**RuBackup**
Система резервного копирования и восстановления данных

# Резервное копирование

# и восстановление виртуальных машин

# программного комплекса

# Р-Виртуализация

RuBackup

Версия 1.9

2022 г.

# Содержание

Введение....3
Установка клиента RuBackup....5
Мастер-ключ....6
Удаление клиента RuBackup....7
Подготовка виртуальной машины ПК Р-Виртаулизация....8
Защитное преобразование резервных копий....9
Локальный лист ограничений....11
Использование оконного менеджера администратора RuBackup....12
Настройки правил глобального расписания RuBackup....17
Утилиты командной строки клиента RuBackup....19
Восстановление резервной копии виртуальной машины....21

# Введение

Система резервного копирования RuBackup позволяет выполнять полное, инкрементальное или дифференциальное резервное копирование виртуальных машин программного комплекса (далее — ПК) Р-Виртуализация 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 виртуальных машин на хост, где установлен ПК Р-Виртаулизация, требуется установить клиента RuBackup и модуль rvirt_vm для клиента RuBackup. В виртуальные машины, для которых предполагается выполнение резервного копирования средствами RuBackup, должны быть установлены дополнения гостевой системы.

Резервное копирование выполняется по заранее заданным правилам в глобальном расписании RuBackup. Клиенту доступно срочное резервное копирование виртуальных машин ПК Р-Виртаулизация, 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»).

Количество дисков в виртуальной машине может быть больше одного, в этом случае резервное копирование выполняется для всех дисков.

В ходе выполнения резервного копирования используется технология создания моментальных снимков виртуальной машины. Перед созданием снимка и сразу после создания снимка, внутри виртуальной машины может

быть выполнен скрипт, который обеспечит консистентность данных приложения, функционирующего в виртуальной машине.

# Установка клиента RuBackup

Для возможности резервного копирования виртуальных машин ПК Р-Виртаулизация при помощи RuBackup на физический сервер ПК Р-Виртаулизация должен быть установлен клиент RuBackup.

**Инсталляция пакетов клиента RuBackup:**

```
# sudo -i
# rpm -i rubackup-client-1.3-1.el7.x86_64.rpm
# rpm -i rubackup-rvirt_vm-1.3-1.el7.x86_64.rpm
```

В файл `.bashrc` необходимо добавить путь к утилитам RuBackup:

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

и применить изменения:

```
# . .bashrc
```

**Настройка клиента Rubackup при помощи утилиты rb_init**

Подробно процедура установки клиента описана в «Руководстве по установке серверов резервного копирования и Linux клиентов RuBackup», 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).

# 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:

```
[rootrosplatforva ~]# hexdump /opt/rubackup/keys/master-key
0000000 e973 053d 10a1 c0c1 40e8 d332 9463 a7ee
0000010 8965 f275 d5e4 a04a d07d a625 d4e8 755f
0000020
[rootrosplatforva ~]#
```

# Удаление клиента RuBackup

Остановить сервис `rubackup-client`:

```
# systemctl disable rubackup-client
# systemctl daemon-reload
```

Удалить клиента RuBackup можно следующим способом:

```
# yum remove rubackup-client.x86_64
```

1. Если есть необходимость удалить клиента RuBackup из конфигурации СРК, то это может сделать системный администратор RuBackup с помощью оконного менеджера rbm.

# Подготовка виртуальной машины ПК

# Р-Виртаулизация

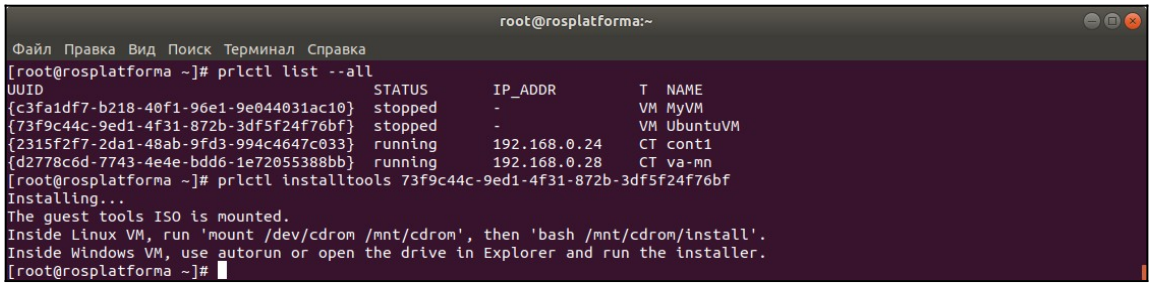
Необходимо установить для каждой виртуальной машины дополнения гостевой операционной системы:

