

**RuBackup**

Система резервного копирования и восстановления данных

# Резервное копирование программного комплекса средств виртуализации «Брест»



Версия 1.9

2022 г.

## Содержание

Введение.....	3
Перед установкой.....	5
Установка клиента RuBackup.....	5
Мастер-ключ.....	8
Удаление клиента RuBackup.....	9
Подготовка виртуальной машины ПК «Брест» для выполнения резервного копирования средствами RuBackup.....	10
Защитное преобразование резервных копий.....	12
Локальный лист ограничений.....	14
Использование оконного менеджера администратора RuBackup.....	15
Использование клиентского менеджера RuBackup.....	31
Утилиты командной строки клиента RuBackup.....	37
Восстановление резервной копии виртуальной машины.....	39

# Введение

Система резервного копирования RuBackup позволяет выполнять резервное копирование шаблонов (*template*) и виртуальных машин программного комплекса «Брест».

Для шаблонов доступно полное резервное копирование, для виртуальных машин – полное, инкрементальное и дифференциальное. Резервное копирование виртуальных машин может происходить 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, измененные со времени выполнения предыдущего полного резервного копирования.

**Инкрементальное резервное копирование** сохраняет только данные, измененные 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 ПК «Брест» на хост *front* требуется установить клиента RuBackup и модули *brst\_template*, *brst\_vm*. На виртуальные машины, для которых предполагается выполнять резервное копирование, 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 «Брест», но в этом случае выполняется полное резервное копирование выбранного ресурса. Так же клиенту может быть доступно локальное расписание, если это разрешено администратором системы резервного копирования.

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 копию выбранным алгоритмом (см. раздел «Защитное преобразование резервных копий»).

Резервное копирование шаблона может быть выполнено как только для его конфигурации, так и совместно с образами, ассоциированными с шаблоном. В ходе выполнения резервного копирования шаблона используется технология клонирования.

Резервное копирование виртуальной машины возможно в трех вариантах:

1) резервное копирование только конфигурации виртуальной машины. При восстановлении такой резервной копии виртуальная машина будет создана точно такой, какой она создается из шаблона. Восстановить такую резервную копию можно только в том случае, если в системе присутствуют образы, которыми она должна пользоваться;

2) резервное копирование конфигурации и частных данных виртуальной машины, которые образовались с момента ее создания. Восстановить такую резервную копию можно только в том случае, если в системе присутствуют образы, которыми она должна пользоваться;

3) резервное копирование конфигурации, частных данных виртуальной машины и образов, которые она использует.

В ходе выполнения резервного копирования виртуальной машины используется технология создания моментальных снимков дисков 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. Количество дисков в виртуальной машине может быть больше одного, в этом случае резервное копирование выполняется для всех дисков.

Для выполнения резервного копирования работающей виртуальной машины на ней должны быть установлены гостевые расширения, а так же при ее создании в ПК «Брест» необходимо включить функцию *QEMU guest agent communication* (это может быть включено как для всего ПК «Брест», так и для отдельного шаблона из которого создаются виртуальные машины). Без гостевых расширений резервное копирование возможно только для выключенных виртуальных машин.

## Перед установкой

Перед установкой клиента RuBackup в системе должны быть установлены необходимые утилиты (см.раздел «Подготовка к установке клиента» в документе «Руководство по установке серверов резервного копирования и Linux клиентов RuBackup»).

## Установка клиента RuBackup

Для резервного копирования ПК «Брест» необходимы следующие пакеты:

`rubackup-common_signed.deb`

`rubackup-client-brest_signed.deb` – клиент резервного копирования;

`rubackup-brest_signed.deb` – модули резервного копирования.

Установка пакетов клиента RuBackup производится из-под учетной записи с административными правами на узел front ПК «Брест» при помощи следующих команд:

```
# dpkg -i rubackup-common_signed.deb
```

```
# dpkg -i rubackup-client_signed.deb
```

```
# dpkg -i rubackup-brest_signed.deb
```

```
root@srv:~# dpkg -i gubackup-client-brest_signed.deb
Выбор ранее не выбранного пакета gubackup-client-brest.
(Чтение базы данных ... на данный момент установлено 137286 файлов и каталогов.)
Подготовка к распаковке gubackup-client-brest_signed.deb ...
Распаковывается gubackup-client-brest (2020-04-22) ...
Настраивается пакет gubackup-client-brest (2020-04-22) ...
root@srv:~# dpkg -i gubackup-brest_signed.deb
Выбор ранее не выбранного пакета gubackup-brest.
(Чтение базы данных ... на данный момент установлено 137334 файла и каталога.)
Подготовка к распаковке gubackup-brest_signed.deb ...
Распаковывается gubackup-brest (2020-04-22) ...
Настраивается пакет gubackup-brest (2020-04-22) ...
root@srv:~#
```

## Настройка клиента с помощью интерактивной утилиты `rb_init`

Порядок настройки клиента с помощью интерактивной утилиты `rb_init` изложен в документе «Руководство по установке серверов резервного копирования и Linux клиентов RuBackup».

При установке клиента RuBackup в ОС Astra Linux 1.6 Смоленск с активированным режимом защитной программной среды, необходимо:

1. Выполнить команду

```
# sudo update-initramfs -u -k all
```

2. Перезагрузить операционную систему

```
# sudo init 6
```

## Компрессор `pigz`

Необходимо сделать символическую ссылку для имитации наличия в ОС компрессора `pigz` (это аналог `gzip`, но использующий в работе несколько ядер процессора):

```
# ln -s /bin/gzip /usr/bin/pigz
```

## Настройка SSH доступа

На фронте необходимо обеспечить беспарольный доступ для пользователя root с узла **front** `root@srv.brest.loc` на узлы с гипервизором

```
root@srv.brest.loc# ssh-keygen -t rsa
```

```
root@srv.brest.loc# cat /root/.ssh/id_rsa.pub
```

Этот публичный ключ нужно добавить в файл `~/.ssh/authorized_keys` на узлах с гипервизором для пользователя **brestdadmin**.

# Мастер-ключ

В ходе инсталляции будет создан мастер-ключ для защитного преобразования резервных копий и ключи для электронной подписи, если электронную подпись предполагается использовать.

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

**Важно!** Ключи рекомендуется после создания скопировать на внешний носитель, а так же распечатать бумажную копию и убрать эти копии в надежное место.

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

```
brestadmin@srv:~$ hexdump /opt/rubackup/keys/master-key
00000000 e973 053d 10a1 c0c1 40e8 d332 9463 a7ee
00000010 8965 f275 d5e4 a04a d07d a625 d4e8 755f
00000020
```

# Удаление клиента RuBackup

Порядок действий при удалении клиента RuBackup изложен в документе «Руководство по установке серверов резервного копирования и Linux клиентов RuBackup».

