РЕД База Данных

Версия 5

Быстрый старт

Содержание

Глава 1

Введение

Данное руководство представляет собой краткое введение в основы СУБД РЕД База Данных. Оно рассчитано на пользователей, которые впервые приступают к работе с СУБД. Настоящий документ поможет быстро начать работать с СУБД, создать свою первую базу данных и управлять ею. Для более детального ознакомления с СУБД обращайтесь к Руководству администратора, описывающему все инструменты и технологии для построения и эффективного управления базами данных РЕД Базы Данных.

Глава 2

Установка РЕД Базы Данных 5

Сервер РЕД Базы Данных и любые созданные вами базы данных должны находиться на жестком диске, физически подключенном к компьютеру (на котором работает сервер). Вы не можете располагать сервер, какие либо его компоненты или какую-либо базу данных на подключенном (`mapped`) диске, разделяемом (`share`) диске или сетевой файловой системе.

Вы можете смонтировать базу данных в режиме `read-only` с `CD-ROM`, но вы не можете запустить сервер РЕД Базы Данных с него.

2.1 Установочные наборы

Скачать СУБД РЕД База Данных можно на официальном сайте.

2.2 Установка сервера РЕД Базы Данных

> Инструкцию по переходу с РЕД Базы Данных 3 на РЕД Базу Данных 5 см. в главе 2 "Миграции" Руководства администратора.

2.3 Установочные диски

Сервер РЕД Базы Данных и все базы данных, которые вы создаете или к которым подключаетесь, должны находиться на жестком диске, физически подключенном к хост-машине. Не стоит размещать компоненты сервера или базы данных на отображаемом диске, общем файловом ресурсе или сетевой файловой системе.

Вы можете открыть базу данных только для чтения (`read-only`) с носителя только для чтения, например с `DVD`, но вы не можете запустить с него сервер РЕД Базы Данных.

2.4 Установочный скрипт или программа

Хотя РЕД Базу Данных можно установить копированием или распаковкой её файлов из архива, настоятельно рекомендуется использовать распространяемый инсталлятор (`.exe` для `Windows`, `.bin` для `Linux`), особенно если вы устанавливаете РЕД Базу Данных в первый раз. Исполняемый файл установки для `Windows` и сценарий для различных `POSIX-платформ` выполняют некоторые важные задачи по установке. При условии, что вы следуете инструкциям по установке, по завершении установки вам ничего не нужно будет делать, кроме как войти в систему и начать работу.

2.5 Архитектура сервера

Во время инсталляции Вам будет предложено выбрать архитектуру сервера: `Classic`, `SuperClassic` или `SuperServer`:

- `Classic`
  - использует отдельный процесс на каждое пользовательское соединение;
  - каждый процесс содержит в себе все что нужно для работы с базой данных: область памяти для метаданных, кэш данных для минимизации повторных чтений из файла БД; память для сортировок;

  - если происходит сбой, другие соединения остаются работоспособными;
  - поддержка мультипроцессорности: в многопроцессорных системах ОС автоматически распределяет процессы по процессорам/ядрам.
- `Superserver`
  - один процесс с общей областью памяти для всех пользовательских соединений;
  - поддержка мультипроцессорности: параллельные запросы пользователей выполняются на разных ядрах;
  - возможный сбой в одном процессе разорвет все подключения;
- `SuperClassic`
  - единый процесс на всех пользователей с общей памятью под сортировки;
  - используется пул потоков ОС для обработки запросов от соединений, таким образом каждое соединение работает в отдельном потоке управляемом ОС, а неактивные соединения не отъедают ресурсы потоков;
  - каждый поток со своим кэшем данных и областью метаданных;
  - поддержка мультипроцессорности: потоки ОС легко распараллеливаются;
  - возможный сбой в одном процессе разорвет все подключения.

Каждый из режимов стабилен, и нет причин полностью отдавать предпочтение какому то одному. Конечно, у вас могут быть свои собственные конкретные соображения. Если Вы сомневаетесь, просто следуйте за установкой по умолчанию. Позже вы можете изменить архитектуру через файл конфигурации `firebird.conf` (параметр `ServerMode`), что потребует перезагрузки, но не переустановки. Режим сервера может быть даже настроен для каждой базы данных.

2.6 Установка на Windows

Запустите установку СУБД «РЕД База Данных» с помощью файла `Red Database-SE-5.x.x.xx-windows-xxxx.exe`, определив разрядность используемой операционной системы.

Инсталляция РЕД Базы Данных осуществляется с помощью стандартного мастера установки программ. В ходе установки мастер собирает всю необходимую для установки сервера информацию, производит копирование файлов и регистрацию программных модулей в реестре `Windows`.

> Для установки РЕД Базы Данных 5 необходимы права администратора.

Выберите язык установки. Предусмотрена установка на русском и английском языках.

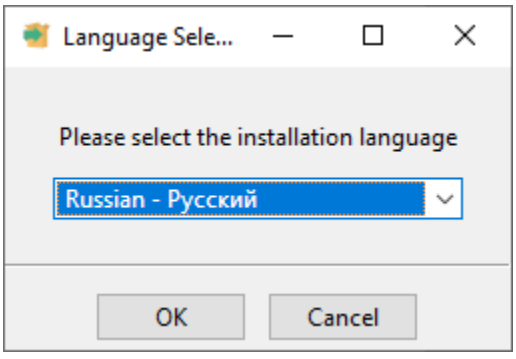


Рисунок 2.1 — Выбор языка

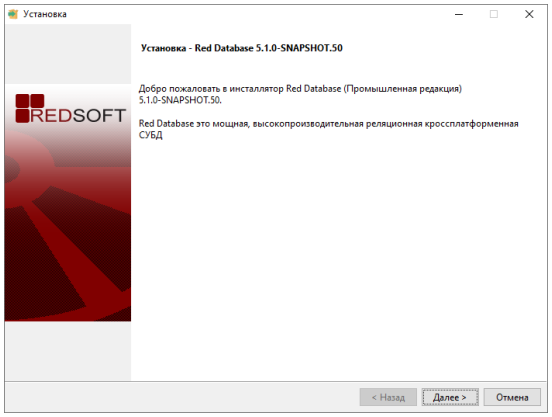


Рис. 2.2 — Приветственное окно установки

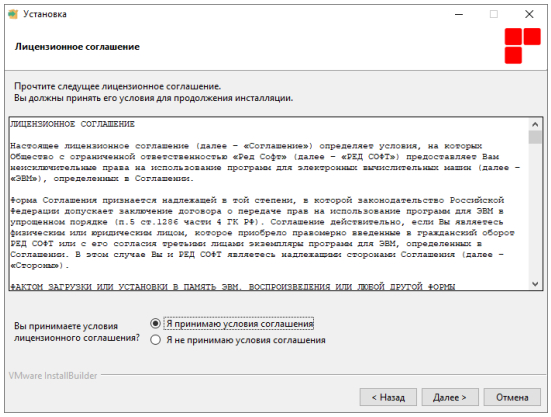
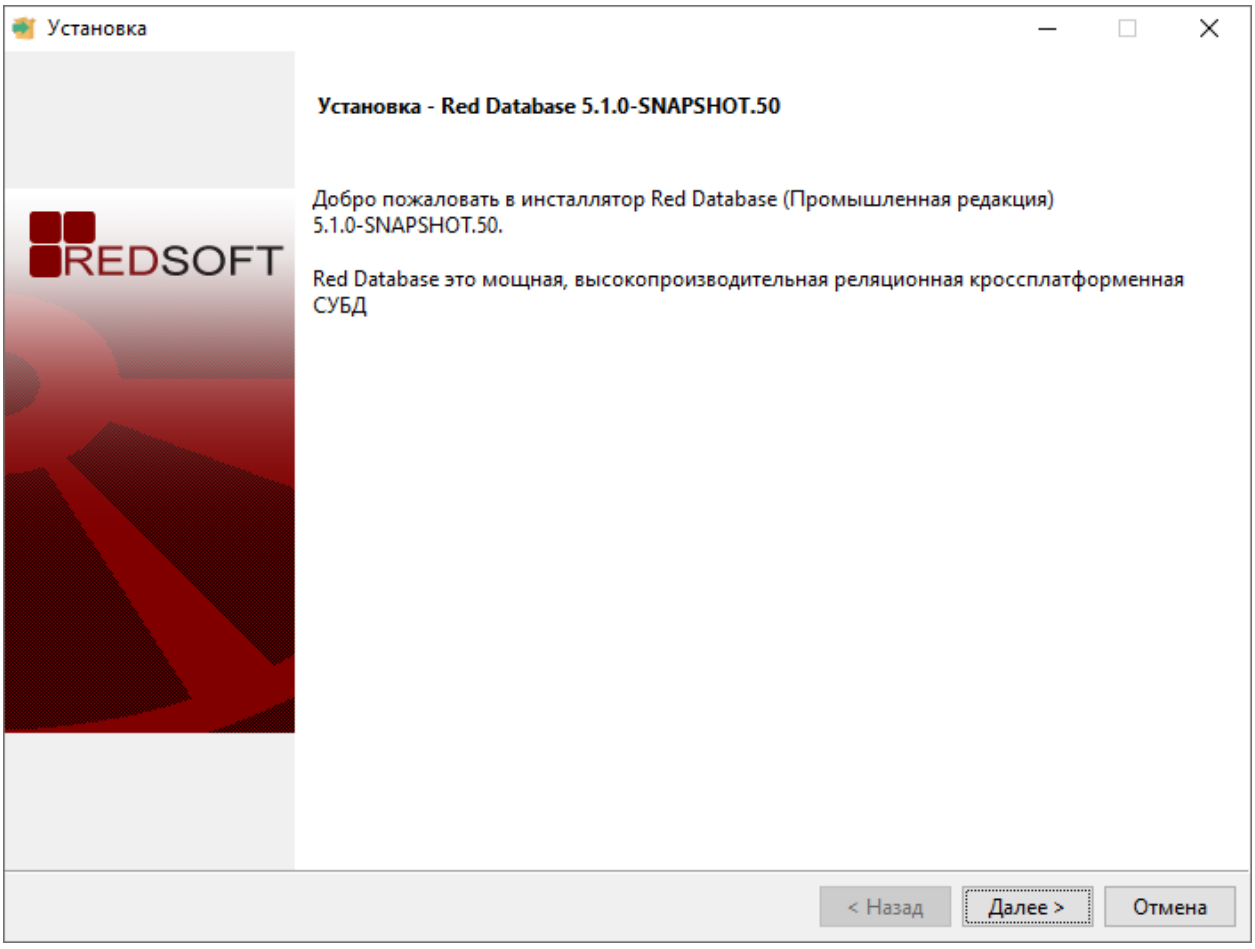
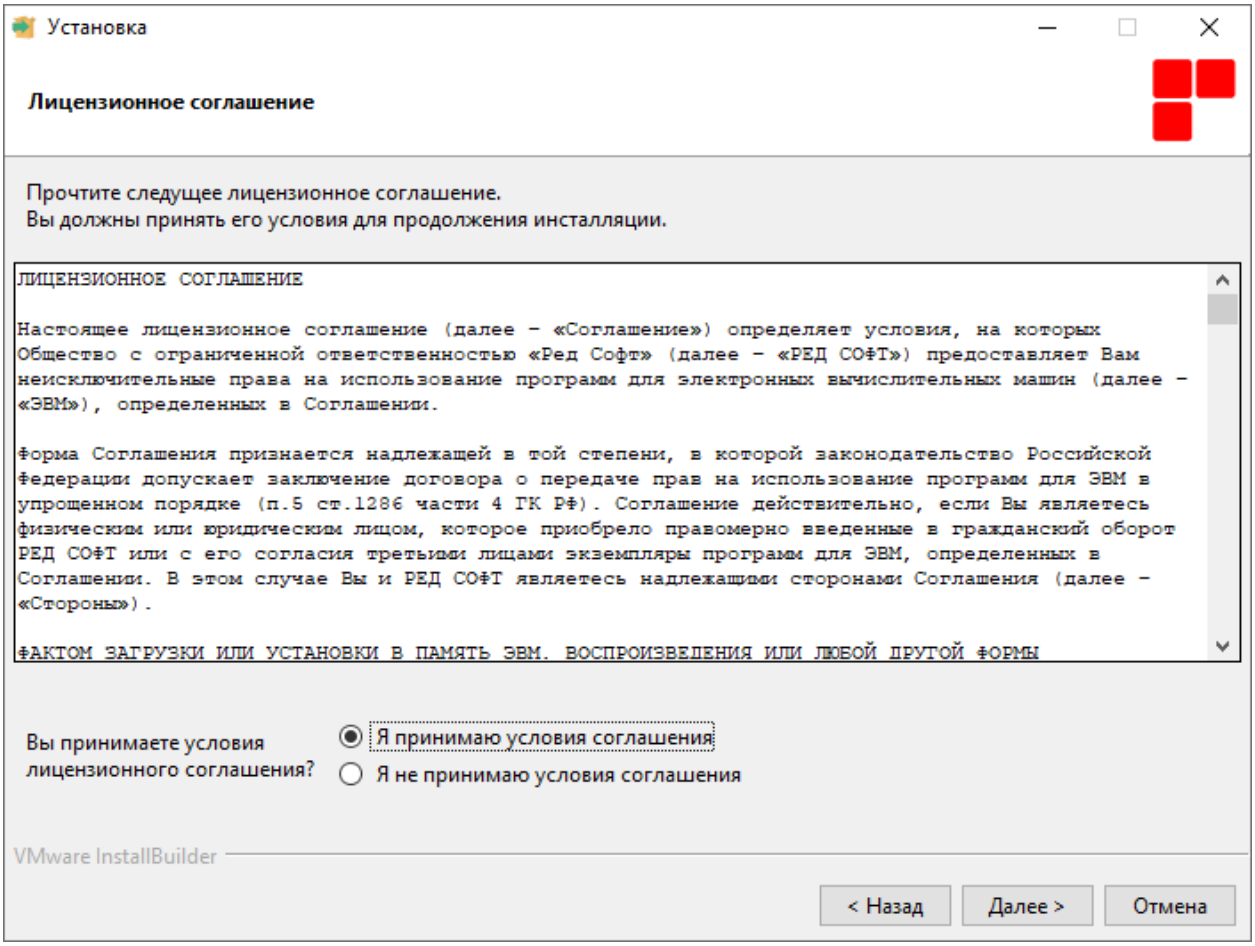


Рис. 2.3 — Лицензионное соглашение





Выберите архитектуру сервера:

