RuBackup
Система резервного копирования и восстановления данных

Резервное копирование

и восстановление виртуальных машин

среды виртуализации oVirt

Версия 1.10

2022 г.

Содержание

Введение....3

Установка клиента RuBackup....5

Мастер-ключ....8

Защитное преобразование резервных копий....9

- Алгоритмы защитного преобразования....10

Использование менеджера администратора RuBackup (RBM)....12

- Запуск RBM....12
- Регулярное резервное копирование виртуальной машины....14
- Срочное резервное копирование....18
- Централизованное восстановление резервных копий....19

Восстановление со стороны клиента....22

Введение

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

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.

Резервное копирование виртуальных машин oVirt выполняется безагентным способом. Это означает, что:

1) в саму виртуальную машину не устанавливается агент RuBackup (однако требуется установка гостевых расширений операционной системы, например qemu-guest-agent);

2) резервное копирование виртуальной машины выполняется целиком, для всех дисков виртуальной машины;

3) в ходе резервного копирования во всех случаях из резервной копии удаляются дублирующие блоки (всегда выполняется локальная дедупликация).

Резервное копирование возможно для виртуальных машин, которые находятся в состоянии online.

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

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

– на один из гипервизоров;

– на несколько гипервизоров в том случае, если это обусловлено необходимостью динамически распределять нагрузку в ходе резервного копирования или обеспечить возможность вывода того или иного гипервизора из эксплуатации без изменений в расписании резервного копирования; в данной схеме необходимо включить эти гипервизоры в кластерную группу клиентов системы резервного копирования.

При любой схеме установки клиент RuBackup имеет возможность выполнять резервное копирование и восстановление всех виртуальных машин среды виртуализации, вне зависимости от того на каком из узлов в настоящий момент функционирует виртуальная машина.

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

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

Поддерживаемые конфигурации

Версия oVirt 4.4

Поддерживаемые типы дисков: IMAGE.

Установка клиента RuBackup

Для возможности резервного копирования виртуальных машин среды виртуализации oVirt необходимо установить пакеты клиента RuBackup на выбранный гипервизор (гипервизоры), см. дистрибутив для oVirt:

- `rubackup-ovirt-common-1.9-1.el8.x86_64.rpm`

- `rubackup-ovirt-client-1.9-1.el8.x86_64.rpm`

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

Основные отличия работы клиента RuBackup в среде виртуализации oVirt состоят в следующем:

1) Клиент RuBackup всегда должен запускаться под пользователем vdsm. В том случае, если вам необходимо запустить клиента не как сервис, а в терминальном режиме, воспользуйтесь командами:

Для запуска клиента

```
# sudo -u vdsm /opt/rubackup/bin/rubackup_client start
```

Для остановки клиента

```
# sudo -u vdsm /opt/rubackup/bin/rubackup_client stop
```

2) В состав клиентского пакета включен только модуль для резервного копирования виртуальных машин oVirt, никаких других модулей в данной конфигурации не предусмотрено.

3) В состав клиентского пакета входят только утилиты командной строки, графический менеджер клиента RBC в состав пакета не включен.

4) Использование возможности автоматически предоставлять NFS файловую систему со стороны сервера резервного копирования для работы клиента oVirt не предусмотрено и не поддерживается.

5) Для создания и восстановления резервных копий на стороне клиента резервного копирования требуется специально выделенное пространство в размере, который составляет двукратный общий объем виртуальных машин, для которых выполняются одновременные операции резервного копирования или восстановления (например, для одновременного резервного копирования 10 виртуальных машин по 10Гб необходимо 200Гб выделенного пространства). При резервном копировании в режиме дедупликации это требование не является обязательным, т. к. весь обмен данными происходит без использования дискового пространства, однако для восстановления виртуальной машины из дедуплицированной резервной копии на клиенте

потребуется место для формирования дисков восстанавливаемой виртуальной машины.

6) Далее необходимо установить пакет *pigz*. Если в официальном репозитории нет компрессора *pigz*, то тогда сделать ссылку, прописав команду:

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

После распаковки пакетов *common* и *client* в файле */root/.bashrc* прописать следующую строчку:

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

Далее перезагрузить окружение:

```
. .bashrc
```

Затем создать создать конфигурационный файл через `rb_init`.

7) После создания каталога для работы с временными файлами (например, при выборе каталога */rubackup-tmp*) необходимо пользователю предоставить к нему доступ:

```
# chown vdsm:kvm /rubackup-tmp
```

Объем этого каталога должен быть не менее двукратного объема виртуальных машин, одновременное резервное копирование которых может выполняться.

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

В ходе инсталляции пакета в системе будет создан файл настроек доступа системы резервного копирования к API oVirt */opt/rubackup/etc/rb_module_ovirt.conf*:

```
engine https://ovirt-engine.yourdomain.local

grant_type password

username admin@internal

password 12345

ca_info      /opt/rubackup/keys/ovirt.ca.crt

timeout 30
```

Далее необходимо выполнить следующие действия:

1. Изменить в этом файле настройки для подключения к API, для чего:

   – создать сертификат доступа к API следующей командой:

```
# curl --output /opt/rubackup/keys/ovirt.ca.crt 'http://ovirt-
engine.yourdomain.local/ovirt-engine/services/pki-resource?
resource=ca-certificate&format=X509-PEM-CA'
```

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

```
Check additional RuBackup modules:
Try to check module: 'oVirt' ...
Execute OS command: /opt/rubackup/modules/rb_module_ovirt -t 2>&1
Module version: 1.9
oVirt version: 4.4
... module 'oVirt' was checked successfully
```

2. В ручном режиме проверить правильность настроек следующей командой:

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

3. После настройки клиента RuBackup дать права пользователю vdsm на использование ключей электронной подписи:

```
# chown -R *vdsm:kvm /opt/rubackup/keys
```

Мастер-ключ

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

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

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

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

```
$ hexdump /opt/rubackup/keys/master-key
0000000 79d1 4749 7335 e387 9f74 c67e 55a7 20ff
0000010 6284 54as 83a3 2053 4818 e183 1528 a343
 0000020
```

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.

