RuBackup
Система резервного копирования и восстановления данных

Резервное копирование ресурсов

ProxMox

RuBackup

Версия 1.9

2022 г.

Содержание

Введение

Система резервного копирования RuBackup позволяет выполнять клиентам резервное копирование виртуальных машин и контейнеров платформы виртуализации Proxmox (см. «Поддерживаемые версии» ниже).

Для виртуальных машин доступно полное, инкрементальное и дифференциальное резервное копирование. Резервное копирование виртуальных машин может происходить без их остановки.

Для контейнеров доступно полное резервное копирование.

Полное резервное копирование – это создание резервной копии всех данных из исходного набора, независимо от того, изменялись данные или нет с момента выполнения последней полной резервной копии.

Дифференциальное резервное копирование сохраняет только данные, изменённые со времени выполнения предыдущего полного резервного копирования.

Инкрементальное резервное копирование сохраняет только данные, изменённые со времени выполнения предыдущей инкрементальной резервной копии, а если такой нет, то со времени выполнения последней полной резервной копии.

Для выполнения резервного копирования виртуальных машин Proxmox на хост требуется установить клиента RuBackup и модули rb_module_proxmox_vm, rb_module_proxmox_containers. На виртуальные машины, для которых предполагается выполнять резервное копирование, должны быть установлены дополнения гостевой систем.

Резервное копирование выполняется по заранее заданным правилам в глобальном расписании RuBackup. Клиенту доступно срочное резервное копирование виртуальных машин Proxmox, но в этом случае выполняется полное резервное копирование выбранного ресурса. Также 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.

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

В ходе выполнения резервного копирования виртуальной машины используется штатная технология резервного копирования при помощи утилиты vzdump, однако полученная резервная копия преобразуется модулем RuBackup для того, чтобы было возможно создавать инкрементальные и дифференциальные резервные копии.

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 Proxmox необходимо включить функцию QEMU guest agent.

В ходе выполнения резервного копирования контейнера используется штатная технология резервного копирования при помощи утилиты vzdump.

Установка клиента RuBackup

Перед установкой клиента на узел Proxmox

Перед установкой клиента на узел Proxmox рекомендуется выполнить обновления:

```
# apt update
# apt upgrade
```

Более подробнее см. по ссылке:

https://pve.proxmox.com/pve-docs/pve-admin-guide.html#sysadmin_package_repositories

Для возможности резервного копирования и восстановления виртуальных машин при помощи СРК RuBackup на сервер следует установить следующие пакеты:

- `rubackup-client.deb` – клиент резервного копирования,
- `rubackup-kvm.deb` – модуль резервного копирования.

Установка пакетов клиента RuBackup производится из-под учетной записи с административными правами при помощи следующих команд:

```
# dpkg -i rubackup-client.deb
# dpkg -i rubackup-proxmox.deb
```

```
root@proxmox:~# dpkg -i rubackup-client.deb
Selecting previously unselected package rubackup-client.
(Reading database ... 46006 files and directories currently installed.)
Preparing to unpack rubackup-client.deb ...
Unpacking rubackup-client (2020-04-30) ...
Setting up rubackup-client (2020-04-30) ...
root@proxmox:~# dpkg -i rubackup-proxmox.deb
Selecting previously unselected package rubackup-proxmox.
(Reading database ... 46084 files and directories currently installed.)
Preparing to unpack rubackup-proxmox.deb ...
Unpacking rubackup-proxmox (2020-07-09) ...
Setting up rubackup-proxmox (2020-07-09) ...
root@proxmox:~#
```

Кроме того, для работы СРК RuBackup необходимо установить дополнительные пакеты:

```
# sudo apt install pigz
```

Для возможности использовать RBC на ОС без графической оболочки:

```
# sudo apt install libgl1-mesa-dev

# sudo apt install libxkbcommon-x11-0
```

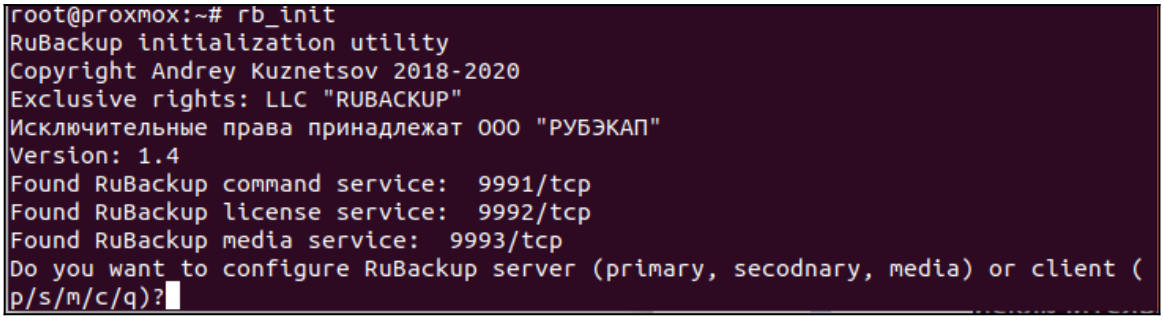
Настройка клиента с помощью интерактивной утилиты rb_init

Для настройки клиента с помощью интерактивной утилиты rb_init необходимо выполнить следующие действия:

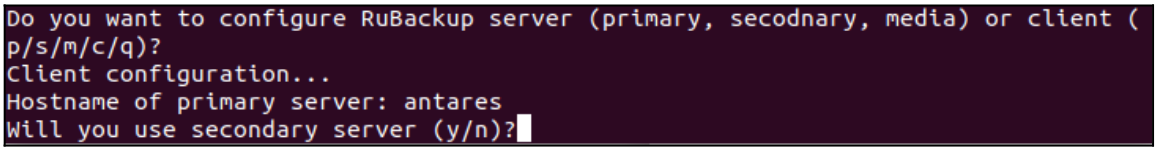
1. Выполнить команду:

```
# /opt/rubackup/bin/rb_init
```

2. Выбрать тип установки. Для клиента нужно нажать клавишу **c:**



3. Ввести имя основного и, если есть, резервного серверов СРК:



Важно! Для всех серверов RuBackup должно быть настроено корректное разрешение имён. В том случае, если клиент RuBackup не может определить IP адрес по имени сервера, то он прекратит свою работу. Используйте корректные настройки DNS или /etc/hosts.

4. Выбрать сетевой интерфейс, по которому разрешено выполнение резервного копирования:

```
Possible interfaces for RuBackup client communication:
lo [0]
ens3 [1]
vmbr0 [2]
tap101i0 [3]
fwbr101i0 [4]
fwpr101p0 [5]
fwln101i0 [6]
Choose client net interface for use:
Selected interface: vmbr0
```

5. Выбрать вариант подписи резервных копий клиента цифровой подписью?

```
Choose client net interface for use:
Selected interface: br0
Will you use digital signature (y/n)?
```

Для создания резервных копий необходимо использовать локальный каталог. Рекомендуется использовать отдельную файловую систему для того, чтобы не произошло случайного переполнения системного раздела:

```
Would you like to use local(l) backup directory or NFS(n) share of RuBackup server (
l/n)?l
Local backup directory [/tmp] : /rubackup-tmp
```

6. Создать мастер-ключ для защитного преобразования резервных копий и создать ключи цифровой подписи, а также ввести пароль для его генерации:

```
Create RuBackup master key...
Passphrase:

Create new secret key
Create new public key
```

В том случае, если планируется тестирование RuBackup, рекомендуется запускать клиента RuBackup в терминальном режиме с помощью следующей команды:

```
# /opt/rubackup/bin/rubackup_client start
```

Остановить RuBackup клиента можно с помощью следующей команды:

```
# /opt/rubackup/bin/rubackup_client stop
```

Для штатной эксплуатации рекомендуется запускать клиента RuBackup как сервис. Для этого необходимо из административной учетной записи:

1. Включить сервис клиента RuBackup:

```
# sudo systemctl enable
  /opt/rubackup/etc/systemd/system/rubackup_client.service
```

```
root@srv:~# sudo systemctl enable /opt/rubackup/etc/systemd/system/rubackup_client.s
ervice
Created symlink /etc/systemd/system/multi-user.target.wants/rubackup_client.service
→ /opt/rubackup/etc/systemd/system/rubackup_client.service.
Created symlink /etc/systemd/system/rubackup_client.service → /opt/rubackup/etc/syst
emd/system/rubackup_client.service.
```

2. Перезагрузить systemclt:

```
# sudo systemctl daemon-reload
```

3. Запустить сервис rubackup_client

```
# sudo systemctl start rubackup_client
```

4. Уточнить статус клиента можно при помощи команды

```
# sudo systemctl status rubackup_client
```

Все дальнейшие операции по резервному копированию и восстановлению шаблонов и виртуальных машин Proxmox должны выполняться под учетной записью root.