1. Определить UUID виртуальной машины, на которую необходимо установить госетвые дополнения:

```
# prlctl list --all
```

2. Установить гостевые дополнения:

```
# prlctl installtools <ID | Name >
```



# 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 файле */opt/rubackup/etc/rubackup_restriction.list.rvirt*.

Наименование ресурса (UUID), 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 оконного 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 можно выполнить двумя вариантами:

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 виртуальных машин на хосте, где функционирует ПК Р-Виртаулизация, должен быть установлен клиент RuBackup и модуль, 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 виртуальных машин ПК Р-Виртаулизация.

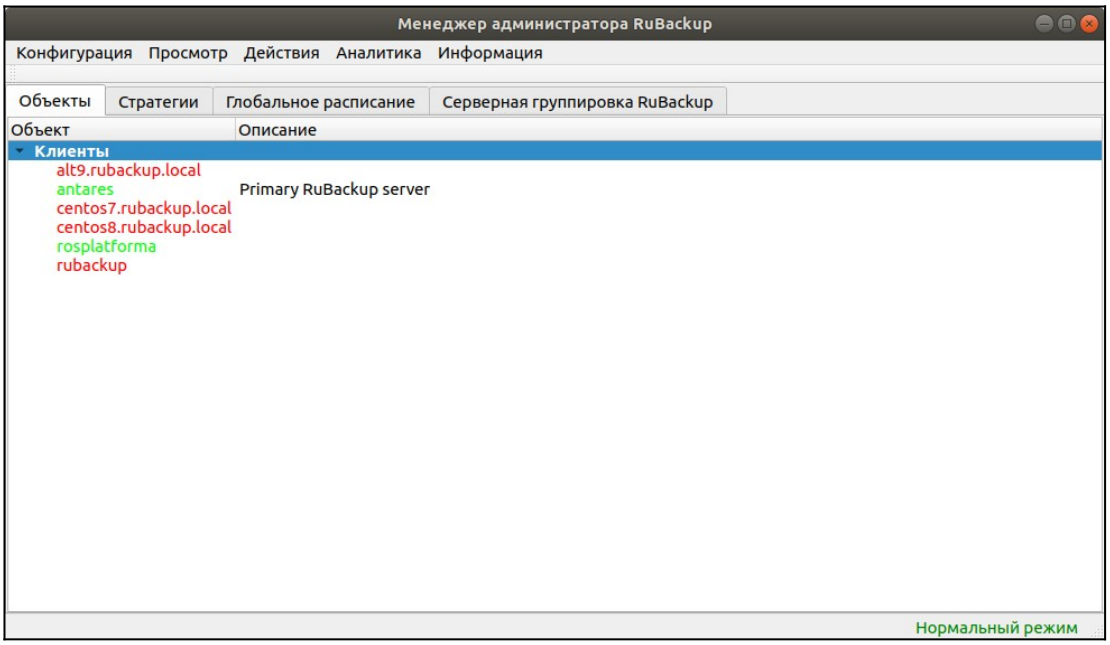



Рисунок 1

1. Выбрать клиентский хост, на котором установлен ПК Р-Виртаулизация и добавить правило резервного копирования (рисунок 2):

