при добавлении принципалов в списки управления доступом к объектам. Для этого также требуется иметь право *Изменение прав пользователей на объекты* или право *Безопасное изменение прав пользователей на объекты* по отношению к принципалу и объекту. В случаях предоставления права *Безопасное изменение прав пользователей на объекты* вы также должны иметь тот же уровень доступа по отношению к объекту.

34.3.7 Права юниверсов (.unv)

Права, описанные в этом разделе, применимы к юниверсам, созданным в средстве создания юниверсов – юниверсам .unv. Перечисленные права являются зависимыми от типа правами, применимыми только к юниверсам, или общими правами, имеющими особое значение в контексте юниверсов.

> ⓘ Примечание
>
> Права на доступ к юниверсам применимы только при импорте юниверсов из CMS в приложение средства создания юниверсов. Эти права не применяются при сохранении юниверса на локальный диск.

Право	Описание
Добавить объекты в каталог	Позволяет добавить наборы ограничений или объекты в юниверс. Для этого также необходимо иметь право *Редактировать ограничения по доступу*.
Просмотр объектов	Обеспечивает доступ к юниверсу и возможность его просмотра.
Редактировать объекты	Данное право позволяет выполнять следующие действия: • Изменять юниверс в CMC или в средстве создания юниверсов. • Устанавливать или снимать блокировку юниверса. Для разблокирования юниверса вам также необходимо иметь право *Разблокировать юниверс*.
Удалить объекты	Позволяет удалять юниверс.
Транслировать объекты	Позволяет сохранять переведенные имена объектов юниверса, используя средство управления переводами. **Примечание** Переводы также можно сохранять при явно предоставленном праве *Редактировать объекты*, если нет явного отказа в праве *Транслировать объекты*.
Новый список значений	Данное право позволяет выполнять следующие действия: • Сопоставлять объектам новые списки значений. • Редактировать существующие списки значений. **Примечание** Это право не лишает вас возможности создавать каскадные списки значений.
Печать юниверса	Позволяет распечатать юниверс.
Отображать значения таблицы или объекта	Позволяет видеть значения, связанные с таблицами или объектами в юниверсе.
Редактировать ограничения по доступу	Позволяет редактировать ограничения по доступу к юниверсу.
Разблокировать юниверс	Позволяет выполнять следующие действия:

Право	Описание
	• Разблокировать юниверс, если он был заблокирован другим пользователем. • Экспортировать юниверс из CMS. Для разблокирования юниверса также требуется право *Редактировать объекты*.
Доступ к данным	Позволяет извлекать данные из юниверса и обновлять документы на основе юниверса. Для этого вам необходимо иметь это право также по отношению к приложению средство создания юниверсов, документу и соединению юниверса.
Создание и редактирование запросов на основе юниверса	Позволяет создавать документы и редактировать запросы, основанные на юниверсе.

34.3.8 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	Позволяет извлекать опубликованный юниверс и изменять его основные ресурсы (бизнес-уровень и основание данных) в средстве дизайна информации. **Примечание** Для этого также требуется следующее право приложения средства дизайна информации: *Извлечь юниверс*.

Право	Описание
Изменить профили безопасности	Позволяет вставлять, изменять и удалять профили безопасности для юниверса в редакторе безопасности средства дизайна информации. **Примечание** Это право не является обязательным для просмотра профилей безопасности или изменения параметров агрегирования профиля безопасности.
Назначить профили безопасности	Позволяет назначать и отменять назначение профилей безопасности для пользователей и групп в редакторе безопасности средства дизайна информации.
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*.

34.3.9 Уровни доступа к объектам для юниверсов

Дизайнеры при создании юниверса в средстве создания юниверсов или бизнес-уровня в средстве дизайна информации выполняют назначение уровня доступа к объекту для каждого объекта в юниверсе. Имеются следующие уровни доступа к объектам:

Общий (по умолчанию)
Управляемый
С ограничениями
Конфиденциальный
Частный

После публикации юниверса в репозитории можно предоставлять доступ к объектам юниверса на основе уровней доступа к объектам, назначенным в приложении. Например, можно предоставить группе "Все" доступ "Общий". При этом пользователям группы "Все" предоставляется возможность видеть объекты в юниверсе, обозначенные как "Общий".

Каждый последующий уровень доступа к объектам предоставляет больший доступ к объектам, чем предыдущий. "Общий" является самым низшим уровнем. Для принципалов с доступом "Общий" возможен только просмотр объектов с назначением "Общий". Для принципалов с доступом "Управляемый" возможен просмотр объектов с назначением "Общий" и "Управляемый". Наивысшим уровнем является "Частный". Он предоставляет принципалам доступ ко всем уровням доступа к объектам, т. е. ко всем объектам в юниверсе.

> ⓘ Примечание
>
> Настройки безопасности на уровне доступа к объекту переопределяют все наследуемые юниверсом настройки безопасности.

> ⓘ Примечание
>
> Для юниверсов .unx 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*.

Связанные сведения

Назначение уровней доступа к объектам для юниверсов [страница 1189]

34.3.9.1 Назначение уровней доступа к объектам для юниверсов

Для установки защиты на уровне доступа к объектам для юниверсов вам необходимо иметь право *Изменение прав пользователей на объекты* по отношению к юниверсу.

1. Выберите юниверс в области *Юниверсы* центрального сервера управления.
2. Выберите *Действие* > *Безопасность юниверса*.
3. В диалоговом окне *Безопасность юниверса* для пользователя или группы выберите уровень доступа к объектам в списке *Уровень безопасности объектов*.

34.3.10 Права соединений

В данном разделе рассматриваются права, которые применимы только к соединениям юниверсов, или общие права, которые имеют особое значение в контексте соединений юниверсов. Эти права применяются к соединениям, опубликованным в репозитории.

Права реляционного соединения

Право	Описание
Просмотр объектов	Позволяет просмотреть соединение.
Изменение объектов	Позволяет изменять параметры соединения.
Загрузить соединение локально	Позволяет использовать юниверсы, созданные для соединений в Web Intelligence Rich Client в автономном режиме. 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. Это право также требуется для редактирования защищенного соединения в средстве дизайна информации.
Удаление объектов	Позволяет удалить соединение.
Копирование объектов в другой каталог	Позволяет копировать соединение из одной папки в другую.
Доступ к данным	Позволяет извлекать содержимое из заданной для соединения базы данных. 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.
Использовать соединение с компонентом Stored Procedures (сохраняемые процедуры)	Позволяет использовать хранимые процедуры в базе данных, указанной в соединении юниверса.

Право	Описание
	Примечание Это право применимо только к юниверсам .unv.
Использование соединения для скриптов Free-Hand SQL	Позволяет выполнять скрипты SQL в соединении.

Права соединения OLAP

Право	Описание
Просмотр объектов	Позволяет просмотреть соединение.
Изменение объектов	Позволяет изменять параметры соединения в редакторе соединения средства дизайна информации.
Удаление объектов	Позволяет удалить соединение.
Копирование объектов в другой каталог	Позволяет копировать соединение из одной папки в другую.
Загрузить соединение локально	Позволяет использовать юниверсы, созданные для соединений в Web Intelligence Rich Client в автономном режиме.

34.3.11 Приложения

34.3.11.1 CMC

Право	Описание
Входить в систему CMC и выполнять просмотр объекта в CMC	Позволяет пользователю выполнять вход в CMC
Разрешить доступ к диспетчеру экземпляров	Разрешает пользователю доступ к диспетчеру экземпляров
Разрешить доступ к запросу взаимосвязей	Разрешает пользователю выполнять запросы взаимосвязей в CMC
Разрешить доступ к запросу безопасности	Разрешает пользователю выполнять запросы безопасности в CMC

34.3.11.2 Стартовая панель BI в стиле Fiori

Право	Описание
Вход на стартовую панель BI в стиле Fiori	Позволяет пользователю входить на стартовую панель BI в стиле Fiori.
Организовать	Позволяет пользователю перемещать и копировать объекты, добавлять объекты в папку Избранное и создавать ярлыки объектов
Отправить в папку "Входящие" Business Objects	Позволяет пользователю отправлять объекты адресатам в папке входящих BI
Отправить адресату электронной почты	Позволяет пользователю отправлять объекты адресатам электронной почты
Отправить в расположение файла	Позволяет пользователю отправлять объекты в расположение файла
Отправить в расположение FTP	Позволяет пользователю отправлять объекты в расположение FTP
Отправить в расположение SFTP	Позволяет пользователю отправлять объекты в расположение SFTP. Свойства SFTP сходны со свойствами FTP, но пользователь должен дополнительно предоставить отпечаток ключа (fingerprint). В свойствах каждого сервера SFTP есть параметр "отпечаток ключа". Проверка отпечатка производится на стороне сервера CMS.

34.3.11.2.1 Права на приложения сотрудничества

Эти права доступа применяются к приложению SAP Jam, настроенному на платформе BI.

Право	Описание
Добавить комментарии по документам, принадлежащим пользователю	Позволяет пользователю комментировать документы и экземпляры, которыми он владеет
Просмотреть комментарии по документам, принадлежащим пользователю	Позволяет пользователю просматривать комментарии к документам и экземплярам, которыми он владеет
Изменение предпочтений для объектов, владельцем которых является пользователь	Отображает меню *Предпочтения* в объекте приложения Без этого права доступа пользователь не может выставлять личные предпочтения в приложениях

Право	Описание
	и меню *Предпочтения* не будет отображаться в приложениях. Например, без этого права пользователи не могут выбирать единицы измерения (дюймы или миллиметры), которые следует использовать в отчетах приложения.

34.3.11.3 Рабочие пространства BI

Право	Описание
Создание и редактирование рабочих пространств BI	Позволяет пользователю создавать новые рабочие пространства BI и изменять существующие рабочие пространства BI
Создание и редактирование модулей	Позволяет пользователю создавать новые модули и изменять существующие модули
Изменение рабочих пространств BI	Позволяет пользователю изменять существующие рабочие пространства BI (но не разрешает создавать новые рабочие пространства)
Изменять предпочтения для объектов, которыми владеет пользователь	Отображает меню *Предпочтения* в объекте приложения Без этого права доступа пользователь не может выставлять личные предпочтения в приложениях и меню *Предпочтения* не будет отображаться в приложениях. Например, без этого права пользователи не могут выбирать единицы измерения (дюймы или миллиметры), которые следует использовать в отчетах в Web Intelligence или приложении стартовой панели BI.

34.3.11.4 Web Intelligence

Права доступа в этом разделе применяются к приложению Web Intelligence (включая Rich Client) и могут влиять на средства просмотра и панели запросов в этом приложении.

Право	Описание
Данные: Включить отслеживание данных	Позволяет пользователю отслеживать измененные данные.
Данные: Включить форматирование измененных данных	Позволяет пользователю выбирать форматирование измененных данных.

Право	Описание
Общие: Включить доступ клиента рабочего стола	Позволяет пользователю использовать Web Intelligence Desktop (Rich Client)
Настольный ПК: Экспорт документов	В Web Intelligence Rich Client пользователь может экспортировать документы в репозиторий платформы BI.
Настольный ПК: Сохранение документов для всех пользователей	В Web Intelligence Rich Client пользователь может сохранять документы локально без какой-либо безопасности.
Документы: Отключить автоматическое обновление при открытии	Отключает автоматическое обновление документов при открытии
Документы: Включить автосохранение	Включает автоматическое сохранение документов, если автоматическое сохранение активировано администратором в CMC
Документы: Включить создание	Позволяет пользователю создавать новые документы
Общие: Изменить настройки Web Intelligence	Позволяет пользователям изменять настройки Web Intelligence в стартовой панели BI
Общие: Включить доступ веб-клиента	Позволяет пользователю использовать веб-клиент Web Intelligence
Запрос: изменить скрипт, созданный из юниверса	На панели запросов позволяет пользователю редактировать SQL- или MDX-скрипты запросов, созданные из юниверса.
Запрос: Изменение Free-Hand SQL	Позволяет пользователю редактировать скрипты запросов Free-Hand SQL.
Запрос: просмотреть скрипт, созданный из юниверса	На панели запросов позволяет пользователю просматривать SQL- или MDX-скрипты запроса, созданные из юниверса.
Запрос: Просмотр Free-hand SQL	Позволяет пользователю просматривать скрипты запросов Free-Hand SQL.
Отчеты: Создание и изменение разрывов	Позволяет пользователю создавать и изменять разрывы.
Отчеты: Создание и изменение правил условного форматирования	Позволяет пользователю создавать и изменять правила условного форматирования.
Отчеты: Создание и изменение встроенного вычисления	Позволяет пользователю создавать и изменять предварительно определенные вычисления.
Отчеты: Создание и изменение элементов управления вводом и групп	Позволяет пользователю создавать и изменять элементы управления вводом.
Отчеты: Создание и изменение фильтров отчета и использование элементов управления вводом	Позволяет пользователю создавать и изменять фильтры отчета, а также использовать элементы управления вводом.
Отчеты: Создание и изменение сортировок и ранжирований	Позволяет пользователю создавать и изменять сортировки и ранжирования.
Отчеты: Создание формул, переменных, групп и ссылок	Позволяет пользователю создавать формулы, переменные, группы и ссылки.

