

IBM Business Monitor



Руководство по установке IBM Business Monitor

версия 7.5.0

IBM Business Monitor



Руководство по установке IBM Business Monitor

версия 7.5.0

Содержание

Глава 1. Установка IBM Business Monitor 1

Глава 2. Планирование установки IBM Business Monitor. 3

Выбор подходящих топологий	3
Топология с одним сервером	3
Топология высокой готовности (сетевое развертывание)	3
Использование предварительно необходимого программного обеспечения.	9
Профайлы	9
Выбор типа профайла	10
Замечания о базе данных	12
Особенности базы данных MONITOR для DB2	14
Особенности базы данных COGNOSCS для DB2	16
Особенности базы данных MONITOR для DB2 for z/OS	16
Особенности базы данных MONITOR для Oracle	18
Особенности базы данных COGNOSCS для Oracle	19
Особенности базы данных MONITOR для Microsoft SQL Server.	21
Особенности базы данных COGNOSCS для Microsoft SQL Server	22
Права доступа к базе данных.	23
Замечания о реестре пользователей.	25
Замечания об обычных пользователях.	25
Примеры путей установки.	26
Установочный каталог для топологии с одним сервером	27
Путь установки для топологии сетевого развертывания с шаблонами среды развертывания.	27
Путь установки для пользовательской топологии сетевого развертывания	28
Установочные каталоги для управляемой среды развертывания для WebSphere Business Modeler	29
Обзор задачи: Установка и настройка	30

Глава 3. Подготовка к установке 33

Требования к аппаратному и программному обеспечению	33
Подготовка операционных систем к установке продукта	33
Подготовка систем AIX к установке	33
Подготовка систем HP-UX к установке	34
Подготовка систем Linux к установке	35
Подготовка систем Solaris к установке.	37
Подготовка систем Windows к установке	38

Глава 4. Установка IBM Business Monitor 39

Установка программного обеспечения IBM Business Monitor	39
Установка из панели запуска продукта	39

Установка IBM Business Monitor без вывода сообщений.	44
Работа с IBM Installation Manager	45
Установка Information Center	49

Глава 5. Создание баз данных 53

Создание или настройка сценариев базы данных с помощью инструмента проектирования базы данных	54
Настройка сценариев базы данных вручную	56
Установка баз данных вручную	59
Создание таблиц службы сообщений вручную	60

Глава 6. Создание и дополнение профайлов. 61

Создание и расширение профайлов с помощью Инструмента управления профайлами.	61
Создание автономных профайлов	62
Создание профайлов администратора развертывания	69
Дополнение профайлов диспетчера развертывания	75
Создание индивидуальных профайлов для узлов	79
Расширение индивидуальных профайлов для узлов	82
Создание и дополнение профайлов с помощью команды manageprofiles	84

Глава 7. Проверка установки. 87

Глава 8. Определение портов 89

Глава 9. Настройка среды 91

Создание среды разработки с помощью шаблона	91
Импортирование определений среды развертывания, основанных на документах эскиза	98
Создание среды разработки с помощью пользовательской топологии	104
Создание кластеров IBM Business Monitor	104
Настройка служб событий CEI	106
Настройка среды с помощью мастера настройки	107
Настройка среды с помощью команд wsadmin	113
Настройка среды вручную	116

Глава 10. Настройка компонентов IBM Business Monitor. 129

Настройка IBM Cognos BI	129
Настройка новой службы IBM Cognos BI	129
Настройка существующей службы IBM Cognos BI	130
Настройка IBM Cognos BI с WebSphere Portal	131
Настройка виджетов IBM Business Monitor для WebSphere Portal	133
Настройка способа получения событий	133
Сведения об асинхронных событиях	133
Получение событий из CEI	135
Настройка Business Space	141
Настройка Business Space	141

Миграция Business Space (заключительные задачи миграции продукта)	267
Настройка бизнес-пространства для работы с Mashup Center	268
Настройка виджетов для работы в WebSphere Portal	270
Настройка конфигурации мониторинга задачи пользователя	278
Установка модели монитора неавтоматизированных задач вручную	278
Разрешение событий для мониторинга задачи пользователя	279
Настройка соединений Business Space в WebSphere Portal	279
Настройка соединений для сводных панелей, основанных на портлетах	280

Настройка модели монитора глобальных процессов	280
Установка модели монитора глобальных процессов вручную	280
Включение событий в модели монитора глобальных процессов	281
Настройка сводных панелей для модели монитора глобальных процессов	282

Глава 11. Установка демонстрационной модели 285

Глава 12. Удаление IBM Business Monitor из системы 287

Удаление IBM Business Monitor из системы	287
Удаление демонстрационной модели	288

Глава 1. Установка IBM Business Monitor

IBM® Business Monitor может быть установлен на нескольких топологиях. Можно установить все компоненты на одном сервере или распределить компоненты по разным серверам. Для создания среды высокой готовности с поддержкой автоматического переноса ресурсов в случае сбоя можно установить IBM Business Monitor в кластерную среду, использующую механизм кластеризации WebSphere Application Server или Process Server.

Важное замечание: IBM Business Monitor работает на нескольких платформах. Сведения о поддерживаемых операционных системах и аппаратном обеспечении, необходимом объеме оперативной и дисковой памяти можно найти на странице: Системные требования для IBM Business Monitor.

Глава 2. Планирование установки IBM Business Monitor

В состав IBM Business Monitor входят несколько компонентов, которые могут быть установлены как на одном сервере, так и на нескольких серверах в сети. В ходе установки можно выбрать различные варианты. При планировании установки IBM Business Monitor необходимо рассмотреть доступные варианты и способы развертывания компонентов в сети.

Предоставляется справочная информация, которая поможет вам определить, какая топология больше всего подходит для вашей среды, и понять, какие опции доступны во время установки.

Перед тем, как приступить к установке IBM Business Monitor, ознакомьтесь со следующей информацией:

Выбор подходящих топологий

IBM Business Monitor может быть установлен в различных конфигурациях. Предусмотрено несколько основных топологий. Возможно, их потребуется настроить для вашей среды.

Следующие топологии иллюстрируют некоторые общие варианты установки, позволяя понять, какие возможные конфигурации развертывания могут существовать:

Топология с одним сервером

При использовании топологии с одним сервером все поддерживаемые продукты и все компоненты IBM Business Monitor устанавливаются на один и тот же физический сервер.

Установка IBM Business Monitor на единственном сервере идеальна для сред тестирования разработки, сред опытных образцов и простых конфигураций развертывания, которые не требуют переключения и поддержки высокой готовности.

Программа установки IBM Business Monitor позволяет установить IBM Business Monitor и WebSphere Application Server. При установке IBM Business Monitor на отдельный сервер также устанавливается служба Cognos. Для просмотра отслеживаемых данных можно использовать бизнес-пространство или сводные панели на основе портлетов.

После установки IBM Business Monitor создайте автономный профайл для определения среды выполнения. Все необходимые компоненты IBM Business Monitor будут созданы, когда вы будете создавать или дополнять автономный профайл.

Топология высокой готовности (сетевое развертывание)

IBM Business Monitor использует возможности высокой готовности в средах сетевого развертывания (ND) WebSphere Application Server или Process Server. Сетевое развертывание предоставляет такие общие требования к среде разработки, как распределение, масштабируемость и надежность. В среде сетевого развертывания можно совместно использовать группу серверов, чтобы обеспечить распределение рабочей нагрузки и отказоустойчивость. Серверы управляются централизованно, с одной административной консоли.

IBM Business Monitor использует ту же модель архитектуры, что и WebSphere Application Server и Process Server. С помощью этой модели создавайте среды, состоящие из ячеек, узлов и серверов, а также по выбору кластеров.

Если вы выберете один из имеющихся шаблонов среды развертывания (одно- или четырехкластерный), то мастер среды развертывания поможет вам настроить необходимые кластеры, серверы и компоненты.

Ячейка - это главный административный домен. Можно представлять себе ячейку как логическую группу серверов, кластеров или и тех, и других. (Кластер - это группа серверов приложений, работающих вместе для распределения рабочей нагрузки и передачи управления в случае неполадки.) С помощью серверов и кластеров можно установить IBM Business Monitor в ячейку, которая поддерживает высокую готовность и масштабируемость.

Управляемый узел (узел в ячейке) содержит один или несколько серверов. Каждый сервер предоставляет среду выполнения. Управляемые серверы создаются в управляемом узле, который, в свою очередь, определяется пользовательским профилем. Все управляемые узлы интегрированы в одном администраторе развертывания, и администратор развертывания управляет всеми управляемыми узлами в ячейке. Серверы могут быть сгруппированы в кластеры, которые также управляются администратором развертывания. В среде сетевого развертывания необходимо распространить приложения между кластерами, чтобы повысить отказоустойчивость отдельных серверов (высокая готовность) и распределить рабочую нагрузку приложения между несколькими эквивалентными серверами (распределение рабочей нагрузки).

Дополнительная информация о высокой готовности приведена в разделе "Сведения о высокой готовности и распределении рабочей нагрузки".

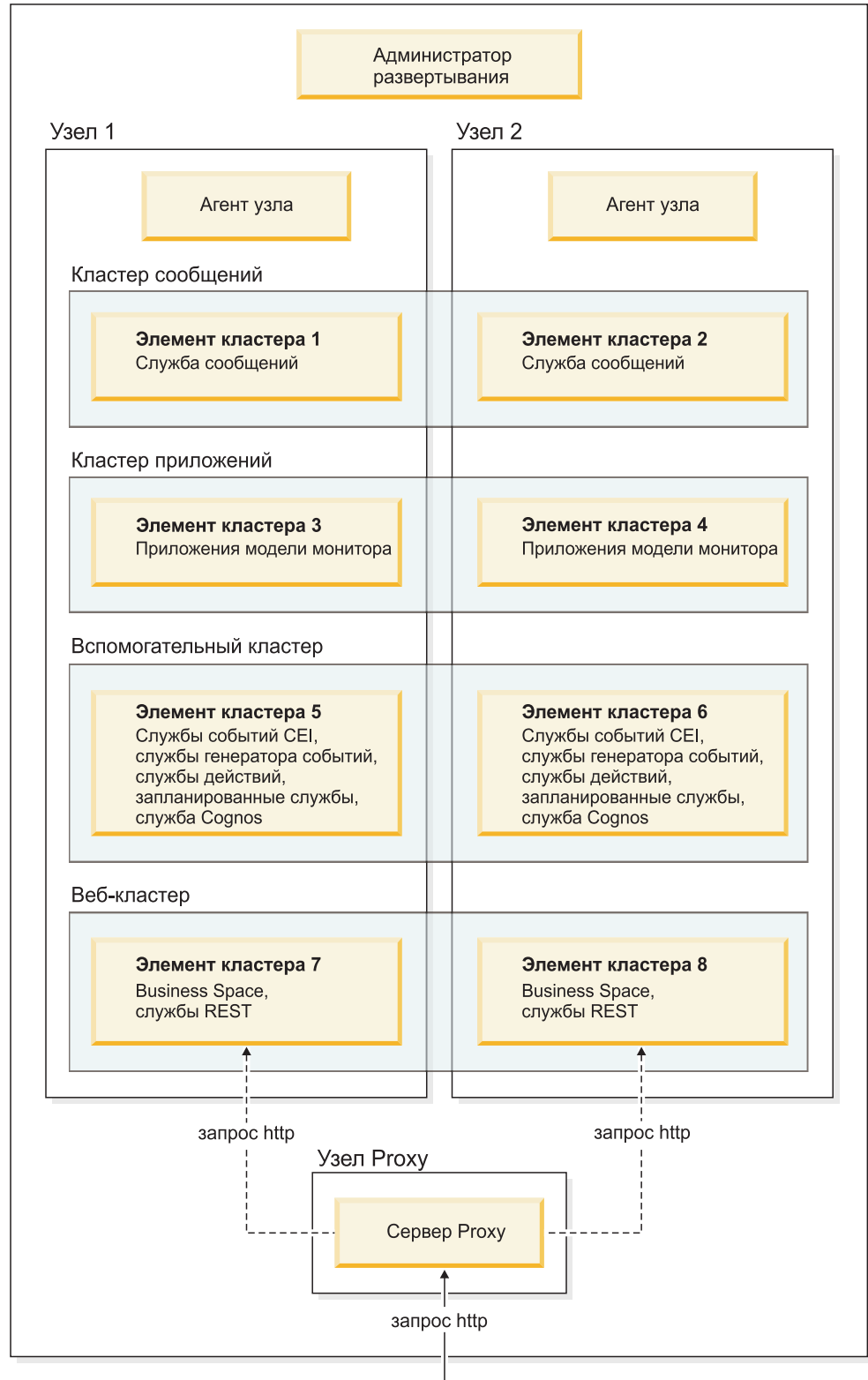
В среде сетевого развертывания обычно настраивается сервер проху или сервер HTTP - по соображениям безопасности и для выравнивания нагрузки. Дополнительная информация о сервере Proху приведена в разделе "Масштабируемость".

Масштабируемость

Установка компонентов и моделей мониторов IBM Business Monitor в кластере позволяет повысить эффективность управления их нагрузкой. Распределение компонентов и моделей мониторов в нескольких кластерах с группировкой компонентов с учетом шаблонов использования ресурсов, позволяет управлять нагрузкой каждого кластера с учетом шаблонов использования ресурсов установленных компонентов. Инструкции по планированию масштабируемой топологии приведены в разделе "Топология с четырьмя кластерами".

На следующей диаграмме показана ячейка с двумя управляемыми узлами.

Ячейка



Службы сообщений

Служба сообщений, созданная для шины интеграции служб IBM Business Monitor, одновременно может быть активна только в одном элементе кластера. Такое

ограничение указать в стратегии шины интеграции служб по умолчанию. Стратегия шины интеграции служб по умолчанию может быть настроена, однако всегда следует использовать стратегию типа "1 из N". Стратегия "1 из N" разрешает только один активный экземпляр службы сообщений в кластере, обеспечивая высокую готовность (защищая компоненты и модели от сбоя отдельного сервера), но не обеспечивая масштабируемость (возможность расширения при добавлении ресурсов).

Уровень использования службы сообщений и повысить производительность можно за счет применения функции, позволяющей службе событий CEI обходить очереди JMS и отправлять события непосредственно в базу данных IBM Business Monitor. Дополнительная информация приведена в разделе "Получение событий с помощью метода масштабирования или метода на основе таблиц".

Вспомогательные компоненты

Компоненты обслуживания включают службу событий CEI, службу IBM Cognos Business Intelligence, службы действий, службы генератора событий и планируемые службы. Добавление новых элементов кластера позволяет повысить производительность (за исключением запланированных служб).

Большая часть нагрузки запланированных служб обрабатывается на сервере базы данных. По мере возрастания нагрузки на запланированные службы следует отслеживать, оценивать и настраивать сервер базы данных. Кроме того, управлять нагрузкой запланированных служб можно путем включения и выключения различных запланированных служб и изменения связанных интервалов. Дополнительная информация приведена в разделе "Управление запланированными службами монитора".

Веб-компоненты

Веб-компоненты включают Business Space, виджеты и службу IBM Business Monitor REST API. Добавление новых элементов кластера позволяет повысить производительность.

В среде сетевого развертывания обычно настраивается сервер проху или сервер HTTP - по соображениям безопасности и для выравнивания нагрузки. Вместо отправки запросов HTTP напрямую в WebSphere Application Server, они направляются на сервер проху, который может разослать запросы на несколько серверов приложений, выполняющих работу. Создайте сервер проху в WebSphere Application Server. Вместо сервера проху или перед ним можно использовать другие серверы маршрутизации, например IBM HTTP Server. Преимущество применения сервера проху заключается в том, что он интегрирован с WebSphere Application Server и поэтому прост в использовании и обслуживании.

Важное замечание: Сервер проху (или альтернативный сервер маршрутизации) необходим для распределения запросов HTTP на выравнивание нагрузки между двумя или более элементами кластера. Сервер проху позволяет клиентам обращаться к приложениям в пределах этой топологии.

Приложения модели монитора

Приложения моделей мониторов поставляются в стандартных файлах EAR. Приложение модели монитора масштабируется по числу элементов кластера.

Особенности памяти

Объем памяти, доступной элементу кластера, зависит от адресного пространства операционной системы и режима работы JVM (32- или 64-разрядный). В 64-разрядном режиме JVM доступно от 500 ГБ до 4 ЭБ памяти; в 32-разрядном режиме - только 2 ГБ (например, 32-разрядный режим Windows).

В случае применения 32-разрядной JVM рекомендуется добавить второй кластер, если планируется развернуть более десяти приложений моделей мониторов (с учетом особенностей нагрузки и моделей).

Топология с четырьмя кластерами

IBM Business Monitor можно установить в разных топологиях. В топологии с четырьмя кластерами можно настроить высокопроизводительную среду

В следующей топологии с четырьмя кластерами используется шаблон среды развертывания Удаленный обмен сообщениями, Удаленная поддержка и Веб-приложения. Он объединяет приложения IBM Business Monitor в четыре логических кластера в одной ячейке.

Кластер службы сообщений

Шины WebSphere Business Monitor и CEI

Кластер поддержки

Службы событий CEI, службы действий, планировщик служб, службы отправки событий, служба Cognos

Кластер приложений

Приложения модели монитора

Веб-кластер

Приложение Business Space, виджеты Business Space, приложение служб REST

Кластер службы сообщений

Служба сообщений для шины IBM Business Monitor

Служба сообщений для шины Инфраструктуры обработки событий общего формата (CEI)

Кластер поддержки

Служба событий CEI

Службы генератора событий

Службы действий

Запланированные службы монитора
Служба IBM Cognos Business Intelligence

Кластер приложения

Приложения модели монитора

Веб-кластер

Приложение Business Space

Виджеты Business Space

Приложение служб передачи данных о состоянии (REST)

Примечание: Для повышения производительности поместите службы генератора событий и службы обработки событий CEI в один и тот же кластер. К службам генератора событий относятся и служба генератора событий REST, и служба генератора событий JMS.

Топология с четырьмя кластерами с IBM Business Process Manager

Можно создать комбинированную среду развертывания из IBM Business Process Manager и IBM Business Monitor с помощью шаблона Удаленный обмен сообщениями, удаленная поддержка и веб-приложения (четырёхкластерный). Поскольку одна среда развертывания IBM Business Monitor может отслеживать все приложения в ячейке, в отдельной ячейке необходимо создать только среду развертывания IBM Business Monitor.

Топология с четырьмя кластерами сочетает кластер IBM Business Monitor и кластер службы обмена сообщениями IBM Business Process Manager в одном кластере. В следующей топологии с четырьмя кластерами используется шаблон среды развертывания Удаленный обмен сообщениями, Удаленная поддержка и Веб-приложения.

Кластер службы сообщений

Служба сообщений для шины IBM Business Monitor

Служба сообщений для шины Инфраструктуры обработки событий общего формата (CEI)

Служба сообщений для шины Process Server

Служба сообщений для шины Performance Data Warehouse

(Только для BPM Advanced) Служба сообщений для шины Архитектуры компонентов служб (SCA)

(Только для BPM Advanced) Служба сообщений для шины Языка выполнения бизнес-процессов (BPEL)

Кластер поддержки

Служба событий CEI

Службы генератора событий

Службы действий

Запланированные службы монитора

Служба IBM Cognos Business Intelligence

Хранилище статистических данных

(Только для BPM Advanced) Администратор бизнес-правил

Кластер приложения

Приложения модели монитора

Приложения процессов

(Только для BPM Advanced) Приложения BPEL

Веб-кластер

Приложение Business Space

Виджеты Business Space

Приложение служб передачи данных о состоянии (REST)

(Только для BPM Advanced) Инструменты Business Process Choreographer

Использование предварительно необходимого программного обеспечения

IBM Business Monitor можно устанавливать на серверах, на которых установлено необходимое программное обеспечение.

Существующие серверы приложений

IBM Business Monitor можно установить на физическом сервере, на котором в данный момент установлена платформа сервера приложения. Для IBM Business Monitor поддерживаются следующие платформы серверов приложений:

- WebSphere Application Server
- Process Server
- WebSphere Enterprise Service Bus

Можно дополнить существующий профайл или создать новый, так чтобы он содержал сервер IBM Business Monitor.

Существующий WebSphere Portal

IBM Business Monitor более не предоставляет сводных панелей на основе портлетов. Однако, виджеты IBM Business Monitor по-прежнему могут быть показаны в WebSphere Portal. Более подробная информация приведена по ссылке на связанную задачу.

Профайлы

Профайл определяет среду выполнения и включает все файлы, которые сервер обрабатывает в среде выполнения. В среде высокой готовности необходимо создать несколько профайлов для эффективного управления сложной системой. Можно создать новые профайлы или расширить существующие профайлы.

IBM Business Monitor содержит шаблоны профайлов для включения функциональности, специфичной для IBM Business Monitor. После установки продукта можно создать и дополнить профайлы или в мастере средства Profile Management, или с помощью команды `manageprofiles`. (В 64-разрядной версии IBM Business Monitor необходимо использовать команду `manageprofiles`.)

Типы профайлов IBM Business Monitor являются расширением одноименных типов профайлов, предоставленных продуктом WebSphere Application Server. Типы профайлов, предоставленные продуктом IBM Business Monitor отличаются от типов профайлов, предоставленных продуктом WebSphere Application Server.

Применение новых профайлов является более эффективным, и этот способ менее склонен к ошибкам, чем многократная установка продукта. Разработчики могут использовать отдельные профайлы для разработки и тестирования. Используя профайлы вместо многократных установок продукта, вы получаете следующие преимущества:

- Вам необходимо обслуживать только один набор файлов базового продукта.
- Экономится дисковое пространство.
- Упрощается обновление продукта.

Выбор типа профайла

Профайл определяет уникальную среду выполнения с отдельными командными файлами, файлами конфигурации и файлами протокола. Профайлы определяют три типа сред: автономный одиночный сервер, администратор развертывания и управляемый узел. С помощью профайлов можно установить в системе более одной рабочей среды без установки нескольких копий продукта.

Для среды с одним сервером создайте автономный профайл.

Для среды сетевого развертывания выполните следующие действия:

1. Создайте профайл администратора развертывания перед созданием других профайлов. Если профайл администратора развертывания создан перед установкой IBM Business Monitor (например, для WebSphere Application Server или Process Server) и его планируется использовать для управления узлами IBM Business Monitor, дополните профайл с помощью шаблона, предоставленного IBM Business Monitor.
2. Для каждого узла, который планируется добавить в кластер сервера, необходимо создать индивидуальный профайл. В качестве альтернативы, можно дополнить существующий пользовательский профайл для каждого узла, который вы планируете добавить.

Примечание: Если на сервере базы данных установлено несколько версий DB2 или несколько экземпляров DB2, то для создания профайла используется версия или экземпляр DB2 по умолчанию. Для управления версией или экземпляром DB2 служит процедура "Установка баз данных вручную", позволяющая администратору базы данных обеспечить использование правильной версии или экземпляра.

Шаблоны для каждого профайла расположены в каталоге `app_server_root/profileTemplates`. Доступны следующие шаблоны профайлов:

Профайл	Когда использовать
Автономный сервер монитора	Для сред с одиночным сервером IBM Business Monitor.
Администратор развертывания сервера монитора	Для настройки среды сетевого развертывания сначала необходимо создать или дополнить этот профайл. Если администратор развертывания был создан после установки IBM Business Monitor и планируется использовать тот же профайл администратора развертывания для управления узлами IBM Business Monitor, расширьте профайл с использованием шаблона, предоставляемого IBM Business Monitor.

Профайл	Когда использовать
Настраиваемый профайл сервера монитора	При настройке среды сетевого развертывания необходимо создать или дополнить пользовательские узлы и затем с помощью административной консоли установить в них специальные приложения.

Автономные профайлы

Для IBM Business Monitor в средах с одним сервером используется автономный профайл, также называемый автономным профайлом сервера приложений.

Каждый автономный узел сервера приложений имеет свою собственную административную консоль, используемую для управления узлом. Автономный узел может включать в себя более одного сервера.

Автономный сервер легко настроить; он содержит консоль Первые шаги, из которой можно запустить и остановить сервер, а также установить пример Showcase. После установки примера на автономном сервере ресурсы примера можно просмотреть в административной консоли.

Можно развернуть свои собственные решения на автономном сервере, но автономный сервер не обеспечивает вместимость, масштабируемость и надежность, которые обычно требуются в рабочей среде. Для рабочей среды лучше использовать среду сетевого развертывания.

Профайлы администратора развертывания

Администратор развертывания - это сервер, который управляет операциями в логической группе (ячейке) других серверов. В среде сетевого развертывания можно совместно использовать группу серверов, чтобы обеспечить распределение рабочей нагрузки и отказоустойчивость. Администратор развертывания является центральным расположением для администрирования серверов и кластеров в ячейке.

Для того чтобы создать администратора развертывания, первым создаваемым или дополняемым профайлом должен быть профайл администратора развертывания. В состав администратора развертывания входит консоль Первые шаги, из которой можно запустить и остановить администратора развертывания, а также открыть его административную консоль. С помощью административной консоли администратора развертывания можно управлять серверами и кластерами в ячейке. Это включает в себя настройку серверов и кластеров, добавление серверов в кластеры, запуск и остановку серверов и кластеров, а также развертывание в них модулей.

Хотя администратор развертывания является типом сервера, невозможно развернуть модули в нем самом.

После создания или дополнения администратора развертывания для IBM Business Monitor в среде сетевого развертывания, можно затем создать пользовательские узлы и объединить их администраторе развертывания или сделать его частью для создания ячейки — группы узлов или кластеров, администрирование которых осуществляется централизованно.

Создайте или дополните профайл администратора развертывания перед созданием или дополнением пользовательских профайлов. Если администратор развертывания создается перед установкой IBM Business Monitor, и пользователь планирует

использовать этот профайл администратора развертывания для управления узлами IBM Business Monitor, то необходимо дополнить профайл с помощью шаблона из IBM Business Monitor.

Индивидуальные профайлы

Для того чтобы настроить среду сетевого развертывания для IBM Business Monitor, создайте пользовательские узлы и объедините их или сделайте частью ячейки администратора развертывания, которая будет ими управлять. В качестве альтернативы, можно дополнить существующий пользовательский профайл для каждого узла, который вы планируете добавить в ячейку. Можно затем с помощью административной консоли установить в них специальные приложения.

Пользовательский профайл является пустым узлом без стандартных приложений и серверов, которые входят в профайл автономного сервера. В процессе создания или дополнения пользовательского профайла вы объединяете узел для идентификации профайла администратора развертывания, который вы планируете использовать для управления узлом. После добавления пользовательского профайла в ячейку администратора развертывания узел становится *управляемым узлом*.

Управляемый узел содержит агент узла и может содержать управляемые серверы. В управляемом узле можно настраивать и выполнять управляемые серверы. Серверы, настроенные в управляемом узле, составляют ресурсы среды развертывания. Эти серверы создаются, настраиваются, запускаются, останавливаются, управляются и удаляются с помощью административной консоли администратора развертывания. Процессы в управляемом узле могут включать в себя элементы кластера, которые администратор развертывания применяет для распределения рабочей нагрузки интенсивно используемых приложений.

Управляемый узел может содержать один или несколько серверов, которые управляются администратором развертывания. Можно развернуть решения для серверов в управляемом узле, но управляемый узел не имеет своей собственной административной консоли. Управляемый узел определяется пользовательским профайлом и содержит консоль Первые шаги.

Замечания о базе данных

В основной базе данных MONITOR хранятся конфигурация IBM Business Monitor, метаданные модели монитора и отслеживаемые данные. Конфигурация IBM Cognos Business Intelligence хранится в отдельной базе данных хранилища материалов IBM Cognos BI по имени COGNOSCS. В ходе создания профайла предполагается, что базы данных MONITOR и COGNOSCS создаются в одном экземпляре базы данных.

Для баз данных MONITOR и COGNOSCS можно использовать имя пользователя общей базы данных. Однако рекомендуется создать разные имена, поскольку IBM Cognos BI при первом запуске создает собственные таблицы хранилища содержимого в схеме базы данных.

Кроме того, база данных MONITOR применяется для хранения схем следующих компонентов в процессе создания автономного профайла:

- Business Space
- Хранилище сообщений службы сообщений инфраструктуры обработки событий общего формата (CEI)
- Хранилище сообщений службы сообщений IBM Business Monitor

Если автономный профайл не применяется, то для этих компонентов можно использовать одну базу данных или разные базы данных. Это также относится к необязательному хранилищу данных CEI, которое по умолчанию не создается и не включается.

Для рабочих сред программное обеспечение базы данных можно выбрать из следующих поддерживаемых продуктов:

- DB2
- DB2 для z/OS
- Oracle
- Microsoft SQL Server

В базе данных монитора хранятся данные нескольких типов. При создании профайла IBM Business Monitor или запуске сценариев баз данных, создаются таблицы баз данных, содержащие данные конфигурации для IBM Business Monitor. Позднее, при установке каждой модели монитора создаются дополнительные таблицы. В ходе обработки событий в этих таблицах сохраняются данные экземпляра модели монитора. Эти таблицы используются сводными панелями.

Совет: В среде сетевого развертывания перед запуском администратора развертывания и созданием других пользовательских профайлов создайте базы данных MONITOR и COGNOSCS.

Совет: Если сервер IBM Cognos BI использует удаленную базу данных COGNOSCS, то на сервере IBM Cognos BI необходимо установить клиент базы данных. Дополнительная информация приведена в разделах, посвященных особенностям разных баз данных.

Создание баз данных

Базы данных MONITOR и COGNOSCS можно создать несколькими способами:

- Если программное обеспечение базы данных установлено на том же сервере, что и IBM Business Monitor, можно с помощью средства Profile Management или команды `managerprofiles` создать локальные базы данных при создании профайла.

Примечание:

- В случае применения DB2 пользователь, создающий профайл, должен обладать правами на создание базы данных.
- Базы данных Oracle и SQL Server: В инструменте управления профайлами или команде `managerprofiles` необходимо указать ИД пользователя и пароль администратора баз данных для создания объектов базы данных в существующем экземпляре базы данных.
- Можно воспользоваться функцией управления профайлами для создания сценариев базы данных с использованием значений конфигурации, которые были выбраны при создании профайла. Выберите опцию создания профайла, чтобы отложить выполнение сценариев баз данных, а затем, через некоторое время, запустите их, чтобы создать объекты баз данных на сервере баз данных.
- Базу данных можно создать вручную, используя сценарии с установочного носителя или из установочного каталога `dbscripts` IBM Business Monitor. Переменные в сценариях можно настроить вручную или с помощью инструмента проектирования базы данных (DbDesignGenerator).

Если в базе данных MONITOR табличные пространства для данных экземпляров переименованы, то при создании схемы для моделей монитора необходимо

экспортировать сценарии создания схемы и изменить имена табличных пространств в соответствии с именами, которые использовались при начальном создании базы данных.

Размер базы данных

Сценарии базы данных IBM Business Monitor для базы данных MONITOR создают несколько табличных пространств для хранения данных. Конфигурация и имена табличных пространств могут быть изменены в зависимости от стандартов предприятия и требований к размеру и производительности. Для установок для разработки и тестирования с минимальным объемом данных должно быть достаточно 1 Гб дискового пространства базы данных. Для рабочих сред размер базы данных зависит от объема данных, которые планируется отслеживать.

Защита баз данных

При создании баз данных пользователю рабочей базы данных по умолчанию предоставляются права на администрирование объектов базы данных, что упрощает создание баз данных и позволяет серверу IBM Business Monitor автоматически управлять схемой базы данных модели монитора при развертывании и удалении моделей. Если требуется создать защищенные базы данных, то обратитесь к разделам Защита среды базы данных MONITOR и Настройка защиты IBM Cognos BI.

Особенности базы данных MONITOR для DB2

Конкретные рекомендации по базам данных находятся в DB2.

Особенности глобализации

DB2 должен устанавливаться с использованием универсального набора символов UTF-8. Применение этого набора символов гарантирует правильное сохранение метаданных модели монитора и данных экземпляра, содержащих символы исходного языка, в базе данных. Кроме того, IBM Cognos Business Intelligence требует базу данных UTF-8. Сценарий `createDatabase.sql` создает базу данных как UTF-8 автоматически.

Сценарий `createDatabase.sql` создает базы данных со следующим параметром расположения по умолчанию:

```
TERRITORY EN_US
```

Для того чтобы изменить язык по умолчанию, укажите в параметре `TERRITORY` поддерживаемое расположение DB2 (см. веб-страницу Поддерживаемые коды расположений и кодовые страницы). Для параметров расположений следует использовать кодовый набор UTF-8. Например, следующее значение позволяет указать Францию:





```
TERRITORY FR_FR
```

Таблица `DIM_TIME` содержит столбец для добавления переведенных названий месяцев в отчеты сводных панелей. По умолчанию для заполнения записей таблицы `DIM_TIME` применяется код локали для английского языка (`EN_US`). Для изменения языка по умолчанию укажите требуемую локаль в файле `createTables.sql` вместо значения `EN_US`. Например, для того чтобы указать французский язык, замените `EN_US` на `FR_FR`. Кроме того, в файле `createTables.sql` предусмотрен оператор SQL, позволяющий переопределить названия месяцев.

Замечания относительно DB2 Express Edition

DB2 Express Edition может использовать максимум 4 ГБ оперативной памяти, даже если система имеет более 4 ГБ памяти. Дополнительную информацию о том, какую версию DB2 использовать, можно найти по связанным справочным ссылкам.

Обратите внимание на известное ограничение программы установки DB2 Express, связанное с добавлением строк на национальных языках (NL) в свойства, передаваемые программе установки IBM Business Monitor. Следующие значения, передаваемые программе установки DB2 Express в процессе установки, не могут содержать строки на национальных языках:

-  **Linux** Имя пользователя экземпляра и пароль: `bpminst` и `bpminst1`
-  **Linux** Имя изолированного пользователя и пароль: `bpmfenc` и `bpmfenc1`
-  **Linux** Имя сервера администрирования (DAS) и пароль: `bpmadmin` и `bpmadmin1`
-  **Windows** Имя пользователя с правами администратора и пароль: `bpmadmin` и `bpmadmin1`

О защите базы данных MONITOR

При использовании Инструмента управления профайлами или команды `managerprofiles` для создания базы данных DB2 пользователь с правами администратора, создающий профайл, также пытается создать базу данных. Пользователь рабочей базы данных IBM Business Monitor (@DB_USER@), который определяется во время создания профайла, должен уже существовать в операционной системе.

Пользователю рабочей базы данных IBM Business Monitor по умолчанию предоставляются права DBADM (администратор базы данных) во время создания базы данных. Это позволяет серверу IBM Business Monitor автоматически управлять схемой базы данных модели монитора в ходе развертывания и удаления модели. Для защиты базы данных можно создать базу данных вручную и предоставить пользователю рабочей базы данных только те права, которые необходимы для выполнения рабочих операций. Дополнительная информация приведена в разделах “Установка баз данных вручную” на стр. 59 и Защита среды базы данных монитора . Обзор прав доступа к базам данных приведен в разделе Права доступа к базам данных.

О блокировке DB2

При большом количестве событий база данных MONITOR блокируется при двух транзакциях или более, ожидающих одной блокировки базы данных. Когда это случается, в одной из транзакций происходит сбой и предпринимаются повторные попытки выполнения.

Для устранения взаимных блокировок в DB2 LUW с сохранением параллельной обработки введите следующее в командном окне DB2:

```
db2set DB2_SKIPINSERTED=ON
db2set DB2_SKIPDELETED =ON
```




Несколько нитей не будут взаимно блокироваться, если для переменных реестра экземпляра DB2, DB2_SKIPINSERTED и DB2_SKIPDELETED указано значение ON.

Особенности базы данных COGNOSCS для DB2

Если служба IBM Cognos Business Intelligence использует удаленную базу данных MONITOR, то на сервере необходимо установить полный клиент базы данных, такой как IBM Data Server Client, для развертывания кубов на сервере IBM Cognos BI.

Удаленную базу данных необходимо добавить в каталог перед публикацией пакетов куба IBM Cognos BI в ходе развертывания модели монитора. В каталоге должно быть указано имя базы данных MONITOR. В противном случае для источника данных WBMONITOR_DB в IBM Cognos BI потребуется указать имя из каталога.

В процессе публикации пакетов кубов на этапе развертывания модели IBM Cognos BI должен обладать доступом к командам клиента DB2.

-  Клиент DB2 должен быть указан в переменной PATH сервера.
-   Пользователь, запускающий сервер IBM Business Monitor, должен быть связан с пользовательским профайлом DB2.

Служба IBM Cognos BI при первом запуске создает таблицы в базе данных хранилища содержимого IBM Cognos BI. Поскольку пользователь базы данных, указанный для доступа к базе данных хранилища содержимого, должен обладать правами доступа для создания таблиц в базе данных, рекомендуется создать нового пользователя базы данных, предназначенного только для работы с базой данных хранилища содержимого.

База данных COGNOSCS должна использоваться только для данных IBM Business Monitor. Не следует добавлять данные прямо в базу данных COGNOSCS или использовать базу данных с другими базами данных для создания отчетов с такими данными (в комбинации с данными, созданными в IBM Business Monitor, или без них).

Расширенная защита IBM Cognos BI

Для создания внутренних таблиц IBM Cognos BI требуются дополнительные права доступа. После первого успешного запуска сервера IBM Cognos BI можно аннулировать дополнительные права доступа, необходимые для создания таблиц в базе данных хранилища содержимого IBM Cognos BI.

Следующая команда позволяет аннулировать дополнительные права доступа (замените переменную @DB_USER@ именем пользователя базы данных IBM Cognos BI):

```
REVOKE CREATETAB,IMPLICIT_SCHEMA ON DATABASE FROM USER @DB_USER@;
```

Дополнительная информация о настройке базы данных для IBM Cognos BI в DB2 приведена в разделе Рекомендуемые параметры для создания хранилища содержимого в DB2 для Linux, Windows и UNIX.

Особенности базы данных MONITOR для DB2 for z/OS

Конкретные рекомендации по базам данных находятся в DB2 для z/OS. Для IBM Business Monitor рекомендуется создать выделенную группу памяти (STOGROUP). Группу памяти следует создать перед созданием базы данных MONITOR.

IBM Cognos BI не поддерживается в z/OS. Кроме того, IBM Cognos BI не поддерживается в случае применения DB2 для z/OS в качестве базы данных MONITOR.

Особенности глобализации

DB2 для z/OS должен устанавливаться с использованием универсального набора символов UTF-8. Применение этого набора символов гарантирует правильное сохранение метаданных модели монитора и данных экземпляра, содержащих символы исходного языка, в базе данных. Сценарий `createDatabase.sql` создает базу данных как UTF-8 автоматически.

Таблица DIM_TIME содержит столбец для добавления переведенных названий месяцев в отчеты сводных панелей. Параметры расположения в z/OS не применяются для создания имен месяцев. В файле `createTables.sql` предусмотрен оператор SQL, позволяющий переопределить названия месяцев.

Общие рекомендации для базы данных

DB2 для z/OS требует добавления двух пулов буферов. Перед запуском сценариев базы данных администратор базы данных должен создать следующие пулы буферов размером 32 КБ:

- BP32K
- TMPBP32

DB2 для z/OS хранит объявленные временные таблицы в базе данных TEMP.

- Создайте выделенный объект STOGROUP для хранения данных IBM Business Monitor.
- Создайте базу данных TEMP с табличным пространством TEMP для хранения объявленных временных таблиц для обработки курсоров, допускающих прокрутку. Примеры приведены ниже.

Для DB2 для z/OS версии 8 необходимо создать временные базу данных и табличное пространство, если они не существуют. Ниже приведен показательный пример определения базы данных TEMP:

```
CREATE DATABASE TEMP AS TEMP STOGROUP SYSDEFLT;  
CREATE TABLESPACE TEMP IN TEMP  
USING STOGROUP SYSDEFLT  
BUFFERPOOL BP32K  
SEGSIZE 32;
```

Для DB2 для z/OS версий 9 и 10 в среде без общих данных, базой данных TEMP является DSND07 и создается во время установки базы данных. Временные табличные пространства добавляются к существующей базе данных TEMP. Ниже приведен показательный пример временного табличного пространства:

```
CREATE TABLESPACE WBITEMP IN DSND07  
USING STOGROUP SYSDEFLT  
BUFFERPOOL BP32K  
SEGSIZE 32;
```

Для DB2 для z/OS версий 9 и 10 в среде с общими данными необходимо создать базу данных WORKFILE. В отдельной подсистеме можно создать только одну базу данных WORKFILE. Ниже приведен пример создания базы данных WORKFILE и временного табличного пространства:

```
CREATE DATABASE WORKTEMP AS WORKFILE STOGROUP SYSDEFLT;  
CREATE TABLESPACE WBITEMP IN WORKTEMP  
USING STOGROUP SYSDEFLT  
BUFFERPOOL BP32K  
SEGSIZE 32;
```

Дополнительные сведения о настройке базы данных TEMP и табличных пространств TEMP приведены в справочной системе DB2 for z/OS Information Center. См. ссылку на связанную информацию.

Примечание: Если вы работаете с DB2 для z/OS и собираетесь применять SPUFI для запуска сценариев базы данных, то воспользуйтесь FTP для передачи файлов на сервер базы данных z/OS. Сценарии базы данных IBM Business Monitor оканчиваются на символ перевода строки. Сервер FTP в z/OS правильно преобразует символ перевода строки в символ конца строки для сценария базы данных.

DB2 для z/OS версии 8 предусматривает применение рабочей базы данных файлов для отдельных операторов SQL, таких как операторы сортировки. Для версии 8 для этого, кроме базы данных TEMP, требуется дополнительное табличное пространство, поддерживающее операции сортировки. В DB2 для z/OS версии 9 или 10 рабочая база данных файлов и база данных TEMP объединяются. Инструкции созданию рабочих баз данных и рекомендации по выбору их размера приведены в справочной системе DB2 for z/OS Information Center.

Для повышения уровня параллелизма в параметре подсистемы RRULOCK укажите значение YES.

Если планируется включить службу перемещения данных, увеличьте число блокировок на одного пользователя (NUMLKUS) по крайней мере до 100000.

Драйвер JDBC

IBM Business Monitor использует драйвер JDBC 4.0. По умолчанию инструмент управления профайлами указывает на файл db2jcc4.jar, расположенный в каталоге app_server_root\jdbcdrivers\DB2. Для экземпляров DB2 для z/OS рекомендуется использовать драйвер JDBC 3.0 db2jcc.jar, поставляемый вместе с DB2.

Особенности базы данных MONITOR для Oracle

Конкретные рекомендации по базам данных находятся на Oracle.

Особенности глобализации

Oracle должен устанавливаться с использованием универсального набора символов UTF-8 (AL32UTF8) вместо стандартного набора символов базы данных по умолчанию (WE8ISO8859P1 - ISO 8859-1, Западная Европа). Применение этого набора символов гарантирует правильное сохранение метаданных модели монитора и данных экземпляра, содержащих символы исходного языка, в базе данных. Кроме того, IBM Cognos BI требует базу данных UTF-8.

Oracle управляет языком и локалью с помощью двух параметров базы данных:

NLS_LANGUAGE

NLS_TERRITORY

Для изменения языка по умолчанию для баз данных укажите в параметре NLS_LANGUAGE поддерживаемый язык Oracle. Параметры расположения задают параметры по умолчанию форматирования данных, денежных единиц и т.д. Укажите параметр NLS_TERRITORY для изменения экземпляра Oracle.

Таблица DIM_TIME содержит столбец для добавления переведенных названий месяцев в отчеты сводных панелей с параметрами времени. По умолчанию для заполнения записей таблицы DIM_TIME применяется код локали из параметра NLS_LANGUAGE. При необходимости измените язык по умолчанию в параметре NLS_LANGUAGE экземпляра Oracle или текущего сеанса перед запуском сценария createTables.sql. Кроме того, в файле createTables.sql предусмотрен оператор SQL, позволяющий переопределить названия месяцев.

О защите MONITOR

В случае применения инструмента управления профайлами или команды `managerprofiles` для создания объектов базы данных Oracle пользователь с правами администратора, указанный при создании профайла, создает объекты базы данных и схему MONITOR. В случае Oracle схема представляет собой набор объектов базы данных и ИД пользователя, который может входить в базу данных.

По умолчанию владельцем схемы MONITOR также является пользователь рабочей базы данных; он обладает правами на создание других схем и объектов базы данных в процессе создания базы данных. Это позволяет серверу IBM Business Monitor автоматически управлять схемой базы данных модели монитора в ходе развертывания и удаления модели. Для защиты базы данных можно создать базу данных вручную. Владельца схемы MONITOR или другого пользователя можно использовать в качестве пользователя рабочей базы данных IBM Business Monitor. В защищенной среде пользователю рабочей базы данных можно предоставить только те права, которые необходимы для выполнения рабочих операций. Обратитесь также к разделам "Установка базы данных вручную" и "Защита среды базы данных MONITOR" по связанным ссылкам.

Драйвер JDBC

Поддержка JDBC предоставляется драйверами JDBC Oracle для JVM 1.6. Файл драйвера JDBC `ojdbc6.jar` является поддерживаемым Oracle драйвером JDBC для использования в WebSphere Application Server версии 7. Файл `ojdbc6.jar` можно использовать для Oracle 10g и Oracle 11g. Сведения о минимальных обязательных параметрах для Oracle приведены в ссылке на связанную информацию.

По умолчанию инструмент управления профайлами указывает на файл `ojdbc6.jar`, расположенный в каталоге `app_server_root\jdbcdrivers\Oracle`. Кроме того, можно загрузить другой файл драйвера JDBC Oracle `ojdbc6.jar` и указать его при запуске инструмента управления профайлами или команды `managerprofiles`.

Восстановление XA

Специальные права доступа необходимо предоставить для обеспечения правильного восстановления XA Oracle. Выполните следующие команды от имени пользователя SYS:

```
grant select on pending_trans$ to <пользователь>;
grant select on dba_2pc_pending to <пользователь>;
grant select on dba_pending_transactions to <пользователь>;
grant execute on dbms_system to <пользователь>;
```

где `<пользователь>` - это имя пользователя базы данных MONITOR, настраиваемое во время создания профайла.

Особенности базы данных COGNOSCS для Oracle

Если служба IBM Cognos Business Intelligence использует удаленную базу данных MONITOR, то на сервере необходимо установить полный клиент базы данных или Oracle Instant Client для развертывания кубов на сервере IBM Cognos BI.

Экземпляр Oracle для IBM Cognos BI должен быть доступен на сервере по записи TNSNAMES в клиенте Oracle. Запись TNSNAMES должна содержать имя экземпляра базы данных, указанное для базы данных MONITOR в ходе создания профайла (например, ORCL). В противном случае для источника данных WBMONITOR_DB в IBM Cognos BI потребуются указать правильную запись TNSNAMES.




В случае применения клиента Oracle Instant Client путь к клиенту должен быть указан в системном пути. Кроме того, в файле TNSNAMES.ORA необходимо указать информацию о сервере базы данных Oracle, а в переменной среды TNS_ADMIN - расположение файла TNSNAMES.ORA.

Важное замечание: Для устранения неполадок вместе с Oracle Instant Client рекомендуется установить утилиту SQLPlus.

В следующем примере показано содержимое допустимого файла TNSNAMES.ORA. (Значение ORCL - это псевдоним соединения с базой данных.)

```
ORCL =
(DESCRIPTION =
(AADDRESS = (PROTOCOL = TCP)(HOST = 127.0.0.1)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = orcl)
)
)
```

В процессе публикации пакетов кубов на этапе развертывания модели IBM Cognos BI должен обладать доступом к командам клиента Oracle.

-  Клиент Oracle должен быть указан в переменной PATH сервера.
-   Пользователь, запускающий сервер IBM Business Monitor, должен быть связан с пользовательским профайлом Oracle.

Служба IBM Cognos BI при первом запуске создает таблицы в базе данных хранилища содержимого IBM Cognos BI. Пользователь базы данных, имеющий доступ к базе данных хранилища содержимого IBM Cognos BI, должен обладать полными правами доступа к Oracle для создания таблиц, панелей, последовательностей, триггеров и т. д. В IBM Cognos BI нельзя указать отдельное имя схемы; объекты IBM Cognos BI создаются в схеме по умолчанию пользователя базы данных. Рекомендуется создать нового пользователя базы данных для использования только в базе данных хранилища материалов.

Важное замечание: Не используйте пользователя SYSTEM для этой цели, поскольку нежелательно, чтобы объекты базы данных IBM Cognos BI создавались в системной области.

База данных COGNOSCS должна использоваться только для данных IBM Business Monitor. Не следует добавлять данные прямо в базу данных COGNOSCS или использовать базу данных с другими базами данных для создания отчетов с такими данными (в комбинации с данными, созданными в IBM Business Monitor, или без них).

Расширенная защита IBM Cognos BI

Для создания внутренних таблиц IBM Cognos BI требуются дополнительные права доступа. После первого успешного запуска сервера IBM Cognos BI можно аннулировать дополнительные права доступа, необходимые для создания таблиц в базе данных хранилища содержимого IBM Cognos BI.

Следующие команды позволяют аннулировать дополнительные права доступа, необходимые для создания схемы IBM Cognos BI, и позволяют обеспечить работу IBM Cognos BI в режиме среды выполнения с ограниченным набором прав доступа:

```
REVOKE CREATE USER FROM @SCHEMA@;
REVOKE ALTER USER FROM @SCHEMA@;
REVOKE DROP USER FROM @SCHEMA@;
```

```

REVOKE CREATE ANY TABLE FROM @SCHEMA@;
REVOKE ALTER ANY TABLE FROM @SCHEMA@;
REVOKE DROP ANY TABLE FROM @SCHEMA@;

REVOKE CREATE ANY SEQUENCE FROM @SCHEMA@;
REVOKE ALTER ANY SEQUENCE FROM @SCHEMA@;
REVOKE DROP ANY SEQUENCE FROM @SCHEMA@;

REVOKE CREATE ANY PROCEDURE FROM @SCHEMA@;
REVOKE ALTER ANY PROCEDURE FROM @SCHEMA@;
REVOKE DROP ANY PROCEDURE FROM @SCHEMA@;

REVOKE CREATE ANY VIEW FROM @SCHEMA@;
REVOKE DROP ANY VIEW FROM @SCHEMA@;

REVOKE CREATE ANY TRIGGER FROM @SCHEMA@;
REVOKE ALTER ANY TRIGGER FROM @SCHEMA@;
REVOKE DROP ANY TRIGGER FROM @SCHEMA@;

REVOKE CREATE ANY INDEX FROM @SCHEMA@;
REVOKE DROP ANY INDEX FROM @SCHEMA@;

REVOKE LOCK ANY TABLE FROM @SCHEMA@;

```

Дополнительная информация о настройке базы данных для IBM Cognos BI в Oracle приведена в разделе Рекомендуемые параметры для создания хранилища содержимого в Oracle.

Особенности базы данных MONITOR для Microsoft SQL Server

Конкретные рекомендации по базам данных приведены в разделе Microsoft SQL Server.

Важное замечание: В ходе установки SQL Server выберите смешанный режим идентификации (Идентификация Windows или идентификация SQL Server).

Важное замечание: Для использования SQL Server с IBM Business Monitor необходимо настроить SQL Server на транзакции XA. SQL Server по умолчанию не настраивается для поддержки транзакций XA. Модуль поддержки XA поставляется вместе с драйвером JDBC Microsoft; он содержит динамическую библиотеку (sqljdbc_xa.dll) и сценарий установки (xa_install.sql). Поскольку транзакции XA по умолчанию выключены, требуется дополнительная настройка с помощью Microsoft Windows Distributed Transaction Coordinator (MSDTC). Инструкции по включению поддержки XA для SQL Server приведены в разделе "Общие сведения о транзакциях XA" в электронной документации по серверу Microsoft SQL Server.

При использовании Инструмента управления профайлами или команды `manageprofiles` для создания базы данных SQL Server пользователь базы данных с правами администратора, определенный при создании профайла, создает базу данных. Пользователь рабочей базы данных IBM Business Monitor (@DB_USER@), который определяется во время создания профайла, должен уже существовать как пользователь базы данных с входом в SQL Server. Для создания пользователя базы данных с входом в базу данных можно использовать следующую команду:

```

CREATE LOGIN @DB_USER@ WITH
PASSWORD = '@DB_PASSWORD@', DEFAULT_DATABASE=@DB_NAME@
CREATE USER @DB_USER@ FOR LOGIN @DB_USER@

```

где DB_USER - это пользователь базы данных IBM Business Monitor, DB_PASSWORD - пароль пользователя базы данных, а DB_NAME - имя базы данных IBM Business Monitor.

По умолчанию пользователю рабочей базы данных IBM Business Monitor предоставляются права владельца базы данных (db_owner) при создании базы данных. Это позволяет серверу IBM Business Monitor автоматически управлять схемой базы данных модели монитора в ходе развертывания и удаления модели. Для защиты базы данных можно создать базу данных вручную и предоставить пользователю рабочей базы данных только те права, которые необходимы для выполнения рабочих операций. Обратитесь также к разделам "Установка базы данных вручную" и "Защита среды базы данных MONITOR" по связанным ссылкам.

Драйверы JDBC SQL Server для JVM 1.6 обеспечивают поддержку JDBC. IBM Business Monitor использует файл sqljdbc4.jar драйвера Microsoft JDBC 2.0. По умолчанию инструмент управления профайлами указывает на файл sqljdbc4.jar, расположенный в каталоге app_server_root\jdbcdrivers\SQLServer. Кроме того, можно загрузить другой файл драйвера JDBC Microsoft sqljdbc4.jar и указать его при запуске инструмента управления профайлами или команды **manageprofiles**. Сведения о минимальных обязательных параметрах для SQL Server приведены в ссылке на связанную информацию.

Особенности глобализации

В процессе создания базы данных SQL Server управляет параметрами локали с помощью параметра COLLATE. Оператор создания баз данных MONITOR и COGNOSCS содержит следующий параметр:

```
COLLATE SQL_Latin1_General_CP1_CS_AS
```

Параметры локали можно изменить, указав в параметре упорядочения поддерживаемое значение для требуемого языка. Например, следующее значение позволяет указать упорядочение для французского языка:

```
COLLATE French_100_CS_AS
```

SQL Server управляет языком по умолчанию с учетом параметров текущего пользователя. Для изменения языка по умолчанию добавьте в файл createDatabase.sql параметр DEFAULT_LANGUAGE, чтобы создать сеанс входа в систему с другим языком по умолчанию. Пример оператора с французским языком по умолчанию:

```
IF NOT EXISTS (SELECT * FROM syslogins WHERE NAME = '@DB_USER@') CREATE LOGIN @DB_USER@ WITH PASSWORD
```

Таблица DIM_TIME содержит столбец для добавления переведенных названий месяцев в отчеты сводных панелей с параметрами времени. По умолчанию для заполнения записей таблицы DIM_TIME применяется код локали из параметра DEFAULT_LANGUAGE. При необходимости измените язык по умолчанию в параметре DEFAULT_LANGUAGE пользователя базы данных перед запуском сценария createTables.sql. Кроме того, в файле createTables.sql предусмотрен оператор SQL, позволяющий переопределить названия месяцев.

Особенности базы данных COGNOSCS для Microsoft SQL Server

Если служба IBM Cognos Business Intelligence использует удаленную базу данных MONITOR, то на сервере необходимо установить полный клиент базы данных Microsoft SQL Server для развертывания кубов на сервере IBM Cognos BI.

Важное замечание: База данных IBM Cognos BI использует упорядочение без учета регистра символов, а база данных IBM Business Monitor использует упорядочение с учетом регистра символов. Упорядочение по умолчанию для базы данных IBM Cognos BI можно заменить только на упорядочение без учета регистра символов.

Microsoft предлагает SQL Server Native Client, который можно использовать вместо полного клиента SQL Server. Этот минимальный вариант установки содержит все требуемые встроенные драйверы. Вместе с внутренним клиентом необходимо загрузить и установить утилиты командной строки SQL Server. Оба компонента можно загрузить с веб-страницы Microsoft SQL Server 2008 Feature Pack, August 2008.

В процессе публикации пакетов кубов на этапе развертывания модели IBM Cognos BI должен обладать доступом к командам клиента SQL Server. Клиент SQL Server должен быть указан в переменной PATH сервера.

Служба IBM Cognos BI при первом запуске создает таблицы в базе данных хранилища содержимого IBM Cognos BI. Поскольку пользователь базы данных, указанный для доступа к базе данных хранилища содержимого, должен обладать правами доступа для создания таблиц в базе данных, рекомендуется создать нового пользователя базы данных, предназначенного только для работы с базой данных хранилища содержимого.

База данных COGNOSCS должна использоваться только для данных IBM Business Monitor. Не следует добавлять данные прямо в базу данных COGNOSCS или использовать базу данных с другими базами данных для создания отчетов с такими данными (в комбинации с данными, созданными в IBM Business Monitor, или без них).

Расширенная защита IBM Cognos BI

Для создания внутренних таблиц IBM Cognos BI требуются дополнительные права доступа. После первого успешного запуска сервера IBM Cognos BI можно аннулировать дополнительные права доступа, необходимые для создания таблиц в базе данных хранилища содержимого IBM Cognos BI.

Следующие команды позволяют аннулировать дополнительные права доступа, необходимые для создания схемы IBM Cognos BI, и позволяют обеспечить работу IBM Cognos BI в режиме среды выполнения с ограниченным набором прав доступа:

```
EXEC sp_droprolemember 'db_datawriter', @COG_DB_USER@
GO
EXEC sp_droprolemember 'db_ddladmin', @COG_DB_USER@
GO
```

Дополнительная информация о настройке базы данных для IBM Cognos BI в SQL Server приведена в разделе Рекомендуемые параметры для создания хранилища содержимого в Microsoft SQL Server.

Права доступа к базе данных

Выясните права доступа, необходимые для создания или доступа к таблицам хранилища данных для каждой системы управления базами данных, поддерживаемой IBM Business Monitor.

При создании схем с помощью программы установки, инструмента управления профайлами или сценариев необходим ИД пользователя с достаточными правами для создания таблиц. После создания таблиц приложения должны иметь достаточные права доступа для выбора, вставки, обновления и удаления информации из таблиц.

В Табл. 1 приведены права доступа к базе данных, необходимые для обращения к хранилищу данных.

Таблица 1. Права доступа к базе данных

Система управления базами данных	Минимальные права доступа для использования таблиц хранилища данных	Дополнительные права доступа, необходимые для создания таблиц хранилища данных
DB2	Для ИД пользователя требуются права доступа SELECT, INSERT, UPDATE и DELETE к таблицам.	ИД пользователя должно иметь право доступа CREATETAB для базы данных и USE для табличного пространства, а также CREATEIN для схемы.
Oracle	<p>ИД пользователя должно иметь право доступа SESSION для соединения с базой данных. Если один и тот же ИД пользователя владеет как схемой хранилища данных, так и компонентом, который соединяется с базой данных, то этот ИД пользователя имеет достаточные права для выполнения операций с таблицами. В противном случае для ИД пользователя требуются объектные права доступа SELECT, INSERT, UPDATE и DELETE к таблицам, которые составляют хранилище данных, и системное право доступа DROP ANY TABLE для возможности использования оператора TRUNCATE TABLE.</p> <p>Базу данных Oracle необходимо создать с помощью набора символов UTF-8, поддерживающего другие пользовательские наборы символов, которые поддерживаются IBM Business Monitor.</p>	<p>ИД пользователя требуются достаточные права доступа для создания реляционных таблиц и индексов в схеме хранилища данных. База данных также требует части пространства в табличном пространстве по умолчанию владельца схемы.</p> <p>В разделе Табл. 2 на стр. 25 описываются дополнительные права доступа к базе данных Oracle для компонентов IBM Business Monitor и WebSphere Enterprise Service Bus.</p>
SQL Server	Настройка SQL Server для идентификации SQL Server и Windows. Это обеспечивает идентификацию на основе ИД входа в систему и пароля сервера SQL. Этот ИД пользователя может быть ИД владельца таблиц или участника группы с достаточными правами на выполнение операторов TRUNCATE TABLE.	Для ИД пользователя требуются права на выполнение оператора CREATE TABLE.

В разделе Табл. 2 описываются дополнительные права доступа к базе данных Oracle для компонентов IBM Business Monitor.

Примечание: Если требуется настроить все следующие компоненты для одной базы данных Oracle, то можно создать расширенный набор всех прав доступа, определяемых для каждого компонента. Если эти четыре компонента настраиваются для нескольких баз данных, то можно задать разные права доступа для каждого.

Таблица 2. Дополнительные права доступа к базе данных Oracle

Компонент	Права доступа к конфигурации	Права доступа к среде выполнения
Общая база данных	CREATE TABLE, CREATE INDEXTYPE, ALTER TABLE, INSERT, CREATE SEQUENCE, CREATE USER, ALTER USER, CREATE TABLESPACE	SELECT, UPDATE, DELETE, INSERT, CREATE VIEW, CREATE PROCEDURE
Модули обмена сообщениями	CREATE TABLE, CREATE INDEXTYPE	SELECT, UPDATE, DELETE, INSERT, DROP ANY TABLE

Замечания о реестре пользователей

В реестре пользователей хранится информация, которая используется при простой идентификации пользователей. Выбор реестра пользователя имеет определяющее значение при планировании среды. В WebSphere Application Server Application Server необходимо настроить тот реестр пользователей, который будет применяться в вашей среде.

Реестр пользователей содержит информацию, которая применяется в ходе идентификации пользователей, запросивших доступ к IBM Business Monitor. Можно настроить несколько типов хранилищ пользователей в виде объединенных хранилищ. Для большинства приложений, развертываемых в рабочей среде, применяется сервер LDAP. При развертывании небольших приложений они находятся на одном сервере, и в этом случае можно использовать файловый реестр пользователей.

Можно выбрать одну из следующих учетных записей пользователя хранилища:

- Встроенные хранилища
- Локальная операционная система
- Автономный реестр LDAP
- Автономный пользовательский реестр




Примечание: Для расширенной защиты поддерживаются следующие реестры пользователей: объединенные хранилища (на основе файлов), объединенные хранилища (LDAP) и автономный реестр LDAP.

Замечания об обычных пользователях

Для того чтобы создать профайл тестирования в ходе установки IBM Business Monitor от имени обычного пользователя, необходимо предварительно установить сервер DB2. Узнайте сведения о базе данных, чтобы их можно было ввести во время установки.

Приведенная в этом разделе информация относится ко всем сценариям **обычной** установки. В ходе **обычной** установки профайлы создаются в автоматическом режиме.

Установку от имени обычного пользователя можно выполнить следующими способами:

- Перед установкой продукта установите сервер DB2. Информация об установке DB2 обычным пользователем (не администратором и не пользователем root) приведена в разделах
 -   Обзор установки обычным пользователем (не root) (Linux и UNIX)
 -  Требуемые учетные записи пользователей для установки продуктов сервера DB2 (Windows)
- Войдите в систему от имени администратора и установите сервер DB2 с помощью программы установки. Предоставьте специальные права доступа обычному пользователю. Затем войдите в систему от имени обычного пользователя и установите продукт с помощью установленного сервера DB2.

Кроме того, вместо создания тестового профайла можно создать профайл после установки. Выполните следующие действия:

1. Установите продукт, но не создавайте профайл. Если установка выполняется от имени обычного пользователя, то на странице Установка пакетов необходимо выключить переключатель для DB2 Express. В системе Windows необходимо также выключить переключатель установки IBM Cognos Business Intelligence.
2. На странице Компоненты разверните серверы и убедитесь, что тестовые профайлы не выбраны.
3. Создайте автономный профайл или администратор развертывания и пользовательские профайлы с помощью инструмента управления профайлами. Если база данных не установлена, выберите вариант **расширенной** установки. **Обычная** установка в этом случае неприменима. Отложите выполнение сценариев базы данных при создании профайла.
4. Если базы данных не были созданы заранее, попросите администратора создать базы данных и таблицы после создания или дополнения профайла.
5. Для сетевого развертывания:
 - a. Объедините пользовательские профайлы с администратором развертывания.
 - b. С помощью административной консоли создайте необходимую среду развертывания.

Примечание: Для применения базы данных DB2 Express, которая поставляется (и может быть установлена) вместе с продуктом, должны быть выполнены следующие требования:

- Удалите из системы все другие версии DB2.
- Установите IBM Business Process Manager от имени обычного пользователя.

Примеры путей установки

IBM Business Monitor предоставляет выбор из нескольких путей установки для создания среды разработки.

Среда с несколькими ячейками - это такая среда, в которой IBM Business Monitor получает события с сервера, который находится в ячейке, отличной от сервера IBM Business Monitor. Среда с несколькими ячейками может включать топологию сетевого развертывания (ND) или топологию одного сервера. В обоих случаях необходимо выполнить несколько действий для включения связи между сервером Инфраструктуры обработки событий общего формата (CEI) и сервера IBM Business Monitor. Информация о том, как включить связь в среде с несколькими ячейками,

приведена в разделе "Настройка приема событий". Пример топологии среды с несколькими ячейками приведен в сценарии "Отслеживание событий из информационной системы предприятия SAP (EIS) без посредника".

Установочный каталог для топологии с одним сервером

При использовании однокластерной топологии IBM Business Monitor и все необходимые компоненты устанавливаются на один и тот же физический сервер.

Для установки сервера IBM Business Monitor и всех необходимых компонентов на один сервер выполните следующие действия (высокого уровня):

1. Выполните предварительные действия по установке из раздела Глава 3, "Подготовка к установке", на стр. 33.
2. Установите IBM Business Monitor согласно инструкциям из раздела "Установка программного обеспечения IBM Business Monitor" на стр. 39. Во время установки продукта у вас есть возможность создать профайл разработки, который предоставляет пробную среду, но не может использоваться в рабочей среде.
3. Если вы не создали профайл разработки, создайте автономный профайл с помощью Инструмента управления профайлами или команды `managerprofiles`, согласно инструкциям из раздела Глава 6, "Создание и дополнение профайлов", на стр. 61.

Все необходимые компоненты IBM Business Monitor будут установлены и настроены автоматически.

При желании вы можете проверить состояние компонентов и внести обновления, используя мастер настройки в административной консоли.

Путь установки для топологии сетевого развертывания с шаблонами среды развертывания

Сетевое развертывание (ND) в IBM Business Monitor основывается на функциях сетевого развертывания, реализуемых в WebSphere Application Server Network Deployment. Выбрав один из доступных шаблонов среды развертывания, используйте мастер среды развертывания для настройки необходимых кластеров, серверов и компонентов.

Принципы те же, что и в сетевом развертывании в WebSphere Application Server Network Deployment. Для IBM Business Monitor существуют два шаблона: однокластерный шаблон и шаблон удаленного обмена сообщениями, шаблон удаленной поддержки и шаблон веб-приложения (четырёхкластерный).

Для установки сервера IBM Business Monitor и всех необходимых компонентов с использованием одно- или четырехкластерной среды развертывания выполните следующие действия (высокого уровня):

1. Выполните предварительные действия по установке из раздела Глава 3, "Подготовка к установке", на стр. 33.
2. Установите IBM Business Monitor согласно инструкциям из раздела "Установка программного обеспечения IBM Business Monitor" на стр. 39. Не создавайте профайл развертывания.
3. Создайте профайл Администратора развертывания с помощью Инструмента управления профайлами или команды `managerprofiles`, согласно инструкциям из раздела Глава 6, "Создание и дополнение профайлов", на стр. 61.

4. За исключением случая, когда вы создали базу данных MONITOR во время создания профайла, выполните сценарии создания базы данных согласно инструкциям из раздела Глава 5, “Создание баз данных”, на стр. 53.
5. Запустите администратор развертывания.
6. Создайте пользовательские узлы, встраиваемые в ячейку Администратора развертывания, согласно инструкциям из раздела Глава 6, “Создание и дополнение профайлов”, на стр. 61.
7. Создайте среду развертывания, выбрав либо однокластерный шаблон, либо четырехкластерный шаблон удаленного обмена сообщениями, поддержки и веб-приложения. Выполните действия из раздела “Создание среды разработки с помощью шаблона” на стр. 91.
8. Настройте дополнительные компоненты, такие как Business Space и IBM Cognos BI, следуя инструкциям из раздела Глава 10, “Настройка компонентов IBM Business Monitor”, на стр. 129.

Кластеры будут созданы, и все необходимые компоненты IBM Business Monitor будут установлены и настроены автоматически.

При желании вы можете проверить состояние компонентов и внести обновления, используя мастер настройки в административной консоли.

Путь установки для пользовательской топологии сетевого развертывания

Вместо того чтобы с помощью мастера настройки среды развертывания создавать одно- или четырехкластерную топологию сетевого развертывания (ND), вы можете создать произвольную топологию по своему усмотрению, воспользовавшись мастером настройки или выполнив задачу wsadmin.

Для установки сервера IBM Business Monitor и всех необходимых компонентов в пользовательской топологии сетевого развертывания выполните следующие действия (высокого уровня):

1. Выполните предварительные действия по установке из раздела Глава 3, “Подготовка к установке”, на стр. 33.
2. Установите IBM Business Monitor согласно инструкциям из раздела “Установка программного обеспечения IBM Business Monitor” на стр. 39. Не создавайте профайл развертывания.
3. Создайте профайл Администратора развертывания с помощью Инструмента управления профайлами или команды `managerprofiles`, согласно инструкциям из раздела Глава 6, “Создание и дополнение профайлов”, на стр. 61.
4. За исключением случая, когда вы создали базу данных MONITOR во время создания профайла, выполните сценарии создания базы данных согласно инструкциям из раздела Глава 5, “Создание баз данных”, на стр. 53.
5. Запустите администратор развертывания.
6. Создайте пользовательские узлы, встраиваемые в ячейку Администратора развертывания, согласно инструкциям из раздела Глава 6, “Создание и дополнение профайлов”, на стр. 61.
7. С помощью административной консоли создайте кластеры, следуя инструкциям из раздела “Создание кластеров IBM Business Monitor” на стр. 104.
8. Настройте службы событий Инфраструктуры событий общего формата (CEI) согласно инструкциям из раздела “Настройка служб событий CEI” на стр. 106.
9. С помощью мастера настройки или команды `wsadmin` настройте среду, следуя инструкциям из раздела “Настройка среды с помощью мастера настройки” на стр. 107

стр. 107 или “Настройка среды с помощью команд wsadmin” на стр. 113. Однако устанавливать необходимые общие компоненты нужно вручную, следуя инструкциям из раздела “Настройка среды вручную” на стр. 116.

10. Настройте дополнительные компоненты, такие как Business Space и IBM Cognos BI, следуя инструкциям из раздела Глава 10, “Настройка компонентов IBM Business Monitor”, на стр. 129.

Установочные каталоги для управляемой среды развертывания для WebSphere Business Modeler

Если для создания и развертывания моделей монитора с целью тестирования используется WebSphere Business Modeler, необходимо установить управляемую среду тестирования. Можно создать управляемую среду тестирования в той же системе, где установлен WebSphere Business Modeler, или на другом сервере, используемом несколькими пользователями WebSphere Business Modeler.

Перед созданием управляемой среды развертывания убедитесь, что имеется не менее 3 Гб памяти в системе, в которой создается управляемая среда развертывания.

Единственный пользователь WebSphere Business Modeler, использующий одну управляемую среду развертывания

Если управляемая среда тестирования создается в той же системе, где установлен WebSphere Business Modeler, или на другом сервере, используйте следующий каталог высокого уровня для установки среды.

Перед началом создания этого пути установки необходимо заранее установить следующие продукты на одной рабочей станции:

- WebSphere Business Modeler 7.0
- Integration Designer 7.5

После установки Integration Designer убедитесь, что опция установки среды тестирования Process Server выбрана.

Для установки WebSphere Business Modeler для отдельного пользователя с использованием одной управляемой среды развертывания выполните следующее:

1. Установить Business Monitor - инструментарий разработки в существующую среду Integration Designer.
2. Создайте файл конфигурации XML, содержащий информацию о соединении для сервера IBM Business Monitor и Business Space. Если файл конфигурации XML уже имеется после установки Integration Designer, можно добавить информацию IBM Business Monitor в качестве дополнительного компонента сервера. Дополнительная информация приведена в разделе "Настройка файла конфигурации сервера".
3. Настройте WebSphere Business Modeler для использования установленной управляемой среды развертывания.

Несколько пользователей WebSphere Business Modeler, использующих одну управляемую среду развертывания

Если управляемая среда тестирования создается в системе, отличной от той, где установлен WebSphere Business Modeler, или для нескольких пользователей WebSphere Business Modeler, используйте следующий каталог высокого уровня для установки среды.

Перед началом создания этого пути установки необходимо заранее установить следующие продукты на одной рабочей станции:

- WebSphere Business Modeler 7.0
- Process Server 7.5 с автономным профайлом

Для установки WebSphere Business Modeler для нескольких пользователей с использованием одной управляемой среды развертывания выполните следующее:

1. С помощью панели запуска продукта IBM Business Monitor установите IBM Business Monitor в существующей среде Process Server. Не создавайте профайл. Следует расширить существующий автономный профайл Process Server.
2. С помощью Инструмента управления профайлом расширьте профайл Process Server шаблоном IBM Business Monitor. Если Business Space не был настроен во время первоначального создания профайла, необходимо настроить Business Space во время расширения профайла.
3. С помощью административной консоли переведите сервер в режим разработки. Выберите **Серверы > Типы серверов > Серверы приложений WebSphere** и щелкните на пункте *имя_сервера*. На вкладке Конфигурация выберите переключатель **Запуск в режиме разработки**, нажмите кнопку **Применить** и сохраните изменения конфигурации.
4. Создайте файл конфигурации XML, содержащий информацию о соединении для сервера IBM Business Monitor и Business Space. Если файл конфигурации XML уже имеется после установки Process Server, можно добавить информацию IBM Business Monitor в качестве дополнительного компонента сервера.
5. Настройте WebSphere Business Modeler для использования установленной управляемой среды развертывания.

Дополнительная информация приведена по связанной ссылке в справочной системе WebSphere Business Modeler Information Center.

Обзор задачи: Установка и настройка

Перед установкой и настройкой IBM Business Monitor for z/OS рекомендуется рассмотреть поток задач для поддерживаемых конфигураций.

На следующей диаграмме показан поток задач верхнего уровня, которые необходимо выполнить перед и после установки IBM Business Monitor for z/OS, а также для настройки продукта.



Для создания полной среды обслуживания приложений IBM Business Monitor for z/OS выполните следующие действия:

1. Установите и настройте базовый сервер приложений (WebSphere Application Server или Process Server).
2. Установите двоичные файлы продукта.
3. Создайте базы данных.
4. Настройте продукт.
5. Запустите сервер.

В зависимости от переменных конфигурации среды и способа настройки файла ответов, может потребоваться выполнить дополнительные задачи настройки .

Глава 3. Подготовка к установке

Перед установкой IBM Business Monitor убедитесь в том, что выполнены все предварительные требования к аппаратному и программному обеспечению. Для некоторых операционных систем требуется специальная подготовка перед установкой.

Требования к аппаратному и программному обеспечению

IBM Business Monitor запускается в операционных системах AIX, HP-UX, Windows, Linux, Linux on zSeries, Solaris и z/OS.

Самые последние требования к аппаратному и программному обеспечению можно найти на веб-странице: [System requirements for IBM Business Monitor](#).

Эти ссылки включают в себя поддерживаемые серверы LDAP. Автономные реестры LDAP также поддерживаются в IBM Business Monitor. Все приведенные ниже текущие определения области доступны для ваших текущих хранилищ учетных записей пользователей:

- Встроенные хранилища
- Локальная операционная система
- Автономный реестр LDAP
- Автономный пользовательский реестр

Подготовка операционных систем к установке продукта

Перед установкой IBM Business Monitor необходимо подготовить операционную систему. Конфигурация зависит от типа используемой операционной системы.

Перед тем как начать подготовку среды установки, выполните следующие задачи:

- Выключите брандмауэр, если он работает в системе, в которую планируется установить IBM Business Monitor.
- Убедитесь, что при входе в систему у вас есть доступ к командам базы данных DB2 или Oracle.
- Выполните дополнительные задачи конкретно для вашей операционной системы.

Подготовка систем AIX к установке

Перед установкой IBM Business Monitor необходимо подготовить операционную систему AIX.

Поскольку WebSphere Application Server является предварительным требованием IBM Business Monitor, выполните следующие обязательные этапы подготовки, описанные в разделе Подготовка операционной системы к установке продукта в справочной службе WebSphere Application Server.

Поскольку определенные этапы относятся к конкретным версиям операционной системы, не все этапы могут быть применимы к вашей среде. Если для этапа не указана конкретная среда, то его необходимо выполнять для всех операционных систем.

Дополнительная информация о подготовке к настройке Installation Manager для работы в 64-разрядных системах AIX приведена в следующем техническом комментарии: <http://www-01.ibm.com/support/docview.wss?uid=swg24027719>

В системе AIX перед установкой IBM Business Monitor выполните следующие действия:

1. Если планируется установить сводные панели на основе портлетов, то перед тем как устанавливать WebSphere Portal или сводные панели на основе портлетов, задайте максимальное число открытых файлов с помощью следующей команды:

```
ulimit -n 8800
```

Можно также внести изменения в файл ограничений на ресурсы, выполнив следующие действия:

- a. Откройте файл `/etc/security/limits`.
- b. Измените или добавьте раздел **default**, включив в него следующую строку:

```
nofiles = 8800
```

- c. Сохранить и закрыть файл.
- d. Выйдите из операционной системы и войдите в нее снова.

2. Установите для **umask** значение 022 с помощью следующей команды:

```
umask 022
```

3. Убедитесь, что установлен браузер Mozilla Firefox версии 3.5.x.x или более поздней.

4. Перед запуском службы перемещения данных увеличьте число процессов, настроенных в операционной системе AIX, чтобы избежать ошибки сброса соединения. Это можно сделать с помощью команды или интерфейса AIX.

- Выполните команду:

```
chgdev -l sys0 -a maxuproc='256'
```

- В интерфейсе AIX введите **smitty**, затем выберите **Системные среды > Изменить / показать характеристики операционной системы > Число процессов, допустимых для пользователя (Кол-во)**.

5. Выполните инструкции по настройке систем AIX.

Подготовка систем HP-UX к установке

Перед установкой IBM Business Monitor необходимо подготовить операционную систему HP-UX.

Поскольку WebSphere Application Server является предварительным требованием IBM Business Monitor, выполните следующие обязательные этапы подготовки, описанные в разделе Подготовка операционной системы к установке продукта в справочной службе WebSphere Application Server.

Поскольку определенные этапы относятся к конкретным версиям операционной системы, не все этапы могут быть применимы к вашей среде. Если для этапа не указана конкретная среда, то его необходимо выполнять для всех операционных систем.

В системе HP-UX перед установкой IBM Business Monitor выполните следующие шаги:

1. Если планируется установить сводные панели на основе портлетов, то перед тем как устанавливать WebSphere Portal или сводные панели на основе портлетов, задайте максимальное число открытых файлов с помощью следующей команды:

```
ulimit -n 8800
```


Можно также внести изменения в файл ограничений на ресурсы, выполнив следующие действия:

- a. Откройте файл `/etc/security/limits`.
 - b. Измените или добавьте раздел **default**, включив в него следующую строку:
`nfiles = 8800`
 - c. Сохранить и закрыть файл.
 - d. Выйдите из операционной системы и войдите в нее снова.
2. Установите для **umask** значение 022 с помощью следующей команды:
`umask 022`
 3. Выполните необходимые действия для Настройки систем HP-UX.

Подготовка систем Linux к установке

Перед установкой IBM Business Monitor необходимо подготовить операционную систему Linux.

Поскольку WebSphere Application Server является предварительным требованием IBM Business Monitor, выполните следующие обязательные этапы подготовки, описанные в разделе Подготовка операционной системы к установке продукта в справочной службе WebSphere Application Server.

Убедитесь, что установлен браузер Mozilla Firefox версии 3.5.x.x или более поздней.

Поскольку определенные этапы относятся к конкретным версиям операционной системы, не все этапы могут быть применимы к вашей среде. Если для этапа не указана конкретная среда, то его необходимо выполнять для всех операционных систем. Инструкции по установке Installation Manager в системе Red Hat Enterprise Linux 6.0 (64-разрядная версия) приведены в разделе Сбой установки Installation Manager в RHEL 6.0 (64-разрядная версия).

Если планируется использовать DB2 Express в системе Red Hat Enterprise Linux 6:

- Перед запуском установки DB2 Express выполните следующую команду от имени пользователя root:

```
sysctl -w kernel.shmmax=268435456
```

Эта команда действует только до перезапуска системы. Для устранения неполадки выполните следующую команду:

```
/etc/sysctl.conf:  
kernel.shmmax = 268435456
```

- Необходимо установить оболочку Korn ksh-версия.rpm.

В системе Linux перед установкой IBM Business Monitor выполните следующие действия:

1. Укажите максимальное число открытых файлов не менее 8800. Как правило, значения по умолчанию недостаточно. Текущее максимальное число открытых файлов можно посмотреть с помощью команды `ulimit -n`. В следующем примере показано, как увеличить максимальное число открытых файлов до 8800.

Linux

- a. Откройте файл `/etc/security/limits.conf`.
- b. Найдите параметр `nofile` и увеличьте его значение. Если не существует строки с параметром `nofile`, добавьте к файлу следующие строки:
`* hard nofile 8800`

* soft nofile 8800

- c. Сохранить и закрыть файл.
- d. Выйдите из системы и войдите снова.

Для просмотра дополнительной информации об этом параметре выполните команду `man limits.conf` или обратитесь к разделу Подготовка операционной системы к установке продукта справочной системы WebSphere Application Server Information Center.

2. Установите следующие пакеты для операционной системы:

Опция	Описание
Red Hat Enterprise Linux 4	compat-libstdc++-33-3.2.3-47.3 compat-db-4.1.25-9 xorg-x11-deprecated-libs-6.8.1 или xorg-x11-deprecated-libs-6.8.2 rpm-build-4.3.3-7.nonplt compat-libstdc++-296-2.96-132.7.2
Red Hat Enterprise Linux 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 libXp-1.0.0-8 rpm-build-4.4.2-37.el5 Только для 64-разрядного ядра: compat-libstdc++-296-2.96-138
Red Hat Enterprise Linux 6	Оболочка Korn ksh-version.rpm Подробные инструкции и список пакетов приведены в разделе Сбой установки Installation Manager в RHEL 6.0 (64-разрядная версия)
SUSE Linux Enterprise Server 9.0	XFree86-libs-32bit-9 glibc-32bit-9 glib-32bit-9 gtk-32bit-9

Можно также установить более поздний выпуск любого из этих пакетов, если имеются новые пакеты с исправленными опечатками. Если имеются дополнительные пакеты конкретно для вашего аппаратного обеспечения, установите их.

Зависимости можно установить с помощью командной строки (все требуемые пакеты). Ниже приведены примеры для администраторов пакетов поддерживаемых вариантов Linux.

- **Red Hat Enterprise Linux 5 (32-разрядная версия):**
`yum install compat-libstdc++-33 compat-db libXp rpm-build RHEL 5.x`
- **Red Hat Enterprise Linux 5 (64-разрядная версия):**
`yum install compat-libstdc++-33 compat-db libXp rpm-build compat-libstdc++-296`
- **SUSE Linux:**
`zypper install XFree86-libs-32bit-9 glibc-32bit-9 glib-32bit-9 gtk-32bit-9`

3. Установите для **umask** значение 022 с помощью следующей команды:

`umask 022`

4. В системах Red Hat Enterprise Linux 5 выключите SELinux или установите для него разрешительный режим.

5. Перезапустите компьютер.
6. Выполните инструкции по настройке систем Linux.

Подготовка систем Solaris к установке

Перед установкой IBM Business Monitor необходимо подготовить операционную систему Solaris.

Поскольку WebSphere Application Server является предварительным требованием IBM Business Monitor, выполните следующие обязательные этапы подготовки, описанные в разделе Подготовка операционной системы к установке продукта в справочной службе WebSphere Application Server.

JVM Java HotSpot была разработана компанией Sun Microsystems для операционной системы Solaris и перенесена в операционную систему HP-UX. Структура кучи Java JVM HotSpot и способ управления кучей отличается от других JVM. В среде может потребоваться дополнительная настройка управления кучей JVM, чтобы избежать ошибок `java.lang.OutOfMemoryError: PermGen` в ходе создания профайла или работы сервера. Может потребоваться обновить значение параметра JVM **MaxPermSize**.

Поскольку определенные этапы относятся к конкретным версиям операционной системы, не все этапы могут быть применимы к вашей среде. Если для этапа не указана конкретная среда, то его необходимо выполнять для всех операционных систем.

Дополнительная информация о подготовке к настройке Installation Manager для работы в 64-разрядных системах AIX приведена в следующем техническом комментарии: <http://www-01.ibm.com/support/docview.wss?uid=swg24027719>

Перед тем как устанавливать IBM Business Monitor, выполните следующие действия в своей системе Solaris:

1. Если планируется установить сводные панели на основе портлетов, то перед тем как устанавливать WebSphere Portal или сводные панели на основе портлетов, задайте максимальное число открытых файлов с помощью следующей команды:

```
ulimit -Hn 8800
```

Можно также внести изменения в файл ограничений на ресурсы, выполнив следующие действия:

- a. Откройте `/etc/system`
 - b. Добавьте в конец файла следующую строку:

```
set rlim_fd_max=8800
```
 - c. Сохранить и закрыть файл.
 - d. Выйдите из операционной системы и войдите в нее снова.
2. Задайте для `umask` значение, равное `022`, с помощью следующей команды:

```
umask 022
```

3. Выполните необходимые действия для Настройки систем Solaris.

Перед созданием или дополнением профайлов IBM Business Monitor в системе Solaris измените значение параметра JVM **MaxPermSize** в соответствии с инструкциями из раздела Исправление ошибок `OutOfMemoryError` при создании профайла в системах Solaris и HP-UX

Подготовка систем Windows к установке

Перед установкой IBM Business Monitor необходимо подготовить операционную систему Windows.

Поскольку установка продукта WebSphere Application Server является предварительным требованием для установки IBM Business Monitor, необходимо выполнить все подготовительные задачи для WebSphere Application Server до установки IBM Business Monitor.

В системе Windows перед установкой IBM Business Monitor выполните следующие шаги:

1. Выполните действия, описанные в разделе Подготовка системы Windows к установке в справочной службе WebSphere Application Server Information Center.
2. Выполните необходимые действия для Настройки систем Windows.

Глава 4. Установка IBM Business Monitor

IBM Business Monitor может быть установлен на нескольких топологиях. Можно установить все компоненты на одном сервере или распределить компоненты по разным серверам. Для создания среды высокой готовности с поддержкой автоматического переноса ресурсов в случае сбоя можно установить IBM Business Monitor в кластерную среду, использующую механизм кластеризации WebSphere Application Server или Process Server.

Важное замечание: IBM Business Monitor работает на нескольких платформах. Сведения о поддерживаемых операционных системах и аппаратном обеспечении, необходимом объеме оперативной и дисковой памяти можно найти на странице: Системные требования для IBM Business Monitor.

Установка программного обеспечения IBM Business Monitor

Установить IBM Business Monitor можно интерактивно или неинтерактивно. В своей среде монитора IBM Business Monitor можно использовать с другим программным обеспечением, включая WebSphere Portal или Process Server.

В случае интерактивной установки IBM Business Monitor необходимо использовать Installation Manager, независимо от того, устанавливаете ли вы все компоненты IBM Business Monitor на одном сервере или же в разных кластерах в среде сетевого развертывания.

В качестве альтернативы, можно заранее создать файл ответов и установить IBM Business Monitor неинтерактивно из командной строки, не взаимодействуя с программой установки IBM Business Monitor.

Установка из панели запуска продукта

Программа панели запуска продукта IBM Business Monitor предоставляет единое расположение для просмотра информации о выпуске IBM Business Monitor, установки WebSphere Application Server, если это необходимо, и запуска процесса установки продукта.

Выполните задачи предварительного этапа установки, описанные в разделе Глава 3, “Подготовка к установке”, на стр. 33, если вы этого еще не сделали.

Для просмотра списка установочных расположений по умолчанию перейдите по ссылке на связанную информацию.

 Для установки или выполнения IBM Business Monitor в операционных системах Windows 7, Windows Vista и Windows Server 2008 требуется повышение полномочий учетной записи пользователя Microsoft Windows. Вне зависимости от того, являетесь ли вы администратором или обычным пользователем, откройте контекстное меню файла `1aunchpad.exe` и выберите команду **Запуск от имени администратора**.

Из панели запуска продукта выполните установку IBM Business Monitor в следующих случаях:

- Установка с дисков DVD продукта

- Установка из электронного установочного образа, расположенного в локальной файловой системе
- Установка из электронного установочного образа, расположенного на общем диске

Для того чтобы запустить программу панели запуска и установить WebSphere Application Server, выполните следующие действия:

1. Вставьте первый диск DVD IBM Business Monitor в накопитель.

  Смонтируйте диск DVD.

