RuBackup
Система резервного копирования и восстановления данных

Резервное копирование и восстановление Ceph RADOS block device

RuBackup

Версия 1.9

2022 г.

Содержание

Введение

Система резервного копирования RuBackup позволяет выполнять клиентам полное, инкрементальное и дифференциальное резервное копирование блочных устройств (RADOS block devices) объектной сети хранения Ceph в «горячем» режиме, без их остановки.

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.

Для выполнения резервного копирования или восстановления блочных устройств Ceph у вас должен быть настроен кластер Ceph.

Для выполнения резервного копирования на хост клиента Ceph, на котором доступны требуемые блочные устройства, требуется установить клиента RuBackup и модуль *ceph_rbd* для клиента RuBackup.

Резервное копирование выполняется по заранее заданным правилам в глобальном расписании RuBackup. Клиенту доступно срочное резервное копирование блочных устройств, 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.

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

В ходе выполнения резервного копирования используется технология создания моментальных снимков блочного устройства Ceph. Перед созданием снимка и сразу после создания снимка, на клиенте Ceph может быть выполнен скрипт, который обеспечит консистентность данных приложения, использующего блочное устройство.

Восстановление резервной копии (или цепочки резервных копий) по умолчанию происходит в хранилище Ceph, но с заранее предустановленным другим именем и, при необходимости, в другой пул. При необходимости резервные копии могут быть восстановлены в файловую систему в виде файлов, которые впоследствии можно экспортировать в кластер Ceph с помощью штатных инструментов Ceph.

Установка клиента RuBackup

Для возможности резервного копирования файловых систем при помощи RuBackup на сервер должен быть установлен клиент RuBackup. Модуль для резервного копирования и восстановления блочных устройств включён в состав клиентского пакета. Подробно процедура установки клиента описана в «Руководстве по установке серверов резервного копирования и Linux клиентов RuBackup», а для операционной системы Windows — в «Руководстве по установке Windows 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 клиента Ceph для выполнения резервного копирования средствами RuBackup

Для подготовки хоста клиента Ceph к выполнению резервного копирования при помощи СРК RuBackup необходимо выполнить следующие действия:

1) Установить модуль *ceph_rbd* RuBackup для возможности выполнения резервного копирования и восстановления блочных устройств Ceph (RADOS block device).

   В зависимости от типа операционной системы:

   ```
   # sudo dpkg -i ./rubackup-ceph-rbd.deb
   ```

   или

   ```
   # sudo rpm -I ./rubackup-ceph-rbd.rpm
   ```

2) Создать каталог для создания резервных копий и хранения временных файлов.

Для создания резервных копий и хранения временных файлов, которые создаются при их восстановлении, требуется определённое пространство. Рекомендуется выделить для этой цели отдельный диск или устройство хранения достаточного размера и примонтировать к */backup-tmp* (либо к иной удобной точке монтирования), во избежание переполнения системного диска. Необходимо определить этот каталог как значение параметра *use-local-backup-directory* в конфигурационном файле */opt/rubackup/etc/config.file* и перезагрузить клиент RuBackup.

В исключительных случаях допустимо использование возможности сервера RuBackup предоставить клиенту NFS каталог для создания резервной копии. Для этого нужно определить значение параметра *nfs-share-mountpoint*, который определяет в какую точку файловой системы будет примонтирован NFS каталог. Параметр *use-local-backup-directory* в этом случае должен быть отключён, а на сервере RuBackup произведены соответствующие настройки

для определения разделяемого каталога. Более подробно см. «Руководство системного администратора RuBackup».

Защитное преобразование резервных копий

При необходимости, сразу после выполнения резервного копирования ваши резервные копии 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.

