

**RuBackup**

Система резервного копирования и восстановления данных

# Резервное копирование РУСТЭК



**RuBackup**

Версия 1.10

2022 г.

# Содержание

Введение.....	3
Установка клиентов RuBackup.....	4
Мастер-ключ.....	5
Защитное преобразование резервных копий.....	6
Менеджер Администратора RuBackup (RBM).....	8
Срочное резервное копирование при помощи RBM.....	14
Централизованное восстановление резервных копий с помощью RBM. 16	
Восстановление со стороны клиента.....	18

## Введение

Система резервного копирования RuBackup позволяет выполнять резервное копирование и восстановление виртуальных машин платформы виртуализации РУСТЭК. Доступно полное, инкрементальное и дифференциальное резервное копирование. Так же возможно выполнять резервное копирование с использованием дедупликации и хранить резервные копии в дедуплицированном хранилище.

Резервное копирование виртуальных машин РУСТЭК выполняется безагентным способом. Это означает, что в виртуальную машину, для которой предполагается создание резервной копии, не устанавливается агент RuBackup (однако требуется установка гостевых расширений операционной системы, например qemu-guest-agent); резервное копирование виртуальной машины выполняется целиком, для всех дисков виртуальной машины; в ходе резервного копирования во всех случаях из резервной копии удаляются дублирующие блоки (всегда выполняется локальная дедупликация).

В случае передачи резервной копии в хранилище дедуплицированных резервных копий всегда происходит передача только тех уникальных блоков (для того же типа источника данных), которых еще нет в хранилище.

Для выполнения резервного копирования виртуальных машин среды виртуализации РУСТЭК необходимо установить клиента резервного копирования RuBackup по одной из следующих схем:

- на одну из виртуальных машин в данной среде виртуализации, для которой настроен доступ к гипервизору (гипервизорам);
- на несколько виртуальных машин в данной среде виртуализации, если это обусловлено необходимостью динамически распределять нагрузку в ходе резервного копирования или обеспечить возможность вывода той или иной виртуальной машины из эксплуатации без изменений в расписании резервного копирования (в данной схеме необходимо включить эти гипервизоры в кластерную группу клиентов системы резервного копирования);

При выполнении резервного копирования применяется технология создания моментальных снимков данных для дисков виртуальной машины, что позволяет не останавливать и не «подмораживать» работу на время резервного копирования.

Перед созданием снимка и сразу после его создания RuBackup может выполнить скрипт внутри виртуальной машины для того, чтобы иметь возможность привести данные приложений внутри виртуальной машины в консистентное состояние.

Также внутри виртуальной машины может быть создан скрипт, располагающийся в файле `/opt/rubackup/scripts/rustack.sh`. В том случае, если внутри виртуальной машины существует такой файл с атрибутами на исполнение, то перед созданием моментального снимка он будет выполнен с аргументом `before`, а сразу после создания моментального снимка он будет выполнен с аргументом `after`.

Примечание – Для возможности запуска скриптов внутри виртуальной машины должны быть выполнены следующие условия:

1) конфигурационный файл настроек доступа к API РУСТЭК `rb_module_rustack.conf` (подробнее в разделе **Установка Клиента RuBackup**) кроме основной пользовательской учетной записи должен содержать учетную запись администратора;

2) для развертывания виртуальной машины, для которой предполагается создание резервных копий, используется гипервизор типа QEMU;

3) для виртуальной машины, на которой развернут клиент RuBackup и модуль `rb_module_rustack`, необходимо:

- установить пакет `libvir-clients`;
- скопировать `ssh` ключ на хосты гипервизоров платформы РУСТЭК.

4) на виртуальной машине, для которой предполагается создание резервных копий, необходимо установить пакет `qemu-guest-agent`.

## Установка клиента RuBackup

Для возможности резервного копирования виртуальных машин среды виртуализации РУСТЭК необходимо установить клиента RuBackup на одну или виртуальных машин в среде виртуализации РУСТЭК, находящихся под управлением операционной системы Ubuntu 18.04 или 20.04, и для которой настроен доступ к гипервизору (гипервизорам). Сюда же необходимо установить модуль `rb_module_rustack` из пакета `rubackup-rustack.deb` (см. дистрибутив для ОС Debian 10).

Подробно процедура установки клиента описана в документе «Руководство по установке серверов резервного копирования и Linux клиентов RuBackup».

При установке клиента рекомендуется использовать функцию централизованного восстановления в тех случаях, когда предполагается восстановление виртуальной машины из средства управления RBM.

В ходе инсталляции пакета в системе будет создан файл настроек доступа системы резервного копирования к API РУСТЭК `/opt/rubackup/etc/rb_module_rustack.conf`:

```
# Mandatory parameters
url https://you.url/
username rustack_user
password secret_pass
domain default
timeout 5
rubackup-vm-name rubackup-ubuntu
#
# Optional parameters required to run
# scripts inside the virtual machine
admin_name admin
admin_password admin_pass
```

Измените в этом файле настройки для подключения к API.