2. Если в системе включено автоматическое выполнение, то автоматически откроется панель запуска IBM Business Monitor. Если автоматическое выполнение не включено в системе:
 - Выполните файл `launchpad.sh`, расположенный в корневом каталоге диска DVD.
 - Выполните файл `launchpad.exe` или `launchpad64.exe` для 64-разрядных систем, расположенный в корневом каталоге диска DVD.
3. Необязательно: Выберите **Установка справочной системы**, чтобы установить справочную систему и документацию. Справочная система — это структура Eclipse для просмотра документации.
4. Если вы являетесь членом группы Администратор в системе Windows или пользователем `root` в системе Linux или UNIX, выберите опцию **Установить от имени администратора**. Очистите этот переключатель, если вы не являетесь администратором, или если вы хотите выполнить установку для своего собственного имени, не предоставляя прав доступа другим пользователям.
5. Если **WebSphere Application Server** еще не установлен, нажмите кнопку **Установить** для запуска установки IBM Business Monitor. Installation Manager будет запущен и настроен автоматически. Перейдите к разделу “Интерактивная установка IBM Business Monitor” на стр. 41 для просмотра оставшихся инструкций по установке.
6. Для установки **IBM Business Monitor** поверх существующей установки **WebSphere Application Server** выберите **Установка в существующем WebSphere Application Server**.
 - a. Если вы являетесь членом группы Администратор в системе Windows или пользователем `root` в системе Linux или UNIX, выберите опцию **Установить от имени администратора**. Очистите этот переключатель, если вы не являетесь администратором, или если вы хотите выполнить установку для своего собственного имени, не предоставляя прав доступа другим пользователям.
 - b. Нажмите кнопку **Импортировать или обновить**.
 - Если появится окно Открыть файл, нажмите **Выполнить**. Откроется Installation Manager.
 - Нажмите кнопку **Импорт** для импорта WebSphere Application Server в Installation Manager. Необходимо импортировать WebSphere Application Server, если он не был ранее импортирован, или если он был обновлен с помощью Установщика обновлений после последнего импорта.
 - Нажмите **Обзор** и выберите каталог, в котором был установлен WebSphere Application Server, например `app_server_root`.
 - Нажмите **Далее**, затем **Импортировать**.
 - Нажмите кнопку **Готово**.
 - В окне Installation Manager нажмите **Обновить**.
 - Выберите группу пакетов **IBM WebSphere Application Server - ND**.

Совет: На странице Обновить пакеты выберите **Показать все** для просмотра доступных обновлений.

- Нажмите **Далее** и следуйте инструкциям на каждой странице, принимая значения по умолчанию. Пакет комплектов для XML будет обновлен до требуемого уровня.
 - Закройте Installation Manager и вернитесь в приложение панели запуска.
- c. Нажмите кнопку **Установить** для начала установки IBM Business Monitor. Если появится окно Открыть файл, нажмите **Выполнить**.
- d. Выберите **Установить IBM Business Monitor**. Installation Manager будет запущен и настроен автоматически. Перейдите к разделу “Интерактивная установка IBM Business Monitor” для просмотра оставшихся инструкций по установке.

В поддерживаемой операционной системе можно нажать кнопку **Установка справочной системы** на панели запуска для установки справочной системы Information Center.

Интерактивная установка IBM Business Monitor

IBM Business Monitor 7.5 можно установить интерактивно с помощью Администратора установки, независимо от того, устанавливаются ли все компоненты на одиночном сервере, или в кластерах среды сетевого развертывания.

Запустите администратор установки из панели запуска продукта. Смотрите раздел “Установка из панели запуска продукта” на стр. 39.

Для просмотра списка установочных расположений по умолчанию перейдите по ссылке на связанную информацию.

Для установки IBM Business Monitor выполните следующие действия:

1. На начальной странице Installation Manager нажмите **Установить пакеты** и нажмите кнопку **Далее** для продолжения. Выбраны следующие пакеты:
 - IBM Cognos Business Intelligence (выключите переключатель, если установка выполняется обычным пользователем в системе Windows)
 - WebSphere Application Server - ND (выключите переключатель, если пакет уже установлен)
 - WebSphere Application Server Feature Pack for XML (выключите переключатель, если пакет уже установлен)
 - DB2 Express (выключите переключатель, если база данных уже установлена или если установка выполняется обычным пользователем)
 - IBM Business Monitor

Если во время проверки предварительных требований получено следующее предупреждающее сообщение, выполните приведенные ниже пошаговые инструкции по увеличению значения ulimit применительно к своей платформе.

В текущей системе обнаружен более низкий уровень ulimit, чем рекомендуемое значение (8799). Увеличьте ulimit. Закройте программу установки. Если вы являетесь пользователем root, откройте командную строку и выполните следующие действия:

- a. Задайте максимальное число открытых файлов с помощью следующей команды:



```
> Linux
```

- 1) Откройте файл /etc/security/limits.conf.
- 2) Найдите параметр nofile и увеличьте его значение. Если не существует строки с параметром nofile, добавьте к файлу следующие строки:
* hard nofile 8800

* soft nofile 8800

- 3) Сохранить и закрыть файл.
 - 4) Выйдите из системы и войдите снова.
 - b. Перезапустите компьютер.
 - c. Перезапустите программу установки.
2. На странице Лицензии ознакомьтесь с лицензионными соглашениями для выбранного пакета.
- Если для установки выбрано несколько пакетов, каждый из них может содержать отдельное лицензионное соглашение. В левой части страницы **Лицензия** последовательно просмотрите лицензионные соглашения всех версий пакета. Выбранные для установки версии пакета (например, базовый пакет и обновление) отображаются под именем пакета.
- a. Выберите **Я принимаю условия лицензионного соглашения**.
 - b. Нажмите **Далее** для продолжения.
3. Если IBM Business Monitor V7.5 является первым пакетом, установленным с помощью Администратора установки, введите путь к *каталогу общих ресурсов* в поле **Каталог общих ресурсов** на странице Расположение или примите путь по умолчанию. Каталог общих ресурсов содержит ресурсы, доступные одной или нескольким группам пакетов.

Важное замечание:

- a. Каталог общих ресурсов можно указать только в ходе установки первого пакета. Для размещения каталога общих ресурсов рекомендуется использовать диск максимальной емкости. Изменить расположение каталога можно только после удаления всех пакетов.
 - b. В имени установочного каталога недопустимы скобки.
 - c.   В имени установочного каталога недопустимы пробелы. Нажмите **Далее** для продолжения.
4. На следующей странице Расположение можно создать *группу пакетов*, в которую следует установить пакет IBM Business Monitor. Для создания новой группы пакетов выполните следующие действия:
- a. Выберите **Создать новую группу пакетов**.
 - b. Введите путь к установочному каталогу группы пакетов. В имени установочного каталога недопустимы скобки. (Для Linux или UNIX. Не включайте пробелы в путь к каталогу.) Имя группы пакетов создается автоматически.
 - c. Нажмите **Далее** для продолжения.
- Мастер установки пакетов выведет сообщение, если он обнаружит какие-то выполняемые процессы (например, сервер WebSphere Application Server). Если это сообщение будет показано, нажмите **Отменить**, остановите выполняющиеся процессы и начните установку снова.
5. На странице Компоненты выберите компоненты пакета, которые вы хотите установить.
- a. Необязательно: Для просмотра отношений зависимости между компонентами выберите переключатель **Показать зависимости**.
 - b. Необязательно: При необходимости щелкните на компоненте для просмотра его краткого описания в поле **Сведения**.
 - c. Выберите или очистите компоненты пакета. Installation Manager автоматически выбирает зависимые компоненты и отображает текущий размер и требования к дисковой памяти.

- Если вы не выберете никаких компонентов, будут установлены файлы лицензии Business Space и IBM Business Monitor.
- Если развернуть **Business Monitor Server** и выбрать один или несколько автономных профайлов разработки, они будут созданы в процессе установки. Для того чтобы создать профайлы разработки Process Server или WebSphere Enterprise Service Bus, эти пакеты уже должны быть установлены. Автономный профайл разработки - это профайл разработки по умолчанию, который предоставляет среду тестирования IBM Business Monitor. В профайле разработки Process Server также включен Администратор бизнес-правил. Для того чтобы создать автономный профайл разработки, необходимо указать идентификационные данные административной защиты (имя пользователя и пароль) для создаваемого сервера.

Автономный профайл разработки не может быть использован в рабочей среде. Если вы решили не устанавливать автономный профайл разработки по умолчанию, вы можете установить его позже, запустив Администратор установки и выбрав **Изменить** на первой странице.

- После выбора компонентов для продолжения нажмите кнопку **Далее**.
- Если вы выбрали автономный профайл разработки, то введите на странице Профайлы одноразовые разрешения для него. Именем пользователя по умолчанию является `admin`, а паролем по умолчанию — `admin`.
- Если база данных уже существует, введите на странице Общие конфигурации идентификационные данные для базы данных. При выборе DB2 Express введите имя пользователя и пароль DB2. Именем пользователя по умолчанию является `bpadmin`, а паролем по умолчанию — `bpadmin1`.

Важное замечание: Измените пароль по умолчанию, если он не соответствует требованиям стратегии паролей операционной системы (такой как Windows 2008).

Ограничение: В именах пользователей недопустимы символы национальных языков.

Нажмите **Далее** для продолжения.

- На странице Обзор просмотрите выбранные вами параметры перед установкой пакета IBM Business Monitor. Если вы хотите изменить выбранные на предыдущих страницах параметры, нажмите кнопку **Назад** и измените их. Если вы удовлетворены выбранными вариантами, нажмите **Установить** для установки пакета. В ходе установки отображается индикатор состояния.
- После завершения установки показывается подтверждающее сообщение.
 - Необязательно: Нажмите кнопку **Показать файл протокола** для просмотра файла протокола текущего сеанса в новом окне. Для продолжения необходимо закрыть окно протокола установки.
 - В поле **Какую программу вы хотите запустить?** укажите, нужно ли запускать Инструмент управления профайлами в тот момент, когда вы выходите из системы. Если автономный профайл разработки уже создан, выберите **Нет**. Для рабочей системы необходимо определить автономный профайл сервера или администратор развертывания, воспользовавшись Инструментом управления профайлами или командой `manageprofiles`. Более подробная информация находится в разделе "Создание и дополнение профайлов".
 - Нажмите кнопку **Готово**, чтобы выйти из Администратора установки.

Для рабочей системы необходимо создать автономный профайл сервера или администратор развертывания с помощью Инструмента управления профайлами или команды `manageprofiles`.

Ограничение: Если вы создали автономный профайл разработки в процессе установки, помните, что он не работает в рабочей среде. Он предназначен для ознакомления с IBM Business Monitor без создания рабочего профайла. Профайл можно запустить из его консоли Первые шаги.

- Откройте командное окно. Перейдите к файлу `profile_root/firststeps.wbm` и выполните команду `firststeps.sh`.
- Выберите **Пуск > Все программы > IBM > Business Monitor 7.5 > Профайлы > имя-профайла > Первые шаги**.
- Перейдите к файлу `profile_root\firststeps.wbm` и запустите команду `firststeps.bat`.

Важное замечание: Для установки или выполнения консоли Первые шаги в Windows 7, Windows Vista или Windows Server 2008, необходимо повысить права доступа учетной записи пользователя Microsoft Windows, щелкнув правой кнопкой мыши на файле `firststeps.bat` и выбрав опцию **Запуск от имени администратора**. Это требуется как для административных, так и для других пользователей.

В поддерживаемой операционной системе можно нажать кнопку **Установка справочной системы** на панели запуска для установки справочной системы Information Center.

Установка IBM Business Monitor без вывода сообщений

Пакет продукта IBM Business Monitor можно установить в режиме *без вывода сообщений*. В ходе установки в режиме без вывода сообщений пользовательский интерфейс недоступен. Вместо него выполняется команда на использование файла ответов, который устанавливает продукт.

Эта процедура установки без вывода сообщений учитывает, что необходимые продукты для установки IBM Business Monitor могут быть или могут не быть предварительно установлены. Эти продукты включают WebSphere Application Server Network Deployment, Installation Manager, и Feature Pack for XML.

Перед установкой IBM Business Monitor просмотрите требования к системе для этого продукта.

Особенно важны необходимые уровни операционной системы и программного обеспечения. Хотя процедура установки автоматически проверяет наличие необходимых исправлений операционной системы, просмотрите перечень предварительных требований, если это еще не сделано. В разделе перечислены все поддерживаемые операционной системы и их исправления и обновления, которые необходимо установить, чтобы получить согласованную операционную систему. Также перечислены требуемые уровни всего необходимого программного обеспечения.

Windows **Важная информация:** для установки или выполнения IBM Business Monitor в Windows 7, Windows Vista или Windows Server 2008 требуется повышение полномочий учетной записи пользователя Microsoft Windows; для этого откройте контекстное меню командной строки, в которой запускается команда установки без вывода сообщений, и выберите команду **Запуск от имени администратора**. Это должен сделать как администратор, так и пользователь без прав администратора.

Установка без вывода сообщений выполняет некоторые из или все следующие задачи:

- Устанавливает Installation Manager, если он не установлен, или обновляет его до соответствующего уровня, если он уже установлен.
- Устанавливает необходимые базовые продукты и IBM Business Monitor с помощью созданного вами файла ответов.

Для того чтобы установить IBM Business Monitor в режиме без вывода сообщений, выполните следующие шаги:

1. Перед установкой прочитайте и примите условия лицензионного соглашения. Добавление параметра `-acceptLicense` в файл ответов означает, что вы принимаете все лицензии.
2. Создайте файл ответов, который установит требуемые базовые продукты и IBM Business Monitor. Скопируйте пример файла ответов в следующий каталог, чтобы создать свой файл ответов:

корневой-каталог-DVD/responsefiles/BPM/template_response.xml

3. Для создания вашего файла ответов измените параметры согласно указаниям в тексте шаблона файла ответов. Файл ответов также можно создать путем записи действий, выполняемых в Installation Manager. При записи файла ответов будет создан файл XML, содержащий все опции, выбранные в Installation Manager. В режиме без вывода сообщений Installation Manager выполняет установку в соответствии с информацией из файла ответов XML.

Важное замечание: Убедитесь, что расположения хранилищ в начале примера файла ответов указывают на правильное хранилище в среде.

4. Запустите следующую команду:

Администратор или пользователь root: 

корневой-каталог-DVD\IM\installc.exe -acceptLicense input

корневой-каталог-DVD/responsefiles\ИД-продукта\template_response.xml -log каталог-протокола\si

корневой-каталог-DVD/IM/installc -acceptLicense input

корневой-каталог-DVD/responsefiles/ИД-продукта/template_response.xml -log каталог-протокола/si

Не администратор/пользователь не root: 

корневой-каталог-DVD\IM\userinstc.exe -acceptLicense input

корневой-каталог-DVD/responsefiles\ИД-продукта\template_response.xml -log каталог-протокола\si

корневой-каталог-DVD/IM/userinstc -acceptLicense input

корневой-каталог-DVD/responsefiles/ИД-продукта/template_response.xml -log каталог-протокола/si

Installation Manager установит все необходимые компоненты и IBM Business Monitor и запишет файл протокола в указанный каталог.

Необходимо определить автономный профайл сервера или администратор развертывания в Инструменте управления профайлами или с помощью команды `managerprofiles`. В рабочей среде могут быть использованы только профайлы, созданные с помощью Инструмента управления профайлами или команды `managerprofiles`.

Работа с IBM Installation Manager

В этом разделе описаны некоторые общие задачи, относящиеся к IBM Installation Manager. Более подробная информация приведена в справочной системе Installation Manager Information Center.

Установка Installation Manager в Windows

Когда вы запускаете установку продукта из панели запуска, то автоматически выполняется установка IBM Installation Manager, если он еще не установлен на рабочей станции. В других случаях необходимо запустить установку Installation Manager.

Для того чтобы установить Installation Manager вручную:

1. Запустите файл `install.exe` из папки IM в установочном образе.
2. Нажмите кнопку **Далее** на странице Установка пакетов.
3. Прочитайте лицензионное соглашение на странице Лицензионное соглашение и выберите **Я согласен с условиями лицензионного соглашения** для принятия условий. Нажмите кнопку **Далее**.
4. Нажмите кнопку **Обзор** на странице Целевая папка, чтобы изменить расположение установки, если требуется. Нажмите кнопку **Далее**.
5. Нажмите кнопку **Установить** на странице Обзор. После завершения установки показывается подтверждающее сообщение.
6. Нажмите **Готово**. Откроется IBM Installation Manager.

Установка Installation Manager в Linux и UNIX

Когда вы запускаете установку продукта из панели запуска, то автоматически выполняется установка IBM Installation Manager, если он еще не установлен на рабочей станции. .

Для того чтобы установить Installation Manager вручную:

1. Откройте окно терминала, работая с правами доступа пользователя root.
2. Выполните файл `install` из папки IM_linux в установочном образе.
3. Нажмите кнопку **Далее** на странице Установка пакетов.
4. Прочитайте лицензионное соглашение на странице Лицензионное соглашение и выберите **Я согласен с условиями лицензионного соглашения** для принятия условий. Нажмите кнопку **Далее**.
5. Если необходимо, измените расположение каталога установки. Нажмите кнопку **Далее**.
6. Нажмите кнопку **Установить** на странице сводной информации. После завершения установки показывается подтверждающее сообщение.
7. Нажмите кнопку **Готово**. Когда вы запускаете установку продукта из панели запуска, то автоматически выполняется установка IBM Installation Manager, если он еще не установлен на рабочей станции.

Запуск Installation Manager в Windows

Когда вы запускаете установку продукта из панели запуска, то автоматически выполняется установка IBM Installation Manager, если он еще не установлен на рабочей станции. Эта автоматическая установка запустит Installation Manager с настроенным значением параметра хранилища и выбранными пакетами IBM Business Monitor. Если вы запускаете Installation Manager непосредственно, необходимо установить параметр хранилища и выбрать пакеты продукта вручную.

Для того чтобы запустить Installation Manager вручную:

1. Откройте меню **Пуск** из **Панели инструментов**.
2. Выберите **Все программы > IBM Installation Manager > IBM Installation Manager**.

Запуск Installation Manager в Linux и UNIX

Когда вы запускаете установку продукта из панели запуска, то автоматически выполняется установка IBM Installation Manager, если он еще не установлен на рабочей станции. Эта автоматическая установка запустит Installation Manager с настроенным значением параметра хранилища и выбранными пакетами IBM Business Monitor. Если вы запускаете Installation Manager непосредственно, необходимо установить параметр хранилища и выбрать пакеты продукта вручную.

Для того чтобы запустить Installation Manager вручную:

1. Откройте окно терминала, работая с правами доступа пользователя root.
2. Перейдите в каталог установки для Installation Manager (по умолчанию `/opt/IBM/InstallationManager/eclipse` для установки пользователем root или *каталог-пользователя/IBM/InstallationManager/eclipse* для установки другим пользователем) и выполните IBMIM.

Удаление Installation Manager из системы Windows

Для удаления Installation Manager вручную выполните следующие действия:

1. Выберите **Пуск > Параметры > Панель управления**, а затем дважды щелкните мышью на **Добавить или удалить программы**.
2. Выберите запись для IBM Installation Manager и нажмите **Удалить**.

Удаление Installation Manager из системы Linux и UNIX

Удалять IBM Installation Manager необходимо с помощью инструмента управления пакетами, который включен в Linux или UNIX.

Для удаления Installation Manager вручную выполните следующие действия:

1. Откройте окно терминала, работая с правами доступа пользователя root.
2. Перейдите в каталог `uninstallation` в установке Installation Manager. По умолчанию этим каталогом является `/var/ibm/InstallationManager/uninstall`.
3. Выполните `./uninstall`.

Обновление Installation Manager с помощью сервера proxu

Серверы proxu позволяют устанавливать соединения с удаленными серверами из-за брандмауэра. Параметры серверов proxu можно задать в Installation Manager или в файле ответов. После включения сервер proxu используется во всех соединениях сервера. Подробные сведения о том, как настроить Installation Manager для сервера proxu, приведены в разделе **Параметры Internet** справочной системы Installation Manager Information Center.

Установка и удаление Installation Manager в режиме без вывода сообщений

IBM Installation Manager можно установить и удалить из системы в режиме без вывода сообщений.

Установка Installation Manager в режиме без вывода сообщений:

Для того чтобы установить Installation Manager в режиме без вывода сообщений, извлеките программу установки и перейдите в подкаталог IM, затем выполните следующую команду:

- `install --launcher.ini -acceptLicense silent-install.ini -log <полное имя файла протокола>`. Например, `install --launcher.ini -acceptLicense silent-install.ini -log /root/mylogs/mylogfile.xml`
- `installc --launcher.ini -acceptLicense silent-install.ini -log <полное имя файла протокола>`. Например: `installc --launcher.ini -acceptLicense silent-install.ini -log c:\mylogfile.xml`

После установки можно использовать Installation Manager или программу установки Installation Manager для установки пакетов в режиме без вывода сообщений.

Удаление Installation Manager из системы Windows в режиме без вывода сообщений:

Для того чтобы удалить Installation Manager из системы Windows в режиме без вывода сообщений, выполните следующие действия:

1. В командной строке перейдите в каталог удаления Installation Manager. Каталог по умолчанию: `C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager\uninstall`.
2. Введите следующую команду: `uninstallc.exe --launcher.ini silent-uninstall.ini`

Удаление Installation Manager из системы Linux в режиме без вывода сообщений:

Для того чтобы удалить Installation Manager из другой системы в режиме без вывода сообщений, выполните следующие действия:

1. В окне терминала перейдите в каталог удаления каталогов Installation Manager. Каталог по умолчанию: `/var/ibm/InstallationManager/uninstall`.
2. Выполните следующую команду: `uninstall --launcher.ini silent-uninstall.ini`

Группы пакетов и каталог общих ресурсов

При установке пакета IBM Business Monitor for z/OS с помощью IBM Installation Manager необходимо установить его в существующую группу пакетов, содержащую WebSphere Application Server.

Группы пакетов

Группа пакетов представляет собой каталог, в котором пакеты совместно используют пользовательский интерфейс или рабочую среду с другими пакетами из этой же группы.

Заметьте, что когда вы устанавливаете несколько пакетов одновременно, все они будут установлены в одну группу пакетов.

Группе пакетов автоматически присваивается имя, однако, вы должны выбрать каталог установки для группы пакетов.

Каталог установки содержит файлы и ресурсы, специфичные для пакетов, установленных в группу пакетов. Встраиваемые модули Eclipse в пакете продукта, которые потенциально могут быть использованы другими группами пакетов, помещаются в каталог общих ресурсов.

Каталог общих ресурсов

Каталог общих ресурсов - это каталог, в котором расположены встраиваемые модули Eclipse, для того чтобы их могли использовать одна или несколько групп пакетов продукта.

Важное замечание: Общий каталог ресурсов можно указать только при первой установке пакета. Лучше всего использовать для этого самый большой диск. Вы не сможете изменить расположение каталога, пока не удалите из системы все пакеты.

Указание параметров хранилища в Installation Manager

Если Installation Manager запускается непосредственно (например, из хранилища, расположенного на веб-сервере), то необходимо указать URL для каталога, который содержит пакет продукта в Installation Manager перед установкой пакета продукта.

Примечание: Если установка производится не с диска DVD и не из установочного образа, получите URL хранилища пакета установки у администратора перед запуском процесса установки.

Для того чтобы добавить, изменить или удалить хранилище в Installation Manager:

1. Запустите Installation Manager.
2. На странице Пуск Installation Manager выберите **Файл > Параметры**, а затем нажмите **Хранилища**. Откроется страница Хранилища, на которой показаны существующие хранилища, их расположения и имеется ли к ним доступ.
3. На странице Хранилища нажмите **Добавить хранилище**.
4. В окне Добавить хранилище введите URL хранилища или найдите его и установите путь к файлу. Типичным расположением хранилища является каталог *каталог-образов/repository.config*, где *каталог-образов* содержит извлеченный установочный образ устанавливаемого продукта.
5. Нажмите кнопку **ОК**. Новое или измененное хранилище появится в списке. Если хранилище не доступно, в столбце **Доступно** будет показан красный крест (x).
6. Нажмите **ОК** для выхода.

Примечание: Для того чтобы Installation Manager нашел хранилища по умолчанию для установленных пакетов, должна быть выбрана опция **Поиск служебных хранилищ в процессе установки и обновления** на странице параметров Хранилища.

Установка Information Center

Справочная система IBM Business Monitor Information Center доступна в Internet. Кроме того, в поддерживаемой операционной системе ее можно установить с помощью панели запуска продукта.

- Установите и запустите Information Center с помощью панели запуска продукта.
 1. В панели запуска выберите **Установка справочной системы**.
 2. Укажите каталог локальной справочной системы Information Center.
 3. Выберите **Установить и запустить справочную систему**. Если появится окно Открыть файл, нажмите **Выполнить**.
- Просмотрите Information Center в Internet. Дополнительная информация приведена в справочной системе IBM Business Process Management Information Center

Запуск и завершение работы локальной справочной системы Information Center

После установки IBM Business Monitor Information Center вы можете просмотреть информацию в локальной системе или предоставить к ней доступ другим пользователям сети.


В этой процедуре `doc_root` представляет каталог, выбранный для установки справочной системы Information Center.

- Для локального просмотра справочной службы выполните следующие действия:
 1. Перейдите в каталог, в котором установлена справочная система Information Center.
 2. Для запуска справочной системы Information Center запустите сценарий, соответствующий вашей операционной системе:
 - `help_start.sh`
 - `help_start.bat`Браузер по умолчанию отображает справочную службу, установленную с продуктом.
 3. Для остановки справочной службы закройте браузер и запустите соответствующий вашей операционной системе сценарий:
 - `help_end.sh`
 - `help_end.bat`
- Для подключения к справочной службе и просмотра ее на других компьютерах сети выполните следующие действия:
 1. Перейдите в каталог, в котором установлен IBM Business Monitor.
 2. Для запуска справочной системы Information Center запустите сценарий, соответствующий вашей операционной системе:
 - `IC_start.sh`
 - `IC_start.bat`Пользователь на другом компьютере должен открыть браузер и перейти по следующему URL-адресу:
`http://имя-хоста:8888/help/index.jsp`
 3. Для остановки справочной службы закройте браузер и запустите соответствующий вашей операционной системе сценарий:
 - `IC_end.sh`
 - `IC_end.bat`

Обновление локальной справочной системы Information Center

Установленную локально версию документации можно обновлять по мере поступления новой документации, если у вас есть соединение с Internet. В локальную справочную систему Information Center можно заносить обновленную документацию и по другим продуктам.

Для обновления документации выполните следующие действия:

1. Щелкните на значке **Обновить** () на панели инструментов справочной системы. Появится список всех уже установленных наборов документации.
2. Нажмите кнопку **Далее**, расположенную в нижней части списка установленной документации. Появится список наборов документации для установки. Эти наборы содержат документацию по продуктам на различных языках и могут также включать наборы документации по различным продуктам.

3. Выберите документацию, которую вы хотите установить.

Совет: Можно выбрать несколько наборов документации.

Документация по выбранному продукту или продуктам будет установлена в справочной системе на вашем компьютере.

Глава 5. Создание баз данных

IBM Business Monitor использует две базы данных: одну — для конфигурации IBM Business Monitor и одну — для хранилища материалов IBM Cognos Business Intelligence.

Базы данных MONITOR и COGNOSCS

По умолчанию база данных для IBM Business Monitor называется MONITOR, а база данных для хранилища материалов IBM Cognos BI называется COGNOSCS.

Базы данных MONITOR и COGNOSCS можно создать в процессе создания автономного профайла или профайла администратора развертывания. Кроме того, их можно создать с помощью инструмента проектирования базы данных (dbDesignGenerator) или вручную с помощью сценария базы данных до или после создания профайла. В среде сетевого развертывания рекомендуется создать эти базы данных перед запуском администратора развертывания и созданием других пользовательских профайлов.

Если сервер IBM Cognos BI уже существует, то создавать базу данных COGNOSCS не требуется, поскольку хранилище материалов уже определено.

Совет: Если сервер IBM Cognos BI использует удаленную базу данных COGNOSCS, то на сервере IBM Cognos BI необходимо установить клиент базы данных. Дополнительная информация приведена в разделах, посвященных особенностям разных баз данных.

Базы данных MONITOR и COGNOSCS могут быть расположены на том же сервере, что и сервер IBM Business Monitor, или на другом сервере. Для автоматического создания баз данных вместе с профайлом инструмент управления профайлов или команду **manageprofiles** необходимо запустить в системе, в которой установлен сервер базы данных. В противном случае используйте файлы сценариев баз данных для создания баз данных. При использовании z/OS, или если сервер баз данных содержит несколько версий или экземпляров базы данных, то создайте базы данных с помощью сценариев баз данных.

Сценарии базы данных

При создании автономного профайла или профайла администратора развертывания создаются сценарии базы данных со значениями, указанными при создании профайла. Такой подход обеспечивает соответствие имен между сервером IBM Business Monitor и базой данных IBM Business Monitor.

При необходимости сценарии базы данных можно создать вручную одним из следующих способов:

- Укажите значения с помощью инструмента проектирования базы данных (DbDesignGenerator), который устанавливается вместе с сервером IBM Business Monitor. Одно из преимуществ применения инструмента проектирования баз данных заключается в возможности одновременной разработки базы MONITOR, базы данных IBM Cognos BI, базы данных Business Space, а также баз данных служб сообщений IBM Business Monitor и инфраструктуры обработки событий

общего формата (CEI). Дополнительная информация приведена в разделе “Создание или настройка сценариев базы данных с помощью инструмента проектирования базы данных”.

- Настройте значения вручную. Дополнительная информация приведена в разделе “Настройка сценариев базы данных вручную” на стр. 56.

После создания и настройки сценариев базы данных запустите их в соответствии с инструкциями, приведенными в разделе “Установка баз данных вручную” на стр. 59.

Таблицы службы сообщений

Службам сообщений для шины интеграции служб IBM Business Monitor и шины Инфраструктуры обработки событий общего формата (CEI) требуются таблицы базы данных. Эти таблицы могут быть созданы автоматически с помощью WebSphere Application Server, если пользователь базы данных IBM Business Monitor обладает достаточными правами доступа и в конфигурации хранилища сообщений шины интеграции служб выбран параметр автоматического создания таблиц. По умолчанию для этой опции указано значение true, если не используется DB2 для z/OS. Кроме того, сценарии базы данных для таблиц службы сообщений можно создать одним из следующих способов:

- Создайте сценарий с помощью инструмента проектирования базы данных (DbDesignGenerator). Дополнительная информация приведена в разделе “Создание или настройка сценариев базы данных с помощью инструмента проектирования базы данных”.
- Создайте таблицы вручную. Дополнительная информация приведена в разделе “Создание таблиц службы сообщений вручную” на стр. 60.

Таблицы Business Space

Если вы используете Business Space, необходимо также настроить таблицы Business Space с помощью сценариев, созданных вместе с автономным профайлом, или с помощью инструмента проектирования базы данных. Дополнительная информация приведена в разделе Настройка таблиц базы данных Business Space в справочной системе Business Space Information Center.

Защита базы данных

При создании баз данных пользователю рабочей базы данных по умолчанию предоставляются права на администрирование объектов базы данных, что упрощает создание баз данных и позволяет серверу IBM Business Monitor автоматически управлять схемой базы данных модели монитора при развертывании и удалении моделей. Если требуется создать защищенные базы данных, то обратитесь к разделам Защита среды базы данных MONITOR и Настройка защиты IBM Cognos BI.

Создание или настройка сценариев базы данных с помощью инструмента проектирования базы данных

С помощью инструмента проектирования базы данных (DbDesignGenerator), который устанавливается вместе с сервером IBM Business Monitor, можно создавать сценарии базы данных, выполняемые до или после создания профайла IBM Business Monitor.

Одним преимуществом использования инструмента проектирования баз данных является возможность проектирования баз данных для IBM Business Monitor, IBM Cognos BI, Business Space и службы сообщений одновременно. Сценарии базы данных создаются для каждого компонента. Кроме того, создается файл dbdesign, который

впоследствии можно передать мастеру среды развертывания для автоматической настройки источников данных при создании сложной топологии IBM Business Monitor.

Если в Инструменте управления профайлами выбран путь **Расширенный**, то можно выбрать опцию **Настройка базы данных с помощью файла эскиза** и указать уже созданный файл эскиза.

Дополнительная информация об инструменте проектирования базы данных приведена в связанных разделах.

Для того чтобы изменить файлы сценария базы данных с помощью инструмента проектирования базы данных, выполните следующие действия:

1. Перейдите в каталог `app_server_root/util/dbUtils`.
2. Выполните команду для запуска утилиты.
 - `DbDesignGenerator.bat`
 - `DbDesignGenerator.sh`
3. В главном меню выберите опцию **(1) Создать эскиз базы данных для автономного профайла или среды развертывания**.
4. В приглашении **Выберите один из следующих поддерживаемых эскизов баз данных** выберите опцию **(1)monitor.nd.topology** или **(2)monitor.standalone**. Опция `monitor.nd.topology` обеспечивает большую гибкость распределения компонентов базы данных в нескольких базах данных.
5. В запросе **Please pick one of the following [database component(s)]** выберите опцию **(1)[Monitor] MONITOR : [master] [status = not complete]**.
6. В запросе **Отредактировать этот компонент базы данных?** введите `y`.
7. В приглашении **Выберите один из следующих поддерживаемых типов баз данных** выберите номер платформы баз данных.
8. Ответьте на последовательность приглашений или нажмите `Enter`, чтобы принять значения по умолчанию там, где это возможно. Вам будет предложено ввести имя базы данных, имя схемы, имя и пароль пользователя и префикс каталога табличного пространства.
9. В запросе **Для пропуска свойств источника данных введите 's' или что-нибудь другое для продолжения** введите `s` (или любой другой символ, кроме `s`) для продолжения ввода информации.
10. Ответьте на последовательность приглашений или нажмите `Enter`, чтобы принять значения по умолчанию там, где это возможно. Появится запрос ввода свойств источника данных.
11. Перед настройкой других компонентов убедитесь, что настройка компонента базы данных IBM Business Monitor завершена. Для завершения настройки базы данных IBM Cognos BI требуется указать идентификационные данные пользователя базы данных. Для остальных параметров можно принять значения по умолчанию.
12. Повторное отображение меню **Please pick one of the following [database component(s)]** указывает, что ввод свойств завершен, если во всех строках показано состояние **[status = complete]**, например **(1)[Monitor] MONITOR : [master] [status = complete]**. Введите `5 [save and exit]` и нажмите `Enter`, чтобы сохранить структуру базы данных.

Компонент базы данных **[Cognos] COGNOSCS** требует дополнительной настройки после завершения настройки **MONITOR**. До завершения настройки для компонента **COGNOSCS** отображается состояние **[status = not complete]**.

13. В приглашении **Введите выходной каталог** нажмите Enter, чтобы принять значение по умолчанию (app_server_root/util/dbUtils), или введите расположение для записи файлов эскиза базы данных.
14. В приглашении **Введите имя выходного файла** нажмите Enter, чтобы принять значение по умолчанию (monitor.standalone.dbdesign), или введите имя файла.
15. В запросе **Создать сценарий базы данных?** введите у и нажимайте клавишу Enter для принятия расположений по умолчанию. Подкаталоги создаются для сценариев баз данных MONITOR и COGNOSCS, сценария хранилища данных службы сообщений и сценариев баз данных Business Space.

Настройка сценариев базы данных вручную

Сценарии базы данных, необходимые для создания баз данных MONITOR и COGNOSCS, поставляются на установочном носителе и копируются на сервер приложений в ходе установки сервера IBM Business Monitor. Эти сценарии баз данных можно настроить вручную для создания базы данных перед установкой сервера или создания профайла.

Для того чтобы изменить файлы сценария базы данных вручную, выполните следующие действия:

1. В текстовом редакторе откройте файл сценария базы данных для программного обеспечения базы данных. Сценарий createDatabase.sql создает базу данных и все необходимые таблицы для IBM Business Monitor. Предоставляются следующие файлы:

Создать базу данных: createDatabase.sql

Создать таблицы (только для базы данных MONITOR): createTables.sql

По умолчанию файлы расположены в следующих каталогах:

(только для распределенных) *корневой_каталог_DVD*/scripts/database/Monitor/*платформа*

корневой_каталог_DVD/scripts/database/Cognos/*платформа*

app_server_root/dbscripts/Monitor

app_server_root/dbscripts/Cognos

app_server_root/profiles/*имя_профайла*/dbscripts/Monitor (автономный)

app_server_root/profiles/*имя_профайла*/dbscripts.wbm (администратор развертывания)

app_server_root/profiles/*имя_профайла*/dbscripts/Cognos

где

корневой_каталог_DVD — это каталог, в который извлечен DVD или загруженный образ

платформа — это операционная система базы данных (например, DB2, Oracle или SQL Server)

корневой-каталог-сервера-приложений — это каталог, в котором установлена IBM Business Monitor

2. Измените следующие переменные в файлах сценария базы данных:

- Для DB2 измените следующие переменные:

@DB_NAME@

Представляет имя базы данных IBM Business Monitor, например MONITOR или Cognos

@SCHEMA@

Представляет имя схемы IBM Business Monitor, например MONITOR или Cognos

@TSDIR@

Каталог табличного пространства

Если в спецификации файла данных табличного пространства @TSDIR@ пропущено, то файл данных будет создан в каталоге администратора базы данных.

@DB_USER@

Пользователь базы данных среды выполнения IBM Business Monitor

- DB2 для z/OS: Измените следующие переменные:

@STOGRP@

Представляет групповое имя хранилища DB2, например SYSDEFLT

@DB_NAME@

Имя базы данных IBM Business Monitor

@SCHEMA@

Имя спецификатора схемы IBM Business Monitor

@DB_USER@

Пользователь базы данных среды выполнения IBM Business Monitor

- Для SQL Server измените следующие переменные:

@DB_NAME@

Представляет имя базы данных IBM Business Monitor, например MONITOR

@SCHEMA@

Представляет имя схемы IBM Business Monitor, например MONITOR

@DB_USER@

Пользователь базы данных среды выполнения IBM Business Monitor

@DB_PASSWORD@

Пароль пользователя базы данных среды выполнения IBM Business Monitor. Можно вручную создать пользователя базы данных и пароль перед запуском сценария или настроить сценарий для их создания в автоматическом режиме. Для создания пользователя базы данных и пароля в сценарии необходимо указать @DB_PASSWORD@.

- Для Oracle измените следующие переменные:

@SCHEMA@

Представляет имя пользователя базы данных, который владеет таблицами базы данных IBM Business Monitor

@DB_PASSWORD@

Пароль пользователя базы данных, заданного в \$\$SCHEMA\$

@TSDIR@

Каталог табличного пространства

Если в спецификации файла данных табличного пространства @TSDIR@ пропущено, то файл данных будет создан в каталоге администратора базы данных. Если в @TSDIR@ указано полное имя, то этот каталог должен существовать до вызова сценария.

@DB_USER@

Пользователь базы данных среды выполнения IBM Business Monitor

Табличные пространства создаются в файле createDatabase.sql. В случае замены имен табличных пространств по умолчанию на пользовательские имена при развертывании моделей необходимо экспортировать сценарии схем моделей и изменить их так, чтобы они указывали на выбранные имена табличных пространств.

Примечание: Только для базы данных MONITOR. При настройке дополнительного экземпляра монитора в отдельной установке Oracle также необходимо заменить строку DEFAULTTS в файле createDatabase.sql с уникальным идентификатором для этого дополнительного экземпляра монитора на следующие четыре строки:

```
CREATE TABLESPACE MONDSTS
  DATAFILE 'DEFAULTTS_MONDSTS.dbf' SIZE 500M AUTOEXTEND ON
  NEXT 100M MAXSIZE UNLIMITED LOGGING;

CREATE TABLESPACE MONDMSTS
  DATAFILE 'DEFAULTTS_MONDMSTS.dbf' SIZE 100M AUTOEXTEND ON
  NEXT 20M MAXSIZE UNLIMITED LOGGING;

CREATE TABLESPACE MONIDXTS
  DATAFILE 'DEFAULTTS_MONIDXTS.dbf' SIZE 250M AUTOEXTEND ON
  NEXT 50M MAXSIZE UNLIMITED LOGGING;

CREATE TABLESPACE MONLOBTS
  DATAFILE 'DEFAULTTS_MONLOBTS.dbf' SIZE 200M AUTOEXTEND ON
  NEXT 40M MAXSIZE UNLIMITED LOGGING; ;
```

Например, если уникальным идентификатором дополнительного экземпляра монитора был MONDEV1_MONDSTS, то измененные ссылки будут выглядеть как:

```
CREATE TABLESPACE MONDSTS
  DATAFILE 'MONDEV1_MONDSTS.dbf' SIZE 500M AUTOEXTEND ON
  NEXT 100M MAXSIZE UNLIMITED LOGGING;

CREATE TABLESPACE MONDMSTS
  DATAFILE 'MONDEV1_MONDMSTS.dbf' SIZE 100M AUTOEXTEND ON
  NEXT 20M MAXSIZE UNLIMITED LOGGING;

CREATE TABLESPACE MONIDXTS
  DATAFILE 'MONDEV1_MONIDXTS.dbf' SIZE 250M AUTOEXTEND ON
  NEXT 50M MAXSIZE UNLIMITED LOGGING;

CREATE TABLESPACE MONLOBTS
  DATAFILE 'MONDEV1_MONLOBTS.dbf' SIZE 200M AUTOEXTEND ON NEXT 40M MAXSIZE UNLIMITED LOGGING;
```

Выполните эту процедуру для каждого дополнительного экземпляра монитора.

Примечание: В IBM Business Monitor версии 6.2 используются иные табличные пространства, нежели в предыдущих версиях. Это означает, что при работе Oracle и развертывании модели 6.1 в IBM Business Monitor 7.5 необходимо выбрать одну из следующих опций:

- Выполнить операторы табличного пространства 6.1 во время установки базы данных 7.5.
- В процессе развертывания модели монитора экспортируйте сценарий базы данных моделей и вручную укажите табличные пространства 7.0. Если выбрана вторая опция, это необходимо делать каждый раз при развертывании модели 6.1 на сервере 7.0.

Простым способом избежать этой неполадки является миграция из 6.1 в 7.5 с развернутыми существующими моделями и затем создание новых моделей в

6.2 или 7.5 IBM Business Monitor Development Toolkit.

Преобразование имен табличных пространств показано в следующей таблице.

Таблица 3. Преобразование имен табличных пространств из предыдущих версий IBM Business Monitor

Текущее табличное пространство	Табличное пространство 6.1.x
MONDSTS	INSTANCE
MONDMSTS	DMSTS
MONIDXTS	INDEXTS
MONLOBTS	LOBTS

3. Сохранить и закрыть файл.

Установка баз данных вручную

С помощью файлов сценариев баз данных можно установить базу данных IBM Business Monitor и базу данных хранилища материалов IBM Cognos Business Intelligence вручную на том же сервере, где расположен IBM Business Monitor, или в качестве удаленных баз данных на другом сервере. Перед выполнением сценариев необходимо настроить переменные среды в сценариях базы данных или вручную, или с помощью инструмента проектирования базы данных.

Перед тем, как приступить к выполнению этой задачи, обратитесь к разделу "Рекомендации по использованию базы данных" и ознакомьтесь с предварительными требованиями базы данных. Например, в случае применения DB2 для z/OS рекомендуется создать выделенную группу памяти (STOGROUP) для IBM Business Monitor. Группу памяти следует создать перед созданием базы данных.

На сервере, на котором устанавливается ПО базы данных, выполните следующие действия:

1. Войдите на сервер базы данных как пользователь с правами доступа на создание табличных пространств и объектов базы данных.
2. Найдите сценарии DDL.
 - Если вы применяете сценарии, доставленные во время установки IBM Business Monitor, то учтите, что эти сценарии находятся в каталогах `app_server_root/dbscripts/Monitor` и `app_server_root/dbscripts/Cognos`.
 - Если вы использовали DbDesignGenerator для генерирования сценариев с вашими подставленными переменными значениями, то учтите, что эти сценарии находятся в выходном каталоге, который вы выбрали во время выполнения утилиты (по умолчанию - `app_server_root/util/dbUtils`).
 - Если вы генерировали сценарии с вашими подставленными переменными значениями во время создания профайла, то учтите, что эти сценарии находятся в выходном каталоге, который вы выбрали во время создания профайла (по умолчанию - `app_server_root/profiles/<профайл>/dbscripts/Monitor`).
3. Из интерфейса командной строки запустите сценарий `createDatabase` дважды, один раз для базы данных MONITOR, и один раз для базы данных COGNOSCS. Для этого выполните следующую команду для применяемой базы данных. Сценарий `createDatabase` создает базу данных и все необходимые таблицы для IBM Business Monitor.
 - **DB2:** `db2 -tf createDatabase.sql`
 - **DB2 for z/OS:** `db2 -tf createDatabase.sql`. Сценарий базы данных можно запустить с помощью утилиты SPUFI или DSNTEP2.

- **Microsoft SQL Server:** `sqlcmd -U dbadmin -P пароль -e -i createDatabase.sql`, где:
dbadmin - это пользователь SQL Server, обладающий правами доступа администратора
4. Для базы данных MONITOR запустите сценарий createTables с помощью одной из следующих команд (Не обязательно создавать таблицы для базы данных IBM Cognos BI):
- **DB2:**
`db2 connect to MONITOR`
`db2 -tf createTables.sql`
`db2 connect reset`
- Примечание:** Во время запуска файла DDL может появиться следующее предупреждающее сообщение: SQL0347W The recursive common table expression "MON023.WBITIME" may contain an infinite loop. SQLSTATE=01605. Это сообщение можно игнорировать без каких-либо последствий.
- **Oracle:** `sqlplus пользователь/пароль@имя-базы-данных @createTables.sql`
 - **Microsoft SQL Server:** `sqlcmd -U пользователь -P пароль -e -i createTables.sql`
5. Запустить WebSphere Application Server.

Создание таблиц службы сообщений вручную

Если таблицы шины интеграции служб (SI) для службы сообщений IBM Business Monitor не были созданы автоматически во время создания автономного профайла или в процессе использования мастера настройки среды развертывания или мастера настройки, то их необходимо создать вручную. Кроме того, необходимо вручную создать таблицы, если применяется хранилище данных службы сообщений DB2 for z/OS.

Также можно создать таблицу службы сообщений инфраструктуры обработки событий общего формата (CEI). Сценарии базы данных для CEI создаются вместе со средой развертывания. Запустите сценарии вручную для завершения настройки, если требуется включить хранилище событий CEI (не рекомендуется для рабочих сред).

С помощью инструмента проектирования базы данных (DbDesignGenerator) создайте сценарии для таблиц шины SI в версии 7.5.

Можно воспользоваться и sibDDLGenerator как альтернативой. Например, командой для создания сценариев DDL SIB для DB2 для z/OS является sibDDLGenerator `-system db2 -version 8.1 -platform zos`.

Документация по sibDDLGenerator содержит список поддерживаемых версий DB2. В документации указаны не все версии DB2, поддерживаемые IBM Business Monitor; тем не менее, можно указать версию 8.1, как показано в примере выше, и созданный файл DDL будет совместим со всеми поддерживаемыми версиями.

Поскольку IBM Business Monitor может иметь службу сообщений CEI, а также службы сообщений IBM Business Monitor, каждая из которых была создана с одинаковыми именами бизнес-пространств и таблиц, необходимо использовать две разные базы данных или два разных имени схем.

Глава 6. Создание и дополнение профайлов

После установки IBM Business Monitor создайте по крайней мере один профайл для подготовки вашей среды выполнения. Создать и дополнить профайлы можно с помощью Инструмента управления профайлами или команды **manageprofiles**.

В случае применения 64-разрядной версии IBM Business Monitor следует выполнить команду **manageprofiles**. При использовании z/OS невозможно выполнить ни одну из команд или Инструмент управления профайлами. См. раздел "Создание обычных конфигураций для IBM Business Monitor для z/OS".

Существует три типа профайлов: профайл автономного сервера, профайл администратора развертывания (профайл управления с помощью сервера администратора развертывания) и пользовательский профайл (управляемый узел). Каждый профайл определяет отдельную среду выполнения с отдельными файлами (команды, файлы конфигурации и файлы протокола).

Создание и расширение профайлов с помощью Инструмента управления профайлами

Инструмент управления профайлами позволяет создать и расширить профайлы для управления средой выполнения.

Ограничение: В 64-разрядной версии IBM Business Monitor необходимо использовать команду **manageprofiles**. Пользовательский интерфейс Profile Management Tool недоступен для 64-разрядных версий. При использовании z/OS обратитесь к разделу "Создание обычных конфигураций для IBM Business Monitor для z/OS".

Для среды с одним сервером создайте автономный профайл.

Для среды сетевого развертывания выполните следующие действия:

1. Создайте профайл администратора развертывания перед созданием других профайлов. Если профайл администратора развертывания создан перед установкой IBM Business Monitor (например, для WebSphere Application Server или Process Server) и его планируется использовать для управления узлами IBM Business Monitor, дополните профайл с помощью шаблона, предоставленного IBM Business Monitor.
2. Для каждого узла, который планируется добавить в кластер сервера, необходимо создать индивидуальный профайл. В качестве альтернативы, можно дополнить существующий пользовательский профайл для каждого узла, который вы планируете добавить.

Примечание: Если на сервере базы данных установлено несколько версий DB2 или несколько экземпляров DB2, то для создания профайла используется версия или экземпляр DB2 по умолчанию. Для управления версией или экземпляром DB2 служит процедура "Установка баз данных вручную", позволяющая администратору базы данных обеспечить использование правильной версии или экземпляра.

В случае применения базы данных Oracle поддержка JDBC предоставляется драйверами JDBC Oracle для JVM 1.6. Файл драйвера JDBC `ojdbc6.jar` является поддерживаемым Oracle драйвером JDBC для использования в WebSphere Application

Server версии 7. Файл `ojdbc6.jar` можно использовать для Oracle 10g и Oracle 11g. Сведения о минимальных обязательных параметрах для Oracle приведены в ссылке на связанную информацию.

По умолчанию инструмент управления профайлами указывает на файл `ojdbc6.jar`, расположенный в каталоге `app_server_root\jdbcdrivers\Oracle`. Кроме того, можно загрузить другой файл драйвера JDBC Oracle `ojdbc6.jar` и указать его при запуске инструмента управления профайлами или команды **manageprofiles**.

В случае применения базы данных SQL Server драйверы JDBC SQL Server для JVM 1.6 обеспечивают поддержку JDBC. IBM Business Monitor использует файл `sqljdbc4.jar` драйвера Microsoft JDBC 2.0. По умолчанию инструмент управления профайлами указывает на файл `sqljdbc4.jar`, расположенный в каталоге `app_server_root\jdbcdrivers\SQLServer`. Кроме того, можно загрузить другой файл драйвера JDBC Microsoft `sqljdbc4.jar` и указать его при запуске инструмента управления профайлами или команды **manageprofiles**. Сведения о минимальных обязательных параметрах для SQL Server приведены в ссылке на связанную информацию.


Создание автономных профайлов

Если во время установки в среде с одним сервером не был создан профайл IBM Business Monitor, то его необходимо установить. Профайл будет создан в каталоге профайлов WebSphere Application Server.

Перед выполнением этой задачи необходимо выполнить следующие задачи:

- Проверить выполнение предварительных требований для аппаратного обеспечения и программного обеспечения
- Установить IBM Business Monitor
- Выполнить вход в систему от имени пользователя с правами на чтение, запись и выполнение программ для каталога профайлов WebSphere Application Server

Выполнить следующие действия для создания профайла одиночного сервера приложений с помощью инструмента управления профайлами:

1. Открыть инструмент управления профайлами с помощью одного из следующих способов:
 - В консоли Первые шаги IBM Business Monitor выберите **Инструмент управления профайлами**.
 -  Выберите **Пуск > Программы > IBM > Business Monitor 7.5 > Инструмент управления профайлами**.
 -  Запустите файл `pmt.bat`, расположенный в следующем каталоге: `app_server_root\bin\ProfileManagement`
 -   Перейдите в каталог `app_server_root/bin/ProfileManagement` и введите `./pmt.sh` в окне терминала.
2. В панели Вас приветствует инструмент управления профайлами проверьте информацию и нажмите **Запустить инструмент управления профайлами**.
3. На панели Профайлы нажмите **Создать** для создания нового профайла.
4. В панели Выбор среды разверните IBM Business Monitor, выберите **Автономный сервер монитора** и нажмите **Далее**.


Ограничение: Если опция IBM Business Monitor не видна, то это может означать, что вы работаете с 64-разрядной версией. Если используется 64-разрядная версия IBM Business Monitor, нельзя использовать Инструмент управления профайлами. Необходимо использовать команду `manageprofiles`.

5. На панели Опции создания профайла выберите тип установки и нажмите кнопку **Далее**.
 - **Создание обычного профайла** (по умолчанию): Создает профайл IBM Business Monitor, который использует параметры конфигурации по умолчанию. Средство Profile Management назначает уникальные имена профайлу, узлу и ячейке. Средство также устанавливает административную консоль, устанавливает приложения по умолчанию и назначает уникальные значения порта. Можно включить административную защиту в процессе настройки. Для соответствующих операционной системы и прав доступа пользователя этот инструмент может создать системную службу для выполнения IBM Business Monitor.
 - **Создание расширенного профайла**: Создание профайла IBM Business Monitor, использующего параметры конфигурации по умолчанию или выбор пользовательских компонентов IBM Business Monitor. Можно назначить свои собственные значения порта. По выбору можно развернуть административную консоль, развернуть примеры приложений и создать определение Web-сервера. В зависимости от операционной системы и прав доступа пользователя можно выбрать выполнение IBM Business Monitor как системной службы. Можно определить конфигурацию модели IBM Business Monitor. Можно указать файл эскиза базы данных или назначить свои собственные значения для конфигурации базы данных IBM Business Monitor. . Можно выбрать конфигурацию IBM Cognos BI для многомерного анализа данных.
6. Если выбран вариант **Создание обычного профайла**, то перейдите к шагу Шаг 11: Панель Административная защита.
7. Дополнительно: На панели Необязательные приложения выберите **Установить административную консоль** и **Установить стандартные приложения**. Приложением по умолчанию является WebSphere Application Server. Выберите **Далее**.
8. Дополнительно: На панели Расположение и имя профайла примите значения по умолчанию для расположения и имени или укажите имя профайла и путь к каталогу, содержащему файлы среды выполнения, такие как команды, файлы конфигурации и файлы протокола. Именем профайла по умолчанию является WBMon01. В системе Windows профайл, как правило, расположен в следующем каталоге: C:\IBM\WebSphere\AppServer\profiles\WBMon01.
9. Дополнительно: Укажите уровень настройки производительности, подходящий для создаваемого профайла. Этот параметр относится к WebSphere Application Server. Дополнительная информация приведена в разделе Тонкая настройка сервера приложений справочной системы WebSphere Application Server Information Center.
10. Дополнительно: На панели Имена узла и хоста введите новые значения или примите значения, предложенные по умолчанию, и нажмите кнопку **Далее**.
 - Имя узла используется для администрирования. Если узел является интегрированным, то его имя должно быть уникальным в ячейке.
 - Имя сервера - это логическое имя сервера IBM Business Monitor.
 - Имя хоста - это имя DNS (краткое или полное) или IP-адрес этого компьютера.
 - Имя ячейки - это логическое имя группы узлов, управляемых данным диспетчером развертывания.
11. В панели Административная защита выберите одну из следующих опций и нажмите **Далее**.
 - Для включения защиты выберите переключатель **Включить защиту администрирования** и введите имя пользователя с паролем.

- Для отключения защиты выключите переключатель **Включить защиту администрирования**.

Информация о том, следует ли включать защиту, приведена в разделе Административная защита справочной системы WebSphere Application Server Information Center.

Если выбрана опция **Создание обычного профайла**, перейдите к Действие 21: Панель Конфигурация базы данных.

12. Дополнительно: в панели Сертификат защиты (часть 1) укажите, нужно ли создавать личный сертификат по умолчанию и корневой сертификат подписания или же их нужно импортировать из хранилищ ключей. Для того чтобы создать новые сертификаты, нажмите **Далее** для перехода на страницу проверки. Для того чтобы импортировать существующие сертификаты из хранилища ключей, найдите их и нажмите **Далее** для перехода на страницу проверки.
13. Дополнительно: в панели Сертификат защиты (часть 2) измените информацию о сертификате для создания новых сертификатов в процессе создания профайла. При импорте существующих сертификатов из хранилищ ключей проверяйте наличие в выбранных сертификатах подходящей информации. Если выбранные сертификаты не содержат ее, нажмите **Назад** для импорта других сертификатов. Необходимо изменить пароль хранилища ключей по умолчанию, чтобы обеспечить защиту файлов хранилища ключей и сертификатов SSL. Более подробная информация о защите соединения между сервером и клиентом находится на странице Защита средств связи в WebSphere Application Server information center.
14. Дополнительно: На панели Назначение портов проверьте порты, которые будут назначены при создании профайлов. Вам может потребоваться отслеживать значения этих портов. Примите значения или укажите другие порты и нажмите **Далее**.
15.  Дополнительно: В системах Windows отображается панель Определение службы Windows. По умолчанию включена опция **Запускать процесс сервера приложений как службу Windows**, и она настроена использовать информацию локальной учетной записи для входа в систему. Примите стандартные параметры Windows или отключите эту опцию и нажмите **Далее**. Для изменения идентификационных данных службы Windows выберите переключатель **Входить в систему от имени указанного пользователя** и введите соответствующие идентификационные данные.

По умолчанию для службы Windows в поле **Тип запуска** указано значение **Автоматически**. Можно изменить **Тип запуска** на **Вручную** или **Выключен** с помощью выпадающего списка.

Поскольку службы являются глобальными настройками операционных систем Windows, любой профайл может запустить службу, и в результате вы можете перепутать способ запуска профайла, например, с командой “startServer”. Для избежания конфликтов служебных запросов между разными профайлами отключите опцию **Запустить процесс сервера приложений как службу Windows**.
16. Дополнительно: На панели Задание определения Web-сервера выберите одну из следующих опций:
 - Если требуется создать определение Web-сервера включите опцию **Включить определение Web-сервера**. Примите последующую предлагаемую информацию Web-сервера или внесите необходимые изменения.

Тип Web-сервера

Возможны следующие типы: IBM HTTP Server, Microsoft Internet Information Services, Sun Java System, Lotus Domino Web Server и Apache Web Server.

Операционная система Web-сервера

Допустимые варианты: Windows, AIX, HP, Solaris и z/OS.

Имя Web-сервера

Введите имя Web-сервера. Имя по умолчанию - "webserver1".

Имя хоста или IP-адрес Web-сервера

Введите имя хоста или IP-адрес Web-сервера. По умолчанию показано имя local host.

Порт Web-сервера (по умолчанию 80)

Введите номер порта или примите значение по умолчанию (80).

- Если создавать определение Web-сервера не требуется, выключите переключатель **Создать определение Web-сервера**.

Определения Web-сервера определяют внешний Web-сервер как WebSphere Application Server, позволяя управлять файлами конфигурации модулей Web-сервера, а также самим Web-сервером. Web-сервер можно установить позже из административной консоли.

17. Дополнительно: На панели Определения Web-сервера (Часть 2) введите путь каталога установки Web-сервера и его модулей.

18. Дополнительно: На панели Модели монитора IBM Business Process Manager выберите **Развернуть модель монитора глобальных процессов IBM Business Monitor**, чтобы установить и настроить приложение модели монитора глобальных процессов. Эта модель позволяет отслеживать процессы BPEL или BPMN, выполняющиеся в IBM Business Process Manager, без генерации и развертывания моделей монитора.

Выберите **Развернуть модель монитора неавтоматизированных задач (требуется IBM Business Process Manager Advanced)** для установки и настройки приложения неавтоматизированных задач. Приложение неавтоматизированных задач требуется для просмотра неавтоматизированных задач на сводной панели с помощью виджета неавтоматизированная задача. Для установки этих приложений необходимо указать имя хоста и номер порта RMI для существующего IBM Business Process Manager. (Порт по умолчанию - 2809.) Перед продолжением создания или расширения профайла необходимо убедиться в существовании базы данных MONITOR или создать ее с помощью Инструмента управления профайлами.

Если эти приложения не были установлены во время установки, можно сделать это позже, следуя инструкциям в разделах "Настройка мониторинга неавтоматизированных задач" и "Настройка модели монитора глобальных процессов".

19. Дополнительно: в панели конфигурации Business Space выберите опцию

Настроить Business Space для развертывания среды Business Space и регистрации виджетов IBM Business Monitor в этой среде.

20. Необязательно: Дополнительно: Настройте базы данных с помощью файла эскиза.

- а. Выберите **Настройка базы данных с помощью файла структуры базы данных** для применения файла структуры вместо указания параметров базы данных на следующих панелях.
- б. Нажмите **Обзор**.
- в. Укажите полное имя пути к файлу эскиза.
- г. Нажмите кнопку **Далее**.
- д. Выберите **Отложить выполнение сценариев базы данных (обязательно выберите при использовании удаленной базы данных)**, для того чтобы запретить автоматическое создание и настройку базы данных или создание таблиц в

существующей базе данных в ходе создания профайла. Если этот переключатель не выбран, то будет создана локальная база данных. Если вы выберете эту опцию, то вы или администратор базы данных должны вручную запустить сценарии из каталога, указанного в поле выходного каталога сценария базы данных на этой странице. Если создаются сценарии для Oracle, то перед их запуском необходимо заменить @DB_PASSWORD@ на пароль для имени схемы.

Примечание: Если на сервере базы данных установлено несколько версий DB2 или несколько экземпляров DB2, то для создания профайла используется версия или экземпляр DB2 по умолчанию. Для управления версией или экземпляром DB2 служит процедура "Установка баз данных вручную", позволяющая администратору базы данных обеспечить использование правильной версии или экземпляра.

Если выбирается указание файла эскиза, то панели настройки базы данных в Инструменте управления профайлами пропускаются. Вместо них расположение файла эскиза помещается в командную строку для выполнения настройки базы данных. Дополнительная информация об использовании файла эскиза для настройки базы данных приведена в разделе "Создание или настройка сценариев базы данных с помощью инструмента проектирования баз данных".

21. На панели Конфигурация базы данных проверьте сведения о конфигурации базы данных MONITOR.
 - a. В поле **База данных** выберите одно из следующих значений.
 - b. Для определения целевого каталога для сформированных сценариев разрешите опцию **Переписать целевой каталог для сформированных сценариев** и введите путь в поле **Целевой каталог для сценариев базы данных**. (Каталог по умолчанию - каталог-monitor\profiles\WBMon01\dbscripts\Monitor\платформа\.)
 - c. Выберите **Отложить выполнение сценариев базы данных (обязательно выберите при использовании удаленной базы данных)**, для того чтобы запретить автоматическое создание и настройку базы данных или создание таблиц в существующей базе данных в ходе создания профайла. Если этот переключатель не выбран, то будет создана локальная база данных. Если вы выберете эту опцию, то вы или администратор базы данных должны вручную запустить сценарии из каталога, указанного в поле выходного каталога сценария базы данных на этой странице. Если создаются сценарии для Oracle, то перед их запуском необходимо заменить @DB_PASSWORD@ на пароль для имени схемы.

Примечание: Если на сервере базы данных установлено несколько версий DB2 или несколько экземпляров DB2, то для создания профайла используется версия или экземпляр DB2 по умолчанию. Для управления версией или экземпляром DB2 служит процедура "Установка баз данных вручную", позволяющая администратору базы данных обеспечить использование правильной версии или экземпляра.

- d. В поле **Имя базы данных** введите имя базы данных или примите имя по умолчанию (MONITOR).
 - e. В поле **Имя схемы** введите имя схемы или примите имя по умолчанию (MONITOR). При использовании DB2 на z/OS имя схемы базы данных IBM Business Monitor должно отличаться от имени схемы общей базы данных Process Server во избежание конфликтов между объектами баз данных.
 - f. Нажмите кнопку **Далее**.
22. На панели конфигурации базы данных (часть 2) выполните следующие действия:

- a. Введите *имя_пользователя* в поле **Имя пользователя** для идентификации базой данных. ИД пользователя, обладающего правами на чтение и запись к таблицам MONITOR.

Примечание: В случае применения базы данных Oracle это поле недоступно для изменения.

- b. Введите *пароль* в поле **Пароль** для идентификации базой данных. Пароль пользователя БД.
- c. Введите *пароль* в поле **Подтверждение пароля**. Этот пароль должен совпадать с паролем в поле **Пароль**.
- d. Укажите или выберите путь к классам драйвера JDBC. Драйверы JDBC для DB2, Oracle и SQL Server расположены в каталоге `каталог-монитор/jdbcdrivers`. Переменная `classpath` для драйвера JDBC установлена для использования файлов определенного продукта на основании типа базы данных, выбранного на панели Конфигурация базы данных. В качестве альтернативы можно нажать кнопку **Обзор** для ввода пути к классам драйвера JDBC.
- База данных DB2: Следующий каталог создается по умолчанию:
`каталог-монитор/jdbcdrivers/DB2`
 - База данных Oracle: Следующий каталог создается по умолчанию:
`каталог-монитор/jdbcdrivers/Oracle`

Файл драйвера JDBC `ojdbc6.jar` является поддерживаемым Oracle драйвером JDBC для использования в WebSphere Application Server версии 7. Файл `ojdbc6.jar` можно использовать для Oracle 10g и Oracle 11g. Сведения о минимальных обязательных параметрах для Oracle приведены в ссылке на связанную информацию.

- База данных SQL Server: Следующий каталог создается по умолчанию:
`каталог-монитор/jdbcdrivers/SQLServer`

Файл драйвера JDBC `sqljdbc4.jar` является драйвером JDBC Microsoft SQL Server 2.0. Сведения о минимальных обязательных параметрах для SQL Server приведены в ссылке на связанную информацию.

- e. Выберите одну из следующих опций для типа драйвера JDBC:
- Для базы данных Oracle:
 - **OCI:** Драйвер OCI требует установки локального клиента Oracle.
 - **Простой:** Простой драйвер использует Java для связи с базой данных и не требует клиента в локальной системе.
 - Профайлы IBM Business Monitor для баз данных DB2 в операционных системах, отличных от z/OS, создаются с драйверами типа 4, а в системах z/OS - с драйверами типа 2. Тип драйвера можно изменить с помощью административной консоли после создания профайла в конфигурации источника данных. Драйвер типа 2 - это драйвер встроенного API, и он требует установки ПО базы данных или клиента базы данных на локальном компьютере. Драйвер типа 4 - это реализация Java. Обычно она обеспечивает наилучшую производительность. Для базы данных MONITOR в локальной системе не требуется программное обеспечение или клиенты базы данных.
- f. Введите *имя-хоста* в **Имя хоста или IP-адрес сервера базы данных**. Значение по умолчанию - `localhost` или полное имя локального хоста; его следует использовать для установки на одном сервере. Если база данных находится на удаленном сервере, необходимо ввести полное имя или IP-адрес.

Примечание: Кроме случая установки на одиночном сервере, *ее* используйте переменную localhost, поскольку члены кластера зависят от действующего имени хоста или IP-адреса.

- g. Введите *номер-порта* в поле **Порт получателя или служебный порт ТСП/IP базы данных**. Это - номер порта, назначенный для службы ТСП/IP, или порт получения базы данных.
 - h. Необязательно: При использовании DB2 в z/OS введите *имя-подсистемы* в поле **Имя подсистемы**. Это расположение базы данных DB2 for z/OS. В имени недопустимы пробелы.
 - i. Если применяется Oracle или SQL Server, то для создания базы данных в автоматическом режиме введите следующую информацию:
 - В поле **Имя администратора базы данных** введите *имя_пользователя_системы*. Это значение представляет имя администратора базы данных для Oracle или SQL Server. Этому пользователю должны быть предоставлены права доступа для создания и удаления баз данных и пользователей.
 - В поле **Пароль** введите *пароль*. Это пароль системного администратора, указанного в предыдущем поле.
 - Введите *пароль* в поле **Подтверждение пароля**.
 - j. Нажмите кнопку **Далее**. Если база данных MONITOR еще не создана, будет показано предупреждающее сообщение. Нажмите кнопку **Да** для продолжения. Базу данных можно создать позднее.
23. На панели Конфигурация IBM Cognos BI настройте IBM Cognos BI для многомерного анализа данных из своих сводных панелей.

- Для развертывания IBM Cognos BI нажмите **Создать конфигурацию нового сервера Cognos** и укажите имя базы данных для хранилища материалов IBM Cognos BI. Имя профайла по умолчанию — COGNOSCS. В случае применения Oracle в качестве имени базы данных должно быть указано глобальное имя базы данных Oracle (его можно просмотреть с помощью следующего запроса: SELECT * FROM GLOBAL_NAME). В Microsoft SQL Server имя базы данных должно отличаться от имени должны быть MONITOR.

Введите имя пользователя базы данных и пароль. Если для хранилища материалов используется то же имя пользователя, что и для базы данных MONITOR, необходимо применять такой же пароль. Поскольку пользователь базы данных, указанный для доступа к базе данных хранилища материалов, должен обладать правами доступа для создания таблиц в базе данных, рекомендуется создать нового пользователя базы данных, предназначенного только для работы с базой данных хранилища материалов.




Также необходимо указать имя администратора и пароль для службы IBM Cognos BI.

Примечание: Имя пользователя и пароль для базы данных хранилища материалов IBM Cognos BI находятся в Cognos_JDBC_Alias, где хранятся все идентификационные данные базы данных. При каждом запуске сервера IBM Business Monitor IBM Cognos BI текущие значения передаются в конфигурацию IBM Cognos BI для обеспечения доступа IBM Cognos BI к хранилищу материалов. Такая интеграция не позволяет изменять имя пользователя и пароль хранилища материалов с помощью приложения Настройка IBM Cognos BI.

- Для использования существующей версии IBM Cognos BI нажмите **Использовать существующую конфигурацию сервера Cognos** и укажите URI внешнего диспетчера сервера IBM Cognos BI. Этот URI можно найти в клиенте конфигурации IBM Cognos BI в меню **Локальная конфигурация > Среда >**

Параметры диспетчера (например, `http://хост:порт/p2pd/servlet/dispatch/ext`). Если административная защита включена на сервере IBM Cognos BI, необходимо указать имя и пароль администратора IBM Cognos BI.

Сервер IBM Cognos BI не должен быть доступен для установки этого значения. Сервер требуется при установке моделей монитора, если вы хотите выполнить многомерный анализ для этих моделей.

24. На панели Краткая информация о создании профайла проверьте информацию. При необходимости внесения изменений нажмите кнопку **Назад** и внесите изменения.
25. Для создания профайла выберите **Создать**.
26. На панели Завершение создания профайла проверьте информацию.
27. Необязательно: Откройте консоль Первые шаги.
 -  Выберите опцию **Запустить Первые шаги в IBM Business Monitor**.
 -   Перейдите в каталог `profile_root/firststeps.wbm` и введите команду `firststeps.sh`.
28. Нажмите кнопку **Готово** для выхода из Profile Management Tool.

Во время создания профайла значения портов были заданы для всех необходимых портов. При изменении портов после установки следует перенастроить значения портов для правильной работы IBM Business Monitor.




Создание профайлов администратора развертывания

Профайл администратора развертывания должен существовать для управления всеми интегрированными серверами в кластере. Для настройки среды сетевого развертывания сначала необходимо создать этот профайл.

Перед выполнением этой задачи необходимо выполнить следующие задачи:

- Проверить выполнение предварительных требований для аппаратного обеспечения и программного обеспечения
- Установить IBM Business Monitor
- Выполнить вход в систему от имени пользователя с правами на чтение, запись и выполнение программ для каталога профайлов WebSphere Application Server
- Установить базу данных

Для того, чтобы создать профайл администратора развертывания с помощью Инструмента управления профайлами, выполните следующие действия:

1. Открыть инструмент управления профайлами с помощью одного из следующих способов:
 - В консоли Первые шаги IBM Business Monitor выберите **Инструмент управления профайлами**.
 -  Выберите **Пуск > Программы > IBM > Business Monitor 7.5 > Инструмент управления профайлами**.
 -  Запустите файл `pmt.bat`, расположенный в следующем каталоге: `app_server_root\bin\ProfileManagement`
 -   Перейдите в каталог `app_server_root/bin/ProfileManagement` и введите `./pmt.sh` в окне терминала.
2. В панели Вас приветствует инструмент управления профайлами проверьте информацию и нажмите **Запустить инструмент управления профайлами**.
3. На панели Профайлы нажмите **Создать** для создания нового профайла.

4. На панели Выбор среды разверните IBM Business Monitor, выберите **Администратор развертывания сервера монитора** и нажмите **Далее**.

Ограничение: Если опция IBM Business Monitor не видна, то это может означать, что вы работаете с 64-разрядной версией. Если используется 64-разрядная версия IBM Business Monitor, нельзя использовать Инструмент управления профайлами. Необходимо использовать команду managerprofiles.


5. На панели Опции создания профайла выберите тип установки и нажмите кнопку **Далее**.

- **Создание обычного профайла** (по умолчанию): Создает профайл администратора развертывания, который использует параметры конфигурации по умолчанию. Средство Profile Management назначает уникальные имена профайлу, узлу, хосту и ячейке. Средство также устанавливает административную консоль и назначает уникальные значения порта. Можно включить административную защиту в процессе настройки. В зависимости от операционной системы и ваших прав доступа инструмент может создать системную службу для запуска администратора развертывания. Можно указать свои собственные значения для конфигурации базы данных IBM Business Monitor.
- **Создание расширенного профайла:** Создает администратора развертывания, который использует параметры конфигурации по умолчанию. Можно указать значения для хоста и ячейки, назначить свои собственные значения портов и выбрать, нужно ли разворачивать административную консоль. В зависимости от операционной системы и ваших прав доступа вам может быть предоставлена опция запуска администратора развертывания в качестве системной службы. Можно указать файл эскиза базы данных или назначить свои собственные значения для конфигурации базы данных IBM Business Monitor.

6. Если выбрана опция **Создание обычного профайла**, перейдите к Действие 10: Панель Административная защита.
7. Дополнительно. На панели Необязательные приложения выберите **Установить административную консоль** и нажмите кнопку **Далее**.
8. Дополнительно: На панели Расположение и имя профайла примите значения по умолчанию для расположения и имени или укажите имя профайла и путь к каталогу, содержащему файлы среды выполнения, такие как команды, файлы конфигурации и файлы протокола. Именем профайла по умолчанию является Dmgr01. В операционной системе Windows, как правило, применяется каталог профайла C:\IBM\WebSphere\AppServer\profiles\Dmgr01.
9. Дополнительно: На панели Имена узла, хоста и ячейки введите новые значения или примите значения, предложенные по умолчанию, и нажмите кнопку **Далее**.
 - Имя узла используется для администрирования. Если узел является интегрированным, то его имя должно быть уникальным в ячейке.
 - Имя хоста - это имя DNS (краткое или полное) или IP-адрес этого компьютера.
 - Имя ячейки - это логическое имя группы узлов, управляемых данным диспетчером развертывания.
10. На панели административной защиты выберите одну из следующих опций и нажмите кнопку **Далее**.
 - Для включения защиты выберите переключатель **Включить защиту администрирования** и введите имя пользователя с паролем.
 - Для отключения защиты выключите переключатель **Включить защиту администрирования**.

Информация о том, следует ли включать защиту, приведена в разделе Административная защита справочной системы WebSphere Application Server Information Center.

Если выбрана опция **Создание обычного профайла**, перейдите к Действие 16: Панель Конфигурация базы данных.

11. Дополнительно: в панели Сертификат защиты (часть 1) укажите, нужно ли создавать личный сертификат по умолчанию и корневой сертификат подписания или же их нужно импортировать из хранилищ ключей. Для того чтобы создать новые сертификаты, нажмите **Далее** для перехода на страницу проверки. Для того чтобы импортировать существующие сертификаты из хранилища ключей, найдите их и нажмите **Далее** для перехода на страницу проверки.
12. Дополнительно: в панели Сертификат защиты (часть 2) измените информацию о сертификате для создания новых сертификатов в процессе создания профайла. При импорте существующих сертификатов из хранилищ ключей проверяйте наличие в выбранных сертификатах подходящей информации. Если выбранные сертификаты не содержат ее, нажмите **Назад** для импорта других сертификатов. Необходимо изменить пароль хранилища ключей по умолчанию, чтобы обеспечить защиту файлов хранилища ключей и сертификатов SSL. Более подробная информация о защите соединения между сервером и клиентом находится на странице Защита средств связи в WebSphere Application Server information center.
13. Дополнительно: На панели Назначение портов проверьте порты, которые будут назначены при создании профайлов. Вам может потребоваться отслеживать значения этих портов. Примите значения или укажите другие порты и нажмите **Далее**.
14.  Дополнительно: В системах Windows отображается панель Определение службы Windows. По умолчанию включена опция **Запускать процесс сервера приложений как службу Windows**, и она настроена использовать информацию локальной учетной записи для входа в систему. Примите стандартные параметры Windows или отключите эту опцию и нажмите **Далее**. Для изменения идентификационных данных службы Windows выберите переключатель **Входить в систему от имени указанного пользователя** и введите соответствующие идентификационные данные.

По умолчанию для службы Windows в поле **Тип запуска** указано значение **Автоматически**. Можно изменить **Тип запуска** на **Вручную** или **Выключен** с помощью выпадающего списка.

Поскольку службы являются глобальными настройками операционных систем Windows, любой профайл может запустить службу, и в результате вы можете перепутать способ запуска профайла, например, с командой “startServer”. Для избежания конфликтов служебных запросов между разными профайлами отключите опцию **Запустить процесс сервера приложений как службу Windows**.
15. Необязательно: Дополнительно: Настройте базы данных с помощью файла эскиза.
 - a. Выберите **Настройка базы данных с помощью файла структуры базы данных** для применения файла структуры вместо указания параметров базы данных на следующих панелях.
 - b. Нажмите **Обзор**.
 - c. Укажите полное имя пути к файлу эскиза.
 - d. Нажмите кнопку **Далее**.
 - e. Выберите **Отложить выполнение сценариев базы данных (обязательно выберите при использовании удаленной базы данных)**, для того чтобы запретить автоматическое создание и настройку базы данных или создание таблиц в

существующей базе данных в ходе создания профайла. Если этот переключатель не выбран, то будет создана локальная база данных. Если вы выберете эту опцию, то вы или администратор базы данных должны вручную запустить сценарии из каталога, указанного в поле выходного каталога сценария базы данных на этой странице. Если создаются сценарии для Oracle, то перед их запуском необходимо заменить @DB_PASSWORD@ на пароль для имени схемы.

Примечание: Если на сервере базы данных установлено несколько версий DB2 или несколько экземпляров DB2, то для создания профайла используется версия или экземпляр DB2 по умолчанию. Для управления версией или экземпляром DB2 служит процедура "Установка баз данных вручную", позволяющая администратору базы данных обеспечить использование правильной версии или экземпляра.

Если выбирается указание файла эскиза, то панели настройки базы данных в Инструменте управления профайлами пропускаются. Вместо них расположение файла эскиза помещается в командную строку для выполнения настройки базы данных. Дополнительная информация об использовании файла эскиза для настройки базы данных приведена в разделе "Создание или настройка сценариев базы данных с помощью инструмента проектирования баз данных".

16. На панели Конфигурация базы данных проверьте сведения о конфигурации базы данных MONITOR.
 - a. Выберите продукт базы данных в списке.
 - b. Для определения целевого каталога для сформированных сценариев разрешите опцию **Переписать целевой каталог для сформированных сценариев** и введите путь в поле **Целевой каталог для сценариев базы данных**. (Каталог по умолчанию - каталог-monitor\profiles\WBMon01\dbscripts\Monitor\платформа\.)
 - c. Выберите сценарии **Отложить выполнение сценариев баз данных (обязательно в случае использования удаленной базы данных)**, если вы не хотите автоматически создавать и настраивать локальную базу данных или создавать таблицы в существующей базе данных во время создания или дополнения профайла. Если этот переключатель не выбран, то будет создана локальная база данных. Если вы выберете эту опцию, то вы или администратор базы данных должны вручную запустить сценарии из каталога, указанного в поле выходного каталога сценария базы данных на этой странице. Если создаются сценарии для Oracle, то перед их запуском необходимо заменить @DB_PASSWORD@ на пароль для имени схемы.

Примечание: Если на сервере базы данных установлено несколько версий DB2 или несколько экземпляров DB2, то для создания профайла используется версия или экземпляр DB2 по умолчанию. Для управления версией или экземпляром DB2 служит процедура "Установка баз данных вручную", позволяющая администратору базы данных обеспечить использование правильной версии или экземпляра.

- d. В поле **Имя базы данных** введите имя базы данных или примите имя по умолчанию (MONITOR).
- e. В поле **Имя схемы** введите имя схемы или примите имя по умолчанию (MONITOR). При использовании DB2 на z/OS имя схемы базы данных IBM Business Monitor должно отличаться от имени схемы общей базы данных Process Server во избежание конфликтов между объектами баз данных.
- f. Нажмите кнопку **Далее**.

17. На панели конфигурации базы данных (часть 2) выполните следующие действия для базы данных MONITOR:

- a. Введите *имя_пользователя* в поле **Имя пользователя** для идентификации базой данных. ИД пользователя, обладающего правами на чтение и запись к таблицам MONITOR.

Примечание: В случае применения базы данных Oracle это поле недоступно для изменения.

- b. Введите *пароль* в поле **Пароль** для идентификации базой данных. Пароль пользователя БД.
- c. Введите *пароль* в поле **Подтверждение пароля**. Этот пароль должен совпадать с паролем в поле **Пароль**.
- d. Укажите или выберите путь к классам драйвера JDBC. Драйверы JDBC для DB2, Oracle и SQL Server расположены в каталоге `каталог-monitor/jdbcdrivers`. Переменная `classpath` для драйвера JDBC установлена для использования файлов определенного продукта на основании типа базы данных, выбранного на панели Конфигурация базы данных. В качестве альтернативы можно нажать кнопку **Обзор** для ввода пути к классам драйвера JDBC.
- База данных DB2: Следующий каталог создается по умолчанию:
`каталог-monitor/jdbcdrivers/DB2`
 - База данных Oracle: Следующий каталог создается по умолчанию:
`каталог-monitor/jdbcdrivers/Oracle`

Файл драйвера JDBC `ojdbc6.jar` является поддерживаемым Oracle драйвером JDBC для использования в WebSphere Application Server версии 7. Файл `ojdbc6.jar` можно использовать для Oracle 10g и Oracle 11g. Сведения о минимальных обязательных параметрах для Oracle приведены в ссылке на связанную информацию.

- База данных SQL Server: Следующий каталог создается по умолчанию:
`каталог-monitor/jdbcdrivers/SQLServer`

Файл драйвера JDBC `sqljdbc4.jar` является драйвером JDBC Microsoft SQL Server 2.0. Сведения о минимальных обязательных параметрах для SQL Server приведены в ссылке на связанную информацию.




- e. Выберите одну из следующих опций для типа драйвера JDBC:
- Для базы данных Oracle:
 - **OCI:** Драйвер OCI требует установки локального клиента Oracle.
 - **Простой:** Простой драйвер использует Java для связи с базой данных и не требует клиента в локальной системе.
 - Профайлы IBM Business Monitor для баз данных DB2 в операционных системах, отличных от z/OS, создаются с драйверами типа 4, а в системах z/OS - с драйверами типа 2. Тип драйвера можно изменить с помощью административной консоли после создания профайла в конфигурации источника данных. Драйвер типа 2 - это драйвер встроенного API, и он требует установки ПО базы данных или клиента базы данных на локальном компьютере. Драйвер типа 4 - это реализация Java. Обычно она обеспечивает наилучшую производительность. Для базы данных MONITOR в локальной системе не требуется программное обеспечение или клиенты базы данных.
- f. Введите *имя-хоста* в **Имя хоста или IP-адрес сервера базы данных**. Значение по умолчанию - `localhost` или полное имя локального хоста; его следует

использовать для установки на одном сервере. Если база данных находится на удаленном сервере, необходимо ввести полное имя или IP-адрес.

Примечание: Кроме случая установки на одиночном сервере, *ее* используйте переменную `localhost`, поскольку члены кластера зависят от действующего имени хоста или IP-адреса.

- g. Введите *номер-порта* в поле **Порт получателя или служебный порт TCP/IP базы данных**. Это - номер порта, назначенный для службы TCP/IP, или порт получения базы данных.
 - h. Необязательно: При использовании DB2 в z/OS введите *имя-подсистемы* в поле **Имя подсистемы**. Это расположение базы данных DB2 for z/OS. В имени недопустимы пробелы.
 - i. Если применяется Oracle или SQL Server, то для создания базы данных в автоматическом режиме введите следующую информацию:
 - В поле **Имя администратора базы данных** введите *имя_пользователя_системы*. Это значение представляет имя администратора базы данных для Oracle или SQL Server. Этому пользователю должны быть предоставлены права доступа для создания и удаления баз данных и пользователей.
 - В поле **Пароль** введите *пароль*. Это пароль системного администратора, указанного в предыдущем поле.
 - Введите *пароль* в поле **Подтверждение пароля**.
 - j. Нажмите кнопку **Далее**. Если база данных MONITOR еще не создана, будет показано предупреждающее сообщение. Нажмите кнопку **Да** для продолжения. Базу данных можно создать позднее.
18. На панели База данных хранилища материалов Cognos, если еще не существует установки IBM Cognos Business Intelligence для использования, введите данные для создания базы данных хранилища материалов IBM Cognos BI для многомерного анализа данных из сводных панелей.
- a. Выберите **Создать новую базу данных хранилища материалов Cognos**.
 - b. Укажите имя базы данных, которая должна использоваться для хранилища материалов IBM Cognos BI. Имя профайла по умолчанию — COGNOSCS. В случае применения Oracle в качестве имени базы данных должно быть указано глобальное имя базы данных Oracle (его можно просмотреть с помощью следующего запроса: `SELECT * FROM GLOBAL_NAME`). В Microsoft SQL Server имя базы данных должно отличаться от имени должны быть MONITOR.
 - c. Введите имя и пароль пользователя базы данных и подтвердите пароль. Если для хранилища материалов используется то же имя пользователя, что и для базы данных MONITOR, необходимо применять такой же пароль. Поскольку этот пользователь должен обладать полными правами доступа, рекомендуется создать нового пользователя для использования только в базе данных хранилище материалов.

Примечание: Имя пользователя и пароль для базы данных хранилища материалов IBM Cognos BI находятся в `Cognos_JDBC_Alias`, где хранятся все идентификационные данные базы данных. При каждом запуске сервера IBM Business Monitor IBM Cognos BI текущие значения передаются в конфигурацию IBM Cognos BI для обеспечения доступа IBM Cognos BI к хранилищу материалов. Такая интеграция не позволяет изменять имя пользователя и пароль хранилища материалов с помощью приложения Настройка IBM Cognos BI.

19. На панели Краткая информация о создании профайла проверьте информацию. При необходимости внесения изменений нажмите кнопку **Назад** и внесите изменения.
20. Для создания профайла выберите **Создать**.
21. На панели Завершение создания профайла проверьте информацию.
22. Необязательно: Откройте консоль Первые шаги.
 -  Выберите опцию **Запустить Первые шаги в IBM Business Monitor**.
 -   Перейдите в каталог `profile_root/firststeps.wbm` и введите команду `firststeps.sh`.
23. Нажмите кнопку **Готово** для выхода из Profile Management Tool.

Во время создания профайла значения портов были заданы для всех необходимых портов. При изменении портов после установки следует перенастроить значения портов для правильной работы IBM Business Monitor.

Дополнение профайлов диспетчера развертывания

В среде сетевого развертывания требуется профайл администратора развертывания. Вместо создания нового профайла можно дополнить существующий профайл администратора развертывания для поддержки IBM Business Monitor.

Перед выполнением этой задачи необходимо выполнить следующие задачи:

- Проверить выполнение предварительных требований для аппаратного обеспечения и программного обеспечения
- Установить IBM Business Monitor
- Выполнить вход в систему от имени пользователя с правами на чтение, запись и выполнение программ для каталога профайлов WebSphere Application Server
- Установить базу данных

Существующий профайл WebSphere Application Server, Process Server или WebSphere Enterprise Service Bus можно дополнить с помощью шаблона IBM Business Monitor. Аналогично, если был установлен WebSphere Application Server, дополненный профайл для IBM Business Monitor, то этот профайл можно дополнить с помощью Process Server или WebSphere Enterprise Service Bus.

Для того, чтобы дополнить профайл администратора развертывания с помощью Инструмента управления профайлами, выполните следующие действия:

1. Открыть инструмент управления профайлами с помощью одного из следующих способов:
 - В консоли Первые шаги IBM Business Monitor выберите **Инструмент управления профайлами**.
 -  Выберите **Пуск > Программы > IBM > Business Monitor 7.5 > Инструмент управления профайлами**.
 -  Запустите файл `pmt.bat`, расположенный в следующем каталоге: `app_server_root\bin\ProfileManagement`
 -   Перейдите в каталог `app_server_root/bin/ProfileManagement` и введите `./pmt.sh` в окне терминала.
2. В панели Вас приветствует инструмент управления профайлами проверьте информацию и нажмите **Запустить инструмент управления профайлами**.
3. На панели Профайлы выберите профайл из списка и нажмите кнопку **Расширить** для расширения существующего профайла. (Можно раскрыть профайл для

просмотра уже выполненных дополнений.) Выбранный для расширения существующий профайл диспетчера развертывания должен быть профайлом диспетчера развертывания IBM Business Monitor.

