RuBackup

Система резервного копирования
и восстановления данных

ОСНОВНЫЕ СВЕДЕНИЯ

ВЕРСИЯ 2.4.0

Содержание

Резервное копирование и восстановление данных . . . 3
Основные функции . . . 4
Надежность и производительность . . . 4
Автоматизация . . . 4
Управляемость . . . 4
Безопасность . . . 5
Преимущества . . . 6
1. Ключевые понятия . . . 7
2. Архитектура . . . 10
3. Многопользовательская модель . . . 13
4. Основные компоненты RuBackup . . . 16
4.1. Клиент резервного копирования . . . 16
4.1.1. Запуск клиента RuBackup . . . 16
4.2. Сервер резервного копирования . . . 18
4.2.1. Запуск сервера RuBackup . . . 18
5. Лицензирование . . . 21
5.1. Типы лицензий . . . 21
5.2. Файл лицензии . . . 23
5.3. Получение сведений о лицензии . . . 23
5.4. Просмотр сведений о лицензии в журнале событий . . . 23
5.5. Просмотр сведений о лицензии в Менеджере администратора RuBackup . . . 24
5.6. Генерирование hardware id . . . 25
5.7. Уведомление о наступлении ограничения лицензии . . . 26

Система резервного копирования RuBackup — клиент-серверное приложение, которое:

- автоматически выполняет резервное копирование СУБД, виртуальных машин,почтовых систем, файловых систем, подсистемы Linux и службы каталогов;
- восстанавливает данные из резервных копий по запросу.

Система резервного копирования RuBackup — единое решение для защиты и восстановления данных корпоративной среды, соответствующее требованиям безопасности: сертификат соответствия ФСТЭК России №4879.

Резервное копирование и восстановление данных

СУБД	Системы виртуализации	Почтовые системы
Tantor Special Edition (с использованием модуля PostgreSQL) Arenadata Greenplum MySQL PostgreSQL + в кластере Patroni Postgres Pro	**ПК СВ «Брест»** АЭРОДИСК vAir Р-Виртуализация РУСТЭК Dynamix KVM OpenStack oVirt/zVirt/REDVirt ROSA Tionix VMmanager VMware vSphere	**RuPost** CommuniGate Pro VK Workmail

Файловые системы	Подсистема Linux	Служба каталогов
Linux (Ext4, Ext3, Ext2, XFS, ZFS, BTRFS) Windows (NTFS)	LVM Linux	**FreeIPA**

Быстрый старт

Начните работу в корпоративной среде

Основные функции

Надежность и производительность

- Полное, инкрементальное и дифференциальное резервное копирование
- Хранение резервных копий в СХД, ленточных библиотеках, облаке S3
- Автоматическая верификация резервных копий (размер файлов, md5sum, электронная подпись)
- Защитное преобразование резервных копий по алгоритмам ГОСТ 34-12-2015 (Kuznyechik), Anubis, ARIA, CAST6, Camellia, Kalyna, MARS, AES, Serpent, Simon, SM4, Speck, Treefish, Twofish
- Сжатие резервных копий на клиенте СРК или на сервере
- Срочное резервное копирование по инициативе клиента СРК или администратора
- Параллелизм — количество одновременных сессий ограничено только аппаратными характеристиками сервера. Параллельные сессии доступны как для СРК в целом, так и для отдельного клиента

Автоматизация

- Аналитика — построение плана резервного копирования с прогнозированием требуемых ресурсов
- Экономия дискового пространства — автоматическое перемещение резервных копий на другие носители и удаление устаревших копий
- Балансировка нагрузки — распределение копий по разным хранилищам в зависимости от выбранной политики
- Глобальное расписание — автоматическое создание резервных копий клиентских устройств
- Локальное расписание — клиенты могут управлять резервным копированием самостоятельно
- Стратегии резервного копирования — автоматические групповые операции с клиентами СРК

Управляемость

- Полноценное управление системой из командной строки
- Графические интерфейсы для пользователя и для администратора СРК
- Взаимодействие с любыми системами через REST API

Безопасность

- Ролевая модель администрирования
- Локальный лист запретов (с regexp) для каждого клиента, ограничивающий доступную для копирования информацию
- Уведомление пользователей о событиях
- Протоколирование всех действий администратора и пользователей в базе данных и системном журнале

