



RuBackup

**Система резервного копирования
и восстановления данных**

**OVIRT, ZVIRT, РЕД
ВИРТУАЛИЗАЦИЯ, ROSA, HOSTVM**

ВЕРСИЯ 2.6.0.0.0, 16.07.2025

Содержание

1. Поддерживаемые платформы виртуализации и типы хранилищ	4
2. Установка клиента RuBackup	5
2.1. Настройка доступа без пароля для пользователя <code>vds</code>	9
3. Мастер-ключ	10
4. Защитное преобразование резервных копий	11
4.1. Алгоритмы защитного преобразования	11
5. Использование менеджера администратора RuBackup (RBM)	12
5.1. Запуск RBM	12
5.2. Регулярное резервное копирование виртуальной машины	15
5.3. Срочное резервное копирование	21
5.4. Централизованное восстановление резервных копий	23
6. Восстановление со стороны клиента	28
7. Конфигурационный файл <code>rb_module_ovirt.conf</code>	30
8. Требования и ограничения для создания инкрементальных РК	37

Система резервного копирования RuBackup позволяет выполнять полное, инкрементальное и дифференциальное **резервное копирование** и восстановление виртуальных машин поддерживаемых платформ виртуализации.

СРК производит локальную дедупликацию и хранение резервных копий в дедуплицированном хранилище. В ходе локальной дедупликации сравниваются между собой блоки данных на клиенте и удаляются дубликаты. При передаче резервной копии в хранилище дедуплицированных резервных копий перемещаются только уникальные блоки (для того же типа источника данных), которых еще нет в хранилище.

Резервное копирование виртуальных машин поддерживаемых платформ виртуализации выполняется безагентным способом:

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 выполняется локальная дедупликация (если она включена) и из резервной копии удаляются дублирующиеся блоки.

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

Для выполнения резервного копирования виртуальных машин поддерживаемых платформ виртуализации необходимо установить клиент 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 копи-

ния.

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 платформы виртуализации и типы хранилищ

Таблица 1. Поддерживаемые платформы виртуализации

Платформа виртуализации	Версия
oVirt	4.4
	4.5
zVirt	4.0
	4.1
	4.2
ROSA Virtualization	2.1
	3.0
	(API Version 4.4, 4.5)
Red Virtualization Engine	7.3.0
HOSTVM	4.5

Таблица 2. Поддерживаемые типы хранилищ

Платформа виртуализации	Поддерживаемые типы хранилищ
oVirt	NFS 2.4.0
	iSCSI 2.4.0
zVirt	NFS 2.4.0
	iSCSI 2.4.0
ROSA Virtualization	NFS 2.4.0
	iSCSI 2.4.0
	FCP 2.4.0
РЕД Виртуализация	NFS 2.4.0
	iSCSI 2.4.0
HOSTVM	NFS 2.5.0

Глава 2. Установка клиента RuBackup

Для возможности резервного копирования виртуальных машин поддерживаемых платформ виртуализации 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».



Для запуска клиента как сервиса перезапустите демон командами:

```
systemctl daemon-reload
systemctl start rubackup_ovirt_client
```

Основные отличия работы клиента RuBackup в поддерживаемых платформах виртуализации 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 поддерживаемых платформ виртуализации, 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 резерв-

ного копирования требуется специально выделенное пространство (каталог для временных операций):

- a. Если значение параметра `backup_using_ovirt_api` `yes`, то требуемый объем пространства см. в главе «Требования и ограничения для создания инкрементальных РК».
- b. Если значение параметра `backup_using_ovirt_api` `no`, то объем пространства рассчитывается так:
 - Если значение параметра `backup_vm_from_native_host` `no` и в качестве хранилища дисков ВМ используется NFS, то для создания резервной копии потребуется не менее 2% от общего объема виртуальных машин, для которых выполняются одновременные операции резервного копирования (например, для одновременного резервного копирования 10 виртуальных машин по 10Гб необходимо 2Гб выделенного пространства). Это связано с тем, что хотя создание резервных копий дисков виртуальных машин и происходит непосредственно из хранилища, однако требуется свободное пространство для временного хранения служебной информации СРК.
 - Если значение параметра `backup_vm_from_native_host` `no` и в качестве хранилища дисков ВМ используется iSCSI ^[2] или FCP ^[3], а также если задача по созданию РК назначена на тот же узел, на котором эта ВМ развернута, то требования к пространству такие же, как и в предыдущем пункте.

Если же задача назначена на узел, отличный от того, на котором развернута ВМ, то объем требуемого пространства будет равен 102% от объема ВМ, для которой производится резервное копирование (100% — для временного хранения копии дисков виртуальной машины + до 2% для хранения служебной информации СРК). Копии дисков такой виртуальной машины загружаются в каталог для временных операций через oVirt API.