Ограничение: Если опция IBM Business Monitor не видна, то это может означать, что вы работаете с 64-разрядной версией. Если используется 64-разрядная версия IBM Business Monitor, нельзя использовать Инструмент управления профайлами. Необходимо использовать команду `managerprofiles`.

4. На панели Выбор дополнения выберите **Администратор развертывания сервера монитора** в списке, после чего нажмите кнопку **Далее**.
5. На панели Опции дополнения профайла выберите **Дополнение профайла** и нажмите кнопку **Далее**. В режиме **обычной** установки отображаются не все панели.
6. Необязательно: Если защита профайла, который вы дополняете, включена, выполните следующие действия на панели Административная безопасность:
 - a. Введите *имя-пользователя* в **Имени пользователя**.
 - b. Введите *пароль* в поле **Пароль**.
 - c. Введите *пароль* в поле **Подтверждение пароля**.
 - d. Нажмите кнопку **Далее**.
7. Необязательно: Дополнительно: Настройте базы данных с помощью файла эскиза.
 - a. Выберите **Настройка базы данных с помощью файла структуры базы данных** для применения файла структуры вместо указания параметров базы данных на следующих панелях.
 - b. Нажмите **Обзор**.
 - c. Укажите полное имя пути к файлу эскиза.
 - d. Нажмите кнопку **Далее**.
 - e. Выберите **Отложить выполнение сценариев базы данных (обязательно выберите при использовании удаленной базы данных)**, для того чтобы запретить автоматическое создание и настройку базы данных или создание таблиц в существующей базе данных в ходе создания профайла. Если этот переключатель не выбран, то будет создана локальная база данных. Если вы выберете эту опцию, то вы или администратор базы данных должны вручную запустить сценарии из каталога, указанного в поле выходного каталога сценария базы данных на этой странице. Если создаются сценарии для Oracle, то перед их запуском необходимо заменить `@DB_PASSWORD@` на пароль для имени схемы.

Примечание: Если на сервере базы данных установлено несколько версий DB2 или несколько экземпляров DB2, то для создания профайла используется версия или экземпляр DB2 по умолчанию. Для управления версией или экземпляром DB2 служит процедура "Установка баз данных вручную", позволяющая администратору базы данных обеспечить использование правильной версии или экземпляра.

Если выбирается указание файла эскиза, то панели настройки базы данных в Инструменте управления профайлами пропускаются. Вместо них расположение файла эскиза помещается в командную строку для выполнения настройки базы данных. Дополнительная информация об использовании файла эскиза для настройки базы данных приведена в разделе "Создание или настройка сценариев базы данных с помощью инструмента проектирования баз данных".

8. На панели Конфигурация базы данных проверьте сведения о конфигурации базы данных MONITOR.

- a. Выберите продукт базы данных в списке.
- b. Для определения целевого каталога для сформированных сценариев разрешите опцию **Переписать целевой каталог для сформированных сценариев** и введите путь в поле **Целевой каталог для сценариев базы данных**. (Каталог по умолчанию - каталог-monitor\profiles\WMon01\dbscripts\Monitor\платформа\.)
- c. Выберите сценарии **Отложить выполнение сценариев баз данных (обязательно в случае использования удаленной базы данных)**, если вы не хотите автоматически создавать и настраивать локальную базу данных или создавать таблицы в существующей базе данных во время создания или дополнения профайла. Если этот переключатель не выбран, то будет создана локальная база данных. Если вы выберете эту опцию, то вы или администратор базы данных должны вручную запустить сценарии из каталога, указанного в поле выходного каталога сценария базы данных на этой странице. Если создаются сценарии для Oracle, то перед их запуском необходимо заменить @DB_PASSWORD@ на пароль для имени схемы.

Примечание: Если на сервере базы данных установлено несколько версий DB2 или несколько экземпляров DB2, то для создания профайла используется версия или экземпляр DB2 по умолчанию. Для управления версией или экземпляром DB2 служит процедура "Установка баз данных вручную", позволяющая администратору базы данных обеспечить использование правильной версии или экземпляра.

- d. В поле **Имя базы данных** введите имя базы данных или примите имя по умолчанию (MONITOR).
 - e. В поле **Имя схемы** введите имя схемы или примите имя по умолчанию (MONITOR). При использовании DB2 на z/OS имя схемы базы данных IBM Business Monitor должно отличаться от имени схемы общей базы данных Process Server во избежание конфликтов между объектами баз данных.
 - f. Нажмите кнопку **Далее**.
9. На панели конфигурации базы данных (часть 2) выполните следующие действия для базы данных MONITOR:
- a. Введите *имя_пользователя* в поле **Имя пользователя** для идентификации базой данных. ИД пользователя, обладающего правами на чтение и запись к таблицам MONITOR.

Примечание: В случае применения базы данных Oracle это поле недоступно для изменения.

- b. Введите *пароль* в поле **Пароль** для идентификации базой данных. Пароль пользователя БД.
- c. Введите *пароль* в поле **Подтверждение пароля**. Этот пароль должен совпадать с паролем в поле **Пароль**.
- d. Укажите или выберите путь к классам драйвера JDBC. Драйверы JDBC для DB2, Oracle и SQL Server расположены в каталоге каталог-monitor/jdbcdrivers. Переменная classpath для драйвера JDBC установлена для использования файлов определенного продукта на основании типа базы данных, выбранного на панели Конфигурация базы данных. В качестве альтернативы можно нажать кнопку **Обзор** для ввода пути к классам драйвера JDBC.
 - База данных DB2: Следующий каталог создается по умолчанию:
каталог-monitor/jdbcdrivers/DB2
 - База данных Oracle: Следующий каталог создается по умолчанию:
каталог-monitor/jdbcdrivers/Oracle

Файл драйвера JDBC ojdbc6.jar является поддерживаемым Oracle драйвером JDBC для использования в WebSphere Application Server версии 7. Файл ojdbc6.jar можно использовать для Oracle 10g и Oracle 11g. Сведения о минимальных обязательных параметрах для Oracle приведены в ссылке на связанную информацию.

- База данных SQL Server: Следующий каталог создается по умолчанию: каталог-monitor/jdbcdrivers/SQLServer

Файл драйвера JDBC sqljdbc4.jar является драйвером JDBC Microsoft SQL Server 2.0. Сведения о минимальных обязательных параметрах для SQL Server приведены в ссылке на связанную информацию.




- e. Выберите одну из следующих опций для типа драйвера JDBC:
- Для базы данных Oracle:
 - **OCI:** Драйвер OCI требует установки локального клиента Oracle.
 - **Простой:** Простой драйвер использует Java для связи с базой данных и не требует клиента в локальной системе.
 - Профайлы IBM Business Monitor для баз данных DB2 в операционных системах, отличных от z/OS, создаются с драйверами типа 4, а в системах z/OS - с драйверами типа 2. Тип драйвера можно изменить с помощью административной консоли после создания профайла в конфигурации источника данных. Драйвер типа 2 - это драйвер встроенного API, и он требует установки ПО базы данных или клиента базы данных на локальном компьютере. Драйвер типа 4 - это реализация Java. Обычно она обеспечивает наилучшую производительность. Для базы данных MONITOR в локальной системе не требуется программное обеспечение или клиенты базы данных.
- f. Введите *имя-хоста* в **Имя хоста или IP-адрес сервера базы данных**. Значение по умолчанию - localhost или полное имя локального хоста; его следует использовать для установки на одном сервере. Если база данных находится на удаленном сервере, необходимо ввести полное имя или IP-адрес.

Примечание: Кроме случая установки на одиночном сервере, *ее* используйте переменную localhost, поскольку члены кластера зависят от действующего имени хоста или IP-адреса.

- g. Введите *номер-порта* в поле **Порт получателя или служебный порт TCP/IP базы данных**. Это - номер порта, назначенный для службы TCP/IP, или порт получения базы данных.
- h. Необязательно: При использовании DB2 в z/OS введите *имя-подсистемы* в поле **Имя подсистемы**. Это расположение базы данных DB2 for z/OS. В имени недопустимы пробелы.
- i. Если применяется Oracle или SQL Server, то для создания базы данных в автоматическом режиме введите следующую информацию:
- В поле **Имя администратора базы данных** введите *имя_пользователя_системы*. Это значение представляет имя администратора базы данных для Oracle или SQL Server. Этому пользователю должны быть предоставлены права доступа для создания и удаления баз данных и пользователей.
 - В поле **Пароль** введите *пароль*. Это пароль системного администратора, указанного в предыдущем поле.
 - Введите *пароль* в поле **Подтверждение пароля**.

- j. Нажмите кнопку **Далее**. Если база данных MONITOR еще не создана, будет показано предупреждающее сообщение. Нажмите кнопку **Да** для продолжения. Базу данных можно создать позднее.
10. На панели База данных хранилища материалов Cognos, если еще не существует установки IBM Cognos Business Intelligence для использования, введите данные для создания базы данных хранилища материалов IBM Cognos BI для многомерного анализа данных из сводных панелей.
 - a. Выберите **Создать новую базу данных хранилища материалов Cognos**.
 - b. Укажите имя базы данных, которая должна использоваться для хранилища материалов IBM Cognos BI. Имя профайла по умолчанию — COGNOSCS. В случае применения Oracle в качестве имени базы данных должно быть указано глобальное имя базы данных Oracle (его можно просмотреть с помощью следующего запроса: SELECT * FROM GLOBAL_NAME). В Microsoft SQL Server имя базы данных должно отличаться от имени должны быть MONITOR.
 - c. Введите имя и пароль пользователя базы данных и подтвердите пароль. Если для хранилища материалов используется то же имя пользователя, что и для базы данных MONITOR, необходимо применять такой же пароль. Поскольку этот пользователь должен обладать полными правами доступа, рекомендуется создать нового пользователя для использования только в базе данных хранилище материалов.

Примечание: Имя пользователя и пароль для базы данных хранилища материалов IBM Cognos BI находятся в Cognos_JDBC_Alias, где хранятся все идентификационные данные базы данных. При каждом запуске сервера IBM Business Monitor IBM Cognos BI текущие значения передаются в конфигурацию IBM Cognos BI для обеспечения доступа IBM Cognos BI к хранилищу материалов. Такая интеграция не позволяет изменять имя пользователя и пароль хранилища материалов с помощью приложения Настройка IBM Cognos BI.

11. На панели Краткая информация о расширении профайла проверьте информацию. При необходимости внесения изменений нажмите кнопку **Назад** и внесите изменения.
12. Выберите **Расширить** для расширения профайла.
13. На панели Расширенный профайл проверьте информацию о расширенном профайле.
14. Необязательно: Откройте консоль Первые шаги.
 -  Выберите опцию **Запустить Первые шаги в IBM Business Monitor**.
 -   Перейдите в каталог profile_root/firststeps.wbm и введите команду firststeps.sh.
15. Нажмите кнопку **Готово** для выхода из Profile Management Tool.

Во время создания профайла значения портов были заданы для всех необходимых портов. При изменении портов после установки следует перенастроить значения портов для правильной работы IBM Business Monitor.

Создание индивидуальных профайлов для узлов





В среде сетевого развертывания для каждого узла, который планируется добавить в кластер сервера IBM Business Monitor, необходимо создать индивидуальный профайл. Профайл будет создан в каталоге профайлов WebSphere Application Server.

Перед выполнением этой задачи необходимо выполнить следующие задачи:

- Проверить выполнение предварительных требований для аппаратного обеспечения и программного обеспечения
- Установить IBM Business Monitor
- Выполнить вход в систему от имени пользователя с правами на чтение, запись и выполнение программ для каталога профайлов WebSphere Application Server
- Убедиться в том, что администратор развертывания выполняется.

Совет: Если вы планируете применять защиту на этих узлах, то ее необходимо настроить перед тем, как продолжить процесс создания пользовательского узла. Подробная информация о настройке защиты приведена по ссылке ниже.

Для того, чтобы создать индивидуальный профайл для каждого элемента кластера с помощью Инструмента управления профайлами, выполните следующие действия:

1. Открыть инструмент управления профайлами с помощью одного из следующих способов:
 - В консоли Первые шаги IBM Business Monitor выберите **Инструмент управления профайлами**.
 -  Выберите **Пуск > Программы > IBM > Business Monitor 7.5 > Инструмент управления профайлами**.
 -  Запустите файл `pmt.bat`, расположенный в следующем каталоге: `app_server_root\bin\ProfileManagement`
 -   Перейдите в каталог `app_server_root/bin/ProfileManagement` и введите `./pmt.sh` в окне терминала.
2. В панели Вас приветствует инструмент управления профайлами проверьте информацию и нажмите **Запустить инструмент управления профайлами**.
3. На панели Профайлы нажмите **Создать** для создания нового профайла.
4. На панели Выбор среды разверните IBM Business Monitor, выберите **Пользовательский профайл сервера монитора** и нажмите **Далее**. Благодаря созданию индивидуального профайла достигается гибкость при создании серверов и кластеров в процессе настройки среды.

Ограничение: Если опция IBM Business Monitor не видна, то это может означать, что вы работаете с 64-разрядной версией. Если используется 64-разрядная версия IBM Business Monitor, нельзя использовать Инструмент управления профайлами. Необходимо использовать команду `manageprofiles`.




5. На панели Опции создания профайла выберите тип установки и нажмите кнопку **Далее**.
 - **Создание обычного профайла** (по умолчанию): Создает пользовательский профайл, который использует параметры конфигурации по умолчанию. Средство Profile Management назначает уникальные имена профайлу, узлу и хосту. Узел будет объединен с существующим администратором развертывания.
 - **Создание расширенного профайла:** Создает пользовательский профайл, который использует параметры конфигурации по умолчанию. Можно указать значения для расположения профайла и имени профайла, узла и хоста. Узел будет объединен с существующим администратором развертывания.
6. Если выбран вариант **Создание обычного профайла**, то перейдите к шагу Шаг 10: Панель объединения.
7. Дополнительно: На панели Расположение и имя профайла примите значения по умолчанию для расположения и имени или укажите имя профайла и путь к каталогу, содержащему файлы среды выполнения, такие как команды, файлы

конфигурации и файлы протокола. Именем профайла по умолчанию является Custom01. В операционной системе Windows, как правило, применяется каталог профайла C:\IBM\WebSphere\AppServer\profiles\Custom01.

8. Необязательно: Дополнительно: Если создаваемый профайл должен быть профайлом по умолчанию, выберите переключатель **Сделать профайлом по умолчанию**. Нажмите кнопку **Далее**.
9. Дополнительно: На панели Имена хоста и узла введите новые значения или примите значения по умолчанию и нажмите **Далее**.
 - Имя узла используется для администрирования. Если узел является интегрированным, то его имя должно быть уникальным в ячейке.
 - Имя хоста - это имя DNS (краткое или полное) или IP-адрес этого компьютера.
10. В панели включения выполните следующие действия для выбора используемого профайла администратора развертывания:

Примечание: Вы можете отложить добавление узла на более поздний срок (с помощью add_node), выбрав **Добавить этот узел позже**. Если вы выберете данную опцию, то все поля будут отключены. Одним преимуществом отложенной операции объединения является то, что не придется создавать профайл второй раз. Если объединение делалось во время создания профайла и по некоторой причине было неудачным (например, из-за рассинхронизации системных часов и часов администратора развертывания), то придется создавать профайл снова для обеспечения его достоверности. Поэтому объединение на более поздней стадии обеспечивает более надежное управление процедурой объединения.

- a. Введите *имя-хоста* в **Имя хоста или IP-адрес администратора развертывания**. Данное значение указывает полное имя хоста или IP-адрес сервера, где был создан профайл администратора развертывания.
- b. Введите *номер-порта* в **Номер порта SOAP администратора развертывания**. Значение по умолчанию - 8879.
- c. Необязательно: Если включена административная защита администратора развертывания, введите *имя-пользователя* в **Имени пользователя**. Имя пользователя должно соответствовать существующему пользователю WebSphere Application Server администратора развертывания. Это значение необходимо для идентификации в администраторе развертывания.
- d. Необязательно: Если включена административная защита администратора развертывания, введите *пароль* в поле **Пароль**. Пароль должен соответствовать введенному имени *пользователя*.
- e. Выберите **Далее**.
11. Если выбрана опция **Создание обычного профайла**, перейдите к Шагу 15: Панель Сводная информация о создании профайла
12. Дополнительно: в панели Настройка базы данных выполните следующие действия:
 - a. Выберите продукт базы данных в выпадающем списке.
 - b. Введите имя каталога или перейдите к каталогу, в котором находятся файлы с путями к классам JDBC в **Расположение (каталог) файлов с путями к классам драйвера JDBC**.
 - c. Нажмите кнопку **Далее**.
13. На панели Краткая информация о создании профайла проверьте информацию. При необходимости внесения изменений нажмите кнопку **Назад** и внесите изменения.
14. Для создания профайла выберите **Создать**.

15. На панели Завершение создания профайла проверьте информацию.
16. Необязательно: Откройте консоль Первые шаги.
 -  Выберите опцию **Запустить Первые шаги в IBM Business Monitor**.
 -   Перейдите в каталог `profile_root/firststeps.wbm` и введите команду `firststeps.sh`.
17. Нажмите кнопку **Готово** для выхода из Profile Management Tool.

Во время создания профайла значения портов были заданы для всех необходимых портов. При изменении портов после установки следует перенастроить значения портов для правильной работы IBM Business Monitor.


Расширение индивидуальных профайлов для узлов

В случае сетевого развертывания для каждого узла, который планируется добавить к кластеру серверов IBM Business Monitor, необходимо создать пользовательский профайл. Вместо создания нового профайла можно дополнить существующий пользовательский профайл на каждом узле.

Перед выполнением этой задачи необходимо выполнить следующие задачи:

- Проверить выполнение предварительных требований для аппаратного обеспечения и программного обеспечения
- Установить IBM Business Monitor
- Выполнить вход в систему от имени пользователя с правами на чтение, запись и выполнение программ для каталога профайлов WebSphere Application Server
- Убедиться в том, что администратор развертывания выполняется.

Для того, чтобы дополнить профайл для каждого члена кластера с помощью Инструмента управления профайлами, выполните следующие действия:




1. Открыть инструмент управления профайлами с помощью одного из следующих способов:
 - В консоли Первые шаги IBM Business Monitor выберите **Инструмент управления профайлами**.
 -  Выберите **Пуск > Программы > IBM > Business Monitor 7.5 > Инструмент управления профайлами**.
 -  Запустите файл `pmt.bat`, расположенный в следующем каталоге: `app_server_root\bin\ProfileManagement`
 -   Перейдите в каталог `app_server_root/bin/ProfileManagement` и введите `./pmt.sh` в окне терминала.
2. В панели Вас приветствует инструмент управления профайлами проверьте информацию и нажмите **Запустить инструмент управления профайлами**.
3. На панели Профайлы выберите профайл из списка и нажмите кнопку **Расширить** для расширения существующего профайла. (Можно раскрыть профайл для просмотра уже выполненных дополнений.) Необходимо выбрать существующий индивидуальный профайл, который в результате расширения станет индивидуальным профайлом IBM Business Monitor. Индивидуальный профайл способствует гибкости при создании серверов и кластеров в процессе настройки среды.

Ограничение: Если опция IBM Business Monitor не видна, то это может означать, что вы работаете с 64-разрядной версией. Если используется 64-разрядная версия

IBM Business Monitor, нельзя использовать Инструмент управления профайлами. Необходимо использовать команду `managerprofiles`.

4. На панели Выбор дополнения выберите **Пользовательский профайл сервера монитора** в списке, после чего нажмите кнопку **Далее**.
5. На панели Опции дополнения профайла выберите **Дополнение профайла** и нажмите кнопку **Далее**. В режиме **обычной** установки отображаются не все панели.
6. В панели включения, если она показана, выполните следующие действия для выбора используемого профайла администратора развертывания:

Примечание: Если профайл ранее не объединялся, то эта панель показана не будет.

- a. Введите *имя-хоста* в **Имя хоста или IP-адрес администратора развертывания**. Данное значение указывает полное имя хоста или IP-адрес сервера, где был создан профайл администратора развертывания.
 - b. Введите *номер-порта* в **Номер порта SOAP администратора развертывания**. Значение по умолчанию - 8879.
 - c. Необязательно: Если включена административная защита администратора развертывания, введите *имя-пользователя* в **Имени пользователя**. Имя пользователя должно соответствовать существующему пользователю WebSphere Application Server администратора развертывания. Это значение необходимо для идентификации в администраторе развертывания.
 - d. Необязательно: Если включена административная защита администратора развертывания, введите *пароль* в поле **Пароль**. Пароль должен соответствовать введенному имени *пользователя*.
 - e. Выберите **Далее**.
7. На панели Настройка базы данных выполните следующие действия:
 - a. Выберите продукт базы данных в списке.
 - b. Введите имя каталога или перейдите к каталогу, в котором находятся файлы с путями к классам JDBC в **Расположение (каталог) файлов с путями к классам драйвера JDBC**.
 - c. Нажмите кнопку **Далее**.
 8. Выберите **Расширить** для расширения профайла.
 9. На панели Расширенный профайл проверьте информацию о расширенном профайле.
 10. Необязательно: Откройте консоль Первые шаги.
 -  Выберите опцию **Запустить Первые шаги в IBM Business Monitor**.
 -   Перейдите в каталог `profile_root/firststeps.wbm` и введите команду `firststeps.sh`.
 11. Нажмите кнопку **Готово** для выхода из Profile Management Tool.

Во время создания профайла значения портов были заданы для всех необходимых портов. При изменении портов после установки следует перенастроить значения портов для правильной работы IBM Business Monitor.

Создание и дополнение профайлов с помощью команды `manageprofiles`

Вместо инструмента управления профайлами, профайлы можно создавать из командной строки с помощью команды **`manageprofiles`**. В случае применения 64-разрядной версии IBM Business Monitor, следует использовать команду **`manageprofiles`**, поскольку инструмент Profile Management Tool не поддерживается. При использовании z/OS обратитесь к разделу "Создание обычных конфигураций для IBM Business Monitor для z/OS".

Перед созданием или расширением профайла внимательно проверьте имеющиеся параметры. Изменить профайл после его создания или расширения будет не просто.

Перед выполнением этой задачи необходимо выполнить следующие задачи:

- Проверить выполнение предварительных требований для аппаратного обеспечения и программного обеспечения
- Установить IBM Business Monitor
- Выполнить вход в систему от имени пользователя с правами на чтение, запись и выполнение программ для каталога профайлов WebSphere Application Server

В случае применения базы данных Oracle поддержка JDBC предоставляется драйверами JDBC Oracle для JVM 1.6. Файл драйвера JDBC `ojdbc6.jar` является поддерживаемым Oracle драйвером JDBC для использования в WebSphere Application Server версии 7. Файл `ojdbc6.jar` можно использовать для Oracle 10g и Oracle 11g. Сведения о минимальных обязательных параметрах для Oracle приведены в ссылке на связанную информацию.

По умолчанию инструмент управления профайлами указывает на файл `ojdbc6.jar`, расположенный в каталоге `app_server_root\jdbcdrivers\oracle`. Кроме того, можно загрузить другой файл драйвера JDBC Oracle `ojdbc6.jar` и указать его при запуске инструмента управления профайлами или команды **`manageprofiles`**.

В случае применения базы данных SQL Server драйверы JDBC SQL Server для JVM 1.6 обеспечивают поддержку JDBC. IBM Business Monitor использует файл `sqljdbc4.jar` драйвера Microsoft JDBC 2.0. По умолчанию инструмент управления профайлами указывает на файл `sqljdbc4.jar`, расположенный в каталоге `app_server_root\jdbcdrivers\SQLServer`. Кроме того, можно загрузить другой файл драйвера JDBC Microsoft `sqljdbc4.jar` и указать его при запуске инструмента управления профайлами или команды **`manageprofiles`**. Сведения о минимальных обязательных параметрах для SQL Server приведены в ссылке на связанную информацию.

Для среды с одним сервером создайте автономный профайл.

Для среды сетевого развертывания выполните следующие действия:

1. Создайте профайл администратора развертывания перед созданием других профайлов. Если профайл администратора развертывания создан перед установкой IBM Business Monitor (например, для WebSphere Application Server или Process Server) и его планируется использовать для управления узлами IBM Business Monitor, дополните профайл с помощью шаблона, предоставленного IBM Business Monitor.
2. Для каждого узла, который планируется добавить в кластер сервера, необходимо создать индивидуальный профайл. В качестве альтернативы, можно дополнить существующий пользовательский профайл для каждого узла, который вы планируете добавить.

Примечание: Если на сервере базы данных установлено несколько версий DB2 или несколько экземпляров DB2, то для создания профайла используется версия или экземпляр DB2 по умолчанию. Для управления версией или экземпляром DB2 служит процедура "Установка баз данных вручную", позволяющая администратору базы данных обеспечить использование правильной версии или экземпляра.

Для создания профайла вручную выполните следующие действия:

1. Откройте командную строку и перейдите в следующий каталог:
`app_server_root/bin`
2. Запустите команду `manageprofiles.bat` или `manageprofiles.sh`, используя требуемые параметры. На справочных страницах приведена подробная информация о параметрах для каждого типа профайла.

Глава 7. Проверка установки

После того, как вы установили IBM Business Monitor и создали профайл, вы можете проверить правильность установки продукта с помощью консоли Первые шаги.

1. Откройте консоль Первые шаги.
 - Откройте командное окно. Перейдите к файлу `profile_root/firststeps.wbm` и выполните команду `firststeps.sh`.
 - На панели Создание профайла закончено выберите опцию **Запустить Первые шаги в IBM Business Monitor**.
 - Выберите **Пуск > Все программы > IBM > Business Monitor 7.5 > Профайлы > имя-профайла > Первые шаги**.
 - Перейдите к файлу `profile_root\firststeps.wbm` и запустите команду `firststeps.bat`.

Важное замечание: Для установки или выполнения консоли Первые шаги в Windows 7, Windows Vista или Windows Server 2008, необходимо повысить права доступа учетной записи пользователя Microsoft Windows, щелкнув правой кнопкой мыши на файле `firststeps.bat` и выбрав опцию **Запуск от имени администратора**. Это требуется как для административных, так и для других пользователей.

2. В консоли Первые шаги выберите опцию выполнения проверки установки.
3. Просмотрите результаты.

Если включена защита IBM Business Monitor, то после завершения установки настройте пользователей, для чего введите ИД и пароль пользователя для псевдонима проверки подлинности MonitorBusAuth. Более подробные сведения приведены в разделе Установка идентификационных данных в защищенной среде IBM Business Monitor.

Помимо опции проверки установки, в консоли Первые шаги предусмотрены опции, позволяющие запустить Инструмент управления профайлами, открыть административную консоль WebSphere Application Server и открыть Business Space.

В Linux или UNIX может потребоваться изменить владельца с пользователя root на другого пользователя. Эта задача выполняется в IBM Business Monitor точно так же, как в WebSphere Application Server или Process Server. Дополнительные сведения приведены в ссылках на связанные разделы (см.ниже).

Если при создании нового профайла IBM Business Monitor или расширении существующего профайла для IBM Business Monitor получен код результата `INSTCONFPARTIALSUCCESS` или `INSTCONFFAILED`, обратитесь к таблице в разделе по связанной справочной ссылке.

Глава 8. Определение портов

Номер порта для веб-интерфейсов, таких как Business Space и сводные панели на основе портлетов, можно найти в конфигурации в административной консоли WebSphere Application Server.

В среде сетевого развертывания (ND) по соображениям защиты и для распределения рабочей нагрузки обычно используется прокси-сервер или сервер HTTP. Входящие запросы HTTP направляются не прямо конкретному участнику кластера, а проходят через прокси-сервер, который их распределяет по участникам кластера, выполняющим работу. В этом случае необходимо знать имя хоста и номер порта прокси-сервера или веб-сервера, передающего запросы в элементы кластера.

- Для того чтобы определить порты сервера приложений, выполните следующие действия:
 1. В административной консоли WebSphere Application Server выберите **Серверы > Типы серверов > Серверы приложений WebSphere**.
 2. Выберите имя сервера или элемента кластера (например, **server1**).
 3. В разделе Соединения выберите **Порты**.

Номер порта для веб-интерфейсов, таких как Business Space и сводные панели на основе портлетов, приведен как WC_defaulthost_secure в защищенной среде и WC_defaulthost в незащищенной среде. Кроме того, на этой странице указан порт начальной загрузки, порт коннектора SOAP и другие порты, которые вам может потребоваться указать при работе с IBM Business Monitor.

- Для того чтобы определить порты сервера проху, выполните следующие действия:
 1. В административной консоли WebSphere Application Server выберите **Серверы > Типы серверов > Серверы Proxu WebSphere**.
 2. Выберите имя сервера (например, **проху**).
 3. В разделе Соединения выберите **Порты**.

Номер порта для веб-интерфейсов, таких как Business Space и сводные панели на основе портлетов, приведен как PROXY_HTTPS_ADDRESS в защищенной среде и PROXY_HTTP_ADDRESS в незащищенной среде. Кроме того, на этой странице указан порт начальной загрузки, порт коннектора SOAP и другие порты, которые вам может потребоваться указать при работе с IBM Business Monitor.

Веб-модули развертываются на виртуальном хосте (по умолчанию - defaulthost). Виртуальные хосты настраиваются в административной консоли путем выбора **Среда > Виртуальные хосты**. Виртуальный хост, выбранный для каждого веб-модуля, должен содержать порт HTTP или HTTPS, используемый сервером (или элементом кластера), на котором развернуты веб-модули. Кроме того, каждый из веб-модулей IBM Business Monitor должен использовать один и тот же виртуальный хост. Большинство приложений IBM Business Monitor, Business Space и REST (файлы EAR) содержат веб-модули.

Глава 9. Настройка среды

После установки IBM Business Monitor в топологии сетевого развертывания необходимо выполнить дополнительные задачи настройки, чтобы установить обязательные ресурсы и полностью подготовить среду для монитора.

Вместе с автономным профайлом для IBM Business Monitor автоматически создаются требуемые ресурсы. Вы можете проверить состояние в Административной консоли или заново развернуть компонент, который был удален вручную, но обычно задачи настройки из данного раздела требуются только для сетевого развертывания (ND).

Создание среды разработки с помощью шаблона

Мастер настройки среды развертывания позволяет создать кластер (или кластеры) и настроить все необходимые компоненты для топологии сетевого развертывания (ND) IBM Business Monitor.

Перед созданием кластеров и настройкой компонентов IBM Business Monitor должны быть выполнены следующие задачи:

- Установлен IBM Business Monitor.
- Создан профайл администратора развертывания IBM Business Monitor или расширен существующий профайл администратора развертывания для поддержки IBM Business Monitor.
- Создана база данных MONITOR.
- Запущен администратор развертывания.
- Создан и объединен по крайней мере один пользовательский профайл IBM Business Monitor или расширен существующий пользовательский профайл для поддержки IBM Business Monitor.
- Запущен пользовательский профайл или профайлы.

Перед запуском процесса конфигурации необходимо настроить автоматическую синхронизацию изменений узлов (в административной консоли выберите **Администрирование системы > Параметры консоли**, затем выберите **Синхронизировать изменения с узлами**). В противном случае потребуется вручную синхронизировать изменения после каждого шага.

Для IBM Business Monitor существуют два шаблона: однокластерный шаблон и шаблон удаленного обмена сообщениями, шаблон удаленной поддержки и шаблон веб-приложения (четырёхкластерный).

Один из необязательных шагов мастера настройки среды развертывания предусматривает импорт документа структуры базы данных. Этот документ определяет конфигурацию базы данных для выбранных компонентов среды развертывания, и информация из документа структуры отображается на странице База данных мастера. IBM Business Monitor содержит инструмент проектирования баз данных (DbDesignGenerator), который запрашивает у пользователей информацию о базах данных (платформа базы данных и имена базы данных, схем и пользователей), предназначенную для IBM Business Monitor. Вывод инструмента проектирования базы данных - это документ структуры базы данных, на основе которого инструмент проектирования базы данных создает сценарии баз данных.

Для настройки среды развертывания выполните следующие действия:

1. В административной консоли выберите **Серверы > Среда развертывания**.
2. Для запуска мастера настройки среды развертывания нажмите **Создать** на странице Среда развертывания.
 - a. Будет выбрана опция **Создать среду развертывания на основе шаблона**.
 - b. Введите уникальное имя для среды развертывания в поле **Имя среды развертывания**.
 - c. Если вы хотите просмотреть все шаги по настройке в мастере, выберите **Подробно: показать все шаги**. Если вы выбрали **Быстро: показать только необходимые шаги**, то мастер покажет только те страницы, которым не назначены значения по умолчанию. Выберите **Быстро: показать только необходимые шаги** только в том случае, если вы согласны принять системные значения по умолчанию для конфигурации среды развертывания. В этом разделе предполагается, что вы выбрали **Подробно: показать все шаги**.
 - d. Нажмите **Далее** для просмотра страницы Компоненты среды развертывания.
3. На странице Компоненты среды развертывания выберите компоненты для среды развертывания и нажмите **Далее**, чтобы просмотреть либо список совместимых компонентов, либо список шаблонов среды развертывания. Компоненты представляют возможности среды развертывания по обработке во время выполнения. Список доступных компонентов на странице Компоненты среды развертывания основан на профайле Администратора развертывания. Если профайл администратора развертывания расширен для включения других продуктов, а также IBM Business Monitor (например, IBM Business Process Manager), страница Компоненты среды развертывания также будет содержать эти компоненты. Значение по умолчанию для компонента среды развертывания соответствует возможностям среды выполнения Администратора развертывания.
4. На странице Выбрать совместимые компоненты среды развертывания выберите требуемые дополнительные компоненты и нажмите **Далее**, чтобы просмотреть список шаблонов, связанных с выбранными компонентами. Для компонента WBM можно создать только одну конфигурацию среды развертывания. Если конфигурация среды развертывания с компонентом WBM уже существует, то вы не сможете продолжить даже в том случае, если конфигурация среды развертывания не создана.
5. На странице Выбрать шаблон среды развертывания выберите шаблон и нажмите **Далее** для перехода к странице Выбрать узлы.

Список шаблонов, показанный на странице Шаблоны среды развертывания, является динамическим. Этот список активируется в зависимости от следующих аспектов среды и параметров конфигурации:

 - Платформы программного обеспечения
 - Опций, выбранных на страницах Выбрать компонент среды развертывания и Выбрать совместимые компоненты среды развертывания.

Обычно у вас есть выбор между шаблоном Один кластер и шаблоном Удаленный обмен сообщениями, Удаленная поддержка и Веб (четыре кластера). Описания этих шаблонов приведены на странице "Топология высокой готовности (сетевое развертывание)" раздела планирования.
6. На странице Выбрать узлы выберите узлы, которые вы хотите включить в эту среду развертывания, затем нажмите **Далее** для перехода к странице Участники кластера.

Выберите один или несколько узлов IBM Business Monitor для среды развертывания. Узлы IBM Business Monitor обозначаются записью для WBM в столбце версии. Если в столбце версии отсутствует запись для WBM, то для

настройки узла в качестве узла IBM Business Monitor необходимо расширить профайл узла для поддержки IBM Business Monitor и перезапустить мастер настройки среды развертывания.

Все выбранные узлы должны быть узлами IBM Business Monitor. Если на шаге 3 были выбраны дополнительные компоненты, то выберите поддерживающие их узлы.

В случае сред высокой готовности и переключения при сбое выберите по крайней мере два узла на разных хостах. Для повышения масштабируемости выберите не менее трех узлов.

Для выбора узла отметьте переключатель рядом с его именем.

7. На странице Кластеры назначьте по крайней мере один элемент кластера, принадлежащий по крайней мере одному узлу, каждой функции среды развертывания.

По умолчанию на каждом узле каждой функции назначается один участник кластера. Для изменения номера замените его в каждом столбце. В случае сетевого развертывания кластеры могут взаимодействовать, предоставляя дополнительные возможности в среде. В зависимости от требований, вы назначаете конкретные функции каждому кластеру в среде развертывания для обеспечения производительности, переключения при сбое и емкости.

Нулевое значение для узла означает, что узел не дает вклада в выбранную функцию, на основе выбранных вами компонентов.

Каждой функции должен быть присвоен по крайней мере один элемент кластера. В случае сред высокой готовности и переключения при сбое выберите по крайней мере два узла для каждой функции. Для обеспечения более высокого уровня масштабируемости укажите большее число элементов кластера для функции.

После присвоения элементов кластера нажмите кнопку **Далее** для перехода на страницы имен кластеров всех типов. Конкретный набор страниц зависит от выбранного шаблона среды развертывания. Если имена кластеров и их элементов настраивать не требуется, то с помощью панели навигации мастера откройте страницу Службы REST и перейдите к следующему шагу.

- a. Необязательно: Настройте имена кластеров и их элементов. На странице Имена кластеров укажите имена кластеров и элементов кластеров. Кроме того, можно изменить краткие имена кластеров и их элементов. Для каждого типа кластеров из выбранного шаблона предусмотрена отдельная страница. Ниже приведено описание страниц:

Поле	Описание	Значение
Кластер	Доступное только для чтения поле, в котором указана функциональная роль кластера.	<p>Значение зависит от типа кластера:</p> <ul style="list-style-type: none"> • Среда развертывания приложений • Вспомогательная инфраструктура • Инфраструктура обмена сообщениями • Инфраструктура веб-приложения <p>Дополнительная информация о функциональной роли каждого типа кластеров приведена в разделе "Типы топологий и шаблоны среды развертывания".</p>

Поле	Описание	Значение
Имя кластера	Создаваемое системой имя элемента кластера по умолчанию.	Значения по умолчанию определяются в соответствии со следующим соглашением: <i>имя среды развертывания.имя типа кластера</i> , где <i>имя типа кластера</i> может принимать одно из следующих значений: <ul style="list-style-type: none"> • AppTarget - Для целевых кластеров развертывания приложений. • Messaging - Для кластеров, выполняющих роль инфраструктуры обмена сообщениями. • Support - Для кластеров, выполняющих роль вспомогательной инфраструктуры. • Web - Для кластеров, выполняющих роль вспомогательных веб-приложений.
Имя элемента кластера	Создаваемое системой имя элемента кластера по умолчанию. Серверы, входящие в состав кластера, называются элементами кластера.	Примите значение по умолчанию, созданное системой, или укажите собственное имя. Имя элемента кластера по умолчанию определяются в соответствии со следующим соглашением: <i>имя-кластера.имя-узла.порядковый-номер-узла</i> . Число имен элементов кластера, показанных в таблице, совпадает с числом элементов, указанным в столбце типа кластера и строке узла на странице Кластеры.

8. На странице Конечные точки службы REST системы настройте конечные точки служб для API Representational State Transfer (REST).

Если вы хотите, чтобы в Business Space были доступны виджеты, то необходимо настроить конечные точки служб REST для этих виджетов. При выборе имени хоста и порта, если вы хотите, чтобы запросы REST направлялись напрямую на конкретный сервер приложений, то укажите имя хоста и порт этого сервера приложений. Если вы хотите, чтобы запросы REST направлялись на сервер проху или HTTP, расположенный перед одним или несколькими серверами приложений, то укажите имя хоста и порт этого сервера проху или HTTP. Во втором случае сервер проху или HTTP должен быть уже настроен. Если это условие не выполнено, пропустите эту страницу и настройте конечные точки позже.

- a. Настройте полный URL ко всем службам REST, выбрав **https://** или **http://** в списке **Протокол**.

- b. Введите имя сервера Proxu или HTTP в поле **Имя хоста или виртуальный хост в сбалансированной среде**.

Укажите имя хоста или виртуального хоста и номер порта для взаимодействия клиента с сервером или кластером. В кластерной среде, как правило, указывается имя хоста и номер порта распределителя нагрузки. Если оставить эти поля пустыми, то по умолчанию будут использоваться имя хоста и номер порта HTTP элемента кластера. В среде с распределением нагрузки значения по умолчанию впоследствии необходимо изменить на имя виртуального хоста и номер порта распределителя нагрузки. Убедитесь, что указано полное имя хоста.

- c. В поле **Порт** введите порт для подключения клиента к серверу или кластеру.
 - d. В таблице служб REST, если вы хотите изменить описание конечной точки службы REST, замените запись в поле Описание. Остальные поля предназначены только для чтения.
 - e. Нажмите **Далее** для перехода к странице Импортировать конфигурацию базы данных.
9. Необязательно: На странице Импортировать конфигурацию базы данных нажмите **Обзор**, чтобы перейти к документу структуры базы данных, или введите путь к документу структуры базы данных и затем нажмите **Далее** для перехода к странице Источники данных. Если вы импортируете документ структуры, то его содержимое отображается на странице База данных мастера. Документ структуры можно создать на основе структуры базы данных, созданной с помощью инструмента проектирования баз данных, или на основе шаблона с выбранными функциями.
10. На странице База данных настройте параметры базы данных для источников данных среды развертывания, затем нажмите **Далее** для перехода к странице Защита.

На этой странице определите информацию базы данных для компонентов, включенных в эту среду развертывания. Везде, где это возможно, мастер предложит значения по умолчанию для параметров, однако вы должны изменить эти значения на те, которые вы определили при планировании среды. При смене провайдеров вы можете нажать кнопку **Изменить провайдер** и отредактировать выбранный провайдер.

Примечание: Если вы импортировали документ структуры базы данных, то информация на странице База данных отражает конфигурацию источника данных согласно этому импортированному документу. Изменения, внесенные в конфигурацию источника данных после импорта документа структуры базы данных, могут быть несовместимы с файлом DDL, созданным инструментом проектирования базы данных и исходными значениями.

Будет ли на этом шаге показан быстрый путь настройки среды развертывания - зависит от нескольких факторов. Такой путь будет показан, если определено несколько баз данных.

Этот путь отображается всегда, когда вы используете провайдер базы данных DB2 для z/OS или Oracle .

Компонент IBM Business Monitor предлагает следующие записи:

Компонент	Источник данных
Источник данных для службы сообщений Business Monitor	Источник данных для службы сообщений IBM Business Monitor.
Хранилище материалов Cognos	Источник данных для хранилища материалов IBM Cognos Business Intelligence. (Отображается только в том случае, если IBM Cognos BI установлен, но не настроен.)

Компонент	Источник данных
Business Space	Источник данных для компонента Business Space. Опция Создать таблицы недоступна для этого компонента. Если среда развертывания содержит компонент Business Space, то таблицы для него необходимо создать вручную.

Если для топологии выбраны другие компоненты продукта, то могут быть показаны дополнительные записи.

Имена схем по умолчанию, показанные на этой странице, могут противоречить соглашению об именах вашего сайта или существующим схемам. По этой причине может потребоваться изменить имя схемы.

Примечание: Базы данных DB2 для z/OS: В качестве значения SQLID DB2 z/OS применяется имя схемы, указанное на панели. При необходимости после завершения работы мастера среды развертывания можно вручную изменить пользовательское свойство currentSQLID созданных источников данных источники, указав другое значение SQLID DB2 z/OS.

Вы можете изменять все ключевые параметры, например, имя базы данных, опцию создания таблиц, имя пользователя среды выполнения источника данных и имя пользователя и пароль для подключения источника данных к базе данных.

Примечание: Базы данных DB2 для z/OS: В качестве имени базы данных применяется имя подсистемы базы данных. Для других версий DB2 применяется имя базы данных MONITOR. Базы данных Oracle: В качестве имени базы данных применяется ИД системы Oracle.

Вы можете выбрать, какую базу данных следует использовать для заданного компонента.

Опция **Создать таблицы** недоступна, если используется провайдер базы данных DB2 для z/OS или Oracle.

Если вы применяете Oracle, то поле **Схема** будет недоступно и пусто, а поле **Имя пользователя** не будет заранее заполняться общим именем пользователя базы данных. Вы должны ввести имя пользователя и пароль для каждого источника данных.

Примечание: Уникальность имен пользователей не контролируется; появление одинаковых имен может вызвать конфликты таблиц.

11. На странице Защита введите идентификационные данные пользователей, необходимые для настройки компонентов IBM Business Monitor. Компонент IBM Business Monitor предлагает следующие записи:

Компонент	ИД и пароль
Псевдоним идентификации для ресурсов JMS службы событий CEI	Укажите идентификационные данные пользователя для защиты шины интеграции служб инфраструктуры событий общего формата (CEI) по умолчанию.
Идентификация доступа к администрированию Cognos	Укажите ИД пользователя и пароль с правами администратора для службы IBM Cognos BI. (Отображается только в том случае, если IBM Cognos BI установлен, но не настроен.)

Если для топологии выбраны другие компоненты продукта, то могут быть показаны дополнительные записи.

12. Необязательно: Если откроется страница Business Process Choreographer, то задайте параметры конфигурации Business Process Choreographer и нажмите

кнопку **Далее** для перехода к странице Веб-приложения системы. На этой странице вы указываете значения для следующих параметров:

- Роли защиты
- Псевдонимы проверки подлинности

13. Необязательно: Если откроется страница Веб-приложения системы, то задайте корневой контекст для веб-приложений, основанных на компонентах, в среде развертывания или примите системные значения по умолчанию для корневых контекстов. Затем нажмите **Далее** для просмотра страницы Сводка.

Таблица содержит следующую управляющую информацию.

Web-приложение

Имя web-приложения.

Некоторые из компонентов, входящих в создаваемую среду развертывания, содержат Web-приложения. Столбец **Web-приложение** может содержать следующие компоненты:

- Business Process Choreographer Explorer
- Business Space
- Администратор бизнес-правил

Корневой контекст

Текущее значение корневого контекста для компонента.

По умолчанию применяется корневой контекст по умолчанию для Web-приложения. Вы можете изменить корневые контексты, введя значение в поле **Корневой контекст**.

Примечание: Корневой контекст Business Space доступен только для чтения и не может быть изменен.

14. Убедитесь, что информация на странице Сводка верна, и нажмите **Закончить и создать среду**, чтобы закончить создание и сохранить конфигурацию среды развертывания. Для того чтобы выйти из сеанса, не завершив создание конфигурации, нажмите **Готово**.

Нажатие **Готово** сохраняет конфигурацию среды развертывания, но не создает ее.

Нажатие **Отмена** отменяет создание конфигурации среды развертывания и не сохраняет ее.

15. В случае создания среды развертывания с помощью кнопки **Завершить и создать среду** необходимо остановить и перезапустить все кластеры и узлы, а также администратор развертывания.

Если на последней странице мастера среды развертывания вместо кнопки **Готова** нажата кнопка **Закончить и создать среду** (среда не создается), то для просмотра конфигурации среды развертывания выберите **Сервер > Среда развертывания > имя среды развертывания**. На этой странице предусмотрена кнопка **Создать**, позволяющая создать среду. Закончив создание конфигурации, просмотрите файлы конфигурации, чтобы проверить внесенные изменения.

Либо сохраните изменения в главной конфигурации, либо аннулируйте их. Если вы выполнили не все необходимые шаги по настройке, то при щелчке на среде развертывания появится список отложенных шагов. После создания среды развертывания необходимо остановить и перезапустить все кластеры, узлы и администратор развертывания.

Импортирование определений среды развертывания, основанных на документах эскиза

Существующее определение среды развертывания, основанное на документе эскиза, можно импортировать из другого администратора развертывания, чтобы использовать его для настройки новой среды развертывания.

- У вас должна быть копия документа эскиза среды развертывания, экспортированного из другого администратора развертывания.
- У вас должен быть доступ к документу эскиза среды развертывания (файлу XML) из администратора развертывания, в который вы импортируете эскиз среды развертывания.
- Администратор развертывания, импортирующий определение среды развертывания, должен поддерживать, по крайней мере, все функции, определенные в документе эскиза среды развертывания. Например, вы можете импортировать эскиз среды развертывания, созданный в администраторе развертывания WebSphere Enterprise Service Bus, в администратор развертывания Process Server, но не наоборот.

Примечание: Если включены защита и проверка прав доступа на основе ролей, то вы должны войти в административную консоль как администратор, чтобы выполнить эту задачу.

Важное замечание: Импортировать одновременно несколько документов эскиза среды развертывания из сжатого файла нельзя. Вы должны извлечь документы эскиза из сжатого файла, а затем импортировать файлы XML по одному.

Перед запуском процесса конфигурации необходимо настроить автоматическую синхронизацию изменений узлов (в административной консоли выберите **Администрирование системы > Параметры консоли**, затем выберите **Синхронизировать изменения с узлами**). В противном случае потребуется вручную синхронизировать изменения после каждого шага.

Импортирование существующего эскиза среды развертывания для создания нового позволяет минимизировать время, затрачиваемое на настройку среды развертывания. Если существующая среда схожа с той, которую вы хотите создать, то экспортируйте и затем импортируйте ее в настраиваемый администратор развертывания.

1. В административной консоли выберите **Серверы > Среда развертывания**.
2. Выберите **Импорт** на странице Среда развертывания, чтобы запустить мастер Настройка среды развертывания.

Мастер будет запущен с выбранной опцией **Создать среду развертывания на основе импортированного эскиза**.

3. Нажмите **Обзор** и выберите документ эскиза среды развертывания (файл XML) для импорта или введите полный путь к нему.
4. Нажмите **Далее**, чтобы загрузить конфигурацию и запустить мастер Импортировать среду развертывания.

Мастер покажет страницу **Выбрать узлы**, за исключением случая, когда все имена узлов соответствуют текущим объединенным узлам. В последнем случае мастер покажет страницу **База данных**.

Важное замечание: При нажатии кнопки **Настроить** в любой панели мастера среда развертывания будет настроена с текущими значениями.

5. Необязательно: В списке возможных узлов на странице **Выбрать узлы** выберите узлы, которые следует включить в среду развертывания, и нажмите **Далее**.

Для выбора узла отметьте переключатель рядом с его именем.

Важное замечание: Кнопка **Далее** недоступна, если выбранные узлы не отвечают ограничениями, налагаемым импортированным эскизом среды развертывания. Например, если среда развертывания должна содержать узел “Mandatory_Node” и еще три узла с произвольными именами, то вы не сможете продолжить, пока не выберете “Mandatory_Node” и три других узла.

6. На странице Кластеры назначьте по крайней мере один элемент кластера, принадлежащий по крайней мере одному узлу, каждой функции среды развертывания.

По умолчанию на каждом узле каждой функции назначается один участник кластера. Для изменения номера замените его в каждом столбце. В случае сетевого развертывания кластеры могут взаимодействовать, предоставляя дополнительные возможности в среде. В зависимости от требований, вы назначаете конкретные функции каждому кластеру в среде развертывания для обеспечения производительности, переключения при сбое и емкости.

Нулевое значение для узла означает, что узел не дает вклада в выбранную функцию, на основе выбранных вами компонентов.

Каждой функции должен быть присвоен по крайней мере один элемент кластера. В случае сред высокой готовности и переключения при сбое выберите по крайней мере два узла для каждой функции. Для обеспечения более высокого уровня масштабируемости укажите большее число элементов кластера для функции.

После присвоения элементов кластера нажмите кнопку **Далее** для перехода на страницы имен кластеров всех типов. Конкретный набор страниц зависит от выбранного шаблона среды развертывания. Если имена кластеров и их элементов настраивать не требуется, то с помощью панели навигации мастера откройте страницу Службы REST и перейдите к следующему шагу.

- a. Необязательно: Настройте имена кластеров и их элементов. На странице Имена кластеров укажите имена кластеров и элементов кластеров. Кроме того, можно изменить краткие имена кластеров и их элементов. Для каждого типа кластеров из выбранного шаблона предусмотрена отдельная страница. Ниже приведено описание страниц:

Поле	Описание	Значение
Кластер	Доступное только для чтения поле, в котором указана функциональная роль кластера.	<p>Значение зависит от типа кластера:</p> <ul style="list-style-type: none"> • Среда развертывания приложений • Вспомогательная инфраструктура • Инфраструктура обмена сообщениями • Инфраструктура веб-приложения <p>Дополнительная информация о функциональной роли каждого типа кластеров приведена в разделе "Типы топологий и шаблоны среды развертывания".</p>

Поле	Описание	Значение
Имя кластера	Создаваемое системой имя элемента кластера по умолчанию.	Значения по умолчанию определяются в соответствии со следующим соглашением: <i>имя среды развертывания.имя типа кластера</i> , где <i>имя типа кластера</i> может принимать одно из следующих значений: <ul style="list-style-type: none"> • AppTarget - Для целевых кластеров развертывания приложений. • Messaging - Для кластеров, выполняющих роль инфраструктуры обмена сообщениями. • Support - Для кластеров, выполняющих роль вспомогательной инфраструктуры. • Web - Для кластеров, выполняющих роль вспомогательных веб-приложений.
Имя элемента кластера	Создаваемое системой имя элемента кластера по умолчанию. Серверы, входящие в состав кластера, называются элементами кластера.	Примите значение по умолчанию, созданное системой, или укажите собственное имя. Имя элемента кластера по умолчанию определяются в соответствии со следующим соглашением: <i>имя-кластера.имя-узла.порядковый-номер-узла</i> . Число имен элементов кластера, показанных в таблице, совпадает с числом элементов, указанным в столбце типа кластера и строке узла на странице Кластеры.

7. На странице Конечные точки службы REST системы настройте конечные точки служб для API Representational State Transfer (REST).

Если вы хотите, чтобы в Business Space были доступны виджеты, то необходимо настроить конечные точки служб REST для этих виджетов. При выборе имени хоста и порта, если вы хотите, чтобы запросы REST направлялись напрямую на конкретный сервер приложений, то укажите имя хоста и порт этого сервера приложений. Если вы хотите, чтобы запросы REST направлялись на сервер проху или HTTP, расположенный перед одним или несколькими серверами приложений, то укажите имя хоста и порт этого сервера проху или HTTP. Во втором случае сервер проху или HTTP должен быть уже настроен. Если это условие не выполнено, пропустите эту страницу и настройте конечные точки позже.

- a. Настройте полный URL ко всем службам REST, выбрав **https://** или **http://** в списке **Протокол**.

- b. Введите имя сервера Proxu или HTTP в поле **Имя хоста или виртуальный хост в сбалансированной среде**.

Укажите имя хоста или виртуального хоста и номер порта для взаимодействия клиента с сервером или кластером. В кластерной среде, как правило, указывается имя хоста и номер порта распределителя нагрузки. Если оставить эти поля пустыми, то по умолчанию будут использоваться имя хоста и номер порта HTTP элемента кластера. В среде с распределением нагрузки значения по умолчанию впоследствии необходимо изменить на имя виртуального хоста и номер порта распределителя нагрузки. Убедитесь, что указано полное имя хоста.

- c. В поле **Порт** введите порт для подключения клиента к серверу или кластеру.
 - d. В таблице служб REST, если вы хотите изменить описание конечной точки службы REST, замените запись в поле Описание. Остальные поля предназначены только для чтения.
 - e. Нажмите **Далее** для перехода к странице Импортировать конфигурацию базы данных.
8. Необязательно: На странице Импортировать конфигурацию базы данных нажмите **Обзор**, чтобы перейти к документу структуры базы данных, или введите путь к документу структуры базы данных и затем нажмите **Далее** для перехода к странице Источники данных. Если вы импортируете документ структуры, то его содержимое отображается на странице База данных мастера. Документ структуры можно создать на основе структуры базы данных, созданной с помощью инструмента проектирования баз данных, или на основе шаблона с выбранными функциями.
9. На странице База данных настройте параметры базы данных для источников данных среды развертывания, затем нажмите **Далее** для перехода к странице Защита.

На этой странице определите информацию базы данных для компонентов, включенных в эту среду развертывания. Везде, где это возможно, мастер предложит значения по умолчанию для параметров, однако вы должны изменить эти значения на те, которые вы определили при планировании среды. При смене провайдеров вы можете нажать кнопку **Изменить провайдер** и отредактировать выбранный провайдер.

Примечание: Если вы импортировали документ структуры базы данных, то информация на странице База данных отражает конфигурацию источника данных согласно этому импортированному документу. Изменения, внесенные в конфигурацию источника данных после импорта документа структуры базы данных, могут быть несовместимы с файлом DDL, созданным инструментом проектирования базы данных и исходными значениями.

Будет ли на этом шаге показан быстрый путь настройки среды развертывания - зависит от нескольких факторов. Такой путь будет показан, если определено несколько баз данных.

Этот путь отображается всегда, когда вы используете провайдер базы данных DB2 для z/OS или Oracle .

Компонент IBM Business Monitor предлагает следующие записи:

Компонент	Источник данных
Источник данных для службы сообщений Business Monitor	Источник данных для службы сообщений IBM Business Monitor.
Хранилище материалов Cognos	Источник данных для хранилища материалов IBM Cognos Business Intelligence. (Отображается только в том случае, если IBM Cognos BI установлен, но не настроен.)

Компонент	Источник данных
Business Space	Источник данных для компонента Business Space. Опция Создать таблицы недоступна для этого компонента. Если среда развертывания содержит компонент Business Space, то таблицы для него необходимо создать вручную.

Если для топологии выбраны другие компоненты продукта, то могут быть показаны дополнительные записи.

Имена схем по умолчанию, показанные на этой странице, могут противоречить соглашению об именах вашего сайта или существующим схемам. По этой причине может потребоваться изменить имя схемы.

Примечание: Базы данных DB2 для z/OS: В качестве значения SQLID DB2 z/OS применяется имя схемы, указанное на панели. При необходимости после завершения работы мастера среды развертывания можно вручную изменить пользовательское свойство currentSQLID созданных источников данных источники, указав другое значение SQLID DB2 z/OS.

Вы можете изменять все ключевые параметры, например, имя базы данных, опцию создания таблиц, имя пользователя среды выполнения источника данных и имя пользователя и пароль для подключения источника данных к базе данных.

Примечание: Базы данных DB2 для z/OS: В качестве имени базы данных применяется имя подсистемы базы данных. Для других версий DB2 применяется имя базы данных MONITOR. Базы данных Oracle: В качестве имени базы данных применяется ИД системы Oracle.

Вы можете выбрать, какую базу данных следует использовать для заданного компонента.

Опция **Создать таблицы** недоступна, если используется провайдер базы данных DB2 для z/OS или Oracle.

Если вы применяете Oracle, то поле **Схема** будет недоступно и пусто, а поле **Имя пользователя** не будет заранее заполняться общим именем пользователя базы данных. Вы должны ввести имя пользователя и пароль для каждого источника данных.

Примечание: Уникальность имен пользователей не контролируется; появление одинаковых имен может вызвать конфликты таблиц.

- На странице Защита введите идентификационные данные пользователей, необходимые для настройки компонентов IBM Business Monitor. Компонент IBM Business Monitor предлагает следующие записи:

Компонент	ИД и пароль
Псевдоним идентификации для ресурсов JMS службы событий CEI	Укажите идентификационные данные пользователя для защиты шины интеграции служб инфраструктуры событий общего формата (CEI) по умолчанию.
Идентификация доступа к администрированию Cognos	Укажите ИД пользователя и пароль с правами администратора для службы IBM Cognos BI. (Отображается только в том случае, если IBM Cognos BI установлен, но не настроен.)

Если для топологии выбраны другие компоненты продукта, то могут быть показаны дополнительные записи.

- Необязательно: Если откроется страница Business Process Choreographer, то задайте параметры конфигурации Business Process Choreographer и нажмите

кнопку **Далее** для перехода к странице Веб-приложения системы. На этой странице вы указываете значения для следующих параметров:

- Роли защиты
- Псевдонимы проверки подлинности

12. Необязательно: Если откроется страница Веб-приложения системы, то задайте корневой контекст для веб-приложений, основанных на компонентах, в среде развертывания или примите системные значения по умолчанию для корневых контекстов. Затем нажмите **Далее** для просмотра страницы Сводка.

Таблица содержит следующую управляющую информацию.

Web-приложение

Имя web-приложения.

Некоторые из компонентов, входящих в создаваемую среду развертывания, содержат Web-приложения. Столбец **Web-приложение** может содержать следующие компоненты:

- Business Process Choreographer Explorer
- Business Space
- Администратор бизнес-правил

Корневой контекст

Текущее значение корневого контекста для компонента.

По умолчанию применяется корневой контекст по умолчанию для Web-приложения. Вы можете изменить корневые контексты, введя значение в поле **Корневой контекст**.

Примечание: Корневой контекст Business Space доступен только для чтения и не может быть изменен.

13. Убедитесь, что информация на странице Сводка верна, и нажмите **Закончить и создать среду**, чтобы закончить создание и сохранить конфигурацию среды развертывания. Для того чтобы выйти из сеанса, не завершив создание конфигурации, нажмите **Готово**.

Нажатие **Готово** сохраняет конфигурацию среды развертывания, но не создает ее.

Нажатие **Отмена** отменяет создание конфигурации среды развертывания и не сохраняет ее.

14. В случае создания среды развертывания с помощью кнопки **Завершить и создать среду** необходимо остановить и перезапустить все кластеры и узлы, а также администратор развертывания.

Если на последней странице мастера среды развертывания вместо кнопки **Готова** нажата кнопка **Закончить и создать среду** (среда не создается), то для просмотра конфигурации среды развертывания выберите **Сервер > Среда развертывания > имя среды развертывания**. На этой странице предусмотрена кнопка **Создать**, позволяющая создать среду. Закончив создание конфигурации, просмотрите файлы конфигурации, чтобы проверить внесенные изменения.

Либо сохраните изменения в главной конфигурации, либо аннулируйте их. Если вы выполнили не все необходимые шаги по настройке, то при щелчке на среде развертывания появится список отложенных шагов. После создания среды развертывания необходимо остановить и перезапустить все кластеры, узлы и администратор развертывания.

Создание среды разработки с помощью пользовательской топологии

Вместо использования одного из предоставляемых шаблонов среды развертывания можно настроить собственные кластеры и настроить компоненты IBM Business Monitor в топологии сетевого развертывания (ND).

Перед созданием кластеров и настройкой компонентов IBM Business Monitor должны быть выполнены следующие задачи:

- Установлен IBM Business Monitor.
- Создан профайл администратора развертывания IBM Business Monitor или расширен существующий профайл администратора развертывания для поддержки IBM Business Monitor.
- Создана база данных MONITOR.
- Запущен администратор развертывания.
- Создан и объединен по крайней мере один пользовательский профайл IBM Business Monitor или расширен существующий пользовательский профайл для поддержки IBM Business Monitor.
- Запущен пользовательский профайл или профайлы.

Следующие инструкции указывают, как создать кластеры, настроить службу событий Инфраструктуры событий общего формата (CEI) и настроить необходимые компоненты с помощью мастера настройки или команд wsadmin.

Создание кластеров IBM Business Monitor

В среде сетевого развертывания компоненты IBM Business Monitor должны быть развернуты в кластерах.

Перед созданием кластеров и настройкой компонентов IBM Business Monitor должны быть выполнены следующие задачи:

- Установлен IBM Business Monitor.
- Создан профайл администратора развертывания IBM Business Monitor или расширен существующий профайл администратора развертывания для поддержки IBM Business Monitor.
- Создана база данных MONITOR.
- Запущен администратор развертывания.
- Создан и объединен по крайней мере один пользовательский профайл IBM Business Monitor или расширен существующий пользовательский профайл для поддержки IBM Business Monitor.
- Запущен пользовательский профайл или профайлы.

С помощью существующего настраиваемого профайла создайте первый элемент кластера. В каждый создаваемый кластер можно добавлять сколько угодно элементов (см. раздел "Добавление элементов кластера"). Для создания кластера IBM Business Monitor выполните следующие действия с помощью административной консоли:

1. На панели навигации выберите **Серверы > Кластеры > Кластеры сервера приложений WebSphere**.
2. Выберите **Создать** для запуска мастера Создать кластер.
3. Укажите имя кластера.

4. Выберите **Предпочитать локальный** для включения оптимизации маршрутизации в области действия хоста. Эти настройки улучшают производительность путем просмотра EJB в элементе кластера в том же узле, если это возможно.
5. Нажмите кнопку **Далее** для перехода к шагу Создайте первого участника кластера.
6. Укажите имя первого элемента кластера.
7. Укажите имя узла для первого элемента кластера. Требуется узел IBM Business Monitor.
8. Выберите **Создать элемент с помощью шаблона сервера приложений**.
9. Выберите шаблон сервера приложений, имя которого содержит строку **defaultWBM**, и нажмите кнопку **Далее**.

Важное замечание: Если шаблон с именем defaultWBM отсутствует, то выберите узел, расширенный для поддержки IBM Business Monitor.

Если первый элемент кластера не был создан с помощью шаблона сервера приложений с именем defaultWBM, то среда IBM Business Monitor не будет работать правильным образом и потребуются удалить все существующие элементы кластера и заново создать первый элемент кластера.

10. Нажмите кнопку **Далее** для перехода к шагу Создайте дополнительных участников кластера.
11. Необязательно: Добавьте дополнительные элементы кластера. Для этого выполните следующие действия для каждого элемента:
 - a. Укажите уникальное имя дополнительного элемента. Имя должно быть уникальным в пределах узла.
 - b. Укажите имя узла для дополнительного элемента кластера. Требуется узел IBM Business Monitor.
 - c. Выберите **Добавить участника**.
12. Нажмите кнопку **Далее** для перехода на панель обзора.
13. Проверьте информацию и нажмите **Готово**.
14. Нажмите **Сохранить**, чтобы сохранить изменения в главном файле конфигурации.

После первичного создания кластера можно добавить дополнительный элемент кластера в любое время.

Для первого запуска после установки службы IBM Cognos Business Intelligence запустите каждый сервер по-отдельности. Не используйте опцию ripplestart, так как она не обеспечивает достаточно времени для инициализации IBM Cognos BI.

Административная консоль может сообщить о неполадках при первом запуске сервера IBM Cognos Business Intelligence. Инициализация каждого экземпляра сервера в базе данных хранилища материалов IBM Cognos Business Intelligence и области диска происходит гораздо дольше, чем обычный запуск IBM Cognos Business Intelligence.

Добавление элементов кластера

В существующий кластер можно добавить произвольное число элементов.

Важное замечание: Если первый элемент кластера не был создан с помощью шаблона сервера приложений с именем defaultWBM, то среда IBM Business Monitor не будет работать правильным образом и потребуются удалить все существующие элементы кластера и заново создать первый элемент кластера.

Для создания дополнительных элементов кластера выполните следующие действия:

1. На панели навигации выберите **Серверы > Кластеры > Кластеры серверов приложений WebSphere > имя-кластера > Элементы кластера**.
2. Выберите **Создать** для запуска мастера Создать новых участников кластера.
3. Для каждого нового элемента кластера выполните следующие действия:
 - a. Укажите уникальное имя дополнительного элемента. Имя должно быть уникальным в пределах узла.
 - b. Укажите имя узла для дополнительного элемента кластера. Требуется узел IBM Business Monitor.
 - c. Выберите **Добавить участника**.
4. Нажмите кнопку **Далее** для перехода на панель обзора.
5. Проверьте информацию и нажмите **Готово**.
6. Нажмите **Сохранить**, чтобы сохранить изменения в главном файле конфигурации.

Примечание: Во время установки IBM Business Monitor служба Cognos также устанавливается на узле и будет настроена на новом сервере при добавлении некоторого элемента в кластер.

Объединение дополнительных узлов

После создания среды высокой готовности можно объединить дополнительные узлы в ячейку.

Важное замечание: IBM Business Monitor не поддерживает сводные панели на основе портала в той же ячейке, что и сервер IBM Business Monitor v7.5.

Для того чтобы объединить существующие узлы в диспетчер развертывания, выполните следующие действия для каждого узла:

1. Запустите администратор развертывания.
2. Из каталога профайла встраиваемого узла выполните команду **addNode**, указав имя хоста администратора развертывания и порт коннектора SOAP администратора развертывания (необязательно).

```
profile_root\bin\addNode.bat имя-хоста-dmgr [порт-soap-dmgr]  
profile_root/bin/addNode.sh dmgr_host_name [dmgr_soap_port]
```

Для запуска этой команды с включенной трассировкой воспользуйтесь опцией **-trace**; например: `addNode имя-хоста -trace`

Для получения дополнительных деталей по запуску команды **Добавить узел** обратитесь в информационный центр WebSphere Application Server.

Настройка служб событий CEI

Перед настройкой компонентов IBM Business Monitor с помощью административной консоли в ячейке сетевого развертывания необходимо создать службу инфраструктуры обработки событий общего формата (CEI), которую IBM Business Monitor может использовать для отправки событий. Эту же службу событий CEI можно также использовать для получения событий.

Служба событий CEI автоматически создается вместе с автономным профайлом для IBM Business Monitor, а также в случае использования мастера настройки среды развертывания. В случае добавления IBM Business Monitor в топологию Process Server допустимо применения службы событий CEI, развернутой с помощью Process Server для IBM Business Monitor. В противном случае, следуйте инструкциям, приведенным на данной странице, для создания новой службы событий CEI.

Команда **wbmDeployCEIEventService** используется для установки службы событий CEI на сервере или в кластере и для создания необходимых для нее ресурсов (шина интеграции служб и служба сообщений). Можно также настроить защиту и включить хранилище данных службы событий CEI по умолчанию, если требуется. (Хранилище данных службы событий не рекомендуется применять в рабочих средах.) В базовой топологии для высокого коэффициента готовности служба событий CEI установлена в кластере поддержки.

Для того чтобы установить и настроить новую службу событий CEI, выполните следующие действия:

1. Откройте командную строку и перейдите в каталог `bin` профайла диспетчера развертывания (по умолчанию `DMGR01`), в котором установлен WebSphere Application Server, или в каталог `bin` автономного профайла в среде с одним сервером.
2. Запустите `wsadmin` с помощью следующей команды:
 - `wsadmin.sh`
 - `wsadmin.bat`
3. Выполните команду **wbmDeployCEIEventService**. Для этого введите в командной строке:

```
(jac1) $AdminTask wbmDeployCEIEventService {-interactive}
(jython) AdminTask.wbmDeployCEIEventService('-interactive')
```

В качестве альтернативы можно выполнить команду, указав все параметры. Для примера используйте связанные ссылки "Настройка компонентов IBM Business Monitor с помощью команд `wsadmin`".

4. Сохраните результаты с помощью следующей команды:

```
(jac1) $AdminConfig save
(jython) AdminConfig.save()
```
5. Для того чтобы синхронизировать узлы, выберите в административной консоли **Администрирование системы > Узлы**, выберите все узлы и нажмите **Полная повторная синхронизация**.
6. Перезапустите Администратор развертывания, чтобы ссылки CEI появились в административной консоли.

Служба событий CEI включена.

Полный список параметров и пример приведены в разделе Служба событий CEI IBM Business Monitor.

Если этап создания хранилища данных не был выполнен при запуске **wbmDeployCEIEventService**, то это можно сделать для службы событий CEI позднее. Инструкции приведены в разделе "Настройка базы данных CEI".

Настройка среды с помощью мастера настройки

Обязательные компоненты среды IBM Business Monitor можно настроить с помощью мастера настройки административной консоли.

Предварительно необходимо выполнить следующие задачи:

- Создайте и объедините по крайней мере один пользовательский профайл IBM Business Monitor или расширьте существующий пользовательский профайл для поддержки IBM Business Monitor (см. раздел "Создание и расширение профайлов").
- Создайте по крайней мере один кластер на основе шаблона сервера приложений `defaultWBM` (см. раздел "Создание кластеров IBM Business Monitor").

- Настройте локальную службу событий CEI, с помощью которой IBM Business Monitor сможет отправлять и принимать события (см. раздел "Настройка служб событий CEI").

Перед запуском процесса конфигурации необходимо настроить автоматическую синхронизацию изменений узлов (в административной консоли выберите **Администрирование системы > Параметры консоли**, затем выберите **Синхронизировать изменения с узлами**). В противном случае потребуется вручную синхронизировать изменения после каждого шага.

Обязательные и дополнительные компоненты можно настроить с помощью раздела настройки IBM Business Monitor административной консоли. За инструкциями по настройке всех компонентов IBM Business Monitor вручную обратитесь к ссылкам на связанную информацию для доступа к информации о соответствующей задаче.

1. На панели навигации выберите **Серверы > Настройка IBM Business Monitor**. Будет показан список обязательных и дополнительных компонентов. Проверьте состояние каждого компонента. Если вы работаете со средой сетевого развертывания и не настроили среду развертывания, то не будет установлен и настроен ни один из компонентов, поэтому следует выполнить оставшиеся действия по их установке и настройке.
2. Настройте службу исходящих событий CEI, выполнив для этого следующие действия. Служба исходящих событий CEI используется для отправки событий из IBM Business Monitor, включая предупреждения. Необходимо настроить фабрику генератора событий, чтобы она указывала на службу исходящих событий CEI.

Важное замечание: Перед настройкой фабрики отправителей событий должна быть создана локальная служба CEI, применяемая IBM Business Monitor для отправки событий. Если необходимо создать локальную службу CEI, получите инструкции в разделе "Настройка служб событий CEI" на стр. 106.

- a. В списке компонентов выберите **Служба исходящих событий CEI**. Будет показано состояние службы исходящих событий CEI и фабрики генератора событий. Если фабрика MonitorEmitterFactory уже существует, в поле состояния будет показано имя службы событий CEI, для работы с которым настроена фабрика генератора. Если вы еще не настроили фабрику генератора, то увидите сообщение "Локальная служба событий CEI существует, но фабрика генератора событий - нет". В этом случае вы должны создать и настроить фабрику генератора.
- b. В разделе **Настроить фабрику генератора событий** выберите сервер или кластер для фабрики генератора событий. В списке показаны все доступные серверы и кластеры. Вы можете выбрать только те серверы, у которых настроена служба событий CEI. (Доступные серверы и кластеры обозначены (*)). Если есть несколько серверов с одинаковым именем, убедитесь в том, что выбран сервер на нужном узле.
- c. Для запуска мастера настройки выберите **Настроить фабрику генератора событий**. Для ячейки будет создана фабрика генератора исходящих событий с именем MonitorEmitterFactory. Поле состояния службы исходящих событий CEI изменится и будет указывать на службу событий CEI, которую использует MonitorEmitterFactory.
- d. Вернитесь на страницу настройки, выбрав **Настройка IBM Business Monitor** в списке путей.

3. Создайте шину интеграции служб и настройте модуль обмена сообщениями, выполнив для этого следующие действия. IBM Business Monitor требует наличия своей собственной шины и модуля обмена сообщениями для возможности отслеживания событий.

Если у вас нет шины, ее можно автоматически создать во время настройки службы сообщений. Шина называется MONITOR.<имя_ячейки>.Bus, и это имя не может быть изменено.

- a. В списке компонентов выберите **Модуль обмена сообщениями**. Будет показано состояние шины интеграции служб и модуля обмена сообщениями.
- b. Для запуска мастера настройки выберите **Настроить модуль обмена сообщениями**.
- c. В панели **Выбрать элемент шины** выберите расположение, в котором должен создаваться модуль обмена сообщениями, и нажмите **Далее**:
 - **Кластер**: Выберите эту опцию для создания модуля обмена сообщениями в существующем кластере. Имя кластера необходимо выбрать из списка.
 - **Сервер**: Выберите эту опцию для создания модуля обмена сообщениями на сервере. Выберите сервер из списка. Если есть несколько серверов с одинаковым именем, убедитесь в том, что выбран сервер на нужном узле.
- d. В панели **Выбрать тип хранилища сообщений** выберите одну из следующих опций и нажмите **Далее**:
 - **Хранилище данных**: Хранилище данных - это хранилище сообщений, содержащее набор таблиц, к которым имеют доступ все участники кластера, в котором находится модуль обмена сообщениями.
 - **Хранилище файлов**: Хранилище файлов - это тип хранилища сообщений, который непосредственно использует файлы в файловой системе посредством операционной системы. Эта опция недоступна, если в панели **Выбрать элемент шины** выбран **Кластер**.
- e. При использовании хранилища данных выберите в панели **Задать свойства хранилища сообщений** одну из следующих опций:
 - **Создайте источник данных по умолчанию с созданным именем JNDI**: По умолчанию для хранилища данных используется имя Derby. Этот параметр недоступен, если выбран параметр **Кластер** на панели **Выбрать участника шины**.
 - **Использовать существующий источник данных**: При выборе этой опции заполните следующие поля:
 - **Имя JNDI источника данных**: Выберите имя JNDI, соответствующее базе данных, с которой планируется работать. Например, jdbc/wbm/MonitorMEDatabase.
 - **Имя схемы**: Введите имя схемы. Например, MONME00.
 - **Псевдоним идентификации**: выберите псевдоним идентификации, который планируется использовать. Необходимо выбрать псевдоним идентификации для создания таблиц. Например, Monitor_JDBC_Alias.
 - **Создать таблицы**: выберите этот параметр для создания таблиц в базе данных. Если этот параметр не выбран, то таблицы должен создать администратор базы данных.
- f. Проверьте информацию в панели **Подтвердить** и нажмите **Готово** для завершения настройки. Поля состояния шины и службы обмена сообщениями будут обновлены с учетом новой информации о конфигурации.

Примечание: Возможно, пройдет некоторое время, прежде чем служба сообщений будет запущена.

- g. Вернитесь на страницу настройки, выбрав **Настройка IBM Business Monitor** в списке путей.
- 4. Убедитесь в том, что шина и служба сообщений имеют правильный ИД пользователя для среды:
 - a. В панели навигации выберите **Защита > Защита шины**.
 - b. Щелкните на шине для сервера IBM Business Monitor. Будет показана страница свойств конфигурации шины.
 - c. В разделе **Дополнительные свойства** выберите **Защита**. Будет показана другая страница свойств.
 - d. В разделе **Стратегия авторизации** щелкните на **Пользователи и группы в роли коннектора шины**.
 - e. Убедитесь в том, что ваш ИД пользователя существует. Если он не существует, выполните следующие действия, чтобы его добавить:
 - 1) Нажмите **Создать**.
 - 2) Выберите **Имя пользователя**, а затем введите новый ИД пользователя в соседнем поле.
 - 3) Нажмите кнопку **ОК**.
- 5. Установите приложение служб действий IBM Business Monitor, выполнив для этого следующие действия. Приложение служб действий вызывает действия, такие как отправка предупреждений сводной панели или рассылка уведомлений по электронной почте, когда оно получает определенные события ситуаций, сгенерированных другими приложениями. События ситуаций обычно указывают на ситуации бизнеса, которые требуют внимания, такие как нехватка бумаги у принтера или достижения исходных параметров определенного значения.
 - a. В списке компонентов выберите **Службы действий**. Будет показано состояние приложения. Если приложение установлено правильно, его расположение отображается в поле состояния.
 - b. В разделе **Развернуть службы действий** выберите из списка сервер или кластер для приложения служб действий. В списке показаны все доступные серверы и кластеры. Необходимо выбрать сервер, на котором установлен IBM Business Monitor. Если есть несколько серверов с одинаковым именем, убедитесь в том, что выбран сервер на нужном узле.
 - c. Для того чтобы установить приложение, выберите **Развернуть службы действий**. Будет установлено приложение и создан профайл группы служб действий монитора. Поле состояние приложения обновится, и в нем будет показано расположение установленного приложения с именем **IBM_WBM_ACTIONSERVICES**. Если это приложение было установлено в кластере, оно будет доступно только после синхронизации всех узлов в кластере.
 - d. Вернитесь на страницу настройки, выбрав **Настройка IBM Business Monitor** в списке путей.
- 6. Установите приложение запланированных служб монитора, выполнив для этого следующие действия. Необходимо установить это приложение для планирования повторяющегося выполнения служб, таких как служба перемещения данных и хронология ключевого индикатора производительности (KPI), для моделей монитора.
 - a. В списке компонентов выберите **Запланированные службы монитора**. Будет показано состояние приложения. Если приложение установлено правильно, его расположение отображается в поле состояния.
 - b. В разделе **Развернуть запланированные службы монитора** выберите из списка сервер или кластер для приложения запланированных служб монитора. В списке показаны все доступные серверы и кластеры. Необходимо выбрать

сервер, на котором установлен IBM Business Monitor. Если есть несколько серверов с одинаковым именем, убедитесь в том, что выбран сервер на нужном узле.

- c. Для того чтобы установить приложение, выберите **Развернуть запланированные службы монитора**. Поле состояние приложения обновится, и в нем будет показано расположение установленного приложения с именем IBM_WBM_DATA_SERVICES. Если это приложение было установлено в кластере, оно будет доступно только после синхронизации всех узлов в кластере.
- d. Вернитесь на страницу настройки, выбрав **Настройка IBM Business Monitor** в списке путей.

Вы можете просмотреть запланированные службы для каждой установленной модели монитора, выбрав **Приложения > Службы монитора > Запланированные службы монитора**.

7. Необязательно: Если для проведения многомерного анализа на сводных панелях планируется использовать службу IBM Cognos Business Intelligence, то в списке компонентов выберите **Служба Cognos**. Будет показано состояние службы. Если служба установлена правильно, ее расположение отображается в поле состояния. (Если служба IBM Cognos BI была установлена с IBM Business Monitor и был создан автономный профайл, то служба IBM Cognos BI уже развернута.)

- a. Для развертывания новой службы IBM Cognos BI выберите сервер или кластер для службы IBM Cognos BI в списке. В списке показаны все доступные серверы и кластеры. (Доступные серверы и кластеры помечены звездочкой (*)). Если есть несколько серверов с одинаковым именем, убедитесь, что выбран сервер на нужном узле.

Укажите имя базы данных, которая должна использоваться для хранилища материалов. В DB2 и Microsoft SQL Server имя базы данных должно отличаться от имени должны быть MONITOR. Введите имя пользователя базы данных и пароль. Если для хранилища материалов используется то же имя пользователя, что и для базы данных MONITOR, необходимо применять такой же пароль. Поскольку пользователь, указанный для работы с базой данных хранилища содержимого, должен обладать правами на создание таблиц в базе данных, рекомендуется создать нового пользователя базы данных только для базы данных хранилища содержимого.

Примечание: Имя пользователя и пароль для базы данных хранилища материалов IBM Cognos BI находятся в Cognos_JDBC_Alias, где хранятся все идентификационные данные базы данных. При каждом запуске сервера IBM Business Monitor IBM Cognos BI текущие значения передаются в конфигурацию IBM Cognos BI для обеспечения доступа IBM Cognos BI к хранилищу материалов. Такая интеграция не позволяет изменять имя пользователя и пароль хранилища материалов с помощью приложения Настройка IBM Cognos BI.

Если административная защита включена, необходимо указать имя и пароль администратора IBM Cognos BI.

Нажмите **Развернуть службу Cognos**. Поле состояние обновится, и в нем будет показано расположение установленной службы. Если эта служба была установлена в кластере, то она будет показываться как недоступная, пока не будут синхронизированы и перезапущены все узлы в кластере. Если развертывание займет больше времени, чем предусмотрено тайм-аутом для ответа административной консоли, то будет выведено сообщение о тайм-ауте. Подождите несколько минут, затем попробуйте перезапустить серверы.

- b. Если версия IBM Cognos BI уже установлена, то в опции **Использовать существующую службу Cognos** укажите URI внешнего диспетчера сервера IBM Cognos BI. Этот URI можно найти в клиенте конфигурации IBM Cognos BI в меню **Локальная конфигурация > Среда > Параметры диспетчера** (например, `http://хост:порт/p2pd/servlet/dispatch/ext`). Если административная защита включена на сервере IBM Cognos BI, необходимо указать имя и пароль администратора IBM Cognos BI.
Выберите **Использовать существующую службу Cognos**. Поле состояние обновится, и в нем будет показано расположение установленной службы.
 - c. Вернитесь на страницу настройки, выбрав **Настройка IBM Business Monitor** в списке путей.
8. Необязательно: Если вы планируете использовать сводные панели IBM Business Monitor в мобильных устройствах, необходимо установить приложение, выполнив для этого следующие действия. Если сводные панели не будут использоваться в мобильных устройствах, выполнять эти действия не требуется.
- a. В списке компонентов выберите **Сводные панели для мобильных устройств**. Будет показано состояние приложения. Если приложение установлено правильно, его расположение отображается в поле состояния.
 - b. В разделе **Развернуть сводные панели для мобильных устройств** выберите из списка сервер или кластер для приложения сводных панелей в мобильных устройствах. В списке показаны все доступные серверы и кластеры. Необходимо выбрать сервер, на котором установлен IBM Business Monitor. Если есть несколько серверов с одинаковым именем, убедитесь в том, что выбран сервер на нужном узле.
 - c. Для того чтобы установить приложение, выберите **Развернуть сводные панели для мобильных устройств**. Поле состояние приложения обновится, и в нем будет показано расположение установленного приложения с именем `IBM_WBM_MOBILE_DASHBOARD`. Если это приложение было установлено в кластере, оно будет доступно только после синхронизации всех узлов в кластере.
 - d. Вернитесь на страницу настройки, выбрав **Настройка IBM Business Monitor** в списке путей.
9. Необязательно: Если вы планируете использовать службы генератора событий Службы сообщений Java (JMS) и Передачи репрезентативного состояния (REST), необходимо установить служебные приложения API, выполнив следующие действия. Вместо непосредственного кодирования или генерации Событий общего формата вы можете затем использовать эти службы генератора событий. Вы предоставляете XML события, а службы генератора событий получают его и упаковывают в Событие общего формата, которое может обрабатывать IBM Business Monitor.
- a. В списке компонентов выберите **Службы генератора входящих событий (JMS и REST)**. Будет показано состояние приложений. Если приложения установлены правильно, их расположения отображаются в поле состояния.
 - b. В разделе **Развернуть службы генератора событий** выберите из списка сервер или кластер для приложений. В списке показаны все доступные серверы и кластеры. Необходимо выбрать сервер, на котором установлен IBM Business Monitor. Если есть несколько серверов с одинаковым именем, убедитесь в том, что выбран сервер на нужном узле.
 - c. Для того чтобы установить приложения, выберите **Развернуть службы генератора событий**. Поле состояния приложений обновится, и в нем будут показаны расположения установленных приложений. Если эти приложения были установлены в кластере, они будут доступны только после синхронизации всех узлов в кластере.

- d. Вернитесь на страницу настройки, выбрав **Настройка IBM Business Monitor** в списке путей.
10. Необязательно: Для настройки шлюза служб REST для виджетов Business Space выполните следующие действия.

Примечание: Поскольку шлюз служб REST является совместно используемым компонентом, его нельзя настроить с помощью мастера настройки. Если вы создаете кластеры с помощью мастера настройки среды развертывания или создаете автономный профайл, то шлюз служб REST настраивается автоматически. Шлюз служб REST должен быть развернут и зарегистрирован с Business Space, прежде чем ваш коллектив сможет использовать виджеты в Business Space.

- a. В Административной консоли выберите **Серверы > Типы серверов > Серверы приложений WebSphere** или **Серверы > Кластеры > Кластеры сервера приложений WebSphere**.
 - b. Щелкните на имени сервера или кластера.
 - c. На странице Конфигурация в разделе **Бизнес-интеграция** выберите **Службы REST**.
11. Необязательно: Для настройки Business Space выполните следующие действия.

Примечание: Поскольку Business Space является совместно используемым компонентом, его нельзя настроить с помощью мастера настройки. Если вы создаете кластеры с помощью мастера настройки среды развертывания или создаете автономный профайл, то Business Space настраивается автоматически.

- a. В Административной консоли выберите **Серверы > Типы серверов > Серверы приложений WebSphere** или **Серверы > Кластеры > Кластеры сервера приложений WebSphere**.
 - b. Щелкните на имени сервера или кластера.
 - c. На странице Конфигурация под **Бизнес-интеграция** выберите **Конфигурация Business Space**.
12. После завершения настройки компонентов синхронизируйте узлы. В административной консоли выберите **Администрирование систем > Узлы**, выберите все узлы и нажмите **Полная повторная синхронизация**. Затем остановите и перезапустите все кластеры и серверы.

Для проверки правильности установки и настройки всех приложений выйдите из административной консоли. Затем войдите в административную консоль и выберите **Серверы > Настройка IBM Business Monitor**. Убедитесь, что все элементы заполнены и помечены зеленой галочкой.

Если не был выбран вариант создания таблиц модуля обмена сообщениями или отсутствуют права доступа для их создания, таблицы должны быть созданы вручную администратором базы данных. См. ссылку на связанный раздел "Создание таблиц модуля обмена сообщениями вручную".

Если вы хотите получить события из источника событий CEI, который выполняется на удаленном сервере, необходимо также выполнить настройку между ячейками. Инструкции приведены в разделе "Настройка приема событий".

Настройка среды с помощью команд wsadmin

Вместо использования мастера настройки можно настроить среду IBM Business Monitor с помощью инструмента администрирования командной строки WebSphere (wsadmin).

Следующие команды `wsadmin` требуются для настройки IBM Business Monitor.

Таблица 4. Требуемые команды `wsadmin`

Команда	Назначение
<code>wbmDeployCEIEventService</code>	Создает и настраивает службу событий CEI, которую требует IBM Business Monitor для получения и отправки событий.
<code>wbmConfigureEventEmitterFactory</code>	Настраивает фабрику генератора событий, которую требует IBM Business Monitor для генерации и отправки событий. Эта команда должна выполняться после команды <code>wbmDeployCEIEventService</code> .
<code>wbmDeployMessagingEngine</code>	Устанавливает и настраивает службу обмена сообщениями и шину интеграции служб, требуемые для IBM Business Monitor.
<code>wbmDeployActionServices</code>	Устанавливает приложение служб действий IBM Business Monitor. Это приложение вызывает действия, такие как отправка предупреждений сводной панели или рассылка уведомлений по электронной почте, когда оно получает определенные события ситуаций. Эта команда должна выполняться после команды <code>wbmConfigureEventEmitterFactory</code> .
<code>wbmDeployScheduledServices</code>	Устанавливает приложение запланированных служб монитора, которое планирует повторяющееся выполнение служб, таких как служба перемещения данных и хронология ключевого индикатора производительности (KPI), для моделей монитора.