При старте клиента RuBackup в журнальном файле `/opt/rubackup/log/RuBackup.log` на клиенте появится следующая запись:

```
Try to check module: 'RUSTACK' ...
Execute OS command: /opt/rubackup/modules/rb_module_rustack -t 2>&1
Module version: 1.10
Nova-api version: v2.1
Cinder version: v3.0
... module 'RUSTACK' was checked successfully
```

В ручном режиме проверить правильность настроек можно при помощи следующей команды:

```
# /opt/rubackup/modules/rb_module_rustack -t
```

## 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
00000000 79d1 4749 7335 e387 9f74 c67e 55a7 20ff
00000010 6284 54as 83a3 2053 4818 e183 1528 a343
00000020
```

# 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 `gbscrypt`. Ключ для защитного преобразования резервных копий располагается на хосте клиента в файле `/opt/rubackup/keys/master-key`. Защитное преобразование данных при помощи `gbscrypt` 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 `gbscrypt`. При таком режиме работы нет необходимости указывать алгоритм преобразования в правиле резервного копирования, иначе архив будет повторно преобразован с использованием мастер-ключа.



## Алгоритмы защитного преобразования

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

Таблица 1 – Алгоритмы защитного преобразования, доступные в утилите gbсруpt.

Алгоритм	Длина ключа, бит	Примечание
Anubis	128, 256	
Aria	128, 256	
CAST6	128, 256	
Camellia	128, 256	
Kalyna	128, 256, 512	Украинский национальный стандарт <u>ДСТУ 7624:2014</u>
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)

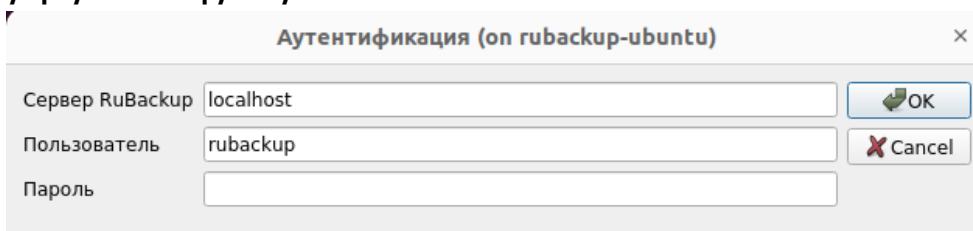
Оконное приложение Менеджер Администратора RuBackup (RBM) предназначено для администрирования серверной группировки RuBackup, включая управление клиентами, глобальным расписанием, хранилищами резервных копий и другими параметрами RuBackup.

В RuBackup 1.9, 1.10 RBM располагается в отдельном пакете и может быть установлен как на сервер резервного копирования, так и на удаленном APM администратора.

RuBackup 1.9, 1.10 предоставляет ролевую модель доступа к системе резервного копирования. При запуске RBM вам потребуется пройти аутентификацию. Уточните login/password для вашей работы у главного администратора СРК. Если вы главный администратор, то используйте для авторизации суперпользователя *rubackup* и тот пароль, который вы задали ему при инсталляции (рисунок 1).

Для запуска RBM следует выполнить команду:

```
# /opt/rubackup/bin/rbm&
```



Аутентификация (on rubackup-ubuntu)

Сервер RuBackup	<input type="text" value="localhost"/>	<input type="button" value="OK"/>
Пользователь	<input type="text" value="rubackup"/>	<input type="button" value="Cancel"/>
Пароль	<input type="password"/>	

Рисунок 1

Для резервного копирования клиент должен быть авторизован администратором RuBackup (рисунок 2).

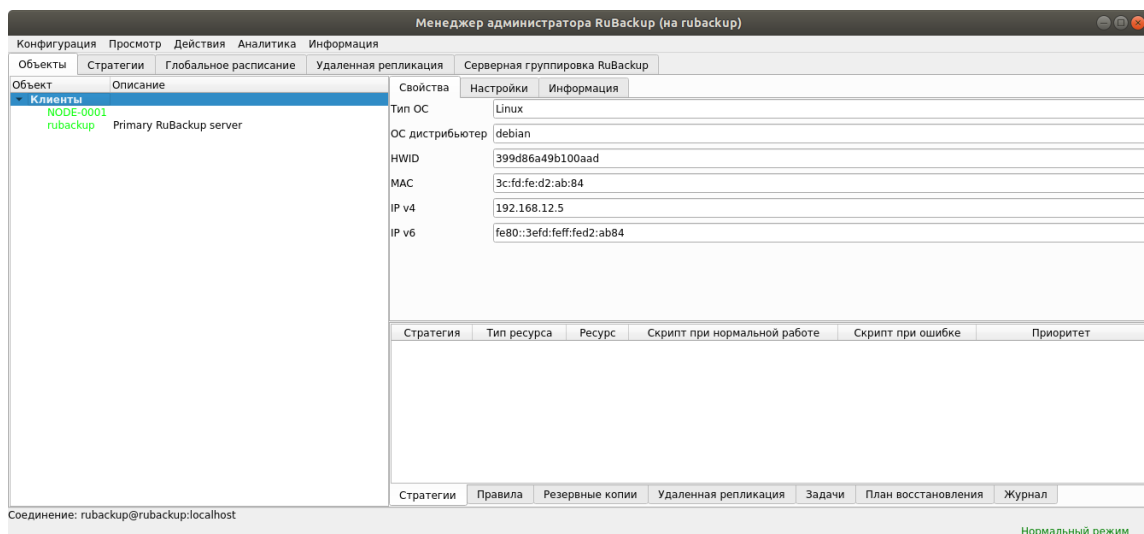


Рисунок 2

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 3):

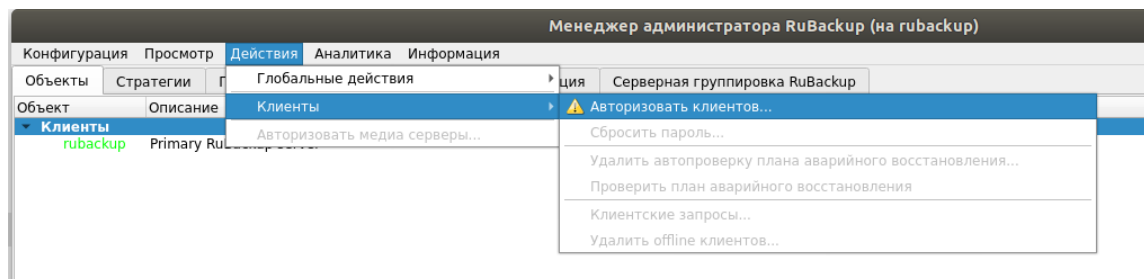


Рисунок 3

2. Выберите нужного неавторизованного клиента и нажмите **Авторизовать** (рисунок 4):

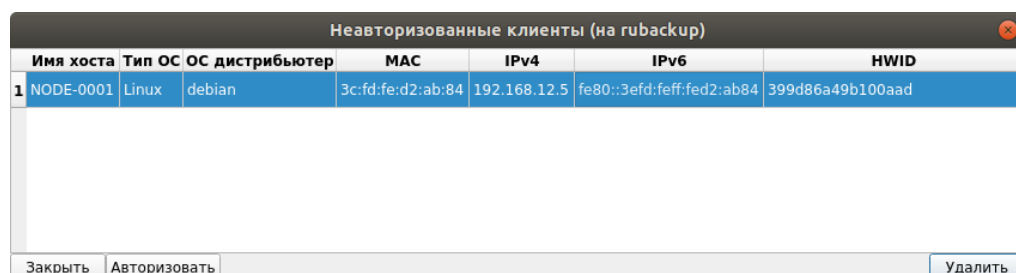


Рисунок 4

После авторизации новый клиент будет виден в главном окне RBM (рисунок 5):

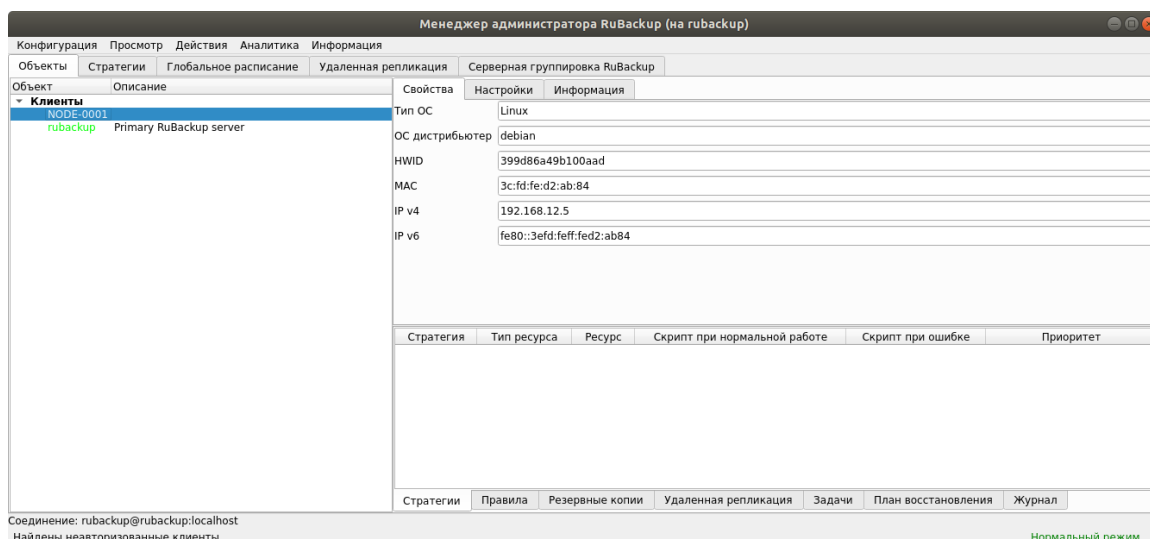


Рисунок 5

Чтобы выполнять регулярное резервное копирование виртуальной машины, необходимо создать правило в глобальном расписании (в случае групповых операций можно так же использовать стратегии резервного копирования). Для этого выполните следующие действия:

1. Выберите клиента и добавьте правило резервного копирования (рисунок 6):

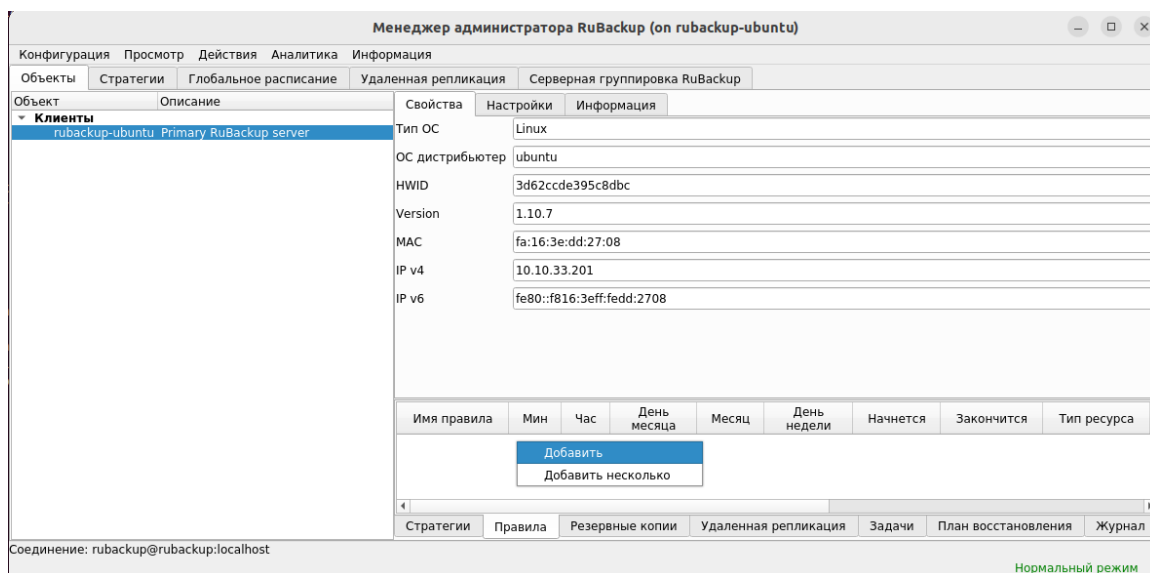


Рисунок 6

2. Выберите тип ресурса: «**RUSTACK**» (рисунок 7):

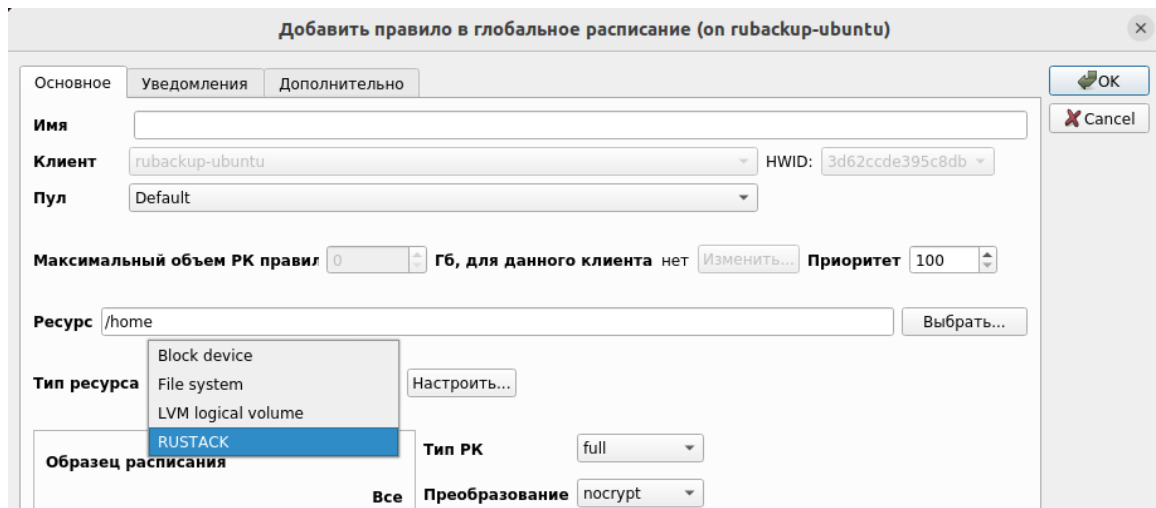


Рисунок 7

3. Выберите ресурс, нажав кнопку **Выбрать** (рисунок 8):

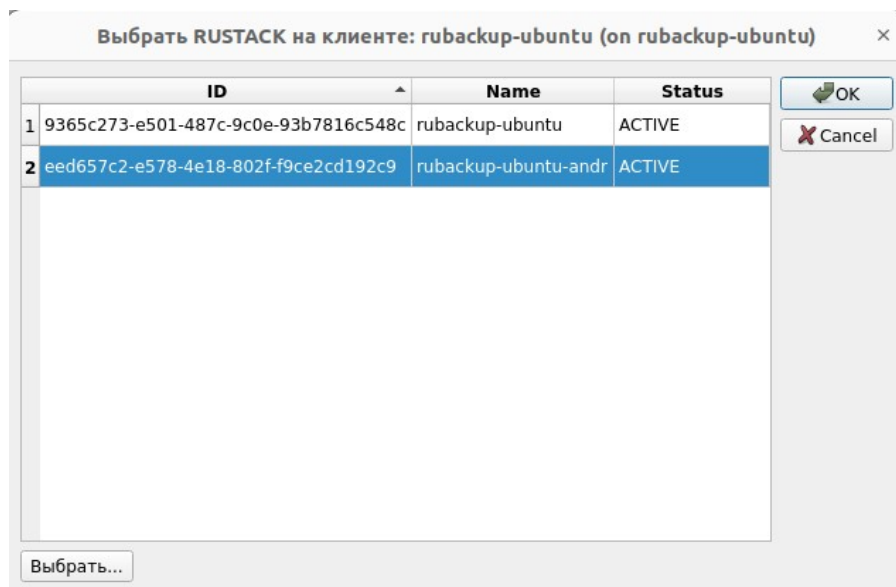


Рисунок 8

4. Установите настройки правила: название правила, пул хранения данных, максимальный объем для резервных копий правила (в ГБ), тип резервного копирования, расписание резервного копирования, срок хранения и необязательный временной промежуток проверки резервной копии (рисунок 9).

