RuBackup

Система резервного копирования
и восстановления данных

РЕЗЕРВНОЕ КОПИРОВАНИЕ ВМ OVIRT, ZVIRT, REDVIRT, ROSA

ВЕРСИЯ 2.4.0, 26.12.2024

Содержание

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

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 полное, инкрементальное и дифференциальное резервное копирование и восстановление виртуальных машин сред виртуализации oVirt версии 4.5.5, zVirt версии 4.0 и ROSA Virtualization версии 2.1. Так же возможно выполнять резервное копирование с использованием дедупликации и хранить резервные копии в дедуплицированном хранилище.

Резервное копирование виртуальных машин oVirt/zVirt/REDVirt/ROSA Virtualization 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/zVirt/REDVirt/ROSA Virtualization 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.

Глава 1. Поддерживаемые конфигурации

Версия zVirt Engine 4.0.

Версия oVirt Engine 4.4, 4.5

Версия ROSA Virtualization 2.1, 3.0 (API Version 4.4, 4.5)

Поддерживаемые типы дисков: IMAGE.

Red Virtualization Engine 7.3.0

Глава 2. Установка клиента RuBackup

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

- `rubackup-ovirt-client-<version>.el8.x86_64.rpm`
- `rubackup-ovirt-common-<version>.el8.x86_64.rpm`,

где `<version>` — номер версии модуля oVirt.

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

Основные отличия работы клиента RuBackup в средах виртуализации oVirt/zVirt/REDVirt/ROSA Virtualization 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:

   Запуск клиента

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

   Остановка 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/ROSA Virtualization, 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 [1] 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 3% от общего объема виртуальных машин, для которых выполняются одновременные операции резервного копирования (например, для одновременного резервного копирования 10 виртуальных машин по 10Гб необходимо 3Гб выделенного пространства). Это связано с тем, что создание резервных копий дисков вирту-

альных машин происходит непосредственно из хранилища, однако требуется свободное пространство в размере 3% от объема резервируемых ресурсов для временного хранения служебной информации.

- Для создания резервной копии выключенной виртуальной машины, диски которой расположены в хранилище iSCSI [2] или FCP [3], требуется место в каталоге для временных операций в размере 103% от её объема (100% — для временного хранения копии диска + 3% для хранения служебной информации). Копии дисков такой виртуальной машины загружаются в каталог для временных операций через oVirt API.
- Для восстановления резервной копии в размере не менее 103% от общего объема виртуальных машин, для которых выполнено резервное копирование (например, для восстановления 10 виртуальных машин по 10 Гб необходимо 103 Гб выделенного пространства). Это связано с тем, что 100% от размера восстанавливаемых ресурсов составляют копии дисков виртуальных машин, а 3% — служебная информация.
- Для восстановления ВМ с использованием механизма загрузки дисков "nbd" в хранилища типа iSCSI и FCP на узле Клиента РК (гипервизоре) должно быть свободное место в размере не менее 203% общего объема ВМ, для которой выполняется операция восстановления.

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.

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 конфигурационный файл клиента RuBackup с помощью консольной утилиты `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`.

1. После создания каталога для работы с временными файлами (например, при

выборе каталога `/rubackup-tmp`) необходимо предоставить к нему доступ пользователю `vdsm`:

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

Временный каталог необходим для хранения:

- Метаданных, которые формирует СРК в процессе создания резервной копии виртуальной машины. Размер формируемых метаданных может достигать 3% от объема одновременно резервируемых виртуальных машин.
- Копий дисков виртуальных машин — для случаев, когда выполняется резервное копирование выключенной виртуальной машины, диски которой расположены в хранилище iSCSI или FCP. В данном случае объем каталога для временных операций должен быть не менее 103% от размера виртуальных машин, для которых выполняется резервное копирование.

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`:

```
# Symbol "#" at the beginning of the line treats as a comment
# "#" in the middle of the line treats as a parameter value
# So please do not use comments in one line with parameter
engine <url>
grant_type <password>
username <username>
password <password>
ca_info <path to a certificate>
timeout <timeout in seconds>

# The mechanism used (backend) to upload the disk to the server. Default:
file
disk_upload_mechanism <file/nbd>

# Set this flag to 'yes' if there is a need to assign a VM backup task the
RuBackup client
# which is running on the same host as the target VM.
# If set 'no' the backup task will be assigned the RuBackup client node used
for backup rule creation.
# Default value: yes
```

```
backup_vm_from_native_host yes

# Specifies the maximum single disk upload timeout in minutes. Default: 2
minutes. Min 1 minute
disk_upload_timeout 2

# Specifies the maximum single disk download timeout in minutes. Default: 10
minutes. Min 1 minute
disk_download_timeout 10

# oVirt ImageTransfer inactivity_timeout in seconds. Default: 60 seconds. Min
5 seconds, max 500 seconds
imagetransfer_inactivity_timeout 60

# Try using the module if the platform version is not compatible with
RuBackup. Default: no
allow_work_with_incompatible_versions no

# Turn on debug of REST requests
# Possible values: yes, no. Default no
curl_verbose no
```

Параметры из конфигурационного файла `rb_module_ovirt.conf` представлены в таблице 1.

Таблица 1. Параметры файла конфигурации модуля резервного копирования oVirt/zVirt/REDVirt/ROSA Virtualization

Параметр	Назначение	Значение по умолчанию
`engine`	IP-адрес для API-запросов в платформу виртуализации oVirt	
`grant_type`	Тип гранта токена аутентификации OAuth для взаимодействия с API-платформой виртуализации	password
`username`	Имя пользователя, от имени которого будут выполняться запросы API	
`password`	Пароль для пользователя, указанного в параметре username	
`ca_info`	Путь до сертификата ssl	
`timeout`	Время ожидания (в секундах) ответа от платформы виртуализации на API запросы. Минимум 1 секунда, максимум 300 секунд, по умолчанию 10 секунд. Если при выполнении задачи на создание РК или восстановление РК ответ от платформы не поступит в течение заданного опцией timeout времени, то соответствующая задача может быть завершена с ошибкой	10

Параметр	Назначение	Значение по умолчанию
`disk_upload_mechanism`	Механизм для чтения данных диска и записи данных на диск внутри платформы виртуализации. Допустимые значения: • nbd — механизм взаимодействия с дисками, реализуемый на основе протокола NBD. Этот бэкенд обеспечивает наилучшую производительность и расширенные функции, такие как zero/dirty extents. • file — механизм взаимодействия с дисками на основе прямого доступа к ним. Этот бэкенд не поддерживает множественные подключения при записи данных, а также функционал zero/dirty extents. `Для восстановления ВМ на платформе виртуализации с используемой версией oVirt ниже 4.5.0 с помощью механизма загрузки дисков "nbd" в хранилища типа iSCSI и FCP необходимо, чтобы диски оригинальной ВМ имели Политику распределения – "Тонкое резервирование", иначе не гарантируется восстановление ВМ. (см. подробнее на странице https://ovirt.github.io/ovirt-imageio/packages.html)`	file
`allow_work_with_incompatible_versions`	Параметр, указывающий, будет ли модуль работать с версией платформы виртуализации, совместимость с которой не была протестирована. Допустимые значения: yes, no. Если модуль не совместим с версией платформы виртуализации и значение параметра установлено в no, модуль завершит свою работу с соответствующим сообщением об ошибке. При необходимости работы с несовместимой версией платформы виртуализации установите параметр в значение yes	no
`disk_upload_timeout`	Таймаут для загрузки каждого диска на платформу при восстановлении. Измеряется в минутах. По умолчанию 2 минуты. Минимальное значение — 1 минута;	2
`disk_download_timeout`	Таймаут для загрузки каждого диска с платформы при бекапе. Измеряется в минутах. По умолчанию 10 минут. Минимальное значение — 1 минута;	10
`imagetransfer_inactivity_timeout`	Параметр определяет какое количество секунд платформа будет ожидать начала загрузки диска после создания ImageTransfer-а. Измеряется в секундах. Минимальное значение — 5 секунд, максимальное значение — 500 секунд.	5