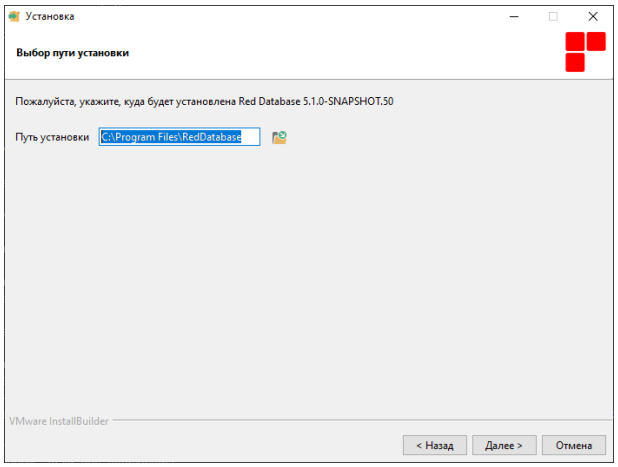


Рис. 2.4 — Выбор каталога установки

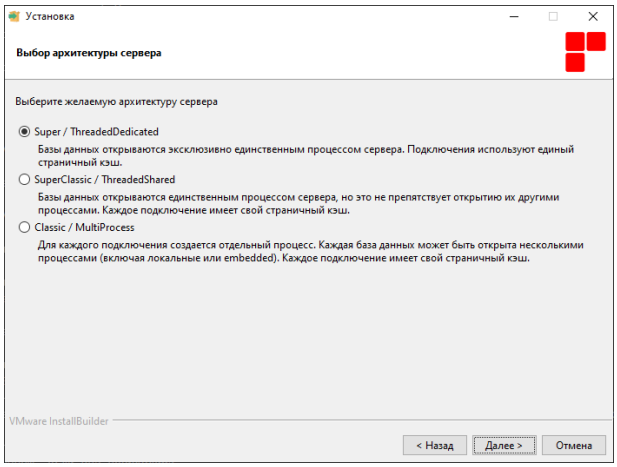
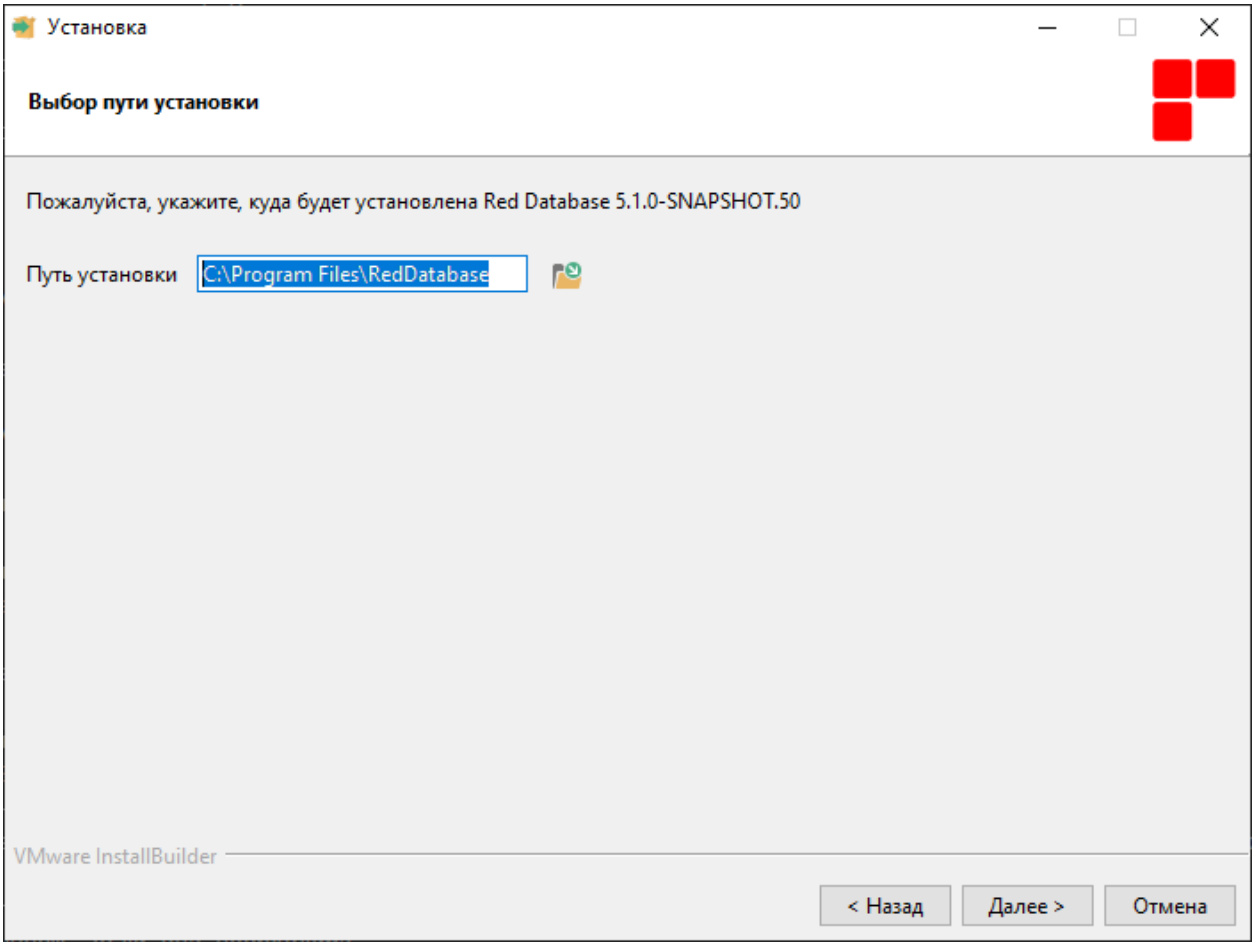
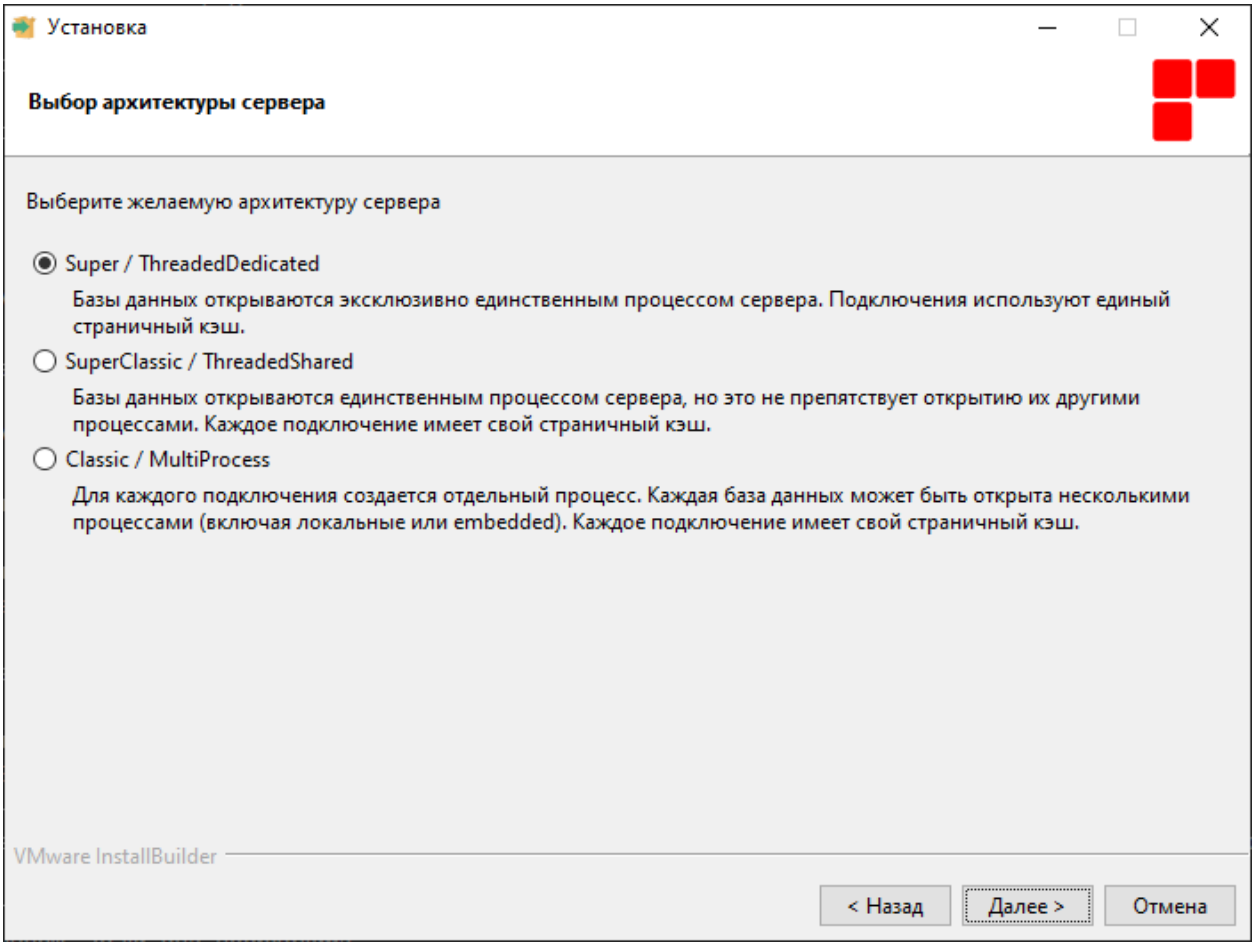


Рис. 2.5 — Выбор архитектуры сервера


Установка
Выбор пути установки
Пожалуйста, укажите, куда будет установлена Red Database 5.1.0-SNAPSHOT.50
Путь установки
C:\Program Files\RedDatabase
VMware InstallBuilder
< Назад
Далее >
Отмена



Изначально в системе существует только один пользователь – администратор сервера `SYSDBA`. Этот пользователь обладает полными правами на выполнение всех функций по управлению работой сервера и работе с базами данных. В процессе инсталляции Вас попросят указать пароль данного пользователя.

Длина пароля может достигать 255 байт, но из-за особенностей алгоритма хеширования, используемого плагинами `Srp`, "эффективная длина" составляет около 20 байт, поэтому вводить пароль длиннее этого значения бесполезно. Заметьте, что если вы введете такой пароль, то при каждом подключении вы должны вводить его в полном объеме - он не сработает, если обрежете его до первых 20 символов.

Мастер установки не предлагает включить традиционную аутентификацию (`Legacy_Auth`). Придется настраивать ее вручную, если она необходима. Если вас беспокоит безопасность, то не следует использовать плагин аутентификации `Legacy_Auth` или включить его временно, пока обновляете существующих клиентов до РЕД Базы Данных 5. Традиционный метод соединения отправляет пароли по сети в незашифрованном виде, не поддерживает протокол шифрования, а также ограничивает полезную длину пароля до 8 байт.

По окончанию процесса установки будет запущен серверный процесс `rdbserver`, который будет запускаться автоматически при перезагрузке сервера. Сервер будет работать как системная служба.

Сервер может работать и в качестве приложения (это менее предпочтительный вариант). Для запуска используйте следующую команду:

```
rdbserver -a
```

Исполняемый файл rdbserver.exe расположен в корневом каталоге установки РЕД Базы Данных.

Остановка выполняется через иконку в системном трее (`Shutdown`).

На официальном сайте можно загрузить исходные коды сервера. Эти исходные коды можно впоследствии использовать для ручной сборки и компиляции бинарных файлов сервера с помощью команды:

```
builds\win32\run_all.bat
```

2.7 Установка на Linux и Unix-подобных системах

2.7.1 Установка в графическом режиме

Файлы РЕД Базы Данных 5 поставляются в виде бинарного пакета. При запуске его из любой графической системы (например, `KDE`) будет вызван мастер установки, который произведет сбор всей необходимой информации и установит СУБД РЕД База Данных 5.

Для установки СУБД РЕД База Данных необходимо скопировать дистрибутивный файл `RedDatabase-5.X.X.X-X-linux-X.bin` на жесткий диск, а в операционной системе назначить в правах этого файла разрешение на исполнение:

```
# chmod +x RedDatabase-5.X.X.X-X-linux-X.bin
```

После этого запустить установку РЕД Базы Данных:

```
# ./RedDatabase-5.X.X.X-X-linux-X.bin
```

Для установки сервера РЕД Базы Данных 5 необходимы права суперпользователя (`root`).

Инсталляция РЕД Базы Данных осуществляется с помощью стандартного мастера установки программ. Прежде всего предлагается выбрать язык установки. Предусмотрена инсталляция на русском и английском языках.