Право	Описание
Отчеты: Включить изменение документа	Позволяет пользователю изменять форматирование отчетов. Без этого права доступа режим разработки недоступен.
Отчеты: Объединение объектов	Разрешает пользователю синхронизировать данные с помощью объединенных измерений в отчетах и в диспетчере данных.
Отчеты: Вставка и удаление отчетов, таблиц, диаграмм и ячеек	• Позволяет пользователю вставлять и удалять отчеты, таблицы, диаграммы и ячейки. • Включает рабочий процесс повторений (копирование/вставка).

34.3.11.5 Средство создания юниверсов

Право	Описание
Проверять целостность юниверса	Позволяет пользователю проверять целостность юниверса
Обновлять окно структуры	Позволяет пользователю обновлять окно структуры
Использовать средство обзора таблиц	Позволяет пользователю просматривать данные в базе данных с помощью средства обзора таблиц
Применить ограничения юниверса	Позволяет пользователю применить предварительно заданные ограничения юниверса к пользователям импортированного юниверса
Связать юниверс	Позволяет пользователю связать два юниверса для общего доступа к компонентам
Создать, изменить или удалить соединения	Позволяет пользователю создавать, изменять и удалять соединения юниверсов, хранящиеся в репозитории платформы BI или в качестве персональных или совместно используемых соединений
Изменять предпочтения для объектов, которыми владеет пользователь	Отображает меню *Предпочтения* в объекте приложения Без этого права доступа пользователь не может выставлять личные предпочтения в приложениях и меню *Предпочтения* не будет отображаться в приложениях. Например, без этого права пользователи не могут выбирать единицы измерения (дюймы или миллиметры), которые следует использовать в отчетах в Web Intelligence или приложении стартовой панели BI.

34.3.11.6 Средство дизайна информации

Право	Описание
Администрирование профилей безопасности	Позволяет пользователю открывать редактор безопасности Для работы с профилями безопасности необходимо также иметь права, предоставленные для юниверса.
Совместное использование проектов	Позволяет пользователю совместно использовать локальные проекты и синхронизировать совместно используемый проект с локальным проектом
Создать, изменить или удалить соединения	• Позволяет пользователю создавать и удалять защищенные соединения из представления "Опубликованные ресурсы" • Позволяет пользователю изменять соединения в редакторе соединений • Позволяет пользователю публиковать соединения в репозитории
Опубликовать юниверс	Позволяет пользователю публиковать юниверсы в репозитории
Извлечь юниверс	Позволяет пользователю извлекать опубликованные юниверсы в локальном проекте для редактирования
Сохранить для всех пользователей	Позволяет пользователю сохранять для всех пользователей при извлечении юниверсов
Вычисление статистики	Позволяет пользователю выбирать таблицы и столбцы для расчета и публикации статистики
Изменять предпочтения для объектов, которыми владеет пользователь	Отображает меню *Предпочтения* в объекте приложения Без этого права доступа пользователь не может выставлять личные предпочтения в приложениях и меню *Предпочтения* не будет отображаться в приложениях. Например, без этого права пользователи не могут выбирать единицы измерения (дюймы или миллиметры), которые следует использовать в отчетах в Web Intelligence или приложении стартовой панели BI.

34.3.11.7 Предупреждения

Право	Описание
Активация предупреждений	Позволяет пользователю активировать события предупреждений. Чтобы активировать предупреждение для документа, требуются следующие дополнительные права: • Права на "Просмотр" и "Составление расписаний" для документа • Права на "Просмотр" и "Активацию" для соответствующего события
Подписка на объекты	Позволяет пользователю подписываться на события предупреждения. Чтобы подписаться на событие, требуются следующие дополнительные права: • Право "Просмотр" для соответствующего события • Право "Подписка" на собственную учетную запись пользователя Чтобы подписаться на предупреждение для документа, требуются следующие дополнительные права: • Право "Просмотр" документа • Право "Просмотр экземпляра" документа • Право "Просмотр" для соответствующего события • Право "Подписка" на собственную учетную запись пользователя
Изменять предпочтения для объектов, которыми владеет пользователь	Отображает меню *Предпочтения* в объекте приложения Без этого права доступа пользователь не может выставлять личные предпочтения в приложениях и меню *Предпочтения* не будет отображаться в приложениях. Например, без этого права пользователи не могут выбирать единицы измерения (дюймы или миллиметры), которые следует использовать в отчетах в Web Intelligence или приложении стартовой панели BI.

34.3.11.8 SAP BusinessObjects Mobile

Право	Описание
Вход в SAP BusinessObjects Mobile	Позволяет пользователю осуществлять вход в платформу BI из приложения Mobile и просматривать документы
Подписка на предупреждения документа	Позволяет пользователю подписываться на документ и предупреждения повторяющихся экземпляров Если пользователю ранее предоставлялось это право (даже если сейчас оно не предоставлено), пользователь все равно может получать предупреждения, на которые подписался. Необходимо отменить подписку на предупреждения, если не следует их получать. Для того чтобы подписаться на предупреждения о документах и повторяющихся экземплярах для расписаний, у пользователя должен быть доступ "Полное управление" к папке `Системные события` в разделе *События* в CMC.
Сохранить документы в локальное хранилище устройства	Позволяет пользователю сохранять документы на мобильных устройствах Если пользователю ранее предоставлялось право "Сохранение документов локально на устройстве" (даже если сейчас оно не предоставлено) и пользователь сохранял документы на мобильном устройстве, документы останутся на устройстве, но не будут синхронизироваться в процессе синхронизации.
Отправить документы с устройства как сообщение электронной почты	Позволяет пользователю отправлять отчеты в сообщениях электронной почты
Изменять предпочтения для объектов, которыми владеет пользователь	Отображает меню *Предпочтения* в объекте приложения Без этого права доступа пользователь не может выставлять личные предпочтения в приложениях и меню *Предпочтения* не будет отображаться в приложениях. Например, без этого права пользователи не могут выбирать единицы измерения (дюймы или миллиметры), которые следует использовать в отчетах в Web Intelligence или приложении стартовой панели BI.

Для получения дополнительных сведений см. *Руководство по установке и развертыванию SAP BusinessObjects Mobile*.

34.3.11.9 Рабочее место администратора BI

Права	Описание
Разрешить доступ к рабочему месту администратора BI	Разрешает доступ к рабочему месту администратора BI в CMC
Разрешить доступ к мониторингу	Разрешает доступ к мониторингу в рабочем месте администратора BI
Разрешить доступ к Visual Difference	Разрешает доступ к Visual Difference в рабочем месте администратора BI
Visual Difference - создать сравнение	Позволяет создать новые сравнения между инфо-объектами в Visual Difference
Visual Difference - удалить сравнение	Позволяет удалить предыдущие сравнения в Visual Difference
Visual Difference - повторно выполнить сравнение	Позволяет повторно выполнить ранее созданные сравнения в Visual Difference
Visual Difference - просмотреть сравнение	Позволяет просмотреть сравнение в Visual Difference

35 Приложение "Свойства серверов"

35.1 О приложении "Свойства серверов"

В приложении "Свойства серверов" перечислены и описаны свойства, которые можно задать для каждого сервера платформ BI.

35.1.1 Общие свойства сервера

Представленные в этом разделе свойства серверов применимы к серверам любого типа.

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.
Порт запросов	Задает 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. **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.	По умолчанию для параметра *Назначать автоматически* задано значение `true`, а поле параметра *Порт запросов* не заполнено.

Свойство	Описание	Значение по умолчанию
Назначать автоматически	Указывает, выполняется ли привязка сервера при каждом его перезапуске к динамически размещенному порту. Для привязки сервера к определенному порту задайте для параметра *Назначать автоматически* значение `true` и укажите допустимый *Порт запросов*.	Значение по умолчанию равно **TRUE**.

Свойства автозапуска

Свойство	Описание	Значение по умолчанию
Автоматически запускать этот сервер при запуске агента Server Intelligence	Определяет, будет ли сервер запускаться автоматически при запуске или перезапуске агента Server Intelligence (SIA). Если для этого параметра задано значение `false`, при запуске или перезапуске агента SIA сервер не начинает работу.	Значение по умолчанию равно **TRUE**.

Свойства идентификатора хоста

Свойство	Описание	Значение 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.	Значение по умолчанию равно **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.

Свойства шаблона конфигурации

Свойство	Описание	Значение по умолчанию
Использовать шаблон конфигурации	Указывает на необходимость использования шаблона конфигурации.	Значение по умолчанию равно **FALSE**.
Восстановить системные значения по умолчанию	Определяет восстановление исходных значений по умолчанию для данного сервера.	Значение по умолчанию равно **FALSE**.

Свойство	Описание	Значение 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 равно **FALSE**.

Свойства службы протокола трассировки

Свойство	Описание	Значение по умолчанию
Уровень журнала	Определяет минимальную серьезность предупреждения, которое необходимо записать, и количество информации, записываемой в серверный файл журнала. Возможные уровни порога журнала: • *Не определен* • *Нет* • *Низкий* • *Средний* • *Высокий*	По умолчанию используется значение **Не определен**.

35.1.2 Свойства основных служб

В категорию "Основные службы" входят следующие серверы:

- Адаптивный сервер заданий
- Адаптивный сервер обработки
- Центральный сервер управления
- Сервер событий
- Сервер репозитория входящих файлов
- Сервер репозитория выходных файлов
- Сервер контейнера веб-приложений

Свойства адаптивного сервера заданий

Общие свойства

Свойство	Описание	Значение по умолчанию
Временный каталог	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. **Примечание** Для вступления в силу изменений требуется перезапустить данный сервер.	%DefaultDataDir%

На адаптивном сервере заданий могут размещаться несколько разных служб. Для каждой службы имеются следующие свойства

Свойства служб

Свойство	Описание	Значение по умолчанию
Максимальное число параллельных заданий	Определяет количество параллельно выполняемых независимых (дочерних) процессов, максимально допустимое для сервера. Максимальное количество заданий можно настроить в соответствии со средой составления отчетов. 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.	5
Максимальное число запросов дочерних объектов	Указывает количество заданий, которые дочерний объект обрабатывает перед повторным запуском.	100

Свойства сервера адаптивной обработки

Общие свойства

Свойство	Описание	Значение по умолчанию
Время ожидания запуска службы (сек)	Определяет количество времени в секундах, в течение которого сервер ожидает запуска служб. Если в течение указанного времени не удалось запустить службу, подобный сбой может возникнуть по одной из двух причин: • 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. Для обнаружения причины обратитесь к файлу журнала сервера. Если службу не удалось запустить в течение указанного времени, возможно, это значение следует увеличить.	1200

Свойства службы прокси аудита клиента

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Свойства службы маркера безопасности

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

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

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

Свойства службы преобразований

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Свойства службы мониторинга

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Свойства службы поиска по платформе

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

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.

