RuBackup

Система резервного копирования
и восстановления данных

РАЗВЁРТЫВАНИЕ СРК

ВЕРСИЯ 2.4.0, 13.03.2025

Содержание

Для развёртывания системы резервного копирования:

1. Подготовьте пакеты компонентов СРК:
   - получите Глава 1;
   - скопируйте их на узлы, на которых будут развёрнуты компоненты СРК.
2. Разверните СУБД PostgreSQL и настройте подключения к БД серверной группировки СРК (основной, резервный, медиа- сервера) и АРМ администратора:
   - Установка СУБД;
   - Настройка СУБД.

   Служебная база данных может быть установлена на узле основного сервера или любом другом доступном по сети узле, удовлетворяющем системным требованиям.
3. Подготовьте узлы к установке компонентов СРК:
   - Подготовка к установке серверной части;
   - Подготовка к установке клиентской части под управлением Linux-систем;
   - Подготовка к установке клиентской части под управлением Windows-систем.
4. Установите пакеты компонентов RuBackup на подготовленных узлах:
   - Установка пакетов серверной части;
   - Установка пакетов клиентской части под управлением Linux-систем;
   - Установка пакетов клиентской части под управлением Windows-систем.
5. Подготовьте лицензионные файлы для авторизации основного, резервного, медиасерверов, предварительно получив их у поставщика, и произведите Раздел 4.2.3.
6. Выполните настройку установленных компонентов СРК в строго определенном порядке:
   a. на серверах (основном, резервном, медиасерверах):
      - Настройка сервера;
   b. на всех клиентах РК:
      - Настройка клиента РК под управлением Linux-систем;
      - Настройка клиента РК под управлением Windows-систем.
7. Выполните настройки:
   a. для пользователей, которые будут взаимодействовать с компонентами СРК:

- Настройка пользователей для серверной части;
- Настройка пользователей для клиентской части под управлением Linux-системы;

b. для узла:

- Настройка узла под управлением Windows-систем.

8. Добавьте сервисы СРК в автозагрузку:
   - Добавление в автозапуск серверной части;
   - Добавление в автозапуск клиентской части под управлением Linux-системы;
   - Добаление в автозапуск клиентской части под управлением Windows-систем.
9. Произведите запуск развёрнутых компонентов СРК:
   - Запуск серверной части;
   - Запуск клиентской части под управлением Linux-системы;
   - Запуск клиентской части под управлением Windows-систем.

Глава 1. Дистрибутивы

Для развёртывания компонентов СРК RuBackup получите актуальные установочные deb/rpm пакеты одним из способов:

- на компакт-диске, полученном от поставщика;
- из дополнительно подключаемого, публичного репозитория;
- скачав актуальные установочные пакеты СРК RuBackup из облачного диска Астры на официальном сайте компании https://www.rubackup.ru/go/.

1.1. Компакт-диск

Пакеты для развёртывания СРК RuBackup могут быть получены от поставщика на компакт-диске, который может быть прочитан большинством приводов CD-ROM.

1.2. Публичный репозиторий

Пакеты для развёртывания СРК RuBackup могут быть установлены из дополнительного публичного репозитория.

Публичные репозитории доступны для операционных систем:

- Astra Linux 1.8;
- Astra Linux 1.7;
- Astra Linux 1.6;
- Debian 12;
- Debian 10;
- Ubuntu 22.04;
- Ubuntu 20.04;
- Ubuntu 18.04;
- CentOS 7;
- CentOS 8;
- РЕД ОС 7.3;
- РЕД ОС 8;
- Red Hat Enterprise Linux 9;
- ROSA Fresh Desktop 12;
- ROSA Enterprise Linux Server 7.3;
- ROSA Enterprise Linux Server 7.9.

1.2.1. Подключение публичного репозитория DEB-систем

1. Создайте файл с информацией о репозиториях:

```
cat <<EOF | sudo tee /etc/apt/sources.list.d/rubackup_deb.list
deb https://dl.astralinux.ru/rubackup/repository-deb-main/ <OS-VERSION>
public
deb https://dl.astralinux.ru/rubackup/repository-deb-main/ <OS-VERSION>
public-testing
EOF
```

   где: `<OS-VERSION>` — версия используемой ОС:

   - astra_1.6;
   - astra_1.7;
   - astra_1.8;
   - debian_10;
   - debian_12;
   - ubuntu_18.04;
   - ubuntu_20.04;
   - ubuntu_22.04.

2. Добавьте ключ репозитория:

```
sudo wget -qO-
https://dl.astralinux.ru/artifactory/api/security/keypair/gc-astra-
official-repo-key/public | gpg --no-default-keyring --keyring gnupg-
ring:/etc/apt/trusted.gpg.d/rubackup-deb.gpg --import - && sudo chmod 644
/etc/apt/trusted.gpg.d/rubackup-deb.gpg
```

3. Обновите список пакетов:

```
sudo apt-get update
```

1.2.2. Подключение публичного репозитория RPM-систем

1. Создайте файл с информацией о репозиториях:
   a. для ОС:
      - CentOS 7;

- CentOS 8;
- РЕД ОС 7.3;
- РЕД ОС 8;
- Red Hat Enterprise Linux 9;
- ROSA Fresh Desktop 12;
- ROSA Enterprise Linux Server 7.9.

```
cat <<EOF | sudo tee /etc/yum.repos.d/rubackup_rpm.repo
[rubackup-rpm-public-repository]
name=rubackup rpm public repository
baseurl=https://dl.astralinux.ru/artifactory/rubackup-rpm-main/<OS-
VERSION>/public/
enabled=1
repo_gpgcheck=1
gpgkey=https://dl.astralinux.ru/artifactory/rubackup-rpm-main/<OS-
VERSION>/public/repodata/repomd.xml.key
gpgcheck=0

[rubackup-rpm-public-testing-repository]
name=rubackup rpm public testing repository
baseurl=https://dl.astralinux.ru/artifactory/rubackup-rpm-main/<OS-
VERSION>/public-testing/
enabled=1
repo_gpgcheck=1
gpgkey=https://dl.astralinux.ru/artifactory/rubackup-rpm-main/<OS-
VERSION>/public-testing/repodata/repomd.xml.key
gpgcheck=0
EOF
```

где: `<OS-VERSION>` — версия используемой ОС:

- centos_7;
- centos_8;
- redos_7.3;
- redos_8;
- rhel_9;
- rosa_12;
- rosa_7.9.

b. для ОС ROSA Enterprise Linux Server 7.3:

```
cat <<EOF | sudo tee /etc/yum.repos.d/rubackup_rpm.repo
[rubackup-rpm-public-repository]
name=rubackup rpm public repository
baseurl=https://dl.astralinux.ru/artifactory/rubackup-rpm-
main/rosa_7.3/public/
enabled=1
repo_gpgcheck=1
gpgkey=https://dl.astralinux.ru/artifactory/rubackup-rpm-
main/rosa_7.3/public/repodata/repomd.xml.key
gpgcheck=0
sslverify=0

[rubackup-rpm-public-testing-repository]
name=rubackup rpm public testing repository
baseurl=https://dl.astralinux.ru/artifactory/rubackup-rpm-
main/rosa_7.3/public-testing/
enabled=1
repo_gpgcheck=1
gpgkey=https://dl.astralinux.ru/artifactory/rubackup-rpm-
main/rosa_7.3/public-testing/repodata/repomd.xml.key
gpgcheck=0
sslverify=0
EOF
```

1.3. Облачный диск Астры

Пакеты для развёртывания СРК RuBackup могут быть скачаны из облачного диска Астры на официальном сайте компании https://www.rubackup.ru/go/.

На диске вы найдёте:

- папки с названиями операционных систем, содержащие совместимые с указанной ОС установочные пакеты для развёртывания компонентов СРК RuBackup (Alt Linux 10, Astra Linux 1.6 и т.д.);
- папку `Experimental`, содержащую:
  - совместимые с указанной ОС экспериментальные установочные пакеты для развёртывания компонентов СРК RuBackup, прошедшие только дизайн-тестирование;
  - папку `Scripts`, содержащую экспериментальные скрипты:
    - `script_block_device_metadata.sh` скрипт резервного копирования метаданных дедуплицированного пула;
    - `upgrade_rubackup_packages.sh` скрипт автоматического обновления;

- папку `Prev_Version`, содержащую установочный пакет модуля резервного копирования и восстановления данных кластеров СУБД PostgreSQL для поддержки нового функционала серверной и клиентской группировок релиза 2.1;
- `RB_key.iso` — специализированный загрузочный образ RuBackup.

Глава 2. Сетевые порты

Безопасное соединение компонентов СРК RuBackup и обмен информацией между ними подразумевает техническую возможность коммуникации по сети. Перед установкой продукта необходимо обеспечить взаимодействие компонентов СРК путем открытия соответствующих портов для входящего и исходящего трафика между серверами, на которых установлены компоненты СРК.

В таблице представлены компоненты СРК RuBackup, которые принимают входящие соединения по указанным портам и протоколам.

Таблица 1. Сетевые порты

Компонент		Целевой сервис	Протокол	Порт	Описание
от	до				
Основной сервер	Медиасервер	rubackup-cmd	TCP	9991	Управление операциями на медиасервере
		rubackup-media	TCP	9993	Управление операциями с данными
Основной сервер	База данных RuBackup на отдельностоящей машине	postgresql	TCP	5432 [1]	Сохранение конфигурационной и оперативной информации
Резервный сервер [2]	Основной сервер	rubackup-cmd	TCP	9991	Обеспечение отказоустойчивости
		rubackup-media	TCP	9993	Передача данных между медиасерверами в составе основного и резервного серверов
Резервный сервер [2]	База данных RuBackup на отдельностоящей машине	postgresql	TCP	5432	Сохранение конфигурационной и оперативной информации
Медиасервер	Медиасервер	rubackup-media	TCP	9993	Передача данных между медиасерверами

Медиасервер	Резервный сервер [2]	rubackup-cmd	TCP	9991	Управление операциями на медиасервере
		rubackup-media	TCP	9993	Управление операциями с данными
Медиасервер	База данных RuBackup на отдельностоящей машине	postgresql	TCP	5432 [1]	Сохранение конфигурационной и оперативной информации
Клиент резервного копирования	Основной сервер	rubackup-cmd	TCP	9991	Управление операциями на клиенте резервного копирования
Клиент резервного копирования	Медиасервер	rubackup-media	TCP	9993	Передача данных между медиасервером и клиентом
Клиент резервного копирования	Резервный сервер [2]	rubackup-cmd	TCP	9991	Управление операциями на клиенте резервного копирования
		rubackup-media	TCP	9993	Передача данных между медиасервером и клиентом
RuBackup REST API	Основной сервер	rubackup-rbm	TCP	9995	Отправка запросов на сервер и получение информации
RuBackup REST AP	База данных RuBackup на отдельностоящей машине	postgresql	TCP	5432 [1]	Получение информации из базы данных
RuBackup REST API	Резервный сервер [2]	rubackup-rbm	TCP	9995	Отправка запросов на сервер и получение информации

Менеджер RuBackup (RBM) на отдельно стоящей машине	База данных RuBackup на отдельностоящей машине	postgresql	TCP	5432 [1]	Сохранение конфигурационной и оперативной информации
Менеджер RuBackup (RBM) на отдельно стоящей машине	Основной сервер	rubackup-rbm	TCP	9995	Управление операциями RuBackup
Менеджер RuBackup (RBM) на отдельно стоящей машине	Резервный сервер [2]	rubackup-rbm	TCP	9995	Управление операциями RuBackup
Клиент, посылающий запрос через RuBackup REST API	Основной сервер	rubackup-api	HTTPS	443 [3]	Управление операциями RuBackup через REST API
Клиент, посылающий запрос через RuBackup REST API	Резервный сервер [2]	rubackup-api	HTTPS	443 [3]	Управление операциями RuBackup через REST API

[1] Если база данных настроена с использованием нестандартного порта, то для подключения к ней продукта RuBackup порт может быть изменен вручную в конфигурационном файле /opt/rubackup/etc/config.file.

[2] При наличии резервного сервера.

[3] Порт для подключения, при необходимости, может быть изменен через переменные окружения в файле /opt/rubackup/etc/rubackup_api.env (см. в «Руководстве по установке и взаимодействию с программным интерфейсом RuBackup REST API»)

Глава 3. Служебная база данных

СУБД PostgreSQL используется для хранения метаданных резервных копий и конфигурационных параметров системы резервного копирования RuBackup.

3.1. Системные требования

Таблица 2. Аппаратные требования к серверу БД RuBackup

Аппаратный компонент	Значение
Процессор	4 ядра
Оперативная память	64 ГБ
Дисковое пространство	3,84 ТБ

Для обеспечения максимального уровня отказоустойчивости и быстродействия при промышленной эксплуатации, рекомендуется использовать в качестве конфигурационной базы RuBackup СУБД PostgreSQL в отказоустойчивой конфигурации с использованием решения Patroni, развернутом на отдельно стоящих машинах, с совокупным объемом дискового пространства 3.84 ТБ, построенного с использованием твердотельных накопителей, подключенных через шину PCI Express (NVMe SSD).

3.2. Установка СУБД

1. Установите из репозитория [1] последнюю доступную версию СУБД PostgreSQL, находясь в папке, где расположен пакет:

Astra Linux, Debian, Ubuntu	`sudo apt install postgresql`
Альт	`sudo apt-get install postgresql-server`
Rosa Cobalt, RHEL	`sudo yum install postgresql`
RedOS, CentOS, Rosa Chrome	`sudo dnf install postgresql-server`

2. Выполните установку последней доступной версии пакета `postgresql-contrib`:

Для Astra Linux SE 1.6 необходимо установить пакет `postgresql-contrib-9.6`.

Astra Linux, Debian, Ubuntu	`sudo apt install postgresql-contrib`
Альт	`sudo apt-get install postgresql-contrib`
Rosa Cobalt, RHEL	`sudo yum install postgresql-contrib`

RedOS, CentOS, Rosa Chrome	`sudo dnf install postgresql-contrib`

3. Произведите инициализацию БД:

Astra Linux, Debian, Ubuntu	-
Альт	`sudo /etc/init.d/postgresql initdb`
Rosa Cobalt, RHEL	`/usr/pgsql-12/bin/postgresql-12-setup initdb`
RedOS, CentOS, Rosa Chrome	`sudo postgresql-setup --initdb`

4. Запустите PostgreSQL:

```
sudo service postgresql start
```

5. Добавьте запуск PostgreSQL в автозагрузку:

```
sudo systemctl enable postgresql
```

3.3. Настройка СУБД

1. Настройте возможность подключения к СУБД для всех серверов, которые будут входить в серверную группировку RuBackup (основной, резервный, медиа- сервера), и АРМ администратора RuBackup, для этого:
   - перейдите в папку, где находится файл `pg_hba.conf`;
   - откройте для редактирования конфигурационный файл `pg_hba.conf`:

     ```
     sudo nano pg_hba.conf
     ```

   - отредактируйте, открывшийся файл, указав ip-адреса и маску сети всех подключаемых серверов и АРМ администратора RuBackup к БД по протоколу IPv4, например:

`local`	`all`	`postgres`		`peer`
# TYPE	DATABASE	USER	ADDRESS	METHOD
# *local* is for Unix domain socket connections only				
`local`	`all`	`all`		`md5`
IPv4 local connections:				
`host`	`all`	`all`	`127.0.0.1/32`	`md5`

host	all	all	192.168.0.50/32	md5
host	all	all	192.168.0.51/32	md5
host	all	all	192.168.0.52/32	md5
host	all	all	192.168.0.53/32	md5

- сохраните изменения.

Добавить ip-адреса подключаемых к БД серверов можно и после установки сервера RuBackup, отредактировав конфигурационный файл `pg_hba.conf` и перезапустив PostgreSQL.

2. Настройте прослушивание подключений к БД для всех серверов, которые будут входить в серверную группировку RuBackup (основной сервер, резервный сервер, медиасервер) с целью последующего удалённого подключения к БД:

   - перейдите в папку, где находится файл `postgresql.conf`;
   - откройте для редактирования конфигурационный файл `postgresql.conf`:

     ```
     sudo nano postgresql.conf
     ```

   - отредактируйте открывшийся файл:
     - в секции `CONNECTIONS AND AUTHENTICATION`, добавив выделенную строку:

# CONNECTIONS AND AUTHENTICATION	
#--	
# - Connection Settings -	
#listen_addresses = 'localhost'	# what IP address(es) to listen on;
listen_addresses = '*'	
	# comma-separated list of addresses;
	# defaults to 'localhost'; use '*' for all
	# (change requires restart)
port = 5432	# (change requires restart)
max_connections = 100	# (change requires restart)

     - при необходимости отредактируйте значение параметра `shared_buffers`. Рекомендуемое значение параметра ~50 % от размера оперативной памяти;
     - при необходимости отредактируйте значение параметра `max_parallel_workers`. Рекомендуемое значение параметра не менее 50 % от количества процессорных ядер, если сервер СУБД совмещен с

сервером RuBackup и 100 %, если сервер СУБД является выделенным.

- сохраните изменения.

3. Чтобы не возникала ошибка при получении мандатных атрибутов, нужно отредактировать конфигурационный файл СУБД PostgreSQL `/etc/parsec/mswitch.conf` в ОС Astra Linux Special Edition с максимальным уровнем защищенности («Смоленск»).

   Данный шаг выполняется только для СУБД PostgreSQL в ОС Astra Linux Special Edition с максимальным уровнем защищенности («Смоленск»).

   - Откройте для редактирования файл `/etc/parsec/mswitch.conf` и измените параметр для создания пользователя СУБД PostgreSQL, который не назначен в ОС Astra Linux Special Edition 1.7:

     ```
     sudo nano /etc/parsec/mswitch.conf
     ```

   - отредактируйте значение указанного параметра, изменив его на `yes`:

     ```
     zero_if_notfound: yes
     ```

   - сохраните изменения.

4. Для применения изменений перезапустите Postgres:

   ```
   sudo service postgresql restart
   ```

5. Проверьте подключение к СУБД, выполнив вход под пользователем `postgres`, введя команду:

   ```
   sudo -u postgres psql
   ```

6. Далее, подключившись к БД, задайте пароль для пользователя `postgres`:

   ```
   alter user postgres password '12345';
   ```

   где `'12345'` — задаваемый пароль пользователя.

7. Завершите работу под пользователем `postgres`:

```
\q
```

3.4. Настройка SSL соединений

Для повышения безопасности сервера базы данных возможно использование надежного шифрования соединений с базой данных.

Для настройки SSL соединений:

1. Создайте сертификаты для сервера PostgreSQL и его клиентов (postgres-клиентов) (см. Раздел 3.4.1).
2. Выполните настройку конфигурационных файлов на сервере PostgreSQL (см. Раздел 3.4.2).
3. После установки пакетов компонентов СРК скопируйте полученные сертификаты и выполните настройку SSL соединений для postgres-клиентов на узлах (см. Раздел 3.4.3):
   - развёрнутой серверной части СРК;
   - использующих приложение «Менеджер администратора RuBackup» или «Веб-интерфейс Tucana».

3.4.1. Выпуск сертификатов

Аутентификация клиента по сертификату позволяет серверу проверить личность подключающегося, подтверждая, что сертификат X.509, представленный postgres-клиентом, подписан доверенным центром сертификации (CA).

Сертификаты SSL проверяются и выдаются Центром сертификации.

Если вы не имеете PKI инфраструктуры открытых ключей, то на отдельном хосте, который может выполнять роль Центра сертификации:

1. Создайте директории, в которые будут сгенерированы сертификаты Центра сертификации, сервера PostgreSQL и для всех postgres-клиентов (в зависимости от архитектуры вашей СРК):

   ```
   mkdir certs && cd certs && mkdir ca pg-server rb-server rb-media rb-rbm
   ```

   где:

   - `ca` - директория для сертификатов Центра сертификации;
   - `pg-server` - директория для сертификатов сервера PostgreSQL;
   - `rb-server` - директория для сертификатов основного сервера RuBackup;

- `rb-media` - директория для сертификатов медиасервера;
- `rb-rbm` - директория для сертификатов APM администратора, если Менеджер администратора RuBackup (RBM) развёрнут на отдельном хосте.

2. Создайте закрытый ключ Центра сертификации, для этого:
   - Перейдите в ранее созданную папку:

     ```
     cd ./ca
     ```

   - Сгенерируйте закрытый ключ для CA (`ca.key`), выполнив команду, например:

     ```
     openssl genrsa -out ca.key 2048
     ```

   - Создайте самоподписанный сертификат Центра сертификации (`ca.crt`) сроком действия 1 год:

     ```
     openssl req -new -x509 -days 365 -key ca.key -out ca.crt
     ```

     где `CN` — это полное имя хоста (FQDN), на котором развёрнут CA.

3. Выпустите сертификат и закрытый ключ для сервера PostgreSQL, для этого:
   - Перейдите в ранее созданную папку:

     ```
     cd ./pg-server
     ```

   - Сгенерируйте закрытый ключ для сервера PostgreSQL `/pg-server/server.key`:

     ```
     openssl genrsa -out server.key 2048
     ```

   - Сгенерируйте запрос на сертификат сервера PostgreSQL `/pg-server/server.csr`:

     ```
     openssl req -new -key server.key -out server.csr
     ```

     где `CN` — это полное имя хоста (FQDN), на котором развёрнут сервер PostgreSQL.

   - Подпишите запрос на сертификат сервера PostgreSQL закрытым ключом Центра сертификации:

```
openssl x509 -req -in server.csr -CA ../ca/ca.crt -CAkey ../ca/ca.key
-CAcreateserial -out server.crt -days 365
```

4. Повторите шаг 3 для каждого postgres-клиента, сгенерировав закрытый ключ (`postgresql.key`) и выпустив сертификат (`postgresql.crt`) для всех postgres-клиентов, указав в сертификате соответствующее FQDN хоста, на котором развёрнут компонент CPK.

3.4.2. Настройка SSL соединения на сервере PostgreSQL

Выполните приведённые ниже настройки, чтобы сервер PostgreSQL прослушивал как обычные, так и SSL соединения через один и тот же TCP-порт и согласовывал использование SSL с любым подключающимся postgres-клиентом.

1. Скопируйте в папку `/etc/postgresql/16/main` на сервер PostgreSQL из папки `/pg-server` Центра сертификации подготовленные:
   - сертификат Центра сертификации (`ca.crt`);
   - подписанный сертификат сервера PostgreSQL (`server.crt`);
   - сгенерированный закрытый ключ сервера PostgreSQL (`server.key`).
2. Для файлов сертификата и закрытого ключа установите полный доступ на чтение и запись только для владельцев:

   ```
   chmod 600 server.crt server.key ca.crt
   ```

   Сделайте владельцем файлов пользователя и группу пользователя `postgres`:

   ```
   chown postgres:postgres server.crt server.key ca.crt
   ```

3. Отредактируйте конфигурационный файл `postgresql.conf`:
   - включите поддержку зашифрованных соединений:

     ```
     ssl = on
     ```

   - укажите путь к файлу сертификата Центра сертификации (или цепочке сертификатов):

     ```
     ssl_ca_file = '/etc/postgresql/16/main/ca.crt'
     ```

     Сертификат CA проверяет, что сертификат postgres-клиента подписан дове-

ренным центром сертификации.

- укажите путь к файлу сертификата сервера PostgreSQL:

```
ssl_cert_file = '/etc/postgresql/16/main/server.crt'
```

Сертификат будет отправлен postgres-клиенту для указания подлинности сервера PostgreSQL.

- укажите путь к файлу закрытого ключа сервера PostgreSQL:

```
ssl_key_file = '/etc/postgresql/16/main/server.key'
```

Закрытый ключ доказывает, что сертификат сервера PostgreSQL был отправлен владельцем; не указывает, что владелец сертификата заслуживает доверия.

4. Чтобы потребовать от postgres-клиента предоставления доверенного сертификата, отредактируйте конфигурационный файл `pg_hba.conf`:
   - добавьте опцию аутентификации `clientcert=verify-ca` или `clientcert=verify-full` в соответствующие `hostssl` строки, где:
     - `clientcert=verify-full` сервер PostgreSQL не только проверяет цепочку сертификатов, но также проверяет, совпадает ли имя пользователя или его сопоставление с `CN` предоставленного сертификата;
     - `clientcert=verify-ca` сервер проверяет, что сертификат postgres-клиента подписан одним из доверенных центров сертификации.

     Также желательно закомментировать все строчки `host`, например:

```
#host    all all 0.0.0.0/0  md5
hostssl all all 0.0.0.0/0 [md5,cert]
clientcert=[verify-ca,verify-full] (1)
```

(1) В старых версиях [0,1]

где:

`md5` — запросить пароль пользователя,

`cert` — аутентификация по сертификату.

Если параметр `clientcert` не указан, сервер проверяет сертификат postgres-клиента по своему файлу CA, только если сертификат postgres-

клиента представлен и CA настроен.

5. Произведите настройку карты имён пользователей.