- Если значение параметра `backup_vm_from_native_host` `yes`, то вне зависимости от типа хранилища требования к свободному месту в каталоге для временных операций такие же, как в пункте.
- Если значение параметра `disk_upload_mechanism` `file`, то для восстановления резервной копии в каталоге распаковки, выбранном пользователем СРК, требуется свободное место в размере не менее 102% от объема виртуальной машины, для которой выполняется резервное копирование (100% от размера восстанавливаемого ресурса составляют данные дисков виртуальной машины, а до 2% — служебная информация СРК).
- Если значение параметра `disk_upload_mechanism` `nbd` и ВМ восстанавливается с дисками в хранилище типа FCP ^[3] или iSCSI ^[2], то для восстановления резервной копии в каталоге распаковки, выбранном пользователем СРК, может потребоваться свободное место в размере не менее

202% от объема виртуальной машины, для которой выполнено резервное копирование (до 200% от размера восстанавливаемого ресурса могут составить данные дисков виртуальной машины, а до 2% — служебная информация СРК). Это обусловлено необходимостью конвертации диска виртуальной машины из формата `qcow2` в `raw` перед загрузкой данных диска в хранилище платформы виртуализации средствами oVirt API. Если диск оригинальной виртуальной машины изначально был в формате `qcow2`, то конвертация требуется и на момент окончания конвертации в каталоге распаковки к этому диску будут относиться два файла: файл диска в формате `qcow2` и файл диска в формате `raw`. Если диск оригинальной виртуальной машины изначально был в формате `raw`, то конвертация не требуется и для восстановления резервной копии в каталоге распаковки потребуется меньше свободного места - до 102% от объема оригинальной виртуальной машины.

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 строку:

```
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 vdsd: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 `vdsd`:

```
chown vdsd: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`: (Глава 7)

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 vds:m: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 vdsmd

Для корректной работы с модулем пользователю vdsmd 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 vdsmd ssh-keygen -t rsa -b 4096 -f /var/lib/vdsmd/.ssh/id_rsa
```

Далее необходимо скопировать публичный ключ пользователя vdsmd, 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 vdsmd 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
```

```
00000000 79d1 4749 7335 e387 9f74 c67e 55a7 20ff
00000010 6284 54as 83a3 2053 4818 e183 1528 a343
00000020
```

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 3. 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](#)).