Свойства Central Management Service

Свойство	Описание	Значение по умолчанию
Порт сервера имен	Определяет порт, на котором CMS прослушивает начальные запросы к службе имен.	6400

Свойство	Описание	Значение по умолчанию
Запросы соединений с системной БД	Определяет количество попыток соединения с системной базой данных CMS, предпринимаемых CMS. Если серверу не удается 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. Показатель CMS *Установленные соединения с системной базой данных* показывает текущее число установленных соединений.	14
Автоматическое повторное подключение к системной базе данных	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.	**TRUE**

Свойства службы единого входа

Свойство	Описание	Значение по умолчанию
Таймаут службы единой регистрации (секунды)	Определяет период времени (в секундах), в течение которого соединение SSO с источником 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.	86400

Свойства сервера событий

Свойства службы событий

Свойство	Описание	Значение по умолчанию
Интервал опроса событий (секунды)	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

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*.	%DefaultInputFRSDir/temp%
Максимальное время бездействия (в минутах)	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
Местоположение файла адаптера для сканирования вирусов	Задает абсолютный путь к местоположению файла адаптера для сканирования вирусов.	

Свойства сервера репозитория исходящих файлов

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.	%DefaultOutputFRSDir/%
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.	%DefaultOutputFRSDir/temp%
Максимальное время бездействия (в минутах)	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

Общие свойства

Свойство	Описание	Значение по умолчанию
Время ожидания запуска службы (сек)	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. Если задано недостаточное время ожидания, которое истекает раньше, чем происходит запуск WACS, следует восстановить настройки по умолчанию WACS в CCM.	1200

Свойства службы протокола трассировки

Свойство	Описание	Значение по умолчанию
Уровень журнала	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). Доступны следующие пункты меню: • *Не определен* • *Нет* • *Низкий* • *Средний* • *Высокий*	Не определено

Свойства службы бизнес-процессов BI

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Свойства службы построителя запросов

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

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

Свойство	Описание	Значение по умолчанию
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
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	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. Допустимы следующие значения: • *secEnterprise* • *secDAP* • *SAPR3* • *secWinAD*	Пустая. Однако если выбрано значение *Включить базовую аутентификацию HTTP*, по умолчанию используется параметр *secEnterprise*.

Веб-служба RESTful – Свойства конфигурации совместного использования ресурсов по всем источникам

Свойство	Описание	Значение по умолчанию
Разрешить источники	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, http://origin1.server.com:8080, http://origin2.server.com:8080. По умолчанию браузеры имеют доступ ко всем доменам (*).	* (звездочка)
Максимальный срок (минуты)	Это максимальный срок кэширования HTTP-запросов браузерами.	1440

Веб-служба – свойства конфигурации доверительной аутентификации

Свойство	Описание	Значение по умолчанию
Метод извлечения	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`. • *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	Это метка, использующаяся для идентификации доверенного пользователя при извлечении маркера входа.	**X-SAP-TRUSTED-USER**

Свойства службы веб-приложения BOE

Тип свойства	Описание	Значение по умолчанию
Тип аутентификации	Тип аутентификации, который используется при входе пользователей на стартовую панель BI. Допустимы следующие значения: • *AD Kerberos* • *Служба SSO AD Kerberos* • *Enterprise* • *LDAP*	*Enterprise*
Домен AD по умолчанию	Домен Active Directory по умолчанию используется, 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».	Пусто
Имя принципала службы	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)

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.	**FALSE**
Домен AD по умолчанию	Используется домен Active Directory по умолчанию, чтобы пользователям не нужно было указывать домен при входе в систему.	(пустой)
Имя принципала службы	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)

Свойства конфигурации HTTP

Свойство	Описание	Значение 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.	**TRUE**
Привязать к имени хоста или IP-адресу	Определяет сетевой интерфейс (IP-адрес или имя хоста), посредством которого предоставляется служба HTTP. Для указания значения снимите флажок с поля *Привязка ко всем IP-адресам*.	`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) заголовка HTTP запроса и ответа.	32768

Конфигурация HTTP через свойства прокси-сервера

Свойство	Описание	Значение 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.	**FALSE**
Привязка ко всем IP-адресам	Привязывать ли порт HTTP через прокси ко всем сетевым интерфейсам.	**ИСТИНА**

Свойство	Описание	Значение по умолчанию
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`
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) заголовка HTTP запроса и ответа.	32768

Свойства конфигурации HTTPS

Свойство	Описание	Значение 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.
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.

Свойство	Описание	Значение по умолчанию
Тип хранилища сертификатов	Тип хранилища сертификатов, в котором содержатся сертификаты и секретные ключи. В большинстве случаев для данного параметра используется значение *PCKS12*. 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)
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*.	**FALSE**
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) заголовка HTTP запроса и ответа.	32768

Свойства параллельной работы (по коннекторам)

Свойство	Описание	Значение 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.

Свойства конфигурации Active Directory

Свойство	Описание	Значение по умолчанию
Расположение файла Krb5.ini	Полный путь к файлу `krb5.ini`, в котором хранятся свойства конфигурации Kerberos.	(пустой)
Расположение файла bscLogin.conf	Полный путь к файлу `bscLogin.conf`.	(пустой)

35.1.3 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.

Свойства службы доступа к данным Excel

Свойство	Описание	Значение по умолчанию
Время ожидания очистки доступа к данным Excel (сек)	Задает время (в секундах) ожидания службой неактивного клиента перед выполнением очистки сеанса клиента.	По умолчанию используется значение 1200 секунд.
Время ожидания замены доступа к данным Excel (сек)	Задает время (в секундах) ожидания службой неактивного клиента перед выполнением выгрузки сеанса клиента на жесткий диск. Рекомендуется, чтобы это значение было меньше значения свойства *Время ожидания очистки доступа к данным Excel (сек)*.	По умолчанию используется значение 600 секунд.

Свойства операции службы

Свойство	Описание	Значение по умолчанию

> → Напоминание
>
> Нет необходимости перезапускать сервер после изменения следующих свойств операции службы.

Свойство	Описание	Значение по умолчанию
Создание пула соединений	Включает или отключает пул соединений. Возможные значения: • Включено – со временем ожидания • Включено – без времени ожидания • Отменено **Примечание** Пул соединений является набором функций кэширования, которые поддерживают соединения в состоянии возможности повторного использования для повышения производительности сервера.	Включено – со временем ожидания
Время ожидания пула соединений	Задает максимальное время простоя для соединений в пуле (в минутах). **Примечание** Это свойство эквивалентно параметру `Max Pool Time` файла `cs.cfg`. Отключение пула эквивалентно тому, что параметр `Max Pool Time` установлен в `0`. Включение пула без времени ожидания эквивалентно тому, что параметр `Max Pool Time` установлен в `-1`. Для получения дополнительных сведений см. *Руководство по доступу к данным*.	**60**
Время простоя неактивности переходных объектов (мин)	Задает, сколько минут должен сохраняться неиспользуемый временный объект на сервере. После этого интервала объект удаляется, а его ресурсы возвращаются.	**60**
Интервал таймера временных объектов	Задает время между проверками активности (в минутах). Через регулярные интервалы сервер ищет возможный объект для удаления.	**5**
Включить образование блоков HTTP	Включает или отключает образование блоков HTTP. **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**.	Включено
Размер блока HTTP	Задает размер (в килобайтах) ответов HTTP, посылаемых сервером.	**64**

Свойства отслеживания низкого уровня

Свойство	Описание	Значение по умолчанию
→ Напоминание 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*.	Отключено
Включить отслеживание программного обеспечения среднего яруса	Включает трассировку всего промежуточного ПО. Для трассировки конкретного промежуточного ПО необходимо настроить файл `cs.cfg` и перезапустить сервер. ⓘ Примечание При этом свойство *Уровень журнала* должно иметь значение *Высокий*.	Отключено

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	Позволяет выбирать источники данных, для которых требуются соединения. Данное свойство используется в качестве фильтра для драйверов. Активные источники данных указываются для загрузки требуемых драйверов **⚠ Предупреждение** По умолчанию сервер загружает все доступные драйверы. Этот параметр используется для специализации серверов. Он особенно полезен при развертывании нескольких серверов CORBA в сети. **→ Напоминание** Драйверы загружаются только для выбранных источников данных. Все другие игнорируются. Если источники данных не выбраны, сервер загружает все доступные драйверы. **ⓘ Примечание** Проверьте в показателях сервера включение выбранных источников данных. Сетевые уровни и базы данных отображаются под *показателями службы соединений*.	Не отмечено
Сетевой уровень	Задает сетевой уровень, используемый соединением. **ⓘ Примечание** Рассматривается только не локализованное имя. Список доступных сетевых уровней содержится в файле `driver.cfg`, находящийся в папке `<connectionserver-install-dir>\connectionServer`.	• `ODBC` для собственных серверов CORBA • `JDBC` для адаптивного сервера CORBA
База данных	Задает базу данных, используемую соединением. **ⓘ 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 `.*` для соответствия любому символу. Например, выражение `MS SQL Server.*$` 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/perlre.html#Regular_Expressions .	Поле остается пустым, пока в него не будет введено имя базы данных.

Свойства службы доступа к пользовательским данным

Свойство	Описание	Значение по умолчанию
Время ожидания очистки доступа к пользовательским данным (сек)	Задает 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)	Задает время (в секундах) ожидания службой неактивного клиента перед выполнением выгрузки сеанса клиента на жесткий диск. Рекомендуется, чтобы это значение было меньше значения свойства *Время ожидания очистки доступа к пользовательским данным (сек)*.	По умолчанию используется значение 600 секунд.

Свойства службы единого входа

Свойство	Описание	Значение по умолчанию
Истечение срока действия единого входа (сек)	Определяет период времени (в секундах), в течение которого соединение SSO остается действительным до окончания срока действия.	По умолчанию используется значение 86400 секунд.

Свойства службы Диспетчера переноса объектов

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Свойства службы ClearCase Диспетчера переноса объектов

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Свойства службы Visual Difference

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Связанные сведения

Общие свойства сервера [страница 1200]

35.1.4 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 2020

- Сервер обработки Crystal Reports 2020

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.

Свойства службы кэша Crystal Reports

Свойство	Описание	Значение по умолчанию
При обновлении средства просмотра всегда выдаются текущие данные	Определяет, будут ли игнорироваться все страницы в кэше при явном обновлении отчета пользователем и будут ли при этом новые данные извлекаться непосредственно из базы данных. **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 CMC и щелкните *Установки по умолчанию* > *Просмотр группы серверов* >.	По умолчанию используется значение **FALSE**.
Предоставлять совместный доступ к данным отчета для клиентов	Определяет возможность совместного использования данных отчета несколькими клиентами. **Примечание** Это свойство можно задать непосредственно в объекте отчета. Его значение для разных отчетов может отличаться, при этом значения, заданные в объекте отчета, имеют приоритет перед параметрами сервера.	По умолчанию используется значение **TRUE**.
Предельное время простоя соединения (в минутах)	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.

Свойство	Описание	Значение по умолчанию
Время ожидания кэша безопасности (в минутах)	Задает время (в минутах), когда сервером используется кэшированная информация об учетных данных для входа, параметрах отчета и соединении с базой данных для обслуживания отчетов перед отправкой запроса в CMS.	По умолчанию используется значение 20 минут.
Самые старые данные, выданные клиенту по запросу (в секундах)	Определяет период времени (в секундах), в течение которого сервер использует кэшированные данные для выполнения запросов из отчетов 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. **Примечание** Это свойство можно задать непосредственно в объекте отчета. Его значение для разных отчетов может отличаться, при этом значения, заданные в объекте отчета, имеют приоритет перед параметрами сервера.	По умолчанию используется значение 0 секунд.
Максимальный размер кэша (КБ)	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.	`%DefaultDataDir%/CrystalReportsCachingServer/temp`
Аргументы Java VM	Задает аргументы командной строки, которые могут быть предоставлены JVM.	Значение по умолчанию не указано.
Имя DLL	Задает имя загруженного в данный момент подключаемого модуля с типом документа. Данное свойство доступно только для чтения.	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.

Свойства службы обработки Crystal Reports

Свойство	Описание	Значение по умолчанию
Предельное время простоя задания (в минутах)	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 процесс за весь срок службы.	Значением по умолчанию является 1000.
При обновлении средства просмотра всегда выдаются текущие данные	Определяет, будут ли игнорироваться все страницы в кэше при явном обновлении отчета пользователем и будут ли при этом новые данные извлекаться непосредственно из базы данных. Определяет необходимость совместного использования данных отчетов несколькими клиентами. **Примечание** Это свойство можно задать непосредственно в объекте отчета. Его значение для разных отчетов может отличаться, при этом значения, заданные в объекте отчета, имеют приоритет перед параметрами сервера. Для установки значения в объекте отчета выберите отчет в CMC и щелкните *Установки по умолчанию* > *Просмотр группы серверов*.	По умолчанию используется значение **FALSE**.

