



RuBackup

Система резервного копирования
и восстановления данных

МОДУЛЬ ПК СВ «БРЕСТ»

ВЕРСИЯ 2.4.0, 02.04.2025

Содержание

1. Установка клиента RuBackup	4
1.1. Настройка клиента с помощью интерактивной утилиты <code>rb_init</code>	4
1.2. Компрессор <code>pigz</code>	5
1.3. Настройка SSH-доступа	5
1.4. Добавление пользователя <code>root</code> в необходимые группы	5
1.5. Дополнительные настройки ПК СВ «БРЕСТ»	6
1.6. Конфигурационный файл модуля	7
1.7. Параметры конфигурационного файла	9
2. Мастер-ключ	13
3. Удаление клиента RuBackup	14
4. Подготовка виртуальной машины ПК СВ «БРЕСТ» для резервного копирования	15
4.1. Linux	15
4.2. Astra Linux Смоленск	15
5. Алгоритмы защитного преобразования	18
6. Локальный список ограничений	19
7. Использование Менеджера администратора RuBackup (RBM)	20
8. Настройка удаленной репликации	29
9. Использование Менеджера клиента RuBackup (RBC)	35
9.1. Вкладка «Резервные копии»	36
9.2. Вкладка «Глобальное расписание»	38
9.3. Вкладка «Задачи»	38
9.4. Вкладка «Локальное расписание»	39
9.5. Вкладка «Ограничения»	39
10. Утилиты командной строки клиента RuBackup	40
10.1. <code>rb_archives</code>	40
10.2. <code>rb_schedule</code>	40
10.3. <code>rb_tasks</code>	41
10.4. <code>rbcrypt</code>	41
11. Централизованное восстановление резервных копий	42

Система резервного копирования RuBackup позволяет выполнять резервное копирование шаблонов (*template*) и виртуальных машин (VM) Программного комплекса «Средства виртуализации «БРЕСТ» (ПК СВ «БРЕСТ») версии 3.3.1.

Для шаблонов доступно полное резервное копирование, для VM — полное, инкрементальное и дифференциальное. Резервное копирование VM может происходить без их остановки.



Перезагрузка виртуальной машины или гипервизора во время резервного копирования или восстановления может привести к **потере данных виртуальной машины!**

До выполнения с VM или гипервизором работ, влекущих за собой перезагрузку, **убедитесь в отсутствии активных задач резервного копирования или восстановления VM.**

Резервная копия средствами RuBackup позволит избежать полной потери данных VM.

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 СВ «БРЕСТ» на хост фронтальной машины требуется установить клиента RuBackup и модули *rb_module_brest_template*, *rb_module_brest_vm*. На VM, 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 СВ «БРЕСТ», а также 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 RuBackup. Также возможно преобразовать резервные копии с

помощью алгоритма защитного преобразования (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.



Если на базе шаблона создана ВМ, образы, ассоциированные с шаблоном, будут недоступны для клонирования. При желании добавить в таком случае в резервную копию образы рекомендуется использовать модуль `rb_module_brest_vm`.

Резервное копирование ВМ возможно в трех вариантах:

1. резервное копирование только конфигурации ВМ. При восстановлении такой резервной копии ВМ будет создана точно такой, какой она создается из шаблона. Восстановить такую резервную копию можно только в том случае, если в системе присутствуют оригинальные образы, которые были с ней ассоциированы на момент создания резервной копии;
2. резервное копирование конфигурации и частных данных ВМ, которые образовались с момента ее создания. Восстановить такую резервную копию можно только в том случае, если в системе присутствуют образы, которые были ассоциированы с ней на момент создания резервной копии
3. резервное копирование конфигурации, частных данных ВМ и образов, которые она использует.

В ходе выполнения резервного копирования ВМ используется технология создания моментальных снимков дисков ВМ. Перед созданием снимка и сразу после создания снимка, внутри ВМ может быть выполнен скрипт, который обеспечит консистентность данных приложения, функционирующего в ВМ. Количество дисков в ВМ может быть больше одного — в этом случае резервное копирование выполняется для всех дисков. По окончании резервного копирования выполняется финализация моментальных снимков ВМ, а неактуальные файлы снимков удаляются.

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

Глава 1. Установка клиента RuBackup

Для резервного копирования ПК СВ «БРЕСТ» необходимы следующие пакеты:

rubackup-common_signed.deb

rubackup-client_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 фронтальной машины ПК СВ «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 rubackup-client-brest_signed.deb
Выбор ранее не выбранного пакета rubackup-client-brest.
(Чтение базы данных ... на данный момент установлено 137286 файлов и
каталогов.
Подготовка к распаковке rubackup-client-brest_signed.deb ...
Распаковывается rubackup-client-brest (2020-04-22) ...
Настраивается пакет rubackup-client-brest (2020-04-22) ...
```

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

1.1. 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
```

1.2. 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
```

1.3. Настройка SSH-доступа

Необходимо обеспечить беспарольный доступ для пользователя root с узла фронтальной машины `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 пользователей `root`, `brestadmin` и `oneadmin`.

1.4. Добавление пользователя root в необходимые группы

Для того чтобы модуль `rb_module_brest_vm` имел возможность создавать моментальные снимки дисков VM, на узле фронтальной машины и узлах гипервизоров требуется добавить пользователя `root` в группы **astra-console**, **astra-admin**, **kvm**, **libvirt**, **libvirt-qemu**, **libvirt-admin**, **oneadmin**.

```
usermod -a -G astra-console root  
  
usermod -a -G astra-admin root  
  
usermod -a -G kvm root  
  
usermod -a -G libvirt root  
  
usermod -a -G libvirt-qemu root  
  
usermod -a -G libvirt-admin root  
  
usermod -a -G oneadmin root
```

1.5. Дополнительные настройки ПК СВ «БРЕСТ»

В случае если фронтальные машины ПК СВ «БРЕСТ» установлены отдельно от узлов виртуализации, а внутри платформы используются хранилища Ceph, для работы модулей RuBackup необходимо выполнить следующие настройки:

1. Авторизуйтесь под пользователем `root` и установите `ceph-deploy` на каждой фронтальной машине:

```
sudo -i  
apt install ceph-deploy
```

2. Создайте пользователя `ceph-adm` на каждой фронтальной машине:

```
adduser ceph-adm
```



Установите такой же пароль, который вы задали при конфигурации Ceph.

1. Добавьте пользователя в группу `sudoers`:

```
echo "ceph-adm ALL = (root) NOPASSWD:ALL" | sudo tee /etc/sudoers.d/ceph-  
adm chmod 0440 /etc/sudoers.d/ceph-adm pdpl-user -i 127 ceph-adm
```

2. Создайте директорию для хранения `ssh`-ключей пользователя `ceph-adm` на каждой фронтальной машине:

```
su - ceph-adm

ssh localhost
```

3. Авторизуйтесь на узле Ceph-кластера по ssh, переключитесь на пользователя `ceph-adm` и скопируйте ssh-ключи и `authorized_keys` пользователя на все фронтальные машины:

```
ssh <имя ноды Ceph-кластера>

su - ceph-adm

scp /home/ceph-adm/.ssh/id_rsa <имя фронтальной машины>:/home/ceph-
adm/.ssh/

scp /home/ceph-adm/.ssh/authorized_keys <имя фронтальной
машины>:/home/ceph-adm/.ssh/
```

4. Авторизуйтесь под пользователем `ceph-adm` на хосте Ceph-кластера и запустите установку управляющих компонентов на фронтальные машины:

```
su - ceph-adm ceph-deploy --username ceph-adm install --cli <имя
фронтальной машины>

ceph-deploy --username ceph-adm admin <имя фронтальной машины>
```

5. Скопируйте с узла кластера Ceph файл `/etc/ceph/ceph.client.libvirt.keyring` на фронтальные машины:

```
scp /etc/ceph/ceph.client.libvirt.keyring <имя фронтальной
машины>:/etc/ceph/
```

1.6. Конфигурационный файл модуля

В ходе инсталляции пакета модуля в системе будет создан файл настроек `/opt/rubackup/etc/rb_module_brest_vm.conf`.

Содержимое конфигурационного файла

```
# Конфигурационный файл заполняется пользователем вручную
#
```



```
# Символ "#" в начале строки воспринимается как комментарий
# "#" в середине строки воспринимается как значение параметра
# По этой причине не стоит добавлять комментарии на одной строке
# с именем и значением параметра
#
# Хост с Termidesk API
#
#termidesk_url: ~
#
# Версия Termidesk api, например draft, v1, v1.1, v2
#
#termidesk_api_version: ~
#
# Учетные данные администратора Brest для Termidesk api
#
#termidesk_username: ~
#termidesk_password: ~
#
# Время ожидания в секундах с момента запроса на создание VM до ее перехода в
состояние
# "POWEROFF" (8) при восстановлении из РК.
# Значение по умолчанию: 300 секунд
# Минимальное значение: 10 секунд
# Максимальное значение: 900 секунд
vm_state_timeout: 300
#
# Опция актуальна если VM, для которой выполняется резервное копирование:
# - содержит диски на базе LVM-LVM хранилища;
# - расположена на хосте, отличном от того, где запущена процедура бэкапа.
# Возможные значения: yes, no.
# Значение по умолчанию: no.
# Если установлено значение "yes", то диски VM отправляются в РК
# непосредственно с хоста, на котором эта VM расположена, т.е. не происходит
промежуточного
# копирования дисков VM на фронтальный хост, где запущена процедура бэкапа.
# Важно отметить, что при этом недоступны опции защищенного преобразования и
цифровой подписи РК.
#
enable_remote_backup: no
#
# Путь до директории на узле виртуализации, в которой будут создаваться
снэпшоты дисков при бэкапе включенной VM.
# Если установлено значение "vm_path", снэпшоты VM создаются в директории VM
на узле виртуализации: /var/lib/datastores/<id хранилища>/<id VM>/
snapshot_path: vm_path
```