Следующие команды `wsadmin` являются необязательными.

Таблица 5. Необязательные команды `wsadmin`

Команда	Назначение
<code>wbmDeployCognosService</code> <code>wbmSetCognosDispatcher</code>	Устанавливает новую службу IBM Cognos Business Intelligence для многомерного анализа или подключается к существующей службе IBM Cognos BI.
<code>wbmSetCognosDatabaseUser</code> <code>wbmSetCognosAdminUser</code>	Изменяет пароли для базы данных хранилища материалов и IBM Cognos BI и администратора IBM Cognos BI.
<code>wbmRemoveCognosService</code>	Удаляет службу IBM Cognos BI, установленную с помощью IBM Business Monitor.
<code>wbmDeployDashboardsForMobileDevices</code>	Устанавливает и настраивает приложение, которое требуется для выполнения сводных панелей в переносимых устройствах.

Таблица 5. Необязательные команды *wsadmin* (продолжение)

Команда	Назначение
wbmDeployEventEmitterServices	Устанавливает и настраивает приложения службы генератора событий REST и службы генератора событий JMS. Генератор событий JMS может асинхронно публиковать события XML в очереди Службы сообщений Java (JMS) без оболочки Событий общего формата, так что события XML могут быть помещены в очередь JMS, даже когда службы IBM Business Monitor недоступны. Генератор событий REST может синхронно публиковать события без оболочки Событий общего формата. Пользователь определяет типы данных схемы XML (XSD), которые описывают структуру бизнес-информации, а API REST генерирует и отправляет событие в правильном формате для IBM Business Monitor.
wbmDeployBPMEmitterService	Устанавливает и настраивает приложение службы генератора событий IBM Business Process Manager для использования в IBM BPM.
wbmConfigureQueueBypassDatasource	Создает источник данных, необходимый для включения соединения в обход очереди, когда IBM Business Monitor установлен в другой ячейке, чем сервер CEI.
wbmDeployAlphabloxService wbmCheckAlphabloxInstall wbmRemoveAlphabloxService wbmEnableAlphabloxConfiguration	Разворачивает и настраивает Alphablox.

Для запуска инструмента *wsadmin* выполните следующие действия:

1. Откройте командную строку и перейдите в каталог `bin` профайла диспетчера развертывания (по умолчанию `DMGR01`), в котором установлен WebSphere Application Server, или в каталог `bin` автономного профайла в среде с одним сервером.
2. Запустите *wsadmin*, выполнив одну из следующих команд:
 - `wsadmin.sh -lang jacl -user <имя_пользователя> -password <пароль>`
 - `wsadmin.sh -lang jython -user <имя_пользователя> -password <пароль>`
 - `wsadmin.bat -lang jacl -user <имя_пользователя> -password <пароль>`
 - `wsadmin.bat -lang jython -user <имя_пользователя> -password <пароль>`
3. Выполните необходимые команды. Следующий пример использует Jacl для выполнения команды `wbmConfigureEventEmitterFactory`, а затем сохраняет изменения:


```
$AdminTask wbmConfigureEventEmitterFactory {-cluster firstCluster}
$AdminConfig save
```

В следующем примере используется Jython:

```
AdminTask.wbmConfigureEventEmitterFactory('[-cluster firstCluster]')
AdminConfig.save()
```

4. После выполнения команд сохраните изменения перед выходом из *wsadmin*. Для того чтобы сохранить изменения, используйте следующий синтаксис:

```
(jac1) $AdminConfig save
(jython) AdminConfig.save()
```

5. Синхронизируйте узлы в среде сетевого развертывания. В административной консоли выберите **Администрирование систем > Узлы**, выберите все узлы и нажмите **Полная повторная синхронизация**. Затем остановите и перезапустите все кластеры и серверы.

Интерактивный режим

При использовании административной команды в интерактивном режиме вы проходите цепочку действий вводя данные. Этот процесс предоставляет текстовый мастер, и он похож на мастер в административной консоли. При использовании параметра `-interactive` показывается приглашение для ввода всех значений.

Следующий пример демонстрирует, как использовать этот параметр.

```
(jac1) $AdminTask wbmConfigureEventEmitterFactory {-interactive}
(jython) AdminTask.wbmConfigureEventEmitterFactory('-interactive')
```

С помощью команды `help` можно получить справку по любой административной команде.

```
(jac1) $AdminTask help wbmConfigureEventEmitterFactory
(jython) print AdminTask.help ('wbmConfigureEventEmitterFactory')
```

Подробное описание команд и их параметров находится в разделе Команды конфигурации (`wsadmin`).

Описание команд Business Space приведено в разделе Команды (сценарии `wsadmin`) для настройки Business Space.

Настройка среды вручную

Настройку среды IBM Business Monitor следует выполнять только с помощью мастера настройки IBM Business Monitor или мастера настройки среды развертывания. Информация данного руководства приведена с целью помочь вам при выполнении более сложных сценариев и устранении неполадок.

Настройка фабрики генератора событий IBM Business Monitor для z/OS

IBM Business Monitor использует службу исходящих событий CEI для создания и отправки событий. Служба событий, в свою очередь, использует фабрику генератора событий, которая требует настройки. Рекомендуется устанавливать фабрику генератора событий с помощью мастера настройки IBM Business Monitor, мастера настройки среды развертывания или задачи `wsadmin`. Настраивать фабрику генератора событий можно и вручную.

В административной консоли администратора развертывания выполните следующие действия:

1. В панели навигации выберите **Интеграция служб > Инфраструктура обработки событий общего формата > Фабрики генератора событий > Стандартная инфраструктура обработки событий общего формата**.
2. В Дополнительных свойствах выберите **Передача службы событий**.
3. В списке **Служба событий** выберите службу событий и нажмите **ОК**.
4. Выберите **Сохранить** для сохранения изменений в главной конфигурации.
5. В панели навигации выберите **Интеграция служб > Инфраструктура обработки событий общего формата > Фабрики генератора событий**.

6. Выберите **ячейка** для **Области**.
7. Нажмите **Создать**.
8. Введите *фабрика* в **Имени**. Где *имя-фабрики* - любое выбранное имя. Например, MonitorEmitterFactory.
9. Введите com/ibm/monitor/MonitorEmitterFactory в **Имя JNDI**.
10. Под **Передача события**:
 - a. Выберите в списке опцию **Поддержка передачи службы событий**.
 - b. В списке в поле **Имя JNDI для передачи службы событий** выберите **Использовать записи ниже**.
 - c. В поле записи под полем **Имя JNDI для передачи службы события** введите одну из следующих опций:
 - Кластер: cell/clusters/*кластер*/com/ibm/events/configuration/bus-transmission/Default
Где:
имя-кластера - это кластер, в котором развернут CEI.
 - Сервер: cell/nodes/*узел*/servers/*сервер*/com/ibm/events/configuration/bus-transmission/Default
Где:
имя-узла - это узел, в котором развернут CEI
имя-сервера - сервер, в котором развернут CEI.
11. Очистите переключатель **Режим совместимости с предыдущим протоколом передачи службы событий**.
12. Нажмите кнопку **ОК** и нажмите кнопку **Сохранить**, чтобы сохранить изменения в главной конфигурации.

Настройка базы данных инфраструктуры обработки событий общего формата (CEI)

Базу данных инфраструктуры обработки событий общего формата (CEI) можно настроить вручную и использовать функциональные возможности CEI для IBM Business Monitor.

В этом разделе описывается процедура настройки базы данных CEI для использования с IBM Business Monitor.

IBM Business Monitor не требует базы данных CEI, и она не рекомендуется, поскольку она неэффективна при обработке событий IBM Business Monitor. Используйте запись и воспроизведение событий.

1. Для создания хранилища данных службы событий CEI выполните соответствующую команду:
 - Команда configEventServiceDB2DB
 - Команда configEventServiceDB2ZOSDB
 - Команда configEventServiceOracleDB
 - Команда configEventServiceSQLServerDB

Важное замечание: Не создавайте хранилище данных служб событий для рабочих сред, поскольку производительность хранимых событий может ухудшиться.

2. После создания сценариев базы данных сохраните изменения с помощью \$AdminConfig save. Помимо сценариев базы данных, команды создают ресурсы JDBC для использования службой событий CEI.

3. Скопируйте созданные сценарии на сервер базы данных. Расположение каталога сценариев зависит от области, в которой развернута CEI. Расположением по умолчанию для сценариев является один из следующих каталогов (в зависимости от области, в которой развернута CEI):

```
profile_root/databases/event/<кластер>/dbscripts/<тип-базы-данных>  
profile_root/databases/event/<узел>/<сервер>/dbscripts/<тип-базы-  
данных>
```

where

profile_root - это каталог профайла для профайла администратора развертывания

имя-кластера — кластер, в котором развернута CEI

имя-узла — узел, в котором развернута CEI

имя-сервера — сервер, на котором развернута CEI

тип-базы-данных — каталог для вашей базы данных, например db2 или oracle

4. Войдите на сервер базы данных как пользователь с правами чтения и записи в базу данных. Откройте командную строку и инициализируйте интерфейс командной строки для программного обеспечения базы данных. Для создания базы данных событий выполните сценарий для соответствующего типа базы данных (например, `cr_event_db2 server <db2_user>`).

Также необходимо создать таблицы служб сообщений для CEI. Ссылки на связанную информацию приведены в разделе "Создание таблиц службы сообщений вручную".

Установка приложения служб действий IBM Business Monitor

Приложение служб действий IBM Business Monitor вызывает действия, такие как отправка предупреждений сводной панели или рассылка уведомлений по электронной почте, когда оно получает определенные события ситуаций, сгенерированных IBM Business Monitor и другими приложениями. События ситуаций обычно указывают на ситуации бизнеса, которые требуют внимания, такие как нехватка бумаги у принтера или достижения исходных параметров определенного значения.

Перед установкой `monactionmgr.ear` необходимо включить CEI и службу стартовых EJB на том сервере, где устанавливается приложение служб действий.

Для установки приложения служб действий выполните следующие действия с помощью административной консоли:

1. На панели навигации выберите **Приложения > Типы приложений > Приложения J2EE для WebSphere**.
2. Нажмите кнопку **Установить**.
3. Выберите одну из следующих опций для **Путь к новому приложению**:
 - **Локальная файловая система**: выберите эту опцию, если файл находится в локальной файловой системе.
 - **Удаленная файловая система**: выберите эту опцию при обращении к административной консоли с помощью Web-браузера в другой системе.
4. Нажмите **Обзор**, выберите файл `monactionmgr.ear` и нажмите **Далее**. После установки файлы EAR расположены в следующих каталогах:
каталог-`monitor/installableApps.wbm`

Где:

каталог-`monitor` - это каталог, в котором установлен IBM Business Monitor

5. На панели выбор опций установки выберите **Далее**.

6. На панели Отобразить модули на сервер выберите *имя-сервера* или *имя-кластера*, где необходимо установить приложение.
7. Выберите переключатели для строк, соответствующих модулям, и нажмите **Применить**.
8. Нажмите кнопку **Далее**.
9. Проверьте информацию и нажмите **Готово**.

Создание профайла группы служб действий монитора

После установки приложения Службы действий монитора необходимо создать профайл группы событий для приема событий.

Перед тем, как приступить к выполнению этой задачи, выполните следующие действия:

- Установить приложение Службы действий монитора
- Настроить службы событий Инфраструктуры обработки событий общего формата (CEI) для IBM Business Monitor
- Запустить и установить администратор

С помощью административной консоли выполните следующие шаги для создания группового профайла события:

1. В панели навигации выберите **Интеграция служб > Инфраструктура обработки событий общего формата > Служба событий**.
2. В Дополнительных свойствах выберите **Службы событий**.
3. Выберите **Сервер по умолчанию Инфраструктуры обработки событий общего формата**.
4. В Дополнительных свойствах выберите **Группы событий**.
5. Нажмите **Создать**.
6. Введите Групповой профайл служб действий для **Имени группы событий**.
7. Введите `CommonBaseEvent[extendedDataElements/@name = 'BusinessSituationName']` для **Строки выбора события**.
8. Выберите **Применить**.
9. В Дополнительных свойствах выберите **Очереди распределений**.
10. Нажмите **Создать**.
11. Выберите `jms/ActionManager/queue` в выпадающем списке **Имя JNDI очереди**.
12. Выберите `jms/ActionManager/QueueConnFactory` в **Имени JNDI фабрики соединений очереди**.
13. Выберите **Применить**.
14. Выберите **Сохранить** для сохранения изменений в главной конфигурации.

Установка запланированных служб монитора

Приложение запланированных служб монитора поддерживает несколько служб, часть из которых оптимизирует производительность или используется для базовой обработки. Его можно настроить на административной консоли WebSphere Application Server. Необходимо установить это приложение для планирования повторяющегося выполнения служб, таких как служба перемещения данных и хронология ключевого индикатора производительности (KPI), для моделей монитора.

Для установки приложения запланированных служб монитора выполните следующее:

1. На панели навигации выберите **Приложения > Типы приложений > Приложения J2EE для WebSphere**.

2. Нажмите кнопку **Установить**.
3. Выберите одну из следующих опций для **Путь к новому приложению**:
 - **Локальная файловая система**: выберите эту опцию, если файл находится в локальной файловой системе.
 - **Удаленная файловая система**: выберите эту опцию при обращении к административной консоли с помощью Web-браузера в другой системе.
4. Нажмите **Обзор**, выберите файл MonitorDataServices.ear и нажмите **Далее**. После установки файлы EAR расположены в следующих каталогах:
 каталог-monitor/installableApps.wbm
 Где:
 каталог-monitor - это каталог, в котором установлен IBM Business Monitor
5. На панели выбор опций установки выберите **Далее**.
6. На панели Отобразить модули на сервер выберите *имя-сервера* или *имя-кластера*, где необходимо установить приложение.
7. Выберите переключатели для строк, соответствующих модулям, и нажмите **Применить**.
8. Нажмите кнопку **Далее**.
9. Проверьте информацию и нажмите **Готово**.

В среде сетевого развертывания после установки приложения планируемых служб монитора необходимо создать ресурс планировщика на том же сервере. Следуйте инструкциям в разделе "Создание и настройка ресурса планировщика".

Создание и настройка ресурсов планировщика:

Ресурс планировщика - это компонент, который управляет обработкой планировщика, делегируя работу локальному администратору заданий, который создан в области действия ячейки в процессе установки. В среде автономного сервера ресурс планировщика создается в процессе установки IBM Business Monitor. В среде сетевого развертывания необходимо создать ресурс планировщика на том же сервере или в том же кластере, где находится файл MonitorDataServices.ear. Этот раздел описывает действия по созданию ресурса планировщика с помощью административной консоли.

Сначала необходимо установить планируемые службы монитора, следуя инструкциям по следующей ссылке.

После установки планируемых служб выполните следующие действия, чтобы создать ресурс планировщика для сервера или кластера.

1. На панели навигации административной консоли выберите **Ресурсы > Планировщики**.
2. В поле **Область действия** выберите область действия сервера или кластера. Это должен быть тот же сервер или кластер, на котором находится файл MonitorDataServices.ear.
3. Нажмите кнопку **Создать**.
4. В поле **Имя** введите имя, отображаемое для ресурса, такого как DataServicesScheduler.
5. В поле **Имя JNDI** введите sched/wbm/DataServicesScheduler.
6. Введите краткое описание этого ресурса планировщика.
7. Необязательно. Введите категорию для классификации или группировки ресурсов.

8. В поле **Имя JNDI источника данных** выберите jdbc/wbm/MonitorDatabase.
9. В качестве псевдонима источника данных выберите **Monitor_JDBC_Alias**.
10. В поле **Префикс таблиц** введите префикс сроки для присвоения таблицам планировщика, включая схему базы данных. Этот префикс используется для различения планировщиков, что позволяет им совместно использовать одну базу данных. В типичной среде монитора этот префикс должен совпадать с префиксом, использованным в DDL установки монитора: <ИМЯ-СХЕМЫ-МОНИТОРА>.MONSCHED_, например, MONITOR.MONSCHED_</ИМЯ-СХЕМЫ-МОНИТОРА>.
11. В поле **Интервал опроса** укажите время в секундах опроса планировщиком базы данных. Для IBM Business Monitor рекомендуется использовать значение от 30 до 60 секунд.
12. В поле **Имя JNDI администратора заданий** выберите администратор заданий, **wm/wbm/DataServicesWorkManager**.
13. Для того чтобы включить административную защиту, разрешая доступ только администраторам, выберите **Использовать роли администратора**.
14. Нажмите **ОК** для сохранения этого планировщика.

Установка сводных панелей на мобильных устройствах

Сводные панели IBM Business Monitor можно использовать в мобильных устройствах. Приложение необходимо установить с помощью административной консоли WebSphere Application Server.

Для установки сводных панелей для мобильных устройств выполните следующие действия:

1. На панели навигации выберите **Приложения > Типы приложений > Приложения J2EE для WebSphere**.
2. Нажмите кнопку **Установить**.
3. Выберите одну из следующих опций для **Путь к новому приложению**:
 - **Локальная файловая система**: выберите эту опцию, если файл находится в локальной файловой системе.
 - **Удаленная файловая система**: выберите эту опцию при обращении к административной консоли с помощью Web-браузера в другой системе.
4. Нажмите **Обзор**, выберите файл MobileDashboard.ear и нажмите **Далее**. После установки файлы EAR расположены в следующих каталогах:
каталог-monitor/installableApps.wbm

Где:

каталог-monitor - это каталог, в котором установлен IBM Business Monitor

5. На панели выбор опций установки выберите **Далее**.
6. На панели Отобразить модули на сервер выберите **имя-сервера** или **имя-кластера**, где необходимо установить приложение.
7. Выберите переключатели для строк, соответствующих модулям, и нажмите **Применить**.
8. Нажмите кнопку **Далее**.
9. Проверьте информацию и нажмите **Готово**.

После установки приложения и моделей монитора можно подключиться к сводной панели через мобильное устройство используя следующий Web-адрес:

<http://имя-хоста:номер-порта/mobile>

Где:

имя-хоста - полное имя или IP-адрес сервера, на котором установлено приложение

номер-порта - стандартный порт приложений IBM Business Monitor

Для обеспечения правильной работы сводных панелей на мобильных устройствах необходимо настроить Business Space. Для настройки Business Space необходимо выполнить такие задачи, как включение виджетов и настройка служб REST.

Установка служб генератора событий

Можно вручную установить службы генератора событий, которые используются в IBM Business Monitor. Прежде чем вручную устанавливать службы генератора событий, необходимо создать для них ресурсы.

Создание ресурсов для устанавливаемых вручную служб генератора событий:

Прежде чем вручную устанавливать службы генератора событий, необходимо создать ресурсы. Если вы не пользуетесь мастером настройки для установки служб генератора событий или развертываете несколько экземпляров таких служб для повышения производительности, то вы должны вручную создать все необходимые ресурсы для служб генератора событий. См. ссылки на связанную информацию. Для создания необходимых ресурсов можно использовать административную консоль IBM Business Monitor.

Прежде чем приступить к выполнению этой задачи, вы должны создать шину интеграции служб (SIB) IBM Business Monitor. Инструкции см. в ссылке на связанную информацию.

Этот раздел содержит инструкции по созданию следующих обязательных ресурсов:

- Целевая очередь JMS
- Целевая очередь ошибок JMS
- Фабрика соединений очереди ошибок
- Фабрика соединений очереди
- Очередь JMS
- Очередь ошибок JMS
- Спецификация активации
- Фабрика генератора событий для службы генератора событий REST
- Фабрика генератора событий для службы генератора событий JMS

Примечание: Если вы впервые создаете эти ресурсы для генератора событий JMS на сервере (если службы событий не были ранее развернуты вручную на сервере или с помощью мастера настройки), то для упрощения установки служб генератора вы можете выбрать применение имен по умолчанию во всех случаях. В следующих шагах указаны имена по умолчанию. Вы можете повторно использовать уже определенные фабрики генератора событий или создать новые. Создайте отдельные фабрики генератора событий для REST и для JMS.

Воспользуйтесь административной консолью IBM Business Monitor для создания ресурсов и создайте ресурсы в указанном порядке.

1. Для создания целевой очереди JMS выполните следующие действия:
 - a. Выберите **Интеграция служб > Шины** и щелкните на **MONITOR.имя_ячейки.шина**.
 - b. Выберите **Целевые ресурсы > Места назначения** и нажмите **Создать**.

- c. При запуске мастера **создания целевой очереди** убедитесь, что выбрана опция **Очередь**, и нажмите **Далее**.
 - d. Назовите ресурс *MonitorEventEmitterQueue2*. Значение по умолчанию - *MonitorEventEmitterQueue*.
 - e. В качестве описания укажите общее описание очереди. Например: *Очередь генератора событий JMS сервера Business Monitor*. Нажмите кнопку **Далее**.
 - f. Выберите **Узел**, на котором находится элемент шины, и нажмите **Далее** и затем **Готово**.
2. Для создания целевой очереди ошибок JMS повторите шаг 1 на стр. 122. Назовите ресурс *MonitorEventEmitterErrorQueue2*. Значение по умолчанию - *MonitorEventEmitterErrorQueue*. В качестве описания введите *Шина очереди ошибок генератора событий JMS сервера Business Monitor*.
 3. Укажите очередь ошибок в качестве целевой очереди исключительных ситуаций.
 - a. Выберите **Интеграция служб > Шины** и щелкните на **MONITOR.имя_ячейки.шина**.
 - b. Выберите **Целевые ресурсы > Места назначения** и выберите целевую очередь, созданную на шаге 1 на стр. 122.
 - c. В разделе **Место назначения исключительных ситуаций** нажмите кнопку **Указать** и укажите имя очереди ошибок, созданной на шаге 2.
 - d. Нажмите **ОК**, затем **Сохранить**.
 4. Для создания фабрики соединений очереди ошибок выполните следующие действия:
 - a. Выберите **Ресурсы > JMS > Фабрики соединений очереди**.
 - b. Выберите подходящий диапазон для новой фабрики соединений очереди ошибок и нажмите **Создать**.
 - c. Нажмите **ОК**, чтобы принять провайдер службы сообщений по умолчанию.
 - d. На вкладке **Конфигурация** введите **Имя**, **Описание** и **Имя JNDI** для новой фабрики соединений очереди ошибок и выберите **Имя шины**. Нажмите **ОК**, затем **Сохранить**. Просмотрите следующие элементы списка:
 - **Имя:** *MonitorEmitterErrorQConnFactory2*
 - Имя по умолчанию: *MonitorEmitterErrorQConnFactory*
 - **Описание:** *ErrorQConnFactory для очереди генератора событий JMS сервера Business Monitor*
 - **Имя JNDI:** *jms/MonitorEventEmitter/ErrorQConnFactory2*
 - Имя JNDI по умолчанию: *jms/MonitorEventEmitter/ErrorQConnFactory*
 - **Имя шины:** выберите целевую очередь ошибок JMS, созданную на шаге 2.
 - e. Укажите Параметры защиты для защищенной среды и нажмите **Применить**. Псевдоним проверки подлинности для восстановления ХА равен *MonitorBusAuth*. Псевдоним проверки подлинности, управляемый контейнером, равен *MonitorBusAuth*.
 5. Для создания фабрики соединений очереди повторите шаг 4. Воспользуйтесь следующей информацией:
 - **Имя:** *MonitorEmitterQConnFactory2*
 - Имя по умолчанию: *MonitorEmitterQueueConnFactory*
 - **Описание:** *QConnFactory для очереди генератора событий JMS сервера Business Monitor*
 - **Имя JNDI:** *jms/MonitorEventEmitter/QueueConnFactory2*
 - Имя JNDI по умолчанию: *jms/MonitorEventEmitter/QueueConnFactory*
 - **Имя шины:** выберите целевую очередь JMS, созданную на шаге 1 на стр. 122.

6. Для создания очереди JMS выполните следующие действия:
 - a. Выберите **Ресурсы > JMS > Очереди**.
 - b. Выберите подходящий диапазон для новой очереди и нажмите **Создать**.
 - c. Нажмите **ОК**, чтобы принять провайдер службы сообщений по умолчанию.
 - d. На вкладке **Конфигурация** введите **Имя** и **Имя JNDI** для новой очереди, затем выберите **Имя шины** и **Имя очереди**. Выберите **Применить**. Просмотрите следующие элементы списка:
 - **Имя:** *MonitorEventEmitterQueue2*
 - Имя по умолчанию: *MonitorEventEmitterQueue*
 - **Имя JNDI:** *jms/MonitorEventEmitter/Queue2*
 - Имя JNDI по умолчанию: *jms/MonitorEventEmitter/Queue*
 - **Имя шины:** *MONITOR.имя_ячейки.Bus*
 - **Имя очереди:** выберите целевую очередь JMS, созданную на шаге 1 на стр. 122.
7. Для создания очереди ошибок JMS повторите шаг 6. Воспользуйтесь следующей информацией:
 - **Имя:** *MonitorEventEmitterErrorQueue2*
 - Имя по умолчанию: *MonitorEventEmitterErrorQueue*
 - **Имя JNDI:** *jms/MonitorEventEmitter/ErrorQueue2*
 - Имя JNDI по умолчанию: *jms/MonitorEventEmitter/ErrorQueue*
 - **Имя шины:** *MONITOR.имя_ячейки.Bus*
 - **Имя очереди:** выберите целевую очередь ошибок JMS, созданную на шаге 2 на стр. 123.
8. Для создания спецификации активации выполните следующие действия:
 - a. Выберите **Ресурсы > JMS > Спецификации активации**.
 - b. Выберите подходящий диапазон для новой спецификацию активации и нажмите **Создать**.
 - c. Нажмите **ОК**, чтобы принять провайдер службы сообщений по умолчанию.
 - d. На вкладке **Конфигурация** введите **Имя**, **Имя JNDI** и выберите **Имя шины**, **Тип места назначения** и **JNDI места назначения** для новой спецификации активации. Просмотрите следующие элементы списка:
 - **Имя:** *MonitorEventEmitterActivationSpec2*
 - Имя по умолчанию: *MonitorEventEmitterActivationSpec*
 - **Имя JNDI:** *jms/MonitorEventEmitter/ActivationSpec2*
 - Имя JNDI по умолчанию: *jms/MonitorEventEmitter/ActivationSpec*
 - **Имя шины:** *MONITOR.имя_ячейки.Bus*
 - **Тип места назначения:** очередь
 - **JNDI места назначения:** выберите место назначения JMS, созданное на шаге 1 на стр. 122.
 - e. Задайте **Псевдоним проверки подлинности** равным *MonitorBusAuth*. Нажмите **ОК**, затем **Сохранить**.
9. Для создания фабрики генератора событий для службы генератора событий REST выполните следующие действия:
 - a. Выберите **Интеграция служб > Инфраструктура событий общего формата > Фабрики генератора событий**.

- b. Выберите подходящий диапазон для новой фабрики генератора событий и нажмите **Создать**.
 - c. На вкладке **Конфигурация** введите **Имя** и **Имя JNDI** для новой фабрики генератора событий. Нажмите кнопку **Применить**. Просмотрите следующие элементы списка:
 - **Имя:** *EmitterFactoryForREST2*
 - Имя по умолчанию: *EmitterFactoryForREST*
 - **Имя JNDI:** *com/ibm/monitor/EmitterFactoryForREST2*
 - Имя JNDI по умолчанию: *com/ibm/monitor/EmitterFactoryForREST*
 - d. В разделе Передача событий выберите **Поддержка передачи службы событий**, выберите **Использовать нижеуказанную запись** и введите *com/ibm/events/configuration/bus-transmission/Default*.
10. Для создания фабрики генератора событий для службы генератора событий JMS повторите шаг 9 на стр. 124. Нажмите **ОК**, затем **Сохранить**. Просмотрите следующие элементы списка:
 - **Имя:** *EmitterFactory2*
 - Имя JNDI: *com/ibm/monitor/EmitterFactory2*
 - **Имя по умолчанию:** *EmitterFactory*
 - Имя JNDI по умолчанию: *com/ibm/monitor/EmitterFactory*
 11. Перезапустите сервер, чтобы изменения вступили в силу. Если вы создаете ресурсы в среде сетевого развертывания (ND), то перезапустите кластер, в котором были созданы ресурсы.

Установка служб генератора событий вручную:

Вы можете вручную установить службы генератора событий, которые используются в IBM Business Monitor. Когда вы вручную устанавливаете службы генератора событий, вы можете использовать существующие ресурсы или создать ресурсы для служб генератора событий.

Если вы выбрали создание ресурсов для служб генератора событий, то вы должны создать их до того, как приступите к установке вручную службы генератора событий. Инструкции по созданию ресурсов приведены в ссылке на связанную информацию.

Примечание: Для повышения производительности в среде сетевого развертывания (ND) разверните приложение IBM_WBM_EMITTER_SERVICES на том сервере, на котором установлена служба событий Инфраструктуры событий общего формата (CEI). Если вы настроили кластеры, разверните службы генератора в кластере поддержки вместе со службой событий CEI.

Для установки служб генератора событий вручную выполните следующие действия:

1. В административной консоли IBM Business Monitor выберите **Приложения > Типы приложений > Приложения предприятия WebSphere**.

Примечание: Если вы создали ресурсы, как описано в разделе Создание ресурсов для установленных вручную служб генератора, то не забудьте перезапустить сервер, прежде чем развернуть приложение. Если вы создали ресурсы в среде сетевого развертывания, то перезапустите кластер, в котором были созданы ресурсы.

2. Нажмите кнопку **Установить**.
3. Выберите одну из следующих опций для **Путь к новому приложению**:

- **Локальная файловая система:** выберите эту опцию, если файл находится в локальной файловой системе.
 - **Удаленная файловая система:** выберите эту опцию при обращении к административной консоли с помощью Web-браузера в другой системе.
4. Нажмите **Обзор**, выберите файл EmitterServices.eag и нажмите **Далее**. После установки файлы EAR расположены в следующих каталогах:
- каталог-monitor/installableApps.wbm

Где:

каталог-monitor - это каталог, в котором установлен IBM Business Monitor

5. В панели **Выбрать опции установки** выберите **Подробно** и нажмите **Далее**. В следующей панели нажмите **Продолжить**.
6. Если приложение служб генератора было уже развернуто администратором или мастером настройки, создайте уникальное имя для приложения. Например: *IBM_WBM_EMITTER_SERVICES2*.
 - a. В панели **Отобразить модули на сервер** выберите *имя_сервера* или *имя_кластера*, на котором необходимо установить приложение.
7. Выберите переключатели для строк, соответствующих модулям, и нажмите **Применить**.
8. Нажмите кнопку **Далее**.
9. Необязательно: Если вы хотите использовать созданные вами ресурсы и не хотите принимать значения по умолчанию, то вы должны внести изменения в содержимое панели **Связать получатели для объектов EJB, управляемых сообщениями**.
 - a. В поле **Имя JNDI целевого ресурса спецификации активации** укажите имя JNDI, которое вы создали на шаге 8 процедуры **Создание ресурсов для ручную установленных служб генератора**. Значение по умолчанию - *jms/MonitorEventEmitter/ActivationSpec*.
 - b. В поле **Имя JNDI места назначения** укажите имя JNDI очереди JMS (не целевой очереди), созданной на шаге 6 процедуры **Создание ресурсов для ручную установленных служб генератора**. Значение по умолчанию - *jms/MonitorEventEmitter/Queue*.
 - c. Задайте параметр **Псевдоним проверки подлинности ActivationSpec** равным **MonitorBusAuth**.
10. Необязательно: В панели **Отобразить ссылки на ресурсы на сами ресурсы** вы можете указать созданные ресурсы или принять значения по умолчанию. Затем нажмите кнопку **Далее**.
 - a. В панели **Имя JNDI целевого ресурса для EventEmitterMDB** укажите имя JNDI, созданное на шаге 9 процедуры **Создание ресурсов для ручную установленных служб генератора**, или примите значение по умолчанию. Значение по умолчанию - *com/ibm/monitor/EmitterFactory*.
 - b. В панели **Имя JNDI целевого ресурса для EventEmitterREST** укажите имя JNDI, созданное на шаге 9 процедуры **Создание ресурсов для ручную установленных служб генератора**, или примите значение по умолчанию. Значение по умолчанию - *com/ibm/monitor/EmitterFactoryForREST*.

Примечание: После того как вы нажмете **Далее**, вы можете увидеть следующую информацию:

ADMA8019E: ресурсы, назначенные приложению, лежат вне целевого диапазона развертывания. Ресурс попадает в целевой диапазон развертывания, если он определен на уровне ячейки, узла, сервера или приложения, когда целевой

объект развертывания - сервер, или на уровне ячейки, кластера или приложения, когда целевой объект развертывания - кластер. Назначьте ресурсы, попадающие в целевой диапазон развертывания приложения, или подтвердите правильность указанных назначений этих ресурсов.

Эта информация не свидетельствует об ошибке. Нажмите **Продолжить**.

11. Необязательно: Если приложение служб генератора было уже развернуто во время установки продукта или развернуто вручную администратором, присвойте связанному корневому контексту этого приложения уникальное имя.
 - a. В панели Отобразить корневые контексты для Web-модулей присвойте связанному корневому контексту имя `/rest/bpm/events2`. Значение по умолчанию - `/rest/bpm/events`.
12. Этот шаг позволяет отобразить пользователей или группы на роль eventEmitters. Либо, вы можете отобразить всех пользователей, подлинность которых проверена, выбрав роль eventEmitters и нажав **Отобразить специальные субъекты** и затем **Все идентифицированные из области приложения**.
 - a. В панели Отобразить роли защиты в пользователей или группы выберите **Роль eventEmitters**, нажмите **Отобразить специальные субъекты** и затем выберите **Все идентифицированные из области приложения в защищенной среде**. Если защита не включена, выберите **Каждый**.
13. Проверьте информацию и нажмите **Готово**.
14. Выберите **Приложения > Приложения предприятия > IBM_WBM_EMITTER_REST_SERVICES** и нажмите **Запустить**.

Установка служб генератора событий с помощью мастера настройки:

Вы можете воспользоваться мастером настройки для установки служб генератора событий для IBM Business Monitor. См. ссылку на связанную информацию.

Глава 10. Настройка компонентов IBM Business Monitor

После установки IBM Business Monitor можно настроить дополнительные компоненты.

Настройка IBM Cognos BI

Для настройки службы IBM Cognos Business Intelligence на выполнение многомерного анализа в сводных панелях можно настроить новую службу IBM Cognos BI после установки IBM Business Monitor или настроить существующую службу IBM Cognos BI на работу с IBM Business Monitor.

Настройка новой службы IBM Cognos BI

При установке IBM Business Monitor можно по выбору установить новую службу IBM Cognos Business Intelligence. Настроить новую службу IBM Cognos BI можно следующими способами: создать среду развертывания, запустить мастер настройки из административной консоли, использовать команду `wbmDeployCognosService` или настроить автономный профайл в Инструменте управления профайлами. Необходимо также создать базу данных IBM Cognos BI и имя пользователя для хранилища материалов.

Требования к размеру

Для элементов кластера требуется по крайней мере 1 Гб дискового пространства для IBM Cognos BI, так как экземпляр среды выполнения должен быть создан на каждом элементе кластера.

Требования к базе данных

Службе IBM Cognos BI требуется отдельная база данных для хранилища материалов. Базу данных IBM Cognos BI можно создать в ходе настройки автономного профайла или профайла администратора развертывания, с помощью инструмента проектирования базы данных (dbDesignGenerator) или вручную с помощью сценариев, поставляемых вместе с IBM Business Monitor.

Служба IBM Cognos BI при первом запуске создает таблицы в базе данных хранилища содержимого IBM Cognos BI. Поскольку пользователь базы данных, указанный для доступа к базе данных хранилища содержимого, должен обладать правами доступа для создания таблиц в базе данных, рекомендуется создать нового пользователя базы данных, предназначенного только для работы с базой данных хранилища содержимого.

В системах, в которых выполняется сервер IBM Cognos BI, должен быть установлен клиент базы данных. Среда WebSphere должна иметь доступ к клиенту, а клиент должен быть настроен для подключения к базе данных MONITOR. Дополнительная информация приведена в разделе "Особенности баз данных" и в документации по конкретной базе данных.

При первом развертывании IBM Cognos BI предварительно настроенная группа с именем Все принадлежит нескольким встроенным группам и ролям в пространстве имен IBM Cognos BI, включая роль Системные администраторы. Необходимо удалить группу Все из всех встроенных групп и ролей и заменить ее группами, ролями или

пользователями с правами ограничения доступа к программному обеспечению и администрированию IBM Cognos BI.

Режимы разрядности

Все серверы IBM Cognos BI настраиваются на работу в том же режиме разрядности, в котором работает администратор развертывания. Например, если администратор развертывания выполняется на 32-разрядной платформе, то все серверы IBM Cognos BI настраиваются на 32-разрядный режим.

Если необходимо изменить режим разрядности, выполните следующие действия для каждого сервера IBM Cognos BI:

1. В административной консоли выберите **Серверы > Типы серверов > Серверы приложений WebSphere > имя сервера**. Будет показана панель Конфигурация.
2. Выбрав опцию Структура сервера, разверните **Java и Управление процессом** и нажмите **Определение процесса**.
3. В **Дополнительных свойствах** выберите **Входы среды**. Щелкните на **RATN** для каждого сервера и измените параметры пути для переменных среды, чтобы они указывали на верный каталог. Для 32-разрядных систем укажите каталог bin. Для 64-разрядных систем укажите каталог bin64.
4. Синхронизируйте узел и перезапустите сервер.

Настройка существующей службы IBM Cognos BI

Если IBM Cognos Business Intelligence уже установлен, можно использовать существующую службу IBM Cognos BI в IBM Business Monitor. Подключиться к существующей службе IBM Cognos BI можно следующими способами: запустить мастер настройки IBM Business Monitor из административной консоли, выполнить команду **wbmSetCognosDispatcher** или создать автономный профайл в Инструменте управления профайлами. Затем необходимо выполнить некоторые задачи настройки.

После подключения IBM Business Monitor к серверу IBM Cognos BI необходимо выполнить дополнительные действия по настройке Business Space и обработке служб данных.

Важное замечание: Удаленная служба IBM Cognos BI должна выполняться на сервере WebSphere, а когда включена административная защита, пользовательское хранилище должно быть одинаковым на сервере IBM Business Monitor и на сервере IBM Cognos BI.

Убедитесь, что клиент запущен и обладает доступом к базе данных IBM Business Monitor.

Если среда развертывания создана из административной консоли, новый IBM Cognos BI установлен автоматически. Для того чтобы удалить его, выполните команду **wbmRemoveCognosService**.

Для настройки Business Space на работу с существующим сервером IBM Cognos BI выполните следующее:

1. Настройте однократный вход в систему между WebSphere Application Server с Business Space и WebSphere Application Server с IBM Cognos BI. См. раздел Включение однократного входа в систему.
2. Настройте IBM Cognos BI на однократный вход в систему. См. раздел Настройка существующей службы IBM Cognos BI для однократного входа в систему.
3. Обновите следующий файл конечной точки.

установочный-каталог/BusinessSpace/registryData/endpoints/cognosEndpoints.xml В каждом из трех разделов `<tns:url>` укажите имя хоста и номер порта сервера IBM Cognos BI в начале строки.

Например, сервера с именем хоста `1c2d266009.example.com` и номером порта `9080` файл будет выглядеть следующим образом:

```
<tns:Endpoint>
<tns:id>{com.ibm.cognos}cognosServiceRootId</tns:id>
<tns:type>{com.ibm.cognos}cognosServiceRootId</tns:type>
<tns:version>1.0.0.0</tns:version>
<tns:url>http://1c2d266009.example.com:9080/p2pd/servlet/dispatch/ext/</tns:url>
<tns:description>Location of backing services for Cognos widgets</tns:description>
</tns:Endpoint>

<tns:Endpoint>
<tns:id>{com.ibm.cognos}cognosDispatcherRootId</tns:id>
<tns:type>{com.ibm.cognos}cognosDispatcherRootId</tns:type>
<tns:version>1.0.0.0</tns:version>
<tns:url>http://1c2d266009.example.com:9080/p2pd/servlet/dispatch/ext/</tns:url>
<tns:description>Location of Cognos Dispatcher</tns:description>
</tns:Endpoint>

<tns:Endpoint>
<tns:id>{com.ibm.cognos}cognosWebContentRootId</tns:id>
<tns:type>{com.ibm.cognos}cognosWebContentRootId</tns:type>
<tns:version>1.0.0.0</tns:version>
<tns:url>http://1c2d266009.example.com:9080/p2pd/servlet/</tns:url>
<tns:description>Location of Cognos Web content</tns:description>
</tns:Endpoint>
</tns:BusinessSpaceRegistry>
```

Дополнительная информация об изменении файлов конечных точек приведена в разделе Включение виджетов Business Space для сред с несколькими ячейками.




4. Выполните команду **updateBusinessSpaceWidgets** для файла `cognosEndpoints.xml`. Выполните инструкции из раздела Включение виджетов Business Space для сред с несколькими ячейками.

Настройка IBM Cognos BI с WebSphere Portal




При использовании IBM Cognos Business Intelligence с WebSphere Portal необходимо обновить раздел `ProxyServlet_Servlet` файла `web.xml`.

Полная информация о настройке Business Space для работы с WebSphere Portal находится в разделе "Настройка виджетов для работы с WebSphere Portal".


1. Экспортируйте файл архива предприятия (EAR) WebSphere Portal `wps.ear` в соответствии с конфигурацией сети. В кластерной среде файл EAR WebSphere Portal должен быть экспортирован из среды сетевого развертывания WebSphere Application Server.
 - a. В командной строке перейдите в каталог `корневой_каталог_профайла_сервера_приложений/bin`.
 - b. Выполните команду для экспорта файла `wps.ear` во временный каталог (все команды должны быть введены в одной строке):
 - **Windows** `wsadmin.bat -user ИД_администратора -password пароль_администратора -c "$AdminApp export wps каталог/wps.ear"`
 - **Linux** **UNIX** `./wsadmin.sh -user ИД_администратора -password пароль_администратора -c '$AdminApp export wps каталог/wps.ear'`где `ИД_администратора` — это ИД пользователя администратора, `пароль_администратора` — это пароль администратора, а `каталог` — это временный каталог.

2. Создайте подкаталог `/wps_expanded`. С помощью инструмента сценариев **EARExpander** раскройте содержимое экспортированного файла EAR (все команды должны быть введены в одной строке).
 -  `EARExpander.bat -ear каталог\wps.ear -operationDir каталог\wps_expanded -operation expand`
 -   `./EARExpander.sh -ear каталог/wps.ear -operationDir каталог/wps_expanded -operation expand`
3. Создайте резервную копию файла `каталог/wps_expanded/wps.war/WEB-INF/web.xml`.
4. Обновите файл `каталог/wps_expanded/wps.war/WEB-INF/web.xml`.
 - a. Откройте файл `web.xml`.
 - b. Найдите следующий раздел:


```
<servlet id="ProxyServlet_Servlet">
  <servlet-name>ProxyServlet</servlet-name>
  <servlet-class>com.ibm.wps.proxy.servlet.ProxyServlet</servlet-class>
</servlet>
```
 - c. Replace the section with the following text:


```
<servlet id="ProxyServlet_Servlet">
  <servlet-name>ProxyServlet</servlet-name>
  <servlet-class>com.ibm.wps.proxy.servlet.ProxyServlet</servlet-class>
  <init-param>
    <param-name>useCtxPathForCookies</param-name>
    <param-value>true</param-value>
  </init-param>
</servlet>
```
5. Удалите исходный файл `wps.ear` из каталога, в который он был первоначально экспортирован.
6. С помощью команды **EARExpander** сверните каталог файлов EAR обратно в файл EAR.
 -  `EARExpander.bat -ear каталог\wps.ear -operationDir каталог\wps_expanded -operation collapse`
 -   `./EARExpander.sh -ear каталог/wps.ear -operationDir каталог/wps_expanded -operation collapse`
7. С помощью команды `wsadmin` обновите файл EAR WebSphere Portal.

Примечание: Если существует управляемая ячейка (с кластером или без кластера), выполните следующее действие в системе администратора развертывания.

-  `wsadmin.bat -user ИД_администратора -password пароль_администратора -c "$AdminApp install каталог/wps.ear {-update -appname wps -nodeployejb}"`
-   `./wsadmin.sh -user ИД_администратора -password пароль_администратора -c '$AdminApp install каталог/wps.ear {-update -appname wps -nodeployejb}'`

где *ИД_администратора* — это ИД пользователя администратора, *пароль_администратора* — это пароль администратора, а *каталог* — это временный каталог.

8. Перезапустите сервер WebSphere Portal. В конфигурации кластера перезапустите кластер.

Настройка виджетов IBM Business Monitor для WebSphere Portal

IBM Business Monitor более не предоставляет сводных панелей на основе портлетов. Однако, виджеты IBM Business Monitor по-прежнему могут быть показаны в WebSphere Portal.

Для того чтобы показать виджеты в WebSphere Portal, выполните следующие действия:

1. Настройте Business Space.
2. Настройте виджеты для работы с WebSphere Portal.
3. Настройте IBM Cognos Business Intelligence для работы с WebSphere Portal.

Настройка способа получения событий

Можно настроить как поток событий из приложений в инфраструктуру обработки событий общего формата (CEI), так и поток событий из CEI в IBM Business Monitor.

Сведения об асинхронных событиях

Поток из генерирующего приложения в инфраструктуру обработки событий общего формата (CEI) может быть синхронным или асинхронным. В случае синхронной передачи событий приложение ожидает подтверждение успешной доставки события перед продолжением обработки транзакций. При асинхронной передаче событий приложение заносит события в очередь и продолжает работу.

Асинхронная передача событий позволяет повысить эффективность генерирующих приложений, что может иметь большое значение в случае мониторинга критически важных приложений. Однако в случае асинхронной передачи события могут поступать в модель монитора не в том порядке, в котором они возникали в отправляющем приложении.

В моделях, для которых важен порядок событий, ошибочная последовательность событий может приводить к возникновению исключительных ситуаций обработки модели и неправильному вычислению данных. Если важно соблюдать порядок событий, то убедитесь, что приложение отправляет события в IBM Business Monitor в синхронном режиме, или определите путь последовательности событий в модели монитора, чтобы указать информацию о порядке их обработки.

Один из способов выяснить, отправляются ли события асинхронно, - просмотреть административную консоль, выбрав **Интеграция служб > Инфраструктура обработки событий общего формата > Фабрики генератора событий**. Выберите фабрику генератора событий, которая может называться, например, как **Генератор инфраструктуры обработки событий общего формата по умолчанию**. В появившемся меню будет показана область Передача событий с параметрами, управляющими режимом отправки событий. Передача JMS выполняется асинхронно, а передача службы событий - синхронно.

Если вы решите использовать асинхронную передачу событий и важно, чтобы события обрабатывались в порядке их возникновения, то определите путь последовательности событий в модели монитора. Дополнительные сведения о том, как определить пути последовательности событий, приведены в ссылках на связанную информацию.

Настройка проверки прав доступа для асинхронной доставки событий

Если вы планируете получать события от приложения, которое использует фабрику генератора событий с асинхронной доставкой, и не пользовались мастером настройки среды развертывания или административной задачей `wbmDeployCEIEventService` для настройки среды, то вы должны настроить сервер IBM Business Monitor для взаимодействия с сервером Инфраструктуры событий общего формата (CEI).

Если вы настроили среду с помощью мастера настройки среды развертывания или административной задачи `wbmDeployCEIEventService`, то нужная конфигурация уже создана автоматически. Необходимо выполнить эту задачу по настройке информации идентификации только для JMS, если вы настраиваете свой сервер CEI или используете другую фабрику генератора событий, а не генератор инфраструктуры обработки событий общего формата по умолчанию.

Для выполнения этой задачи необходимо войти в административную консоль WebSphere Application Server. Если используется удаленный сервер CEI и метод получения событий на основе очередей, необходимо настроить связь с шиной интеграции служб перед началом выполнения этой задачи. См. связанную задачу "Настройка управления событиями на основе очереди в среде с несколькими ячейками".

Для выполнения процедуры, описанной в этом разделе, вместо административной консоли можно использовать задачу `wsadmin setEventServiceJmsAuthAlias`.

С помощью административной консоли WebSphere Application Server выполните следующие действия:

1. Укажите псевдонимы проверки прав доступа для фабрики соединений очереди.
 - a. На панели навигации выберите **Ресурсы > JMS > Фабрики соединений очереди**.
 - b. Выберите **CommonEventInfrastructure_QueueCF** в списке фабрик соединений очереди.
 - c. В разделе Параметры защиты выберите псевдоним в списке **Псевдоним идентификации для восстановления ХА**. Псевдоним должен быть связан с пользователем, которому присвоена роль коннектора шины CEI. (В окне **Интеграция служб > Шины** выберите столбец **Защита** для шины **Шина CommonEventInfrastructure**.)
 - d. Выберите псевдоним в списке **Псевдоним идентификации, управляемой контейнером**. Как правило, можно выбрать псевдоним, указанный на предыдущем шаге.
 - e. Нажмите **ОК** для сохранения изменений в основной конфигурации.
2. Укажите псевдоним проверки прав доступа для спецификации активации.
 - a. На панели навигации выберите **Ресурсы > JMS > Спецификации активации**.
 - b. Выберите **CommonEventInfrastructure_ActivationSpec** в списке спецификаций активации.
 - c. В разделе Параметры защиты выберите псевдоним в списке **Псевдоним идентификации**.
 - d. Нажмите **ОК** для сохранения изменений в основной конфигурации.
3. Укажите псевдонимы проверки прав доступа для фабрики соединений раздела.
 - a. На панели навигации выберите **Ресурсы > JMS > Фабрики соединений раздела**.
 - b. Выберите **CommonEventInfrastructure_AllEventsTopicCF** в списке фабрик соединений раздела.

- c. В разделе Параметры защиты выберите псевдоним в списке **Псевдоним идентификации для восстановления ХА**. Псевдоним должен быть связан с пользователем, которому присвоена роль коннектора шины CEI. (В окне **Интеграция служб > Шины** выберите столбец **Защита** для шины **Шина CommonEventInfrastructure**.)
- d. Выберите псевдоним в списке **Псевдоним идентификации, управляемой контейнером**. Как правило, можно выбрать псевдоним, указанный на предыдущем шаге.
- e. Нажмите **ОК** для сохранения изменений в основной конфигурации.

Получение событий из CEI

В IBM Business Monitor можно выбрать получение событий с сервера инфраструктуры обработки входящих событий общего формата (CEI) с использованием двух разных типов передачи: JMS (на основе очередей) и передачи посредством таблиц (также называемых обходом очереди).

Доставка событий посредством очередей использует Службу сообщений Java (JMS) для передачи событий из CEI в модель монитора. Доставка событий на основе таблиц (ранее называемая обходом очереди) использует таблицу базы данных для передачи событий из CEI в модель монитора. При использовании доставки событий посредством таблиц работа может быть распределена между несколькими элементами кластера. Для большинства сред применение этого метода повышает производительность и упрощает настройку системы.

Получение событий с помощью доставки событий посредством таблиц

Можно настроить службу событий Инфраструктуры событий общего формата (CEI) для отправки событий в таблицу базы данных событий для модели монитора. Связь с шиной интеграции служб и связанные ресурсы настраивать не требуется. Обход очереди JMS повышает производительность, исключая дополнительное действие сохранения, которое требуется для очереди.

При использовании доставки событий посредством таблиц в IBM Business Monitor 7.5 работа может быть распределена между несколькими элементами кластера. Для большинства сред применение этого метода повышает производительность и упрощает настройку системы.

- **Модели до версии 6.2:** Доставка событий на основе таблиц не поддерживается. При использовании этого метода в версии ниже, чем 6.2, необходимо сначала обновить модель монитора с помощью Business Monitor - инструментарий разработки. Измените номер версии, создайте новый файл EAR и разверните новую версию модели монитора. Если вы решили не обновлять модель, необходимо использовать метод на основе очередей.
- **Модели версии 6.2 и 7:** эти модели могут использовать метод на основе таблиц (ранее называемый обходом очереди). Для того чтобы воспользоваться усовершенствованиями масштабируемости в версии 7.5, необходимо обновить модель монитора с помощью Business Monitor - инструментарий разработки версии 7.5.
- **Модели версии 7.5:** Эти модели могут использовать усовершенствования масштабируемости, если применяется доставка событий на основе таблиц.

Ограничение: При использовании SQL Server в качестве базы данных для применения метода доставки событий посредством таблиц генерирующее приложение должно работать на WebSphere Application Server 7.0 (или Process Server 7.0) или следующих версий. Необходимо использовать метод на основе очередей.

Метод на основе таблиц можно использовать в среде с одной или несколькими ячейками. Для выполнения настройки этого метода выберите следующую задачу, соответствующую вашей среде.

Настройка доставки событий посредством таблиц в среде с одной ячейкой:

В случае среды с одним (автономным) сервером или если на каждом узле ячейки установлен IBM Business Monitor версии 7.0 (или версии 7.0.0.3 для z/OS) или выше, то дополнительные действия по настройке получения событий не требуются. Если служба событий Инфраструктуры событий общего формата (CEI) развернута на узле в ячейке без IBM Business Monitor или Process Server, то вы должны установить файлы JAR IBM Business Monitor для маршрутизации событий на этом узле CEI.

Process Server версии 7.0 и следующих на распределенных платформах (и Process Server версии 7.0.0.3 и следующих на платформах z/OS) предоставляют файлы, необходимые для поддержки удаленной отправки событий. Если используется Process Server более ранней версии, то выполните следующие этапы для настройки доставки событий посредством таблиц в среде с одной ячейкой.

1. В каталоге `app_server_root/scripts.wbm/crossCell` локальной установки сервера IBM Business Monitor найдите подходящий файл, в зависимости от операционной системы и версии WebSphere Application Server, под управлением которой работает служба событий CEI.
 - `monitorCommunicationWithWAS70BasedCells.tar`,
`monitorCommunicationWithWAS61BasedCells.tar` или
`monitorCommunicationWithWAS60BasedCells.tar`.
 - `monitorCommunicationWithWAS70BasedCells.zip`,
`monitorCommunicationWithWAS61BasedCells.zip` или
`monitorCommunicationWithWAS60BasedCells.zip`.
2. Скопируйте подходящий файл в каталог `app_server_root/plugins` в каждой установке WebSphere Application Server на удаленном узле, на котором размещен целевой объект CEI и не установлен IBM Business Monitor или Process Server версии 7.0 (или версии 7.0.0.3 для z/OS) и выше, и извлеките содержимое.
3. В каждой установке WebSphere Application Server, в которой вы извлекли содержимое файла, выполните следующие действия:
 - a. Завершите работу всех виртуальных машин Java (JVM), использующих `app_server_root/java/bin/java`, в том числе агентов узлов, серверов, администраторов развертывания и приглашений `wsadmin`.
 - b. Выполните `profile_root/bin/osgiCfgInit` для каждого профайла в установке WebSphere Application Server.
 - c. Перезапустите все агенты узлов и серверы.

Настройка доставки событий посредством таблиц в среде с несколькими ячейкам:

Если IBM Business Monitor установлен в другой ячейке, нежели служба событий CEI, то необходимо выполнить дополнительные действия по настройке для включения связи между ячейками.

Для защищенных перед выполнением этой задачи должны быть выполнены следующие задачи:

- Если защита включена или в локальной, или в удаленной ячейке, то она должна быть включена в обеих.
- Если защита включена, то следует установить соединение SSL между удаленным сервером CEI и локальным сервером IBM Business Monitor (см. раздел Настройка соединения SSL между серверами в среде с несколькими ячейками).

- В ячейках необходимо настроить общие ключи LTRA. Кроме того, ячейкам необходимо присвоить один и тот же ИД (см. раздел Совместное использование ключей LTRA).
- Параметр **Применять подтверждение идентификации** должен быть включен в локальной и удаленной ячейках (см. раздел Активация подтверждения идентификации).

Если в среде с несколькими ячейками IBM Business Monitor не установлен в удаленной ячейке, отправляющей события, то необходимо настроить администратор развертывания и серверы CEI в удаленной ячейке для отправки событий в таблицы. Process Server версии 7.0 и следующих на распределенных платформах (и Process Server версии 7.0.0.3 и следующих на платформах z/OS) предоставляют файлы, необходимые для поддержки удаленной отправки событий. В предыдущих версиях Process Server эти файлы не предоставлялись автоматически. Таким образом, инструкции незначительно отличаются, если отправляющая события удаленная ячейка представляет собой распределенную ячейку, в которой установлен продукт Process Server версии 7.0 (версии 7.0.0.3 для z/OS) или более поздней версии.

Для настройки управления событиями на основе таблиц между несколькими ячейками выполните следующее:

- Если Process Server версии 7.0 (версии 7.0.0.3 для z/OS) или более высокой версии **не** установлен в удаленной ячейке (ячейке без IBM Business Monitor):
 1. В каталоге `app_server_root/scripts.wbm/crossCell` локальной установки сервера IBM Business Monitor найдите подходящий файл, в зависимости от операционной системы и версии WebSphere Application Server, под управлением которой работает служба событий CEI.
 - `monitorCommunicationWithWAS70BasedCells.tar` или `monitorCommunicationWithWAS61BasedCells.tar`.
 - `monitorCommunicationWithWAS70BasedCells.zip` или `monitorCommunicationWithWAS61BasedCells.zip`.
 2. Скопируйте подходящий файл в каталог `app_server_root/plugins` удаленного администратора развертывания и извлеките его содержимое.
 3. Скопируйте такой же файл файл в каталог `app_server_root/plugins` в каждой установке WebSphere Application Server в удаленной ячейке, в которой размещен целевой объект CEI и не установлен IBM Business Monitor или Process Server версии 7.0 (или версии 7.0.0.3 для z/OS) и выше, и извлеките содержимое.
 4. В каждой установке WebSphere Application Server, в которой вы извлекли содержимое файла, выполните следующие действия:
 - a. Завершите работу всех виртуальных машин Java (JVM), использующих `app_server_root/java/bin/java`, в том числе агентов узлов, серверов, администраторов развертывания и приглашений `wsadmin`.
 - b. Выполните `profile_root/bin/osgiCfgInit` для каждого профайла в установке WebSphere Application Server.
 - c. Перезапустите все агенты узлов и серверы.
 5. В удаленном администраторе развертывания или автономном сервере выполните команду `wbmConfigureQueueBypassDataSource wsadmin`. Пример применения и список параметров этой команды приведены в разделе CEI на основе таблиц. После выполнения команды и сохранения изменений конфигурации перезапустите удаленный администратор развертывания или автономный сервер.
- Если Process Server версии 7.0 (версии 7.0.0.3 для z/OS) или более высокой версии **установлен** в удаленной ячейке (ячейке без):

1. В удаленном администраторе развертывания или автономном сервере выполните команду `wbmConfigureQueueBypassDataSource wsadmin`. Пример применения и список параметров этой команды приведены в разделе CEI на основе таблиц.
2. После выполнения команды и сохранения изменений конфигурации перезапустите удаленный администратор развертывания или автономный сервер.

При развертывании модели монитора с помощью удаленного CEI необходимо выбрать опцию **Удаленного** расположения CEI, как описано в действии "Выбор опций CEI модели монитора" в разделе Развертывание моделей монитора.

Если сервер CEI установлен в системе z/OS: После завершения настройки CEI на основе таблиц в процессе развертывания модели монитора в протоколы CEI в системе z/OS заносится следующее сообщение об ошибке:

```
CEI61Configur E
com.ibm.wbimonitor.observationmgr.spi.impl.CEI61RemoteConfigurationSessionImpl
reloadCEIConfig(String[] eventServerAppNames) CWMRT7314E: Ошибка при попытке перезагрузки конфигурац
```

Для настройки CEI выполните следующее:

1. Перезапустите сервер или кластер CEI (CEI отправки в z/OS).
2. В системе администратора развертывания IBM Business Monitor запустите метод `confirmCEIServerReboot(String modelID)` объекта MBean служб жизненного цикла, указав тем самым на перезапуск CEI. Для запуска команды из командной строки `wsadmin` выполните следующие действия:
 - a. Установите соединение с объектом MBean служб жизненного цикла:


```
wsadmin> set ls [$AdminControl completeObjectName type=LifecycleServices,*]
```
 - b. Убедитесь, что CEI перезапущен:


```
wsadmin> $AdminControl invoke $ls confirmCEIServerReboot { "<model ID>"}
```

Получение событий с помощью доставки событий посредством очереди

Для получения событий с использованием очередей Службы сообщений Java (JMS) дополнительные действия выполнять не требуется, если включать связь между сервером IBM Business Monitor и удаленным сервером CEI не требуется. Необходимо использовать метод управления событиями на основе очередей, если применяется модель монитора, созданная с помощью IBM Business Monitor 6.1 в среде IBM Business Monitor 7.5 без обновления модели монитора.

В среде с одной или несколькими ячейками можно использовать управление событиями на основе очередей. Если сервер CEI находится в удаленной ячейке, в которой установлен IBM Business Monitor, то необходимо выполнить дополнительную настройку для включения связи между двумя ячейками.

Настройка доставки событий посредством очередей в среде с одной ячейкой:

Если IBM Business Monitor установлен в той же ячейке, что и служба событий CEI, и для получения событий используются очереди, то больше не требуется выполнять никаких действий. При установке IBM Business Monitor требуемые файлы JAR скопированы в соответствующие папки, и создана шина интеграции служб.

Настройка доставки событий посредством очередей в среде с несколькими ячейкам:

Если IBM Business Monitor установлен в другой ячейке, чем сервер CEI, необходимо выполнить дополнительные действия по настройке для включения связи между

ячейками. Для того чтобы получать события из очереди JMS в такой среде, необходимо настроить сервер IBM Business Monitor для получения событий из удаленного CEI сервера.

Перед завершением задачи убедитесь, что выполнены следующие действия:

- Развернута и настроена удаленная служба CEI.
- Создана шина интеграции служб для локального сервера IBM Business Monitor.

Для защищенных сред должны быть выполнены следующие задачи:

- Если защита включена или в локальной, или в удаленной ячейке, то она должна быть включена в обеих.
- Если защита включена, то следует установить соединение SSL между удаленным сервером CEI и локальным сервером IBM Business Monitor (см. раздел Настройка соединения SSL между серверами в среде с несколькими ячейками).
- В ячейках необходимо настроить общие ключи LTPA. Кроме того, ячейкам необходимо присвоить один и тот же ИД (см. раздел Совместное использование ключей LTPA).
- Параметр **Применять подтверждение идентификации** должен быть включен в локальной и удаленной ячейках (см. раздел Активация подтверждения идентификации).

Для настройки метода управления событиями на основе очередей следует установить файлы, предназначенные для всех ячеек, создать удаленную шину интеграции служб, а также создать связь между локальной и удаленной шинами. Process Server версии 7.0 и следующих на распределенных платформах (и Process Server версии 7.0.0.3 и следующих на платформах z/OS) предоставляют файлы, необходимые для поддержки удаленной отправки событий.

Для настройки управления событиями на основе очередей между несколькими ячейками выполните следующее:

Важное замечание: Если в удаленной ячейке установлен Process Server версии 7.0 (или версии 7.0.0.3 для z/OS) или следующих, то можно пропустить этапы 1-3 и перейти сразу к этапу 4.

1. В каталоге `app_server_root/scripts.wbm/crossCell` установки локального сервера IBM Business Monitor найдите подходящий файл в зависимости от операционной системы и версии WebSphere Application Server, в которых выполняется сервер CEI.
`monitorCommunicationWithWAS70BasedCells.tar,`
`monitorCommunicationWithWAS61BasedCells.tar` или
`monitorCommunicationWithWAS60BasedCells.tar.`
`monitorCommunicationWithWAS70BasedCells.zip,`
`monitorCommunicationWithWAS61BasedCells.zip` или `or`
`monitorCommunicationWithWAS60BasedCells.zip.`
2. Скопируйте подходящий файл в каталог `app_server_root/plugins` удаленного сервера CEI (или автономного сервера, или удаленного администратора развертывания) и извлеките его содержимое.
3. Из каталога `app_server_root/bin` на удаленном сервере CEI запустите соответствующую команду, чтобы настроить сервер приложений для распознавания файла `.jar: osgicfgInit.bat` или `osgicfgInit.sh`.
4. Из каталога `app_server_root/scripts.wbm/crossCell` локального сервера IBM Business Monitor выберите один из следующих методов для запуска утилиты

настройки шины интеграции служб для всех ячеек. Дополнительные сведения об этой утилите приведены в ссылках на связанную информацию.

- Для интерактивного запуска команды введите:

```
configRemoteMonitorBus.sh
configRemoteMonitorBus.bat
```

- Для запуска команды с использованием файла свойств, просмотрите файл configRemoteMonitorBus.props и измените все необходимые свойства. configRemoteMonitorBus.props Файл является примером файла свойств, размещенном в каталоге app_server_root/scripts.wbm/crossCell, однако можно создать свой собственный файл свойств для личной конфигурации:

```
configRemoteMonitorBus.sh -props имя_файла_свойств
configRemoteMonitorBus.bat -props имя_файла_свойств
```

Где:

имя_файла_свойств - это полное имя файла свойств, содержащего необходимые значения для конфигурации. Путь к файлу свойств должен быть полностью задан для сценария, чтобы было можно осуществлять его поиск. Утилита конфигурации перекрестных ячеек создает шину интеграции служб в удаленной ячейке. Имя шины задается в формате MONITOR.<удаленная_ячейка>.bus, где <удаленная_ячейка> - это имя удаленной ячейки.

5. По завершении сценария перезагрузите локальный IBM Business Monitor и удаленный CEI сервер.
6. Убедитесь, что удаленная шина интеграции служб существует и связь между локальной и удаленной шиной успешно создана, выполнив этапы в разделе "Проверка удаленной шины IBM Business Monitor и связи с шиной интеграции служб".

При развертывании модели монитора с помощью удаленного CEI необходимо выбрать опцию **Удаленного** расположения CEI, как описано в действии "Выбор опций CEI модели монитора" в разделе Развертывание моделей монитора.

В защищенной среде: Модель монитора можно развернуть в защищенной среде с удаленным CEI и управлением событиями на основе очередей. После развертывания модели монитора необходимо выполнить установку, следуя инструкциям из раздела "Выполнение установки модели монитора в защищенной среде на основе очередей".

Проверка удаленной IBM Business Monitor шины и связь интеграции служб.:

После настройки сервера IBM Business Monitor на использование сервера инфраструктуры обработки событий общего формата (CEI) на удаленном WebSphere Application Server или Process Server необходимо убедиться, что связь между удаленной шиной и шиной интеграции служб создана успешно.

Для того чтобы убедиться в том, что связь между удаленной шиной и шиной интеграции служб существует и активна, выполните следующее:

1. Из административной консоли на удаленном WebSphere Application Server или Process Server нажмите **Совмещение обслуживания > Шины**.
2. Щелкните на шине MONITOR.<имя-ячейки>.bus, которую нужно проверить, где <имя-ячейки> — имя ячейки, где установлен удаленный сервер CEI.
3. В опции Топология нажмите **Службы сообщений**. Будет определена одна служба сообщений. В поле **Состояние** зеленая стрелка отображает активность сервера для работы с сообщениями.

- Щелкните на службе сообщений и затем выберите **Дополнительные свойства > Связи с шиной интеграции служб**. При соединении удаленной ячейки с отдельной установкой монитора и установки монитора с отдельной удаленной ячейкой определяется одна связь. Однако может быть более одной связи. В поле **Статус** зеленая стрелка отображает активность сервера для работы с сообщениями.
- Дополнительно: для проверки по протоколу System.out найдите сообщение следующего вида. Для каждой системы служба сообщений имеет свое имя:
CWSIP0382I: Сервер для работы с сообщениями FADB84EB685E209F ответил на запрос о подписке, топ

Примечание: Ту же самую процедуру можно выполнить на сервере IBM Business Monitor и проверить, активна ли связь с шиной интеграции служб на стороне сервера IBM Business Monitor.

Настройка Business Space

Можно настроить продукт Business Space на основе WebSphere, предоставляющий общий интерфейс для пользователей приложения, который предназначен для создания, управления и интеграции веб-интерфейсов в портфеле IBM Business Process Management, WebSphere Enterprise Service Bus и других продуктах IBM.

Настройка Business Space

Установите и настройте Business Space, созданное с использованием WebSphere для настройки общего интерфейса создания, управления и интеграции веб-интерфейсов для приложений.

Необходимо установить продукт. При установке продукта файлы Business Space добавляются в настроенные профайлы.

Business Space поддерживает следующие продукты баз данных:

- DB2 Universal
- DB2 for IBM i
- DB2 for z/OS
- Microsoft SQL Server
- Oracle 11g

Для того чтобы узнать, какие базы данных поддерживаются конкретным продуктом IBM, используемым с Business Space, прочитайте информацию о поддерживаемых базах данных продукта.

Если устанавливается IBM Business Process Manager, WebSphere Enterprise Service Bus или IBM Business Monitor и создается профайл автономного сервера в обычном режиме, Business Space автоматически устанавливается и настраивается с базой данных DB2 Express. В случае профайла автономного сервера можно использовать расширенный режим инструмента управления профайлами для настройки Business Space на работу в среде выполнения. См. раздел "Настройка Business Space с помощью инструмента управления профайлами".

Для всех продуктов: в случае настройки администратора развертывания и пользовательских профайлов самый простой способ настройки Business Space - воспользоваться мастером настройки среды развертывания. См. раздел "Настройка Business Space с помощью мастера настройки среды развертывания".

В среде автономного сервера или в случае использования мастера среды развертывания для настройки среды выполнения конечные точки служб REST

настраиваются и включаются автоматически. Для настройки служб REST в других средах используйте страницу административной консоли Службы REST. Для того чтобы в Business Space были доступны виджеты, необходимо настроить конечные точки служб REST для этих виджетов. Конечные точки REST необходимо зарегистрировать, чтобы Business Space связал виджеты с конечными точками и виджеты появились в палитре.

При работе с администратором развертывания и пользовательскими профайлами продукт Business Space можно настроить с помощью административной консоли.

После выполнения первоначальной настройки с помощью инструмента управления профайлами или административной консоли необходимо настроить таблицы базы данных для Business Space. См. раздел "Настройка таблиц базы данных Business Space".

При любом способе настройки Business Space необходимо убедиться, что Business Space работает с защитой среды. См. раздел "Настройка защиты Business Space".

Business Space создан на основе технологии Lotus Mashups. Часто задаваемые вопросы и общая информация по диагностике и устранению неполадок Lotus Mashups приведена по адресу <http://www.lotus.com/idd/mashupswiki.nsf/xpViewCategories.xsp?lookupName=Troubleshooting&SessionID=CDFG4HK6EQ>.

После установки и настройки Business Space среду выполнения можно открыть с помощью следующего URL: <http://хост:порт/BusinessSpace>, где *хост* - имя хоста, где находится сервер, а *порт* - номер порта сервера.

Настройка Business Space в профайле продукта с помощью инструмента управления профайлами

Business Space, созданное с использованием WebSphere можно настроить как часть профайла продукта с помощью инструмента управления профайлами.

После установки продукта можно запустить инструмент управления профайлами. Кроме того, после установки продукта функции инструмента управления профайлами доступны из командной строки через параметр **-configureBSpace** утилиты **manageprofiles**. В обоих случаях Business Space устанавливается с тем продуктом базы данных, который указан для общей базы данных. При выборе базы данных, которая не поддерживается в Business Space, инструмент управления профайлами настраивает Business Space для работы с базой данных IBM DB2 Express.

При использовании утилиты командной строки **manageprofiles** руководствуйтесь документацией по **manageprofiles** для данного продукта управления бизнес-процессами. Просмотрите следующие замечания по использованию **manageprofiles**:

- При использовании Oracle или SQL Server на автономном сервере следует не применять параметр **-dbCreateNew**, а создать базу данных вручную.
- При наличии удаленной базы данных в кластерной среде необходимо вручную создать базу данных, скопировать сгенерированные сценарии в удаленную систему, где находится база данных, и выполнить сценарии из этого расположения.

Для администратора развертывания и пользовательских профайлов можно использовать административную консоль или мастер Настройка среды развертывания. См. разделы "Настройка Business Space с помощью административной консоли" и "Настройка Business Space с помощью мастера Настройка среды развертывания". При использовании инструмента управления профайлами для создания администратора развертывания и пользовательских

профайлов (управляемых узлов) с параметром создания профайла **Среда развертывания Business Space** автоматически настраивается в среде развертывания, но необходимо вручную выполнить сценарии настройки таблиц базы данных.

Для применения расширенных параметров конфигурации в профайле автономного сервера следует использовать страницы административной консоли для настройки Business Space. Например, если вместо базы данных, выбранной для профайла, требуется назначить другой источник данных (базу данных IBM Business Monitor или общую базу данных IBM Business Process Manager); Business Space должен настраиваться с помощью административной консоли.

Если необходимо использовать расширенные параметры конфигурации, которые требуют применения административной консоли, выполните следующие действия:

- При создании профайла автономного сервера с помощью инструмента управления профайлами используйте вариант создания профайла **Расширенный** и выключите переключатель **Настроить Business Space**, чтобы настроить Business Space позднее с помощью административной консоли.
- См. раздел "Настройка Business Space с помощью административной консоли".

Также, если Business Space нежелательно настраивать как часть профайла продукта, можно создать отдельные профайлы Business Space. Например, для разделения нагрузки может потребоваться разнести пользовательский интерфейс и базовую программу по разным узлам. Для того чтобы распределить рабочую нагрузку, можно сервер Business Process Manager установить в систему для высокой рабочей нагрузки, а Business Space - в удаленную систему. Система базовой программы оптимизируется под задачи базовой программы, а система Business Space настраивается на обработку данных HTTP. См. раздел "Создание профайлов Business Space" на стр. 144.

- Для автономного сервера запустите инструмент управления профайлами, выберите **Профайл автономного сервера** и выполните следующие действия.
 1. Выполните одно из следующих действий на странице Параметры создания профайла:
 - Выберите **Обычный** создания профайла, если подходит установка и конфигурация Business Space по умолчанию с базой данных DB2 Express. (Пропустите шаги с b. по e.)
 - Выберите **Расширенный**, если требуется настроить дополнительные параметры для создаваемого профайла. Затем на странице Конфигурация Business Space включите переключатель **Настроить Business Space**.
Business Space настраивается для работы с источником данных продукта.
 2. При назначении имени хоста для профайла должно использоваться полное имя.
 3. На странице Проект базы данных есть параметр использования файла проекта базы данных, созданного с помощью инструмента проектирования баз данных, который содержит конфигурацию всех баз данных для продукта, включая конфигурацию базы данных для Business Space. Дополнительная информация о файлах эскиза базы данных приведена в разделе "Создание файла свойств эскиза базы данных Business Space" на стр. 203.
 4. Создайте профайл с помощью инструмента управления профайлами. Business Space установлен. Он настроен на работу с продуктом базы данных, который указан для общей базы данных (или с DB2 Express, если продукт базы данных не поддерживается).
 5. Если база данных является удаленной, после выполнения инструмента управления профайлами необходимо настроить ее таблицы. См. раздел "Настройка таблиц базы данных Business Space".

- Для среды развертывания запустите инструмент управления профайлами, выберите **Профайл среды развертывания** или **Пользовательский профайл** и выполните следующие действия.
 1. На странице Параметры создания профайла выберите **Среда развертывания**, чтобы настроить каждый профайл с помощью значений пользовательской конфигурации и использовать в среде развертывания на основе указанного шаблона.
 2. Выполните действия в инструменте управления профайлами для создания профайла администратора развертывания и пользовательских профайлов (управляемых узлов).
 3. После добавления всех пользовательских узлов выполните сценарии для настройки таблиц базы данных вручную.

Важное замечание: Если базой данных продукта является Oracle, Business Space настраивается с помощью инструмента управления профайлами или утилиты командной строки `manageprofiles` на использование той же базы данных со схемой по умолчанию `IBMBUSSP` и паролем по умолчанию, который был введен во время создания профайла. Для использования другого пароля для имени пользователя `IBMBUSSP` необходимо с помощью административной консоли изменить ресурсы JDBC (источник данных `jdbc/mashupsDS`). Измените значение псевдонима идентификации в соответствии с паролем для имени схемы Business Space. Сохраните изменения и перезапустите сервер.

Перед использованием Business Space настройте защиту, необходимую для работы с Business Space и используемыми виджетами. См. раздел "Настройка защиты для Business Space".

Совет: Business Space использует прокси-компонент для подключения к службам REST. Если в некоторых случаях службы REST не отвечают, измените параметры тайм-аута соединения из Business Space в службы REST в зависимости от производительности серверов службы REST. См. раздел Изменение параметров тайм-аута для прокси Ajax Business Space.

Создание профайлов Business Space:

Для создания и дополнения профайлов Business Space можно использовать инструмент управления профайлами или утилиту командной строки `manageprofiles`. Профайлы представляют собой наборы файлов, определяющих среду выполнения для администратора развертывания, управляемого узла или автономного сервера.

Если Business Space настроен как часть профайла продукта, выполнять эти задачи необязательно.

Создание профайлов Business Space для автономной конфигурации:

Создать профайлы Business Space для автономной среды можно с помощью Инструмента управления профайлами или утилиты командной строки `manageprofiles`.

Если Business Space настроен как часть профайла продукта, то выполнять эти задачи необязательно.

Создание профайлов Business Space для автономной конфигурации с помощью Инструмента управления профайлами:

С помощью Инструмента управления профайлами можно создавать автономные профайлы для Business Space.




- Просмотрите полный список предварительных требований по созданию или дополнению профайла, приведенный в разделе Концепции профайла справочной системы WebSphere Application Server Information Center.
- Когда вы используете Инструмент управления профайлами вместе с графическим пользовательским интерфейсом Motif в операционной системе Solaris, размер по умолчанию Инструмента управления профайлами может быть недостаточен для просмотра всех сообщений и кнопок.
- Если вы собираетесь использовать файл эскиза базы данных в качестве информации о базе данных Business Space, то выполните процедуру из раздела “Создание файла свойств эскиза базы данных Business Space” на стр. 203.

Выполните эту процедуру, если вы создаете профайл Business Space для автономной конфигурации. Процедура охватывает и Расширенное, и Обычное создание профайла.

Если Business Space настроен как часть профайла продукта, то выполнять эту задачу необязательно.

1. Запустите Инструмент управления профайлами.

Выполните одну из следующих команд:

-   `каталог_установки/bin/ProfileManagement/pmt.sh`
-  `каталог_установки\bin\ProfileManagement\pmt.bat`

Откроется начальная страница.

2. На начальной странице выберите **Запустить Инструмент управления профайлами** или щелкните на вкладке Инструмент управления профайлами.

Откроется вкладка Профайлы.

Вкладка Профайлы содержит список профайлов, созданных на вашем компьютере. Для создания новых и дополнения существующих профайлов можно воспользоваться Инструментом управления профайлами.

3. На вкладке Профайлы нажмите **Создать**.

В отдельном окне откроется страница Выбор среды.

4. На странице Выбор среды выберите опцию **Автономный профайл** и нажмите **Далее**.

5. На странице Опции создания профайла выберите между **Обычным созданием профайла** и **Расширенным созданием профайла**.

6. Если вы выбрали опцию **Обычное создание профайла**, выполните следующие действия.

- a. На странице Административная защита введите имя пользователя и пароль, подтвердите пароль и нажмите **Далее**.

Вся конфигурация профайла, включая опции и базы данных, задается по умолчанию и отображается на странице Обзор профайла.




- b. На странице Обзор профайла нажмите **Создать**, чтобы создать профайл, или **Назад**, чтобы изменить характеристики профайла.

Информация о ходе настройки отображается в окне Ход настройки профайла. По окончании создания профайла появляется страница Создание профайла закончено с сообщением **Инструмент управления профайлами успешно создал профайл**.

Внимание: Если во время создания профайла возникнут ошибки, то вместо сообщения об успешном завершении могут появиться другие сообщения, например:

- **Инструмент управления профайлами создал профайл, но с ошибками**, что означает, что профайл был создан, но во время его создания возникли ошибки.
- **Инструмент управления профайлами не создал профайл**, что означает, что создать профайл не удалось.

На странице Создание профайла закончено указан файл протокола, который поможет вам устранить неполадки.

7. Если вы выбрали опцию **Расширенное создание профайла**, выполните следующие действия.
 - a. На странице Развертывание необязательных приложений отметьте переключатели, если вы хотите развернуть административную консоль и приложение по умолчанию.
 - b. На странице Имя и расположение профайла выполните следующие действия:
 - 1) В поле Имя профайла укажите уникальное имя или оставьте значение по умолчанию. У каждого создаваемого профайла должно быть имя. Если профайлов несколько, вы сможете различать их по именам. Если вы решили не оставлять имя по умолчанию, то, в случае Windows, укажите краткое имя, поскольку длина путей к файлам ограничена.
 - 2) В поле Каталог профайла укажите каталог профайла или выберите его с помощью кнопки Обзор. Указанный каталог будет содержать файлы для среды выполнения, например, команды, файлы конфигурации и файлы протоколов. Каталог по умолчанию зависит от платформы:
 -  **Linux**  **UNIX** каталог_установки/profiles/имя_профайла
 -  **Windows** каталог_установки\profiles\имя_профайлагде *имя_профайла* - это указанное имя.Поле каталога профайла должно отвечать следующим требованиям:
 - *имя_профайла* должно быть уникальным.
 - Указанный каталог должен быть пустым.
 - Каталог должен быть доступен вашему ИД пользователя.
 - Для создания профайла должно быть достаточно памяти.
 - 3) Необязательно: отметьте переключатель **Применять этот профайл по умолчанию**, если вы хотите, чтобы создаваемый профайл применялся по умолчанию. Этот переключатель появляется только при наличии профайла в системе.

Команды автоматически применяют профайл по умолчанию. Первый профайл, который вы создаете на рабочей станции, становится профайлом по умолчанию. Профайл по умолчанию - это цель по умолчанию для команд, выполняемых из каталога bin в каталоге установки продукта. Если на рабочей станции только один профайл, то каждая команда работает с ним. Если профайлов несколько, то некоторые команды требуют выбрать профайл.
 - 4) Нажмите **Далее**.
- c. На странице Имена узла и хоста выполните следующие действия для создаваемого профайла:
 - В поле Имя узла введите имя узла или оставьте значение по умолчанию. Имена узлов следует выбирать максимально короткими, но вместе с тем уникальными в среде разработки.

- В поле **Имя хоста** введите имя хоста или оставьте значение по умолчанию.
- В поле **Имя ячейки** введите имя ячейки или оставьте значение по умолчанию.

Нажмите **Далее** для перехода к странице **Административная защита**.

- На странице **Административная защита** введите имя пользователя и пароль, затем подтвердите пароль. Нажмите **Далее**.
- На странице **Сертификат защиты (Часть 1)** укажите, следует ли создавать новые или импортировать существующие сертификаты. Выполните следующие действия:
 - Для создания нового личного сертификата по умолчанию и нового подписывающего сертификата root выберите **Создать новый личный сертификат по умолчанию** и **Создать новый подписывающий сертификат root** и нажмите **Далее**.
 - Для импорта существующих сертификатов выберите **Импортировать существующий личный сертификат по умолчанию** и **Импортировать существующий личный подписывающий сертификат root** и укажите следующую информацию:
 - В поле **Путь** введите путь к существующему сертификату.
 - В поле **Пароль** введите пароль к сертификату.
 - В поле **Тип хранилища ключей** выберите тип хранилища ключей для импортируемого сертификата.
 - В поле **Псевдоним хранилища ключей** выберите псевдоним хранилища ключей для импортируемого сертификата.
 - Нажмите **Далее**.

Когда вы импортируете личный сертификат в качестве личного сертификата по умолчанию, импортируйте вместе с ним подписавший его сертификат root. В противном случае Инструмент управления профайлами добавит подписант личного сертификата в файл `trust.p12`. Если вы импортируете личный сертификат по умолчанию или подписывающий сертификат root, то укажите путь и пароль, а затем выберите тип и псевдоним хранилища ключей для каждого импортируемого сертификата.

- На странице **Сертификат защиты (Часть 2)** проверьте правильность информации сертификата и нажмите **Далее** для перехода к странице **Назначение значений портов**.

Если вы создаете сертификаты, то вы можете использовать значения по умолчанию или изменить их для создания новых сертификатов. Личный сертификат по умолчанию действителен в течение одного года (по умолчанию) и подписывается подписывающим сертификатом root. Подписывающий сертификат root - это собственный сертификат, действительный в течение 15 лет (по умолчанию). Пароль к хранилищу ключей по умолчанию для подписывающего сертификата root - WebAS. Измените пароль. Пароль не может содержать символов из набора двухбайтовых символов (DBCS), поскольку некоторые типы хранилищ ключей, в том числе PKCS12, не поддерживают их. Поддерживаемые типы хранилищ ключей зависят от провайдеров, указанных в файле `java.security`.

Когда вы создаете один или оба сертификата или импортируете один или оба сертификата, создаются следующие файлы хранилища ключей:

- `key.p12`: содержит личный сертификат по умолчанию.
- `trust.p12`: содержит подписывающий сертификат из сертификата root по умолчанию.
- `root-key.p12`: содержит подписывающий сертификат root.

- `default-signers.p12`: содержит подписывающие сертификаты, которые добавляются в любой новый файл хранилища ключей, который вы создаете после установки и запуска сервера. По умолчанию подписант сертификата `root` по умолчанию и подписывающий сертификат `DataPower®` содержатся в этом файле хранилища ключей.
- `deleted.p12`: содержит сертификаты, удаляемые задачей `deleteKeyStore`, так что их можно восстановить при необходимости.
- `ltpa.jceks`: содержит ключи Простого протокола идентификации третьих сторон (ЛТРА) по умолчанию для сервера, применяемые серверами среды для обмена информацией друг с другом.

Всем этим файлам присваивается один и тот же пароль, когда вы создаете или импортируете сертификаты. Это либо пароль по умолчанию, либо указанный вами пароль. Импортированный сертификат добавляется в файл `key.p12` или `root-key.p12`. Если вы импортируете ненужные сертификаты, нажмите **Назад**, чтобы сменить импортируемый сертификат.


- g. На странице Назначение значений портов проверьте уникальность портов, указанных для профайла, и нажмите **Далее**.

Инструмент управления профайлами обнаруживает порты, используемые в настоящее время другими продуктами IBM WebSphere, и показывает рекомендуемые значения портов, не конфликтующие с уже существующими. Если у вас есть другие приложения, использующие указанные порты, то убедитесь, что порты не конфликтуют. Если вы отказались от развертывания административной консоли на странице Развертывание необязательных приложений, то ее порты будут недоступны на странице Назначение значений портов. Порты распознаются как занятые, если они назначены профайлу, созданному во время установки, которую выполнял текущий пользователь, или если они используются в настоящее время.

Хотя Инструмент управления профайлами проверяет порты, когда вы обращаетесь к странице Назначение значений портов, выбор опций на последующих его страницах может привести к конфликтам портов. Порты не назначаются, пока создание профайла не будет закончено. Если вы подозреваете возможность конфликта портов, то вы сможете выяснить это после создания профайла.

Определить, какие порты использовались во время создания профайла, можно с помощью файла `profile_root/properties/portdef.props`. В этом файле перечислены ключи и значения, которые использовались при задании портов. При обнаружении конфликта портов вы можете переназначить порты вручную. Инструкции по переназначению портов приведены в разделе Обновление портов в существующих профайлах справочной системы WebSphere Application Server Network Deployment Information Center. Запустите файл `updatePorts.ant` посредством сценария `ws_ant`, описанного в этом разделе.

- h. Если вы выполняете установку на платформе Linux или Windows и у вас есть права доступа `root` или административной группы, то будет показана страница Определение службы Linux или Windows. На странице Определение службы укажите, будет ли служба Windows или Linux запускать сервер процессов, и нажмите **Далее**, чтобы просмотреть страницу Определение веб-сервера.

 Страница Определение службы Windows откроется на платформе Windows только в том случае, если у идентификатора пользователя, устанавливающего службу Windows, есть права доступа административной группы. Если профайл настроен как служба Windows, то продукт запускает службы Windows для процессов, запущенных командой `startServer` или `startManager`. Например, если вы настроите сервер или Администратор

развертывания в качестве службы Windows и выполните команду startServer или startManager, то команда wasservice запустит определенные службы.

Важное замечание: Если вы решили войти в систему с указанной учетной записью пользователя, то вы должны указать идентификатор и пароль для пользователя, которому предстоит запустить службу, а также тип запуска (по умолчанию - Вручную). В ИД пользователя не должно быть пробелов. ИД пользователя должен входить в административную группу и у него должны быть расширенные права пользователя: Вход в систему в качестве службы. Если ИД пользователя входит в административную группу, то Инструмент управления профайлами предоставляет ему расширенные права доступа, если у него еще нет их. Во время удаления профайла можно удалить службу Windows, добавленную во время создания профайла.