Необходимо определить следующие переменные среды (добавить следующие строки в файл /root/.bashrc):

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

Для целей тестирования рекомендуется включить режим verbose в конфигурационном файле /opt/rubackup/etc/config.file:

```
# RuBackup configuration file
# created by rb_init
#
#
use-local-backup-directory /rubackup-tmp
node client
logfile /opt/rubackup/log/RuBackup.log
who-is-primary-server antares
local-schedule-file /opt/rubackup/etc/rubackup.lsf
client-inet-interface eth0
parallelizm 8
verbose yes
rbd_algorythm sha
rbd_block_size 1048576
rbd_hash_length 512
digital-signature yes
digital-sign-hash sha1
client-shutdown scenario cancel-if-tasks
```

После изменения конфигурационного файла необходимо перезапустить клиента RuBackup.

По окончании данной процедуры клиент RuBackup настроен. Для возможности выполнения резервного копирования потребуется авторизация клиента системным администратором СРК.

Мастер-ключ

В ходе установки клиента RuBackup будет создан мастер-ключ для защитного преобразования резервных копий, а также ключи для электронной подписи, если предполагается использовать электронную подпись.

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

Важно! Ключи рекомендуется после создания скопировать на внешний носитель, а также распечатать бумажную копию и убрать эти копии в надёжное место.

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

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

Удаление клиента RuBackup

Удаление клиента RuBackup возможно из-под учетной записи с административными правами.

Удалить сервис rubackup-client:

```
# systemctl disable rubackup-client

# systemctl daemon-reload
```

Удалить клиента RuBackup можно следующим способом:

```
# apt remove rubackup-proxmox

# apt remove rubackup-client
```

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

Защитное преобразование резервных копий

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

Защитное преобразование осуществляется входящей в состав RuBackup утилитой `rbcrypt`. Ключ для защитного преобразования резервных копий располагается на хосте клиента в файле `/opt/rubackup/keys/master-key`. Защитное преобразование данных при помощи `rbcrypt` возможно с длиной ключа 256 бит (по умолчанию), а также 128, 512 или 1024 бита в зависимости от выбранного алгоритма преобразования.

Автоматическое защитное преобразование и обратное преобразование резервных копий клиентом RuBackup возможны при помощи ключей длиной 256 бит, однако утилита rbcryt поддерживает ключи длиной 128, 256, 512 и 1024 бита (в зависимости от выбранного алгоритма преобразования). Если необходимо для правила глобального расписания выбрать особый режим преобразования, с длиной ключа, отличной от 256 бит и с ключом, располагающемся в другом месте, то вы можете воспользоваться возможностью сделать это при помощи скрипта, выполняющегося после выполнения резервного копирования (определяется в правиле глобального расписания администратором RuBackup). При этом необходимо, чтобы имя преобразованного файла осталось таким же, как и ранее, иначе задача завершится с ошибкой. Провести обратное преобразование такого файла после восстановления его из резервной копии следует вручную при помощи утилиты преобразования. При таком режиме работы нет необходимости указывать алгоритм преобразования в правиле резервного копирования, либо архив будет преобразован ещё раз автоматически с использованием мастер-ключа.

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

Таблица 1 – Алгоритмы защитного преобразования, доступные в утилите `rbcrypt`

Алгоритм	Длина ключа, бит	Примечание
Anubis	128, 256	
Aria	128, 256	
CAST6	128, 256	
Camellia	128, 256	
Kalyna	128, 256, 512	Украинский национальный стандарт ДСТУ 7624:2014
Kuznyechik	256	Российский национальный стандарт ГОСТ Р 34.12-2015
MARS	128, 256	
Rijndael	128, 256	Advanced Encryption Standard (AES)
Serpent	128, 256	
Simon	128	
SM4	128	Китайский национальный стандарт для беспроводных сетей
Speck	128, 256	
Threefish	256, 512, 1024	
Twofish	128, 256	

Локальный лист ограничений

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

Наименование ресурса (VMID виртуальной машины), 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 лист ограничений его необходимо создать из-под учетной записи с административными привилегиями.

Подготовка виртуальной машины для выполнения резервного копирования средствами RuBackup

Для виртуальной машины необходимо включить возможность взаимодействия с гостевыми дополнениями (рисунок 11):

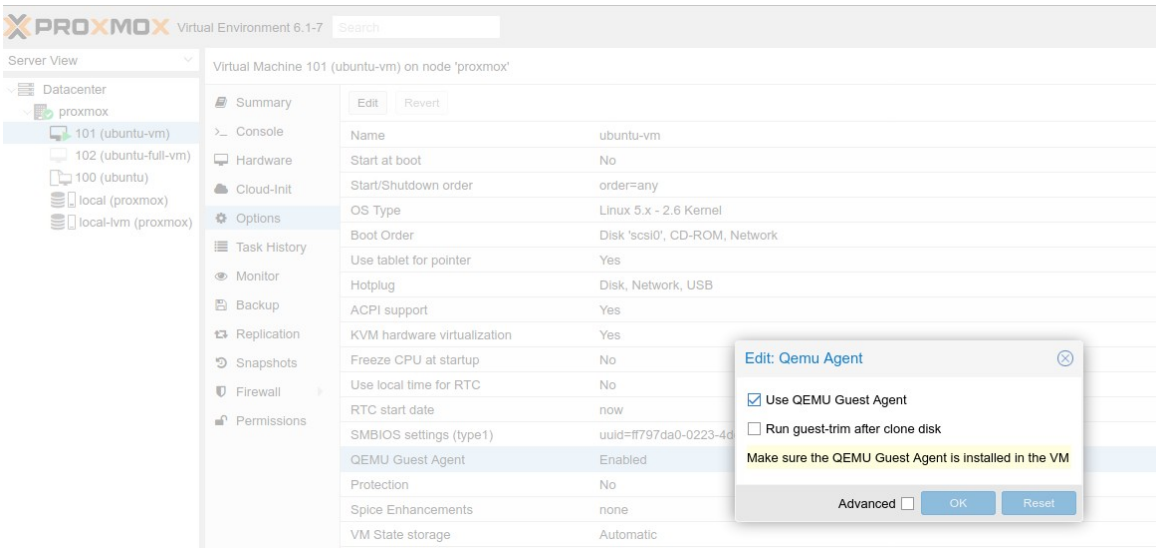


Рисунок 1

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.

Менеджер 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.