```
#
# Необходимая доля свободного пространства в процентах на диске в директории,
# в которой будут созданы снимки дисков включенной ВМ при ее
резервировании.
free_to_total_storage_space_ratio: 30
#
# Если для опции 'remove_old_snapshots_if_found' установлено значение 'yes',
# и на момент выполнения задачи резервирования ВМ для дисков данной ВМ
обнаружены неактуальные файлы снимков,
# созданные данным модулем, например в случае нештатного завершения
предыдущей задачи резервирования,
# то на текущей итерации бэкапа модуль выполнит удаление неактуальных файлов
снимков.
# В аналогичной ситуации при значении 'no' данного параметра задача
резервирования ВМ завершится с ошибкой.
# Возможные значения: yes, no
# Значение по умолчанию: no
remove_old_snapshots_if_found: no
#
# Если для опции 'commit_old_snapshots_if_found' установлено значение 'yes',
# и на момент выполнения задачи резервирования ВМ обнаружен
нефинализированный снимок ВМ,
# созданный данным модулем, например в случае нештатного завершения
предыдущей задачи резервирования,
# то на текущей итерации бэкапа модуль выполнит финализацию снимка.
# В случае успеха задача резервирования ВМ продолжит свое выполнение.
# Возможные значения: yes, no
# Значение по умолчанию: no
commit_old_snapshots_if_found: no
```

1.7. Параметры конфигурационного файла

- **vm_state_timeout** — параметр восстановления ВМ из резервной копии (см. раздел Централизованное восстановление резервных копий).
- **enable_remote_backup** — параметр ускорения процедуры резервного копирования.

Возможные значения:

- `enable_remote_backup: no` (**значение по умолчанию**)
- `enable_remote_backup: yes`

Параметр предназначен для ускорения процедуры резервного копирования ВМ, в случае если данная ВМ запущена на узле «Брест», отличном от того, на котором

запущена процедура резервного копирования, а диски VM находятся в хранилище типа LVM_LVM.

Чтобы процедура резервного копирования работала корректно для значения `enable_remote_backup: yes`:

1. Настройте для пользователя `root` ssh-доступ с аутентификацией по ключу между узлом, на котором запущена процедура резервного копирования, и узлом, на котором находится VM, для которой нужно осуществить процедуру резервного копирования.
2. На узле с VM, для которой нужно осуществить операцию резервного копирования, нужно установить клиент CPK RuBackup той же версии, что и на узле, с которого будет осуществляться процедура резервного копирования.
3. На узле с VM, для которой нужно осуществить операцию резервного копирования, нужно создать папку в том же месте, которое указано в параметре `use-local-backup-directory` файла `/opt/rubackup/etc/config.file` на узле, с которого осуществляется процедура создания резервной копии.
4. В случае значения опции `enable_remote_backup: yes` для процедуры создания резервной копии будут недоступны операции защищенного преобразования и цифровой подписи PK.
 - `snapshot_path` — параметр задает путь на узле виртуализации, по которому будут создаваться снимки дисков резервируемой VM.
5. Не каждую директорию можно указывать для параметра без предварительной подготовки. Для некоторых директорий следует так же указать путь в файле `/usr/sbin/pdp-init-libvirt` в переменной `LIBVIRT_DIRS`. После того, как директория будет указана, необходимо перезапустить сервис `libvirt` командой: `systemctl restart libvirtd.service`. Для проверки, что все установлено правильно можно выполнить команду: `sudo pdp-ls -Md <path_to_dir>`.

Вывод должен быть такой: `Уровень_3:Высокий:Категория_1,Категория_2,0xffffffffffffffc:ccnr <path_to_dir>`.

Если вывод выглядит так: `Уровень_0:Низкий:Нет:0x0 <path_to_dir>`, то директория не добавлена в список `LIBVIRT_DIRS` или процесс `libvirtd` не перезапущен.

Значение по умолчанию — `vm_path` означает, что снимки создаются в каталоге VM там же, где находятся диски VM. Если задано значение, отличное от значения по умолчанию, и при этом значение не является директорией или указанная директория не существует на момент бэкапа, то задача по созданию PK будет завершаться с ошибкой с соответствующим сообщением в журнале.

- `free_to_total_storage_space_ratio` — параметр соотношения свободного пространства к общему пространству хранения.
 1. Значение параметра должно учитываться при создании снимков дисков

включенной VM при бэкапе. Если в каталоге, определенном с помощью параметра `snapshot_path`, соотношение свободного места к общему размеру места меньше значения, заданного с помощью `free_to_total_storage_space_ratio`, то задача на создание РК завершится с ошибкой с соответствующим сообщением в журнале.

Единица измерения параметра — проценты, Значение по умолчанию — 30 %

Параметры, необходимые для выполнения резервного копирования виртуальных машин «Брест», находящихся в кластере Termidesk:

- `termidesk_url` — адрес хоста с Termidesk API.
 - `termidesk_api_version` — версия Termidesk API.
 - `termidesk_username` — логин администратора Brest для Termidesk API.
 - `termidesk_password` — пароль администратора Brest для Termidesk API.
1. После заполнения данных параметров Вы сможете указать одну из VM Termidesk при выборе ресурса копирования. Процесс восстановления VM в Termidesk также происходит на основе данных из конфигурационного файла модуля.
- `remove_old_snapshots_if_found` - удаление неактуальных снимков состояния (снэпшотов)

Если для параметра `remove_old_snapshots_if_found` установлено значение `yes` и на момент выполнения задачи резервного копирования VM для дисков данной VM обнаружены неактуальные файлы снимков состояния, созданные данным модулем (например, в случае нештатного завершения предыдущей задачи резервного копирования), то в ходе текущего резервного копирования модуль удалит неактуальные снимки состояния.

Если в аналогичной ситуации значение параметра 'no', то задача резервного копирования VM завершится с ошибкой.

Возможные значения:

- `remove_old_snapshots_if_found: no` **(значение по умолчанию)**
- `remove_old_snapshots_if_found: yes`
- `'commit_old_snapshots_if_found'` - финализация снимков состояния (снэпшотов)

Если для опции `commit_old_snapshots_if_found` установлено значение `yes` и на момент выполнения задачи резервного копирования VM обнаружен нефинализированный снимок состояния VM, созданный данным модулем (например, в случае нештатного завершения предыдущей задачи резервного копирования), то в ходе текущего резервного копирования модуль выполнит финализацию снимка состояния.

В случае успеха задача резервирования VM продолжит свое выполнение.

При значении `no` в такой же ситуации задача резервного копирования завершится с ошибкой.

Возможные значения:

- `commit_old_snapshots_if_found: no` **(значение по умолчанию)**
- `commit_old_snapshots_if_found: yes`

Глава 2. Мастер-ключ

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



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



После создания ключи рекомендуется 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:

```
brestadmtn@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
```

Глава 3. 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

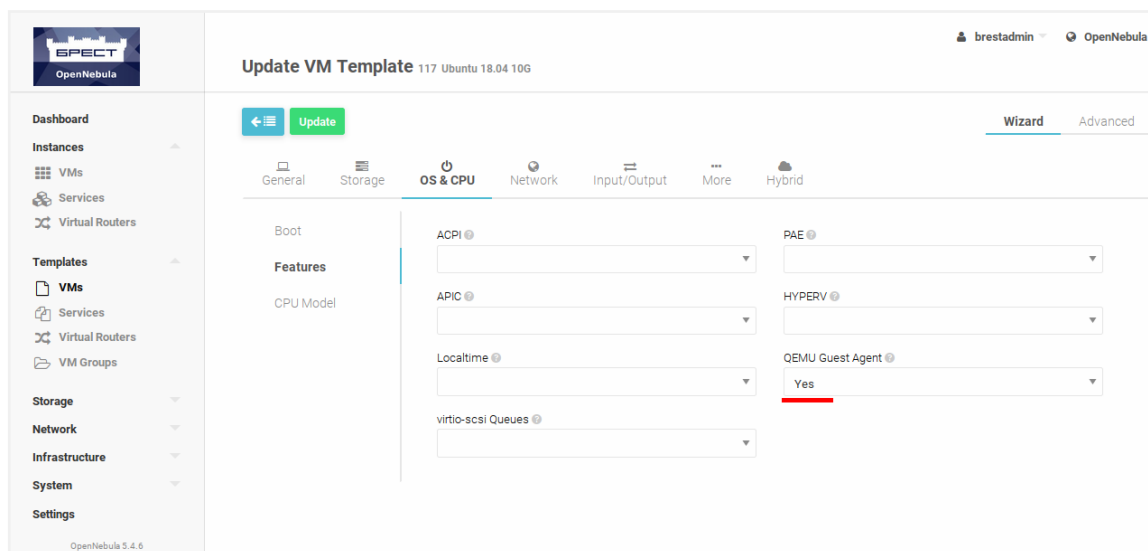
```
sudo update-initramfs -u -k all
```

2. Перезагрузить операционную систему