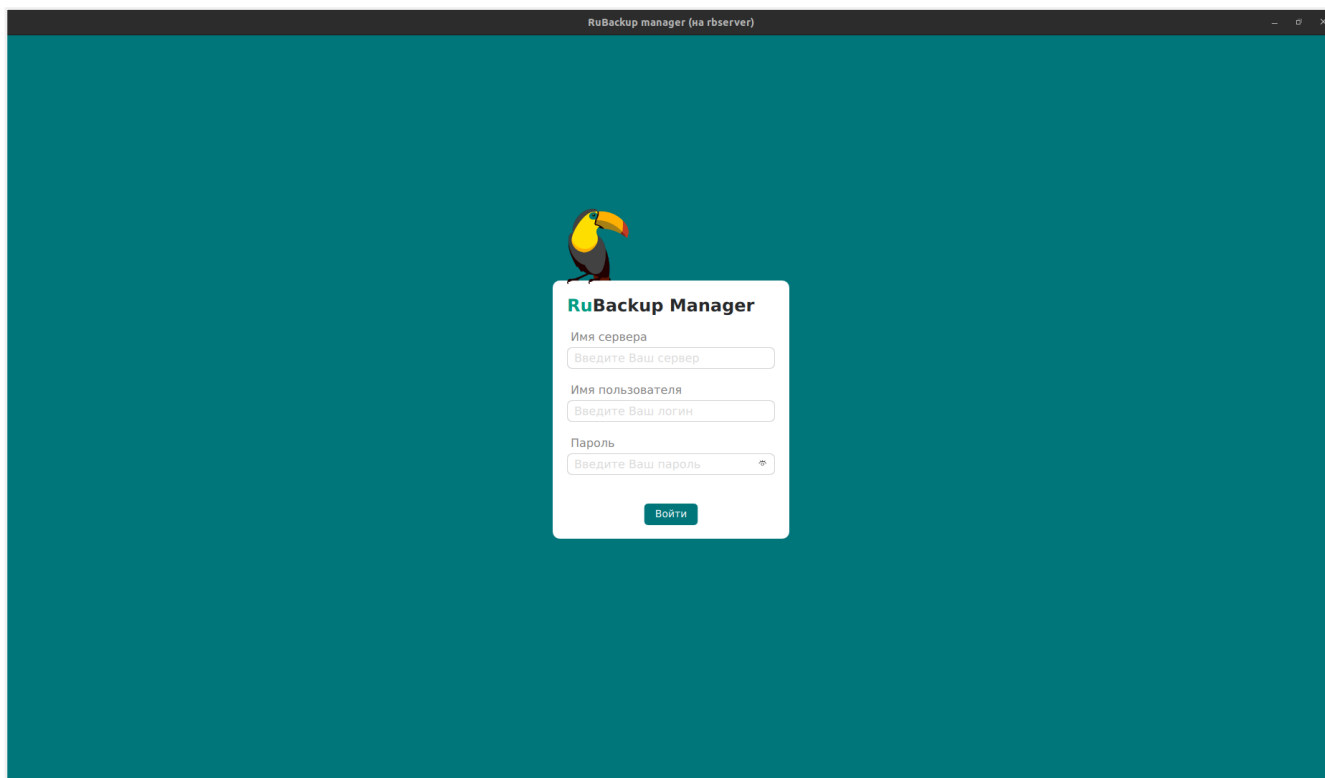


Рисунок 1.

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.

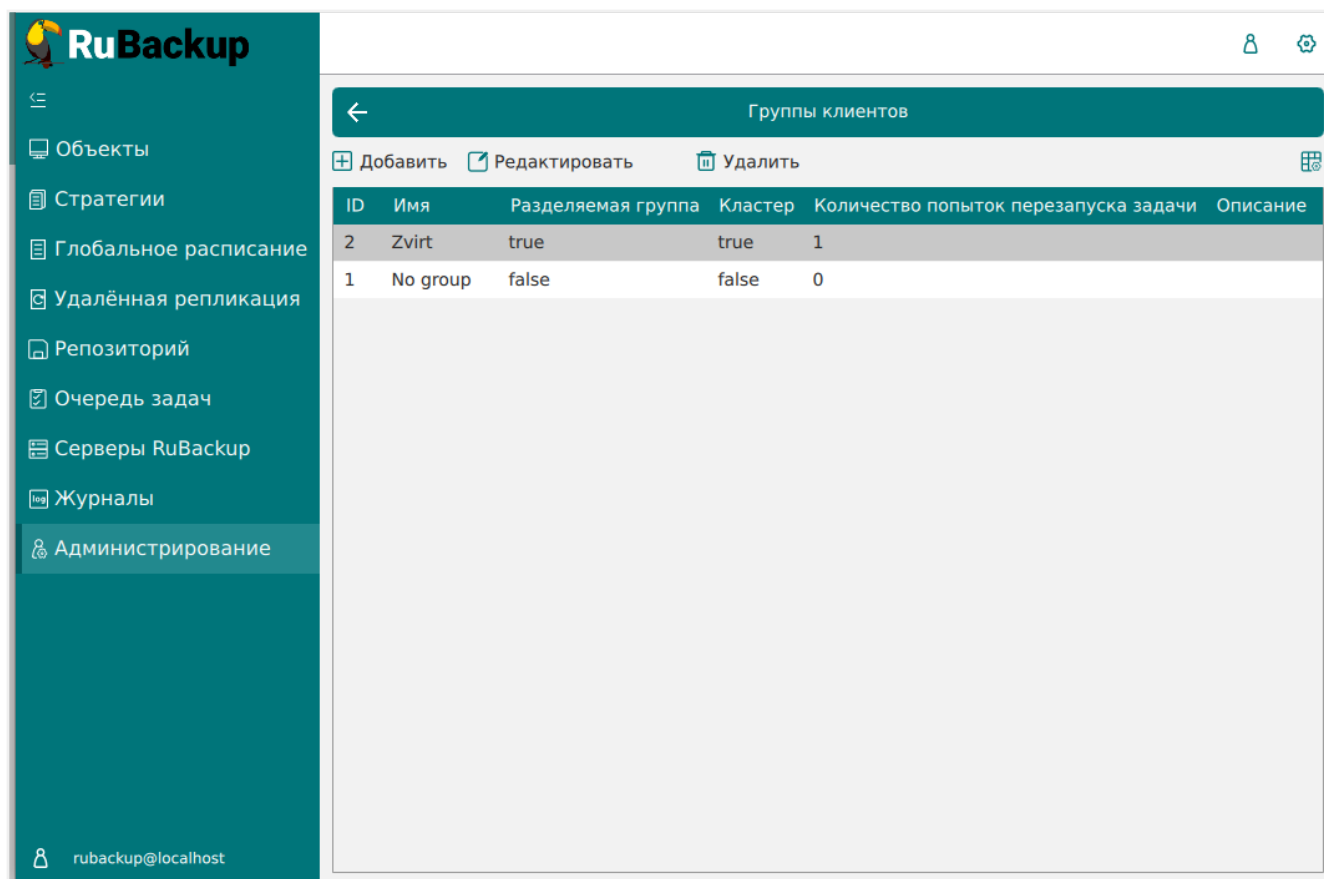


Рисунок 2.