Параметр	Назначение	Значение по умолчанию
`curl_verbose`	Параметр выводит дополнительную информацию по REST API запросам, при значении yes.	no
`backup_vm_from_native_host`	Параметр определяет, будет ли задача резервного копирования виртуальной машины назначена клиенту RuBackup, который работает на том же хосте, что и целевая ВМ. • Если значение установлено на **yes**, задача будет назначена клиенту RuBackup на том же хосте. Клиент СРК при этом должен быть добавлен в кластерную группу вместе с другими клиентами СРК, размещенными на узлах платформы виртуализации. Для информации о добавлении клиента в кластрную группу см. раздел «Группы клиентов» Руководства системного администратора RuBackup. • Если значение установлено на **no**, задача будет назначена клиенту RuBackup, используемому при создании правила резервного копирования.	yes

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'
     ```

   - изменить права доступа для сертификата следующей командой:

     ```
     chown vdsm:kvm /opt/rubackup/keys/ovirt.ca.crt
     ```

     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
```

2.1. Настройка доступа без пароля для пользователя vdsm

Для корректной работы с модулем пользователю `vdsm` необходим доступ без пароля по ssh. К пользователю `root` на остальных узлах виртуализации, где установлен клиент RuBackup.

Для этого необходимо проверить наличие ssh ключа на данном узле, если ключ отсутствует, создать его следующей командой:

```
sudo -u vdsm ssh-keygen -t rsa -b 4096 -f /var/lib/vdsm/.ssh/id_rsa
```

Далее необходимо скопировать публичный ключ пользователя `vdsm`, находящийся в файле `id_rsa.pub` и записать в файл `/root/.ssh/authorized_keys` на всех остальных узлах виртуализации, где установлен клиент RuBackup.

После вышеописанных действий необходимо убедиться, что все выполнено правильно, попробовать подключиться с одного узла виртуализации на другой командой:

```
sudo -u vdsm ssh root@<hostname>
```

Если при подключении система не требовала пароль — настройка выполнена верно.

[1] NFS — Network File System (см. подробнее на странице https://www.ovirt.org/documentation/administration_guide/

[2] iSCSI — Internet Small Computer System Interface (см. подробнее на странице https://www.ovirt.org/documentation/administration_guide/

[3] FCP — Fibre Channel Protocol (см. подробнее на странице https://www.ovirt.org/documentation/administration_guide/

Глава 3. 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.

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

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
```

Глава 4. 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).

Подробнее о защитном преобразовании резервных копий — см. раздел «Защитное преобразование резервных копий» документа «Руководство системного администратора RuBackup».

4.1. Алгоритмы защитного преобразования

Для выполнения защитного преобразования доступны алгоритмы, представленные в таблице.

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

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

Глава 5. Использование менеджера администратора RuBackup (RBM)

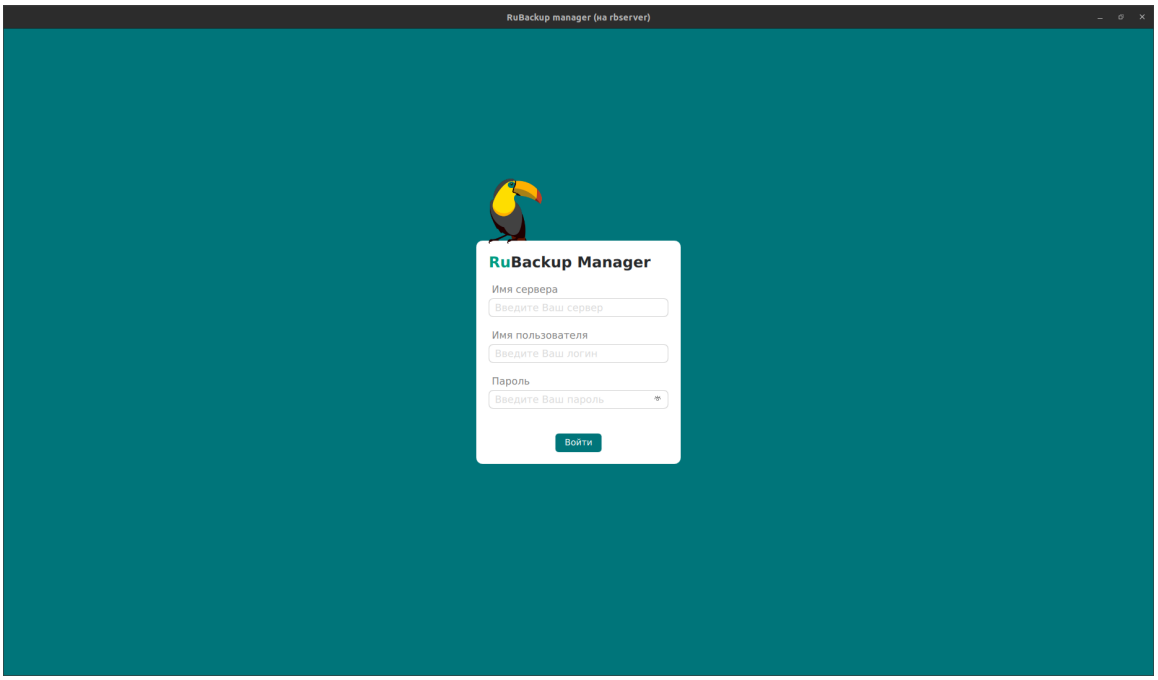
Оконное приложение «Менеджер администратора RuBackup» (RBM) предназначено для общего администрирования серверной группировки RuBackup, управления клиентами резервного копирования, глобальным расписанием резервного копирования, хранилищами резервных копий и другими параметрами RuBackup.

5.1. Запуск RBM

Для запуска RBM следует выполнить команду:

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

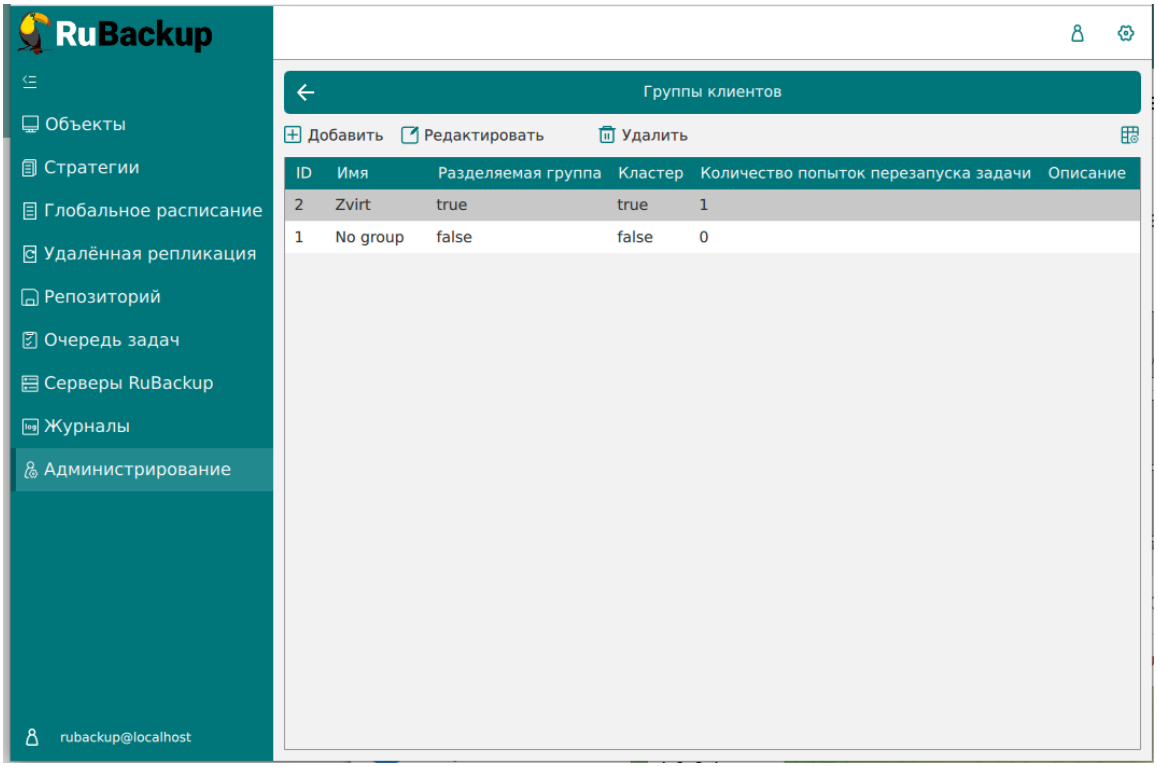
При запуске RBM вам потребуется пройти аутентификацию. Уточните логин и пароль для вашей работы у главного администратора СРК. Если вы главный администратор, то используйте для авторизации суперпользователя `rubackup` и тот пароль, который вы задали ему при инсталляции (рисунок 1).