```
sudo init 6
```

Глава 4. Подготовка виртуальной машины ПК СВ «БРЕСТ» для резервного копирования

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



4.1. Linux

В операционной системе ВМ необходимо установить пакет `qemu-guest-agent` в зависимости от типа операционной системы:

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

или

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

4.2. Astra Linux Смоленск

Необходимо использовать диск разработки и добавить соответствующий iso image в операционную систему ВМ 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 ВМ.

В ПК СВ «БРЕСТ» доступны следующие базовые технологии хранения:

- Filesystem — файловая технология хранения. Данная технология хранения также включает сетевую файловую систему (Network File System — NFS);
- LVM — блочная технология хранения с использованием LVM (Logical Volume Manager — менеджер логических томов);
- Ceph — программно-определяемая технология хранения Ceph;
- Raw Device Mapping — прямое подключение к ВМ существующих блочных устройств, используется только для организации хранилища образов;
- iSCSI-Libvirt — прямое подключение к ВМ существующих устройств iSCSI, используется только для организации хранилища образов.

В таблице приведено описание доступных методов передачи данных (драйверов) для используемых базовых технологий хранения.

Таблица 1. Технологии хранения и методы передачи данных

Технологии хранения	Методы передачи данных между хранилищем образов и системным хранилищем
Filesystem	<p>ssh — образы копируются с помощью ssh-протокола;</p> <p>shared — образы экспортируются в соответствующий каталог системного хранилища на узле виртуализации;</p> <p>qcow2 — аналогично shared, но для образов формата qcow2. Образы создаются и передаются с помощью команды <code>qemu-img</code> с использованием оригинального образа в качестве опорного файла.</p>
Ceph	<p>ceph — все образы экспортируются в Ceph-пулы;</p> <p>ssh — rbd-файл, ассоциируемый с образом, экспортируется в файл локальной файловой системы узла виртуализации.</p>
LVM	<p>fs_lvm — образы хранятся как обычные файлы, при создании ВМ они выгружаются в логические тома (LV);</p> <p>lvm_lvm — создаются отдельные группы LVM-томов для хранилища образов и системного хранилища;</p> <p>lvm_thin — создаются отдельные группы LVM-томов для хранилища образов и системного хранилища, но системное хранилище организуется индивидуально для каждого узла виртуализации.</p>

Технологии хранения	Методы передачи данных между хранилищем образов и системным хранилищем
Raw Devices	dev — образы представляют собой существующие блочные устройства в узлах.
iSCSI libvirt	iscsi — образы представляют собой компоненты iSCSI target.

На данный момент в модулях RuBackup (*rb_module_brest_template* и *rb_module_brest_vm*) реализована поддержка следующих комбинаций технологий хранения и методов передачи данных между хранилищем образов и системным хранилищем:

- Filesystem с драйвером **qcow2**;
- Filesystem с драйвером **shared (NFS)**;
- Ceph с драйвером **ceph**;
- LVM с драйвером **lvm_lvm**.

Примечания:

При использовании варианта хранилища Ceph с драйвером Ceph для корректной работы модуля RuBackup требуется, чтобы на фронтальные машины ПК СВ «БРЕСТ» была установлена утилита rbd (утилита для манипуляции с образами rados block device).

В СРК RuBackup версии 2.0.99 U1 недоступно восстановление ВМ, расположенных на хранилище Ceph с непостоянным образом.

Глава 5. Алгоритмы защитного преобразования

В кластерной серверной группировке при восстановлении зашифрованной резервной копии на другом клиенте группировки необходимо использовать тот же мастер-ключ клиента, с помощью которого делалась данная копия.

Таблица 2. Алгоритмы защитного преобразования, доступные в утилите `rbfd`

Алгоритм	Поддерживаемая 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	

Глава 6. Локальный список ограничений

В том случае, если какие-либо конкретные ресурсы клиента не должны попасть в резервную копию, их можно включить в локальный список ограничений на клиенте. Списки ограничений располагаются в файлах:

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

Наименование ресурса (ID VM или шаблона), для которого нет необходимости выполнять резервное копирование, должно быть указано в отдельной строке списка ограничений.

Для того, чтобы списки 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 списки ограничений их необходимо создать из-под учетной записи с административными привилегиями.

Глава 7. Использование Менеджера администратора RuBackup (RBM)

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

Запуск менеджера администратора RBM:

Вариант 1

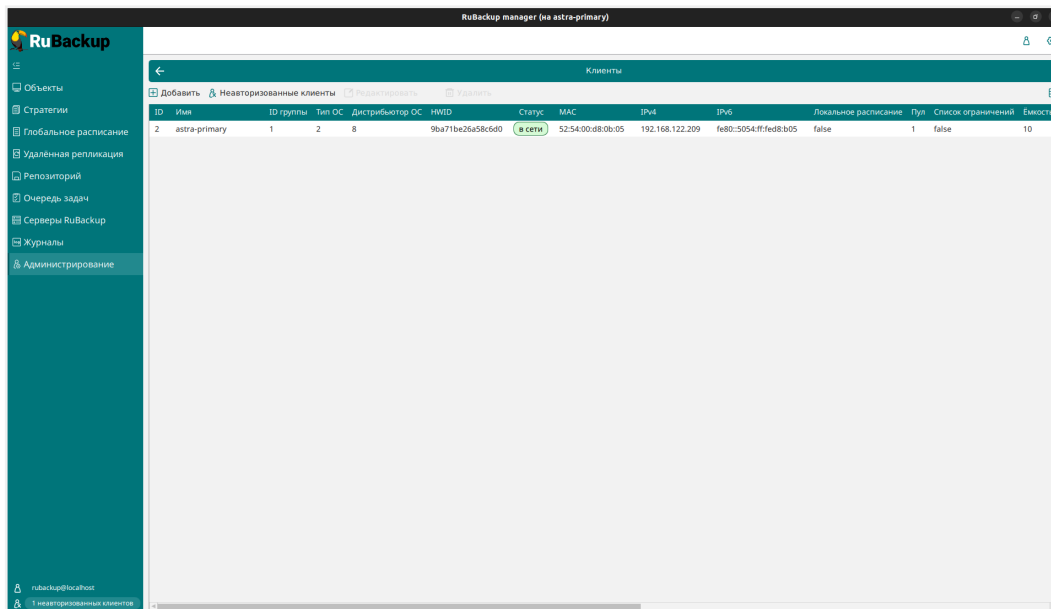
```
sudo LD_LIBRARY_PATH=/opt/rubackup/lib /opt/rubackup/bin/rbm
```

Вариант 2

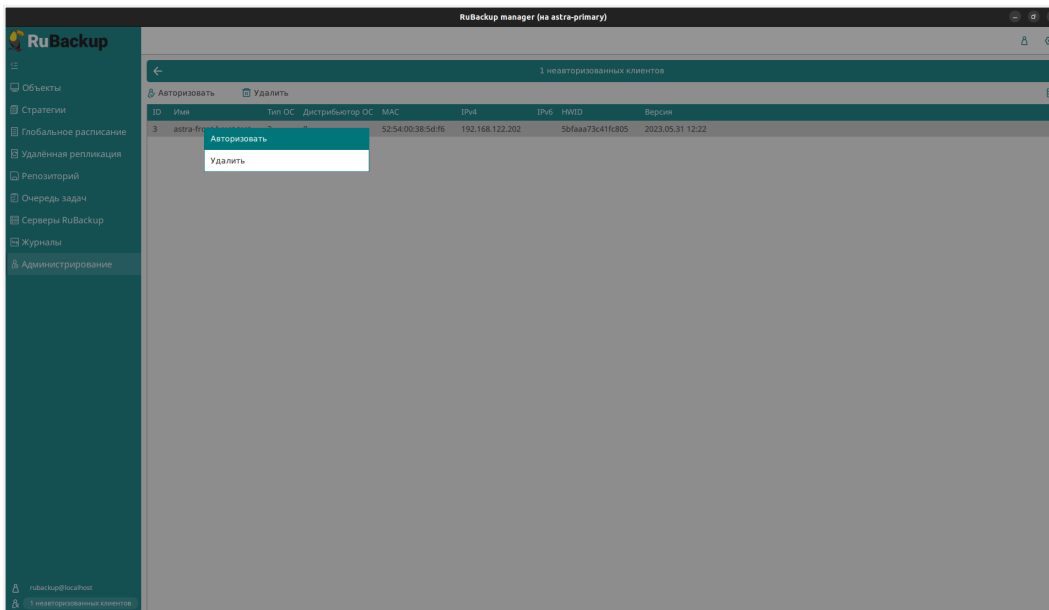
```
ssh -X root@you_rubackup_server
```

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

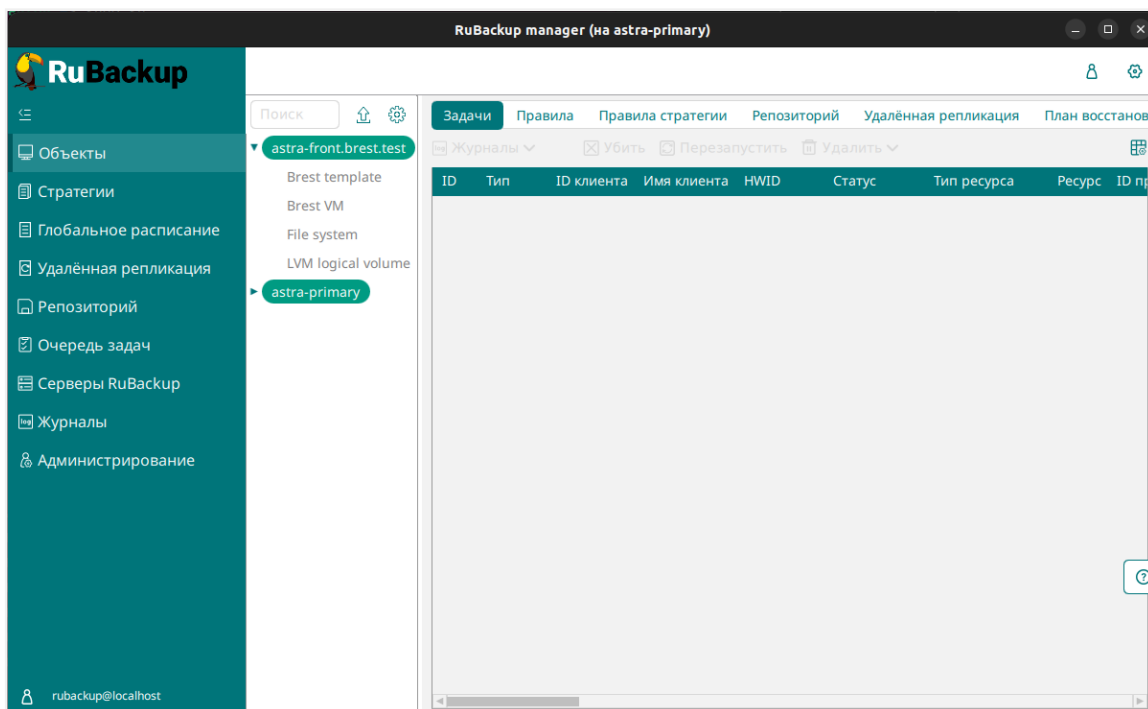
В том случае, если клиент RuBackup был установлен, но не авторизован, в нижней части окна RBM будет сообщение о том, что найдены неавторизованные клиенты (рисунок 2).



Все новые клиенты должны быть авторизованы в системе резервного копирования. Для этого нужно выбрать клиент и нажать кнопку «Авторизовать» либо выбрать «Авторизовать» из меню по щелчку правой кнопкой мыши (рисунок 3).

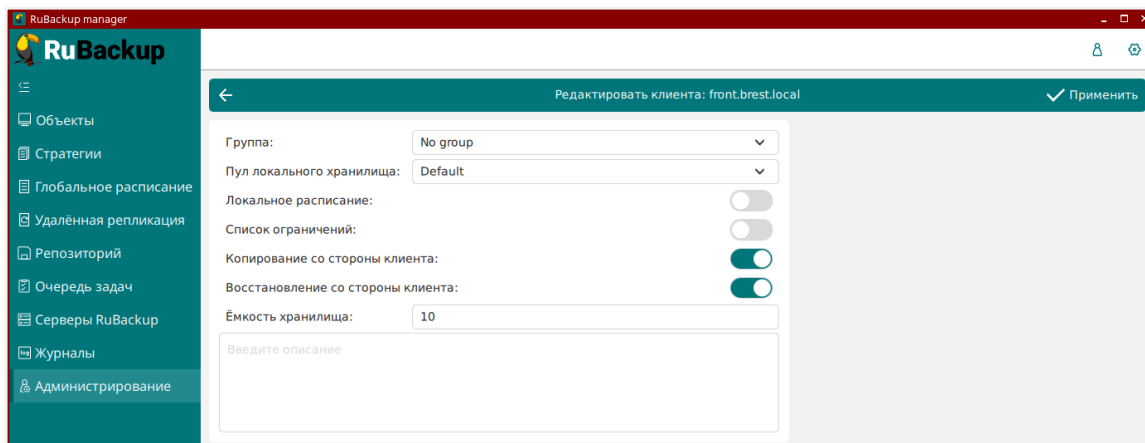


После авторизации новый клиент появится в главном окне RBM (рисунок 4).



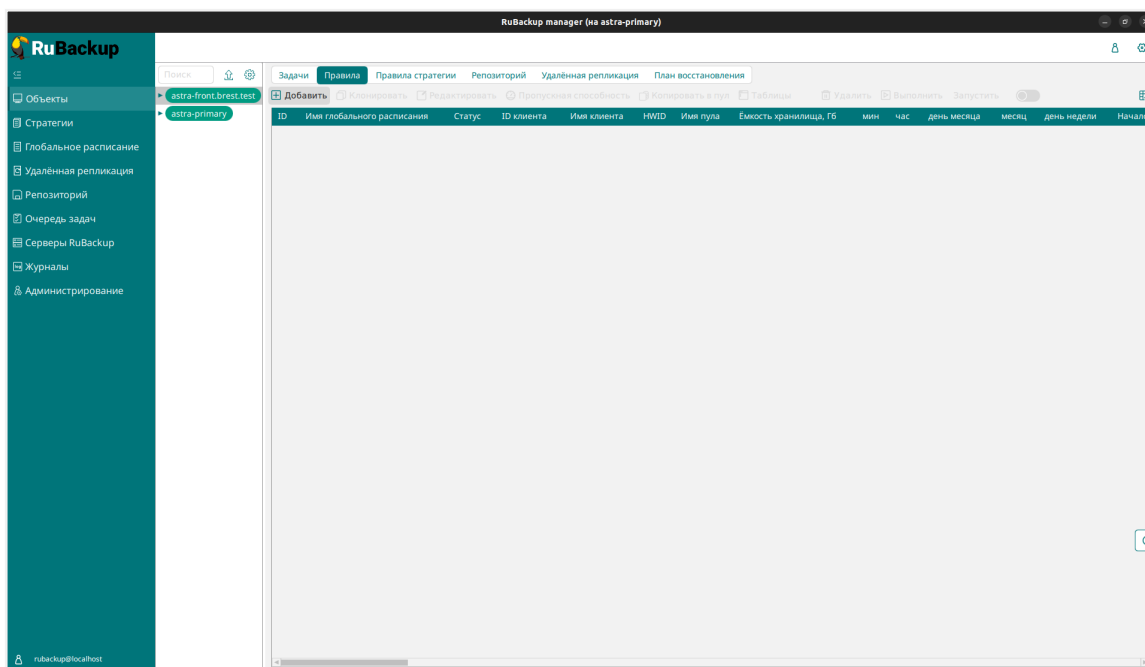
Клиенты могут быть сгруппированы администратором по какому-либо общему признаку. В случае необходимости восстанавливать резервные копии на другом хосте клиенты должны принадлежать к разделяемой группе (такая группа отмечается шрифтом *italic*). Например, если в такую группу включить два сервера фронтальной машины двух разных ПК СВ «БРЕСТ», то можно реплицировать между ними шаблоны и VM или переносить их с одного комплекса на другой.

Перевести клиента из одной группы в другую можно, выбрав клиента в меню Администрирование → Клиенты и нажав на кнопку «Редактировать» (рисунок 5):



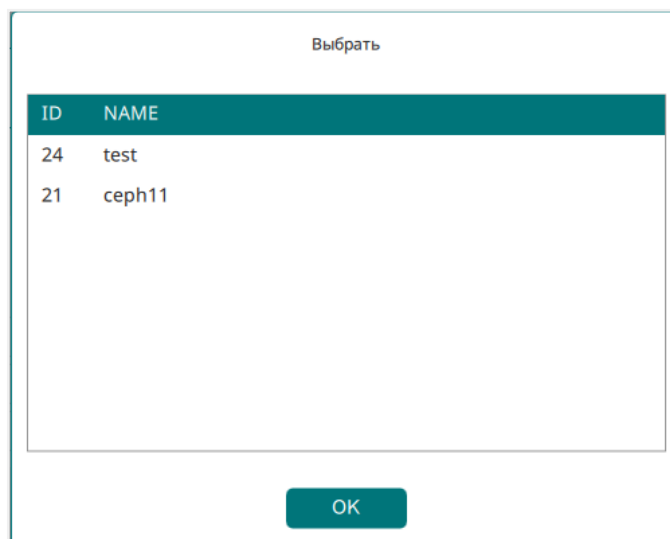
Для того, чтобы выполнять регулярное резервное копирование шаблона или VM, необходимо создать правило в глобальном расписании.

Выберите клиентский хост, на котором установлена фронтальная машина ПК СВ «БРЕСТ» и добавьте правило резервного копирования (рисунок 6):

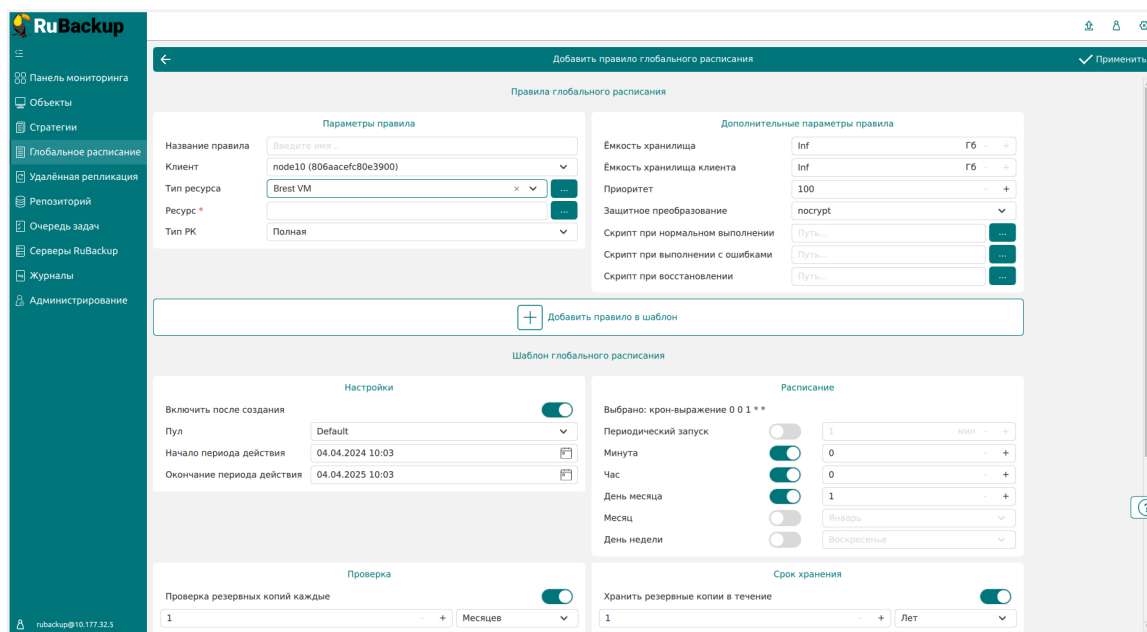


Выберите тип ресурса «Brest VM» для VM или «Brest template» для шаблона.

Выберите ресурс, для которого будет выполняться правило (рисунок 7).



Установите прочие необходимые настройки (рисунок 8). Подробнее о создании правил глобального расписания читайте в документе «Руководство системного администратора RuBackup».



Правила для выполнения резервных копий VM могут иметь дополнительные настройки — нажмите на иконку «...» рядом с выбором Типа ресурса (рисунок 9, Таблица 3).

Brest VM

backup_if_shutdown

dd_block_size - +

script_before_snapshot

script_after_snapshot

execution_script_timeout - +

backup_only_config

backup_only_delta

Таблица 3. Значения параметров виртуальных машин

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

Параметр	Описание	Значение по умолчанию	Допустимые значения
backup_only_config	<p>Выполнять резервное копирование только конфигурации VM. Будет выполняться только полное резервное копирование.</p> <p>Если значение параметра <code>true</code>, значение параметра <code>backup_only_delta</code> учитываться не будет.</p> <p>Если значение параметра <code>false</code>, будет выполняться резервное копирование и конфигурации VM, и дисков, входящих в её состав.</p>	false	true, false
backup_only_delta	<p>В случае <code>true</code> выполняет резервное копирование только частных данных VM, которые появились после ее создания, данные из образов в резервную копию не попадают.</p> <p>В случае <code>false</code> резервная копия будет выполнена в том числе для образов VM, исключая CDRом.</p>	true	true, false
new_name	Имя VM, которое будет использоваться в сохраняемой конфигурации VM при создании резервной копии. В том случае, если этот параметр пуст, конфигурация VM будет сохранена с прежним её именем.		