Для авторизации неавторизованного клиента в RBM необходимо выполнить следующие действия:

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

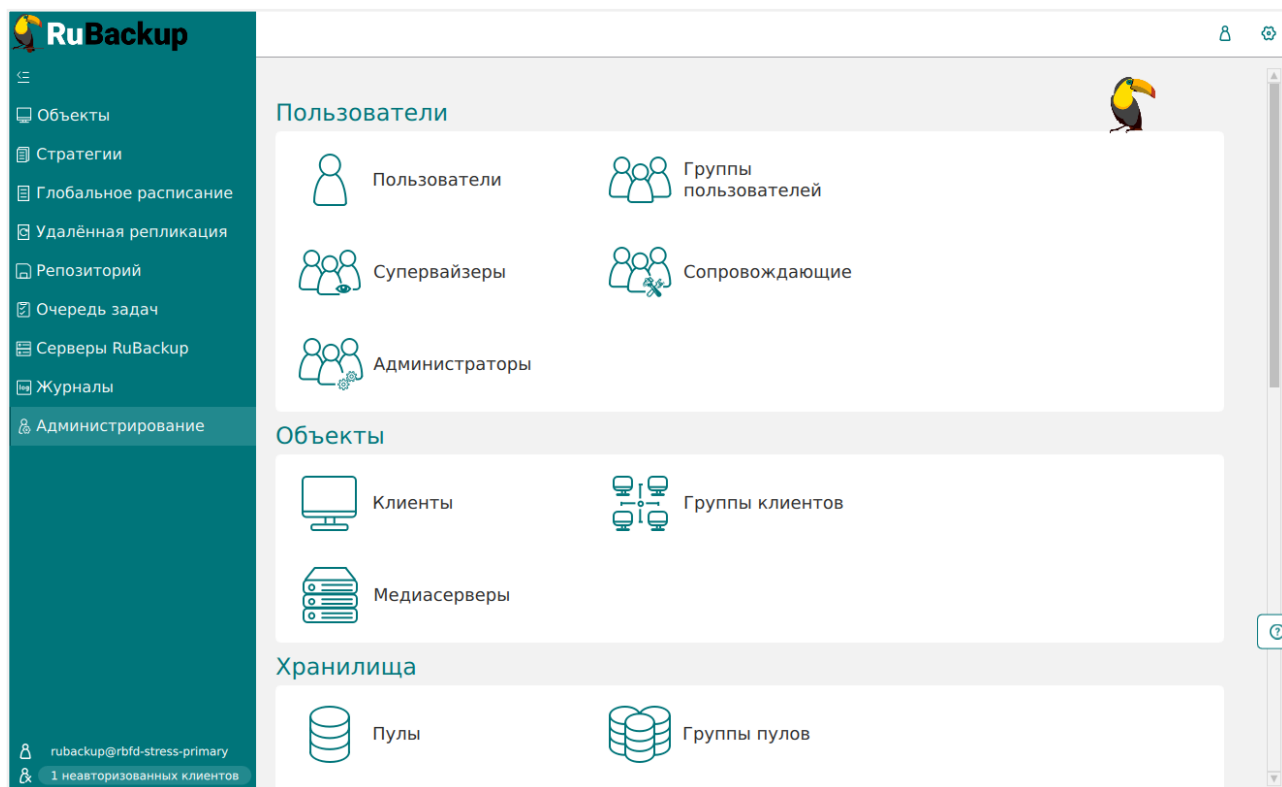


Рисунок 3.

- На верхней панели перейдите на вкладку **Неавторизованные клиенты** (Рисунок 4):