Если для правила глобального расписания необходимо выбрать особый режим защитного преобразования с длиной ключа, отличной от 256 бит, и с ключом, расположенным в другом месте, то вы можете сделать это при помощи скрипта, выполняющегося после выполнения резервного копирования (определяется в правиле глобального расписания администратором RuBackup). При этом необходимо, чтобы имя преобразованного файла осталось таким же, как и ранее, иначе задача завершится с ошибкой. Провести обратное преобразование такого файла после восстановления его из архива следует вручную при помощи утилиты `rbcrypt`. При таком режиме работы нет необходимости указывать алгоритм преобразования в правиле резервного копирования, иначе архив будет повторно преобразован с использованием мастер-ключа.

Алгоритмы защитного преобразования

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

Таблица 1 – Алгоритмы защитного преобразования, доступные в утилите `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	

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 другими параметрами RuBackup.

Запуск RBM

Для запуска RBM следует выполнить команду:

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

При запуске RBM вам потребуется пройти аутентификацию. Уточните *login/password* для вашей работы у главного администратора СРК. Если вы главный администратор, то используйте для авторизации суперпользователя *rubackup* и тот пароль, который вы задали ему при инсталляции (рисунок 1).

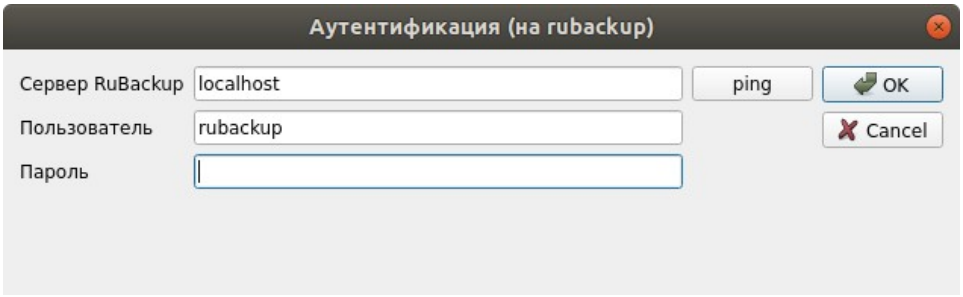


Рисунок 1

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).

Для резервного копирования клиент должен быть авторизован администратором RuBackup.

Если клиент RuBackup установлен, но не авторизован, в нижней части окна RBM появится сообщение о том, что найдены неавторизованные клиенты.

Все новые клиенты должны быть авторизованы в системе резервного копирования RuBackup.

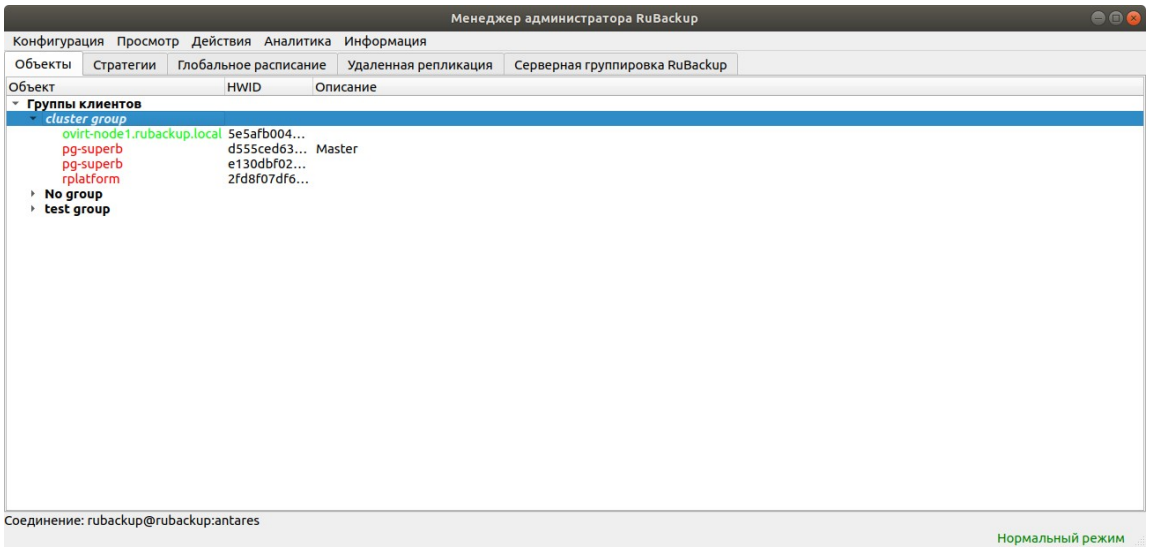


Рисунок 2

Для авторизации неавторизованного клиента в RBM необходимо выполнить следующие действия:

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

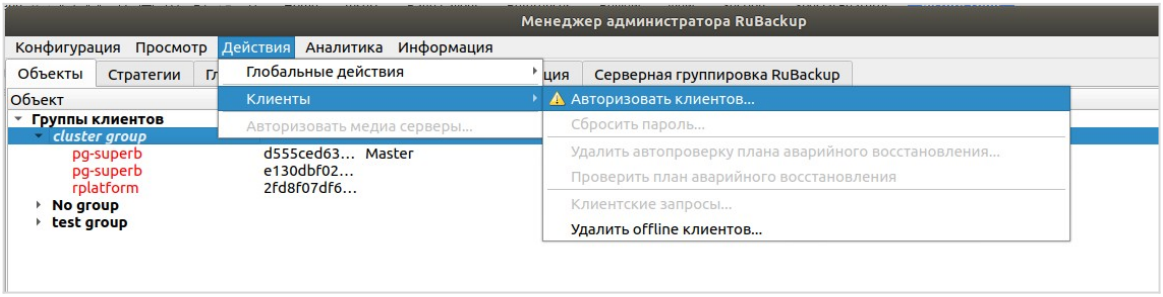


Рисунок 3

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

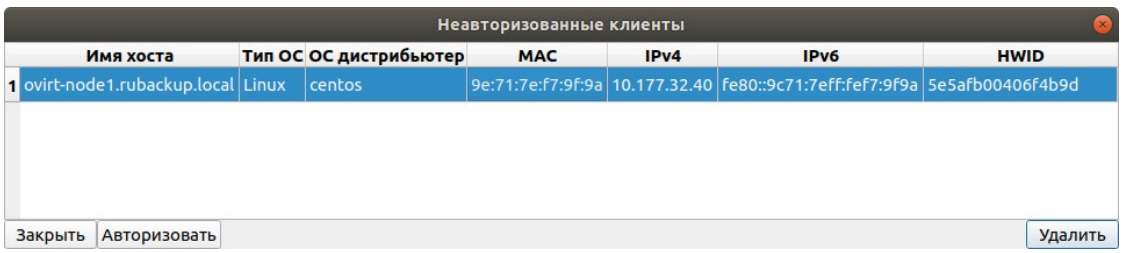


Рисунок 4

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

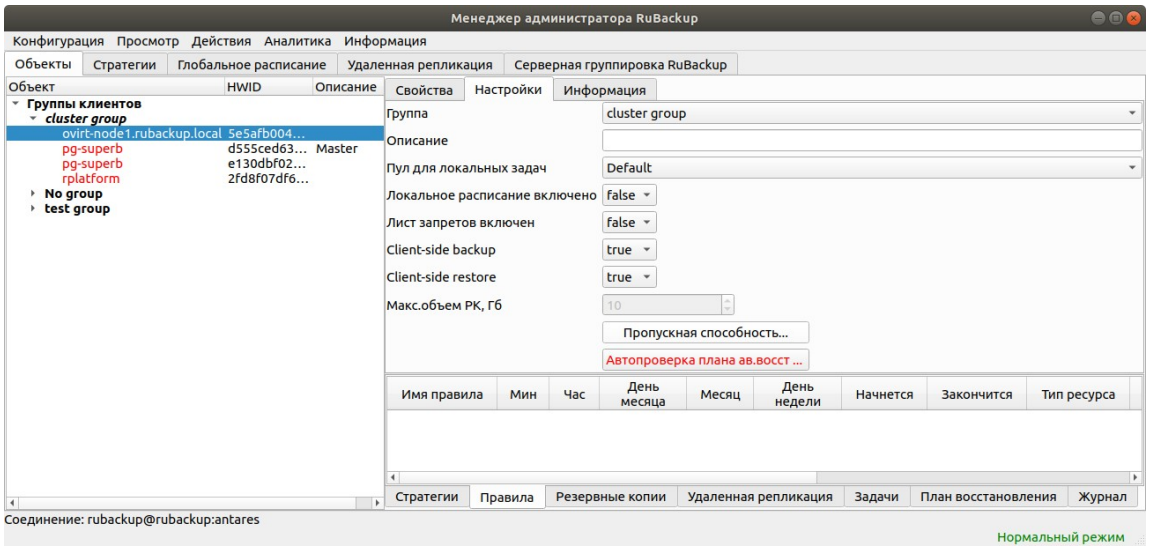


Рисунок 5

Регулярное резервное копирование виртуальной машины

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

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

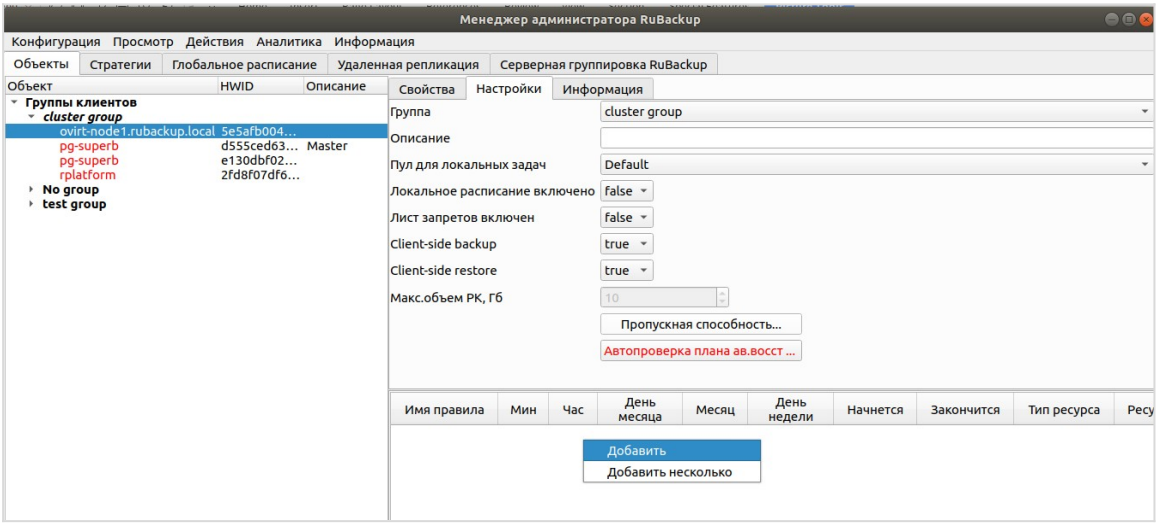


Рисунок 6

2. В среде виртуализации oVirt всегда доступно одно значение: «**oVirt**» (рисунок 7).