В том случае, если дополнительными настройками не заданы скрипты, которые могли бы выполняться в VM, но в ней существует исполняемый скрипт `/opt/rubackup/scripts/rubackup-brest.sh`, 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 — нажмите на иконку «...» рядом с выбором Типа ресурса (рисунком 10, Таблица 4).

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 шаблон сохраняется в резервную копию. В том случае, если этот параметр пуст, шаблон будет создан с прежним именем. Если такое имя уже есть в системе, к нему будет добавлен постфикс.		

В блоках «Резервные копии» и «Устаревшие резервные копии» можно определить условие перемещения резервных копий в другой пул, а также включить автоматическое удаление устаревших резервных копий, настроить уведомление об удалении и разрешить клиенту удалять резервные копии правила (рисунки 10 и 11).

Резервные копии

Переместить в пул через

1 - + Days

Пул Default

Устаревшие резервные копии

Автоматическое удаление

Уведомлять Nobody

Клиент может удалить резервные копии этого правила

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 фронтальной машины ПК СВ «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;
6. периодическое выполнение проверки целостности резервной копии;
7. хранение резервных копий в течение определенного срока, 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 спустя 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 в RuBackup она появляется в главной очереди задач. Отслеживать исполнение правил может как администратор, с помощью RBM, так и 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.

Глава 8. Настройка удаленной репликации

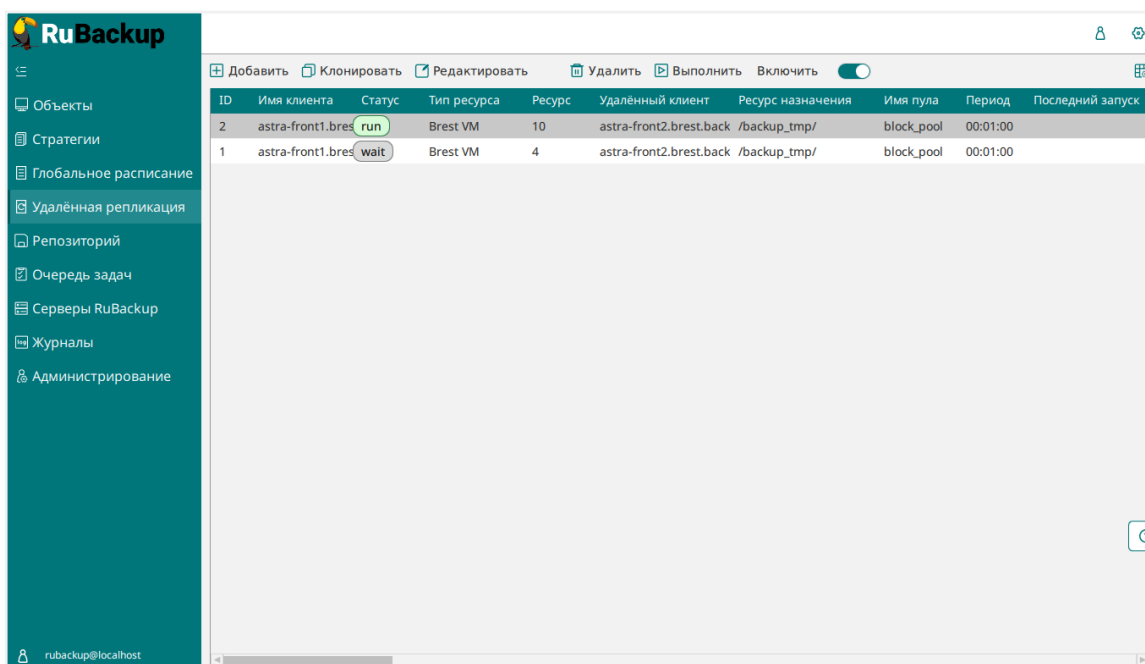
Для осуществления удаленной репликации на сервере резервного копирования должен быть настроен хотя бы один пул типа «Блочное устройство», содержащий минимум одно блочное устройство для использования в качестве дедуплицированного хранилища резервных копий (более подробную информацию см. в руководстве «Дедупликация в RuBackup»).

Репликация VM поддерживается не для всех методов передачи данных (драйверов) для используемых базовых технологий хранения. Доступные методы передачи данных для репликации перечислены в Таблице .

Таблица 5. Поддерживаемые для репликации технологии хранения и методы передачи данных

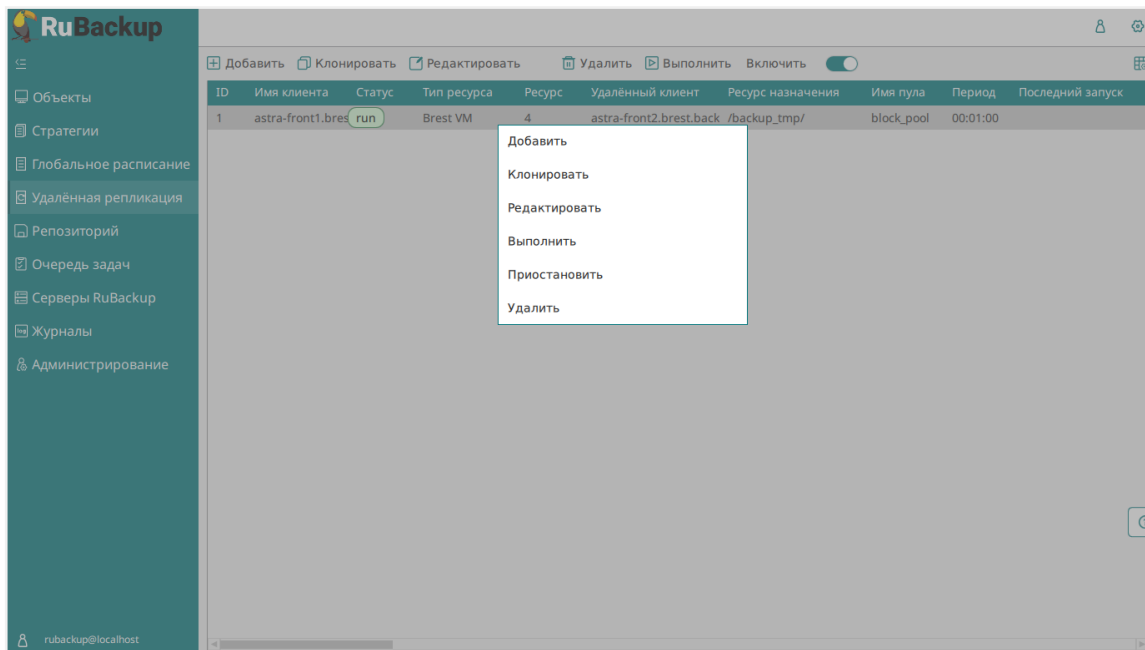
Технологии хранения	Методы передачи данных между хранилищем образов и системным хранилищем
Filesystem	<ul style="list-style-type: none">• ssh• shared• qcow2
LVM	lvm_lvm

Управление правилами удаленной репликации осуществляется при помощи Менеджера администратора RuBackup (RBM). Вкладка «**Удалённая репликация**» в главном окне RBM содержит информацию обо всех правилах непрерывной удалённой репликации. Включенные правила имеют статус «run», выключенные — «wait» (рисунок 12).



Управление правилами удалённой репликации осуществляется с помощью кнопок на верхней панели или в контекстном меню, вызываемом нажатием правой кнопки

МЫШИ (рисунок 13).



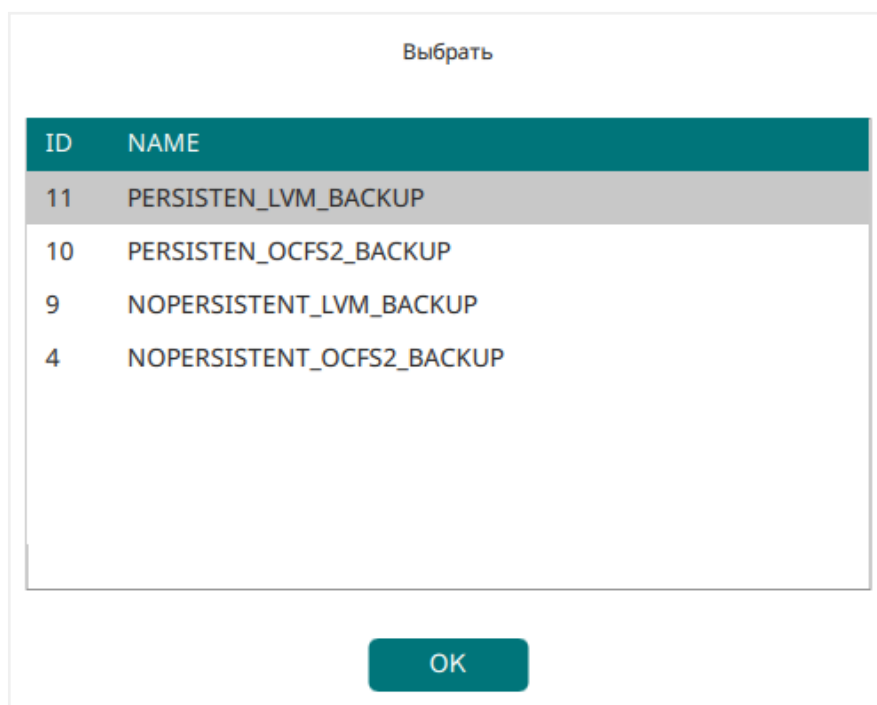
Доступны следующие действия:

- Добавить новое правило удалённой репликации.
- Клонировать правило.
- Редактировать правило.
- Выполнить правило немедленно.
- Запустить/приостановить — перевести правило из «wait» в «run» и наоборот.
- Удалить правило репликации.

При добавлении нового правила непрерывной удалённой репликации необходимо установить следующие параметры (рисунок 14):

- Блок «Источник»:

- Клиент — выберите клиент системы резервного копирования, откуда будут передаваться данные.
- Ресурс — нажмите на иконку «...» рядом с надписью «Ресурс» и выберите необходимую VM (рисунок 15). После выбора, в поле отобразится идентификатор VM.



- Тип ресурса — выберите «Brest VM».
- Блок «Место назначения»:
 - Клиент — выберите клиент системы резервного копирования, на который будут передаваться данные.
 - Каталог распаковки — выберите директорию, в которую будут переданы реплицированные данные. Репликация может быть выполнена непосредственно на другую инсталляцию ПК СВ «БРЕСТ» в рабочую директорию. Для успешного выполнения репликации требуется наличие свободного места в данном каталоге, которое превышает объем бэкапируемых данных.

Примечание: При репликации VM, развернутой на одной инсталляции ПК СВ «БРЕСТ» на другую инсталляцию ПК СВ «БРЕСТ» необходимо учитывать, что данные инсталляции должны быть идентичными (одинаковые ID устройств: хранилищ, виртуальных сетей и др.). Также должны быть идентичны хранилища, используемые в среде виртуализации.

- Параметры восстановления для модуля — выберите «Brest VM».
 - Период репликации.
 - Хранение реплик (количество хранимых реплик в репозитории).
 - Дата начала и окончания действия правила.
 - Пул для хранения резервных копий (можно использовать только пул типа «Блочное устройство»).
 - Настройки уведомлений о событиях правила.

Примечания:

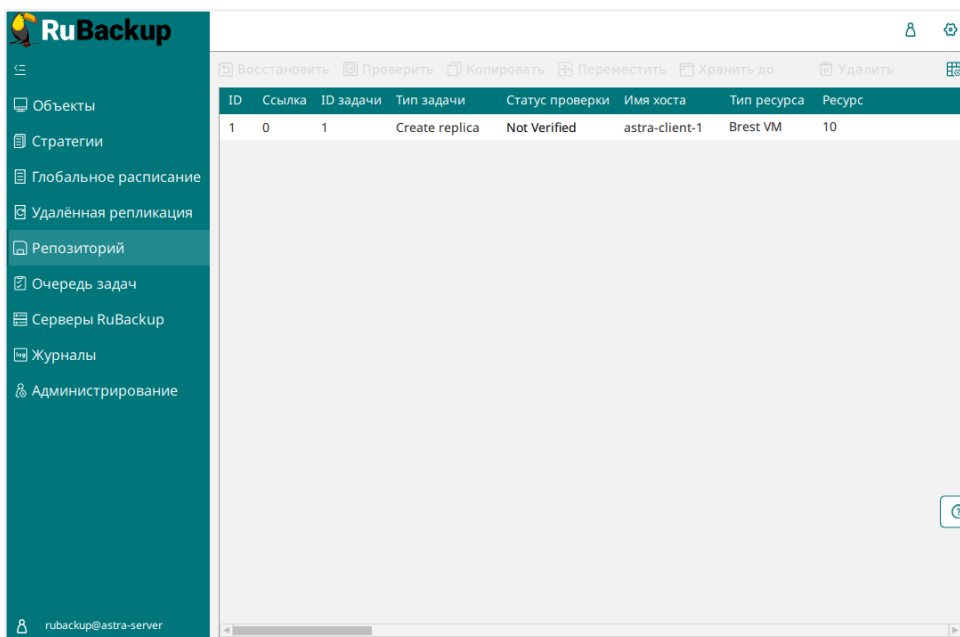
- При репликации будет считано имя VM из её конфигурации, сохраненной в резервной копии. Если VM с таким именем не существует в системе, то она будет создана с нуля. В другом случае данные дисков VM из резервной копии будут реплицированы в соответствующие диски существующей VM. Если в рамках опции восстановления «new_name» задано требуемое имя VM, то при проверке наличия VM в системе будет использовано это имя, а не то, которое сохранено в конфигурации VM в резервной копии. Для информации о параметрах восстановления для модулей **Brest VM** и **Brest Template** см. [таблицу 6](#) и [таблицу 7](#) соответственно.
- Значение параметра восстановления «restore_only_config» модуля **Brest VM** не учитывается при применении реплики.

Перед настройкой непрерывной репликации необходимо оценить время, необходимое и достаточное для завершения операций по созданию и применению реплики, и в соответствии с этим настраивать период репликации правила. Вы также можете изменить настройки правила после его создания ([рисунок 16](#)).

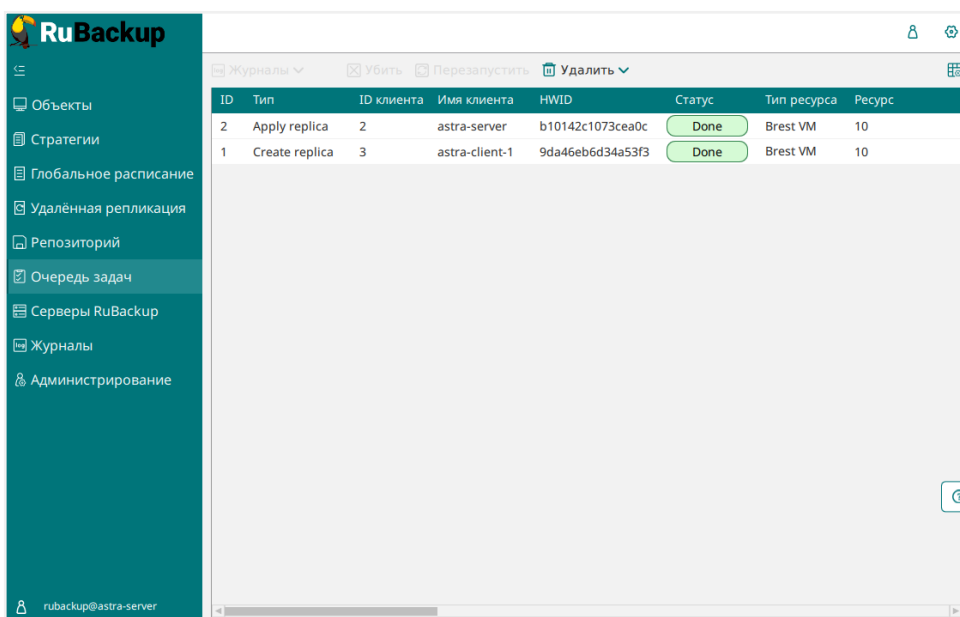
The screenshot shows the RuBackup web interface for configuring a remote replication rule. The interface is organized into several sections:

- Header:** "Добавить удалённую репликацию" (Add remote replication) with a "Применить" (Apply) button.
- Источник (Source):**
 - Клиент (Client): astra-front1.brest.backup (6647366f1a7276cb)
 - Ресурс * (Resource): 10
 - Тип ресурса (Resource type): Brest VM
- Место назначения (Destination):**
 - Клиент (Client): astra-front2.brest.backup (0e64d13ffd3...)
 - Каталог распаковки * (Catalog): /backup_tmp/
 - Параметры восстановления для модуля: (Restoration parameters): Brest VM
- Параметры (Parameters):**
 - Запускать каждый (Run every): 1 mins
 - Хранение реплик (Retention): 1
 - Начало периода действия (Start date): 28.08.2023 14:46
 - Окончание периода действия (End date): 28.08.2024 14:46
 - Начало рабочего окна (Start window): 14:46:00.000
 - Конец рабочего окна (End window): 14:46:00.000
 - Пул (Pool): block_pool
- Уведомления (Notifications):** A section at the bottom, partially visible.

Реплики располагаются в репозитории в виде записей с типом задачи «Create replica» ([рисунок 17](#)).



В ходе работы старые реплики будут удаляться из репозитория, для чего в главной очереди задач будут создаваться соответствующие задачи (рисунок 18).



Глава 9. Использование Менеджера клиента RuBackup (RBC)

Принцип взаимодействия Менеджера клиента RuBackup (RBC) 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. RBC отправляет команду пользователя клиенту, а клиент отправляет ее серверу. В том случае, если действие допустимо, сервер RuBackup отдаст обратную команду клиенту и/или перенаправит ее медиасерверу RuBackup для дальнейшей обработки. Это означает, что RBC 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 RBC, вы можете просто закрыть приложение, все действия будут выполнены системой резервного копирования (однако стоит дождаться сообщения о том, что задание принято к исполнению и проконтролировать это на вкладке «Задачи»).

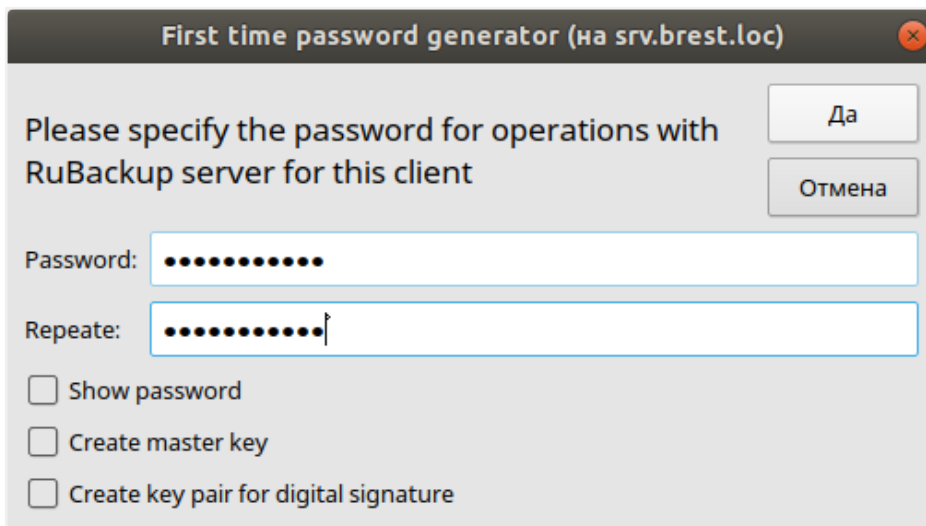
Графический интерфейс клиентского менеджера поддерживает русский и английский языки.

Запуск клиентского менеджера (для примера использован хост фронтальной машины ПК СВ «БРЕСТ» `srv.brest.loc`):

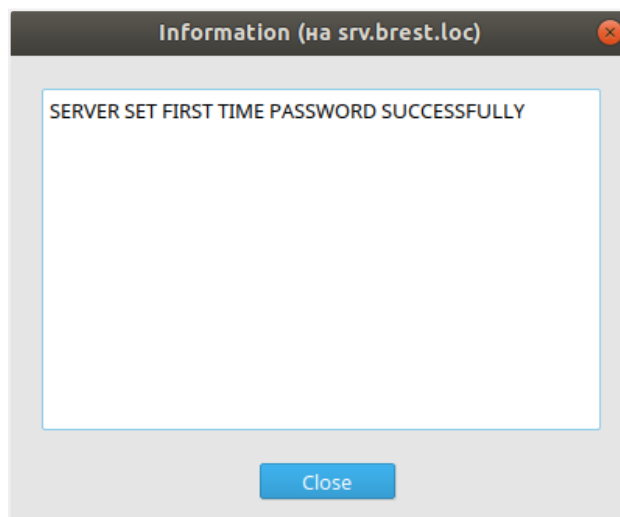
```
ssh -Xroot@srv.brest.loc
```