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).

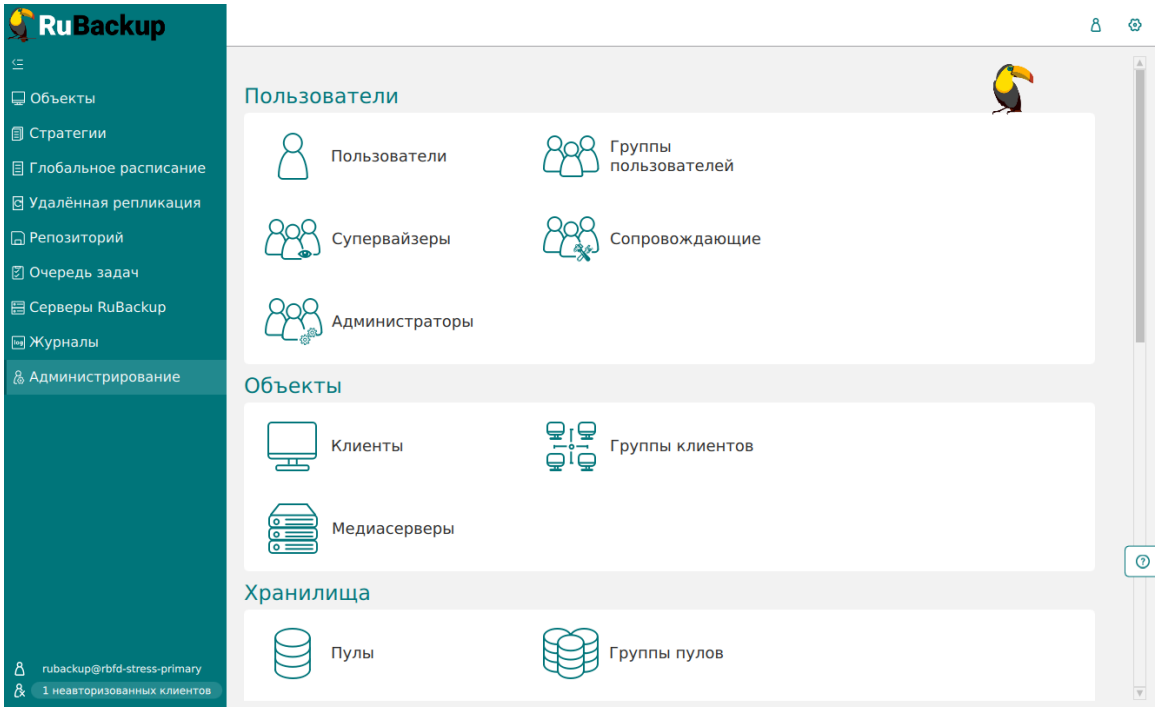
Для резервного копирования клиент должен быть авторизован администратором RuBackup.

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.

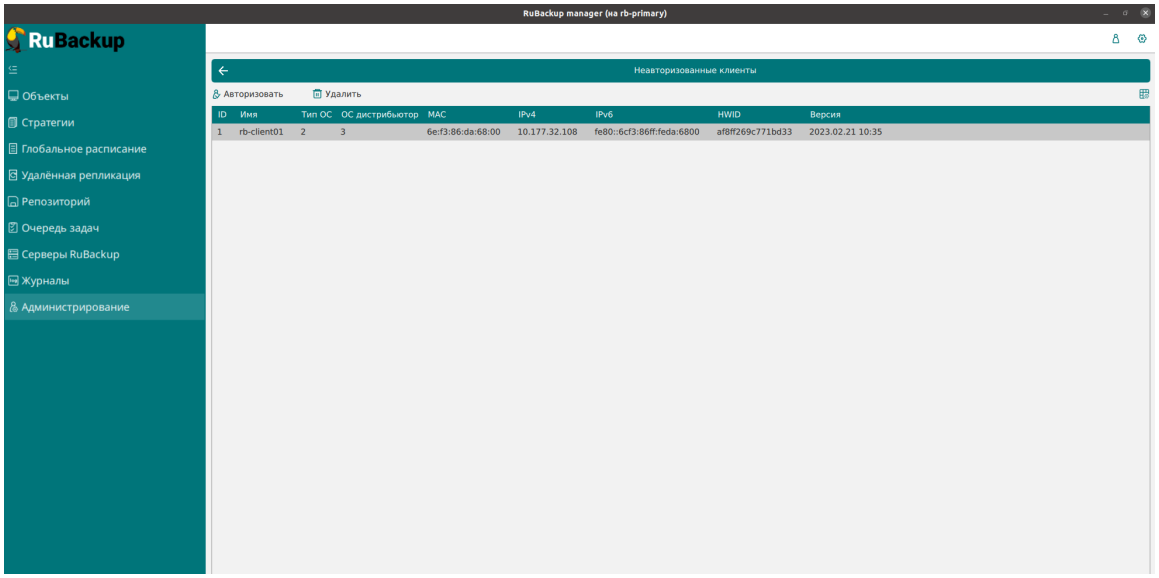


Для авторизации неавторизованного клиента в RBM необходимо выполнить следующие действия:

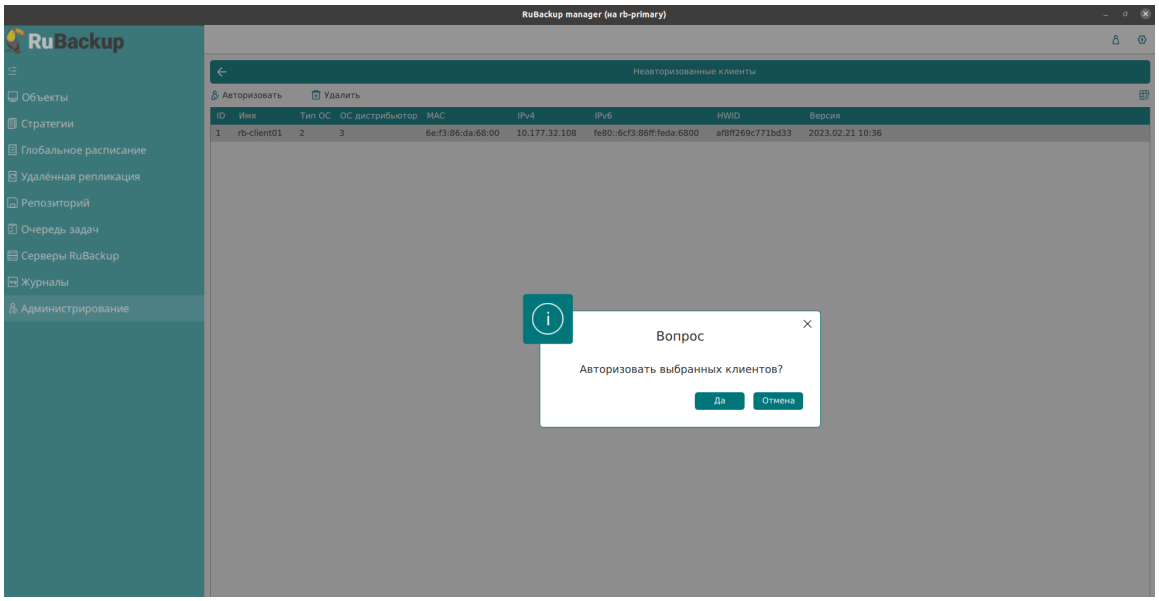
1. Нажмите на вкладку «**Администрирование**» и выберите иконку «**Клиенты**» (рисунок 3).