Windows **Замечания о IPv6 при запуске профайлов в качестве служб Windows:** профайлы, предназначенные для запуска в качестве службы Windows, не запускаются при использовании IPv6, если служба настроена для запуска в качестве локальной системы. Создайте пользовательскую переменную среды для включения IPv6. Так как эта переменная среды является пользовательской, а не локальной системной, она доступна только той службе Windows, которая запущена от имени этого пользователя. По умолчанию, когда новый профайл создается и настраивается для работы в качестве службы Windows, служба настраивается для работы в качестве локальной системы. Когда служба Windows пытается начать работу, она не может получить доступ к пользовательской переменной среды, задающей IPv6, и поэтому пытается начать работу в режиме IPv4. В этом случае сервер запускается неправильно. Для устранения этой неполадки, при создании профайла укажите, что служба Windows запускается от имени того ИД пользователя, для которого определена переменная среды, задающая IPv6, а не как локальная системная служба.

Linux Страница Определение службы Linux появляется только в том случае, если текущая операционная система является поддерживаемой версией Linux и у текущего пользователя есть соответствующие права доступа. Продукт пытается запустить службы Linux для процессов, запущенных командой startServer или startManager. Например, если вы настроите сервер или Администратор развертывания как службу Linux и выполните команду startServer или startManager, то команда wasservice запустит определенные службы. По умолчанию продукт не настроен для запуска в качестве службы Linux. Для создания службы необходимо, чтобы пользователь, запускающий Инструмент управления профайлами, был пользователем root. Если вы запустите Инструмент управления профайлами под управлением пользователя, отличного от root, то страница Определение службы Linux не появится и служба создана не будет. Вы должны указать имя пользователя, под управлением которого запускается служба. Для удаления службы Linux пользователь должен быть пользователем root или у него должны быть соответствующие права на удаление службы. В противном случае будет создан сценарий удаления, который сможет запустить пользователь root, чтобы удалить службу от имени текущего пользователя.

- i. Если вы выполняете установку на любой другой платформе или как пользователь, отличный от root, на платформе Linux или Windows, то будет показана страница Определение веб-сервера. Для немедленного включения определения веб-сервера в профайл выполните следующие действия:
 - 1) Отметьте переключатель **Создать определение веб-сервера**.
 - 2) Укажите характеристики веб-сервера на странице и нажмите **Далее**.
 - 3) Укажите характеристики веб-сервера на части 2 страницы и нажмите **Далее**.

Если вы применяете веб-сервер для отправки запросов на сервер, то вам необходимо добавить определение веб-сервера. Его можно добавить сейчас или позже. Если вы зададите определение веб-сервера во время создания данного профайла, то сможете установить веб-сервер и его модуль после создания профайла. Однако вы должны установить оба этих объекта в каталогах, указанных на страницах определения веб-сервера. Если вы определите веб-сервер в Business Space после создания данного профайла, то вы должны будете определить веб-сервер в отдельном профайле.

- 4) Нажмите **Далее**.
- j. Если для настройки баз данных вы хотите воспользоваться уже созданным файлом эскиза базы данных, то выполните следующие действия, вместо того чтобы заполнять страницы Конфигурация базы данных.
 - 1) Выберите опцию **Использовать файл эскиза базы данных** для конфигурации базы данных.
 - 2) Нажмите **Обзор**.
 - 3) Укажите полное имя пути к файлу эскиза.
 - 4) Нажмите **Далее**.
- k. Если вы не использовали файл эскиза базы данных, то на странице Конфигурация базы данных выполните следующие действия:
 - 1) В списке **Выбрать продукт базы данных** выберите продукт для использования профайлом.
 - 2) Отметьте переключатель **Переопределить каталог вывода по умолчанию для сценариев базы данных**, если вы хотите задать каталог, в который будут записываться сценарии SQL, согласно которым создаются таблицы баз данных. Если вы не отметите переключатель, то сценарии будут заноситься в каталог по умолчанию.
 - 3) Нажмите **Далее** для перехода к странице Конфигурация базы данных (Часть 2).

Содержимое страницы Конфигурация базы данных (Часть 2) зависит от значения, указанного в списке **Выбрать продукт базы данных** на странице Конфигурация базы данных.

- l. На странице Конфигурация базы данных (Часть 2) задайте оставшиеся параметры конфигурации базы данных: В зависимости от продукта базы данных, вы должны указать имя пользователя и пароль для идентификации в базе данных, информацию о драйвере JDBC, хост, порт и схему.
- m. На странице **Обзор профайла** нажмите **Создать**, чтобы создать профайл, или **Назад**, чтобы изменить характеристики профайла.

Информация о ходе настройки отображается в окне **Ход настройки профайла**. По окончании создания профайла появляется страница **Создание профайла закончено** с сообщением **Инструмент управления профайлами успешно создал профайл**.

Внимание: Если во время создания профайла возникнут ошибки, то вместо сообщения об успешном завершении могут появиться другие сообщения, например:

- **Инструмент управления профайлами создал профайл, но с ошибками**, что означает, что профайл был создан, но во время его создания возникли ошибки.
- **Инструмент управления профайлами не создал профайл**, что означает, что создать профайл не удалось.

На странице Создание профайла закончено указан файл протокола, который поможет вам устранить неполадки.

Создание профайлов Business Space для автономной конфигурации с помощью утилиты командной строки manageprofiles:

С помощью утилиты командной строки manageprofiles можно создавать профайлы Business Space для конфигурации автономного сервера Business Space.

Прежде чем запускать утилиту командной строки manageprofiles, выполните следующие задачи:

- Просмотрите полный список предварительных требований по созданию или дополнению профайла, приведенный в разделе Концепции профайла справочной системы WebSphere Application Server Information Center.
- Просмотрите примеры команд создания профайла.
- Убедитесь, что в данный момент утилита командной строки manageprofiles не запущена по отношению к выбранному профайлу. Если выдается сообщение об ошибке, выясните, не выполняется ли другое действие по созданию или дополнению профайла в данный момент. Если это так, дождитесь его завершения.

В этой задаче указано, как с помощью утилиты командной строки manageprofiles можно создавать профайлы Business Space для автономной конфигурации Business Space. Для того чтобы создать профайл с помощью утилиты командной строки manageprofiles, выполните следующие действия.

1. Найдите шаблон профайла default.bspace для автономных профайлов Business Space, определяющих автономные серверы.
Шаблоны для каждого профайла находятся в каталоге *каталог_установки/profileTemplates/BusinessSpace*.
2. Определите, какие параметры необходимы для создания профайла, изучив раздел “Утилита командной строки manageprofiles (для профайлов Business Space)” на стр. 175. Просмотрите значения по умолчанию и определите, какие значения необходимо указать для профайла. Например, вы можете задать параметры -templatePath, -enableAdminSecurity, -adminUserName, -adminPassword, -dbType, -dbUserId, dbPassword, -dbJDBCClasspath, -dbName, -bspaceSchema, -dbHostName, -dbServerPort и -dbDelayConfig.
3. Запустите файл из командной строки. Простой пример:

```
manageProfiles -create -templatePath
каталог_установки/profileTemplates/BusinessSpace/default.bspace
-enableAdminSecurity true -adminUserName ИД_администратора
-adminPassword пароль_администратора
-dbType DB2_Universal -dbUserId ИД_пользователя_db2 -dbPassword
пароль_пользователя_db2
-dbJDBCClasspath каталог_установки/jdbcdrivers/DB2 -dbName
база_данных -bspaceSchema
схема_базы_данных -dbHostName хост -dbServerPort
порт -dbDelayConfig false
```

Команда показывает индикатор хода своего выполнения. Дождитесь окончания ее выполнения. Когда файл ответов анализируется подобно любому другому файлу ответов, он проходит обычную синтаксическую проверку. Отдельные значения в файле ответов считаются параметрами командной строки.

Создание профайлов Business Space для конфигурации сетевого развертывания:

Создать профайлы Business Space для среды сетевого развертывания можно с помощью Инструмента управления профайлами или утилиты командной строки `manageprofiles`.

Если Business Space настроен как часть профайла продукта, то выполнять эти задачи необязательно.

Создание профайлов Business Space для конфигурации сетевого развертывания с помощью Инструмента управления профайлами:

С помощью Инструмента управления профайлами можно создавать профайлы Business Space для конфигурации сетевого развертывания: вы должны создать профайл Администратора развертывания и настраиваемые профайлы (управляемые узлы).




- Просмотрите полный список предварительных требований по созданию или дополнению профайла, приведенный в разделе Концепции профайла справочной системы WebSphere Application Server Information Center.
- Когда вы используете Инструмент управления профайлами вместе с графическим пользовательским интерфейсом Motif в операционной системе Solaris, размер по умолчанию Инструмента управления профайлами может быть недостаточен для просмотра всех сообщений и кнопок.

Выполните эту процедуру, если вы создаете профайл Business Space для конфигурации сетевого развертывания. Вы должны создать профайлы Администратора развертывания и настраиваемые профайлы для управляемых узлов. Процедура охватывает и Расширенное, и Обычное создание профайла.

Если Business Space настроен как часть профайла продукта, то выполнять эту задачу необязательно.

1. Создайте профайл Администратора развертывания.
 - a. Запустите Инструмент управления профайлами.

Выполните одну из следующих команд:

 -   `каталог_установки/bin/ProfileManagement/pmt.sh`
 -  `каталог_установки\bin\ProfileManagement\pmt.bat`
 - b. На начальной странице выберите **Запустить Инструмент управления профайлами** или щелкните на вкладке Инструмент управления профайлами. Откроется вкладка Профайлы.

Вкладка Профайлы содержит список профайлов, созданных на вашем компьютере. Для создания новых и дополнения существующих профайлов можно воспользоваться Инструментом управления профайлами.
 - c. На вкладке Профайлы нажмите **Создать**.

В отдельном окне откроется страница Выбор среды.
 - d. На странице Выбор среды разверните раздел **Business Space на основе WebSphere**, выберите опцию **Business Space на основе Администратора развертывания WebSphere** и нажмите **Далее**.
 - e. На странице Опции создания профайла выберите между **Обычным созданием профайла** и **Расширенным созданием профайла**.
 - f. Если вы выбрали опцию **Обычное создание профайла**, выполните следующие действия.

- 1) На странице Административная защита введите имя пользователя и пароль, подтвердите пароль и нажмите **Далее**. Вся конфигурация профайла, включая опции и базы данных, задается по умолчанию и отображается на странице Обзор профайла.
- 2) На странице Обзор профайла нажмите **Создать**, чтобы создать профайл, или **Назад**, чтобы изменить характеристики профайла.

Информация о ходе настройки отображается в окне **Ход настройки профайла**. По окончании создания профайла появляется страница **Создание профайла закончено** с сообщением **Инструмент управления профайлами успешно создал профайл**.

Внимание: Если во время создания профайла возникнут ошибки, то вместо сообщения об успешном завершении могут появиться другие сообщения, например:




- **Инструмент управления профайлами создал профайл, но с ошибками**, что означает, что профайл был создан, но во время его создания возникли ошибки.
- **Инструмент управления профайлами не создал профайл**, что означает, что создать профайл не удалось.

На странице Создание профайла закончено указан файл протокола, который поможет вам устранить неполадки.

- g. Если вы выбрали опцию **Расширенное создание профайла**, выполните следующие действия.

- 1) На странице Развертывание необязательных приложений отметьте переключатели, если вы хотите развернуть административную консоль и приложение по умолчанию.
- 2) На странице Имя и расположение профайла выполните следующие действия:

- a) В поле Имя профайла укажите уникальное имя или оставьте значение по умолчанию. У каждого создаваемого профайла должно быть имя. Если профайлов несколько, вы сможете различать их по именам. Если вы решили не оставлять имя по умолчанию, то, в случае Windows, укажите краткое имя, поскольку длина путей к файлам ограничена.
- b) В поле Каталог профайла укажите каталог профайла или выберите его с помощью кнопки Обзор. Указанный каталог будет содержать файлы для среды выполнения, например, команды, файлы конфигурации и файлы протоколов. Каталог по умолчанию зависит от платформы:

-   *каталог_установки/profiles/имя_профайла*
-  *каталог_установки\profiles\имя_профайла*

где *имя_профайла* - это указанное имя.

Поле каталога профайла должно отвечать следующим требованиям:

- *имя_профайла* должно быть уникальным.
 - Указанный каталог должен быть пустым.
 - Каталог должен быть доступен вашему ИД пользователя.
 - Для создания профайла должно быть достаточно памяти.
- c) Необязательно: отметьте переключатель **Применять этот профайл по умолчанию**, если вы хотите, чтобы создаваемый профайл применялся по умолчанию. Этот переключатель появляется только при наличии профайла в системе.

Команды автоматически применяют профайл по умолчанию. Первый профайл, который вы создаете на рабочей станции, становится профайлом по умолчанию. Профайл по умолчанию - это цель по умолчанию для команд, выполняемых из каталога bin в каталоге установки продукта. Если на рабочей станции только один профайл, то каждая команда работает с ним. Если профайлов несколько, то некоторые команды требуют выбрать профайл.

d) Нажмите **Далее**.

3) На странице Имена узла и хоста выполните следующие действия для создаваемого профайла:

- a) В поле Имя узла введите имя узла или оставьте значение по умолчанию. Имена узлов следует выбирать максимально короткими, но вместе с тем уникальными в среде разработки.
- b) В поле Имя хоста введите имя хоста или оставьте значение по умолчанию.
- c) В поле Имя ячейки введите имя ячейки или оставьте значение по умолчанию.

Нажмите **Далее** для перехода к странице Административная защита.

4) На странице Административная защита введите имя пользователя и пароль, затем подтвердите пароль. Нажмите **Далее**.

5) На странице Сертификат защиты (Часть 1) укажите, следует ли создавать новые или импортировать существующие сертификаты. Выполните следующие действия:

- Для создания нового личного сертификата по умолчанию и нового подписывающего сертификата root выберите **Создать новый личный сертификат по умолчанию** и **Создать новый подписывающий сертификат root** и нажмите **Далее**.
- Для импортирования существующих сертификатов выберите **Импортировать существующий личный сертификат по умолчанию** и **Импортировать существующий личный подписывающий сертификат root** и укажите следующую информацию:
 - В поле Путь введите путь к существующему сертификату.
 - В поле Пароль введите пароль к сертификату.
 - В поле Тип хранилища ключей выберите тип хранилища ключей для импортируемого сертификата.
 - В поле Псевдоним хранилища ключей выберите псевдоним хранилища ключей для импортируемого сертификата.
 - Нажмите **Далее**.

Когда вы импортируете личный сертификат в качестве личного сертификата по умолчанию, импортируйте вместе с ним подписавший его сертификат root. В противном случае Инструмент управления профайлами добавит подписант личного сертификата в файл trust.p12. Если вы импортируете личный сертификат по умолчанию или подписывающий сертификат root, то укажите путь и пароль, а затем выберите тип и псевдоним хранилища ключей для каждого импортируемого сертификата.

6) На странице Сертификат защиты (Часть 2) проверьте правильность информации сертификата и нажмите **Далее** для перехода к странице Назначение значений портов.

Если вы создаете сертификаты, то вы можете использовать значения по умолчанию или изменить их для создания новых сертификатов. Личный

сертификат по умолчанию действителен в течение одного года (по умолчанию) и подписывается подписывающим сертификатом root. Подписывающий сертификат root - это собственный сертификат, действительный в течение 15 лет (по умолчанию). Пароль к хранилищу ключей по умолчанию для подписывающего сертификата root - WebAS. Измените пароль. Пароль не может содержать символов из набора двухбайтовых символов (DBCS), поскольку некоторые типы хранилищ ключей, в том числе PKCS12, не поддерживают их. Поддерживаемые типы хранилищ ключей зависят от провайдеров, указанных в файле `java.security`.

Когда вы создаете один или оба сертификата или импортируете один или оба сертификата, создаются следующие файлы хранилища ключей:

- `key.p12`: содержит личный сертификат по умолчанию.
- `trust.p12`: содержит подписывающий сертификат из сертификата root по умолчанию.
- `root-key.p12`: содержит подписывающий сертификат root.
- `default-signers.p12`: содержит подписывающие сертификаты, которые добавляются в любой новый файл хранилища ключей, который вы создаете после установки и запуска сервера. По умолчанию подписант сертификата root по умолчанию и подписывающий сертификат DataPower® содержатся в этом файле хранилища ключей.
- `deleted.p12`: содержит сертификаты, удаляемые задачей `deleteKeyStore`, так что их можно восстановить при необходимости.
- `ltpa.jseks`: содержит ключи Простого протокола идентификации третьих сторон (LTPA) по умолчанию для сервера, применяемые серверами среды для обмена информацией друг с другом.

Всем этим файлам присваивается один и тот же пароль, когда вы создаете или импортируете сертификаты. Это либо пароль по умолчанию, либо указанный вами пароль. Импортированный сертификат добавляется в файл `key.p12` или `root-key.p12`. Если вы импортируете ненужные сертификаты, нажмите **Назад**, чтобы сменить импортируемый сертификат.

- 7) На странице Назначение значений портов проверьте уникальность портов, указанных для профайла, и нажмите **Далее**.

Инструмент управления профайлами обнаруживает порты, используемые в настоящее время другими продуктами IBM WebSphere, и показывает рекомендуемые значения портов, не конфликтующие с уже существующими. Если у вас есть другие приложения, использующие указанные порты, то убедитесь, что порты не конфликтуют. Если вы отказались от развертывания административной консоли на странице Развертывание необязательных приложений, то ее порты будут недоступны на странице Назначение значений портов. Порты распознаются как занятые, если они назначены профайлу, созданному во время установки, которую выполнял текущий пользователь, или если они используются в настоящее время.

Хотя Инструмент управления профайлами проверяет порты, когда вы обращаетесь к странице Назначение значений портов, выбор опций на последующих его страницах может привести к конфликтам портов. Порты не назначаются, пока создание профайла не будет закончено. Если вы подозреваете возможность конфликта портов, то вы сможете выяснить это после создания профайла.

Определить, какие порты использовались во время создания профайла, можно с помощью файла `profile_root/properties/portdef.props`. В этом файле перечислены ключи и значения, которые использовались при

задании портов. При обнаружении конфликта портов вы можете переназначить порты вручную. Инструкции по переназначению портов приведены в разделе Обновление портов в существующих профайлах справочной системы WebSphere Application Server Network Deployment Information Center. Запустите файл `updatePorts.ant` посредством сценария `ws_ant`, описанного в этом разделе.

- 8) Если вы выполняете установку на платформе Linux или Windows и у вас есть права доступа `root` или административной группы, то будет показана страница Определение службы Linux или Windows. На странице Определение службы укажите, будет ли служба Windows или Linux запускать сервер процессов, и нажмите **Далее**, чтобы просмотреть страницу Определение веб-сервера.

Windows Страница Определение службы Windows откроется на платформе Windows только в том случае, если у идентификатора пользователя, устанавливающего службу Windows, есть права доступа административной группы. Если профайл настроен как служба Windows, то продукт запускает службы Windows для процессов, запущенных командой `startServer` или `startManager`. Например, если вы настроите сервер или Администратор развертывания как службу Windows и выполните команду `startServer` или `startManager`, то команда `wasservice` запустит определенные службы.

Важное замечание: Если вы решили войти в систему под управлением указанной учетной записи пользователя, то вы должны указать идентификатор и пароль для пользователя, который будет запускать службу, а также тип запуска (по умолчанию - Вручную). В ИД пользователя не должно быть пробелов. ИД пользователя должен входить в административную группу и у него должны быть расширенные права пользователя: Вход в систему в качестве службы. Если ИД пользователя входит в административную группу, то Инструмент управления профайлами предоставляет ему расширенные права доступа, если у него еще нет их. Во время удаления профайла можно удалить службу Windows, добавленную во время создания профайла.

Windows **Замечания о IPv6 при запуске профайлов в качестве служб**

Windows: профайлы, предназначенные для запуска в качестве службы Windows, не запускаются при использовании IPv6, если служба настроена для запуска в качестве локальной системы. Создайте пользовательскую переменную среды для включения IPv6. Так как эта переменная среды является пользовательской, а не локальной системной, она доступна только той службе Windows, которая запущена от имени этого пользователя. По умолчанию, когда новый профайл создается и настраивается для работы в качестве службы Windows, служба настраивается для работы в качестве локальной системы. Когда служба Windows пытается начать работу, она не может получить доступ к пользовательской переменной среды, задающей IPv6, и поэтому пытается начать работу в режиме IPv4. В этом случае сервер запускается неправильно. Для устранения этой неполадки, при создании профайла укажите, что служба Windows запускается от имени того ИД пользователя, для которого определена переменная среды, задающая IPv6, а не как локальная системная служба.

Linux Страница Определение службы Linux появляется только в том случае, если текущая операционная система является поддерживаемой версией Linux и у текущего пользователя есть соответствующие права доступа. Продукт пытается запустить службы Linux для процессов, запущенных командой `startServer` или `startManager`. Например, если вы

настроите сервер или Администратор развертывания как службу Linux и выполните команду startServer или startManager, то команда wasservice запустит определенные службы. По умолчанию продукт не настроен для запуска в качестве службы Linux. Для создания службы необходимо, чтобы пользователь, запускающий Инструмент управления профайлами, был пользователем root. Если вы запустите Инструмент управления профайлами под управлением пользователя, отличного от root, то страница Определение службы Linux не появится и служба создана не будет. Вы должны указать имя пользователя, под управлением которого запускается служба. Для удаления службы Linux пользователь должен быть пользователем root или у него должны быть соответствующие права на удаление службы. В противном случае будет создан сценарий удаления, который сможет запустить пользователь root, чтобы удалить службу от имени текущего пользователя.

- 9) На странице Обзор профайла нажмите **Создать**, чтобы создать профайл, или **Назад**, чтобы изменить характеристики профайла.

Информация о ходе настройки отображается в окне Ход настройки профайла. По окончании создания профайла появляется страница Создание профайла закончено с сообщением **Инструмент управления профайлами успешно создал профайл**.

Внимание: Если во время создания профайла возникнут ошибки, то вместо сообщения об успешном завершении могут появиться другие сообщения, например:




- **Инструмент управления профайлами создал профайл, но с ошибками**, что означает, что профайл был создан, но во время его создания возникли ошибки.
- **Инструмент управления профайлами не создал профайл**, что означает, что создать профайл не удалось.

На странице Создание профайла закончено указан файл протокола, который поможет вам устранить неполадки.

2. Запустите профайл Администратора развертывания.

Запустите Администратор развертывания, введя команду startServer из каталога *каталог_профайла/bin*.

Синтаксис команды:




-   startServer.sh *имя_сервера*
-  startServer.bat *имя_сервера*

Дополнительная информация о команде startServer приведена в разделе Команда startServer в Information Center продукта WebSphere Application Server версии 7.0.

3. Создайте настраиваемые профайлы (управляемые узлы).

- a. Запустите Инструмент управления профайлами.

Выполните одну из следующих команд:

-   *каталог_установки/bin/ProfileManagement/pmt.sh*
-  *каталог_установки\bin\ProfileManagement\pmt.bat*

- b. На начальной странице выберите **Запустить Инструмент управления профайлами** или щелкните на вкладке Инструмент управления профайлами.

Откроется вкладка Профайлы.




Вкладка Профайлы содержит список профайлов, созданных на вашем компьютере. Для создания новых и дополнения существующих профайлов можно воспользоваться Инструментом управления профайлами.

- c. На вкладке Профайлы нажмите **Создать**.
В отдельном окне откроется страница Выбор среды.
- d. На странице Выбор среды разверните раздел **Business Space на основе WebSphere**, выберите опцию **Business Space на основе настраиваемого профайла WebSphere** и нажмите **Далее**.
- e. На странице Опции создания профайла выберите между **Обычным созданием профайла** и **Расширенным созданием профайла**.
- f. Если вы выбрали опцию **Обычное создание профайла**, выполните следующие действия.
 - 1) На странице Объединение выберите добавление узла в Администратор развертывания - сейчас, в процедуре создания профайла, или позже, с помощью команды addNode, вне процедуры создания профайла. Отметьте или сотрите отметку с переключателя **Добавить этот узел позже** и нажмите **Далее**.
 - 2) На странице Обзор профайла нажмите **Создать**, чтобы создать профайл, или **Назад**, чтобы изменить характеристики профайла.
Информация о ходе настройки отображается в окне Ход настройки профайла. По окончании создания профайла появляется страница Создание профайла закончено с сообщением **Инструмент управления профайлами успешно создал профайл**.

Внимание: Если во время создания профайла возникнут ошибки, то вместо сообщения об успешном завершении могут появиться другие сообщения, например:

- **Инструмент управления профайлами создал профайл, но с ошибками**, что означает, что профайл был создан, но во время его создания возникли ошибки.
- **Инструмент управления профайлами не создал профайл**, что означает, что создать профайл не удалось.

На странице Создание профайла закончено указан файл протокола, который поможет вам устранить неполадки.

- g. Если вы выбрали опцию **Расширенное создание профайла**, выполните следующие действия.
 - 1) На странице Имя и расположение профайла выполните следующие действия:
 - a) В поле Имя профайла укажите уникальное имя или оставьте значение по умолчанию. У каждого создаваемого профайла должно быть имя. Если профайлов несколько, вы сможете различать их по именам. Если вы решили не оставлять имя по умолчанию, то, в случае Windows, укажите краткое имя, поскольку длина путей к файлам ограничена.
 - b) В поле Каталог профайла укажите каталог профайла или выберите его с помощью кнопки Обзор. Указанный каталог будет содержать файлы для среды выполнения, например, команды, файлы конфигурации и файлы протоколов. Каталог по умолчанию зависит от платформы:
 -  **Linux**  **UNIX** каталог_установки/profiles/имя_профайла
 -  **Windows** каталог_установки\profiles\имя_профайлагде *имя_профайла* - это указанное имя.

Поле каталога профайла должно отвечать следующим требованиям:

- *имя_профайла* должно быть уникальным.
 - Указанный каталог должен быть пустым.
 - Каталог должен быть доступен вашему ИД пользователя.
 - Для создания профайла должно быть достаточно памяти.
- c) Необязательно: отметьте переключатель **Применять этот профайл по умолчанию**, если вы хотите, чтобы создаваемый профайл применялся по умолчанию. Этот переключатель появляется только при наличии профайла в системе.

Команды автоматически применяют профайл по умолчанию. Первый профайл, который вы создаете на рабочей станции, становится профайлом по умолчанию. Профайл по умолчанию - это цель по умолчанию для команд, выполняемых из каталога bin в каталоге установки продукта. Если на рабочей станции только один профайл, то каждая команда работает с ним. Если профайлов несколько, то некоторые команды требуют выбрать профайл.

d) Нажмите **Далее**.

2) На странице Имена узла и хоста выполните следующие действия для создаваемого профайла:

- a) В поле Имя узла введите имя узла или оставьте значение по умолчанию. Имена узлов следует выбирать максимально короткими, но вместе с тем уникальными в среде разработки.
- b) В поле Имя хоста введите имя хоста или оставьте значение по умолчанию.
- c) В поле Имя ячейки введите имя ячейки или оставьте значение по умолчанию.

Нажмите **Далее** для перехода к странице Административная защита.

3) На странице Объединение выберите добавление узла в Администратор развертывания - сейчас, в процедуре создания профайла, или позже, с помощью команды addNode, вне процедуры создания профайла. Отметьте или сотрите отметку с переключателя **Добавить этот узел позже** и нажмите **Далее**.

4) На странице Сертификат защиты (Часть 1) укажите, следует ли создавать новые или импортировать существующие сертификаты. Выполните следующие действия:

- Для создания нового личного сертификата по умолчанию и нового подписывающего сертификата root выберите **Создать новый личный сертификат по умолчанию** и **Создать новый подписывающий сертификат root** и нажмите **Далее**.
- Для импортирования существующих сертификатов выберите **Импортировать существующий личный сертификат по умолчанию** и **Импортировать существующий личный подписывающий сертификат root** и укажите следующую информацию:
 - В поле Путь введите путь к существующему сертификату.
 - В поле Пароль введите пароль к сертификату.
 - В поле Тип хранилища ключей выберите тип хранилища ключей для импортируемого сертификата.
 - В поле Псевдоним хранилища ключей выберите псевдоним хранилища ключей для импортируемого сертификата.
 - Нажмите кнопку **Далее**.

Когда вы импортируете личный сертификат в качестве личного сертификата по умолчанию, импортируйте вместе с ним подписавший его сертификат root. В противном случае Инструмент управления профайлами добавит подписант личного сертификата в файл trust.p12. Если вы импортируете личный сертификат по умолчанию или подписывающий сертификат root, то укажите путь и пароль, а затем выберите тип и псевдоним хранилища ключей для каждого импортируемого сертификата.

- 5) На странице Сертификат защиты (Часть 2) проверьте правильность информации сертификата и нажмите **Далее** для перехода к странице Назначение значений портов.

Если вы создаете сертификаты, то вы можете использовать значения по умолчанию или изменить их для создания новых сертификатов. Личный сертификат по умолчанию действителен в течение одного года (по умолчанию) и подписывается подписывающим сертификатом root. Подписывающий сертификат root - это собственный сертификат, действительный в течение 15 лет (по умолчанию). Пароль к хранилищу ключей по умолчанию для подписывающего сертификата root - WebAS. Измените пароль. Пароль не может содержать символов из набора двухбайтовых символов (DBCS), поскольку некоторые типы хранилищ ключей, в том числе PKCS12, не поддерживают их. Поддерживаемые типы хранилищ ключей зависят от провайдеров, указанных в файле java.security.

Когда вы создаете один или оба сертификата или импортируете один или оба сертификата, создаются следующие файлы хранилища ключей:

- key.p12: содержит личный сертификат по умолчанию.
- trust.p12: содержит подписывающий сертификат из сертификата root по умолчанию.
- root-key.p12: содержит подписывающий сертификат root.
- default-signers.p12: содержит подписывающие сертификаты, которые добавляются в любой новый файл хранилища ключей, который вы создаете после установки и запуска сервера. По умолчанию подписант сертификата root по умолчанию и подписывающий сертификат DataPower[®] содержатся в этом файле хранилища ключей.
- deleted.p12: содержит сертификаты, удаляемые задачей deleteKeyStore, так что их можно восстановить при необходимости.
- ltpa.jseks: содержит ключи Простого протокола идентификации третьих сторон (ЛТРА) по умолчанию для сервера, применяемые серверами среды для обмена информацией друг с другом.

Всем этим файлам присваивается один и тот же пароль, когда вы создаете или импортируете сертификаты. Это либо пароль по умолчанию, либо указанный вами пароль. Импортированный сертификат добавляется в файл key.p12 или root-key.p12. Если вы импортируете ненужные сертификаты, нажмите **Назад**, чтобы сменить импортируемый сертификат.

- 6) На странице Обзор профайла нажмите **Создать**, чтобы создать профайл, или **Назад**, чтобы изменить характеристики профайла.

Информация о ходе настройки отображается в окне Ход настройки профайла. По окончании создания профайла появляется страница Создание профайла закончено с сообщением **Инструмент управления профайлами успешно создал профайл.**

Внимание: Если во время создания профайла возникнут ошибки, то вместо сообщения об успешном завершении могут появиться другие сообщения, например:




- **Инструмент управления профайлами создал профайл, но с ошибками**, что означает, что профайл был создан, но во время его создания возникли ошибки.
- **Инструмент управления профайлами не создал профайл**, что означает, что создать профайл не удалось.

На странице Создание профайла закончено указан файл протокола, который поможет вам устранить неполадки.

4. Войдите в административную консоль Администратора развертывания.
5. В зависимости от того, хотите вы развернуть Business Space в кластере или на управляемых серверах, создайте один из следующих объектов:
 - Для кластера:
 - a. Создайте кластер серверов приложений.
 - b. Добавьте один или несколько участников в кластер (это настраиваемые профайлы Business Space, которые были созданы ранее).
 - Для каждого управляемого сервера:
 - a. Создайте сервер приложений.
 - b. Выберите узел управляемого сервера, который станет созданным ранее настраиваемым профайлом Business Space.
6. Остановите профайл Администратора развертывания.

Остановите Администратор развертывания, введя команду `stopServer` из каталога *каталог_профайла/bin*.

Синтаксис команды:

-   `stopServer.sh имя_сервера -username имя_пользователя -password пароль`
-  `stopServer.bat имя_сервера -username имя_пользователя -password пароль`

Если в профайле защита выключена, параметры `-username` и `-password` необязательны.

Дополнительная информация о команде `stopServer` приведена в разделе Команда `stopServer` в Information Center продукта WebSphere Application Server версии 7.0.

7. Перейдите в каталог *каталог_установки/BusinessSpace/config.ospace/MetadataFiles* и, в зависимости от типа базы данных, который вы будете использовать для Business Space, скопируйте соответствующий файл в рабочий каталог. Не изменяйте расширение этого файла: оно должно быть `.properties`.
 - a. Отредактируйте копию этого файла, изменив значения в соответствии с вашей базой данных. Обратите особое внимание на свойство `wasHome` и убедитесь, что оно задано правильно.
 - b. По окончании внесения в файл информации, соответствующей вашей базе данных, сохраните его.

Закончив создание профайлов и указав в них информацию, соответствующую вашей базе данных, вы можете приступить к настройке Business Space в среде; для этого выполните следующие действия.

1. Для каждого кластера или управляемого сервера выполните команду **`installBusinessSpace`**, чтобы установить файлы EAR Business Space в среде выполнения. Задайте либо параметр **`clusterName`**, либо параметры **`nodeName`** и

serverName, в зависимости от того, как вы настроили топологию сетевого развертывания. См. раздел “Настройка Business Space с помощью командной строки” на стр. 200.

2. Для каждого кластера или управляемого сервера выполните команду **configureBusinessSpace**, задав либо параметр **clusterName**, либо параметры **nodeName** и **serverName**, в зависимости от того, как вы настроили топологию сетевого развертывания. Кроме того, задайте параметр **bspacedbDesign**. Значением этого параметра должен быть путь к ранее отредактированному файлу свойств базы данных. См. раздел “Настройка Business Space с помощью командной строки” на стр. 200.
3. Сохраните конфигурацию wsadmin.
4. Создайте и настройте базу данных Business Space. См. раздел “Настройка базы данных Business Space” на стр. 203.
5. Запустите Администратор развертывания.
6. Запустите кластеры или управляемые серверы.

Создание профайлов Business Space для конфигурации сетевого развертывания с помощью утилиты командной строки managerprofiles:

С помощью утилиты командной строки managerprofiles можно создавать профайлы Администратора развертывания и настраиваемые профайлы (управляемые узлы) для конфигурации сетевого развертывания Business Space.

Прежде чем запускать утилиту командной строки managerprofiles, выполните следующие задачи:

- Просмотрите полный список предварительных требований по созданию или дополнению профайла, приведенный в разделе Концепции профайла справочной системы WebSphere Application Server Information Center.
- Просмотрите примеры команд создания профайла.
- Убедитесь, что в данный момент утилита командной строки managerprofiles не запущена по отношению к выбранному профайлу. Если выдается сообщение об ошибке, выясните, не выполняется ли другое действие по созданию или дополнению профайла в данный момент. Если это так, дождитесь его завершения.

В этой задаче указано, как с помощью утилиты командной строки managerprofiles можно создавать профайлы Business Space для конфигурации сетевого развертывания Business Space. Для того чтобы создать профайл с помощью утилиты командной строки managerprofiles, выполните следующие действия.

1. Создайте профайл Администратора развертывания.
 - a. Найдите шаблон dmgr.bspace для профайлов Администратора развертывания Business Space, определяющих Администраторы развертывания. Администратор развертывания предоставляет единый административный интерфейс логической группе серверов на одной или нескольких рабочих станциях.
Шаблоны для каждого профайла находятся в каталоге *каталог_установки/profileTemplates/BusinessSpace*.
 - b. Определите, какие параметры необходимы для создания профайла, изучив раздел “Утилита командной строки managerprofiles (для профайлов Business Space)” на стр. 175. Просмотрите значения по умолчанию и определите, какие значения необходимо указать для профайла. Например, вы можете задать параметры -templatePath, -serverType, -enableAdminSecurity, -adminUserName и -adminPassword.
 - c. Запустите файл из командной строки. Простой пример:


```
manageProfiles -create -templatePath каталог_установки/profileTemplates/BusinessSpace/dmgr.  
-serverType DEPLOYMENT_MANAGER -enableAdminSecurity true -adminUserName  
ИД_администратора -adminPassword  
пароль_администратора
```

Команда показывает индикатор хода своего выполнения. Дождитесь окончания ее выполнения. Когда файл ответов анализируется подобно любому другому файлу ответов, он проходит обычную синтаксическую проверку. Отдельные значения в файле ответов считаются параметрами командной строки.

2. Запустите профайл Администратора развертывания.

Запустите Администратор развертывания, введя команду startServer из каталога *каталог_профайла/bin*.

Синтаксис команды:

- ▶ Linux  startServer.sh имя_сервера
- ▶ Windows startServer.bat имя_сервера

Дополнительная информация о команде startServer приведена в разделе Команда startServer в Information Center продукта WebSphere Application Server версии 7.0.

3. Создайте настраиваемые профайлы (управляемые узлы).

- Найдите шаблон managed.bspaces для настраиваемых профайлов Business Space, которые, будучи добавленными в Администратор развертывания, определяют управляемые узлы. Если вашему решению требуется среда развертывания, то в среду выполнения необходимо добавить один или несколько управляемых узлов. Настраиваемый профайл содержит пустой узел, который необходимо добавить в ячейку Администратора развертывания, чтобы сделать его рабочим. Добавление настраиваемого профайла превращает его в управляемый узел. Добавляйте узел только в том случае, если версия Администратора развертывания, в который вы добавляете узел, не ниже версии создаваемого настраиваемого профайла.

Шаблоны для каждого профайла находятся в каталоге *каталог_установки/profileTemplates/BusinessSpace*.

- Определите, какие параметры необходимы для создания профайла, изучив раздел “Утилита командной строки manageprofiles (для профайлов Business Space)” на стр. 175. Просмотрите значения по умолчанию и определите, какие значения необходимо указать для профайла. Например, вы можете задать параметры -templatePath, -dmgrAdminUserName, -dmgrAdminPassword, -dmgrPort и -dmgrHost.

- Запустите файл из командной строки. Простой пример:

```
manageProfiles -create -templatePath каталог_установки/profileTemplates/BusinessSpace/manag  
-dmgrAdminUserName ИД_администратора_Администратора_развертывания  
-dmgrAdminPassword пароль_администратора_Администратора_развертывания  
-dmgrPort порт_Администратора_развертывания -dmgrHost  
хост_Администратора_развертывания
```

Команда показывает индикатор хода своего выполнения. Дождитесь окончания ее выполнения. Когда файл ответов анализируется подобно любому другому файлу ответов, он проходит обычную синтаксическую проверку. Отдельные значения в файле ответов считаются параметрами командной строки.




4. Войдите в административную консоль Администратора развертывания.

- В зависимости от того, хотите вы развернуть Business Space в кластере или на управляемых серверах, создайте один из следующих объектов:

- Для кластера:
 - a. Создайте кластер серверов приложений.
 - b. Добавьте один или несколько участников в кластер (это настраиваемые профайлы Business Space, которые были созданы ранее).
 - Для каждого управляемого сервера:
 - a. Создайте сервер приложений.
 - b. Выберите узел управляемого сервера, который станет созданным ранее настраиваемым профайлом Business Space.
6. Остановите профайл Администратора развертывания.

Остановите Администратор развертывания, введя команду `stopServer` из каталога *каталог_профайла/bin*.

Синтаксис команды:

-   `stopServer.sh имя_сервера -username имя_пользователя -password пароль`
-  `stopServer.bat имя_сервера -username имя_пользователя -password пароль`

Если в профайле защита выключена, параметры `-username` и `-password` необязательны.

Дополнительная информация о команде `stopServer` приведена в разделе Команда `stopServer` в Information Center продукта WebSphere Application Server версии 7.0.

7. Перейдите в каталог *каталог_установки/BusinessSpace/config.ospace/MetadataFiles* и, в зависимости от типа базы данных, который вы будете использовать для Business Space, скопируйте соответствующий файл в рабочий каталог. Не изменяйте расширение этого файла: оно должно быть `.properties`.
- a. Отредактируйте копию этого файла, изменив значения в соответствии с вашей базой данных. Обратите особое внимание на свойство `wasHome` и убедитесь, что оно задано правильно.
 - b. По окончании внесения в файл информации, соответствующей вашей базе данных, сохраните его.

Закончив создание профайлов и указав в них информацию, соответствующую вашей базе данных, вы можете приступить к настройке Business Space в среде; для этого выполните следующие действия.

1. Для каждого кластера или управляемого сервера выполните команду **`installBusinessSpace`**, чтобы установить файлы EAR Business Space в среде выполнения. Задайте либо параметр **`clusterName`**, либо параметры **`nodeName`** и **`serverName`**, в зависимости от того, как вы настроили топологию сетевого развертывания. См. раздел “Настройка Business Space с помощью командной строки” на стр. 200.
2. Для каждого кластера или управляемого сервера выполните команду **`configureBusinessSpace`**, задав либо параметр **`clusterName`**, либо параметры **`nodeName`** и **`serverName`**, в зависимости от того, как вы настроили топологию сетевого развертывания. Кроме того, задайте параметр **`bspacedbDesign`**. Значением этого параметра должен быть путь к ранее отредактированному файлу свойств базы данных. См. раздел “Настройка Business Space с помощью командной строки” на стр. 200.
3. Сохраните конфигурацию `wsadmin`.
4. Создайте и настройте базу данных Business Space. См. раздел “Настройка базы данных Business Space” на стр. 203.
5. Запустите Администратор развертывания.

6. Запустите кластеры или управляемые серверы.

Дополнение профайлов Business Space для автономной конфигурации:

Для дополнения профайлов Business Space для автономной среды можно использовать инструмент управления профайлами или утилиту командной строки `manageprofiles`.

Если Business Space настроен как часть профайла продукта, выполнять эти задачи необязательно.

Дополнение профайлов Business Space для автономной конфигурации с помощью инструмента управления профайлами:

Для дополнения автономных профайлов для Business Space можно использовать инструмент управления профайлами.

Знание концепций профайлов, включая различия между автономными профайлами, профайлами сетевого развертывания и пользовательскими профайлами. Понимание разницы между обычным и расширенным дополнением профайла и знание того, в каких случаях какой вариант следует применять. При обычном дополнении профайл дополняется параметрами конфигурации по умолчанию. Расширенное дополнение профайла позволяет указать собственные значения параметров дополняемого профайла.




- Ознакомьтесь с полным списком предварительных требований для создания или дополнения профайла в разделе Концепции профайлов в WebSphere Application Server Information Center.
- При использовании инструмента управления профайлами с графическим пользовательским интерфейсом Motif в операционной системе Solaris стандартный размер инструмента может оказаться недостаточным для отображения всех сообщений и кнопок.
- Если предполагается использовать файл эскиза базы данных с информацией о базе данных Business Space, выполните действия из раздела “Создание файла свойств эскиза базы данных Business Space” на стр. 203.

Эту процедуру следует применять при дополнении профайла Business Space для автономной конфигурации. Здесь описываются Обычный и Расширенный варианты создания профайла.

Если Business Space дополнен как часть профайла продукта, выполнять эту задачу необязательно.

1. Запустите инструмент управления профайлами.

Используйте одну из следующих команд:

-   `каталог-установки/bin/ProfileManagement/pmt.sh`
-  `каталог-установки\bin\ProfileManagement\pmt.bat`

Откроется начальная страница .

2. На начальной странице нажмите **Запустить инструмент управления профайлами** или выберите вкладку Инструмент управления профайлами.

Откроется вкладка Профайлы.

Вкладка Профайлы содержит текущий список профайлов в системе. В данной процедуре предполагается, что будет выполнено дополнение существующего профайла сервера приложений с Business Space в автономной конфигурации.

3. Выберите профайл, который требуется дополнить, и нажмите **Дополнить**. Если дополнение профайла не предусмотрено, кнопка **Дополнить** будет недоступна для выбора.

В отдельном окне откроется страница Выбор типа дополнения.

4. На странице Выбор дополнения доступен вариант **Автономный профайл**, если профайл может быть дополнен для Business Space. Нажмите **Далее**.
5. На странице Параметры дополнения профайла выберите **Обычный** или **Расширенный**.

При обычном дополнении профайл дополняется параметрами конфигурации по умолчанию. Расширенное дополнение профайла позволяет указать собственные значения параметров дополняемого профайла.

6. При выборе варианта **Обычный** дополнения профайла выполните следующие действия.
 - a. На странице Административная защита еще раз введите имя и пароль администратора для дополняемого профайла.
 - b. На странице Обзор дополнения профайла нажмите **Дополнить**, чтобы дополнить профайл, или **Назад**, чтобы изменить параметры профайла.
Состояние процесса дополнения показывается в окне Состояние процесса настройки. По завершении процесса дополнения профайла должна открыться страница Профайл дополнен с сообщением **Инструмент управления профайлами дополнил профайл**.

Внимание: При возникновении ошибок во время дополнения профайла показываются другие сообщения, например:

- **Инструмент дополнения профайлов дополнил профайл, но при этом возникли ошибки.** Это сообщение означает, что профайл дополнен, но возникли ошибки.
- **Инструменту управления профайлами не удалось дополнить профайл.** Это сообщение означает, что профайл не дополнен.

На странице Профайл дополнен указан файл протокола, к которому можно обратиться для устранения неполадок.

7. При выборе варианта **Дополнение расширенного профайла** выполните следующие действия.
 - a. На странице Административная защита еще раз введите имя и пароль администратора для дополняемого профайла.
 - b. Если для настройки базы данных дополняемого профайла предполагается использовать существующий файл эскиза, вместо настройки на страницах Настройка базы данных выполните следующие действия.
 - 1) Выберите **Использовать файл эскиза базы данных** для настройки базы данных.
 - 2) Нажмите **Обзор**.
 - 3) Укажите полное имя пути к файлу эскиза.
 - 4) Нажмите **Далее**.
 - c. Если файл эскиза базы данных не применяется, выполните на странице Настройка базы данных следующие действия:
 - 1) В списке Выберите продукт базы данных выберите продукт базы данных, который будет использоваться профайлом.
 - 2) Включите переключатель **Переопределить каталог вывода по умолчанию для сценариев базы данных**, если требуется указать каталог, куда сценарии

SQL для создания таблиц базы данных будут записывать данные. Если этот переключатель выключен, сценарии выводят данные в каталог по умолчанию.

- 3) Нажмите **Далее**, чтобы перейти на страницу Настройка базы данных (часть 2).

Информация на странице Настройка базы данных (часть 2) зависит от значения, выбранного в списке Выберите продукт базы данных на странице Настройка базы данных.

- d. На странице Настройка базы данных (часть 2) укажите параметры конфигурации базы данных. В зависимости от продукта базы данных необходимо указать имя пользователя и пароль для идентификации в базе данных, информацию о драйвере JDBC, хост, порт и схему.
- e. На странице Обзор дополнения профайла нажмите **Дополнить**, чтобы дополнить профайл, или **Назад**, чтобы изменить параметры профайла. Состояние процесса дополнения показывается в окне Состояние процесса настройки. По завершении процесса дополнения профайла должна открыться страница Профайл дополнен с сообщением **Инструмент управления профайлами дополнил профайл**.

Внимание: При возникновении ошибок во время дополнения профайла показываются другие сообщения, например:

- **Инструмент дополнения профайлов дополнил профайл, но при этом возникли ошибки.** Это сообщение означает, что профайл дополнен, но возникли ошибки.
- **Инструменту управления профайлами не удалось дополнить профайл.** Это сообщение означает, что профайл не дополнен.

На странице Профайл дополнен указан файл протокола, к которому можно обратиться для устранения неполадок.

Если дополняется профайл, в котором уже настроена защита с хранилищем пользователей, не являющимся одним из объединенных хранилищ по умолчанию; необходимо скорректировать параметр `MashupAdminForOOBSpace` в файле `ConfigServices.properties`. См. раздел “Выбор хранилища пользователей для Business Space” на стр. 225.

Дополнение профайлов Business Space для автономной конфигурации с помощью утилиты командной строки `manageprofiles`:

Автономные профайлы для Business Space можно дополнять из командной строки с помощью утилиты `manageprofiles`.

Перед тем как дополнять профайл с помощью утилиты **`manageprofiles`**, выполните следующие задачи:

- Ознакомьтесь с полным списком предварительных требований для создания или дополнения профайла в разделе Концепции профайлов в WebSphere Application Server Information Center.
- Посмотрите примеры команд для создания профайла.
- Убедитесь, что в этом профайле утилита командной строки `manageprofiles` еще не выполняется. Если откроется сообщение об ошибке; проверьте, не выполняется ли другая операция создания или дополнения профайла. Если выполняется, дождитесь ее завершения.
- Остановите все серверы, связанные с дополняемым профайлом.

- Узнайте, добавлен ли дополняемый профайл в администратор развертывания. Если дополняемый профайл добавлен в конфигурацию администратора развертывания, его нельзя дополнять с помощью утилиты командной строки `manageprofiles`.
- Определите, с помощью какого шаблона (администратора развертывания, автономного или управляемого) был создан существующий профайл. Для этого просмотрите реестр профайлов в файле *каталог-установки/properties/profileRegistry.xml*. Не изменяйте этот файл, им можно пользоваться только для просмотра шаблонов. В этой процедуре подразумевается, что дополняется профайл автономный профайл Process Server.

Для того чтобы дополнить профайл Business Space для автономной конфигурации с помощью утилиты командной строки **manageprofiles** выполните следующие действия.

Если Business Space дополнен как часть профайла продукта, выполнять эту задачу необязательно.

1. Найдите шаблон профайла `default.bspace` для автономных профайлов Business Space, который определяет автономные серверы.

Шаблоны для каждого профайла находятся в каталоге *каталог-установки/profileTemplates/BusinessSpace*.

Для внесения изменений в существующие профайлы с помощью шаблона дополнения используется параметр **augment**. Когда указан параметр **augment**, утилита командной строки **manageprofiles** выполняет обновление или дополнение профайла, указанного в параметре **-profileName**, с помощью шаблона, указанного в параметре **-templatePath**. Шаблоны дополнения, доступные для использования, зависят от того, какие продукты IBM и каких версий установлены в среде. В параметре **-templatePath** следует указывать полный путь, поскольку если указан относительный путь, дополнение указанного профайла будет выполнено не полностью.

2. Запустите файл из командной строки. Параметр **-profilePath** указывать не следует. Простой пример:

```
manageProfiles -augment -profileName имя-профайла -templatePath
каталог-установки/profileTemplates/BusinessSpace/default.bspace -cellName имя-ячейки
-nodeName имя-узла -enableAdminSecurity true -adminUserName admin
-adminPassword admin -dbType DB2_Universal -dbUserId имя-пользователя-базы-данных
-dbPassword пароль-базы-данных -dbJDBCClasspath каталог-установки/jdbcdrivers/DB2
-dbName имя-базы-данных -bSpaceSchema схема-базы-данных -dbHostName
имя-хоста-базы-данных -dbServerPort порт-базы-данных -dbDelayConfig false
```

После выполнения команды в окно консоли будет выведена информация о состоянии.

Если дополняется профайл, в котором уже настроена защита с хранилищем пользователей, не являющимся одним из объединенных хранилищ по умолчанию; необходимо скорректировать параметр `MashupAdminForOOBSpace` в файле `ConfigServices.properties`. См. раздел “Выбор хранилища пользователей для Business Space” на стр. 225.

Дополнение профайлов Business Space для конфигурации сетевого развертывания:

Для дополнения профайлов Business Space для конфигурации сетевого развертывания можно использовать инструмент управления профайлами или утилиту командной строки `manageprofiles`.

Если Business Space настроен как часть профайла продукта, выполнять эти задачи необязательно.

Дополнение профайлов Business Space для конфигурации сетевого развертывания с помощью инструмента управления профайлами:

Для дополнения профайлов Business Space для среды сетевого развертывания можно использовать инструмент управления профайлами.

Знание концепций профайлов, включая различия между автономными профайлами, профайлами сетевого развертывания и пользовательскими профайлами. Понимание разницы между обычным и расширенным дополнением профайла и знание того, в каких случаях какой вариант следует применять. При обычном дополнении профайл дополняется параметрами конфигурации по умолчанию. Расширенное дополнение профайла позволяет указать собственные значения параметров дополняемого профайла.

- Ознакомьтесь с полным списком предварительных требований для создания или дополнения профайла в разделе Концепции профайлов в WebSphere Application Server Information Center.
- При использовании инструмента управления профайлами с графическим пользовательским интерфейсом Motif в операционной системе Solaris стандартный размер инструмента может оказаться недостаточным для отображения всех сообщений и кнопок.




Эту процедуру следует применять при дополнении профайла Business Space для конфигурации сетевого развертывания. Здесь описываются Обычный и Расширенный варианты дополнения профайла. В этой процедуре предполагается, что есть профайл администратора развертывания и пользовательские профайлы (управляемые узлы), которые требуется добавить в Business Space.

Если Business Space дополнен как часть профайла продукта, выполнять эту задачу необязательно.

1. Дополните профайл администратора развертывания.

- a. Запустите инструмент управления профайлами.

Используйте одну из следующих команд:

-   `каталог-установки/bin/ProfileManagement/pmt.sh`
-  `каталог-установки\bin\ProfileManagement\pmt.bat`

- b. На начальной странице нажмите **Запустить инструмент управления профайлами** или выберите вкладку Инструмент управления профайлами.

Откроется вкладка Профайлы.

Вкладка Профайлы содержит список профайлов, созданных в системе. С помощью инструмента управления профайлами можно создать новые профайлы и дополнить существующие.

- c. На вкладке Профайлы нажмите **Дополнить**.

В отдельном окне откроется страница Выбор типа дополнения.

- d. На странице Выбор дополнения разверните раздел **Business Space на основе WebSphere**, выберите **Администратор развертывания Business Space** и нажмите **Далее**.

- e. На странице Параметры дополнения профайла выберите **Обычный** или **Расширенный**.

- f. На странице Административная защита введите имя пользователя, пароль и подтверждение пароля и нажмите **Далее**. Всем параметрам конфигурации

профайла, включая параметры профайла, будут присвоены значения по умолчанию; эти значения показываются на странице Обзор дополнения профайла.

- g. На странице Обзор дополнения профайла нажмите **Дополнить**, чтобы дополнить профайл, или **Назад**, чтобы изменить параметры профайла. Состояние процесса настройки показывается в окне Состояние процесса настройки. По завершении процесса дополнения профайла откроется страница Профайл дополнен с сообщением **Инструмент управления профайлами дополнил профайл**.

Внимание: При возникновении ошибок во время дополнения профайла показываются другие сообщения, например:




- **Инструмент дополнения профайлов дополнил профайл, но при этом возникли ошибки.** Это сообщение означает, что профайл дополнен, но возникли ошибки.
- **Инструменту управления профайлами не удалось дополнить профайл.** Это сообщение означает, что профайл не дополнен.

На странице Профайл дополнен указан файл протокола, к которому можно обратиться для устранения неполадок.

2. Запустите профайл.

Запустите профайл командой `startServer` из каталога *корневой-каталог-профайла/bin*.

Синтаксис команды:




-   `startServer.sh имя-сервера`
-  `startServer.bat имя-сервера`

Дополнительная информация о команде `startServer` приведена в разделе Команда `startServer` в Information Center продукта WebSphere Application Server версии 7.0.

3. Дополните пользовательские профайлы (управляемые узлы).

- a. Запустите инструмент управления профайлами.

Используйте одну из следующих команд:

-   `каталог-установки/bin/ProfileManagement/pmt.sh`
-  `каталог-установки\bin\ProfileManagement\pmt.bat`

- b. На начальной странице нажмите **Запустить инструмент управления профайлами** или выберите вкладку Инструмент управления профайлами.

Откроется вкладка Профайлы.

Вкладка Профайлы содержит список профайлов, созданных в системе. С помощью инструмента управления профайлами можно создать новые профайлы и дополнить существующие.

- c. На вкладке Профайлы нажмите **Дополнить**.

В отдельном окне откроется страница Выбор типа дополнения.

- d. На странице Выбор дополнения разверните раздел **Business Space на основе WebSphere**, выберите **Пользовательский профайл Business Space** и нажмите **Далее**.

- e. На странице Параметры дополнения профайла выберите **Обычный** или **Расширенный**.

- f. На странице Объединение выберите добавление узла в администратор развертывания немедленно, во время создания профайла, или позднее,

отдельно от создания профайла, командой addNode. Включите или выключите переключатель **Добавить этот узел позднее** и нажмите **Далее**.

- g. На странице Обзор дополнения профайла нажмите **Создать**, чтобы создать профайл, или **Назад**, чтобы изменить параметры профайла.

Состояние процесса настройки показывается в окне Состояние процесса настройки. По завершении процесса дополнения профайла откроется страница Профайл дополнен с сообщением **Инструмент управления профайлами дополнил профайл**.

Внимание: При возникновении ошибок во время создания профайла показываются другие сообщения, например:




- **Инструмент дополнения профайлов дополнил профайл, но при этом возникли ошибки.** Это сообщение означает, что профайл создан, но возникли ошибки.
- **Инструменту управления профайлами не удалось дополнить профайл.** Это сообщение означает, что профайл создать не удалось.

На странице Профайл дополнен указан файл протокола, к которому можно обратиться для устранения неполадок.

4. Войдите в административную консоль администратора развертывания.
5. Необязательно: Если кластера или управляемых серверов еще нет, выполните одно из следующих действий для своей среды:
 - Для кластера:
 - a. Создайте кластер сервера приложений.
 - b. Добавьте в кластер один или несколько элементов (пользовательских профайлов Business Space, созданных ранее).
 - Для каждого управляемого сервера:
 - a. Создайте сервер приложений.
 - b. Выберите для узла управляемого сервера созданный ранее пользовательский профайл Business Space.
6. Остановите профайл администратора развертывания.

Остановите администратор развертывания командой stopServer из каталога *каталог-профайла/bin*.

Синтаксис команды:

-   stopServer.sh *имя-сервера* -username *имя-пользователя* -password *пароль*
-  stopServer.bat *имя-сервера* -username *имя-пользователя* -password *пароль*

Если в профайле защита выключена, параметры -username и -password необязательны.

Дополнительная информация о команде stopServer приведена в разделе Команда stopServer в Information Center продукта WebSphere Application Server версии 7.0.

7. Перейдите в каталог *каталог-установки/BusinessSpace/config.ospace/MetadataFiles* и скопируйте в рабочий каталог файл, соответствующий типу базы данных, которая будет использоваться для Business Space. Расширение этого файла менять нельзя, оно должно быть .properties.
 - a. Укажите в копии этого файла значения параметров для используемой базы данных. Обратите особое внимание на свойство wasHome и убедитесь, что оно правильное.
 - b. После ввода информации о базе данных в файл сохраните его.

После создания профайлов и настройки параметров базы данных для профайлов можно настроить Business Space в среде; для этого выполните следующие действия.

1. Для каждого кластера или управляемого сервера выполните команду **installBusinessSpace**, чтобы установить файлы EAR Business Space в среду выполнения. Укажите параметр **clusterName** или параметры **nodeName** и **serverName** в зависимости от настроенной топологии сетевого развертывания. См. раздел “Настройка Business Space с помощью командной строки” на стр. 200.
2. Для каждого кластера или управляемого сервера выполните команду **configureBusinessSpace** с параметром **clusterName** или параметрами **nodeName** и **serverName** в зависимости от настроенной топологии сетевого развертывания. Также укажите параметр **bspacedbDesign**. Значение этого параметра должно быть путем к файлу свойств базы данных, который редактировался на одном из предыдущих шагов. См. раздел “Настройка Business Space с помощью командной строки” на стр. 200.
3. Сохраните конфигурацию wsadmin.
4. Создайте и настройте базу данных Business Space. См. раздел “Настройка базы данных Business Space” на стр. 203.
5. Запустите администратор развертывания.
6. Запустите кластеры или управляемые серверы.

Если дополняется профайл, в котором уже настроена защита с хранилищем пользователей, не являющимся одним из объединенных хранилищ по умолчанию; необходимо скорректировать параметр `MashupAdminForOOBSpace` в файле `ConfigServices.properties`. См. раздел “Выбор хранилища пользователей для Business Space” на стр. 225.

Дополнение профайлов Business Space для конфигурации сетевого развертывания с помощью утилиты командной строки `manageprofiles`:

Профайлы Business Space для конфигурации сетевого развертывания можно дополнять из командной строки с помощью утилиты `manageprofiles`.

Перед тем как дополнять профайл с помощью утилиты **manageprofiles**, выполните следующие задачи:

- Ознакомьтесь с полным списком предварительных требований для создания или дополнения профайла в разделе Концепции профайлов в WebSphere Application Server Information Center.
- Посмотрите примеры команд для создания профайла.
- Убедитесь, что в этом профайле утилита командной строки `manageprofiles` еще не выполняется. Если откроется сообщение об ошибке; проверьте, не выполняется ли другая операция создания или дополнения профайла. Если выполняется, дождитесь ее завершения.
- Остановите все серверы, связанные с дополняемым профайлом.
- Узнайте, добавлен ли дополняемый профайл в администратор развертывания. Если дополняемый профайл добавлен в конфигурацию администратора развертывания, его нельзя дополнять с помощью утилиты командной строки `manageprofiles`.
- Определите, с помощью какого шаблона (администратора развертывания, автономного или управляемого) был создан существующий профайл. Для этого просмотрите реестр профайлов в файле *каталог-установки/properties/profileRegistry.xml*. Не изменяйте этот файл, им можно пользоваться только для просмотра шаблонов. В этой процедуре подразумевается, что дополняется профайл администратора развертывания Business Space на основе WebSphere.

Для того чтобы дополнить профайл Business Space для конфигурации сетевого развертывания с помощью утилиты командной строки **manageprofiles** выполните следующие действия. В этой процедуре предполагается, что есть профайл администратора развертывания и пользовательские профайлы (управляемые узлы), которые требуется добавить в Business Space.

Если Business Space дополнен как часть профайла продукта, выполнять эту задачу необязательно.

1. Дополните профайл администратора развертывания.

- a. Найдите шаблон dmgr.bspace для профайлов администратора развертывания Business Space, содержащий определения администраторов развертывания. Администратор развертывания служит единым интерфейсом администрирования логической группы серверов на одной или нескольких рабочих станциях.

Шаблоны для каждого профайла находятся в каталоге *каталог-установки/profileTemplates/BusinessSpace*.

- b. Определите, какие параметры требуются для дополнения профайла (см. раздел “Утилита командной строки manageprofiles (для профайлов Business Space)” на стр. 175). Проверьте значения по умолчанию и определите, подходят ли они для профайла.

Для внесения изменений в существующие профайлы с помощью шаблона дополнения используется параметр **augment**. Когда указан параметр **augment**, утилита командной строки **manageprofiles** выполняет обновление или дополнение профайла, указанного в параметре **-profileName**, с помощью шаблона, указанного в параметре **-templatePath**. Шаблоны дополнения, доступные для использования, зависят от того, какие продукты IBM и каких версий установлены в среде. В параметре **-templatePath** следует указывать полный путь, поскольку если указан относительный путь, дополнение указанного профайла будет выполнено не полностью.

- c. Запустите файл из командной строки. Простой пример:




```
manageProfiles -augment -profileName имя-профайла
               -templatePath каталог-установки/profileTemplates/BusinessSpace/dmgr.bspace
               -serverType DEPLOYMENT_MANAGER -cellName имя-ячейки-управления
               -nodeName имя-узла-управления -enableAdminSecurity true
               -adminUserName имя-администратора -adminPassword пароль-администратора
```

Во время выполнения команды система показывает ее состояние. Дождитесь завершения выполнения.

2. Запустите профайл администратора развертывания.

Запустите профайл командой startServer из каталога *корневой-каталог-профайла/bin*.

Синтаксис команды:

-   startServer.sh *имя-сервера*
-  startServer.bat *имя-сервера*

Дополнительная информация о команде startServer приведена в разделе Команда startServer в Information Center продукта WebSphere Application Server версии 7.0.

3. Дополните пользовательские профайлы (управляемые узлы).

- a. Найдите шаблон managed.bspace для пользовательских профайлов Business Space, который определяет управляемые узлы при добавлении в администратор развертывания. Если для решения требуется среда развертывания, то в рабочей среде должен быть хотя бы один управляемый

узел. Пользовательский профайл содержит пустой узел, который будет работать только после добавления в ячейку администратора развертывания. Добавленный в ячейку пользовательский профайл становится управляемым узлом. Добавлять узел можно лишь в том случае, если выпуск администратора развертывания, на который будет добавлен профайл, не ниже выпуска создаваемого пользовательского профайла.

Шаблоны для каждого профайла находятся в каталоге *каталог-установки/profileTemplates/BusinessSpace*.

- b. Определите, какие параметры требуются для дополнения профайла (см. раздел “Утилита командной строки `manageprofiles` (для профайлов Business Space)” на стр. 175). Проверьте значения по умолчанию и определите, подходят ли они для профайла.

Для внесения изменений в существующие профайлы с помощью шаблона дополнения используется параметр **augment**. Когда указан параметр **augment**, утилита командной строки **manageprofiles** выполняет обновление или дополнение профайла, указанного в параметре **-profileName**, с помощью шаблона, указанного в параметре **-templatePath**. Шаблоны дополнения, доступные для использования, зависят от того, какие продукты IBM и каких версий установлены в среде. В параметре **-templatePath** следует указывать полный путь, поскольку если указан относительный путь, дополнение указанного профайла будет выполнено не полностью.

- c. Запустите файл из командной строки. Простой пример:




```
manageProfiles -augment -profileName имя-профайла
               -templatePath каталог-установки/profileTemplates/BusinessSpace/managed.bspace
               -dmgrAdminUserName имя-администратора -dmgrAdminPassword пароль-администратора
               -dmgrPort порт-администратора-развертывания -dmgrHost имя-хоста-администратора-развертывания
               имя-ячейки-управления -nodeName имя-узла
```

Во время выполнения команды система показывает ее состояние. Дождитесь завершения выполнения.

4. Войдите в административную консоль администратора развертывания.
5. Необязательно: Если кластера или управляемых серверов еще нет, выполните одно из следующих действий для своей среды:
 - Для кластера:
 - a. Создайте кластер сервера приложений.
 - b. Добавьте в кластер один или несколько элементов (пользовательских профайлов Business Space, созданных ранее).
 - Для каждого управляемого сервера:
 - a. Создайте сервер приложений.
 - b. Выберите для узла управляемого сервера созданный ранее пользовательский профайл Business Space.
6. Остановите профайл администратора развертывания.

Остановите администратор развертывания командой `stopServer` из каталога *каталог-профайла/bin*.

Синтаксис команды:

-   `stopServer.sh имя-сервера -username имя-пользователя -password пароль`
-  `stopServer.bat имя-сервера -username имя-пользователя -password пароль`

Если в профайле защита выключена, параметры `-username` и `-password` необязательны.

Дополнительная информация о команде `stopServer` приведена в разделе Команда `stopServer` в Information Center продукта WebSphere Application Server версии 7.0.

7. Перейдите в каталог *каталог-установки*/`BusinessSpace/config.bspace/MetadataFiles` и скопируйте в рабочий каталог файл, соответствующий типу базы данных, которая будет использоваться для Business Space. Расширение этого файла менять нельзя, оно должно быть `.properties`.
 - a. Укажите в копии этого файла значения параметров для используемой базы данных. Обратите особое внимание на свойство `wasHome` и убедитесь, что оно правильное.
 - b. После ввода информации о базе данных в файл сохраните его.

После создания профайлов и настройки параметров базы данных для профайлов можно настроить Business Space в среде; для этого выполните следующие действия.

1. Для каждого кластера или управляемого сервера выполните команду **`installBusinessSpace`**, чтобы установить файлы EAR Business Space в среду выполнения. Укажите параметр **`clusterName`** или параметры **`nodeName`** и **`serverName`** в зависимости от настроенной топологии сетевого развертывания. См. раздел “Настройка Business Space с помощью командной строки” на стр. 200.
2. Для каждого кластера или управляемого сервера выполните команду **`configureBusinessSpace`** с параметром **`clusterName`** или параметрами **`nodeName`** и **`serverName`** в зависимости от настроенной топологии сетевого развертывания. Также укажите параметр **`bspacedbDesign`**. Значение этого параметра должно быть путем к файлу свойств базы данных, который редактировался на одном из предыдущих шагов. См. раздел “Настройка Business Space с помощью командной строки” на стр. 200.
3. Сохраните конфигурацию `wsadmin`.
4. Создайте и настройте базу данных Business Space. См. раздел “Настройка базы данных Business Space” на стр. 203.
5. Запустите администратор развертывания.
6. Запустите кластеры или управляемые серверы.

Если дополняется профайл, в котором уже настроена защита с хранилищем пользователей, не являющимся одним из объединенных хранилищ по умолчанию; необходимо скорректировать параметр `MashupAdminForOOBSpace` в файле `ConfigServices.properties`. См. раздел “Выбор хранилища пользователей для Business Space” на стр. 225.

Утилита командной строки `manageprofiles` (для профайлов Business Space):



Утилита командной строки `manageprofiles` создает профайл, который представляет собой набор файлов, определяющих среду выполнения для администратора развертывания, управляемого узла или автономного сервера. С ее помощью можно создать профайл Business Space на основе WebSphere. Это необязательная информация, если продукт Business Space настроен в профайле продукта.

Профайл определяет среду развертывания и включает в себя все файлы, обрабатываемые сервером во время выполнения.

Утилита командной строки `manageprofiles` и ее графический пользовательский интерфейс (инструмент управления профайлами) являются единственными средствами создания профайлов, или единственными средствами создания сред выполнения. С помощью утилиты командной строки `manageprofiles` можно также дополнять и удалять профайлы.

Командный файл расположен в каталоге *install_root/bin*. Командный файл - это сценарий с именем *manageprofiles.sh* для платформ Linux и UNIX или *manageprofiles.bat* для платформ Windows.

Утилита командной строки *manageprofiles* создает протокол для каждого создаваемого, удаляемого или расширяемого профайла. Эти протоколы расположены в указанных ниже каталогах (в зависимости от платформы):

-  *install_root/logs/manageprofiles*
-  *install_root\logs\manageprofiles*

Имена файлов:

- *profile_name_create.log*
- *profile_name_augment.log*
- *profile_name_delete.log*

Шаблоны для каждого профайла расположены в каталоге установочный-каталог/*profileTemplates/BusinessSpace* directory. В этом каталоге расположены различные подкаталоги, соответствующие разным типам профайлов. Эти пути к каталогам необходимо указывать, если в утилите командной строки *manageprofiles* задан параметр *-templatePath*. Кроме того, можно указать шаблоны профайлов, расположенные за пределами корневого каталога установки. Для *BusinessSpace* доступны следующие шаблоны:

- *default.bspace*: для профайла автономного сервера *BusinessSpace*, определяющего автономный сервер.
- *dmgr.bspace*: для профайла администратора развертывания *BusinessSpace*, определяющего администратор развертывания.
- *managed.bspace*: для пользовательского профайла *BusinessSpace*, определяющего, при объединении с администратором развертывания, управляемый узел.

Синтаксис

Утилита командной строки *manageprofiles* служит для выполнения следующих задач:

- Создание профайла (параметр *-create*).
- Расширение профайла (параметр *-augment*).

Ограничение: Использование профайлов, дополнение которых было отменено (параметр *-unaugment*), не поддерживается.

- Удаление профайла (параметр *-delete*).
- Удаление всех профайлов (параметр *-deleteAll*)
- Отображение списка всех профайлов (параметр *-listProfiles*)
- Получение имени существующего профайла по его имени (параметр *-getName*)
- Получение имени существующего профайла по пути к нему (параметр *-getPath*)
- Проверка реестра профайлов (параметр *-validateRegistry*)
- Проверка и обновление реестра профайлов (параметр *-validateAndUpdateRegistry*)
- Получение имени профайла по умолчанию (параметр *-getDefaultName*)
- Указание имени профайла по умолчанию (параметр *-setDefaultName*)
- Создание резервной копии профайла (параметр *-backupProfile*)
- Восстановление профайла (параметр *-restoreProfile*)
- Использование файла ответов, в котором содержится информация, необходимая для работы утилиты командной строки *manageprofiles* (параметр *-response*)

Для получения подробной справочной информации, включая обязательные параметры для каждой из задач, выполняемых с помощью утилиты командной строки `manageprofiles`, укажите параметр **-help**. Ниже приведен пример использования параметра `help` с параметром **-augment** утилиты командной строки `manageprofiles` в операционных системах Windows: `manageprofiles.bat -augment -help`. В выводе указано, какие параметры являются обязательными, а какие - нет.

Вывод команды

После выполнения команды отображается сообщение, аналогичное одному из приведенных ниже. (Формулировка может отличаться в зависимости от того, выполнялось ли действие по созданию, удалению или расширению профайла.)

- `INSTCONFSUCCESS`: Создание профайла выполнено успешно.
- `INSTCONFFAILED`: Не удалось создать профайл.
- `INSTCONFPARTIALSUCCESS`: Отдельные вспомогательные действия по настройке на заключительном этапе установки не выполнены.

В некоторых случаях сообщения выводятся несколько раз. Например, строка `INSTCONFSUCCESS` отображается в командной строке три раза. Дополнительная информация приведена в разделе *Файлы протоколов установки и создания профайлов*.

Параметры

При создании профайла `BusinessSpace` следует использовать только параметры, описанные в справочной системе `Information Center` для продукта `BusinessSpace`. Все параметры следует указывать с учетом регистра.

-adminUserName *adminUser_ID*

Задает ИД пользователя для административной защиты. Этот параметр является обязательным при расширении существующего профайла, в котором включена административная защита.

-adminPassword *adminPassword*

Пароль для ИД пользователя административной защиты, указанного в параметре `-adminUserName`. Этот параметр является обязательным при расширении существующего профайла, в котором включена административная защита.

-расширить

Для изменения существующего профайла с помощью шаблона дополнения используется параметр `augment`. Если указан параметр `augment`, утилита командной строки `manageprofiles` обновит или дополнит профайл, указанный в параметре `-profileName`, с помощью шаблона, заданного параметром `-templatePath`. Шаблоны дополнения, доступные для использования, зависят от того, какие продукты IBM и каких версий установлены в среде.

Важное замечание: Не изменяйте файлы из каталога *установочный-каталог/profileTemplates* вручную. Например, в процессе создания профайла для изменения портов следует использовать инструмент управления профайлами или аргументы `-startingPort` или `-portsFile` команды `manageprofiles` вместо изменения файла в каталоге шаблонов профайлов.

Укажите полный путь к файлу в параметре `-templatePath`. Пример:
`manageprofiles(.bat)(.sh) -augment -profileName profile_name -templatePath fully_qualified_template_path`

-backupProfile

Выполняет резервное копирование файловой системы из папки профайла и метаданных профайла из файла реестра профайлов.

-backupFile *backupFile_name*

Создает резервную копию файла реестра профайлов в указанном файле. Вместо *backupFile_name* необходимо указать полный путь к файлу.

-bspacedbDesign *файл-структуры-базы-данных*

Задаёт путь к файлу структуры базы данных Business Space. Примеры файлов структуры расположены в каталоге *установочный-каталог/BusinessSpace/config.bspace/MetadataFiles*.

-bspaceSchemaName *схема-базы-данных*

Имя схемы базы данных. Если значение не указано, то для большинства типов баз данных применяется значение IBMUSSP.

-cellName *имя-ячейки*

Указывает имя ячейки профайла. Укажите уникальное имя ячейки для каждого профайла. В ходе дополнения профайла укажите ячейку исходного профайла. Значение этого параметра по умолчанию складывается из сочетания сокращенного имени хоста, константы Cell и номера, например:

```
if (DMgr)
    shortHostNameCellCellNumber
else
    shortHostNameNodeNodeNumberCell
```

, где *CellNumber* - это порядковый номер, начиная с 01, а *NodeNumber* - номер узла, используемый для определения имени узла. В значении этого параметра недопустимы пробелы и следующие специальные символы: *, ?, ", <, >,, /, \ и |.

-create

Создает профайл. Команда `manageprofiles -create -templatePath fully_qualified_file_path_to_template -help` позволяет просмотреть информацию о создании профайла. Доступные шаблоны:

- default.bspace: для профайла автономного сервера BusinessSpace, определяющего автономный сервер.
- dmgr.bspace: для профайла администратора развертывания BusinessSpace, определяющего администратор развертывания.
- managed.bspace: для пользовательского профайла BusinessSpace, определяющего, при объединении с администратором развертывания, управляемый узел.
-

-dbBspacePassword *пароль-базы-данных-bspace*

Этот параметр необходим, если во время создания профайла указаны выбранные пользователем имя и пароль пользователя и если задано значение ORACLE для параметра dbType. Значение по умолчанию: dbPassword.

-dbBspaceUserId *пользователь-базы-данных-bspace*

Этот параметр необходим, если во время создания профайла указаны выбранные пользователем имя и пароль пользователя. Значение по умолчанию: IBMUSSP.

-dbConnectionLocation *db2_location*

Расположение базы данных DB2 для z/OS.

-dbCreateNew

Позволяет разрешить создание новой базы данных или применение существующей. Допустимые значения: true или false. Значение по умолчанию: true.

-dbDelayConfig

Позволяет отложить создание таблицы, пока не будет создан профайл. Допустимые значения: `true` или `false`. Значение по умолчанию: `false`. При работе с удаленной базой данных необходимо указать значение `true`, которое позволяет отложить выполнение сценариев базы данных.

-dbDriverType *db_driver_type*

Тип драйвера базы данных. Допустим только для Oracle. Для базы данных Oracle укажите значение `ORACLE`. Для баз данных, отличных от Oracle, это значение указывается автоматически с учетом операционной системы сервера. Для экземпляров сервера в системе z/OS применяется тип 2. Во всех остальных операционных системах используется тип 4.

-dbDriverVersion *db_driver_version*

Версия драйвера базы данных. Этот параметр допустим только для Microsoft SQL Server. Для базы данных SQL Server укажите значение 1.2 для драйвера Microsoft SQL JDBC 1.2 либо 2.0 для драйвера Microsoft SQL JDBC 2.0. Если значение не указано, используется значение по умолчанию 2.0.

-dbHostName *db_host_name*

Имя хоста или IP-адрес сервера базы данных. Значение по умолчанию: `localhost`.

-dbJDBCClasspath *jdbc_driver_location*

Расположение файлов драйвера JDBC. Для доступа к базе данных Oracle необходимо установить драйвер `ojdbc6.jar`. В Oracle 10g драйвера `ojdbc6.jar` нет. Его можно загрузить с веб-сайта Oracle.

-dbName *db_name*

Имя базы данных. По умолчанию указано значение `orcl` (базы данных Oracle) или `BSPACE` (другие поддерживаемые базы данных).

-dbOutputScriptDir *db_output_dir*

Расположение экспортированных сценариев базы данных. Этот параметр доступен только в том случае, если выбран переключатель Переопределить целевой каталог для созданных сценариев. Значением должен быть абсолютный путь. Если будет указан относительный путь, сценарии SQL не будут экспортированы и выполнены, что приведет к многочисленным исключительным ситуациям во время запуска сервера.

-dbPassword *db_pswd*

Пароль для идентификации в базе данных.

-dbServerPort *db_port_number*

Порт сервера базы данных. При необходимости номер порта по умолчанию можно изменить.

-dbStorageGroup *db_stg_group*

Имя группы носителей для баз данных DB2 z/OS.

-dbSysPassword *sys_pwd*

Это обязательный параметр, если для параметра `dbDelayConfig` указано значение `false`, а для параметра `dbType` указано значение `ORACLE`.

-dbSysUserId *sys_user_id*

Этот ИД должен обладать правами доступа `SYSDBA`. Не следует использовать внутреннего пользователя Oracle с именем `sys`. Это обязательный параметр, если для параметра `dbDelayConfig` указано значение `false`, а для параметра `dbType` указано значение `ORACLE`.

-dbType *db_type*

Тип базы данных. Задайте одно из следующих значений для типа базы данных, которая используется с Business Space.

- DB2 Universal = DB2_Universal
- DB2 DataServer = DB2_DataServer
- DB2 Universal for z/OS = DB2UDBOS390
- Oracle = Oracle
- Microsoft SQL Server = MSSQLSERVER_MICROSOFT или MSSQLSERVER_DATADIRECT

-dbUserId *db_userid*

ИД пользователя для всех типов баз данных. Задает идентификатор пользователя с правами доступа для создания и удаления баз данных. Источник данных WebSphere использует этот ИД для идентификации при подключении к базе данных. Для баз данных DB2 задает ИД пользователя базы данных, которому будут принадлежать таблицы базы данных. Для баз данных DB2 для z/OS определяет ИД пользователя, обладающего правами доступа для создания и удаления баз данных. Это обязательный параметр. Важная информация: Параметр `-dbUserId` должен содержать допустимый ИД предоставления прав к базе данных. Дополнительная информация об ИД предоставления прав приведена в разделе ИД и имена предоставления прав на странице с информацией об ограничениях свойств DB2.

-debug

Включает функцию отладки утилиты Apache Ant, которая используется утилитой командной строки **manageprofiles**.

-defaultPorts

Присваивает профайлу значения портов по умолчанию или базовые значения портов.

Не указывайте этот параметр вместе с параметром `-startingPort` или `-portsFile`.

Если не задан параметр `-startingPort`, `-defaultPorts` или `-portsFile`, то при создании профайла команда **manageprofiles** использует набор рекомендуемых портов, создаваемый в автоматическом режиме. Рекомендуемые значения портов могут отличаться от значений портов по умолчанию, в зависимости от доступности портов по умолчанию.

Примечание: Этот параметр не следует указывать в случае применения шаблона управляемого профайла.

-delete

Удаление профайла.

Каталог профайла не удаляется вместе с профайлом. Например, если профайл создан в каталоге `/usr/WebSphere/AppServer/profiles/AppSrvr01`, то этот каталог будет сохранен после удаления профайла.

Его можно удалить или оставить. Однако в каталоге *каталог-профайла*/`logs` сохраняется информация об удалении профайла из системы. Например, можно сохранить файл `_nodeuninst.log`, чтобы определить причину какой-либо неполадки, возникшей при удалении из системы.

При удалении профайла, для которого зарегистрированы шаблоны дополнения в реестре профайлов, действия по отмене дополнения выполняются автоматически.

-deleteAll

Удаление всех зарегистрированных профайлов.

Каталог профайла не удаляется вместе с профайлом. Например, если профайл создан в каталоге `/usr/WebSphere/AppServer/profiles/AppSrvr01`, то этот каталог будет сохранен после удаления профайла.

Его можно удалить или оставить. Однако в каталоге *каталог-профайла*/`logs` сохраняется информация об удалении профайла из системы. Например, можно сохранить файл `_nodeuninst.log`, чтобы определить причину какой-либо неполадки, возникшей при удалении из системы.

При удалении профайла, для которого зарегистрированы шаблоны дополнения в реестре профайлов, действия по отмене дополнения выполняются автоматически.

-dmgrAdminUserName *имя_пользователя*

Если включена административная защита администратора развертывания, введите допустимое имя пользователя.

-dmgrAdminPassword *пароль*

Если включена административная защита администратора развертывания, введите пароль для указанного имени пользователя.

-dmgrHost *имя-хоста-администратора-развертывания*

Рабочая станция, на которой запущен администратор развертывания. Укажите этот параметр и параметр **dmgrPort**, чтобы объединить пользовательский профайл при его создании или дополнении. Этот параметр доступен с шаблоном профайла `managed.bspace`.

Имя хоста может представлять собой полное или краткое имя DNS или IP-адрес рабочей станции администратора развертывания.

Если этот необязательный параметр указан, то утилита командной строки **manageprofiles** попытается объединить пользовательский узел с ячейкой администратора развертывания при создании пользовательского профайла. Этот параметр игнорируется при создании профайла администратора развертывания или профайла автономного сервера.

Если во время объединения пользовательского узла администратор развертывания не запущен, то в протоколах будет зарегистрирован индикатор состояния установки `INSTCONFFAILED`, указывающий на полный сбой. Созданный индивидуальный профайл будет не пригоден для использования. Необходимо переместить каталог пользовательского профайла за пределы хранилища профайлов (корневой установочный каталог профайла) и только после этого создать новый пользовательский профайл с тем же именем.

Если тип коннектора JMX по умолчанию изменен, с помощью команды **manageprofiles** нельзя выполнить объединение. Вместо нее следует использовать команду **addNode**.

Значение этого параметра по умолчанию - `localhost`. Значение этого параметра должно представлять собой имя хоста в соответствующем формате; в нем недопустимы пробелы и специальные символы, такие как `*`, `?`, `"`, `<`, `>`, `,`, `/`, `\` и `|`. В сочетании с параметром `dmgrPort` также необходимо наличие соединения с администратором развертывания.

-dmgrPort *порт-администратора-развертывания*

Идентифицирует порт SOAP администратора развертывания. Укажите этот параметр и параметр **dmgrHost**, чтобы объединить пользовательский профайл при его создании или дополнении. Администратор развертывания быть запущен и доступен.

Если тип коннектора JMX по умолчанию изменен, с помощью команды **manageprofiles** нельзя выполнить объединение. Вместо нее следует использовать команду **addNode**.

Значение этого параметра по умолчанию - 8879. Указанный номер порта должен быть положительным целым числом. Вместе с параметром `dmgrHost` необходимо указать соединение с администратором развертывания.

-enableAdminSecurity true | false

Включает административную защиту. Допустимые значения: `true` и `false`. Значение по умолчанию: `false`. При создании профайлов для среды развертывания необходимо указать для этого параметра значение `true`. Используйте этот параметр только при создании профайлов. Этот параметр не требуется указывать в случае дополнения существующего профайла.

Если для параметра **enableAdminSecurity** указано значение `true`, то дополнительно необходимо указать значения параметров `-adminUserName` и `-adminPassword`. Если во время установки сервера приложений также были установлены примеры, то при создании профайла, для которого включена административная защита, необходимо указать и параметр `-samplesPassword`. Если параметр `-samplesPassword` не задан при включенной административной защите, профайл будет создан успешно, но при попытке запуска примеров в системном протоколе сервера будут зарегистрированы исключительные ситуации и сбои.

Linux -enableService true | false

Разрешает создание службы Linux. Допустимые значения: `true` и `false`. Значение этого параметра по умолчанию - `false`. Используйте этот параметр только при создании профайлов. Этот параметр не требуется указывать в случае дополнения существующего профайла.

Если утилита командной строки **manageprofiles** запущена с параметром `-enableService`, для которого задано значение `true`, то служба Linux создается вместе с профайлом при запуске команды пользователем `root`. Если утилита командной строки **manageprofiles** запускается обычным пользователем, профайл создается, а служба Linux - нет. Служба Linux не создается, поскольку обычный пользователь не обладает правами доступа, необходимыми для настройки этой службы. После создания профайла выводится результат - `INSTCONPARTIALSUCCESS`, а в протокол создания профайла `install_root/logs/manageprofiles/profile_name_create.log` включается сообщение, указывающее на то, что текущий пользователь имеет недостаточно прав доступа для настройки службы Linux.

-federateLater true | false

Позволяет разрешить объединение управляемого профайла во время создания профайла или позднее с помощью команды **addNode**. При создании профайла Business Space значение указывать не нужно. Используется значение по умолчанию - `true`.

-getDefaultName

Возвращает имя профайла по умолчанию.

-getName

Получает имя профайла, зарегистрированного в указанном параметре `-profilePath`.

-getPath

Получает расположение в файловой системе для профайла с указанным именем. Требуется параметр `profileName`.

-help

Отображает формат команды.

-hostName ИМЯ_ХОСТА

Задает имя хоста, на котором создается профайл. Этот параметр не требуется

указывать в случае дополнения существующего профайла. Это значение должно совпадать с именем хоста, указанным при установке исходного продукта. Значением этого параметра по умолчанию является длинная форма имени в соответствии с системой имен доменов. Этот параметр обязателен только для создания профайла. Значение этого параметра должно представлять собой допустимое имя хоста IPv6; в нем недопустимы пробелы и специальные символы, такие как *, ?, ", <, >, ,, /, \ и |.

-importPersonalCertKS *keystore_path*

Путь к файлу хранилища ключей, который используется для импорта личного сертификата при создании профайла. Личный сертификат - это личный сертификат сервера по умолчанию.

Если личный сертификат импортируется как стандартный личный сертификат, импортируйте базовый сертификат, подписавший этот личный сертификат. В противном случае утилита `managerprofiles` добавит общий ключ личного сертификата в файл `trust.p12` и создаст базовый сертификат подписи.

Параметры `-importPersonalCertKS` и `-personalCertDN` являются взаимоисключающими. Если личный сертификат не создан или не импортирован вручную, то он создается по умолчанию.

Если указан по крайней мере один из параметров, начинающихся с `-importPersonal`, необходимо указать все эти параметры.

-importPersonalCertKSType *keystore_type*

Тип файла хранилища ключей, указанного в параметре `-importPersonalCertKS`. Допустимые значения: `JCEKS`, `CMSKS`, `PKCS12`, `PKCS11` и `JKS`. Этот список может меняться в зависимости от провайдера, указанного в файле `java.security`.

Если указан по крайней мере один из параметров, начинающихся с `-importPersonal`, необходимо указать все эти параметры.

-importPersonalCertKSPassword *keystore_password*

Пароль файла хранилища ключей, указанного в параметре `-importPersonalCertKS`.

