RuBackup
Система резервного копирования и восстановления данных

Резервное копирование и восстановление BTRFS

RuBackup

Версия 1.9

2022 г.

Содержание

Введение

Система резервного копирования RuBackup позволяет выполнять клиентам полное и инкрементальное резервное копирование файловых систем и подразделов (subvolumes) BTRFS. Резервное копирование выполняется только для примонтированных файловых систем и их подразделов.

Полное резервное копирование – это создание резервной копии всех данных из исходного набора, независимо от того, изменялись данные или нет с момента выполнения последней полной резервной копии.

Дифференциальное резервное копирование сохраняет только данные, изменённые со времени выполнения предыдущего полного резервного копирования.

Инкрементальное резервное копирование сохраняет только данные, изменённые со времени выполнения предыдущей инкрементальной резервной копии, а если такой нет, то 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 клиент может выполнить срочное резервное копирование файловых систем или подразделов BTRFS, но в этом случае будет выполнено полное резервное копирование выбранного ресурса.

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

Полное резервное копирование может быть выполнено с применением сжатия на стороне клиента или на стороне сервера RuBackup. Также возможно провести защитное преобразование резервной копии выбранным алгоритмом (см. раздел «Защитное преобразование резервных копий»).

Перед выполнением резервного копирования файловой системы или подраздела BTRFS создаётся снимок состояния (снэпшот), непосредственно для которого выполняется резервная копия. Перед выполнением снимка и сразу после этого возможно выполнение скрипта, который может обеспечить целостность данных на файловой системе BTRFS. По окончании резервного копирования снимок удаляется.

Если требуется резервное копирование отдельного каталога, который располагается в большой файловой системе BTRFS, рекомендуется выделить его как подраздел BTRFS и выполнить резервное копирование этого подраздела.

Внимание! Если в файловой системе BTRFS присутствуют подразделы, то их содержимое не будет в включено в резервную копию собственно файловой системы. Для каждого подраздела необходимо создать отдельное правило резервного копирования.

Краткая информация о BTRFS

Установка btrfs (может отличаться для разных ОС):

```
$ sudo apt install btrfs-tools
```

Показать список всех монтированных файловых систем:

```
$ sudo btrfs filesystem show -m
```

Создать файловую систему на существующем блочном устройстве:

```
$ sudo mkfs.btrfs /dev/vdb
```

Примонтировать файловую систему:

```
$ sudo mount /dev/vdb /btrfs
```

Создать подраздел:

```
$ sudo btrfs subvolume create /btrfs/sv1
```

Показать список всех подразделов монтированной файловой системы `/btrfs`:

```
$ sudo btrfs subvolume list -qtu /btrfs
```

Показать только снимки:

```
$ sudo btrfs subvolume list -qtus /btrfs
```

Создать снимок:

```
$ sudo btrfs subvolume snapshot -r /btrfs/sv1 /btrfs/sv1.snapshot
```

Удалить снимок:

```
$ sudo btrfs subvolume delete /btrfs/sv1.snapshot
```

Установка клиента RuBackup

Для возможности резервного копирования и восстановления данных BTRFS при помощи RuBackup на сервер должен быть установлен клиент RuBackup со всеми необходимыми модулями. Подробно процедура установки клиента описана в «Руководстве по установке серверов резервного копирования и Linux клиентов RuBackup».

Клиент RuBackup представляет собой фоновое системное приложение (демон или сервис), обеспечивающее взаимодействие с серверной группировкой RuBackup. Для выполнения резервного копирования клиент RuBackup должен работать от имени суперпользователя (root для Linux и Unix).

Подготовка хоста BTRFS для выполнения резервного копирования средствами RuBackup

Для резервного копирования при помощи RuBackup на сервер должен быть установлен клиент RuBackup и модуль резервного копирования **rb_module_btrfs**.

Установка модуля производится при помощи следующей команды:

```
$ sudo dpkg -i rubackup-btrfs.deb
Выбор ранее не выбранного пакета rubackup-btrfs.
(Чтение базы данных … на данный момент установлено 115108 файлов и
каталогов.)
Подготовка к распаковке rubackup-btrfs.deb …
Распаковывается rubackup-btrfs (2020-12-03) …
Настраивается пакет rubackup-btrfs (2020-12-03) …
```

Имя пакета может отличаться в зависимости от используемой операционной системы.

Подробно процедуру установки клиента см. «Руководство по установке серверов резервного копирования и Linux клиентов RuBackup».

Удаление клиента RuBackup

Удаление клиента RuBackup возможно из учётной записи с административными правами.

Для удаления сервиса `rubackup-client` используйте команды:

```
$ sudo systemctl disable rubackup-client
$ sudo systemctl daemon-reload
```

Для удаления клиента RuBackup и модуля **rb_module_btrfs** используйте команды:

```
$ sudo apt remove rubackup-btrfs
$ sudo apt remove rubackup-client
```

При необходимости удалить клиент RuBackup из конфигурации системы резервного копирования, это может сделать системный администратор RuBackup с помощью оконного Менеджера Администратора (RBM).

Мастер-ключ

В ходе установки клиента RuBackup будет создан мастер-ключ для защитного преобразования резервных копий, а также ключи для электронной подписи, если предполагается использовать электронную подпись.

Внимание! При утере ключа вы не сможете восстановить данные из резервной копии, если она была преобразована с помощью защитных алгоритмов.

Важно! Ключи рекомендуется после создания скопировать на внешний носитель, а также распечатать бумажную копию и убрать эти копии в надёжное место.

Мастер-ключ рекомендуется распечатать при помощи утилиты `hexdump`, так как он может содержать неотображаемые на экране символы:

```
$ hexdump /opt/rubackup/keys/master-key
0000000 79d1 4749 7335 e387 9f74 c67e 55a7 20ff
0000010 6284 54as 83a3 2053 4818 e183 1528 a343
0000020
```

Защитное преобразование резервных копий

При необходимости, сразу после выполнения резервного копирования архивы могут быть преобразованы на хосте клиента. Таким образом, важные данные будут недоступны для администратора RuBackup или других лиц, которые могли бы получить доступ к резервной копии (например, на внешнем хранилище картриджей ленточной библиотеки или на площадке провайдера облачного хранилища для ваших резервных копий).

Защитное преобразование осуществляется входящей в состав RuBackup утилитой `rbcrypt`. Ключ для защитного преобразования резервных копий располагается на хосте клиента в файле `/opt/rubackup/keys/master-key`. Защитное преобразование данных при помощи `rbcrypt` возможно с длиной ключа 256 бит (по умолчанию), а также 128, 512 или 1024 бита в зависимости от выбранного алгоритма преобразования.