Для запуска менеджера администратора RBM необходимо выполнить команду:

```
# ssh -X user@rubackup_server

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

На вкладке **Объекты** в левой части представлен список клиентов системы резервного копирования, в котором указано имя, уникальный HWID и описание. Клиенты, которые в данный момент находятся в online, будут отмечены зеленым цветом. Клиенты в состоянии offline – красным (рисунок 2):

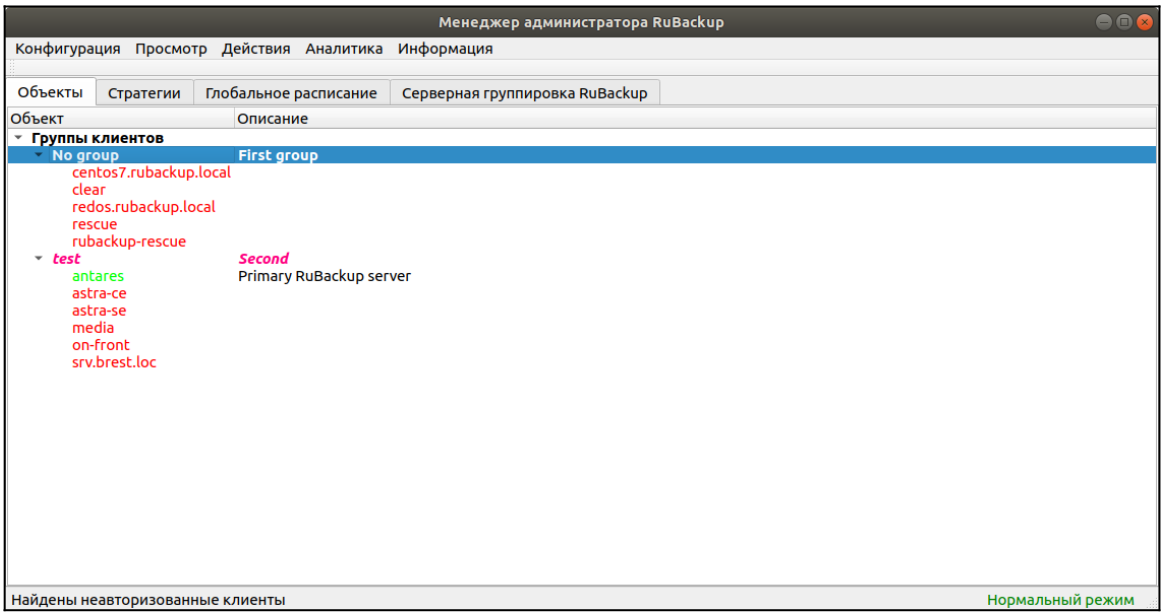


Рисунок 2

В том случае, если клиент RuBackup был установлен, но не авторизован, в нижней части окна RBM будет сообщение о том, что найдены неавторизованные клиенты. Все новые клиенты должны быть авторизованы в системе резервного копирования. Все новые клиенты должны быть авторизованы в системе резервного копирования:

Для авторизации неавторизованного клиента в RBM выполните следующие действия:

1 Откройте меню **Действия → Клиенты → Авторизовать клиентов** (рисунок 3):

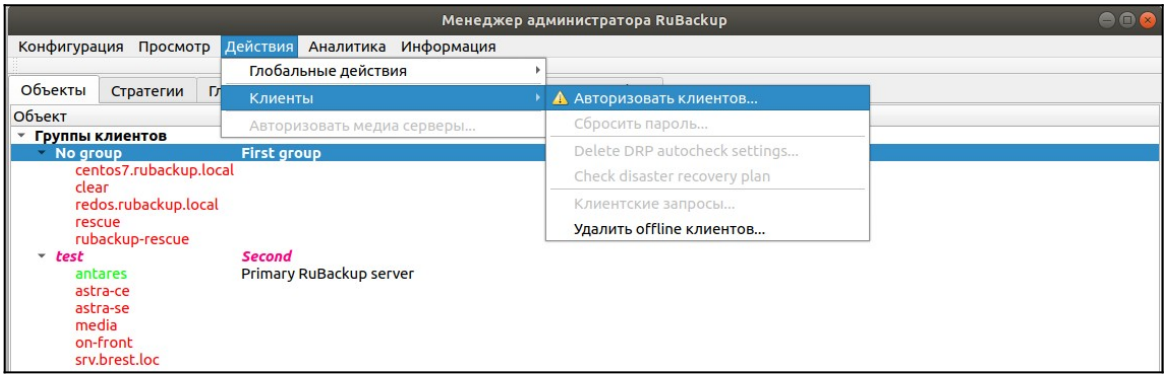


Рисунок 3

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

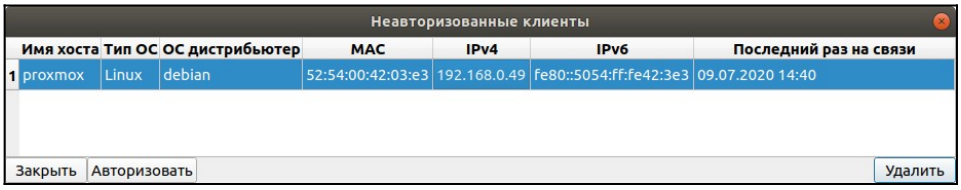


Рисунок 4

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

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).

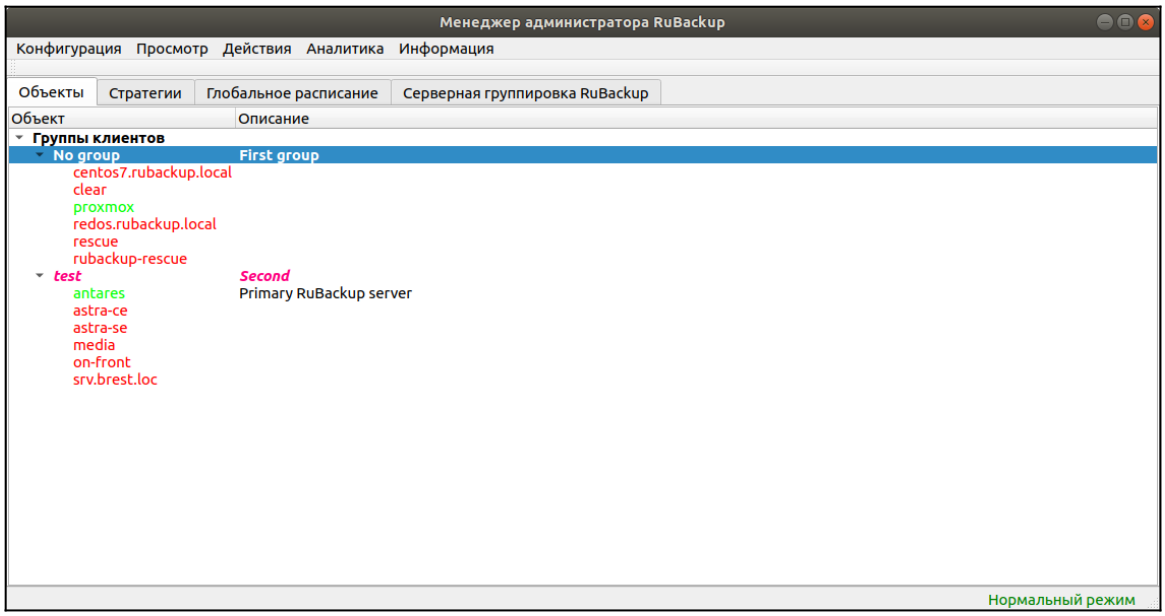


Рисунок 5

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

Для этого необходимо выполнить следующие действия:

1. Выбрать клиентский хост, на котором установлен Proxmox и добавить правило резервного копирования (рисунок 6):

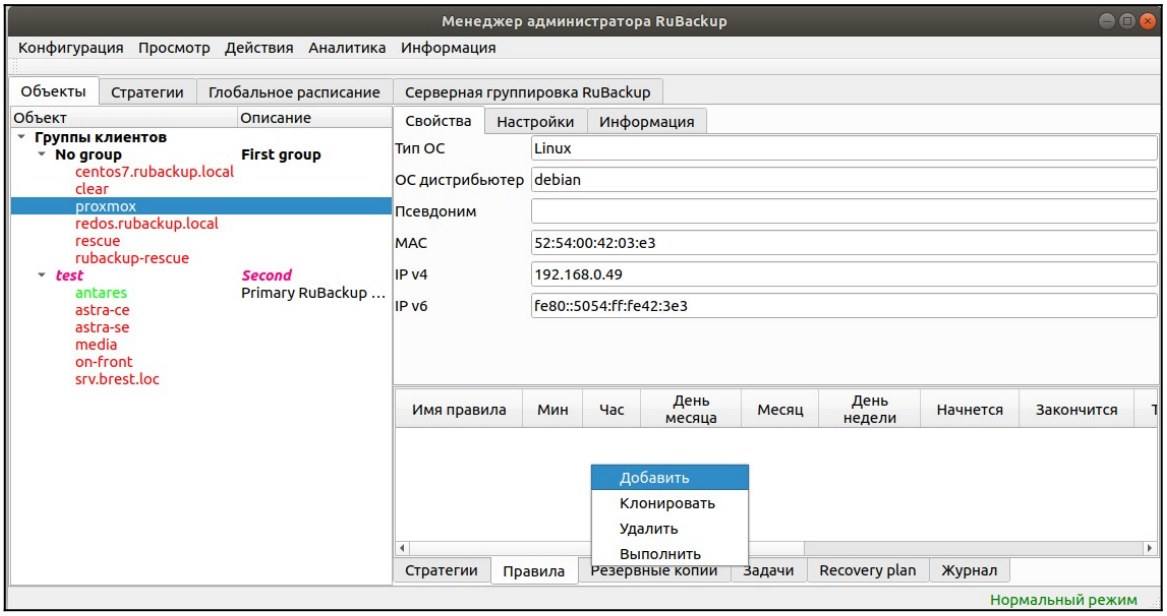


Рисунок 6

2. Выбрать тип ресурса «*Proxmox VM*» или «*Proxmox container*» (рисунок 7):