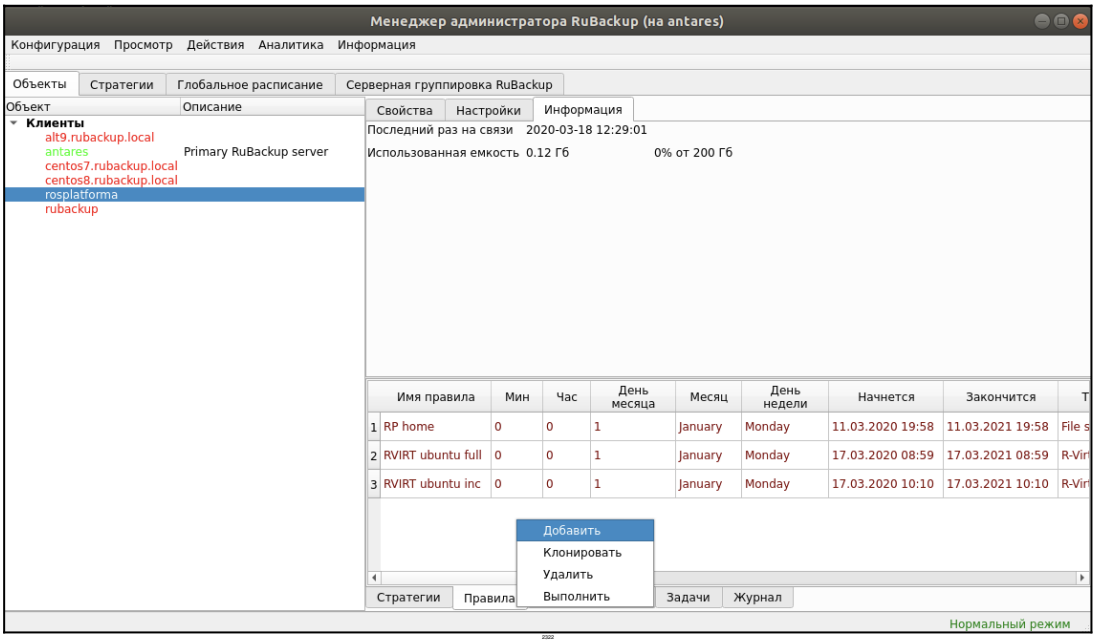



Рисунок 2

2. Выбрать тип ресурса «R-Virtualization VM» (рисунок 3):

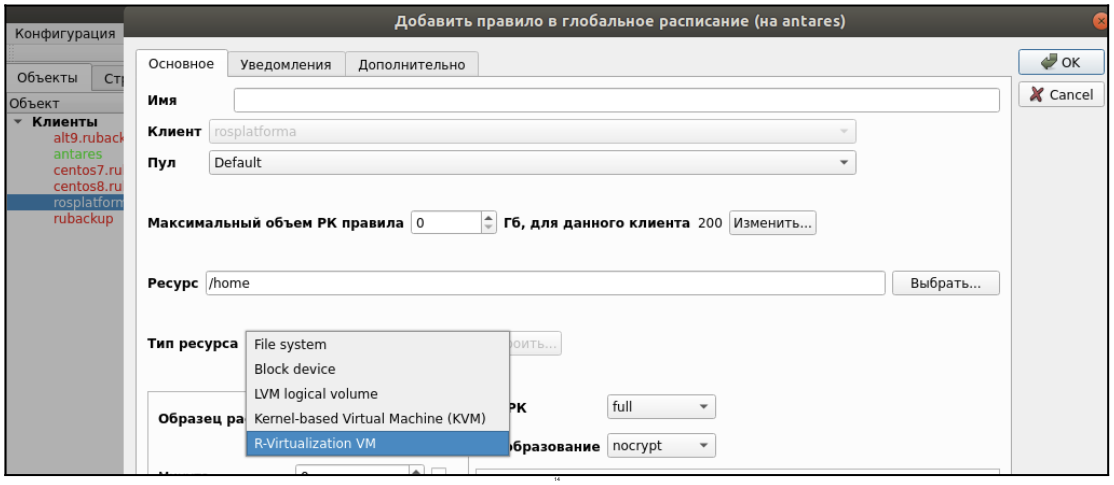



Рисунок 3

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

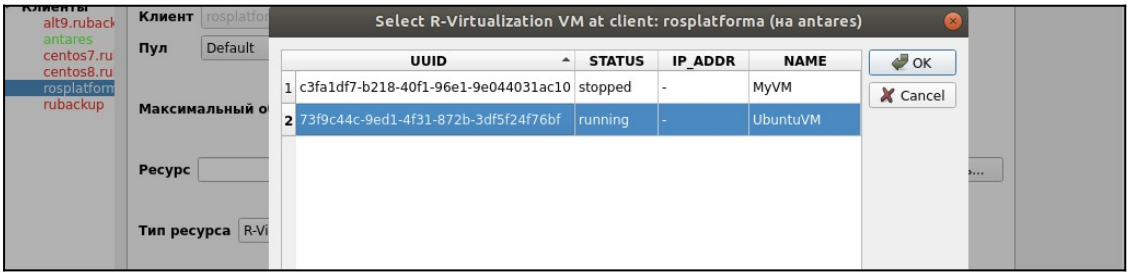



Рисунок 4

4. Установить прочие настройки: тип резервного копирования (Full), максимальный объем для резервных копий данного правила (100 Гб), срок хранения (2 недели), через какой промежуток времени требуется выполнить проверку резервной копии или не проверять её вовсе (рисунок 5).