Свойство	Описание	Значение по умолчанию
Предоставлять совместный доступ к данным отчета для клиентов	Определяет возможность совместного использования данных отчета несколькими клиентами. Определяет необходимость совместного использования данных отчетов несколькими клиентами. **ⓘ Примечание** Это свойство можно задать непосредственно в объекте отчета. Его значение для разных отчетов может отличаться, при этом значения, заданные в объекте отчета, имеют приоритет перед параметрами сервера.	По умолчанию используется значение **TRUE**.
Предельное время простоя соединения (в минутах)	Определяет время в минутах, в течение 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.	Значением по умолчанию является 0.
Самые старые данные, выданные клиенту по запросу (в секундах)	Определяет период времени (в секундах), в течение которого сервер использует кэшированные данные для выполнения запросов из отчетов 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. **ⓘ 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.	Значением по умолчанию является 0.

Свойство	Описание	Значение 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.	%DefaultDataDir%/CrystalReportsProcessingServer/temp
Путь к классу Java	Имена классов Java и путь к этим классам, требуемые сервером.	%CommonJavaLibDir%/procCR.jar
Аргументы дочерней Java VM	Задает аргументы командной строки, поставляемые в дочерние процессы, созданные сервером.	Dbusinessobjects.connectivity.directory=%CONNECTIONSERVER_DIR%,Dcom.businessobjects.mds.cs.ImplementationID=csEX

Свойства службы единого входа

Свойство	Описание	Значение по умолчанию
Таймаут службы единой регистрации (секунды)	Определяет период времени (в секундах), в течение которого соединение SSO остается действительным до окончания срока действия.	По умолчанию используется значение 86400 секунд.

Свойства сервера приложений отчетов Crystal Reports 2020

Примечание

При изменении любого из этих свойств необходимо перезапустить сервер, чтобы изменения вступили в силу.

Свойства службы просмотра и изменений Crystal Reports 2020

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.	По умолчанию используется значение **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.
Предельное время простоя соединения (в минутах)	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.
Число записей базы данных для считывания при предварительном просмотре или обновлении отчета (-1, если 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, равное 20000 записям.

Свойство	Описание	Значение по умолчанию
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	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.	`%DefaultDataDir%/CrystalReportsRasServer/temp`

Свойства службы единого входа

Свойство	Описание	Значение по умолчанию
Таймаут службы единой регистрации (секунды)	Определяет период времени (в секундах), в течение которого соединение SSO остается действительным до окончания срока действия.	По умолчанию используется значение 86400 секунд.

Свойства сервера обработки Crystal Reports 2020

Примечание

При изменении любого из этих свойств необходимо перезапустить сервер, чтобы изменения вступили в силу.

Свойства службы обработки Crystal Reports 2020

Свойство	Описание	Значение по умолчанию
Предельное время простоя задания (в минутах)	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 процесс за весь срок службы.	Значением по умолчанию является 1000.

Свойство	Описание	Значение по умолчанию
При обновлении средства просмотра всегда выдаются текущие данные	Определяет, будут ли игнорироваться все страницы в кэше при явном обновлении отчета пользователем и будут ли при этом новые данные извлекаться непосредственно из базы данных. Определяет необходимость совместного использования данных отчетов несколькими клиентами. **Примечание** Это свойство можно задать непосредственно в объекте отчета. Его значение для разных отчетов может отличаться, при этом значения, заданные в объекте отчета, имеют приоритет перед параметрами сервера. Для установки значения в объекте отчета выберите отчет в CMC и щелкните *Установки по умолчанию* > *Просмотр группы серверов* >.	По умолчанию используется значение **FALSE**.
Предоставлять совместный доступ к данным отчета для клиентов	Определяет возможность совместного использования данных отчета несколькими клиентами. Определяет необходимость совместного использования данных отчетов несколькими клиентами. **Примечание** Это свойство можно задать непосредственно в объекте отчета. Его значение для разных отчетов может отличаться, при этом значения, заданные в объекте отчета, имеют приоритет перед параметрами сервера.	По умолчанию используется значение **TRUE**.
Предельное время простоя соединения (в минутах)	Определяет время в минутах, в течение 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.	Значением по умолчанию является 0.

Свойство	Описание	Значение по умолчанию
Самые старые данные, выданные клиентам по запросам (сек)	Определяет период времени (в секундах), в течение которого сервер использует кэшированные данные для выполнения запросов из отчетов 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. **ⓘ 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.	Значением по умолчанию является 0.
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.	%DefaultDataDir%/CrystalReports2020ProcessingServer/temp
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.

Свойство	Описание	Значение по умолчанию
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.	Значением по умолчанию является 20000.

Свойства службы единого входа

Свойство	Описание	Значение по умолчанию
Таймаут службы единой регистрации (секунды)	Определяет период времени (в секундах), в течение которого соединение SSO остается действительным до окончания срока действия.	По умолчанию используется значение 86400 секунд.

35.1.5 Свойства служб Analysis

Категория служб Analysis включает адаптивный сервер обработки:

Свойства службы Multi-Dimensional analysis service

Свойство	Описание	Значение по умолчанию
Максимальное количество сеансов клиента	Задает 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.

Свойство	Описание	Значение по умолчанию
Максимальное число ячеек, возвращаемых запросом	Указывает число ячеек, возвращаемых пользователю в одном запросе. Предотвращается выполнение пользователем запросов, возвращающих чересчур большое число ячеек, для чего требуется большой объем памяти. Если запрос пользователя превышает этот предел для ячеек, пользователь получает сообщение об ошибке.	По умолчанию используется значение 100000 ячеек.
Максимальное число элементов, возвращаемых при фильтрации	Задает число элементов, извлекаемых при фильтрации по элементам. Очень большое число извлекаемых элементов может потребовать потребления большого объема памяти.	По умолчанию используется значение 100000 элементов.

Свойства службы веб-приложений BEx

Свойство	Описание	Значение по умолчанию
Максимальное количество сеансов клиента	Максимальное количество клиентских сеансов, допустимых в службе.	Значение по умолчанию составляет 15 сеансов.
Главная система SAP BW	Имя OLAP-соединения с системой BW, созданного в платформе BI.	Имя по умолчанию – SAP_BW.
Назначение RFC сервера JCo	Имя RFC-назначения сервера JCo Server, введенное в системе BW.	По умолчанию значение не указано.
Хост шлюза сервера JCo	Имя хоста шлюза сервера JCo Server, определенное в системе BW.	По умолчанию значение не указано.
Служба шлюза сервера JCo	Имя службы шлюза сервера JCo Server, определенное в системе BW.	По умолчанию значение не указано.
Количество соединений с сервером JCo	Указывает число автоматически созданных программ, которые могут использоваться для обработки запросов на обслуживание из ABAP в Java.	Значение по умолчанию равно 3 соединениям.

35.1.6 Свойства служб объединения данных

Категория служб объединения данных включает адаптивный сервер обработки:

Свойства службы объединения данных

Свойство	Описание	Значение по умолчанию
Максимальное число соединений	Задает максимальное число соединений, разрешенных на сервере.	По умолчанию используется значение 32767.
Размер пула потока выполнения	Задает максимальное число запросов, которые могут выполняться параллельно в данный момент.	Значением по умолчанию является 10.
Время ожидания неактивного соединения	Задает время (в секундах), по истечении которого неактивное соединение закрывается.	По умолчанию используется значение 10800 секунд.

Свойство	Описание	Значение по умолчанию
Время ожидания неактивного оператора	Задает время (в секундах), по истечении которого неактивный оператор запроса закрывается.	По умолчанию используется значение 600 секунд.

35.1.7 Свойства служб Web Intelligence

К категории служб Web Intelligence относятся следующие серверы:

- Адаптивный сервер обработки
- Сервер обработки Web Intelligence

Параметры адаптивного сервера обработки

Параметры командной строки

Свойство	Описание	Значение по умолчанию
Развертывание до уровня	Указывает уровень извлечения данных из запросов BEx. 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.	`-Dsap.sl.bics.expandToLevel=n` n может быть любым целым числом от 0 до 99. Если n=0 или этот параметр не указан, иерархии не будут использовать параметр "Развертывание до уровня".

Свойство	Описание	Значение по умолчанию
Выбор переменной опции выбора	Указывает опцию выбора для выбора переменной. Если для свойства указан интервал, текстовое окно недоступно, пользователи могут выбрать только начальные и конечные значения в диалоговом окне "Подсказки". Если значением этого свойства является многозначность, тогда доступно текстовое поле "Введите значение" и пользователи могут вводить значения переменных выбора BW. **Примечание** Это свойство не обновляет локально установленные Web Intelligence Rich Client. Для получения сведений об обновлении локального реестра таких установок см. "Руководство по установке Web Intelligence Rich Client".	`-Dsap.sl.bics.variableComplexSelectionMapping=n` где n может быть или интервалом, или многозначностью. **Примечание** До версии BI 4.1 SP05 значением по умолчанию для этого параметра был интервал. Если добавить это свойство в настройки адаптивного сервера обработки и указать многозначность, в существующих документах потребуется выполнить следующие действия: • Документ должен быть очищен. • Значения по умолчанию для подсказок запросов должны быть изменены для совместимости с многозначным выбором.

Свойства службы мониторинга Web Intelligence

Свойство	Описание	Значение по умолчанию
Включить мониторинг	Определяет, включен ли мониторинг для службы.	**TRUE**
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)	Задает время (в секундах) ожидания службой неактивного клиента перед выполнением очистки сеанса клиента.	1200
Время ожидания очистки отслеживаемых ресурсов по умолчанию (сек)	Определяет время ожидания службой неактивного клиента перед выполнением выгрузки сеанса клиента на жесткий диск (в секундах). Рекомендуется, чтобы это значение было меньшим значения свойства "Время ожидания очистки отслеживаемых ресурсов по умолчанию (сек)".	600
Включить профилирование службы		**TRUE**
Включить мониторинг активности службы		**TRUE**

Свойства службы визуализации

Свойство	Описание	Значение по умолчанию
Время ожидания очистки подсистемы визуализации(сек)	Задает время (в секундах) ожидания службой неактивного клиента перед выполнением очистки сеанса клиента.	1200
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

Свойства службы Rebean

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Свойства службы восстановления документов

Свойство	Описание	Значение по умолчанию
Свойства конфигурации отсутствуют		

Свойства службы моста DSL

Свойство	Описание	Значение по умолчанию
Время ожидания очистки подсистемы моста DSL (сек)	Задает 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.