После удаления клиента RuBackup в ОС Astra Linux 1.6 Смоленск с активированным режимом защитной программной среды, необходимо:

1. Выполнить команду

```
# sudo update-initramfs -u -k all
```

2. Перезагрузить операционную систему

```
# sudo init 6
```

# Подготовка виртуальной машины ПК «Брест» для выполнения резервного копирования средствами RuBackup

Для шаблона, на базе которого будут создаваться виртуальные машины, необходимо включить возможность взаимодействия с гостевыми дополнениями (рисунок 1):

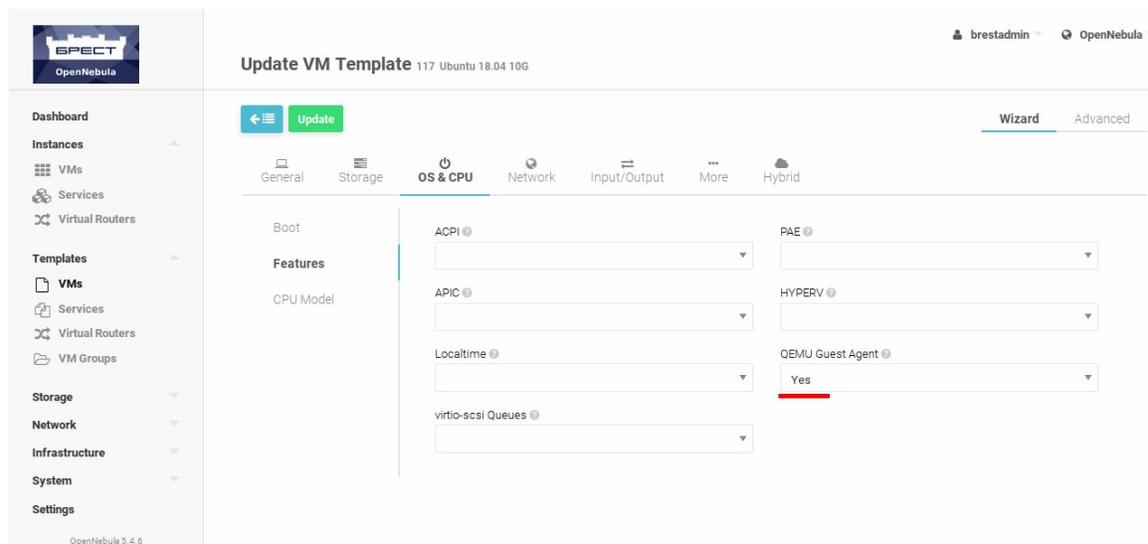


Рисунок 1

## Linux

В операционной системе виртуальной машины необходимо установить пакет `qemu-guest-agent`.

```
# apt-get install qemu-guest-agent
```

или

```
# yum install qemu-guest-agent
```

в зависимости от типа операционной системы.

### Для Astra Linux Смоленск:

Необходимо использовать диск разработки и добавить соответствующий iso image в операционную систему виртуальной машины как виртуальный CDROM.

После этого необходимо выполнить следующие команды:

```
# sudo apt-cdrom add
```

```
# sudo apt update
```

```
# sudo apt install qemu-guest-agent
```

Хранилища данных (Datastores) — служат для хранения базовых образов виртуальных машин.

Поддерживаемые типы хранилищ ПК СВ «Брест» и их характеристики представлены в таблице 1.

Таблица 1 – Поддерживаемые типы хранилищ ПК СВ «Брест»

Тип хранилища	Тип системы	Состав	Примечание
OCFS2	файловая	модуль ядра и userspace инструментарий для работы с ФС	может быть развернуто совместно с DRBD
Ceph	распределенная	хранилище system хранилище images	может быть использовано для предоставления доступа к создаваемым в нем блочным устройствам RBD

# Защитное преобразование резервных копий

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

Ключ для преобразования резервных копий располагается на клиенте в файле `/opt/rubackup/keys/master-key`. Пользователь сам должен задать ключ длиной 256 бит (32 байта).

Преобразование осуществляется специальной утилитой преобразования `rbcrypt`. Автоматическое защитное преобразование и обратное преобразование резервных копий клиентом RuBackup возможны при помощи ключей длиной 256 бит, однако утилита `rbcrypt` поддерживает ключи длиной 128, 256, 512 и 1024 бита (в зависимости от выбранного алгоритма). 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. Выполнить 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 еще раз автоматически с использованием мастер-ключа.

Доступные для выполнения преобразования алгоритмы представлены в таблице 2.

Таблица 2 – Алгоритмы преобразования

<b>Наименование алгоритма</b>	<b>Поддерживаемая rbcсупт длина ключа, бит</b>	<b>Примечание</b>
Anubis	128, 256	
Aria	128, 256	
CAST6	128, 256	
Camellia	128, 256	
Kalyна	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	Chinese national standard for Wireless LAN
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. Листы ограничений располагаются в файлах

```
/opt/rubackup/etc/rubackup_restriction.list.brest_vm
```

```
/opt/rubackup/etc/rubackup_restriction.list.brest_template
```

Наименование ресурса (ID виртуальной машины или шаблона), 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).

По умолчанию в предустановленных пакетах нет вышеуказанных файлов. При необходимости использовать листы ограничений их необходимо создать из-под учетной записи с административными привилегиями.

# 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:

Вариант 1:

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

Вариант 2:

```
# ssh -X root@you_rubackup_server
```

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

В том случае, если клиент RuBackup был установлен, но не авторизован, в нижней части окна RBM будет сообщение о том, что найдены неавторизованные клиенты (рисунок 2).

Все новые клиенты должны быть авторизованы в системе резервного копирования (рисунок 3).