class
: borderless

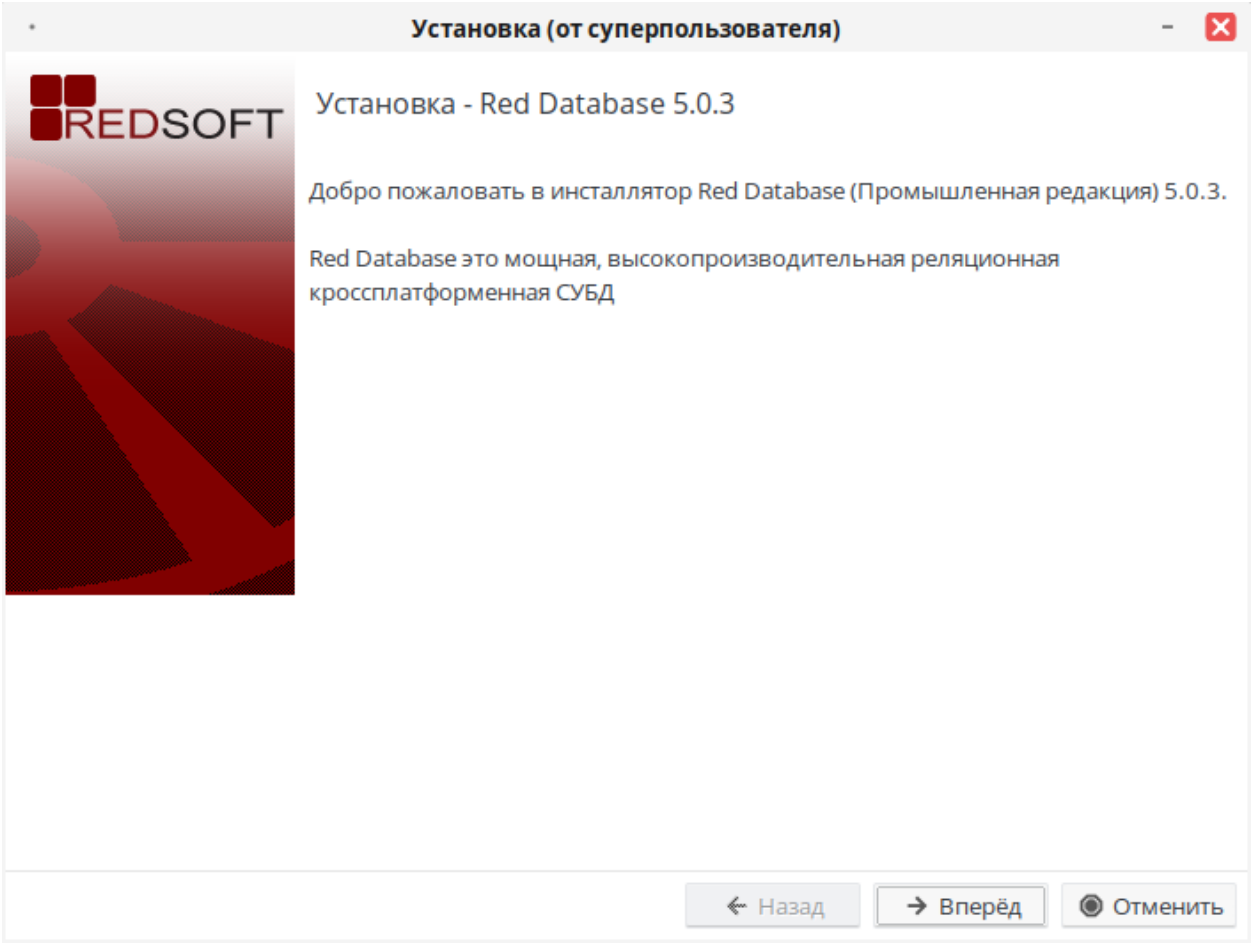


Рисунок 2.6 — Приветственное окно установки

- –

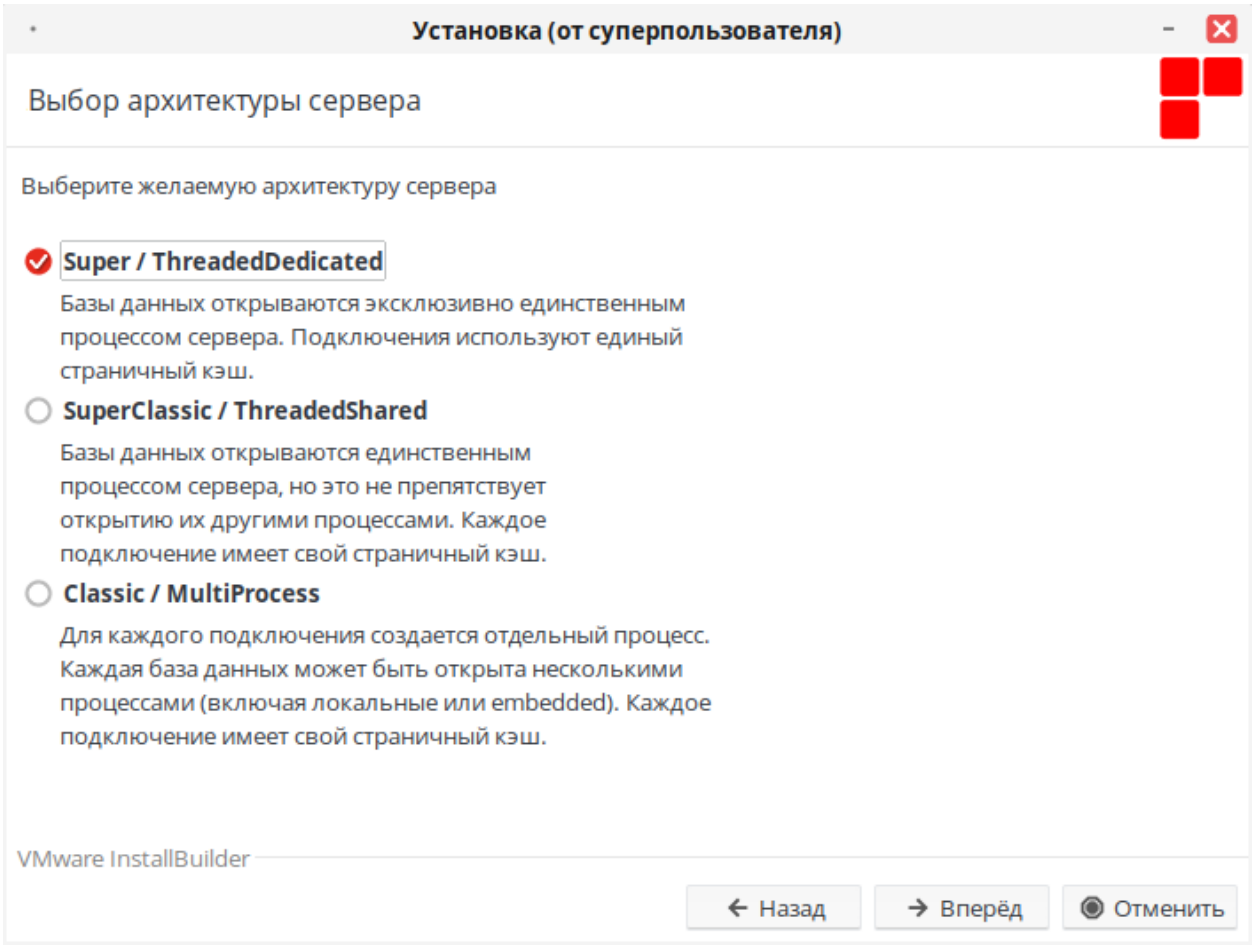
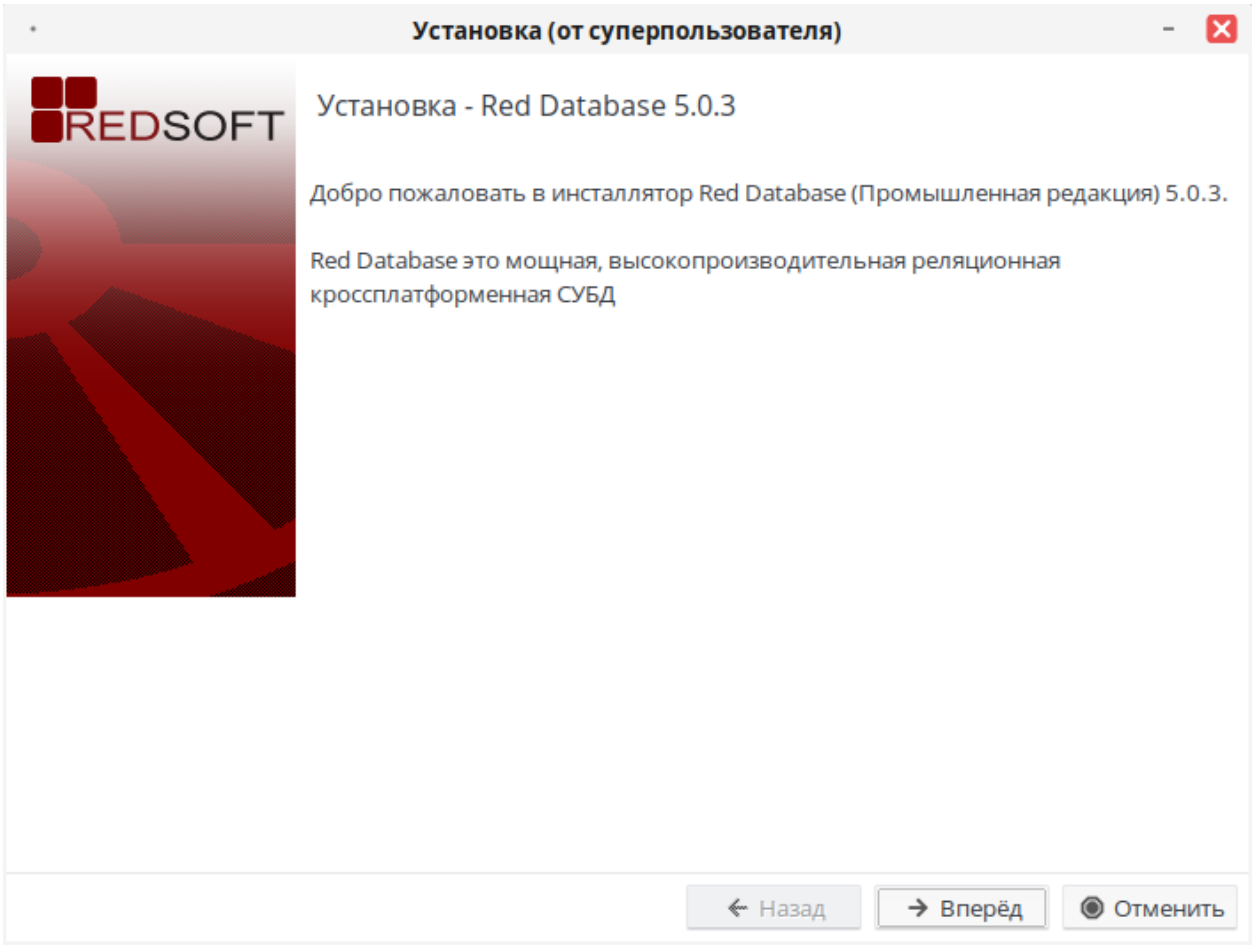
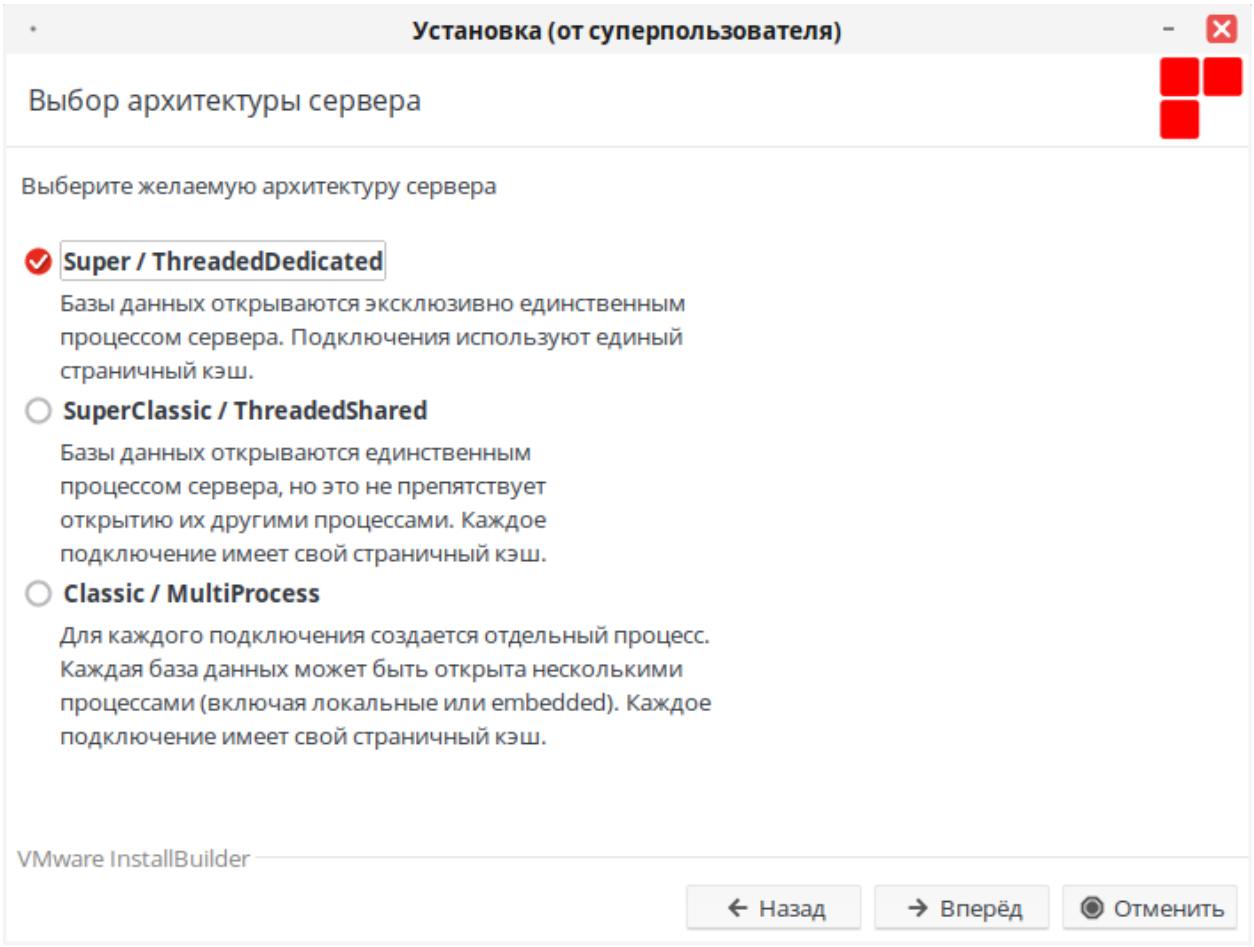


Рисунок 2.7 — Выбор архитектуры сервера

–


Установка (от суперпользователя)
REDSOFT
Установка - Red Database 5.0.3
Добро пожаловать в инсталлятор Red Database (Промышленная редакция) 5.0.3.
Red Database это мощная, высокопроизводительная реляционная кроссплатформенная СУБД
Назад
Вперёд
Отменить



Во время инсталляции необходимо выбрать архитектуру сервера: `Classic`, `SuperClassic` или `SuperServer`. Подробнее о каждой архитектуре было описано *выше*.

Изначально в системе существует только один пользователь - администратор сервера `SYSDBA`. Этот пользователь обладает полными правами на выполнение всех функций по управлению работой сервера и работе с базами данных. В процессе инсталляции нужно указать пароль данного пользователя.