Если для правила глобального расписания необходимо выбрать особый режим защитного преобразования с длиной ключа, отличной от 256 бит, и с ключом, расположенным в другом месте, то вы можете сделать это при помощи скрипта, выполняющегося после выполнения резервного копирования (определяется в правиле глобального расписания администратором RuBackup). При этом необходимо, чтобы имя преобразованного файла осталось таким же, как и ранее, иначе задача завершится с ошибкой. Провести обратное преобразование такого файла после восстановления его из архива следует вручную при помощи утилиты `rbcrypt`. При таком режиме работы нет необходимости указывать алгоритм преобразования в правиле резервного копирования, иначе архив будет повторно преобразован с использованием мастер-ключа.

Для выполнения защитного преобразования доступны алгоритмы, представленные в таблице 1.

`Таблица 1 – Алгоритмы защитного преобразования, доступные в утилите rbcrypt.`

Алгоритм	Длина ключа, бит	Примечание
Anubis	128, 256	
Aria	128, 256	

Алгоритм	Длина ключа, бит	Примечание
CAST6	128, 256	
Camellia	128, 256	
Kalyna	128, 256, 512	Украинский национальный стандарт ДСТУ 7624:2014
Kuznyechik	256	Российский национальный стандарт ГОСТ Р 34.12-2015
MARS	128, 256	
Rijndael	128, 256	Advanced Encryption Standard (AES)
Serpent	128, 256	
Simon	128	
SM4	128	Китайский национальный стандарт для беспроводных сетей
Speck	128, 256	
Threefish	256, 512, 1024	
Twofish	128, 256	

Менеджер администратора RuBackup

(RBM)

Оконное приложение «Менеджер администратора RuBackup» (RBM) предназначено для общего администрирования серверной группировки RuBackup, управления клиентами резервного копирования, глобальным расписанием резервного копирования, хранилищами резервных копий и пр.

RBM может быть запущено администратором на основном сервере резервного копирования RuBackup.

Для запуска RBM следует выполнить команду:

```
# ssh -X user@rubackup_server
# /opt/rubackup/bin/rbm&
```

Пользователь, запускающий RBM, должен входить в группу `rubackup`.

На вкладке **Объекты** в левой части представлен список клиентов системы резервного копирования, в котором указано имя, уникальный HWID и описание. Клиенты, которые в данный момент находятся в online, будут отмечены зеленым цветом. Клиенты в состоянии offline – красным (рисунок 1).

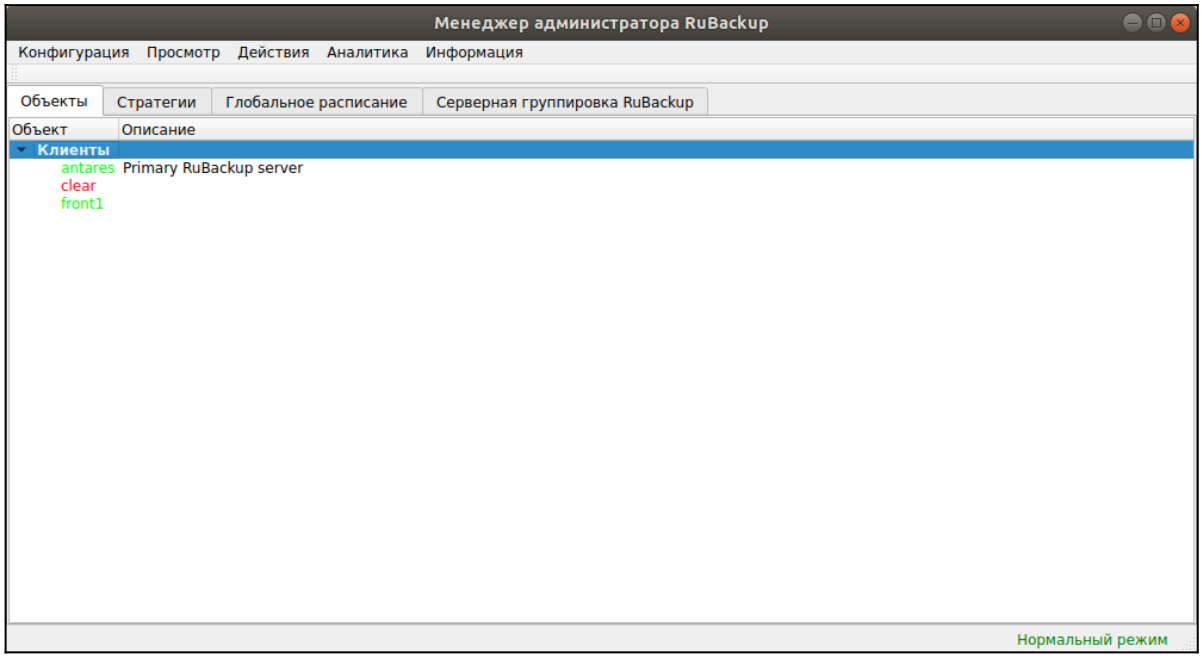


Рисунок 1

Для резервного копирования данных BTRFS на хосте должен быть установлен клиент RuBackup и соответствующий модуль, обеспечивающий резервное копирование. Клиент должен быть авторизован администратором RuBackup (см. раздел «Клиенты» менеджера администратора RuBackup).

Если клиент RuBackup установлен, но не авторизован, в нижней части окна RBM появится сообщение о том, что найдены неавторизованные клиенты. Все новые клиенты должны быть авторизованы в системе резервного копирования RuBackup.

Для авторизации неавторизованного клиента в RBM выполните следующие действия:

1. Откройте меню **Действия → Клиенты → Авторизовать клиентов** (рисунок 2).

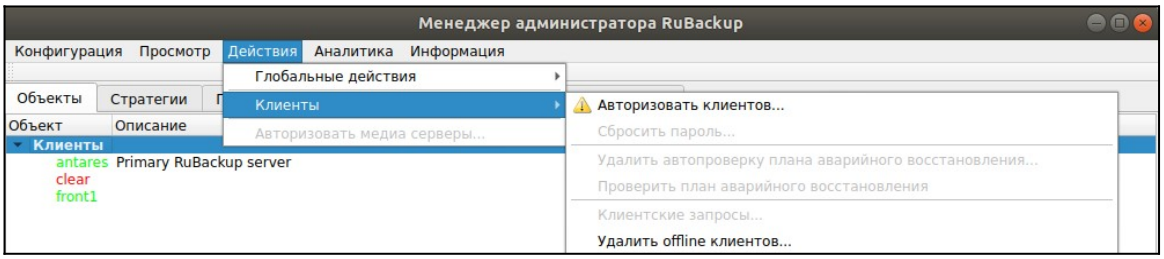


Рисунок 2

2. Выберите нужного неавторизованного клиента и нажмите **Авторизовать** (рисунок 3).

