RuBackup
Система резервного копирования и восстановления данных

Резервное копирование

и восстановление виртуальных машин

сред виртуализации oVirt/zVirt/REDVirt

RuBackup

Версия 2.1

19.04.2024 г.

Содержание

Введение....3
Поддерживаемые конфигурации....4
Установка клиента RuBackup....5
Мастер-ключ....9
Защитное преобразование резервных копий....10
Алгоритмы защитного преобразования....11
Использование менеджера администратора RuBackup (RBM)....12
Запуск RBM....12
Регулярное резервное копирование виртуальной машины....16
Срочное резервное копирование....22
Централизованное восстановление резервных копий....24
Восстановление со стороны клиента....27

Введение

Модуль для резервного копирования и восстановления виртуальных машин сред виртуализации oVirt/zVirt/REDVirt тестировался и заявлен в поддержку только со средой виртуализации zVirt.

Работа модуля со средами виртуализации oVirt и REDVirt заявлена в экспериментальном режиме, что означает отсутствие поддержки со стороны RuBackup для данных сред виртуализации.

Система резервного копирования RuBackup позволяет выполнять клиентам полное, инкрементальное и дифференциальное резервное копирование и восстановление виртуальных машин сред виртуализации oVirt/zVirt/REDVirt. 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/zVirt/REDVirt 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 zVirt Engine 4.5.

Поддерживаемые типы дисков: IMAGE.

Установка клиента RuBackup

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

```
rubackup-ovirt-client-2.0.99.U2.67-1.el8.x86_64.rpm
```

```
rubackup-ovirt-common-2.0.99.U2.67-1.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) Запуск rubackup_client необходимо выполнять от имени пользователя vdsm в root директории (/). В том случае, если вам необходимо запустить клиент не как сервис, а в терминальном режиме, воспользуйтесь командами:

Для запуска клиента:

```
# cd /
```

```
# 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/zVirt/REDVirt, 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:

- Для создания резервной копии в размере не менее 10% общего объема виртуальных машин, для которых выполняются одновременные операции резервного копирования (например, для одновременного резервного копирования 10 виртуальных машин по 10Гб необходимо 10Гб выделенного пространства). Это связано с тем, что создание резервных копий дисков виртуальных машин происходит непосредственно из хранилища, однако требуется свободное пространство в размере 10% от объема резервируемых ресурсов для временного хранения служебной информации.
- Для восстановления резервной копии в размере не менее 110% общего объема виртуальных машин, для которых выполнено резервное копирование (например, для восстановления 10 виртуальных машин по 10Гб необходимо 110Гб выделенного пространства). Это связано с тем, что 100% от размера восстанавливаемых ресурсов составляют копии дисков виртуальных машин, а 10% — служебная информация.

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`.

При конфигурации клиента с использованием электронной подписи, после выполнения rb_init на клиенте необходимо выполнить команду:

```
chown vdsm:kvm /opt/rubackup/keys/secret-key.pem
```

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

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

Временный каталог необходим для хранения:

- Текстового файла с конфигурацией виртуальных машин.
- Архива со служебной информацией резервной копии.

Объем временного каталога должен быть не менее 10% 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/servic
es/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:

```
Try to check module: 'oVirt' ...
Execute OS command: /opt/rubackup/modules/rb_module_ovirt -t 2>&1
[2024-02-01 08:37:31] Info: Module version: 2.0
[2024-02-01 08:37:31] Info: zVirt Engine version: 4.5
... module 'oVirt' was checked successfully
Execute OS command: /opt/rubackup/modules/rb_module_ovirt -c 2>&1
```

2. В ручном режиме проверить правильность настроек следующей командой:

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

Мастер-ключ

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

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

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

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

```
$ hexdump /opt/rubackup/keys/master-key
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).

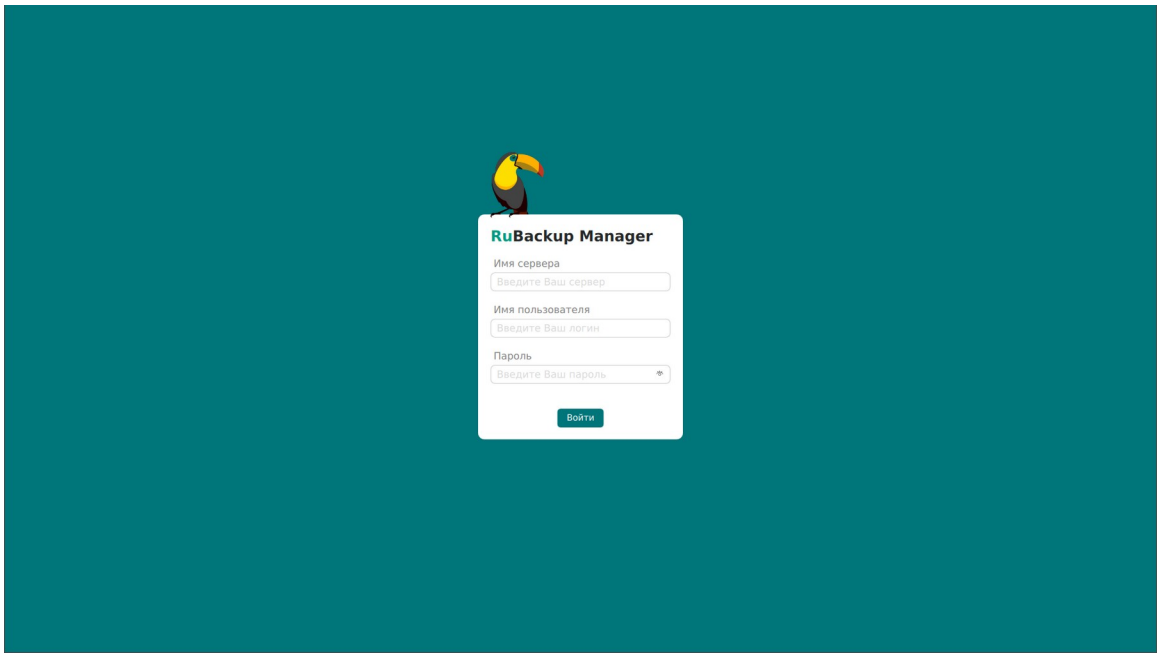


Рисунок 1

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.

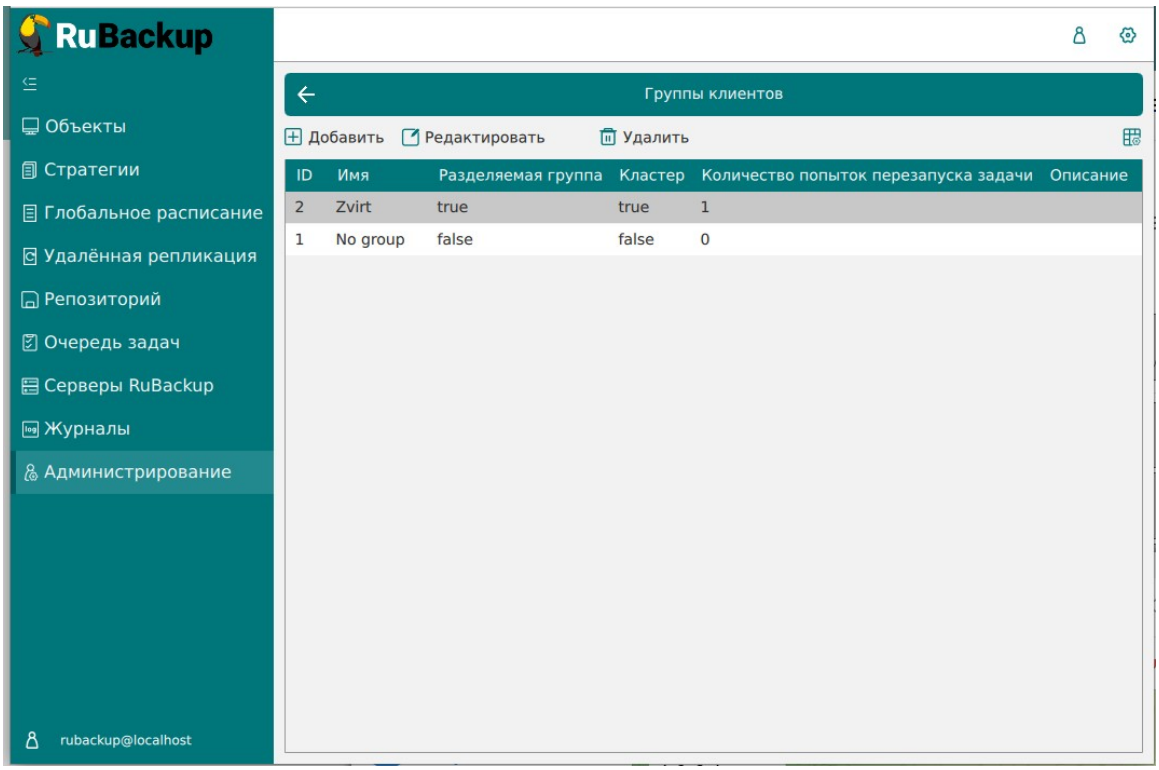


Рисунок 2

Для авторизации неавторизованного клиента в RBM необходимо выполнить следующие действия:

1. Нажмите на вкладку «**Администрирование**» и выберите иконку «**Клиенты**» (Рисунок 3).

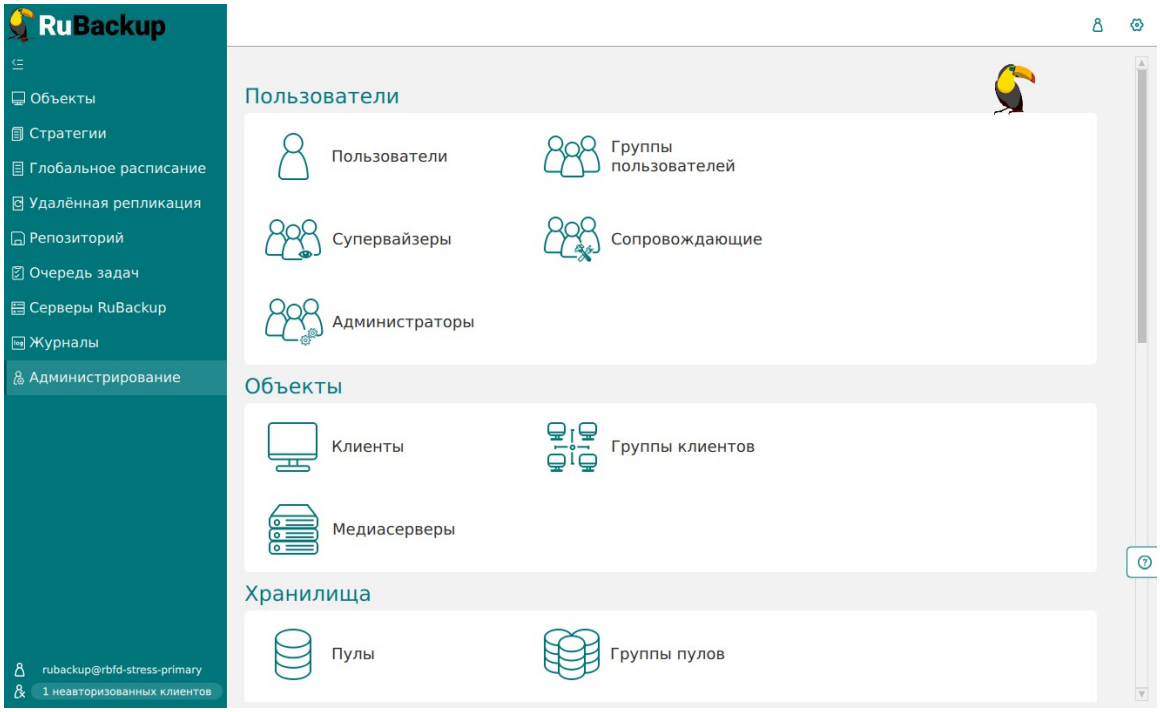


Рисунок 3

2. На верхней панели перейдите на вкладку «**Неавторизованные клиенты**» (Рисунок 4):

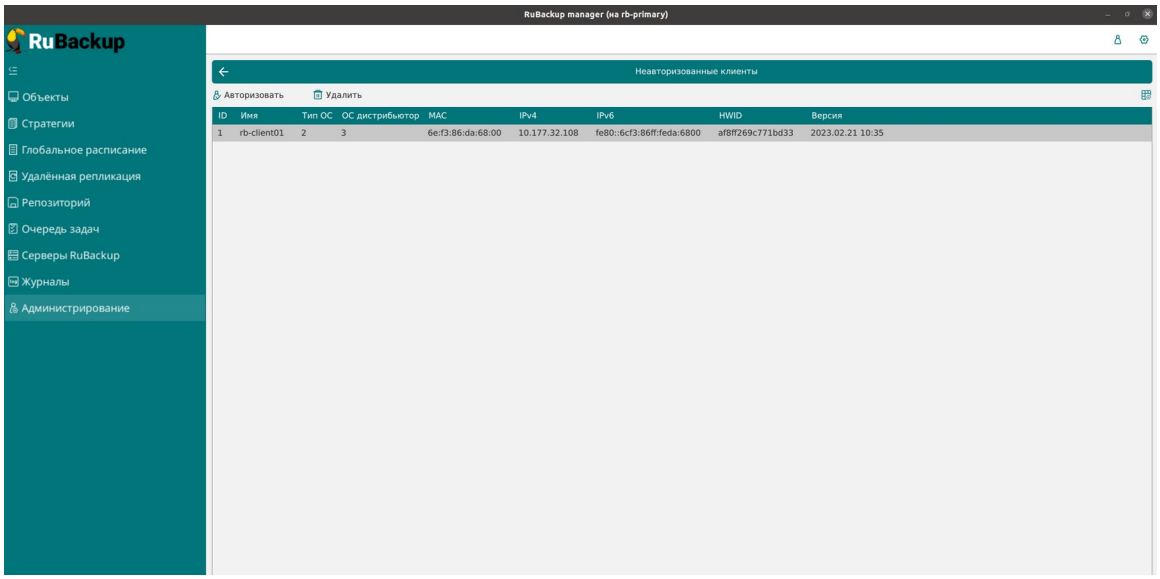


Рисунок 4