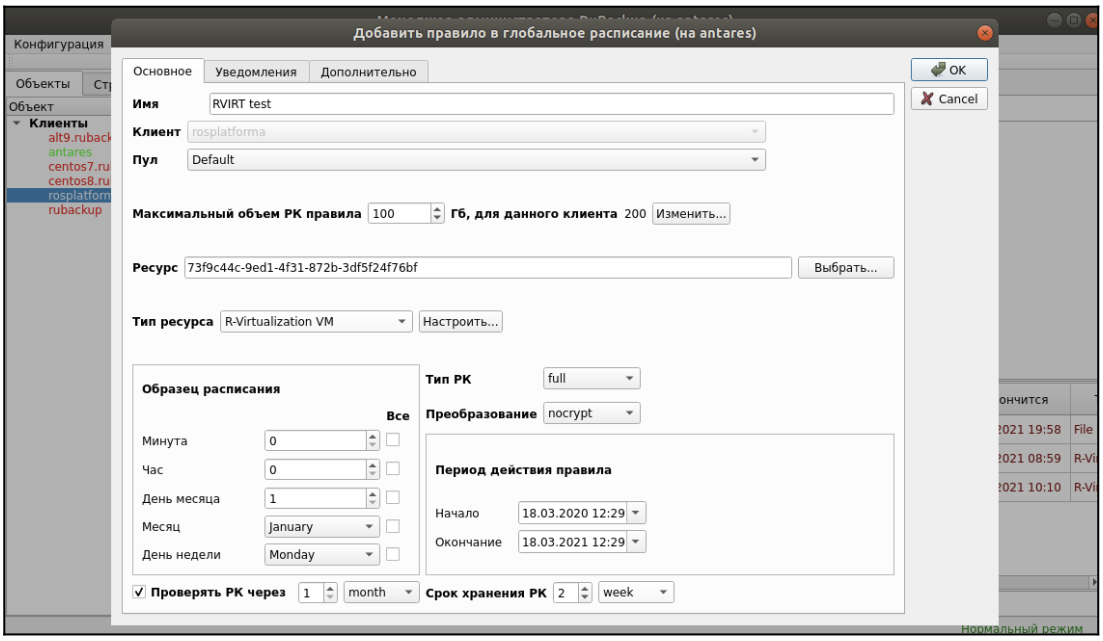



Рисунок 5

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):

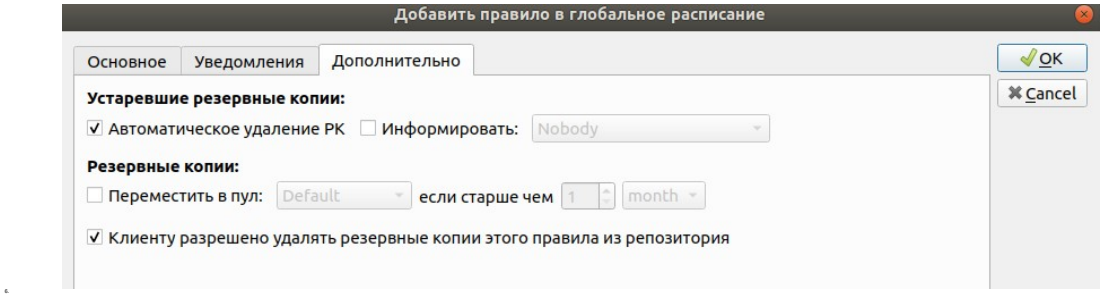



Рисунок 6

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 виртуальных машин ПК Р-Виртаулизация в дополнительных настройках правила резервного копирования возможно задать выполнение скрипта непосредственно перед созданием снимка виртуальной машины и непосредственно сразу после создания снимка виртуальной машины.