Рисунок 3

После авторизации новый клиент будет виден в главном окне RBM (рисунок 4):

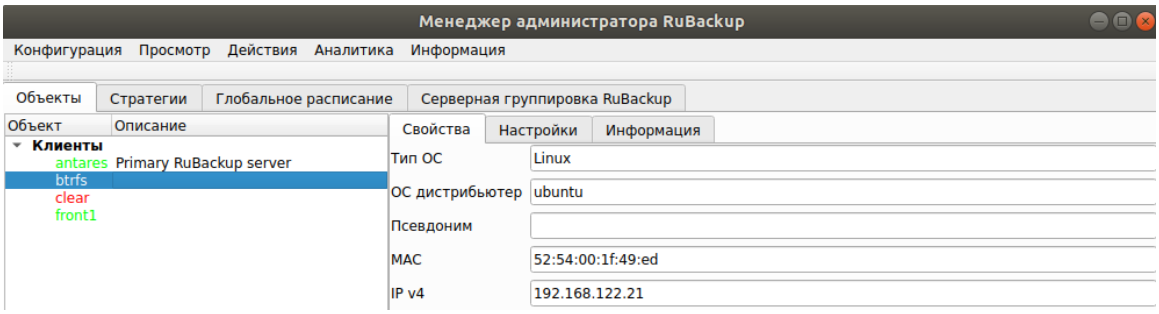


Рисунок 4

Чтобы выполнять регулярное резервное копирование файловых систем или подразделов BTRFS, необходимо создать правило в глобальном расписании.

Для этого необходимо выполнить следующие действия:

1. Выберите хост клиента, на котором находится BTRFS, и добавьте правило резервного копирования (рисунок 5).

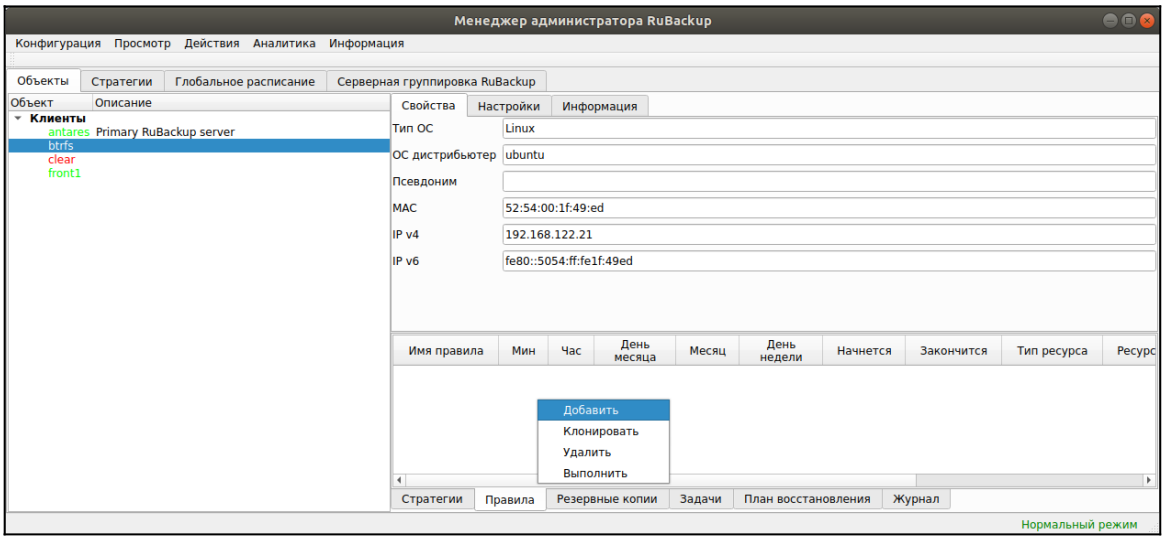


Рисунок 5

2. Выбрать тип ресурса «**Btrfs (B-tree FS)**» (рисунок 6):

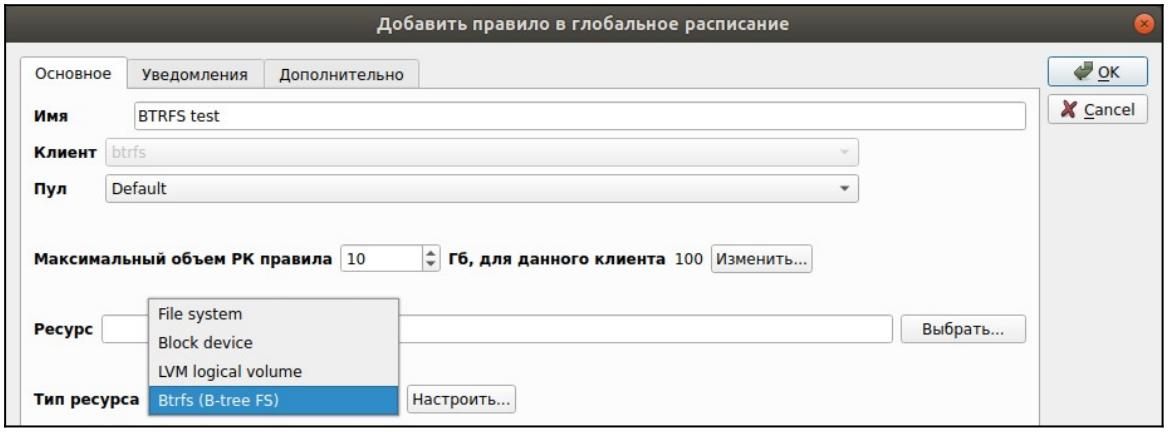


Рисунок 6

3. Нажать кнопку «**Выбрать...**» и выбрать ресурс, для которого будет выполняться правило (рисунок 7):

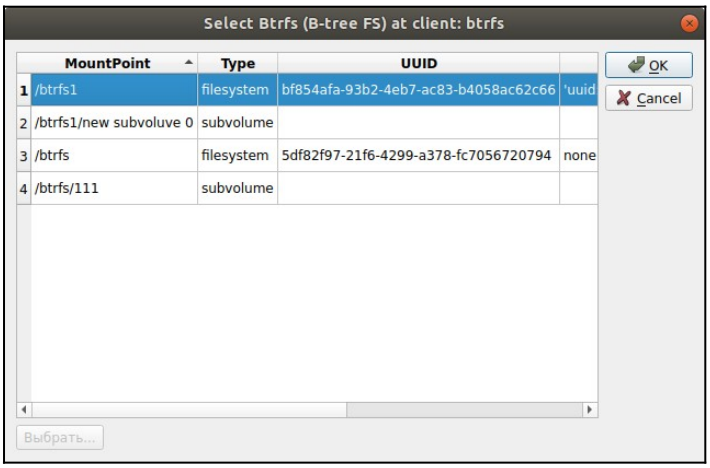


Рисунок 7

4. Установите настройки правила: название правила, пул хранения данных, максимальный объём для резервных копий правила (в ГБ), тип резервного копирования, расписание резервного копирования, срок хранения и необязательный временной промежуток проверки резервной копии (рисунок 8).