3. Нажмите на требуемого неавторизованного клиента правой кнопкой мыши и выберите «**Авторизовать**» (Рисунок 5):

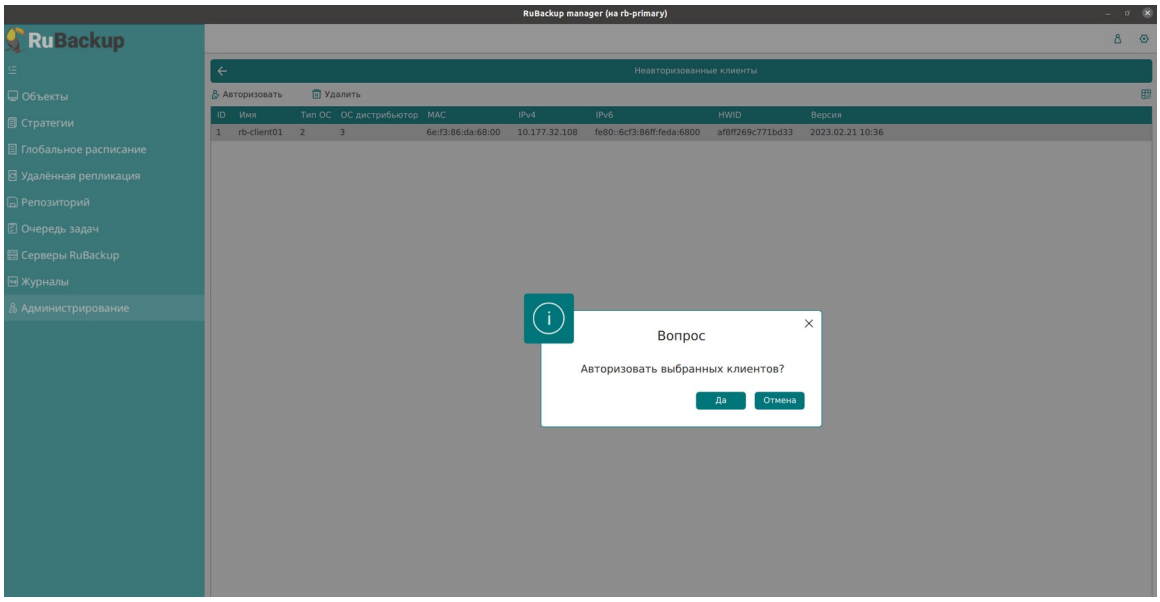


Рисунок 5

После авторизации клиент будет виден на вкладе «**Объекты**» (Рисунок 6):

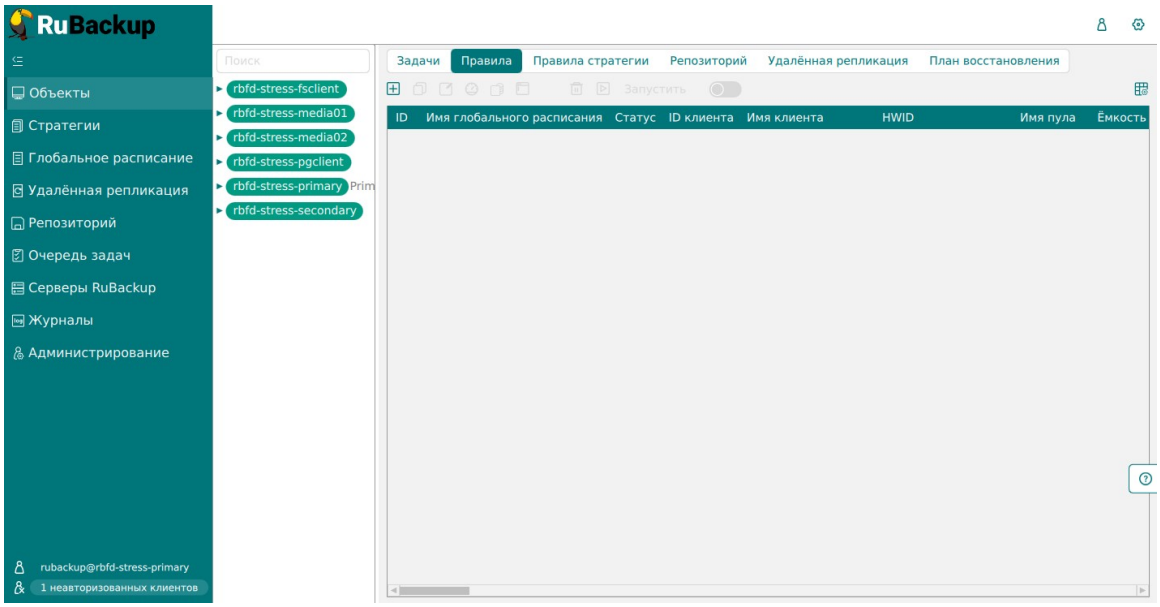


Рисунок 6

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. Находясь в разделе «**Объекты**», выберите вкладку «**Правила**» и нажмите на иконку «**+**» (Рисунок 7):

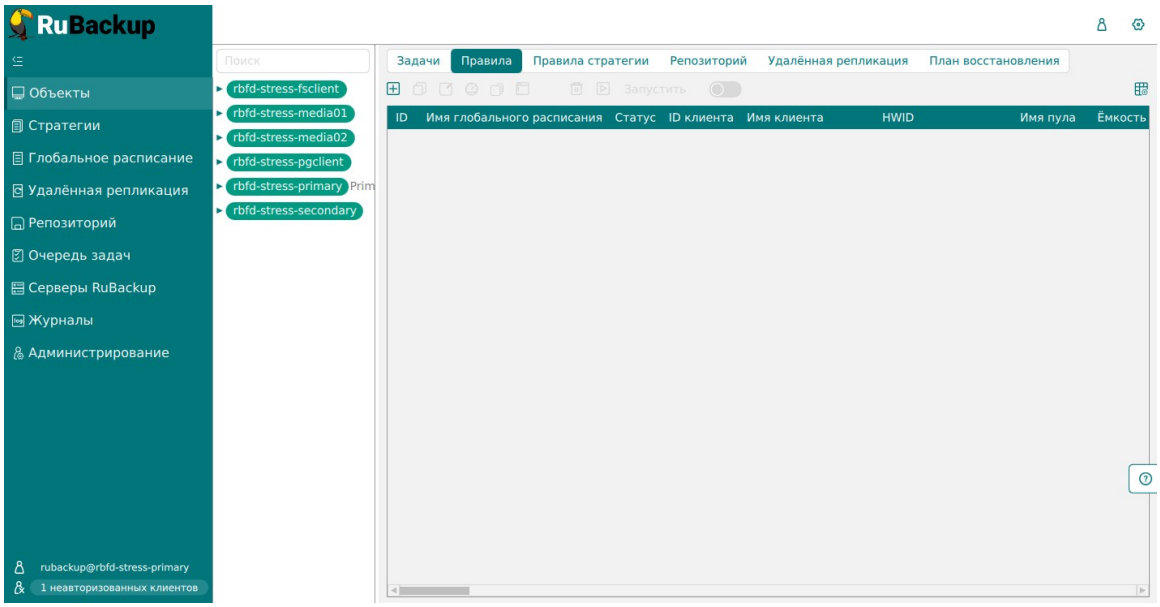


Рисунок 7

2. Выберите клиент, вместе с которым установлен модуль RuBackup, предназначенный для резервного копирования виртуальных машин oVirt/zVirt/REDVirt.

3. Выберите тип ресурса «**oVirt**» (Рисунок 8):

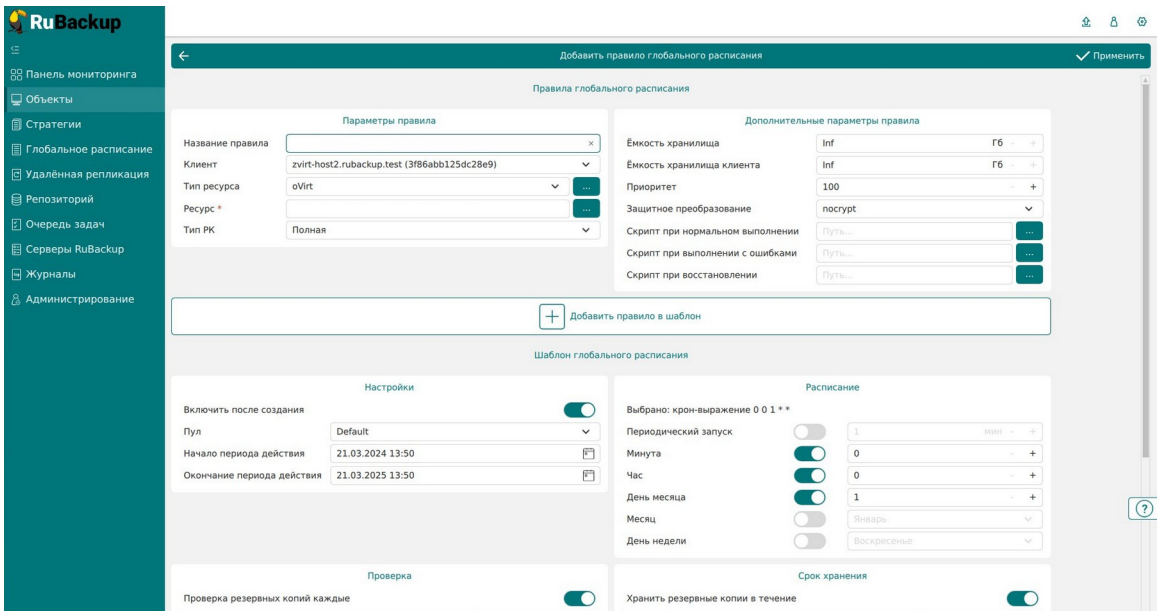


Рисунок 8

4. Нажмите на иконку «**...**» рядом с надписью «**Ресурс**» и выберите виртуальную машину, для которой требуется создать резервную копию (Рисунок 9):

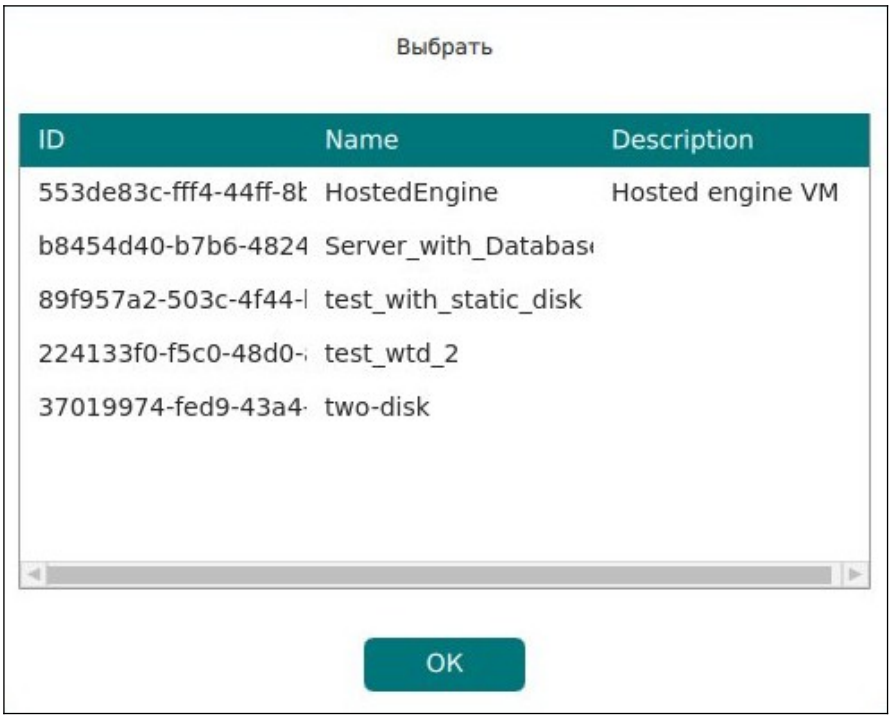


Рисунок 9