   При использовании внешней системы аутентификации, такой как `Ident`, имя пользователя операционной системы, инициировавшего подключение, может не совпадать с именем пользователя базы данных (роли), который должен использоваться. В этом случае карта имен пользователей может быть применена для сопоставления имени пользователя операционной системы с именем пользователя базы данных

   Чтобы использовать сопоставление имен пользователей, отредактируйте:

   - конфигурационный файл `pg_hba.conf` — укажите в значении параметра `map=map-name`:

     ```
     hostssl all all 0.0.0.0/0 md5 clientcert=verify-full map=sslmap
     ```

   - конфигурационный файл `pg_ident.conf`, хранящийся в каталоге данных кластера — настройте карты имен пользователей, добавьте, например:

     ```
     # MAPNAME SYSTEM-USERNAME PG-USERNAME
     sslmap    postgres        postgres
     sslmap    postgres        rubackup
     ```

     где:

     - в столбце `SYSTEM-USERNAME` укажите `CN` сертификата postgres-клиента;
     - в столбце `PG-USERNAME` укажите имя пользователя, с которым нужно сопоставить.

6. Для применения изменений перезапустите сервер:

   ```
   sudo systemctl restart postgresql
   ```

3.4.3. Настройка SSL соединения на узлах компонентов RuBackup

Для подключения серверных компонентов RuBackup и АРМ администратора СРК (использующего приложение «Менеджер администратора RuBackup») к служебной базе данных PostgreSQL с использованием защищённого соединения выполните приведённые ниже настройки на соответствующих узлах (postgres-клиентах):

- развёрнутой серверной части СРК;

- использующих приложение «Менеджер администратора RuBackup».

Настройка SSL соединения на узлах компонентов RuBackup

1. Перенесите из соответствующей postgres-клиенту папки на узле Центра сертификации подготовленные:
   - сертификат Центра сертификации (ca.crt), чтобы postgres-клиент мог проверить, что конечный сертификат сервера PostgreSQL был подписан его доверенным корневым сертификатом;
   - сертификат postgres-клиента (узла компонента СРК) (postgresql.crt);
   - сгенерированный закрытый ключ сервера/клиента СРК (postgresql.key).
2. Для файлов сертификата и закрытого ключа установите полный доступ на чтение и запись только для владельцев:

```
chmod 600 server.crt server.key ca.crt
```

3. Сделайте владельцем файлов пользователя, от имени которого будет запущен компонент СРК (postgres-клиент):

```
chown suser:suser server.crt server.key ca.crt
```

4. Настройка SSL соединения на узле компонента RuBackup выполняется **после установки пакетов СРК** одним из способов:
   - при настройке компонента СРК серверной или клиентской части;
   - при внесении правки в файл настроек сервера (полученный после конфигурирования компонента СРК).
5. Для настройки SSL-соединения с БД предварительно необходимо выполнить настройку служебной базы данных в соответствии с разделом Раздел 3.3 и подготовить сертификаты.
   a. `Enter sslmode ( allow, disable, prefer, require, verify-ca, verify-full ) [ require ]`

      `Enter path for sslrootcert file:`

      `Enter path for sslcert file:`

      `Enter path for sslkey file:`

      - выберите и введите название выбранного режима SSL в соответствии с таблицей.

По умолчанию выбран режим `require`.

Таблица 3. Описание режимов SSL

sslmode	Защита от прослушивания	Защита от MITM	Утверждение
disable	Нет	Нет	Мне не важна безопасность и я не приемлю издержки, связанные с шифрованием.
allow	Возможно	Нет	Мне не важна безопасность, но я приемлю издержки, связанные с шифрованием, если на этом настаивает сервер.
prefer	Возможно	Нет	Мне не важна безопасность, но я предпочитаю шифрование (и приемлю связанные издержки), если это поддерживает сервер.
require	Да	Нет	Я хочу, чтобы мои данные шифровались, и я приемлю сопутствующие издержки. Я доверяю сети в том, что она обеспечивает подключение к нужному серверу
verify-ca	Да	Зависит от политики ЦС	Я хочу, чтобы мои данные шифровались, и я приемлю сопутствующие издержки. Мне нужна уверенность в том, что я подключаюсь к доверенному серверу
verify-full	Да	Да	Я хочу, чтобы мои данные шифровались, и я приемлю сопутствующие издержки. Мне нужна уверенность в том, что я подключаюсь к доверенному серверу и это именно указанный мной сервер

- укажите расположение подготовленных сертификатов:
  - в поле `sslrootcert` укажите расположение сертификата центра сертификации;
  - в поле `sslcert` укажите расположение сертификата настраиваемого хоста;
  - в поле `sslkey` укажите расположение закрытого ключа настраиваемого хоста.Ы

3.5. Настройка балансировщика нагрузки

При наличии прокси-сервера HAProxy, принимающего запросы к служебной базе данных СРК RuBackup, рекомендуется выполнить следующие действия:

1. В файле `haproxy.cfg` задайте одинаковое значение для параметров `timeout client` и `timeout server`. Рекомендуемое значение 48h или более.

   Согласно официальной документации [2] значения параметров `timeout client` и `timeout server` должны быть идентичные.

2. Убедитесь, что в настройках служебной СУБД PostgreSQL отсутствуют таймауты, а если присутствуют, то выставить такие же значения как и в настройках HAProxy (см. пункт 1).

3. Добавьте в файл `haproxy.cfg` в строку с проверкой узла PostgreSQL параметр `shutdown-sessions`, например:

```
"server primary 192.168.122.60:3306 check on-marked-down shutdown-
sessions".
```

4. Завершите все активные задачи в СРК RuBackup.
5. Остановите сервис сервера СРК RuBackup, выполнив в терминале на узле сервера СРК RuBackup:

```
sudo systemctl stop rubackup_server
```

6. Перезапустите СУБД PostgreSQL, выполнив:

```
sudo systemctl restart postgresql
```

7. Запустите сервис сервера СРК RuBackup, выполнив в терминале на узле сервера СРК RuBackup:

```
sudo systemctl start rubackup_server
```

[1] Для некоторых ОС возможно потребуется подключить дополнительный репозиторий
[2] https://docs.haproxy.org/2.6/configuration.html

Глава 4. Серверная часть

Серверная часть СРК RuBackup может состоять из обязательного компонента — основного сервера, и одного или нескольких необязательных компонентов — резервного сервера и медиасервера.

Основной сервер — это главный управляющий сервер, обеспечивающий взаимодействие компонентов СРК. В случае установки способом «Всё в одном», в процессе которой все компоненты СРК RuBackup развёрнуты на одном хосте, основной сервер выполняет функцию медиасервера.

Резервный сервер, в случае отказа основного сервера, поддержит функционал основного сервера RuBackup, а клиенты системы резервного копирования автоматически подключатся к резервному серверу. После восстановления функционирования основного сервера клиенты подключатся обратно к основному серверу.

Медиасервер (это узел, на котором подключено устройство хранения) – ёмкое дисковое устройство или библиотека магнитных лент. Он наполняет ее поступающими резервными копиями данных и управляет им по требованию сервера резервного копирования. Каждый медиасервер ассоциирован с пулом, который содержит логические устройства одного типа — хранилища.

4.1. Системные требования

В данном подразделе приведены системные требования для каждого серверного компонента СРК RuBackup, предъявляемые к техническим средствам, необходимым для нормального функционирования СРК RuBackup.

В случае установки на один хост нескольких компонентов СРК RuBackup (например, при способе установки «Всё в одном») следует консолидировать соответствующие аппаратные требования, предъявляемые к техническому средству, на которое производится установка.

4.1.1. Аппаратные требования

Основной/резервный сервер

Минимальные аппаратные требования, необходимые для стабильного функционирования сервера СРК RuBackup приведены в таблице.

Таблица 4. Аппаратные требования, предъявляемые к серверу RuBackup

Аппаратный компонент	Объем хранимых данных			Примечание
	48 ТБ	96 ТБ	144 ТБ	
Процессор	10 ядер, 20 потоков (2 потока на 1 ядро или более)			Рекомендуемые модели: Intel Xeon 4210, AMD EPYC 7000 или более современные

Оперативная память	128 ГБ	256 ГБ	256 ГБ	—
Твердотельный накопитель (SSD)	RAID 1, 2 диска по 480 ГБ каждый			Объём дискового пространства для установки операционной системы и компонентов RuBackup, за исключением конфигурационной базы данных RuBackup.
Твердотельный накопитель, подключенный через шину PCI Express (NVMe SSD)	3.84 ТБ			Рекомендуется в случае развертывания инстанса PostgreSQL для конфигурационной базы данных RuBackup на той же машине, где установлен сервер RuBackup. Диски NVMe SSD позволяют повысить производительность операций в фильтре Блума и скорость обработки данных при выполнении процессов дедупликации. 3.84 Тб предусматривают потенциальный рост объемов обрабатываемых данных. Для обеспечения максимального уровня отказоустойчивости и быстродействия при промышленной эксплуатации рекомендуется использовать в качестве конфигурационной базы RuBackup СУБД PostgreSQL в отказоустойчивой конфигурации, например, с использованием решения Patroni, развернутом на отдельностоящих машинах.
Жесткий диск (HDD) или флэш-накопитель (flash drive)	RAID 50, 12 дисков по 4 ТБ каждый	RAID 50, 12 дисков по 8 ТБ каждый	RAID 50, 12 дисков по 12 ТБ каждый	Рекомендуется в случае активного использования машины с основным сервером в качестве медиасервера, для возможности расширения дискового пространства под хранение резервных копий. В случае хранения данных на опосредованных СХД, данный компонент не используется.
Сеть	2 сетевых адаптера с пропускной способностью 10 Гб каждый, с 2 портами (dual port)			—

Медиасервер

Рекомендуемая конфигурация медиасервера зависит от совокупного объема хранимых данных и схожа с конфигурацией сервера RuBackup. Для расчета конфигурации медиасервера воспользуйтесь таблицей.

Таблица 5. Аппаратные требования, предъявляемые к медиасерверу

Аппаратный компонент	Объем хранимых данных			Примечание
	48 ТБ	96 ТБ	144 ТБ	
Процессор	10 ядер, 20 потоков (2 потока на 1 ядро или более)			Рекомендуемые модели: Intel Xeon 4210, AMD EPYC 7000 или более современные
Оперативная память	128 ГБ	256 ГБ	256 ГБ	—

Твердотельный накопитель (SSD)	RAID 1, 2 диска по 480 ГБ каждый			Объём дискового пространства для установки операционной системы и компонентов RuBackup, за исключением конфигурационной базы данных RuBackup.
Жесткий диск (HDD) или флэш-накопитель (flash drive)	RAID 50, 12 дисков по 4 ТБ каждый	RAID 50, 12 дисков по 8 ТБ каждый	RAID 50, 12 дисков по 12 ТБ каждый	Для возможности расширения дискового пространства под хранение резервных копий. В случае хранения данных на опосредованных СХД, данный компонент не используется.
Сеть	2 сетевых адаптера с пропускной способностью 10 Гб каждый, с 2 портами (dual port)			—

4.1.2. Программные требования

Программные требования к среде функционирования серверной части СРК RuBackup приведены в таблице и определены:

- перечнем операционных систем, совместимых с компонентами СРК RuBackup;
- перечнем зависимостей пакетов для каждой совместимой ОС;
- открытыми портами (см. раздел «Сетевые порты»).

Таблица 6. Программные требования предъявляемые к серверу RuBackup (совместимые ОС и зависимости пакетов)

Пакеты сервера СРК (rubackup_common, rubackup_client, rubackup-server)	
Поддерживаемая ОС	**Пакет зависимости**
Astra 1.6	openssl, parsec-base, parsec-cap, parsec-mac, libcurl3 или libcurl4, mailutils или bsd-mailx, libsasl2-2, libldap-2.4-2
Astra 1.7	openssl, parsec-base, parsec-cap, parsec-mac, openssl, libcurl3 или libcurl4, mailutils или bsd-mailx, libsasl2-2, libldap-2.4-2, libpugixml1v5
Astra 1.8	openssl, parsec-base, parsec-cap, parsec-mac libcurl3 или libcurl4, mailutils или bsd-mailx, libsasl2-2, libldap-2.5-0, libpugixml1v5
Debian 10	openssl, libcurl3 или libcurl4, mailutils или bsd-mailx, libsasl2-2, libldap-2.4-2, libpugixml1v5
Debian 12	openssl, libcurl3 или libcurl4, mailutils или bsd-mailx, libsasl2-2, libldap-2.5-0,
Ubuntu 18.04	openssl, libcurl3 или libcurl4, mailutils или bsd-mailx, libsasl2-2, libldap-2.4-2
Ubuntu 20.04	openssl, libcurl3 или libcurl4, mailutils или bsd-mailx, libsasl2-2, libldap-2.4-2, libpugixml1v5
Ubuntu 22.04	openssl, libcurl3 или libcurl4, mailutils или bsd-mailx, libsasl2-2, libldap-2.5-0, libpugixml1v5

Пакеты сервера СРК (rubackup_common, rubackup_client, rubackup-server)	
ALT Linux 10	qt5-qtbase-gui mailutils, libsasl2-3, libldap, pugixml
CentOS 7	qt5-qtbase-gui, mailx, cyrus-sasl, openldap, pugixml
CentOS 8	qt5-qtbase-gui, mailx, cyrus-sasl, openldap, pugixml
RedOS 7.3	qt5-qtbase-gui, mailx, cyrus-sasl, openldap, pugixml
RedOS 8	qt5-qtbase-gui, mailx, cyrus-sasl, openldap, pugixml
RHEL 9	qt5-qtbase-gui, s-nail, cyrus-sasl, openldap, pugixml
Rosa Cobalt 7.3	qt5-qtbase-gui, mailx, cyrus-sasl, openldap
Rosa Cobalt 7.9	qt5-qtbase-gui, mailx, cyrus-sasl, openldap
Rosa Chrome 12	lib64qt5gui5, mailutils, lib64sasl2, lib64ldap2.4_2, lib64pugixml1

4.2. Установка

4.2.1. Подготовка к установке

Установка зависимостей пакетов

Данный шаг предназначен для установки локальных пакетов. Если вы устанавливаете пакеты из репозитория, то пропустите этот шаг.

Для успешного развёртывания сервера СРК RuBackup необходимо наличие установленных зависимостей пакетов в соответствии с таблицей, в зависимости от используемой операционной системы на узле развёртывания сервера RuBackup, для этого:

1. Проверьте наличие установленных пакетов зависимостей в ОС, например:

   Astra Linux, Debian, Ubuntu `dpkg-query -l`

   Альт `apt list --installed`

   Rosa Cobalt, RHEL `yum list с опцией installed`

   RedOS, CentOS, Rosa Chrome `dnf list installed`

2. Если вы используете операционную систему CentOS 7, CentOS 8 или RHEL 9, то добавьте репозиторий `EPEL` [1], поддерживаемый в рамках проекта Fedora и содержащий некоторые пакеты, которые не вошли в стандартный набор RHEL (CentOS):

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```

Файл репозитория будет автоматически загружен в каталог `/etc/yum.repos.d/epel.repo` и активирован.

3. Если вы используете операционную систему CentOS 7 или CentOS 8, то также рекомендуется включить репозиторий `PowerTools`, поскольку пакеты `EPEL` могут зависеть от пакетов из него:

```
sudo dnf config-manager --set-enabled powertools
```

4. Если вы используете операционную систему RHEL 9, то также рекомендуется включить репозиторий `codeready-builder-for-rhel-8-*-` репозиторий `rpm`, поскольку пакеты `EPEL` могут зависеть от пакетов из него:

```
ARCH=$( /bin/arch )

sudo subscription-manager repos --enable "codeready-builder-for-rhel-8-
$\{ARCH}-rpms"
```

5. Обновите репозитории пакетов в системе:

Astra Linux, Debian, Ubuntu	`sudo apt update`
Альт	`sudo apt-get update`
Rosa Cobalt, RHEL	`sudo yum update`
RedOS, CentOS, Rosa Chrome	`sudo dnf update`

6. Установите недостающие зависимости пакетов из таблицы:

Astra Linux, Debian, Ubuntu	`sudo apt install <namepackage>`
Альт	`sudo apt-get install <namepackage>`
Rosa Cobalt, RHEL	`sudo yum install <namepackage>`
RedOS, CentOS, Rosa Chrome	`sudo dnf install <namepackage>`

Настройка публичного репозитория

Данный шаг предназначен для установки из публичного репозитория. Если вы устанавливаете локальные пакеты, то пропустите этот шаг.

Подключение публичного репозитория DEB-систем

1. Создайте файл с информацией о репозиториях:

```
cat <<EOF | sudo tee /etc/apt/sources.list.d/rubackup_deb.list
deb https://dl.astralinux.ru/rubackup/repository-deb-main/ <OS-VERSION>
public
deb https://dl.astralinux.ru/rubackup/repository-deb-main/ <OS-VERSION>
public-testing
EOF
```

где: `<OS-VERSION>` — версия используемой ОС:

- astra_1.6;
- astra_1.7;
- astra_1.8;
- debian_10;
- debian_12;
- ubuntu_18.04;
- ubuntu_20.04;
- ubuntu_22.04.

2. Добавьте ключ репозитория:

```
sudo wget -qO-
https://dl.astralinux.ru/artifactory/api/security/keypair/gc-astra-
official-repo-key/public | gpg --no-default-keyring --keyring gnupg-
ring:/etc/apt/trusted.gpg.d/rubackup-deb.gpg --import - && sudo chmod 644
/etc/apt/trusted.gpg.d/rubackup-deb.gpg
```

3. Обновите список пакетов:

```
sudo apt-get update
```

Подключение публичного репозитория RPM-систем

1. Создайте файл с информацией о репозиториях:
   a. для ОС:
      - CentOS 7;
      - CentOS 8;
      - РЕД ОС 7.3;
      - РЕД ОС 8;

- Red Hat Enterprise Linux 9;
- ROSA Fresh Desktop 12;
- ROSA Enterprise Linux Server 7.9.

```
cat <<EOF | sudo tee /etc/yum.repos.d/rubackup_rpm.repo
[rubackup-rpm-public-repository]
name=rubackup rpm public repository
baseurl=https://dl.astralinux.ru/artifactory/rubackup-rpm-main/<OS-
VERSION>/public/
enabled=1
repo_gpgcheck=1
gpgkey=https://dl.astralinux.ru/artifactory/rubackup-rpm-main/<OS-
VERSION>/public/repodata/repomd.xml.key
gpgcheck=0

[rubackup-rpm-public-testing-repository]
name=rubackup rpm public testing repository
baseurl=https://dl.astralinux.ru/artifactory/rubackup-rpm-main/<OS-
VERSION>/public-testing/
enabled=1
repo_gpgcheck=1
gpgkey=https://dl.astralinux.ru/artifactory/rubackup-rpm-main/<OS-
VERSION>/public-testing/repodata/repomd.xml.key
gpgcheck=0
EOF
```

где: `<OS-VERSION>` — версия используемой ОС:

- centos_7;
- centos_8;
- redos_7.3;
- redos_8;
- rhel_9;
- rosa_12;
- rosa_7.9.

b. для ОС ROSA Enterprise Linux Server 7.3:

```
cat <<EOF | sudo tee /etc/yum.repos.d/rubackup_rpm.repo
[rubackup-rpm-public-repository]
name=rubackup rpm public repository
```

```
baseurl=https://dl.astralinux.ru/artifactory/rubackup-rpm-
main/rosa_7.3/public/
enabled=1
repo_gpgcheck=1
gpgkey=https://dl.astralinux.ru/artifactory/rubackup-rpm-
main/rosa_7.3/public/repodata/repomd.xml.key
gpgcheck=0
sslverify=0

[rubackup-rpm-public-testing-repository]
name=rubackup rpm public testing repository
baseurl=https://dl.astralinux.ru/artifactory/rubackup-rpm-
main/rosa_7.3/public-testing/
enabled=1
repo_gpgcheck=1
gpgkey=https://dl.astralinux.ru/artifactory/rubackup-rpm-
main/rosa_7.3/public-testing/repodata/repomd.xml.key
gpgcheck=0
sslverify=0
EOF
```

Настройка переменных среды

Выполните настройку переменных среды для пользователя `root`:

1. Авторизуйтесь под пользователем root:

```
sudo -i
```

2. Настройте переменные среды для пользователя `root`:

```
sudo nano /root/.bashrc
```

- отредактируйте файл, добавив строки:

```
PATH=$PATH:/opt/rubackup/bin
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/rubackup/lib
export PATH
export LD_LIBRARY_PATH
```

- сохраните изменения.

Эти переменные также можно определить в файле

`/etc/environment`.

3. Перейдите в каталог `/root`:

```
cd /root
```

4. Перезагрузите переменные окружения:

```
source ~/.bashrc
```

Настройка SSL соединения с базой данных

Пропустите этот шаг, если не требуется защищённое подключение компонентов RuBackup к служебной базе данных.

Если необходимо использовать для подключения к базе данных PostgreSQL защищённое соединение, то выполните приведённые ниже настройки на хостах, на которых развёрнуты компоненты СРК (postgres-клиенты):

1. Перенесите из соответствующей postgres-клиенту папки на узле Центра сертификации подготовленные:
   - сертификат Центра сертификации (ca.crt), чтобы клиент СРК мог проверить, что конечный сертификат сервера PostgreSQL был подписан его доверенным корневым сертификатом;
   - сертификат сервера/клиента СРК (postgresql.crt);
   - сгенерированный закрытый ключ сервера/клиента СРК (postgresql.key).
2. Для файлов сертификата и закрытого ключа установите полный доступ на чтение и запись только для владельцев:

```
chmod 600 server.crt server.key ca.crt
```

3. Сделайте владельцем файлов пользователя, от имени которого будет запущен компонент СРК (postgres-клиент):

```
chown suser:suser server.crt server.key ca.crt
```

4.2.2. Установка пакетов

Установку пакетов производить строго в приведённой последовательности!

1. Установите одним из способов:
   - из локальных пакетов, находясь в папке с пакетами:

Astra Linux, Debian, Ubuntu	`sudo apt install ./<namepackage>.deb`
Альт	`sudo apt-get install ./<namepackage>.rpm`
Rosa Cobalt, RHEL	`sudo yum install ./<namepackage>.rpm`
RedOS, CentOS, Rosa Chrome	`sudo dnf install ./<namepackage>.rpm`

   - из репозитория:

Astra Linux, Debian, Ubuntu	`sudo apt install <namepackage>.deb`

   где `<namepackage>` — устанавливаемый пакет СРК RuBackup актуальной версии в **приведённой последовательности**:

   a. `rubackup-common`;
   b. `rubackup-client`;
   c. `rubackup-server`;

   необязательные пакеты, используются для настройки сервера с помощью графической утилиты:

   d. `rubackup-common-gui`;
   e. `rubackup-init-gui`.

   По умолчанию настройка сервера осуществляется в терминале с помощью утилиты `rb_init`, которая не требует дополнительной инсталляции.

2. Выполните обновление конфигурации и примените изменения.

   Данный шаг выполняется только для ОС Astra Linux Special Edition 1.6 или 1.7 с активированным режимом защитной программной среды!

   - Обновите конфигурацию, выполнив команду:

     ```
     sudo update-initramfs -u -k all
     ```

   - Примените изменения, выполнив команду:

```
sudo reboot
```

4.2.3. Установка лицензии

Получение лицензионного файла

Для получения лицензионного файла сервера (основного, резервного и медиасерверов) у поставщика:

1. Полностью разверните серверную группировку запланированной архитектуры системы резервного копирования RuBackup, установив пакеты серверной части программы на узлах.
2. На каждом сервере получите идентификатор `hardware id`

   ```
   rubackup_server hwid
   ```

3. Зафиксируйте любым удобным способом для какого типа сервера (основной, резервный, медиа) получен идентификатор.
4. Предоставьте поставщику полученные идентификаторы удобным способом и получите лицензионные файлы для серверных компонентов СРК RuBackup на адрес электронной почты пользователя.

Установка лицензионного файла

Установите лицензионный файл на каждом узле лицензируемого сервера СРК RuBackup.

Для установки лицензионного файла:

1. Переместите файл лицензии в папку `/opt/rubackup/etc/`, выполнив команду, находясь в папке с подготовленным файлом лицензионного ключа:

   ```
   cp <файл_лицензии> /opt/rubackup/etc/rubackup.lic
   ```

2. Активация лицензии произойдёт после запуска сервера.

4.3. Настройка

4.3.1. Настройка сервера

Предварительно необходимо настроить сетевое взаимодействие компонентов СРК RuBackup, используя `FQDN`, `hostname` или `ip-адрес` (далее по тексту — адрес).

Настройку компонентов СРК RuBackup следует произвести на каждом узле в строго приведённом порядке (в зависимости от архитектуры):

1. настройка основного сервера;
2. настройка резервного сервера;
3. настройка медиасервера (выполняется для каждого медиасервера);
4. настройка клиента системы резервного копирования (выполняется для каждого клиента СРК).

Настройку компонентов СРК RuBackup возможно выполнить одним из способов:

- настройка сервера в интерактивном режиме при помощи утилиты `rb_init`;
- настройка сервера в неинтерактивном режиме при помощи утилиты `rb_init` (однострочной командой с заданными параметрами);
- настройка сервера с помощью графической утилиты мастера настройки RuBackup `rb_init_gui`.