Преимущества

- Лучшая производительность среди российских решений
- Единственное решение с многопоточностью — на всех этапах позволяет выполнять самые жесткие требования к срокам RPO и RTO
- Широкие возможности интеграции — полнофункциональный REST API, толстый клиент и Web, CLI, документация для интеграторов и клиентов
- Надежность и масштабируемость — встроенные алгоритмы кластеризации и балансировки нагрузки между узлами СРК, резервирование собственных компонентов СРК
- Глубокая интеграция с Postgres — поддержка инкрементальных и дифференциальных копий (PTRACK, DELTA, PAGE), использование механизмов работы с томами (LVM и аппаратные снэпшоты)

Узнайте больше

[1] Справочный центр находится в стадии разработки

Глава 1. Ключевые понятия

Серверная группировка RuBackup состоит из основного сервера, необязательного резервного сервера и медиасерверов. В простейшем случае медиасервером является основной сервер резервного копирования (а также резервный сервер, при наличии).

Клиент системы резервного копирования — это отдельный сервер, компьютер или виртуальная машина, на которой установлено клиентское ПО RuBackup для выполнения резервного копирования. Для удобства клиенты могут быть объединены в **группы клиентов**.

На программном уровне сервером RuBackup называется также фоновый процесс (сервис) на сервере СРК, а клиентом RuBackup — фоновое клиентское ПО.

Хранение данных резервных копий (архивов) реализовано в виде хранилищ (storage). Каждое **хранилище** входит в определенный **пул**. Пул — это логическое объединение однотипных устройств хранения резервных копий. Каждый **пул** принадлежит определенному **медиасерверу**. Таким образом, организация хранения данных резервных копий имеет следующую структуру:

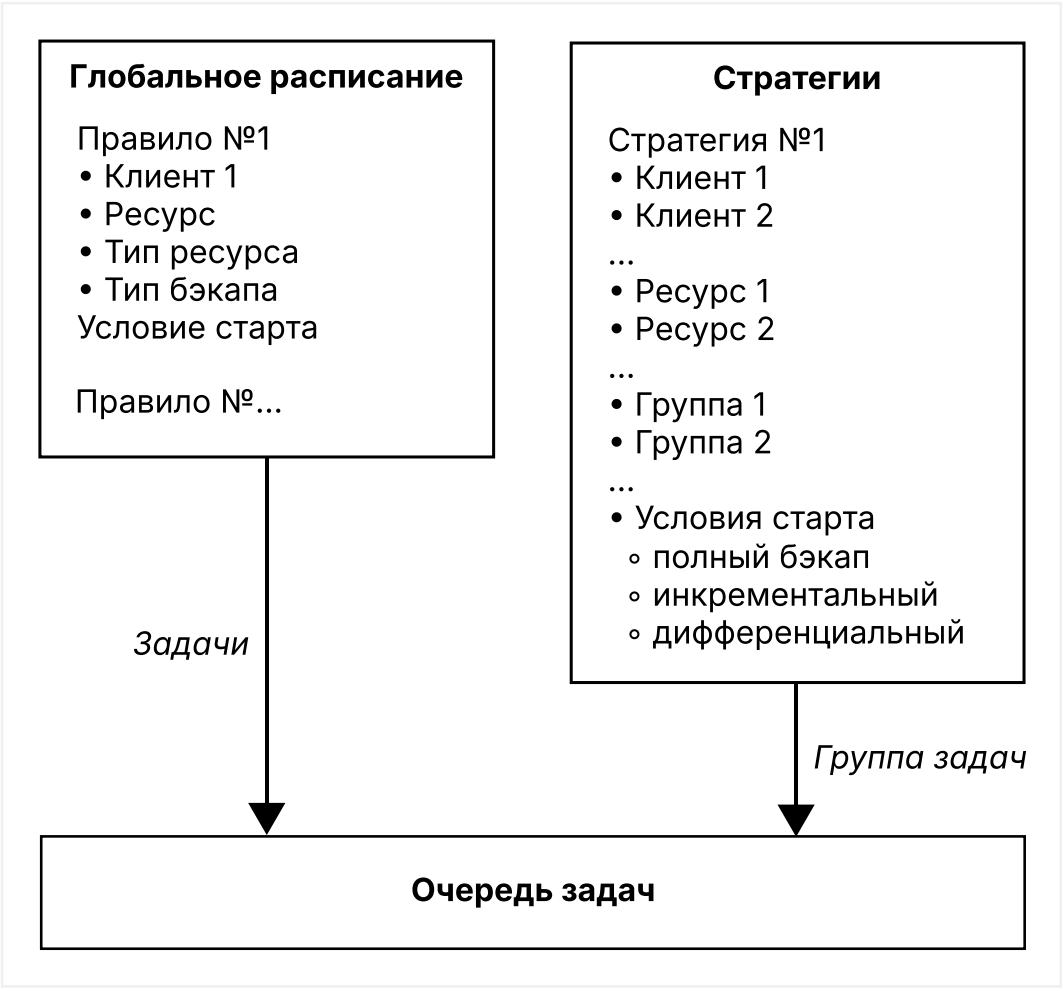
```
Медиасервер → Пул → Хранилище
```

Метаданные резервных копий хранятся в **репозитории**. Непосредственно **резервные копии** располагаются в **хранилищах** резервных копий, которые ассоциированы с **пулами** хранения резервных копий. Хранилища бывают пяти типов:

1. файловая система;
2. ленточная библиотека;
3. облако;
4. блочные устройства;
5. определяемые клиентом.