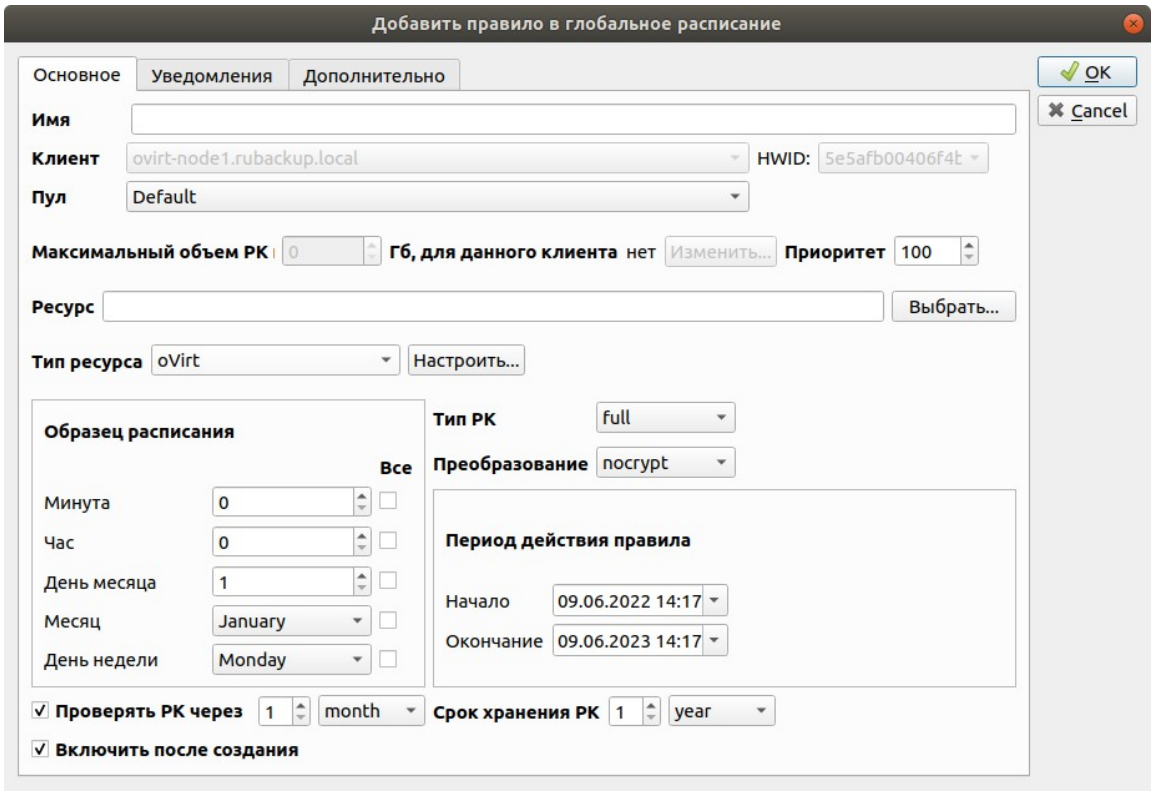


Рисунок 7

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

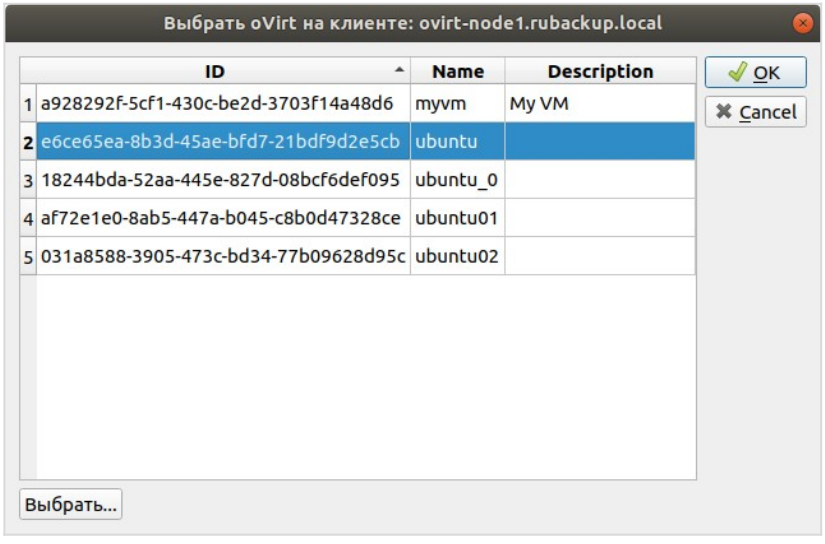


Рисунок 8

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

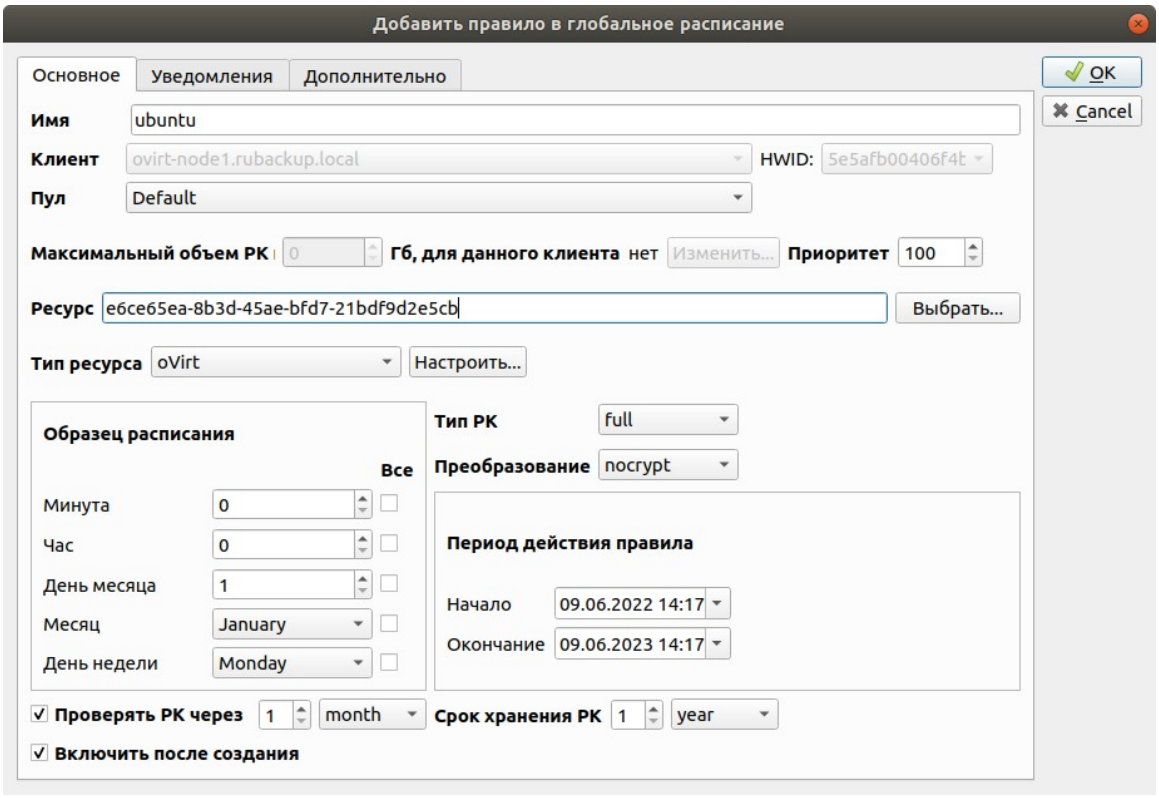


Рисунок 9

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

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

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

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

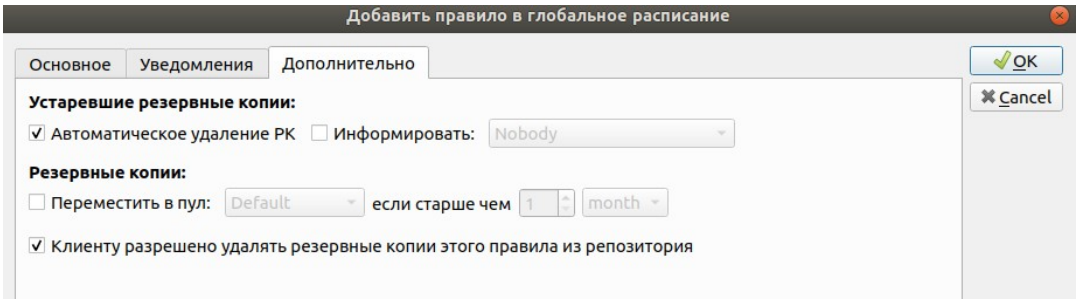


Рисунок 10

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

1) Выполнить скрипт на клиенте скрипт на клиенте перед началом резервного копирования.

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

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

4) Выполнить защитное 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 или утилит командной строки, так и клиент при помощи RBC или утилиты командной строки `rb_tasks`.

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

Срочное резервное копирование

В случае необходимости срочного резервного копирования созданного правила глобального расписания, следует вызвать правой кнопкой мыши контекстное меню «Выполнить» (рисунок 11):