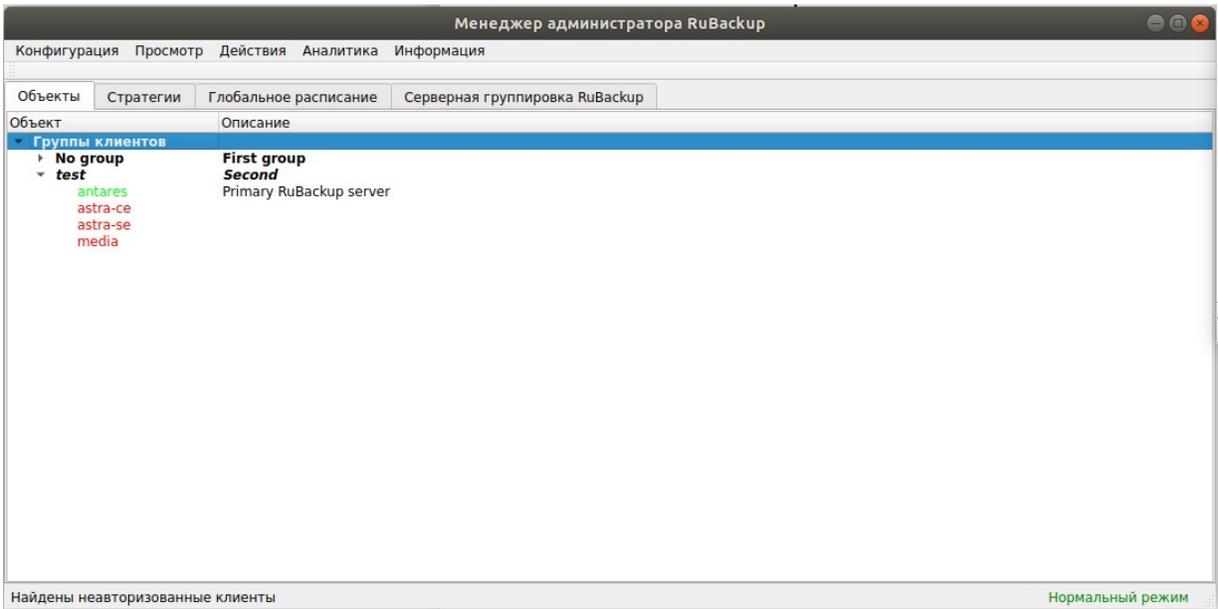


Рисунок 2

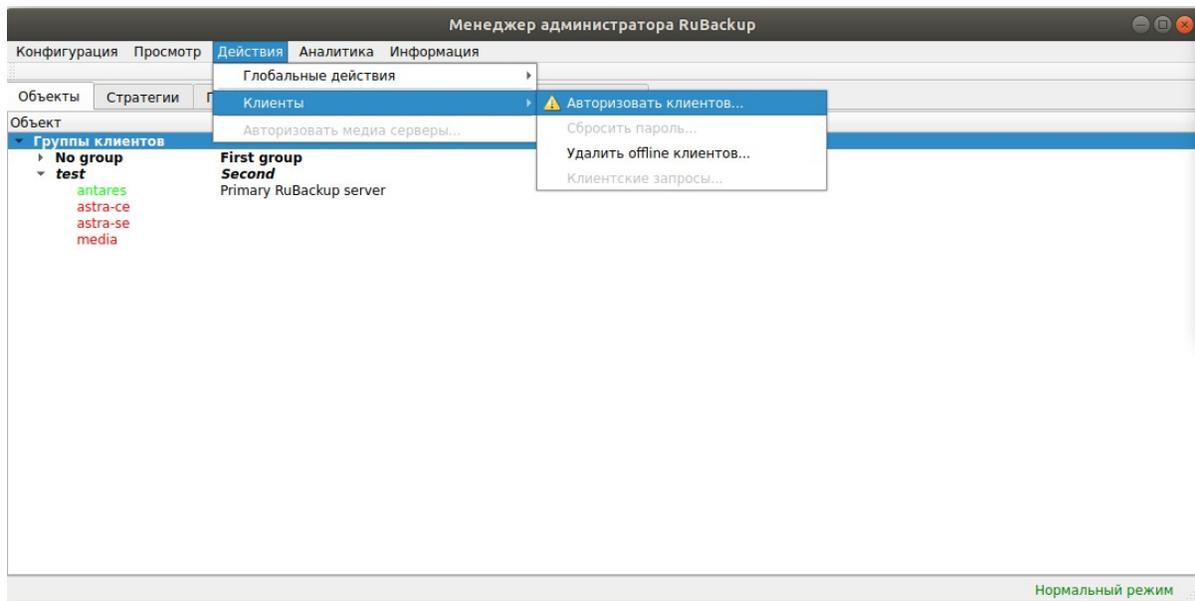


Рисунок 3

Неавторизованные клиенты будут видны в окне (рисунок 4).

Неавторизованные клиенты						
Имя хоста	Тип ОС	ОС дистрибьютер	MAC	IPv4	IPv6	Последний раз на связи
1	srv.brest.loc	Linux	astra	52:54:00:6c:7c:3b	10.49.1.10	23.04.2020 16:01

Закреть    Авторизовать    Удалить

Рисунок 4

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

Менеджер администратора RuBackup	
Объекты	Стратегии
Объект	Описание
<ul style="list-style-type: none"> <li>Группы клиентов <ul style="list-style-type: none"> <li><b>No group</b> <ul style="list-style-type: none"> <li>redos.rubackup.local</li> <li>srv.brest.loc</li> </ul> </li> <li><b>test</b> <ul style="list-style-type: none"> <li>antares</li> <li>astra-ce</li> <li>astra-se</li> <li>media</li> </ul> </li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li><b>First group</b></li> <li><b>Second</b> Primary RuBackup server</li> </ul>

Нормальный режим

Рисунок 5

Клиенты могут быть сгруппированы администратором по какому-либо общему признаку. В случае необходимости восстанавливать резервные копии на другом хосте клиенты должны принадлежать к разделяемой группе (такая группа отмечается шрифтом *italic*). Например, если в такую группу включить два сервера front двух разных ПК «Брест», то можно реплицировать между ними шаблоны и виртуальные машины или переносить их с одного комплекса на другой. Перевести клиента из одной группы в другую можно следующим образом (рисунок 6):

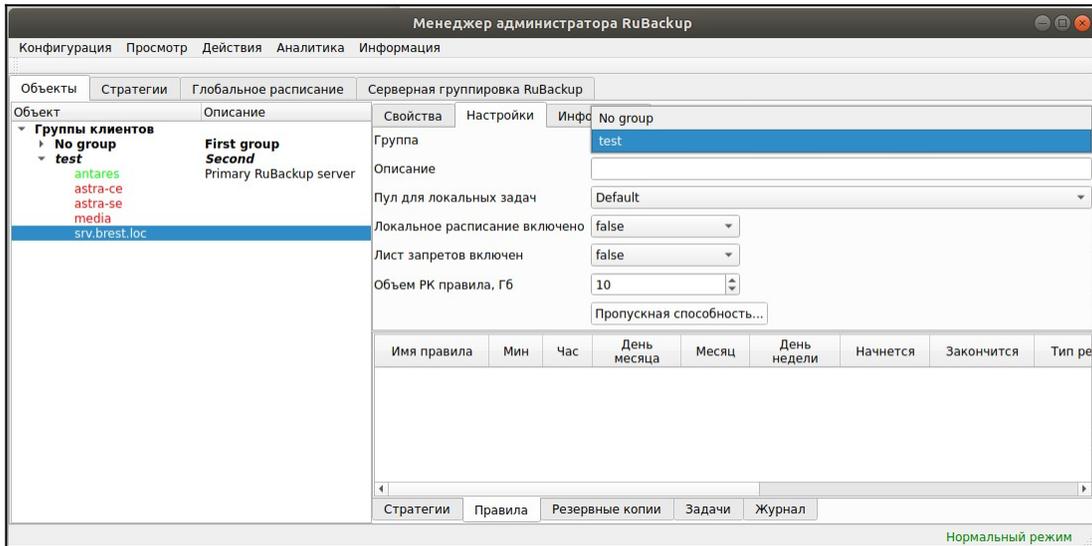


Рисунок 6

Для того, чтобы выполнять регулярное резервное копирование шаблона или виртуальной машины, необходимо создать правило в глобальном расписании.