Все действия СРК реализованы в виде **задач**, которые объединены в **очереди задач**, в зависимости от типа.

Периодические задания резервного копирования и восстановления данных реализованы в виде **правил глобального расписания**, которые входят в **глобальное расписание** резервного копирования (рисунок 1).



Одновременные действия над группами ресурсов реализованы в виде **стратегий**, которые создают **задачи** резервного копирования в соответствии с **расписаниями** для всех ресурсов и клиентов, которые их касаются.

Система уведомлений RuBackup использует **пользователей** и **группы пользователей** RuBackup для уведомления о событиях системы резервного копирования.

Автономный режим работы клиента — использование клиента СРК RuBackup без сервера резервного копирования. При этом сохраняется возможность использования некоторых клиентских функциональных модулей для создания резервных копий. Чтобы узнать, поддерживается ли использование модуля в автономном режиме, запустите исполнимый файл модуля с опцией --autonomous и проверьте код возврата.

Пример 1. Команда проверки поддержки автономного режима для модуля rb_module_filesystem

```
sudo /opt/rubackup/modules/rb_module_filesystem –autonomous
```

Пример 2. Команда проверки кода возврата

```
echo $?
```

Код возврата «0» говорит о том, что модуль поддерживает автономный режим, другие коды возврата говорят о том, что автономный режим не поддерживается.

Неинтерактивный режим работы — режим для сценариев массового развертывания, например при использовании Ansible.

Резервный сервер и медиасервер не функционируют с тестовой лицензией!

Глава 2. Архитектура

В минимальной конфигурации СРК RuBackup представляет собой один сервер резервного копирования и один клиент резервного копирования, установленный на том же хосте, на котором работает сервер резервного копирования.

Сервер резервного копирования представляет собой системное фоновое приложение (служба, демон), внутри которого одновременно выполняются множество потоков, отвечающих за разные функции системы резервного копирования.

В простейшем случае единственный сервер резервного копирования взаимодействует с клиентами, координирует задания СРК и хранит резервные копии на доступных ему ресурсах: файловых системах, картриджах ленточных библиотек и облачных сервисах.

В случае обслуживания высококритичных сервисов, система резервного копирования может быть дополнена резервным сервером. В случае отказа основного сервера, резервный сервер автоматически 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.

Взаимодействие между системой резервного копирования и ее клиентами обеспечивает основной сервер резервного копирования RuBackup, либо резервный сервер, если он функционирует в режиме замещения основного сервера.

И основной, и резервный серверы включают в себя функционал медиасервера. Медиасервер предназначен для хранения резервных копий, получения их от клиентов и передачи клиентам файлов резервных копий по запросу.

При увеличении количества клиентов, а также при увеличении количества ресурсов, на которых предполагается хранить резервные копии, могут возникнуть задачи распределения нагрузки. В этом случае в серверную группировку могут быть добавлены медиасерверы, с помощью которых можно перераспределить задачи резервного копирования на несколько серверов резервного копирования или построить иерархическую систему хранения резервных копий.

Система резервного копирования RuBackup может выполнять полное, инкрементальное и дифференциальное (разностное) резервное копирование информационных ресурсов разных типов: отдельные файлы и каталоги, блочные устройства, на которых располагаются сырые данные или файловые системы, логические тома LVM, виртуальные машины и базы данных. Функционал резервного копирования и восстановления ресурсов разных типов реализован в соответствующих модулях на клиенте.

Полное резервное копирование — это создание резервной копии всех данных из

исходного набора, независимо от того, изменялись ли данные с момента выполнения последней полной резервной копии.

Дифференциальное (разностное) резервное копирование сохраняет только данные, измененные со времени выполнения предыдущего полного резервного копирования.

Инкрементальное резервное копирование сохраняет только данные, измененные со времени выполнения предыдущей инкрементальной резервной копии, а при отсутствии таковой — со времени выполнения последней полной резервной копии.