Автоматическое защитное преобразование и обратное преобразование резервных копий клиентом RuBackup возможны при помощи ключей длиной 256 бит, однако утилита rbcryt поддерживает ключи длиной 128, 256, 512 и 1024 бита (в зависимости от выбранного алгоритма преобразования). Если необходимо для правила глобального расписания выбрать особый режим преобразования, с длиной ключа, отличной от 256 бит и с ключом, располагающемся в другом месте, то вы можете воспользоваться возможностью 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 резервной копии следует вручную при помощи утилиты преобразования. При таком режиме работы нет необходимости указывать алгоритм преобразования в правиле резервного копирования, либо архив будет преобразован ещё раз автоматически 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	
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	

Локальный лист ограничений

В том случае, если какие-либо конкретные ресурсы клиента не должны попасть в резервную копию, их можно включить в локальный лист ограничений на клиенте. Лист ограничений располагается в каталоге */opt/rubackup/etc/rubackup_restriction.list.ceph_rbd.*

Наименование ресурса, для которого нет необходимости выполнять резервное копирование, должно быть указано в отдельной строке листа ограничений.

Для того, чтобы листы ограничений имели силу, необходимо включить эту возможность для клиента в конфигурации RuBackup (см. Руководство системного администратора RuBackup).

Использование менеджера администратора RuBackup

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.

Запуск менеджера администратора RBM:

Вариант 1:

```
# sudo LD_LIBRARY_PATH=/opt/rubackup/lib /opt/rubackup/bin/rbm
```

Вариант 2:

```
# ssh -X you_rubackup_server
# sudo LD_LIBRARY_PATH=/opt/rubackup/lib /opt/rubackup/bin/rbm
```

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).

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

При помощи менеджера администратора RuBackup можно создать в глобальном расписании одно или несколько правил резервного копирования блочных устройств Ceph.

Для этого необходимо выполнить следующие действия:

1. Выбрать клиентский хост, на котором установлен клиент Ceph и добавить правило резервного копирования (рисунок 2).