Настройка сервера в терминале (интерактивный режим)

Выполните настройку компонента СРК RuBackup:

- Запустите на каждом узле, на котором развёрнут сервер СРК, интерактивную утилиту `rb_init`:

```
sudo /opt/rubackup/bin/rb_init
```

- Далее настройте компонент СРК в интерактивном режиме:
  1. `You MUST agree with the End User License Agreement (EULA) before installing RuBackup (y[es]/n[o]/r[ead]/q[uit])`

     основной, резервный, медиасервер: Примите лицензионное соглашение (EULA), нажав клавишу **<y>**.

  2. `Do you want to configure RuBackup server (primary, secondary, media) or client (p/s/m/c/q)?`

     основной сервер: Выберите сценарий настройки основного (primary) сервера, нажав клавишу **<p>**;

     резервный сервер: Выберите сценарий настройки резервного (secondary) сервера, нажав клавишу **<s>**;

     медиасервер: Выберите сценарий настройки медиа (media) сервера, нажав клавишу **<m>**.

Настройка соединения с базой данных:

3. `Enter hostname or IP address of PostgreSQL server [ localhost ]:`

   основной, резервный, медиасервер: Укажите адрес, на котором развёрнута служебная база данных PostgreSQL:

   - если СУБД PostgreSQL развёрнута на отдельном узле от основного сервера, то следует указать адрес соответствующего узла;
   - если СУБД PostgreSQL и основной сервер развёрнуты на одном узле, то нажмите клавишу **<Enter>**, чтобы в качестве адреса сервера использовался localhost (выбранный по умолчанию).

4. `Please enter password for "postgres" database user:`

   основной сервер: Укажите пароль пользователя базы данных postgres, заданный на шаге 6 в разделе setup-database.pdf.

5. `Do you want to use a secure SSL connection to the database 'rubackup' (y/n/q)?`

   основной, резервный, медиасервер: Укажите, необходимо ли использовать защищенное SSL-соединение со служебной базой данных СРК RuBackup, нажав клавишу **<y>** (да) или **<n>** (нет).

   Если настройка SSL-соединения с БД не требуется, нажмите клавишу **<n>**.

   По умолчанию подключение будет установлено с параметром `sslmode=allow`, в этом случае для подключения к БД будут использованы файлы сертификатов и закрытых ключей, которые расположены в папке `/opt/rubackup/keys`, при подключении к БД данные будут шифроваться.

   Если в конфигурации PostgreSQL SSL выключен, то по умолчанию `sslmode` будет `disable`.

   Для продолжения настройки SSL соединения с БД нажмите клавишу **<y>**. Для настройки SSL-соединения с БД предварительно необходимо выполнить настройку служебной базы данных в соответствии с разделом setup-database.pdf и подготовить сертификаты в соответствии с разделом setup-ssl.pdf.

   a. `Enter sslmode ( allow, disable, prefer, require, verify-ca, verify-full ) [ require ]`

      `Enter path for sslrootcert file:`

      `Enter path for sslcert file:`

`Enter path for sslkey file:`

- выберите и введите название выбранного режима SSL в соответствии с таблицей.

По умолчанию выбран режим `require`.

Таблица 7. Описание режимов SSL

sslmode	Защита от прослушивания	Защита от MITM	Утверждение
disable	Нет	Нет	Мне не важна безопасность и я не приемлю издержки, связанные с шифрованием.
allow	Возможно	Нет	Мне не важна безопасность, но я приемлю издержки, связанные с шифрованием, если на этом настаивает сервер.
prefer	Возможно	Нет	Мне не важна безопасность, но я предпочитаю шифрование (и приемлю связанные издержки), если это поддерживает сервер.
require	Да	Нет	Я хочу, чтобы мои данные шифровались, и я приемлю сопутствующие издержки. Я доверяю сети в том, что она обеспечивает подключение к нужному серверу
verify-ca	Да	Зависит от политики ЦС	Я хочу, чтобы мои данные шифровались, и я приемлю сопутствующие издержки. Мне нужна уверенность в том, что я подключаюсь к доверенному серверу
verify-full	Да	Да	Я хочу, чтобы мои данные шифровались, и я приемлю сопутствующие издержки. Мне нужна уверенность в том, что я подключаюсь к доверенному серверу и это именно указанный мной сервер

- укажите расположение подготовленных сертификатов:
  - в поле `sslrootcert` укажите расположение сертификата центра сертификации;
  - в поле `sslcert` укажите расположение сертификата настраиваемого хоста;
  - в поле `sslkey` укажите расположение закрытого ключа настраиваемого хоста.

6. `Enter name of RuBackup superuser [ rubackup ]:`

основной, резервный, медиасервер: Введите имя суперпользователя СРК RuBackup, который будет создан на следующем шаге.

По умолчанию при нажатии клавиши **<Enter>** используется имя суперпользователя — `rubackup`.

В имени суперпользователя запрещено использовать следующие символы: пробел, \, $, #, `, /, ?, *, ., ,, ;, :, %, ^, &, <, >

7. `Database user "rubackup" doesn't exist. Do you want to create database user "rubackup" (y/n)?`

   основной, резервный, медиасервер: Создайте суперпользователя базы данных, нажав клавишу **<y>**

8. `Please enter password for "rubackup" database user:`

   основной, резервный, медиасервер: Задайте пароль для суперпользователя служебной базы данных `rubackup` (имя БД по умолчанию), создаваемой на следующем шаге

9. `Enter RuBackup database name [ rubackup ]: Database "rubackup" doesn't exist. Do you want to create database "rubackup" on "localhost" host (y/n)?`

   основной, резервный, медиасервер: Введите имя базы данных, используемой СРК RuBackup и подтвердите создание базы данных, нажав клавишу **<y>**.

   В имени базы данных запрещено использовать следующие символы: пробел, \, $, #, `, /, ?, *, ., ,, ;, :, %, ^, &, <, >.

   По умолчанию, при нажатии клавиши **<Enter>** в качестве имени создаваемой базы данных используется `rubackup`.

Настройка хранилища для дефолтного пула:

10. `Do you want to add a required file system to the 'Default' pool in the configuration? (y/n)?`

    основной сервер: Добавьте локальное файловое хранилище для дефолтного пула.

    Если хранилище не будет создано, то все созданные резервные копии будут сохранены в аварийном хранилище (по умолчанию `/tmp/rubackup_emergency_storage_local_catalog`).

    a. `Enter path: /default_pool`

       `Path "/default_pool" doesn't exist. Do you want to create it? (y/n)`

       основной сервер: Введите путь к директории, которая будет ассоциирована с дефолтным пулом и создайте локальное файловое хранилище, нажав клавишу **<y>**.

Настройка основного сервера:

11. `Hostname of primary server:`

    резервный, медиасервер: Укажите адрес основного сервера.

Настройка резервного сервера:

12. `Will you use secondary server (y/n)?`

    основной, медиасервер: Если в конфигурации подразумевается резервный (secondary) сервер, то выберите эту возможность, нажав клавишу **<y>**

13. `Hostname of secondary server:`

    основной, медиасервер: Укажите адрес резервного сервера.

Настройка клиента СРК:

14. `Choose client net interface ID for use:`

    `Selected interface:` **основной, резервный, медиасервер**: Выберите сетевой интерфейс, посредством которого клиенту RuBackup разрешено взаимодействовать с системой резервного копирования.

15. `Do you allow centralized recovery (y/n)?`

    основной, резервный, медиасервер: Укажите, нужно ли включить централизованное восстановление данных?

    В случае выбора **<y>**, централизованное восстановление данных из резервной копии будет доступно с помощью приложения «Менеджер администратора RuBackup» (RBM), с помощью консольной утилиты `rbfd` или приложения «Менеджера клиента RuBackup» (RBC).

    В случае выбора **<n>**, централизованное восстановление данных из резервной копии с помощью приложения «Менеджер администратора RuBackup» будет отключено, восстановление из резервной копии будет возможно с помощью консольной утилиты `rbfd` или приложения «Менеджера клиента RuBackup»

16. `Do you plan to use continuous remote replication to apply remote replicas on this client (y/n)?y`

    основной, резервный, медиасервер: Укажите, будет ли использоваться непрерывная удаленная репликация на клиенте СРК.

17. `Enter local backup directory path [/tmp] : /rubackup-tmp Would you like to create /rubackup-tmp (y/n)?`

    основной, резервный, медиасервер: Укажите директорию для временных операций с файлами резервных копий и подтвердите создание каталога для временных файлов, нажав клавишу **<y>**.

18. `Set amount threads parallelizm for server [ 8 ]:`

    основной, медиасервер: Укажите количество потоков для одновременной обработки задач резервного копирования на основном сервере (каждый поток имеет отдельное соединение со служебной базой данных СРК).

19. `Set amount threads parallelizm media server [ 8 ]:`

    основной, медиасервер: Укажите количество потоков для одновременной обработки задач резервного копирования на медиасервере (каждый поток имеет отдельное соединение со служебной базой данных СРК).

20. `Create RuBackup master key…`

    основной, резервный, медиасервер: Автоматическое создание мастер-ключа, который необходим при создании пары ключей для электронно-цифровой подписи резервных копий и защитного преобразования резервных копий.

21. `Will you use digital signature (y/n)?`

    основной, резервный, медиасервер: Укажите, хотите ли вы создать ключи электронно-цифровой подписи, необходимые для дополнительной защиты резервных копий.

22. `Do you want to enable system monitoring of this client (y/n)?`

    основной, резервный, медиасервер: Укажите, хотите ли вы включить системный мониторинг для данного клиента.

    Файл мониторинга производительности системных компонентов будет размещён в папке `/opt/rubackup/monitoring/`.

23. `Do you want to set a soft memory threshold? (y/n)?`

    основной, резервный, медиасервер: Укажите, хотите ли вы установить верхний предел оперативной памяти, которая может использоваться при резервном копировании на клиенте (точность верхней границы объема памяти не гарантируется).

    a. `Enter the allowed amount of memory for backup in GB (integer value):`

основной, резервный, медиасервер: В случае выбора **<y>** укажите максимально допустимый объём оперативной памяти, который может быть использован при резервном копировании на клиенте в ГБ (целое число).

24. `Do you want to use ipv4[1] ipv6[2] or both[3] in DNS requests?:`

    основной, резервный, медиасервер: Выберите какие публичные имена будут использованы DNS-сервером.

25. `Do you want to enable RuBackup security audit ([y]es, [n]o, [q]uit) (y/n/q)?`

    основной сервер: Укажите, хотите ли вы включить аудит безопасности (формирование журнала событий информационной безопасности).

    Аудит событий является частью системы обнаружения вторжений, посредством сохранения информации о запросах в самой базе данных с использованием триггеров, срабатывающих на изменение данных (добавление, изменение или удаление данных в БД RuBackup).

    Позднее возможно включить/отключить данную опцию с помощью утилиты для работы с журналом событий информационной безопасности `rb_security`

26. `Choose security audit type ([e]ssential only, [t]asks (additionally to essential), [q]uit)(e/t/q)?e`

    основной сервер: Укажите, какой тип аудита вы хотите включить:

    - `essential only` — журналирование всех значимых таблиц, кроме очередей задач и временных таблиц;
    - `tasks (additionally to essential)` — журналирование всех значимых таблиц и задач в очередях

Настройка сервера в терминале (неинтерактивный режим)

Неинтерактивный режим работы необходим для выполнения сценариев массового развертывания, например, при использовании *Ansible* — программного решения для удаленного управления конфигурациями серверов.

Администратор имеет возможность настроить СРК RuBackup в `bash/shell` однострочной командой и, как следствие, использовать эту команду в скриптах для автоматизации процесса.

Настройка СРК RuBackup осуществляется с помощью интерактивной утилиты `rb_init` (неинтерактивный режим). Описание утилиты приведено в документе Утилиты командной строки..

Настройка сервера с помощью графической утилиты

Настройка сервера (основного, медиа или резервного) RuBackup с помощью мастера СРК RuBackup возможна с помощью графической утилиты мастера настройки RuBackup.

- Запустите мастер настройки RuBackup (графическое приложение `rb_init_gui`):

```
rb_init_gui&
```

- После запуска мастера настройки RuBackup заполните открывшиеся формы:
  1. Нажмите **Да** для продолжения настройки компонента СРК RuBackup.

     Графическая утилита `rb_init_gui` запущена в экспериментальном режиме (Рисунок 1).

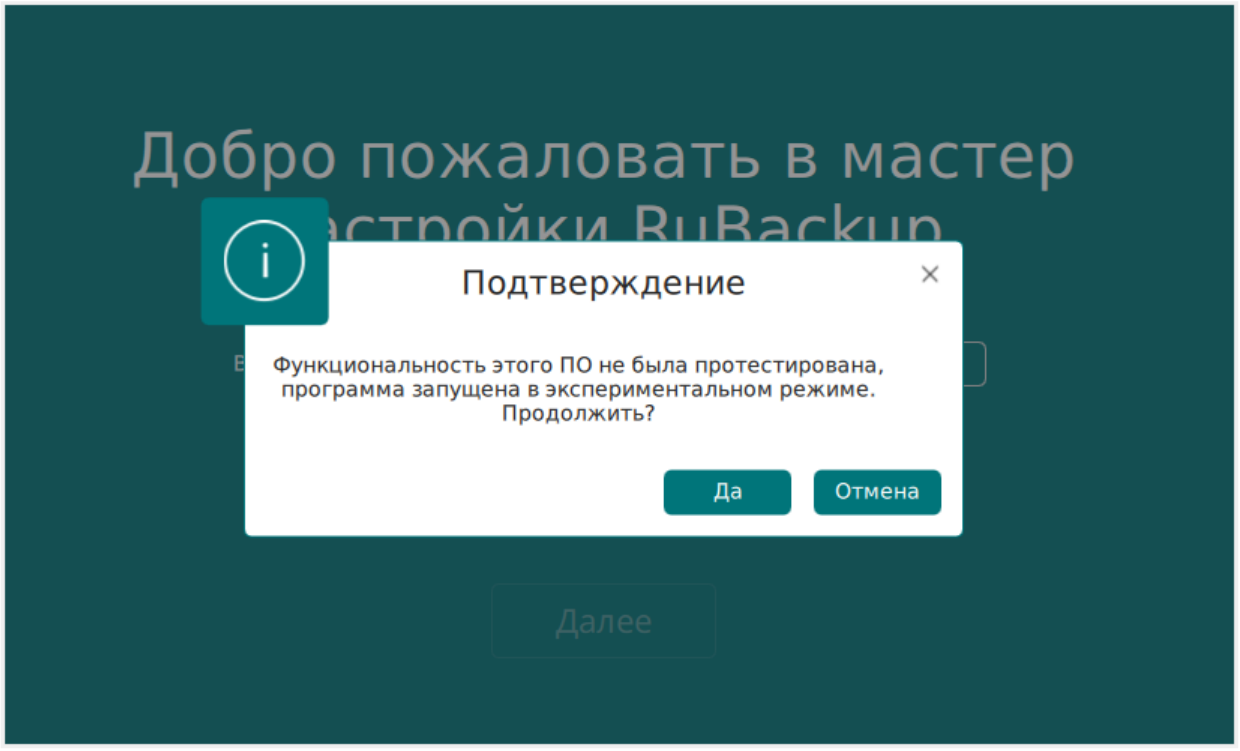


Рисунок 1. Окно предупреждения о работе утилиты в экспериментальном режиме

  2. В приветственном окне (Рисунок 2):
     - выберите язык интерфейса приложения из предложенных вариантов (русский или английский);
     - примите лицензионное соглашения для продолжения настройки RuBackup, проставив отметку в чек-боксе ✓ **Применить**.

       Для ознакомления нажмите на активный элемент **[Лицензионное соглашение]** и в открывшемся окне подтверждения скопируйте в буфер ссылку на лицензионное соглашение для дальнейшего просмотра в брау-

зере;

- нажмите **[Далее]**.

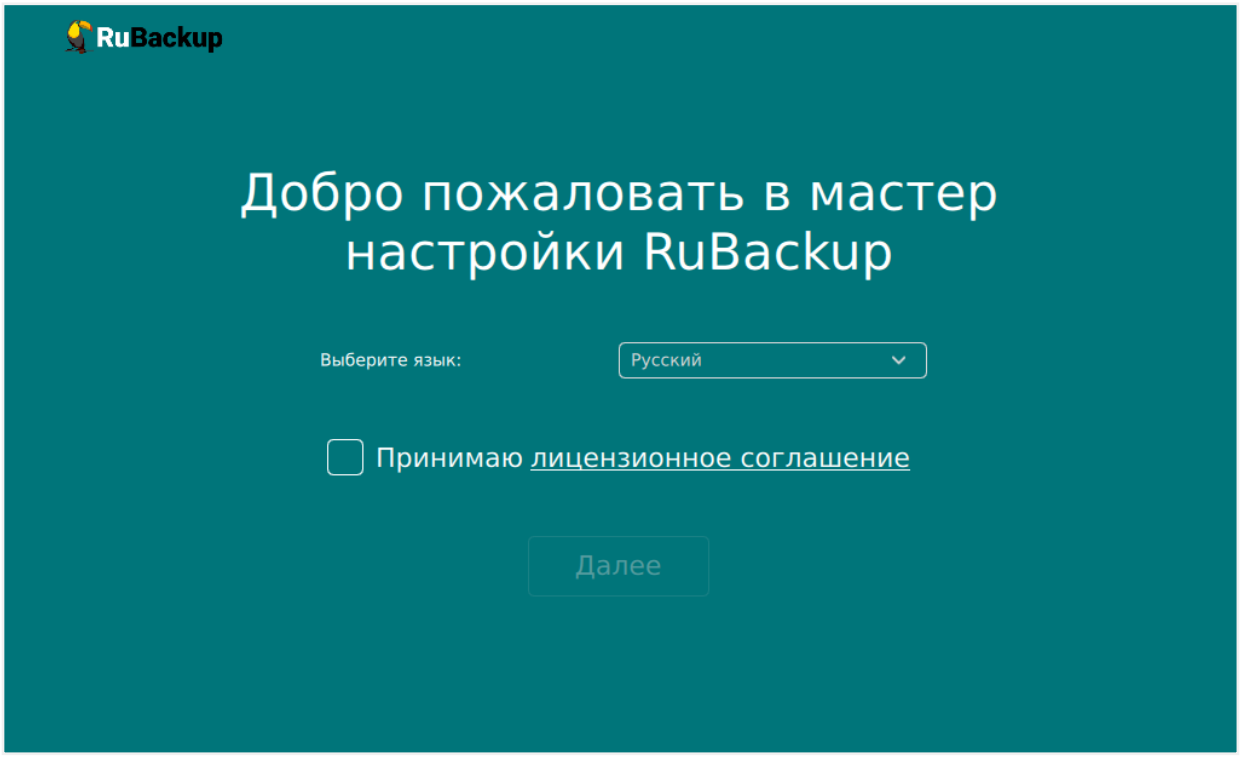


Рисунок 2. Приветственное окно Мастера настройки RuBackup

3. В открывшемся окне выберете настраиваемый компонент.

   Если на настраиваемом узле установлен пакет `rubackup-server`, то мастер настройки автоматически предлагает произвести настройку серверного компонента (Рисунок 3):

   - основной сервер;
   - резервный сервер;
   - медиасервер.

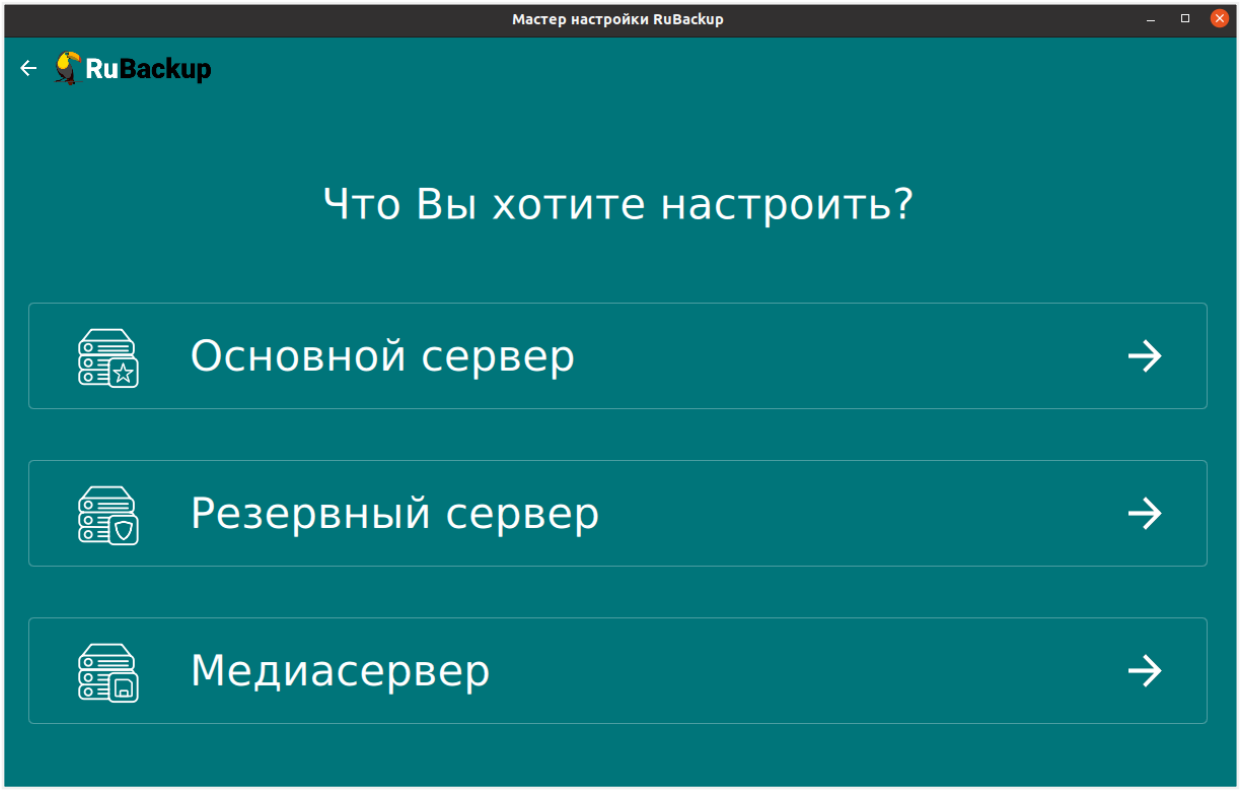
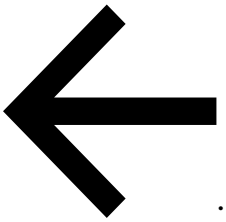


Рисунок 3. Окно выбора настраиваемого компонента RuBackup

4. Заполните открывшуюся форму настраиваемого компонента СРК RuBackup.

   Для возврата на предыдущий шаг и редактирования выбора используйте  .

   a. Блок **Общие параметры**:

      основной, резервный, медиасервер:

      - В поле **Количество сетевых потоков** укажите количество потоков для одновременной обработки задач резервного копирования на основном сервере (каждый поток имеет отдельное соединение со служебной базой данных СРК)

      основной, резервный, медиасервер:

      - В поле **Версия IP для DNS запросов** выберите какие публичные имена будут использованы DNS-сервером.

      основной, резервный, медиасервер:

      - Активируйте переключатель **Перезапись мастер-ключа** для автоматического формирования нового мастер-ключа и перезаписи (при

наличии) текущего мастер-ключа, который необходим при создании пары ключей электронно-цифровой подписи резервных копий и защитного преобразования резервных копий.

b. Блок **Параметры сервера**:

резервный, медиасервер:

- В поле **Имя основного сервера** укажите `ip-адрес` или `FQDN` основного сервера RuBackup (в соответствии с настройками файла `hosts` узла основного сервера).

основной, резервный, медиасервер:

- В поле **Адрес сервера PostgreSQL** [2] укажите адрес, на котором развёрнута СУБД PostgreSQL:

  - если СУБД PostgreSQL развёрнута на отдельном от основного сервера узле, то следует указать адрес соответствующего узла;
  - если СУБД PostgreSQL и основной сервер развёрнуты на одном узле, то оставьте значение `localhost`, выбранное по умолчанию ---

основной сервер:

- В поле **Пароль PostgreSQL** [2] укажите пароль пользователя базы данных `postgres`

основной сервер:

- В поле **Имя суперпользователя RuBackup** укажите имя суперпользователя базы данных `rubackup` (имя БД по умолчанию).

  Суперпользователь будет создан в процессе настройки основного сервера.

основной, резервный, медиасервер:

- В поле **Пароль пользователя RuBackup** [2] укажите пароль для суперпользователя базы данных `rubackup` (имя БД по умолчанию).

основной сервер:

- В поле **Имя базы RuBackup** введите имя базы данных (по умолчанию в качестве имени базы данных используется `rubackup`), которая будет использоваться в качестве служебной БД или будет создана в случае её отсутствия.