Для резервного копирования виртуальных машин, в которых содержатся диски с типом «Предварительно размеченный», необходимо заранее в настройках диска установить флаг «Включить инкрементальное резервное копирование» (Рисунок 10). В случае, если флаг будет выключен, при резервном копировании не гарантируется восстановление с развертыванием.

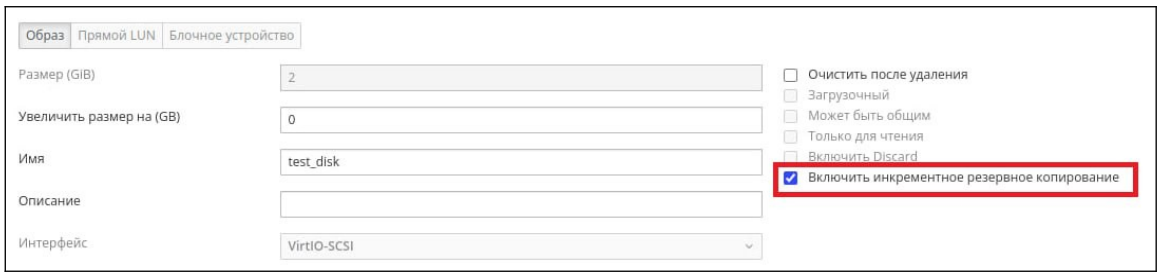


Рисунок 10

5. Установите настройки правила: название правила, пул хранения данных, приоритет выполнения правила, тип резервной копии (полная, инкрементальная или дифференциальная), расписание резервного копирования, срок хранения и необязательный временной промежуток проверки копии (Рисунок 11):

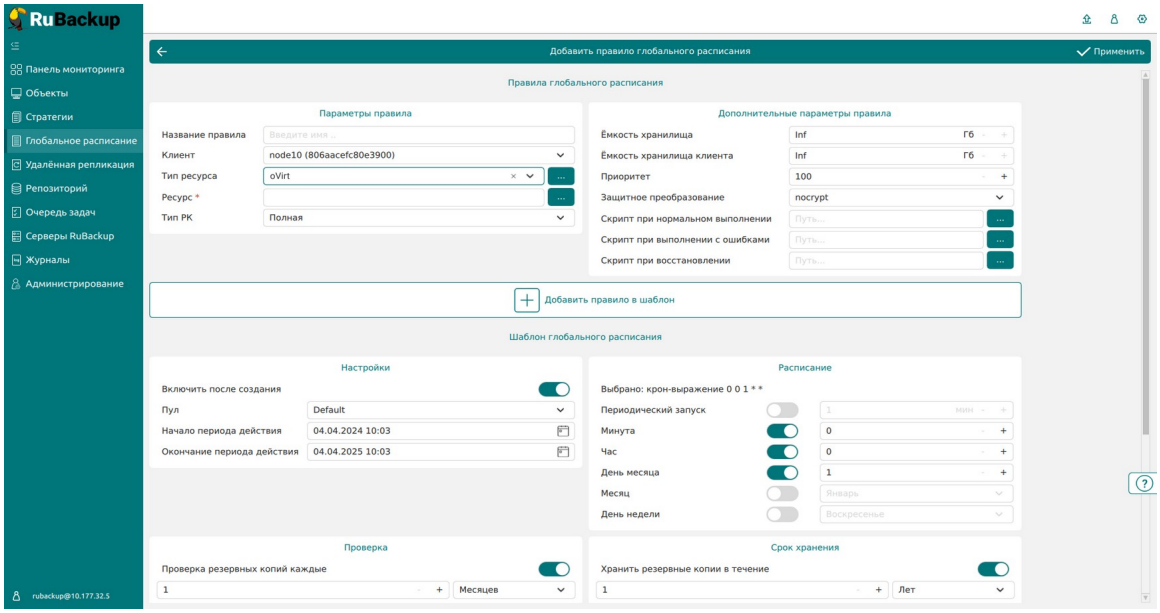


Рисунок 11

6. Нажав на иконку «**...**» рядом с выбранным типом ресурса «**oVirt**», установите дополнительные настройки правила резервного копирования (Рисунок 12, Таблица 2).

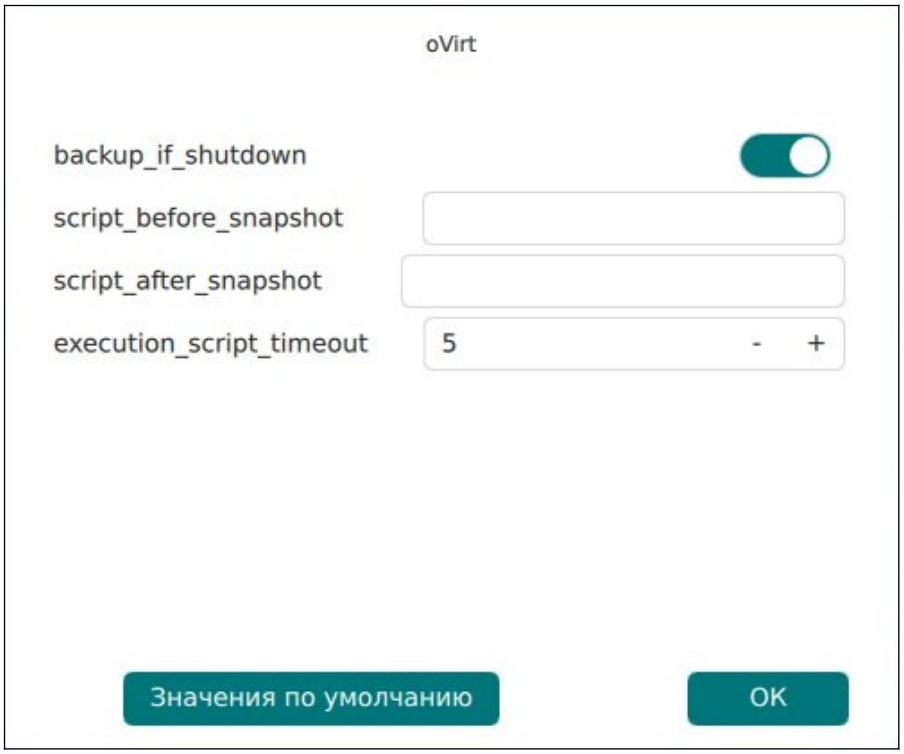


Рисунок 12