class
: borderless

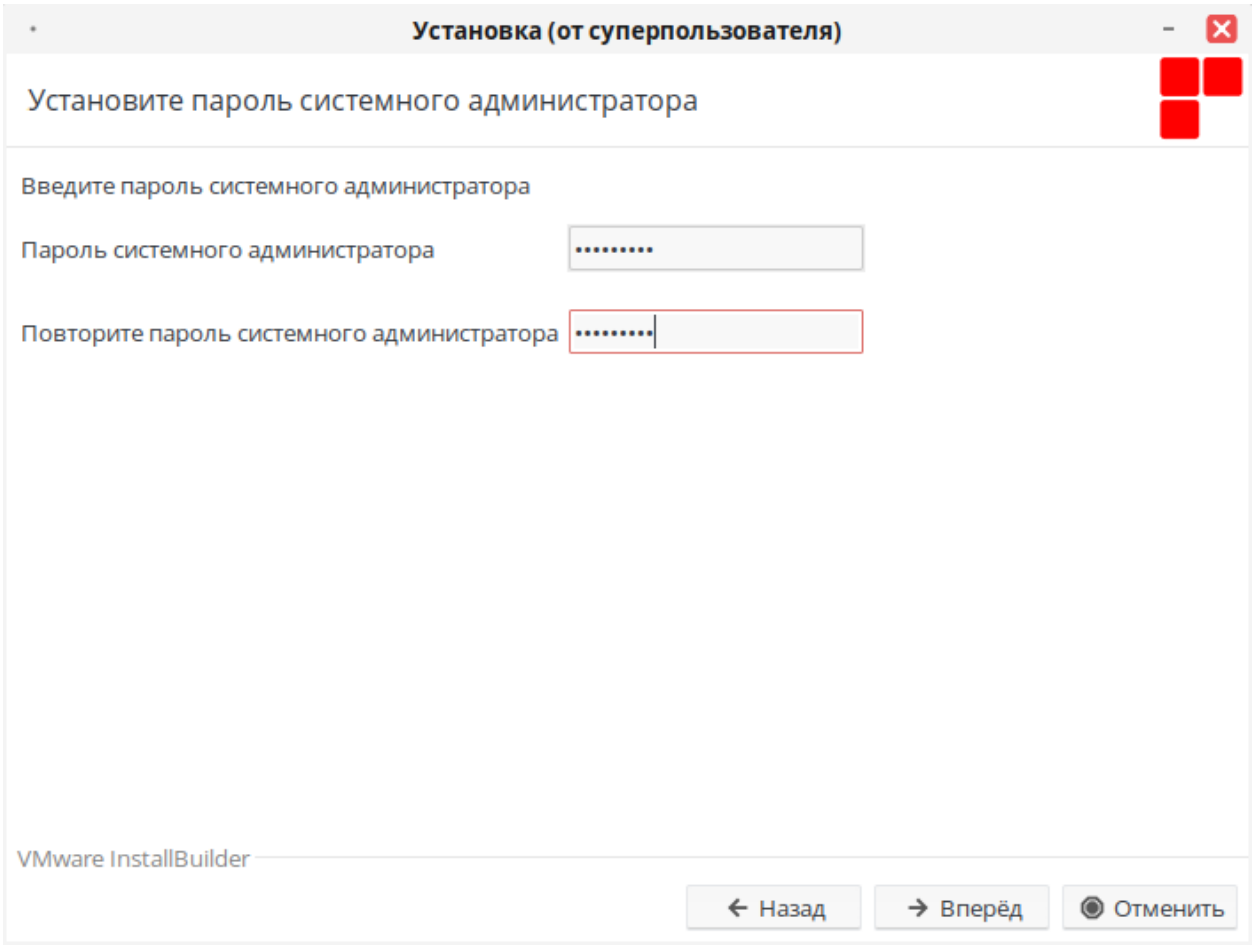


Рисунок 2.8 — Установка пароля

- –

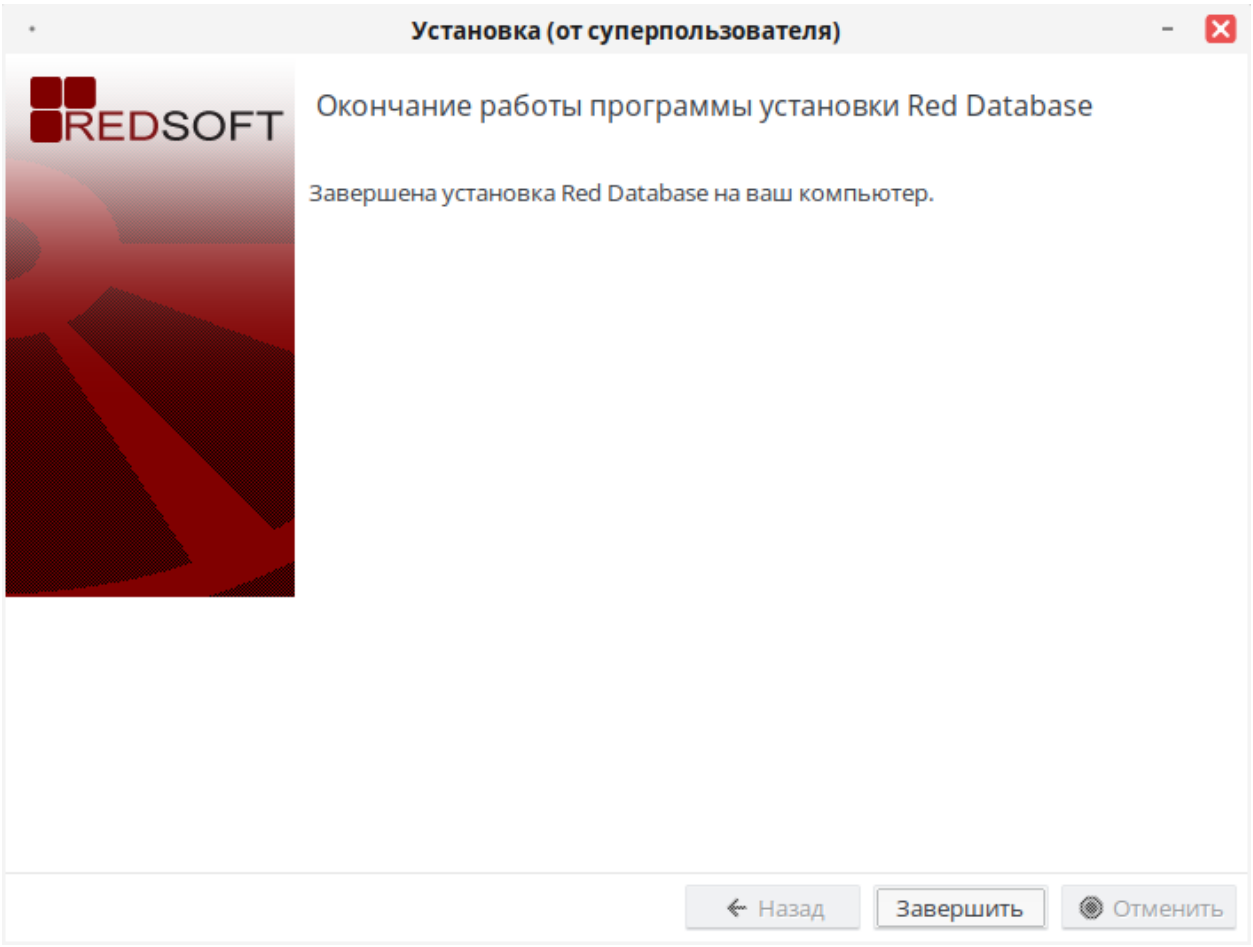
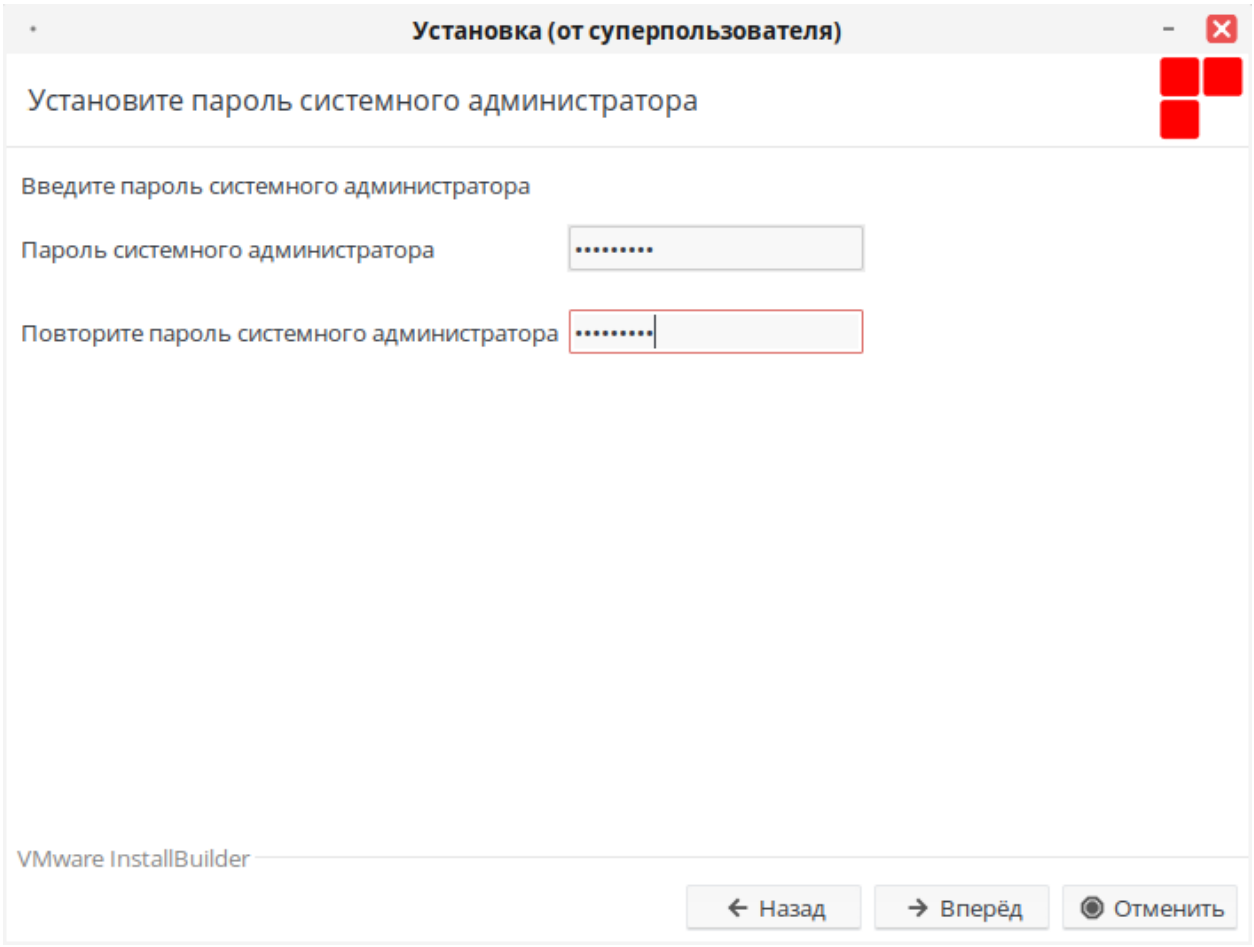
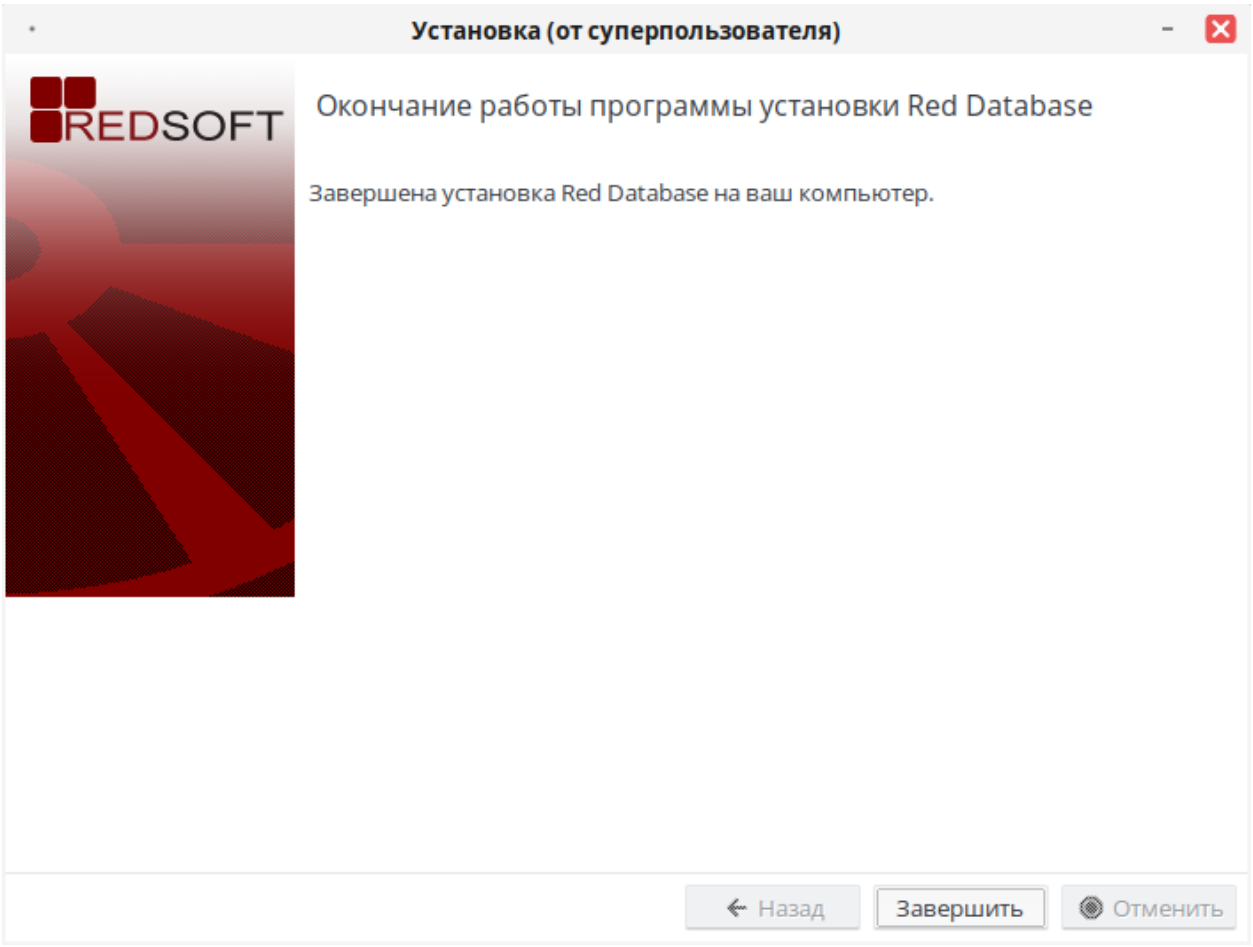


Рисунок 2.9 — Завершение установки

–


Установка (от суперпользователя)
Установите пароль системного администратора
Введите пароль системного администратора
Пароль системного администратора
Повторите пароль системного администратора
VMware InstallBuilder
Назад
Вперёд
Отменить



После установки сервер автоматически не запускается. Нужно сделать это вручную в зависимости от типа системы `Linux` и вашего установочного пакета. Управление запуском и остановкой сервера осуществляет демон инициализации `systemd`:

```
systemctl start firebird
systemctl stop firebird
```

или `init` скрипт:

```
/etc/init.d/firebird start
/etc/init.d/firebird stop
```

2.7.2 Установка в текстовом режиме

Для инсталяции в текстовом режиме необходимо запустить установку с ключом `--mode text`:

```
# ./RedDatabase-5.X.X.X-X-linux-X.bin --mode text
```

В таком режиме программа установки будет выводить запросы на подтверждение тех или иных параметров установки, таких как выбор компонентов или пароль пользователя `SYSDBA`. В случае, если на тот или иной запрос мастера установки предусмотрен ответ по умолчанию, то такой вариант обозна-

чен заглавной буквой, и в этом случае этот вариант можно подтвердить нажатием клавиши «Ввод», в случае, если значение по умолчанию не предусмотрено, то необходимо обязательно ответить на вопрос «Да» (Y) или «Нет» (N).

2.8 Установка отладочных символов

1. Скачайте архив с отладочными символами на официальном сайте. Версия отладочных символов должна совпадать с версией установленной РЕД Базы Данных. Загрузка доступна только авторизованному пользователю.
2. Распакуйте содержимое архива в папку /opt/RedDatabase:

```
tar -xvf RedDatabase-5.X.X.X-X-dbg-linux-X.tar.gz -strip-components 1
```

2.9 Установка только клиентской части

На каждой машине удаленного клиента должна быть установлена клиентская библиотека - libfbclient.so для POSIX-клиентов, fbclient.dll для Windows-клиентов, соответствующая версии сервера РЕД Базы Данных.

Дистрибутивы РЕД Базы Данных не предлагают опции по установке только клиентской части. В общем случае, когда нужно обеспечить взаимодействие клиента с Posix-сервером или другим компьютером под Windows, необходимо взять необходимые файлы из архива bin/linux/x86_64/RedDatabase-SE-5.x.x.xx-linux-X.tar.gz или bin/windows/x86_64/RedDatabase-SE-5.x.x.xx.

2.9.1 Для Windows

Скопируйте из zip-архива в отдельную директорию следующие файлы:

- Утилиту для регистрации клиента instclient.exe;
- Клиентскую библиотеку fbclient.dll;
- Папку plugins;
- Файл с сообщениями сервера firebird.msg;
- Файл конфигурации firebird.conf;
- Все dll-файлы, лежащие в корневом каталоге;
- Необходимые инструменты командной строки для работы с базой данных, например, isql.

Затем запустите скрипт регистрации клиента instclient, который скопирует все нужные файлы в каталог System32 и сделает необходимые записи в реестре:

```
instclient.exe install fbclient
```

2.9.2 Для Linux и других Posix-клиентов

Для выполнения установки необходимо войти в систему с правами администратора (root). Для большинства дистрибутивов Linux предлагается следующая процедура ручной установки клиента РЕД Базы Данных:

1. Скопируйте каталог /lib из tar.gz-архива в каталог /opt/RedDatabase на клиенте;
2. Создайте символические ссылки, выполнив следующие команды:

```
ln -s /opt/RedDatabase/lib/libfbclient.so.5.0.n /usr/lib/libfbclient.
so
ln -s /opt/RedDatabase/lib/libtommath.so.0.0.m /usr/lib/libtommath.so
```

Если используете программы, требующие наличия устаревших библиотек, создайте дополнительно следующие символические ссылки:

```
ln -s /opt/RedDatabase/lib/libfbclient.so.5.0.n /usr/lib/libgds.so.0
ln -s /opt/RedDatabase/lib/libfbclient.so.5.0.n /usr/lib/libgds.so
```

3. Скопируйте папку `plugins`, файл `firebird.msg` и файл конфигурации `firebird.conf` из `tar.gz-архива` в каталог `/opt/RedDatabase на клиенте`;
4. Скопируйте необходимые инструменты командной строки для работы с базой данных. Например, `isql`.