Свойства службы Information Engine

Свойство	Описание	Значение по умолчанию
Включить список значений кэша	Определяет необходимость включения кэширования списка значений на сервере обработки Web Intelligence.	**TRUE**
Размер пакета списка значений (записи)	Определяет максимальное число записей (или значений) для каждого пакета списка значений.	1000

Свойство	Описание	Значение по умолчанию
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

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
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 Допустимым диапазоном является от 1 до 20.
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 `<Максимальное число соединений>`. Если это свойство включено, значение, заданное для свойства `<Максимальное число соединений>`, распознается сервером; в противном случае свойство игнорируется.	**TRUE**

Свойство	Описание	Значение по умолчанию
Предельное время простоя соединения (в минутах)	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
Максимальное число соединений	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. **Примечание** Свойство `<Разрешить ошибки макс. размера карты документа>` должно быть включено, чтобы это свойство могло быть распознано сервером.	200 Допустимым диапазоном является от 5 до 65535.
Включить анализ памяти	Определяет необходимость включения анализа памяти. Если это свойство включено, то следующие свойства будут активны и распознаны сервером: • `<Максимальный порог памяти>` • `<Верхний порог памяти>` • `<Нижний порог памяти>` Если память серверного процесса превышает значение `<Верхний порог памяти>`, единственной разрешенной операцией является сохранение документов. Если память процесса превышает значение `<Максимальный порог памяти>`, все операции останавливаются и завершаются неудачно.	**TRUE**
Нижний порог памяти (МБ)	Определяет нижнее пороговое значение использования памяти.	**3500**
Верхний порог памяти (МБ)	Определяет верхнее пороговое значение использования памяти.	**4500**
Макс. порог памяти (МБ)	Определяет максимальное пороговое значение использования памяти.	**6000**
Включить мониторинг службы APS	Включает мониторинг сервера службой APS, размещаемой на адаптивном сервере обработки.	**TRUE**
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

Свойство	Описание	Значение по умолчанию
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**.	**FALSE**

Свойства службы обработки Web Intelligence

Свойство	Описание	Значение по умолчанию
Включить использование HTTP URL	Указывает, может ли сервер получать доступ к файлам, сохраненным удаленно.	**TRUE**
Значение прокси	Задает адрес прокси-сервера данной сети. Это значение необходимо задавать только в случае, если в сети имеется прокси-сервер и выполняется попытка доступа к файлам, сохраненным удаленно.	(пустой)

Свойства общей службы Web Intelligence

Свойство	Описание	Значение по умолчанию
Таймаут кэша (мин)	Определяет период времени (в минутах) перед выполнение 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 `<Максимальный размер кэша документов>`, `<Макс. сжатие кэша документов>` и `<Максимальное число документов в кэше>`.	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.	**FALSE**
Включить кэш документов	Определяет необходимость включения кэша документов. Если свойство включено, в кэш можно загрузить предварительно запланированные документы Web Intelligence.	**TRUE**
Включить кэш реального времени	Определяет необходимость включения кэша реального времени. Если этой 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.	**TRUE**

Свойство	Описание	Значение по умолчанию
Максимальный размер кэша документов (кбайт)	Определяет максимальный размер кэша для документов. По достижении ограничения кэш документов будет очищен на основе свойства `<Максимальное сжатие кэша документов>`.	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
Макс. размер символьного потока (МБ)	Определяет максимальный размер символьного потока, переданного клиенту Web Intelligence. **Примечание** Если значение свойства *Макс. размер символьного потока* превышено, документ Web Intelligence создан не будет и клиент получит сообщение об ошибке.	5 Допустимый диапазон: от 1 до 4095 МБ.
Макс. размер потока двоичных данных (МБ)	Определяется максимальный размер (в мегабайтах) потока двоичных данных, переданных клиенту Web Intelligence. **Примечание** Если значение свойства *Макс. размер потока двоичных данных* превышено, документ Web Intelligence создан не будет и клиент получит сообщение об ошибке.	50 Допустимый диапазон: от 1 до 4095 МБ.
Каталог изображений	Определяет расположение каталога изображений.	(пусто)
Выходной каталог кэша	Определяет расположение кэша.	(пусто)

Общие свойства

Свойство	Описание	Значение по умолчанию
Таймаут службы единой регистрации (секунды)	Определяет период времени (в секундах), в течение которого соединение SSO остается действительным до окончания срока действия.	86400

Связанные сведения

Параметры пороговых значений серверной памяти Web Intelligence [страница 1238]

35.1.7.1 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".

Нижний порог памяти

Если достигнуто ограничение `<Нижний порог памяти>`, сервер переносит неактивные документы на жесткий диск, выделяя дополнительную память для активных документов. С этого момента каждый пользователь может иметь до одного активного документа вместо `<максимального числа документов на одного пользователя>`.

Верхний порог памяти

Если достигнуто ограничение `<Верхний порог памяти>`, на сервере будут выполняться следующие действия для высвобождения ресурсов и защиты сервера:

- Сервер будет отклонять новые соединения и вызовы клиентов. В документах Web Intelligence разрешено только использование параметра *Сохранить*. Пользователи, запрашивающие выполнение операций, получат 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>`.
- Он попытается закрыть документы, предназначенные только для чтения.
- Если во время очистки системы высвобождено недостаточное количество памяти, сервер начинает закрывать документы, открытые в режиме *редактирования*. 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 вычисляется по следующей формуле: `<Верхний порог памяти>` – (20%*(`<Верхний порог памяти>`)). Например, если для свойства "Верхний порог памяти" задано значение 4500 МБ, безопасным уровнем является:

  ```
  4500MB - .20*4500MB = 3600MB
  ```

  Во время вызова клиента сервер не может закрывать документы. При достижении верхнего порога не будут закрыты любые обновленные или экспортированные в другой формат документы, а также длительные операции. Если сервер не сможет высвободить достаточный объем памяти, и значение`<Верхнего порога памяти>` все еще будет превышено, произойдет перезапуск.

Максимальный порог памяти

Если достигнуто ограничение <Максимальный порог памяти>, все текущие операции прерываются. Все вызовы клиентов будут прекращены, а соответствующие документы – закрыты.

36 Приложение "Показатели сервера"

36.1 О 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 BI.

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: • 0 = красный (Осторожно) • 1 = янтарный (Внимание) • 2 = зеленый (Работает нормально)
Состояние включения сервера	Это состояние указывает, включен или выключен сервер. Возможные значения: • 0 = отключено • 1 = включено
Состояние работы сервера	Это состояние указывает состояние работы сервера. Возможные значения: • 0 = ОСТАНОВЛЕНО • 1 = ЗАПУСК • 2 = ИНИЦИАЛИЗАЦИЯ • 3 = ВЫПОЛНЕНИЕ • 4 = ОСТАНОВКА • 5 = СБОЙ • 6 = ВЫПОЛНЕНИЕ С ОШИБКАМИ • 7 = ВЫПОЛНЕНИЕ С ПРЕДУПРЕЖДЕНИЯМИ

36.1.1 Общие показатели сервера

Приведенные ниже показатели относятся к компьютеру, на котором работает указанный сервер.

Показатели работы компьютера

Показатель	Описание
Имя компьютера	Имя компьютера, на котором выполняется сервер.
Операционная система	Операционная система на компьютере, на котором выполняется сервер.
Тип ЦП	Тип центрального процессора на компьютере, на котором выполняется сервер. Этот показатель недоступен на адаптивных серверах обработки или серверах контейнеров веб-приложений (WACS).
ЦП	Количество ЦП, доступных для сервера. Для многоядерных систем этот показатель может означать количество логических ЦП, а не число физических процессоров. Этот показатель недоступен на адаптивных серверах обработки или серверах контейнеров веб-приложений (WACS).
Число ядер	Отображает число ядер компьютера, на котором размещен сервер платформы BI.
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 (ГБ)	Размер диска, на котором установлена платформа BI, в гигабайтах. Этот показатель недоступен на адаптивных серверах обработки или серверах контейнеров веб-приложений (WACS).
Использованное дисковое пространство (ГБ)	Используемый объем диска, на котором установлена платформа BI, в гигабайтах. Учитывается место, которое занимает платформа BI и другие программы на компьютере. Этот показатель недоступен на адаптивных серверах обработки или серверах контейнеров веб-приложений (WACS).

Следующие показатели описывают указанный сервер SAP BusinessObjects.

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 CMC.
Версия	Версия сервера.
Время начала	Время последнего запуска сервера.
PID	Уникальный идентификатор процесса на сервере. Операционная система на компьютере, на котором выполняющийся сервер создает PID. С помощью этого PID можно идентифицировать нужный сервер.
Имя хоста	Список имен хостов (через запятую), которые в данный момент используются сервером.
IP-адрес хоста	Список IP-адресов (через запятую), на которых сервер прослушивает ответы.

Показатель	Описание
Порт запросов	Порт, с которого сервер получает запросы от других серверов. Если сервер прослушивает отчеты с нескольких IP-адресов, порт запросов для сервера всегда будет одним и тем же. Если этот порт используется каким-то другим процессом, сервер не запустится. Проверьте, не используется ли этот порт другими процессами.
Занятые потоки на сервере	Число потоков на сервере, которые обслуживают запрос в данный момент. Если это число равно максимальному размеру пула потоков сервера, это указывает на то, что система не может параллельно обрабатывать дополнительные запросы, и новые запросы должны ожидать, пока занятые потоки не станут доступными.

Показатели аудита

Показатель	Описание
Текущее число проверяемых событий в очереди	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. **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.

Регистрация показателей службы

Показатель	Описание
Каталог протоколирования	Файлы журналов для сервера, доступные в этом местоположении.

36.1.2 Показатели центрального сервера управления

В таблице ниже приведены показатели сервера, которые отображаются на экране *Показатели* центральных серверов управления (CMS).

Показатели центрального сервера управления

Показатель	Описание
Соединение с базой данных аудита установлено	Указывает, есть ли работоспособное соединение сервера CMS к базе данных аудита. Значение «1» свидетельствует о наличии соединения. Значение «0» свидетельствует об отсутствии соединения с базой данных аудита. Если CMS играет роль аудитора, это значение должно быть равно «1». Если оно равно «0», следует определить, почему не удается установить соединение с базой данных аудита.

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)	Длительность последнего цикла опроса в секундах. Указывает максимальную задержку доставки данных о событии в базу данных аудита в течение предыдущего цикла опроса. • 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	Процентная доля цикла опроса, которую CMS затрачивает на сбор данных о проверяемых объектах. Все остальное время CMS находится в состоянии покоя между опросами. 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.
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.

Показатель	Описание
Число сеансов, установленных серверами	Число параллельных сеансов, созданных серверами платформы BI с помощью CMS. Если это число превышает 250, создайте дополнительный CMS.
Число сеансов, установленных всеми пользователями	Число параллельных сеансов, которые обрабатываются сервером CMS в момент загрузки экрана *Показатели*. Чем больше это число, тем больше пользователей работает в системе. Если это число превышает 250, создайте дополнительный CMS.
Задания, завершившиеся сбоем	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.
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.

Показатель	Описание
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.
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 удается 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.

Показатель	Описание
Существующие учетные записи именованных пользователей	Общее число имеющихся в кластере пользователей с именованными лицензиями на параллельный доступ.

36.1.3 Показатели сервера соединений

Для сервера соединений характерны следующие показатели.

Показатели службы соединений

Показатель	Описание
Источники данных	Создает список источников данных, активируемых на странице *Свойства*. Выводится следующая информация для каждой пары сетевого уровня и базы данных: • *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)* **Примечание** Для получения дополнительных сведений о пулах соединений см. *Руководство по доступу к данным*.

36.1.4 Показатели сервера событий

В следующей таблице приведены показатели сервера, которые отображаются на экране *Показатели* серверов событий.

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.

36.1.5 Показатели сервера репозитория файлов

В следующей таблице приведены показатели сервера, которые отображаются на экране *Показатели* серверов репозитория входных и выходных файлов.

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).

36.1.6 Показатели адаптивного сервера обработки

В следующей таблице приведены показатели сервера, которые отображаются на экране *Показатели* адаптивного сервера обработки.

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.

Показатель	Описание
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.
Процент остановленной системы в течение GC (последние 5 минут)	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. 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.
Процент остановленной системы в течение GC (последние 15 минут)	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. 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.
Количество ошибок страниц в течение GC (последние 5 минут)	Количество ошибок страниц, возникших во время сборки мусора в памяти в течение предыдущих пяти минут. Любое положительное число свидетельствует о высокой нагрузке на систему и недостатке в ней памяти.
Количество ошибок страниц в течение GC (последние 15 минут)	Количество ошибок страниц, возникших во время сборки мусора в памяти в течение предыдущих пятнадцати минут. Любое положительное число свидетельствует о высокой нагрузке на систему и недостатке в ней памяти.
Количество полных GC	Количество полных очисток памяти с момента запуска системы. Быстрое увеличение этого значения может свидетельствует о недостатке памяти в системе.

Показатель	Описание
Количество конфликтов при блокировках JVM	Количество синхронизованных объектов, в которых есть ожидающие доступа потоки. Любое значение, намного превышающее 0, может свидетельствовать о наличии потоков, которые больше не будут выполняться. Инициируйте дамп потоков, чтобы получить больше сведений о причине проблемы.
Сведения об отладке JVM	Доступны отладочные сведения о виртуальной машине Java SAP, включая данные о состоянии, номер порта, а также о прикрепленном клиенте (при его наличии).
Сведения о версии JVM	Сведения о версии виртуальной машины Java SAP.
Счетчик заблокированных потоков JVM	Количество заблокированных потоков. Любое значение, намного превышающее 0, свидетельствует о наличии потоков, которые больше не будут выполняться. Инициируйте дамп 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.

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.activeOLAPConnection Count	Число открытых соединений между клиентами OLAP и службой.