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 виртуальной машины ПК Р-Виртаулизация необходимо при помощи менеджера администратора RuBackup создать правило в глобальном расписании, в котором указать тип ресурса **R-Virtualization VM**. При создании правила в глобальном расписании администратор RuBackup будет видеть список всех виртуальных машин на хосте гипервизора и может выбрать требуемую виртуальную машину (для этого необходимо, чтобы на клиенте работал клиентский фоновый процесс).

При создании правила резервного копирования можно определить следующие параметры:

– тип резервного копирования (полный, дифференциальный или инкрементальный);

– разрешенный максимальный объем для всех резервных копий правила;

– необходимость преобразования резервной копии тем или иным алгоритмом . Преобразование будет выполняться на стороне клиента;

– шаблон времени и даты создания задачи резервного копирования;

– флаг и период автоматической проверки резервной копии;

– срок хранения резервных копий создаваемого правила;

– пул хранения, в котором будут размещены резервные копии;

– необходимость автоматического удаления резервной копии, срок хранения которой истёк;

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

– возможность для клиента удалять резервные копии из репозитория;

– настройки системы уведомления RuBackup для создаваемого правила. Уведомления могут происходить в следующих случаях:

1) нормальное исполнение процедуры резервного копирования;
2) исполнение процедуры резервного копирования с ошибками;
3) проверка резервной копии;
4) окончание периода действия создаваемого правила;
5) окончание выделенного объёма для хранения резервных копий правила;
6) окончание срока хранения резервной копии.

– Дополнительные настройки правила для выполнения резервного копирования виртуальной машины ПК Р-Виртаулизация :

1) скрипт внутри виртуальной машины, который будет выполнен непосредственно перед созданием снимка состояния виртуальной машины;
2) скрипт внутри виртуальной машины, который будет выполнен непосредственно после создания снимка состояния виртуальной машины;
3) таймаут в секундах, по истечение которого незавершившийся скрипт внутри виртуальной машины считается завершившимся неудачно;
4) размер блока данных для выполнения копирования информации с raw устройств виртуальной машины;
5) необходимость выполнять резервное копирование, если виртуальная машина находится в выключенном состоянии.

**Запуск скрипта внутри виртуальной машины при резервном копировании**

В том случае, если дополнительными настройками правила резервного копирования не задан скрипт, который должен быть выполнен внутри виртуальной машины перед и после создания снэпшота, но в виртуальной машине присутствует файл */opt/rubackup/scripts/rubackup-rvirt.sh*, то он будет выполнен с аргументом *before* перед созданием снэпшота и с аргументом *after* – после создания снэпшота. Значение таймаута в этом случае равняется 5 секундам.