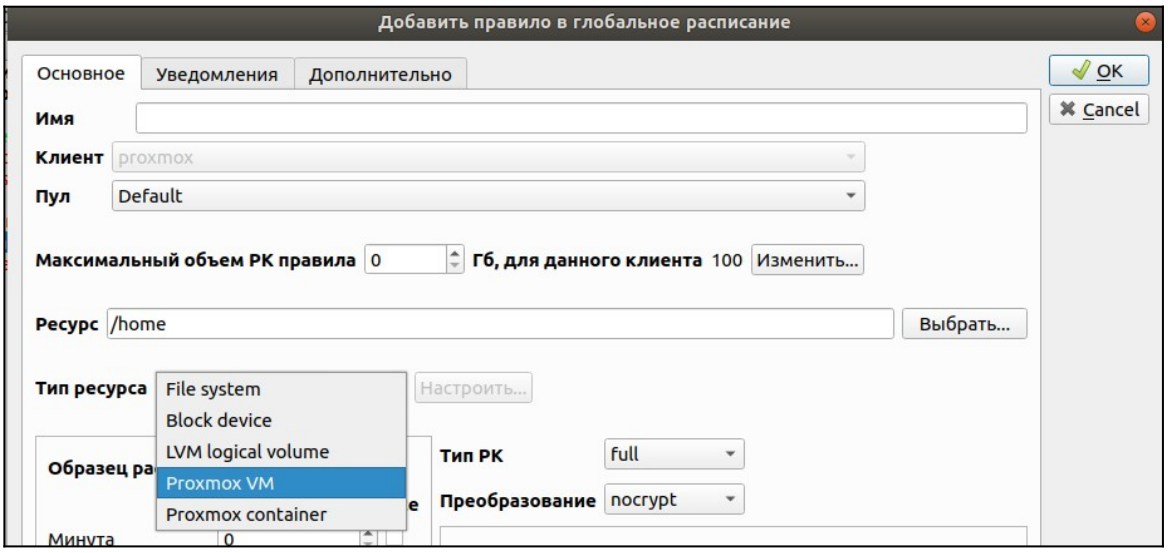


Рисунок 7

3. Выбрать ресурс, для которого будет выполняться правило (рисунок 8):

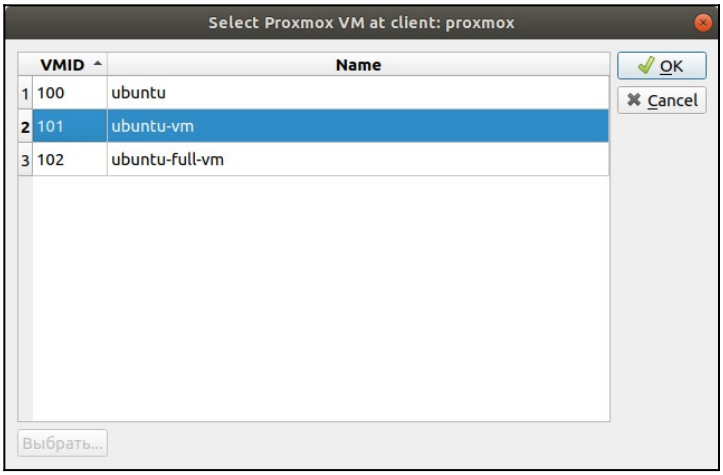


Рисунок 8

4. Установить 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 9).

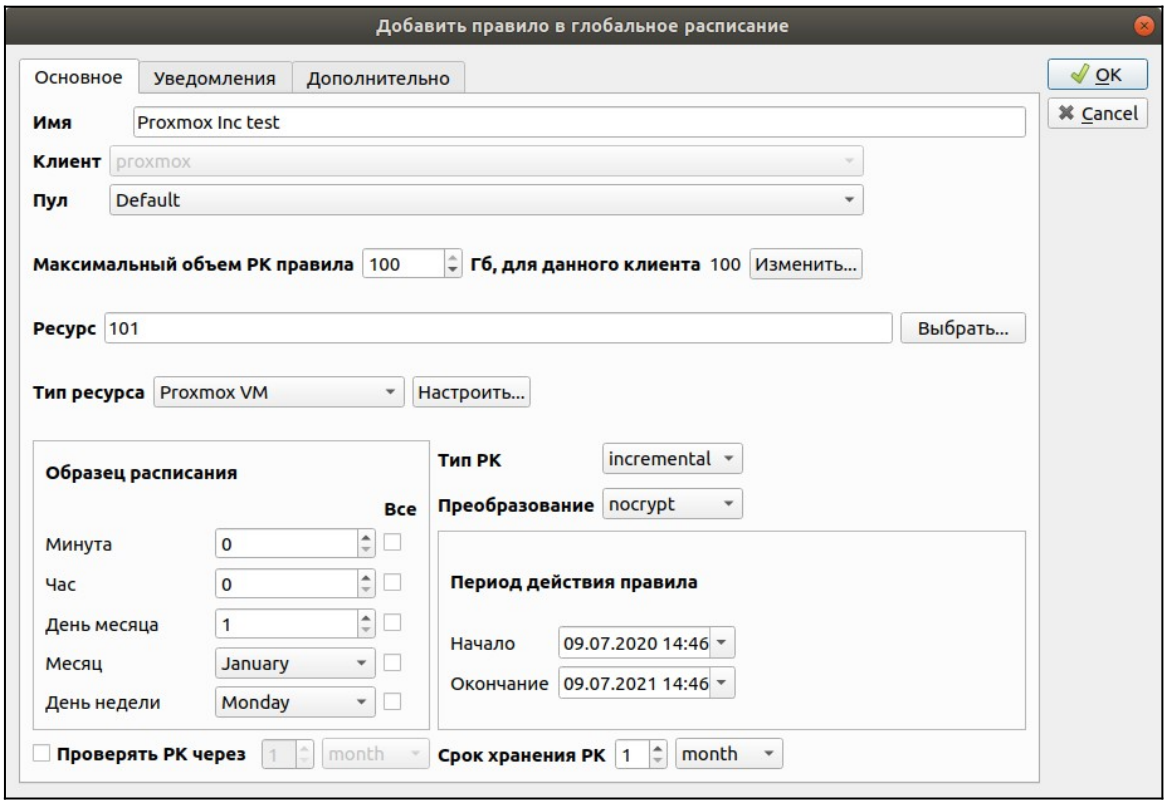


Рисунок 9

5. Правила для выполнения резервных копий виртуальных машин могут иметь дополнительные настройки (рисунок 10).

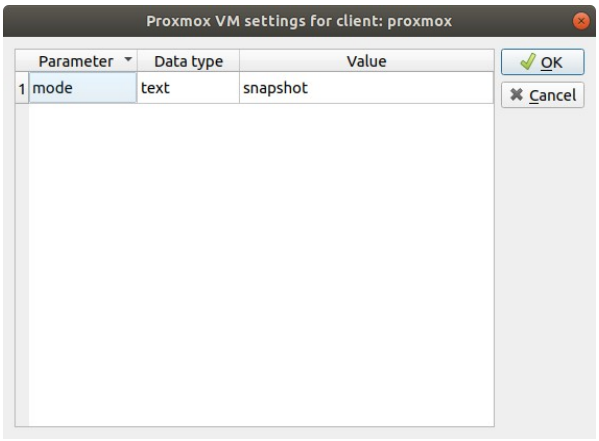


Рисунок 10

Описание параметра и его значения представлены в таблице 2.

Таблица 2 – Описание параметра настройки

Параметр	Описание	Значение по умолчанию	Допустимые значения
mode	Способ выполнения резервной копии	snapshot	snapshot, suspend, stop

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.

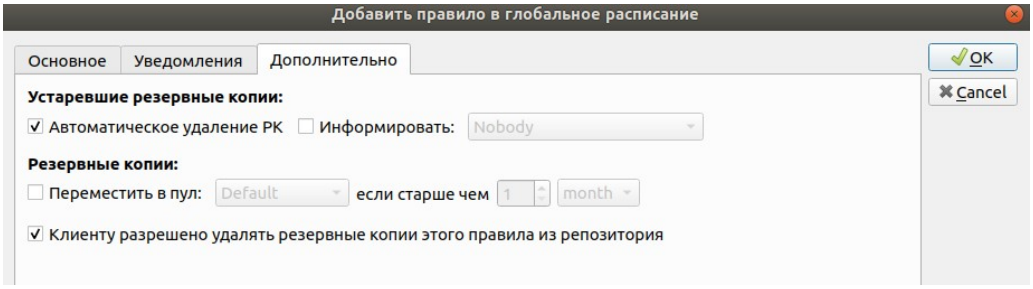


Рисунок 11

Вновь созданное правило будет обладать статусом «wait», это означает что оно не будет порождать задач на выполнение резервного копирования до той поры, пока администратор RuBackup не запустит его и оно изменит свой статус на «run». При необходимости работу правила можно будет приостановить или запустить в любой момент времени по желанию администратора. Так же администратор может инициировать немедленное создание задачи при статусе правила «wait».

Правило глобального расписания имеет срок жизни, определяемый при его создании, а так же предусматривает следующие возможности:

1) Выполнить скрипт на клиенте (то есть на хосте Proxmox) перед началом резервного копирования.

2) Выполнить скрипт на клиенте после успешного окончания резервного копирования.

3) Выполнить скрипт на клиенте после неудачного завершения резервного копирования.