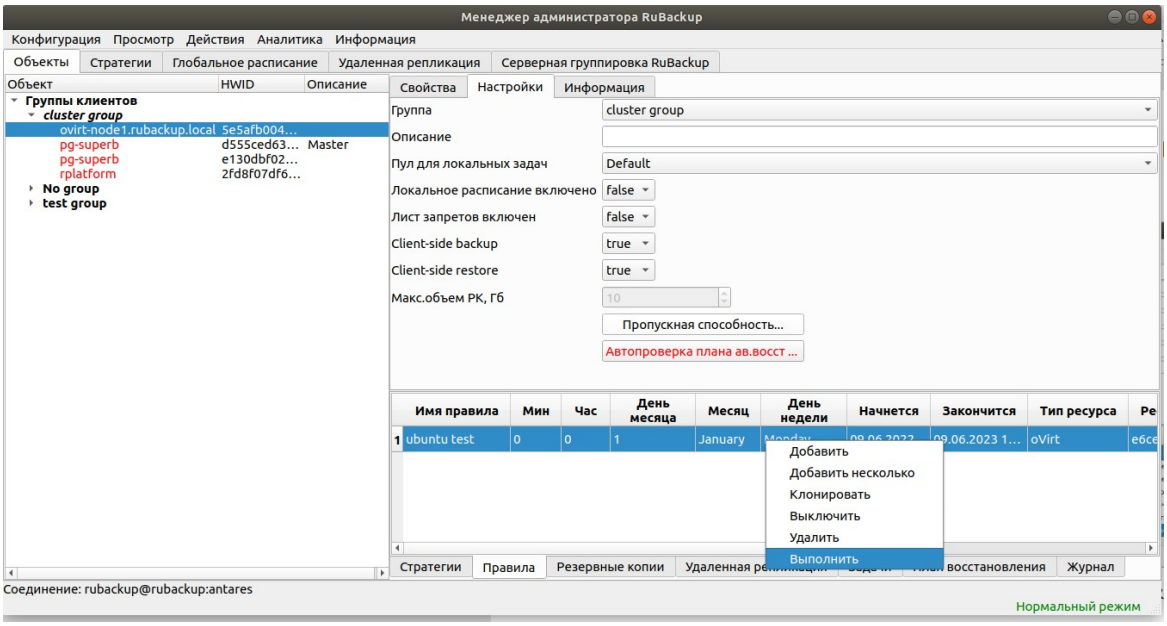
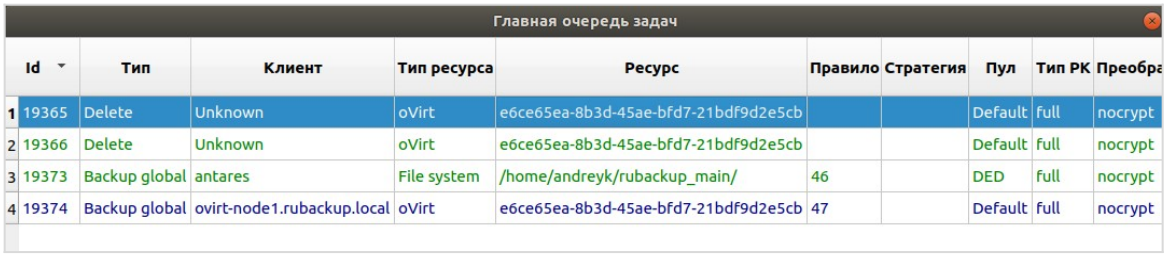


Рисунок 11

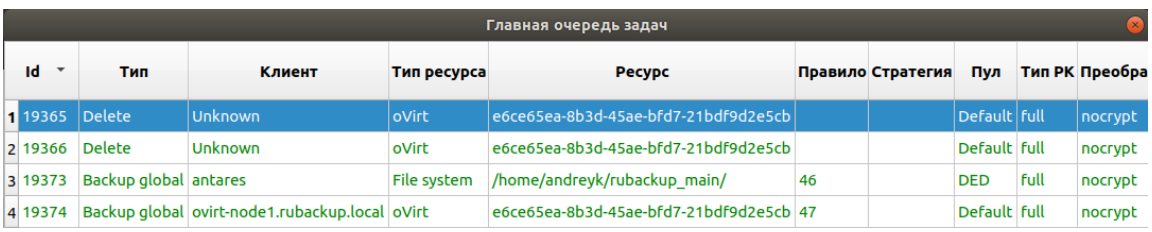
Проверить ход выполнения резервного копирования можно в окне «Главная очередь задач» (рисунок 12).



	Id	Тип	Клиент	Тип ресурса	Ресурс	Правило	Стратегия	Пул	Тип РК	Преобра
1	19365	Delete	Unknown	oVirt	e6ce65ea-8b3d-45ae-bfd7-21bdf9d2e5cb			Default	full	nocrypt
2	19366	Delete	Unknown	oVirt	e6ce65ea-8b3d-45ae-bfd7-21bdf9d2e5cb			Default	full	nocrypt
3	19373	Backup global	antares	File system	/home/andreyk/rubackup_main/	46		DED	full	nocrypt
4	19374	Backup global	ovirt-node1.rubackup.local	oVirt	e6ce65ea-8b3d-45ae-bfd7-21bdf9d2e5cb	47		Default	full	nocrypt

Рисунок 12

При успешном завершении резервного копирования появится окно (рисунок 13):



	Id	Тип	Клиент	Тип ресурса	Ресурс	Правило	Стратегия	Пул	Тип РК	Преобра
1	19365	Delete	Unknown	oVirt	e6ce65ea-8b3d-45ae-bfd7-21bdf9d2e5cb			Default	full	nocrypt
2	19366	Delete	Unknown	oVirt	e6ce65ea-8b3d-45ae-bfd7-21bdf9d2e5cb			Default	full	nocrypt
3	19373	Backup global	antares	File system	/home/andreyk/rubackup_main/	46		DED	full	nocrypt
4	19374	Backup global	ovirt-node1.rubackup.local	oVirt	e6ce65ea-8b3d-45ae-bfd7-21bdf9d2e5cb	47		Default	full	nocrypt

Рисунок 13

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 не желательно, например когда восстановление данных является зоной ответственности владельца клиентской системы, эта функциональность может быть отключена на клиенте (см. «Руководство системного администратора RuBackup»).