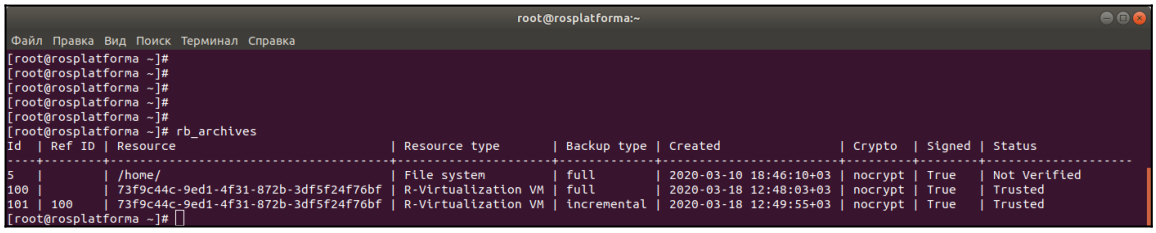
# Утилиты командной строки клиента

# RuBackup

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

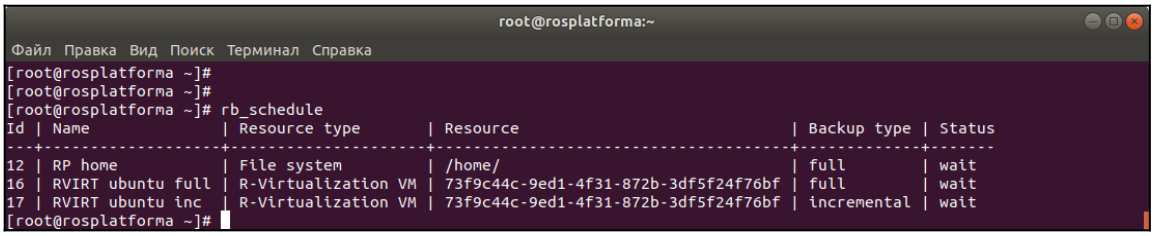
### rb_archive

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



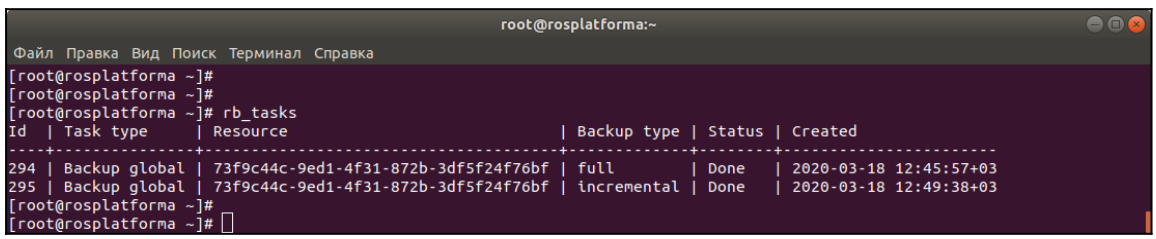

### rb_schedule

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




### rb_tasks

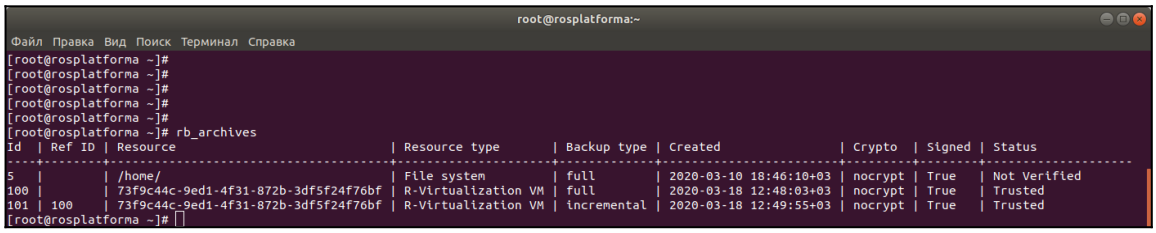
Утилита предназначена для просмотра задач клиента, которые присутствуют в главной очереди задач системы резервного копирования.



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

# Восстановление резервной копии виртуальной машины

Для восстановления резервной копии виртуальной машины необходимо определить идентификатор резервной копии, которую необходимо восстановить, например, при помощи команды `rb_archives`:




В приведенном примере в системе резервного копирования присутствуют две резервные копии виртуальной машины с UUID 73f9c44c-9ed1-4f31-872b-3df5f24f76bf: полная и инкрементальная. В случае восстановления полной резервной копии нужно выполнить команду

```
# rb_archives -x 100
```

В случае восстановления инкрементальной резервной копии будет сформирована цепочка восстановления: вначале будет восстановлена полная резервная копия и на нее будут наложены изменения из инкрементальных резервных копий. Все это будет выполнено автоматически после выполнения команды

```
# rb_archives -x 101
```

Физические файлы виртуальной машины будут восстановлены в текущий каталог, где будет создана директория именованная как UUID восстанавливаемой виртуальной машины (в примере выше - 73f9c44c-9ed1-4f31-872b-3df5f24f76bf). В том случае, если виртуальную машину нужно восстановить в каком-то ином каталоге, то необходимо использовать при восстановлении опцию -d.