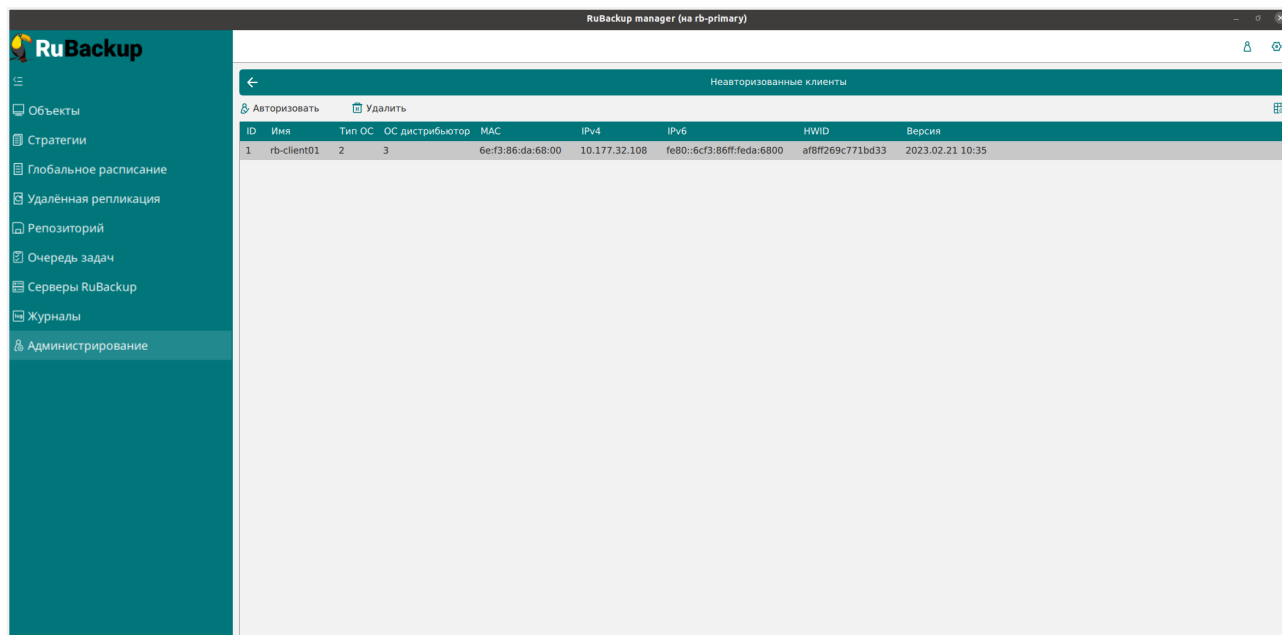


Рисунок 4.

- Нажмите на требуемого неавторизованного клиента правой кнопкой мыши и выберите **Авторизовать** (Рисунок 5):

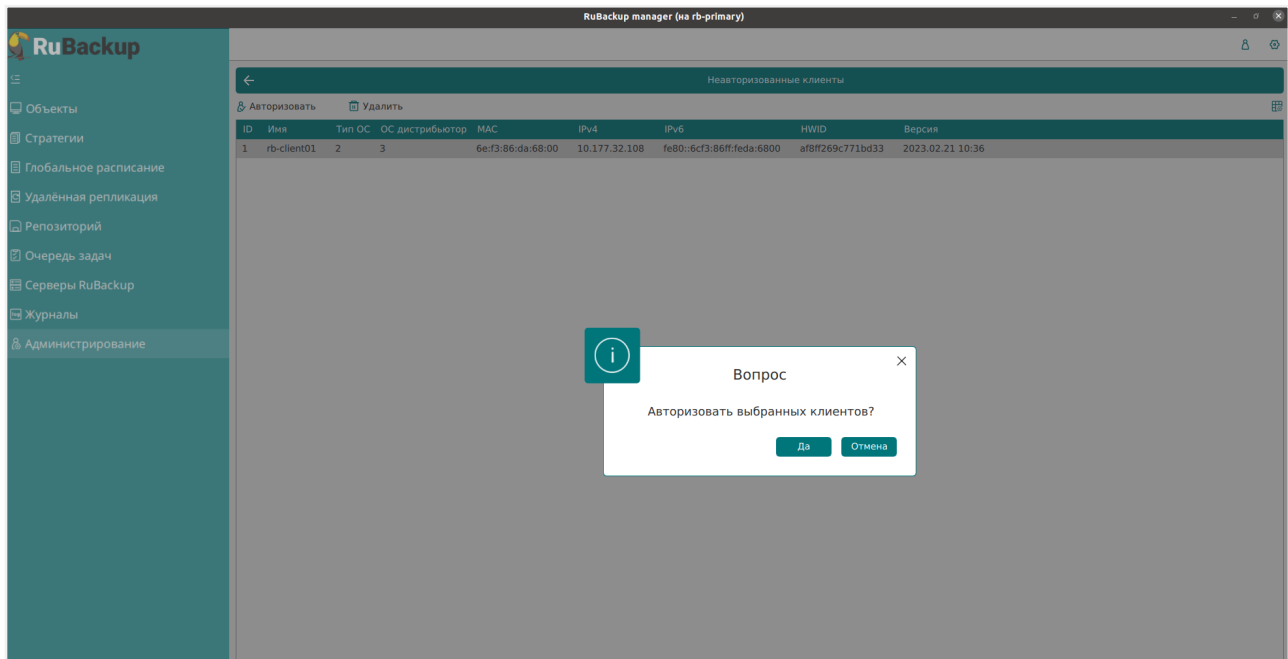


Рисунок 5.