В имени базы данных запрещено использовать следующие символы: пробел, \, $, #, `, /, ?, *, ., ,, ;, :, %, ^, &, <, >

основной сервер:

- При обновлении в поле **Если база уже существует** выберите действие с существующей базой данных:
  - `keep` — пропустить действие, База данных будет сохранена в текущем состоянии;
  - `drop` — удалить существующую базу данных;
  - `upgrade` — обновить существующую базу данных.
- При удалении и обновлении существующей базы данных по умолчанию будет сделана резервная копия данных, если переключатель **Отключить дамп** деактивирован , если активировать данный переключатель, то резервное копирование для текущей базы данных перед удалением/обновлением выполнено не будет.
- Если резервное копирование существующей базу данных будет выполнено, то в поле **Формат дампа** выберите тип резервной копии базы данных:
  - `custom archives` — custom-архив, восстановление выполняется с помощью утилиты `pg_restore`. Резервная копия в формате `custom` занимает меньше места на диске, по сравнению с форматом `plain`.

    Настройте **Уровень сжатия дампа**;
  - `plain` — текстовый sql-скрипт.
- Для типа резервной копии БД `custom archives` в поле **Уровень сжатия дампа** выберите степень сжатия резервной копии базы данных (значение от 0 до 9). Чем выше степень сжатия, тем меньше архив занимает места на диске и тем дольше выполняется процедура резервного копирования базы данных.
- В поле **Путь к папке дампа** [2] выберите путь для сохранения резервной копии - по умолчанию это директория, откуда была вызвана утилита.

основной, резервный, медиасервер:

- В поле **Сетевой интерфейс** выберите сетевой интерфейс, посредством которого клиенту RuBackup разрешено взаимодействовать с системой резервного копирования.

основной сервер:

- В поле **Путь файловой системы для добавления в «Default»** [2] необходимо назначить для пула Default хотя бы один каталог для хранения резервных копий.

основной, резервный, медиасервер:

- В поле **Локальный каталог резервного копирования** укажите локальный каталог для временного хранения файлов с метаданными, создаваемых при операциях резервного копирования (по умолчанию при нажатии клавиши **Enter** в качестве директории для временных операций с файлами резервных копий используется `/tmp`). Если указанная директория не существует, то будет создана.

основной, медиасервер:

- В поле **Имя резервного сервера** укажите `ip-адрес` или `FQDN` основного сервера RuBackup (в соответствии с настройками файла `hosts` узла основного сервера).

основной, резервный, медиасервер:

- В поле **Количество параллельных задач** укажите количество потоков для одновременной обработки задач резервного копирования на медиасервере.

  Каждый поток имеет отдельное соединение со служебной базой данных СРК.

основной, резервный, медиасервер:

- В поле **Объём памяти дедупликации, байт** для ограничения потребления оперативной памяти сервером при дедупликации резервных копий.

  При использовании дедупликации рекомендуется минимальный объем оперативной памяти сервера 64 GB `effective_cache_size` ~70 % от размера оперативной памяти `work_mem` 32 MB.

основной, резервный, медиасервер:

- Активируйте переключатель **«Непрерывная удалённая репликация»** ◐ при необходимости на клиенте.

  Непрерывная удалённая репликация осуществляется только в хранилище блочного типа.

основной, резервный, медиасервер:

- Активируйте переключатель **Разрешать централизованное восстановление для клиента** для восстановления данных из резервной копии с помощью приложения «Менеджер администратора RuBackup» (RBM), с помощью консольной утилиты `rbfd` или приложения «Менеджера клиента RuBackup» (RBC).

  В случае деактивированного переключателя восстановление из резервной копии будет возможно с помощью консольной утилиты `rbfd` или приложения «Менеджера клиента RuBackup» на узле клиента резервного копирования. Централизованное восстановление данных из резервной копии с помощью приложения «Менеджер администратора RuBackup» (используемой на любом узле) будет отключено.

основной, резервный, медиасервер:

- Активируйте переключатель **Создать ключи ЭЦП**, если хотите создать ключи электронно-цифровой подписи.

  Резервная копия может быть подписана цифровой подписью для последующего контроля и предупреждения угрозы её подмены.

основной, резервный, медиасервер:

- Активируйте переключатель **Перезаписать ключи цифровой подписи**, для создания новой связки ключей, используемых для электронно-цифровой подиси.

основной сервер:

- Активируйте переключатель **Аудит безопасности** для журналирования всех значимых таблиц, кроме очередей задач и временных таблиц.

  Для расширения регистрируемых событий активируйте переключатель **Аудит задач** для журналирования всех значимых таблиц и задач в очередях.

  Позднее возможно включить/отключить данную опцию и изменить выбранный тип аудита с помощью утилиты для работы с журналом событий информационной безопасности `rb_security`.

c. Блок **Настройка SSL**:

основной, резервный, медиасервер:

- При необходимости настройки защищённого соединения со служебной базой данных активируйте переключатель **Использовать SSL соединение с базой данных** и настройте параметры:

- в поле **SSL режим работы с Postgres** выберите соответствующий режим работы (в зависимости от настроек узла, на котором установлена БД). Подробное описание режимов смотри в Настройка SSL соединений.

  Если в конфигурации PostgreSQL SSL выключен, то по умолчанию SSL режим будет `disable`;

- в поле **Корневой сертификат** [2] укажите полный путь к сертификату доверенного Центра сертификации (прописав в поле или выбрав по нажатию рядом с полем кнопки), который необходимо заранее разместить в папке `opt/rubackup/keys`;
- в поле **Сертификат клиента** [2] укажите полный путь к сертификату (открытому ключу) настраиваемого узла, выданный доверенным Центром сертификации (прописав в поле или выбрав по нажатию рядом с полем кнопки), который необходимо заранее разместить в папке `opt/rubackup/keys`;
- в поле **Ключ клиента** [2] укажите полный путь к закрытому ключу сертификата настраиваемого узла, выданный доверенным Центром сертификации (прописав в поле или выбрав по нажатию рядом с полем кнопки), который необходимо заранее разместить в папке `opt/rubackup/keys`.

5. После заполнения всех полей формы настраиваемого компонента СРК RuBackup нажмите **[Далее]**.

   В окне подтверждения нажмите **Да** для настройки компонента СРК RuBackup (Рисунок 4).

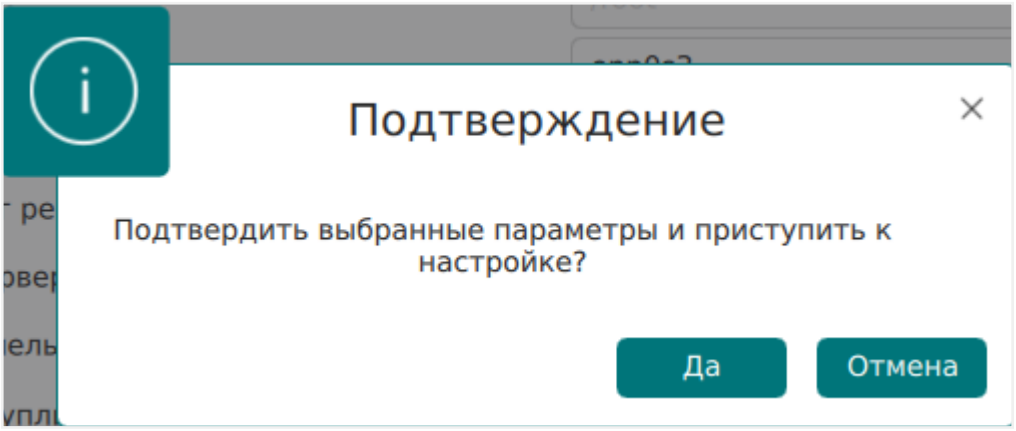


Рисунок 4. Окно подтверждения выбранных параметров

6. Если в форме настраиваемого компонента СРК RuBackup указаны папки, которых не существует, то будет выведено подтверждение для их создания (Рисунок 5).

   В окне подтверждения нажмите **Да** для создания папок.

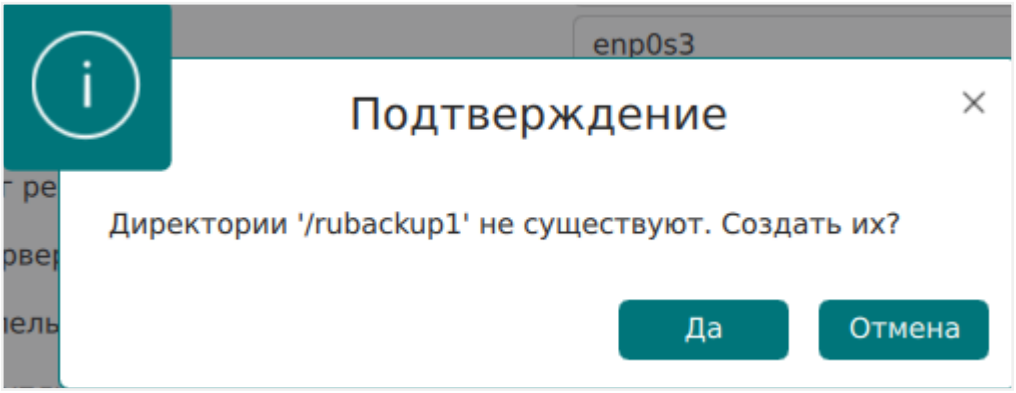


Рисунок 5. Окно подтверждения создания директорий

7. В случае успешной настройки пользователь будет уведомлён сообщением (Рисунок 6), в котором приведена информация:

- о лицензионном соглашении;
- правообладатель;
- версия продукта;
- имя текущего узла;
- тип настроенного компонента СРК RuBackup;
- о создании конфигурационного файла `/opt/rubackup/etc/config.file`;
- дополнительно могут быть приведены рекомендации и предупреждения по настройкам параметров.

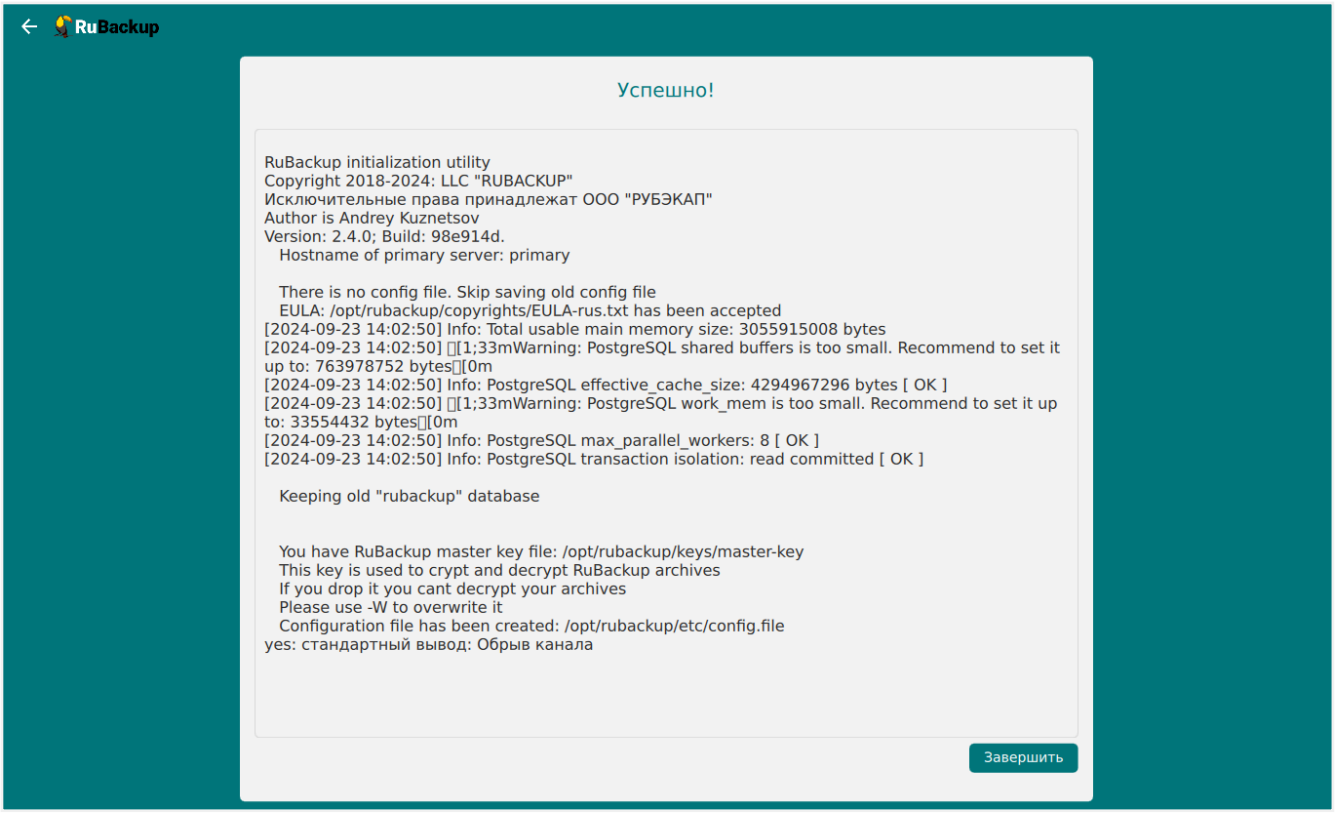


Рисунок 6. Окно результатов выполненной настройки сервера

1. Нажмите **Завершить** для завершения работы приложения.

4.3.2. Настройка пользователей

Пользователи, от имени которых будет осуществляться запуск утилит командной строки RuBackup или приложения для управления СРК RuBackup (RBM, RBC, Tucana):

- иметь правильно настроенные переменные среды;
- входить в группу `rubackup`.

Выполните приведённые ниже настройки для пользователей на всех узлах с развёрнутыми компонентами СРК RuBackup.

Настройка переменных среды

1. Настройте переменные среды для всех пользователей, которые будут работать с СРК RuBackup, выполнив команду:

```
sudo nano /<имя пользователя>/.bashrc
```

   - отредактируйте файл, добавив строки:

```
PATH=$PATH:/opt/rubackup/bin
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/rubackup/lib
export PATH
export LD_LIBRARY_PATH
```

   - сохраните изменения.

Эти переменные также можно определить в файле `/etc/environment`.

2. Перезагрузите переменные окружения, выполнив команду:

```
source ~/.bashrc
```

Добавление в группу

Группа `rubackup` автоматически создаётся в процессе установки пакета `rubackup-common`.

Добавьте пользователя в группу `rubackup`, выполнив команду:

```
sudo usermod -a -G rubackup <имя пользователя>
```

4.3.3. Добавление в автозапуск

1. Добавьте сервис клиента РК в автозапуск при загрузке ОС:

   ```
   sudo systemctl enable rubackup_client.service
   ```

2. Добавьте сервис сервера РК в автозапуск при загрузке ОС:

   ```
   sudo systemctl enable rubackup_server.service
   ```

3. Перезагрузите настройки ОС:

   ```
   sudo systemctl daemon-reload
   ```

4.4. Запуск

Произведите активацию серверной части СРК RuBackup, выполнив на каждом узле с развёрнутым сервером (основным, резервным, медиа) RuBackup запуск сервиса клиента и сервиса сервера.

4.4.1. Запуск сервиса клиента

Для запуска сервиса клиента выполните команду:

```
sudo systemctl start rubackup_client.service
```

4.4.2. Запуск сервиса сервера

Для запуска сервиса сервера выполните команду:

```
sudo systemctl start rubackup_server.service
```

4.4.3. Просмотр статуса сервиса клиента

Для запуска просмотра статуса сервиса клиента выполните команду:

```
sudo systemctl status rubackup_client.service
```

4.4.4. Просмотр статуса сервиса сервера

Для просмотра статуса сервиса сервера выполните команду:

```
sudo systemctl status rubackup_server.service
```

4.4.5. Остановка сервиса клиента

Для останова сервиса клиента выполните команду:

```
sudo systemctl stop rubackup_client.service
```

4.4.6. Остановка сервиса сервера

Для останова сервиса сервера выполните команду:

```
sudo systemctl stop rubackup_server.service
```

[1] Выполните установку актуальной версии репозитория EPEL, для примера приведена установка репозитория EPEL 8
[2] обязательное для заполнения поле

Глава 5. Клиентская часть

Клиентская часть СРК RuBackup может состоять из одного или нескольких клиентов резервного копирования, которые могут быть объединены в группы клиентов.

Клиент резервного копирования — это отдельный сервер, компьютер или виртуальная машина, которая содержит данные для резервирования (ресурс) и на которой установлено клиентское ПО RuBackup для выполнения резервного копирования.

5.1. Linux

5.1.1. Системные требования

В данном подразделе приведены системные требования для каждого клиентского компонента СРК RuBackup, предъявляемые к техническим средствам, необходимым для нормального функционирования СРК RuBackup.

В случае установки на один хост нескольких компонентов СРК RuBackup (например, при способе установки «Всё в одном») следует консолидировать соответствующие аппаратные требования, предъявляемые к техническому средству, на которое производится установка.

Аппаратные требования

Минимальные аппаратные требования, необходимые для стабильного функционирования клиента системы резервного копирования приведены в таблице.

Таблица 8. Аппаратные требования, предъявляемые к Клиенту системы резервного копирования

Аппаратный компонент	Значение
Процессор	1 ядро

Аппаратный компонент	Значение
Оперативная память (RAM) [1]	*Пример 1. расчёт RAM при однопоточном режиме резервирования:* *Пример 2. расчёт RAM при многопоточном режиме резервирования:* $$RAM = RAM_1 + RAM_2 + ... + RAM_N$$ где: RAM_1 — объём оперативной памяти необходимый для резервирования одного ресурса; $0,04xV_{ресурса}$— 4% от размера резервируемого ресурса; N — количество единовременно резервируемых ресурсов

Аппаратный компонент	Значение
Дисковое пространство (HDD)[2]	*Пример 3. расчёт HDD по формуле:* где: *K=1* — при однопоточном режиме резервировании; *K= worker_parallelism* при многопоточном режиме (enable_multithreading) и слабой дедупликация (enable_flexible_dedup); enable multithreading — флаг, указывающий на использование многопоточности; enable flexible dedup — флаг, указывающий на использование гибкой дедупликации; *worker parallelism* — количество рабочих потоков, используемых для выполнения резервирования; _объём ресурса _— общий объём данных, подлежащих резервированию; *размер блока* — размер блока данных, используемого для обработки данных во время резервирования; *размер хеша* — размер хеша, используемого для идентификации данных; *20*— максимальный размер сериализованной позиции в файле; *1* — временная база для вычисления сигнатуры или отправки хешей на сервер; *размер метаданных* – это 0.02 * объем ресурса

Примеры расчётов оперативной памяти и дискового пространства:

Ресурс	Хеш	Блок	K	Размер метаданных	Дисковое пространство (ГБ)
536870912000	64	8192	8	10737418240	56
536870912000	64	8192	32	10737418240	179
536870912000	64	8192	64	10737418240	343
536870912000	64	8192	128	10737418240	671

536870912000	64	1048576	8	10737418240	10
536870912000	64	1048576	32	10737418240	11
536870912000	64	1048576	64	10737418240	12
536870912000	64	1048576	128	10737418240	15
1099511627776	64	8192	8	21990232555	114
1099511627776	64	8192	32	21990232555	366
1099511627776	64	8192	64	21990232555	702
1099511627776	64	8192	128	21990232555	1374
1099511627776	64	1048576	8	21990232555	21
1099511627776	64	1048576	32	21990232555	23
1099511627776	64	1048576	64	21990232555	25
1099511627776	64	1048576	128	21990232555	31

Программные требования

Программные требования к среде функционирования клиентской части СРК RuBackup приведены в таблице и определены:

- перечнем операционных систем, совместимых с компонентами СРК RuBackup;
- перечнем зависимостей пакетов для каждой совместимой ОС;
- открытыми портами (см. раздел «Сетевые порты»).

Таблица 9. Программные требования к предъявляемые к серверу RuBackup (совместимые ОС и зависимости пакетов)

Пакеты основного сервера СРК	Поддерживаемая ОС	Пакет зависимости
rubackup_common, rubackup_client	Astra 1.6, Astra 1.7, Astra 1.8	openssl, parsec-base, parsec-cap, parsec-mac
	Debian 10, Debian 12, Ubuntu 18.04, Ubuntu 20.04,Ubuntu 22.04	openssl
	Альт 10, CentOS 7, CentOS 8, RedOS 7.3, RedOS 8, RHEL 9, Rosa Cobalt 7.3, Rosa Cobalt 7.9	qt5-qtbase-gui
	Rosa Chrome 12	lib64qt5gui5

5.1.2. Установка

Подготовка к установке

Установка зависимостей пакетов

Данный шаг предназначен для установки локальных пакетов. Если вы

устанавливаете пакеты из репозитория, то пропустите этот шаг.

Для успешного развёртывания сервера СРК RuBackup необходимо наличие установленных зависимостей пакетов в соответствии с таблицей, в зависимости от используемого типа операционной системы на узле развёртывания клиента резервного копирования RuBackup, для этого:

1. Проверьте наличие установленных пакетов зависимостей в ОС, например:

Astra Linux, Debian, Ubuntu	`dpkg-query -l`
Альт	`apt list --installed`
Rosa Cobalt, RHEL	`yum list с опцией installed`
RedOS, CentOS, Rosa Chrome	`dnf list installed`

2. Если вы используете операционную систему CentOS 7, CentOS 8 или RHEL 9, то добавьте репозиторий `EPEL` [3], поддерживаемый в рамках проекта Fedora и содержащий некоторые пакеты, которые не вошли в стандартный набор RHEL (CentOS):

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```

   Файл репозитория будет автоматически загружен в каталог `/etc/yum.repos.d/epel.repo` и активирован.

3. Если вы используете операционную систему CentOS 7 или CentOS 8, то также рекомендуется включить репозиторий `PowerTools`, поскольку пакеты `EPEL` могут зависеть от пакетов из него:

   ```
   sudo dnf config-manager --set-enabled powertools
   ```

4. Если вы используете операционную систему RHEL 9, то также рекомендуется включить репозиторий `codeready-builder-for-rhel-8-*-` репозиторий `rpm`, поскольку пакеты `EPEL` могут зависеть от пакетов из него:

   ```
   ARCH=$( /bin/arch )

   sudo subscription-manager repos --enable "codeready-builder-for-rhel-8-$\{ARCH}-rpms"
   ```

5. Обновите репозитории пакетов в системе:

Astra Linux, Debian, Ubuntu	`sudo apt update`
Альт	`sudo apt-get update`
Rosa Cobalt, RHEL	`sudo yum update`
RedOS, CentOS, Rosa Chrome	`sudo dnf update`

6. Установите недостающие зависимости пакетов из таблицы:

Astra Linux, Debian, Ubuntu	`sudo apt install <namepackage>`
Альт	`sudo apt-get install <namepackage>`
Rosa Cobalt, RHEL	`sudo yum install <namepackage>`
RedOS, CentOS, Rosa Chrome	`sudo dnf install <namepackage>`

Настройка публичного репозитория

Данный шаг предназначен для установки из публичного репозитория. Если вы устанавливаете локальные пакеты, то пропустите этот шаг.

Подключение публичного репозитория DEB-систем

1. Создайте файл с информацией о репозиториях:

```
cat <<EOF | sudo tee /etc/apt/sources.list.d/rubackup_deb.list
deb https://dl.astralinux.ru/rubackup/repository-deb-main/ <OS-VERSION>
public
deb https://dl.astralinux.ru/rubackup/repository-deb-main/ <OS-VERSION>
public-testing
EOF
```

где: `<OS-VERSION>` — версия используемой ОС:

- astra_1.6;
- astra_1.7;
- astra_1.8;
- debian_10;
- debian_12;
- ubuntu_18.04;
- ubuntu_20.04;
- ubuntu_22.04.