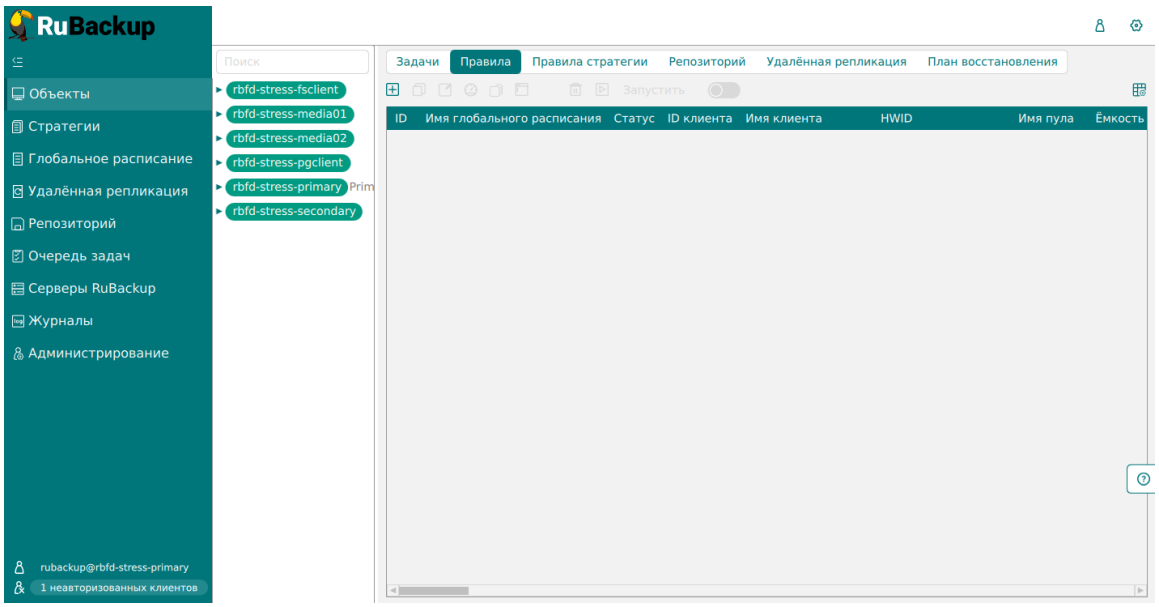
2. На верхней панели перейдите на вкладку «**Неавторизованные клиенты**» (рисунок 4):



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



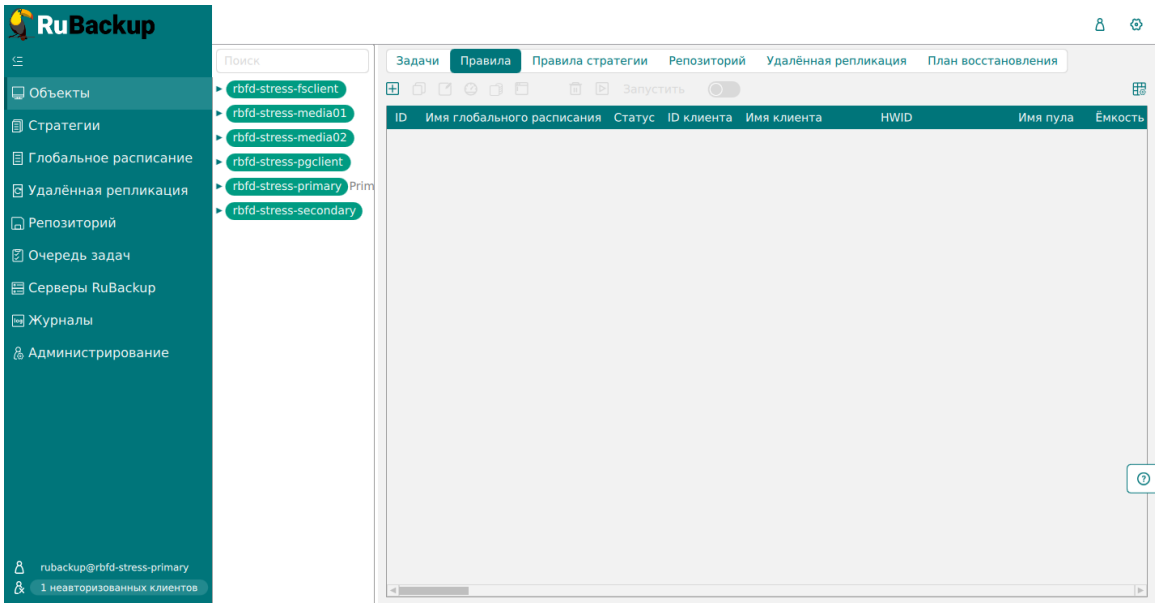
После авторизации клиент будет виден на вкладе «**Объекты**» (рисунок 6):



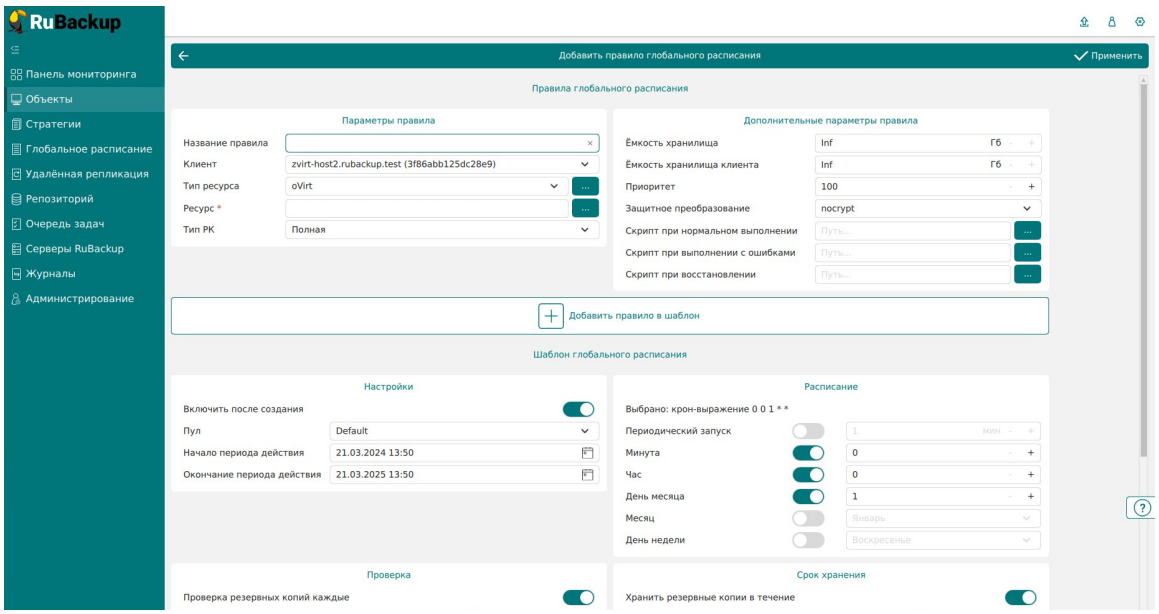
5.2. Регулярное резервное копирование виртуальной машины

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:

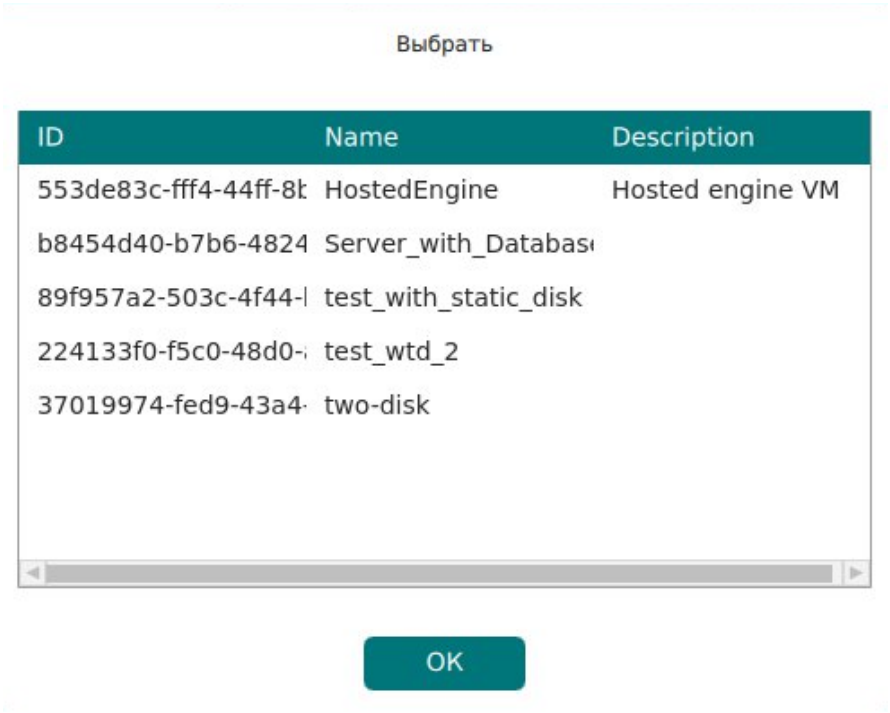
1. Находясь в разделе «**Объекты**», выберите вкладку «**Правила**» и нажмите на иконку «+» (рисунок 7):



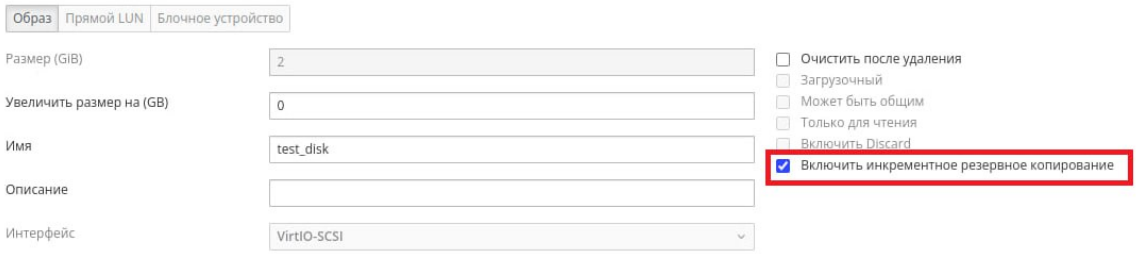
2. Выберите клиент, вместе с которым установлен модуль RuBackup, предназначенный для резервного копирования виртуальных машин oVirt/zVirt/REDVirt/ROSA Virtualization.
3. Выберите тип ресурса «**oVirt**» (рисунок 8):



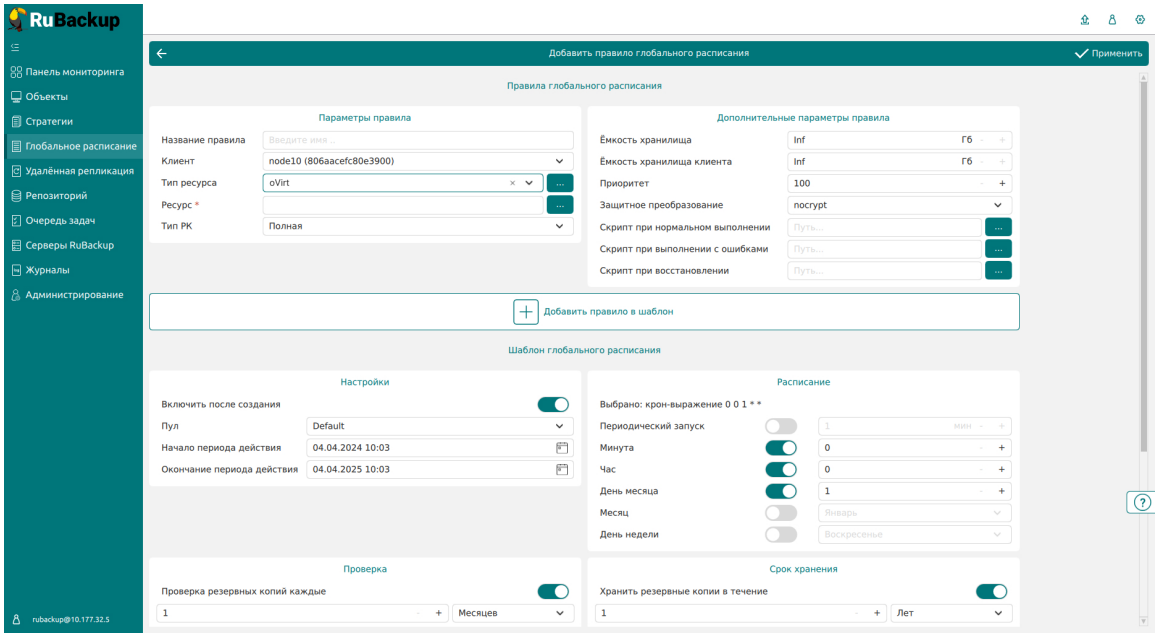
4. Нажмите на иконку «**…**» рядом с надписью «**Ресурс**» и выберите виртуальную машину, для которой требуется создать резервную копию (рисунок 9):



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.



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):



6. Нажав на иконку «**…**» рядом с выбранным типом ресурса «**oVirt**», установите дополнительные настройки правила резервного копирования (рисунок 12, Таблица 3).