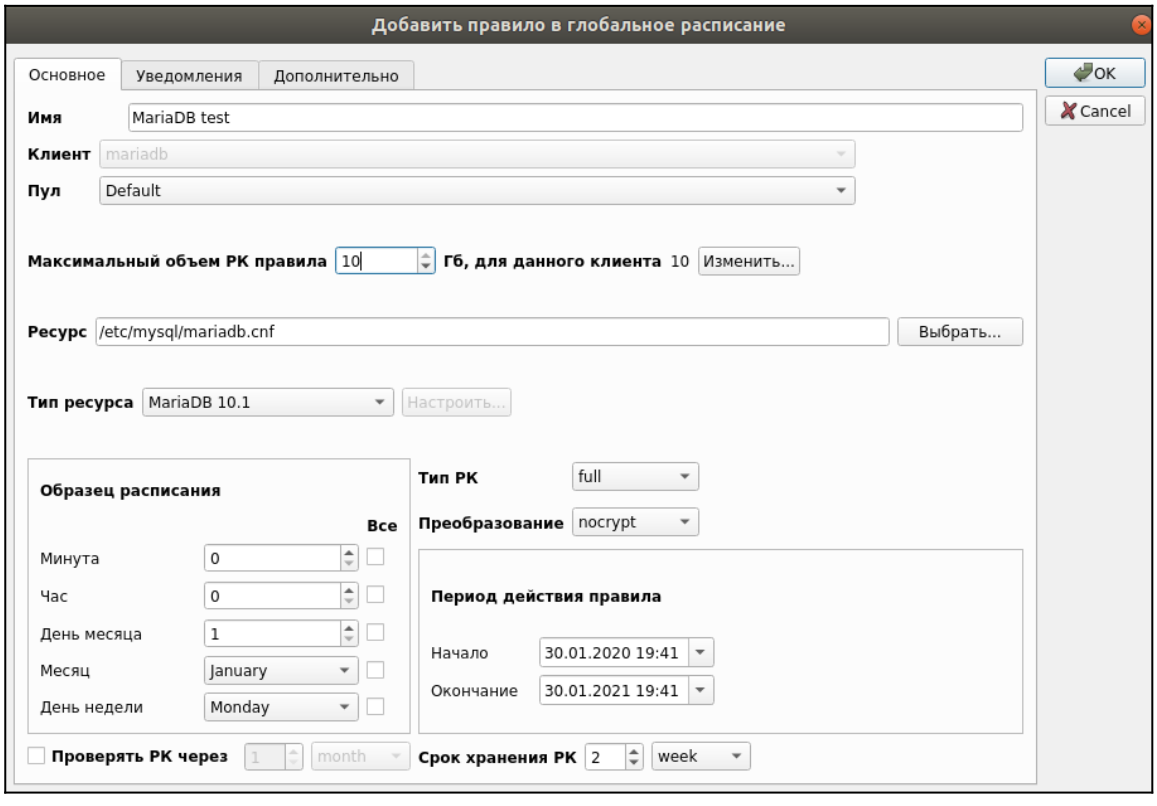


Рисунок 8

5. На вкладке «Дополнительно» можно установить разрешение для клиента удалять резервные копии, установить автоматическое удаление устаревших резервных копий или определить условие их перемещения в другой пул (рисунок 9).

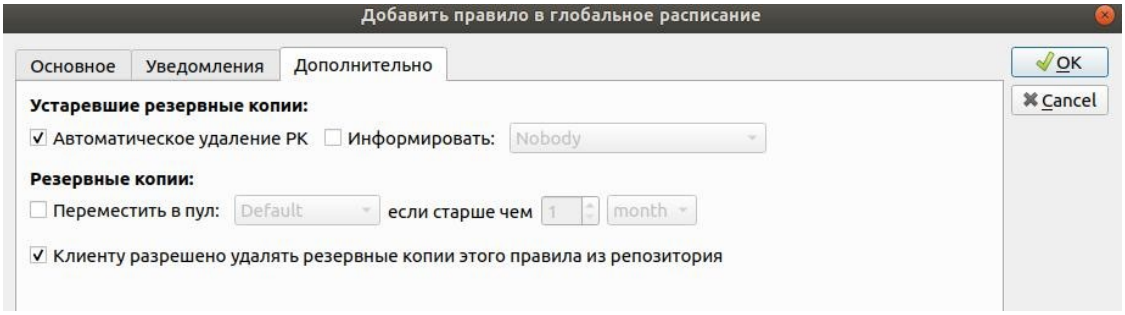


Рисунок 9

Внимание! Если в файловой системе BTRFS присутствуют подразделы, то их содержимое не будет в включено в резервную копию собственно файловой системы. Для каждого подраздела необходимо создать отдельное правило резервного копирования. Если вы не создадите отдельные правила для защиты подразделов, то может оказаться, что в резервных копиях файловой системы нет тех данных, которые были расположены на подразделах, и в ходе восстановления для подразделов будут восстановлены пустые каталоги.

Вновь созданное правило будет обладать статусом «wait», это означает что оно не будет порождать задач на выполнение резервного копирования до той поры, пока администратор RuBackup не запустит его и оно изменит свой статус на «run». При необходимости работу правила можно будет приостановить или запустить в любой момент времени по желанию администратора. Так же администратор может инициировать немедленное создание задачи при статусе правила «wait».

Правило глобального расписания имеет срок жизни, определяемый при его создании, а так же предусматривает следующие возможности:

1) Выполнить скрипт на клиенте перед началом резервного копирования.

2) Выполнить скрипт на клиенте после успешного окончания резервного копирования.

3) Выполнить скрипт на клиенте после неудачного завершения резервного копирования.

4) Выполнить преобразование резервной копии на клиенте.

5) Выполнить сжатие резервной копии на клиенте или на сервере после передачи ему резервной копии.

6) Периодически выполнять проверку целостности резервной копии.

7) Хранить резервные копии определённый срок, а после его окончания удалять их из хранилища резервных копий и из записей репозитория, либо

просто уведомлять пользователей системы резервного копирования об окончании срока хранения.