2.10 Процедуры после установки

После установки необходимо настроить политику безопасности по умолчанию, выполнив следующую команду:

```
ALTER POLICY "DEFAULT" AS
        PSWD_MIN_LEN = 8,
        PSWD_NEED_DIFF_CASE = true,
        PSWD_NEED_CHAR = 5,
        PSWD_NEED_DIGIT = 2,
        MAX_FAILED_COUNT = 4;
```

Политика безопасности по умолчанию:

- Длина пароля не менее 8 символов;
- Пароль должен содержать символы в разных регистрах;
- Пароль должен содержать минимум 5 букв;
- Пароль должен содержать минимум 2 цифры;
- Максимальное количество неуспешных попыток аутентификации до блокировки равно 4.

Для включения политик в конфигурационном файле `firebird.conf` укажите плагин `Policy` в параметре `PolicyPlugin`:

```
PolicyPlugin = Policy
```

Для обеспечения контроля целостности выполните следующее:

1. Добавьте в секцию `Service` файла `/lib/systemd/system/firebird.service` проверку целостности процедур:

```
ExecStartPost=sh -c'LD_PRELOAD=""/opt/RedDatabase/bin/mint -M check -d
<путь к файлу базы данных> -o procedures -u sysdba -p masterkey -C
<алиас>-R 80 -i <путь к файлу сохранения> -I AT_SIGNATURE|| true'
```

Загрузите изменения службы:

```
systemctl daemon-reload
```

2. Создайте задачу cron, которая будет выполнять проверку целостности каждые 12 часов:

```
crontab -e

0 */12 * * * /opt/RedDatabase/bin/mint -M check -d <путь к файлу базы
данных>
-o procedures -u sysdba -p masterkey -C "CN_cert,CN_issuer,CN_serial"
-R 80 -I AT_SIGNATURE -i <путь к файлу сохранения>
```

Для настройки регистрации событий безопасности в `firebird.conf` необходимо указать параметр `AuditTraceConfigFiles = fbtrace_sec.conf`:

```
AuditTraceConfigFiles = fbtrace_sec.conf;
```

2.11 Проверка работы сервера

На данном этапе предполагается, что вы будете использовать сетевой протокол `TCP/IP` для соединения клиента и сервера.

2.11.1 Шаг 1. Опросите сервер

Опросите (пропингуйте) сервер. Эта процедура позволит убедиться, что клиентская машина в состоянии видеть (на уровне сети) сервер:

```
ping <ip-адрес сервера>
```

Также можно пинговать сервер по его имени, если оно известно:

```
ping <имя сервера>
```

Обратите внимание, что если Вы соединяетесь с сервером локальным клиентом, т.е. клиент работает на том же компьютере, что и сервер, то можно воспользоваться loopback-интерфейсом:

```
ping localhost
или
ping 127.0.0.1
```

Убедившись, что сервер доступен с клиента, можно переходить к следующему шагу.

2.11.2 Шаг 2. Убедитесь, что сервер запущен

Большинство установочных пакетов запускают сервер РЕД Базы Данных в качестве одного из последних шагов установки, а также следят за тем, чтобы сервер запускался при каждой перезагрузке.

После запуска сервер РЕД Базы Данных должен быть запущен:

- На `Linux` или других `Unix-подобных` системах - Как сервис;
- На `Windows` - Как сервис или как приложение. Сервис используется по умолчанию и крайне рекомендуется.

Проверка сервера на Linux

Используйте команду top командной строки для проверки запущенных процессов в интерактивном режиме. Если сервер РЕД Базы Данных 5 запущен, вы должны увидеть процесс с именем rdbserver и, возможно, также rdbguard (процесс Guardian).

Ниже показан вывод top, ограниченный grep, чтобы отображать только строки, содержащие строку rdb:

```
[user@centos6 ]$ top -b -n1 | grep rdb
3835 firebird 20 0 31288 920 516 S 0.0 0.0 0:00.00 rdbguard
3836 firebird 20 0 127m 2468 1980 S 0.0 0.1 0:00.01 rdbserver
```

Как альтернатива, вместо команды top, Вы можете использовать ps -ax или ps -aux, при необходимости перенаправив вывод grep.

Другой способ проверить сервер после установки - запустить клиент (например, isql) и подключиться к базе данных или создать ее. Эти операции описаны далее в этом руководстве.

Если окажется, что сервер не был запущен, то сделайте это вручную. В зависимости от типа системы Linux и вашего установочного набора выполните следующее:

```
/etc/init.d/firebird start

или

systemctl start firebird
systemctl enable firebird.
```

Проверка сервера на Windows

Нажмите Win + R, введите services.msc, затем Enter или OK. Или нажмите Пуск (или Win), найдите "Службы" и откройте приложение "Службы".

В списке сервисов найдите сервер RedDatabase. Если сервер по каким-то причинам не запущен, можете сделать это сейчас, нажав правой кнопкой мыши на запись RedDatabaseServerDefaultInstance и выбрав "Запустить".

Проверка сервера на Windows, запущенного как приложение

Если РЕД База Данных запущена и работает как приложение, она будет представлена значком в системном трее:

- Зеленый и серый символ сервера, если он управляется Guardian;
- Круглый желто-черный символ, если приложение работает автономно.

Мигающий значок означает, что сервер находится в процессе запуска (или, по крайней мере, пытается это сделать). Красный значок или значок с расположенным над ним красным знаком стоп означает, что запуск не удался.

Один из способов узнать запущен сервер или нет - нажать Ctrl + Alt + Del, выбрать "Диспетчер задач" и поискать процесс RedDatabase (и, возможно, rdbguard) в списке задач. Может потребоваться установить флажок "Показывать процессы всех пользователей", чтобы этот процесс стал видимым.

В некоторых случаях может потребоваться запустить Guardian или сервер один раз через меню "Пуск". Иногда требуется перезагрузка.

Вы можете выключить сервер через меню, которое появляется, если нажать правой кнопкой мыши на значке в трее. Обратите внимание, что при этом значок также исчезает, то есть вы можете

перезапустить РЕД Базу Данных через меню Пуск.

В режиме `Classic` (но не `SuperClassic`) для каждого соединения запускается новый процесс, поэтому количество процессов `RedDatabase` всегда равно количеству клиентских соединений плюс одно. Завершение работы через меню значка в трее приводит к завершению только первого процесса (слушателя). Остальные процессы, если они присутствуют, будут продолжать нормально функционировать, каждый из них завершится, когда клиент отключится от базы данных. Разумеется, после закрытия слушателя новые подключения невозможны.

Глава 3

Расположение на диске по умолчанию

В таблицах ниже показано, где находятся файлы и каталоги РЕД Базы Данных после стандартной установки.

3.1 Linux

В следующей таблице показано расположение компонентов по умолчанию при установке РЕД Базы Данных в Linux. Расположение может отличаться в других Unix-подобных системах или дистрибутивах Linux.

Таблица 3.1 — Расположение компонентов РЕД Базы Данных на Linux

Компонент	Имя файла	Расположение
Каталог установки (здесь и далее обозначается как $(install))	-	/opt/RedDatabase (может отличаться в зависимости от дистрибутива)
Конфигурационные файлы	firebird.conf, databases.conf и так далее.	$(install)
Документация	Различные файлы	
Сервер РЕД Базы Данных	rdbserver	$(install)/bin
Утилиты командной строки	isql, gbak, nbackup, gfix, gstat и другие	$(install)/bin
Плагины	libEngine13.so, libSrp.so, libudr_engine.so и другие	$(install)/plugins
Демонстрационная база данных	employee.fdb	$(install)/examples/empbuild
Дополнительные библиотеки сервера	libib_util.so	$(install)/lib
Клиентские библиотеки	libfbclient.so.5.0.n. Создаются обычные симлинки (*. so.2, *.so). Устаревшие симлинки libgds.* также устанавливаются.	/usr/lib[64] На самом деле компонент находится в $(install)/lib, но нужно использовать ссылки в /usr/lib[64])

3.2 Windows

В таблице ниже %ProgramFiles% относится к папке программ Windows. Обычно это C:\Program Files, но может быть и другой путь, например D:\Programs. Аналогично, %windir% относится к каталогу Windows. Обязательно прочитайте примечания под таблицей, особенно если вы запускаете РЕД

Базу Данных на 64-битной системе Windows.

Таблица 3.2 — Расположение компонентов РЕД Базы Данных на Windows

Компонент	Имя файла	Расположение
Каталог установки (здесь и далее обозначается как $(install))	-	%ProgramFiles%FirebirdFirebird_5_0
Конфигурационные файлы	firebird.conf, databases.conf и так далее.	$(install)
Сервер РЕД Базы Данных	rdbserver	$(install)
Утилиты командной строки	isql, gbak, nbackup, gfix, gstat и другие	$(install)
Плагины	libEngine13.so, libSrp.so, libudr_engine.so и другие	$(install)plugins
Демонстрационная база данных	employee.fdb	$(install)examplesempbuild
Интернационализация	fbintl.conf, fbintl.dll	$(install)intl
Дополнительные библиотеки сервера	icu*.dll, ib_util.dll	$(install)
Клиентские библиотеки	fbclient.dll, gds32.dll	$(install)
Некоторые необходимые исполняемые библиотеки Microsoft	msvcp140.dll, vcruntime140.dll	$(install)
32-битные версии библиотек для использования с 64-битным Firebird	fbclient.dll, msvcp140.dll, vcruntime140.dll	$(install)WOW64 (с дополнительной копией в SysWOW64 - см. второе примечание под таблицей)

Примечания:

Типичное расположение системного каталога Windows, как в 32, так и в 64-битных системах - %windir%\System32, например C:\Windows\System32.

В 64-битных системах Windows каталог Program Files зарезервирован для 64-битных программ. Если вы попытаетесь установить 32-битное приложение в эту папку, оно будет автоматически перенаправлено в каталог, который в англоязычных версиях называется Program Files (x86). В других языковых версиях название может быть иным.

Аналогично, каталог System32 зарезервирован для 64-битных библиотек, а 32-битные библиотеки помещаются в SysWOW64. Именно так: 64-битные библиотеки находятся в System32, а 32-битные - в SysWOW64.

Если вы не знаете об этом, у вас могут возникнуть трудности с размещением 32-битных компонентов Firebird в 64-битной системе Windows. WOW означает Windows on Windows.

Глава 4

Настройка и управление сервером

4.1 Управление пользователями

В версии 5 управление пользователями осуществляется с помощью команд SQL. Утилита gsec по-прежнему существует, но устарела и её использовать не рекомендуется.

Учетные записи пользователей хранятся в базе данных безопасности security3.fdb, которая находится в корневой директории установки сервера. Подключение к обычной базе данных всегда происходит с включением базы данных безопасности для верификации пользователей. Конечно, это делается прозрачно и пользователю не нужно явно подключаться к security3.fdb.

Начиная с РЕД Базы Данных 3 можно использовать не одну, а несколько баз данных безопасности, каждая из которых управляет определенным набором баз данных. База данных может даже выступать в качестве собственной базы данных безопасности.

4.1.1 Изменение пароля SYSDBA

Одна учетная запись РЕД Базы Данных создается автоматически в процессе установки - SYSDBA. Эта учетная запись обладает всеми привилегиями на сервере и не может быть удалена. В зависимости от версии, ОС и архитектуры, программа установки сделает следующее:

- Установит пользователя SYSDBA с паролем masterkey;
- Попросит ввести пароль во время установки;
- Сгенерирует случайный пароль и сохранит его в файле SYSDBA.password в каталоге установки.

Если пароль пользователя SYSDBA - masterkey, то в целях безопасности следует немедленно его изменить. Для этого запустите isql или другой клиент РЕД Базы Данных и подключитесь к базе данных. В этом примере используется база данных employee, поскольку ее псевдоним всегда присутствует в свежеустановленной РЕД Базе Данных:

```
connect localhost:employee user sysdba password masterkey;

Database: localhost:employee, User: SYSDBA
```

Измените пароль пользователя SYSDBA:

```
alter user sysdba set password 'Pdmso3Tjdn';
```

> Вместо SYSDBA также можно использовать CURRENT USER, который всегда ссылается на пользователя, под которым вы вошли в систему.

Если команда выполнена успешно, вы не получите никаких сообщений. Вместо этого isql просто выведет следующее сообщение SQL>, указывая тем самым, что все в порядке и дальнейший ввод не ожидается.

Обратите внимание, что в отличие от имен пользователей, пароли всегда чувствительны к регистру.

В зависимости от настроек UserManager и AuthServer в файлах firebird.conf или databases.conf, у вас может быть несколько учетных записей SYSDBA. Обязательно измените пароль для всех.

Если вы использовали традиционную аутентификацию (Legacy_Auth), возможно, стоит удалить учетную запись SYSDBA, так как она небезопасна и ограничивает максимальную длину пароля 8 символами.

4.2 Добавление пользователя

РЕД База Данных позволяет создавать множество различных пользовательских учетных записей. Пользователь может стать владельцем базы данных, а также иметь различные виды доступа к базам данных и объектам баз данных, которые ему не принадлежат.

Подключившись к базе данных как SYSDBA, можно добавить учетную запись пользователя следующим образом:

```
create user testuser password 'tecmImbdl';
```

Полный синтаксис для управления пользователями:

```
CREATE USER <имя пользователя>
  <атрибут> [<атрибут> ...]
  [TAGS (<пользовательская переменная> [, <пользовательская переменная> ...]]

[CREATE OR] ALTER {USER <имя пользователя> | CURRENT USER}
  [SET] [<атрибут> [<атрибут> ...]]
  [TAGS (<пользовательская переменная> [, <пользовательская переменная> ...]]

DROP USER <имя пользователя>)
  [USING PLUGIN <плагин>]

<атрибут> ::=
  PASSWORD '<пароль>'
| FIRSTNAME '<имя>'
| MIDDLENAME '<второе имя>'
| LASTNAME '<фамилия>'
| {GRANT | REVOKE} ADMIN ROLE
| {ACTIVE | INACTIVE}
| USING PLUGIN <плагин>

<пользовательская переменная> ::=
  <имя тега> = '<значение>'
| DROP <имя тега>
```

Теги - это необязательные пары ключ-значение, которые могут быть определены пользователем. Ключ (имя тега) должен быть действительным SQL-идентификатором, а значение - строкой длиной не более 255 байт (не NULL).

Только SYSDBA и администраторы могут использовать все эти команды. Обычные пользователи могут изменять свои атрибуты (такие как пароль, части имени и теги, но не ACTIVE/INACTIVE) с помощью ALTER USER <имя пользователя> или ALTER CURRENT USER. Изменить имя учетной записи невозможно.

Пример:

```
create user dubya password 'Xwha007_noma' firstname 'GW' lastname 'Shrubbery';

create user lorna password 'Mayday_domaka' tags (Street = 'Main Street', Number = '888
');

alter user benny tags (shoesize = '8', hair = 'blond', drop weight);
alter current user set password 'SomethingEvenMoreSecretThanThis';
alter user dubya set inactive;
drop user ted;
```

4.3 База данных безопасности

Учетные записи пользователей РЕД Базы Данных хранятся в базе данных безопасности, которая обычно находится в каталоге установки и называется `security5.fdb` (псевдоним: `security.db`). За исключением встроенных соединений, при подключении к базе данных всегда используется база данных безопасности, по которой проверяются учетные данные пользователя. Это делается открыто, пользователю не нужно делать явное подключение к базе данных безопасности.