Таблица 2 – Дополнительные параметры правила резервного копирования виртуальных машин oVirt/zVirt/REDVirt

Параметр	Описание	Значение по умолчанию	Допустимые значения
backup_if_shutdown	Параметр, задающий возможность резервного копирования выключенной виртуальной машины: • true — возможно создание резервной копии выключенной виртуальной машины. • false — создание резервной копии выключенной виртуальной машины невозможно. Задача на резервное копирование будет завершена с ошибкой.	true	true, false

Параметр	Описание	Значение по умолчанию	Допустимые значения
script_before_snapshot	Полный путь к скрипту внутри виртуальной машины, который будет выполнен перед созданием снэпшота для данной виртуальной машины.		
script_after_snapshot	Полный путь к скрипту внутри виртуальной машины, который будет выполнен после создания снэпшота для данной виртуальной машины.		
execution_script_timeout	Время в секундах, в течение которого модуль RuBackup будет ожидать выполнения скриптов внутри виртуальной машины до и после создания снэпшота.	5	1 - 600

7. Для правила резервного копирования также можно настроить уведомления при нормальном его выполнении или при возникновении ошибки в процессе выполнения, уведомления при окончании срока действия правила, уведомления при окончании ёмкости в пуле, уведомления при удалении устаревших резервных копий, возможность и периодичность перемещения резервных копий в другой пул данных (Рисунок 13):

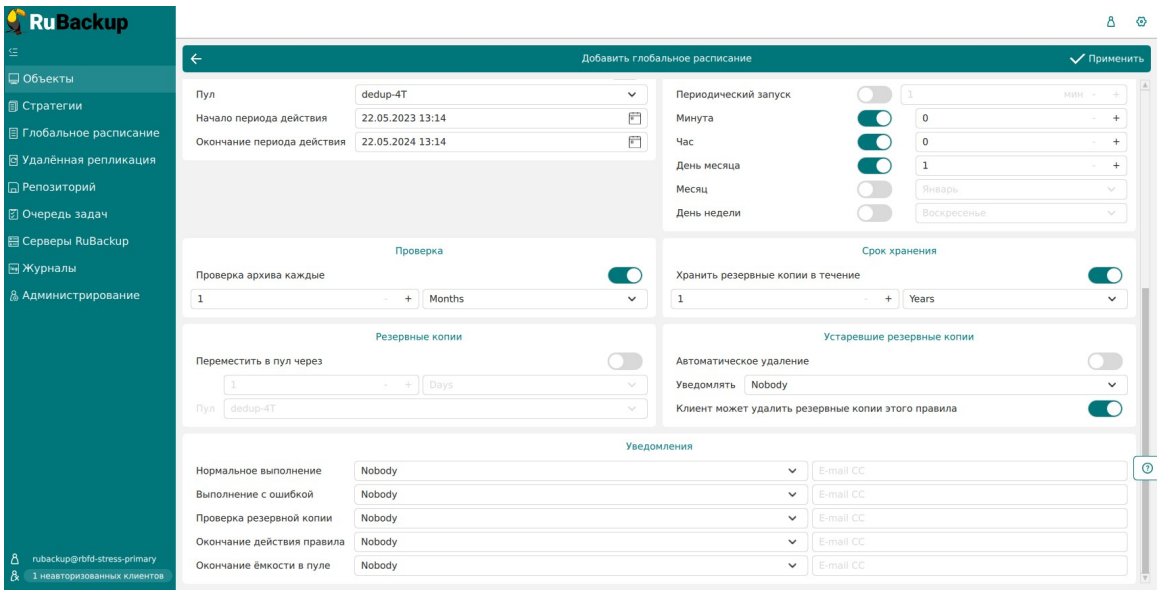


Рисунок 13

5. После выполнения настроек правила резервного копирование нажмите на кнопку «**Добавить правило в шаблон**» (Рисунок 14). В результате чего правило для выбранного типа ресурса (oVirt) и выбранного ресурса (виртуальной машины) появится в списке правил.

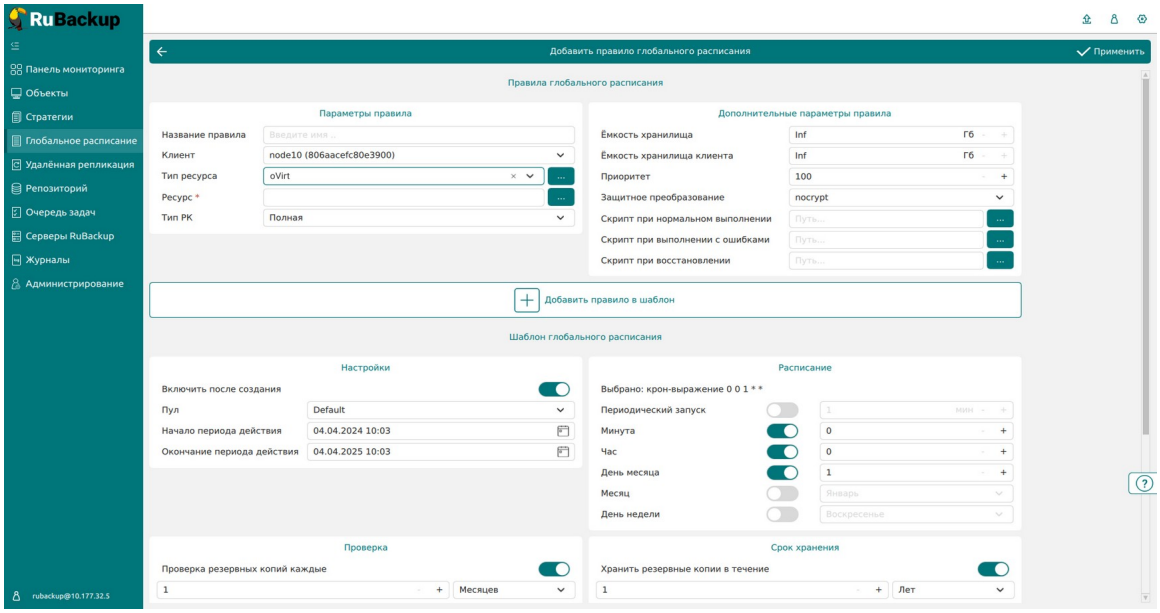


Рисунок 14

6. Нажмите на кнопку «**Применить**» в правом-верхнем углу для завершения настройки и создания правила.

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 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 15):