Если указан по крайней мере один из параметров, начинающихся с `-importPersonal`, необходимо указать все эти параметры.

-importPersonalCertKSAlias *keystore_alias*

Псевдоним сертификата в файле хранилища ключей, указанного в параметре `-importPersonalCertKS`. Сертификат добавляется в файл хранилища ключей сервера по умолчанию и используется как личный сертификат сервера по умолчанию.

Если указан по крайней мере один из параметров, начинающихся с `-importPersonal`, необходимо указать все эти параметры.

-importSigningCertKS *keystore_path*

Путь к файлу хранилища ключей, который используется для импорта базового сертификата при создании профайла. Базовый сертификат - это сертификат, используемый в качестве базового сертификата сервера по умолчанию.

Параметры `-importSigningCertKS` и `-signingCertDN` являются взаимоисключающими. Если базовый сертификат подписи не создан или не импортирован вручную, то он создается по умолчанию.

Если указан по крайней мере один из параметров, начинающихся с `-importSigning`, необходимо указать все эти параметры.

-importSigningCertKSType *keystore_path*

Тип файла хранилища ключей, указанного в параметре `-importSigningCertKS`.

Допустимые значения: JCEKS, CMSKS, PKCS12, PKCS11 и JKS. Этот список может меняться в зависимости от провайдера, указанного в файле `java.security`.

Если указан по крайней мере один из параметров, начинающихся с `-importSigning`, необходимо указать все эти параметры.

-importSigningCertKSPassword *keystore_password*

Пароль файла хранилища ключей, указанного в параметре `-importSigningCertKS`.

Если указан по крайней мере один из параметров, начинающихся с `-importSigning`, необходимо указать все эти параметры.

-importSigningCertKSAlias *keystore_alias*

Псевдоним сертификата в файле хранилища ключей, указанного в параметре `-importSigningCertKS`. Сертификат добавляется в базовое хранилище ключей сервера по умолчанию и используется в качестве базового сертификата сервера по умолчанию.

Если указан по крайней мере один из параметров, начинающихся с `-importSigning`, необходимо указать все эти параметры.

-isDefault

Указывает, что профайл, указанный в параметре `-profileName` после регистрации, должен быть профайлом по умолчанию. При вызове команд для профайла по умолчанию не следует указывать атрибут команды `-profileName`.

-keyStorePassword *keyStore_password*

Пароль, используемый для всех файлов хранилищ ключей, созданных одновременно с профайлом. Файлы хранилищ ключей создаются для личного сертификата по умолчанию и для базового сертификата подписи.

-listAugments




Отображает список зарегистрированных дополнений профайла из реестра профайлов. В сочетании с параметром `-listAugments` необходимо задать параметр `-profileName`.

-listProfiles

Отображает список всех определенных профайлов.

-nodeName *имя-узла*

Имя узла, создаваемого одновременно с новым профайлом. Используйте уникальное значение в пределах ячейки или рабочей станции. Каждый профайл, совместно использующий один и тот же набор исполняемых файлов продукта, должен иметь уникальное имя узла. В ходе дополнения профайла укажите узел исходного профайла.

   Значение этого параметра по умолчанию состоит из краткого имени хоста, типа профайла и номера, например:

```
if (DMgr)
  shortHostNameCellManagerNodeNumber
else
  shortHostNameNodeNodeNumber
```

, где *NodeNumber* - это порядковый номер, начиная с 01.

В значении этого параметра недопустимы пробелы и специальные символы, такие как *, ?, ", <, >, ,, /, \ и |.

-omitAction *feature1 feature2... featureN*

Необязательный параметр, исключающий свойства профайла.

Каждый шаблон профайла содержит предварительно определенные необязательные компоненты. Опция `samplesInstallAndConfig` доступна только при установке продукта вместе с примерами приложений. Вместе с параметром `-omitAction` можно использовать следующие необязательные функции для перечисленных ниже шаблонов профайла:

- **по умолчанию** - Сервер приложений
 - `deployAdminConsole`
 - `samplesInstallAndConfig`
 - `defaultAppDeployAndConfig`
- **dmgr** - Администратор развертывания
 - `deployAdminConsole`

-personalCertDN *distinguished_name*

Отличительное имя личного сертификата, создаваемого одновременно с профайлом. Укажите отличительное имя в кавычках. Этот личный сертификат по умолчанию находится в файле хранилища ключей сервера. Параметры `-importPersonalCertKSType` и `-personalCertDN` являются взаимоисключающими. См. описание параметров `-personalCertValidityPeriod` и `-keyStorePassword`.

-personalCertValidityPeriod *validity_period*

Необязательный параметр, определяющий промежуток времени (число лет), в течение которого действителен личный сертификат по умолчанию. Если этот параметр не указан вместе с параметром `-personalCertDN`, то личный сертификат по умолчанию будет действителен в течение одного года.

-portsFile *file_path*

Необязательный параметр, указывающий путь к файлу, определяющему параметры порта для нового профайла. Этот параметр не требуется указывать в случае дополнения существующего профайла.

Не указывайте этот параметр вместе с параметром `-startingPort` или `-defaultPorts`.

Если не задан параметр `-startingPort`, `-defaultPorts` или `-portsFile`, то при создании профайла команда **manageprofiles** использует набор рекомендуемых портов, создаваемый в автоматическом режиме. Рекомендуемые значения портов могут отличаться от значений портов по умолчанию, в зависимости от доступности портов по умолчанию.

-profileName *имя-профайла*

Задает имя профайла. При создании профайла используйте уникальное значение.

Каждый профайл, совместно использующий один и тот же набор исполняемых файлов продукта, должен иметь уникальное имя. Имя профайла по умолчанию состоит из типа профайла и номера, например:

profileType ProfileNumber

, где вместо *profileType* используется значение `AppSrv`, `Dmgr` или `Custom`, а *ProfileNumber* - это порядковый номер, создающий уникальное имя профайла. В значении этого параметра недопустимы пробелы и специальные символы, такие как `*`, `?`, `"`, `<`, `>`, `,`, `/`, `\` и `|`. Имя используемого профайла выбрать нельзя.

-profilePath *каталог-профайла*

Полный путь к профайлу, в документации справочной системы Information Center обозначаемый как *каталог-профайла*.

Пример:

`-profilePath каталог-профайла`

Используйте этот параметр только при создании профайлов. Этот параметр не требуется указывать в случае дополнения существующего профайла.

Windows **На платформах Windows:** Если полный путь содержит пробелы, то значение следует заключить в кавычки.

Значение по умолчанию состоит из имени каталога *install_root*, вложенного каталога профайлов и имени файла.

Пример значения по умолчанию при создании профайла:

```
WS_WSPROFILE_DEFAULT_PROFILE_HOME/profileName,
```

где *WS_WSPROFILE_DEFAULT_PROFILE_HOME* определяется в файле *wasprofile.properties* в каталоге *install_root/properties*.

Значение этого параметра должно представлять собой допустимый путь в целевой системе, в настоящий момент не используемый.

Необходимо обладать правами доступа для записи в каталог.

-response response_file

Осуществляет доступ ко всем функциям API из командной строки с помощью утилиты командной строки **manageprofiles**.

Интерфейсом командной строки можно управлять с помощью файла ответов, в котором содержатся входные аргументы для данной команды в файле свойств в формате "ключ-значение". Ниже приведен пример файла ответов для операции создания:

```
создать
profileName=testResponseFileCreate
profilePath=каталог-профайла
templatePath=install_root/profileTemplates/default
nodeName=myNodeName
cellName=myCellName
hostName=myHostName
omitAction=myOptionalAction1, myOptionalAction2
```

Windows **На платформах Windows:** В операторе пути в операционных системах Windows можно использовать прямую (/) либо обратную косую черту (\). Если в операторе пути используются символы обратной косой черты, то в файле ответов для правильного распознавания пути обязательны двойные символы обратной косой черты. Ниже приведен пример файла ответов для операции создания с двойными символами обратной косой черты:

```
создать
templatePath=C:\\WebSphere\\AppServer\\profileTemplates\\BusinessSpace\\default.bspace
```

При добавлении свойств, обозначающих отличительные имена для сертификатов, перед запятыми обязательно наличие двойных символов обратной косой черты (\\). Обратите внимание, что ключ (*personalCertDN*) и значение разделяет не знак равенства, а пробел. Это обусловлено тем, что знак равенства встречается в значениях свойств. Ниже приведен пример оператора записи сертификата в файле ответов с двойными символами обратной косой черты:

```
personalCertDN cn=machine_name.dnx_suffix.com\\,ou=machine_name
Node04Cell\\,ou=machine_nameNode04\\,o=IBM\\,c=US
```

Для того чтобы определить, какие входные аргументы являются обязательными для различных типов шаблонов профайлов и действий, вызовите утилиту командной строки **manageprofiles** с параметром **-help**.

-restoreProfile

Восстанавливает резервную копию профайла. Следует использовать вместе с параметром **-backupFile**.

-samplesPassword *samplesPassword*

Создает пароль, используемый для примеров. Этот пароль служит для ограничения доступа к примерам веб-приложений, установленным одновременно с сервером приложений.

-serverType DEPLOYMENT_MANAGER

Задает тип профайла управления. Укажите DEPLOYMENT_MANAGER для профайла управления. Этот параметр обязателен при создании профайла управления.

> Linux **-serviceUserName** *service_user_ID*

ИД пользователя, применяемый при создании службы Linux; служба Linux будет работать от имени этого пользователя. Служба Linux запускается каждый раз входе этого пользователя в систему.

-setDefaultName

Позволяет выбрать один из существующих профайлов в качестве профайла по умолчанию. Следует использовать вместе с параметром `-profileName`, например:
`manageprofiles(.bat)(.sh) -setDefaultName -profileName имя-профайла`

-signingCertDN *distinguished_name*

Отличительное имя базового сертификата подписи, создаваемого одновременно с профайлом. Укажите отличительное имя в кавычках. Этот личный сертификат по умолчанию находится в файле хранилища ключей сервера. Параметры `-importSigningCertKS` и `-signingCertDN` являются взаимоисключающими. Если базовый сертификат подписи не создан или не импортирован вручную, то он создается по умолчанию. См. описание параметров `-signingCertValidityPeriod` и `-keyStorePassword`.

-signingCertValidityPeriod *validity_period*

Необязательный параметр, определяющий промежуток времени (число лет), в течение которого действителен базовый сертификат подписи. Если этот параметр не указан вместе с параметром `-signingCertDN`, то базовый сертификат подписания будет действителен в течение 20 лет.

-startingPort *startingPort*

Задает начальный номер порта для генерирования и присвоения всех портов для профайла.

Этот параметр не требуется указывать в случае дополнения существующего профайла. Значения портов присваиваются последовательно, начиная со значения **-startingPort**; используемые порты при этом пропускаются. Система распознает порты, используемые в настоящий момент, и управляет выделением портов во избежание конфликтов между ними.

Не указывайте этот параметр вместе с параметром **-defaultPorts** или **-portsFile**.

Если не задан параметр **-startingPort**, **-defaultPorts** или **-portsFile**, то при создании профайла команда **manageprofiles** использует набор рекомендуемых портов, создаваемый в автоматическом режиме. Рекомендуемые значения портов могут отличаться от значений портов по умолчанию, в зависимости от доступности портов по умолчанию.

Примечание: Этот параметр не следует указывать в случае применения шаблона управляемого профайла.

-templatePath *путь-шаблона*

Путь к каталогу файла шаблонов в корневом каталоге установки. В каталоге `profileTemplates` расположены различные подкаталоги, соответствующие разным типам профайлов и отличающиеся в зависимости от типа

установленного продукта. Эти пути к каталогам необходимо указывать при использовании опции **-templatePath**. Можно указать шаблоны профайлов, расположенные за пределами корневого каталога установки.

Используйте абсолютные пути. Этот параметр должен быть задан как каталог и указывать на допустимый каталог шаблонов. Для Business Space доступны следующие шаблоны:

- **default.bspace**: для профайла автономного сервера Business Space, определяющего автономный сервер.
- **dmgr.bspace**: для профайла администратора развертывания Business Space, определяющего администратор развертывания.
- **managed.bspace**: для пользовательского профайла Business Space, определяющего, при объединении с администратором развертывания, управляемый узел.

-validateAndUpdateRegistry

Проверяет наличие в файловой системе всех профайлов из реестра профайлов. Удаляет все отсутствующие профайлы из реестра. Возвращает список отсутствующих профайлов, удаленных из реестра.

-validateRegistry

Проверяет наличие в файловой системе всех профайлов из реестра профайлов. Возвращает список недостающих профайлов.

-validatePorts

Указывает порты, подлежащие проверке на предмет того, не являются ли они зарезервированными или уже используемыми. С помощью этого параметра можно идентифицировать неиспользуемые порты. Если порт определен как используемый, операция создания профайла будет приостановлена и будет выдано сообщение об ошибке. Этот параметр можно использовать в любое время в командной строке команды `create`. Рекомендуется использовать его вместе с параметром `portsFile`.

-webFormConfig true | false

Указывает, настроен ли продукт Business Space для работы с IBM Forms Server для поддержки виджетов управления неавтоматизированными задачами. Значение этого параметра по умолчанию - `false`. Задайте значение `true`, чтобы настроить Business Space для использования IBM Forms Server. Параметры **webFormConfig** и **webFormInstallRoot** являются обязательными для настройки IBM Forms Server. Этот параметр допустим только для профайлов автономного сервера.

Примечание: Конфигурация IBM Forms Server с этими параметрами допустима только для локальных экземпляров IBM Forms Server.

-webServerCheck true | false

Позволяет разрешить или запретить настройку определений веб-сервера. Допустимые значения: `true` и `false`. Значение этого параметра по умолчанию - `false`. Используйте этот параметр только при создании профайлов. Этот параметр не требуется указывать в случае дополнения существующего профайла.

-webServerHostname *webserver_host_name*

Имя хоста сервера. Значением этого параметра по умолчанию является полное имя хоста локальной рабочей станции. Используйте этот параметр только при создании профайлов. Этот параметр не требуется указывать в случае дополнения существующего профайла.

-webServerInstallPath *webserver_installpath_name*

Установочный каталог локального или удаленного веб-сервера. Используйте

этот параметр только при создании профайлов. Этот параметр не требуется указывать в случае дополнения существующего профайла.

Значение этого параметра по умолчанию зависит от операционной системы локальной рабочей станции и от значения параметра `webServerType`. Пример:

AIX

```
webServerType=IHS: webServerInstallPath defaulted to /usr/IBM/HTTPServer
webServerType=IIS: webServerInstallPath defaulted to n\a
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to /opt/sun/webserver
webServerType=DOMINO: webServerInstallPath defaulted to ?
webServerType=APACHE: webServerInstallPath defaulted to ?
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to n/a
```

HP-UX

```
webServerType=IHS: webServerInstallPath defaulted to /opt/IBM/HTTPServer
webServerType=IIS: webServerInstallPath defaulted to n\a
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to /opt/sun/webserver
webServerType=DOMINO: webServerInstallPath defaulted to
webServerType=APACHE: webServerInstallPath defaulted to
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to n/a
```

> Linux

```
webServerType=IHS: webServerInstallPath defaulted to /opt/IBM/HTTPServer
webServerType=IIS: webServerInstallPath defaulted to n\a
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to /opt/sun/webserver
webServerType=DOMINO: webServerInstallPath defaulted to
webServerType=APACHE: webServerInstallPath defaulted to
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to n/a
```

Solaris

```
webServerType=IHS: webServerInstallPath defaulted to /opt/IBM/HTTPServer
webServerType=IIS: webServerInstallPath defaulted to n\a
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to /opt/sun/webserver
webServerType=DOMINO: webServerInstallPath defaulted to
webServerType=APACHE: webServerInstallPath defaulted to
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to n/a
```

> Windows

```
webServerType=IHS: webServerInstallPath defaulted to C:\Program Files\IBM\HTTPServer
webServerType=IIS: webServerInstallPath defaulted to C:\
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to C:\
webServerType=DOMINO: webServerInstallPath defaulted to
webServerType=APACHE: webServerInstallPath defaulted to
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to n/a
```

-webServerName *webserver_name*

Имя веб-сервера. Значение этого параметра по умолчанию - `webserver1`.

Используйте этот параметр только при создании профайлов. Этот параметр не требуется указывать в случае дополнения существующего профайла.

-webServerOS *webserver_operating_system*

Операционная система, используемая на этом веб-сервере. Допустимые значения: `windows`, `linux`, `solaris`, `aix`, `hpux`, `os390` и `os400`. Этот параметр используется вместе с параметром `webServerType`.

Используйте этот параметр только при создании профайлов. Этот параметр не требуется указывать в случае дополнения существующего профайла.

-webServerPluginPath *webserver_pluginpath*

Путь к встроенным модулям, используемым веб-сервером. Значение этого

параметра по умолчанию - `install_root/plugins`. Используйте этот параметр только при создании профайлов. Этот параметр не требуется указывать в случае дополнения существующего профайла.

-webServerPort *webserver_port*

Указывает порт, применяемый для доступа к веб-серверу. Значение этого параметра по умолчанию - 80. Используйте этот параметр только при создании профайлов. Этот параметр не требуется указывать в случае дополнения существующего профайла.

-webServerType *webserver_type*

Тип веб-сервера. Допустимые значения: IHS, SUNJAVASYSTEM, IIS, DOMINO, APACHE и HTTPSERVER_ZOS. Этот параметр используется вместе с параметром **webServerOS**. Используйте этот параметр только при создании профайлов. Этот параметр не требуется указывать в случае дополнения существующего профайла.

Windows **-winserviceAccountType** *specifieduser* | *localsystem*

Тип учетной записи владельца службы Windows, созданной для профайла. Используйте этот параметр только при создании профайлов. Этот параметр не требуется указывать в случае дополнения существующего профайла.

Допустимые значения: *specifieduser* и *localsystem*. Значение *localsystem* позволяет запустить службу Windows под локальной учетной записью пользователя, создавшего профайл. Значение этого параметра по умолчанию - *system*.

Windows **-winserviceCheck** *true* | *false*

Допустимые значения - *true* или *false*. Укажите значение *true*, чтобы создать службу Windows для процесса сервера, созданного в профайле. Укажите значение *false*, чтобы запретить создание службы Windows. Значение этого параметра по умолчанию - *false*.

Используйте этот параметр только при создании профайлов. Этот параметр не требуется указывать в случае дополнения существующего профайла.

Windows **-winservicePassword** *winservice_password*

Укажите пароль для указанного пользователя или локальной учетной записи пользователя, который должен быть владельцем службы Windows. Используйте этот параметр только при создании профайлов. Этот параметр не требуется указывать в случае дополнения существующего профайла.

Windows **-winserviceStartupType** *manual* | *automatic* | *disabled*

Возможные значения для запуска службы Windows

- *manual*
- *automatic*
- *disabled*

Значение этого параметра по умолчанию - *manual*.

Используйте этот параметр только при создании профайлов. Этот параметр не требуется указывать в случае дополнения существующего профайла.

Windows **-winserviceUserName** *winservice_user_ID*

Укажите свой ИД пользователя. Операционная система Windows проверит, обладаете ли вы правами на создание служб Windows. Ваш ИД пользователя должен принадлежать к группе Администраторов и обладать следующими расширенными правами пользователя:

- Действовать как часть операционной системы
- Вход в качестве службы

Значением этого параметра по умолчанию является текущее имя пользователя. В значении этого параметра недопустимы пробелы и специальные символы, такие как *, ?, ", <, >, ,, /, \ и |. Указанный пользователь должен обладать соответствующими правами доступа для создания службы Windows. Необходимо указать верный пароль для выбранного имени пользователя.

Используйте этот параметр только при создании профайлов. Этот параметр не требуется указывать в случае дополнения существующего профайла.

Настройка Business Space с помощью мастера конфигурации среды развертывания

Конфигурация Business Space и конфигурация служб REST для виджетов в Business Space автоматически включаются в мастер Настройка среды развертывания. Можно выбрать службы REST для настройки.

Прежде чем выполнять эту задачу, выполните следующие действия:

- Установите продукт.
- Создайте профайл, назначив для него полное имя хоста.
- Включите защиту, если требуется установить защищенную среду для Business Space.

При установке администратора развертывания и пользовательских профайлов этот метод является самым простым способом настройки Business Space.

1. На странице консоли администрирования выберите **Серверы > Среда развертывания > Создать**. Последовательность страниц мастера помогает пройти весь процесс создания среды развертывания.
2. Создайте новую среду развертывания или импортируйте файл, содержащий определения среды развертывания. Можно создать среду развертывания на основе одного из шаблонов, поставляемых IBM, или создать собственную среду развертывания.
3. На странице Шаблоны среды развертывания выберите один из шаблонов среды развертывания.
4. На странице Выбор узлов назначьте узлы, участвующие в среде развертывания.
5. На странице Кластеры укажите количество элементов кластера от каждого узла, которые необходимо присвоить определенным функциям среды развертывания.
6. На странице База данных настройте источник данных для Business Space, один из компонентов, перечисленных в таблице. Можно изменить описание, проверить соединение и установить продукт базы данных, который будет использоваться для поставщика. Переключатель **Создать таблицы** на этой странице для Business Space включить нельзя. Таблицы базы данных для Business Space необходимо настроить вручную. Список продуктов базы данных содержит все базы данных, поддерживаемые каждым компонентом.
7. На странице Защита настройте псевдонимы идентификации, используемые WebSphere при доступе к компонентам защиты. На этой странице можно изменить имя пользователя и пароль псевдонима идентификации. Эти псевдонимы используются для доступа к компонентам защиты, однако не предоставляют доступ к источникам данных.
8. Для конфигурации IBM Business Process Manager укажите информацию, необходимую для настройки целевой среды развертывания приложений для поддержки развертывания компонентов Business Process Choreographer. Укажите значения корневых контекстов, почтового сеанса администратора защиты и неавтоматизированных задач, используемых мастером для настройки Business Process Choreographer этой среды развертывания.

9. Для конфигурации IBM Business Process Manager настройте администратор бизнес-правил на выполнение в кластере или на сервере.
10. На странице Службы REST настройте службы для виджетов, которые должны быть доступны в Business Space для среды выполнения.
 - Укажите номер порта и хост или виртуальный хост, необходимый клиенту для обмена данными с сервером или кластером. В кластерной среде обычно используется имя хоста и номер порта сервера распределения рабочей нагрузки.
 - Если поля хоста и порта останутся незаполненными, то будут использоваться значения по умолчанию, принятые для хоста отдельного элемента кластера и его порта HTTP. В среде с распределением нагрузки в дальнейшем необходимо будет изменить значения по умолчанию, указав имя виртуального хоста и порт сервера распределения рабочей нагрузки. Должно быть указано полное имя хоста.
 - Укажите описание для виджетов, если это необходимо.
11. На следующей странице нажмите **Готово** или **Завершить и создать среду**.
12. Выполните сценарии для настройки таблиц базы данных для Business Space перед запуском среды развертывания или кластеров. См. раздел "Настройка таблиц базы данных Business Space".

Совет: Business Space использует прокси-компонент для подключения к службам REST. Если в некоторых случаях службы REST не отвечают, измените параметры тайм-аута соединения из Business Space в службы REST в зависимости от производительности серверов служб REST. См. раздел Изменение параметров тайм-аута для прокси Ajax Business Space.

Настройка Business Space для сред сетевого развертывания

При работе в распределенной среде или среде сетевого развертывания необходимо настроить Business Space с помощью административной консоли или команд.

При использовании администратора развертывания и пользовательских профайлов необходимо настроить конечные точки служб REST, настроить Business Space, зарегистрировать конечные точки REST и настроить таблицы базы данных.

Настройка служб REST:

Если вы работаете в среде автономного сервера или применяете мастер среды развертывания для настройки среды выполнения, то службы Representational State Transfer (REST) настраиваются и подключаются автоматически. В других средах воспользуйтесь административной консолью для настройки служб REST.

Если вы хотите, чтобы в Business Space были доступны виджеты, то вы должны настроить для них службы REST. Впоследствии вы должны будете зарегистрировать конечные точки REST, чтобы Business Space связал с ними виджеты и эти виджеты появились в палитре, став доступными.

Вы можете настроить все службы REST для конкретного сервера или кластера. Либо вы можете выбрать отдельные службы для настройки. Управлять конфигурацией отдельных служб можно путем просмотра всех служб провайдера служб или просмотра всех служб среды.

Службы REST обычно предоставляются через шлюз REST. Некоторые службы REST реализуются посредством выделенного системного приложения. Приложение Шлюз служб REST подключает обычные системные службы REST. Это приложение создается во время настройки служб REST.

В кластерных средах все задачи администрирования и настройки служб REST выполняются через приложение Администратор шлюза служб REST в Администраторе развертывания. Это приложение используется со следующими виджетами:

- Браузер модулей
- Сборка модулей
- Свойства модулей
- Шлюз Proxu
- Работоспособность модулей
- Работоспособность системы

Настройка всех служб REST в административной консоли:

С помощью страницы административной консоли Службы REST настройте все службы Representational State Transfer (REST) для среды.

Перед выполнением этой задачи необходимо установить продукт управления бизнес-процессами WebSphere.

Развертывание служб REST выполняется автоматически в профайле автономного сервера. Для других типов конфигураций вы можете воспользоваться страницей административной консоли, чтобы настроить службы REST для всех виджетов продукта в Business Space. На странице Службы REST вы можете просмотреть все службы для среды и включить или отключить каждую из них по отдельности.

Вам также необходимо зарегистрировать конечные точки REST в Business Space. Business Space связывает виджеты с этими конечными точками, и виджеты появляются в палитре, становясь доступными. Инструкции по регистрации конечных точек REST в Business Space приведены в разделе Настройка Business Space и регистрация конечных точек REST с помощью административной консоли.

Если вы хотите настроить несколько экземпляров одной и той же конечной точки служб REST, то вы должны вручную отредактировать файл конечных точек и файл метаданных виджетов. Дополнительная информация приведена в разделе Включение виджетов Business Space для работы с несколькими конечными точками.

Приложение Шлюз служб REST подключает обычные системные службы REST. Это приложение создается во время настройки служб REST.

1. Выберите **Службы > Службы REST > Службы REST**.

Появится страница Службы REST с перечнем всех служб REST в среде.

2. В разделе **Диапазон** выберите опцию **Все**, чтобы просмотреть все службы REST в среде, либо выберите сервер или кластер, в котором вы включили службы REST. Если в выбранном диапазоне отсутствуют ожидаемые службы REST, включите Шлюз служб REST или связанные провайдеры служб REST на сервере или в кластере. См. раздел Настройка служб REST для сервера, кластера или компонента.

3. В таблице служб REST для провайдера, в каждой строке отметьте переключатель **Включено**, если вы хотите включить отдельную службу REST, или сотрите отметку с переключателя **Включено**, если вы хотите отключить ее.

4. Для каждой отдельной службы, которую вы хотите включить, введите осмысленное описание в столбце **Описание**.
5. Нажмите **ОК** для фиксации изменений в службах.
 - Настройте Business Space.
 - Настройте таблицы базы данных (если вы используете удаленную базу данных или среду сетевого развертывания).
 - Зарегистрируйте конечные точки служб REST.
 - В случае нескольких экземпляров конечных точек служб, например, когда вы распределяете работу между двумя кластерами и хотите, чтобы виджеты показывали данные из каждого кластера, вы должны вручную включить дополнительные виджеты для каждого дополнительного кластера.
 - Настройте защиту Business Space.

Настройка служб REST в поставщике служб:

Настройка служб Representational State Transfer (REST) в поставщике служб с помощью страницы административной консоли настройки поставщиков служб REST.

Перед выполнением этой задачи необходимо установить продукт управления бизнес-процессами WebSphere.

Развертывание служб REST выполняется автоматически в профайле автономного сервера. Для других типов конфигураций административная консоль позволяет настраивать службы REST для всех виджетов продукта в Business Space. На странице административной консоли настройки поставщиков служб можно просмотреть все службы выбранного поставщика служб и включить или выключить каждую службу отдельно. Эта страница позволяет управлять конфигурацией отдельной службы в процессе работы со всеми службами поставщика служб.

При этом необходимо зарегистрировать конечные точки REST с помощью Business Space. Затем Business Space связывает виджеты с этими конечными точками, и виджеты появляются в палитре для использования. Проверка регистрации конечных точек REST с помощью бизнес-пространства описана в разделе Настройка бизнес-пространства и регистрация конечных точек REST с помощью административной консоли.

Если требуется настроить несколько экземпляров одной конечной точки служб REST, необходимо вручную отредактировать файл конечных точек и файл метаданных виджетов. Дополнительная информация приведена в разделе Включение виджетов бизнес-пространства для работы с несколькими конечными точками.

Приложение REST Services Gateway включает общие системные службы REST. Приложение REST Services Gateway устанавливается при настройке служб REST.

Следующие поставщики служб REST доступны и настроены в показанной области:

- **REST Services Gateway:** Для добавления REST Services Gateway для данной области выберите **Серверы > Типы серверов > мой-сервер > Интеграция бизнес-процессов > Службы REST** или **Серверы > Кластеры > мой-кластер > Интеграция бизнес-процессов > Службы REST**. Настройте поставщика шлюзов служб REST для данного сервера или кластера.
- **REST Services Gateway Dmgr:** Поставщик REST Services Gateway в администраторе развертывания настраивается автоматически при создании профайла администратора развертывания для IBM Business Process Manager или WebSphere Enterprise Service Bus. Этот поставщик предоставляет

административные службы REST, используемые виджетами Обзор модулей, Администрирование модулей, Монитор состояния и Шлюз Proxu.

1. Выберите **Службы > Службы REST > Поставщики служб REST**.

Откроется страница Поставщики служб REST, на которой представлены все поставщики служб REST.

2. Щелкните на ссылке поставщика, чтобы настроить службы для группы служб REST, которыми владеет данный поставщик.

Откроется страница Настройка поставщиков служб REST, на которой представлены все службы REST поставщика.

3. Выберите **Протокол** из списка всех служб REST, которые нужно настроить и которые доступны в Business Space. Настройте полный путь URL, выбрав **https://** или **http://** и заполнив поля **Имя хоста или виртуальный хост в среде сбалансированной нагрузки** и **Порт**. Используйте полное имя хоста.

Если требуется, чтобы запросы REST направлялись непосредственно серверу приложений, то введите имя хоста сервера приложений и его порт. Если требуется, чтобы запросы REST направлялись серверу Proxu или серверу HTTP, расположенному перед одним или несколькими серверами приложений, введите имя хоста и порт сервера Proxu или сервера HTTP, который уже настроен. В среде с распределителем нагрузки или сервером Proxu между браузером и бизнес-пространством и службами REST убедитесь в том, что назначение для протокола, хоста и порта соответствует URL браузера для доступа к бизнес-пространству.

4. В таблице, в которой приведены службы REST поставщика, в каждой строке включите переключатель **Включена**, чтобы включить отдельную службу REST, или выключите переключатель **Включена**, чтобы выключить отдельную службу REST.

5. Для каждой включенной отдельной службы введите значимое описание в столбец **Описание**.

6. Нажмите кнопку **ОК**, чтобы сохранить изменения в службах.

- Настройте Business Space.
- Настройте таблицы базы данных (если используется удаленная база данных или среда сетевого развертывания).
- Зарегистрируйте конечные точки служб REST.
- В случае нескольких экземпляров конечных точек служб, например, если задание распределяется на двух кластерах и нужно, чтобы виджеты показывали данные из каждого кластера, необходимо включить дополнительные виджеты вручную для каждого дополнительного кластера.
- Настройте защиту для Business Space.

Настройка служб REST для сервера, кластера или компонента:

С помощью страницы административной консоли Службы REST настройте службы Representational State Transfer (REST) для сервера, кластера или компонента.

Перед выполнением этой задачи необходимо установить продукт управления бизнес-процессами WebSphere.

Развертывание служб REST выполняется автоматически в профайле автономного сервера. Для других типов конфигураций вы можете воспользоваться страницей административной консоли Службы REST, чтобы настроить службы для сервера, кластера или компонента.

Эта задача настраивает приложение провайдера служб REST для конкретного сервера или кластера. Вы должны настроить приложение провайдера, прежде чем службы REST станут доступны на сервере или в кластере. Дополнительная информация о провайдерах служб REST приведена в разделе Настройка служб REST в провайдере служб.

Вам также необходимо зарегистрировать конечные точки REST в Business Space. Business Space связывает виджеты с этими конечными точками, и виджеты появляются в палитре, становясь доступными. Инструкции по регистрации конечных точек REST в Business Space приведены в разделе Настройка Business Space и регистрация конечных точек REST с помощью административной консоли.

Если вы хотите настроить несколько экземпляров одной и той же конечной точки служб REST, то вы должны вручную отредактировать файл конечных точек и файл метаданных виджетов. Дополнительная информация приведена в разделе "Включение виджетов Business Space для работы с несколькими конечными точками."

Приложение Шлюз служб REST подключает обычные системные службы REST. Это приложение создается во время настройки служб REST.

1. Выберите одну из следующих опций.
 - Для служб REST на сервере выберите **Серверы > Типы серверов > Серверы приложений WebSphere > имя_сервера > Business Integration > Службы REST.**
 - Для служб REST в кластере выберите **Серверы > Кластеры > Кластеры сервера приложений WebSphere > имя_кластера > Business Integration > Службы REST.**

Появится страница Службы REST со всеми службами REST по умолчанию, которые можно настроить для виджетов Business Space для использования с продуктом или компонентом (Администратором бизнес-поток или Администратором неавтоматизированных задач). Если служба REST уже настроена, то будет показано соответствующее сообщение.

2. Выберите **Протокол** из списка для всех служб REST, которые вы хотите настроить, так чтобы они стали доступны в Business Space. Настройте полный URL, выбрав **https://** или **http://** и затем заполнив поля **Имя хоста или виртуального хоста в среде с распределением нагрузки** и **Порт**. Укажите полное имя хоста.

Если вы хотите, чтобы запросы REST направлялись напрямую на конкретный сервер приложений, то укажите имя хоста и порт этого сервера приложений. Если вы хотите, чтобы запросы REST направлялись на сервер Проху или HTTP, расположенный перед одним или несколькими серверами приложений, то укажите имя хоста и порт этого сервера Проху или HTTP, который вы уже настроили. В среде, в которой браузер, с одной стороны, и Business Space и службы REST - с другой, разделены сервером распределения нагрузки или сервером Проху, вы должны проследить за тем, чтобы значения протокола, хоста и порта соответствовали URL браузера, по которому доступен Business Space. То же ограничение относится ко всем средам, использующим виджеты Business Space с поддержкой Flex.

3. В таблице служб REST, в каждой строке отметьте переключатель **Включено**, если вы хотите включить отдельную службу REST, или сотрите отметку с переключателя **Включено**, если вы хотите отключить ее.
4. В таблице служб REST введите осмысленное описание каждой службы REST в поле **Описание**.
5. Нажмите **ОК** для фиксации изменений в службах.

Если впоследствии вы захотите изменить конфигурацию служб REST, то вы сможете вернуться к странице Службы REST или с помощью других страниц административной консоли изменить конфигурацию конечных точек служб REST.

Страница провайдеров служб REST позволяет выбрать провайдер служб для настройки. Страница служб REST, открытая из **Службы > Службы REST**, позволяет настроить все службы REST в среде.

- Настройте Business Space.
- Настройте таблицы базы данных (если вы используете удаленную базу данных или среду сетевого развертывания).
- Зарегистрируйте конечные точки служб REST.
- В случае нескольких экземпляров конечных точек служб, например, когда вы распределяете работу между двумя кластерами и хотите, чтобы виджеты показывали данные из каждого кластера, вы должны вручную включить дополнительные виджеты для каждого дополнительного кластера.
- Настройте защиту Business Space.

Настройка служб REST с помощью командной строки:

Все виджеты, необходимые продукту, устанавливаются вместе с Business Space, созданное с использованием WebSphere. Службы Representational State Transfer (REST) для виджетов должны быть настроены, подключены и зарегистрированы в Business Space, прежде чем они станут доступны вашему коллективу в Business Space. Если вы не пользуетесь страницей административной консоли Службы REST, то выполните команду **updateRESTGatewayService**.

Перед выполнением этой задачи необходимо установить продукт управления бизнес-процессами WebSphere.

Развертывание служб REST выполняется автоматически в профайле автономного сервера. Для других типов конфигураций вы можете воспользоваться страницей административной консоли Службы REST или командой **updateRESTGatewayService**, чтобы настроить службы для интерфейсов прикладных программ (API) REST для всех виджетов продукта в Business Space.

Вам также необходимо зарегистрировать конечные точки REST в Business Space. Business Space связывает виджеты с этими конечными точками, и виджеты появляются в палитре, становясь доступными.

Если вы хотите настроить несколько экземпляров одной и той же конечной точки служб REST, то вы должны вручную отредактировать файл конечных точек и файл метаданных виджетов. Дополнительная информация приведена в разделе "Включение виджетов Business Space для нескольких конечных точек."

1. Откройте командное окно.
Команду **wsadmin** можно найти в каталоге *каталог_профайла/bin* для среды автономного сервера или в каталоге *каталог_профайла_администратора_развертывания/bin* для среды сетевого развертывания.
2. В командной строке введите команду **wsadmin**, чтобы запустить среду **wsadmin**.
3. С помощью команды **updateRESTGatewayService** настройте службы REST, указав кластер или сервер и узел. Параметр **-enable** необязателен; по умолчанию он равен **true**.
4. Запустите команду сохранения.

В следующем примере используется Jython для выполнения команды **updateRESTGatewayService** и последующего сохранения изменений. Службы REST настраиваются в кластере.

```
AdminTask.updateRESTGatewayService(['-clusterName  
имя_кластера'])  
AdminConfig.save()
```

В следующем примере используется Jacl:

```
$AdminTask updateRESTGatewayService {-clusterName  
имя_кластера}  
$AdminConfig save
```

- Настройте Business Space.
- Настройте таблицы базы данных (если вы используете удаленную базу данных или среду сетевого развертывания).
- Зарегистрируйте конечные точки служб REST.
- В случае нескольких экземпляров конечных точек служб, например, когда вы распределяете работу между двумя кластерами и хотите, чтобы виджеты показывали данные из каждого кластера, вы должны вручную включить дополнительные виджеты для каждого дополнительного кластера.
- Настройте защиту Business Space.

Настройка Business Space и регистрация конечных точек REST с помощью административной консоли:

Business Space, созданное с использованием WebSphere можно установить и настроить с помощью административной консоли.

Прежде чем выполнять эту задачу, выполните следующие действия:

- Установите программное обеспечение продукта и создайте профайл. В процессе установки продукта добавляются файлы Business Space для настраиваемого профайла. Профайл пользователя не настроен для Business Space, пока Business Space не будет явно настроен в профайле.
- Включите защиту, если требуется установить защищенную среду для Business Space.
- Настройте службы REST. В среде автономного сервера или в случае использования мастера среды развертывания для настройки среды развертывания конечные точки служб REST настраиваются и включаются автоматически. Для настройки служб REST в других средах используйте страницу административной консоли служб REST. Если необходимо, чтобы в Business Space были доступны виджеты, настройте для них службы REST. На странице административной консоли Конфигурация Business Space необходимо зарегистрировать конечные точки REST, чтобы в Business Space виджеты были связаны с конечными точками и появились в палитре.
- Для того чтобы настроить Business Space на сервере или в кластере с помощью источника данных, отличного от источника данных продукта, перед настройкой Business Space с помощью административной консоли создайте источник данных в области сервера или кластера с правильным именем JNDI jdbc/mashupDS.
- В Oracle для использования схемы таблиц Business Space, отличной от той, которая используется базой данных продукта, выполните следующие действия, чтобы вручную создать источник данных, а затем откройте страницу Конфигурация Business Space:
 1. Создайте схему с помощью программного обеспечения продукта базы данных.
 2. С помощью административной консоли настройте провайдер JDBC.
 3. С помощью административной консоли создайте источник данных с именем JNDI jdbc/mashupDS в области сервера или кластера, в зависимости от среды.

4. Создайте псевдоним идентификации с помощью административной консоли. Установите для имени пользователя созданную вами схему и установите идентификацию в соответствии с настройкой Oracle.
5. Установите псевдоним идентификации в источнике данных.

При использовании сред развертывания или других расширенных конфигураций профайла необходимо с помощью административной консоли настроить Business Space для работы со средой выполнения. Business Space - это веб-интерфейс для бизнес-пользователей приложения, которое выполняется в установленном профайле. В Business Space администратор и пользователи приложения могут настраивать содержимое продукта в портфеле управления бизнес-процессами WebSphere.

1. Убедитесь, что административная консоль запущена.
2. На панели навигации выберите **Серверы > Типы серверов > Серверы приложений WebSphere** или **Серверы > Кластеры > Кластеры сервера приложений WebSphere**.
3. Выберите имя сервера или целевого объекта кластера.
4. На странице Конфигурация под **Бизнес-интеграция** выберите **Конфигурация Business Space**. Откроется страница Конфигурация Business Space. Если Business Space уже настроен; эту страницу можно просматривать, но нельзя изменять поля.
5. Выберите опцию **Установить службу Business Space**.
6. В поле **Имя схемы базы данных** введите имя схемы, которая должна использоваться для базы данных Business Space.

Примечание: В Oracle имя схемы совпадает с именем пользователя, указанным в псевдониме идентификации в источнике данных.

7. Если в поле **Существующий источник данных Business Space** источник данных не указан, перейдите в **Создать источник данных Business Space с помощью** и выберите источник данных для подключения к базе данных, которая будет использоваться в Business Space.

При указании источника данных в поле **Создать источник данных Business Space с помощью:** создается источник данных для Business Space с именем JNDI jdbc/mashupDS, которое смоделировано в выбранном источнике данных.

Источник данных Business Space создается на сервере или в кластере, где настроен Business Space, даже если источник данных продукта находится на другом сервере или кластере.

Совет: Если требуемый существующий источник данных не показан, необходимо закрыть страницу Конфигурация Business Space, установить базу данных и источник данных, а затем перезапустить страницу Конфигурация Business Space для завершения настройки. Более подробная информация приведена в разделе **Перед тем, как начать**.

8. Нажмите кнопку **ОК**.
9. Для того чтобы зарегистрировать подходящую среду развертывания (кластер или сервер) для конечных точек REST системы для каждого виджета в Business Space, выберите **Регистрация конечных точек служб REST**.

Выбираемый целевой объект для типа конечной точки службы REST может определять область данных, отображаемую в некоторых виджетах. Или можно выбрать определенный кластер или сервер для оптимизации производительности или доступности.

Если применяются виджеты неавтоматизированных задач, в строке для типов Службы процессов и Службы задач можно выбрать несколько поставщиков служб REST для сервера или кластера. Выберите поставщика с именем

Name=Federated REST Services, Name=Business Process Choreographer REST services или Name=BPD engine REST services. Если задачи и процессы выполняются и в Business Process Choreographer и в службе определения бизнес-процессов (BPD); выберите Federated REST Services. Если используются только процессы и задачи, выполняющиеся в Business Process Choreographer (моделируемые в Integration Designer); выберите Business Process Choreographer REST services. Если используются только те процессы и задачи, которые выполняются в службе BPD (моделируемые в Process Designer); выберите BPD engine.

Если цель не указана, то конечная точка REST этого типа не регистрируется в Business Space, а виджеты, для которых требуется конечная точка службы REST этого типа, не показываются в Business Space.

10. Сохраните конфигурацию.
11. Выполните сценарии для настройки таблиц базы данных Business Space перед запуском среды развертывания или кластеров. Эти сценарии были сгенерированы после создания конфигурации. См. раздел Настройка базы данных Business Space.

Примечание: При работе с Oracle пароль проверки подлинности доступа к псевдониму источника данных Business Space совпадает с именем схемы Business Space. Значение по умолчанию для схемы - IBMBUSSP. При настройке Business Space можно задать другую схему в административной консоли или в командной строке. В этом случае пароль по умолчанию совпадает с указанной схемой. Для использования другого пароля для имени пользователя Business Space необходимо с помощью административной консоли изменить ресурсы JDBC (источник данных jdbc/mashupsDS). Измените значение псевдонима идентификации в соответствии с паролем для имени схемы Business Space. Сохраните изменения и перезапустите сервер.

Примечание: Business Space использует прокси-компонент для подключения к службам REST. Если в некоторых случаях службы REST не отвечают, измените параметры тайм-аута соединения из Business Space в службы REST в зависимости от производительности серверов службы REST. См. раздел Изменение параметров тайм-аута для прокси Ajax Business Space.

Настройка Business Space с помощью командной строки:

Business Space, созданное с использованием WebSphere можно установить и настроить с помощью команды **wsadmin**. Команду **wsadmin** можно использовать для выполнения той же конфигурации Business Space, которую позволяет выполнить административная консоль.

Перед выполнением этой задачи необходимо выполнить следующие задачи:

- Установите программное обеспечение продукта и создайте профайл. При установке продукта файлы Business Space включаются вместе с установкой для профайлов. Ваш профайл не будет настроен для Business Space, пока явно не будет настроен Business Space на профайле.
- Если требуется настроить защищенную среду для Business Space, включите защиту.
- Если планируется использовать файл эскиза базы данных для информации о базе данных бизнес-пространства, выполните этапы в разделе “Создание файла свойств эскиза базы данных Business Space” на стр. 203.
- Настройка служб Representational State Transfer (REST). В случае среды с автономным сервером или использования мастера среды развертывания для настройки среды выполнения конечные точки служб REST настраиваются и

включаются автоматически. В случае других сред используйте страницу административной консоли Службы REST для настройки служб REST. Если вы хотите, чтобы в Business Space были доступны виджеты, то вы должны настроить конечные точки служб REST для этих виджетов. Необходимо зарегистрировать конечные точки REST, чтобы бизнес-пространство связывало виджеты с конечными точками и виджеты появились в палитре для использования.

- Если нужно настроить бизнес-пространство на сервере или в кластере с использованием другого источника данных, кроме источника данных продукта, создайте источник данных на сервере или в области кластера с правильным именем JNDI jdbc/mashupDS перед настройкой бизнес-пространства (перед выполнением команды **configureBusinessSpace**).
- В случае Oracle для использования другой схемы таблиц бизнес-пространства, чем та, которая используется базой данных продукта, выполните следующие действия для создания источника данных вручную перед выполнением команд установки и настройки Business Space в следующей процедуре:
 - С помощью административной консоли настройте провайдер JDBC.
 - С помощью административной консоли создайте источник данных с именем JNDI jdbc/mashupDS на сервере или в области кластера в зависимости от вашей среды.

Для настройки Business Space можно использовать командную строку, если требуется написать сценарии для настройки Business Space вместо использования административной консоли.

Если вы не уверены, не настроен ли уже Business Space, можно выполнить команду **getBusinessSpaceDeployStatus**, чтобы узнать не настроен ли Business Space на сервере, в кластере или ячейке. Дополнительная информация об этой команде приведена в разделе "Команда getBusinessSpaceDeployStatus".

Для настройки бизнес-пространства выполните следующее.

1. Откройте командное окно.

Команду **wsadmin** можно найти в каталоге *каталог_профайла/bin* для среды автономного сервера или в каталоге *каталог_профайла_администратора_развертывания/bin* для среды сетевого развертывания.

2. В командной строке введите команду **wsadmin**, чтобы запустить среду **wsadmin**.
3. Используйте команду **installBusinessSpace** для установки файлов архива предприятия (EAR) Business Space в вашу среду выполнения.
4. Используйте команду **configureBusinessSpace** для настройки источника данных для Business Space и скопируйте сценарии, которые настраивают таблицы базы данных, в *корневой-каталог-профайлов/dbscripts/BusinessSpace/имя-узла_имя-сервера/тип-базы-данных/имя-базы-данных* для автономного сервера или в *корневой-каталог-профайлов/dbscripts/BusinessSpace/имя-кластера/тип-базы-данных/имя-базы-данных* для кластера.

Необходимо выполнить сценарии, настраивающие таблицы базы данных. Дополнительная информация о сценариях приведена в разделе "Настройка базы данных Business Space" на стр. 203.

В случае использования файла эскиза базы данных для настройки базы данных можно использовать параметр **-bspacedbDesign** для обозначения этого файла при выполнении команды **configureBusinessSpace**.

5. После каждой команды выполните `AdminConfig.save()` (Jython) или `$AdminConfig.save()` (Jacl).

6. Перед запуском среды развертывания или кластеров выполните сценарии настройки таблиц базы данных для бизнес-пространства. Дополнительная информация приведена в разделе Настройка таблиц базы данных бизнес-пространства.

При настройке Business Space устанавливается графический пользовательский интерфейс на основе браузера для бизнес-пользователей вашего приложения, которое выполняется с заданным профайлом. В Business Space вы и пользователи вашего приложения можете настраивать содержимое из продуктов портфеля управления бизнес-процессами WebSphere.

В следующем примере Jython используется для выполнения команд **installBusinessSpace** и **configureBusinessSpace** для установки файлов EAR и настройки источника данных для Business Space в кластере. В этом примере схема и база данных продукта определяются для использования с Business Space при установке нескольких продуктов. В ситуации, когда установлены IBM Business Process Manager и IBM Business Monitor, в этом примере создается источник данных Business Space с использованием свойств источника данных IBM Business Process Manager.

```
AdminTask.installBusinessSpace('[-clusterName myCluster -save true]')
AdminTask.configureBusinessSpace('[-clusterName myCluster -schemaName mySchema -productTypeForDatasource WPS -save true]')
```

В следующем примере используется Jacl:

```
$AdminTask installBusinessSpace {-clusterName myCluster -save true}
$AdminTask configureBusinessSpace {-clusterName myCluster -schemaName mySchema -productTypeForDatasource WPS -save true}
```

Совет: При использовании Oracle паролю псевдонима идентификации источника данных бизнес-пространства присваивается имя, совпадающее с именем схемы бизнес-пространства. По умолчанию применяется значение схемы IBMBUSSP. При настройке Business Space можно указать другую схему на административной консоли или в командной строке. В этом случае по умолчанию применяется тот же пароль, что и у схемы. Для применения другого пароля для имени пользователя бизнес-пространства необходимо использовать административную консоль для обновления ресурсов JDBC: Поиск источника данных jdbc/mashupsDS. Измените значение псевдонима идентификации, чтобы оно совпадало с паролем имени схемы бизнес-пространства. Сохраните изменения и перезапустите сервер.

После настройки Business Space необходимо выполнить следующие действия, чтобы включить Business Space для среды выполнения.

- Зарегистрируйте конечные точки с помощью команды **registerRESTserviceEndpoint**.
- Настройте защиту для Business Space и виджетов, используемых вашей группой. Дополнительная информация приведена в разделе "Настройка защиты для Business Space".

Совет: Бизнес-пространство использует компонент Proxu для соединения с вашими службами REST. В некоторых случаях, когда службы REST не отвечают, требуется обновить параметры тайм-аута соединения для служб REST из бизнес-пространства в зависимости от производительности серверов служб REST. Дополнительная информация приведена в разделе Изменение параметров тайм-аута для Proxu Ajax бизнес-пространства.

Создание файла свойств эскиза базы данных Business Space:

Если тип базы данных Business Space отличается от типа по умолчанию, создайте файл свойств эскиза базы данных; это упростит процесс создания базы данных.

Шаблоны файлов эскиза для каждого типа базы данных находятся в каталоге *каталог-установки/BusinessSpace/config.bspace/MetadataFiles*; например, шаблон файла эскиза для DB2 называется *BSpace_DB2-distributed.properties*.

1. Создайте новый файл, скопировав файл шаблона подходящего типа базы данных.
2. В файле свойств эскиза базы данных настройте значения свойств в соответствии со своей конфигурацией. В файле есть комментарии, помогающие выбрать правильные значения свойств.

Укажите полный путь к файлу свойств эскиза базы данных одним из следующих способов в зависимости от среды продукта и средства настройки:

- Если для настройки Business Space с профайлом используется инструмент управления профайлами; укажите файл эскиза базы данных, выбрав команду **Использовать файл эскиза базы данных**.
- Если для настройки Business Space с профайлом применяется утилита командной строки **manageprofiles**, укажите файл эскиза базы данных в параметре **-bspacedbDesign**.
- Если для настройки Business Space используется команда **configureBusinessSpace**, укажите файл эскиза базы данных в параметре **-bspacedbDesign**.

Настройка базы данных Business Space:

Можно вручную установить таблицы базы данных для Business Space на удаленном сервере базы данных с помощью сценариев, созданных программой установки. При использовании среды развертывания или удаленной базы данных необходимо установить эти таблицы после настройки Business Space.

Перед тем как приступить к выполнению этой задачи, выполните следующие действия:

- Установите продукт.
- Создайте профайлы и настройте серверы или кластеры для Business Space.
- (для Oracle) Создайте базу данных.
- (для Microsoft SQL Server) Задайте идентификацию экземпляра SQL Server. Драйвер JDBC для SQL Server поддерживает только смешанный режим идентификации. Поэтому во время создания экземпляра SQL Server следует выбрать тип идентификации **SQL Server и Windows**.
- Для всех баз данных убедитесь, что база данных установлена с кодировкой UTF-8, если в среде будет использоваться Business Space.
- Убедитесь, что сервер приложения с Business Space остановлен.

Если при использовании DB2 for z/OS необходимые ресурсы не были настроены во время базовой установки продукта, выполните следующие дополнительные действия перед выполнением этой задачи:

- Создайте базу данных TEMP и табличное пространство TEMP для хранения объявленных временных таблиц для обработки допускающих прокрутку курсоров.
- Создайте выделенный объект STOGROUP для хранения данных Business Space.

Для DB2 for z/OS, если необходимо использовать другую группу носителей (например, если нежелательно, чтобы таблицы базы данных Business Space

добавлялись в одну базу данных и группу носителей с общей базой данных), измените и выполните сценарий `createTablespace_BusinessSpace.sql` после настройки Business Space и перед настройкой таблиц базы данных Business Space.

- Измените файл `createTablespace_BusinessSpace.sql` в каталоге *каталог-профайла/dbscripts/BusinessSpace/имя-узла_имя-сервера/тип-базы-данных/имя-базы-данных* (для автономного сервера) или в *каталог-профайла/dbscripts/BusinessSpace/имя-кластера/тип-базы-данных/имя-базы-данных* (для кластера), где *тип-базы-данных* - DB2zOS.
- Поменяйте значение VCAT с @VCAT@ на имя или псевдоним каталога интегрированных средств каталогов для использования группой носителей.

Если используется DB2 V9.x и требуется повысить производительность, измените файл `createTablespace_BusinessSpace.sql`. Файл `createTablespace_BusinessSpace.sql` находится в каталоге *каталог-профайла/dbscripts/BusinessSpace/имя-узла_имя-сервера/тип-базы-данных/имя-базы-данных* (для автономного сервера) или *каталог-профайла/dbscripts/BusinessSpace/имя-кластера/тип-базы-данных/имя-базы-данных* (для кластера).

- Поменяйте IMMEDIATE SIZE 8000 PAGESIZE 32K на IMMEDIATE SIZE 8000 AUTOMATIC PAGESIZE 32K.
- Добавьте строку PREFETCHSIZE AUTOMATIC после EXTENTSIZE 16 под CREATE SYSTEM TEMPORARY TABLESPACE @TSDIR@TMPTP и CREATE REGULAR TABLESPACE @TSDIR@REGTP.

Сценарий `configBusinessSpaceDB` настраивает таблицы для Business Space с заданной базой данных. (При создании таблиц в существующей базе данных вместо сценария `configBusinessSpaceDB` следует использовать сценарий `createDBTables`, поставляемый с продуктом.)

Для настройки таблиц базы данных для Business Space выполните следующие действия.



1. Убедитесь, что используется идентификатор пользователя с достаточными полномочиями для создания таблиц.
2. Найдите сценарий в настроенном профайле и сохраните его в системе, где находится база данных.
 - Для всех баз данных, за исключением DB2 for z/OS, найдите сценарий `configBusinessSpaceDB.bat` или `configBusinessSpaceDB.sh`.
 - Для WebSphere Enterprise Service Bus for z/OS, если требуется настроить таблицы базы данных Business Space вместе со всеми остальными объектами базы данных, найдите сценарий `createDB.sh`.
 - Для DB2 for z/OS, если не выполнять сценарий `createDB.sh`, необходимо по отдельности выполнить файлы Business Space. Найдите `createDatabase.sql`, `createStorageGroup_BusinessSpace.sql`, `createTablespace_BusinessSpace.sql` и `createTable_BusinessSpace.sql`.

По умолчанию сценарии находятся в следующем каталоге: *каталог-профайла/dbscripts/BusinessSpace/имя-узла_имя-сервера/тип-базы-данных/имя-базы-данных* для автономного сервера или *каталог-профайла/dbscripts/BusinessSpace/имя-кластера/тип-базы-данных/имя-базы-данных* для кластера. Обновленные сценарии (с информацией, которая была введена во время создания профайла) находятся в настроенном профайле для сервера или кластера. Если использовался мастер настройки среды развертывания, сценарии находятся в профайле администратора развертывания. Во время настройки удаленной базы данных, скопируйте сценарии из системы, где установлен продукт, в удаленную систему.

3. Для **WebSphere Enterprise Service Bus for z/OS**: при настройке DB2 for z/OS можно использовать сценарий `createDB.sh` для настройки таблиц базы данных Business Space в одной базе данных со всеми остальными объектами базы данных. См. раздел "Создание объектов базы данных DB2 с помощью сценария `createDB.sh`" в документации WebSphere Enterprise Service Bus for z/OS.

4. В командной строке выполните одну из следующих команд в зависимости от платформы.

Скопируйте каталог с пакетными файлами и сценариями в каталог, где находится база данных, и выполните команду в этом каталоге. ИД пользователя должен иметь доступ к интерпретатору команд для этого типа базы данных и права доступа на выполнение команд.

-   Для платформ **Linux, UNIX и z/OS**:
`configBusinessSpaceDB.sh`

-  Для платформ **Windows**: `configBusinessSpaceDB.bat`

Для DB2 и SQL Server используйте необязательный параметр **-createDB**, если необходимо создать другую базу данных вместо использования существующей.

Ограничение: Если используется SQL Server, после выполнения сценария базы данных в файле `systemout.log` могут появиться следующие предупреждения: ... Предупреждение! Максимальная длина ключа 900 байт При использовании объединенных хранилищ в качестве реестра пользователей на эти предупреждения можно не обращать внимания. Если используется автономный реестр LDAP, количество символов в записях отличительных имен (DN) пользователей организации не должно превышать 131. Если количество символов некоторых записей DN превышает 131, вместо реестра учетных записей пользователей следует выбрать объединенные хранилища.

Для DB2 for z/OS выполните следующие файлы по порядку:

- `createDatabase.sql`
- `createStorageGroup_BusinessSpace.sql`
- `createTablespace_BusinessSpace.sql`
- `createTable_BusinessSpace.sql`

5.    Для DB2 и DB2 for z/OS: свяжите интерфейс командной строки с базой данных Business Space с помощью следующих команд:

```
db2 connect to имя-базы-данных
db2 bind каталог-установки-DB2\bnd\@db2cli.lst blocking all grant
public
db2 connect reset
```

где

имя-базы-данных - имя базы данных Business Space

каталог-установки-DB2 - каталог, в котором установлена DB2

6. Если база данных Business Space создается повторно после предыдущего удаления; перед тем как приступить к использованию среды Business Space, необходимо импортировать шаблоны и пространства Business Space. Выполните действия из раздела Обновление шаблонов и пространств Business Space после установки или обновления виджетов.
- Обновите конечные точки для виджетов, которые должны быть доступны в Business Space.
 - Настройте защиту для Business Space и используемых виджетов.

Регистрация конечных точек службы REST виджетов Business Space с помощью командной строки:

При настройке Business Space с помощью административной консоли необходимо зарегистрировать конечные точки Representational State Transfer (REST), чтобы ваша группа могла использовать виджеты в Business Space. Если конечные точки не были зарегистрированы с помощью административной консоли на страницах регистрации конечных точек настройки бизнес-пространства и системных служб REST, то необходимо использовать команду **registerRESTServiceEndpoint**.

Перед выполнением этой задачи необходимо выполнить следующие задачи:

- Установите продукт.
- Настройте службы REST для виджетов, используемых в Business Space, с помощью страницы административной консоли Службы REST или команды **updateRESTGatewayService**. В случае среды с автономным сервером или использования мастера среды развертывания для настройки среды выполнения службы REST настраиваются и включаются автоматически.
- Настройте Business Space с помощью страницы административной консоли Настройка бизнес-пространства или команд **installBusinessSpace** и **configureBusinessSpace**.
- Настройте таблицы базы данных (если используется удаленная база данных или среда сетевого развертывания).

Службы REST регистрируются автоматически в случае среды с автономным сервером и настройки бизнес-пространства с помощью административной консоли или инструмента управления профайлами, или если для настройки среды выполнения использовался мастер среды развертывания. В противном случае необходимо настроить службы REST и затем зарегистрировать их.

Можно использовать страницу административной консоли регистрации конечных точек системных служб REST или команду **registerRESTServiceEndpoint** для регистрации конечных точек служб REST для всех виджетов вашего продукта в Business Space. Затем Business Space автоматически связывает виджеты с этими конечными точками, и эти виджеты появляются в палитре Business Space для использования.

Команду **registerRESTServiceEndpoint** можно использовать для регистрации некоторого набора конечных точек данного поставщика, целевого объекта развертывания или всех уникальных конечных точек в ячейке. Эта команда регистрирует конечные точки служб REST, которые находятся в той же ячейке, что и Business Space.

1. Откройте командное окно.
Команду **wsadmin** можно найти в каталоге *каталог_профайла/bin* для среды автономного сервера или в каталоге *каталог_профайла_администратора_развертывания/bin* для среды сетевого развертывания.
2. В командной строке введите команду **wsadmin**, чтобы запустить среду **wsadmin**.
3. Используйте команду **registerRESTServiceEndpoint** для регистрации конечных точек Business Space служб REST для всех виджетов вашего продукта.
4. После каждой команды выполняйте команду сохранения.

В следующем примере Jython используется для выполнения команды **registerRESTServiceEndpoint** и затем для сохранения изменений. Она регистрирует все настроенные и включенные службы REST в кластере с Business Space.

```
AdminTask.registerRESTServiceEndpoint('[-clusterName
  имя-кластера-служб-rest -businessSpaceClusterName
  имя-кластера-бизнес-пространства]')
AdminConfig.save()
```

где *имя-кластера-служб-rest* – имя кластера, в котором настроены службы REST, а *имя-кластера-бизнес-пространства* – имя кластера, в котором развернуто бизнес-пространство.

В следующем примере используется Jacl:

```
$AdminTask registerRESTServiceEndpoint
{-clusterName имя-кластера-служб-rest
-businessSpaceClusterName имя-кластера-бизнес-пространства}
$AdminConfig save
```

где *имя-кластера-служб-rest* – имя кластера, в котором настроены службы REST, а *имя-кластера-бизнес-пространства* – имя кластера, в котором развернуто бизнес-пространство.

Параметры **appName**, **webModuleName**, **type**, **name**, **version**, **nodeName**, **serverName** или **clusterName** являются необязательными.

Если параметры **type**, **appName** и **webModuleName** не заданы, то регистрируются все уникальные конечные точки служб REST, настроенных на целевом объекте развертывания.

Если любой из этих параметров не задан, то регистрируются все уникальные конечные точки служб REST, настроенных на любом целевом объекте развертывания.

Совет: Бизнес-пространство использует компонент Proxu для соединения с вашими службами REST. В некоторых случаях, когда службы REST не отвечают, требуется обновить параметры тайм-аута соединения для служб REST из бизнес-пространства в зависимости от производительности серверов служб REST. Дополнительная информация приведена в разделе Изменение параметров тайм-аута для Proxu Ajax бизнес-пространства.

Настройка сервера Proxu или сервера распределения нагрузки для поддержки Business Space:

Если вы применяете Business Space в среде с сервером Proxu или сервером распределения нагрузки, то вы должны настроить среду для правильной работы Business Space и виджетов.

В среде сетевого развертывания, или кластерной среде, обычно настраивается сервер проху или сервер HTTP - по соображениям безопасности и для выравнивания нагрузки. Вместо отправки запросов HTTP напрямую серверу приложений они направляются на сервер проху, который может разослать запросы на несколько серверов приложений, выполняющих работу.

Вместо сервера проху или перед ним можно использовать другие серверы маршрутизации, например IBM HTTP Server.

Важное замечание: Сервер проху (или альтернативный сервер маршрутизации) необходим для распределения запросов HTTP на выравнивание нагрузки между двумя или более элементами кластера. Сервер проху позволяет клиентам обращаться к приложениям в пределах этой топологии.

В среде, в которой браузер, с одной стороны, и Business Space и службы REST - с другой, разделены сервером распределения нагрузки или сервером Proxy, вы должны проследить за тем, чтобы значения протокола служб REST, хоста и порта соответствовали URL браузера, по которому доступен Business Space. На странице провайдеров служб REST на административной консоли убедитесь, что для всех провайдеров, например Администратора бизнес-потоков и Администратора неавтоматизированных задач, правильно заданы протокол, хост и порт. Дополнительная информация об изменении служб REST приведена в разделе Настройка служб REST в провайдере служб.

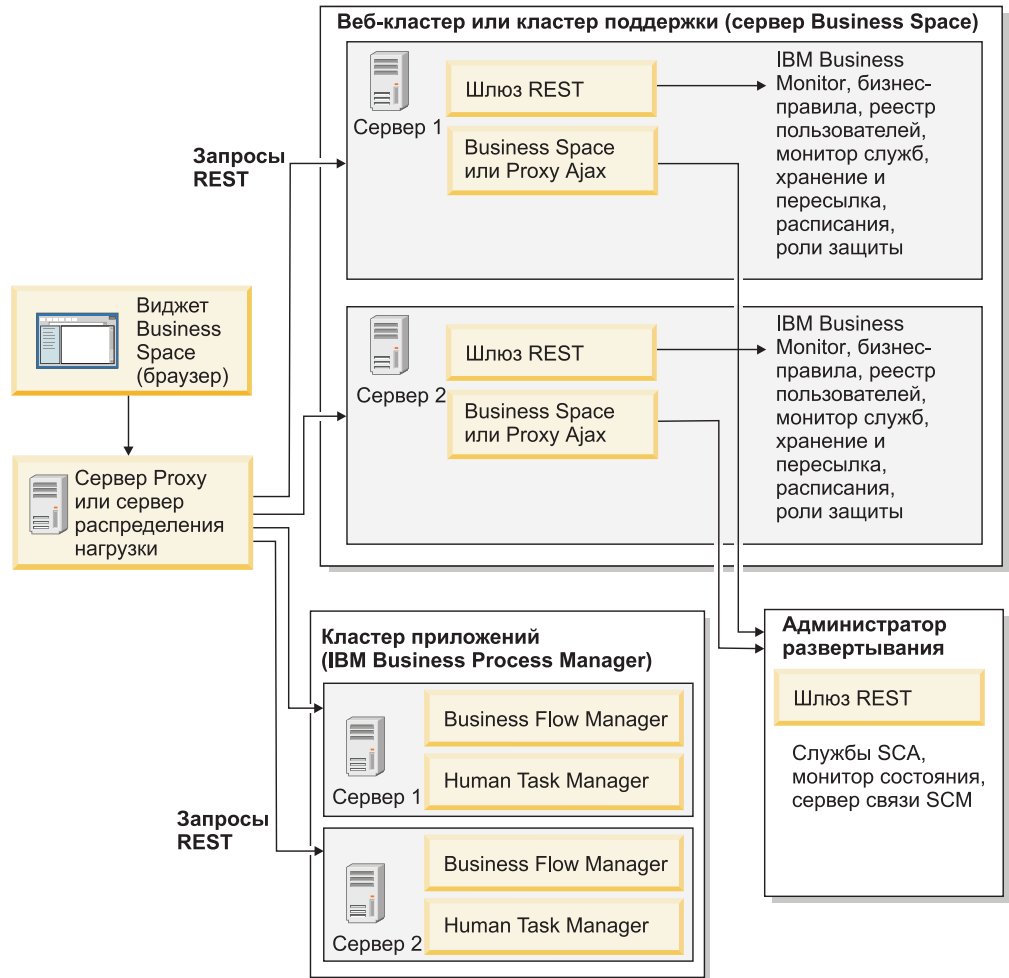


Рисунок 1. Типичная топология

Если вы применяете IBM HTTP Server, то вы должны выполнить дополнительные действия по связыванию модулей с веб-сервером и настройке псевдонимов хостов.

Если вы применяете сервер Proxy WebSphere Application Server, то вы должны убедиться, что для него включены все модули.

Если вы применяете обратный Proxy для сервера HTTP, то вы должны связать URL Business Space и виджетов.

Настройка IBM HTTP Server для Business Space:

При использовании IBM HTTP Server необходимо выполнить дополнительные действия по настройке Business Space для работы в такой среде.

Перед настройкой IBM HTTP Server для работы с Business Space выполните следующие действия:

- Установите IBM HTTP Server
- Включите SSL для IBM HTTP Server.
- Добавьте определение веб-сервера для IBM HTTP Server в сервер приложений.
В процессе установки встраиваемого модуля IBM HTTP Server в системе веб-сервера создается сценарий `configureвеб-сервер`. Сценарий `configureвеб-сервер` предназначен для связывания модулей веб-приложения с веб-сервером. Поэтому выполните этот сценарий после создания среды развертывания.

1. Убедитесь, что модули связаны с веб-сервером. Для каждого приложения, требуемого в Business Space, веб-сервер должен быть одним из выбранных назначений.

- a. Войдите в административную консоль как администратор.
- b. Выберите **Приложения > Типы приложений > Приложения J2EE WebSphere**.
- c. На панели Приложения J2EE выберите имя приложения.

Отметьте следующие приложения. В списке можно выбрать некоторые или все приложения, которые используются с Business Space.

- **BPMAdministrationWidgets_имя-узла_имя-сервера** (для WebSphere Enterprise Service Bus и IBM Business Process Manager)
- **BusinessSpaceHelpEAR_имя-узла_имя-сервера** (для всех продуктов)
- **BSpaceEAR_имя-узла_имя-сервера** (для всех продуктов)
- **BSpaceForms_имя-узла_имя-сервера** (для всех продуктов)
- **HumanTaskManagementWidgets_имя-узла_имя-сервера** (для IBM Business Process Manager и IBM Business Monitor)
- **REST Services Gateway** (для всех продуктов)
- **REST Services Gateway Dmgr** (для WebSphere Enterprise Service Bus и IBM Business Process Manager)
- **mm.was_имя-узла_имя-сервера** (для всех продуктов)
- **WBMDashboardWeb_имя-узла_имя-сервера** (для IBM Business Monitor)
- **webWidgets_имя-узла_имя-сервера** (для WebSphere Enterprise Service Bus)

d. Для каждого приложения на вкладке Конфигурация в разделе Модули выберите **Управление модулями**.

e. На странице Управление модулями приложения веб-сервер должен быть одним из выбранных назначений каждого модуля.

- В таблице отметьте столбец Сервер для каждого модуля, чтобы веб-сервер был одним из выбранных назначений. Например, для приложения `mm.was_имя-узла_имя-сервера` найдите веб-сервер, показанный в столбце Сервер: **WebSphere:cell=qaxs41Cell02,node=qaxs41Node03,server=httpserver WebSphere:cell=qaxs41Cell02,cluster=Golden.WebApp**.
- Если необходимо добавить веб-сервер, включите переключатель рядом с именем модуля. Затем с помощью клавиши Ctrl выберите несколько назначений в списке Кластеры и серверы. Например, для того чтобы веб-сервер обслуживал приложение, выберите кластер сервера приложений и веб-сервер, удерживая клавишу Ctrl. Нажмите **Применить**, **ОК** и **Сохранить** для сохранения внесенных изменений.

2. Убедитесь, что псевдоним имени хоста `default_host` содержит правильные сведения для каждого элемента кластера, веб-сервера или прокси-сервера.
 - a. Войдите в административную консоль как администратор.
 - b. Выберите **Серверы > Типы серверов > Серверы приложений WebSphere**.
 - c. Для каждого элемента кластера выберите имя сервера приложений и посмотрите номер порта для имени порта **WC_defaulthost**.
 - Под разделом Средства связи разверните **Порты**.
 - Запомните номер порта для имени порта **WC_defaulthost**.
 - d. В левой области навигации административной консоли выберите **Среда > Виртуальные хосты**.
 - e. Выберите имя **default_host**.
 - f. Под Дополнительными свойствами выберите **Псевдонимы хоста**.
 - g. Если имя хоста и номер порта для элементов кластера не показаны в списке; нажмите **Создать**, чтобы добавить в список отсутствующую запись. Для имени хоста поддерживается Групповой символ * (звездочка).
 - h. После добавления новой записи нажмите **Сохранить** и **Синхронизировать**.

Настройка сервера Proxy WebSphere Application Server для бизнес-пространства:

При использовании сервера Proxy WebSphere Application Server убедитесь, что все модули включены для сервера Proxy и бизнес-пространство работает в вашей среде.

Перед настройкой сервера Proxy WebSphere Application Server на работу с бизнес-пространством выполните следующее:

1. Убедитесь, что используется последняя версия WebSphere Application Server.
2. Создайте сервер Proxy (выберите **Серверы > Типы серверов > Серверы Proxy WebSphere**). Дополнительная информация приведена в разделе Setting up the proxy server справочной системы WebSphere Application Server Information Center.
3. Убедитесь, что выбран протокол HTTP.
1. Убедитесь, что модули преобразуются в сервер Proxy WebSphere Application Server. Для каждого приложения, требуемого бизнес-пространством, убедитесь, что модули включены для сервера Proxy.
 - a. Войдите в административную консоль как администратор.
 - b. Выберите **Приложения > Типы приложений > Приложения J2EE WebSphere**.
 - c. На панели Приложения J2EE выберите имя приложения.

Проверьте следующие приложения. Могут присутствовать некоторые или все приложения из этого в зависимости от того, какие продукты используются с бизнес-пространством.

- **BPMAAdministrationWidgets_имя-узла_имя-сервера** (для WebSphere Enterprise Service Bus и IBM Business Process Manager)
- **BusinessSpaceHelpEAR_имя-узла_имя-сервера** (для всех продуктов)
- **BSpaceEAR_имя-узла_имя-сервера** (для всех продуктов)
- **BSpaceForms_имя-узла_имя-сервера** (для всех продуктов)
- **HumanTaskManagementWidgets_имя-узла_имя-сервера** (для IBM Business Process Manager и IBM Business Monitor)
- **REST Services Gateway** (для всех продуктов)
- **REST Services Gateway Dmgr** (для WebSphere Enterprise Service Bus и IBM Business Process Manager)
- **mm.was_имя-узла_имя-сервера** (для всех продуктов)

- **WBMDashboardWeb_имя-узла_имя-сервера** (для IBM Business Monitor)
 - **webWidgets_имя-узла_имя-сервера** (для WebSphere Enterprise Service Bus)
- d. Для каждого приложения на вкладке **Конфигурация** в разделе **Модули** нажмите **Управлять модулями**.
 - e. На странице Управление модулями вашего приложения щелкните на каждом модуле и выберите **Настройка Proxu веб-модулей**.
 - f. Убедитесь, что опция **Включить Proxu** выбрана.
2. Убедитесь, что псевдоним имени хоста хост-по-умолчанию содержит правильную информацию для каждого элемента кластера, веб-сервера или сервера Proxu.
 - a. Войдите в административную консоль как администратор.
 - b. Выберите **Серверы > Типы серверов > Серверы приложений WebSphere**.
 - c. Для каждого элемента кластера выберите имя сервера приложений и проверьте номер порта для имени порта **хост-по-умолчанию-WS**.
 - В разделе Соединения разверните **Порты**.
 - Посмотрите номер порта **хост-по-умолчанию-WS**.
 - d. В области навигации в левой части административной консоли выберите **Среда > Виртуальные хосты**.
 - e. Выберите **хост-по-умолчанию**.
 - f. В разделе **Дополнительные свойства** выберите **Псевдонимы хостов**.
 - g. Если имя хоста и номер порта для элементов кластера отсутствуют в списке, нажмите кнопку **Создать** для добавления отсутствующей записи в список. В имени хоста можно использовать символ подстановки * (звездочка).
 - h. Для добавления новой записи нажмите кнопку **Сохранить** и затем нажмите **Синхронизировать**.
 3. Для использования протокола HTTP настройте сервер Proxu WebSphere Application Server.
 - a. Войдите в административную консоль как администратор.
 - b. Выберите **Серверы > Типы серверов > Серверы Proxu WebSphere** и затем выберите ранее созданный сервер Proxu.
 - c. Разверните **Параметры сервера Proxu HTTP** и нажмите **Параметры Proxu**.
 - d. Нажмите **Пользовательские свойства** и добавьте новое свойство с именем `cache.query.string` для имени и значение `true`.
 - e. Нажмите кнопку **Сохранить** и перезапустите сервер Proxu.

Преобразование URL Business Space для обратного прокси-сервера:

Если для сервера HTTP установлен обратный прокси, то при настройке сервера HTTP для работы с Business Space необходимо преобразовать URL для Business Space и виджетов, которые используются в коллективе.

1. Измените файл конфигурации сервера HTTP.
2. Преобразуйте все URL для Business Space и виджетов, с которыми работают бизнес-пользователи в решении среды выполнения.

Адреса для общей среды Business Space (все продукты):

- /BusinessSpace/*
- /mum/*
- /help/*
- /BspaceWebformsProxu/*
- /themes/*
- /pageBuilder2/*

Дополнительные адреса для виджетов IBM Business Monitor:

- /BusinessDashboard/*
- /DashboardABX/*
- /monitorServerComponent/*
- /mobile/*
- /rest/*
- /p2pd/*
- /AlphabloxServer/*
- /AlphabloxAdmin/*
- /AlphabloxTooling/*
- /BloxBUILDER/*

Дополнительные адреса для виджетов IBM Business Process Manager:

- /BspaceWidgetsHM/*
- /SecurityManagerWidgets/*
- /BspaceWidgetsBCM/*
- /rest/*
- /PolymorphicWidget/*
- /scaWidget/*
- /ServiceMonitorGraphWidget/*
- /StoreAndForward/*

Дополнительные адреса для виджетов WebSphere Enterprise Service Bus:

- /BspaceWidgetsHM/*
- /rest/*
- /PolymorphicWidget/*
- /scaWidget/*
- /ServiceMonitorGraphWidget/*
- /StoreAndForward/*

Включение API объединения сред развертывания:

API объединения позволяет просматривать процессы и задачи, созданные в Process Designer и Integration Designer, в одном списке задач. Если среда состоит из нескольких кластеров в одной ячейке или нескольких ячеек, домены объединения необходимо настроить вручную соответствующими командами.

Область раздела: Этот раздел предназначен для следующих продуктов:

- IBM Business Process Manager Advanced

Перед тем как приступить к выполнению этой задачи, необходимо выполнить следующие действия:

- Установить продукт.
- Создать профайлы и настроить Business Space в среде развертывания (сервер или кластер).
- Настроить таблицы базы данных (при работе с удаленной базой данных или средой развертывания).

API объединения автоматически настраивается для продукта как часть приложения REST Services Gateway. Если эту конфигурацию необходимо изменить для среды с несколькими средами развертывания, используйте команды wsadmin.

1. Откройте командное окно.

Команду `wsadmin` можно найти в каталоге *каталог-профайла/bin* для среды автономного сервера или в каталоге *каталог-профайла-администратора-развертывания/bin* для среды сетевого развертывания.

2. В командной строке введите команду **wsadmin**, чтобы запустить среду **wsadmin**.
3. Командой **createBPMApiFederationDomain** создайте домен объединения, а операцией **addTarget** добавьте среды развертывания в домен.

имя-домена-объединения в параметре имени должно быть уникальным.

В следующем примере добавляется домен объединения с именем `myCustomFederationDomain`, выполняющий объединение сервера (с именем узла `myNode` и именем сервера `myServer`) и кластера (с именем `myCluster`).

- Пример на языке Python:

```
AdminTask.createBPMApiFederationDomain('[-nodeName имя-узла
-serverName имя-сервера -name myCustomFederationDomain -addTarget [{"
myNode myServer ""} [{" "" "" myCluster}]]')
```

- Пример на языке JACL:

```
$AdminTask createBPMApiFederationDomain {-nodeName имя-узла
-serverName имя-сервера -name myCustomFederationDomain -addTarget {{""
myNode myServer ""} {" "" "" myCluster}}}
```

Для изменения конфигурации API объединения доступны другие команды.

- Если требуется удалить домен объединения вместе с целевыми расположениями в нем, используйте команду **deleteBPMApiFederationDomain**.
- Для просмотра списка всех доменов объединения используйте команду **listBPMApiFederationDomains**.
- Если требуется добавить или удалить целевые расположения домена объединения, используйте команду **modifyBPMApiFederationDomain**.
- Для просмотра сведений о домене объединения используйте команду **showBPMApiFederationDomain**.

Включение виджетов Business Space для сред с несколькими ячейками:

Если Business Space и службы REST работают в разных ячейках или если виджеты и Business Space находятся в разных ячейках, файлы конечных точек необходимо изменить вручную.

Перед выполнением этой задачи необходимо выполнить следующие задачи:

- Установить продукт.
- Создать профайлы и настроить Business Space в среде развертывания (на сервере или в кластере).
- Настроить таблицы базы данных (если используется удаленная база данных или среда развертывания).

Все необходимые для продукта виджеты будут установлены вместе с Business Space, но для работы с виджетами в Business Space необходимо настроить и зарегистрировать конечные точки. Настроить и зарегистрировать конечные точки можно на страницах административной консоли. Но если продукт и службы REST установлены не в одной ячейке с Business Space, необходимо изменить файлы конечных точек служб REST так, чтобы они ссылались на службам REST, а виджеты правильно работали в Business Space.

Измените следующие файлы конечных точек в зависимости от того, какие продукты установлены в системе и какие виджеты используются с Business Space:

- IBM Business Monitor: `monitorEndpoints.xml`
- IBM Business Monitor с IBM Cognos Business Intelligence: `cognosEndpoints.xml`
- WebSphere Enterprise Service Bus: `webWidgetEndpoints.xml` (для виджетов Администрирование стратегии передачи, Браузер служб и Шлюз-прокси), `bpmAdministrationEndpoints.xml` (для виджетов Администрирование)
- IBM Business Process Manager: `wpsEndpoints.xml`, `bpmAdministrationEndpoints.xml` (для виджетов Администрирование), `webWidgetEndpoints.xml` (для виджетов Администрирование стратегии передачи, Браузер служб и Шлюз-прокси), `HumanTaskManagementEndpoints.xml` (для бизнес-процессов и неавтоматизированных задач), `bspacesWFSEndpoints.xml` (для использования Lotus Webform Server с виджетами Управление неавтоматизированными задачами)
- Все продукты: `wsumEndpoint.xml` (для членства пользователей)

Зарегистрировать конечные точки и включить виджеты может администратор, выполнив следующие действия.

1. Скопируйте виджеты из ячейки, где они установлены, в ячейку, где был настроен Business Space во время установки продукта. Виджеты находятся в каталоге `установочный-каталог\BusinessSpace\widgets`; их можно скопировать во временную папку.
2. Выполните команду **`installBusinessSpaceWidgets`**; эта команда устанавливает, развертывает и регистрирует виджеты, расположенные в каталоге `установочный-каталог\BusinessSpace\widgets`.
 - a. Убедитесь, что целевой сервер (в среде с автономным сервером) или администратор развертывания (в среде сетевого развертывания) готов к работе, и откройте командное окно в этом профайле.
Команда `wsadmin` находится в каталоге `profiles\имя-профайла\bin`.
 - b. В командной строке введите команду **`wsadmin`**, чтобы запустить среду **`wsadmin`**.
 - c. Выполните команду **`installBusinessSpaceWidgets`**. В кластерной среде укажите параметр **`-clusterName`**. В среде с автономным сервером укажите параметры **`-serverName`** и **`-nodeName`**. Укажите в параметре **`-widgets`** полный путь к каталогу или файлу с виджетами.
3. Найдите файлы конечных точек в каталоге `каталог-установки\BusinessSpace\registryData\endpoints`. В кластерной среде необходимо использовать сервер приложений, на котором создан профайл администратора развертывания. Все имена файлов оканчиваются на `Endpoints.xml` или `Endpoint.xml`.
4. Для каждого копируемого файла конечных точек создайте резервную копию.
5. В профайле администратора развертывания первой ячейки создайте следующий каталог (если он еще не создан): `каталог-профайла\BusinessSpace\registryData\` (где `каталог-профайла` - это как правило `установочный-каталог\profiles\имя-профайла` или `установочный-каталог\pf\имя-профайла`) и скопируйте в него файл регистрации конечных точек.
6. Настройте конечные точки, изменяя файлы конечных точек. Каждая конечная точка в файле конечных точек обозначена блоком `<tns:Endpoint>`. Найдите блок, который требуется изменить.

Совет: Конечные точки, которые не планируется активировать, рекомендуется удалить из файла.

Расположение, определяемое конечной точкой, указывается в `<tns:url>`. Это значение представляет собой путь в веб-модуле и имеет форму полного или

относительного HTTP URL. По умолчанию задан относительный URL. Поменяйте его на полный URL, например `https://виртуальный-хост.ком:виртуальный-порт/rest/bpm/htm` или `http://host1:9445/WBPublishingDRAFT/`, где протокол, хост и номер порта определяют путь доступа к веб-модулю продукта.

Для того чтобы определить номер порта сервера, выполните следующие действия:

- Войдите в административную консоль.
- Выберите **Серверы > Типы серверов > Серверы приложений WebSphere**.
- Выберите сервер, для которого требуется найти номер порта, и разверните раздел Порты.

Все приложения работают с одним портом, указанным в параметре **wc_defaulthost** (незащищенный хост) или в параметре **wc_defaulthost_secure** (защищенный хост).

Примечание: При доступе к веб-модулям через сервер HTTP в целях распределения нагрузки используйте значения имени хоста и номера порта сервера HTTP.

7. В ячейке, где настроен сервер Business Space, выполните команду **updateBusinessSpaceWidgets** для обновления URL конечных точек после изменения файлов XML конечных точек.
 - a. Откройте командное окно для своего профайла. Команда **wsadmin** находится в каталоге `profiles\имя-профайла\bin`. В кластерной среде выполните команду в каталоге `каталог-профайла-администратора-развертывания\bin`. В среде автономного сервера выполните команду в каталоге `каталог-профайла\bin`.
 - b. В командной строке введите команду **wsadmin**, чтобы запустить среду **wsadmin**.
 - c. Выполните команду **updateBusinessSpaceWidgets**. В кластерной среде укажите параметр **-clusterName**. В среде с автономным сервером укажите параметры **-serverName** и **-nodeName**. Укажите в параметре **-endpoints** полный путь к каталогу с файлами конечных точек виджетов или к отдельному файлу конечных точек.
8. Перезапустите сервер.