Выберите клиентский хост, на котором установлен *front* ПК «Брест» и добавьте правило резервного копирования (рисунок 7):

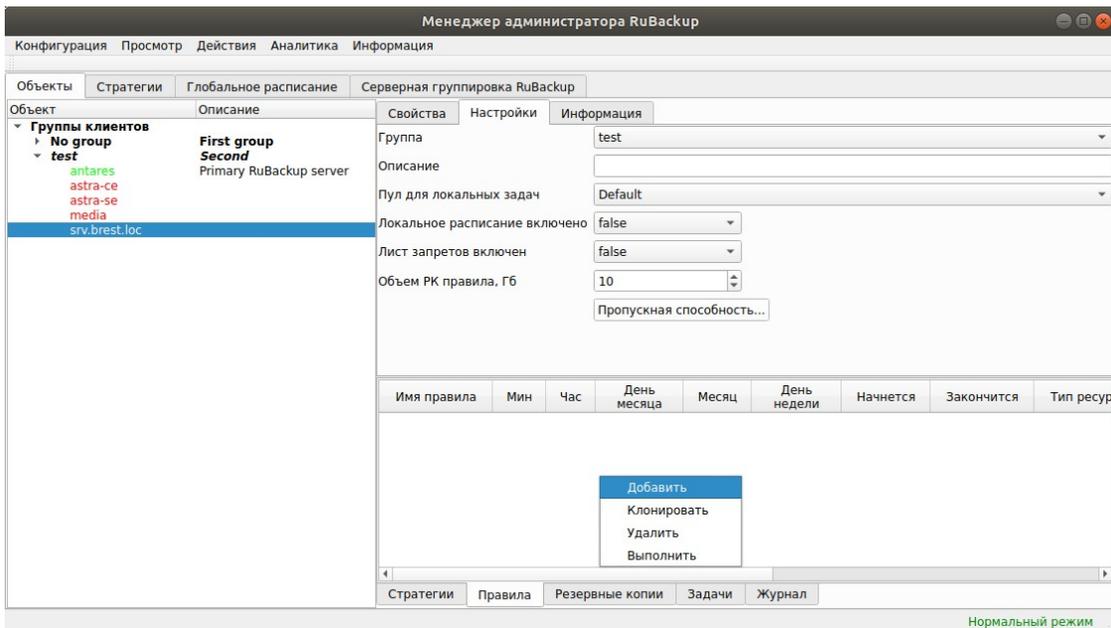


Рисунок 7

Выберите тип ресурса «*Brest VM*» для виртуальных машин или «*Brest template*» для шаблона (рисунок 8).

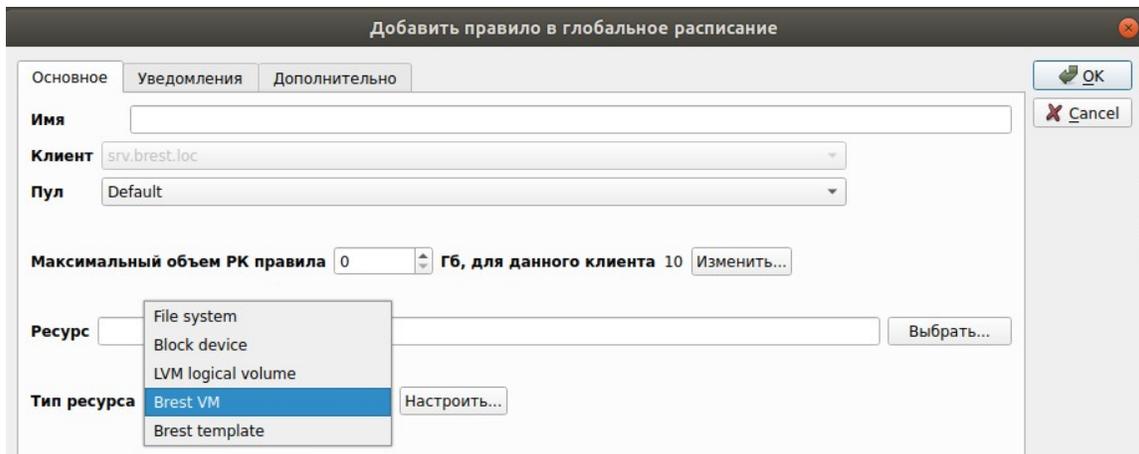


Рисунок 8

Выберите ресурс, для которого будет выполняться правило (рисунок 9).

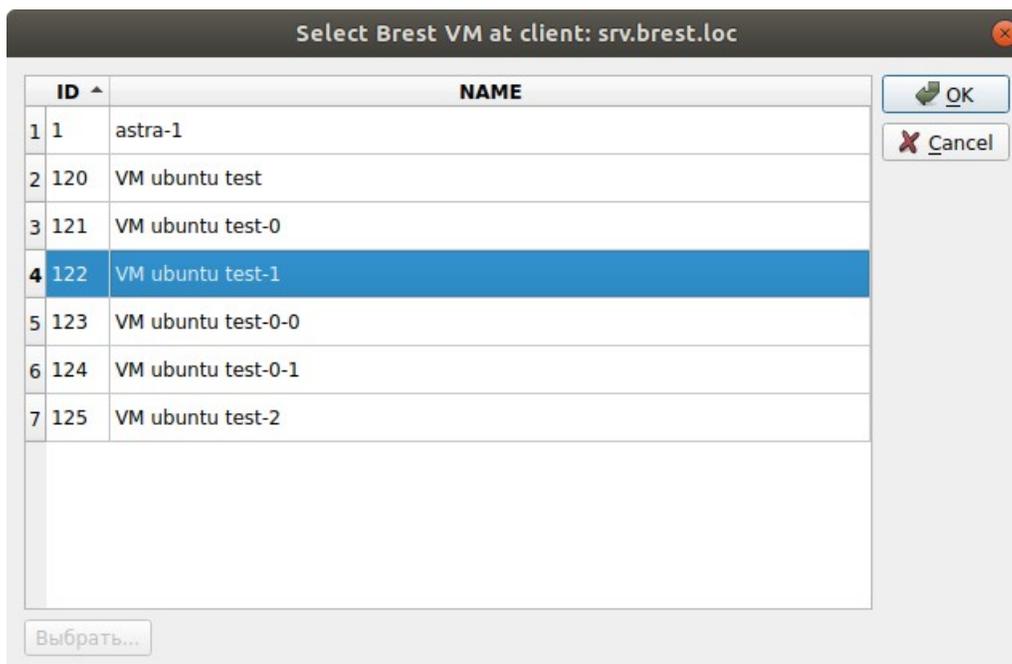


Рисунок 9

Установите прочие настройки: расписание резервного копирования, тип резервного копирования, максимальный объем для резервных копий данного правила, срок хранения, через какой промежуток времени требуется выполнить проверку резервной копии (рисунок 10).