```
rbc&
```

В том случае, если клиентская операция выполняется впервые, потребуется ввести пароль клиента ([рисунок 19](#)). Без ввода пароля получить резервную копию для клиента из хранилища невозможно.



В случае успешного выполнения появится окно (рисунок 20).



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 RBC расположены переключающиеся вкладки, позволяющие управлять резервными копиями, расписанием резервного копирования и просматривать текущие задачи клиента.

9.1. Вкладка «Резервные копии»

	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/andrejk/RBv2/	full	Default	119562240	28641	2020-04-20 14:59:57+03	00:00:00.63

В таблице на вкладке «Резервные копии» (рисунок 21) 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 потребуется 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`), либо `SAFE_DIRS` для хранилищ ПК СВ «БРЕСТ».



При восстановлении образов, ассоциированных с ВМ или шаблонами, файлы образов, извлеченные из резервной копии, помещаются модулем RuBackup в одну из безопасных директорий (`SAFE_DIRS`), определенных в ПК СВ «БРЕСТ» для хранилища образов. По умолчанию для этих целей определена директория `/var/tmp`. При восстановлении ВМ или шаблона вместе с образами из резервной копии необходимо учитывать объем свободного места в безопасной директории на хосте фронтальной машины. Распространенной практикой является монтирование дополнительной файловой системы в безопасную директорию.

RBC 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 восстановления необходимо, чтобы в каталоге, предназначенном для создания и временного хранения резервных копий было свободное место, которое превышает объем бэкапируемых данных (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 будут проверены размер файлов резервной копии и проверена сама резервная копия. Если резервная копия не была подписана цифровой подписью, то будет проверен размер файлов резервной копии.

9.2. Вкладка «Глобальное расписание»

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

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

Во вкладке «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 удаление правила 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.

9.3. 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

В таблице вкладки «Задачи» (рисунок 22) 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 задач фиксируется в специальном журнале задач сервера RuBackup, при необходимости статус любой задачи, даже удаленной из очереди, можно уточнить у администратора RuBackup. Также 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**»).



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.

9.4. 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.

9.5. 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.

Глава 10. Утилиты командной строки клиента RuBackup

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

10.1. rb_archives

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

10.2. rb_schedule

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

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

10.3. 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
```