Начиная с РЕД Базы Данных 3 можно использовать несколько баз данных безопасности, причем каждая база данных безопасности управляет определенным набором баз данных. База данных может даже выступать в качестве собственной базы данных безопасности.

Если используется несколько баз данных безопасности, то управление учетными записями пользователей при подключении к базе данных всегда будет влиять на учетные записи в базе данных безопасности, которая управляет этой базой данных. Чтобы подстраховаться, перед выполнением операторов управления пользователями лучше подключиться к самой базе данных безопасности. В последних версиях РЕД Базы Данных подключение к базе данных безопасности было запрещено, но теперь это снова возможно, хотя по умолчанию только локально, используя встроенный сервер или `XNET` в `Windows`.

4.4 Администраторы с ролью RDB$ADMIN

`SYSDBA` и другие пользователи с правами администратора могут предоставлять пользователям роль `RDB$ADMIN` в базе данных безопасности `security5.fdb`. Для этого используется директива `GRANT ADMIN ROLE`:

```
create user testuser password 'bigsekrit7foryou' grant admin role;
alter user john grant admin role;
```

Первая команда создает пользователя testuser в качестве администратора, который может добавлять, изменять и удалять пользователей. Вторая команда предоставляет привилегии администратора существующему пользователю john.

Чтобы отозвать привилегии администратора используется `ALTER USER ... REVOKE ADMIN ROLE`.

`GRANT ADMIN ROLE` и `REVOKE ADMIN ROLE` - это не операторы `GRANT` и `REVOKE`, а предложения операторов `CREATE` и `ALTER USER`. Фактическое имя роли здесь - `RDB$ADMIN`. Эта роль существует и в обычных базах данных.

Каждый пользователь, получивший права администратора, может предоставлять их другим. Поэтому не существует явного варианта `WITH ADMIN OPTION`.

Также можно предоставить права администратора существующему пользователю, подключившись к базе данных безопасности и выполнив оператор `GRANT`:

```
grant rdb$admin to <имя пользователя>
```

4.4.1 Разница между SYSDBA и RDB$ADMIN

Пользователи с ролью RDB$ADMIN в базе данных безопасности могут создавать, изменять и удалять пользователей, но, в отличие от SYSDBA, они автоматически не имеют привилегий в обычных базах данных.

В отличие от SYSDBA, администраторы должны явно указывать роль RDB$ADMIN, чтобы использовать свои права системного администратора:

```
connect security.db user testuser password bigsekrit7foryou role rdb$admin
```

Такое подключение к базе данных безопасности может не сработать, если используется Superserver. В Windows это можно обойти, добавив xnet:// к пути или псевдониму базы данных, но на POSIX это невозможно. Единственное решение - подключиться к обычной базе данных через сервер, например, используя localhost:employee.

Начиная с РЕД Базы Данных 5 больше не нужно иметь привилегии RDB$ADMIN в обычной базе данных, чтобы выполнять операторы управления пользователями в базе данных безопасности, достаточно привилегий в базе данных безопасности.

> Роль RDB$ADMIN в базе данных дает получателю права SYSDBA только в этой базе данных!
>
> Если это база данных безопасности, получатель роли RDB$ADMIN может управлять учетными записями пользователей, но не имеет привилегий в других базах данных.
>
> Если это обычная база данных, то получатель роли RDB$ADMIN может управлять этой базой данных, как SYSDBA, но у него нет привилегий в других базах данных, а также нет привилегий для администрирования пользователей.
>
> Можно предоставить пользователю роль RDB$ADMIN в нескольких базах данных, включая базу данных безопасности.

Чтобы предоставить пользователю права администратора в обычной базе данных, можно воспользоваться следующим способом:

```
grant rdb$admin to testuser
```

Предоставлять права может владелец базы данных, SYSDBA, а также любой другой пользователь, имеющий роль RDB$ADMIN в этой базе данных и указавший ее при подключении. Каждый пользователь RDB$ADMIN в базе данных может передавать свою роль другим, поэтому не существует опции WITH ADMIN.

Глава 5

Безопасность

Ниже приведены некоторые рекомендации по защите сервера и баз данных.

Запуск сервера РЕД Базы Данных не системным пользователем

В Unix-подобных системах РЕД База Данных по умолчанию работает от имени пользователя `reddatabase`, а не от имени `root`. На серверных платформах `Windows` также можно запускать службу РЕД Базы Данных под определенной учетной записью пользователя (например, `RedDatabase`). По умолчанию запуск службы выполняется от имени пользователя `LocalSystem`, что представляет собой риск для безопасности, если система подключена к Интернету.

Смена пароля SYSDBA

Если в качестве пароля системного администратора указан `masterkey`, то необходимо изменить его для обеспечения безопасности. Подробнее о смене пароля см. раздел *Изменение пароля SYSDBA*.

Не создавайте пользовательские базы данных от имени SYSDBA

`SYSDBA` - это учетная запись, имеющая полные права доступа ко всем базам данных РЕД Базы Данных. Пароль `SYSDBA` должен быть известен только нескольким доверенным администраторам баз данных. Не стоит использовать эту учетную запись для создания и наполнения обычных баз данных. Вместо этого создайте обычные учетные записи пользователей и предоставьте им привилегию `CREATE DATABASE`, а также предоставляйте имена и пароли этих учетных записей своим пользователям по мере необходимости. Можно сделать это с помощью операторов управления пользователями `SQL`, как показано выше (см. раздел *Добавление пользователя*), или с помощью инструментов администрирования.

Защита базы данных на уровне файловой системы

Любой, у кого есть доступ к файлу базы данных на уровне файловой системы, может скопировать его и извлечь из него все данные. Любой, у кого есть доступ к файлу базы данных на уровне файловой системы на запись, может повредить его или вовсе удалить.

Кроме того, любой человек, имеющий доступ к базе данных на уровне файловой системы, может установить встроенное соединение с базой данных под видом любого пользователя (включая `SYSDBA`). Это может быть особенно опасно, если речь идет о базе данных безопасности.

Только серверный процесс РЕД Базы Данных должен иметь доступ к файлам базы данных. Пользователям не нужен и не должен быть предоставлен доступ к файлам, даже только для чтения. Пользователи обращаются к базам данных через сервер, а сервер следит за тем, чтобы пользователи получали только разрешенный тип доступа к любым объектам в базе данных.

Отключение встроенных (embedded) соединений

Если вам не нужен прямой доступ, вы можете полностью отключить встроенный режим (прямой доступ на уровне файловой системы), настроив параметр `Providers` в файле `firebird.conf`. По умолчанию параметр имеет следующее значение:

```
#Providers = Remote,Engine13,Loopback
```

Раскомментируйте строку и удалите `Engine13`, отвечающий за встроенные соединения:

```
Providers = Remote,Loopback
```

Провайдер `Remote` отвечает за удаленные соединения. Провайдер `Loopback` отвечает за `TCP/IP` соединения через `localhost`, а также `XNET` соединения с базами данных на локальной машине в `Windows`. Все эти типы соединений требуют полной аутентификации и открывают файл базы данных серверным процессом, а не пользовательским.

Параметр `Providers` также можно настроить для каждой базы данных отдельно. Можно установить значение по умолчанию в файле `firebird.conf`, как показано выше, а затем переопределить его для конкретных баз данных в файле `databases.conf` следующим образом:

```
base_alias = opt/DB/testDB.fdb
{
        Providers = Remote,Loopback
}
```

Первая строка определяет псевдоним базы данных, а всё, что находится между фигурными скобками - это параметры для конкретной базы данных. Файл `databases.conf` находится в том же каталоге, что и файл `firebird.conf`.

Использование псевдонимов (алиасов) баз данных

Псевдонимы баз данных скрывают от клиента физическое расположение баз данных. Используя псевдонимы, клиент может, например, подключиться к `frodo:zappa`, не зная, что реальное местоположение - `frodo:/var/firebird/music/underground/mothers_of_invention.fdb`. Псевдонимы также позволяют менять расположение баз данных, в то время как клиенты продолжат использовать существующие строки подключения.

Псевдонимы указываются в файле `databases.conf`, в следующем формате на `Windows`:

```
poker = E:\Games\Data\PokerBase.fdb
blackjack.fdb = C:\Firebird\Databases\cardgames\blkjk_2.fdb
```

И на `Linux`:

```
books = /home/bookworm/database/books.fdb
zappa = /var/firebird/music/underground/mothers_of_invention.fdb
```

Добавлять псевдониму расширение `.fdb` (или любое другое) вовсе не обязательно. Но, если вы его указываете, то должны указать его и при использовании псевдонима для подключения к базе данных.

Псевдонимы, введенные и сохраненные, вступают в силу немедленно. Нет необходимости перезапускать сервер.

Ограничение доступа к базам данных

Сервер РЕД Базы Данных можно настроить на работу только с определенными базами данных. Для этого необходимо указать список доступных для сервера баз данных в конфигурационном файле сервера `firebird.conf` (параметр `DatabaseAccess`). Доступ к базам данных на сервере может быть полным (`Full`), ограниченным (`Restrict`) или запрещенным (`None`). Для того, чтобы запретить

доступ, следует выставить значение параметра, равное None. Для ограничения доступа используется значение Restrict. В этом случае после слова Restrict указываются директории, в которых могут быть сохранены файлы баз данных.

```
DatabaseAccess = Restrict /db;/mnt/mirrordb
```

Обратите внимание, что это не то же самое, что защита доступа на уровне файловой системы, о которой говорилось ранее. Если значение DatabaseAccess не равно Full, сервер откажется открывать любые базы данных за пределами заданной области, даже если у него достаточно прав на файлы баз данных.

Выберите метод аутентификации

РЕД База Данных поддерживает следующие методы аутентификации при подключении к базам данных:

1. Srp (Secure Remote Password). Пользователь должен идентифицировать себя с помощью имени пользователя и пароля, которые сервер проверяет по базе данных безопасности. Максимальная эффективная длина пароля составляет около 20 байт, хотя вы можете задавать более длинные пароли до 255 символов. Используется шифрование сетевого трафика. Сервер поддерживает различные плагины аутентификации Srp, по умолчанию используется Srp256, который использует SHA256 для подтверждения пользователя.
2. Win_Sspi (Windows Security Support Provider Interface). Пользователь автоматически авторизуется с помощью учетной записи Windows. Используется шифрование сетевого трафика.
3. Legacy_Auth. Небезопасный метод, используемый в предыдущих версиях РЕД Базы Данных. Пароли могут быть длиной не более 8 байт и передаются по сети в незашифрованном виде. По возможности избегайте этого метода.
4. Многофакторная аутентификация.

Аутентификация определяется двумя параметрами конфигурации:

- AuthServer определяет, как пользователь может подключиться к локальному серверу. По умолчанию установлено значение Srp256. Для Windows - Srp256, Win_Sspi. В случае с Windows пользователь будет проходить аутентификацию с помощью своей учетной записи Windows, если он не сможет предоставить свои пользовательские данные, что приведет к неудачному использованию метода Srp256, который будет применен первым.
- AuthClient определяет, как локальный клиент пытается проверить подлинность пользователя при установлении соединения. Обычно это Srp256, Srp, Win_Sspi, Legacy_Auth.

Если Legacy_Auth разрешен на стороне сервера, необходимо также установить для параметра WireCrypt значение Enabled или Disabled, но не Required.

Если Legacy_Auth разрешен, также необходимо изменить значение параметра UserManager на Srp, Legacy_UserManager (или Legacy_UserManager, Srp, если требуется управлять традиционными учетными записями по умолчанию и/или через gsec). В операторах управления пользователями можно использовать предложение USING PLUGIN, чтобы указать используемый менеджер пользователей. Доступны только менеджеры пользователей, перечисленные в UserManager.

Параметры AuthServer, AuthClient, WireCrypt и UserManager настраиваются в файле firebird.conf и могут быть опеределены для каждой базы данных в файле databases.conf.

Обратите внимание, что включение Win_Sspi на сервере активирует плагин, но пока не дает учетным записям Windows никакого доступа к базам данных. Если войти, например, в базу данных employee без учетных данных (и убедиться, что не установлено встроенное соединение), это приведет к появлению сообщения об ошибке:

```
SQL> connect xnet://employee;
Statement failed, SQLSTATE = 28000
Missing security context for employee
```

Решение заключается в создании в качестве SYSDBA или администратора глобального отображения, которое дает учетной записи Windows доступ к базам данных, но без привилегий. Для этого используется следующая команда:

```
create global mapping trusted_auth
using plugin win_sspi
from any user to user
```

Trusted_auth - это просто имя, выбранное для отображения. Можно использовать другой идентификатор. FROM ANY USER означает, что отображение действительно для любого пользователя, прошедшего аутентификацию с помощью плагина Win_Sspi. TO USER означает, что каждый пользователь будет идентифицирован под именем своей учетной записи Windows в каждой базе данных, к которой он подключается. Если вместо этого указать to user bob, то каждый пользователь Windows, аутентифицированный плагином Win_Sspi, будет представлен в базе данных под именем bob.

С использованием такого отображения соединение «Windows trusted» работает:

```
SQL> connect xnet://employee;
Database: xnet://employee, User: SOFA\PAUL
SQL> select current_user from rdb$database;

USER
==============================
SOFA\PAUL
```

В случае встроенных соединений, то есть соединений без сервера, обрабатываемых Engine13, когда клиентский процесс напрямую открывает файл базы данных, пользователь также входит в систему от имени своей учетной записи Windows, если он не указывает имя пользователя при подключении. Однако для этого не требуется включения Win_Sspi и явного отображения:

```
SQL> connect employee;
Database: employee, User: PAUL
SQL> select current_user from rdb$database;

USER
==============================
PAUL
```

Определите, должны ли администраторы Windows иметь права SYSDBA

В РЕД Базе Данных 2.1 и ниже администраторы Windows автоматически получали права SYSDBA во всех базах данных, включая базу данных безопасности. В более поздних версиях это поведение убрали.

Если необходимо применить автоматическое отображение SYSDBA, войдите в систему под именем SYSDBA и выполните команду:

```
create global mapping win_admin_sysdba
using plugin win_sspi
from predefined_group domain_any_rid_admins
to user sysdba
```

Это предоставит всем администраторам Windows права SYSDBA в каждой базе данных, включая базу данных безопасности, чтобы они могли управлять учетными записями пользователей, при условии, что они прошли аутентификацию с использованием плагина Win_Sspi. Для этого они должны подключаться без указания учетных данных пользователя и убедиться, что провайдер Engine13 не работает. Для этого можно воспользоваться строкой подключения в формате xnet://<локальный путь или алиас>.

Чтобы предоставить одному администратору все права SYSDBA, используйте следующую команду:

```
create global mapping frank_sysdba
using plugin win_sspi
from user "sofa\frank"
to user sysdba
```

Двойные кавычки в примере необходимы из-за обратной косой черты в имени пользователя.

Можно удалить отображение с помощью команды:

```
DROP [GLOBAL] MAPPING <имя отображения>
```

Например:

```
drop global mapping win_admin_sysdba;
drop global mapping frank_sysdba;
```

Ключевое слово GLOBAL необходимо, если отображение глобальное, и вы не подключены напрямую к базе данных безопасности, в которой зарегистрировано отображение.

Глава 6

Работа с базой данных

6.1 Строки подключения

Если хотите подключиться к базе данных или создать ее, необходимо, помимо всего прочего, передать клиентскому приложению или вызываемым вами процедурам строку подключения. Строка подключения однозначно идентифицирует местоположение базы данных на компьютере, в локальной сети и даже в Интернете.