**Добавить правило в глобальное расписание**

Основное    Уведомления    Дополнительно

**Имя**    Резервное копирование виртуальной машины ПК Брест

**Клиент**    srv.brest.loc

**Пул**    Default

**Максимальный объем РК правила**    50    Гб, для данного клиента    100    Изменить...

**Ресурс**    1    Выбрать...

**Тип ресурса**    Brest VM    Настроить...

**Образец расписания**

Минута    0   

Час    0   

День месяца    1   

Месяц    January   

День недели    Sunday

**Тип РК**    full

**Преобразование**    nocrypt

**Период действия правила**

Начало    23.04.2020 16:18

Окончание    23.04.2021 16:18

Проверять РК через    1    month    **Срок хранения РК**    3    month

OK    Cancel

Рисунок 10

Правила для выполнения резервных копий виртуальных машин могут иметь дополнительные настройки (рисунок 11, таблица 3).

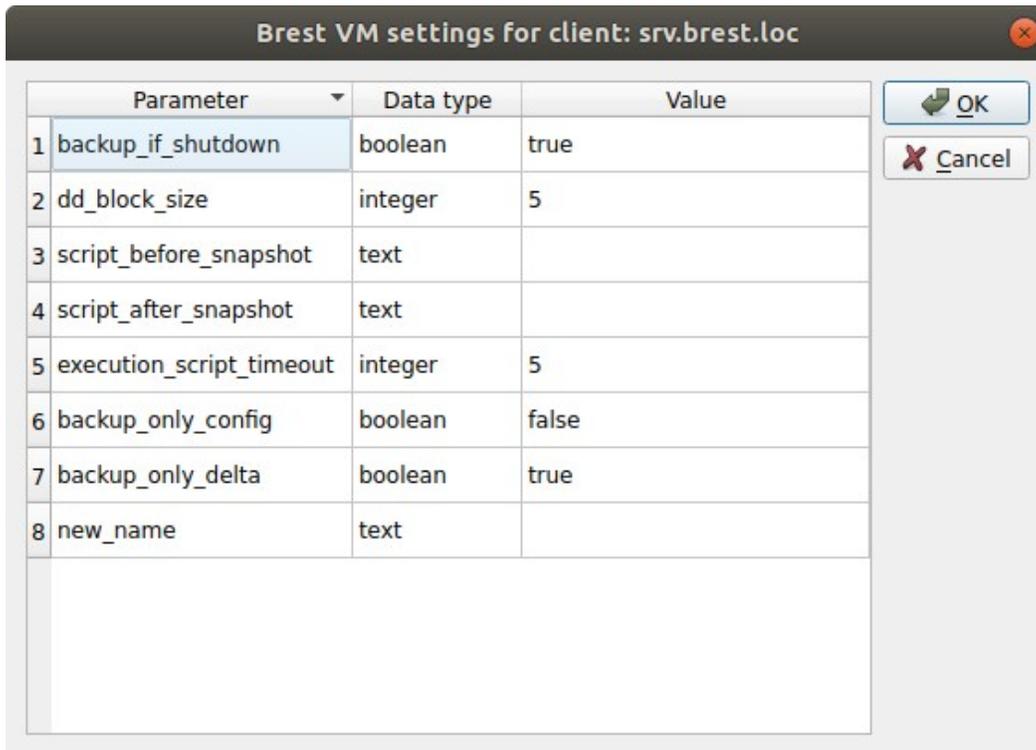


Рисунок 11

Таблица 3 – Значения параметров виртуальных машин

Параметр	Описание	Значение по умолчанию	Допустимые значения
backup_if_shutdown	Выполнять ли резервное копирование если ВМ выключена	true	true, false
dd_block_size	Размер блока в Мб для операций DD	5	>=1
script_before_snapshot	Скрипт внутри ВМ, который будет выполнен перед операцией мгновенного снимка		
script_after_snapshot	Скрипт внутри ВМ, который будет выполнен после операции мгновенного снимка		
execution_script_timeout	Период в секундах в течение которого скрипт должен быть завершен. Если скрипт не будет	5	>=1

Параметр	Описание	Значение по умолчанию	Допустимые значения
	завершен, операция резервного копирования будет прервана		
backup_only_config	Выполнять резервное копирование только конфигурации VM. В данном случае всегда выполняется полное резервное копирование. В случае true перекрывает значение параметра backup_only_delta	false	true, false
backup_only_delta	В случае true выполняет резервное копирование только частных данных виртуальной машины, которые появились после ее создания, данные из образов в резервную копию не попадают. В случае false резервная копия будет выполнена в том числе для образов виртуальной машины, исключая CDROM	true	true, false
new_name	Имя, с которым создавать виртуальную машину при восстановлении из резервной копии. В том случае, если этот параметр пуст, то виртуальная машина будет создана с прежним именем. Если такое имя уже есть в системе, то к нему будет добавлено число.		

В том случае, если дополнительными настройками не заданы скрипты, которые могли бы выполняться в виртуальной машине, но в ней существует исполняемый скрипт `/opt/rubackup/scripts/rubackup-brest.sh`, то перед выполнением моментального снимка он будет выполнен с параметром `before`, а после выполнения моментального снимка он будет выполнен с параметром `after`.

Правила для выполнения резервных копий шаблонов могут иметь дополнительные настройки (рисунок 12, таблица 4).