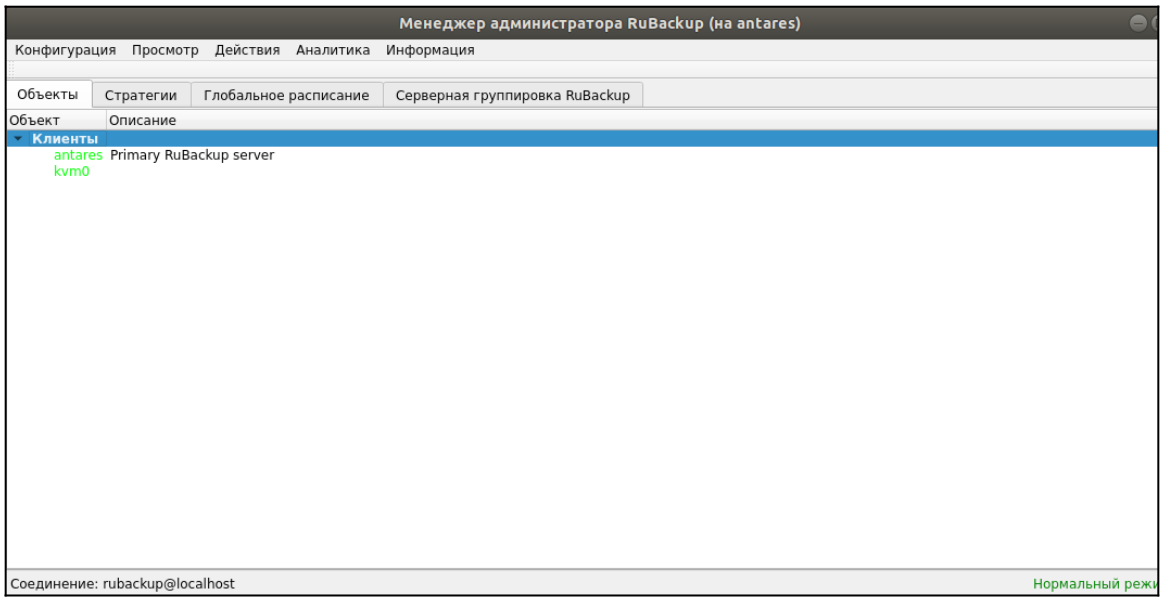


Рисунок 1

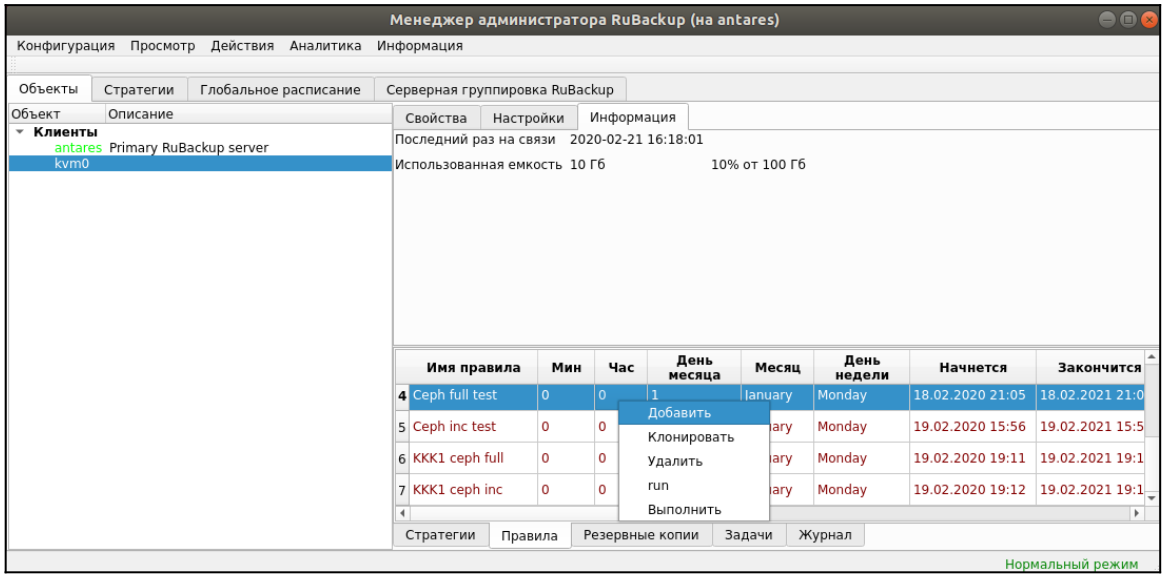


Рисунок 2

2. Выбрать тип ресурса «Ceph block device» (рисунок 3):

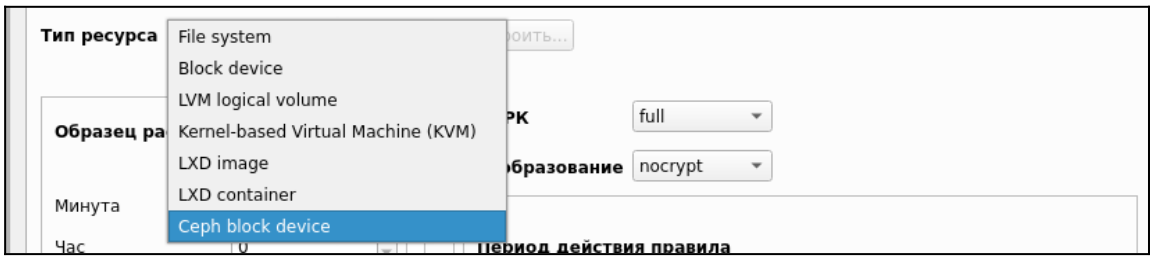


Рисунок 3

3. Выбрать ресурс, для которого будет выполняться правило (рисунок 4):