8) Через определённый срок после создания резервной копии автоматически переместить её на другой пул хранения резервных копий, например на картридж ленточной библиотеки.

9) Уведомлять пользователей системы резервного копирования о результатах выполнения тех или иных операций, связанных с правилом глобального расписания.

10) В дополнительных настройках ресурса Btrfs в правиле резервного копирования возможно задать (рисунок 10):

– скрипт, который необходимо выполнить перед созданием снимка состояния (снэпшота);

– скрипт, который необходимо выполнить сразу после создания снимка состояния (снэпшота).

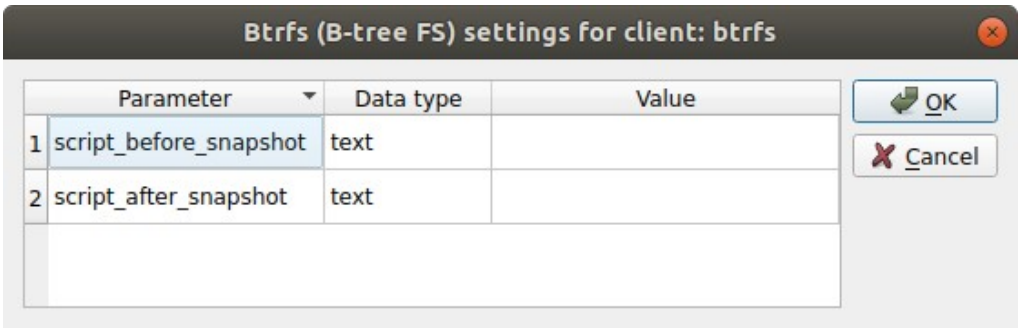


Рисунок 10

Вызов скриптов может быть необходим для того, чтобы сообщить приложению, использующему файловую систему, чтобы оно привело данные к консистентному состоянию.

При создании задачи RuBackup она появляется в главной очереди задач. Отслеживать исполнение правил может как администратор, с помощью RBM, так клиент при помощи RBC.

После успешного завершения резервного копирования резервная копия будет размещена в хранилище резервных копий, а информация о ней будет размещена в репозитории RuBackup.

Менеджер клиента RuBackup

Принцип взаимодействия клиентского менеджера с системой резервного копирования состоит в том, что пользователь может сформировать ту или иную команду (желаемое действие) и отправить его серверу резервного копирования RuBackup. Взаимодействие пользователя с сервером резервного копирования производится через клиента (фоновый процесс) резервного копирования. Клиентский менеджер отправляет команду пользователя клиенту, клиент отправляет её серверу. В том случае, если действие допустимо, то сервер RuBackup отдаст обратную команду клиенту и/или перенаправит её медиасерверу RuBackup для дальнейшей обработки. Это означает, что клиентский менеджер обычно не ожидает завершения того или иного действия, но ожидает ответа от клиента, что задание принято. Это позволяет инициировать параллельные запросы клиента к серверу резервного копирования, но требует от пользователя самостоятельно контролировать чтобы не было «встречных» операций, когда происходит восстановление данных, и в этот же момент эти же данные требуются для создания новой резервной копии. После того, как вы отдали ту или иную команду при помощи клиентского менеджера, вы можете просто закрыть приложение, все действия будут выполнены системой резервного копирования (однако стоит дождаться сообщения что задание принято к исполнению и проконтролировать это во вкладке «Задачи»).

Графический интерфейс клиентского менеджера поддерживает русский и английский языки.

Для запуска RBC следует выполнить команду:

```
# ssh -X user@btrfs_host
# /opt/rubackup/bin/rbc&
```

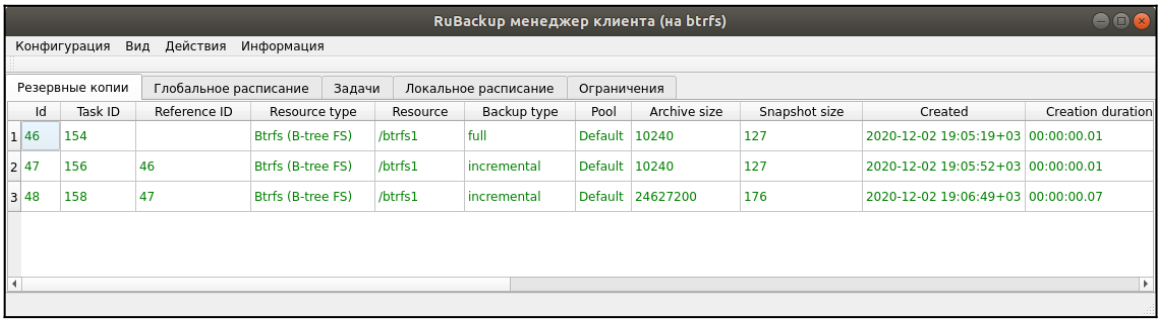
Пользователь, запускающий RBC, должен входить в группу `rubackup`.

При первом запуске клиентского менеджера необходимо задать пароль, при помощи которого впоследствии можно будет запросить восстановление резервной копии. Без ввода пароля получить резервную копию для клиента из хранилища невозможно. Хэш пароля восстановления хранится в базе данных RuBackup сервера. При необходимости можно изменить пароль при помощи клиентского менеджера (меню «**Конфигурация**» → «**Изменить пароль**»).

На главной странице клиентского менеджера расположены переключающиеся вкладки, позволяющие управлять резервными копиями, расписанием резервного копирования и просматривать текущие задачи клиента.

Вкладка «Резервные копии»

В таблице вкладки «Резервные копии» содержится информация обо всех резервных копиях клиента, которые хранятся в репозитории RuBackup (рисунок 11). Дифференциальные резервные копии ссылаются на полные резервные копии, инкрементальные резервные копии ссылаются на полные резервные копии или предыдущие инкрементальные, так что при необходимости восстановить данные можно одной командой инициировать восстановление всей цепочки резервных копий.



	Id	Task ID	Reference ID	Resource type	Resource	Backup type	Pool	Archive size	Snapshot size	Created	Creation duration
1	46	154		Btrfs (B-tree FS)	/btrfs1	full	Default	10240	127	2020-12-02 19:05:19+03	00:00:00.01
2	47	156	46	Btrfs (B-tree FS)	/btrfs1	incremental	Default	10240	127	2020-12-02 19:05:52+03	00:00:00.01
3	48	158	47	Btrfs (B-tree FS)	/btrfs1	incremental	Default	24627200	176	2020-12-02 19:06:49+03	00:00:00.07

Рисунок 11

Во вкладке «Резервные копии» пользователю доступны следующие действия:

Удалить выбранную резервную копию.