Резервное копирование выполняется по заранее заданным правилам в глобальном расписании RuBackup, а также в соответствии с правилами локального расписания клиента, если это разрешено клиенту администратором RuBackup. Также клиенту доступно срочное резервное копирование тех или иных файлов, но в этом случае выполняется полное резервное копирование выбранного ресурса.

Восстановление резервной копии возможно по инициативе клиента. Для восстановления данных пользователь должен ввести пароль, позволяющий выполнить восстановление.

Резервное копирование может быть выполнено с применением сжатия на стороне клиента или на стороне сервера RuBackup. Возможно произвести защитное преобразование резервной копии выбранным алгоритмом. При необходимости резервная копия может быть подписана цифровой подписью на стороне клиента для последующего контроля и предупреждения угрозы ее подмены.

Система резервного копирования может быть настроена таким образом, что резервные копии будут перемещаться на другие устройства хранения (например с дискового устройства хранения на картридж ленточной библиотеки) по достижении определенного срока хранения. Устаревшие резервные копии могут быть удалены из СРК автоматически или сообщение о том, что их следует удалить, будет отправлено администраторам СРК. Время от времени может выполняться проверка резервных копий по разным критериям.

Общий объем резервных копий, хранящихся в системе резервного копирования, может быть ограничен для клиента СРК, или для правила резервного копирования, или для стратегии резервного копирования.

Правила резервного копирования глобального расписания RuBackup имеют определенные время и даты начала и окончания действия. При необходимости правило можно выключить или вновь включить в работу.

Внутренние автоматические работы с резервными копиями — перемещение, удаление, проверка — осуществляются в заранее определенное сервисное окно, чтобы данные операции не пересекались с операциями резервного копирования.

Особое внимание в системе резервного копирования RuBackup уделено вопросам разграничения доступа к резервным копиям. Ключи для защитного преобразования резервных копий располагаются на клиенте и не могут быть скопированы при выполнении резервного копирования (исключаются принудительно из резервных копий). Чтобы восстановить резервную копию требуется ввести пароль, который задается при начале работы клиента с системой резервного копирования. В базе данных системы резервного копирования пароли клиентов не хранятся в чистом виде, но в виде хешей.

Управление системой резервного копирования может осуществляться как с помощью оконных средств администрирования, так и с использованием утилит командной строки.

Базовая конфигурация RuBackup, как клиента, так и сервера, содержится в конфигурационном файле `/opt/rubackup/etc/config.file`. Этот файл содержит информацию об основном и резервном серверах резервного копирования и режиме работы узла (основной сервер, резервный сервер, медиасервер или клиент) и т.п.

Глобальные настройки системы резервного копирования, а также информация о клиентах СРК, глобальном расписании, стратегиях, репозитории резервных копий и пр. хранятся в базе данных rubackup в СУБД PostgreSQL. Для изменения большинства параметров конфигурации СРК не требуется изменять какие-либо сложные конфигурационные файлы и останавливать функционирование СРК. Изменения производятся online с помощью штатных средств администрирования RuBackup.

Клиент RuBackup имеет модульную архитектуру. Клиент RuBackup отвечает за взаимодействие с сервером RuBackup с одной стороны, и с модулями резервного копирования и восстановления с другой стороны. Собственно процедуры резервного копирования и восстановления реализованы в модулях RuBackup. Модуль RuBackup — это утилита, которая отвечает за резервное копирование и восстановление ресурса определенного типа (например, блочных устройств или базы данных) и упаковку резервных копий.

API модуль RuBackup является открытым и может быть использован для разработки модулей третьими лицами. Модули подробно описаны в соответствующих документах.

Глава 3. Многопользовательская модель

В СРК RuBackup реализован многопользовательский режим работы, т. е. назначение типа пользователя и предоставление ему набора полномочий для выполнения определенных рабочих задач в соответствии с его ролью.

В СРК RuBackup предусмотрены следующие типы пользователей:

1. суперпользователь (владелец базы данных RuBackup);
2. супервайзер;
3. сопровождающий;
4. администратор;
5. аудитор.