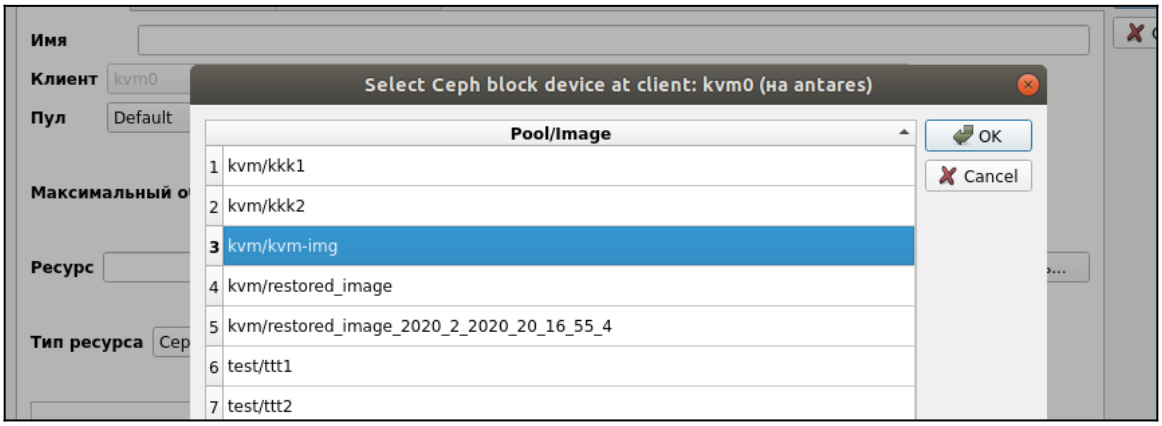


Рисунок 4

4. Установить прочие настройки: тип резервного копирования (Full), максимальный объем для резервных копий данного правила (100 Гб), срок хранения (2 недели), условия запуска выполнения резервного копирования (каждый день в полночь) (рисунок 5).

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 6).