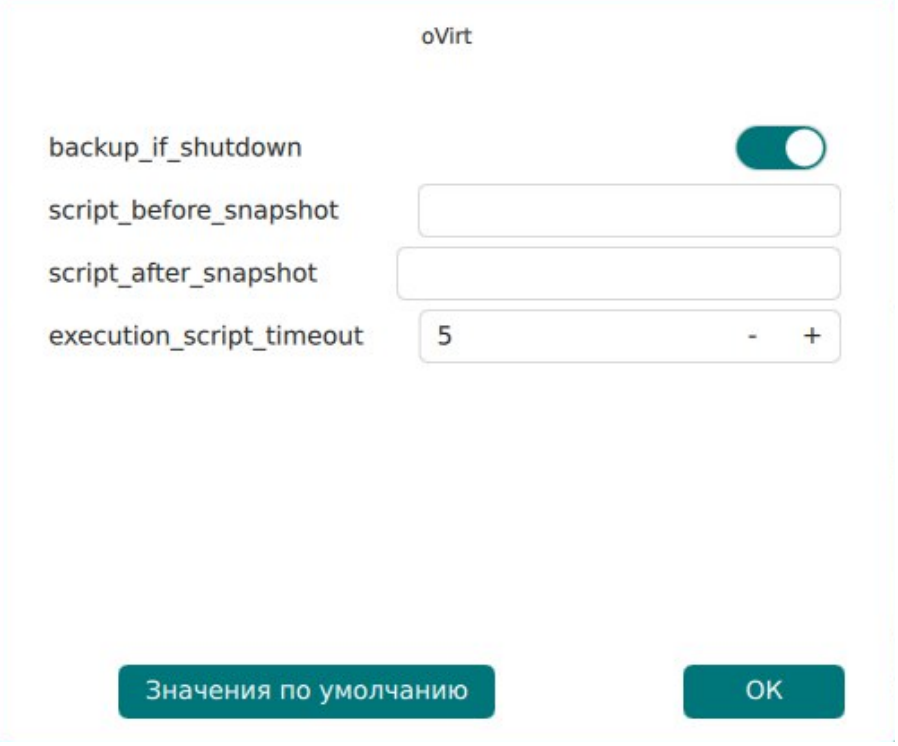
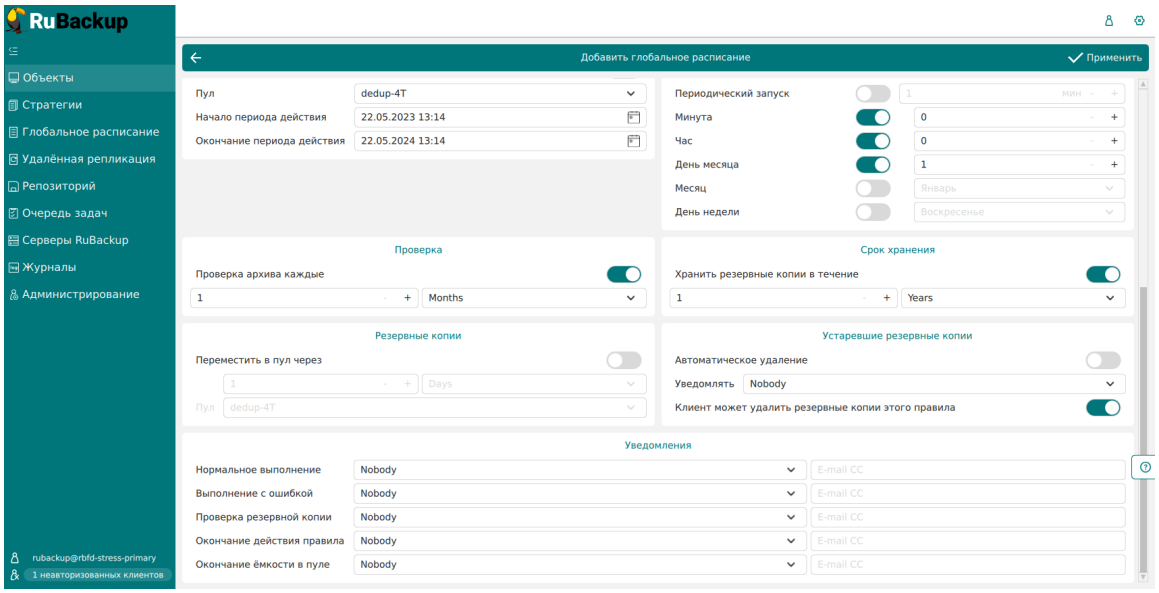


Таблица 3. Дополнительные параметры правила резервного копирования виртуальных машин oVirt/zVirt/REDVirt/ROSA Virtualization

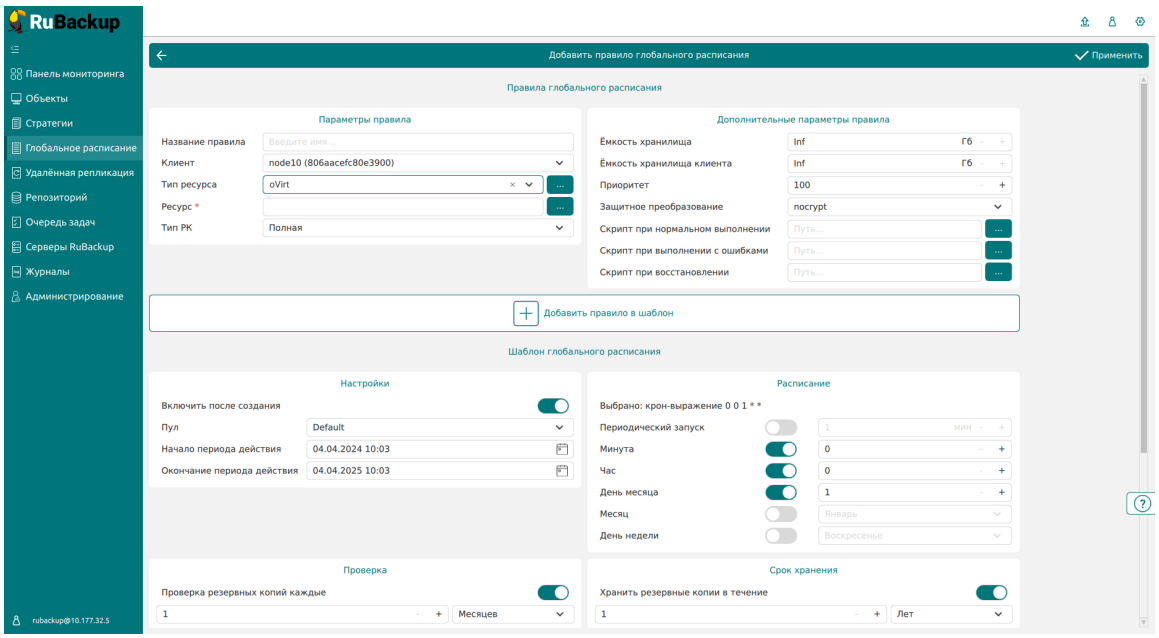
Параметр	Описание	Значение по умолчанию	Допустимые значения
`backup_if_shutdown`	Параметр, задающий возможность резервного копирования выключенной виртуальной машины: • `true` — возможно создание резервной копии выключенной виртуальной машины. • `false` — создание резервной копии выключенной виртуальной машины невозможно. Задача на резервное копирование будет завершена с ошибкой. Резервное копирование выключенных виртуальных машин возможно для виртуальных машин, базирующихся в хранилище типа NFS, iSCSI или FCP	`true`	`true`, `false`
`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

- Если в процессе резервного копирования выключенной виртуальной машины при значении `true` параметра `backup_if_shutdown` пользователь включит данную виртуальную машину, то резервная копия может получиться неконсистентной.
- Для успешного восстановления резервной копии, диски которой находятся в хранилищах типа NFS, iSCSI или FCP необходимо при создании диска установить флаг «Включить инкрементальное резервное копирование». В противном случае восстановить ВМ из хранилища типа NFS, iSCSI или FCP невозможно.

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):



8. 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.



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

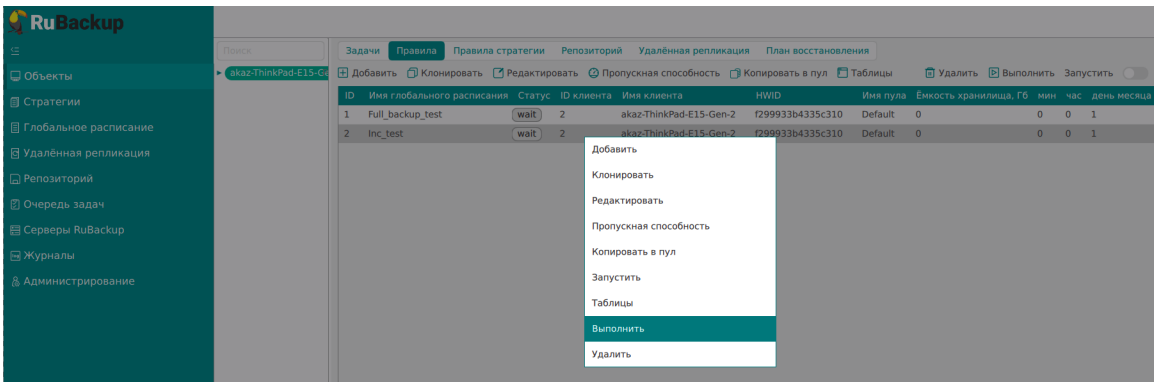
Вновь созданное правило будет иметь статус *run*. Если необходимо создать правило, которое пока не должно порождать задач резервного копирования, нужно убрать отметку «**Включить после создания**».

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`.