6.1.1 Локальные строки подключения

Явная локальная строка подключения состоит из пути и имени файла в формате файловой системы, используемой на серверной машине, например:

- На `Linux` или другом `Unix-подобном` сервере:

```
/opt/firebird/examples/empbuild/employee.fdb
```

- На `Windows`:

```
C:\Biology\Data\Primates\Apes\populations.fdb
```

Многие клиенты также допускают относительные пути (например, `..\examples\empbuild\employee.fdb`), но их нужно использовать с осторожностью, поскольку не всегда очевидно, как они будут расширены. Случайно можно подключиться к другой базе данных и внести изменения, которые могут привести к катастрофическим последствиям.

Вместо пути к файлу строка локального подключения может представлять собой псевдоним базы данных, который задается в файле `databases.conf`. Формат псевдонима зависит только от того, как он определен в конфигурационном файле, а не от файловой системы сервера. Например: `zappa`, `blackjack.fdb`, `poker`.

При получении локальной строки подключения клиент РЕД Базы Данных сначала попытается установить встроенное соединение с файлом базы данных, минуя аутентификацию, но соблюдая привилегии и ограничения `SQL` для указанного пользователя и роли. Встроенное подключение устанавливается, если провайдер `Engine13` включен в файле `firebird.conf` или `databases.conf`, что по умолчанию так. Если файл базы данных существует, но соединение не устанавливается, потому что клиентский процесс не имеет необходимых привилегий доступа к файлу, выполняется попытка клиент-серверного соединения (с помощью провайдера `Loopback`), в следующем порядке:

1. В `Windows` с помощью `XNET` на локальной машине;
2. Используя `TCP/IP` через `localhost`.

Можно принудительно использовать определенный протокол и пропустить попытку установки встроенного соединения, добавив протокол в формате `URL`:

- `inet://zappa`. `TCP/IP-соединение` с использованием псевдонима на локальной машине.
- `inet:///opt/firebird/examples/citylife.fdb`. `TCP/IP-соединение` с использованием абсолютного пути на локальной `POSIX-машине`. Обратите внимание на дополнительную косую черту для корневого каталога.
- `inet://C:\Work\Databases\Drills.fdb`. `TCP/IP-соединение` по абсолютному пути на локальной машине `Windows`.
- `xnet://security.db`. `XNET-соединение` с использованием псевдонима на локальной машине

Windows.

- xnet://C:\Programmas\Firebird\Firebird_3_0\security3.fdb. XNET-соединение с использованием полного пути на локальной машине Windows.

Если XNET-соединение не удаётся установить, это может быть связано с тем, что локальный протокол не работает должным образом на вашей машине. Если используете Windows с включенными терминальными службами, это можно исправить, установив для IpcName значение Global\FIREBIRD в конфигурационном файле firebird.conf.

Если настройка IpcName не помогла, и нет возможности включить локальный протокол, то можно обойти проблему, используя inet:// или добавляя localhost: перед путем к базе данных или псевдонимом, превращая их в строки TCP/IP-соединения.

6.1.2 TCP/IP строки подключения

У РЕД Базы Данных есть два формата строк TCP/IP-соединения:

1. {inet|inet4|inet6}://[<хост>[:<порт>]/]<путь или псевдоним>
2. <хост>[/порт]:<путь или псевдоним>

Где:

- Хост - имя сервера или IP-адрес. Адреса IPv6 следует заключать в квадратные скобки ([ ]).
- Порт - номер порта или имя сервиса.
- Путь или псевдоним - либо абсолютный путь к базе данных и имя файла на машине сервера, либо псевдоним базы данных, определенный на машине сервера.

Примеры:

Для Linux/Unix:

```
pongo:/opt/firebird/examples/empbuild/employee.fdb
inet://pongo//opt/firebird/examples/empbuild/employee.fdb
bongo/3052:fury
inet://bongo:3052/fury
112.179.0.1:/var/Firebird/databases/butterflies.fdb
inet://112.179.0.1//var/Firebird/databases/butterflies.fdb
localhost:blackjack.fdb
inet://localhost/blackjack.fdb
```

Для Windows:

```
siamang:C:\Biology\Data\Primates\Apes\populations.fdb
inet://siamang/C:\Biology\Data\Primates\Apes\populations.fdb
sofa:D:\Misc\Friends\Rich\Lenders.fdb
inet://sofa/D:\Misc\Friends\Rich\Lenders.fdb
inca/fb_db:D:\Traffic\Roads.fdb
inet://inca:fb_db/D:\Traffic\Roads.fdb
127.0.0.1:Borrowers
inet://127.0.0.1/Borrowers
```

Обратите внимание, что псевдонимы в строках подключения не дают никакого представления об операционной системе сервера. Да это и не нужно: вы общаетесь с сервером под Linux точно так же, как и с сервером под Windows. На самом деле, указание явного пути к базе данных - это один из редких случаев, когда нужно знать разницу.

6.1.3 XNET строки соединения

Синтаксис XNET URL:

```
xnet://<путь или псевдоним>
```

Поскольку XNET - это локальный протокол, нельзя указывать имя хоста или порт.

6.2 Подключение к существующей базе данных

Пример базы данных с именем employee.fdb находится в examples/empbuild вашего каталога установки РЕД Базы Данных. Она также доступна под псевдонимом employee.

Если вы переносите или копируете демонстрационную базу данных, убедитесь, что она находится на жестком диске, физически подключенном к серверной машине. Общие ресурсы, отображаемые диски или (в Unix) смонтированные файловые системы SMB (Samba) не подойдут. Это же правило применимо к любым базам данных, которые вы создаете или используете.

Подключение к базе данных требует явной или неявной аутентификации. Для работы с объектами базы данных, такими как таблицы, представления и функции, пользователю, под которым вы вошли в систему, нужны явные права доступа к этим объектам, если только вы не являетесь их владельцем (вы владеете объектом, если вы его создали) или не подключены как SYSDBA или пользователь с ролью RDB$ADMIN. В базе данных employee.fdb для PUBLIC (т. е. любого аутентифицированного пользователя) было выделено достаточно прав, чтобы можно было видеть и изменять данные по своему усмотрению.

Рассмотрим аутентификацию от имени SYSDBA с использованием пароля masterkey. Также в примерах будем работать с локальными базами данных и использовать псевдонимы везде, где это возможно. Все, что вы узнаете в этих разделах, можно применить и к удаленным базам данных, просто указав строку TCP/IP-соединения.

6.2.1 Подключение с помощью isql

РЕД База Данных поставляется вместе с утилитой командной строки isql (Interactive SQL utility). Можно использовать её несколькими способами для подключения к базе данных. Один из них - запустить ее в интерактивном режиме. Перейдите в каталог, где находятся утилиты РЕД Базы Данных, и введите isql (Windows) или ./isql (Linux) в командной строке.

Например:

```
C:\Programmas\Firebird\Firebird_3_0>isql
Use CONNECT or CREATE DATABASE to specify a database
SQL>connect xnet://employee user sysdba password masterkey;
```

В isql каждый оператор SQL должен заканчиваться точкой с запятой. Если при нажатии на Enter строка не заканчивается точкой с запятой, isql считает, что оператор продолжается на следующей строке, и сообщение изменится с SQL на CON. Это позволяет разбивать длинные операторы на несколько строк. Если вы нажмете Enter после оператора, но забудете точку с запятой, просто введите ее после сообщения CON на следующей строке и снова нажмите Enter.

Если строка подключения не начинается с имени хоста или протокола, будет предпринята попытка установить встроенное подключение. Это может закончиться ошибкой, если у вашей учетной записи в операционной системе нет достаточных прав доступа к файлу базы данных. В этом случае подключитесь к localhost:<путь к базе или псевдоним> или укажите протокол xnet:// (только для Windows) или inet://. Тогда серверный процесс (обычно работающий от имени пользователя reddatabase на POSIX или LocalSystem на Windows) откроет файл. С другой стороны, сетевые соединения могут не установиться, если пользователь создал базу данных во встроенном режиме, а сервер не имеет достаточных прав доступа.

Путь, имя пользователя и пароль можно заключить в одинарные (') или двойные (") кавычки. Если путь содержит пробелы, кавычки обязательны. Имена пользователей с учетом регистра (созданные следующим образом: `create user "Jantje" password ...`) и имена пользователей, содержащие пробелы, международные символы также должны быть заключены в двойные кавычки.

На этом этапе `isql` сообщит, что подключение установлено:

```
Database: xnet://employee, User: SYSDBA
SQL>
```

Теперь можно работать с базой данных `employee`. С помощью `isql` можно запрашивать данные, получать информацию о метаданных, создавать объекты базы данных, запускать скрипты и многое другое.

Чтобы вернуться в командную строку операционной системы введите следующее:

```
SQL> quit;
```

Также можно ввести `EXIT` вместо `QUIT`, разница в том, что `EXIT` сначала зафиксирует все открытые транзакции, сделав внесенные изменения окончательными.

6.2.2 Подключение с помощью РБДЭксперт

Создание подключения

РБДЭксперт позволяет одновременно использовать несколько подключений к базе данных. Информацию о подключении отображает `Браузер баз данных`.

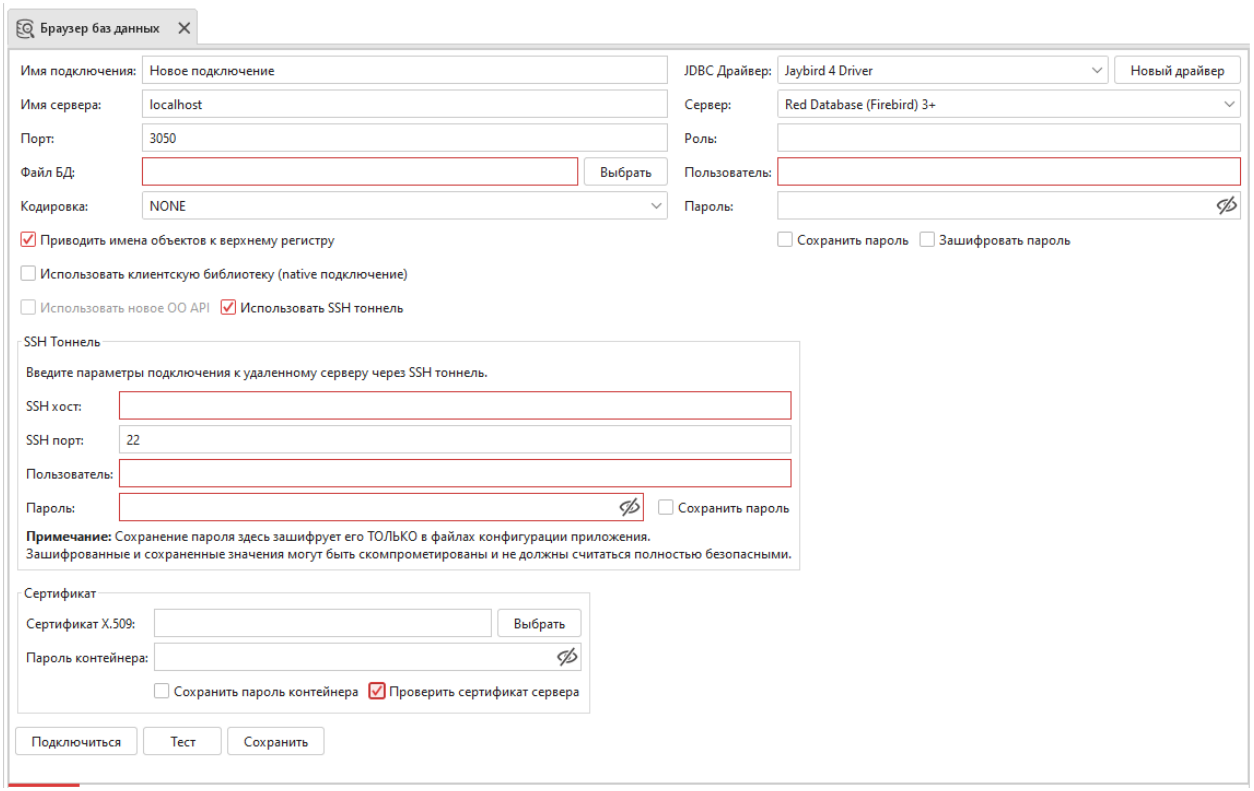


Рисунок 6.1 — Браузер баз данных

Для создания подключения выберите соответствующий пункт в меню База данных или нажмите на кнопку `Создать подключение` в панели инструментов. Заполните поля в открывшемся окне и нажмите на кнопку `Подключиться`.

При попытке подключения может возникнуть ошибка шифрования сетевого соединения. Для поддержки шифрования необходима версия `Java` не ниже `1.8.0_161` или установленное `JCE` дополнение. В противном случае следует изменить значение параметра `WireCrypt = Disabled` в `firebird.conf`.

Подключение к существующей базе данных

Для установки соединения с существующей базой данных двойным кликом выберите нужное подключение в дереве подключений:

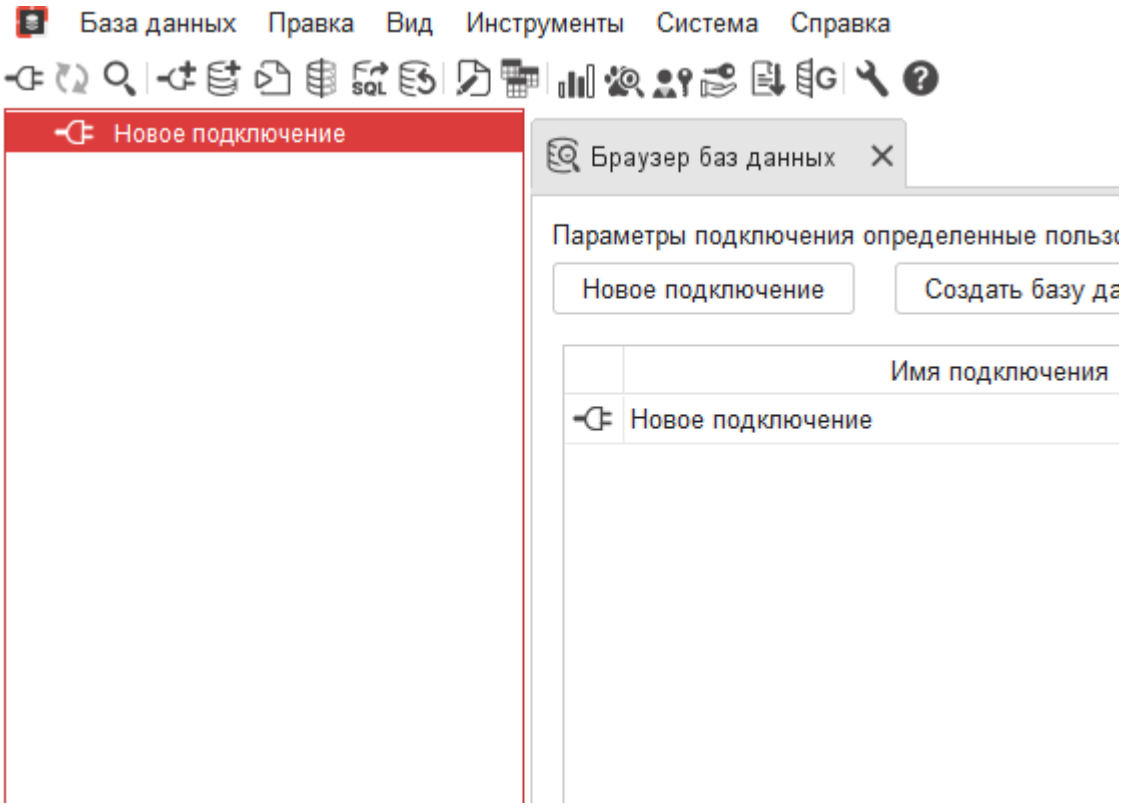


Рисунок 6.2 — Дерево подключений

Введите имя пользователя и пароль в открывшемся окне, а затем нажмите на кнопку `Войти`.