Суперпользователь является привилегированным администратором, которому позволены любые действия в СРК. Суперпользователь создаётся при конфигурации основного сервера. Имя суперпользователя и пароль задаются также при конфигурации. Чтобы поменять пароль суперпользователя в конфигурационном файле сервера, используйте команду:

```
rb_init –passwd
```

```
root@rbs:~# rb_init --passwd
RuBackup initialization utility
Copyright 2018-2022: LLC "RUBACKUP"
Исключительные права принадлежат ООО "РУБЭКАП"
Author is Andrey Kuznetsov
Version: 2.0 Build: 48024de
password found in /opt/rubackup/etc/config.file

Please enter old password:
Enter new password:
Repeat password:
  Copy old config file to: /opt/rubackup/etc/config.file.old.2024-Jan-18H16-
05-32
Password was changed successfully
root@rbs:~#
```

Для смены пароля в служебной базе данных rubackup:

1. Подключитесь к базе данных, используя пользователя rubackup или postgres, с помощью команды:

```
sudo -u rubackup psql
```

или

```
sudo -u postgres psql
```

2. Выполните команду:

```
sql ALTER USER rubackup PASSWORD '<new-password>';
```

Суперпользователь создается при создании базы данных rubackup и является владельцем базы данных. Таким образом, в списке пользователей СРК пользователя Суперпользователя увидеть нельзя, также как и нельзя создать еще одного пользователя с таким же именем.

У суперпользователя есть следующие возможности:

- добавлять новых пользователей в систему. При этом выбранная группа пользователя влияет только на задачи уведомления. Чтобы пользователь мог получить административные привилегии в СРК, его нужно добавить в супервайзеры, сопровождающие или администраторы;
- менять пароль для других пользователей с помощью RBM.

Супервайзер может выполнять действия, доступные Суперпользователю, за исключением:

- любых действий с пользователями кроме назначения ролей Сопровождающего и Администратора;
- изменения глобальной конфигурации СРК.

Сопровождающий отвечает за медиасервер и может управлять устройствами хранения на этом медиасервере.

Администратор отвечает за группу клиентов и может выполнять их настройки и действия, связанные с клиентами, входящими в группу. Администратор в дереве объектов видит только своих клиентов, и имеет доступ к правилам глобального расписания, резервным копиям и задачам только своих клиентов.

Аудитор — роль, предназначенная для сотрудников информационной безопасности. Аудитору доступен просмотр всех настроек и информации в СРК (кроме настроек глобальной конфигурации) без возможности редактирования. Также аудитору доступны для просмотра все журналы, включая «Журнал событий ИБ».

Порядок назначения типов пользователя, их поиска и удаления можно найти в Пользователи.

Глава 4. Основные компоненты RuBackup

4.1. Клиент резервного копирования

Клиент резервного копирования RuBackup представляет собой фоновое приложение (сервис, демон), взаимодействующее с сервером RuBackup.

Расположение	`/opt/rubackup/bin/rubackup_client`
Запуск	`rubackup_client start`
Остановка	`rubackup_client stop`
Перезагрузка	`rubackup_client restart`
Текущий статус (результат 0 — клиент работает, 1 — не работает)	`rubackup_client status`
Получить HWID	`rubackup_client hwid`

4.1.1. Запуск клиента RuBackup

Для штатной эксплуатации рекомендуется запускать клиент RuBackup как сервис. Для этого выполните следующие действия:

1. Включите сервис клиента RuBackup:

```
sudo systemctl enable \
/opt/rubackup/etc/systemd/system/rubackup_client.service
```

2. Перезагрузите `systemctl`:

```
sudo systemctl daemon-reload
```

3. Запустите сервис `rubackup_client`:

```
sudo systemctl start rubackup_client
```

Уточнить статус клиента RuBackup можно при помощи команды:

```
sudo systemctl status rubackup_client
```

```
  rubackup_client.service - RuBackup client
```

```
Loaded: loaded (/etc/systemd/system/rubackup_client.service; enabled;
vendor preset: enabled)

Active: active (running) since Mon 2023-02-20 11:17:59 UTC; 6 days ago

Process: 1760 ExecStart=/opt/rubackup/bin/rubackup_client start
(code=exited, status=0/SUCCESS)

Main PID: 1763 (rubackup_client)

Tasks: 3 (limit: 4610)

Memory: 60.9M

CGroup: /system.slice/rubackup_client.service

  1763 /opt/rubackup/bin/rubackup_client start

фев 20 12:18:07 rb-primary rubackup_client[1763]: [2023-02-20 12:18:07]
Info: Removing obsolete snapshot file:
/rubackup-tmp/rb-
primary_TaskID_1_NORuleOrStrategy_0_D2023_2_20H12_14_16_BackupType_1_Resource
Type_>

фев 20 12:18:07 rb-primary rubackup_client[1763]: [2023-02-20 12:18:07]
Info: bool RbModuleUniversal::run_rbfd_command(const string&,
std::string&, pid_t&, std::string&):rbfd command: /opt/rubackup/bin/rbfd -a >

фев 20 12:18:07 rb-primary rubackup_client[1763]: RBFD PID: 62636

фев 20 12:18:07 rb-primary rubackup_client[1763]: Set status for task
ID: 3 from: Start_Transfer to: Transmission

фев 20 12:18:10 rb-primary rubackup_client[1763]: [193B blob data]

фев 20 12:18:10 rb-primary rubackup_client[1763]: [2023-02-20 12:18:10]
Info: The archive '1' has been unpacked successfully

фев 20 12:18:10 rb-primary rubackup_client[1763]: Final progress: 7832
100%

фев 20 12:18:10 rb-primary rubackup_client[1763]: Set status for task
ID: 3 from: Transmission to: Finish_Transfer
```

```
фев 20 12:18:10 rb-primary rubackup_client[1763]: Set status for task
ID: 3 from: Finish_Transfer to: Done

фев 20 12:18:10 rb-primary rubackup_client[1763]: Task w
```