Это действие возможно в том случае, если в правиле глобального расписания есть соответствующее разрешение. Кроме того, при необходимости выполнить удаление резервной копии потребуется вести пароль клиента.

Восстановить цепочку резервных копий.

Это действие запускает процесс восстановления цепочки резервных копий на системе клиента.

Клиентский менеджер не ожидает окончания восстановления всех резервных копий, пользователь должен проконтролировать во вкладке «Задачи» что все созданные задачи на восстановление данных завершились успешно (статус задач «Done»). Для успешного выполнения этого действия требуется наличие достаточного свободного места в каталоге, предназначенном для создания и временного хранения резервных копий (см.опцию use-local-backup-directory).

Проверить резервную копию.

Это действие инициирует создание задачи проверки резервной копии. В том случае, если резервная копия была подписана цифровой подписью, то будет проверены размер файлов резервной копии, md5 сумма и проверена сама резервная копия. Если резервная копия не была подписана цифровой подписью, то будут проверены размер файлов резервной копии и md5 сумма.

Вкладка «Глобальное расписание»

В таблице вкладки «Глобальное расписание» содержится информация обо всех правилах в глобальном расписании RuBackup для этого клиента. (рисунок 12).

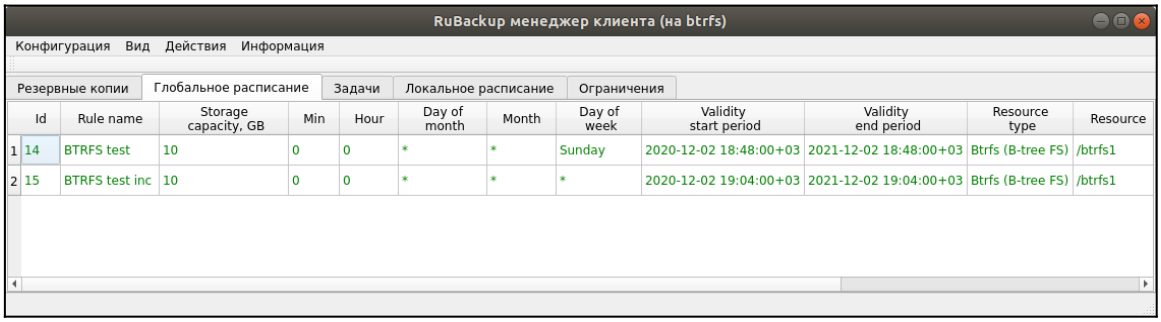


Рисунок 12

Во вкладке «Глобальное расписание» пользователю доступны следующие действия:

Запросить новое правило.

Это действие вызывает диалог подготовки нового правила в глобальном расписании RuBackup для данного клиента. Запрос на добавление правила требует одобрения администратора RuBackup, одобрение может быть сделано в оконном менеджере администратора RuBackup.

Запросить удалить правило из глобального расписания.

Это действие формирует запрос к администратору RuBackup об удалении выбранного пользователем правила из глобального расписания RuBackup. Запрос на удаление правила требует одобрения администратора RuBackup, одобрение может быть сделано в оконном менеджере администратора RuBackup.

Вкладка «Задачи»

В таблице вкладки «Задачи» содержится информация обо всех задачах в главной очереди заданий RuBackup для этого клиента (рисунок 13).

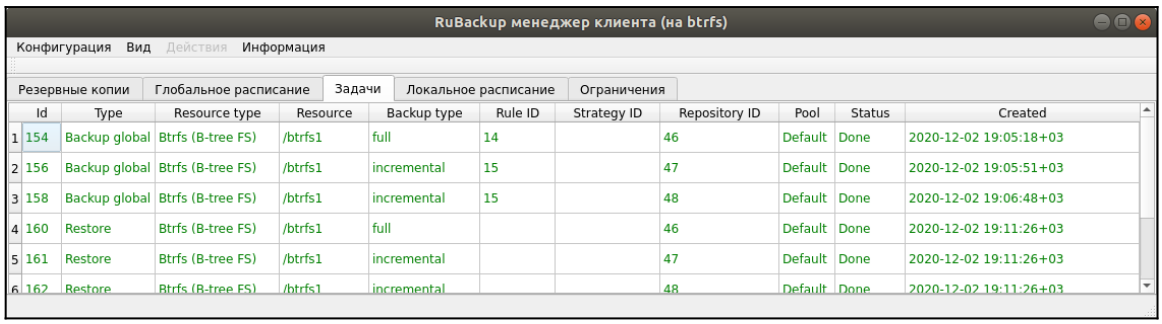


Рисунок 13

В зависимости от настроек резервного сервера RuBackup выполненные задачи и задачи, завершившиеся неудачно, через какое-то время могут быть

автоматически удалены из главной очереди задач. Информация о выполнении заданий фиксируется в специальном журнале задач сервера RuBackup, при необходимости статус любой задачи, даже удалённой из очереди, можно уточнить у администратора RuBackup. Так же информация о выполнении задач клиента заносится в локальный журнальный файл на клиенте. В клиентском менеджере можно открыть окно отслеживания журнального файла (меню «**Информация**» → «**Журнальный файл**»).

Вкладка «Локальное расписание»

Во вкладке «Локальное расписание» можно определить правила, задаваемые клиентом для тех или иных локальных ресурсов. Для работы локального расписания эта возможность должна быть включена администратором RuBackup для клиента.

Вкладка «Ограничения»

Во вкладке «Ограничения» могут быть определены локальные ресурсы, резервное копирование которых нежелательно. Для работы локальных ограничений эта возможность должна быть включена администратором RuBackup для клиента.

Утилиты командной строки клиента

RuBackup

Для управления RuBackup со стороны клиента, помимо клиентского оконного менеджера, можно воспользоваться утилитами командной строки:

rb_archive

Утилита предназначена для просмотра списка резервных копий клиента в системе резервного копирования, создания срочных резервных копий, их удаления, проверки и восстановления.

```
# rb_archives
Id | Ref ID | Resource                | Resource type     | Backup
type | Created             | Crypto  | Signed | Status
---+--------+-------------------------+------------------
+------------+--------------------+---------+--------+--------
46 |        | /btrfs1                 | Brtfs (B-tree FS) | full
| 2020-12-01 12:02:00 | nocrypt | True   | Trusted
47 | 46     | /btrfs1                 | Brtfs (B-tree FS) |
incremental | 2020-12-01 15:02:08 | nocrypt | True   | Trusted
48 | 47     | /btrfs1                 | Brtfs (B-tree FS) |
incremental | 2020-12-02 10:00:11 | nocrypt | True   | Trusted
49 |        | /btrfs1                 | Brtfs (B-tree FS) | full
| 2020-12-02 11:02:14 | nocrypt | True   | Trusted
50 |        | /btrfs1/new subvolume 0 | Brtfs (B-tree FS) | full
| 2020-12-02 11:02:14 | nocrypt | True   | Trusted
```