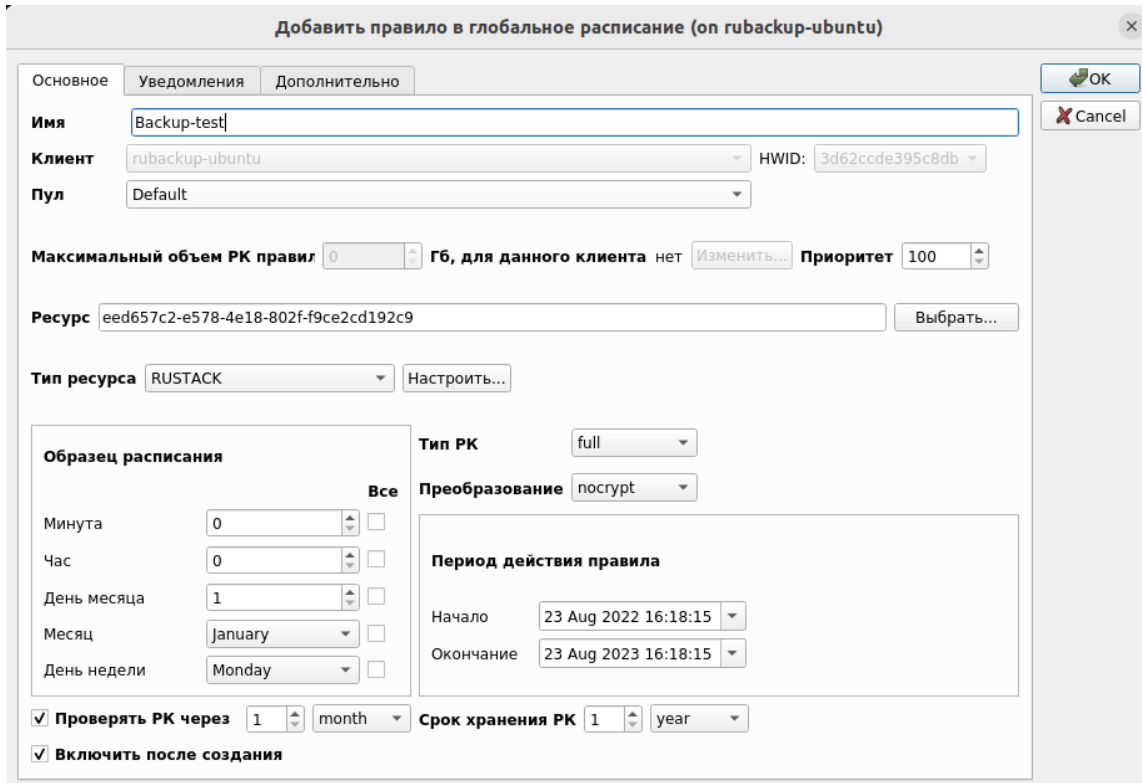


Рисунок 9

При помощи кнопки «Настроить...» можно выполнить тонкие настройки правила резервного копирования, например определить скрипт, который будет выполнен внутри виртуальной машины перед созданием моментального снимка и сразу после его создания. Это может быть необходимо для приведения данных приложения в консистентное состояние, синхронизации кэша и т.п.

Так же внутри виртуальной машины может быть создан скрипт, располагающийся в файле `/opt/rubackup/scripts/rustack.sh`. В том случае, если внутри виртуальной машины существует такой файл с атрибутами на исполнение, то перед созданием моментального снимка он будет выполнен с аргументом `before`, а сразу после создания моментального снимка он будет выполнен с аргументом `after`.

На вкладке «Дополнительно» можно настроить автоматическое удаление устаревших резервных копий, определить условие их перемещения в другой пул и установить разрешение для клиента удалять резервные копии (рисунок 10):

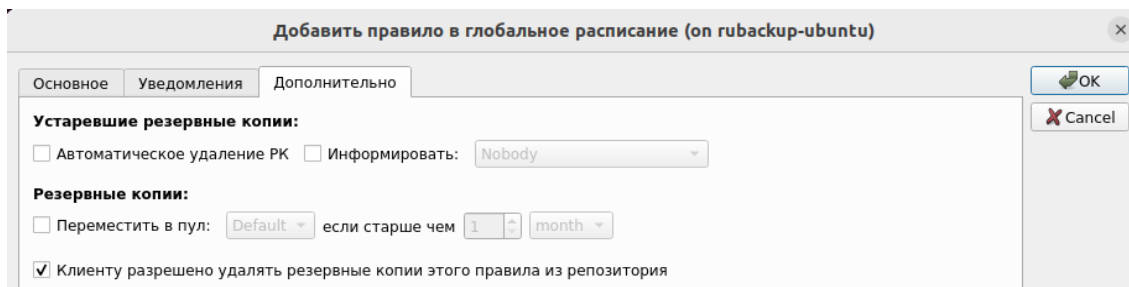


Рисунок 10

Вновь созданное правило будет иметь статус `run`. Если необходимо создать правило, которое пока не должно порождать задач резервного копирования, нужно убрать отметку «Включить после создания». При необходимости, администратор может приостановить работу правила или немедленно запустить его (т.е. инициировать немедленное создание задачи при статусе правила `wait`).

Правила глобального расписания имеют срок жизни, определяемый при их создании, а также предоставляют следующие возможности:

- выполнить защитное преобразование резервной копии на клиенте;