4) Выполнить преобразование резервной копии на клиенте.

5) Периодически выполнять проверку целостности резервной копии.

6) Хранить резервные копии определённый срок, а после его окончания удалять их из хранилища резервных копий и из записей репозитория, либо просто уведомлять пользователей системы резервного копирования об окончании срока хранения.

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

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

При создании задачи RuBackup она появляется в главной очереди задач. Отслеживать исполнение правил может как администратор, с помощью RBM, так клиент при помощи RBC.

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

Менеджер клиента RuBackup (RBC)

Принцип взаимодействия клиентского менеджера (RBC) с системой резервного копирования состоит в том, что пользователь может сформировать ту или иную команду (желаемое действие) и отправить его серверу резервного копирования RuBackup. Взаимодействие пользователя с сервером резервного копирования производится через клиента (фоновый процесс) резервного копирования. Клиентский менеджер отправляет команду пользователя клиенту, клиент отправляет её серверу. В том случае, если действие допустимо, то сервер RuBackup отдаст обратную команду клиенту и/или перенаправит её медиасерверу RuBackup для дальнейшей обработки. Это означает, что, как правило, 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 клиент отдал какую-либо команду при помощи RBC, он может просто закрыть приложение, все действия будут выполнены системой резервного копирования (тем не менее, 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 proxmox):