2. Добавьте ключ репозитория:

```
sudo wget -qO-
https://dl.astralinux.ru/artifactory/api/security/keypair/gc-astra-
official-repo-key/public | gpg --no-default-keyring --keyring gnupg-
ring:/etc/apt/trusted.gpg.d/rubackup-deb.gpg --import - && sudo chmod 644
/etc/apt/trusted.gpg.d/rubackup-deb.gpg
```

3. Обновите список пакетов:

```
sudo apt-get update
```

Подключение публичного репозитория RPM-систем

1. Создайте файл с информацией о репозиториях:
   a. для ОС:
      - CentOS 7;
      - CentOS 8;
      - РЕД ОС 7.3;
      - РЕД ОС 8;
      - Red Hat Enterprise Linux 9;
      - ROSA Fresh Desktop 12;
      - ROSA Enterprise Linux Server 7.9.

```
cat <<EOF | sudo tee /etc/yum.repos.d/rubackup_rpm.repo
[rubackup-rpm-public-repository]
name=rubackup rpm public repository
baseurl=https://dl.astralinux.ru/artifactory/rubackup-rpm-main/<OS-
VERSION>/public/
enabled=1
repo_gpgcheck=1
gpgkey=https://dl.astralinux.ru/artifactory/rubackup-rpm-main/<OS-
VERSION>/public/repodata/repomd.xml.key
gpgcheck=0

[rubackup-rpm-public-testing-repository]
name=rubackup rpm public testing repository
baseurl=https://dl.astralinux.ru/artifactory/rubackup-rpm-main/<OS-
VERSION>/public-testing/
enabled=1
```

```
repo_gpgcheck=1
gpgkey=https://dl.astralinux.ru/artifactory/rubackup-rpm-main/<OS-
VERSION>/public-testing/repodata/repomd.xml.key
gpgcheck=0
EOF
```

где: `<OS-VERSION>` — версия используемой ОС:

- centos_7;
- centos_8;
- redos_7.3;
- redos_8;
- rhel_9;
- rosa_12;
- rosa_7.9.

b. для ОС ROSA Enterprise Linux Server 7.3:

```
cat <<EOF | sudo tee /etc/yum.repos.d/rubackup_rpm.repo
[rubackup-rpm-public-repository]
name=rubackup rpm public repository
baseurl=https://dl.astralinux.ru/artifactory/rubackup-rpm-
main/rosa_7.3/public/
enabled=1
repo_gpgcheck=1
gpgkey=https://dl.astralinux.ru/artifactory/rubackup-rpm-
main/rosa_7.3/public/repodata/repomd.xml.key
gpgcheck=0
sslverify=0

[rubackup-rpm-public-testing-repository]
name=rubackup rpm public testing repository
baseurl=https://dl.astralinux.ru/artifactory/rubackup-rpm-
main/rosa_7.3/public-testing/
enabled=1
repo_gpgcheck=1
gpgkey=https://dl.astralinux.ru/artifactory/rubackup-rpm-
main/rosa_7.3/public-testing/repodata/repomd.xml.key
gpgcheck=0
sslverify=0
EOF
```

Настройка переменных среды

Выполните настройку переменных среды для пользователя `root`:

1. Авторизуйтесь под пользователем root:

```
sudo -i
```

2. Настройте переменные среды для пользователя `root`:

```
sudo nano /root/.bashrc
```

   - отредактируйте файл, добавив строки:

```
PATH=$PATH:/opt/rubackup/bin
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/rubackup/lib
export PATH
export LD_LIBRARY_PATH
```

   - сохраните изменения.

Эти переменные также можно определить в файле `/etc/environment`.

3. Перейдите в каталог `/root`:

```
cd /root
```

4. Перезагрузите переменные окружения:

```
source ~/.bashrc
```

Настройка SSL соединения с базой данных

Пропустите этот шаг, если не требуется защищённое подключение компонентов RuBackup к служебной базе данных.

Если необходимо использовать для подключения к базе данных PostgreSQL защищённое соединение, то выполните приведённые ниже настройки на узлах, на которых развёрнуты компоненты СРК (postgres-клиенты):

1. Перенесите из соответствующей postgres-клиенту папки на узле Центра сер-

тификации подготовленные:

- сертификат Центра сертификации (ca.crt), чтобы клиент СРК мог проверить, что конечный сертификат сервера PostgreSQL был подписан его доверенным корневым сертификатом;
- сертификат клиента резервного копирования (postgresql.crt);
- сгенерированный закрытый ключ клиента резервного копирования (postgresql.key).

2. Для файлов сертификата и закрытого ключа установите полный доступ на чтение и запись только для владельцев:

```
chmod 600 server.crt server.key ca.crt
```

3. Сделайте владельцем файлов пользователя, от имени которого будет запущен клиент резервного копирования (postgres-клиент):

```
chown suser:suser server.crt server.key ca.crt
```

Установка пакетов

Установку пакетов производить строго в приведённой последовательности!

1. Установите одним из способов:

- из локальной папки со скачанными пакетами:

Astra Linux, Debian, Ubuntu	`sudo apt install ./<namepackage>.deb`
Альт	`sudo apt-get install ./<namepackage>.rpm`
Rosa Cobalt, RHEL	`sudo yum install ./<namepackage>.rpm`
RedOS, CentOS, Rosa Chrome	`sudo dnf install ./<namepackage>.rpm`

- из репозитория:

Astra Linux, Debian, Ubuntu	`sudo apt install <namepackage>.deb`

где `<namepackage>` — устанавливаемый пакет СРК RuBackup актуальной версии в приведённой последовательности:

a. `rubackup-common`;

b. `rubackup-client`;

необязательные пакеты, используются для настройки сервера с помощью графической утилиты:

c. `rubackup-common-gui`;

d. `rubackup-init-gui`.

По умолчанию настройка сервера осуществляется в терминале с помощью утилиты `rb_init`, которая не требует дополнительной инсталляции.

2. Выполните обновление конфигурации и примените изменения.

Данный шаг выполняется только для ОС Astra Linux Special Edition 1.6 или 1.7 с активированным режимом защитной программной среды!

- Обновите конфигурацию:

```
sudo update-initramfs -u -k all
```

- Примените изменения:

```
sudo reboot
```

5.1.3. Настройка

Настройка клиента РК

Настройку компонентов СРК RuBackup следует произвести на каждом узле в строго приведённом порядке (в зависимости от архитектуры) :

1. настройка основного сервера;
2. настройка резервного сервера;
3. настройка медиасервера (выполняется для каждого медиасервера);
4. настройка клиента системы резервного копирования (выполняется для каждого клиента СРК).

Необходимо предварительно настроить сетевое взаимодействие узлов компонентов СРК RuBackup, используя `FQDN`, `hostname` или `ip-адрес` (далее по тексту — адрес).

Настройка клиента РК в терминале (интерактивный режим)

Выполните настройку компонента СРК RuBackup:

- Запустите на каждом узле, на котором развёрнут клиент РК, интерактивную утилиту `rb_init`:

```
sudo /opt/rubackup/bin/rb_init
```

- Далее настройте компонент СРК в интерактивном режиме. Клиент РК может быть настроен для работы в клиент-серверном режиме или в автономном режиме.

Клиент-серверный режим работы клиента РК

1. `You MUST agree with the End User License Agreement (EULA) before installing RuBackup (y[es]/n[o]/r[ead]/q[uit])`

   Примите лицензионное соглашение (EULA), нажав клавишу **<y>**.

2. `Choose client mode: client-server or autonomous (c/a)?`

   Выберите сценарий настройки клиента: клиент-сервер **<c>**.

Настройка соединения с основным сервером

3. `Hostname of primary server:`

   Укажите адрес основного (primary) сервера.

Настройка соединения с резервным сервером

4. `Will you use secondary server (y/n)?`

   Если в конфигурации подразумевается резервный (secondary) сервер, то выберите эту возможность, нажав клавишу **<y>**.

   a. `Hostname of secondary server:`

      Укажите адрес резервного (secondary) сервера.

Настройка клиента резервного копирования:

5. `Choose client net interface ID for use:`

   `Selected interface:`

Выберите сетевой интерфейс, посредством которого клиенту RuBackup разрешено взаимодействовать с системой резервного копирования.

6. `Do you allow centralized recovery (y/n)?`

   Укажите, нужно ли включить централизованное восстановление данных?

   В случае выбора **<y>**, централизованное восстановление данных из резервной копии будет доступно с помощью утилиты «Менеджер администратора RuBackup» (RBM), с помощью консольной утилиты `rbfd` или утилиты «Менеджера клиента RuBackup» (RBC).

   В случае выбора **<n>**, централизованное восстановление данных из резервной копии с помощью утилиты «Менеджер администратора RuBackup» будет отключено, восстановление из резервной копии будет возможно с помощью консольной утилиты `rbfd` или утилиты «Менеджера клиента RuBackup».

7. `Do you plan to use continuous remote replication to apply remote replicas on this client (y/n)?`

   Укажите, будет ли использоваться непрерывная удаленная репликация на клиенте РК.

8. `Enter local backup directory path [/tmp] :`

   Укажите директорию для временных операций с файлами резервных копий и подтвердите создание каталога для временных файлов, нажав клавишу **<y>**.

   a. `Would you like to create / (y/n)?`

      Подтвердите создание каталога для временных файлов, в случае, если указанного каталога ещё не существует.

9. `Create RuBackup master key…`

   Автоматическое создание мастер-ключа, который необходим при создании пары ключей для электронно-цифровой подписи резервных копий и защитного преобразования резервных копий.

10. `Will you use digital signature (y/n)?`

    `Create new secret key`

    `Create new public key`

    Укажите, хотите ли вы создать ключи электронно-цифровой подписи. Резервная копия может быть подписана цифровой подписью для последующего контроля и предупреждения угрозы её подмены.

11. `Do you want to enable system monitoring of this client (y/n)?`

    Укажите, хотите ли вы включить системный мониторинг для данного клиента.

    Файл мониторинга производительности системных компонентов будет размещён в папке `/opt/rubackup/monitoring/`.

12. `Do you want to set a soft memory threshold? (y/n)?`

    Укажите, хотите ли вы установить верхний предел оперативной памяти, которая может использоваться при резервном копировании на клиенте (точность верхней границы объема памяти не гарантируется).

    a. `Enter the allowed amount of memory for backup in GB (integer value):`

       В случае выбора **<y>** укажите максимально допустимый объём оперативной памяти, который может быть использован при резервном копировании на клиенте в ГБ (целое число).

13. `Do you want to use ipv4[1] ipv6[2] or both[3] in DNS requests?`

    Выберите какие публичные имена будут использованы DNS-сервером.

Автономный режим работы клиента РК

1. `You MUST agree with the End User License Agreement (EULA) before installing RuBackup (y[es]/n[o]/r[ead]/q[uit])`

   Примите лицензионное соглашение (EULA), нажав клавишу **<y>**.

2. `Choose client mode: client-server or autonomous (c/a)?`

   Выберите сценарий настройки клиента: автономный <a>.

   Автономный режим работы клиента — использование клиента РК без серверной части. При этом сохраняется возможность использования любых функциональных модулей для создания резервных копий

3. `Enter local backup directory path [/tmp] : /rubackup-tmp Would you like to create /rubackup-tmp (y/n)?`

   Укажите директорию для временных операций с файлами резервных копий и подтвердите создание каталога для временных файлов, нажав клавишу **<y>**.

4. `Would you like to use a catalog, or dedicated device, or network share to store your archives? (c/d/n)`

   Укажите хотите ли вы использовать каталог, выделенное устройство или сетевой ресурс для хранения своих архивов?

- **<c>** - укажите путь к каталогу на вашем локальном жёстком диске для хранения резервных копий;
- **<d>** - будут показы все ваши устройства и потребуется указать выбранное устройство для хранения резервных копий;
- **<n>** - укажите сетевой каталог для хранения резервных копий

5. `Create RuBackup master key…`

   Автоматическое создание мастер-ключа, который необходим при создании пары ключей для электронно-цифровой подписи резервных копий и защитного преобразования резервных копий.

6. `Do you want to use ipv4[1] ipv6[2] or both[3] in DNS requests?`

   Выберите какие публичные имена будут использованы DNS-сервером

Настройка клиента РК в терминале (неинтерактивный режим)

Неинтерактивный режим работы необходим для выполнения сценариев массового развертывания, например, при использовании Ansible — программного решения для удаленного управления конфигурациями серверов.

Администратор имеет возможность настроить СРК RuBackup в bash/shell однострочной командой и, как следствие, использовать эту команду в скриптах для автоматизации процесса.

Настройка СРК RuBackup осуществляется с помощью интерактивной утилиты `rb_init` (неинтерактивный режим). Описание утилиты см. Утилиты командной строки.

Настройка клиента РК с помощью графической утилиты

Настройка клиента резервного копирования возможна с помощью графической утилиты мастера настройки RuBackup.

- Запустите мастер настройки RuBackup (графическое приложение `rb_init_gui`), выполнив команду:

```
rb_init_gui&
```

- После запуска мастера настройки RuBackup заполните открывшиеся формы:

  1. Нажмите **Да** для продолжения настройки компонента СРК RuBackup.

     Графическая утилита `rb_init_gui` запущена в экспериментальном режиме (Рисунок 7).

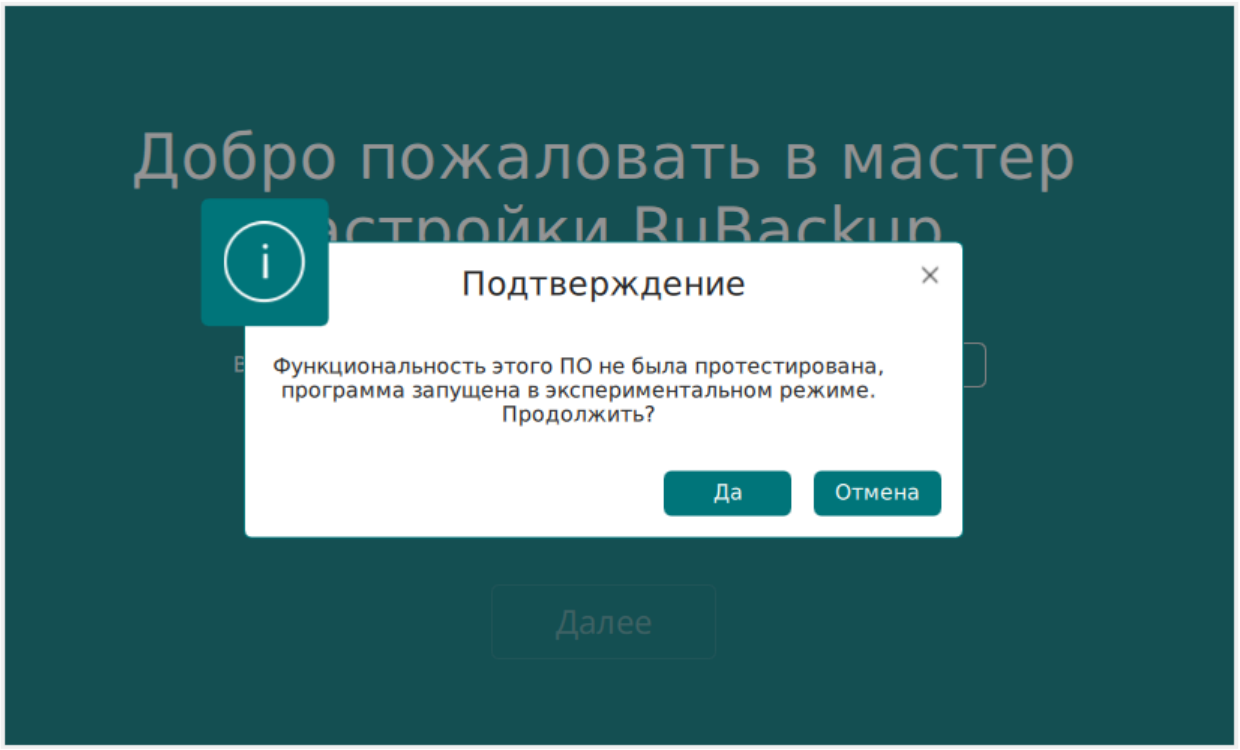


Рисунок 7. Окно предупреждения о работе утилиты в экспериментальном режиме

2. В приветственном окне (Рисунок 8):

   - выберите язык интерфейса приложения из предложенных вариантов (русский или английский);
   - примите лицензионное соглашения для продолжения настройки компонента RuBackup, проставив отметку в чек-боксе ✓ **Принимаю лицензионное соглашение**.

     Для ознакомления нажмите на активный элемент **[Лицензионное соглашение]** и скопируйте в буфер ссылку на лицензионное соглашение для дальнейшего просмотра в браузере;

   - нажмите **[Далее]**.

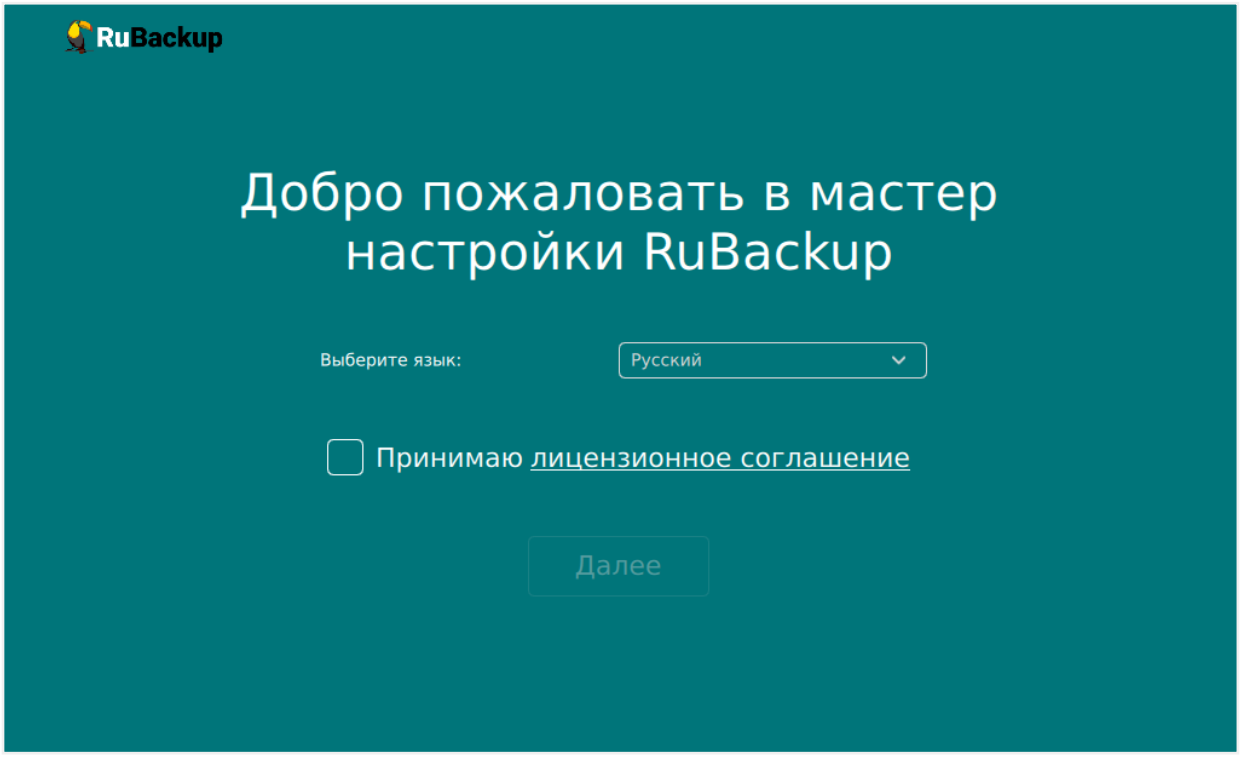


Рисунок 8. Приветственное окно Мастера настройки RuBackup

3. В открывшемся окне выберете режим настраиваемого клиента резервного копирования (Рисунок 9):

- автономный режим клиента РК предусматривает использование функций СРК без серверной части с сохранением возможности использования любых функциональных модулей для создания резервных копий;
- клиент-серверный режим клиента РК предусматривает использований всех доступных функций СРК.

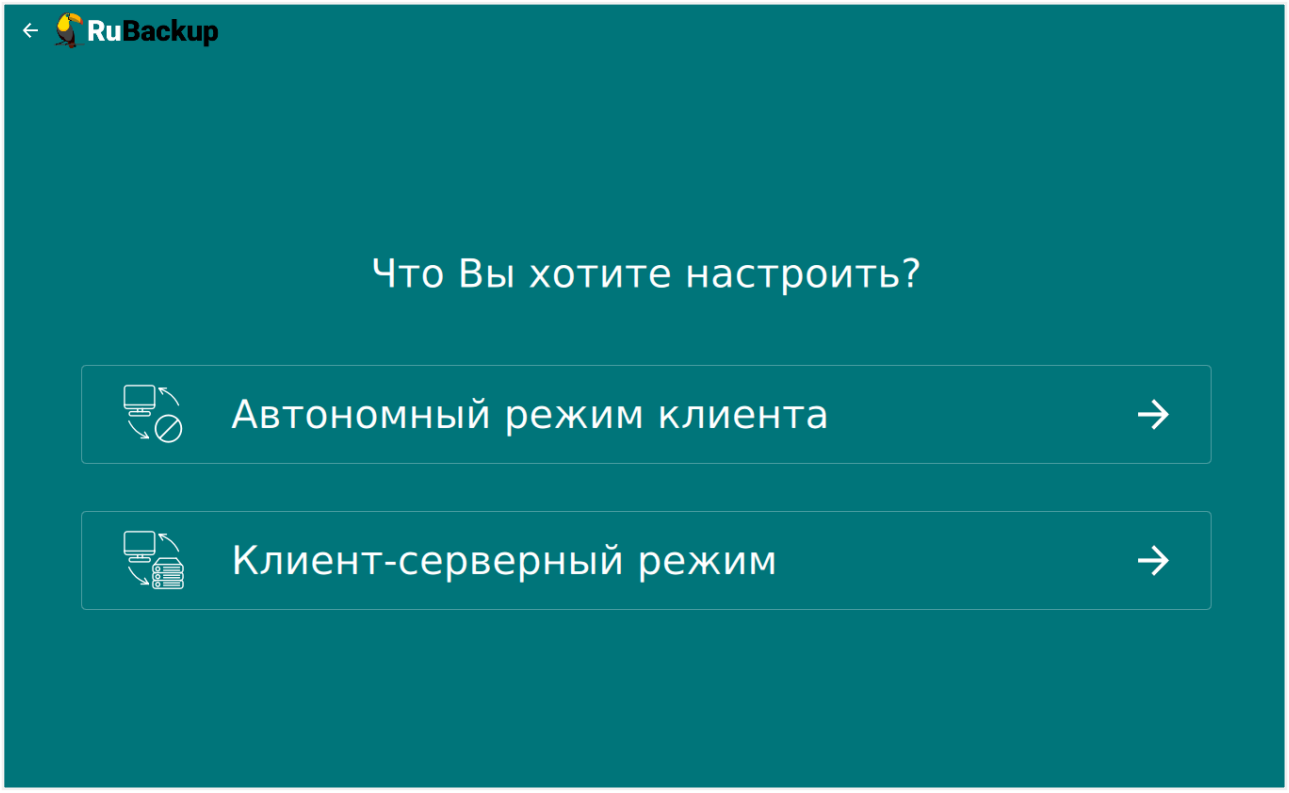


Рисунок 9. Окно выбора режима настраиваемого компонента RuBackup

Клиент-серверный режим работы клиента РК

1. Заполните открывшуюся форму настраиваемого клиента резервного копирования RuBackup.
   a. Блок **Общие параметры**
      - В поле **Количество сетевых потоков** укажите количество потоков для одновременной обработки задач резервного копирования на основном сервере (каждый поток имеет отдельное соединение со служебной базой данных СРК)
      - В поле **Версия IP для DNS запросов** выберите какие публичные имена будут использованы DNS-сервером.
      - Активируйте переключатель **Перезапись мастер-ключа** для автоматического формирования нового мастер-ключа и перезаписи (при наличии) текущего мастер-ключа.
   b. Блок **Параметры клиент-серверного режима**
      - В поле **Имя основного сервера** укажите `ip-адрес` или `FQDN` основного сервера RuBackup (в соответствии с настройками файла `hosts` узла основного сервера).
      - В поле **Имя резервного сервера** укажите `ip-адрес` или `FQDN` основного сервера RuBackup (в соответствии с настройками файла `hosts` узла основного сервера).
      - В поле **Сетевой интерфейс** выберите сетевой интерфейс, посредством

которого клиенту РК разрешено взаимодействовать с системой резервного копирования.

- В поле **Локальный каталог резервного копирования** укажите локальный каталог для временного хранения файлов с метаданными, создаваемых при операциях резервного копирования (по умолчанию при нажатии клавиши **Enter** в качестве директории для временных операций с файлами резервных копий используется `/tmp`). Если указанная директория не существует, то будет создана.
- В поле **Количество параллельных задач** укажите количество потоков для одновременной обработки задач резервного копирования на медиасервере (каждый поток имеет отдельное соединение со служебной базой данных СРК).
- В поле **Объём памяти дедупликации, байт** для ограничения потребления оперативной памяти сервером при дедупликации резервных копий.

  При использовании дедупликации рекомендуется минимальный объем оперативной памяти сервера 64 GB `effective_cache_size` ~70 % от размера оперативной памяти `work_mem` 32 MB.

- Активируйте переключатель **Непрерывная удалённая репликация** при необходимости на клиенте. Непрерывная удалённая репликация осуществляется только в хранилище блочного типа.
- Активируйте переключатель **Разрешать централизованное восстановление для клиента** для восстановления данных из резервной копии в приложении «Менеджер администратора RuBackup» (RBM), с помощью консольной утилиты `rbfd` или приложения «Менеджер клиента RuBackup» (RBC).

  В случае деактивированного переключателя восстановление из резервной копии будет возможно с помощью консольной утилиты `rbfd` или приложения «Менеджер клиента RuBackup» на узле клиента резервного копирования.

  Централизованное восстановление данных из резервной копии с помощью приложения «Менеджер администратора RuBackup» (используемом на любом узле) будет отключено.

- Активируйте переключатель **Создать ключи ЭЦП**, если хотите создать ключи электронно-цифровой подписи.

  Резервная копия может быть подписана цифровой подписью для последующего контроля и предупреждения угрозы её подмены.

- Активируйте переключатель **Системный мониторинг для клиента**, если хотите включить системный мониторинг для данного клиента.

Файл мониторинга производительности системных компонентов будет размещён в папке `/opt/rubackup/monitoring/`.

- Активируйте переключатель **Перезаписать ключи цифровой подписи** , для создания новой связки ключей, используемых для электронно-цифровой подписи.

2. После заполнения всех полей формы настраиваемого компонента СРК RuBackup нажмите **[Далее]**.