Ниже приведен пример файла конечных точек для виджетов IBM Business Monitor.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- START NON-TRANSLATABLE -->
<tns:BusinessSpaceRegistry
  xmlns:tns="http://com.ibm.bspace/BusinessSpaceRegistry"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://com.ibm.bspace/BusinessSpaceRegistry
  BusinessSpaceRegistry.xsd ">

  <tns:Endpoint>
    <tns:id>{com.ibm.wbimonitor}monitorServiceRootId</tns:id>
    <tns:type>{com.ibm.wbimonitor}monitorServiceRootId</tns:type>
    <tns:version>1.0.0.0</tns:version>
    <tns:url>/rest/</tns:url>
    <tns:description>Location of backing services for Monitor widgets</tns:description>
  </tns:Endpoint>

</tns:BusinessSpaceRegistry>
<!-- END NON-TRANSLATABLE -->
```

- После выполнения команды **installBusinessSpaceWidgets** или **updateBusinessSpaceWidgets** необходимо вручную обновить шаблоны и пространства Business Space. См. раздел Обновление шаблонов и пространств Business Space после установки или обновления виджетов.
- Если создано несколько экземпляров конечных точек служб, (например, для распределения нагрузки по двум кластерам), то для того чтобы виджеты показывали данные из каждого кластера, необходимо вручную включить дополнительные виджеты из каждого дополнительного кластера. Необходимо изменить файлы конечных точек виджетов и файлы каталогов виджетов. См. раздел Включение виджетов Business Space для работы с несколькими конечными точками.
- Если в среде включена защита, она должна быть правильно настроена для работы с Business Space.

Настройка виджетов Business Space на работу с несколькими конечными точками:

Если настроен экземпляр Business Space и требуется создать в среде еще один экземпляр конечных точек служб, необходимо настроить Business Space таким образом, чтобы виджеты могли показывать данные из нескольких конечных точек. Требуется изменить два файла: файл конечных точек, регистрирующий конечные точки в Business Space, и файл каталога виджетов, содержащий определения виджетов.

Перед выполнением этой задачи необходимо выполнить следующие задачи:

- Установить продукт.
- Создать сервер или кластер и настроить его для Business Space.
- Настроить таблицы базы данных (если используется удаленная база данных или среда развертывания).
- Настроить дополнительные службы REST для дополнительных виджетов.

В среде развертывания задачи могут быть разбиты на несколько разделов. Например, может быть два кластера, один из которых обрабатывает бухгалтерские данные, а другой - данные страховки. Однако конечная точка службы работает только в одном кластере. Для доступа к обоим разделам задач из Business Space необходимо зарегистрировать два отдельных виджета (по виджету на раздел), чтобы они были доступны в Business Space. Например, в каталоге могли бы быть виджеты Список неавтоматизированных задач бухгалтерского учета и Список задач страхования (оба с одинаковыми фактическими кодами списка задач).

Необходимо вручную изменить файл конечных точек и файл каталога виджетов.

Файлы конечных точек виджетов входят в состав каждого продукта и добавляются во время установки продукта. Требуется изменение одного или нескольких следующих файлов конечных точек в зависимости от установленных продуктов и виджетов, которые используются в Business Space:

- IBM Business Monitor: `monitorEndpoints.xml`
- IBM Business Monitor с IBM Cognos Business Intelligence: `cognosEndpoints.xml`
- WebSphere Enterprise Service Bus: `webWidgetEndpoints.xml` (для виджетов Администрирование стратегии передачи, Браузер служб и Шлюз-прокси), `bpmAdministrationEndpoints.xml` (для виджетов Администрирование)
- IBM Business Process Manager: `wpsEndpoints.xml`, `bpmAdministrationEndpoints.xml` (для виджетов Администрирование), `webWidgetEndpoints.xml` (для виджетов Администрирование стратегии передачи, Браузер служб и Шлюз-прокси), `HumanTaskManagementEndpoints.xml` (для

бизнес-процессов и неавтоматизированных задач), `bospaceWFSEndpoints.xml` (для использования Lotus Webform Server с виджетами Управление неавтоматизированными задачами)

- Все продукты: `wsumEndpoint.xml` (для членства пользователей)

Файлы каталогов виджетов содержат определения виджетов продукта. Требуется изменение одного или нескольких следующих файлов виджетов в зависимости от установленных продуктов и виджетов, которые используются в Business Space:

- IBM Business Monitor: `catalog_WBMonitor.xml`
- WebSphere Enterprise Service Bus: `catalogProxyGateway.xml` и `catalog_ServiceAdmin.xml`
- IBM Business Process Manager: `catalog_BPMAAdministration.xml`, `catalog_BusinessRules.xml`, `catalog_ServiceAdmin.xml` и `catalog_HumanTaskManagement.xml`

Файлы конечных точек и файлы каталогов виджетов находятся в каталоге *каталог-установки\BusinessSpace\registryData*. Файлы конечных точек находятся в подкаталоге `endpoints`, файлы каталогов находятся в подкаталоге `catalogs`.

Каталог *каталог-установки\BusinessSpace\registryData* содержит файлы шаблонов конечных точек и каталогов виджетов. При необходимости можно создать копию одного из этих шаблонов и внести в нее свои изменения.

1. Для создания нескольких экземпляров виджета необходимо установить приложения, предоставляющие виджеты, с уникальными именами приложения и корневым контекстом для каждого экземпляра виджета.
 - a. Для каждого экземпляра виджета разверните приложение виджета в среде развертывания Business Space (сервер или кластер, где выполняется приложение **BSpaceEAR_сервер_узел**). В зависимости от используемых продуктов разверните один или несколько файлов EAR:
 - `BPMAAdministrationWidgets_имя-узла_имя-сервера` (для WebSphere Enterprise Service Bus и IBM Business Process Manager)
 - `HumanTaskManagementWidgets_имя-узла_имя-сервера` (для IBM Business Process Manager и IBM Business Monitor)
 - `WBMDashboardWeb_имя-узла_имя-сервера` (для IBM Business Monitor)
 - `webWidgets_имя-узла_имя-сервера` (для WebSphere Enterprise Service Bus)
 - b. Во время развертывания присвойте уникальные имена приложению и корневым контекстам веб-модулей. Запомните имена используемых корневых контекстов.
2. Измените новые конечные точки служб REST для дополнительных сред развертывания приложения (серверы или кластеры, где развернуто приложение служб REST). Создайте файл конечных точек для добавления конечных точек служб.
 - a. Найдите файлы конечных точек в каталоге *каталог-установки\BusinessSpace\registryData\endpoints*. Скопируйте файл шаблона конечных точек и удалите из него все конечные точки, которые изменять не нужно.
 - b. Добавьте в файл конечных точек дополнительную конечную точку службы с помощью элемента `<tns:Endpoint>` с уникальным ИД (`<tns:id>`) и URL для новой конечной точки (`<tns:url>`), но с той же версией и (необязательно) всеми локалями, как у исходной конечной точки. Тип (`<tns:type>`) должен совпадать с ИД (`<tns:id>`). Можно изменить имя и описание, например Список задач страхования моего коллектива.

- c. При добавлении конечных точек следует обратить внимание на следующую информацию:
- `<tns:id>` - ИД может быть любой строкой, но при этом должен быть уникальным для всех зарегистрированных конечных точек. Добавляя дополнительные конечные точки, проверяйте уникальность их ИД.
 - `<tns:type>` - тип должен совпадать с `<tns:id>`.
 - `<tns:url>` - если URL для конечной точки относительный; предполагается, что конечная точка REST и сервер Business Space находятся на одном хосте. Если URL относительный; он должен совпадать с развернутым корневым контекстом и иметь начальный и конечный разделители пути, например `<tns:url>/BSpaceWidgetsWPS2/</tns:url>`. Если конечная точка находится в удаленной системе, укажите в этом поле абсолютный URL с конечным разделителем пути.
 - `<tns:description>` - описание, более подробно раскрывающее природу набора данных, с которыми работает данная конечная точка. Оно может быть на основе кластера, работающего с набором данных, или описывать природу набора данных, например неавтоматизированные задачи страховых требований или неавтоматизированные задачи бухгалтерских данных.

d. Сохраните изменения.

Пример конечной точки службы из файла `monitorEndpoints.xml`:

```
<tns:Endpoint>
  <tns:id>{com.ibm.wbimonitor}monitorServiceRootId</tns:id>
  <tns:type>{com.ibm.wbimonitor}monitorServiceRootId</tns:type>
  <tns:version>1.0.0.0</tns:version>
  <tns:url>/rest/</tns:url>
  <tns:description>Расположение служб для виджетов Monitor</tns:description>
</tns:Endpoint>
```

3. Добавьте конечную точку для каждого экземпляра виджета в файл конечных точек.
- a. Измените файл конечных точек, созданный на шаге 2. Добавьте дополнительную конечную точку с помощью элемента `<tns:Endpoint>` с уникальным ИД (`<tns:id>`). Тип (`<tns:type>`) должен совпадать с ИД (`<tns:id>`). URL для новой конечной точки (`<tns:url>`) должен совпадать с корневым контекстом, развернутым на шаге 1 и иметь начальный и конечный разделители пути, например `<tns:url>/BSpaceWidgetsWPS2/</tns:url>`. Добавляемая конечная точка виджета должна иметь такую же версию, как у исходной конечной точки, и может содержать все ее локали. Можно изменить имя и описание.
- b. При добавлении конечных точек следует обратить внимание на следующую информацию:
- `<tns:id>` - ИД может быть любой строкой, но при этом должен быть уникальным для всех зарегистрированных конечных точек. Добавляя дополнительные конечные точки, проверяйте уникальность их ИД.
 - `<tns:type>` - тип должен совпадать с `<tns:id>`.
 - `<tns:url>` - URL конечной точки виджета должен совпадать с корневым контекстом и иметь начальный и конечный разделители пути, например `<tns:url>/BSpaceWidgetsWPS2/</tns:url>`.
 - `<tns:description>` - описание, более подробно раскрывающее природу набора данных, с которыми работает данная конечная точка. Оно может быть на основе кластера, работающего с набором данных, или описывать природу набора данных, например неавтоматизированные задачи страховых требований или неавтоматизированные задачи бухгалтерских данных.

с. Сохраните изменения.

Пример конечной точки виджета из файла `monitorEndpoints.xml`:

```
<tns:Endpoint>
<tns:id>{com.ibm.wbimonitor}monitorWidgetRootId2</tns:id>
  <tns:type>{com.ibm.wbimonitor}monitorWidgetRootId2</tns:type>
  <tns:version>1.0.0.0</tns:version>
  <tns:url>/newMonitorWidgetContextRoot/</tns:url>
  <tns:description>Расположение виджетов Monitor</tns:description>
</tns:Endpoint>
```

4. Создайте файл каталога виджетов для новых определений виджетов.

- a. Найдите файл каталога виджетов в каталоге *каталог-установки* \BusinessSpace\registryData\catalogs. Создайте копию файла шаблона каталога. Для имени нового файла рекомендуется использовать следующий формат: `catalog_виджет.xml` (без пробелов в имени файла), где *виджет* - значение ИД элемента `<catalog>` в файле. Удалите все элементы `<category>`, которые не предполагается изменять. В категориях, с которыми ведется работа, удалите все элементы `<entry>`, которые не будут изменяться.
- b. Добавьте элемент `<entry>` с уникальным ИД, например `id="{com.ibm.bspace.widget}ид-виджета`, и уникальным именем, например `unique-name="{com.ibm.bspace.widget}имя-виджета`. Остальные определения можно оставить как есть.
- c. Поменяйте заголовок и описание, чтобы новый виджет был доступен как отдельный виджет в Business Space (они должны отражать сущность новой конечной точки). Например, можно указать Список задач страхования моего коллектива в элементе `<title>` виджета. Заголовок должен помогать бизнес-пользователям в выборе правильного виджета. Описание должно информировать бизнес-пользователей о природе данных и функциональности выбираемого виджета.
- d. Добавьте в новый файл XML каталога виджетов ссылку на новую конечную точку виджета. Для этого укажите в определении `<tns:id>` конечной точки виджета, которая была добавлена на шаге 3.а.

Например, укажите ...

```
<definition>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId2/com/
ibm/wbimonitor/common/iWidgets/instances_iWidget.xml</definition>
```

...

- e. Убедитесь, что `endpoint://` в элементе `<metadata>` файла каталога совпадает с типом и ИД файла конечной точки (элементы `<tns:type>` и `<tns:id>`).
- f. Убедитесь, что `"refVersion"` : в элементе `<metadata>` файла каталога совпадает с версией в файле конечной точки (элемент `<tns:version>`).
- g. Сохраните изменения.

Пример файла каталога виджетов:

```
<entry id="{com.ibm.wbimonitor}instances"
unique-name="{com.ibm.wbimonitor}instances">
  <title>
    <!-- END NON-TRANSLATABLE -->
    <nls-string xml:lang="en">Экземпляры</nls-string>
    <!-- START NON-TRANSLATABLE -->
  </title>
  <description>
    <!-- END NON-TRANSLATABLE -->
    <nls-string xml:lang="en">Экземпляры</nls-string>
    <!-- START NON-TRANSLATABLE -->
  </description>
  <shortDescription>
    <!-- END NON-TRANSLATABLE -->
    <nls-string xml:lang="en">Этот виджет показывает сводную панель с
доступным контекстом монитора в отдельных экземплярах или в
определенных пользователем группах экземпляров контекста.</nls-string>
    <!-- START NON-TRANSLATABLE -->
  </shortDescription>
</definition>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId
```

```

/com/ibm/wbimonitor/common/iWidgets/instances_iWidget.xml</definition>
  <content>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/img/
thumb_instances.gif</content>
  <preview>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/img/
prev_instances.gif</preview>
  <previewThumbnail>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/
img/prev_instances.gif</previewThumbnail>
  <help>endpoint://{com.ibm.bspace}bSpaceWidgetHelpRootId/topic/
com.ibm.bspace.help.widg.mon.doc/topics/help_instance_whatIs.html</help>
  <icon>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/img/
icon_instances.gif</icon>
  <metadata name="com.ibm.mashups.builder.autoWiringEnabled">true
</metadata>
  <metadata name="com.ibm.bspace.version">7.0.0</metadata>
  <metadata name="com.ibm.bspace.owner">International Business
Machines Corp.</metadata>
  <metadata name="com.ibm.bspace.serviceEndpointRefs">
[{"name":"serviceUrlRoot", "required":"true",
"refId":"endpoint://{com.ibm.wbimonitor}monitorServiceRootId",
"refVersion":"1.0.0.0"}]</metadata>
</entry>

```

5. Поместите новый файл конечной точки и новый файл каталога в сжатый файл и выполните команду **updateBusinessSpaceWidgets**, указав в параметре **-widgets** расположение сжатого файла.
 - После выполнения команды **updateBusinessSpaceWidgets** необходимо вручную обновить шаблоны и пространства Business Space. См. раздел Обновление шаблонов и пространств Business Space после установки или обновления виджетов.
 - Если Business Space и службы REST работают в разных ячейках, файлы конечных точек необходимо обновить вручную.
 - Если в среде включена защита, она должна быть правильно настроена для работы с Business Space.

Настройка виджетов для нескольких продуктов:

Настроить или добавить виджеты Business Space для одного продукта в Business Space, где уже настроен другой продукт, можно с помощью команды **installBusinessSpaceWidgets**.

Перед тем как приступить к выполнению этой задачи, необходимо выполнить следующие действия:

- Выполнить все действия по установке и настройке продукта и настроить Business Space.
- Выполнить все действия по установке и настройке дополнительного продукта.

Можно установить более одного продукта, работающего с Business Space, и настроить виджеты для обоих продуктов после установки второго продукта. Однако, если второй продукт установлен после настройки Business Space на работу с виджетами первого продукта, необходимо с помощью команды **installBusinessSpaceWidgets** добавить и настроить виджеты второго продукта для работы в той же среде Business Space.

В автономном дополнении виджеты устанавливаются автоматически. Например, виджеты устанавливаются при создании автономного профайла IBM WebSphere Process Server, настройке сервера для Business Space, установке IBM Business Monitor и добавлении уже настроенного сервера в IBM Business Monitor.

1. Запустите профайл администратора развертывания и откройте в нем окно команд.
Команда **wsadmin** находится в каталоге `profiles/имя-профайла/bin`.
2. В командной строке введите команду **wsadmin**, чтобы запустить среду **wsadmin**.

3. Командой **installBusinessSpaceWidgets** установите, разверните и зарегистрируйте виджеты из каталога *корневой-каталог-установки/BusinessSpace/widgets*.

В следующем примере используется язык Jython для выполнения команды **installBusinessSpaceWidgets**, которая устанавливает виджеты для IBM Business Monitor для работы в среде Business Space, предварительно настроенной для IBM Business Process Manager.

```
AdminTask.installBusinessSpaceWidgets('[-nodeName  
имя-узла  
-serverName имя-сервера -widgets  
корневой-каталог-установки\BusinessSpace\widgets\WBM\widgets_WBMonitor.zip]')
```

Пример на языке JACL:

```
$AdminTask  
installBusinessSpaceWidgets {-nodeName имя-узла  
-serverName имя-сервера -widgets  
корневой-каталог-установки\BusinessSpace\widgets\WBM\widgets_WBMonitor.zip}
```

Для того чтобы включить Business Space для данной среды выполнения после настройки виджетов, необходимо выполнить следующие действия.

- После выполнения команды **installBusinessSpaceWidgets** или **updateBusinessSpaceWidgets**, вручную обновите пространства и шаблоны Business Space. См. раздел Обновление шаблонов и пространств Business Space после установки или обновления виджетов.
- Настройте службы REST. См. раздел Настройка служб REST.
- Зарегистрируйте конечные точки REST. См. раздел "Настройка Business Space и регистрация конечных точек REST с помощью административной консоли".
- Проверьте правильность настройки защиты для работы с Business Space и используемыми в коллективе виджетами. См. раздел Настройка защиты для Business Space.

Настройка конкретных виджетов для работы в бизнес-пространстве

Некоторые виджеты, поставляемые с продуктом, требуют дополнительной настройки для использования в бизнес-пространстве.

Продукт управления бизнес-процессами включает несколько виджетов, некоторые из которых требуют дополнительной настройки для связи с вашим решением из бизнес-пространства.

Настройка монитора служб:

Если создается новый сервер и требуется использовать виджет Монитор служб в бизнес-пространстве для определения времени ответов и производительности выполнения запросов для служб, используемых или вызываемых модулем SCA, настройте и включите монитор служб в административной консоли.

Требуемая роль защиты для этой задачи: Если административная защита включена, то для выполнения этой задачи необходима регистрация в роли администратора.

Монитор служб имеет архитектуру клиент/сервер.

- Агент монитора служб: Определяет производительность и время ответов для операций и отправляет данные измерений серверу монитора служб

- Сервер монитора служб: Собирает и объединяет измерения времени ответов и производительности от всех работающих агентов монитора служб и затем вычисляет и сохраняет статистические данные.

В среде развертывания сервер работает в кластере поддержки, а агент – в кластере приложений на сервере, на котором развернут ваш модуль. В среде с автономным сервером сервер и агент работают на автономном сервере.

Важное замечание: Если для доступа к бизнес-пространству используется внешний сервер, необходимо настроить сервер HTTP на закодированные косые черты. Дополнительная информация содержится в документации по серверу HTTP.

1. Войдите в административную консоль с правами доступа администратора.
2. Настройте сервер монитора служб.
 - a. В консоли выберите **Серверы > Типы серверов > Серверы приложений WebSphere > имя-сервера > Монитор служб**.
 - b. На странице Монитор служб нажмите **Включить монитор служб**.
 - c. Просмотрите значения по умолчанию для размера буфера монитора служб и предела размера очереди и при необходимости измените их.
 - d. Укажите целевые объекты для монитора служб. Это агенты монитора служб, из которых требуется собирать данные.

Таблица 6. Отслеживание

Целевые объекты для отслеживания	Выполняемые этапы
Отслеживание всех работающих агентов монитора служб	Необходимо выбрать опцию Все включенные агенты монитора служб .
Отслеживание конкретного поднабора работающих агентов монитора служб	<ol style="list-style-type: none"> 1. Выключите опцию Все включенные агенты монитора служб. Появится таблица набора данных; если это новая конфигурация, то таблица будет пустой. 2. Нажать Добавить. Откроется страница Обзор целевых объектов развертывания. 3. В таблице набора данных на странице Обзор целевых объектов развертывания выберите целевой объект развертывания, агент которого нужно отслеживать. 4. Нажмите кнопку ОК для возврата на страницу Сервер монитора служб. 5. Повторяйте этапы с 2 по 4, пока все агенты, которые нужно отслеживать, не будут добавлены.

- e. На странице Сервер монитора служб нажмите кнопку **ОК**. Конфигурация будет сохранена и начнет действовать немедленно.
3. Настройте агент монитора служб.
 - a. В консоли выберите **Серверы > Типы серверов > Серверы приложений WebSphere > имя-сервера > Агент монитора служб**.
 - b. На странице Агент монитора служб нажмите **Включить агент монитора служб**.
 - c. Просмотрите значения по умолчанию для конфигурации агента и при необходимости измените их.
 - d. Нажмите кнопку **ОК**.

Настройка защиты для Business Space

При использовании Business Space, созданное с использованием WebSphere со своей средой необходимо рассмотреть опции защиты в отношении того, как ваша группа будет работать с артефактами в Business Space. Если требуется включить защиту для бизнес-пространства, то настройте защиту приложений и назначьте хранилище пользователей. Для того чтобы определить администраторов Business Space, назначьте роль администратора.

Для того чтобы получить наилучшие результаты, включите защиту до настройки Business Space. Для включения защиты позднее используйте страницу Администрирование глобальной защиты административной консоли, чтобы включить как административную защиту, так и защиту приложений. На той же странице административной консоли также можно назначить хранилище учетных записей пользователей, включая изменение опции объединенных хранилищ по умолчанию на другое хранилище пользователей. Для назначения пользователей, которые могут выполнять действия администратора бизнес-пространства в среде бизнес-пространства, назначьте роль администратора бизнес-пространства. Для вашей конкретной среды может потребоваться другая конфигурация защиты.

Важное замечание: По умолчанию конфигурация Ajax Proxy, используемая для виджетов бизнес-пространства, не ограничивает доступ к любому IP-адресу. Для удобства Ajax Proxy по умолчанию настраивается открытой и не является защитой для рабочих сценариев. Для настройки Ajax Proxy таким образом, чтобы показывалось содержимое только выбранных сайтов или блокировалось содержимое выбранных сайтов, выполните действия в разделе Блокирование IP-адресов с помощью Ajax Proxy бизнес-пространства.

Включение защиты для Business Space:

Если планируется использовать защищенную среду, включите защиту перед настройкой Business Space. Но при необходимости защиту можно вручную включить позднее. Для того чтобы включить защиту для Business Space, необходимо включить как защиту приложений, так и административную защиту.

Перед выполнением этой задачи необходимо выполнить следующие задачи:

- Регистрация ИД пользователя в реестре пользователей для продукта.

Business Space предварительно настроен на идентификацию и предоставление прав доступа. При доступе пользователя к тем или иным URL Business Space ему предлагается пройти идентификацию. Неидентифицированные пользователи перенаправляются на страницу входа в систему. Business Space доступен по протоколам HTTP или HTTPS. При использовании веб-сервера, например IBM HTTP Server, в его параметрах необходимо настроить поддержку HTTPS.

Если есть опасения, что без защиты SSL пароли могут быть перехвачены; подумайте о запрете доступа по протоколу HTTP через WebSphere Application Server. Дополнительная информация о защите приведена в разделе Настройка, включение и миграция защиты в WebSphere Application Server Information Center.

Для включения защищенного доступа к Business Space необходимо настроить реестр пользователей и включить защиту приложений. Предоставление доступа к пространствам и информационному наполнению страниц Business Space управляется внутренне в Business Space как часть управления пространствами.

1. Инструкции по защите приведены в документации по продукту.

2. Для приложения Business Space на странице административной консоли Глобальная защита выберите **Включить административную защиту** и **Включить защиту приложений**.

3. Если требуется включить или выключить защиту после настройки Business Space с профайлом, необходимо изменить значение свойства noSecurityAdminInternalUserOnly в файле ConfigServices.properties.

Свойство noSecurityAdminInternalUserOnly задает ИД администратора Business Space, когда защита выключена. По умолчанию, если защита выключена, в конфигурации Business Space это свойство равно **BPMAAdministrator**. Когда защита включена, это свойство по умолчанию равно ИД администратора сервера приложений. Если требуется включить или выключить защиту после настройки Business Space, используйте ИД администратора сервера приложений.

a. Присвойте свойству noSecurityAdminInternalUserOnly в файле ConfigServices.properties ИД администратора сервера приложений. Файл ConfigServices.properties находится в *каталог-профайла\BusinessSpace\имя-узла\имя-сервера\mm.runtime.prof\config\ConfigService.properties* для автономного сервера или *каталог-профайла-администратора-развертывания\BusinessSpace\имя-кластера\mm.runtime.prof\config\ConfigService.properties* для кластера.

b. Выполните команду **updatePropertyConfig** с помощью клиента сценариев wsadmin.

- Для автономного сервера:

Пример на языке Jython:

```
AdminTask.updatePropertyConfig(['-serverName имя-сервера -nodeName имя-узла  
-propertyName "каталог-профайла\BusinessSpace\имя-узла\имя-сервера  
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"'])  
AdminConfig.save()
```

Пример на языке Jacl:

```
$AdminTask updatePropertyConfig {-serverName имя-сервера -nodeName имя-узла  
-propertyName "каталог-профайла\BusinessSpace\имя-узла\имя-сервера  
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}  
$AdminConfig save
```

- Для кластера:

Пример на языке Jython:

```
AdminTask.updatePropertyConfig(['-clusterName имя-кластера -propertyName  
"корневой-каталог-диспетчера-развертывания\BusinessSpace\имя-кластера\mm.runtime.prof\  
config\ConfigService.properties" -prefix "Mashups_"'])  
AdminConfig.save()
```

Пример на языке Jacl:

```
$AdminTask updatePropertyConfig {-clusterName имя-кластера -propertyName  
"корневой-каталог-диспетчера-развертывания\BusinessSpace\имя-кластера\mm.runtime.prof\  
config\ConfigService.properties" -prefix "Mashups_"}  
$AdminConfig save
```

c. Перезапустите сервер.

d. Войдите в Business Space и назначьте новый ИД администратора владельцем пространств по умолчанию.

- После включения административной защиты и защиты приложений при входе в Business Space будет показываться приглашение для ввода ИД пользователя и пароля. Для входа необходимо ввести правильные ИД и пароль пользователя из выбранного реестра пользователей. После включения административной защиты при входе в административную консоль необходимо использовать ИД пользователя с административными правами доступа.

- Если у профайла продукта требуется поменять хранилище учетных записей пользователей по умолчанию, следуйте инструкциям раздела Выбор хранилища учетных записей.
- Если среда состоит из нескольких ячеек, Business Space и продукт находятся на разных узлах и эти узлы в разных ячейках; настройте сертификаты для единого входа в систему (SSO) и SSL. Следуйте инструкциям раздела “Настройка SSO и SSL для Business Space” на стр. 228.
- Инструкции по выбору пользователей, которые имеют право выполнять действия администратора Business Space в среде Business Space, приведены в разделе “Назначение роли администратора Business Space” на стр. 237.

Выбор хранилища пользователей для Business Space:

Опция объединенных хранилищ является опцией хранилища учетных записей пользователей по умолчанию для профайлов. При необходимости для своей среды можно изменить тип хранилища учетных записей пользователей.

Перед выполнением этой задачи необходимо выполнить следующие задачи:

- Включите защиту приложений и административную защиту. Обратитесь к разделу “Включение защиты для Business Space” на стр. 223.
- Убедитесь, что ваш ИД пользователя зарегистрирован в реестре пользователей вашего продукта.

Для включения идентифицируемого доступа к Business Space необходимы настроенный реестр пользователей и включенная защита приложений. Информация о защите приложений приведена в разделе “Включение защиты для Business Space” на стр. 223.

Замечания по использованию реестра учетных записей пользователей с Business Space:

- В зависимости от используемого типа конфигурации LDAP ваши параметры могут влиять на возможность успешного доступа к Business Space. Убедитесь в правильности настройки фильтров пользователей, фильтров групп и параметров преобразования. Дополнительная информация приведена в разделе Настройка фильтров поиска упрощенного протокола доступа к каталогам документации по WebSphere Application Server.
- В зависимости от используемого типа конфигурации объединенных хранилищ ваши параметры могут влиять на возможность успешного доступа к Business Space. Убедитесь, что области настроены правильно. Дополнительная информация приведена в разделе Управление областью в конфигурации объединенных хранилищ документации по WebSphere Application Server.
- Защита LDAP по умолчанию настроена на использование свойства идентификации `uid` (ИД пользователя) для выполнения поиска в Business Space. Если защита LDAP изменяется на использование другого уникального поля LDAP, например `mail` (адрес электронной почты) в качестве свойства идентификации, то необходимо изменить свойство `userIdKey` в файле `ConfigServices.properties`, чтобы поиск выполнялся в Business Space. Выполните этап 3 далее.
- Если используется база данных Microsoft SQL и автономный реестр LDAP, убедитесь, что отличительное имя пользователя (DN) не превышает 450 символов. Если какая-либо из записей DN пользователя превышает 450 символов, необходимо выбрать опцию **Объединенные хранилища** для хранилища учетных записей пользователей.
- Использование опции **Объединенные хранилища** предоставляет дополнительные возможности в виджетах и среде, такие как дополнительные возможности поиска.

При поиске пользователей для совместного использования областей и страниц область поиска включает адрес электронной почты, полное имя пользователя и ИД пользователя.

1. На странице административной консоли Глобальная защита под разделом **Хранилище учетных записей пользователей** выберите **Объединенные хранилища**, **Локальная операционная система**, **Автономный реестр LDAP** или **Автономный реестр пользователей**.
2. Перезапустите сервер.
3. Если требуется изменить хранилище пользователей по умолчанию из опции **Объединенные хранилища** по умолчанию, измените свойство MashupAdminFor00BSpace в файле ConfigServices.properties с назначением правильного ИД пользователя (свойства UID для хранилища пользователей) в качестве достоверного ИД администратора.

- a. Скопируйте измененный файл в пустую папку в вашей системе. Файл ConfigServices.properties находится в *корневой-каталог-профайлов\BusinessSpace\имя-узла\имя-сервера\mm.runtime.prof\config\ConfigService.properties* для автономного сервера или в *корневой-каталог-профайлов-администратора-развертывания\BusinessSpace\имя-кластера\mm.runtime.prof\config\ConfigService.properties* для кластера.
- b. Выполните команду **updatePropertyConfig** с помощью клиента сценариев wsadmin.

- Для автономного сервера:

В следующем примере используется Jython:

```
AdminTask.updatePropertyConfig('[-serverName имя-сервера -nodeName имя-узла  
-propertyFileName "корневой-каталог-профайлов\BusinessSpace\имя-узла\имя-сервера  
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')
```

В следующем примере используется Jacl:

```
$AdminTask updatePropertyConfig {-serverName имя-сервера -nodeName имя-узла  
-propertyFileName "корневой-каталог-профайлов\BusinessSpace\имя-узла\имя-сервера  
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}  
$AdminConfig save
```

- Для кластера:

В следующем примере используется Jython:

```
AdminTask.updatePropertyConfig('[-clusterName имя-кластера -propertyFileName  
"корневой-каталог-профайлов-администратора-развертывания\BusinessSpace\имя-кластера\mm.run  
config\ConfigService.properties" -prefix "Mashups_"]')
```

В следующем примере используется Jacl:

```
$AdminTask updatePropertyConfig {-clusterName имя-кластера -propertyFileName  
"корневой-каталог-профайлов-администратора-развертывания\BusinessSpace\имя-кластера\mm.run  
config\ConfigService.properties" -prefix "Mashups_"}  
$AdminConfig save
```

- c. Войдите в бизнес-пространство и переназначьте владельцев областей по умолчанию на новый ИД администратора.
4. При использовании хранилища LDAP с уникальным полем LDAP, например mail (адрес электронной почты) для свойства идентификации вместо uid (ИД пользователя) измените свойство userIdKey в файле ConfigServices.properties, чтобы поиск выполнялся в Business Space.
 - a. Файл ConfigServices.properties находится в *корневой-каталог-профайлов\BusinessSpace\имя-узла\имя-сервера\mm.runtime.prof\config\ConfigService.properties* для автономного сервера или в *корневой-каталог-профайлов-администратора-развертывания*

BusinessSpace*имя-кластера*\mm.runtime.prof\config\
ConfigService.properties для кластера.

- b. Измените атрибут `userIdKey` из `uid` соответственно свойству идентификации, например, `mail`.
- c. Скопируйте измененный файл в пустую папку в вашей системе.
- d. Выполните команду **updatePropertyConfig** с помощью клиента сценариев `wsadmin`.

- Для автономного сервера:

В следующем примере используется Jython:

```
AdminTask.updatePropertyConfig(['-serverName имя-сервера -nodeName имя-узла  
-propertyName "корневой-каталог-профайлов\BusinessSpace\имя-узла\имя-сервера  
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"'])  
AdminConfig.save()
```

В следующем примере используется Jacl:

```
$AdminTask updatePropertyConfig {-serverName имя-сервера -nodeName имя-узла  
-propertyName "корневой-каталог-профайлов\BusinessSpace\имя-узла\имя-сервера  
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}  
$AdminConfig save
```

- Для кластера:

В следующем примере используется Jython:

```
AdminTask.updatePropertyConfig(['-clusterName имя-кластера -propertyName  
"корневой-каталог-профайлов-администратора-развертывания\BusinessSpace\имя-кластера\mm.r  
config\ConfigService.properties" -prefix "Mashups_"'])  
AdminConfig.save()
```

В следующем примере используется Jacl:

```
$AdminTask updatePropertyConfig {-clusterName имя-кластера -propertyName  
"корневой-каталог-профайлов-администратора-развертывания\BusinessSpace\имя-кластера\mm.r  
config\ConfigService.properties" -prefix "Mashups_"}  
$AdminConfig save
```

5. Если требуется ограничить вход в Business Space некоторым поднабором пользователей или групп, то можно изменить преобразование роли защиты Business Space Java EE.
 - a. Обновите преобразование пользователя/группы для двух приложений J2EE: **BSpaceEAR_узел_сервер** и **mm.was_узел_сервер** (для среды с автономным сервером) или **BSpaceEAR_кластер** и **mm.was_кластер** (для среды сетевого развертывания).
 - b. Выберите **Приложения > Типы приложений > Приложения J2EE WebSphere** и выберите два приложения.
 - c. На правой панели в разделе Подробные свойства выберите **Преобразование роли защиты в пользователя/группу**.
 - d. Повторите преобразование ролей **businessspaceusers** и **Allauthenticated** из двух приложений с удалением специального субъекта.
 - e. Нажмите **Преобразовать специальные субъекты** и выберите **Нет**.
 - f. Нажмите **Преобразовать пользователей** или **Преобразовать группы** и назначьте роль выбранным пользователям или группам.

Изменение преобразования ролей защиты Java EE не влияет на функцию поиска пользователя/группы в бизнес-пространстве.

6. Перезапустите сервер.
7. Войдите в бизнес-пространство и переназначьте владельцев областей по умолчанию на новый ИД администратора.
 - Для задания идентификации страницам и областям в Business Space можно управлять идентификацией при создании страниц и областей Business Space.

- Информация о том, кто может выполнять действия администратора бизнес-пространства в среде бизнес пространства, приведена в разделе “Назначение роли администратора Business Space” на стр. 237.

Примечание:

Причиной следующих ошибок в файле SystemOut.log могут быть лишние атрибуты в вашем реестре пользователей, которые не могут обрабатываться:

```
00000046 SystemErr R вызвана: com.ibm.websphere.wim.exception.WIMSystemException: CWWIM1013E
Значение секретаря свойства недопустимо для сущностного объекта EJB uid=xxx,c=us,ou=yuy,о=ibm.com.
00000046 SystemErr R at com.ibm.ws.wim.adapter.lldap.LdapAdapter.setPropertyValue
(LdapAdapter.java:3338)
```

Для обхода этих атрибутов задайте следующие атрибуты в файле ConfigServices.properties:

```
com.ibm.mashups.user.userProfile = LIMITED
com.ibm.mashups.user.groupProfile = LIMITED
```

Файл ConfigServices.properties находится в *корневой-каталог-профайлов\BusinessSpace\имя-узла\имя-сервера\mm.runtime.prof\config\ConfigService.properties* для автономного сервера или в *корневой-каталог-профайлов-администратора-развертывания\BusinessSpace\имя-кластера\mm.runtime.prof\config\ConfigService.properties* для кластера. После изменения файла ConfigServices.properties выполните команду **updatePropertyConfig** с помощью клиента сценариев wsadmin, следуя инструкциям в пункте 4.d. выше.

Примечание:

Если защита Java EE в кластере включена, рассмотрите возможность ужесточения записи в стратегии сервера для расположения справки бизнес-пространства.

Стратегия расположения справки бизнес-пространства следующая:

```
grant codeBase      "file:${was.install.root}/profiles/имя-профайла/temp/
имя-узла/-" {

    permission java.security.AllPermission;

};
```

Ужесточите стратегию заменой на:

```
grant codeBase      "file:${was.install.root}/profiles/имя-профайла/temp/
имя-узла/имя-сервера/BusinessSpaceHelpEAR_имя-узла_имя-сервера/
BusinessSpaceHelp.war/-" {

    permission java.security.AllPermission;

};
```

Настройка SSO и SSL для Business Space:

Для удаленных сред, в которых бизнес-пространство и ваш сервер продуктов находятся в разных ячейках, настройте конфигурации однократного входа в систему (SSO) и Secure Sockets Layer (SSL) вручную.

Перед выполнением этой задачи необходимо выполнить следующие задачи:

- Включите защиту приложений и административную защиту. Обратитесь к разделу “Включение защиты для Business Space” на стр. 223.
 - Убедитесь, что ваш ИД пользователя зарегистрирован в реестре пользователей вашего продукта.
1. Если Business Space удален от расположения, в котором выполняется ваш продукт, и если узел, в котором выполняется Business Space, и узел, в котором выполняется ваш продукт, не находятся в одной ячейке, то необходимо выполнить действия по обеспечению включения SSO вручную. Например, если используется более одного продукта, серверы находятся в разных узлах и требуется, чтобы все они могли работать с сервером Business Space, то необходимо вручную настроить SSO. Для включения SSO выполните следующие действия:
 - a. На административной консоли для каждого сервера откройте страницу Глобальная защита, выбрав **Защита > Глобальная защита**. Разверните **Веб- и SIP-защита** и щелкните на **однократный вход в систему (SSO)**, чтобы переключатель **Включен** включился.
 - b. Убедитесь, что все узлы используют одинаковую информацию **Хранилище учетных записей пользователей** (см. этап 3).
 - c. Выполните действия в разделе Импорт и экспорт ключей справочной системы WebSphere Application Server Information Center.
 2. Если в файле конечных точек используется HTTPS, расположением конечных точек является другой узел, а не Business Space, и сертификат SSL является собственным сертификатом SSL, то его необходимо импортировать.
Подписанты должны быть настроены в соответствующих хранилищах доверенных сертификатов для сервера бизнес-пространства и сервера продуктов. Обратитесь к разделу Защита соединений с помощью Secure Sockets Layer (SSL) справочной системы WebSphere Application Server Information Center.
Дополнительная информация о SSO и SSL содержится в справочной системе WebSphere Application Server Information Center.

Настройка защиты для системных служб REST:

Для настройки защиты данных в виджетах на основе пользователей и групп необходимо изменить пользователей, которые преобразуются в приложение шлюза служб REST.

Перед выполнением этой задачи необходимо выполнить следующие задачи:

- Включите защиту приложений и административную защиту. Обратитесь к разделу “Включение защиты для Business Space” на стр. 223.
- Убедитесь, что ваш ИД пользователя зарегистрирован в реестре пользователей вашего продукта.

Преобразование пользователей в приложение поставщика служб REST влияет на все службы поставщика.

Для просмотра зависимых служб выберите **Службы > Службы REST > Поставщики служб REST** и выберите соответствующее приложение поставщика в списке поставщиков.

1. На административной консоли выберите одну из следующих опций:
 - Для серверной среды выберите **Приложения > Типы приложений > Приложения J2EE WebSphere > REST Services Gateway**
 - Кроме того, для среды сетевого развертывания выберите **Приложения > Типы приложений > Приложения J2EE WebSphere > REST Services Gateway Dmgr**

2. На правой панели в разделе Подробные свойства выберите **Преобразование роли защиты в пользователя/группу**.
3. Для управления доступом к данным во всех виджетах служб REST добавьте пользователей и группы к роли **RestServicesUser**.

Рекомендации по организации защиты виджетов Business Space:

В зависимости от виджетов, используемых в Business Space вместе с продуктом управления бизнес-процессами, можно присвоить роли административных групп для управления доступом к данным в виджете или создать дополнительный уровень доступа к виджету на основе ролей.

Административные групповые роли и виджеты

Для управления доступом к данным в виджетах служат административные групповые роли и назначенные им пользователи. Для того чтобы выяснить, кто назначен этим ролям, откройте административную консоль, выберите **Пользователи и группы > Административные групповые роли** и выберите группу. Появится список Роли.

Двумя примерами виджетов, которые могут потребовать изменений в административных групповых ролях, служат Бизнес-правила и Бизнес-переменные.

Для виджета Состояние системы следующие административные роли обладают правами на отслеживание, разрешают доступ к административной консоли и разрешают пользователям, которым они присвоены, обращаться к данным в виджете Состояние системы:

- **Отслеживать**
- **Настройщик**
- **Оператор**
- **Администратор**
- **Администратор защиты**
- **Ответственный за развертывание**
- **iscadmins**

Пользователям, которым присвоены эти административные групповые роли, доступны данные в виджете Работоспособность системы. Пользователям, которым не присвоены эти роли, недоступны данные в виджете Работоспособность системы.

Ролевой доступ в виджетах

Настройка Tivoli Access Manager WebSEAL для работы с бизнес-пространством:

Если используется Tivoli Access Manager WebSEAL и требуется использовать его с бизнес-пространством, то необходимо выполнить некоторые дополнительные этапы настройки.

Перед выполнением этой задачи необходимо выполнить следующие задачи:

- Включите защиту приложений и административную защиту. Обратитесь к разделу “Включение защиты для Business Space” на стр. 223.
- Убедитесь, что ваш ИД пользователя зарегистрирован в реестре пользователей вашего продукта.

Для использования Tivoli Access Manager WebSEAL с бизнес-пространством необходимо настроить защиту Tivoli Access Manager на включение внешнего

поставщика Java Authorization Contract for Containers (JACC), настроить WebSEAL на работу с Tivoli Access Manager, настроить WebSEAL на работу с вашим сервером приложений продукта и настроить пересечения хоста для вашей среды.

1. Настройте Tivoli Access Manager на включение внешнего поставщика JACC.

- a. Выполните одно из следующих действий для выбора использования административной консоли или команд wsadmin.
 - Для того чтобы использовать административную консоль для настройки Tivoli Access Manager на включение JACC, выполните следующее:
 - 1) Включите глобальную защиту.
 - a) Выберите **Защита > Глобальная защита**.
 - b) Выберите **Административная защита, Защита приложений и Защита Java 2** с сервером LDAP, на котором настраивается Tivoli Access Manager.
 - c) Выберите **Глобальная защита > LDAP**, введите следующую информацию и нажмите **ОК**.

Имя	Описание
ИД пользователя сервера	Введите тот же ИД пользователя, который был введен в качестве отличительного имени администратора (DN) в параметрах Tivoli Access Manager. Пример: user1
Пароль пользователя сервера	puser1
Хост	LDAP настроен с Tivoli Access Manager
Порт	Пример: 389
Базовое отличительное имя (DN)	Пример: o=ibm, c=us
DN связывания	Пример: cn=SecurityMaster, secAuthority=Default
Пароль связывания	пароль для пользователя SecurityMaster

- d) Сохраните конфигурацию и перезапустите сервер.
- 2) Включите внешнюю идентификацию с Tivoli Access Manager и JACC.
 - a) Выберите **Защита > Глобальная защита > Службы внешней идентификации**.
 - b) В списке **Служба идентификации** выберите **Внешняя служба JACC** и нажмите кнопку **Настроить**. Свойства по умолчанию для Tivoli Access Manager являются правильными. Не изменяйте значения по умолчанию.
 - c) В разделе **Дополнительные свойства** выберите **Свойства Tivoli Access Manager**. Выберите **Включить встроенный Tivoli Access Manager**, введите следующую информацию и нажмите кнопку **ОК**.

Имя	Значение
Набор портов прослушивания клиента	По умолчанию применяются 8900 - 8999. Его следует изменить только в том случае, если требуется использовать другие порты.
Сервер стратегий (имя:порт)	Укажите свой <i>сервер-стратегий:порт</i> . Пример: windomain3.rtp.raleigh.ibm.com:7135
Серверы идентификации и приоритет (имя:порт:приоритет)	Укажите свой <i>сервер-идентификации:порт:приоритет</i> . Пример: windomain3.rtp.raleigh.ibm.com:7136:1

Имя	Значение
Имя пользователя администратора	Оставьте имя пользователя по умолчанию sec_master , если другое имя администратора на сервере Tivoli Access Manager использоваться не будет.
Пароль пользователя-администратора	domino123
Суффикс отличительного имени в реестре пользователей	Введите имя для вашего сервера приложений. Пример: o=ibm,c=us
Домен защиты	Оставьте для домена защиты значение по умолчанию . Измените этот параметр, если домен по умолчанию на сервере Tivoli Access Manager использоваться не будет. Измените этот параметр, если на сервере Tivoli Access Manager созданы несколько доменов и нужно соединиться и использовать другой домен, кроме домена по умолчанию .
Отличительное имя пользователя администратора	Введите полное имя пользователя. Пример: cn=user1,o=ibm,c=us Примечание: Этот пользователь соответствует ИД пользователя сервера , настроенному на панели реестра пользователей LDAP.

Сервер соединяется с сервером Tivoli Access Manager и создает несколько файлов свойств на сервере приложений. Этот процесс может занять несколько минут. В случае возникновения ошибки, проверьте расположение system Out и исправьте ошибку.

- Для того чтобы использовать утилиту wsadmin для настройки Tivoli Access Manager на включение JACC, выполните следующее. Выполните следующую процедуру на сервере администратора развертывания один раз. Параметры конфигурации направляются на управляемые серверы, включая агенты узлов, при выполнении синхронизации. Для того чтобы изменения конфигурации вступили в силу необходимо перезапустить сами управляемые серверы.

- 1) Убедитесь, что запущены все управляемые серверы, включая агенты узлов.
- 2) Запустите сервер.
- 3) Запустите утилиту командной строки, выполнив команду **wsadmin** из каталога *корневой-каталог-установки/bin*.
- 4) По запросу wsadmin выполните команду **configureTAM**, включив соответствующую информацию из следующей таблицы:

Пример Jacl:

```
$AdminTask configureTAM -interactive
```

Пример Jython:

```
AdminTask.configureTAM('-interactive')
```

Затем введите следующую информацию:

Имя	Значение
имя узла для вашего сервера продукта	Укажите один узел или введите звездочку (*), чтобы выбрать все узлы.

Имя	Значение
Сервер стратегий Tivoli Access Manager	Введите имя сервера стратегий Tivoli Access Manager и порт соединения. Используйте следующий формат: <i>сервер-стратегий:порт</i> . Порт связи с сервером стратегий задается во время настройки Tivoli Access Manager. Порт по умолчанию - 7135.
Сервер идентификации Tivoli Access Manager	Введите имя сервера идентификации Tivoli Access Manager. Используйте следующий формат: <i>сервер-идентификации:порт.приоритет</i> . Порт связи с сервером идентификации задается во время настройки Tivoli Access Manager. Порт по умолчанию - 7136. Можно задать несколько серверов идентификации через запятую. Преимущества настройки нескольких серверов идентификации могут пригодиться в случае передачи управления и для повышения производительности. Значение приоритета определяет порядок использования сервера идентификации. Пример: <code>auth_server1:7136:1,auth_server2:7137:2</code> . Значение 1 для приоритета необходимо указать даже в случае настройки одного сервера идентификации.
отличительное имя администратора для вашего сервера продукта	Введите полное отличительное имя ИД администратора защиты для вашего сервера продукта. Пример: <code>cn=wasadmin,o=organization,c=country</code> . Дополнительная информация приведена по ссылке на связанный раздел.
Суффикс отличительного имени реестра пользователей Tivoli Access Manager	Например: <code>o=organization,c=country</code>
Имя пользователя-администратора Tivoli Access Manager	Введите ИД пользователя администратора Tivoli Access Manager, созданный во время настройки Tivoli Access Manager. В качестве этого ИД обычно используется <code>sec_master</code> .
Пароль пользователя-администратора Tivoli Access Manager	Введите пароль администратора Tivoli Access Manager.
Домен защиты Tivoli Access Manager	Введите имя домена защиты Tivoli Access Manager, используемого для хранения пользователей и групп. Если домен защиты не был установлен во время настройки Tivoli Access Manager, нажмите кнопку Возврат , чтобы принять значение по умолчанию.
Набор портов приема встроенного Tivoli Access Manager	Сервер продукта прослушивает порт TCP/IP на обновления базы данных идентификации из сервера стратегий. Поскольку в определенном узле и системе может быть запущено несколько процессов, для данного процесса необходим список портов. Укажите через запятую порты, используемые в качестве портов приема клиентами Tivoli Access Manager. Если требуется указать диапазон портов, укажите через двоеточие нижнее и верхнее значения. Например: <code>7999,9990:9999</code> .

Имя	Значение
Отложить	Если задать этой опции значение да, то конфигурация сервера управления будет отложена до следующего перезапуска. Если задать значение нет, то конфигурация сервера управления вступит в силу немедленно. Управляемые серверы будут настроены при своем очередном перезапуске.

- 5) После ввода всей необходимой информации выберите **F**, чтобы сохранить свойства конфигурации, или **C**, чтобы отменить процесс настройки и аннулировать введенную информацию.

Пример с сервером SVTM TAM60:

```
wsadmin>$AdminTask configureTAM -interactive
Настроить встроенный Tivoli Access Manager
```

Эта команда настраивает встроенный Tivoli Access Manager на указанном узле или узлах WebSphere Application Server.

```
Имя узла WebSphere Application Server (nodeName): *
*Сервер стратегий Tivoli Access Manager (policySvr): windomain3.rtp.raleigh.ibm.com:7135
*Сервер идентификации Tivoli Access Manager (authSvrs): windomain3.rtp.raleigh.ibm.com:7135
*Отличительное имя администратора WebSphere Application Server (wasAdminDN): cn=was61admin
*Суффикс отличительного имени реестра пользователей Tivoli Access Manager (dnSuffix): o=ibm.com
Имя пользователя администратора Tivoli Access Manager (adminUid): [sec.master]
*Пароль пользователя администратора Tivoli Access Manager (adminPasswd): domino123
Домен защиты Tivoli Access Manager (secDomain): [По умолчанию]
Набор портов приема встроенного Tivoli Access Manager (portSet): [9900:9999]
Defer (отложенный): [нет]
```

Настроить встроенный Tivoli Access Manager

F (Закончить)

C (Отмена)

Выберите [F, C]: [F] F

```
WASX7278I: Созданная командная строка: $AdminTask configureTAM {-policySvr windomain3.rtp.raleigh.ibm.com:7135}
Параметры действий настройки встроенного Tivoli Access Manager успешно сохранены.
Перезапустите экземпляры WebSphere Application Server, выполняемые на целевом узле или узлах.
wsadmin>
```

- 6) На административной консоли выберите **Защита > Глобальная защита > Внешние поставщики идентификации**. Затем выберите **Внешняя идентификация с помощью службы JACC** и нажмите **ОК**.
- 7) Перейдите к основному экрану защиты и нажмите **ОК**. Сохраните и синхронизируйте изменения.
- 8) Перезапустите все процессы в ячейке.
- b. Если приложения устанавливались перед включением Tivoli Access Manager (например, была включена защита LDAP, установлены некоторые защищенные приложения, и пользователи и группы преобразованы в роли защиты), то передайте информацию о преобразовании ролей защиты из файлов описаний на сервер стратегий Tivoli Access Manager. Выполните одно из следующих действий для выбора использования административной консоли или команд `wsadmin`.
- Об использовании команды `wsadmin propagatePolicyToJACCProvider` см. раздел Передача стратегии защиты установленных приложений поставщику JACC с помощью сценариев `wsadmin`.
 - Об использовании административной консоли см. раздел Передача стратегий и ролей защиты для ранее развернутых приложений.
2. Настройте WebSEAL на работу с Tivoli Access Manager.

- a. Убедитесь, что WebSEAL установлен и настроен правильно.
- b. Для создания защищенной учетной записи пользователя в Tivoli Access Manager, которую можно использовать для настройки TAI, введите следующие команды:

```
pdadmin -a sec_master -p domino123
pdadmin sec_master> user create -gsouser -no-password-policy taiuser
"cn=taiuser,ou=websphere,o=ibm,c=us" taiuser taiuser ptaiuser
pdadmin sec_master> user modify taiuser password-valid yes
pdadmin sec_master> user modify taiuser account-valid yes
```

- c. Создайте пересечение между WebSEAL и вашим сервером приложений продукта с помощью опции **-c iv_creds** для TAI++ и **-c iv_user** для TAI. Введите любую из следующих команд в виде одной строки с использованием переменных, подходящих для данной среды:

```
Для TAI++
server task webseald-server create -t tcp -b supply -c iv_creds
-h имя-хоста -p номер-порта-сервера-приложений-websphere
/имя-пересечения
```

Совет: *имя-пересечения* должно начинаться с /.

- d. В файле конфигурации WebSEAL *каталог-установки-webseald/etc/webseald-default.conf* задайте следующий параметр:

```
basicauth-dummy-passwd=ид-пароль-пользователя-webseald
```

Например, для задания taiuser/ptaiuser в Tivoli Access Manager задайте следующий параметр: `basicauth-dummy-passwd = ptaiuser`

При использовании идентификации на основе форм задайте следующие параметры:

```
forms-auth=both
ba-auth=none
```

- 3. Настройте WebSEAL на работу с вашим сервером приложений продукта, включив перехватчик TAI++ на сервере.
 - a. В административной консоли выберите **Глобальная защита > Механизмы идентификации и истечение срока действия**.
 - b. Разверните пункт **Защита Веб и SIP** и выберите **Группа доверия**. Поставьте отметку в переключателе и нажмите кнопку **Применить**.
 - c. Выберите **Перехватчики > TAMTrustAssociationInterceptorPlus > пользовательские свойства** и добавьте следующие свойства:

Имя	Значение
com.ibm.websphere.security.webseald.configURL	\${WAS_INSTALL_ROOT}/java/jre/PdPerm.properties
com.ibm.websphere.security.webseald.id	iv-creds
com.ibm.websphere.security.webseald.loginId	taiuser (если пользователь taiuser/ptaiuser был создан в Tivoli Access Manager)

- d. Перезапустите ячейку .
- e. Для доступа к клиенту перейдите на `https://имя-сервера-webseald:порт-webseald/имя пересечения/web-uri-для-клиента`.
- 4. Настройте пересечение хоста для вашей среды так, чтобы появились виджеты бизнес-пространства. Выполните одно из следующих действий для выбора использования виртуальных пересечений хоста или прозрачных пересечений хоста.

- При использовании виртуальных пересечений хоста создайте виртуальное пересечение хоста. Виртуальное пересечение хоста исключает необходимость в отдельных пересечениях.
 - a. Убедитесь, что виртуальный хост настроен. Виртуальные пересечения хоста сопоставляют хост и номер порта и направляют адреса на целевой хост. Фильтрации URL не происходит, и все соответствующие запросы направляются на целевой хост.
 - b. Убедитесь, что все следующие приложения доступны на том же виртуальном хосте. Могут присутствовать некоторые или все приложения в зависимости от того, какие продукты используются с бизнес-пространством.
 - BPMAdministrationWidgets_имя-узла_имя-сервера (для WebSphere Enterprise Service Bus и IBM Business Process Manager)
 - BusinessSpaceHelpEAR_имя-узла_имя-сервера (для всех продуктов)
 - BSpaceEAR_имя-узла_имя-сервера (для всех продуктов)
 - BSpaceForms_имя-узла_имя-сервера (для всех продуктов)
 - HumanTaskManagementWidgets_имя-узла_имя-сервера (для IBM Business Process Manager и IBM Business Monitor)
 - PageBuilder2_имя-узла_имя-сервера (для всех продуктов)
 - REST Services Gateway (для всех продуктов)
 - REST Services Gateway Dmgr (для WebSphere Enterprise Service Bus и IBM Business Process Manager)
 - mm.was_имя-узла_имя-сервера (для всех продуктов)
 - WBMDashboardWeb_имя-узла_имя-сервера (для IBM Business Monitor)
 - webWidgets_имя-узла_имя-сервера (для WebSphere Enterprise Service Bus)

Примечание: Этот список охватывает только те приложения, которые требуются бизнес-пространству. В этот список можно добавить другие приложения для сценариев, не связанных с бизнес-пространством, с помощью Tivoli Access Manager WebSEAL.

- c. Выполните следующую команду с помощью pdadmin: `server task сервер-webseal virtualhost create -t протокол -h целевой-хост [-p порт] [-v имя-виртуального-хоста] метка-виртуального-хоста`

Воспользуйтесь следующей информацией:

- *сервер-webseal* – имя сервера WebSEAL, на котором создается запись виртуального хоста.
- *протокол* – тип транспортного протокола. Допустимы записи: `tcp`, `ssl`, `tcpproxу` и `sslproxу`.
- *целевой-хост* – хост требуемого приложения.
- *имя-виртуального-хоста* используется для направления запросов HTTP на виртуальное пересечение хоста. Если значение не введено, то выбираются целевой хост и порт по умолчанию. Например, если для *имя-виртуального-хоста* задано `myvirthost.ibm.com:80`, то WebSEAL находит URL, содержащие `myvirthost.ibm.com:80`, и направляет их на хост, предусмотренный в команде pdadmin.
- *метка-виртуального-хоста* – метка, используемая для идентификации записи в WebSEAL. Она должна быть уникальной.

Для правильной работы бизнес-пространства записи `ssl` и `tcp` должны быть созданы для данного типа транспортного протокола. Когда требуется поддержка как Secure Sockets Layer (SSL), так и Transmission Control Protocol (TCP) в одном виртуальном пересечении хоста, необходимо использовать

опцию `-g` *метка-виртуального-хоста*, где *метка-виртуального-хоста* является оригинальной меткой виртуального хоста для совместного использования конфигурации. Эта опция находит ранее созданное виртуальное пересечение хоста (которое было создано ранее, где *метка-виртуального-хоста* совпадает с меткой, предусмотренной в опции `-g`) и будет использовать эту конфигурацию. Второй записи еще требуется ее собственная *метка-виртуального-хоста*, но она может совместно использовать целевой хост, порт и другие значения. Если опция `-g` не будет предусмотрена, то второй виртуальный хост не будет создан, поскольку WebSEAL будет видеть целевой хост и порт как идентичные ранее созданному пересечению (что недопустимо).

- При использовании прозрачных пересечений хоста создайте ряд прозрачных пересечений путей для виджетов для каждого продукта.
 - a. Выполните следующую команду с помощью `pdadmin`: `server task сервер-webseal create -t прозрачный тип (ssl) или (tcp) -x -h hostname путь`
Например, введите: `server task webseald-default create -t tcp -x -h monServer.ibm.com /BusinessSpace`.
 - b. Создайте следующие корневые контексты для вашего продукта:
Преобразование URL бизнес-пространства для обратного сервера Proxy.
- 5. Выполните дополнительные этапы настройки для устранения неполадок с cookie браузера и виртуальными хостами.
 - a. Для устранения переименования cookie бизнес-пространства добавьте следующее содержимое в файл конфигурации WebSEAL:
[сохранять-имена-cookie]
name = com.ibm.bspace.UserName
name = com.ibm.wbimonitor.UserName
 - b. Необязательно: При использовании виртуальных хостов не по умолчанию с корневым контекстом могут возникнуть неполадки со страницами бизнес-пространства. Может потребоваться защита пересечения от перезаписи JavaScript на страницах бизнес-пространства добавлением пересечения `-j` к корневному контексту. Запустите следующую команду: `server task default-webseald create -f -h имя-хоста -p номер-порта -t tcp -b supply -c iv-user,iv-creds,iv-groups -x -s -j -J trailer/корневой контекст`

Назначение роли администратора Business Space:

В Business Space можно назначить пользователей-администраторов (или администраторов Business Space). Администратор может просматривать, редактировать и удалять все области и страницы, может управлять и создавать шаблоны и может изменять владельца области путем изменения ИД владельца.

Перед выполнением этой задачи необходимо выполнить следующие задачи:

- Включите защиту приложений и административную защиту. Обратитесь к разделу “Включение защиты для Business Space” на стр. 223.
- Убедитесь, что ваш ИД пользователя зарегистрирован в реестре пользователей вашего продукта.

Назначьте роль администратора Business Space с помощью следующей роли защиты сервера приложений: **Admin**. Этот метод предоставляет гибкость в назначении роли любому числу существующих пользователей и групп организации. Он не требует

создания группы администраторов в реестре пользователей с единственной целью действия в качестве фокусной точки для администратора Business Space.

Если администратор Business Space уже назначен из более ранней версии, чем версия 7.5, то администратор можно изменить на группу пользователей. Обратитесь к разделу Назначение группы пользователей как администратора бизнес-пространства.

- При настройке администраторов Business Space с ролью администратора впервые выполните следующее.

1. Войдите в административную консоль продукта.
2. Выберите **Приложения > Типы приложений > Приложения J2EE WebSphere** и выберите одно из следующих приложений:
 - **mm.was_узел_сервер** (для среды с автономным сервером)
 - **mm.was_кластер** (для среды сетевого развертывания)
3. Нажмите **Преобразования роли защиты в пользователя/группу**.
4. Выберите строку для роли **Admin** и нажмите кнопку **Преобразовать пользователей** или **Преобразовать группы** для преобразования пользователей или групп в роль Admin.
5. Нажмите кнопку **Сохранить**.
6. Перезапустите сервер.

- Если администраторы уже назначены на основе групп пользователей и нужно переключиться этот более простой способ управления администраторами с помощью роли, выполните следующее.

1. Откройте файл конфигурации.
 - Для автономного сервера: *корневой-каталог-профайлов\BusinessSpace\имя-узла\имя-сервера\mm.runtime.prof\config\ConfigService.properties*
 - Для кластера: *корневой-каталог-профайлов-администратора-развертывания\BusinessSpace\имя-кластера\mm.runtime.prof\config\ConfigService.properties*
2. Измените следующие значения свойств в файле конфигурации.

```
com.ibm.mashups.adminGroupName = {com.ibm.mashups.J2EERole.Admin}
com.ibm.mashups.widget.attributes.configure.groups=
```
3. Выполните команду **updatePropertyConfig** в среде wsadmin профайла.

- Для автономного сервера:

В следующем примере используется Jython:

```
AdminTask.updatePropertyConfig('[-serverName имя-сервера -nodeName имя-узла
-propertyFileName "корневой-каталог-профайлов\BusinessSpace\имя-узла\имя-сервера
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')
```

```
AdminConfig.save()
```

В следующем примере используется Jacl:

```
$AdminTask updatePropertyConfig {-serverName имя-сервера -nodeName имя-узла
-propertyFileName "корневой-каталог-профайлов\BusinessSpace\имя-узла\имя-сервера
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

- Для кластера:

В следующем примере используется Jython:

```
AdminTask.updatePropertyConfig('[-clusterName имя-кластера -propertyFileName
"корневой-каталог-профайлов-администратора-развертывания\BusinessSpace\имя-кластера\mm.runt
config\ConfigService.properties" -prefix "Mashups_"]')
```

```
AdminConfig.save()
```

В следующем примере используется Jacl:


```
$AdminTask updatePropertyConfig {-clusterName имя-кластера -propertyFileName  
"корневой-каталог-профайлов-администратора-развертывания\BusinessSpace\имя-кластера\m.  
config\ConfigService.properties" -prefix "Mashups_"}  
$AdminConfig save
```

4. Перезапустите сервер.
5. Приведенный выше этап используется для назначения пользователей ролям администратор Business Space.

Назначение администратора Business Space группе пользователей:

Пользователей Business Space можно назначить администраторами (или администраторами Business Space) на основе групп пользователей. Это удобно, если вы работали в более ранней версии, чем 7.5, и роль администратора уже назначена группе пользователей.

Перед выполнением этой задачи необходимо выполнить следующие задачи:

- Включите защиту приложений и административную защиту. Обратитесь к разделу “Включение защиты для Business Space” на стр. 223.
- Убедитесь, что ваш ИД пользователя зарегистрирован в реестре пользователей вашего продукта.

Совет: Если группы пользователей ранее назначались администратором Business Space, то можно переключиться на этот более простой способ назначения администраторов Business Space с помощью роли. Обратитесь к разделу “Назначение роли администратора Business Space” на стр. 237.

Администратор может просматривать, редактировать и удалять все области и страницы, может управлять и создавать шаблоны и может изменять владельца области путем изменения ИД владельца.

Если административная защита была включена при настройке Business Space, просмотрите следующую информацию о группах и администраторах:

- Пользователям, относящимся к специальной группе пользователей (**администраторы**), роль администратора назначается по умолчанию. Таким образом, назначение роли администратора определяется участием в группе пользователей.
- В среде с одним сервером сервер Business Space создает группу пользователей **администраторы** в реестре пользователей по умолчанию. ИД администратора, представляемый во время настройки, автоматически добавляется в эту группу как участник.
- В среде сетевого развертывания группа пользователей **администраторы** не создается автоматически. Для создания группы пользователей и добавления участников в эту группу в реестре пользователей по умолчанию используйте сценарий createSuperUser.py.
- Если используется другой реестр пользователей (например, LDAP) вместо реестра пользователей по умолчанию или если реестр пользователей по умолчанию используется, но вы не хотите использовать группу пользователей **администраторы**, то необходимо определить группу пользователей для использования в качестве администраторов бизнес-пространства. Предоставляемое значение должно быть допустимо для реестра пользователей. Например, для LDAP можно предоставить имя, аналогичные cn=administrators, dc=company, dc=com. Дополнительная информация об определении этой группы пользователей приведена в инструкциях по изменению группы администраторов в следующем разделе “Пошаговые инструкции”.

- Для Business Space в WebSphere Portal группа **wpsadmins** по умолчанию также используется для роли администратора. Участникам этой группы предоставляется роль администратора бизнес-пространства.

Примечание: Для использования Business Space в WebSphere Portal должна быть включена защита.

Если административная защита не была включена при настройке Business Space, то только специальный ИД пользователя **BPMAadministrator** обладает ролью администратора Business Space.

В среде сетевого развертывания необходимо выполнить сценарий `createSuperUser.py` для назначения роли администратора, то есть для создания группы пользователей и добавления участников. Перед запуском сценария выполните следующее:

- Убедитесь, что имя группы **администраторы** по умолчанию не изменилось.
 - Используйте хранилище по умолчанию для реестра пользователей.
 - Запустите сервер или администратор развертывания для вашей среды Business Space с профайлом с установленным Business Space.
1. Найдите сценарий *корневой-каталог-установки*\BusinessSpace\scripts\createSuperUser.py для назначения роли администратора пользователю.
 2. Откройте командную строку и измените каталоги на следующий каталог: *корневой-каталог-профайлов*\bin, где *корневой-каталог-профайлов* представляет каталог для профайла, в котором установлен Business Space.
 3. Введите следующую команду: `wsadmin -lang jython -f корневой-каталог-установки\BusinessSpace\scripts\createSuperUser.py краткое-имя-пользователя пароль` где *краткое-имя-пользователя* – уникальный идентификатор пользователя в Virtual Member Manager (VMM) и *пароль* – пароль VMM этого пользователя. Если этот пользователь существует в VMM, то добавляется в группу администраторов.

Примечание: Если путь содержит пробел, например если *каталог-установки* имеет имя Мой каталог установки, то имена путей необходимо заключить в кавычки. Например, введите следующую команду: `wsadmin -lang jython -f "\My install dir\BusinessSpace\scripts\createSuperUser.py" краткое-имя-пользователя-в-VMM`.

Для открытия Business Space используйте следующий URL: `http://хост:порт/BusinessSpace`, где *хост* – имя хоста с работающим сервером и *порт* – номер порта вашего сервера.

Имя специальной группы пользователей по умолчанию **администраторы** можно изменить. Для проверки существующего имени группы или изменения его выполните следующее.

Проверьте значение показателя `com.ibm.mashups.adminGroupName` в файле конфигурации:

- *корневой-каталог-профайлов*\BusinessSpace\имя-узла\имя-сервера\mm.runtime.prof\config\ConfigService.properties на автономном сервере или
- *корневой-каталог-профайлов-администратора-развертывания*\BusinessSpace\имя-кластера\mm.runtime.prof\config\ConfigService.properties в кластере.

Для изменения группы администраторов на автономном сервере выполните следующее:

1. Измените показатель `com.ibm.mashups.adminGroupName` в файле конфигурации *корневой-каталог-профайлов\BusinessSpace\имя-узла\имя-сервера\mm.runtime.prof\config\ConfigService.properties*.
2. Выполните команду `updatePropertyConfig` в среде `wsadmin` профайла: `$AdminTask updatePropertyConfig {-serverName имя-сервера -nodeName имя-узла -propertyName "корневой-каталог-профайлов\BusinessSpace\имя-узла\имя-сервера\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}` и выполните команду `$AdminConfig save`.
3. Перезапустите сервер.

Для изменения группы администраторов в кластере выполните следующее:

1. Измените показатель `com.ibm.mashups.adminGroupName` в файле конфигурации *корневой-каталог-профайлов-администратора-развертывания\BusinessSpace\имя-кластера\mm.runtime.prof\config\ConfigService.properties*.
2. Выполните команду `updatePropertyConfig` в среде `wsadmin` профайла среды развертывания: `$AdminTask updatePropertyConfig {-clusterName имя-кластера -propertyName "корневой-каталог-профайлов-администратора-развертывания\BusinessSpace\имя-кластера\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}` и выполните команду `$AdminConfig save`.
3. Перезапустите администратор развертывания.

Для изменения группы администраторов на автономном сервере, когда защита не включена, выполните следующее:

1. Измените показатель `noSecurityAdminInternalUserOnly` в файле конфигурации *корневой-каталог-профайлов\BusinessSpace\имя-узла\имя-сервера\mm.runtime.prof\config\ConfigService.properties*.
2. Выполните команду `updatePropertyConfig` в среде `wsadmin` профайла: `$AdminTask updatePropertyConfig {-serverName имя-сервера -nodeName имя-узла -propertyName "корневой-каталог-профайлов\BusinessSpace\имя-узла\имя-сервера\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}` и выполните команду `$AdminConfig save`.
3. Перезапустите сервер.

Для изменения группы администраторов в кластере, когда защита не включена, выполните следующее:

1. Измените показатель `noSecurityAdminInternalUserOnly` в файле конфигурации *корневой-каталог-профайлов-администратора-развертывания\BusinessSpace\имя-кластера\mm.runtime.prof\config\ConfigService.properties*.
2. Выполните команду `updatePropertyConfig` в среде `wsadmin` профайла среды развертывания: `$AdminTask updatePropertyConfig {-clusterName имя-кластера -propertyName "корневой-каталог-профайлов-администратора-развертывания\BusinessSpace\имя-кластера\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}` и выполните команду `$AdminConfig save`.
3. Перезапустите администратор развертывания.

Запрет на создание бизнес-пространств для пользователей:

В ходе настройки Business Space можно запретить создание бизнес-пространств обычным пользователям.

По умолчанию все пользователи могут создавать бизнес-пространства. При необходимости доступ к Business Space можно ограничить таким образом, чтобы создавать и импортировать бизнес-пространства могли только пользователи с правами администратора. Администраторы Business Space могут создавать бизнес-пространства и передавать их принадлежность другим пользователям. Владельцы пространств обладают такими же правами на администрирование как и создатели пространств. Например, они могут управлять правами пользователей на просмотр и изменение пространства и его свойств, а также добавлять страницы.

Примечание: В Business Space для Business Space нельзя запретить пользователям создавать бизнес-пространства.

Для того чтобы запретить обычным пользователям создавать бизнес-пространства, выполните следующие действия.

1. В файле конфигурации укажите для параметра `com.ibm.mashups.lockeddown` значение `true`:
 - Для автономного сервера: *каталог-профайла*\BusinessSpace\имя-узла\имя-сервера\mm.runtime.prof\config\ConfigService.properties
 - Для кластера: *каталог-профайла-администратора-развертывания*\BusinessSpace\имя-кластера\mm.runtime.prof\config\ConfigService.properties

Значение по умолчанию `false` разрешает создавать бизнес-пространства всем пользователям. Если указано значение `true`, то создавать бизнес-пространства могут только администраторы.

2. Выполните команду **updatePropertyConfig** в среде `wsadmin` профайла:

- Для автономного сервера:

В следующем примере используется Jython:

```
AdminTask.updatePropertyConfig(['-serverName имя-сервера
-nodeName имя-узла
-propertyFileName "каталог-профайла\BusinessSpace\имя-узла\имя-сервера
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')
AdminConfig.save()
```

В следующем примере используется Jacl:

```
$AdminTask updatePropertyConfig {-serverName имя-сервера -nodeName имя-узла
-propertyFileName "каталог-профайла\BusinessSpace\имя-узла\имя-сервера
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

- Для кластера:

В следующем примере используется Jython:

```
AdminTask.updatePropertyConfig(['-clusterName имя-кластера -propertyFileName
"каталог-профайла-администратора-развертывания\BusinessSpace\имя-кластера\mm.runtime.prof\
config\ConfigService.properties" -prefix "Mashups_"]')
AdminConfig.save()
```

В следующем примере используется Jacl:

```
$AdminTask updatePropertyConfig {-clusterName имя-кластера -propertyFileName
"каталог-профайла-администратора-развертывания\BusinessSpace\имя-кластера\mm.runtime.prof\
config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

В следующих сеансах работы с Business Space пользователи не смогут создавать бизнес-пространства без прав администратора.

Разрешение поисков для реестров пользователей без символов подстановки:

Если реестр пользователей настроен на неиспользование символов подстановки, необходимо выполнить дополнительные настройки, чтобы поиски в бизнес-пространстве работали правильно, и для виджетов, которые выполняют поиски в реестре пользователей.

Перед выполнением этой задачи необходимо выполнить следующие задачи:

- Включите защиту приложений и административную защиту. Обратитесь к разделу “Включение защиты для Business Space” на стр. 223.
- Убедитесь, что ваш ИД пользователя зарегистрирован в реестре пользователей вашего продукта.

По умолчанию, когда пользователь бизнес-пространства выполняет поиск пользователей или групп вводом одного или нескольких символов, бизнес-пространство автоматически добавляет символы подстановки. Например, если реестр пользователей находится на сервере LDAP и пользователь вводит `smit`, бизнес-пространство превращает этот ввод в запрос `*smit*`, чтобы результаты включали имена, подобные `Smith`, `Smithers` и `Psmith`. Однако, если автоматическое добавление символов подстановки не нужно, например, если реестр пользователей не допускает их, то можно выключить эту опцию.

Для выключения автоматического добавления символов подстановки в поисках в вашей среде выполните следующее:

- Для автономного сервера выполните следующее:

1. Обновите файл конфигурации *корневой-каталог-профайлов\BusinessSpace\имя-узла\имя-сервера\mm.runtime.prof\config\ConfigService.properties* `com.ibm.mashups.user.stripWildcards=true`.

2. Выполните команду **updatePropertyConfig** в среде `wsadmin` профайла:

В следующем примере используется Jython:

```
AdminTask.updatePropertyConfig(['-serverName имя-сервера -nodeName  
имя-узла -propertyFileName "корневой-каталог-профайлов\BusinessSpace\  
имя-узла\имя-сервера\mm.runtime.prof\config\ConfigService.properties"  
-prefix "Mashups_"'])  
AdminConfig.save()
```

В следующем примере используется Jacl:

```
$AdminTask updatePropertyConfig {-serverName имя-сервера -nodeName  
имя-узла -propertyFileName "корневой-каталог-профайлов\BusinessSpace\  
имя-узла\имя-сервера\mm.runtime.prof\config\ConfigService.properties"  
-prefix "Mashups_"}  
$AdminConfig save
```

3. Перезапустите сервер.

- Для кластера выполните следующее:

1. Обновите файл конфигурации *корневой-каталог-профайлов-администратора-развертывания\BusinessSpace\имя-кластера\mm.runtime.prof\config\ConfigService.properties* `com.ibm.mashups.user.stripWildcards=true`.

2. Из администратора развертывания выполните команду **updatePropertyConfig** в среде `wsadmin` профайла:

В следующем примере используется Jython:

```
AdminTask.updatePropertyConfig(['-clusterName имя-кластера  
-propertyFileName "корневой-каталог-профайлов-администратора-  
развертывания\BusinessSpace\имя-кластера\mm.runtime.prof\config\  
ConfigService.properties" -prefix "Mashups_"'])
```

```
AdminConfig.save()
```

В следующем примере используется Jacl:

```
$AdminTask updatePropertyConfig {-clusterName имя-кластера  
-propertyName "корневой-каталог-профайлов-администратора-  
развертывания\BusinessSpace\имя-кластера\mm.runtime.prof\config\  
ConfigService.properties" -prefix "Mashups_"}  
$AdminConfig save
```

3. Перезапустите администратор развертывания.

Настройка прокси Business Space Ajax

Может потребоваться изменение некоторых параметров прокси Business Space Ajax, таких как тайм-аут или блокирование IP-адресов для защищенных рабочих сред.

Файл прокси Ajax `proxy-config.xml` находится в следующих расположениях:

- При использовании среды Business Space, поставляемой в месте с продуктом управления бизнес-процессами, *корневой-каталог-профайла/BusinessSpace/имя-узла/имя-сервера/mm.runtime.prof/config/proxy-config.xml*.

Описание неполадок прокси Ajax можно найти в технических комментариях IBM Mashups по адресу <http://www-01.ibm.com/support/search.wss?tc=SSWP9P>.

Важное замечание: По умолчанию в конфигурации прокси Ajax для виджетов Business Space разрешен доступ ко всем IP-адресам. Для удобства прокси Ajax по умолчанию настроен как открытый; это небезопасно для рабочих сценариев. Для того чтобы настроить прокси Ajax на показ только информации с выбранных сайтов или на блокировку информации с выбранных сайтов, следуйте инструкциям в разделе Блокировка IP-адресов с помощью прокси Ajax Business Space.

1. Измените файл `proxy-config.xml` по необходимости.

Например, для изменения параметров тайм-аута для прокси Ajax Business Space необходимо изменить значение `proxy:value` для `socket-timeout`.

2. Выполните команду **updateBlobConfig** с помощью клиента сценариев `wsadmin`, указав параметры **-serverName** и **-nodeName** для автономного сервера или параметр **-clusterName** для кластера, указав в параметре **-propertyName** путь к файлу `proxy-config.xml`, а в параметре **-prefix** значение `Mashups_`.

Пример на языке Jython: `AdminTask.updateBlobConfig(['-serverName имя-сервера -nodeName имя-узла -propertyName "profile_root/
BusinessSpace/node_name/server_name/mm.runtime.prof/config/proxy-
config.xml" -prefix "Mashups_"'])`

Пример на языке Jacl: `$AdminTask updateBlobConfig {-serverName имя-сервера
-nodeName имя-узла -propertyName "profile_root/BusinessSpace/
node_name/server_name/mm.runtime.prof/config/proxy-config.xml" -prefix
"Mashups_"}`

Изменение параметров тайм-аута для прокси Ajax Business Space:

Business Space использует прокси-компонент для подключения к службам REST. Если службы REST не отвечают, измените параметры тайм-аута подключения Business Space к службам REST в зависимости от производительности серверов службы REST.

Если возникает тайм-аут соединений со службами REST, измените следующие параметры.

Если используется среда Business Space, поставляемая вместе с продуктом управления бизнес-процессами; значение socket-timeout по умолчанию равно 30 с. Измените его на более подходящее значение.

Если используется Business Space с WebSphere Portal, значение socket-timeout по умолчанию равно 10 с. Поменяйте его на более подходящее значение (30 с, если используются виджеты администрирования IBM Business Process Manager).

1. Откройте файл proxy-config.xml. Информация о расположении файла прокси Ajax приведена в разделе “Настройка прокси Business Space Ajax” на стр. 244.
2. Измените proxy:value для socket-timeout. Время указывается в миллисекундах.

```
<proxy:meta-data>
  <proxy:name>socket-timeout</proxy:name>
  <proxy:value>30000</proxy:value>
</proxy:meta-data>
```
3. Настройте прокси Ajax для своей среды. См. раздел “Настройка прокси Business Space Ajax” на стр. 244.

Блокирование IP-адресов с помощью прокси Ajax Business Space:

Прокси Ajax перенаправляет запросы от виджетов на сервер продукта и целевой сервер, если эти серверы находятся не на одном узле сети с сервером Business Space. По умолчанию в конфигурации прокси Ajax разрешен доступ ко всем IP-адресам; это небезопасно для рабочих сред. Настройте прокси Ajax таким образом, чтобы он показывал только информацию с выбранных сайтов или блокировал информацию с выбранных сайтов.

Важное замечание: По умолчанию в конфигурации прокси Ajax для виджетов Business Space разрешен доступ ко всем IP-адресам. Для удобства прокси Ajax по умолчанию настроен как открытый; это небезопасно для рабочих сценариев. Для того чтобы настроить прокси Ajax на показ только информации с выбранных сайтов или на блокировку информации с выбранных сайтов, выполните следующие действия.

Если необходимо ограничить доступ к определенным IP-адресам, можно настроить параметры прокси Ajax для фильтрации IP-адресов, что позволяет разрешать или запрещать доступ. Правила для черного и белого списков определяются в файле proxy-config.xml.

1. Откройте файл proxy-config.xml. Информация о расположении файла прокси Ajax приведена в разделе “Настройка прокси Business Space Ajax” на стр. 244.
2. Добавьте правила фильтрации для разрешения или запрещения доступа.
Для того чтобы определить правило черного списка для определенного IP-адреса или набора адресов, используйте элемент proxy:deny. Для того чтобы определить правило белого списка для определенного IP-адреса или набора адресов, используйте элемент proxy:allow. Правила фильтрации применяются по порядку, последнее применимое правило фильтрации имеет приоритет перед предыдущими.

```
<proxy-rules
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:proxy="http://www.ibm.com/xmlns/prod/sw/ajax/proxy-config/1.1">
  <proxy:mapping contextpath="/proxy/*" />

  <proxy:policy url="*" acf="none">
  <proxy:actions>
  <proxy:method>GET</proxy:method>
  </proxy:actions>
  </proxy:policy>
```



```
<proxy:ipfilter>
<proxy:deny>9.6.0.0/255.255.0.0</proxy:deny>
<proxy:allow>9.6.1.0/255.255.255.0</proxy:allow>
<proxy:deny>9.6.1.4</proxy:deny>
</proxy:ipfilter>
</proxy-rules>
```

В этом примере фильтр IP-адресов выполняет следующие фильтры:

- blocks all 9.6.*.* IP addresses
- allows 9.6.1.* but blocks the specific IP address 9.6.1.4

Таким образом, в этом случае прокси запрещает доступ к IP-адресам 9.6.2.5 и 9.6.120.7 и выдает следующее сообщение: VMWPX0018E: Указанный IP-адрес целевого хоста запрещен правилом.

Прокси разрешает доступ к адресам 9.6.1.5 и 9.6.1.120, но запрещает доступ к адресу 9.6.1.4.

При добавлении новых правил фильтрации их можно комбинировать различными способами, но прокси всегда обрабатывает правила по порядку. Всегда срабатывает последнее применимое правило, все запрещающие и разрешающие правила перед ним не учитываются.

3. Настройте прокси Ajax для своей среды. См. раздел “Настройка прокси Business Space Ajax” на стр. 244.

Команды (сценарий `wsadmin`) для настройки Business Space

Просмотрите объект сценария или класс команд, чтобы получить сведения о синтаксисе команд.

Для того чтобы открыть этот раздел в оглавлении справочной системы Information Center, нажмите кнопку **Показать в оглавлении**, расположенную на границе справочной системы Information Center.

Команда `configureBusinessSpace`:

Команда `configureBusinessSpace` предназначена для настройки базы данных в Business Space, созданное с использованием WebSphere.

Эта команда настраивает источник данных для Business Space и генерирует сценарии создания и настройки таблиц баз данных.

После выполнения команды сохраните изменения в главной конфигурации с помощью одной из следующих команд:

- Для Jython:
`AdminConfig.save()`
- Для Jacl:
`$AdminConfig save`

Если сервер приложений не выполняется, укажите параметр `-conntype NONE` при выполнении этой команды.

Обязательные параметры

-serverName *имя-сервера*

Параметр, задающий имя сервера для конфигурации. Для настройки Business Space на сервере необходимо указать как **serverName**, так и **nodeName**.

-nodeName *имя-узла*

Параметр, задающий имя узла для конфигурации. Для настройки Business Space на сервере необходимо указать как **serverName**, так и **nodeName**.

-clusterName *имя_кластера*

Параметр, задающий имя кластера для конфигурации. Для настройки Business Space в кластере необходимо указать параметр **clusterName**.

Необязательные параметры

-dbName *имя-базыданных*

Задаёт базу данных для Business Space. Если сервер приложений и DB2 входят в состав одного образа z/OS, то необходимо указать параметр **-dbName**.

-schemaName *имя-схемы*

Необязательный параметр, задающий схему базы данных для конфигурации базы данных Business Space. Значение по умолчанию - IBMUSSP.

-tablespaceDir *путь-к-табличному-пространству*

Необязательный параметр, задающий путь к каталогу или префикс имени для файлов, используемых как физические расположения табличных пространств. Значение по умолчанию - BSP. Допустим для DB2, Oracle и SQL Server (в остальных случаях игнорируется). В случае SQL Server этот параметр применяется к основному файлу данных и файлам протокола.

-tableNamePrefix *префикс-табличного-пространства*

Необязательный параметр, задающий строку префикса, которая добавляется в начало имен табличных пространств, чтобы обеспечить их уникальность. Значение по умолчанию - BSP. Если длина префикса имени табличного пространства превышает четыре символа, то он усекается до четырех символов. Допустим для DB2, DB2 z/OS V8, DB2 z/OS V9 и Oracle (в остальных случаях игнорируется).

-dbLocationName *расположение_базы_данных*

Необязательный параметр, задающий имя расположения базы данных в z/OS. Значение по умолчанию - BSP или имя базы данных продукта. Допустим в DB2 z/OS V8 и V9 (в остальных случаях игнорируется).

-storageGroup *группа-хранения*

Необязательный параметр, задающий группу хранения в z/OS для Business Space. В случае применения z/OS необходимо обновить созданные сценарии баз данных перед их запуском. Дополнительная информация о сценариях приведена в разделе "Настройка таблиц баз данных Business Space".

-bspacedbDesign *файл_эскиза_базы_данных*

Необязательный параметр, задающий файл эскиза базы данных, который применяется для определения всей информации о конфигурации базы данных, включая схему и каталог табличного пространства. Если файл структуры базы данных указывается с помощью параметра **-bspacedbDesign**, то **-schemaName**, **-tablespaceDir** и **-storageGroup** указывать необязательно. Исключение составляет случай, когда требуется переопределить содержимое файла структуры базы данных.

Примечание: В качестве источника данных Business Space всегда используется имя JNDI jdbc/mashupDS, поэтому имя JNDI из файла структуры базы данных не применяется. Если источник данных с именем JNDI jdbc/mashupDS существует, то эта команда прерывается без настройки профайла. Исключение составляет случай, если задан параметр **-replaceDataSource true**.

-productTypeForDatasource база-данных-продукта

Необязательный параметр, задающий свойства, которые следует применять для создания источника данных для Business Space. Если указан параметр **productTypeForDatasource**, то создается источник данных для Business Space с именем JNDI jdbc/mashupDS, который моделируется на основе источника данных установленного продукта, такого как IBM Process Server, WebSphere Enterprise Service Bus, IBM Business Monitor и WebSphere Business Compass. Допустимые значения: WPS (IBM Business Process Manager или WebSphere Enterprise Service Bus), WPBS (WebSphere Business Compass) и WBM (IBM Business Monitor). Если также задан параметр **bspacedbDesign**, то параметр **productTypeForDatasource** переопределяет тип базы данных и провайдер JDBC, а имя JNDI из файла структуры базы данных не применяется.

Примечание: Если источник данных с именем JNDI jdbc/mashupDS существует, то эта команда прерывается без настройки профайла. Исключение составляет случай, если задан параметр `-replaceDatasource true`.

-replaceDatasource true|false

Необязательный параметр, указывающий, следует ли выполнять команду **configureBusinessSpace**, если профайл уже настроен. Значение по умолчанию: `false`. Если профайл настроен для Business Space, то создается источник данных с именем JNDI jdbc/mashupDS. Если источник данных существует, то команда **configureBusinessSpace** без параметра `-replaceDatasource true` не изменяет конфигурацию. Если указано значение `true`, то команда удалит источник данных вместе со связанным провайдером JDBC, создаст их заново, а также создаст новые сценарии DDL.

-save true|false

Этот параметр указывает сохранение изменений конфигурации. Значение по умолчанию: `false`.

Примеры

В следующем примере команда **configureBusinessSpace** применяется для настройки источника данных Business Space на сервере.

- Пример Jython:

```
AdminTask.configureBusinessSpace(['-nodeName myNode -serverName myServer'])
```
- Пример Jacl:

```
$AdminTask configureBusinessSpace {-nodeName myNode -serverName myServer}
```

В следующем примере команда **configureBusinessSpace** применяется для настройки источника данных Business Space в кластере и сохранения изменений.

- Пример Jython:

```
AdminTask.configureBusinessSpace(['-clusterName myCluster -save true'])
```
- Пример Jacl:

```
$AdminTask configureBusinessSpace {-clusterName myCluster -save true}
```

В следующем примере команда **configureBusinessSpace** применяется для настройки источника данных Business Space в кластере, с именем схемы и источником данных продукта, предназначенными для IBM Process Server.

- Пример Jython:

```
AdminTask.configureBusinessSpace('[-clusterName myCluster  
-schemaName myCluster -productTypeForDatasource WPS -save true]')
```

- Пример Jacl:

```
$AdminTask configureBusinessSpace {-clusterName myCluster  
-schemaName myCluster -productTypeForDatasource WPS -save true}
```

В следующем примере команда **configureBusinessSpace** применяется для настройки источника данных Business Space в кластере с помощью информации о базе данных из файла структуры базы данных.

- Пример Jython:

```
AdminTask.configureBusinessSpace('[-clusterName myCluster  
-bspacedbDesign "C:/Bspace_dbDesign.properties" -save true]')
```

- Пример Jacl:

```
$AdminTask configureBusinessSpace {-clusterName myCluster  
-bspacedbDesign "C:/Bspace_dbDesign.properties" -save true}
```

Команда **createBPMApiFederationDomain**:

Команда **createBPMApiFederationDomain** применяется для настройки доменов объединения в среде с несколькими целевыми средами развертывания, чтобы процессы и задачи, созданные в Process Designer и Integration Designer, можно было просмотреть в одном списке.