```
# ssh -X root@proxmox
```

```
root@proxmox:~# rbc&
[1] 31243
root@proxmox:~# Logfile is /opt/rubackup/log/RuBackup.log
```

Пользователь, запускающий RBC, должен входить в группу rubackup.

При первом запуске клиентского менеджера необходимо задать пароль, при помощи которого впоследствии можно будет запросить восстановление резервной копии (рисунок 12). Без ввода пароля получить резервную копию для клиента из хранилища невозможно. Хэш пароля восстановления хранится в базе данных RuBackup сервера. При необходимости можно изменить пароль при помощи клиентского менеджера (меню «**Конфигурация**» → «**Изменить пароль**»).

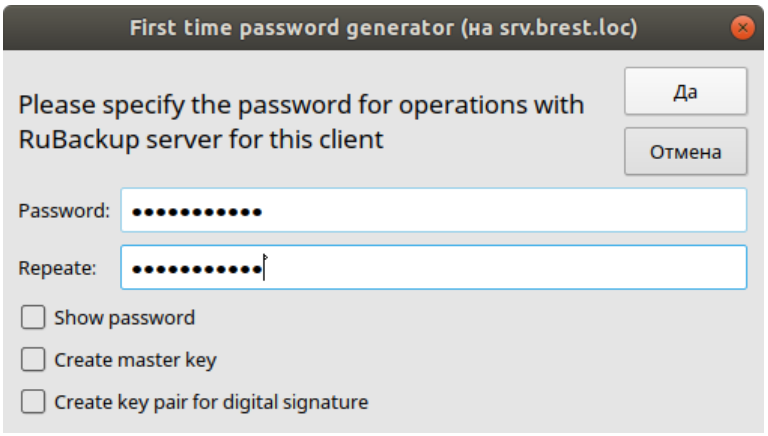


Рисунок 12

В случае успешного выполнения (рисунок :

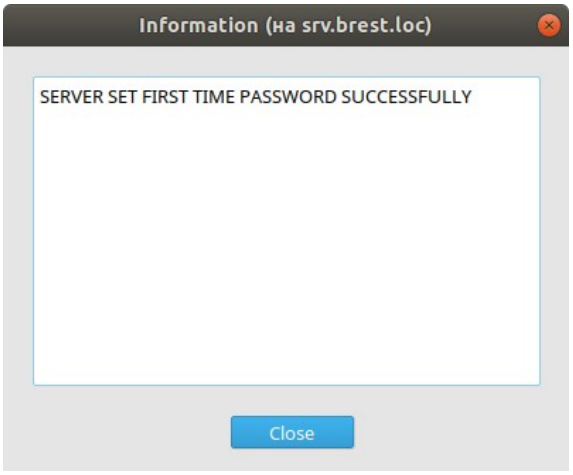
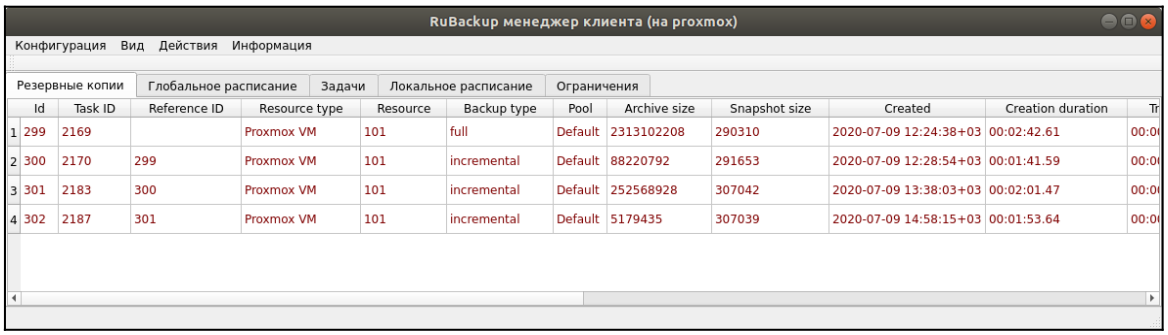


Рисунок 13

Главная страница RBC содержит переключающиеся вкладки, позволяющие управлять резервными копиями, расписанием резервного копирования, а также просматривать текущие задачи клиента, локальное расписание и ограничения.

Вкладка «Резервные копии»

В таблице вкладки «Резервные копии» содержится информация обо всех резервных копиях клиента, которые хранятся в репозитории RuBackup (рисунок 14). Дифференциальные резервные копии ссылаются на полные резервные копии, инкрементальные резервные копии ссылаются на полные резервные копии или предыдущие инкрементальные, так что при необходимости восстановить данные можно одной командой инициировать восстановление всей цепочки резервных копий.



	Id	Task ID	Reference ID	Resource type	Resource	Backup type	Pool	Archive size	Snapshot size	Created	Creation duration	Tr
1	299	2169		Proxmox VM	101	full	Default	2313102208	290310	2020-07-09 12:24:38+03	00:02:42.61	00:0
2	300	2170	299	Proxmox VM	101	incremental	Default	88220792	291653	2020-07-09 12:28:54+03	00:01:41.59	00:0
3	301	2183	300	Proxmox VM	101	incremental	Default	252568928	307042	2020-07-09 13:38:03+03	00:02:01.47	00:0
4	302	2187	301	Proxmox VM	101	incremental	Default	5179435	307039	2020-07-09 14:58:15+03	00:01:53.64	00:0

Рисунок 14

Во вкладке «Резервные копии» пользователю доступны следующие действия:

Удалить выбранную резервную копию.

Это действие возможно в том случае, если в правиле глобального расписания есть соответствующее разрешение. Кроме того, при необходимости выполнить удаление резервной копии потребуется вести пароль клиента.

Восстановить цепочку резервных копий.

Это действие запускает процесс восстановления цепочки резервных копий на локальной файловой системе клиента.

При восстановлении резервной копии или цепочки резервных копий клиент должен выбрать место для восстановления файлов резервной копии. Рекомендуется использовать либо временный каталог для операций с резервными копиями (например, `/rubackup-tmp`). RBC не ожидает окончания восстановления всех резервных копий. Клиент должен проконтролировать на вкладке «Задачи» успешное завершение созданных задач 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. параметр `use-local-backup-directory`).

Проверить резервную копию.

Это действие инициирует создание задачи проверки резервной копии. В том случае, если резервная копия была подписана цифровой подписью, то будет проверены размер файлов резервной копии, md5 сумма и проверена сама резервная копия. Если резервная копия не была подписана цифровой подписью, то будут проверены размер файлов резервной копии и md5 сумма.

Вкладка «Глобальное расписание»

В таблице вкладки «Глобальное расписание» содержится информация обо всех правилах в глобальном расписании RuBackup для этого клиента. (рисунок 15).

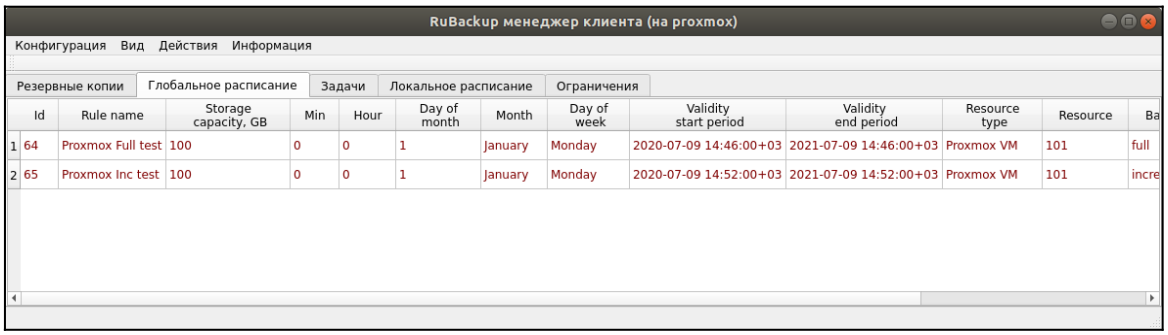


Рисунок 15

Во вкладке «Глобальное расписание» пользователю доступны следующие действия:

Запросить новое правило.

Это действие вызывает диалог подготовки нового правила в глобальном расписании RuBackup для данного клиента. Запрос на добавление правила требует одобрения администратора RuBackup, одобрение может быть сделано в оконном менеджере администратора RuBackup.

Запросить удалить правило из глобального расписания.

Это действие формирует запрос к администратору RuBackup об удалении выбранного пользователем правила из глобального расписания RuBackup. Запрос на удаление правила требует одобрения администратора RuBackup, одобрение может быть сделано в оконном менеджере администратора RuBackup.

Вкладка «Задачи»

В таблице вкладки «Задачи» содержится информация обо всех задачах в главной очереди заданий RuBackup для этого клиента (рисунок 16). В зависимости от настроек резервного сервера RuBackup выполненные задачи и задачи, завершившиеся неудачно, через какое-то время могут быть автоматически удалены из главной очереди задач. Информация о выполнении заданий фиксируется в специальном журнале задач сервера RuBackup, при необходимости статус любой задачи, даже удалённой из очереди, можно уточнить у администратора RuBackup. Так же информация о выполнении задач клиента заносится в локальный журнальный файл на клиенте. В клиентском менеджере можно открыть окно отслеживания журнального файла (меню «**Информация**» → «**Журнальный файл**»).

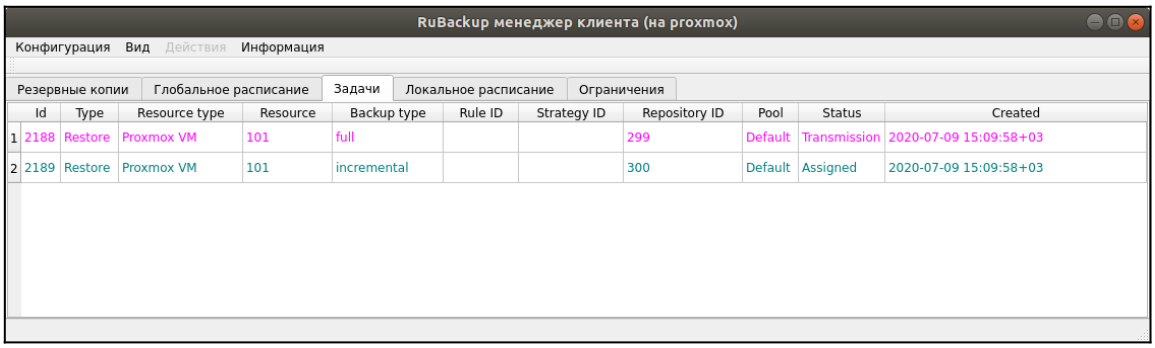


Рисунок 16

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_archives

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

```
root@proxmox:~# rb_archives
Set password:
Repeate password:
Id  | Ref ID | Resource | Resource type | Backup type | Created               | Crypto  | Signed | Status
----+--------+----------+---------------+-------------+-----------------------+---------+--------+-------------------
299 |        | 101      | Proxmox VM    | full        | 2020-07-09 12:24:38+03 | nocrypt | True   | Not Verified
300 | 299    | 101      | Proxmox VM    | incremental | 2020-07-09 12:28:54+03 | nocrypt | True   | Not Verified
301 | 300    | 101      | Proxmox VM    | incremental | 2020-07-09 13:38:03+03 | nocrypt | True   | Not Verified
```

rb_schedule

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

```
root@proxmox:~# rb_schedule
Id | Name              | Resource type | Resource | Backup type | Status
---+-------------------+---------------+----------+-------------+-------
64 | Proxmox Full test | Proxmox VM    | 101      | full        | wait
65 | Proxmox Inc test  | Proxmox VM    | 101      | incremental | wait
root@proxmox:~#
```

rb_tasks

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