   В окне подтверждения нажмите **Да** для настройки компонента СРК RuBackup(Рисунок 10).

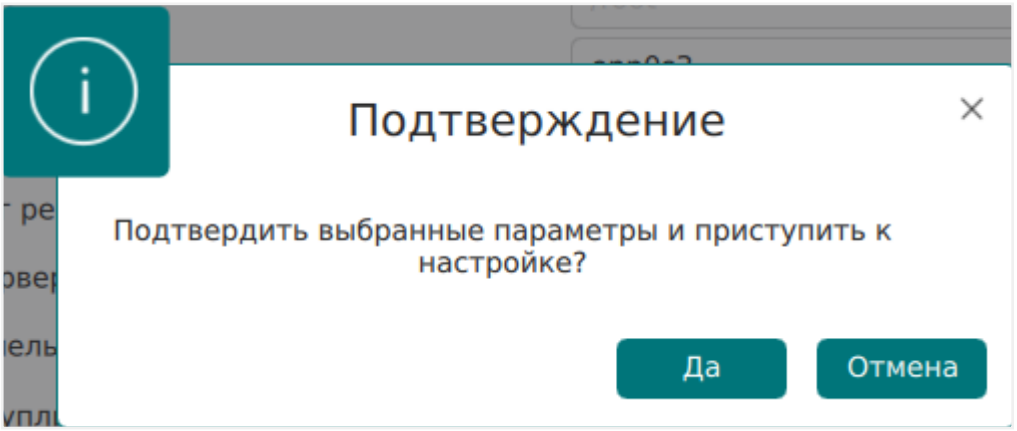


Рисунок 10. Окно подтверждения выбранных параметров

3. Если в форме настраиваемого компонента СРК RuBackup указаны папки, которых не существует, то будет выведено подтверждение для их создания (Рисунок 11).

   В окне подтверждения нажмите **Да** для создания папок.

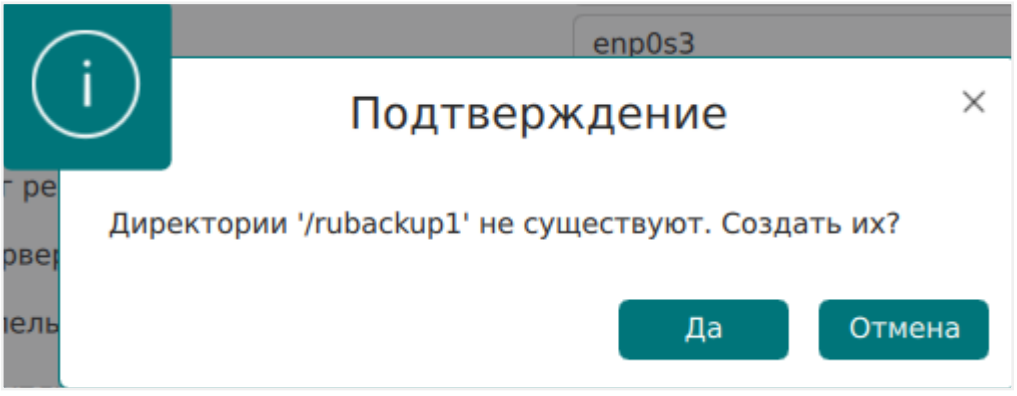


Рисунок 11. Окно подтверждения создания директорий

4. В случае успешной настройки пользователь будет уведомлён сообщением (Рисунок 12), в котором приведена информация:

   - о лицензионном соглашении;
   - правообладатель;

- версия продукта;
- имя текущего узла;
- тип настроенного компонента СРК RuBackup;
- о создании конфигурационного файла `/opt/rubackup/etc/config.file`;
- дополнительно могут быть приведены рекомендации и предупреждения по настройкам параметров.

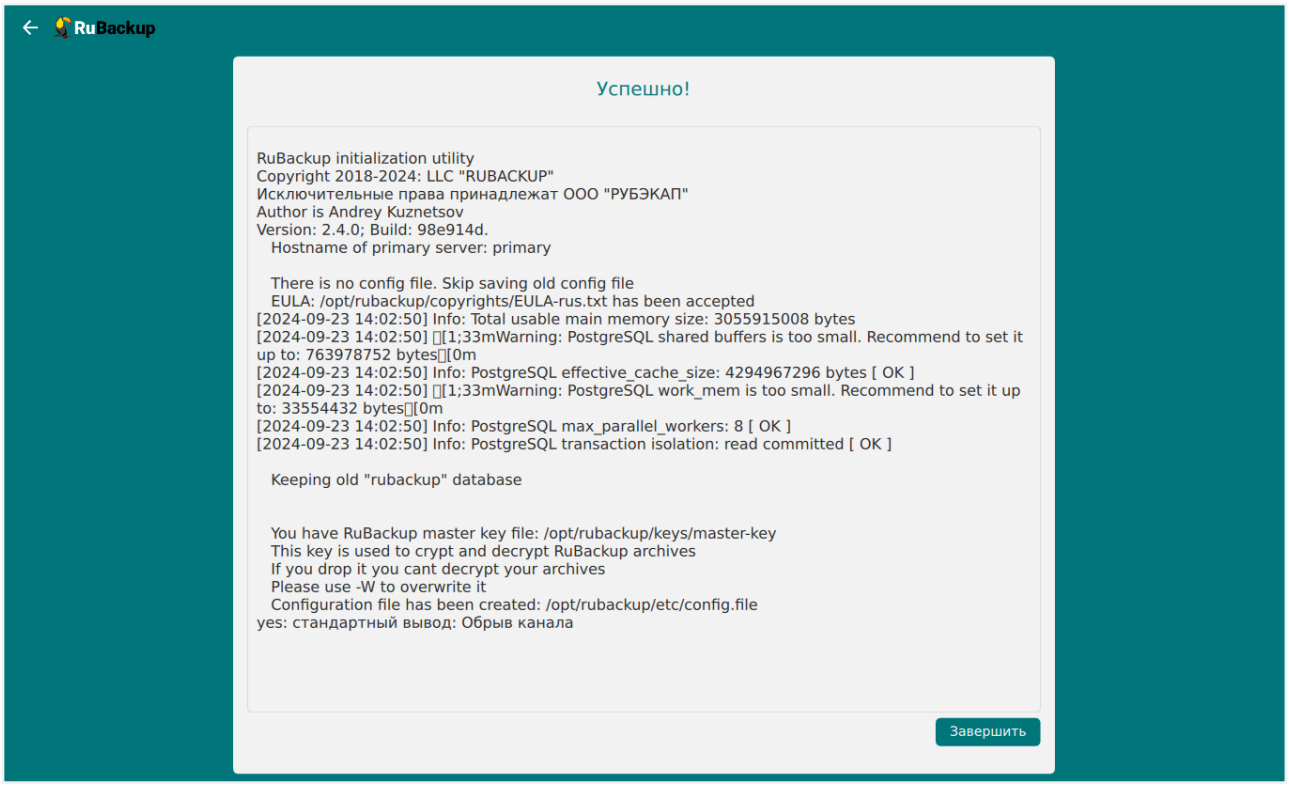


Рисунок 12. Окно результатов выполненной настройки клиента РК

5. Нажмите **Завершить** для завершения работы приложения.

Автономный режим работы клиента РК

1. Заполните открывшуюся форму настраиваемого клиента резервного копирования.
   a. Блок **Общие параметры**
      - В поле **Количество сетевых потоков** укажите количество потоков для одновременной обработки задач резервного копирования на основном сервере (каждый поток имеет отдельное соединение со служебной базой данных СРК)
      - В поле **Версия IP для DNS запросов** выберите какие публичные имена будут использованы DNS-сервером.
      - Активируйте переключатель **Перезапись мастер-ключа** для автоматического формирования нового мастер-ключа и перезаписи (при наличии) текущего мастер-ключа.

b. Блок **Параметры автономного клиента**

- В поле **Каталог архивирования** [4] выберите каталог для временного хранения резервных копий. Если этот параметр не определен в файле конфигурации, то клиент будет запрашивать у медиасервера временное пространство для операций с резервными копиями (NFS папку).
- В поле **Метод сжатия** выберите тип сжатия резервных копий:
  - `none` — без сжатия;
  - `fast` — многопоточный аналог `optimal`;
  - `optimal` — стандартная утилита сжатия Linux;
  - `best` — больший коэффициент сжатия, чем `optimal`, при большем времени.
- В поле **Тип хранилища резервных копий** выберите тип каталога для хранения резервных копий:
  - локальный каталог — каталог расположен на текущем узле клиента резервного копирования. Если выбран этот тип хранилища, то в поле **Локальный каталог резервного копирования** укажите полный путь к каталогу (прописав в поле или выбрав по нажатию рядом с полем кнопки **[...]**;
  - сетевой каталог — общий каталог с сетевым доступом. Если выбран этот тип хранилища, то необходимо:
    - В поле **Тип сетевого каталога** выбрать протокол для обеспечения удалённой связи: `nfs` (для ОС UNIX и Linux) или `cifs` (для ОС Windows).
    - В поле **Предназначенное устройство** укажите выделенное локальное устройство (например: `/dev/sdb`) или сетевой ресурс для хранения резервных копий (например: `srv://net_share`).
    - В поле **Параметры монтирования** укажите место монтирования файловых системы LTFS. Для работы с лентами LTO RuBackup использует файловую систему LTFS. По умолчанию точка монтирования — каталог `/opt/rubackup/mnt`.

2. После заполнения всех полей формы настраиваемого компонента СРК RuBackup нажмите **[Далее]**.

   В окне подтверждения нажмите **Да** для настройки компонента СРК RuBackup (Рисунок 13).

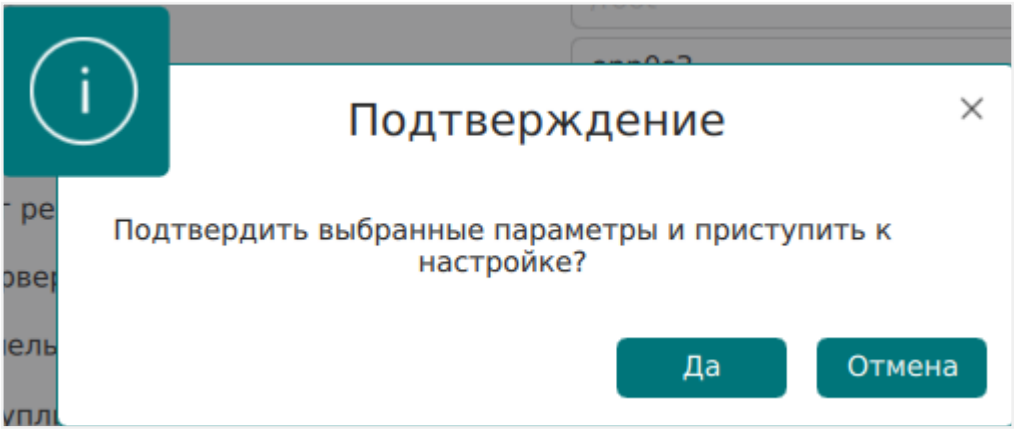


Рисунок 13. Окно подтверждения выбранных параметров

3. Если в форме настраиваемого компонента СРК RuBackup указаны папки, которых не существует, то будет выведено подтверждение для их создания (Рисунок 14).

   В окне подтверждения нажмите **Да** для создания папок.

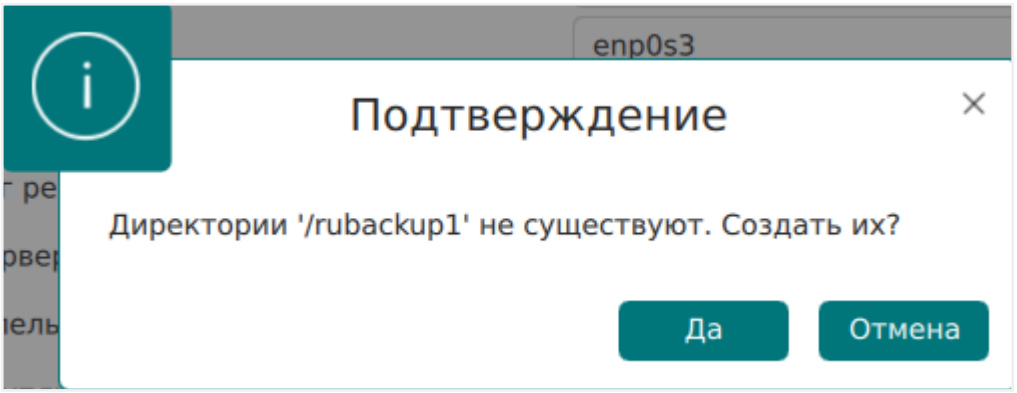


Рисунок 14. Окно подтверждения создания директорий

4. В случае успешной настройки пользователь будет уведомлён сообщением, в котором приведена информация:

   - о лицензионном соглашении;
   - правообладатель;
   - версия продукта;
   - имя текущего узла;
   - тип настроенного компонента СРК RuBackup;
   - о создании конфигурационного файла `/opt/rubackup/etc/config.file`;
   - дополнительно могут быть приведены рекомендации и предупреждения по настройкам параметров.

5. Нажмите **Завершить** для завершения работы приложения.

Настройка пользователей

Пользователи, от имени которых будет осуществляться запуск утилит командной строки RuBackup или приложения для управления СРК RuBackup (RBM, RBC, Tucana):

- иметь правильно настроенные переменные среды;
- входить в группу `rubackup`.

Выполните приведённые ниже настройки для пользователей на всех узлах с развёрнутыми компонентами СРК RuBackup.

Настройка переменных среды

1. Настройте переменные среды для всех пользователей, которые будут работать с СРК RuBackup:

   ```
   sudo nano /<имя пользователя>/.bashrc
   ```

   - отредактируйте файл, добавив строки:

   ```
   PATH=$PATH:/opt/rubackup/bin
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/rubackup/lib
   export PATH
   export LD_LIBRARY_PATH
   ```

   - сохраните изменения.

   Эти переменные также можно определить в файле `/etc/environment`.

2. Перезагрузите переменные окружения:

   ```
   source ~/.bashrc
   ```

Добавление в группу

Группа `rubackup` автоматически создаётся в процессе установки пакета `rubackup-common`.

Добавьте пользователя в группу `rubackup`:

```
sudo usermod -a -G rubackup <имя пользователя>
```

Добавление в автозапуск

1. Добавьте сервис клиента РК в автозапуск при загрузке ОС:

```
sudo systemctl enable rubackup_client.service
```

2. Перезагрузите настройки ОС:

```
sudo systemctl daemon-reload
```

5.1.4. Запуск

Произведите активацию клиентской части СРК RuBackup, выполнив на каждом узле с развёрнутым клиентом резервного копирования запуск сервиса клиента.

Для успешного запуска клиента РК в клиент-серверном режиме предварительно необходимо запустить серверную часть СРК.

Запуск сервиса клиента

Для запуска сервиса клиента РК выполните команду:

```
sudo systemctl start rubackup_client.service
```

Просмотр статуса сервиса клиента

Для просмотра статуса сервиса клиента выполните команду:

```
sudo systemctl status rubackup_client.service
```

Остановка сервиса клиента

Для останова сервиса клиента выполните команду:

```
sudo systemctl stop rubackup_client.service
```

5.2. Windows

5.2.1. Системные требования

В данном подразделе приведены системные требования для каждого клиентского компонента СРК RuBackup, предъявляемые к техническим средствам, необходи-

мым для нормального функционирования СРК RuBackup.

Аппаратные требования

Требования к аппаратным средствам клиента РК

Узел, выполняющий функции клиента РК, на котором предполагается развёртывание, должен обладать характеристиками, приведёнными в таблице Таблица 10.

Таблица 10. Требования к аппаратным средствам клиента РК

Аппаратное требование	Значение		Примечание
Процессор	Однопоточный режим	Многопоточный режим	—
	1 ядро	Количество ядер = количеству потоков	
Твердотельный накопитель	Значение требуемого дискового пространства может быть рассчитано по формуле		Не менее 400 ГБ
Оперативная память	Сумма значений оперативной памяти для всех задач резервного копирования		Где оперативная память одного ресурса равна 1ГБ + 4% от размера целевого ресурса
Интерфейсное устройство	Сетевой адаптер		—

Пример 4. Формула расчёта дискового пространства

$$V = \frac{Vol_{resource}}{Size_{block}} \times (Size_{hash} + 20) \times (K + 1) + Size_{metadata}$$

где:

- K = 1 при однопоточном режиме;
- K = `worker_parallelism`, если заданы многопоточный режим (`enable_multithreading`) и слабая дедупликация (`enable_flexible_dedup`);
  - `worker_parallelism` — количество рабочих потоков, используемых для выполнения РК;
  - `enable_multithreading` — флаг, указывающий на использование многопоточности;
  - `enable_flexible_dedup` — флаг, указывающий на использование гибкой дедупликации;
- $Vol_{resource}$ — общий объём данных, подлежащих РК;
- $Size_{block}$ — размер блока данных, используемого для обработки данных во время РК (для пулов типов "File system", "Tape library", "Cloud" размер блока является фиксированным и равен 16384 Б);

- $Size_{hash}$ — размер хеша, используемого для идентификации данных;
- *20* — максимальный размер сериализованной позиции в файле;
- *1* — временная база для вычисления сигнатуры или отправки хешей на сервер;
- $Size_{metadata}$ — это 0.02 × объем ресурса

Программные требования

Программные требования к среде функционирования клиентской части СРК RuBackup:

- 64-битная операционная система (одна из):
- Windows Server 2012;
- Windows Server 2016;
- Windows Server 2019;
- Windows Server 2022.
- библиотека OpenSSL версия 3.3.0, установленная в директорию `C:\OpenSSL-Win64`;
- пакет Microsoft Visual C++ версия 2015.

5.2.2. Установка

Подготовка к установке

Сетевые настройки

На узле развёртывания клиента резервного копирования:

1. Откройте системный файл `C:\Windows\system32\drivers\etc\hosts`.
2. Проверьте наличие строки с данными всех узлов серверной части RuBackup (основной сервер, резервный и медиасервер при наличии).

Настройка служебной СУБД PostgreSQL

Для разрешения использования символа `\` выполните следующие действия:

1. Отредактируйте конфигурационный файл `postgresql.conf` на узле служебной базы данных PostgreSQL.
2. Для параметр `standard_conforming_strings` установите значение `on`.
3. Сохраните изменения.

Установка пакета Microsoft Visual C++

Установите пакет _Microsoft Visual C footnote:[Подробное описание приведено в официальной документации на программный продукт Microsoft Visual C] :

1. Скачайте пакеты *Microsoft Visual C++* 32- и 64-разрядные версии 2015 с официального сайта *Microsoft*.
2. Запустите поочерёдно загруженные файлы `vc_redist.x86.exe` и `vc_redist.x64.exe`.
3. Следуйте инструкциям установщика.

Установка пакета OpenSSL

Установите библиотеки *OpenSSL* [5] версия 3.3.0:

1. Скачайте дистрибутив *OpenSSL* версии 3.3.0 для 64-разрядной ОС Windows на официальном сайте разработчика.
2. Запустите исполняемый файл `Win64OpenSSl-<version>.exe` и укажите директорию `C:\OpenSSL-Win64`, в которую будет установлено приложение.
3. Пропишите путь к приложению в переменных среды Windows:
   - откройте окно **Панель управления** — **Система и безопасность** — **Система**;
   - выберите **Изменить параметры** — вкладка **Дополнительно**;
   - нажмите кнопку **Переменные среды**;
   - откройте раздел **Системные переменные** в текущем окне;
   - откройте переменную `PATH`;
   - создайте два значения:
     - полный путь к папке, в которую установили приложение `C:\OpenSSL-Win64`;
     - подпапку `C:\OpenSSL-Win64\bin`;
   - нажмите **OK** для сохранения изменений.

Установка пакетов

1. Предварительно скачайте пакет клиента резервного копирования `RuBackup_client_installer<version>.exe`, где <version> — актуальная версия пакета (см. ROOT:page$distribution.pdf).
2. Запустите загруженный файл `RuBackup_client_installer<version>.exe` с правами администратора.
3. Выберите язык интерфейса установщика, примите лицензионное соглашение и начните установку.
4. Для ОС Windows Server версии 2012 и версии 2016: перезагрузите ОС для при-

менения настроек.

5.2.3. Настройка

Настройка клиента РК

Настройку компонентов СРК RuBackup следует произвести на каждом узле в строго приведённом порядке (в зависимости от архитектуры) :

1. настройка основного сервера;
2. настройка резервного сервера;
3. настройка медиасервера (выполняется для каждого медиасервера);
4. настройка клиента системы резервного копирования (выполняется для каждого клиента СРК).

Необходимо предварительно настроить сетевое взаимодействие узлов компонентов СРК RuBackup, используя `FQDN`, `hostname` или `ip-адрес` (далее по тексту — адрес).

Настройка клиента РК в терминале (интерактивный режим)

Выполните настройку компонента СРК RuBackup:

- Запустите на каждом узле, на котором развёрнут клиент РК, интерактивную утилиту `rb_init`:

```
start C:\RuBackup-win-client\bin\rb_init.exe
```

Клиент-серверный режим работы клиента РК

1. `You MUST agree with the End User License Agreement (EULA) before installing RuBackup (y[es]/n[o]/r[ead]/q[uit])`

   Примите лицензионное соглашение (EULA), нажав клавишу **<y>**.

2. `Choose client mode: client-server or autonomous (c/a)?`

   Выберите сценарий настройки клиента: клиент-сервер **<c>**.

Настройка соединения с основным сервером

3. `Hostname of primary server:`

   Укажите адрес основного (primary) сервера.

Настройка соединения с резервным сервером

4. `Will you use secondary server (y/n)?`

   Если в конфигурации подразумевается резервный (secondary) сервер, то выберите эту возможность, нажав клавишу **<y>**.

   a. `Hostname of secondary server:`

      Укажите адрес резервного (secondary) сервера.

Настройка клиента резервного копирования:

5. `Choose client net interface ID for use:`

   `Selected interface:`

   Выберите сетевой интерфейс, посредством которого клиенту RuBackup разрешено взаимодействовать с системой резервного копирования.

6. `Do you allow centralized recovery (y/n)?`

   Укажите, нужно ли включить централизованное восстановление данных?

   В случае выбора **<y>**, централизованное восстановление данных из резервной копии будет доступно с помощью утилиты «Менеджер администратора RuBackup» (RBM), с помощью консольной утилиты `rbfd` или утилиты «Менеджера клиента RuBackup» (RBC).

   В случае выбора **<n>**, централизованное восстановление данных из резервной копии с помощью утилиты «Менеджер администратора RuBackup» будет отключено, восстановление из резервной копии будет возможно с помощью консольной утилиты `rbfd` или утилиты «Менеджера клиента RuBackup».

7. `Do you plan to use continuous remote replication to apply remote replicas on this client (y/n)?`

   Укажите, будет ли использоваться непрерывная удаленная репликация на клиенте РК.

8. `Enter local backup directory path [/tmp] :`

   Укажите директорию для временных операций с файлами резервных копий и подтвердите создание каталога для временных файлов, нажав клавишу **<y>**.

   a. `Would you like to create / (y/n)?`

      Подтвердите создание каталога для временных файлов, в случае, если ука-

занного каталога ещё не существует.

9. `Create RuBackup master key…`

   Автоматическое создание мастер-ключа, который необходим при создании пары ключей для электронно-цифровой подписи резервных копий и защитного преобразования резервных копий.

10. `Will you use digital signature (y/n)?`

    `Create new secret key`

    `Create new public key`

    Укажите, хотите ли вы создать ключи электронно-цифровой подписи. Резервная копия может быть подписана цифровой подписью для последующего контроля и предупреждения угрозы её подмены.

11. `Do you want to enable system monitoring of this client (y/n)?`

    Укажите, хотите ли вы включить системный мониторинг для данного клиента.

    Файл мониторинга производительности системных компонентов будет размещён в папке `/opt/rubackup/monitoring/`.

12. `Do you want to set a soft memory threshold? (y/n)?`

    Укажите, хотите ли вы установить верхний предел оперативной памяти, которая может использоваться при резервном копировании на клиенте (точность верхней границы объема памяти не гарантируется).

    a. `Enter the allowed amount of memory for backup in GB (integer value):`

       В случае выбора **<y>** укажите максимально допустимый объём оперативной памяти, который может быть использован при резервном копировании на клиенте в ГБ (целое число).

13. `Do you want to use ipv4[1] ipv6[2] or both[3] in DNS requests?`

    Выберите какие публичные имена будут использованы DNS-сервером.

Автономный режим работы клиента РК

Автономный режим работы клиента резервного копирования в среде функционирования ОС Windows Server не поддерживается.

Настройка узла

Добавление исключения в антивирус

1. При использовании антивируса *Windows Defender* необходимо исключить папку `C:\RuBackup-win-client` из автоматической проверки:

   ```
   Add-MpPreference -ExclusionPath C:\RuBackup-win-client
   ```

2. Для проверки исключений *Windows Defender* выведите полный список исключений:

   ```
   Get-MpPreference | fl excl*
   ```

Добаление в автозапуск

Добавьте сервис клиента РК в автозапуск при загрузке ОС:

1. Откройте **Диспетчер серверов** — **Средства** — **Службы**.
2. Выберите **RuBackup Service** — **Свойства** — вкладка **Общие**.
3. Для параметра **Тип запуска** установите значение **Автоматически**(Рисунок 15).