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

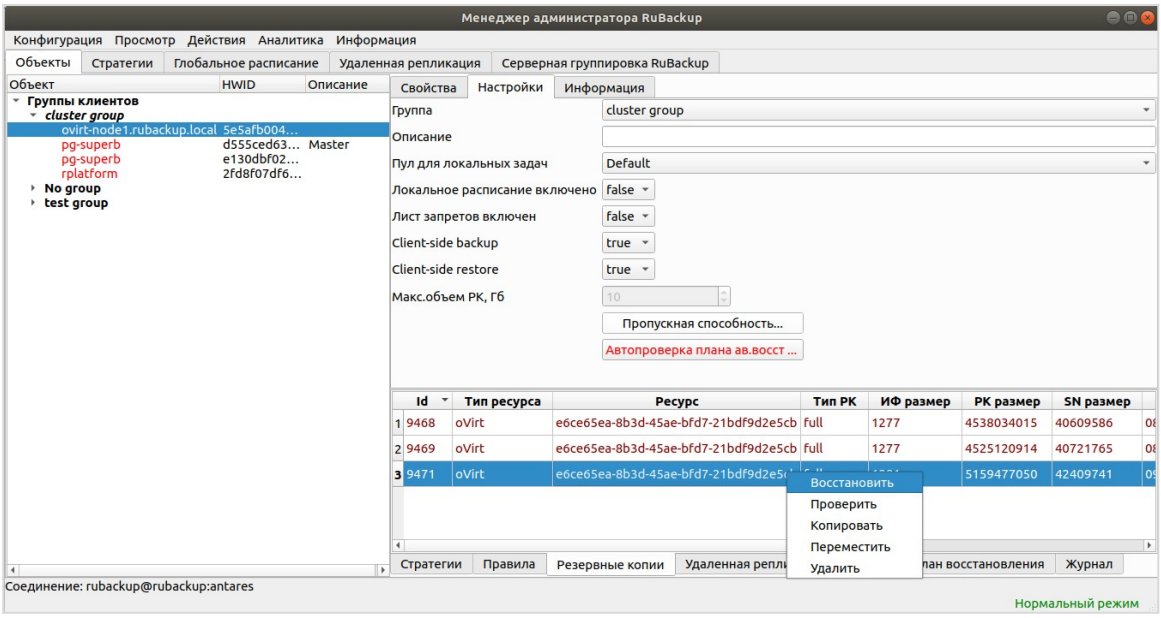


Рисунок 14

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

В том случае, если необходимо восстановить резервную копию в локальный каталог на клиенте без развертывания виртуальной машины в среде виртуализации, то необходимо снять отметку «Развернуть, если применимо» (рисунок 15):

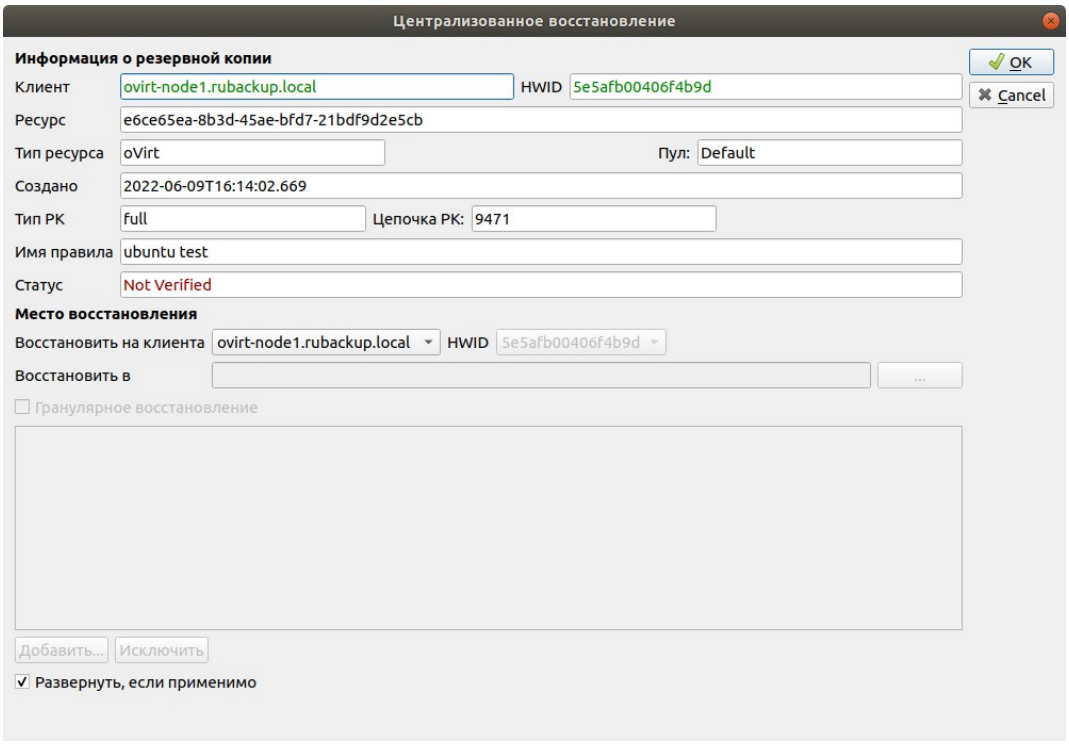
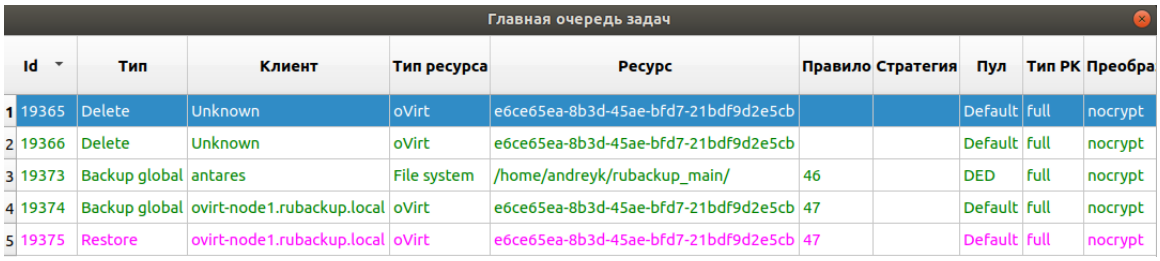