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.

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.

Показатель	Описание
Выполняемая индексация	TRUE, если выполняется индексация. В противном случае – значение FALSE.
Число индексированных документов	Отображений числа документов, индексированных с момента запуска службы.

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 MDAS и сервером.

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.
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.

Показатель	Описание
Число запросов на стадии оптимизации запроса	Общее число выполняющихся в настоящий момент запросов на стадии оптимизации.
Число запросов на стадии выполнения запроса	Общее число выполняющихся в настоящий момент запросов на стадии выполнения.
Число загруженных соединителей	Общее число блоков соединений, загруженных в службе.
Число активных соединений на загруженных блоках соединений	Общее число активных соединений на блоках соединений, загруженных в службе.
Служба объединения данных доступна	*TRUE*, если служба доступна. В противном случае этот параметр имеет значение *FALSE*.

Показатели службы соединений

Показатель	Описание
Источники данных	Списки в таблице являются источниками данных, активируемыми на странице *Свойства*. Выводится следующая информация для каждой пары сетевого уровня и базы данных: • 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) Для получения дополнительных сведений о пулах соединений см. *руководство по доступу к данным*.

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 CMC.

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 CMC в соответствующий момент времени. В другие моменты значение показателя может отличаться от настройки, установленной на странице CMC.
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.

Показатели службы веб-приложений BEx

Показатель	Описание
Число сеансов	Общее число активных сеансов в службе веб-приложений BEx.

36.1.7 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".

Показатели сервера контейнера веб-приложений

Показатель	Описание
Список выполняющихся средств связи WACS	Список всех работающих средств связи на сервере. Если отображаются не все коннекторы (HTTP, HTTPS и HTTP через прокси), то средство соединения не включено, или в нем возник сбой во время запуска.
Ошибка запуска одного или нескольких соединителей WACS	Показывает, имеются ли отказавшие соединители. 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.

Связанные сведения

Показатели адаптивного сервера обработки [страница 1247]

36.1.8 Показатели адаптивного сервера заданий

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*.
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 SFTP допустима	Принимает значение *TRUE*, если сервер может отправлять документы на целевой сервер SFTP, указанный в окне *Адресат* сервера. В противном случае этот параметр имеет значение *FALSE*. Несовпадение отпечатка ключа для сервера SFTP может вызвать проблемы.
Установка по умолчанию адресатов папки "Входящие" допустима	Принимает значение *TRUE*, если сервер может отправлять объекты в целевую папку "Входящие", указанную в окне *Адресат* сервера. В противном случае этот параметр имеет значение *FALSE*.
Установка по умолчанию адресатов эл. почты допустима	Принимает значение *TRUE*, если сервер может отправлять объекты по адресу электронной почты, указанному в окне *Адресат* сервера. В противном случае этот параметр имеет значение *FALSE*.
Службы планирования	Таблица, в которой представлены службы, выполняемые на сервере.
Дочерние элементы	Таблица, в которой представлены дочерние процессы, выполняемые на сервере.

В следующей таблице описываются показатели для каждой из служб планирования, выполняющихся на сервере.

Показатели службы планирования

Показатель	Описание
Служба планирования	Имя службы.

Показатель	Описание
Полученные запросы заданий	Количество заданий, которые предположительно выполняются на сервере.
Параллельные задания	Количество одновременно выполняющихся в службе заданий. Если это количество большое, служба занята.
Пиковые задания	Максимальное количество параллельных заданий, которые одновременно выполнялись на службе.
Максимально допустимое число параллельных заданий	Количество параллельно выполняемых независимых (дочерних) процессов, максимально допустимое для службы. Этот параметр задается в окне *Свойства* сервера.
Создания заданий, завершившиеся сбоем	Количество заданий в службе, в которых возник сбой.

В следующей таблице описываются показатели для каждого дочернего процесса, который выполняется на сервере.

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.
Сбой связи	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*.

36.1.9 Показатели Crystal Reports Server

В следующей таблице приведены показатели сервера, которые отображаются на экране *Показатели* для серверов обработки Crystal Reports и Crystal Reports 2020.

Показатели сервера обработки Crystal Reports

Показатель	Описание
Открытые задания	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 объекта InfoObject, обслуживаемого 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 (в килобайтах), 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.

Показатели кэш-сервера Crystal Reports

Показатель	Описание
Удачных обращений в кэш (%)	Процент запросов, относительно последних 500 запросов, выполненных с кэшированными данными.

Показатель	Описание
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 объекта InfoObject, используемого сервером в первую очередь. Значение этого показателя не меняется.
Среднее время обработки (мс)	Среднее время (в миллисекундах), затраченное сервером на обработку последних полученных им 500 запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.
Максимальное время обработки (мс)	Максимальное время (в миллисекундах), затраченное сервером на обработку одного из последних 500 запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.
Минимальное время обработки (мс)	Минимальное время (в миллисекундах), затраченное сервером на обработку одного из последних 500 запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.
Число запросов в очереди	Число обрабатываемых и ожидающих обработку запросов. Если это время постоянно велико и увеличивается, рассмотрите возможность создания дополнительных серверов на других компьютерах.
Имя DLL объекта	Имя подключаемого модуля обработки для сервера. Значение этого показателя не меняется.
Объем кэш-памяти	Объем данных (в килобайтах), кэшируемых в настоящий момент сервером на диск.
Число открытых соединений	Число соединений, открытых в данный момент между сервером и клиентами.
Передано данных (КБ)	Общий объем данных (в килобайтах), переданных клиентам с момента запуска сервера.

В следующей таблице приведены показатели сервера, которые отображаются на экране *Показатели* для серверов приложений отчетов Crystal Reports 2020.

Показатели сервера приложений отчетов Crystal Reports 2020

Показатель	Описание
metric_currentdoccount **Примечание** Этот показатель отображается на странице «Мониторинг» консоли CMC как «document_s_».	Количество документов, обрабатываемых в настоящий момент сервером.

Показатель	Описание
metric_totaldoccount **Примечание** Этот показатель отображается на странице «Мониторинг» консоли CMC как «document_s_».	Количество документов, обработанных сервером с момента его запуска.
metric_currentagentthreadcount **Примечание** Этот показатель отображается на странице «Мониторинг» консоли CMC как «agent thread_s_».	Количество потоков, обрабатываемых в настоящий момент сервером.
metric_totalagentthreadcount **Примечание** Этот показатель отображается на странице «Мониторинг» консоли CMC как «agent thread_s_».	Количество потоков, обработанных сервером с момента его запуска.

36.1.10 Показатели сервера Web Intelligence

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.

Показатель	Описание
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.
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).

37 Приложение заполнителя сервера и узла

37.1 Заполнители сервера и узлов

За исключением *%SERVER_FRIENDLY_NAME%* и *%SERVER_NAME%*, эти заполнители относятся ко всем серверам на одном узле.

> **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%*

> **Предупреждение**
>
> Заполнители, отличные от предназначенных для редактирования, не следует изменять ни в коем случае. Системный администратор должен обеспечить, чтобы права на редактирование в узле были только у соответствующих лиц из группы администраторов (которые предназначены для управления узлом). Для всех остальных пользователей, включая других членов группы администраторов, должны быть установлены ограничения на просмотр объектов узла или управление ими путем применения соответствующих прав безопасности. Если какое-либо значение заполнителя случайно повреждено и CMS не появляется, см. SAP-ноту 3269127.

> **Примечание**
>
> См. статью 3278916 в базе знаний SAP, чтобы узнать, как ограничить изменяемые заполнители, чтобы избежать возможного вредоносного вмешательства в ландшафт BI.

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_bobj/enterprise_xi40/<платформа>/`
%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_bobj/enterprise_xi40/<платформа>/`
%CACHESERVER_EXE%	Имя исполняемого файла кэш-сервера Crystal Reports.	В ОС Windows это `crcache.exe`. В ОС Unix: `boe_crcached.bin`.
%CMS_EXE%	Имя исполняемого файла центрального сервера управления.	В ОС Windows это `cms.exe`. В ОС UNIX это `boe_cmsd`.
%CONNECTIONSERVER32_EXE%	Имя исполняемого файла 32-битного сервера соединений.	В Windows, `ConnectionServer32.exe`. В UNIX, `ConnectionServer32`.
%CONNECTIONSERVER_DIR%	Корневая папка сервера соединений.	В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer`. В UNIX: `<INSTALLDIR>/sap_bobj/enterprise_xi40/dataAccess/connectionServer`
%CONNECTIONSERVER_EXE%	Имя исполняемого файла 64-битного сервера соединений.	В ОС Windows это `ConnectionServer.exe`. В UNIX это `ConnectionServer`.

Заполнитель	Описание	Значения по умолчанию
%CRCPP_BINDIR%	Каталог, где расположены двоичные файлы сервера Crystal Reports C++.	В Windows: `<INSTALLDIR>\SAP BusinessObjectsEnterprise XI 4.0\win32_x86`. В UNIX каталог будет аналогичным следующему: `<INSTALLDIR>/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9`.
%CRCPP_DefaultWorkingDir%	Рабочий каталог по умолчанию для серверов Crystal Reports C++.	В Windows: `<INSTALLDIR>\SAP BusinessObjectsEnterprise XI 4.0\win32_x86`. В UNIX каталог будет аналогичным следующему: `<INSTALLDIR>/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9`.
%CRYSTALRAS_EXE%	Имя исполняемого файла сервера Report Application Server.	В ОС Windows это `crystalras.exe`. В ОС UNIX это `boe_crystalrasd`.
%CR_ODBCINI%	Полное имя (включая путь) файла `.odbc.ini`. **	В UNIX это `<INSTALLDIR>/bobje/odbc.ini`. Для Windows это пустая строка.
%CommonJavaBundlesDir%	Папка, где находится OSGI.	В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bundles`. В UNIX: `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/lib/bundles`.
%CommonJavaLibDir%	Папка, где находятся общие библиотеки Java.	В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib`. В UNIX: `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/lib`.
%DLLEXT%	Расширение по умолчанию `DLL`- или `SO`-файла.	В ОС Windows это `.dll`. В ОС UNIX это `.so`.
%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».

Заполнитель	Описание	Значения по умолчанию
%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-битных 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 «:».
%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: `<INSTALLDIR>/sap_bobj/data/Auditing/`.
%DefaultDataDir%	Временный каталог, используемый сервером заданий.	В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Data`. В UNIX: `<INSTALLDIR>/sap_bobj/data/`.

Заполнитель	Описание	Значения по умолчанию
%DefaultInputFRSDir%	Корневая папка на сервере репозитория входных файлов.	В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\FileStore\Input`. В UNIX: `<INSTALLDIR>/sap_bobj/data/frsinput`.
%DefaultLoggingDir%	Местоположение, где хранятся файлы журнала.	В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging`. В UNIX: `<INSTALLDIR>/sap_bobj/logging`.
%DefaultOutputFRSDir%	Корневая папка на сервере репозитория входных файлов.	В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\FileStore\Output`. В UNIX: `<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: `<INSTALLDIR>/sap_bobj/enterprise_xi40/<платформа>`.
%DefaultWorkingDir32%	Рабочий каталог для 32-битных серверов.	В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. В UNIX: `<INSTALLDIR>/sap_bobj/enterprise_xi40/<платформа>`.
%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`.
%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».

Заполнитель	Описание	Значения по умолчанию
%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: `<INSTALLDIR>/sap_bobj/enterprise_xi40`.
%EnterpriseDir32%	Местоположение, где установлена 32-битная версия платформы SAP BusinessObjects Business Intelligence.	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 исполняемого 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, где установлена 32-битная версия платформы SAP BusinessObjects Business Intelligence.	Это значение задается во время установки.
%IntroscopeAgentEnableInstrumentation%	Указывает, включены ли инструментальные средства для серверов Java, которые используют агент Introscope Agent Enterprise.	Допустимы значения TRUE и FALSE. Значение зависит от того, был ли включен диспетчер Introscope Agent Enterprise во время установки платформы SAP BusinessObjects Business Intelligence.
%IntroscopeAgentEnterpriseManagerHost%	Имя хоста диспетчера Introscope Agent Enterprise, куда отправляются данные инструментальных средств.	Это значение задается во время установки.
%IntroscopeAgentEnterpriseManagerPort%	Имя хоста диспетчера Introscope Agent Enterprise, куда отправляются данные инструментальных средств.	Это значение задается во время установки.