4.2. Сервер резервного копирования

Сервер резервного копирования RuBackup представляет собой фоновое приложение (сервис, демон).

Расположение	`/opt/rubackup/bin/rubackup_server`
Запуск	`rubackup_server start`
Остановка	`rubackup_server stop`
Перезагрузка	`rubackup_server restart`
Текущий статус (результат 0 — сервер работает, 1 — не работает)	`rubackup_server status`
Получить HWID	`rubackup_server hwid`

4.2.1. Запуск сервера RuBackup

Для штатной эксплуатации рекомендуется запускать сервер RuBackup как сервис. Для этого выполните следующие действия:

1. Включите сервис клиента RuBackup:

```
sudo systemctl enable \
/opt/rubackup/etc/systemd/system/rubackup_client.service
```

2. Включите сервис сервера RuBackup:

```
sudo systemctl enable \
/opt/rubackup/etc/systemd/system/rubackup_server.service
```

3. Перезагрузите `systemctl`:

```
sudo systemctl daemon-reload
```

4. Запустите сервис `rubackup_client`:

```
sudo systemctl start rubackup_client
```

5. Запустите сервис `rubackup_server`:

```
sudo systemctl start rubackup_server
```

Уточнить статус сервера RuBackup можно при помощи команды:

```
sudo systemctl status rubackup_server
```

```
  rubackup_server.service - RuBackup server

Loaded: loaded (/etc/systemd/system/rubackup_server.service; enabled;
vendor preset: enabled)

Active: active (running) since Mon 2023-02-20 11:19:36 UTC; 6 days ago

Process: 1897 ExecStart=/opt/rubackup/bin/rubackup_server start
(code=exited, status=0/SUCCESS)

Main PID: 1912 (rubackup_server)

Tasks: 29 (limit: 4610)

Memory: 254.0M

CGroup: /system.slice/rubackup_server.service

  1912 /opt/rubackup/bin/rubackup_server start


фев 27 07:26:20 rb-primary rubackup_server[1912]: Warning: Pool: Cloud1
has no any file system

фев 27 07:26:21 rb-primary rubackup_server[1912]: Warning: Pool: Cloud1
has no any file system

фев 27 07:26:22 rb-primary rubackup_server[1912]: Warning: Pool: Cloud1
has no any file system

фев 27 07:26:23 rb-primary rubackup_server[1912]: Warning: Pool: Cloud1
has no any file system
```

```
фев 27 07:26:24 rb-primary rubackup_server[1912]: Warning: Pool: Cloud1
has no any file system

фев 27 07:26:25 rb-primary rubackup_server[1912]: Warning: Pool: Cloud1
has no any file system

фев 27 07:26:26 rb-primary rubackup_server[1912]: Warning: Pool: Cloud1
has no any file system

фев 27 07:26:27 rb-primary rubackup_server[1912]: Warning: Pool: Cloud1
has no any file system

фев 27 07:26:28 rb-primary rubackup_server[1912]: Warning: Pool: Cloud1
has no any file system

фев 27 07:26:29 rb-primary rubackup_server[1912]: Warning: Pool: Cloud1
has no any file system
```

Если у вас возникает проблема запуска сервиса RuBackup, и служебная база данных RuBackup в PostgreSQL установлена на отдельном сервере (например, при добавлении в конфигурацию резервного или медиасервера), выполните следующие действия:

1. Удалите зависимости `postgresql.service` в параметрах Requires и After в разделе Unit в юнит-файле:

   ```
   /opt/rubackup/etc/systemd/system/rubackup_server.service
   ```

2. Перезагрузите `systemctl`:

   ```
   sudo systemctl daemon-reload
   ```

Глава 5. Лицензирование

Для использования полного функционала системы резервного копирования и восстановления данных RuBackup требуется установить лицензионный файл для каждого развёрнутого серверного компонента — основного, резервного и медиасерверов.