rb_schedule

Утилита предназначена для просмотра имеющихся правил клиента в глобальном расписании резервного копирования.

```
# rb_schedule
Id | Name            | Resource type     | Resource
| Backup type | Status
---+-----------------+------------------
+-------------------------+-------------+-------
14 | BTRFS test      | Brtfs (B-tree FS) | /btrfs1
| full        | run
15 | BTRFS test inc  | Brtfs (B-tree FS) | /btrfs1
| incremental | run
16 | BTRFS subvolume | Brtfs (B-tree FS) | /btrfs1/new subvolume 0
| full        | wait
```

rb_tasks

Утилита предназначена для просмотра задач клиента, которые присутствуют в главной очереди задач системы резервного копирования.

```
# rb_tasks
Id  | Task type     | Resource      | Backup type | Status |
Created
----+--------------+--------------+-------------+--------
+----------------------
154 | Backup global | /btrfs1       | full        | Done   | 2020-
12-02 12:01:16+03
156 | Backup global | /btrfs1       | incremental | Done   | 2020-
12-02 13:01:53+03
158 | Backup global | /btrfs1       | incremental | Done   | 2020-
12-02 14:05:26+03
160 | Restore       | /btrfs1       | full        | Done   | 2020-
12-02 15:06:45+03
161 | Restore       | /btrfs1       | incremental | Done   | 2020-
12-02 15:06:45+03
162 | Restore       | /btrfs1       | incremental | Done   | 2020-
12-02 15:06:45+03
```

Ознакомиться с функциями утилит командной строки можно при помощи команды man или в руководстве «Утилиты командной строки RuBackup».

Восстановление резервной копии

Вы можете восстановить резервную копию в любую файловую систему, не обязательно BTRFS. При необходимости, после восстановления файлы и каталоги могут быть перемещены в требуемое место.

Рекомендуется производить восстановление во временный каталог, чтобы случайно не утратить имеющиеся файлы, и поместить их в требуемое место после проверки.

Внимание! Если в файловой системе BTRFS присутствуют подразделы, то их содержимое не будет в включено в резервную копию собственно файловой системы. Для каждого подраздела необходимо создать отдельное правило резервного копирования. Если вы не создадите отдельные правила для защиты подразделов, то может оказаться, что в резервных копиях файловой системы нет тех данных, которые были расположены на подразделах, и в ходе восстановления для подразделов будут восстановлены пустые каталоги.

Клиент может осуществить восстановление данных резервной копии в оконном Менеджере Клиента RuBackup (RBC), либо при помощи утилиты командной строки `rb_archives`.

Восстановление резервной копии в RBC

Для восстановления данных резервной копии в оконном Менеджере Клиента RuBackup (RBC) выполните следующие действия.

1. Выделите нужную резервную копию и в контекстном меню выберите **Восстановить** (рисунок 14):

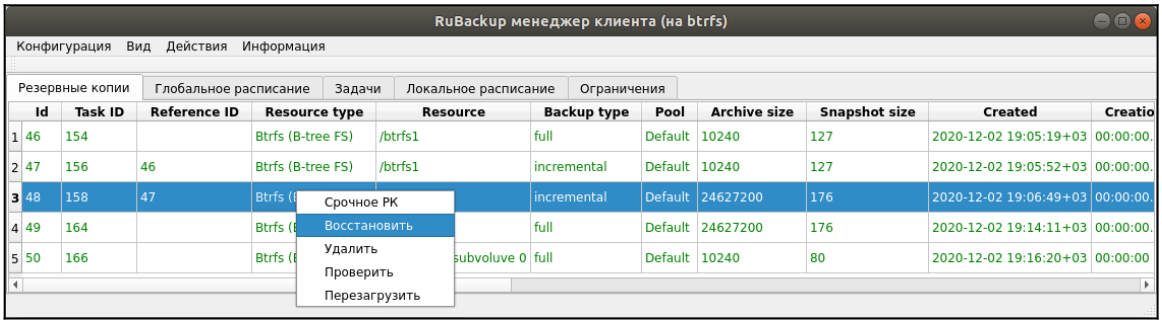


Рисунок 14

2. Для восстановления потребуется ввести пароль клиента. Затем RBC выведет информационное сообщение о дальнейших действиях (рисунок 15):

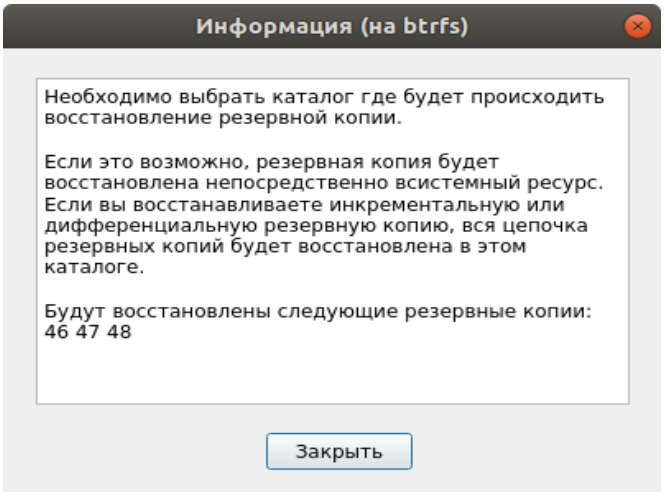


Рисунок 15

3. Укажите место восстановления резервной копии (рисунок 16):