Заполнитель	Описание	Значения по умолчанию
%IntroscopeAgentEnterpriseManagerTransport%	Транспорт, используемый при отправке данных инструментальных средств диспетчеру Introscope Agent Enterprise. Допустимые значения: • TCP • HTTP • HTTPS • SSL	TCP
%IntroscopeAgentEnterpriseManagerTransportHTTP%	Класс, используемый при отправке данных инструментальных средств диспетчеру Introscope Agent Enterprise через HTTP.	com.wily.isengard.postofficehub.link.net.HttpTunnelingSocketFactory
%IntroscopeAgentEnterpriseManagerTransportHTTPS%	Класс, используемый при отправке данных инструментальных средств диспетчеру Introscope Agent Enterprise через HTTPS.	com.wily.isengard.postofficehub.link.net.HttpTunnelingSocketFactory
%IntroscopeAgentEnterpriseManagerTransportSSL%	Класс, используемый при отправке данных инструментальных средств диспетчеру Introscope Agent Enterprise через SSL.	com.wily.isengard.postofficehub.link.net.SSLSocketFactory
%IntroscopeAgentEnterpriseManagerTransportTCP%	Класс, используемый при отправке данных инструментальных средств диспетчеру Introscope Agent Enterprise через TCP.	com.wily.isengard.postofficehub.link.net.DefaultSocketFactory
%IntroscopeDir%	Папка, в которой установлен Introscope Agent Enterprise Manager.	В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\wily`. В UNIX: `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/wily`.
%JAVAW_EXE%	Имя исполняемого файла для виртуальной машины Java, в которой нет окна консоли.	В ОС Windows это `javaw.exe`. В ОС UNIX это `java`.
%JAVA_EXE%	Имя исполняемого файла для виртуальной машины Java.	В ОС Windows это `java.exe`. В ОС UNIX это `java`.
%JOBSERVERCHILD_EXE%	Имя исполняемого файла дочернего настраиваемого сервера заданий.	В ОС Windows это `JobServerChild.exe`. В ОС UNIX это `boe_jobcd`.
%JOBSERVER_EXE%	Имя исполняемого файла настраиваемого сервера заданий.	В ОС Windows это `JobServer.exe`. В ОС UNIX это `boe_jobsd`.

Заполнитель	Описание	Значения по умолчанию
%JdkBinDir%	Папка, где находятся двоичные файлы JDK.	В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`. В UNIX: `<INSTALLDIR>/sap_bobj/<ПЛАТФОРМА>/sapjvm/bin`.
%JreBinDir%	Папка, где находятся двоичные файлы JRE.	В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\bin`. В UNIX: `<INSTALLDIR>/sap_bobj/<ПЛАТФОРМА>/sapjvm/jre/bin`.
%JVM_ARCH_ENVIRONMENT%	Указывает, на какой JVM работает компьютер: 32-битной или 64-битной.	Для компьютеров с 32-битной ОС UNIX используется значение по умолчанию «-d32». Для 64-битных компьютеров используется значение по умолчанию «-d64». Для компьютеров с ОС Windows это пустая строка.
%JVM_HEADLESS_MODE%	Аргумент командной строки, который указывает, работает ли JVM в режиме с неполным набором устройств ввода-вывода.	В ОС Windows -Djava.awt.headless=false. В ОС UNIX -Djava.awt.headless=true
%JVM_HEAP_DUMP_ON_OUT_OF_MEMORY_ERROR%	Параметры командной строки, задающие поведение JVM при обнаружении ошибок "Недостаточно памяти".	"-XX:+HeapDumpOnOutOfMemoryError" "-XX:HeapDumpPath=%DefaultLoggingDir%" "-XX:+ExitVMOnOutOfMemoryError"
%JVM_SHARED_MEMORY_SEGMENT%	Параметры командной строки для включения расширений JVM и задания номера экземпляра JVM.	По умолчанию этот заполнитель является пустым.
%LANGUAGEPACKSDIR%	Папка, в которой хранятся языковые пакеты развертывания.	В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Languages`. В UNIX: `<INSTALLDIR>/sap_bobj/enterprise_xi40/Languages/`.
%LANGUAGEPACKSDIR32%	Папка, в которой установлены языковые пакеты развертывания в 32-битных системах.	. В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Languages`. В UNIX: `<INSTALLDIR>/sap_bobj/enterprise_xi40/Languages/`.

Заполнитель	Описание	Значения по умолчанию
%LSTDir%	Папка, в которой хранятся файлы конфигурации LST.	В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\lst`. В UNIX: `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/lst`.
%MDAS_JVM_OS_STACK_SIZE%	Указывает размер стека JVM для Multi-Dimensional analysis service.	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 2020.	В ОС Windows это `crproc.exe`. В UNIX это `boe_crprocd.bin`.
%PJSContainerDir%	Папка, в которой расположены JAR-файлы контейнера APS.	В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container`. В UNIX: `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/pjs/container`.
%PJSServicesDir%	Папка, в которой расположены JAR-файлы службы APS.	В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services`. В UNIX: `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/pjs/services`.
%Platform%	Операционная система компьютера, на котором выполняется платформа SAP BI.	Операционная система компьютера, на котором выполняется платформа SAP BI.
%Platform32%	Операционная система компьютера, на котором выполняется 32-битная версия платформы SAP BI.	Операционная система компьютера, на котором выполняется платформа SAP BI.
%RasBinDir%	Корневая папка сервера приложений отчетов.	В Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. В UNIX: `<INSTALLDIR>/sap_bobj/enterprise_xi40/<ПЛАТФОРМА>/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.

Заполнитель	Описание	Значения по умолчанию
%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>/sap_bobj/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>/sap_bobj/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`.
%WEBI_LD_PRELOAD_ONCE%	Имя переменной среды LD_PRELOAD_ONCE для платформы.	$LD_PRELOAD_ONCE$

Связанные сведения

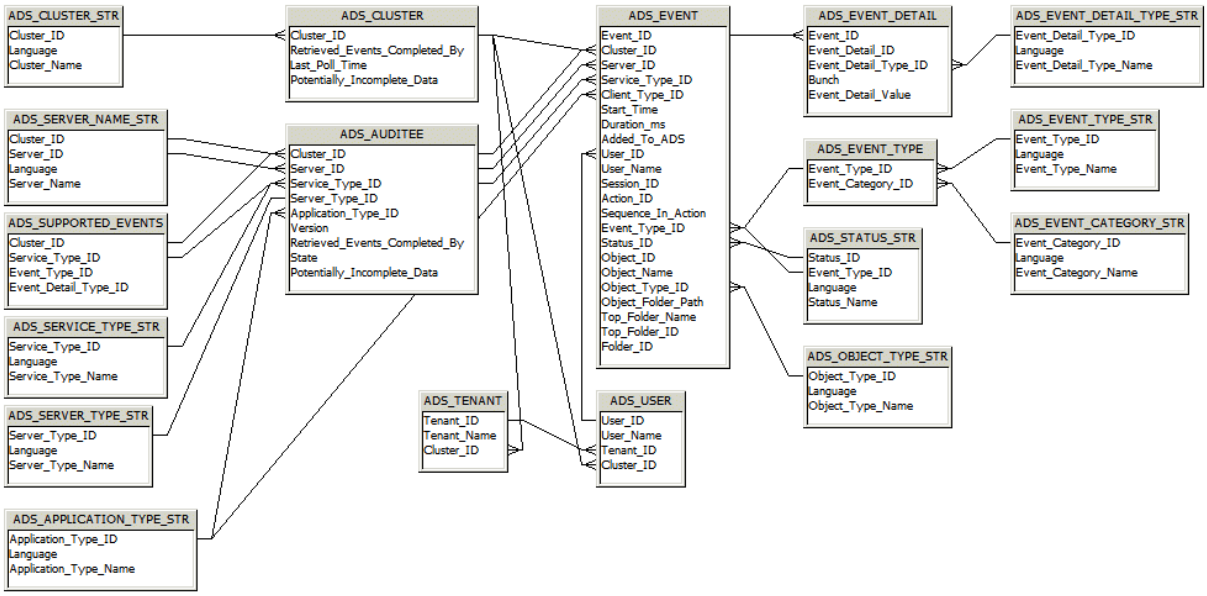
Просмотр и изменение заполнителей для узла [страница 522]

38 Приложение выполнения аудита схемы хранилища данных

38.1 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.

38.2 Диаграмма схемы



38.3 Auditing Data Store Tables

ADS_APPLICATION_TYPE_STR table

This table provides a multilingual dictionary of client application-type names.

Column Name	Type	Description
Application_Type_ID	Character (64)	The application-type CUID for the application.
Language	Character (10)	Code for the language in which the application type is recorded; for example `<EN>`, or `<DE>`.
Application_Type_Name	Character (255)	The text name of the application type; Crystal Reports or Web Intelligence for example.

ADS_AUDITEE table

This table records property information for all auditee servers that are part of the deployment.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID for the cluster the auditee belongs to.
Server_ID	Character (64)	CUID of the server that triggered the event. If the event is client-triggered, will record the CUID of the adaptive processing server that processed the event.
Service_Type_ID	Character (64)	Service-type CUID of the service that triggered the event. Client-triggered events will record an application-type CUID.
Server_Type_ID	Character (64)	The server-type CUID for the server that triggered the event.
Application_Type_ID	Character (64)	The application-type CUID for the client that triggered the event. For server events, the ID of the service-type will be recorded.
Version	Character (64)	The version of the server or client that triggered the event at the time it was recorded.
Retrieved_Events_Completed_By	Datetime	The last time the Auditor CMS polled this auditee for its temporary files. This indicates that all events from this auditee competed prior to this date/time are in the ADS.
State	Integer	The state (Running, Not Running, Deleted) that the auditee was in.
Potentially_Incomplete_Data	Integer	Shows if this auditee may have events that were not transferred to the ADS.

ADS_CLUSTER table

This table records information on any clusters that contain Auditees.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster.

Column Name	Type	Description
Retrieved_Events_Completed_By	Datetime	Shows how current the auditing information in the database for that cluster is. Records the oldest retrieved auditing timestamp for all currently running auditee servers at any given moment. This indicates all events completed prior to this date are in the ADS.
Last_Poll_Time	Datetime	The last time the auditor CMS polled the auditees in this cluster.
Potentially_Incomplete_Data	Integer	Indicates potentially incomplete audit information within the cluster: "0" = all servers have transferred data normally; and "1" = at least one running or non-running server in the cluster has its *Potentially Incomplete Data* flag set, meaning that one auditee has events that haven't transferred to the ADS.

ADS_CLUSTER_STR table

This table provides a reference record of the different clusters in your deployment.

Column Name	Type	Description
Cluster_ID	Character (64)	A unique ID of the cluster.
Language	Character (10)	Code for the language setting for the cluster, for example, `<EN>`, or `<DE>`.
Cluster_Name	Character (255)	The name of the cluster.

ADS_EVENT table

This table records the basic properties for each event, and is the central linking point for other tables in the schema.

Column Name	Type	Description
Event_ID	Character (64)	A unique ID generated for the event.
Cluster_ID	Character (64)	The GUID of the auditee's cluster. This is recorded because multiple clusters may use the same ADS.
Server_ID	Character (64)	The CUID of the server that triggered the event.
Service_Type_ID	Character (64)	• The CUID of the service-type that triggered the event. Services on a server will record their service-type CUID. • Client applications (BI launch pad or Web Intelligence for example) will record their application-type CUID.
Client_Type_ID	Character (64)	Records the Client Type ID of the client that established the session.