Лицензированию подлежит каждый сервер СРК RuBackup. Лицензирование клиентов СРК RuBackup не требуется.

Лицензионный договор (EULA) на право использования программного продукта СРК RuBackup находится в папке `/opt/rubackup/copyrights/`, а также доступен для ознакомления на официальном сайте https://www.rubackup.ru/. Используя программный продукт пользователь принимает условия лицензионного договора.

5.1. Типы лицензий

Лицензия на СРК RuBackup может быть нескольких типов, в зависимости от ограничений для лицензиата. Способы лицензирования системы резервного копирования RuBackup приведены в Типы лицензий СРК RuBackup.

Все серверные компоненты системы резервного копирования RuBackup подлежат единому типу лицензирования.

Таблица 1. Типы лицензий СРК RuBackup

Параметр лицензирования Тип лицензии	Конфигурация	Объём резервируемых данных	Срок действия	Ограничение
backend	Без ограничений	Суммарный объём всех хранимых резервных копий в системе СРК*	Бессрочная или срочная	При исчерпании объёма лицензии невозможно выполнить резервное копирование, но восстановление данных доступно. Минимальная лицензия — 1 ТБ
frontend	Без ограничений	Суммарный объём полных уникальных резервных копий источников данных**	Бессрочная или срочная	Учитывается только наи-большая резервная копия клиента СРК RuBackup. Минимальная лицензия — 1 ТБ

Параметр лицензирования Тип лицензии	Конфигурация	Объём резервируемых данных	Срок действия	Ограничение
По конфигурации	Количество клиентов системы резервного копирования, количество сокетов сервера***	Максимальный объём хранимых резервных копий 250 ТБ*	Бессрочная или срочная	Минимальная конфигурация: 1 сервер и 10 клиентов. Для каждого клиента (не зависимо от конфигурации) доступно резервное копирование файловой системы и LVM-томов
backend тестовая	1 сервер	1 ТБ	1 год	Получение автоматическое при запуске основного сервера
Временная	По запросу	По запросу	По запросу	Предоставляется по запросу

- учитывается объём всех резервных копий после сжатия и дедупликации, объём хранимых метаданных;
  - учитывается объём резервных копий после сжатия, но до дедупликации, если она используется, также учитывается объём хранимых метаданных;
    - учитываются только используемые (заполненные) сокеты
- ёмкость — максимальный размер резервируемых данных (ТБ);
- использованная ёмкость — размер использованных резервированных данных (байт);
- дата начала лицензии — дата установки и запуска лицензируемого сервера в формате YYYY.MM.DD, с представлением времени в 24-часовой нотации hh:mm;
- дата окончания действия лицензии — дата аннулирования лицензии и прекращения доступа к функции резервного копирования данных (функция восстановления данных из ранее сделанных резервных копий доступна) в формате YYYY.MM.DD, с представлением времени в 24-часовой нотации hh:mm;
- заказчик, по запросу которого предоставлена лицензия;
- сокеты — количество лицензируемых разъёмов на материнской плате сервера;
- клиенты СРК RuBackup;
- HWID — идентификатор хоста, на котором развёрнут лицензируемый сервер.

5.2. Файл лицензии

- Файл лицензии имеет расширение .lic и должен находится в каталоге /opt/rubackup/etc/ с именем файла rubackup.lic.
- При запуске СРК RuBackup система программного лицензирования будет осуществлять поиск лицензии в каталоге /opt/rubackup/etc/.
- Проверка файла лицензии осуществляется каждый час после запуска сервера по следующим параметрам:
  - тип сервера СРК RuBackup: основной, резервный, медиа;
  - идентификатор хоста лицензируемого сервера hardware id;
  - в зависимости от типа лицензии:
  - суммарный объём резервируемых данных;
  - суммарный объём созданных полных резервных копий;
  - срок действия;
  - количество одномоментно подключенных клиентов резервного копирования.

5.3. Получение сведений о лицензии

Сведения об установленной лицензии доступны для просмотра в журнале событий на хосте лицензированного сервера и в Менеджере администратора RuBackup.

5.4. Просмотр сведений о лицензии в журнале событий

Для просмотра сведений о лицензии в журнале событий `RuBackup.log`:

1. Добавьте сведения об установленной лицензии на хосте лицензированного сервера СРК RuBackup (после его запуска) в журнал событий, выполнив команду в терминале:

   ```
   rubackup_server license
   ```

   Команда добавляет в журнал событий `/opt/rubackup/log/RuBackup.log` данные об установленной на сервере лицензии.