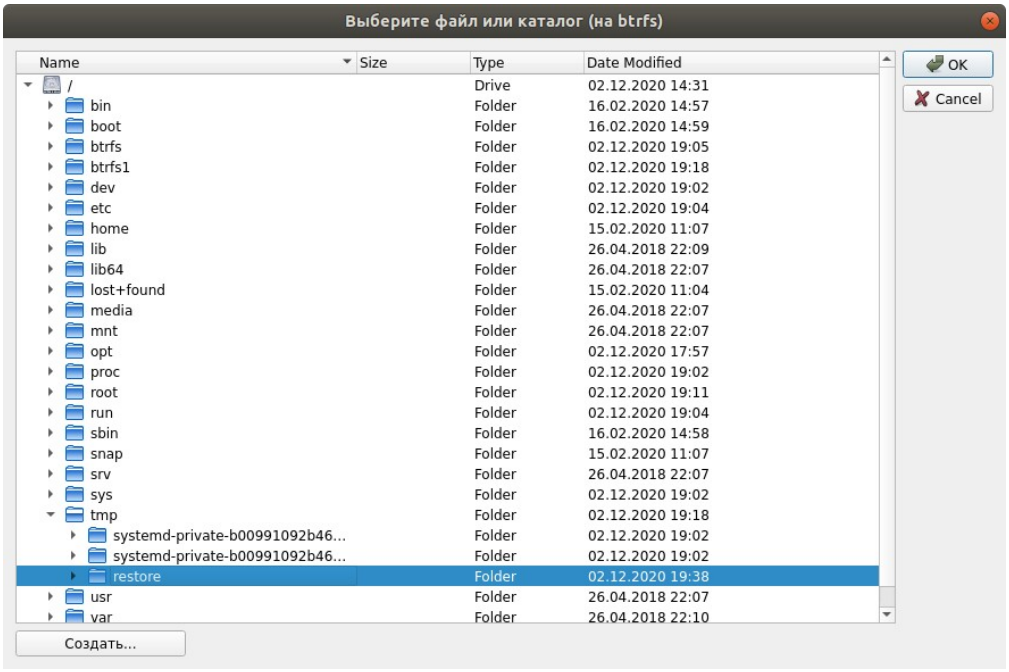


Рисунок 16

4. RBC выведет информационное сообщение о том, какие резервные копии будут восстановлены (рисунок 17):

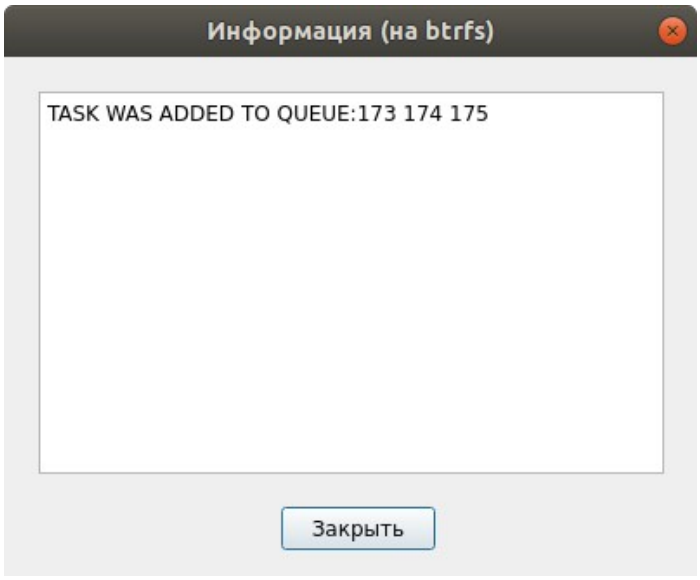
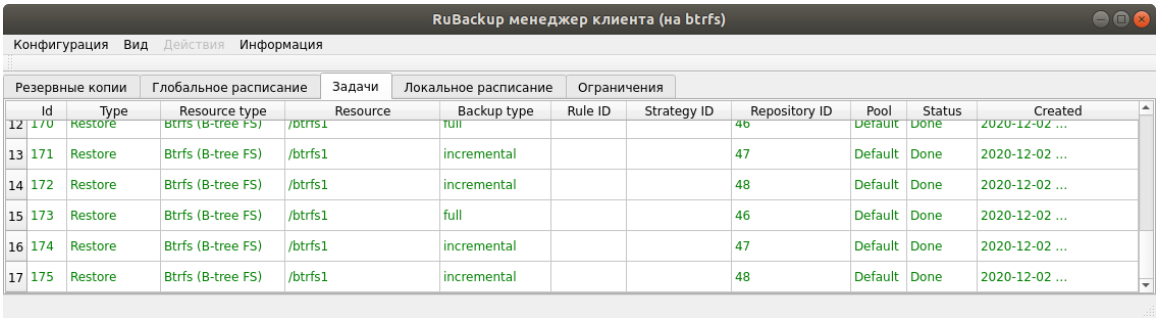


Рисунок 17

Для контроля процесса восстановления RBC автоматически переключится на вкладку «Задачи», в которой можно проконтролировать результат (рисунок 18):



	Id	Type	Resource type	Resource	Backup type	Rule ID	Strategy ID	Repository ID	Pool	Status	Created
12	170	Restore	Btrfs (B-tree FS)	/btrfs1	full			46	Default	Done	2020-12-02 ...
13	171	Restore	Btrfs (B-tree FS)	/btrfs1	incremental			47	Default	Done	2020-12-02 ...
14	172	Restore	Btrfs (B-tree FS)	/btrfs1	incremental			48	Default	Done	2020-12-02 ...
15	173	Restore	Btrfs (B-tree FS)	/btrfs1	full			46	Default	Done	2020-12-02 ...
16	174	Restore	Btrfs (B-tree FS)	/btrfs1	incremental			47	Default	Done	2020-12-02 ...
17	175	Restore	Btrfs (B-tree FS)	/btrfs1	incremental			48	Default	Done	2020-12-02 ...

Рисунок 18

Восстановление при помощи утилиты rb_archives

Для восстановления резервных копий клиент может использовать утилиту командной строки `rb_archives`. Вызов следующий:

```
# rb_archives
Id | Ref ID | Resource                | Resource type     | Backup
type | Created             | Crypto  | Signed | Status
---+--------+-------------------------+-------------------
+------------+---------------------+---------+--------+--------
46 |        | /btrfs1                 | Brtfs (B-tree FS) | full
| 2020-12-01 12:02:00 | nocrypt | True   | Trusted
47 | 46     | /btrfs1                 | Brtfs (B-tree FS) |
incremental | 2020-12-01 15:02:08 | nocrypt | True   | Trusted
48 | 47     | /btrfs1                 | Brtfs (B-tree FS) |
incremental | 2020-12-02 10:00:11 | nocrypt | True   | Trusted
49 |        | /btrfs1                 | Brtfs (B-tree FS) | full
| 2020-12-02 11:02:14 | nocrypt | True   | Trusted
50 |        | /btrfs1/new subvolume 0 | Brtfs (B-tree FS) | full
| 2020-12-02 11:02:14 | nocrypt | True   | Trusted

# rb_archives -x 48
Password:
----> Restore archive chain: 46 47 48  < ----
Record ID: 46 has status: Trusted
Record ID: 47 has status: Trusted
Record ID: 48 has status: Trusted
[RBC] Request to restore next archive(s) ID from repository: 46 47
48  to /root/test
TASK WAS ADDED TO QUEUE: 170 171 172
```

В примере выше цепочка резервных копий была восстановлена в текущий каталог (`/root/test/`). Чтобы восстановить данные в другое место можно использовать параметр `-d` (подробно см. руководство «Утилиты командной строки RuBackup»).