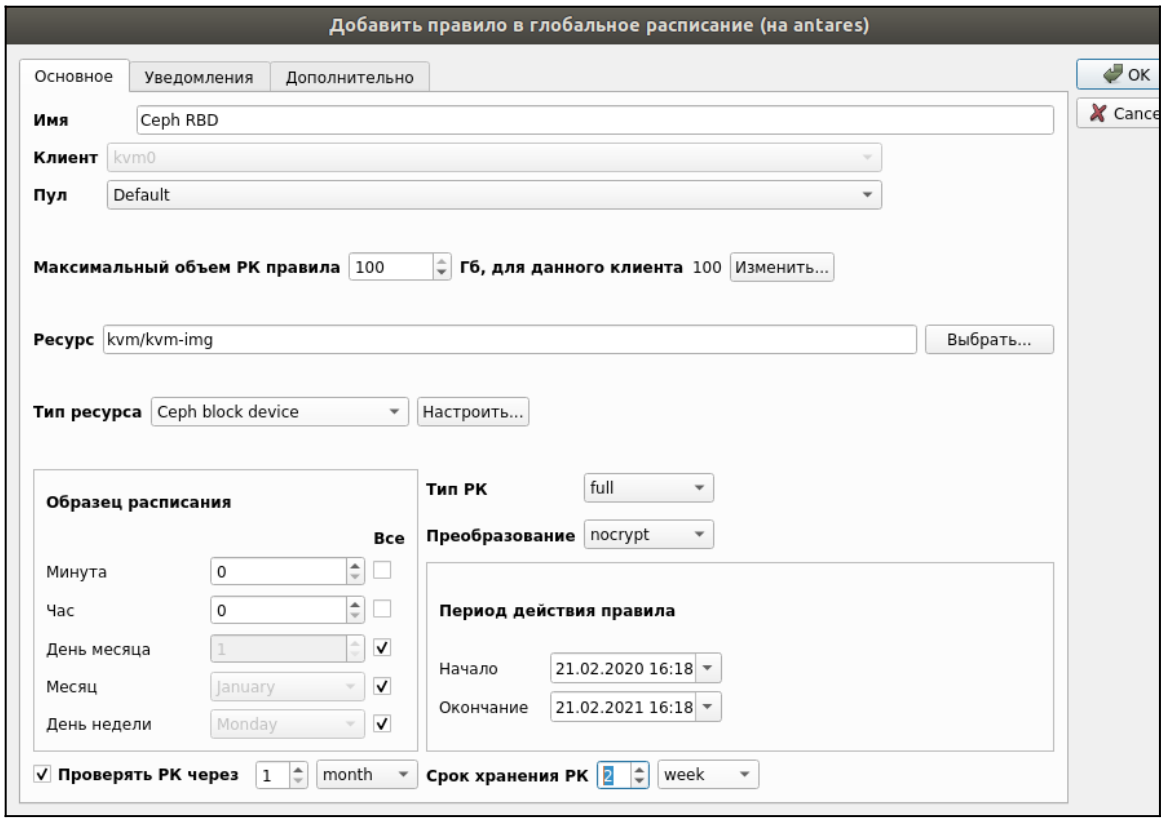


Рисунок 5

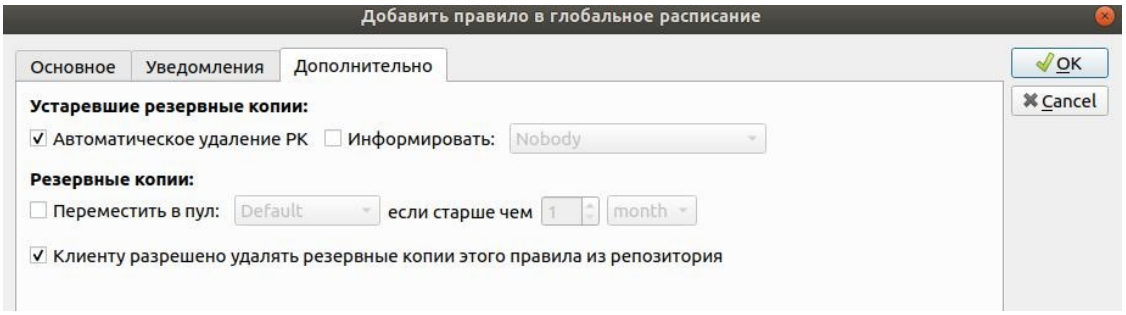


Рисунок 6

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 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) Для блочных устройств Ceph в дополнительных настройках правила резервного копирования возможно задать выполнение скрипта непосредственно перед созданием снимка блочного устройства и непосредственно сразу после создания снимка блочного устройства.

5) Выполнить преобразование резервной копии на клиенте.

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

7) Периодически выполнять проверку целостности резервной копии.

8) 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.

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

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

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.

Настройки правил глобального расписания RuBackup

Для выполнения резервного копирования блочного устройства необходимо при помощи менеджера администратора RuBackup создать правило в глобальном расписании, в котором указать соответствующий тип ресурса **Ceph block device**. При создании правила в глобальном расписании администратор RuBackup будет видеть список всех блочных устройств на клиенте и может выбрать требуемое (для этого необходимо, чтобы на клиенте работал клиентский фоновый процесс).

При создании правила резервного копирования можно определить следующие параметры:

1) тип резервного копирования (полный, дифференциальный или инкрементальный).;

2) разрешенный максимальный объем для всех резервных копий правила;

3) необходимость преобразования резервной копии тем или иным алгоритмом (преобразование будет выполняться на стороне клиента);

4) шаблон времени и даты создания задачи резервного копирования;

5) флаг и период автоматической проверки резервной копии;

6) срок хранения резервных копий создаваемого правила;

7) пул хранения, в котором будут размещены резервные копии;

8) необходимость автоматического удаления резервной копии, срок хранения которой истёк;

9) перемещение резервной копии в другой пул, при достижении определённого срока с момента её создания;

10) возможность для клиента удалять резервные копии из репозитория;

11) настройки системы уведомления RuBackup для создаваемого правила;

Уведомления могут происходить в следующих случаях:

- нормальное исполнение процедуры резервного копирования;
- исполнение процедуры резервного копирования с ошибками;

– проверка резервной копии;

– окончание периода действия создаваемого правила;

– окончание выделенного объёма для хранения резервных копий правила;

– окончание срока хранения резервной копии;

12) дополнительные настройки правила для выполнения резервного копирования блочного устройства Ceph (рисунок 7):