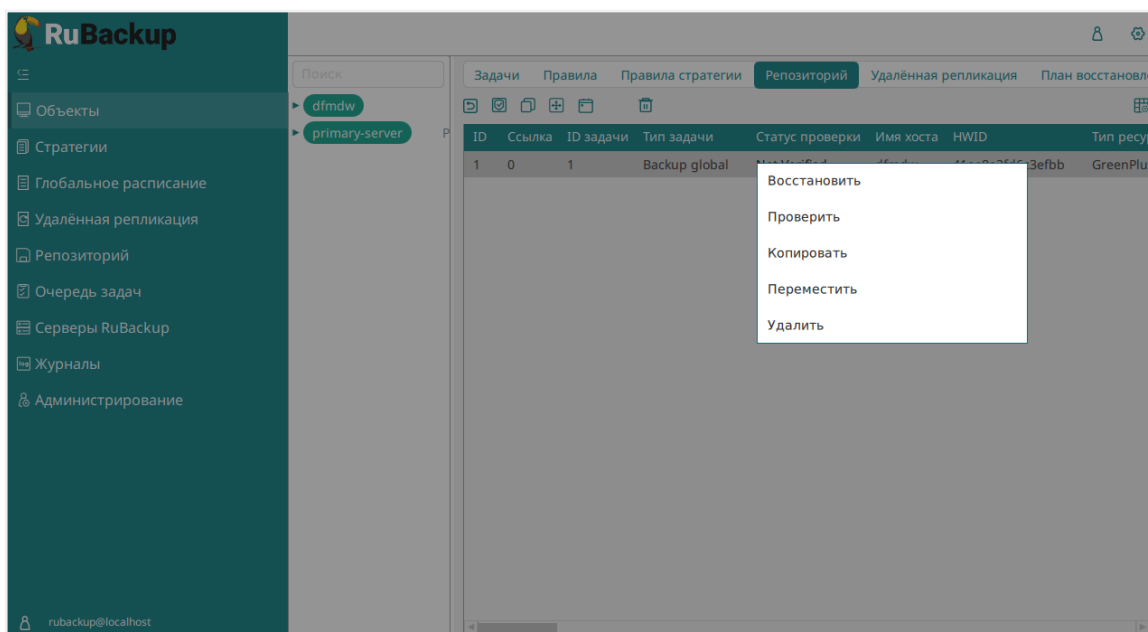
10.4. rbcrypt

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».