Рисунок 15

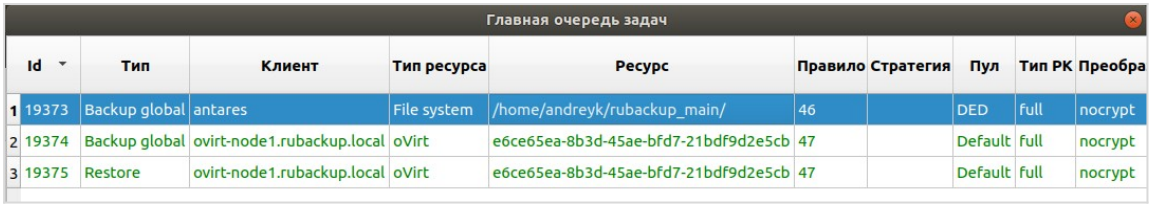
Проверить ход выполнения восстановления резервной копии можно в окне «Главная очередь задач» (рисунок 16) :



	Id	Тип	Клиент	Тип ресурса	Ресурс	Правило	Стратегия	Пул	Тип РК	Преобра
1	19365	Delete	Unknown	oVirt	e6ce65ea-8b3d-45ae-bfd7-21bdf9d2e5cb			Default	full	nocrypt
2	19366	Delete	Unknown	oVirt	e6ce65ea-8b3d-45ae-bfd7-21bdf9d2e5cb			Default	full	nocrypt
3	19373	Backup global	antares	File system	/home/andreyk/rubackup_main/	46		DED	full	nocrypt
4	19374	Backup global	ovirt-node1.rubackup.local	oVirt	e6ce65ea-8b3d-45ae-bfd7-21bdf9d2e5cb	47		Default	full	nocrypt
5	19375	Restore	ovirt-node1.rubackup.local	oVirt	e6ce65ea-8b3d-45ae-bfd7-21bdf9d2e5cb	47		Default	full	nocrypt

Рисунок 16

При успешном завершении восстановления виртуальной машины появится окно (рисунок 17):



	Id	Тип	Клиент	Тип ресурса	Ресурс	Правило	Стратегия	Пул	Тип РК	Преобра
1	19373	Backup global	antares	File system	/home/andreyk/rubackup_main/	46		DED	full	nocrypt
2	19374	Backup global	ovirt-node1.rubackup.local	oVirt	e6ce65ea-8b3d-45ae-bfd7-21bdf9d2e5cb	47		Default	full	nocrypt
3	19375	Restore	ovirt-node1.rubackup.local	oVirt	e6ce65ea-8b3d-45ae-bfd7-21bdf9d2e5cb	47		Default	full	nocrypt

Рисунок 17

Успешный запуск восстановленной виртуальной машины можно проконтролировать в окне (рисунок 18):

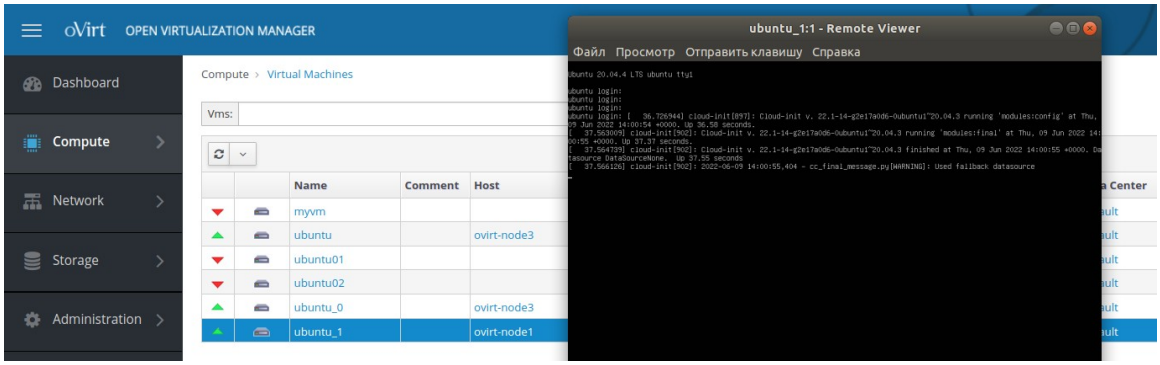
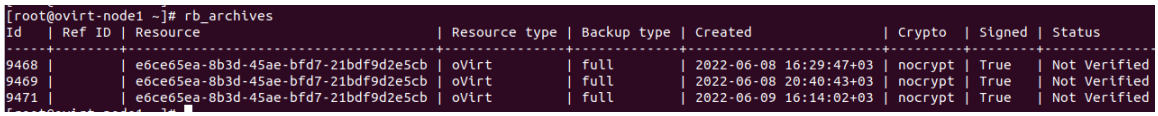


Рисунок 18

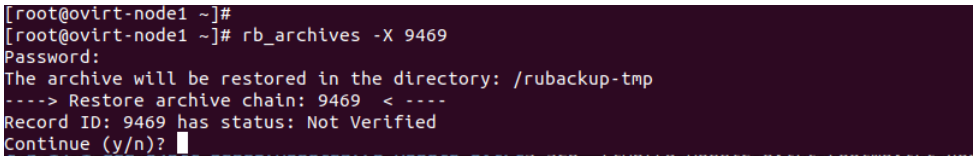
Восстановление со стороны клиента

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

Просмотр списка доступных резервных копий:



Запрос на восстановление резервной копии:



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