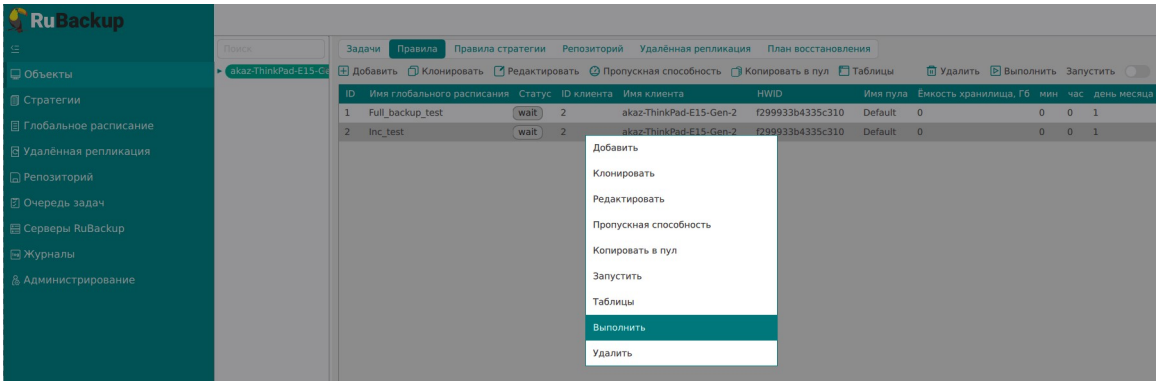


Рисунок 15

Проверить ход выполнения резервного копирования можно в окне «Очередь задач» (рисунок 16).

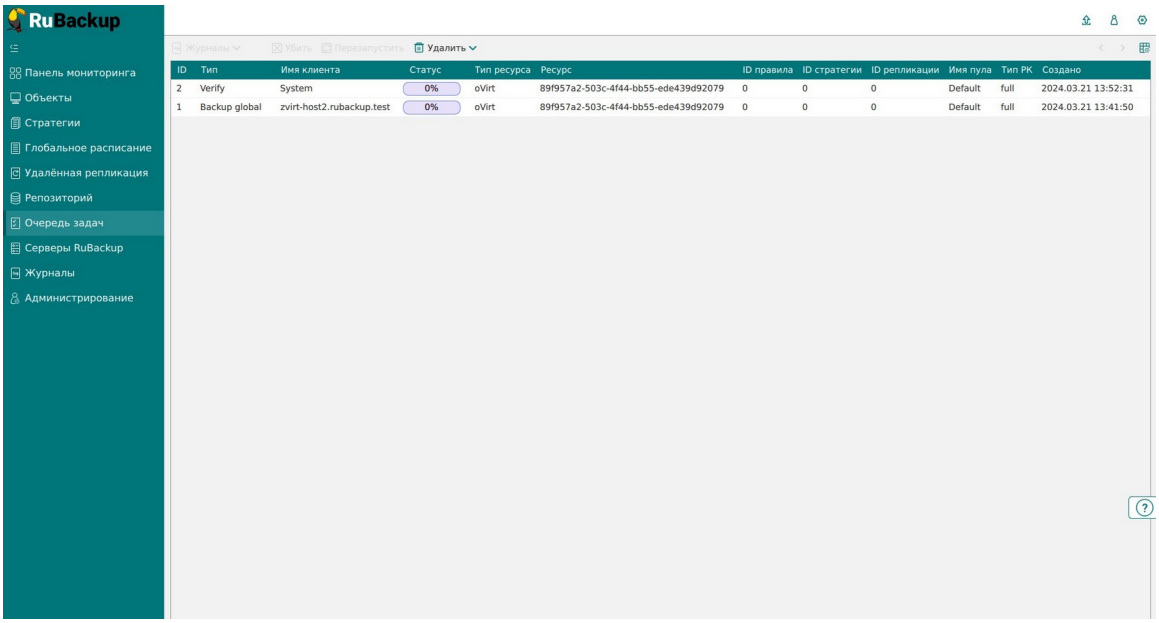


Рисунок 16

При успешном завершении резервного копирования соответствующая задача перейдет в статус «**Done** (рисунок 17):

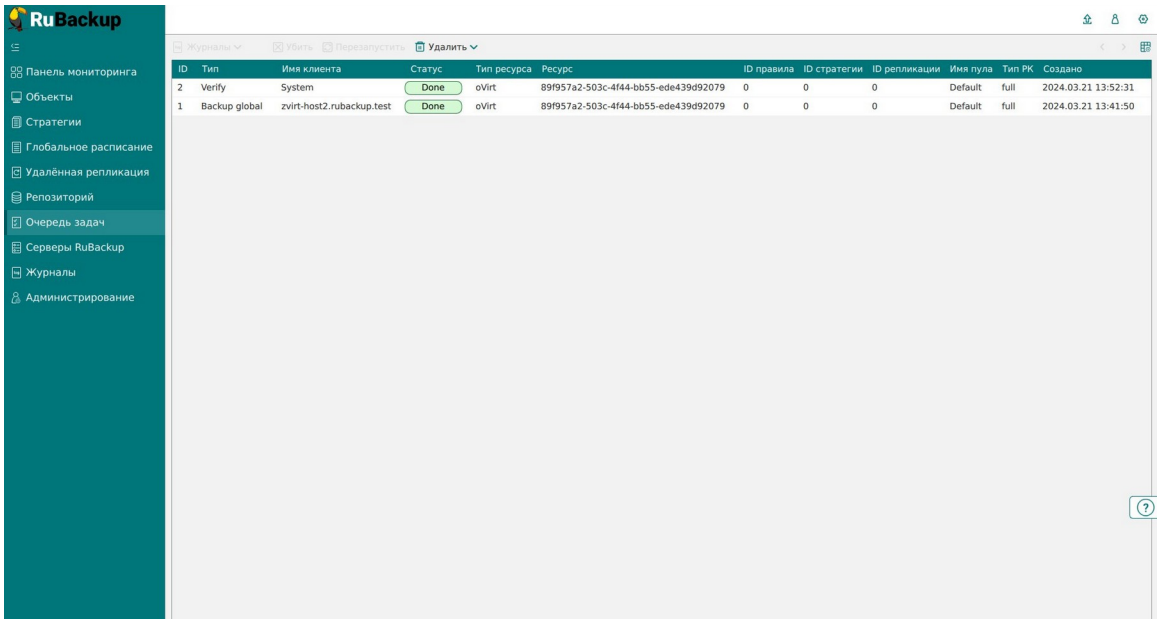


Рисунок 17

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 18):

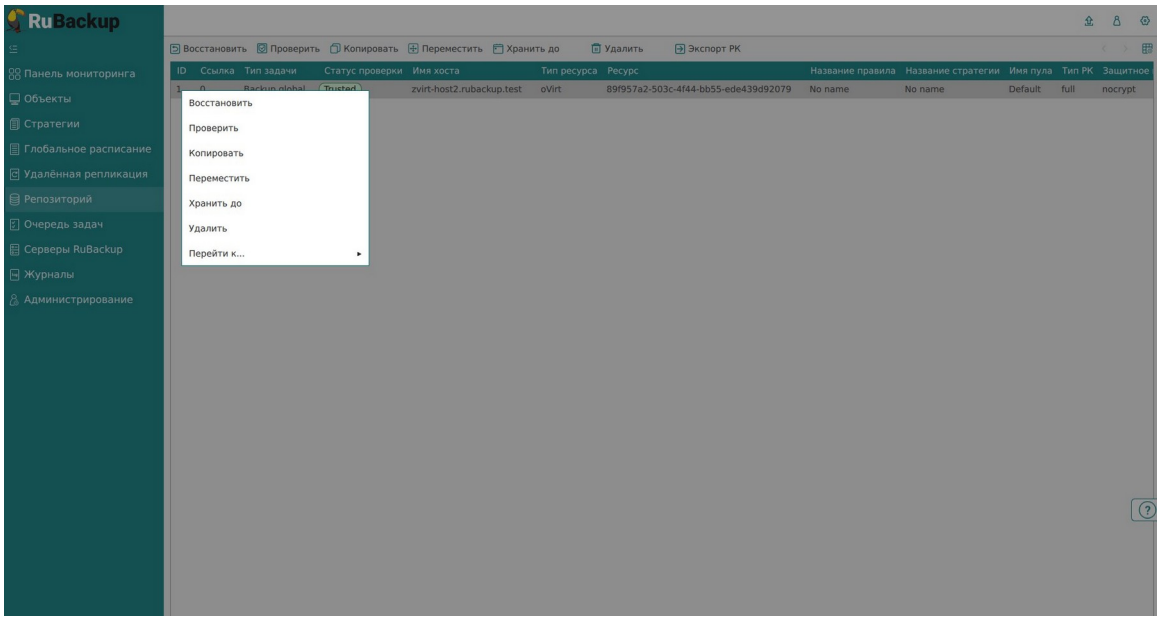


Рисунок 18

В окне централизованного восстановления можно увидеть основные параметры резервной копии и определить каталог распаковки (Рисунок 19). Объем каталога распаковки должен быть на 10% больше объема виртуальных машин, одновременное восстановление которых будет выполняться.

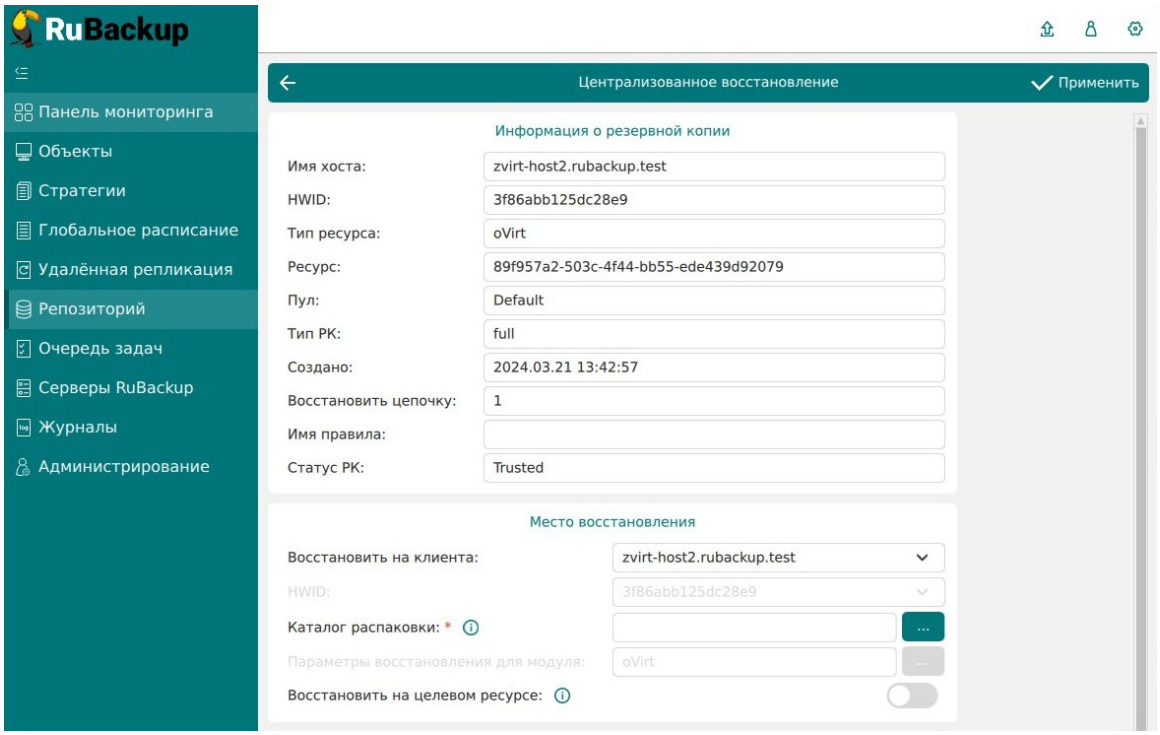


Рисунок 19

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 20):

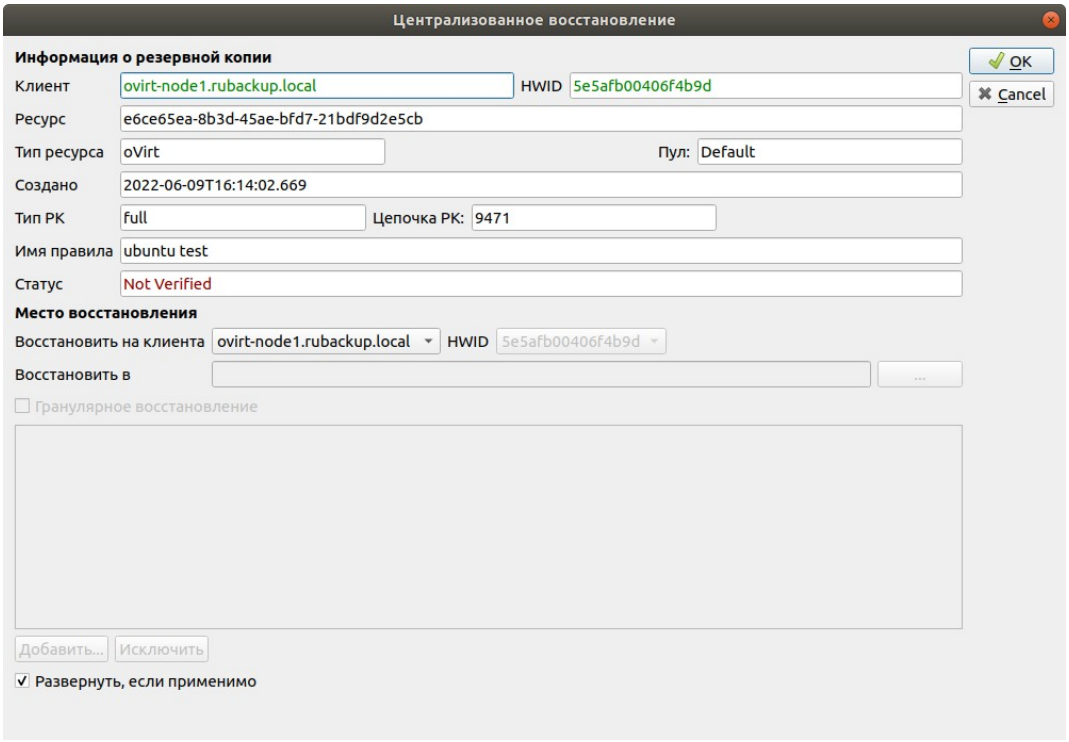


Рисунок 20