В том случае, если в ПК Р-Виртаулизация присутствует виртуальная машина, резервные копии которой востребованы к восстановлению, то она будет зарегистрирована в ПК Р-Виртаулизация с новым UUID и к ее имени будет добавлен порядковый номер (рисунок 7):

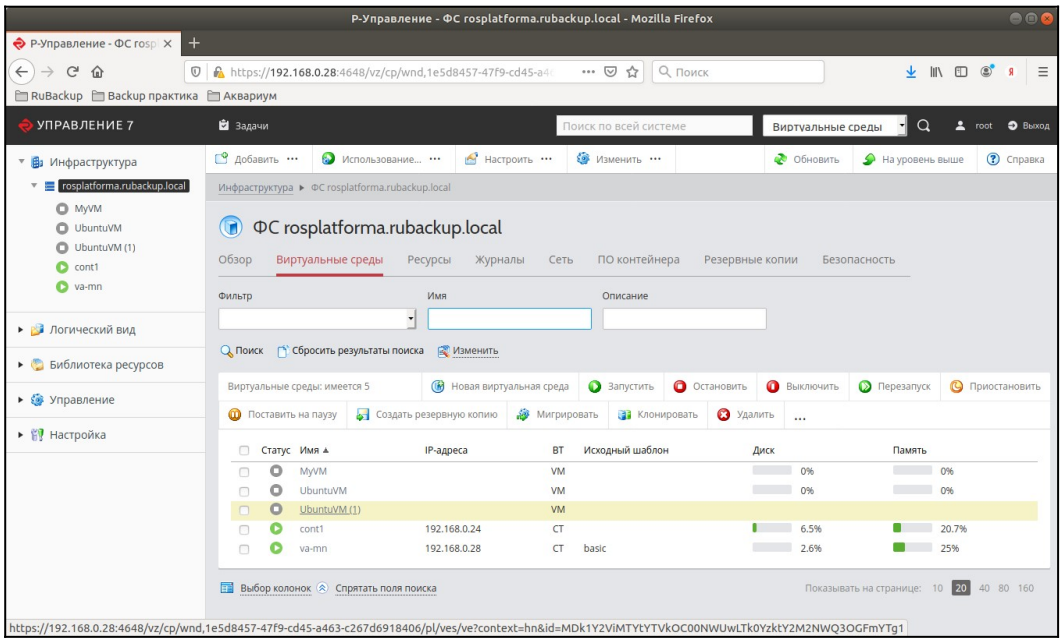



Рисунок 7

В том случае, если в ПК Р-Виртаулизация схожей виртуальной машины нет, то будет создана виртуальная машина с исходным именем, но с новым UUID (рисунок 8):

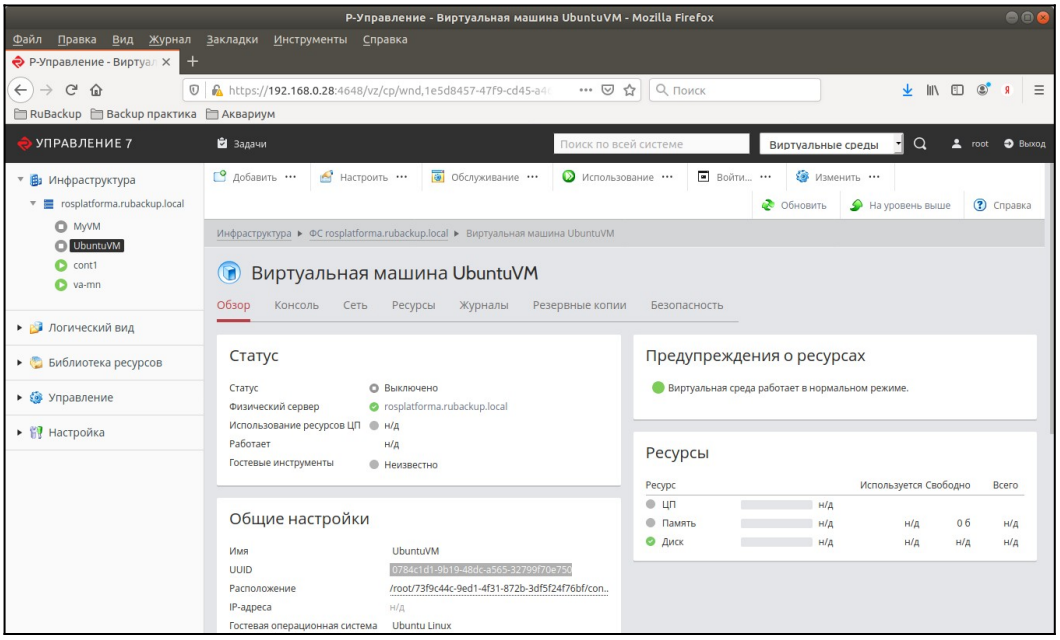



Рисунок 8