```
root@proxmox:~# rb_tasks
Id   | Task type     | Resource | Backup type | Status | Created
-----+---------------+----------+-------------+--------+-----------------------
2187 | Backup global | 101      | incremental | Done   | 2020-07-09 14:56:20+03
root@proxmox:~#
```

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

Восстановление резервной копии виртуальной машины

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

```
root@proxmox:~# rb_archives
Id  | Ref ID | Resource | Resource type | Backup type | Created               | Crypto  | Signed | Status
----+--------+----------+---------------+-------------+-----------------------+---------+--------+-------------------
299 |        | 101      | Proxmox VM    | full        | 2020-07-09 12:24:38+03 | nocrypt | True   | Not Verified
300 | 299    | 101      | Proxmox VM    | incremental | 2020-07-09 12:28:54+03 | nocrypt | True   | Not Verified
301 | 300    | 101      | Proxmox VM    | incremental | 2020-07-09 13:38:03+03 | nocrypt | True   | Not Verified
302 | 301    | 101      | Proxmox VM    | incremental | 2020-07-09 14:58:15+03 | nocrypt | True   | Not Verified
```

В приведенном примере в системе резервного копирования присутствуют четыре резервные копии. Виртуальная машина с идентификатором 101 может быть восстановлена с использованием инкрементальной резервной копии с идентификатором 300. Для этого необходимо выполнить команду

```
# rb_archives -x 300
```

В случае успешно принятой задачи команда вернет список созданных задач, а восстановление будет происходить в фоновом режиме.

Проконтролировать процесс восстановления можно при помощи rb_task:

```
root@proxmox:~# rb_tasks
Id   | Task type | Resource | Backup type | Status       | Created
-----+-----------+----------+-------------+--------------+-----------------------
2189 | Restore   | 101      | incremental | Done         | 2020-07-09 15:09:58+03
2190 | Restore   | 101      | full        | Done         | 2020-07-09 15:19:38+03
2191 | Restore   | 101      | incremental | Transmission | 2020-07-09 15:19:38+03
```

или при помощи RBC:

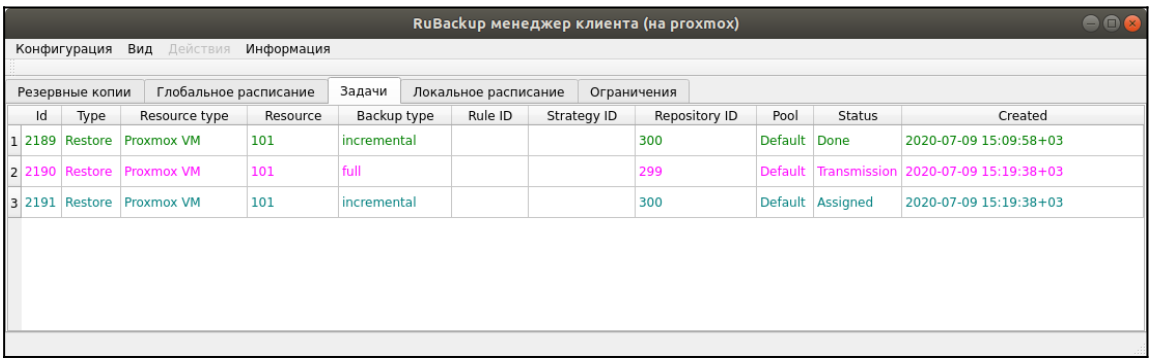


Рисунок 17

Кроме того, можно детально проконтролировать происходящее при помощи журнала:

```
Set status for task ID: 2191 from: Finish_Transfer to: Execution
File: /root/proxmox_TaskID_2169_RuleID_61_D2020_7_9H12_21_34_BackupType_1_Resour
ceType_23/disk-drive-scsi0.raw was patched by /root/proxmox_TaskID_2170_RuleID_6
3_D2020_7_9H12_27_12_BackupType_2_ResourceType_23/disk-drive-scsi0.raw.pt
File: /root/proxmox_TaskID_2169_RuleID_61_D2020_7_9H12_21_34_BackupType_1_Resour
ceType_23/disk-drive-scsi1.raw was patched by /root/proxmox_TaskID_2170_RuleID_6
3_D2020_7_9H12_27_12_BackupType_2_ResourceType_23/disk-drive-scsi1.raw.pt
Try to restore VM with VMID: 101
VMID: 101 exists. Try to get another VMID...
VM will be restored with new VMID: 103
Congratulations!!! VM was restored with VMID: 103
Set status for task ID: 2191 from: Execution to: Done
Task was done. ID: 2191
```

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.

Виртуальная машина будет восстановлена с таким же VMID, как и у оригинальной в момент выполнения резервного копирования. Если виртуальная машина с этим VMID существует в системе, то восстановленной виртуальной машине будет присвоен первый свободный номер после оригинального. В примере выше виртуальная машина была восстановлена с VMID 103 (рисунок 18):

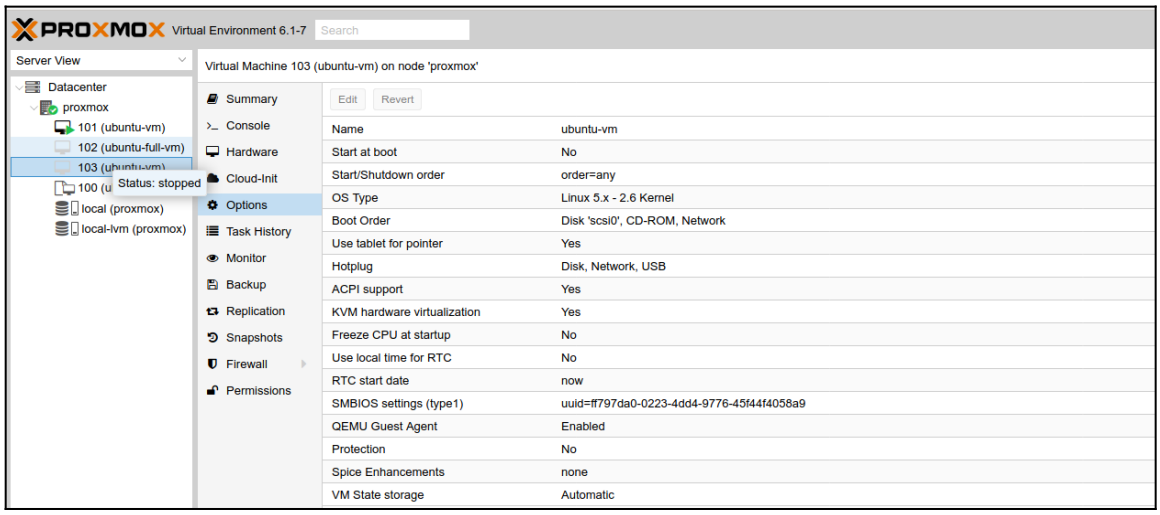


Рисунок 18

После восстановления можно запустить и проверить виртуальную машину (рисунок 19:

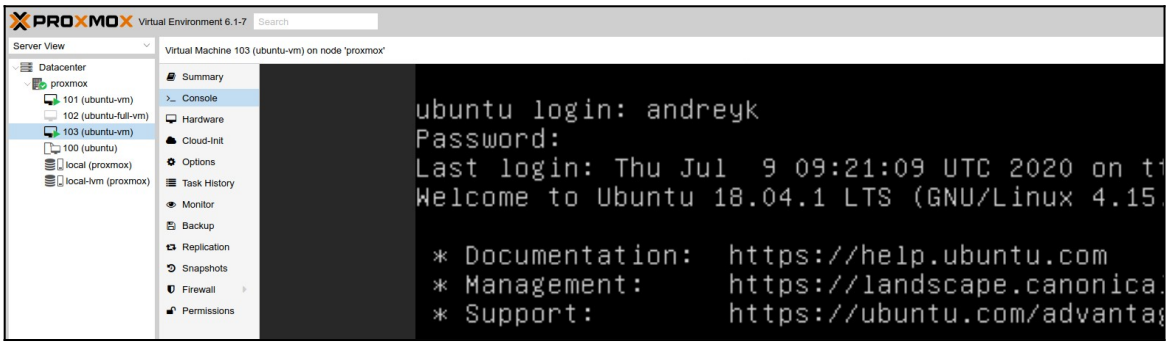


Рисунок 19

Восстановление резервной копии контейнера

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