После авторизации клиент будет виден на вкладке **Объекты** (Рисунок 6):

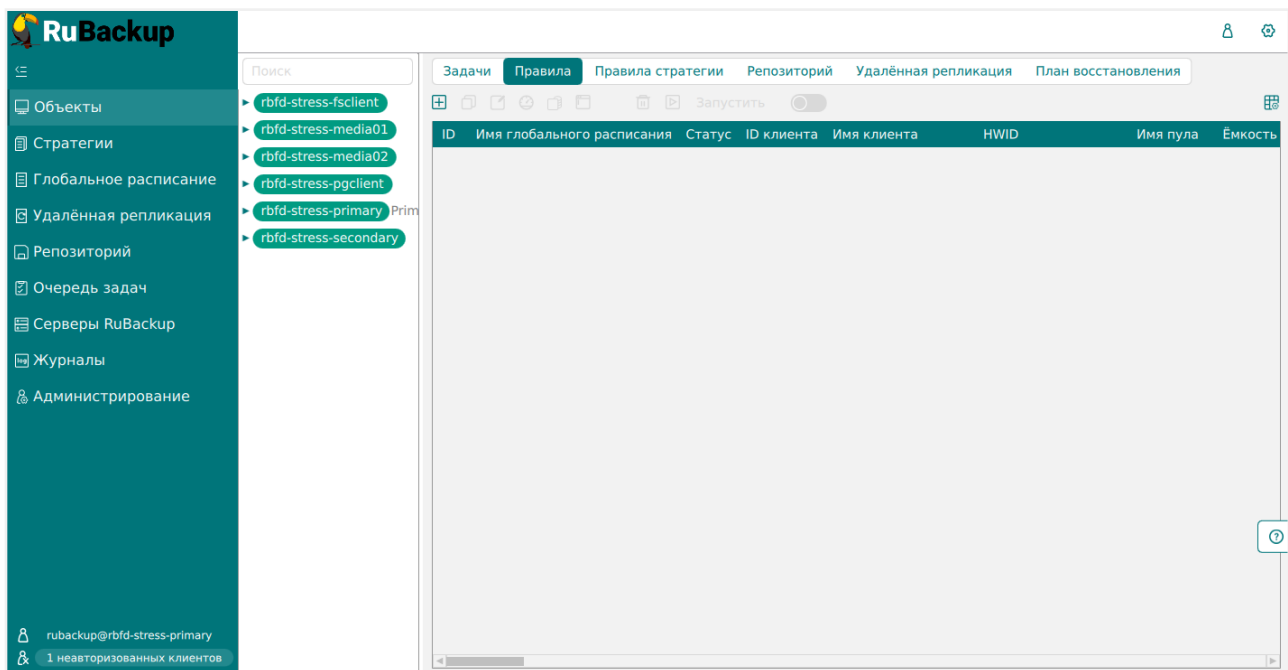


Рисунок 6.

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).



Перезагрузка виртуальной машины или гипервизора во время резервного

копирования или восстановления может привести к **потере данных виртуальной машины!**

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

Резервная копия средствами RuBackup позволит избежать полной потери данных ВМ.