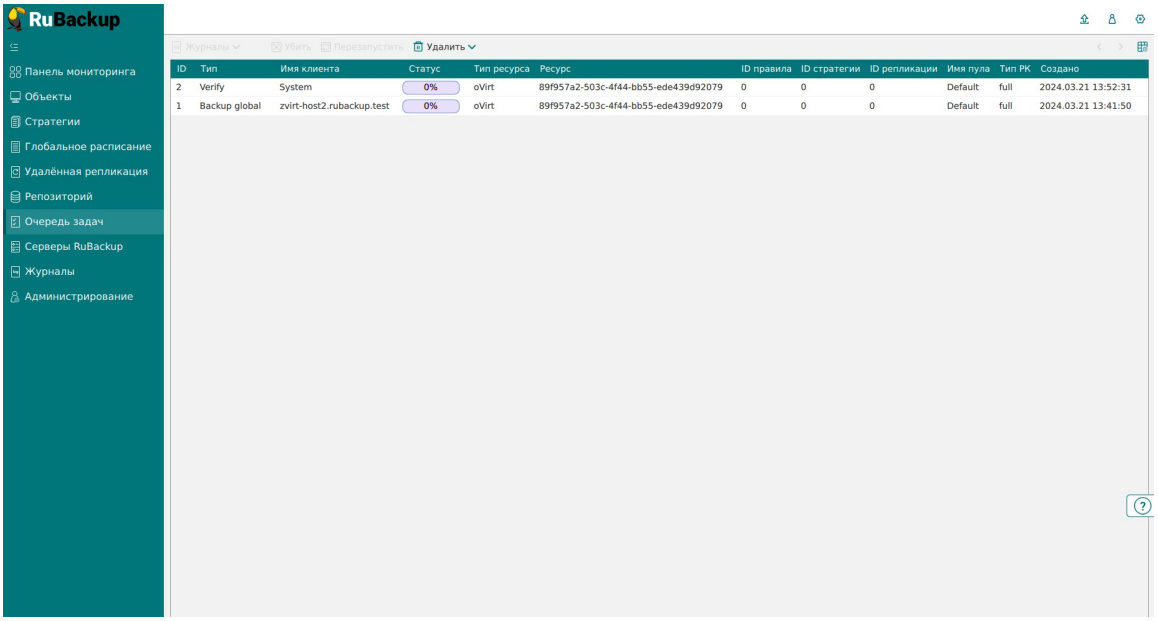
После успешного завершения резервного копирования резервная копия будет размещена в хранилище резервных копий, а информация о ней будет размещена в репозитории RuBackup.

5.3. Срочное резервное копирование

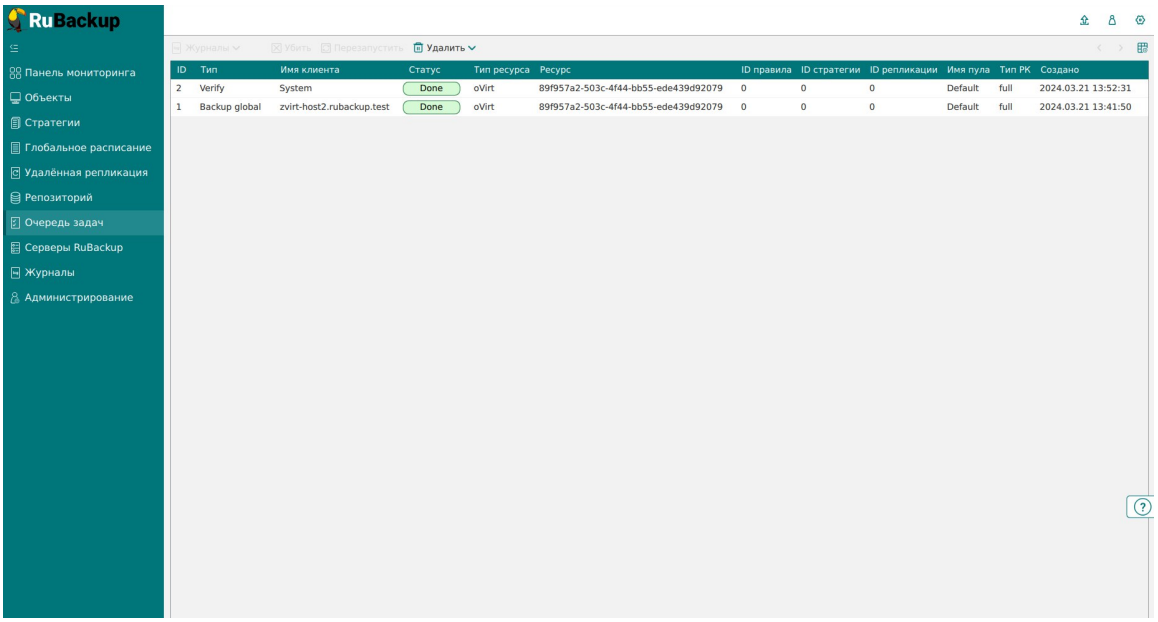
В случае необходимости срочного резервного копирования созданного правила глобального расписания, следует вызвать правой кнопкой мыши контекстное меню «Выполнить» (рисунок 15):



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



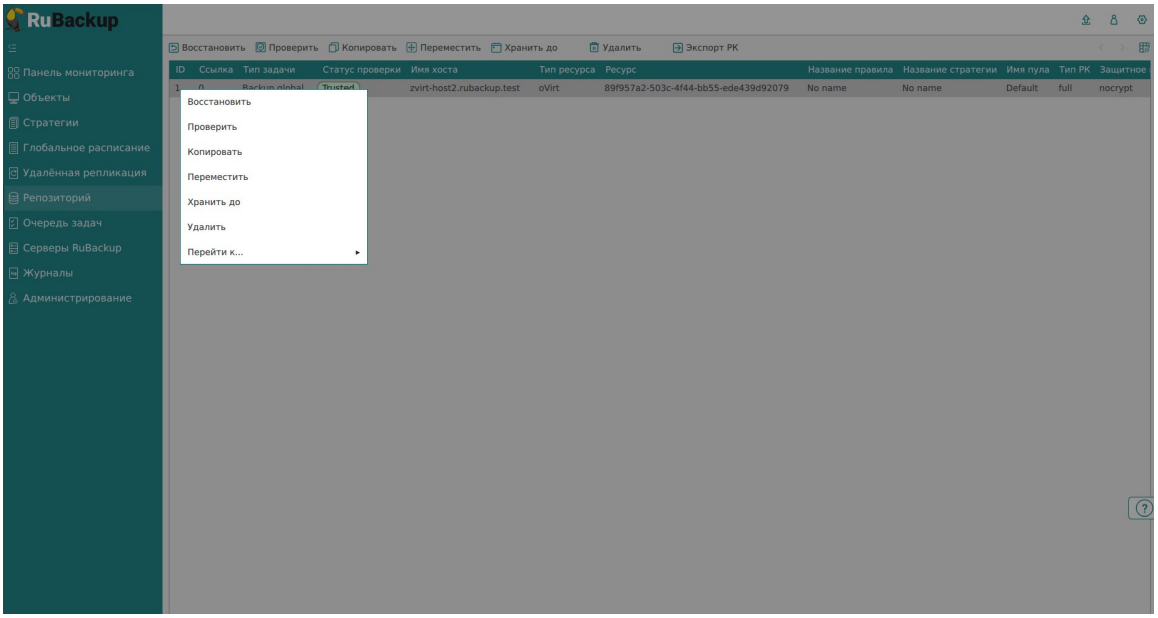
При успешном завершении резервного копирования соответствующая задача перейдет в статус «**Done** (рисунок 17):