Убедитесь в том, что у пользователя vdsm имеются права на внесение изменений в каталоге, в который производится распаковка, например, /rubackup-tmp. Из консоли на клиенте выполните команду:

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

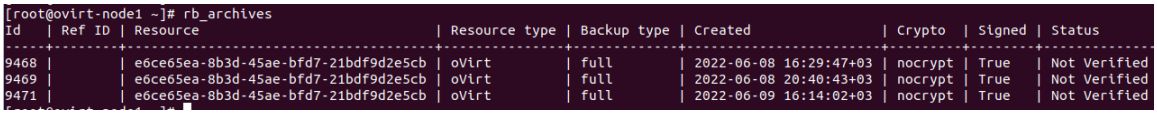
Проверить ход выполнения восстановления резервной копии можно в окне «Очередь задач».

Успешный запуск восстановленной виртуальной машины можно проконтролировать в среде виртуализации zVirt. При успешном запуске виртуальная машина будет в статусе online.

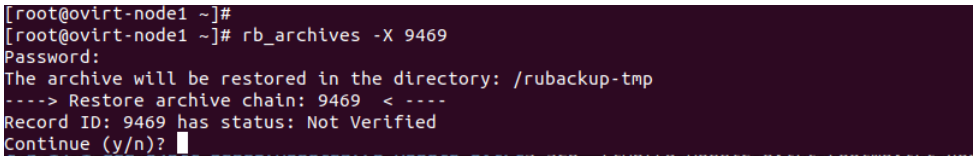
Восстановление со стороны клиента

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:



После создания каталога для распаковки резервной копии, например, /rubackup-tmp, необходимо обеспечить пользователю vdsm возможность делать изменения внутри данного каталога:

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

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.