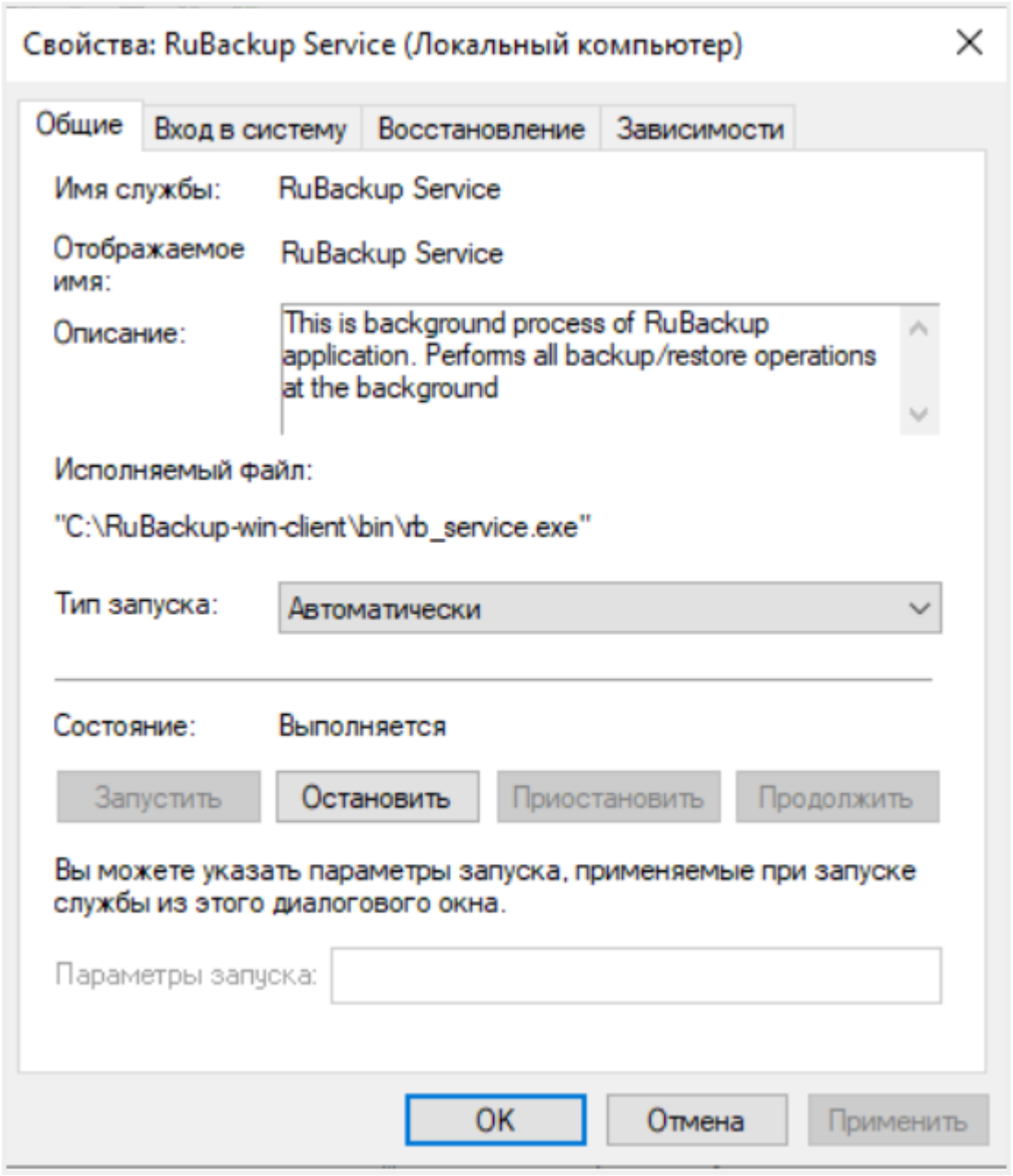


Рисунок 15. Окно «Свойства RuBackup Service»

4. Нажмите **OK** для сохранения изменений.

5.2.4. Запуск

Произведите активацию клиентской части СРК RuBackup, выполнив на каждом узле с развёрнутым клиентом резервного копирования запуск сервиса клиента.

Для успешного запуска клиента РК в клиент-серверном режиме предварительно необходимо запустить серверную часть СРК.

Запуск сервиса клиента

Запустите сервис клиента резервного копирования:

1. Откройте **Диспетчер серверов** — **Средства** — **Службы**.
2. Выберите **RuBackup Service** и запустите его.

[1] Для пула типа "Block device" размера блока может быть задан при создании пула. Значением по умолчанию является 131072 Б. Для получения более подробной информации по настройке пулов обратитесь к секции "Пулы" раздела "Хранилища" Руководства системного администратора RuBackup. Для пулов типов "File system", "Tape library", "Cloud" размер блока является фиксированным и равен 16384 Б. Для всех типов пулов длина ключа хеш-функции зависит от выбранной хеш-функции в настройках пула. Например, для хеш-функции SHA1 длина ключа составляет 20 Б

[2] ** Резервное копирование: объём свободного дискового пространства, составляющий не менее 3% от совокупного объёма данных, резервное копирование которых осуществляется единовременно. Восстановление данных: объем свободного дискового пространства должен быть не менее совокупного объема единовременно восстанавливаемых данных с использованием данного клиента. Многопоточное резервное копирование: объём свободного дискового пространства зависит от выбранных параметров: количества потоков, размера блока и длины хеша. Чем больше используется потоков, тем больше требуемый объём. Чем меньше выбранный размер блока, тем больше требуется доступного пространства на диске. Чем больше длина хеша, тем больше требуется памяти. Расчёт требуемого объёма: Приблизительный расчёт требуемого объёма доступного пространства в многопоточном режиме можно оценить как (worker_parallelism *)% от ресурса. Это означает, что для каждого рабочего потока, который будет использоваться при многопоточной обработке данных, потребуется определённый объём доступного пространства на диске.

[3] Выполните установку актуальной версии репозитория EPEL, для примера приведена установка репозитория EPEL 8

[4] обязательное для заполнения поле (если оно активно)

[5] Подробное описание приведено в официальной документации на программный продукт OpenSSL

Глава 6. Результаты установки

6.1. Каталог установки

При установке инсталляционный rpm/deb-пакет будет автоматически распакован в директорию:

- для *Linux-систем*: `/opt/rubackup`.
- для *Windows-систем*: `C:\RuBackup-win-client\`

Структура установленных пакетов СРК RuBackup приведена в таблице.

Таблица 11. Структура установленных пакетов СРК RuBackup

Структурный элемент	Назначение элемента
`/opt/rubackup`	Директория, в которой распакован установочный комплект компонента RuBackup, а также используемые дополнительные инструменты
Пакет rubackup-common	
`/opt/rubackup/keys/client/`	Папка содержит сертификат и закрытый ключ клиента для внутреннего взаимодействия компонентов СРК по протоколу SSL
`/opt/rubackup/keys/server/`	Папка содержит сертификат и закрытый ключ сервера для внутреннего взаимодействия компонентов СРК по протоколу SSL
`/opt/rubackup/keys/rootCA/`	Папка содержит самоподписанный сертификат и закрытый ключ центра сертификации для внутреннего взаимодействия компонентов СРК по протоколу SSL
`/opt/rubackup/etc/`	Папка содержит конфигурационные файлы СРК RuBackup
`/opt/rubackup/etc/ld.so.conf.d/rubackup.conf`	Вспомогательный конфигурационный файл, указывающий ОС путь к дополнительным библиотекам, используемых СРК RuBackup
`/opt/rubackup/copyrights/`	Папка содержит файлы лицензионных соглашений
`/opt/rubackup/rc/icons/`	Папка содержит иконки интерфейса
Пакет rubackup-client	
`/opt/rubackup/etc/systemd/system/`	Папка содержит сервисы СРК RuBakup
`/opt/rubackup/etc/rubackup.lsf`	Файл локального расписания Клиента системы резервного копирования
`/opt/rubackup/etc/systemd/system/rubackup_client.service`	Сервис клиентской части СРК RuBakup

Структурный элемент	Назначение элемента
`/opt/rubackup/scripts/`	Папка содержит скрипты управления СРК RuBackup
`/opt/rubackup/scripts/test-script.sh`	Пример скрипта для выполнения при резервном копировании
`/opt/rubackup/log/`	Папка содержит журналы событий и задач
`/opt/rubackup/man/`	Папка содержит инструкции по использованию утилит
`/opt/rubackup/modules/`	Папка содержит исполнительные модули, поддерживающие резервное копирование и восстановление целевого ресурса (поддерживаемого клиентом СРК)
`/opt/rubackup/modules/rb_module_lvm`	Исполняемый модуль для резервного копирования и восстановления логических томов LVM
`/opt/rubackup/modules/rb_module_filesystem`	Исполняемый модуль резервного копирования файловой системы
`/opt/rubackup/bin/`	Папка содержит консольные утилиты, поддерживаемые на клиенте для управления резервным копированием и восстановлением данных
`/opt/rubackup/bin/rb_schedule`	Утилита клиента RuBackup для просмотра правил глобального расписания клиента в системе резервного копирования
`/opt/rubackup/bin/rb_replicas`	Утилита клиента RuBackup для управления правилами репликации на клиенте. Вы можете просмотреть список всех правил репликации, а также запустить выбранное правило
`/opt/rubackup/bin/rb_health_check`	Утилита клиента RuBackup для проверки конфигурации клиента и его окружения. Выполняется проверка переменных окружения, версии медиасервера. Проверяется подключение клиента к базе данных, серверу, медиасерверу и толстому клиенту
`/opt/rubackup/bin/rubackup_client`	Клиент резервного копирования RuBackup представляет собой фоновое приложение (сервис, демон), запущенное на хосте клиента и взаимодействующее с сервером RuBackup
`/opt/rubackup/bin/rb_init`	Утилита администратора RuBackup для первоначальной настройки клиента сразу после развёртывания пакета исполняемых файлов. Неинтерактивный режим необходим для сценариев массового развертывания

Структурный элемент	Назначение элемента
`/opt/rubackup/bin/rb_archives`	Утилита клиента RuBackup предназначена для просмотра списка резервных копий клиента в системе резервного копирования, создания срочных резервных копий, их удаления, проверки и восстановления. Работает только в том случае, если на клиенте работает служба (сервис, демон) клиента rubackup_client
`/opt/rubackup/bin/rbfd`	Утилита администратора RuBackup для создания и восстановления полных и инкрементальных резервных копий ресурсов в любых файловых системах. Ресурсом может быть файл, каталог или блочное устройство
`/opt/rubackup/bin/rb_tasks`	Утилита клиента RuBackup для просмотра списка задач клиента в системе резервного копирования RuBackup
`/opt/rubackup/bin/rb_client_defined_storages`	Утилита администратора RuBackup для управления клиентскими хранилищами. Вы можете просматривать, добавлять и удалять клиентские хранилища в конфигурации
`/opt/rubackup/rc/`	Папка содержит конфигурационные скрипты программы
`/opt/rubackup/mnt/`	Предоставляется как временная точка монтирования для файловых систем
Пакет rubackup-server	
`/opt/rubackup/etc/systemd/system/`	Папка одержит сервисы СРК RuBackup
`/opt/rubackup/etc/systemd/system/rubackup_server.service`	Сервис Серверной части СРК RuBackup
`/opt/rubackup/man/`	Папка содержит файлы описаний утилит
`/opt/rubackup/log/`	Папка содержит файлы журнала событий
`/opt/rubackup/log/RuBackup.log`	Системный журнал событий, также содержит информацию о лицензии
`/opt/rubackup/log/task.log`	Журналы событий, содержащие события задач СРК
`/opt/rubackup/log/module_.log`	Журналы событий исполняемых модулей
`/opt/rubackup/log/rbfd`	Информация о процессе выполнения создания РК для каждой задачи, которая использует rbfd
`/opt/rubackup/lib/`	Папка содержит библиотеки, необходимые для работы СРК RuBackup
`/opt/rubackup/bin/`	Папка содержит исполняемые файлы для запуска утилит
`/opt/rubackup/bin/rb_modules`	Утилита администратора RuBackup для управления Модулями

Структурный элемент	Назначение элемента
`/opt/rubackup/bin/rb_tape_libraries`	Утилита администратора RuBackup для управления ленточными библиотеками в системе резервного копирования RuBackup. Вы можете просматривать информацию о ленточных библиотеках в серверной группировке RuBackup, синхронизировать ленточную библиотеку с информацией о ней в базе данных,импортировать, экспортировать и перемещать картриджи в ленточной библиотеке, а также производить LTFS форматирование картриджей, находящихся в слотах ленточной библиотеки.
`/opt/rubackup/bin/rb_media_servers`	Утилита администратора RuBackup для управления медиасерверами RuBackup. Вы можете просматривать список медиасерверов, добавлять их, удалять или изменять их описания. медиасервер предназначен для взаимодействия с клиентами при создании, восстановлении и передаче резервных копий
`/opt/rubackup/bin/rb_user_groups`	Утилита администратора RuBackup для управления группами пользователей. Вы можете просматривать группы пользователей, добавлять и удалять их, а также изменять их название и описание
`/opt/rubackup/bin/rubackup_server`	Сервер резервного копирования RuBackup представляет собой системное фоновое приложение (служба, демон), внутри которого одновременно выполняются множество потоков, отвечающих за разные функции системы резервного копирования
`/opt/rubackup/bin/rb_local_filesystems`	Утилита администратора RuBackup для управления хранилищами резервных копий типа Файловая система. Хранилища такого типа должны быть ассоциированы с пулом того же типа
`/opt/rubackup/bin/rb_security`	Утилита RuBackup для работы с журналом событий информационной безопасности
`/opt/rubackup/bin/rb_clients`	Утилита администратора RuBackup для управления клиентами RuBackup. Вы можете просматривать список клиентов, а также добавлять, удалять или изменять их.
`/opt/rubackup/bin/rb_update`	Утилита администратора RuBackup для управления обновлениями баз данных. Создает sql инструкции, позволяющие сделать обновление базы данных
`/opt/rubackup/bin/rb_block_devices`	Утилита администратора RuBackup для управления блочными устройствами

Структурный элемент	Назначение элемента
`/opt/rubackup/bin/rb_global_config`	Утилита администратора RuBackup для управления параметрами глобальной конфигурации серверной группировки RuBackup. Параметры глобальной конфигурации действительны для всех серверов, входящих в кластер серверов RuBackup
`/opt/rubackup/bin/rb_global_schedule`	Утилита администратора RuBackup для управления глобальным расписанием RuBackup. Глобальное расписание состоит из отдельных правил, которые могут выполняться по определённым условиям для определённого ресурса на клиенте системы резервного копирования. Можно просматривать список правил глобального расписания, экспортировать настройки правила в файл и импортировать правило из файла в глобальное расписание, удалять правила из глобального расписания, останавливать функционирование правила или запускать его в работу, а также немедленно создавать задачу на основе правила глобального расписания
`/opt/rubackup/bin/rb_repository`	Утилита администратора RuBackup для доступа к записям репозитория. Позволяет просматривать список резервных копий, удалять и перемещать резервные копии, проверять их целостность и выполнять их репликацию (копирование) в другие пулы. Для выполнения этих действий утилита создаёт соответствующую задачу в главной очереди задач и заканчивает своё выполнение до того момента, как задача будет выполнена
`/opt/rubackup/bin/rb_users`	Утилита администратора RuBackup для управления пользователями. Вы можете просматривать список пользователей, добавлять, удалять и изменять их
`/opt/rubackup/bin/rb_tape_cartriges`	Утилита администратора RuBackup для управления картриджами ленточных библиотек. Вы можете просматривать список картриджей, добавлять, удалять или изменять их. Каждый картридж принадлежит какому-либо пулу типа ленточная библиотека
`/opt/rubackup/bin/rb_inventory`	Утилита администратора RuBackup для внесения в базу данных RuBackup информации о резервных копиях, которые были сделаны вне текущей конфигурации RuBackup, например, в другой серверной группировке RuBackup

Структурный элемент	Назначение элемента
`/opt/rubackup/bin/rb_interoperation`	Утилита администратора RuBackup для управления задачами импорта или экспорта резервных копий между независимыми системами резервного копирования. Вы можете управлять списком систем, для которых существует возможность импорта или экспорта. Добавлять, просматривать, редактировать, удалять, останавливать и запускать правила экспорта или импорта. Также вы сможете проверять очередь задач и удалять выполненные задачи или завершившиеся с ошибкой. У вас будет возможность создать задачу на экспорт резервной копии из репозитория
`/opt/rubackup/bin/rb_clouds`	Утилита администратора RuBackup для просмотра конфигурации, добавления или удаления облаков S3 в системе резервного копирования
`/opt/rubackup/bin/rb_copy2pool`	Утилита администратора RuBackup для управления репликацией. Предоставляет возможность создавать точные копии (реплики) резервных копий для правил резервного копирования и для стратегий резервного копирования
`/opt/rubackup/bin/rb_notifications`	Утилита администратора RuBackup для управления очередью уведомлений. В очереди уведомлений содержатся все актуальные уведомления групп пользователей RuBackup о происходящих в системе событиях. Уведомления могут быть настроены в правилах глобального расписания и в стратегиях
`/opt/rubackup/bin/rb_remote_replication`	Утилита администратора RuBackup для управления непрерывной удалённой репликацией. Непрерывная удалённая репликация состоит из отдельных правил, которые могут выполняться по определённым условиям для определённого ресурса. Можно просматривать список правил непрерывной удалённой репликации, экспортировать настройки правила в файл и импортировать правило из файла, удалять правила, останавливать функционирование правила или запускать его в работу
`/opt/rubackup/bin/rb_pools`	Утилита администратора RuBackup для управления пулами. Вы можете просматривать список пулов, добавлять, удалять и изменять их. Каждый пул принадлежит какому-либо медиасерверу. Пулы используются для группирования устройств хранения резервных копий

Структурный элемент	Назначение элемента
`/opt/rubackup/bin/rb_tl_task_queue`	Утилита администратора RuBackup для управления Очередью задач ленточных библиотек
`/opt/rubackup/bin/rb_block_device_check`	Утилита администратора RuBackup для проверки целостности резервных копий на блочном устройстве
`/opt/rubackup/bin/rb_client_group`	Утилита администратора RuBackup для управления группами клиентов. Вы можете просматривать группы клиентов, добавлять их, удалять или изменять их название и описание. Группировка клиентов может потребоваться в случае необходимости выполнения групповых операций резервного копирования в стратегиях
`/opt/rubackup/bin/rb_bandwidth`	Утилита администратора RuBackup для управления ограничениями пропускной способности при выполнении операций резервного копирования для клиентов или правил глобального расписания. Вы можете установить одно или несколько ограничений пропускной способности для определённого клиента СРК или для какого-либо правила глобального расписания
`/opt/rubackup/bin/rb_task_queue`	Утилита администратора RuBackup для управления главной очередью задач. В очереди задач содержатся все актуальные задачи на создание, восстановление, удаление, перемещение и проверку резервных копий
`/opt/rubackup/bin/rb_cloud_task_queue`	Утилита администратора RuBackup для просмотра задач, которые связаны с облачными операциями. При хранении резервных копий в облаке S3 вам может потребоваться загрузить резервную копию в облако или выгрузить какой-либо из файлов резервной копии из облака
`/opt/rubackup/bin/rb_strategies`	Утилита администратора RuBackup для управления стратегиями
`/opt/rubackup/bin/rb_log_viewer`	Утилита администратора RuBackup для просмотра и управления журналами сообщений
`/opt/rubackup/rc/init/`	Содержит конфигурационные скрипты программы
`/opt/rubackup/mnt/`	Предоставляется как временная точка монтирования для файловых систем
Пакет rubackup-common-gui	
`/opt/rubackup/keys/rbm/`	Папка содержит сертификат и закрытый ключ приложения RBM для внутреннего взаимодействия компонентов СРК по протоколу SSL
`/opt/rubackup/gui/plugins/`	Папка содержит плагины

Структурный элемент	Назначение элемента
`/opt/rubackup/gui/lib/`	Папка содержит библиотеки, используемые графическим приложением RBM
`/opt/rubackup/gui/qml/`	Папка содержит QML-библиотеки, используемые графическим приложением RBM
`/opt/rubackup/gui/rc/`	Папка содержит настройки графического отображения, в т.ч. темы, переводы приложения RBM
`/opt/rubackup/gui/rc/themes/`	Файлы тем приложения RBM

6.2. Сетевые сервисы

В результате настройки компонентов СРК RuBackup будут добавлены необходимые сетевые сервисы в файл `/etc/services`:

- `rubackup-cmd` — сервис обеспечивает командное взаимодействие серверов и клиентов СРК RuBackup;
- `rubackup-lic` — сервис лицензирования;
- `rubackup-media` — сервис обеспечивает взаимодействие между медиасерверами и передачу файлов.

6.3. Конфигурационный файл

Данные, полученные после настройки (с помощью утилиты `rb_init` или `rb_init_gui`), сохраняются в файле:

- для *Linux-систем*: `/opt/rubackup/etc/config.file`;
- для *Windows-систем*: `C:\RuBackup-win-client\etc\config.file.txt`.

Таблица 12. Описание параметров конфигурационного файла

Параметр	Назначение	Допустимые значения (по умолчанию)
`server-inet-interfaces`	**Сервер**. Список сетевых интерфейсов сервера, посредством которых серверу резервного копирования разрешено взаимодействовать с клиентами	
`dbname`	**Сервер**. Имя служебной базы данных	(`rubackup`)
`user`	**Сервер**. Пользователь служебной базы данных	(`rubackup`)
`password crypted`	**Сервер**. Закодированное значение пароля пользователя служебной базы данных	-

`host`	**Сервер**. FQDN или IP адрес сервера, на котором расположена служебная база данных	Необходима настройка правильного разрешения имен
`port`	**Сервер**. Порт подключения служебной базы данных	(`5432`)

`server-shutdown_scenario`	**Сервер**. Сценарий выключения сервера	`immediately`
		`after-all-tasks`
		`cancel-if-tasks`
		(`cancel-if-tasks`)

`remote-replication`	**Сервер**. Удаленная репликация	`yes`
		`no`
		(`yes`)

`deduplication-task-memory`	**Сервер**. Исключение дублирующих копий повторяющихся данных	(`268435456`)
`parallelizm`	**Сервер**. Количество параллельных нитей сетевого асинхронного сервера RuBackup	`1-4096` `8`

`use-product-uuid false`	**Сервер**. Для версии СРК RuBackup 2.1 и более поздней: Генерировать идентификатора *hardware id* узла лицензируемого сервера на основании:
	• *для ОС Linux*: идентификатора UUID материнской платы, установленного производителем платы, и закодированной информации в DMI BIOS;
	• *для ОС Windows*: имени хоста hostname;
	Для версии СРК RuBackup 2.0 и ранее: параметра нет, `hardware id` генерируется на основании идентификатора `/etc/machine-id` и имени хоста `/etc/hostname`
		`false`
		`true`
		(`false`)

`parallelizm_media`	**Медиасервер** Количество параллельных нитей сетевого асинхронного медиасервера RuBackup	`1-4096` (`8`)

`centralized-recovery`	**Сервер, клиент**. Централизованное восстановление данных из резервной копии с помощью приложения «Менеджер администратора RuBackup» (используемой на любом узле). В случае, если централизованное восстановление отключено, то выполнить восстановление возможно только на клиенте резервного копирования с помощью утилиты командной строки rbfd или «Менеджера клиента RuBackup»	`yes`
		`no`
		(`yes`)

`node`	**Сервер, клиент**. Тип узла RuBackup	`primaryserver`
		`secondaryserver`
		`mediaserver`
		`client`

`who-is-primary-server`	**Сервер, клиент**. Имя хоста основного сервера RuBackup	Необходима настройка правильного разрешения имен
`who-is-secondary-server`	**Сервер, клиент**. Имя хоста резервного сервера RuBackup	Необходима настройка правильного разрешения имен
`logfile`	**Сервер, клиент**. Расположение системного файла журнала событий	

`used-ip-version`	**Сервер. Клиент**. Укажите какие публичные имена будут использованы DNS-сервером	`ipv4`
		`ipv6 `
		`both`

`client-hello-timeout`	**Сервер. Клиент**. Время ожидания ответа от сервера на HELLO сообщение, отправленное при запуске задачи от клиента. Задается в секундах.	`>0 ` (`240`)

`use-ip-instead-hostname`	**Сервер. Клиент**. Использовать ip адрес вместо hostname для разрешения связи между элементами СРК	`false`
		`true`
		(`false`)

`use-local-backup-directory`	**Клиент**. Каталог для временного хранения резервных копий. Если этот параметр не определен в файле конфигурации, то клиент будет запрашивать у медиасервера временное пространство для операций с резервными копиями (NFS папку)	`/tmp`
`client-inet-interface`	**Клиент**. Сетевой интерфейс клиента. Используется для отображения дополнительной информации о клиенте в СРК RuBackup. Медиасервер осуществляет связь с основным или резервным сервером, а также с клиентской утилитой rbfd через сетевой интерфейс, указываемый в этом параметре.	
`parallel-tasks`	**Клиент**. Максимальное количество одновременно выполняемых задач	`1-64` (`2`)

`rbd_algorithm`	**Клиент**. Выбор хэш функции при дедупликации	`sha1`, `sha2`, `skein`, `streebog`, `blake2b` (`sha2`)
`rbd_block_size`	**Клиент**. Размер блока данных при дедупликации, байт	8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576, по умолчанию — 16384
`rbd_hash_length`	**Клиент**. Допустимая длина хэша	`256` `512` (`256`)
`client-shutdown_scenario`	**Клиент**. Сценарий выключения клиента	`immediately ` `` `after-all-tasks` `` `cancel-if-tasks` (`cancel-if-tasks`)
`reconnect-period-count`	**Клиент**. Количество периодов переподключения	`>0` (`3`)
`reconnect-period-timeout`	**Клиент**. Таймаут между периодами переподключения	`>0` (`20` секунд)
`reconnect-count`	**Клиент**. Количество попыток переподключения в рамках одного периода	`>0 ` (`3`)
`reconnect-timeout`	**Клиент**. Таймаут между попытками переподключения в рамках одного периода	`>0` (`5` секунд)
`digital-signature`	**Клиент**. Использовать электронно- цифровую подпись	`yes` `no` (`yes`)

`digital-sign-hash`	**Клиент**. Хеш-функция для электронно-цифровой подписи	В соответствии с openssl digest command см. openssl help (`sha1`)

`monitoring-client`	**Клиент**. Мониторинг состояния системы	`yes`
		
		`no`
		
		(`yes`)

`memory-threshold`	**Клиент**. Снижение потребления оперативной памяти при полном резервном копировании Для хранения уникальных хешей и обеспечения дедупликации нужно выделить на диске дополнительное место ~0.3% от размера ресурса. Ограничения: - При использовании параметра в кластерной группе убедитесь, что все клиенты группы имеют одну версию СРК. - Параметр используется только для создания полной резервной копии	Не менее 4 ГБ и не более значения свободной оперативной памяти в системе Значение параметра не гарантирует точность верхней границы потребления памяти. Для выключения параметра можно задать его равным 0 или удалить из конфиг файла.