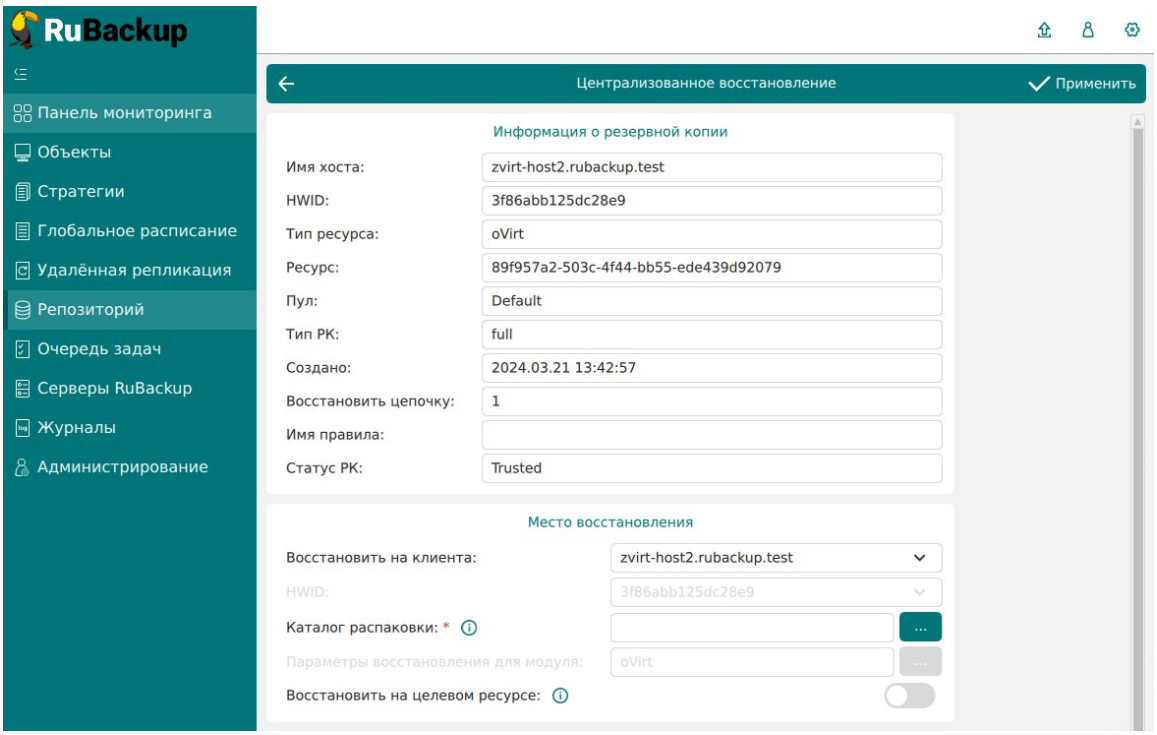
5.4. Централизованное восстановление резервных копий

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):



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.



В случае восстановления виртуальной машины из резервной копии будет выполнена проверка наличия в среде виртуализации виртуальной машины с таким же именем, как у восстанавливаемой. 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.

Для восстановления на платформе активируйте переключатель «Восстановить на целевом ресурсе». В том случае, если необходимо восстановить резервную копию в локальный каталог на клиенте без развертывания виртуальной машины в среде виртуализации, выключите этот переключатель.

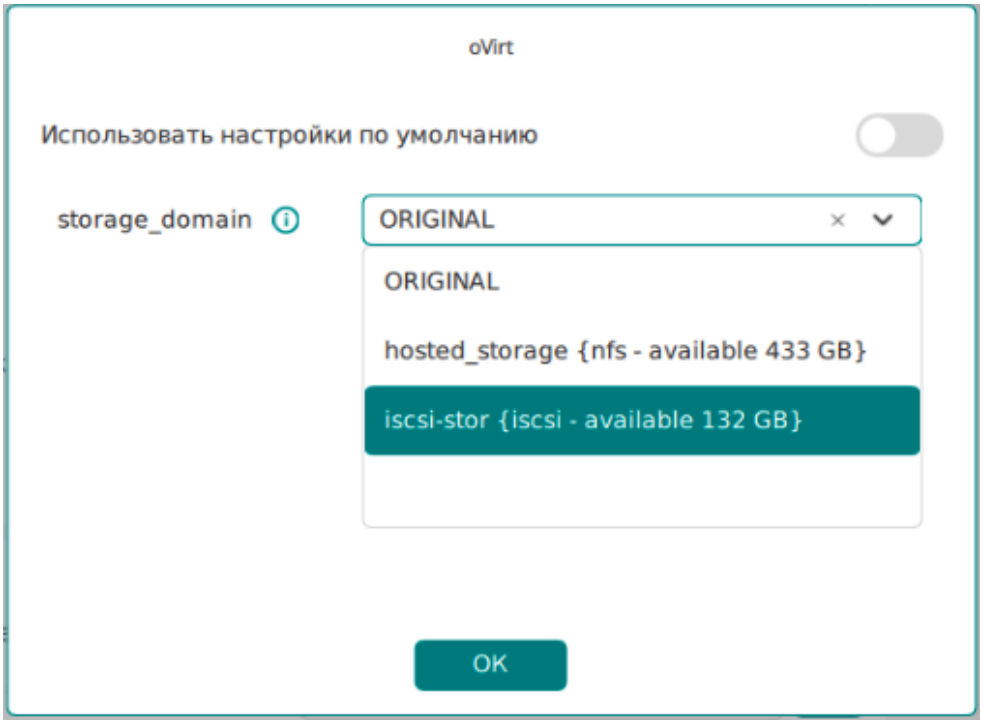
Убедитесь в том, что у пользователя `vdsm` имеются права на внесение изменений в каталоге, в который производится распаковка, например, `/rubackup-tmp`. Из консоли на клиенте выполните команду:

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

Если предполагается выполнить восстановление из резервной копии с развертыванием ВМ в платформе виртуализации, можно предварительно задать хранилище (NFS, iSCSI и FCP), в котором будут созданы диски создаваемой ВМ. Для этого откройте «Параметры восстановления для модуля oVirt», в открывшемся окне выберите требуемое значение для параметра `storage_domain` (рисунок 20).

В выпадающем окне представлена информация в виде: `<name> {<storage-type> – available <size> GB}`

В начале указано имя хранилища — `<name>`, типа хранилища — `<storage-type>` (NFS, iSCSI или FCP) и объем доступного пространства — `available <size> GB` (указано в Гигабайтах)



По умолчанию для параметра `storage_domain` выбрано значение `ORIGINAL`, при котором модуль будет создавать диски в том же хранилище, в котором они были на момент бэкапа у оригинальной виртуальной машины.

Для корректного восстановление резервной копии необходимо удостовериться, что в выбранном хранилище достаточно свободного места.

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.

Глава 6. 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

```
[root@ovirt-node1 ~]# rb_archives
Id   | Ref ID | Resource                                | Resource type | Backup
type | Created                | Crypto  | Signed | Status
-----+--------+-----------------------------------------+---------------+
-------------+------------------------+---------+--------+-------------
9468 |        | e6ce65ea-8b3d-45ae-bfd7-21bdf9d2e5cb | oVirt         | full
| 2022-06-08 16:29:47+03 | nocrypt | True   | Not Verified
9469 |        | e6ce65ea-8b3d-45ae-bfd7-21bdf9d2e5cb | oVirt         | full
| 2022-06-08 20:40:43+03 | nocrypt | True   | Not Verified
9471 |        | e6ce65ea-8b3d-45ae-bfd7-21bdf9d2e5cb | oVirt         | full
| 2022-06-09 16:14:02+03 | nocrypt | True   | Not Verified
```

Запрос на восстановление резервной копии

```
[root@ovirt-nodel -]#
[root@ovirt-nodel -]# rb_archives -X 9469
Password:
The archive will be restored in the directory: /rubackup-tmp
----> Restore archive chain: 9469 <----
Record ID: 9469 has status: Not Verified
Continue (y/n)?
```

Для восстановления резервной копии в хранилище типа NFS, iSCSI или FCP, необходимо указать имя хранилища с параметром `-e`:

```
rb_archives -x <archive_id> -e storage_domain:hosted_storage
```

Пример 1. Восстановление резервной копии в исходное хранилище

```
rb_archives -x <archive_id> -e storage_domain:ORIGINAL
```

Если параметр `storage_domain` не задан или если задано значение `ORIGINAL`, то при восстановлении РК диски ВМ будут созданы в том же хранилище, в котором они

были на момент бэкапа у оригинальной виртуальной машины.

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 случае, если резервная копия должна быть развернута, т.е. необходимо восстановить виртуальную машину в среду виртуализации, необходимо использовать опцию `-x`.

В случае, когда требуется восстановить резервную копию в локальном каталоге клиента без развертывания, нужно использовать опцию `-X`.