Глава 11. Централизованное восстановление резервных копий

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 нежелательно, 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, его можно инициировать, перейдя во вкладку «Репозиторий» на верхней панели RBM. Для этого найдите в списке требуемую резервную копию, нажмите на нее правой кнопкой мыши и выберите в контекстном меню «Восстановить» (рисунок 23):



В окне централизованного восстановления можно увидеть основные параметры резервной копии, выбрать узел клиента, на который будет восстановлена резервная копия, задать путь назначения для восстановления резервной копии.

В том случае, если необходимо восстановить резервную копию в локальный каталог на фронтальной машине без развертывания шаблона или VM, снимите отметку «Развернуть, если применимо» (рисунок 24).

Место восстановления

Восстановить на клиента:

HWID:

Путь назначения: *

Restore parameters of module:

Развернуть, если применимо:

Узнать статус узлов кластера можно с помощью команды `onezone show 0`:

```
root@astra-front1:/home/suser# onezone show 0
ZONE 0 INFORMATION
ID          : 0
NAME       : OpenNebula

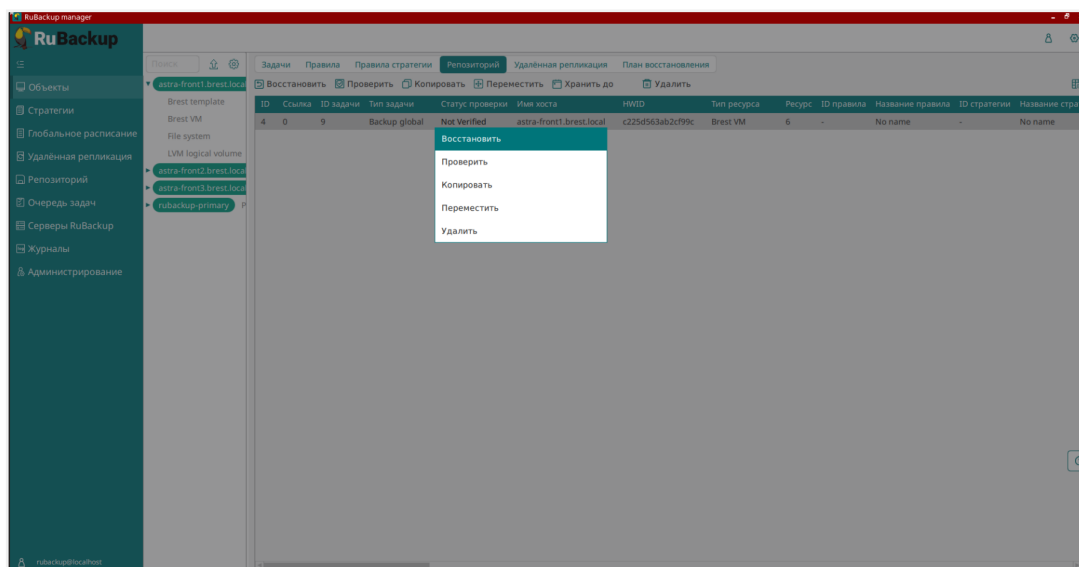
ZONE SERVERS
ID NAME          ENDPOINT
0 astra-front1.br http://astra-front1.brest.local:2633/RPC2
1 astra-front2.br http://astra-front2.brest.local:2633/RPC2
2 astra-front3.br http://astra-front3.brest.local:2633/RPC2

HA & FEDERATION SYNC STATUS
ID NAME          STATE   TERM   INDEX   COMMIT   VOTE   FED_INDEX
0 astra-front1.br follower 334    295465 295465   2     -1
1 astra-front2.br follower 334    295465 295465  -1     -1
2 astra-front3.br leader   334    295465 295465   2     -1

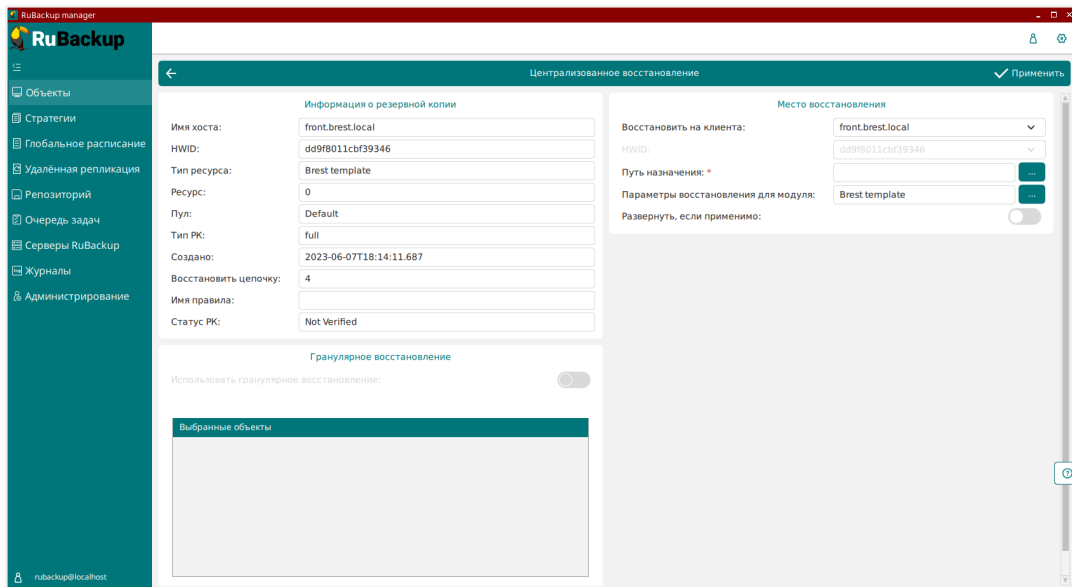
ZONE TEMPLATE
ENDPOINT="http://localhost:2633/RPC2"
```

В данном примере лидером является узел `astra-front3.brest.local` и именно на этом узле необходимо выполнять команды для восстановления.

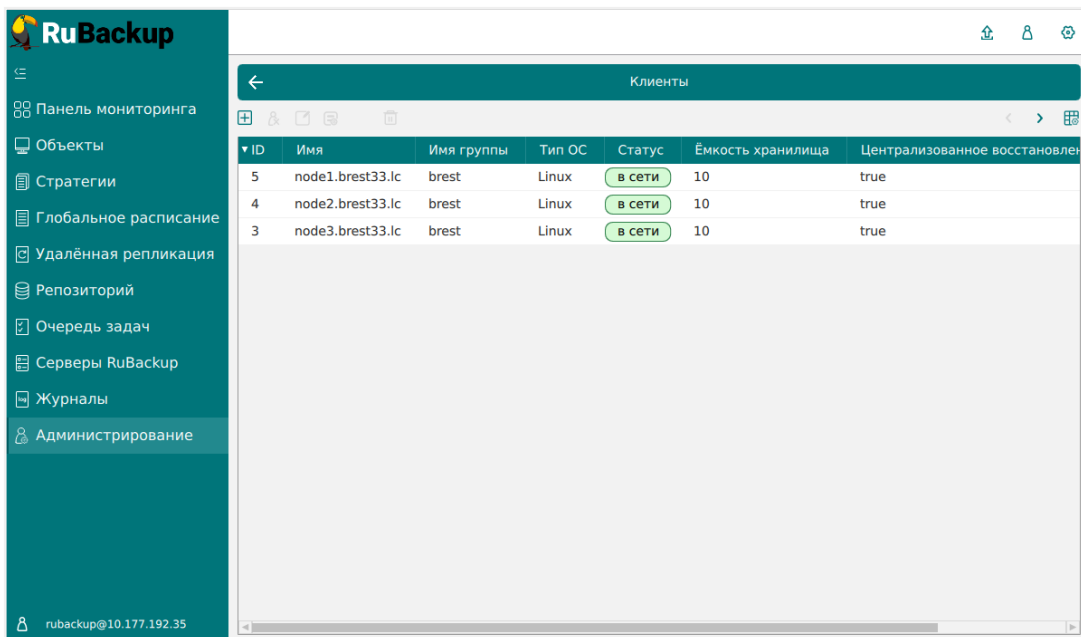
При восстановлении резервной копии с помощью RBM необходимо выбрать нужную резервную копию, кликнуть по ней правой кнопкой мыши и выбрать «Восстановить» из выпадающего списка (рисунок 25).



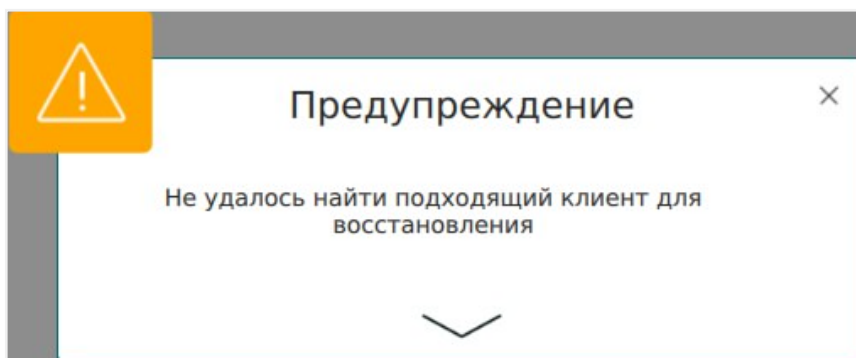
Затем необходимо выбрать нужные параметры в блоке «Место восстановления» (рисунок 26).



Для восстановления резервной копии необходимо добавить клиентов РК, установленных на узлах кластера Брест, в общую разделяемую группу (рисунок 27).