6.3 Создание базы данных с помощью isql

Существует несколько способов создания базы данных с помощью `isql`. Здесь мы рассмотрим один простой способ создания базы данных в интерактивном режиме.

6.3.1 Запуск isql

Чтобы создать базу данных в интерактивном режиме с помощью утилиты командной строки `isql`, введите `isql` (в `Windows`) или `./isql` (в `Linux`) в командной строке в каталоге, где находятся утилиты РЕД Базы Данных.

```
C:\Programmas\RedDatabase>isql
Use CONNECT or CREATE DATABASE to specify a database
```

6.3.2 Оператор CREATE DATABASE

Теперь можно создать новую базу данных в интерактивном режиме. Например, необходимо создать базу данных с именем `test.fdb` и сохранить ее в каталоге `data` на диске `D`:

```
SQL>create database 'D:\data\test.fdb' page_size 8192
CON>user 'sysdba' password 'masterkey';
```

В операторе `CREATE DATABASE` обязательно нужно заключать в кавычки (одинарные или двойные) путь и пароль. Заключение имени пользователя в кавычки необязательно, если только оно не чувствительно к регистру или не содержит пробелов, международных символов или любых других символов, которые не допускаются в обычном (без кавычек) идентификаторе.

Если строка подключения не начинается с имени хоста или протокола, будет предпринята попытка создания файла базы данных под именем владельца операционной системы. Если добавите `localhost:` или протокол к пути или псевдониму, серверный процесс создаст файл и станет его владельцем.

База данных будет создана и появится сообщение `SQL`. Теперь соединение с новой базой данных установлено и можно приступить к созданию тестовых объектов в ней.

Чтобы убедиться, что база данных действительно существует, можно выполнить следующий запрос:

```
SQL>select * from rdb$relations;
```

Этот запрос выбирает все строки в системной таблице `RDB$RELATIONS`, где РЕД База Данных хранит метаданные для таблиц. "Пустая" база данных на самом деле не пуста: она содержит ряд системных таблиц и других объектов. Системные таблицы будут расти по мере того, как в базу данных будут добавляться пользовательские объекты.

Чтобы вернуться в командную строку, введите `QUIT` или `EXIT`.

6.3.3 Создание базы данных от имени пользователя без привилегий

Если вы попытаетесь создать базу данных не во встроенном режиме от имени пользователя, который не является администратором (т.е. `SYSDBA` или пользователь с ролью `RDB$ADMIN`), результат будет следующим:

```
SQL>create database 'xnet://D:\data\mydb.fdb' user 'john' password 'lennon';
Statement failed, SQLSTATE = 28000
no permission for CREATE access to DATABASE D:\DATA\MYDB.FDB
```

Пользователи, которые не являются администраторами, должны явно получить право на создание баз данных от администратора:

```
SQL>grant create database to user john;
```

Обладатель привилегии `CREATE DATABASE`, который при этом не является администратором, может создавать базы данных.

6.4 Создание базы данных с помощью РБДЭксперт

Для создания базы данных выберите соответствующий пункт в меню `База данных` или нажмите на кнопку `Создать базу данных` в панели инструментов. Заполните поля в открывшемся окне и нажмите на кнопку `Создать`.

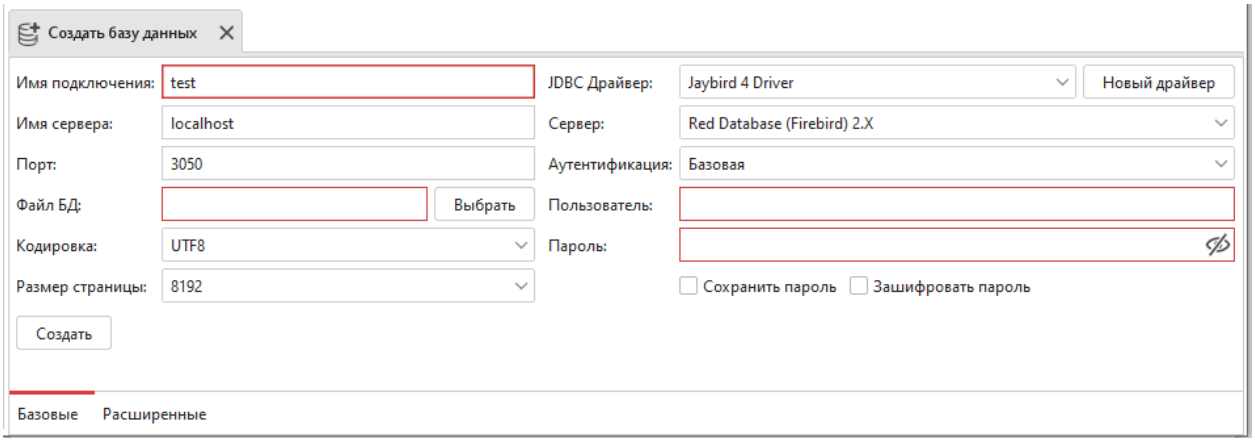


Рисунок 6.3 — Создание базы данных

При попытке создания базы данных может возникнуть ошибка шифрования сетевого соединения. Для поддержки шифрования необходима версия `Java` не ниже `1.8.0_161` или установленное `JCE` дополнение. В противном случае следует изменить значение параметра `WireCrypt = Disabled` в `firebird.conf`.

Глава 7

Особенности SQL

Каждая система управления базами данных имеет свои особенности в реализации SQL. РЕД База Данных придерживается стандарта SQL.

7.1 Деление целого числа на целое число

РЕД База Данных соответствует стандарту SQL, обрезая результат вычисления деления целого на целое до следующего меньшего целого числа. Это может привести к неожиданным результатам, если вы не знаете об этом.

Например, это вычисление корректно в SQL:

```
1 / 3 = 0
```

Если вы переходите с СУБД, в которой деление целого на целое выполняется с плавающим коэффициентом, вам нужно изменить все затронутые выражения, чтобы использовать тип `float` или `numeric` для делимого, делителя или обоих.

Например, приведенный выше пример можно изменить таким образом, чтобы получить ненулевой результат:

```
1.000 / 3 = 0.333
```

7.2 Работа со строками

7.2.1 Символ разделителя строк

Строки в РЕД Базе Данных разделяются парой символов одинарной кавычки (апострофа): `'I am a string'` (код ASCII 39, а не 96). Двойные кавычки нельзя использовать в качестве разделителя строк в SQL-запросах.

7.2.2 Апострофы в строках

Если вам необходимо использовать апостроф в строке, нужно экранировать символ апострофа, поставив перед ним другой апостроф.

Например, эта строка выдаст ошибку:

```
'Joe's Emporium'
```

Потому что синтаксический анализатор встречает апостроф и интерпретирует строку как `'Joe'`, за которой следуют какие-то неизвестные ключевые слова. Чтобы сделать эту строку допустимой, нужно продублировать символ апострофа:

```
'Joe''s Emporium'
```

Обратите внимание, что это две одинарные кавычки, а не одна двойная.

Также можно использовать альтернативный литерал строки `quote`, позволяющий использовать кавычки без экранирования:

```
q'{Joe's Emporium}'
```

7.2.3 Конкатенация строк

Символ конкатенации в SQL - это "||", или пара символов ASCII 124 без пробела между ними. В SQL символ "+" является арифметическим оператором, и его использование для конкатенации строк приведет к ошибке. Следующее выражение добавляет к значению символьного столбца строку "Reported by:":

```
'Reported by: ' || LastName
```

РЕД База Данных выдаст ошибку, если результат конкатенации строк превысит максимальный размер VARCHAR в 64 Кб. Если только потенциально возможный результат слишком длинный, вы получите предупреждение, но операция будет завершена успешно.

7.2.4 Идентификаторы с двойными кавычками

До появления стандарта SQL-92 было запрещено использовать в базе данных имена объектов (идентификаторы), которые дублировали ключевые слова, были чувствительны к регистру или содержали пробелы или специальные символы. В SQL-92 введен новый синтаксис, позволяющий сделать любые из них допустимыми при условии, что идентификаторы определены внутри пар двойных кавычек (ASCII 34) и на них всегда ссылаются с использованием разделителей двойных кавычек.

Если определить идентификатор в двойных кавычках, его чувствительность к регистру и обязательное использование двойных кавычек останутся обязательными.

РЕД База Данных допускает исключение из правил при некоторых условиях. Если идентификатор, который был определен в двойных кавычках и определен в верхнем регистре, не является ключевым словом, и соответствует остальным правилам обычных идентификаторов, то его можно использовать в SQL без кавычек и без учета регистра. Но как только вокруг него появятся двойные кавычки, необходимо снова проверить регистр.

Если есть таблицы "TESTTABLE" и "TestTable", обе определенные в двойных кавычках, то выполнив команду:

```
select * from TestTable;
```

в результате получите записи из "TESTTABLE", а не из "TestTable".

Если нет веских причин для определения идентификаторов в кавычках, рекомендуется избегать их.

7.3 Выражения, содержащие NULL

В SQL NULL не является значением. Это состояние элемента данных, при котором его значение неизвестно. Поскольку значение неизвестно, NULL не может вести себя как значение. Если попытаться выполнить арифметические действия с NULL или связать его со значениями в других выражениях, результатом операции почти всегда будет NULL. Это не ноль, не пустота и не "пустая строка", и он не ведет себя как любое из этих значений.

Все следующие выражения возвращают NULL:

- 1 + 2 + 3 + NULL
- NOT (NULL)

- `'Home ' || 'sweet ' || NULL`

Следующее выражение вернет `NULL`, если `FirstName` или `LastName` - `NULL`. В противном случае оно объединит два имени с пробелом между ними, даже если любая из переменных является пустой строкой:

```
FirstName || ' ' || LastName
```

Рассмотрим несколько примеров `PSQL` (`Procedural SQL`) с if-конструкциями:

- Равенство (`'='`):

```
if (a = b) then
        MyVariable = 'Equal';
else
        MyVariable = 'Not equal';
```

После выполнения данного кода переменная `MyVariable` примет значение `"Not equal"`, если и `a`, и `b` будут `NULL`. Причина в том, что `a = b` дает `NULL`, если хотя бы одно из них является `NULL`. Если тестовое выражение оператора `if` равно `NULL`, оно ведет себя как `false`: блок `then` пропускается, а блок `else` выполняется.

Хотя в этом случае выражение может вести себя как `false`, оно все равно является `NULL`. Если попытаетесь инвертировать его с помощью `not()`, то получите еще один `NULL`, а не `"true"`.

- Не равно (`'<>'`):

```
if (a <> b) then
        MyVariable = 'Not equal';
else
        MyVariable = 'Equal';
```

В этом случае переменная `MyVariable` примет значение `'Equal'`, если `a = NULL`, а `b` - нет, или наоборот.

7.3.1 Ключевое слово DISTINCT

Функция `IS [NOT] DISTINCT`, позволяющая проверять на равенство с учетом `NULL`. Семантика следующая:

- Два выражения не равны (`DISTINCT`), если у них разные значения или если одно из них `NULL`, а другое - нет;
- Они равны (`NOT DISTINCT`), если имеют одинаковое значение или оба являются `NULL`.

Если ни один из операндов не является `NULL`, `IS DISTINCT` работает точно так же, как оператор `"<>"`, а `IS NOT DISTINCT` - как оператор `"="`.

`IS DISTINCT` и `IS NOT DISTINCT` всегда возвращают `true` или `false`, и никогда `NULL`.

Используя `DISTINCT`, можно переписать первый пример с `PSQL` следующим образом:

```
if (a is not distinct from b) then
        MyVariable = 'Equal';
else
        MyVariable = 'Not equal';
```

А второй:

```
if (a is distinct from b) then
        MyVariable = 'Not equal';
else
        MyVariable = 'Equal';
```

Глава 8

Защита данных

8.1 Резервное копирование

РЕД База Данных поставляется с двумя утилитами для резервного копирования и восстановления баз данных: `gbak` и `nbackup`. Обе утилиты можно найти в каталоге установки (на `Windows`) или в его подкаталоге `bin` (на `Linux`). Резервное копирование баз данных может быть выполнено, пока пользователи подключены к системе и работают с базой данных. Резервная копия отображает состояние базы данных на момент начала создания резервной копии.

Регулярное резервное копирование и периодическое восстановление должны быть запланированной частью работы с базой данных.

Глава 9

Как не повредить базу данных

9.1 Не отключайте Forced Writes

По умолчанию РЕД База Данных создаёт новые базы данных со включенной опцией `forced writes` (принудительной записью). При этом любые подтвержденные изменения сразу записываются в файл базы данных.

Можно настроить базу данных на использование асинхронной записи данных. При этом измененные или новые данные будут храниться в кэше для периодической отправки на диск подсистемой ввода-вывода операционной системы. Обычно такую конфигурацию называют `forced writes off`. К ней иногда прибегают в попытке повысить производительность при выполнении больших пакетных операций.

9.1.1 Отключение forced writes на Windows

> Не отключайте `forced write` на `Windows`!

Было замечено, что серверные платформы `Windows` не очищают кэш записей до тех пор, пока служба `RedDatabase` не будет закрыта. Если на сервере `Windows` что-то пойдёт не так и система ввода-вывода окажется недоступной, то работа пользователей будет потеряна в процессе перезагрузки.

9.1.2 Отключение forced writes на Linux

Серверы `Linux` безопаснее в случае выполнения операций с временно отключенным `forced writes`. Но не стоит оставлять `forced writes` отключенным после завершения большой пакетной задачи.

9.2 Не выполняйте восстановление из резервной копии в работающую базу данных

Одна из опций восстановления в утилите `gbak` (`gbak -rep[lace_database]`) позволяет восстановить резервную копию поверх существующей базы данных. При этом возможно, что восстановление будет происходить без предупреждения, пока пользователи подключены к базе данных. В результате почти наверняка произойдет повреждение базы данных.

Обратите внимание, что краткая форма этой команды `gbak -rep`, а не `gbak -r`, как это было в старых версиях РЕД Базы Данных. Опция `gbak -r` теперь является сокращением от `gbak -recreate_database`, которое работает так же, как и `gbak -c[reate]`, и выдает ошибку, если указанная база данных уже существует. Можно принудительно перезаписать существующую базу данных, добавив флаг `o[verwrite]`. Этот флаг поддерживается только с `gbak -r`, но не с `gbak -c`.

Если это возможно, рекомендуется восстановить базу данных на свободное место на диске с помощью опции `gbak -c` и протестировать восстановленную базу данных с помощью `isql` или предпочитаемого вами инструмента администрирования. Если восстановленная база данных в порядке, отключите старую базу данных. Для этого можно использовать инструмент командной строки `gfix`. На всякий случай сделайте копию файловой системы старой базы данных, а затем скопируйте файлы восстановленной базы данных поверх их существующих аналогов.

9.3 Не позволяйте пользователям входить в систему во время восстановления с опцией -rep

Если вы не заблокируете доступ пользователей при выполнении восстановления с помощью `gbak -rep`, то пользователи смогут войти в систему и выполнить операции с данными. Это приведет к повреждению данных.