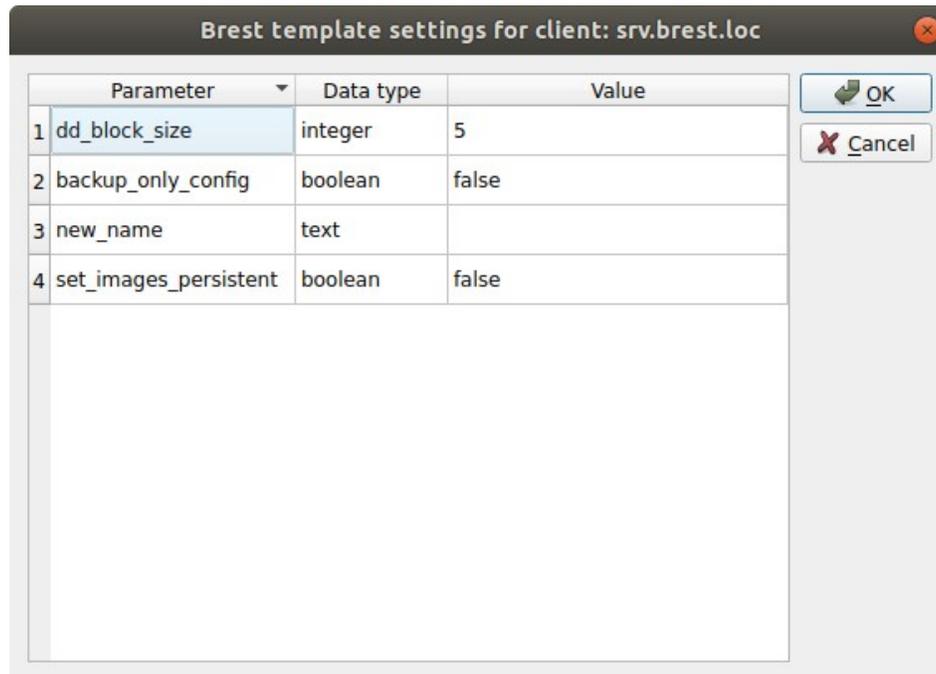


Рисунок 12

Таблица 4 – Значения параметров резервных копий шаблонов

Параметр	Описание	Значение по умолчанию	Допустимые значения
dd_block_size	Размер блока в Мб для операций DD	5	>=1
backup_only_config	Выполнять резервное копирование только конфигурации шаблона, без ассоциированных с ним образов	false	true, false
new_name	Имя, с которым создавать шаблон при восстановлении из резервной копии. В том случае, если этот параметр пуст, то шаблон будет создан с прежним именем. Если такое имя уже есть в системе, то к нему будет добавлено число.		
set_images_persistent	Установить для всех образов шаблона параметр PERSISTENT=yes после восстановления	false	true, false

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.

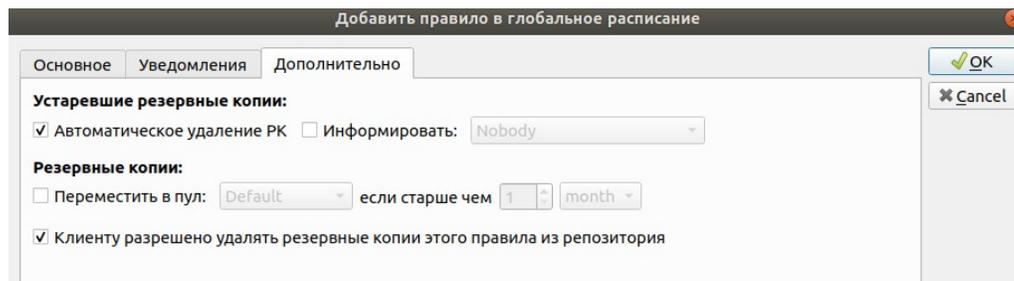


Рисунок 13

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) выполнение скрипта на клиенте (то есть на хосте *front* ПК «Брест») перед началом резервного копирования;
- 2) выполнение скрипта на клиенте после успешного окончания резервного копирования;
- 3) выполнение скрипта на клиенте после неудачного завершения резервного копирования;
- 4) выполнение преобразования резервной копии на клиенте;
- 5) выполнение сжатия резервной копии на клиенте или на сервере после передачи ему резервной копии;
- 6) периодическое выполнение проверки целостности резервной копии;
- 7) хранение резервных копий определенный срок, а после его окончания удаление их из хранилища резервных копий и из записей репозитория, либо простое уведомление пользователей системы резервного копирования об окончании срока хранения;

8) автоматическое перемещение резервной копии через определенный срок после ее создания в другой пул хранения резервных копий, например, на картридж ленточной библиотеки;

9) уведомление 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.

# 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 ее 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 ее серверу. В том случае, если действие допустимо, то сервер RuBackup отдаст обратную команду клиенту и/или перенаправит ее 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 в закладке «Задачи»).

Графический интерфейс клиентского менеджера поддерживает русский и английский языки.

Запуск клиентского менеджера (для примера использован хост *front* ПБ «Брест» `srv.brest.loc`):

```
# ssh -X root@srv.brest.loc  
  
# gbc&
```

В том случае, если клиентская операция выполняется впервые, потребуется ввести пароль клиента (рисунок 14). Без ввода пароля получить резервную копию для клиента из хранилища невозможно.

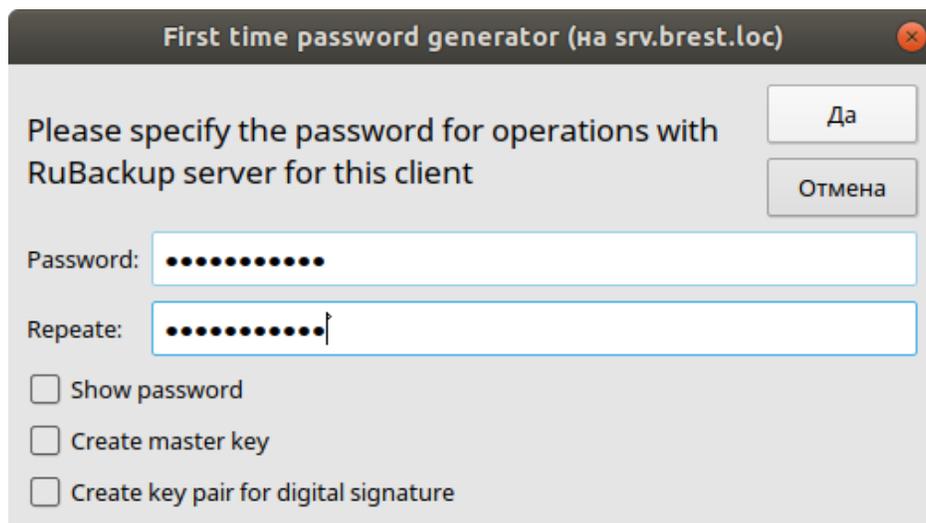


Рисунок 14

В случае успешного выполнения появится окно (рисунок 15).

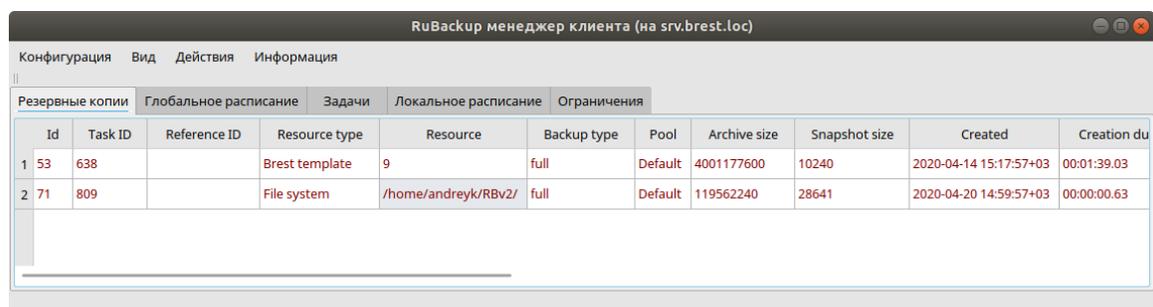


Рисунок 15

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»



The screenshot shows the RuBackup client manager interface. The title bar reads "RuBackup менеджер клиента (на srv.brest.loc)". The main menu includes "Конфигурация", "Вид", "Действия", and "Информация". The "Резервные копии" tab is active, showing a table with the following data:

	Id	Task ID	Reference ID	Resource type	Resource	Backup type	Pool	Archive size	Snapshot size	Created	Creation du
1	53	638		Brest template	9	full	Default	4001177600	10240	2020-04-14 15:17:57+03	00:01:39.03
2	71	809		File system	/home/andreyk/RBV2/	full	Default	119562240	28641	2020-04-20 14:59:57+03	00:00:00.63

Рисунок 16

В таблице вкладки «Резервные копии» (рисунок 16) содержится информация обо всех резервных копиях клиента, которые хранятся в репозитории RuBackup. 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.