Глава 7. Менеджер администратора RuBackup

7.1. Системные требования

В данном подразделе приведены системные требования для каждого серверного компонента СРК RuBackup, предъявляемые к техническим средствам, необходимым для нормального функционирования СРК RuBackup.

В случае установки на один хост нескольких компонентов СРК RuBackup (например, при способе установки «Всё в одном») следует консолидировать соответствующие аппаратные требования, предъявляемые к техническому средству, на которое производится установка.

7.1.1. Аппаратные требования

Основной/резервный сервер

Минимальные аппаратные требования, необходимые для стабильного функционирования приложения «Менеджер администратора RuBackup» приведены в таблице.

Таблица 13. Аппаратные требования, предъявляемые к узлу развёртывания приложения «Менеджер администратора RuBackup»

Аппаратный компонент	Значение
Процессор	Не менее 4 ядер
Оперативная память	Не менее 4 ГБ
Дисковое пространство	Не менее 30 ГБ

7.1.2. Программные требования

Программные требования к среде функционирования приложения «Менеджер администратора RuBackup» приведены в таблице и определены:

- перечнем операционных систем, совместимых с компонентами СРК RuBackup;
- перечнем зависимостей пакетов для каждой совместимой ОС;
- открытыми портами (см. раздел port.pdf).

Таблица 14. Программные требования, предъявляемые к узлу развёртывания приложения «Менеджер администратора RuBackup» (совместимые ОС и зависимости пакетов)

Пакеты СРК	Поддерживаемая ОС	Пакет зависимости
rubackup_common, rubackup_common-gui, rubackup_rbm	Astra 1.6	libicu57, wget, gnupg2, xauth (для запуска RBM через SSH)
	Astra 1.7, Debian 10	libicu63, wget, gnupg2, xauth (для запуска RBM через SSH)
	Astra 1.8, Debian 12	libicu72, wget, gnupg2, xauth (для запуска RBM через SSH)
	Ubuntu 18.04	libicu60, wget, gnupg2, xauth (для запуска RBM через SSH)
	Ubuntu 20.04	llibicu66, wget, gnupg2, xauth (для запуска RBM через SSH)
	Ubuntu 22.04	libicu70, wget, gnupg2, xauth (для запуска RBM через SSH)
	Альт 10	libicu69, libxkbcommon-x11, xauth (для запуска RBM через SSH)
	CentOS 7	libicu50.2
	CentOS 8	libicu60.3
	RedOS 7.3	libicu65.1
	RedOS 8	libicu71.1
	RHEL 9	libicu67.1
	Rosa Cobalt 7.3	qt5-qtbase-gui, libicu, libxkbcommon-x11, libicu50.2
	Rosa Cobalt 7.9	qt5-qtbase-gui, libicu, libxkbcommon-x11, libicu50.1.2, libxkbcommon-x11
	Rosa Chrome 12	qt5-qtbase-gui, lib64icudata71, libxkbcommon-x11

7.2. Установка

Графическое приложение «Менеджер администратора RuBackup» возможно установить:

- на узле компонента RuBackup;
- на АРМ администратора СРК.

7.2.1. Подготовка к установке

Установка зависимостей пакетов

Данный шаг предназначен для установки локальных пакетов. Если вы устанавливаете пакеты из репозитория, то пропустите этот шаг.

Для успешного развёртывания Менеджера администратора RuBackup необходимо наличие установленных зависимостей пакетов в соответствии с таблицей, в зависимости от используемой операционной системы, для этого:

1. Проверьте наличие установленных зависимостей пакетов в ОС:

Astra Linux, Debian, Ubuntu	`dpkg-query -l`
Альт	`apt list --installed`
Rosa Cobalt, RHEL	`yum list --installed`
RedOS, CentOS, Rosa Chrome	`dnf list installed`

2. Обновите репозитории пакетов в системе:

Astra Linux, Debian, Ubuntu	`sudo apt update`
Альт	`sudo apt-get update`
Rosa Cobalt, RHEL	`sudo yum update`
RedOS, CentOS, Rosa Chrome	`sudo dnf update`

3. Установите недостающие зависимости пакетов из таблицы:

Astra Linux, Debian, Ubuntu	`sudo apt install <namepackage>`
Альт	`sudo apt-get install <namepackage>`
Rosa Cobalt, RHEL	`sudo yum install <namepackage>`
RedOS, CentOS, Rosa Chrome	`sudo dnf install <namepackage>`

Настройка публичного репозитория

Данный шаг предназначен для установки из публичного репозитория. Если вы устанавливаете локальные пакеты, то пропустите этот шаг.

Для подключения репозитория:

1. Добавьте ключ репозитория:

```
sudo wget -qO -
https://edge.astralinux.ru/artifactory/api/security/keypair/gc-astra-
official-repo-key/public | sudo apt-key add -
```

При возникновении ошибок с добавлением ключа убедитесь, что в

файле `/etc/resolv.conf` указаны корректные серверы доменных имен.

2. Отредактируйте список используемых репозиториев:

```
sudo nano /etc/apt/sources.list
```

и добавив строку для подключения дополнительного публичного репозитория:

```
deb https://dl.astralinux.ru/rubackup/repository-deb-main/ [OS-VERSION]
public
```

где: `OS-VERSION` - версия используемой ОС:

- Astra Linux 1.8;
- Astra Linux 1.7;
- Astra Linux 1.6;
- Debian 10;
- Ubuntu 20.04;
- Ubuntu 18.04.

3. Обновите список пакетов:

```
sudo apt-get update
```

Настройка переменных среды

Выполните настройку переменных среды для пользователя `root`:

1. Авторизуйтесь под пользователем `root`:

```
sudo -i
```

2. Настройте переменные среды для пользователя `root`:

```
sudo nano /root/.bashrc
```

- отредактируйте файл, добавив строки:

```
PATH=$PATH:/opt/rubackup/bin
```

```
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/rubackup/lib
export PATH
export LD_LIBRARY_PATH
```

- сохраните изменения.

Эти переменные также можно определить в файле `/etc/environment`.

3. Перейдите в каталог `/root`:

```
cd /root
```

4. Перезагрузите переменные окружения:

```
source ~/.bashrc
```

Настройка служебной базы данных

Данный шаг выполняется только при установке Менеджера администратора RuBackup на АРМ администратора СРК. При установке на узел компонента СРК пропустите этот шаг.

На узле служебной базы данных СРК RuBackup выполните настройку для подключения Менеджера администратора RuBackup к служебной базе данных в соответствии с разделом setup-database.pdf.

Настройка SSL соединения с базой данных

Данный шаг выполняется только при установке Менеджера администратора RuBackup на АРМ администратора СРК. При установке на узел компонента СРК пропустите этот шаг.

Данная настройка выполняется при необходимости создания защищённого подключения к служебной базе данных. В ином случае данную настройку можно пропустить.

Для подключения к базе PostgreSQL данных через защищённое соединение выполните приведённые ниже настройки на текущем хосте:

1. Перенесите из соответствующей postgres-клиенту папки на узле Центра сертификации подготовленные:
   - сертификат Центра сертификации (ca.crt), чтобы postgres-клиент мог проверить, что конечный сертификат сервера PostgreSQL был подписан его дове-

ренным корневым сертификатом;
- сертификат клиента (postgresql.crt);
- сгенерированный закрытый ключ клиента (postgresql.key).

2. Разместите сертификаты и закрытый ключ в каталоге по умолчанию:

Для ОС Linux	`~/.postgresql/`
Для ОС Windows	`%appdata%\postgresql\`

3. Для файлов сертификата и закрытого ключа установите полный доступ на чтение и запись только для владельцев:

```
chmod 600 server.crt server.key ca.crt
```

4. Для файлов сертификата и закрытого ключа сделайте владельцем файлов пользователя, от имени которого будет запущен RBM (postgres-клиент):

```
chown suser:suser server.crt server.key ca.crt
```

5. После установки пакетов RBM выполните настройку параметра `SSLMode` в конфигурационном файле `~/.rbm2/.rb_gui_main_settings` (см. раздел Конфигурационный файл) или в графической утилите RBM в окне «Настройки — Локальная конфигурация» параметр *Режим SSL соединения с PostgreSQL*, установив значение, указанное для сервера СРК.
6. Для применения изменений перезапустите настраиваемый клиент:

```
opt/rubackup/bin/rbm
```

7. Выполните проверку сертификата:

```
openssl verify -verbose -CAfile RootCert.pem Intermediate.pem
```

7.2.2. Установка пакетов

Установку пакетов производить строго в приведённой последовательности!

1. Установите одним из способов:
   - из локальной папки со скачанными пакетами:

Astra Linux, Debian, Ubuntu	`sudo apt install ./<namepackage>.deb`
Альт	`sudo apt-get install ./<namepackage>.rpm`
Rosa Cobalt, RHEL	`sudo yum install ./<namepackage>.rpm`
RedOS, CentOS, Rosa Chrome	`sudo dnf install ./<namepackage>.rpm`

- из репозитория:

Astra Linux, Debian, Ubuntu	`sudo apt install <namepackage>.deb`

где `<namepackage>` — устанавливаемый пакет RuBackup актуальной версии в приведённой последовательности:

a. `rubackup-common` - только при установке на АРМ администратора (при установке на узел компонента СРК данный пакет ранее был установлен);
b. `rubackup-common-gui`;
c. `rubackup-rbm`.

7.3. Настройка

7.3.1. Настройка переменных среды

1. Настройте переменные среды для всех пользователей, которые будут работать с СРК:

```
sudo nano /<имя пользователя>/.bashrc
```

- отредактируйте файл, добавив строки:

```
PATH=$PATH:/opt/rubackup/bin
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/rubackup/lib
export PATH
export LD_LIBRARY_PATH
```

- сохраните изменения.

Эти переменные также можно определить в файле `/etc/environment`.

2. Перезагрузите переменные окружения:

```
source ~/.bashrc
```

7.3.2. Добавление в группу

Группа `rubackup` автоматически создаётся в процессе установки пакета `rubackup-common`.

Добавьте пользователя в группу `rubackup`:

```
sudo usermod -a -G rubackup <имя пользователя>
```

7.4. Результаты установки

7.4.1. Каталог установки

При установке инсталляционный rpm/deb-пакет будет автоматически распакован в директорию `/opt/rubackup`.

Структура установленных пакетов сервера (основного, резервного или медиа) приведена в таблице.

Таблица 15. Структура установленных пакетов основного сервера

Структурный элемент	**Назначение элемента**
`/opt/rubackup`	Директория, в которой распакован установочный комплект компонента RuBackup, а также используемые дополнительные инструменты
Пакет `rubackup-common`	
`/opt/rubackup/keys/client/`	Папка содержит сертификат и закрытый ключ клиента для внутреннего взаимодействия компонентов СРК по протоколу SSL
`/opt/rubackup/keys/server/`	Папка содержит сертификат и закрытый ключ сервера для внутреннего взаимодействия компонентов СРК по протоколу SSL
`/opt/rubackup/keys/rootCA/`	Папка содержит самоподписанный сертификат и закрытый ключ центра сертификации для внутреннего взаимодействия компонентов СРК по протоколу SSL
`/opt/rubackup/etc/`	Папка содержит конфигурационные файлы СРК RuBackup
`/opt/rubackup/etc/ld.so.conf.d/rubackup.conf`	Вспомогательный конфигурационный файл, указывающий ОС путь к дополнительным библиотекам, используемых СРК RuBackup

Структурный элемент	Назначение элемента
`/opt/rubackup/copyrights/`	Папка содержит файлы лицензионных соглашений
`/opt/rubackup/rc/icons/`	Папка содержит иконки интерфейса
Пакет `rubackup-common-gui`	
`/opt/rubackup/keys/rbm/`	Папка содержит сертификат и закрытый ключ приложения RBM для внутреннего взаимодействия компонентов СРК по протоколу SSL
`/opt/rubackup/gui/plugins/`	Папка содержит плагины
`/opt/rubackup/gui/lib/`	Папка содержит библиотеки, используемые графическим приложением RBM
`/opt/rubackup/gui/qml/`	Папка содержит QML-библиотеки, используемые графическим приложением RBM
`/opt/rubackup/gui/rc/`	Папка содержит настройки графического отображения, в т.ч. темы, переводы приложения RBM
`/opt/rubackup/gui/rc/themes/`	Файлы тем приложения RBM
Пакет `rubackup-rbm`	
`~/.rbm2/.logs`	Журнал событий, содержащий события в соответствии с установленным уровнем логирования, для служебного использования
`~/.rbm2/.rb_gui_column_settings`	Файл настройки колонок таблиц в окне RBM для запоминания настроек пользователя (true — показать колонку, false — скрыть колонку)
`~/.rbm2/.rb_gui_main_settings`	Конфигурационный файл, содержащий информацию о параметрах и настройках RBM
`/opt/rubackup/gui/rc/langs/`	Файлы с текстами переводов интерфейса приложения RBM
`/opt/rubackup/gui/rc/info/`	Информационные подсказки приложения RBM
`/opt/rubackup/bin/rbm`	Исполняемый файл приложения RBM

7.4.2. Добавленные сервисы

В результате настройки будут добавлены необходимые сетевые сервисы в файл `/etc/services`:

- `rubackup-rbm` — сервис обеспечивает командное взаимодействие между средствами управления (RBM) и основным сервером группировки.

7.4.3. Конфигурационный файл

Данные, полученные после установки Менеджера администратора RuBackup, сохраняются в файле `home/<username>/.rbm2/.rb_gui_main_settings`.

Таблица 16. Описание параметров конфигурационного файла `/home/<username>/.rbm2/.rb_gui_main_settings`

Параметр	Значение по умолчанию	Возможные значения	Описание
`ExitWithoutConfirmation`	`false`	`false`, `true`	Выход пользователя из RBM без подтверждения
`ExperimentalLogic`	`false`	`false`, `true`	Функция экспериментального режима (не протестированные дополнительные возможности RBM)
`Hostname`	`localhost`	FQDN, hostname или ip-адрес	Адрес текущего хоста
`IdleTimeoutInMinutes`	5	Целое число от 5 до 29	Время бездействия пользователя для автоматического выхода из RBM (в минутах)
`InfoHints`	`true`	`false`, `true`	Показывать справочные подсказки
`Lang`	`Ru`	`Ru`, `En`	Язык на элементах графического интерфейса RBM
`LogsLevel`	0	Уровень логирования	
		0	Нет сообщений
		1	Fatal
		2	Critical | Fatal
		3	Warning | Critical | Fatal
		4	Debug | Warning | Critical | Fatal
		5	Info | Debug | Warning | Critical | Fatal
`RecordPerPage`	50	Целое неотрицательное число	Максимальное количество записей в таблице окна RBM на одной странице

`SSLMode` [1]	allow	Режим SSL-соединения с СУБД PostgreSQL	
		`disable`	Мне не важна безопасность и я не приемлю издержки, связанные с шифрованием
		`allow`	Мне не важна безопасность, но я приемлю издержки, связанные с шифрованием, если на этом настаивает сервер
		`prefer`	Мне не важна безопасность, но я предпочитаю шифрование (и приемлю связанные издержки), если это поддерживает сервер
		`require`	Я хочу, чтобы мои данные шифровались, и я приемлю сопутствующие издержки. Я доверяю сети в том, что она обеспечивает подключение к нужному серверу
		`verify-ca`	Я хочу, чтобы мои данные шифровались, и я приемлю сопутствующие издержки. Мне нужна уверенность в том, что я подключаюсь к доверенному серверу
		`verify-full`	Я хочу, чтобы мои данные шифровались, и я приемлю сопутствующие издержки. Мне нужна уверенность в том, что я подключаюсь к доверенному серверу и это именно указанный мной сервер
`SessionIsBlocked`	`false`	`false`, `true`	Автоматический выход из системы, если пользователь не активен в течении времени, указанного для параметра *IdleTimeoutInMinutes*

`Theme`	`default_theme`	`dark2_theme`	Настройка внешнего вида графического интерфейса RBM
		`dark_theme`	
		`default_theme`	
		`pink_theme`	
		`vtb_theme`	
`UpdateTablePeriod`	5	Целое число от 1 до 999999	Период времени, через который информация на странице будет обновлена (в секундах)
`UseMsAdAuthByDefault`	`false`	`false`, `true`	Использование базы данных MS AD по умолчанию
`Username`	`rubackup`	Имя пользователя, входящего в группу `rubackup`	Имя учётной записи пользователя, используемой для входа в RBM и подключения к СУБД PostgreSQL
`UsernameWithDomain`	`rubackup`	FQDN	Имя учётной записи пользователя, используемой для входа в RBM и подключения к базе данных MS AD
		Имя пользователя, входящего в группу `rubackup`	Если происходит подключение к СУБД PostgreSQL, то укажите значение параметра `Username`

[1] для настройки SSL соединения выполните действия, указанные в подразделе «Ошибка: источник перекрёстной ссылки не найден» настоящего документа

Глава 8. Настройка ограничения на количество открытых файловых дескрипторов на хосте с сервером RuBackup

При увеличении количества входящих соединений (если число клиентов/медиа серверов в группировке растёт и/или на клиентах включена функция многопоточной передачи данных) сервер RuBackup может достичь предела выделенных лимитов на открытые файловые дескрипторы. Сетевые соединения также используют файловые дескрипторы.

Ограничения на количество открытых файловых дескрипторов устанавливает администратор узла, на котором запущен сервер RuBackup. Достижение этого ограничения приводит к ошибкам при выполнении резервного копирования/восстановления. Иногда сервер RuBackup может аварийно завершить работу.

8.1. Зависимость количества файловых дескрипторов

В зависимости от способа запуска сервера RuBackup, максимальное число (лимит) открытых дескрипторов будет разным.

Чтобы рассчитать необходимое количество файловых дескрипторов, учтите следующее:

- В режиме простоя сервер использует около 100 файловых дескрипторов.
- Каждый подключённый клиент РК или медиасервер добавляет по два открытых файловых дескриптора на сервере.
- Выполнение любой задачи на стороне клиента РК при выключенном параметре `network_parallelism` [1] требует двух дополнительных файловых дескриптора на сервере.
- При активированном параметре `network_parallelism` клиент РК открывает *N* соединений к серверу, где N — значение, заданное для этого параметра. В рамках каждого сетевого соединения, как правило, на стороне сервера требуется запросить информацию из базы данных, поэтому требуемое число открытых файловых дескрипторов будет *N*2*.

8.2. Расчёт необходимого количества файловых дескрипторов

Проверьте, рассчитав по формулам, число нужных вам файловых дескрипторов и

убедитесь, что на узле сервера RuBackup их достаточно.

Пример 5. Общая формула для расчёта необходимого количества файловых дескрипторов:

где:

- МС — число медиасерверов;
- КЛ — число клиентов;
- N — значение, заданное для сетевого параллелизма, параметра network_parallelism. Если сетевой параллелизм выключен, то N=2.

Пример расчета 1

Рассмотрим пример расчёта необходимого количества файловых дескрипторов для системы, состоящей из одного сервера RuBackup, двух медиасерверов и 50 клиентов. Предположим, что сетевой параллелизм отключён.

Необходимое количество файловых дескрипторов рассчитывается следующим образом:

```
100 (для основного сервера)+2*2 (для медисерверов)+50*2 (для клиентов в
простое)+50*2 (для клиентов с задачами одновременно) = 304
```

Таким образом, общее количество необходимых файловых дескрипторов составляет 304.

Стандартное значение лимита — 1024, будет достаточным.

Пример расчета 2

Рассмотрим пример расчёта необходимого количества файловых дескрипторов для системы, состоящей из одного сервера RuBackup, двух медиасерверов и 50 клиентов. Предположим, что сетевой параллелизм включён со значением 40.

Необходимое количество файловых дескрипторов рассчитывается следующим образом:

```
100 (для основного сервера) + 2*2 (для медиасерверов) + 50*2 (для клиентов в
простое) + 50*40 (для всех клиентов с задачами одновременно)= 2204
```

Таким образом, общее количество необходимых файловых дескрипторов составляет 2204.

Стандартное значение лимита в 1024 будет недостаточным для такой системы, поэтому рекомендуется увеличить лимит. Желательно установить лимит в 3000 файловых дескрипторов для запаса.

8.3. Способы настройки ограничения количества открытых файловых дескрипторов

Настройка ограничения количества открытых файловых дескрипторов производится в зависимости от способа запуска сервера.

8.3.1. Настройка ограничения количества открытых файловых дескрипторов при ручном запуске сервера

Для настройки ограничения количества открытых файловых дескрипторов при ручном запуске сервера:

1. Остановите сервер (в случае ручного запуска сервера):

   ```
   rubackup_server stop
   ```

2. Для проверки текущего лимита выполните:

   ```
   sudo ulimit -n
   ```

   По умолчанию ограничение количества открытых файловых дескрипторов установлено 1024 файла.

3. Изменение лимита открытых файловых дескрипторов возможно выполнить для текущей сессии пользователя `root` или установить постоянное значение.

   a. Для временного изменения лимита открытых файловых дескрипторов только в текущей сессии пользователя `root` необходимо выполнить команду:

      ```
      ulimit -n N
      ```

      где `N` — это желаемое значение лимита открытых файловых дескрипторов.

      Внесённые изменения будут отменены после завершения текущей сессии.

   b. Для установки постоянного лимита открытых файловых дескрипторов:

      - отредактируйте файл `/etc/security/limits.conf`:

```
sudo nano /etc/security/limits.conf
```

и добавив строки:

```
root hard nofile N
root soft nofile N
```

где `N` — это желаемое значение лимита открытых файловых дескрипторов;

- сохраните изменения;
- завершите сессию и откройте новую сессию;
- проверьте значение лимита открытых файловых дескрипторов:

```
ulimit -n
```

4. Перезапустите сервер:

```
rubackup_server start
```

8.3.2. Настройка ограничения количества открытых файловых дескрипторов при запуске сервисов сервера

Для настройки ограничения количества открытых файловых дескрипторов при запуске сервисов сервера:

1. Для проверки текущего лимита выполните:

```
sudo ulimit -n
```

По умолчанию ограничение количества открытых файловых дескрипторов задаётся в службе `systemd` и стандартное значение — 1024 файла.

2. Для изменения лимита открытых файловых дескрипторов:
   - откройте файл `/etc/systemd/system/rubackup_server.service`:

```
sudo nano /etc/systemd/system/rubackup_server.service
```

   - отредактируйте секцию [`Service`], добавив строку:

```
LimitNOFILE=N
```

где `N` — это желаемое значение лимита открытых файловых дескрипторов;

- сохраните изменения.

3. Загрузите обновленный конфигурационный файл сервиса в службу `systemd`:

```
systemctl daemon-reload
```

4. Перезапустите сервис сервера RuBackup:

```
systemctl stop rubackup_server

systemctl start rubackup_server
```

[1] Параметр задает количество потоков, которые будут передавать блоки данных на медиасервер