```
root@proxmox:/rubackup-tmp# rb_archives
Id  | Ref ID | Resource | Resource type     | Backup type | Created               | Crypto  | Signed | Status
----+--------+----------+-------------------+-------------+-----------------------+---------+--------+-----------------
299 |        | 101      | Proxmox VM        | full        | 2020-07-09 12:24:38+03 | nocrypt | True   | Not Verified
300 | 299    | 101      | Proxmox VM        | incremental | 2020-07-09 12:28:54+03 | nocrypt | True   | Not Verified
301 | 300    | 101      | Proxmox VM        | incremental | 2020-07-09 13:38:03+03 | nocrypt | True   | Not Verified
302 | 301    | 101      | Proxmox VM        | incremental | 2020-07-09 14:58:15+03 | nocrypt | True   | Not Verified
329 |        | 104      | Proxmox container | full        | 2020-07-15 18:30:19+03 | nocrypt | True   | Not Verified
330 |        | 101      | Proxmox VM        | full        | 2020-07-15 19:43:51+03 | nocrypt | True   | Not Verified
```

В приведенном примере в системе резервного копирования присутствует резервная копия контейнера в VMID 104, идентификатор резервной копии - 329.

Для этого необходимо выполнить команду:

```
# rb_archives -x 329
```

В случае успешно принятой задачи команда вернет список созданных задач, а восстановление будет происходить в фоновом режиме.

Проконтролировать процесс восстановления можно при помощи rb_task:

```
root@proxmox:/rubackup-tmp# rb_tasks
Id   | Task type | Resource | Backup type | Status       | Created
-----+-----------+----------+-------------+--------------+-----------------------
2304 | Restore   | 104      | full        | Transmission | 2020-07-15 19:57:14+03
```

или при помощи RBC (рисунок 20):

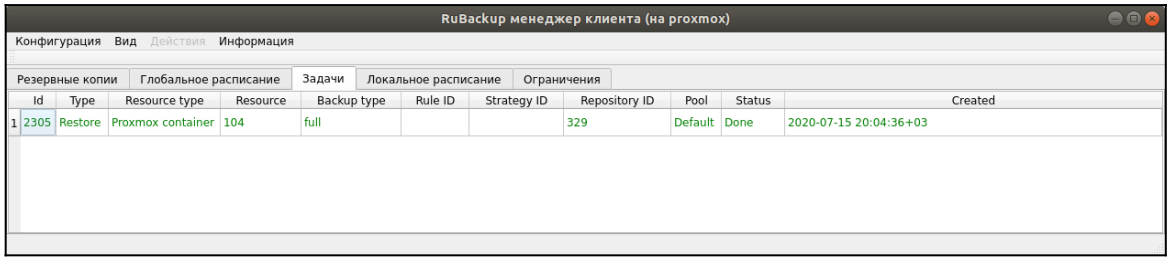


Рисунок 20

Кроме того, можно детально проконтролировать происходящее при помощи журнала:

```
Set status for task ID: 2305 from: Start_Transfer to: Transmission
Set status for task ID: 2305 from: Transmission to: Finish_Transfer
Set status for task ID: 2305 from: Finish_Transfer to: Execution
md5sum of transferred file is ok: 74d446238d1f17befbc73d58294a6ea6
Transfer file is succesed: /root/proxmox_TaskID_2300_RuleID_67_D2020_7_15H18_29
_57_BackupType_1_ResourceType_24.tar.gz
Execute OS command: /opt/rubackup/modules/rb_module_proxmox_container -r /root/
proxmox_TaskID_2300_RuleID_67_D2020_7_15H18_29_57_BackupType_1_ResourceType_24.
tar.gz -z 4 -e last:true,tmp_catalog:/rubackup-tmp,rbd_hash_algorithm:sha,rbd_h
ash_length:512,rbd_block_size:1048576,container_vmid:104,container_storage:loca
l-lvm,mode:snapshot -d /root 2>&1
Try to restore container with VMID: 104 into the storage: local-lvm
VMID: 104 exists. Try to get another VMID...
VM will be restored with new VMID: 106
Set status for task ID: 2305 from: Execution to: Done
Task was done. ID: 2305
```

Контейнер будет восстановлен с таким же VMID, как и у оригинального в момент выполнения резервного копирования, в то же самое хранилище. Если контейнер с этим VMID существует в системе, то восстановленному контейнеру будет присвоен первый свободный номер после оригинального. В примере выше контейнер был восстановлен с VMID 106 (рисунок 21):

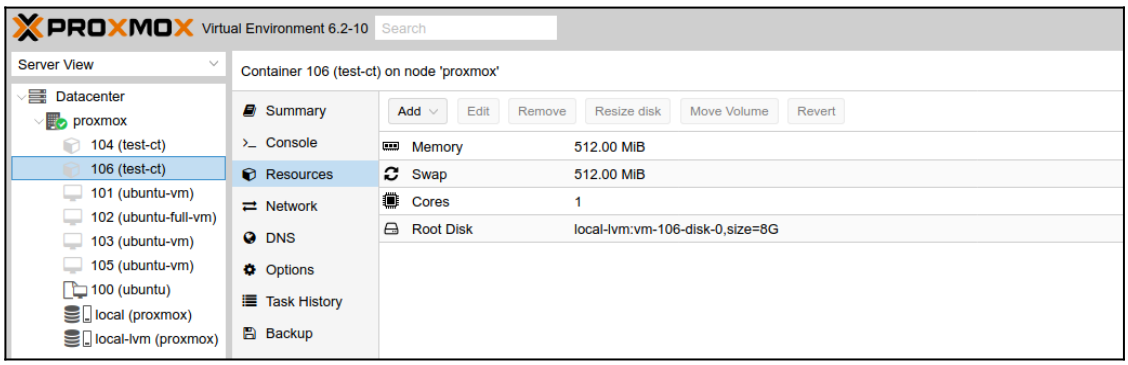


Рисунок 21

В том случае, если хранилища с таким же именем, в котором располагался оригинальный контейнер, в системе нет на момент восстановления резервной копии, то восстановление произойдет в первое хранилище, где могут располагаться контейнеры.

После восстановления можно запустить и проверить контейнер (рисунок 22):

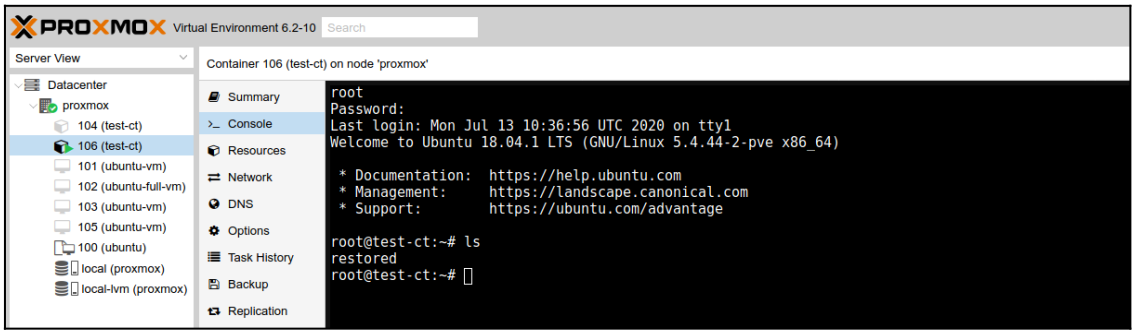


Рисунок 22

Поддерживаемые версии

Поддерживаемые версии ProxMox представлены в таблице 3.

Таблица 3 – Поддерживаемые версии ProxMox

Версия ProxMox	**rb_module_proxmox_vm**	**rb_module_proxmox_ container**
6.1-7/13e58d5e	Да	Нет
6.2-10/a20769ed	Да	Да