Во вкладке «Резервные копии» пользователю доступны следующие действия:

- 1) 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 потребуются вести пароль клиента.

- 2) Восстановить цепочку резервных копий.

Это действие запускает процесс восстановления цепочки резервных копий на локальной файловой системе клиента. При восстановлении резервной копии или цепочки резервных копий пользователь должен выбрать место для восстановления файлов резервной копии. Рекомендуется использовать либо временный каталог для операций с резервными копиями

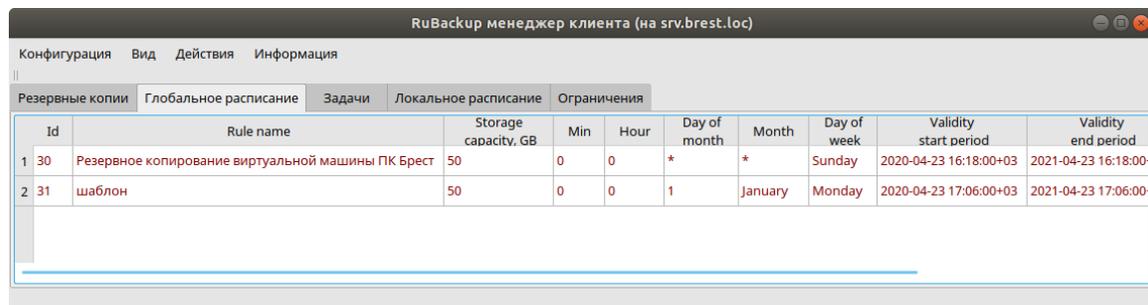
(например, /rubackup-tmp), или SAFE\_DIRS для datastore ПК «Брест» (по умолчанию /var/tmp).

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).

### 3) 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»



The screenshot shows the RuBackup client manager interface. The title bar reads 'RuBackup менеджер клиента (на srv.brest.loc)'. The main menu includes 'Конфигурация', 'Вид', 'Действия', and 'Информация'. Below the menu, there are tabs for 'Резервные копии', 'Глобальное расписание', 'Задачи', 'Локальное расписание', and 'Ограничения'. The 'Глобальное расписание' tab is active, displaying a table with the following data:

Id	Rule name	Storage capacity, GB	Min	Hour	Day of month	Month	Day of week	Validity start period	Validity end period
1 30	Резервное копирование виртуальной машины ПК Брест	50	0	0	*	*	Sunday	2020-04-23 16:18:00+03	2021-04-23 16:18:00
2 31	шаблон	50	0	0	1	January	Monday	2020-04-23 17:06:00+03	2021-04-23 17:06:00

Рисунок 17

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

В закладке «Глобальное расписание» пользователю доступны следующие действия:

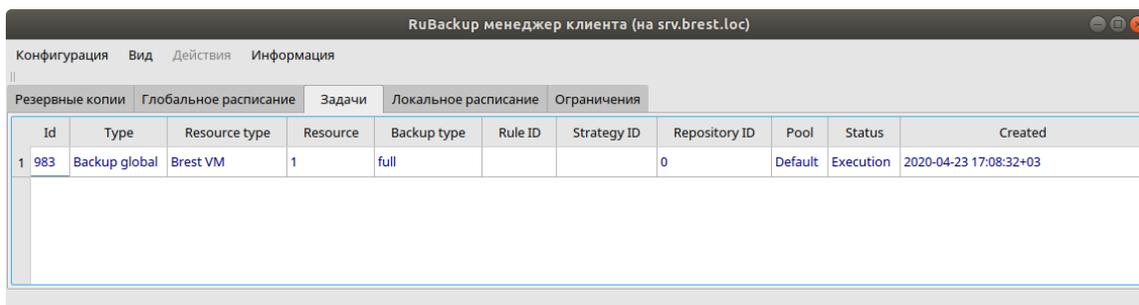
### 1) Запросить новое правило.

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.

2) 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»



Id	Type	Resource type	Resource	Backup type	Rule ID	Strategy ID	Repository ID	Pool	Status	Created
1 983	Backup global	Brest VM	1	full			0	Default	Execution	2020-04-23 17:08:32+03

Рисунок 18

В таблице вкладки «Задачи» (рисунок 18) содержится информация обо всех задачах в главной очереди заданий RuBackup для этого клиента. 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 удаленной 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**»).

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.

```
root@srv:~# rb_archives
```

Id	Ref ID	Resource	Resource type	Backup type	Created	Crypto	Signed	Status
53	9	Brest template	Brest template	full	2020-04-14 15:17:57+03	nocrypt	True	Not Verified
111	117	Brest template	Brest template	full	2020-04-28 13:54:09+03	nocrypt	True	Not Verified
117	131	Brest VM	Brest VM	full	2020-04-28 20:54:42+03	nocrypt	True	Not Verified
134	31	OpenNebula VM	OpenNebula VM	full	2020-04-29 14:16:01+03	nocrypt	True	Not Verified
135	19	OpenNebula template	OpenNebula template	full	2020-04-29 14:18:29+03	nocrypt	True	Not Verified
136	1	Brest VM	Brest VM	full	2020-04-29 19:12:25+03	nocrypt	True	Not Verified
137	131	Brest VM	Brest VM	full	2020-04-30 09:46:47+03	nocrypt	True	Not Verified

```
root@srv:~#
```

### rb\_schedule

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

```
root@srv:~# rb_schedule
```

Id	Name	Resource type	Resource	Backup type	Status
37	Brest template	Brest template	117	full	wait
39	Brest VM test 131	Brest VM	131	full	wait
42	Astra test	Brest VM	1	full	wait

```
root@srv:~#
```

### rb\_tasks

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

```
root@srv:~# rb_tasks
```

Id	Task type	Resource	Backup type	Status	Created
1116	Restore	131	full	Done	2020-04-30 10:03:27+03

```
root@srv:~#
```

## **rbcrypt**

Утилита клиента RuBackup для защитного преобразования файлов на стороне клиента RuBackup.