2. Для просмотра сведений о лицензии в журнале событий, например, выполните, команду в терминале:

```
sudo tail -f /opt/rubackup/log/RuBackup.log
```

В терминале будет выведена следующая информация о лицензии:

- имя хоста, на котором развёрнут сервер, и его описание;
- роль сервера (основной, резервный, медиа);
- идентификатор хоста лицензированного сервера hwid;
- дату начала действия лицензии;
- дату окончания действия лицензии;
- тип лицензии;
- максимальный размер резервируемых данных;
- размер использованных резервируемых данных.

5.5. Просмотр сведений о лицензии в Менеджере администратора RuBackup

Для просмота сведений об установленных на серверах СРК RuBakup лицензиях:

1. Запустите Менеджер администратора RuBackup (RBM).
2. Выполните авторизацию пользователя.
3. В верхней панели RBM нажмите кнопку Настройка и в выпадающем меню выберите пункт «Лицензия».
4. В открывшемся окне «Лицензии» приведены сведения об установленных текущих лицензиях серверной части СРК RuBackup, данные будут выведены в соответствии с типом лицензии:

   - имя хоста, на котором развёрнут лицензируемый сервер;
   - описание хоста, на котором развёрнут лицензируемый сервер;
   - тип узла — тип лицензируемого сервера (основной, резервный или медиа-сервер);
   - тип лицензии — возможные значения: backend, frontend, configuration (см. таблицу 6);
   - ёмкость — максимальный размер резервируемых данных (ТБ);
   - использованная ёмкость — размер использованных резервированных данных (байт);
   - дата начала лицензии — дата установки и запуска лицензируемого серверва в формате YYYY.MM.DD, с представлением времени в 24-часовой нотации hh:mm;

- дата окончания действия лицензии — дата аннулирования лицензии и прекращения доступа к функии резервного копирования данных (функция восстановления данных из ранее сделанных резервных копий доступна) в формате YYYY.MM.DD, с представлением времени в 24-часовой нотации hh:mm;
- заказчик, по запросу которого предоставлена лицензия;
- сокеты — количество лицензируемых разъёмов на материнской плате сервера;
- клиенты СРК RuBackup;
- HWID — идентификатор хоста, на котором развёрнут лицензируемый сервер.

5. Для лицензии типа «по конфигурации» возможен просмотр установленных расширений: по двойному нажатию ЛКМ на лицензию или выделив лицензию и нажав появившуюся кнопку. В окне «Расширения лицензии» будут выведены все расширения, определяющие, какие именно источники данных можно использовать для создания резервных копий, поддерживаемые соответствующими модулями СРК RuBackup.

5.6. Генерирование hardware id

Идентификатор хоста лицензируемого сервера hardware id генерируется на основании данных, приведённых в Условия формирования идентификатора hardware id.

Таблица 2. Условия формирования идентификатора hardware id

<table>
<tr><th>Версия RuBackup</th><th>ОС</th><th>Данные для формирования hardware id</th><th>Параметр config.file</th><th>Значение по умолчанию</th></tr>
<tr><td rowspan="2">Установка версии 2.1 и более поздняя</td><td>Linux</td><td>данные псевдо-файла sys/class/dmi/id/product_uuid, содержащего идентификатор UUID материнской платы, установленный производителем платы, и закодированной информации в DMI BIOS</td><td rowspan="2">use_product_uuid</td><td rowspan="2">true</td></tr>
<tr><td>Windows</td><td>имя хоста hostname</td></tr>
<tr><td>Установлена версия ранее 2.1</td><td rowspan="2">Linux</td><td rowspan="2">идентификатор /etc/machine-id и имя хоста /etc/hostname</td><td>нет</td><td>нет</td></tr>
<tr><td>Обновление установленной версии ранее 2.1</td><td>use_product_uuid</td><td>false</td></tr>
</table>

5.7. Уведомление о наступлении ограничения лицензии

Чтобы обеспечить бесперебойную работу СРК RuBackup, действие лицензий рекомендуется продлевать до истечения параметров лицензирования.

В случае срочной лицензии система уведомляет клиента об окончании срока действия лицензии не позднее, чем за 45 дней при запуске сервера — в терминале будет выведено предупреждение об истечении срока действия лицензии.

Также актуальность лицензии всегда можно проверить в консоли Менеджера администратора RuBackup или вывести сведения о текущей лицензии в терминал.

Дополнительная информация:

Установка лицензии

Обновление лицензии