- периодически выполнять проверку целостности резервной копии;
- хранить резервные копии определённый срок, по окончании которого удалять их из хранилища резервных копий и из записей репозитория, либо уведомлять клиента об окончании срока хранения;
- через определённый срок после создания резервной копии автоматически переместить её в другой пул хранения резервных копий, например, на картридж ленточной библиотеки;
- 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 выполнение правил может как администратор (при помощи RBM или утилит командной строки), так и клиент (при помощи RBC или утилиты командной строки `rb_tasks`).

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

# Срочное резервное копирование при помощи RBM

В том случае, если необходимо выполнить срочное резервное копирование созданного правила глобального расписания, то это можно сделать, вызвав правой кнопкой мыши контекстное меню «Выполнить» (рисунок 11):

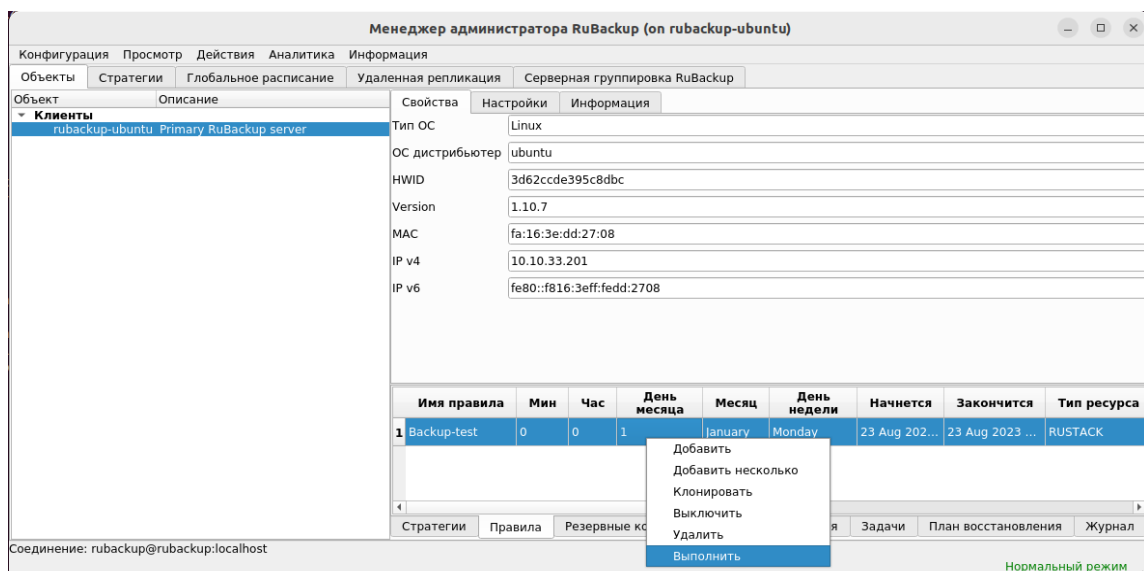


Рисунок 11

Проверить ход выполнения резервного копирования можно в окне «Главная очередь задач» (рисунок 12):

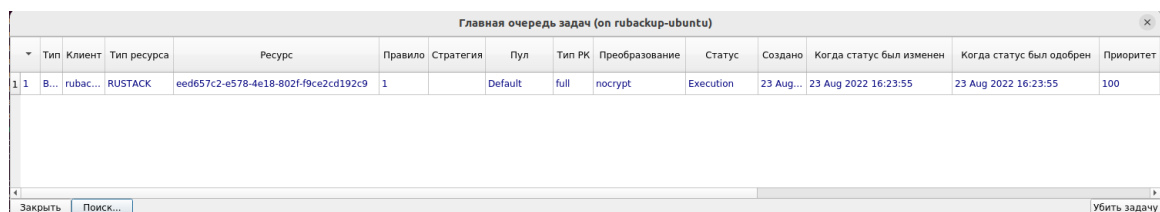


Рисунок 12

При успешном завершении резервного копирования строка копирования будет выделена зеленым цветом (рисунок 13):



Главная очередь задач (on rubackup-ubuntu)															
№	Тип	Клиент	Тип ресурса	Ресурс	Правило	Стратегия	Пул	Тип РК	Преобразование	Статус	Создано	Когда статус был изменен	Когда статус был одобрен	Приоритет	
1	1	В...	rubac...	RUSTACK	eed657c2-e578-4e18-802f-f9ce2cd192c9	1		Default	full	noscrypt	Done	23 Aug...	23 Aug 2022 16:57:28	23 Aug 2022 16:57:28	100

Закреть Поиск... Убить задачу

Рисунок 13