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

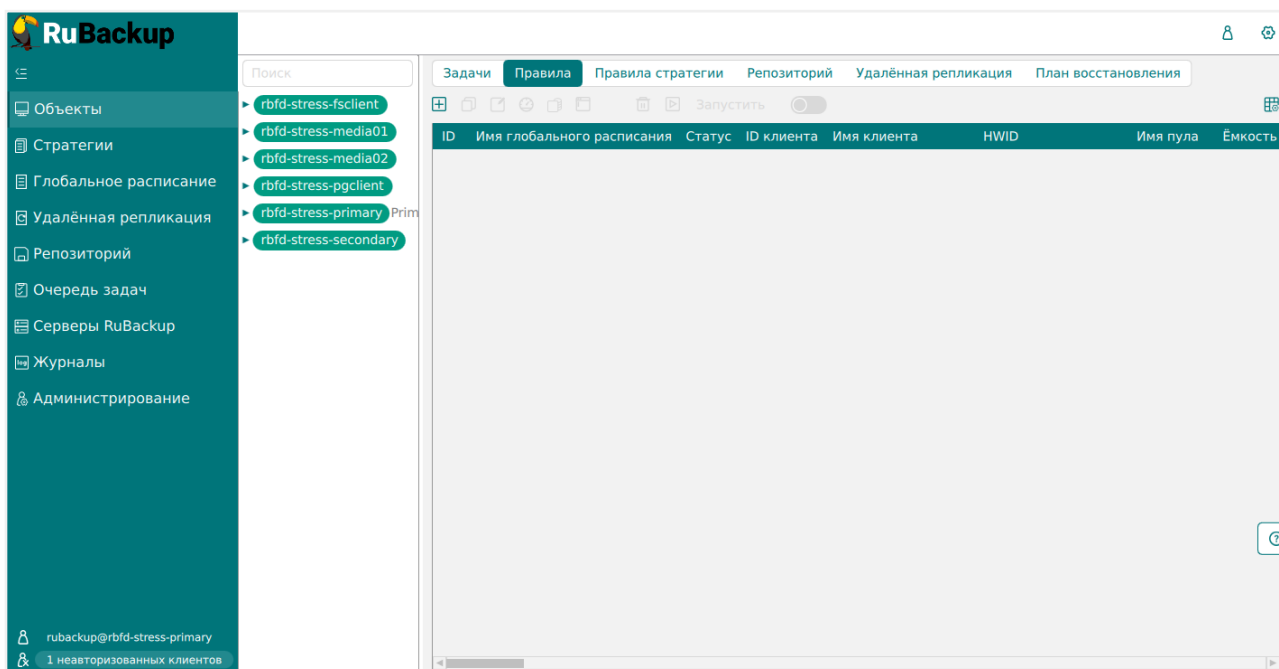


Рисунок 7.

2. Выберите клиент, вместе с которым установлен модуль RuBackup, предназначенный для резервного копирования виртуальных машин поддерживаемых платформ виртуализации.
3. Выберите тип ресурса **oVirt** (Рисунок 8):

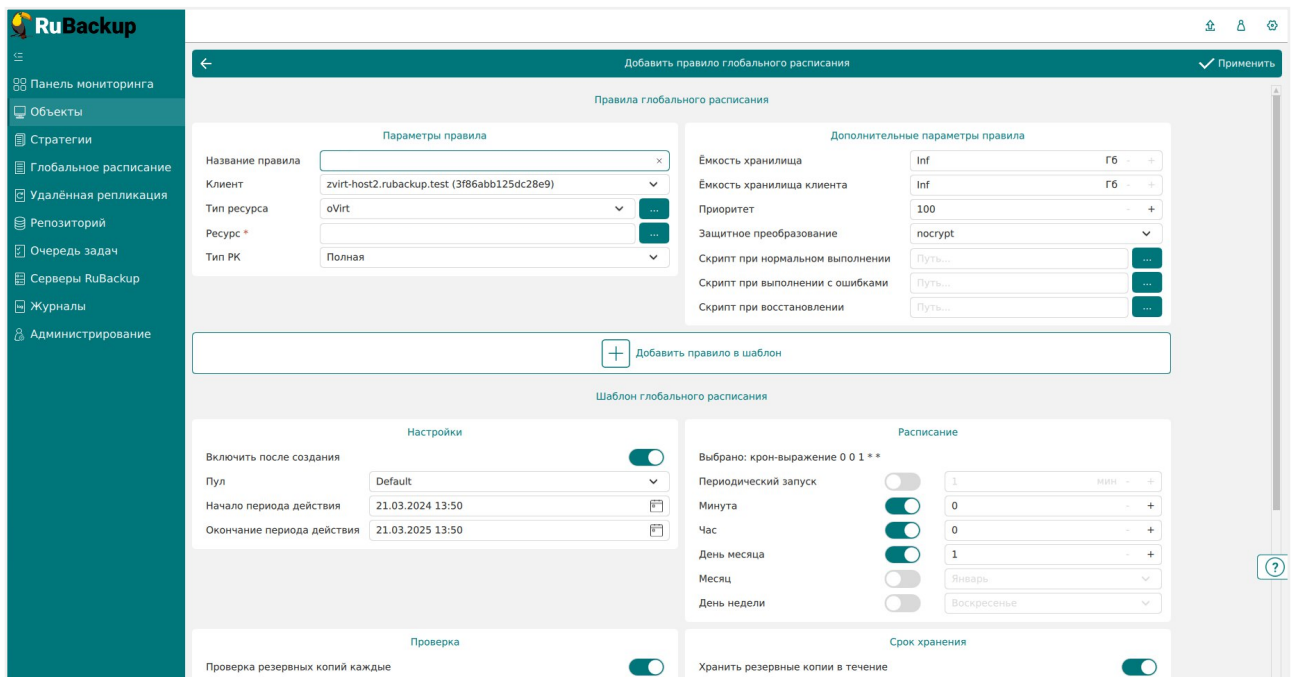


Рисунок 8.