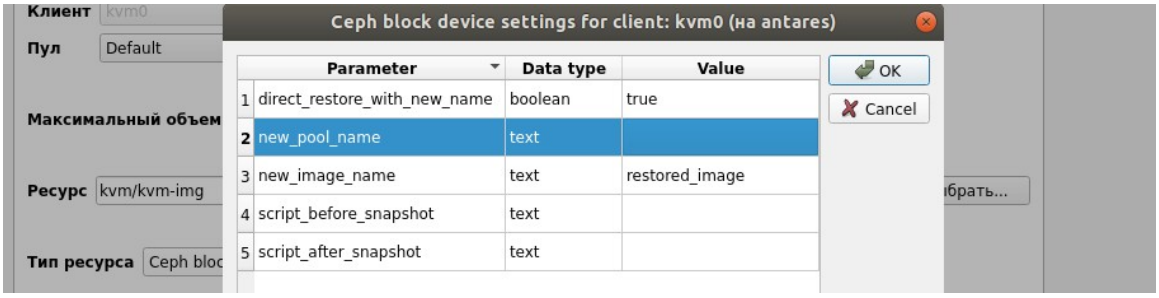


Рисунок 7

– `direct_restore_with_new_name` – при установленном значении `true` резервная копия будет восстановлена во вновь созданное устройство с новым именем;

– `new_pool_name` – создать новое устройство в указанном пуле при (внимание: пул должен быть создан заранее);

– `new_image_name` – создать новое устройство и заданным именем для восстановления резервной копии;

– `script_before_snapshot` – скрипт, который будет выполнен на клиенте непосредственно перед созданием снимка блочного устройства;

– `script_after_snapshot` – скрипт, который будет выполнен непосредственно после создания снимка состояния блочного устройства.

Использование клиентского менеджера 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.

Запуск клиентского менеджера:

Вариант 1:

```
# sudo LD_LIBRARY_PATH=/opt/rubackup/lib/opt/rubackup/bin/rbc
```

Вариант 2:

```
# ssh -X you_rubackup_client
# sudo LD_LIBRARY_PATH=/opt/rubackup/lib /opt/rubackup/bin/rbc
```

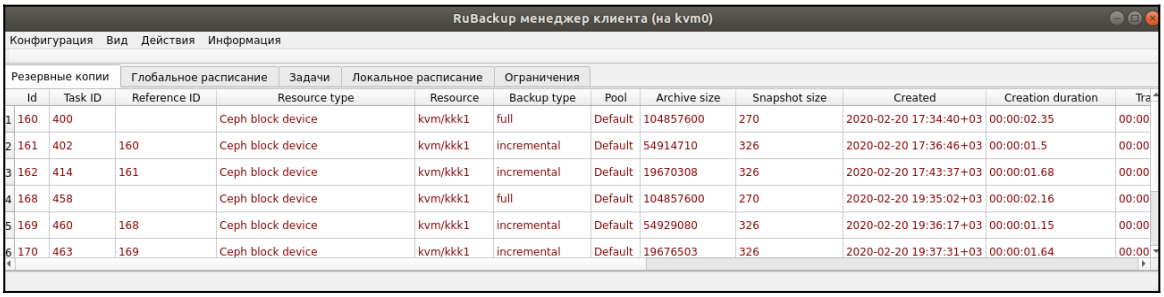
При первом запуске клиентского менеджера необходимо задать пароль, при помощи которого впоследствии можно будет запросить восстановление резервной копии. Без ввода пароля получить резервную копию для клиента из хранилища невозможно. Хэш пароля восстановления хранится в базе данных

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 8). 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	Tra
1	160	400		Ceph block device	kvm/kkk1	full	Default	104857600	270	2020-02-20 17:34:40+03	00:00:02.35	00:00
2	161	402	160	Ceph block device	kvm/kkk1	incremental	Default	54914710	326	2020-02-20 17:36:46+03	00:00:01.5	00:00
3	162	414	161	Ceph block device	kvm/kkk1	incremental	Default	19670308	326	2020-02-20 17:43:37+03	00:00:01.68	00:00
4	168	458		Ceph block device	kvm/kkk1	full	Default	104857600	270	2020-02-20 19:35:02+03	00:00:02.16	00:00
5	169	460	168	Ceph block device	kvm/kkk1	incremental	Default	54929080	326	2020-02-20 19:36:17+03	00:00:01.15	00:00
6	170	463	169	Ceph block device	kvm/kkk1	incremental	Default	19676503	326	2020-02-20 19:37:31+03	00:00:01.64	00:00

Рисунок 8

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. В том случае, если правилом резервного копирования установлено, что резервную копию (или цепочку резервных копий) необходимо восстановить в виде файлов в файловую систему, пользователь может выбрать каталог для восстановления (см. direct_restore_with_new_name).