# Централизованное восстановление резервных копий с помощью RBM

Система резервного копирования RuBackup предусматривает возможность восстановления резервных копий как со стороны клиента системы, так и со стороны администратора СРК. В тех случаях, когда централизованное восстановление резервных копий не желательно, например когда восстановление данных является зоной ответственности владельца клиентской системы, эта функциональность может быть отключена на клиенте (см. «Руководство системного администратора RuBackup»).

В тех случаях, когда централизованное восстановление на клиенте доступно, то его можно инициировать, вызвав правой кнопкой мыши контекстное меню «Восстановить» (рисунок 14):

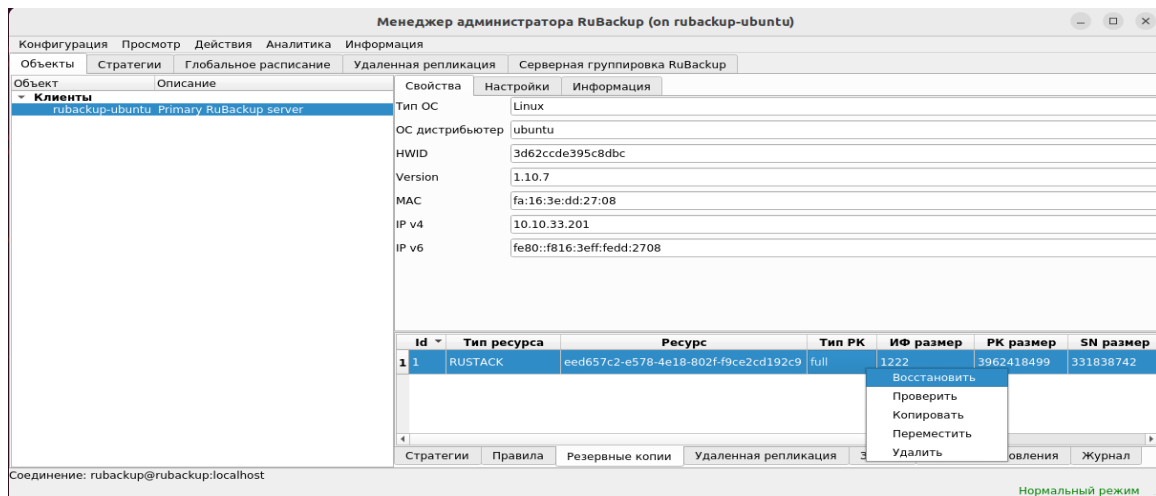


Рисунок 14

В окне централизованного восстановления можно увидеть основные параметры резервной копии и, если это применимо, определить место восстановления резервной копии. В случае восстановления виртуальной машины из резервной копии будет выполнена проверка наличия в среде виртуализации виртуальной машины с таким же именем. Если такой виртуальной машины нет, то будет произведено восстановление с оригинальным именем. Если виртуальная машина с таким именем уже есть, то к имени виртуальной машины будет добавлен цифровой постфикс (рисунок 15).

**Централизованное восстановление (on rubackup-ubuntu)**

**Информация о резервной копии**

Клиент:  HWID:

Ресурс:

Тип ресурса:  Пул:

Создано:

Тип РК:  Цепочка РК:

Имя правила:

Статус:

**Место восстановления**

Восстановить на клиента:  HWID:

Восстановить в:

Гранулярное восстановление

Развернуть, если применимо

Рисунок 15