Column Name	Type	Description
Start_Time	Datetime	The date and time (UTC) when the event operation started (including milliseconds).
Duration_ms	Integer	Duration of operation in milliseconds. Value may be zero (0) for certain events. For Example: with View event type, if the document gets loaded quickly, the value will be `0`.
Added_to_ADS	Datetime	The date and time (UTC) when the event was recorded in the ADS.
User_ID	Character (64)	The CUID of the user who performed the action.
User_Name	Character (255)	The name associated with the ID of the user who performed the action. Recorded in the Auditor CMS's default language.
Session_ID	Character (64)	GUID of the session during which the event was triggered. If there is no associated session, the field will be null.
Action_ID	Character (64)	ID of the user action that triggered the event. Used to group events that result from a single user action.
Sequence_In_Action	Integer	For multi-server (or client and multi-server) events, the server or client application in the sequence that triggered the event. In all scheduling workflows the sequence ID will always be 0.
Event_Type_ID	Integer	Type of event (View or Save, for example).
Status_ID	Integer	Status of the operation (for example, "0" = succeeded, "1" = failed).
Object_ID	Character (64)	CUID of the object that the operation was performed on.
Object_Name	Character (255)	The name of the object the operation was performed on. Recorded in the Auditor CMS's default language.
Object_Type_ID	Character (64)	CUID of object-type that the operation was performed on.
Object_Folder_Path	Character (255)	The full folder path (for example `Country/Region/City`) for the object the operation was performed on. Recorded in the Auditor CMS's default language. If the folder path cannot be determined this, value will be set to null.
Folder_ID	Character (64)	The CUID of the folder for the object the operation was performed.
Top_Folder_Name	Character (255)	Name of top level folder for the object. For example, if the object is located in `Country/Region/City` then `Country` will be recorded.
Top_Folder_ID	Character (64)	The CUID of the top-level folder where the object resides. For example, if object is located in `Country/Region/City` then the CUID of the `Country` folder will be recorded.

ADS_EVENT_CATEGORY_STR Table

This table provides a multilingual dictionary of event category names.

Column Name	Type	Description
Event_Category_ID	Integer	The event-category ID.
Language	Character (10)	Code for the language that the event category name is recorded in; for example `<EN>`, or `<DE>`.
Event_Category_Name	Character (255)	The name of the event category.

ADS_EVENT_DELETES

Do not use or report off of this table. It is intended for internal system use, and may be removed in future releases.

ADS_EVENT_DETAIL table

This table records event detail properties.

Column Name	Type	Description
Event_Detail_ID	Integer	GUID for the event detail.
Event_ID	Character (64)	Parent event GUID.
Event_Detail_Type_ID	Integer	Type of event detail.
Bunch	Integer	If the detail is part of a series, this is used to tie them together. For example, if a report had prompts for State and Country, a user may enter "USA" for the Country prompt, and "California" and "Nevada" for the State prompt. This would produce event details with two bunches. Bunch 1 would consist of: • Prompt Name: Country • Prompt Value: USA Bunch 2 would consist of: • Prompt Name: State • Prompt Value: California • Prompt Value: Nevada
Event_Detail_Value	Character (longtext)	The value of the event detail.

ADS_EVENT_DETAIL_TYPE_STR table

This table provides a multilingual dictionary of event detail type names.

Column Name	Type	Description
Event_Detail_ID	Integer	The event detail-type ID for the event detail.
Language	Character (10)	Code for the language that the event detail name is recorded in; for example `<EN>`, or `<DE>`.
Event_Detail_Type_Name	Character (255)	The text name of the event detail type.

ADS_EVENT_TYPE table

This table provides a reference record for the different categories of events.

Column Name	Type	Description
Event_Type_ID	Integer	The unique identifier for the type of event.
Event_Category_ID	Integer	Category of event. For example, common, Web Intelligence, or Life-Cycle Management.

ADS_EVENT_TYPE_STR Table

This table provides a multilingual dictionary of event type names.

Column Name	Type	Description
Event_Type_ID	Integer	The event-type ID for the event.
Language	Character (10)	Code for the language that the event category name is recorded in; for example `<EN>`, or `<DE>`.
Event_Type_Name	Character (255)	The text name of the event type; View or Logon for example.

ADS_OBJECT_TYPE_STR Table

This table provides a multilingual dictionary of event object names.

Column Name	Type	Description
Object_Type_ID	Character (64)	Object-type CUID of the object
Language	Character (10)	Code for the language that the object type name is recorded in; for example `<EN>`, or `<DE>`.
Object_Type_Name	Character (255)	Name of the object type.

ADS_SERVER_NAME_STR table

This table provides a multilingual dictionary of server names. Values will be updated when servers are renamed.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster that the server belongs to.
Server_ID	Character (64)	The CUID of the server.
Language	Character (10)	Code for the language of the server name; for example `<EN>`, or `<DE>`.
Server_Name	Character (255)	The name of the server.

ADS_SERVICE_TYPE_STR table

This table provides a multilingual dictionary of service-type names.

Column Name	Type	Description
Service_Type_ID	Character (64)	The service-type or service-category CUID for the service.
Language	Character (10)	Code for the language the service-type name is recorded in, for example `<EN>`, or `<DE>`.
Service_Type_Name	Character (255)	The name of the service-type.

ADS_STATUS_STR Table

This table provides a multilingual dictionary of event status names.

Column Name	Type	Description
Status_ID	Integer	The numerical representation of the operation's status.
Event_Type_ID	Integer	ID of the event's event-type. For example, 1002 for View.
Language	Character (10)	Code for the language that the event status is recorded in; for example `<EN>`, or `<DE>`.
Status_Name	Character (255)	A text description of the event's status; Succeeded or Failed, for example.

ADS_SUPPORTED_EVENTS table

This table records a list of supported events and associated event details for each type of service or client application.

Column Name	Type	Description
Cluster_ID	Character (64)	The cluster GUID that the service belongs to.
Service_Type_ID	Character (64)	Service-type CUID of the service that triggered the event. If the event is triggered by a client application, then an application-type CUID is recorded.
Event_Type_ID	Integer	ID for the type of event recorded (ID of Save, for example).
Event_Detail_Type_ID	Integer	CUID that identifies the type of event detail captured for that event (File Path, for example).

ADS_TENANT Table

This table records the relationship between tenant names and tenant IDs.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster.
Tenant_ID	Character (64)	The CUID of the tenant.
Tenant_Name	Character (255)	The name of the tenant.

ADS_USER Table

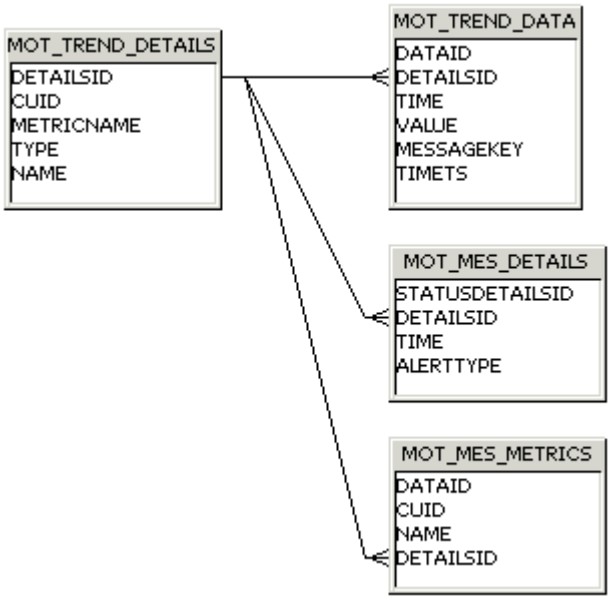
This table records the relationship between users and tenants.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster.
User_ID	Character (64)	The CUID of the user.
User_Name	Character (255)	The name of the user.
Tenant_ID	Character (64)	The CUID of the tenant.

39 Приложение "Схема базы данных мониторинга"

39.1 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

Имя столбца	Тип	Ключ	Описание
MetricName	VARCHAR(255)	Нет данных	Имя показателя
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 доступно значение "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

40 Приложение "Рабочая таблица системной копии"

40.1 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.	
Версия, пакет поддержки и уровень исправлений.	
Расположения хранения файлов для каждого репозитория входящих и исходящих файлов FRS в развертывании.	
Местоположение папки базы данных Диспетчера переноса объектов и папок Subversion, если планируется копировать Диспетчер переноса объектов.	
Местоположение папки базы данных мониторинга, если планируется копировать базу данных мониторинга.	

Свойство	Значение
Путь к папке семантического уровня.	

Важные положения об отказе от ответственности в отношении правовых вопросов

Гиперссылки

Некоторые ссылки обозначаются значком и/или текстом, отображаемым при наведении мыши. Эти ссылки обеспечивают доступ к дополнительной информации.
Подробнее о значках:

- Ссылки со значком Вы собираетесь перейти на сайт, размещенный не на сервере SAP. Используя такие ссылки, вы соглашаетесь (если иное не оговорено особо в соглашениях с SAP) со следующим:
  - Сайт по ссылке не содержит документацию SAP. Не разрешается подавать рекламации в отношении любых продуктов SAP на основе содержащейся на таком сайте информации.
  - SAP не выражает ни согласия, ни несогласия с информацией, содержащейся на сайте по ссылке, а также не гарантирует ее доступность и правильность. SAP не несет ответственности за любой ущерб, вызванный использованием такой информации, за исключением тех случаев, когда такой ущерб вызван намеренными нарушениями или халатностью со стороны компании SAP.
- Ссылки со значком Вы закрываете документацию по определенному продукту или сервису SAP и переходите на веб-сайт, расположенный на сервере SAP. Используя такие ссылки, вы соглашаетесь (если иное не оговорено особо в соглашениях с SAP) с тем, что не разрешается подавать рекламации в отношении любых продуктов SAP на основе содержащейся на таком сайте информации.

Видео-ролики, размещенные на внешних платформах

Некоторые видео-ролики могут указывать на сторонние платформы размещения видео-роликов. SAP не может гарантировать в будущем доступность видео-роликов, сохраненных на этих платформах. Кроме того, любые рекламные объявления или другой контент, размещенные на этих платформах (например, предлагаемые видео-ролики или ссылки на другие видео-ролики, размещенные на одном сайте), не входят в сферу управления или ответственности SAP.

Бета-версии и другие экспериментальные функции

Экспериментальные функции не являются частью официально поставляемого SAP объема, гарантируемого для будущих версий. Это означает, что экспериментальные функции могут быть изменены компанией SAP в любое время и по любой причине без предварительного уведомления. Экспериментальные функции не предназначены для продуктивного использования. Не разрешается демонстрировать, тестировать, проверять, анализировать или иначе использовать экспериментальные функции в фактической операционной среде либо с использованием данных, для которых не выполнено резервное копирование.
Экспериментальные функции предназначены для получения обратной связи, которая позволяет нашим клиентам и партнерам влиять на разработку будущих продуктов. Предоставляя обратную связь (например, в SAP Community), вы соглашаетесь с тем, что права на интеллектуальную собственность относительно ваших отзывов и производных работ останутся в исключительной собственностью SAP.

Пример кода

Примером кода является любой код и/или фрагменты кода программного обеспечения. Они не предназначены для продуктивного использования. Этот код предназначен только для пояснения и иллюстрирования синтаксиса и правил составления текста программ. SAP не гарантирует правильность и полноту примеров кода. SAP не несет ответственности за любые ошибки и ущерб, вызванные использованием примеров кода, за исключением тех случаев, когда такой ущерб вызван намеренными нарушениями или халатностью со стороны компании SAP.

Язык, свободный от предрассудков

SAP поддерживает культуру многообразия и инклюзивности. Когда это возможно, в нашей документации мы используем безоценочный язык для обозначения людей из любой культуры или этнической группы, любого пола и уровня способностей.

www.sap.com/contactsap

© SAP SE или аффилированная компания SAP, 2024. 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 SE или аффилированной компании SAP запрещены. Информация, содержащаяся в настоящей публикации, может быть изменена без предварительного уведомления.

Некоторые программные продукты, предлагаемые на рынке компанией SAP SE 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 SE и ее аффилированной компанией исключительно в информационных целях, без предоставления каких-либо гарантий. Компания SAP или ее аффилированные компании не несут ответственности за ошибки или пропуски в настоящих материалах. Гарантии, если таковые предоставляются, в отношении продуктов и услуг компании SAP или ее аффилированной компании 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 упомянутые здесь продукты и услуги SAP, как и соответствующие логотипы, являются товарными знаками или зарегистрированными товарными знаками SAP SE (или аффилированной компании SAP) на территории Германии и других стран. Все иные названия продуктов и услуг являются товарными знаками соответствующих компаний.

Для получения дополнительной информации и уведомлений о товарных знаках см. https://www.sap.com/cis/about/legal/trademark.html.

THE BEST RUN SAP