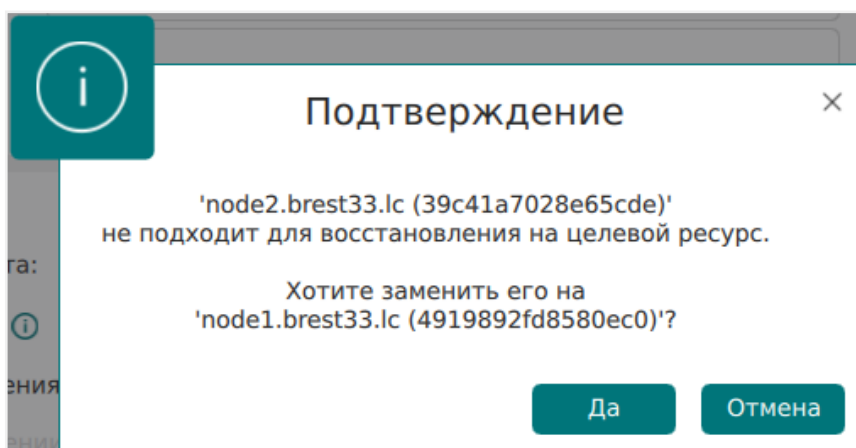


Если клиент РК не находится в общей разделяемой группе и не является лидером кластера, то при попытке восстановления будет выведено предупреждение (рисунок 28).

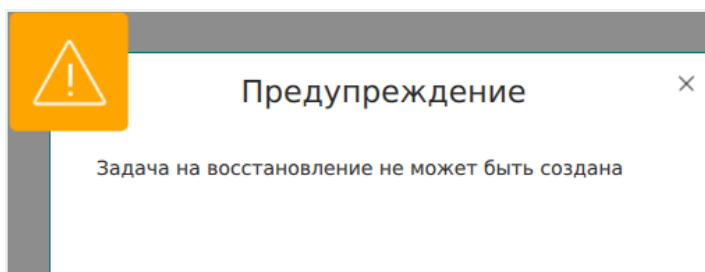


Восстановление резервной копии с развёртыванием должно выполняться только на тот узел, который является лидером в данный момент.

Перед запуском задачи на восстановление резервной копии, СРК выполняет проверку роли выбранного оператором клиента. Если выбранный оператором узел не является лидером и активирован параметр «**Восстановить на целевом ресурсе**», СРК проверяет остальных клиентов разделяемой группы и предлагает автоматически заменить выбранный узел на лидера(рисунки 29).



Если пользователь соглашается заменить целевой ресурс на лидера, то будет запущена задача на восстановление. В случае, если пользователь отказывается, будет выведена ошибка (рисунки 30).



Для настройки параметров восстановления, которые относятся к модулям резервного копирования и восстановления *Brest VM* и *Brest template* нажмите на иконку «...» рядом с полем «**Параметры восстановления для модуля:**» (Таблица 6, Таблица 7).

Таблица 6. Параметры восстановления резервных копий шаблона

Параметр	Описание	Значение по умолчанию	Допустимые значения
new_name	Имя, с которым шаблон будет создан при восстановлении из резервной копии. В том случае, если этот параметр пуст, шаблон будет создан с прежним именем. Если шаблон с таким именем уже есть в системе, к имени будет добавлен постфикс.		
set_images_persistent	Установить для всех образов шаблона параметр PERSISTENT=yes при восстановлении.	false	true, false
restore_only_config	Выполнить восстановление из резервной копии только конфигурации шаблона, без ассоциированных с ним образов.	false	true, false
dd_block_size	Размер блока в Мб для операций DD.	5	>=1

Таблица 7. Параметры восстановления виртуальной машины из резервной копии

Параметр	Описание	Значение по умолчанию	Допустимые значения
restore_only_config	Выполнить восстановление из резервной копии только конфигурации ВМ, без восстановления ассоциированных с ней дисков.	false	true, false
keep_cdrom	<p>Если на момент создания резервной копии к ВМ был подключен CDROM, то информация об этом CDROM сохраняется в резервной копии.</p> <p>Если выполняется восстановление резервной копии, а опция keep_cdrom имеет значение false, то перед созданием ВМ информация о CDROM будет удалена из конфигурации ВМ, то есть в созданной в процессе восстановления виртуальной машине CDROM не будет подключен.</p> <p>Если выполняется восстановление резервной копии, а опция keep_cdrom имеет значение true и при этом оригинальный образ, отвечающий за CDROM, на момент резервного копирования ВМ отсутствует внутри платформы ПК СВ «БРЕСТ», задача на восстановление из резервной копии завершится с ошибкой.</p>	false	true, false

Параметр	Описание	Значение по умолчанию	Допустимые значения
new_name	Имя, с которым VM будет создана при восстановлении из резервной копии. В том случае, если этот параметр пуст, VM будет создана с прежним именем. Если VM с таким именем уже есть в системе, к имени будет добавлен постфикс.		
dd_block_size	Размер блока в Мб для операций DD.	5	>=1
restore_on_current_node	При включенном переключателе VM будет создана на том же узле клиента, на который выполнена распаковка резервной копии. Переключатель можно использовать только в том случае, если вычислительные узлы ПК СВ «Брест» расположены на фронтальных машинах ПК СВ «Брест». То есть фронтальная машина соответствует вычислительному узлу. Задача на восстановление должна запускаться на узле ПК СВ «Брест», находящемся в состоянии leader .	false	true, false

Примечания

При установленном флаге `restore_only_config` происходит следующее:

1. Модуль проверяет наличие образов дисков, которые присутствовали в конфигурации VM на момент резервного копирования.
2. Если оригинальные образы отсутствуют, задача восстановления завершается с ошибкой.
3. Если в конфигурации VM есть диски, созданные на основе «постоянного образа» и на момент восстановления они присутствуют внутри платформы, но не в состоянии `ready`, задача восстановления завершается с ошибкой.
4. Если внутри платформы есть VM с оригинальным именем, генерируется новое имя (добавляется постфикс к имени). Информация о новом имени VM помещается в `vm.xml` — файл, который был сформирован при резервном копировании.
5. Из результирующего `vm.xml` создается VM внутри платформы.
6. Данные дисков VM (даже если они были сохранены при резервном копировании) не подменяются у вновь созданной при восстановлении VM — т.е. на выходе получается VM с такой же конфигурацией, как и на момент резервного

копирования, которая базируется на оригинальных образах дисков.

Для восстановления резервной копии шаблона или VM с помощью утилиты командной строки `rb_archives` необходимо определить идентификатор резервной копии, которую необходимо восстановить, например, при помощи команды `rb_archives`:

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

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

```
rb_archives -x 137
```

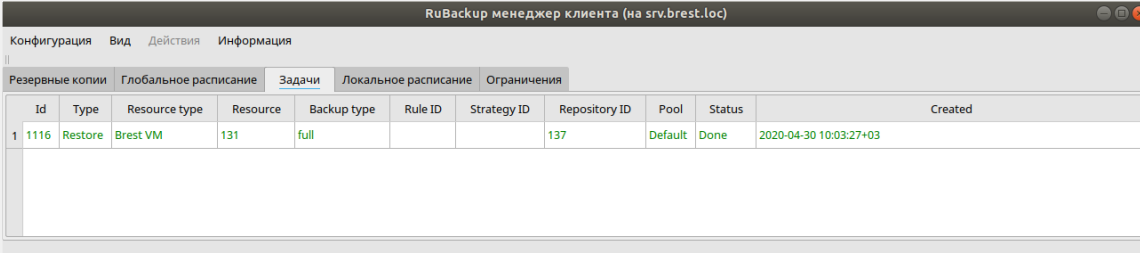
В случае успешно принятой задачи команда вернет «ок», а восстановление будет происходить в фоновом режиме.

```
root@srv:~# rb_archives -x 137
Password:
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_tasks`:

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

или при помощи RBC (рисунок 31):



The screenshot shows the RuBackup client manager interface. The window title is "RuBackup менеджер клиента (на srv.brest.loc)". The interface has a menu bar with "Конфигурация", "Вид", "Действия", and "Информация". Below the menu bar are several tabs: "Резервные копии", "Глобальное расписание", "Задачи", "Локальное расписание", and "Ограничения". The "Задачи" tab is selected, displaying a table with the following data:

Id	Type	Resource type	Resource	Backup type	Rule ID	Strategy ID	Repository ID	Pool	Status	Created
1	Restore	Brest VM	131	full			137	Default	Done	2020-04-30 10:03:27+03

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_Re
sourceType_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_Re
sourceType_17/hda.2
Thu Apr 30 10:08:07 2020: Task was done. ID: 1116
```

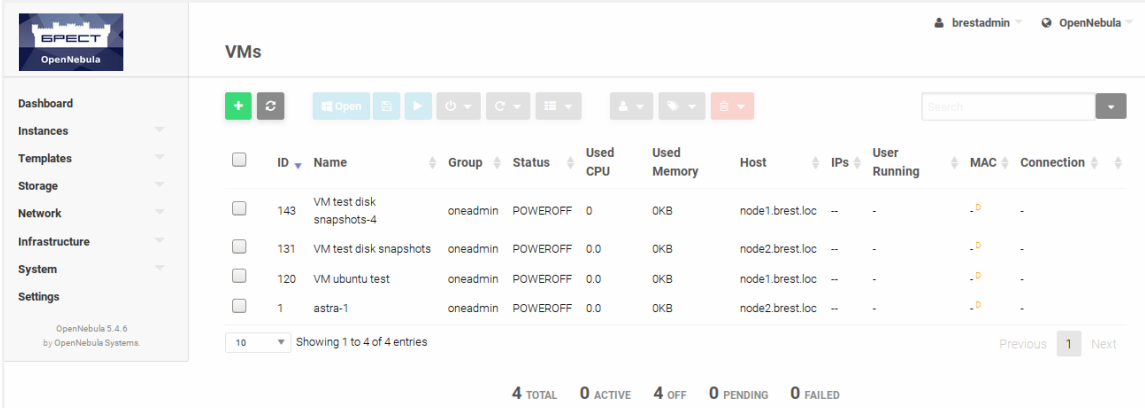
В модулях RuBackup также предусмотрено ведение отдельного журнала, в котором фиксируется подробная информация о выполнении задачи на создание резервной копии или восстановление из резервной копии. Ниже перечислены пути к соответствующим файлам журналов:

- `/opt/rubackup/log/rb_module_brest_template.log`

- `/opt/rubackup/log/rb_module_brest_vm.log`

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 СВ «БРЕСТ» появилась новая VM (ID 143), полностью идентичная той, которая была в системе в момент резервного копирования (рисунок 32):



The screenshot shows the OpenNebula web interface for managing VMs. The left sidebar contains navigation options: Dashboard, Instances, Templates, Storage, Network, Infrastructure, System, and Settings. The main area displays a table of VMs with columns for ID, Name, Group, Status, Used CPU, Used Memory, Host, IPs, User Running, MAC, and Connection. There are four VMs listed, all with a status of POWEROFF. A summary at the bottom indicates 4 TOTAL VMs, with 0 ACTIVE, 4 OFF, 0 PENDING, and 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	-	-	-	-

Showing 1 to 4 of 4 entries

4 TOTAL 0 ACTIVE 4 OFF 0 PENDING 0 FAILED