В том случае, если необходимо восстановить резервную копию в локальный каталог на клиенте без развертывания виртуальной машины в среде виртуализации, то необходимо снять отметку «Развернуть, если применимо».

Проверить ход выполнения восстановления резервной копии можно в окне «Главная очередь задач» (рисунок 16):

Главная очередь задач (on rubackup-ubuntu)

№	Тип	Клиент	Тип ресурса	Ресурс	Правило	Стратегия	Пул	Тип РК	Преобразование	Статус	Создано	Когда статус был изменен	Когда статус был одобрен
1	B...	rubac...	RUSTACK	eed657c2-e578-4e18-802f-f9ce2cd192c9	1		Default	full	noscrypt	Done	23 Aug...	23 Aug 2022 16:57:28	23 Aug 2022 16:57:28
2	R...	rubac...	RUSTACK	eed657c2-e578-4e18-802f-f9ce2cd192c9	1		Default	full	noscrypt	Transmission	23 Aug...	23 Aug 2022 17:05:23	23 Aug 2022 17:05:23

Закорыть    Поиск...    Убить задачу

Рисунок 16

При успешном завершении восстановления виртуальной машины строка ресурса будет выделена зеленым цветом (рисунок 17):

Главная очередь задач (on rubackup-ubuntu)

№	Тип	Клиент	Тип ресурса	Ресурс	Правило	Стратегия	Пул	Тип РК	Преобразование	Статус	Создано	Когда статус был изменен	Когда статус был одобрен
1	B...	rubac...	RUSTACK	eed657c2-e578-4e18-802f-f9ce2cd192c9	1		Default	full	noscrypt	Done	23 Aug...	23 Aug 2022 16:57:28	23 Aug 2022 16:57:28
2	R...	rubac...	RUSTACK	eed657c2-e578-4e18-802f-f9ce2cd192c9	1		Default	full	noscrypt	Done	23 Aug...	23 Aug 2022 17:14:25	23 Aug 2022 17:14:25

Закорыть    Поиск...    Убить задачу

Рисунок 17

## Восстановление со стороны клиента

В случае необходимости восстановления резервной копии со стороны клиента вы можете воспользоваться утилитой командной строки `rb_archives`:

Просмотр списка доступных резервных копий:

```
root@rubackup-ubuntu:~# rb_archives
Id | Ref ID | Resource | Resource type | Backup type | Created | Crypto | Signed | Status
-----+-----+-----+-----+-----+-----+-----+-----+-----
1 | | eed657c2-e578-4e18-802f-f9ce2cd192c9 | RUSTACK | full | 2022-08-23 16:57:08+03 | nocrypt | True | Not Verified
2 | 1 | eed657c2-e578-4e18-802f-f9ce2cd192c9 | RUSTACK | incremental | 2022-08-23 17:49:47+03 | nocrypt | True | Not Verified
```

Запрос на восстановление резервной копии:

```
root@rubackup-ubuntu:~# rb_archives -X 2
Password:
The archive will be restored in the directory: /rubackup-tmp
----> Restore archive chain: 1 2 < ----
Record ID: 1 has status: Not Verified
Continue (y/n)? yes
Record ID: 2 has status: Not Verified
Continue (y/n)? yes
TASK WAS ADDED TO QUEUE:4 5
```

В том случае, если резервная копия должна быть развернута, т. е. необходимо восстановить виртуальную машину в среду виртуализации, то необходимо использовать опцию `-x`, в том случае когда требуется восстановить резервную копию в локальном каталоге клиента без развертывания, нужно использовать опцию `-X`.