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,

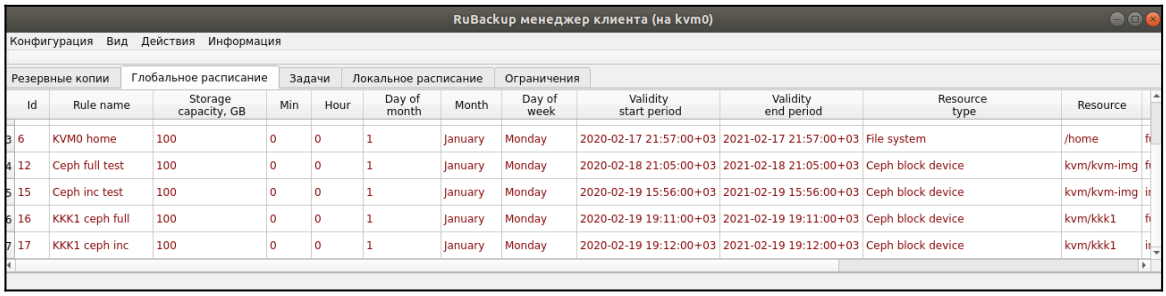
предназначенном для создания и временного хранения резервных копий (см.опцию use-local-backup-directory).

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 9).



	Id	Rule name	Storage capacity, GB	Min	Hour	Day of month	Month	Day of week	Validity start period	Validity end period	Resource type	Resource	
3	6	KVM0 home	100	0	0	1	January	Monday	2020-02-17 21:57:00+03	2021-02-17 21:57:00+03	File system	/home	fi
4	12	Ceph full test	100	0	0	1	January	Monday	2020-02-18 21:05:00+03	2021-02-18 21:05:00+03	Ceph block device	kvm/kvm-img	fi
5	15	Ceph inc test	100	0	0	1	January	Monday	2020-02-19 15:56:00+03	2021-02-19 15:56:00+03	Ceph block device	kvm/kvm-img	in
6	16	KKK1 ceph full	100	0	0	1	January	Monday	2020-02-19 19:11:00+03	2021-02-19 19:11:00+03	Ceph block device	kvm/kkk1	fi
7	17	KKK1 ceph inc	100	0	0	1	January	Monday	2020-02-19 19:12:00+03	2021-02-19 19:12:00+03	Ceph block device	kvm/kkk1	in

Рисунок 9

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 10). 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**»).

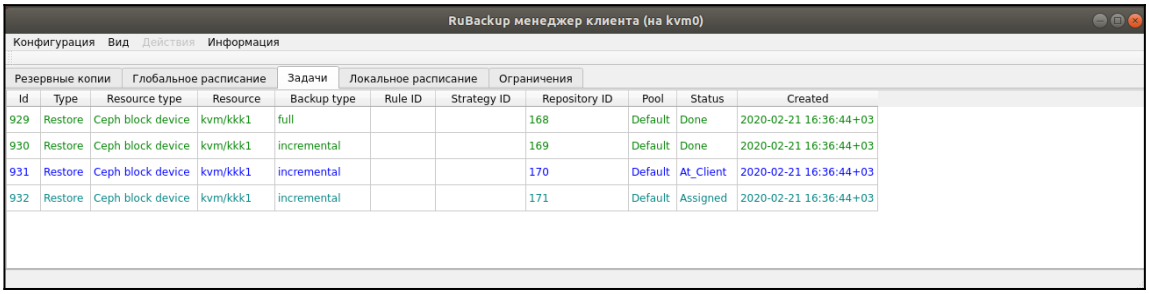


Рисунок 10

Примечание – Информация о выполнении служебных задач в данной вкладке не отображается. Служебными являются задачи проверки, удаления, перемещения резервных копий, а также их копирования в другой пул.

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.