Более подробно ознакомиться с функциями утилит командной строки можно при помощи команды `man` или в руководстве «Утилиты командной строки RuBackup».

# Восстановление резервной копии виртуальной машины

Восстановление резервной копии с развёртыванием должно выполняться только на тот узел, который является лидером в данный момент.

Узнать статус узлов кластера можно с помощью команды:

```
onezone show 0
```

```
brestadmin@node3:~$ onezone show 0
ZONE 0 INFORMATION
-----
ID          : 0
NAME       : OpenNebula

ZONE SERVERS
-----
ID  NAME          ENDPOINT
0  node1.brest2.lo http://192.168.10.21:2633/RPC2
1  node2.brest2.lo http://192.168.10.22:2633/RPC2
2  node3.brest2.lo http://192.168.10.23:2633/RPC2

HA & FEDERATION SYNC STATUS
-----
ID  NAME          STATE    TERM    INDEX    COMMIT    VOTE    FED_INDEX
0  node1.brest2.lo follower 310     2678404 2678404  -1     -1
1  node2.brest2.lo follower 310     2678404 2678404  2      -1
2  node3.brest2.lo leader   310     2678404 2678404  2      -1
```

В данном примере лидером является узел **node3.brest2.local** и именно на этом узле необходимо выполнять команды для восстановления.

При восстановлении копии с помощью RBM необходимо будет выбрать этот узел из выпадающего списка «Восстановить на клиента» (рисунок 19).

Централизованное восстановление

**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 19

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

```
root@srv:~# gb_archives
```

Id	Ref ID	Resource	Resource type	Backup type	Created	Crypto	Signed	Status
53	9	Brest template	Brest template	full	2020-04-14 15:17:57+03	nocrypt	True	Not Verified
111	117	Brest template	Brest template	full	2020-04-28 13:54:09+03	nocrypt	True	Not Verified
117	131	Brest VM	Brest VM	full	2020-04-28 20:54:42+03	nocrypt	True	Not Verified
134	31	OpenNebula VM	OpenNebula VM	full	2020-04-29 14:16:01+03	nocrypt	True	Not Verified
135	19	OpenNebula template	OpenNebula template	full	2020-04-29 14:18:29+03	nocrypt	True	Not Verified
136	1	Brest VM	Brest VM	full	2020-04-29 19:12:25+03	nocrypt	True	Not Verified
137	131	Brest VM	Brest VM	full	2020-04-30 09:46:47+03	nocrypt	True	Not Verified

```
root@srv:~#
```

В приведенном примере в системе резервного копирования присутствуют семь резервных копий. Виртуальная машина с идентификатором 131 может быть восстановлена из полной резервной копии с идентификатором 137. Для этого необходимо выполнить команду

```
# gb_archives -x 137
```

В случае успешно принятой задачи команда вернет «ок», а восстановление будет происходить в фоновом режиме.

```

root@srv:~# rb_archives -x 137
Password:
1
Restore archive chain: 137
[RBC] Request to restore next archive(s) ID from repository: 137 to: /root
ok

```

Проконтролировать процесс восстановления можно при помощи `rb_task`:

```

root@srv:~# rb_tasks
Id | Task type | Resource | Backup type | Status | Created
-----+-----+-----+-----+-----+-----
1116 | Restore | 131 | full | Done | 2020-04-30 10:03:27+03
root@srv:~#

```

или при помощи RBC (рисунок 20):

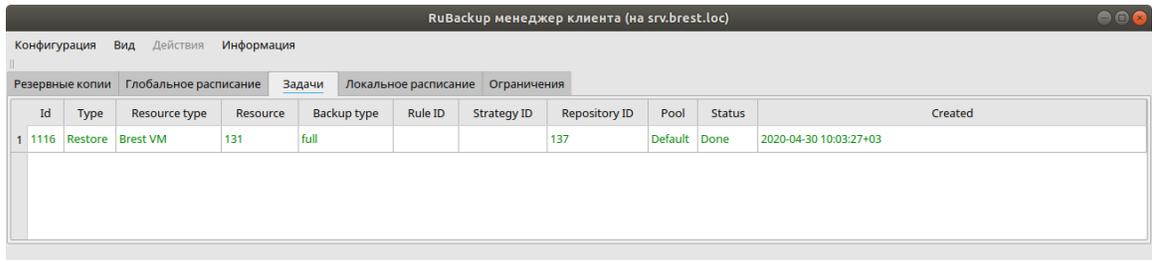


Рисунок 20

Проконтролировать процесс можно при помощи журнала:

```

root@srv:~# tail -f /opt/rubackup/log/RuBackup.log
Thu Apr 30 10:04:14 2020: Virtual machine with name: VM test disk snapshots-3 is exists.
Thu Apr 30 10:04:14 2020: Check new virtual machine name: VM test disk snapshots-4
Thu Apr 30 10:04:14 2020: Virtual machine will be restored with the name: VM test disk snapshots-4
Thu Apr 30 10:04:14 2020: Image: Ubuntu 18.04 10G is exist
Thu Apr 30 10:04:14 2020: Create new virtual machine from: /root/srv.brest.loc_TaskID_1114_RuleID_39_D2020_4_30H09_44_24_BackupType_1_ResourceType_17/vm.xml
Thu Apr 30 10:04:15 2020: Check VM creating...
Thu Apr 30 10:07:56 2020: VM created ID: 143
Thu Apr 30 10:07:56 2020: Restore VM data to: /var/lib/one/datastores/101/143
Thu Apr 30 10:07:56 2020: Required commit for: /root/srv.brest.loc_TaskID_1114_RuleID_39_D2020_4_30H09_44_24_BackupType_1_ResourceType_17/hda.2
Thu Apr 30 10:08:07 2020: Task was done. ID: 1116

```

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.

После выполнения восстановления в ПК «Брест» появилась новая виртуальная машина (ID 143), полностью идентичная той, которая была в системе в момент резервного копирования (рисунок 21):

OpenNebula 5.4.6  
by OpenNebula Systems

VMs

brestadmin OpenNebula

Showing 1 to 4 of 4 entries

4 TOTAL 0 ACTIVE 4 OFF 0 PENDING 0 FAILED

ID	Name	Group	Status	Used CPU	Used Memory	Host	IPs	User Running	MAC	Connection
143	VM test disk snapshots-4	oneadmin	POWEROFF	0	0KB	node1.brest.loc	--	-	-	-
131	VM test disk snapshots	oneadmin	POWEROFF	0.0	0KB	node2.brest.loc	--	-	-	-
120	VM ubuntu test	oneadmin	POWEROFF	0.0	0KB	node1.brest.loc	--	-	-	-
1	astra-1	oneadmin	POWEROFF	0.0	0KB	node2.brest.loc	--	-	-	-

Рисунок 21