Команда **createBPMApiFederationDomain** с шагом **addTarget** создает домен объединения, позволяющий объединить задачи и процессы нескольких целевых сред развертывания. С помощью API объединения можно просмотреть процессы и задачи, созданные в Process Designer и Integration Designer, в одном списке задач. API объединения автоматически настраивается в продукте в процессе применения шлюза служб REST. При необходимости конфигурацию среды с несколькими целевыми средами развертывания можно изменить с помощью команд **wsadmin**, предназначенных для создания доменов объединения и управления ими. Шаг **addTarget** позволяет добавить целевые среды развертывания в домен объединения. API объединения объединяет все системы из добавленных сред развертывания.

После выполнения команды сохраните изменения в главной конфигурации с помощью одной из следующих команд:

- Для Jython:

```
AdminConfig.save()
```

- Для Jacl:

```
$AdminConfig save
```

Если сервер приложений не выполняется, укажите параметр **-conntype NONE** при выполнении этой команды.

Целевой объект

Область для создания домена объединения. Целевой объект можно использовать вместо параметров **nodeName**, **serverName** и **clusterName**.

Обязательные параметры

-serverName *имя-сервера*

Параметр, указывающий имя сервера, который будет применяться для администрирования домена объединения. Вместе с этим параметром необходимо указать параметр **nodeName**. Не указывайте этот параметр, если указан параметр

clusterName или целевой объект. Если целевое расположение развертывания не задано, то домен объединения создается в области ячейки.

-nodeName *имя-узла*

Параметр, указывающий имя узла, который будет применяться для администрирования домена объединения. Вместе с этим параметром необходимо указать параметр **serverName**. Не указывайте этот параметр, если указан параметр **clusterName** или целевой объект. Если целевое расположение развертывания не задано, то домен объединения создается в области ячейки.

-clusterName*имя_кластера*

Параметр, указывающий имя кластера, который будет применяться для администрирования домена объединения. Не указывайте этот параметр, если указаны параметры **nodeName** и **serverName** или целевой объект. Если целевое расположение развертывания не задано, то домен объединения создается в области ячейки.

-name *имя-домена-объединения*

Имя создаваемого домена объединения. Это имя должно быть уникальным. Это обязательный параметр.

Требуемые параметры для шага addTarget

-targetCellName *имя-ячейки*

Параметр, указывающий имя ячейки, применяемой в качестве целевого объекта объединения. Если этот параметр указан, а параметры **nodeName**, **serverName** и **clusterName** не заданы, то API выполняет объединение по всем системам ячейки.

-targetNodeName *имя-узла*

Параметр, указывающий имя узла, применяемого в качестве целевого объекта объединения. Если этот параметр указан, то API выполняет объединение по системам этого узла. Вместе с этим параметром необходимо указать параметр **targetServerName**. Этот параметр не следует указывать вместе с параметром **targetClusterName**.

-targetServerName *имя-сервера*

Параметр, указывающий имя сервера, применяемого в качестве целевого объекта объединения. Если этот параметр указан, то API выполняет объединение по системам этого сервера. Вместе с этим параметром необходимо указать параметр **targetNodeName**. Этот параметр не следует указывать вместе с параметром **targetClusterName**.

-targetClusterName *имя-кластера*

Параметр, указывающий имя кластера, применяемого в качестве целевого объекта объединения. Если этот параметр указан, то API выполняет объединение по системам этого кластера. Этот параметр не следует указывать вместе с параметром **targetNodeName** или **targetServerName**.

Примеры

В следующем примере команда **createBPMApiFederationDomain** применяется для добавления домена объединения **myCustomFederationDomain**, в состав которого входит сервер (с именем узла **myNode** и именем сервера **myServer**) и кластер (с именем **myCluster**).

- Пример Jython:

```
AdminTask.createBPMApiFederationDomain(['-nodeName имя-узла  
-serverName имя-сервера -name myCustomFederationDomain  
-addTarget [{" myNode myServer "} [{" " " " myCluster}]]')
```

- Пример Jacl:

```
$AdminTask createBPMApiFederationDomain {-nodeName имя-узла  
-serverName имя-сервера -name myCustomFederationDomain  
-addTarget {" " myNode myServer " " } {" " " " myCluster}}
```

Команда deleteBPMApiFederationDomain:

Команда **deleteBPMApiFederationDomain** позволяет удалить домен объединения вместе с целевыми объектами.

Эта команда удаляет домен объединения вместе с целевыми объектами для задач и процессов объединения в пределах одной или нескольких целевых сред развертывания. С помощью API объединения можно просмотреть процессы и задачи, созданные в Process Designer и Integration Designer, в одном списке задач. API объединения автоматически настраивается в продукте в процессе применения шлюза служб REST. При необходимости конфигурацию среды с несколькими целевыми средами развертывания можно изменить с помощью команд wsadmin, предназначенных для создания доменов объединения и управления ими.

После выполнения команды сохраните изменения в главной конфигурации с помощью одной из следующих команд:

- Для Jython:
AdminConfig.save()
- Для Jacl:
\$AdminConfig save

Если сервер приложений не выполняется, укажите параметр `-conntype NONE` при выполнении этой команды.

Целевой объект

Область для удаления домена объединения. Целевой объект можно использовать вместо параметров **nodeName**, **serverName** и **clusterName**.

Обязательные параметры

-serverName *имя-сервера*

Параметр, указывающий имя сервера, который будет применяться для администрирования домена объединения. Вместе с этим параметром необходимо указать параметр **nodeName**. Не указывайте этот параметр, если указан параметр **clusterName** или целевой объект. Если целевое расположение развертывания не задано, то домен объединения администрируется в области ячейки.

-nodeName *имя-узла*

Параметр, указывающий имя узла, который будет применяться для администрирования домена объединения. Вместе с этим параметром необходимо указать параметр **serverName**. Не указывайте этот параметр, если указан параметр **clusterName** или целевой объект. Если целевое расположение развертывания не задано, то домен объединения администрируется в области ячейки.

-clusterName*имя_кластера*

Параметр, указывающий имя кластера, который будет применяться для администрирования домена объединения. Не указывайте этот параметр, если указаны параметры **nodeName** и **serverName** или целевой объект. Если целевое расположение развертывания не задано, то домен объединения администрируется в области ячейки.

-name *имя-домена-объединения*

Имя домена объединения, который требуется удалить. Это имя должно быть уникальным. Это обязательный параметр.

Примеры

В следующем примере команда **deleteBPMApiFederationDomain** применяется для удаления домена объединения

- Пример Jython:

```
AdminTask.deleteBPMApiFederationDomain(['-nodeName myNode -serverName myServer -name myFederationD
```

- Пример Jacl:

```
$AdminTask deleteBPMApiFederationDomain {-nodeName myNode -serverName myServer -name myFederationD
```

Команда **getBusinessSpaceDeployStatus**:

Используйте команду **getBusinessSpaceDeployStatus** для проверки, настроен ли Business Space, созданное с использованием WebSphere в конкретной целевой среде развертывания.

Эта команда проверяет, настроен ли Business Space на указанном сервере, узле или кластере. Если параметры не заданы, она проверяет, настроен ли Business Space в ячейке.

После выполнения команды сохраните изменения в главной конфигурации с помощью одной из следующих команд:

- Для Jython:

```
AdminConfig.save()
```

- Для Jacl:

```
$AdminConfig save
```

Если сервер приложений не выполняется, укажите параметр **-connType NONE** при выполнении этой команды.

Обязательные параметры

-serverName *имя-сервера*

Этот параметр указывает имя сервера, на котором проверяется настройка Business Space.

-nodeName *имя-узла*

Этот параметр указывает имя узла, на котором проверяется настройка Business Space.

-clusterName *имя_кластера*

Этот параметр указывает имя кластера, на котором проверяется настройка Business Space.

Примеры

В следующем примере команда **getBusinessSpaceDeployStatus** проверяет, настроен ли Business Space на сервере.

- Пример Jython:

```
AdminTask.getBusinessSpaceDeployStatus(['-nodeName myNode -serverName myServer'])
```

- Пример Jacl:


```
$AdminTask getBusinessSpaceDeployStatus {-nodeName myNode -serverName myServer}
```

В следующем примере команда **getBusinessSpaceDeployStatus** проверяет, настроен ли Business Space в кластере.

- Пример Jython:

```
AdminTask.getBusinessSpaceDeployStatus('[-clusterName myCluster]')
```

- Пример Jacl:

```
$AdminTask getBusinessSpaceDeployStatus {-clusterName myCluster}
```

Следующий пример используется команду **getBusinessSpaceDeployStatus** для возврата списка всех назначений развертывания (сервер и кластеры), настроенных для Business Space в ячейке.

Если команда выполняется из каталога `bin` корневого каталога, она возвращает список всех целевых сред развертывания (сервер и кластеры), настроенных для Business Space в ячейке.

Если команда выполняется из каталога `bin` корневого каталога установки, она возвращает список всех целевых сред развертывания (сервер и кластеры), настроенных для Business Space в том же установочном каталоге.

- Пример Jython:

```
AdminTask.getBusinessSpaceDeployStatus()
```

- Пример Jacl:

```
$AdminTask getBusinessSpaceDeployStatus
```

Команда **installBusinessSpace**:

Команда **installBusinessSpace** используется для установки Business Space, созданное с использованием WebSphere в среде выполнения.

Команда **installBusinessSpace** устанавливает файлы архива предприятия (EAR) Business Space в среде выполнения.

После выполнения команды сохраните изменения в главной конфигурации с помощью одной из следующих команд:

- Для Jython:

```
AdminConfig.save()
```

- Для Jacl:

```
$AdminConfig save
```

Если сервер приложений не выполняется, укажите параметр `-conntype NONE` при выполнении этой команды.

Обязательные параметры

-serverName *имя-сервера*

Параметр, задающий имя сервера для конфигурации. Для настройки Business Space на сервере необходимо указать как **serverName**, так и **nodeName**.

-nodeName *имя-узла*

Параметр, задающий имя узла для конфигурации. Необходимо указать имя сервера, имя узла или имя кластера. Для настройки Business Space на сервере необходимо указать как **serverName**, так и **nodeName**.

-clusterName*имя_кластера*

Параметр, задающий имя кластера для конфигурации. Для настройки Business Space в кластере необходимо указать параметр **clusterName**.

Необязательные параметры

-noWidgets true|false

Необязательный параметр, который предотвращает установку виджетов продукта в целевом развертывании, если равен true. Если необходимо установить виджеты, используйте команду **installBusinessSpaceWidgets** после успешной настройки Business Space. Значение по умолчанию: false.

-save true|false

Этот необязательный параметр указывает сохранение изменений конфигурации. Значение по умолчанию: false.

Примеры

В следующем примере команда используется **installBusinessSpace** для установки на сервере файлов EAR Business Space.

- Пример Jython:

```
AdminTask.installBusinessSpace('[-nodeName myNode -serverName myServer -save true]')
```

- Пример Jacl:

```
$AdminTask installBusinessSpace {-nodeName myNode -serverName myServer -save true}
```

В следующем примере команда используется **installBusinessSpace** для установки в кластере файлов EAR Business Space.

- Пример Jython:

```
AdminTask.installBusinessSpace('[-clusterName myCluster -save true]')
```

- Пример Jacl:

```
$AdminTask installBusinessSpace {-clusterName myCluster -save true}
```

Команда installBusinessSpaceWidgets:

Команда **installBusinessSpaceWidgets** используется для установки, развертывания и регистрации виджетов, применяемых с помощью Business Space, созданное с использованием WebSphere.

Команда **installBusinessSpaceWidgets** устанавливает, развертывает и регистрирует назначенные виджеты, содержащиеся в сжатом файле или файле EAR. Если виджеты уже развернуты, команда **installBusinessSpaceWidgets** обновляет двоичные файлы и информацию о регистрации.

Структура сжатого файла виджета содержит следующие элементы:

- [ear\widgets_*имя*.ear] один или несколько файлов EAR.
- [catalog\catalog_*имя*.xml]
- [endpoints*.xml] конечные точки виджета
- [templates*.zip] Шаблоны должны находиться в сжатом файле в формате шаблона IBM Lotus Mashups.
- [help\eclipse\plugins*]

Все папки не требуются. Допустимы пустые папки.

После выполнения команды сохраните изменения в главной конфигурации с помощью одной из следующих команд:

- Для Jython:
`AdminConfig.save()`
- Для Jacl:
`$AdminConfig save`

Если сервер приложений не выполняется, укажите параметр `-conntype NONE` при выполнении этой команды.

Обязательные параметры

-serverName *имя-сервера*

Параметр, задающий имя сервера для конфигурации. Для настройки Business Space на сервере необходимо указать как **serverName**, так и **nodeName**.

-nodeName *имя-узла*

Параметр, задающий имя узла для конфигурации. Необходимо указать имя сервера, имя узла или имя кластера. Для настройки виджетов Business Space на сервере необходимо указать как **serverName**, так и **nodeName**.

-clusterName *имя_кластера*

Параметр, задающий имя кластера для конфигурации. Для настройки виджетов Business Space в кластере необходимо указать параметр **clusterName**.

-widgets *путь-к-виджетам*

Этот параметр указывает одно из следующего:

- Полный путь к каталогу, в котором расположены сжатые файлы или файлы EAR, содержащие виджеты. Если задан каталог, то будут установлены все виджеты для всех сжатых файлов и файлов EAR в этом каталоге.
- Полный путь к отдельному сжатому файлу, в котором расположены виджеты.
- Полный путь к отдельному файлу EAR, в котором расположены виджеты.

-save *true|false*

Этот параметр указывает сохранение конфигурации. Значение по умолчанию: `true`.

Необязательные параметры

-save *true|false*

Этот параметр указывает сохранение конфигурации. Значение по умолчанию: `true`.

Примеры

Следующий пример использует команду **installBusinessSpaceWidgets** для установки, развертывания и регистрации виджетов на сервере.

- Пример Jython:

```
AdminTask.installBusinessSpaceWidgets('[-nodeName имя-узла  
-serverName имя_сервера -widgets  
установочный-каталог/BusinessSpace/widgets/MyWidget.zip]')
```
- Пример Jacl:

```
$AdminTask installBusinessSpaceWidgets {-nodeName имя-узла  
-serverName имя_сервера -widgets  
установочный-каталог/BusinessSpace/widgets/MyWidget.zip}
```

Следующий пример использует команду **installBusinessSpaceWidgets** для установки, развертывания и регистрации виджетов в кластере.

- Пример Jython:

```
AdminTask.installBusinessSpaceWidgets('[-clusterName имя-кластера  
-widgets X:/WPS/Temp]')
```

- Пример Jacl:

```
$AdminTask installBusinessSpaceWidgets {-clusterName имя-кластера  
-widgets X:/WPS/Temp}
```

После выполнения команды **installBusinessSpaceWidgets** или **updateBusinessSpaceWidgets** требуется вручную обновить пространства и шаблоны Business Space. Дополнительная информация приведена в разделе Обновление шаблонов и пространств Business Space после установки или обновления виджетов.

Команда **listBPMApiFederationDomains**:

Команда **listBPMApiFederationDomains** позволяет просмотреть список всех доменов объединения в среде.

Эта команда отображает все домены объединения на уровне сервера или кластера. С помощью API объединения можно просмотреть процессы и задачи, созданные в Process Designer и Integration Designer, в одном списке задач. API объединения автоматически настраивается в продукте в процессе применения шлюза служб REST. При необходимости конфигурацию среды с несколькими целевыми средами развертывания можно изменить с помощью команд wsadmin, предназначенных для создания доменов объединения и управления ими.

Если сервер приложений не выполняется, укажите параметр **-connType NONE** при выполнении этой команды.

Целевой объект

Область для администрирования домена объединения. Целевой объект можно использовать вместо параметров **nodeName**, **serverName** и **clusterName**.

Обязательные параметры

-serverName *имя-сервера*

Параметр, указывающий имя сервера, который будет применяться для администрирования домена объединения. Вместе с этим параметром необходимо указать параметр **nodeName**. Не указывайте этот параметр, если указан параметр **clusterName** или целевой объект. Если целевое расположение развертывания не задано, то домен объединения администрируется в области ячейки.

-nodeName *имя-узла*

Параметр, указывающий имя узла, который будет применяться для администрирования домена объединения. Вместе с этим параметром необходимо указать параметр **serverName**. Не указывайте этот параметр, если указан параметр **clusterName** или целевой объект. Если целевое расположение развертывания не задано, то домен объединения администрируется в области ячейки.

-clusterName*имя_кластера*

Параметр, указывающий имя кластера, который будет применяться для администрирования домена объединения. Не указывайте этот параметр, если

указаны параметры **nodeName** и **serverName** или целевой объект. Если целевое расположение развертывания не задано, то домен объединения администрируется в области ячейки.

Примеры

В следующем примере команда **listBPMApiFederationDomains** применяется для просмотра всех доменов объединения на сервере.

- Пример Jython:

```
AdminTask.listBPMApiFederationDomains('[-nodeName myNode -serverName myServer]')
```

- Пример Jacl:

```
$AdminTask listBPMApiFederationDomains {-nodeName myNode -serverName myServer}
```

Команда **modifyBPMApiFederationDomain**:

Команда **modifyBPMApiFederationDomain** позволяет добавить или удалить целевые расположения из домена объединения с помощью шагов **addTarget** и **deleteTarget**.

Эта команда добавляет или удаляет целевые среды из домена объединения. API объединения автоматически настраивается в продукте в процессе применения шлюза служб REST. При необходимости конфигурацию среды с несколькими целевыми средами развертывания можно изменить с помощью команд **wsadmin**, предназначенных для создания доменов объединения и управления ими. Шаг **addTarget** позволяет добавить целевые среды развертывания в домен объединения. Среда развертывания удаляется из домена объединения на шаге **deleteTarget**. API объединения объединяет все системы из добавленных сред развертывания.

После выполнения команды сохраните изменения в главной конфигурации с помощью одной из следующих команд:

- Для Jython:

```
AdminConfig.save()
```

- Для Jacl:

```
$AdminConfig save
```

Если сервер приложений не выполняется, укажите параметр **-conntype NONE** при выполнении этой команды.

Целевой объект

Область для администрирования домена объединения. Целевой объект можно использовать вместо параметров **nodeName**, **serverName** и **clusterName**.

Обязательные параметры

-serverName *имя-сервера*

Параметр, указывающий имя сервера, который будет применяться для администрирования домена объединения. Вместе с этим параметром необходимо указать параметр **nodeName**. Не указывайте этот параметр, если указан параметр **clusterName** или целевой объект. Если целевое расположение развертывания не задано, то домен объединения администрируется в области ячейки.

-nodeName *имя-узла*

Параметр, указывающий имя узла, который будет применяться для администрирования домена объединения. Вместе с этим параметром необходимо

указать параметр **serverName**. Не указывайте этот параметр, если указан параметр **clusterName** или целевой объект. Если целевое расположение развертывания не задано, то домен объединения администрируется в области ячейки.

-clusterName *имя_кластера*

Параметр, указывающий имя кластера, который будет применяться для администрирования домена объединения. Не указывайте этот параметр, если указаны параметры **nodeName** и **serverName** или целевой объект. Если целевое расположение развертывания не задано, то домен объединения администрируется в области ячейки.

-name *имя-домена-объединения*

Имя изменяемого домена объединения. Это имя должно быть уникальным. Это обязательный параметр.

Обязательные параметры операций addTarget и deleteTarget

-targetCellName *имя-ячейки*

Параметр, указывающий имя ячейки, применяемой в качестве целевого объекта объединения. Если этот параметр задан, а параметры **nodeName**, **serverName** и **clusterName** не заданы, то API выполняет объединение по всем системам ячейки.

-targetNodeName *имя-узла*

Параметр, указывающий имя узла, применяемого в качестве целевого объекта объединения. Если этот параметр указан, то API выполняет объединение по системам этого сервера. Вместе с этим параметром должен быть задан параметр **targetServerName**. Этот параметр не следует указывать вместе с параметром **targetClusterName**.

-targetServerName *имя-сервера*

Параметр, указывающий имя сервера, применяемого в качестве целевого объекта объединения. Если этот параметр указан, то API выполняет объединение по системам этого сервера. Вместе с этим параметром необходимо указать параметр **targetNodeName**. Этот параметр не следует указывать вместе с параметром **targetClusterName**.

-targetClusterName *имя-кластера*

Параметр, указывающий имя сервера, применяемого в качестве целевого объекта объединения. Если этот параметр указан, то API выполняет объединение по системам этого кластера. Этот параметр не следует указывать вместе с параметром **targetNodeName** или **targetServerName**.

Примеры

В следующем примере команда **modifyBPMApiFederationDomain** применяется для удаления домена целевой среды развертывания (**myNode**, **myServer**) и добавления новой среды развертывания (**myNewNode**, **myNewServer**).

- Пример Jython:

```
AdminTask.modifyBPMApiFederationDomain('[-nodeName имя-узла  
-serverName имя-сервера -name myCustomFederationDomain  
-deleteTarget [{" myNode myServer ""}]')  
-addTarget [{" myNewNode myNewServer ""}]')
```

- Пример Jacl:

```
$AdminTask modifyBPMApiFederationDomain {-nodeName имя-узла  
-serverName имя-сервера -name myCustomFederationDomain  
-deleteTarget [{" myNode myServer ""}]  
-addTarget [{" myNewNode myNewServer ""}]}
```

Команда `registerRESTServiceEndpoint`:

Команда `registerRESTServiceEndpoint` используется для регистрации настроенных и включенных конечных точек REST, чтобы сотрудники коллектива могли применять виджеты в Business Space.

Эта команда регистрирует конечные точки службы REST для правильного подключения Business Space к виджетам для продукта. Эта команда регистрирует конечные точки служб REST, расположенные в одной ячейке с Business Space.

После выполнения команды сохраните изменения в главной конфигурации с помощью одной из следующих команд:

- Для Jython:
`AdminConfig.save()`
- Для Jacl:
`$AdminConfig save`

Если сервер приложений не выполняется, укажите параметр `-conntype NONE` при выполнении этой команды.

Обязательные параметры

`-clusterName`*имя_кластера_служб_rest*

Этот параметр указывает имя кластера для службы REST. Для регистрации конечных точек служб REST для кластера необходимо указать параметр `clusterName`.

`-nodeName`*имя-узла-служб-rest*

Этот параметр указывает имя узла для службы REST. Для регистрации конечных точек служб REST для сервера необходимо указать как `serverName`, так и `nodeName`.

`-serverName`*имя-сервера-служб-rest*

Этот параметр указывает имя сервера для службы REST. Для регистрации конечных точек служб REST для сервера необходимо указать как `serverName`, так и `nodeName`.

`-businessSpaceClusterName`*имя_кластера_бизнес_пространства*

Имя кластера Business Space. Если экземпляр Business Space настроен в кластере, то необходимо указать параметр `businessSpaceClusterName`.

`-businessSpaceNodeName`*имя_узла_бизнес_пространства*

Имя узла Business Space. Если экземпляр Business Space настроен на сервере, то необходимо указать как `businessSpaceServerName`, так и `businessSpaceNodeName`.

`-businessSpaceServerName`*имя_сервера_бизнес_пространства*

Имя сервера Business Space. Если экземпляр Business Space настроен на сервере, то необходимо указать как `businessSpaceServerName`, так и `businessSpaceNodeName`.

Необязательные параметры

`-appName`*имя_приложения_поставщика*

Имя приложения поставщика службы REST.

`-name` *имя-службы-rest*

Имя службы REST.

-typeимя-типа-службы

Тип службы. Этот параметр является необязательным. Если этот параметр не указан, регистрируются все уникальные конечные точки службы REST, настроенные для указанного провайдера службы REST в указанной целевой среде развертывания. Если требуется указать определенную конечную точку службы, используйте значение `<tns:type>`, которое находится в файле конечных точек для виджета. Файлы конечных точек расположены в каталоге *корневой_каталог_установки\BusinessSpace\registryData\endpoints*. Например, *bpmAdministrationEndpoints.xml* содержит все типы конечных точек службы, которые используются в виджетах Администрирование. Значением элемента `<tns:type>` является `{com.ibm.bpm}SCA`:

```
<tns:Endpoint>
  <tns:id>{com.ibm.bpm}SCA</tns:id>
  <tns:type>{com.ibm.bpm}SCA</tns:type>
  <tns:version>6.2.0.0</tns:version>
  <tns:url>/rest/sca/v1</tns:url>
  <tns:description>Location backend SCA REST Services
  for Module Administration widgets and Service Monitoring widget
</tns:description>
</tns:Endpoint>
```

Для Jacl необходимо заключать значение в двойные кавычки, например: ...
`-type "{com.ibm.bpm}SCA" ...`

-versionимя-версии

Версия поставщика службы REST.

-webModuleNameимя-веб-модуля

Имя веб-модуля поставщика службы REST.

Примеры

Следующий пример использует команду **registerRESTServiceEndpoint**. Команда регистрирует все настроенные и разрешенные службы REST в кластере с Business Space.

- Пример Jython:

```
AdminTask.registerRESTServiceEndpoint('[-clusterName
название-кластера-служб-rest -businessSpaceClusterName
имя-кластера-бизнес-пространства]')
```

- Пример Jacl:

```
AdminTask registerRESTServiceEndpoint {-clusterName
название-кластера-служб-rest -businessSpaceClusterName
имя-кластера-бизнес-пространства}
```

Команда showBPMApiFederationDomain:

С помощью команды **showBPMApiFederationDomain** можно просмотреть сведения о домене объединения.

Эта команда отображает сведения о целевых средах, настроенных на уровне узла, сервера или кластера для конкретного домена объединения. API объединения автоматически настраивается в продукте в процессе применения шлюза служб REST. При необходимости конфигурацию среды с несколькими целевыми средами развертывания можно изменить с помощью команд `wsadmin`, предназначенных для создания доменов объединения и управления ими.

Если сервер приложений не выполняется, укажите параметр `-conntype NONE` при выполнении этой команды.

Целевой объект

Область для администрирования домена объединения. Целевой объект можно использовать вместо параметров **nodeName**, **serverName** и **clusterName**.

Обязательные параметры

-serverName *имя-сервера*

Параметр, указывающий имя сервера, который будет применяться для администрирования домена объединения. Вместе с этим параметром необходимо указать параметр **nodeName**. Не указывайте этот параметр, если указан параметр **clusterName** или целевой объект. Если целевое расположение развертывания не задано, то домен объединения администрируется в области ячейки.

-nodeName *имя-узла*

Параметр, указывающий имя узла, который будет применяться для администрирования домена объединения. Вместе с этим параметром необходимо указать параметр **serverName**. Не указывайте этот параметр, если указан параметр **clusterName** или целевой объект. Если целевое расположение развертывания не задано, то домен объединения администрируется в области ячейки.

-clusterName *имя_кластера*

Параметр, указывающий имя кластера, который будет применяться для администрирования домена объединения. Не указывайте этот параметр, если указаны параметры **nodeName** и **serverName** или целевой объект. Если целевое расположение развертывания не задано, то домен объединения администрируется в области ячейки.

-name *имя-домена-объединения*

Имя домена объединения, который требуется просмотреть. Это имя должно быть уникальным. Это обязательный параметр.

Примеры

В следующем примере команда **showBPMApiFederationDomain** применяется для просмотра сведений о домене объединения.

- Пример Jython:

```
AdminTask.showBPMApiFederationDomain(['-nodeName myNode -serverName myServer -name myFederationDomain'])
```

- Пример Jacl:

```
$AdminTask showBPMApiFederationDomain {-nodeName myNode -serverName myServer -name myFederationDomain}
```

Команда **uninstallBusinessSpaceWidgets**:

Команда **uninstallBusinessSpaceWidgets** используется для удаления виджетов и определений виджетов из профайла, включая удаление отдельных ресурсов виджетов (приложение, каталог, конечные точки, пространства, шаблоны, справка).

Команда **uninstallBusinessSpaceWidgets** удаляет файлы виджета в назначенном сжатом файле или файле EAR. Структура сжатого файла виджета содержит следующие элементы:

- [ear\widgets_*имя*.ear] один или несколько файлов EAR.
- [catalog/catalog_*имя*.xml]
- [endpoints*.xml] конечные точки виджета

- [templates*.zip] Шаблоны должны находиться в сжатом файле в формате шаблона IBM Lotus Mashups.
- [help\eclipse\plugins*]

Все папки не требуются. Допустимы пустые папки.

Примечание: При настройке конечной точки REST без использования команды **updateBusinessSpaceWidgets** изменения конечной точки будут потеряны после выполнения команды **uninstallBusinessSpaceWidgets**.

После выполнения команды сохраните изменения в главной конфигурации с помощью одной из следующих команд:

- Для Jython:
AdminConfig.save()
- Для Jacl:
\$AdminConfig save

Если сервер приложений не выполняется, укажите параметр `-conntype NONE` при выполнении этой команды.

Обязательные параметры

-serverName *имя-сервера*

Параметр, задающий имя сервера для конфигурации. Для настройки Business Space на сервере необходимо указать как **serverName**, так и **nodeName**.

-nodeName *имя-узла*

Параметр, задающий имя узла для конфигурации. Для настройки Business Space на сервере необходимо указать как **serverName**, так и **nodeName**.

-clusterName *имя_кластера*

Параметр, задающий имя кластера для конфигурации. Для настройки Business Space в кластере необходимо указать параметр **clusterName**.

-widgets*путь-к-виджетам*

Этот параметр указывает одно из следующего:

- Полный путь к каталогу, в котором расположены сжатые файлы или файлы EAR, содержащие виджеты. Если задан каталог, то будут установлены все виджеты для всех сжатых файлов и файлов EAR в этом каталоге.
- Полный путь к отдельному сжатому файлу, в котором расположены виджеты.
- Полный путь к отдельному файлу EAR, в котором расположены виджеты.

Необязательные параметры

-save true|false

Этот параметр указывает сохранение изменений конфигурации. Значение по умолчанию: true.

Пример

В следующем примере команда **uninstallBusinessSpaceWidgets** используется для удаления виджетов из кластера.

Примечание: Примеры приведены исключительно в целях иллюстрации. Они содержат значения переменных и не предназначены для использования в качестве фрагментов кода.

- Пример Jython:

```
AdminTask.uninstallBusinessSpaceWidgets('[-clusterName  
имя-кластера -widgets X:/WPS/Temp]')
```

- Пример Jacl:

```
$AdminTask uninstallBusinessSpaceWidgets {-clusterName  
имя-кластера -widgets X:/WPS/Temp}
```

Команда **updateBusinessSpaceWidgets**:

Команда **updateBusinessSpaceWidgets** используется для обновления предварительно настроенных виджетов Business Space и их конечных точек, каталогов, шаблонов и встраиваемых модулей справки.

Команда **updateBusinessSpaceWidgets** обновляет двоичные файлы виджета, файлы каталога, файлы конечной точки, шаблоны и встраиваемые модули справки для виджетов, которые были предварительно установлены и настроены для Business Space.

Команда **updateBusinessSpaceWidgets** обновляет файлы виджета в назначенном сжатом файле или файле архива предприятия (EAR). Структура сжатого файла виджета содержит следующие элементы:

- [ear\widgets_имя.ear] один или несколько файлов EAR.
- [catalog\catalog_имя.xml]
- [endpoints*.xml] конечные точки виджета
- [templates*.zip] Шаблоны должны находиться в сжатом файле в формате шаблона IBM Lotus Mashups.
- [help\eclipse\plugins*]

Все папки не требуются. Допустимы пустые папки.

После выполнения команды сохраните изменения в главной конфигурации с помощью одной из следующих команд:

- Для Jython:
AdminConfig.save()
- Для Jacl:
\$AdminConfig save

Если сервер приложений не выполняется, укажите параметр `-connType NONE` при выполнении этой команды.

Обязательные параметры

-serverName *имя-сервера*

Параметр, задающий имя сервера для конфигурации. Для настройки виджетов Business Space на сервере необходимо указать как **serverName**, так и **nodeName**.

-nodeName *имя-узла*

Параметр, задающий имя узла для конфигурации. Необходимо указать имя сервера, имя узла или имя кластера. Для настройки виджетов Business Space на сервере необходимо указать как **serverName**, так и **nodeName**.

-clusterName*имя_кластера*

Параметр, задающий имя кластера для конфигурации. Для настройки Business Space в кластере необходимо указать параметр **clusterName**.

Необязательные параметры

-widgets*путь-к-виджету*

Параметр, который указывает полный путь к каталогу, в котором расположены файлы архива предприятия (EAR) или сжатые файлы виджета, или полный путь к определенному файлу EAR или сжатому файлу виджета.

-endpoints*путь-конечной-точке*

Параметр, который указывает полный путь к каталогу, в котором расположены файлы конечной точки виджета, или полный путь к определенному файлу конечной точки.

-catalogs*путь_к_каталогу*

Параметр, который указывает полный путь к каталогу, в котором расположены файлы каталога виджета, или полный путь к определенному файлу каталога.

-templates*путь-к-шаблону*

Параметр, который указывает полный путь к каталогу, в котором расположены файлы шаблона виджета, или полный путь к определенному файлу шаблона.

-helpplugins*путь-к-справке*

Параметр, который указывает полный путь к каталогу, в котором расположены файлы встраиваемого модуля электронной справки виджета, или полный путь к определенному файлу встраиваемого модуля электронной справки.

-noWidgets true|false

Позволяет запретить обновление файлов EAR виджетов из сжатого файла виджетов.

-noEndpoints true|false

Позволяет запретить обновление файлов заданной конечной точки из сжатого файла виджетов.

-noCatalogs true|false

Позволяет запретить обновление файлов определения каталога из сжатого файла виджетов.

-noTemplates true|false

Позволяет запретить обновление шаблонов из сжатого файла виджетов.

-noHelp true|false

Позволяет запретить обновление файлов справки из сжатого файла виджетов.

-save true|false

Этот параметр указывает сохранение конфигурации. Значение по умолчанию: true.

Примеры

В следующем примере команда **updateBusinessSpaceWidgets** используется для обновления виджетов в кластере.

Пример Jython:

```
AdminTask.updateBusinessSpaceWidgets('[-clusterName имя-кластера  
-widgets путь_к_виджету']')
```

Пример Jacl:

```
$AdminTask updateBusinessSpaceWidgets {-clusterName имя-кластера  
-widgets путь_к_виджету}
```

В следующем примере команда используется **updateBusinessSpaceWidgets** для обновления виджетов на сервере.

Пример Jython:

```
AdminTask.updateBusinessSpaceWidgets('[-nodeName имя-узла  
-serverName имя_сервера -widgets  
путь_к_виджету]')
```

Пример Jacl:

```
$AdminTask updateBusinessSpaceWidgets {-nodeName имя-узла  
-serverName имя_сервера -widgets  
путь_к_виджету}
```

После выполнения команды **installBusinessSpaceWidgets** или **updateBusinessSpaceWidgets** требуется вручную обновить пространства и шаблоны Business Space. Дополнительная информация приведена в разделе Обновление шаблонов и пространств Business Space после установки или обновления виджетов.

Команда updateRESTGatewayService:

Команда **updateRESTGatewayService** используется для обновления службы шлюза REST для включения и настройки служб REST.

Эта команда обновляет службу шлюза REST, после чего службы REST становятся настроенными и включенными. В конфигурации с автономным сервером службы REST развертываются автоматически. Для других типов конфигураций на странице административной консоли Службы REST или с помощью команды **updateRESTGatewayService** можно настроить службы REST для всех виджетов продукта в Business Space.

После выполнения команды сохраните изменения в главной конфигурации с помощью одной из следующих команд:

- Для Jython:
AdminConfig.save()
- Для Jacl:
\$AdminConfig save

Если сервер приложений не выполняется, укажите параметр **-conntype NONE** при выполнении этой команды.

Обязательные параметры

-clusterName *имя_кластера*

Этот параметр указывает имя кластера для службы REST. Для настройки служб REST в кластере необходимо указать параметр **clusterName**.

-nodeName *имя-узла*

Этот параметр указывает имя узла для службы REST. Для настройки служб REST на сервере необходимо указать как **serverName**, так и **nodeName**.

-serverName *имя-сервера*

Этот параметр указывает имя сервера для службы REST. Для настройки служб REST на сервере необходимо указать как **serverName**, так и **nodeName**.

-enable true | false

Указывает, включена ли служба REST. Допустимые значения: true и false.

Необязательные параметры

-type*имя-типа-службы*

Тип службы REST.

-version*имя-версии*

Версия службы REST.

Примеры

В следующем примере команда **updateRESTGatewayService** обновляет службу шлюза REST, после чего службы REST становятся настроенными и включенными.

- Пример Jython:

```
AdminTask.updateRESTGatewayService('[-nodeName node1 -serverName  
server1 -type "{com.ibm.bpm}TimeTable" -version 6.2.0.0 -enable  
true]')
```

- Пример Jacl:

```
$AdminTask updateRESTGatewayService {-nodeName node1 -serverName  
server1 -type "{com.ibm.bpm}TimeTable" -version 6.2.0.0 -enable true}
```

Обновление шаблонов и областей бизнес-пространства после установки или обновления виджетов:

Для обновления шаблонов и областей бизнес-пространства после выполнения команды **installBusinessSpaceWidgets** или **updateBusinessSpaceWidgets** в кластерной среде требуются действия, выполняемые вручную.

После использования команды **installBusinessSpaceWidgets** или **updateBusinessSpaceWidgets** необходимо выполнить следующие дополнительные действия.

1. Если бизнес-пространство настроено в кластере, выполните следующее:
 - a. Укажите пользовательский профайл для файла oobLoadedStatus properties:
 - 1) В профайле администратора развертывания откройте файл *корневой-каталог-профайлов-администратора-развертывания* \BusinessSpace*имя-кластера*\mm.runtime.prof\config\ConfigService.properties.
 - 2) Найдите имя ячейки, узел и сервер в свойствах com.ibm.mashups.directory.templates или com.ibm.mashups.directory.spaces.
Например, в com.ibm.mashups.directory.templates = config/cells/Cell101/nodes/Node01/servers/Server1/mm/templates можно найти пользовательский профайл по имени ячейки Cell101 и имени узла Node01.
 - 3) Найдите пользовательский профайл с помощью имен ячейки, узла и сервера.
 - b. В пользовательском профайле откройте файл *корневой-каталог-пользовательских-профайлов* \BusinessSpace*имя-кластера* \mm.runtime.prof\public\oobLoadedStatus.properties и обновите свойство importTemplates.txt или importSpaces.txt:
importTemplates.txt=true
importSpaces.txt=true
Если база данных бизнес-пространства была создана после удаления или если требуется перезагрузить тему по какой-то причине, также обновите следующее свойство:
importThemes.txt=true

- c. Снова синхронизируйте пользовательский профайл.
 - 1) Откройте административную консоль и выберите **Администрирование системы > Узлы**.
 - 2) Нажмите **Полностью синхронизировать повторно**.
 - d. Перезапустите кластер.
2. Если бизнес-пространство настроено на управляемом сервере, выполните следующее:
- a. В пользовательском профайле, в котором расположен управляемый сервер, откройте файл *корневой-каталог-пользовательских-профайлов\BusinessSpace\имя-узла\имя-сервера\mm.runtime.prof\public\oobLoadedStatus.properties* и обновите свойство `importTemplates.txt` или `importSpaces.txt`:


```
importTemplates.txt=true
importSpaces.txt=true
```

Если база данных бизнес-пространства была создана после удаления или если требуется перезагрузить тему по какой-то причине, также обновите следующее свойство:

```
importThemes.txt=true
```
 - b. Снова синхронизируйте пользовательский профайл.
 - 1) Откройте административную консоль и выберите **Администрирование системы > Узлы**.
 - 2) Нажмите **Полностью синхронизировать повторно**.
 - c. Перезапустите сервер.

Миграция Business Space (заключительные задачи миграции продукта)

После миграции продукта до V7.5 необходимо выполнить дополнительные задачи для Business Space, перед тем как запускать серверы или кластеры.

Прежде чем выполнять эту задачу, необходимо выполнить миграцию рабочего сервера или кластера и проверить успешность миграции.

Также необходимо выполнить миграцию базы данных, которая используется для Business Space. Для миграции баз данных и данных следуйте инструкциям для своего продукта.

Если выполняется миграция с более ранней версии продукта и настроен Business Space, после миграции необходимо выполнить следующие действия, прежде чем можно будет пользоваться Business Space.

1. Если в предыдущем выпуске были пользовательские виджеты, вручную подготовьте эти виджеты к работе в Business Space V7.5. См. раздел Миграция пользовательских виджетов.

Совет: Миграция данных версия 7.0 упрощает миграцию каталога и конечных точек пользовательских виджетов; в этом случае не придется еще раз вручную выполнять их миграцию.

2. Если в предыдущем выпуске Business Space и службы REST работали в разных ячейках или если виджеты и Business Space находились в разных ячейках, необходимо обновить файлы конечных точек. См. раздел Включение виджетов Business Space для сред с несколькими ячейками.

3. Если в предыдущем выпуске использовался IBM Forms Server в среде с виджетами Управление неавтоматизированными задачами, вручную настройте Business Space для работы с IBM Forms Server 4.0 и компонентом Webform Server.
 - a. Установите IBM Forms Server 4.0.
 - b. В административной консоли продукта обновите следующие переменные среды:
 - В ссылках на API поменяйте 76 на 80, например `${LFS_API_DIR};${LFS_API_DIR}/80/system;`
 - Присвойте переменной LFS_DIR путь к каталогу установки IBM Forms Server 4.0, например `c:\Program Files\IBM Forms Server\4.0\WebformServer.`

См. раздел Настройка IBM Forms Server для виджетов Управление неавтоматизированными задачами в Business Space.
4. Если из предыдущей среды Business Space были экспортированы пространства или шаблоны, импортируйте их в Business Space версии 7.5, чтобы они стали доступны для использования. См. разделы Импорт пространств и Импорт шаблонов.

Совет: При миграции шаблонов с версии 6.x сначала импортируйте их как пространства в Администратор пространств, а затем преобразуйте импортированные пространства в шаблоны командой **Действия > Сохранить как шаблон**.

После выполнения этих процедур миграции Business Space V7.5 готов к работе.

Совет: Если использовался Business Space версия 6.2; перед тем как приступить к работе с Business Space V7.5, необходимо очистить кэш браузера. Это предотвратит ненамеренное использование кода и изображений из Business Space версия 6.2.

Настройка бизнес-пространства для работы с Mashup Center

Настройка бизнес-пространства для работы с IBM Mashup Center предоставляет пользователям бизнес-пространства возможность публиковать шаблоны и страницы в каталоге Mashup Center, использовать шаблоны Mashup для создания пространств и импортировать отдельные страницы из Mashup Center в бизнес-пространство.

Для применения Business Space совместно с Mashup Center требуется действующая лицензия на Mashup Center. Business Space поддерживает только виджеты, которые зарегистрированы в Business Space или опубликованы в Mashup Center.

Если Mashup Center (включая IBM InfoSphere MashupHub) и Business Space установлены на разных серверах приложений, то между этими серверами необходимо создать среду единого входа в систему. Для этого в качестве реестра пользователей среды должно быть настроено объединенное хранилище. Дополнительная информация приведена в разделах Импорт ключей LTPA и Экспорт ключей LTPA в справочной системе WebSphere Application Server Information Center. Кроме того, настройте сертификаты SSL. Дополнительная информация приведена в разделе Защита соединений с помощью протокола Secure Sockets Layer (SSL) в справочной системе WebSphere Application Server Information Center.

Для того чтобы обеспечить взаимодействие Business Space с Mashup Center, выполните одну из следующих процедур для автономного сервера или кластерной среды.

- Для автономного сервера выполните следующие действия:

1. Измените свойство `com.ibm.mashups.hub.url` в файле конфигурации *каталог-профайла\BusinessSpace\имя-узла\имя-сервера\mm.runtime.prof\config\ConfigService.properties*, указав в нем URL компонента Mashup Center MashupHub (*протокол://хост:порт/mashuphub*).
2. Выполните команду **updatePropertyConfig** в среде wsadmin профайла:
В следующем примере используется Jython:

```
AdminTask.updatePropertyConfig('[-serverName имя-сервера -nodeName
имя-узла -propertyName "каталог-профайла\BusinessSpace\имя-узла\
имя-сервера\mm.runtime.prof\config\ConfigService.properties" -prefix
"Mashups_"]')
```

```
AdminConfig.save()
```

 В следующем примере используется Jacl:

```
$AdminTask updatePropertyConfig {-serverName имя-сервера -nodeName
имя-узла -propertyName "каталог-профайла\BusinessSpace\имя-узла\
имя-сервера\mm.runtime.prof\config\ConfigService.properties" -prefix
"Mashups_"}
```

```
$AdminConfig save
```
3. Откройте файл конфигурации *каталог-профайла\BusinessSpace\имя-узла\имя-сервера\mm.runtime.prof\config\Endpoints.properties* и укажите в свойстве `oob.Widget.url` URL Mashup Center (*протокол://хост:порт/*).
4. Выполните команду **updatePropertyConfig** в среде wsadmin профайла:
В следующем примере используется Jython:

```
AdminTask.updatePropertyConfig('[-serverName имя-сервера -nodeName
имя-узла -propertyName "каталог-профайла\BusinessSpace\имя-узла\
имя-сервера\mm.runtime.prof\config\Endpoints.properties" -prefix
"Mashups_"]')
```

```
AdminConfig.save()
```

 В следующем примере используется Jacl:

```
$AdminTask updatePropertyConfig {-serverName имя-сервера -nodeName
имя-узла -propertyName "каталог-профайла \BusinessSpace\имя-узла\
имя-сервера \mm.runtime.prof\config\Endpoints.properties" -prefix
"Mashups_"}
```

```
$AdminConfig save
```
5. Перезапустите сервер.
- В кластере выполните следующие действия:
 1. Измените свойство `com.ibm.mashups.hub.url` в файле конфигурации *каталог-профайла-администратора-развертывания\BusinessSpace\имя-кластера\mm.runtime.prof\config\ConfigService.properties*, указав в нем URL компонента Mashup Center MashupHub (*протокол://хост:порт/mashuphub*).
 2. С помощью администратора развертывания выполните команду **updatePropertyConfig** в среде wsadmin профайла:
В следующем примере используется Jython:

```
AdminTask.updatePropertyConfig('[-clusterName имя-кластера
-propertyFileName "каталог-профайла-администратора-развертывания\
BusinessSpace\имя-кластера\mm.runtime.prof\config\
ConfigService.properties" -prefix "Mashups_"]')
```

```
AdminConfig.save()
```

 В следующем примере используется Jacl:

```
$AdminTask updatePropertyConfig {-clusterName имя-кластера
-propertyFileName "каталог-профайла-администратора-развертывания\
```

- ```
BusinessSpace\имя-кластера\mm.runtime.prof\config\
ConfigService.properties" -prefix "Mashups_" }
$AdminConfig save
```
- Откройте файл конфигурации *каталог-профайла\BusinessSpace\имя-узла\имя-сервера\mm.runtime.prof\config\Endpoints.properties* и укажите в свойстве `oob.Widget.url` URL Mashup Center (*протокол://хост:порт/*).
  - С помощью администратора развертывания выполните команду **updatePropertyConfig** в среде wsadmin профайла:  
В следующем примере используется Jython:  

```
AdminTask.updatePropertyConfig('[-clusterName имя-кластера
-propertyFileName "каталог-профайла-администратора-развертывания\
BusinessSpace\имя-кластера\mm.runtime.prof\config\
Endpoints.properties" -prefix "Mashups_"]')
```

 AdminConfig.save()  
 В следующем примере используется Jacl:  

```
$AdminTask updatePropertyConfig {-clusterName имя-кластера
-propertyFileName "каталог-профайла-администратора-развертывания\
BusinessSpace\имя-кластера\mm.runtime.prof\config\
Endpoints.properties" -prefix "Mashups_" }
$AdminConfig save
```
  - Перезапустите администратор развертывания.

## Настройка виджетов для работы в WebSphere Portal

Если используется IBM WebSphere Portal, виджеты Business Space можно настроить на работу в среде WebSphere Portal.

Перед настройкой виджетов на работу в WebSphere Portal необходимо выполнить следующие задачи:

- Установить WebSphere Portal 7.0.0.1 или выше.
- Установить и настроить продукт IBM, который включает Business Space 7.5.
- Настроить Business Space и службы REST, чтобы у виджетов был доступ к службам во время выполнения. См. раздел “Настройка служб REST” на стр. 192.
- Настроить SSL и SSO. См. раздел “Настройка SSO и SSL для виджетов WebSphere Portal” на стр. 274.
- Настроить виджеты, если это необходимо.
- Если используются виджеты Управление неавтоматизированными задачами в кластерной среде, должны быть установлены формы Dojo на одном узле с виджетами.

Во время настройки виджетов Business Space на работу в WebSphere учтите следующее:

- Нельзя устанавливать свой серверный продукт в профайл WebSphere Portal.

**Ограничение:** Не все виджеты продукта поддерживают работу в WebSphere Portal. Список поддерживаемых сред должен быть в документации продукта.

- Создайте на сервере приложений WebSphere Portal ссылки на конечные точки. Для правильной работы Business Space в WebSphere Portal необходимо создать записи ссылок на конечные точки Business Space и продукта. Конечные точки должны быть созданы на сервере WebSphere Portal, но создаются они удаленно командой **updateEndpointBindingsOnPortal** на сервере продукта.
  - Запустите сервер WebSphere Portal и сервер продукта.

- b. Скопируйте файлы конечных точек из Business Space и продукта во временный каталог системы, где установлен продукт, например `c:/tmp/endpoints/`.

Файлы конечных точек находятся на сервере продукта в каталоге *каталог-профайла/BusinessSpace/имя-узла/имя-сервера/mm.runtime.prof/endpoints/*. Копировать нужно только те файлы конечных точек, для которых требуется создать записи. Файлы, которые ранее уже были обработаны командой `updateEndpointBindingsOnPortal`, копировать необязательно.

- c. В распределенной среде укажите правильные URL в файлах конечных точек.

Поскольку конечные точки регистрируются на сервере приложений, где работает сервер WebSphere Portal, все конечные точки должны указывать на удаленный сервер Business Space. Конечные точки должны содержать полное имя или IP-адрес удаленного хоста, например:

```
<tns:Endpoint>
 <tns:id>{com.ibm.bspace}bspaceCommonWidgetRootId</tns:id>
 <tns:type>{com.ibm.bspace}bspaceCommonWidgetRootId</tns:type>
 <tns:version>1.0.0.0</tns:version>
 <tns:url>http://<хост-business-space>:<порт>/BusinessSpace/</tns:url>
 <tns:description>Расположение общих виджетов Business Space</tns:description>
</tns:Endpoint>
```

Выполните действия из раздела “Включение виджетов Business Space для сред с несколькими ячейками” на стр. 213.

- d. Откройте сеанс `wsadmin` на сервере продукта. Выполните сценарий `wsadmin.bat` или `wsadmin.sh` в каталоге *каталог-профайла/bin/*. Сеанс `wsadmin` подключается к локальной виртуальной машине Java сервера приложений продукта.
- e. В сеансе `wsadmin` выполните команду `updateEndpointBindingsOnPortal`. (В среде сетевого развертывания она должна выполняться на администраторе развертывания.)

- Пример на языке Jython:

```
AdminTask.updateEndpointBindingsOnPortal(['-nodeName
имя-узла-портала -serverName портал-websphere
-endpointBindingDirectoryName каталог-файлов-конечных-точек -host
хост-или-IP-адрес-сервера-портала -port порт-soap-портала-(по-
умолчанию-10025) -user имя-администратора-портала -password
пароль-администратора-портала'])
```

- Пример на языке JACL:

```
$AdminTask updateEndpointBindingsOnPortal {-nodeName
имя-узла-портала -serverName портал-websphere
-endpointBindingDirectoryName каталог-файлов-конечных-точек -host
хост-или-IP-адрес-сервера-портала -port порт-soap-портала-(по-
умолчанию-10025) -user имя-администратора-портала -password
пароль-администратора-портала}
```

- f. Перезапустите сервер WebSphere Portal.
- g. Проверьте конечные точки, перейдя в провайдер среды ресурсов **Конечные точки гибрида WP**. Выберите **Ресурсы > Провайдеры среды ресурсов > Пользовательские свойства**.
2. Настройте прокси Ajax на сервере WebSphere Portal. Для того чтобы сервер продукта был доступен по удаленным URL с сервера WebSphere Portal, необходимо настроить прокси Ajax.
- a. Добавьте в файл `proxu-config.xml` фрагмент кода из примера стратегии прокси, приведенного в разделе “Обязательные записи в файле `proxu-config.xml` для настройки виджетов на сервере WebSphere Portal” на стр. 276.

b. Выполните сценарий **checkin-wp-proxy-config**.

В кластерной среде этот сценарий должен выполняться на главном узле.

```
ConfigEngine.[bat|sh] checkin-wp-proxy-config
-DProxyConfigFileName=каталог/имя-временного-файла-прокси
-DWasPassword=пароль-пользователя-сервера-приложений
-DWasUserid=имя-пользователя-сервера-приложений -DPortalAdminId=имя-
администратора-websphere-portal -DPortalAdminPwd=пароль-
администратора-websphere-portal, где каталог/имя-временного-файла-прокси
- полный путь к измененному файлу wp.proxy.config.xml.
```

Дополнительная информация о настройке прокси приведена в документации WebSphere Portal по адресу [http://www-10.lotus.com/ldd/portalwiki.nsf/dx/Global\\_proxy\\_configuration\\_wp7](http://www-10.lotus.com/ldd/portalwiki.nsf/dx/Global_proxy_configuration_wp7).

c. В административной консоли перезапустите приложение **Настройка прокси AJAX**.

3. Зарегистрируйте виджеты Business Space в WebSphere Portal.

Виджеты Business Space регистрируются как виджеты iWidget в WebSphere Portal функцией группового импорта с помощью специально предназначенного для WebSphere Portal файла каталога виджетов, поставляемого вместе с продуктом. Файл XML каталога находится в корневом каталоге файла WAR продукта. Каждый продукт имеет свой корневой контекст.

Существует два типа виджетов: общие виджеты и виджеты конкретного продукта.

Корневой контекст для общих виджетов Business Space - /BusinessSpace, файл каталога - catalog\_commonWidgets\_portal.xml. Пример URL файла XML каталога для общих виджетов Business Space: [http://localhost:9080/BusinessSpace/catalog\\_commonWidgets\\_portal.xml](http://localhost:9080/BusinessSpace/catalog_commonWidgets_portal.xml).

Ниже приведены примеры URL продуктов управления бизнес-процессами:

- IBM Business Monitor: <http://business-space-c-monitor:порт/BusinessDashboard/catalog.xml>
- IBM Business Monitor с IBM Cognos Business Intelligence: <http://business-space-c-monitor:порт/CognosWidgets/catalog.xml>
- Виджеты Управление неавтоматизированными задачами: [http://business-space-c-business-process-manager:порт/ HumanTaskManagementWidgets/portal\\_catalog.xml](http://business-space-c-business-process-manager:порт/HumanTaskManagementWidgets/portal_catalog.xml)

a. Выполните следующую команду в каталоге *профайл-wp*\ConfigEngine, чтобы зарегистрировать виджет iWidget с помощью файла XML catalog продукта:

```
ConfigEngine.[bat|sh] register-iwidget-definition
-DIWidgetCatalog=url-файла-xml-каталога -DWasPassword=пароль
-DWasUserid=ИД -DPortalAdminId=ИД -DPortalAdminPwd=пароль
-DRegistrationAspects=catalogTitlesOverule,considerWidgetParam,considerUniqueName
```

Пример для IBM Business Monitor:

```
ConfigEngine.bat register-iwidget-definition -DIWidgetCatalog=http://
localhost:9080/BusinessDashboard/catalog.xml -DWasPassword=admin
-DWasUserid=admin -DPortalAdminId=admin -DPortalAdminPwd=admin
-DRegistrationAspects=catalogTitlesOverule,considerWidgetParam,considerUniqueName
```

b. Для того чтобы убедиться, что команда выполнена правильно, найдите строку Return Value:0. Дополнительная информация о необязательных командах приведена в документации WebSphere Portal по адресу [http://www-10.lotus.com/ldd/portalwiki.nsf/dx/Task\\_registeriwidgetdefinition\\_wp7](http://www-10.lotus.com/ldd/portalwiki.nsf/dx/Task_registeriwidgetdefinition_wp7).

4. Активируйте пункты меню для виджетов Business Space, чтобы они появились в WebSphere Portal: Справка, Обновить и Отправить виджет. См. инструкции по



адресу [http://www-10.lotus.com/ldd/portalwiki.nsf/dx/Consolidated\\_Steps\\_for\\_Creating\\_Custom\\_Themes\\_in\\_WP7\\_](http://www-10.lotus.com/ldd/portalwiki.nsf/dx/Consolidated_Steps_for_Creating_Custom_Themes_in_WP7_).

- a. Измените свою пользовательскую схему с помощью клиента WebDAV. URL WebDAV: <http://хост-портала:10039/wps/mycontenthandler/dav/fs-type1>.
- b. Перейдите к теме WebSphere Portal, которую требуется обновить. Например, для обновления темы *тема*, перейдите в `/fs-type1/themes/тема/` и найдите файл HTML темы для своей локали. Загрузите его с помощью клиента WebDAV и измените.

- 1) Найдите строку `<a rel="dynamic-content" href="dyn-cs:id:config@tl:oid:csa2.theme"></a>`

- 2) Добавьте после этой строки следующий тег сценария:

```
<script type="text/javascript">
 var com_ibm_bspace_endpoint = com.ibm.mashups.services.ServiceManager.getService
 (com.ibm.mashups.enabler.services.ConfigService.SERVICE_NAME).getConfigObject
 (com.ibm.mashups.enabler.services.ConfigConstants.ENDPOINT_CONFIG_PROVIDER).getValue
 ("{com.ibm.bspace}bSpaceServerRootId.url");
 var bSpaceURL = com.ibm.mm.enabler.utils.URLHelper.rewriteURL
 (com_ibm_bspace_endpoint + "com/ibm/bSpace/common/util/widget/BSpacePortalThemeHelper.js");
 var bSpaceRemoteJS = document.createElement('script');
 bSpaceRemoteJS.setAttribute("type", "text/javascript");
 bSpaceRemoteJS.setAttribute("language", "JavaScript");
 bSpaceRemoteJS.setAttribute("src", bSpaceURL);
 document.getElementsByTagName("head")[0].appendChild(bSpaceRemoteJS);
</script>
```

- 3) Сохраните измененный файл HTML темы с помощью клиента WebDAV.

- c. Откройте файл `widgetActions.json`. Например, для темы *тема*, этот файл находится в каталоге `/fs-type1/themes/тема/menuDefinitions/`.
- d. Добавьте в файл следующие записи и сохраните его в WebSphere Portal с помощью клиента WebDAV. Убедитесь, что порядковый номер в файле уникален.

```
{
 bundlePackage: "com.ibm.bspace.bundles",
 bundleName: "Theme",
 bundleKey: "theme_refresh",
 iconClass: "",
 ordinal: 160,
 enabled: true,
 visibilityFn: confirmBspaceRefreshMenuVisibility,
 actionFn: refreshBSpaceWidgetImpl,
 id: "BspaceWidgetActions:widgetRefresh"
},
{
 bundlePackage: "com.ibm.bspace.bundles",
 bundleName: "Theme",
 bundleKey: "theme_help",
 iconClass: "",
 ordinal: 150,
 enabled: true,
 metadata: {
 mode: com.ibm.mm.iwidget.Constants.mode.HELP
 },
 visibilityFn: confirmBspaceHelpMenuVisibility,
 actionFn: bspaceWidgetHelpMenuImpl,
 id: "BspaceWidgetActions:widgetHelp"
},
{
 bundlePackage: "com.ibm.bspace.bundles",
 bundleName: "Theme",
 bundleKey: "theme_sendWidget_control",
 iconClass: "",
 ordinal: 170,
```



```
enabled: true,
visibilityFn:confirmBspaceSendWidgetVisibility,
actionFn: bspaceWidgetSendWidgetImpl,
id: "BspaceWidgetActions:sendWidget"
},
```

- e. Очистите кэш браузера и перезагрузите виджеты, чтобы появились добавленные пункты меню.

После настройки Business Space на работу с WebSphere Portal, выполните следующие задачи:

- Если IBM Business Monitor используется с IBM Cognos Business Intelligence, необходимо обновить раздел ProxyServlet\_Servlet в файле web.xml. См. документацию IBM Business Monitor.
- Для того чтобы найти и добавить виджет iWidget из Business Space на страницу WebSphere Portal и начать работу в среде WebSphere Portal, выполните следующие действия. Выберите **Действия > Изменить страницу**.
- Для того чтобы включить обмен событиями между виджетами iWidget и стандартными портлетами на одной странице WebSphere Portal и обеспечить сохранение состояния навигации у виджетов при перемещении между страницами, настройте на страницах с виджетами Business Space сборку на стороне клиента. См. документацию WebSphere Portal.

## Настройка SSO и SSL для виджетов WebSphere Portal

Если нужно, чтобы виджеты продукта работали в WebSphere Portal, необходимо настроить единый вход в систему (SSO) между WebSphere Portal и продуктом, содержащим виджеты Business Space; кроме того, должны быть настроены сертификаты SSL для обмена между WebSphere Portal и продуктом, содержащим виджеты Business Space.

Необходимо настроить единый вход в систему (SSO) между серверами WebSphere Portal и продукта, содержащего виджеты Business Space. Кроме того, должно быть настроено соединение SSL между WebSphere Portal и продуктом, содержащим виджеты Business Space. Для этого требуется обмен подписывающими сертификатами SSL между серверами.

На сервере WebSphere Portal и сервере продукта должны использоваться одинаковые имена пользователя и пароли для входа в административную консоль.

1. Настройте единый вход в систему (SSO) между WebSphere Portal и продуктом, содержащим виджеты Business Space.
  - a. Войдите в административную консоль администратора развертывания продукта, содержащего виджеты Business Space.
  - b. Следуйте инструкциям раздела Импорт и экспорт ключей в WebSphere Application Server Information Center.
2. Настройте сертификаты SSL для обмена между сервером WebSphere Portal и сервером продукта, содержащего виджеты Business Space.

Убедитесь, что подписывающие сертификаты для сервера WebSphere Portal и сервера продукта настроены в подходящих хранилищах доверенных сертификатов. См. раздел Защищенный обмен данными с помощью SSL в WebSphere Application Server Information Center.

## Команда `updateEndpointBindingsOnPortal`

Команда `updateEndpointBindingsOnPortal` позволяет создать ссылки на конечные точки на сервере приложений WebSphere Portal, предоставив тем самым участникам коллектива возможность работы с виджетами Business Space на сервере WebSphere Portal.

Эта команда создает на сервере приложений WebSphere Portal ссылки на конечные точки REST. Ссылки на конечные точки Business Space и других продуктов необходимо создать для обеспечения правильной работы Business Space в среде WebSphere Portal. Виджеты Business Space регистрируются на сервере WebSphere Portal в качестве объектов `iWidget` в процессе группового импорта с помощью файла каталога виджетов продукта в формате WebSphere Portal. Файл XML каталога доступен в корневом каталоге файла WAR продукта. Каждый продукт содержит отдельный корневой контекст. Эта команда предназначена только для провайдера среды ресурсов с именем `WP Mashup Endpoints`.

Перед выполнением этой команды необходимо установить WebSphere Portal V7.0.0.1 или более поздней версии, настроить Business Space и службы REST, а также настроить SSL и SSO. Дополнительная информация приведена в разделе Настройка Business Space в WebSphere Portal.

После выполнения команды сохраните изменения в главной конфигурации с помощью одной из следующих команд:

- Для Jython:  
`AdminConfig.save()`
- Для JACL:  
`$AdminConfig save`

### Обязательные параметры

**-serverName** *имя-сервера-WebSphere-Portal*

Параметр, указывающий имя целевого сервера для настройки WebSphere Portal. Для настройки Business Space на сервере необходимо указать как **serverName**, так и **nodeName**.

**-nodeName** *имя-узла-WebSphere-Portal*

Параметр, указывающий имя целевого узла для настройки WebSphere Portal. Для настройки Business Space на сервере необходимо указать как **serverName**, так и **nodeName**.

**-clusterName** *имя-кластера-WebSphere-Portal*

Параметр, указывающий имя целевого кластера для настройки WebSphere Portal. Для настройки Business Space в кластере необходимо указать только параметр **clusterName**. Не указывайте параметр **serverName** или **nodeName**.

**-host** *IP-адрес-или-имя-хоста-сервера-портала*

Параметр, указывающий IP-адрес или имя хоста удаленного сервера WebSphere Portal.

**-port** *порт-SOAP-портала-по-умолчанию-10025*

Параметр, указывающий имя порта SOAP удаленного сервера WebSphere Portal.

**-user** *ИД-администратора-портала*

Параметр, указывающий ИД администратора для удаленного сервера WebSphere Portal.

**-password** *пароль-администратора-портала*

Параметр, указывающий пароль администратора для удаленного сервера WebSphere Portal.

**-endpointBindingDirectoryName** *каталог-с-файлами-конечных-точек*

Параметр, указывающий каталог с файлами конечных точек. Убедитесь, что в этом каталоге отсутствуют другие файлы.

## Примеры

Следующий пример создает ссылки на конечные точки на сервере приложений WebSphere Portal для автономной среды.

- Пример Jython:

```
AdminTask.updateEndpointBindingsOnPortal(['-nodeName имя-узла-портала
-serverName WebSphere_Portal -endpointBindingDirectoryName
каталог-с-файлами-конечных-точек -host IP-адрес-или-имя-хоста-сервера-портала
-port порт-SOAP-портала-по-умолчанию-10025 -user
ИД-администратора-портала -password пароль-администратора-портала'])
```

- Пример Jacl:

```
$AdminTask updateEndpointBindingsOnPortal {-nodeName имя-узла-портала
-serverName WebSphere_Portal -endpointBindingDirectoryName
каталог-с-файлами-конечных-точек -host IP-адрес-или-имя-хоста-сервера-портала
-port порт-SOAP-портала-по-умолчанию-10025 -user
ИД-администратора-портала -password пароль-администратора-портала}
```

Следующий пример создает ссылки на конечные точки на сервере приложений WebSphere Portal для кластерной среды.

- Пример Jython:

```
AdminTask.updateEndpointBindingsOnPortal(['-clusterName
имя-кластера-портала -endpointBindingDirectoryName локальный-каталог-с-файлами-конечных-точек
-host IP-адрес-или-имя-хоста-сервера-портала -port
порт-SOAP-по-умолчанию-8879 -user ИД-администратора-портала -password
пароль-администратора-портала'])
```

- Пример Jacl:

```
$AdminTask updateEndpointBindingsOnPortal {-clusterName
имя-кластера-портала -endpointBindingDirectoryName локальный-каталог-с-файлами-конечных-точек
-host IP-адрес-или-имя-хоста-сервера-портала -port
порт-SOAP-по-умолчанию-8879 -user ИД-администратора-портала -password
пароль-администратора-портала}
```

## Обязательные записи в файле proxy-config.xml для настройки виджетов на сервере WebSphere Portal

Приведены примеры записей в файле proxy-config.xml, необходимых для настройки Proxu Ajax на сервере WebSphere Portal. Для того чтобы разрешить применение удаленных URL на сервер продукта с сервера WebSphere Portal, необходимо настроить Proxu Ajax.

В следующем фрагменте кода XML приведена стратегия Proxu, требуемая для продуктов управления бизнес-процессами. Она необходим для всех удаленных URL, которые планируется открывать с помощью сервера Proxu WebSphere Portal, например, на сервере Business Space или на сервере управления бизнес-процессами. Замените <REMOTE\_BPM\_URL> на удаленный URL, который должен открываться с помощью сервера Proxu WebSphere Portal.

**Совет:** Значение `socket-timeout` по умолчанию: 10 секунд. Business Space использует компонент посредника для подключения к службам передачи репрезентативного состояния (REST). Если службы REST не отвечают, укажите для свойства `socket-timeout` более подходящее значение, например 30 секунд. См. раздел “Изменение параметров тайм-аута для прокси Ajax Business Space” на стр. 244.

Для того чтобы разрешить доступ к нескольким удаленным серверам или URL на уровне сервера Proxu WebSphere Portal, настройте конфигурацию Proxu с помощью записей динамической стратегии. Стратегия Proxu будет зависеть от конкретной среды развертывания. Различные способы настройки Proxu WebSphere Portal рассмотрены в документации по WebSphere Portal.

Файл `proxu-config.xml` расположен в каталоге `каталог-WebSphere-Portal\base\wp.proxu.config\installableApps\wp.proxu.config.ear\wp.proxu.config.war\WEB-INF`.

**Важное замечание:** Обновленный файл `proxu-config.xml` должен быть проверен и утвержден администраторами WebSphere Portal перед применением на сервере WebSphere Portal.

```
<!-- BPM/Business Space proxu policy -->

<proxu:policy url="<REMOTE_BPM_URL>" acf="none">
 <proxu:actions>
 <proxu:method>GET</proxu:method>
 <proxu:method>HEAD</proxu:method>
 <proxu:method>POST</proxu:method>
 <proxu:method>DELETE</proxu:method>
 <proxu:method>PUT</proxu:method>
 </proxu:actions>
 <proxu:cookies>
 <proxu:cookie>LtpaToken</proxu:cookie>
 <proxu:cookie>LtpaToken2</proxu:cookie>
 <proxu:cookie>JSESSIONID</proxu:cookie>
 <proxu:cookie>CRN</proxu:cookie>
 <proxu:cookie>caf</proxu:cookie>
 <proxu:cookie>cam_passport</proxu:cookie>
 <proxu:cookie>cc_session</proxu:cookie>
 <proxu:cookie>userCapabilities</proxu:cookie>
 <proxu:cookie>usersessionid</proxu:cookie>
 </proxu:cookies>
 <proxu:headers>
 <proxu:header>User-Agent</proxu:header>
 <proxu:header>Accept*</proxu:header>
 <proxu:header>Content*</proxu:header>
 <proxu:header>Authorization*</proxu:header>
 <proxu:header>X-Method-Override</proxu:header>
 <proxu:header>Set-Cookie</proxu:header>
 <proxu:header>If-Modified-Since</proxu:header>
 <proxu:header>If-None-Match</proxu:header>
 <proxu:header>X-Server</proxu:header>
 <proxu:header>X-Update-Nonce</proxu:header>
 <proxu:header>X-Requested-With</proxu:header>
 <proxu:header>com.ibm.lotus.openajax.virtualhost</proxu:header>
 <proxu:header>com.ibm.lotus.openajax.virtualport</proxu:header>
 <proxu:header>Slug</proxu:header>
 <proxu:header>SOAPAction</proxu:header>
 </proxu:headers>
</proxu:policy>

<proxu:meta-data>
<proxu:name>forward-http-errors</proxu:name>
<proxu:value>true</proxu:value>
```

```
</proxy:meta-data>
<proxy:meta-data>
<proxy:name>socket-timeout</proxy:name>
<proxy:value>30000</proxy:value>
</proxy:meta-data>
```

---

## Настройка конфигурации мониторинга задачи пользователя

Модель монитора неавтоматизированных задач требуется для просмотра неавтоматизированных задач на сводной панели с помощью виджета Неавтоматизированные задачи IBM Business Monitor. Эти модель и виджет поддерживают только неавтоматизированные задачи, работающие в процессе Business Process Execution Language (BPEL) на сервере IBM Business Process Manager Advanced. Если вы решили не устанавливать модели монитора неавтоматизированных задач при создании профайла, то можно установить и настроить модель монитора неавтоматизированных задач позже из административной консоли.

В этом разделе описывается процедуры установки файла EAR, включения защиты для монитора неавтоматизированных задач на IBM Business Process Manager Advanced и включения событий.

### Установка модели монитора неавтоматизированных задач вручную

Если модель монитора глобальных неавтоматизированных задач не устанавливается во время создания профайла IBM Business Monitor, то это можно сделать позднее. Файл GlobalHTMMAplication.ear уже находится на вашем жестком диске, даже если вы не устанавливали модель монитора неавтоматизированных задач во время создания профайла.

Для установки файла GlobalHTMMAplication.ear, необходимого для работы модели монитора неавтоматизированных задач, выполните следующие действия:

1. В административной консоли выберите **Приложения > Модели монитора**. В таблице будут показаны все установленные модели монитора.
2. Нажмите кнопку **Установить**.
3. Выберите **Локальная файловая система** и нажмите кнопку **Обзор**.
4. Перейдите в папку, содержащую файл .ear: app\_server\_root/installableApps.wbm/monitorModels, выберите GlobalHTMMAplication.ear и нажмите **Открыть**.
5. Включите опцию "Предлагать ввод только необходимой дополнительной информации".
6. Нажмите **Далее** и принимайте все значения по умолчанию, пока не достигнете страницы Сводка.
7. На странице Сводка проверьте правильность указанной информации и нажмите кнопку **Готово**.
8. Необязательно. Нажмите кнопку **Просмотреть изменения** перед сохранением или отменой.
9. Нажмите кнопку **Сохранить**, чтобы сохранить главную конфигурацию и модель.

После установки файла EAR необходимо настроить сводные панели, указав информацию о соединении с Business Process Choreographer. Необходимо также выполнить преобразование ролей для настройки защиты для пользователей модели монитора неавтоматизированных задач.

## Разрешение событий для мониторинга задачи пользователя

После настройки безопасности для отслеживания неавтоматизированных задач появляется возможность для BPEL-объединения задач или оставить события задач по отдельности, используя Integration Designer. Эти задачи затем передаются в IBM Business Process Manager Advanced.

Перед выполнением этой задачи выполните следующие задачи:

- Настройте удаленную CEI в IBM Business Process Manager Advanced, если сервер процессов работает на удаленном сервере
- Настройте защиту IBM Business Process Manager Advanced
- Присвойте пользователям и группам роли системного администратора и системного монитора

Для создания событий включите создание событий на уровне CEI и укажите формат 7.0 в IBM Integration Designer.

**Примечание:** Модель монитора неавтоматизированных задач поддерживает формат 6.0.2.

Следует разрешить создание событий для каждой BPEL задачи пользователя и каждой отдельно стоящей задачи.

За дополнительной информацией о включении создания событий обратитесь к списку связанных задач.

## Настройка соединений Business Space в WebSphere Portal

Необходимо вручную задать информацию о соединениях Business Space для сводной панели WebSphere Portal. Программа установки использует данную информацию для проверки соединения и подтверждения, что IBM Business Process Manager Advanced установлено должным образом для использования параметра отслеживания пользовательской задачи.

Для задания информации о соединениях сводные панели вручную выполните следующее:

1. Войдите в WebSphere Application Server консоль администратора, где IBM Business Monitor установлен сервер.
2. В панели навигации выберите **Серверы > Типы серверов > Веб-серверы > Сервер1**. Отобразится панель Конфигурация.
3. Выбрав опцию Структура сервера, разверните **Java и Управление процессом** и нажмите **Определение процесса**.
4. Выбрав опцию Дополнительные свойства, нажмите **Java Virtual Machine > Общие свойства**.
5. Нажмите **Новое** для создания новых свойств. Отобразится панель Общих свойств.
6. Добавьте следующие свойства и значения:
  - В поле **Название** введите DashboardBPCHost. В поле **Значение** введите имя хоста или IP-адрес Process Server. Выберите **Применить**.
  - В поле **Название** введите DashboardBPCRMIPort. В поле **Значение** введите порт начальной загрузки, например 2813. Выберите **Применить**.
7. Нажмите **ОК** для сохранения новых свойств.



## Настройка соединений для сводных панелей, основанных на портлетах

Необходимо вручную задать информацию о соединениях Business Process Choreographer для сводных панелей, основанных на портлетах. Программа установки использует данную информацию для проверки соединения и подтверждения, что WebSphere Portal установлено должным образом для использования параметра отслеживания пользовательской задачи.

Для задания информации о соединениях вручную для сводных панелей, основанных на портлетах выполните следующее:

1. Войдите в WebSphere Portal административную консоль.
2. В панели навигации выберите **Серверы > Типы серверов > Серверы приложений WebSphere > WebSphere\_Portal**. Будет показана панель Конфигурация.
3. Выбрав опцию Структура сервера, разверните **Java и Управление процессом** и нажмите **Определение процесса**.
4. Выбрав опцию Дополнительные свойства, нажмите **Java Virtual Machine > Общие свойства**.
5. Нажмите **Новое** для создания новых свойств. Отобразится панель Общих свойств.
6. Добавьте следующие свойства и значения:
  - В поле **Название** введите DashboardBPCHost. В поле **Значение** введите имя хоста или IP-адрес Process Server. Выберите **Применить**.
  - В поле **Название** введите DashboardBPCRMIPort. В поле **Значение** введите порт начальной загрузки, например 2813. Выберите **Применить**.
7. Нажмите **ОК** для сохранения новых свойств.

---

## Настройка модели монитора глобальных процессов

Модель монитора глобальных процессов позволяет вам отслеживать любой процесс BPEL и неавтоматизированные задачи без создания модели монитора или выполнения шагов развертывания. Процессы обнаруживаются динамически и отслеживаются на основе выдаваемых ими событий. Собранные данные можно просматривать в Business Space с помощью Экземпляры, KPI и виджетов создания отчетов.

Дополнительную информацию об использовании модели монитора глобального процесса можно найти в разделе Монитор глобальных процессов на веб-сайте Управление бизнес-процессами — Примеры и учебники или в статье developerWorks по ссылке Связанная информация.

## Установка модели монитора глобальных процессов вручную

Если вы решили не устанавливать модель монитора глобальных процессов при создании профайла IBM Business Monitor, то вы сможете установить ее позже, выполнив приведенную ниже процедуру. Файл GlobalProcessMonitorV75.ear копируется на жесткий диск даже в том случае, если модель монитора глобальных процессов не была установлена в ходе создания профайла. Установите этот файл с помощью административной консоли.

Для установки файла GlobalProcessMonitorV75.ear выполните следующие действия:

1. В административной консоли выберите **Приложения > Модели монитора**. В таблице будут показаны все установленные модели монитора.



2. Нажмите кнопку **Установить**.
3. Выберите **Локальная файловая система** и нажмите кнопку **Обзор**.
4. Перейдите в папку, содержащую файл .ear: app\_server\_root/installableApps.wbm/monitorModels, выберите GlobalProcessMonitorV75.ear и нажмите кнопку **Открыть**.
5. Включите опцию "Предлагать ввод только необходимой дополнительной информации".
6. Нажмите **Далее** и принимайте все значения по умолчанию, пока не достигнете страницы Сводка.
7. На странице Сводка проверьте правильность указанной информации и нажмите кнопку **Готово**.
8. Необязательно. Нажмите кнопку **Просмотреть изменения** перед сохранением или отменой.
9. Нажмите кнопку **Сохранить**, чтобы сохранить главную конфигурацию и модель.

Если процессы, которые вы планируете отслеживать, выполняются на том же сервере, то дальнейшая настройка не требуется. В противном случае модель монитора необходимо настроить для получения событий как из удаленного сервера CEI (IBM Business Process Manager) в соответствии с инструкциями из раздела "Настройка способа получения событий", так и из локального сервера CEI (IBM Business Monitor), поскольку модель монитора глобального процесса может отправлять события себе.

## Включение событий в модели монитора глобальных процессов

Для того чтобы включить монитор глобальных процессов для отслеживания процессов и неавтоматизированных задач, необходимо включить создание событий VPEL с помощью Integration Designer. События, которые вы включаете, определяют, каким объемом информации будет располагать IBM Business Monitor после выполнения процессов и неавтоматизированных задач. Создание событий для Business Process Manager включено по умолчанию.

Ниже приведены общие рекомендации по выбору событий VPEL для включения:

- Для каждого процесса, который вы хотите отслеживать, включите все события на уровне процессов. Обычно процесс выдает лишь несколько событий во время выполнения (запуск, завершение, сбой, удаление).
- Включите все события для каждой интересующей вас операции (обычно это операции персонала и активизации).
- Для каждой отслеживаемой операции персонала откройте вкладку Сведения панели Свойства и найдите ссылку на соответствующую неавтоматизированную задачу (если она не существует, создайте ее с помощью кнопки Открыть). Перейдите по ссылке на неавтоматизированную задачу, перейдите на вкладку Монитор событий панели Свойства и включите необходимые события контроля.
- Если вы отслеживаете и процесс, и вызываемый им подпроцесс, то включите все события для связывающей их операции активизации.
- Отключите события коротких автоматизированных шагов.
- Включите все события автономных неавтоматизированных задач, которые вы хотите отслеживать.
- По возможности, включите все события циклов, поскольку это предоставит вам хронологию итераций цикла со значениями системного времени.
- Включите события изменения тех и только тех переменных процесса, которые вы хотите отслеживать.

Дополнительная информация о включении генерирования событий приведена в документации по Integration Designer 7.5. Соответствующая ссылка приведена ниже.

## Настройка сводных панелей для модели монитора глобальных процессов

Монитор глобальных процессов получает события о процессах и неавтоматизированных задачах, выполняющихся в IBM Business Process Manager. Он обнаруживает развернутые определения процессов и задач на основе событий, которые те выдают во время работы, и отслеживает выполняющиеся процессы и задачи. С помощью Экземпляры, KPI и виджетов создания отчетов можно настроить свою сводную панель для этой модели монитора или можно воспользоваться одним из предоставленных бизнес-пространств в качестве отправной точки.

Две конфигурации Business Space предоставляются в следующих расположениях:

- `app_server_root/installableApps.wbm/monitorModels/BusinessSpace/GlobalProcessMonitor_BusinessSpace.zip`
- `app_server_root/installableApps.wbm/monitorModels/BusinessSpace/GlobalProcessMonitor_BusinessSpace_Advanced.zip`

Общая структура этих конфигураций одинакова, но в улучшенной версии показаны дополнительные технические сведения, в частности, значение миллисекунд и часовой пояс в системном времени; идентификаторы экземпляров процессов и задач, хронологии миграции экземпляров процессов и счетчики контрольных событий. Для загрузки предпочитаемой конфигурации воспользуйтесь функцией Импортировать, предоставляемой Business Space. Ей можно воспользоваться "как есть" или взять ее за основу при настройке персонализированных окон сводной панели.

Для начала вам рекомендуется разобраться со структурой контекста монитора следующей модели:

Определение процесса  
    Выполнение процесса  
        Шаг выполнения процесса  
            Выполнение связанной задачи  
            Переменная выполнения процесса  
Определение шага  
    Выполнение шага  
        Выполнение связанной задачи

Определение задачи  
    Выполнение задачи

Существуют дополнительные определения контекста монитора для данных, которые не могут содержаться в показателе и поэтому требуют дочерних контекстов монитора. Их следует рассматривать как контейнеры данных, являющиеся частью их родительского контекста монитора. Они не показаны в приведенной выше структуре, в которой выделена лишь главная структура контекста монитора для данной модели монитора.

Контекст монитора Определение процесса соответствует развернутому шаблону процессов в IBM Business Process Manager. Он отслеживает этот шаблон и предоставляет обзорную информацию о числе запущенных, выполняющихся и завершившихся процессов; минимальном, максимальном и среднем времени выполнения; и т.д. Переходя к контексту монитора Выполнение процесса, вы найдете информацию о конкретном выполняющемся процессе (время запуска, текущее состояние, время завершения и т.п.) Дочерними объектами контекста Выполнение процесса являются контексты монитора для его отдельных шагов (операций,

неавтоматизированных задач и т.д.) и переменных процесса. Для шагов, представляющий собой неавтоматизированные задачи, доступен еще один уровень, на котором показаны связанные выполнения, включая все подзадачи, добавленные во время выполнения.

Кроме того, вы можете перейти от контекста монитора Определение процесса к контексту монитора Определение шага, чтобы просмотреть все известные шаги этого шаблона процесса. (Обнаруживаются только шаги, которые выполнялись хотя бы один раз и отправляли события в IBM Business Monitor.) Продолжив перемещение, вы попадете на уровень Выполнение шага, содержащем ту же информацию, что и уровень Шаг выполнения процесса, но сгруппированную другим способом. Все выполнения заданного определения шага, в отличие от всех шагов, образующих одно выполнение процесса. Для шагов, представляющий собой неавтоматизированные задачи, доступен еще один уровень, на котором показаны связанные выполнения, включая все подзадачи, добавленные во время выполнения.

При настройке сводных панелей - пользовательских или предоставленных - вы можете выбрать показатели, которые должны быть показаны в виджетах. Показатели с префиксом Auh в имени предназначены только для внутренней обработки; добавлять их в сводную панель не следует.



---

## Глава 11. Установка демонстрационной модели

Версия IBM Business Monitor, предназначенная для одного сервера, поставляется с примером модели ипотечного кредитования, который иллюстрирует некоторые функциональные возможности IBM Business Monitor. Если вы создали автономный профайл, то вы можете установить демонстрационную модель Наилучший кредитор с помощью консоли Первые шаги.

Демонстрационная модель Better Lender расположена в следующем каталоге:

```
app_server_root/installableApps.wbm/samples/mortgageLending/
app_server_root\installableApps.wbm\samples\mortgageLending\
```

Имя модели: MortgageLendingBAMApplication.ear.

Если автономный профайл создан, то выберите один из следующих методов.

- (Не для z/OS:) Установите демонстрационную модель с помощью консоли Первые шаги.

1. Откройте консоль Первые шаги из автономного профайла с помощью одной из следующих опций:
  - На панели Создание профайла закончено выберите опцию **Запустить Первые шаги в IBM Business Monitor**.
  - Выберите **Пуск > Все программы > IBM > Business Monitor 7.5 > Профайлы > имя-профайла > Первые шаги**.
  - Перейдите к файлу profile\_root\firststeps.wbm и запустите команду firststeps.bat.

**Важное замечание:** Для установки или выполнения консоли Первые шаги в Windows 7, Windows Vista или Windows Server 2008, необходимо повысить права доступа учетной записи пользователя Microsoft Windows, щелкнув правой кнопкой мыши на файле firststeps.bat и выбрав опцию **Запуск от имени администратора**. Это требуется как для административных, так и для других пользователей.

- Откройте командное окно. Перейдите к файлу profile\_root/firststeps.wbm и выполните команду firststeps.sh.
2. В консоли Первые шаги выберите **Демонстрационная модель**.

**Примечание:** Если включена защита, будет выдан запрос на ввод ИД и пароля пользователя WebSphere Application Server.

- Установите демонстрационную модель с помощью административной консоли. Выберите **Приложения > Модели монитора**. Выберите **Установить** и перейдите к файлу MortgageLendingBAMApplication.ear. Для установки используйте параметры по умолчанию.

После завершения установки запустите сервер, а затем откройте Business Space для просмотра пространства Наилучший кредитор. (В консоли Первые шаги имеются опции для запуска сервера и запуска Business Space.)



---

## Глава 12. Удаление IBM Business Monitor из системы

Можно удалить IBM Business Monitor с помощью опции удаления из системы в Администраторе установки.

---

### Удаление IBM Business Monitor из системы

В программе Installation Manager предусмотрена опция Удалить, позволяющая удалить пакеты из отдельного установочного расположения. Можно также удалить все установленные пакеты из каждого установочного каталога.

Для того чтобы удалить из системы пакеты, необходимо войти в систему с помощью той же учетной записи пользователя, которая использовалась для установки пакетов продукта. Пакет не может быть удален, когда другой пакет имеет зависимость от него, если зависимый пакет не выбран также для удаления из системы.

1. Закройте программы, установленные с помощью Администратора установки.
2. Остановите все работающие серверы.
3. Запустите Installation Manager. На начальной странице выберите **Удаление из системы**.  В Windows также можно выбрать **Пуск > Программы > IBM > IBM Business Monitor > Удалить из системы**.
4. На странице Удалить пакеты выберите IBM Business Monitor и связанные пакеты и нажмите **Далее**.  Если на предыдущем шаге было выбрано **Пуск > Программы > IBM > IBM Business Monitor > Удалить из системы**, IBM Business Monitor будет уже выбран для удаления на странице Удалить пакеты.
5. На странице Общая информация просмотрите список пакетов, которые будут удалены из системы и затем нажмите **Удалить из системы**. После завершения удаления из системы откроется страница Завершение.
6. Нажмите **Готово**, чтобы выйти из мастера.

При удалении IBM Business Monitor вместе с ним будут удалены все профайлы, добавленные в IBM Business Monitor, включая все профайлы WebSphere Application Server, добавленные в IBM Business Monitor. Для автономных профайлов сервера монитора служба IBM Cognos BI удаляется.

Примеры моделей монитора не удаляются из системы для обеспечения сохранения настроек моделей. Для удаления этих моделей из системы обратитесь к разделу Удаление моделей монитора и данных.

#### Linux

Если предполагается повторная установка IBM Business Monitor, необходимо удалить оставшиеся записи DB2 Express в файле `/etc/service`. Это необходимо, поскольку для новой установки порт 50000 должен быть свободен. Найдите файл `/etc/service` и удалите все упоминания DB2 Express и порта 50000. Пример:

```
db2c_bpminst 50000/tcp
```

или

```
db2c_db2inst1 50000/tcp
```



---

## Удаление демонстрационной модели

IBM Business Monitor поставляется с примером модели ипотечного кредитования, который иллюстрирует некоторые функциональные возможности IBM Business Monitor. Эту модель можно установить с помощью программы Первые шаги.

Для того, чтобы удалить демонстрационную модель:

1. Удалите сводную панель Наилучший кредитор с помощью Администратора бизнес-пространства.
2. Удалите шаблоны предупреждений с помощью административной консоли WebSphere Application Server.
3. Если включена защита, удалите роль пользователя в административной консоли WebSphere Application Server.
4. Удалите модель с помощью административной консоли WebSphere Application Server.





Напечатано в Дании