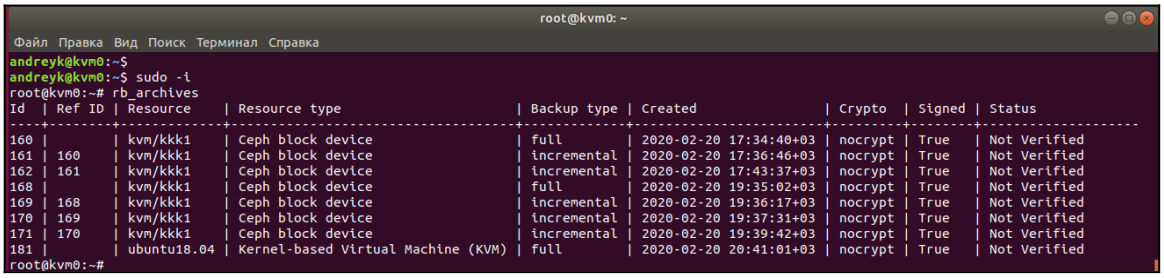
Утилиты командной строки клиента

RuBackup

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

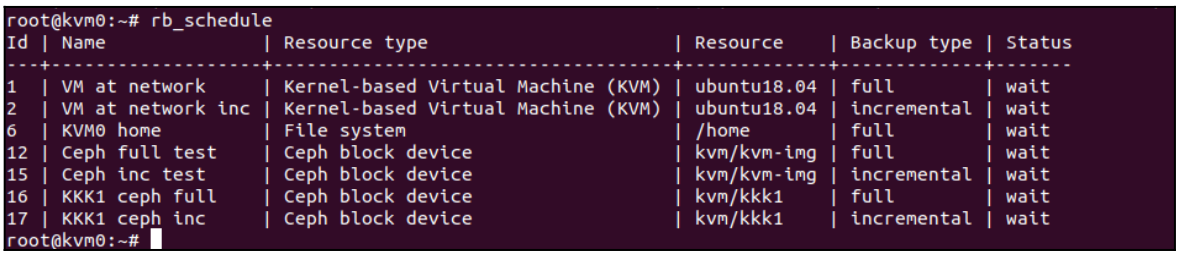
rb_archive

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



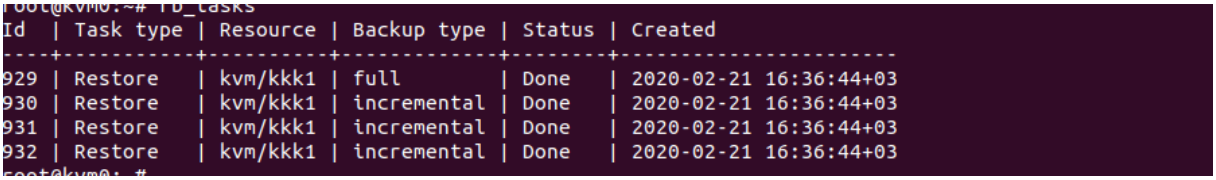
rb_schedule

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



rb_tasks

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



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

Действия после восстановления резервной копии

В том случае, если правилом резервного копирования для ресурса типа Ceph block device установлена дополнительная настройка `direct_restore_with_new_name` в значение `false`, то восстановление произойдёт в выбранный пользователем локальный каталог.

В том случае, если вы восстанавливаете цепочку резервных копий (полную и несколько инкрементальных), то в каталоге будет находится один файл с расширением .full и несколько с расширением diff.

Для импорта полной резервной копии нужно воспользоваться командой:

```
# /usr/bin/rbd import archive.full pool/new_image_name
```

Для импорта инкрементальных или дифференциальной резервной копии необходимо выполнить следующие команды:

```
# /usr/bin/rbd snap create pool/new_image_name@rubackup-full.snap

# /usr/bin/rbd import-diff archive.diff pool_new_image_name

# /usr/bin/rbd rename pool/new_image_name@rubackup-inc.snap pool/new_image_name@rubackup-inc-prev.snap
```

В случае нескольких инкрементальных копий для каждой из них повторить последние две команды.

По окончании восстановления выполнить:

```
# /usr/bin/rbd snap purge pool/new_image_name
```