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

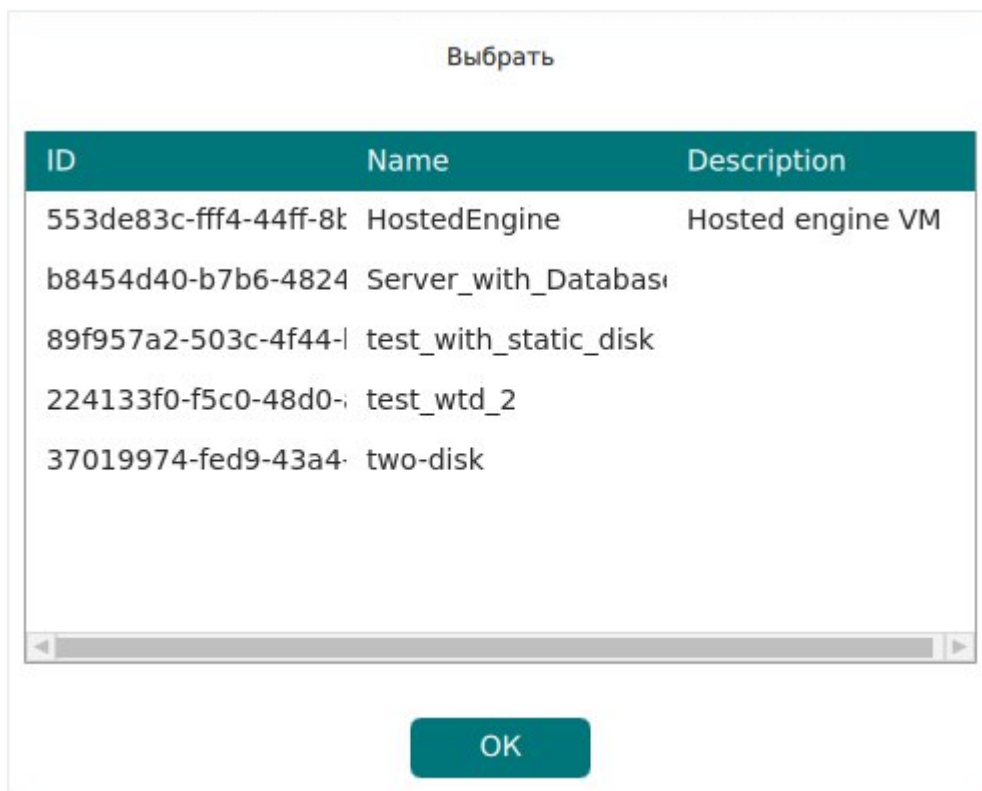


Рисунок 9.

Для резервного копирования виртуальных машин, в которых содержатся диски с типом «Предварительно размеченный», необходимо заранее в настройках диска установить флаг «Включить инкрементальное резервное копирование» (Глава 8) (Рисунок 10). В случае, если флаг будет выключен, при резервном

копировании не гарантируется восстановление с развертыванием.

Рисунок 10.

- 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.

- Нажав на иконку ... рядом с выбранным типом ресурса oVirt, установите дополнительные настройки правила резервного копирования ([Рисунок 12](#), [Таблица 4](#)).

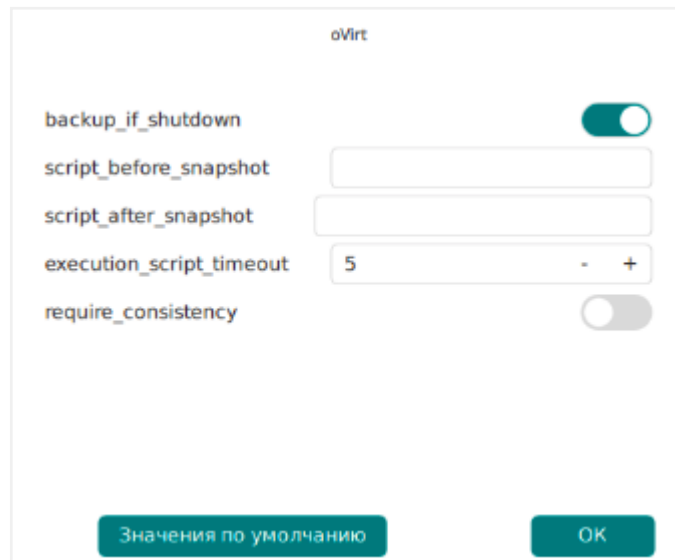


Рисунок 12.

Таблица 4. Дополнительные параметры правила резервного копирования виртуальных машин поддерживаемых платформ виртуализации

Параметр	Описание	Значение по умолчанию	Допустимые значения
backup_if_shutdown	Параметр, задающий возможность резервного копирования выключенной виртуальной машины: <code>true</code> — возможно создание резервной копии выключенной виртуальной машины. <code>false</code> — 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	<code>true</code>	<code>true</code> , <code>false</code>
script_before_snapshot	Полный путь к скрипту внутри виртуальной машины, который будет выполнен перед созданием снимка для данной виртуальной машины		
script_after_snapshot	Полный путь к скрипту внутри виртуальной машины, который будет выполнен после создания снимка 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 снимка	5	1...600
require_consistency	Параметр, выполняющий проверку на заморозку ВМ. При значении параметра <code>true</code> резервное копирование ВМ завершится ошибкой, если ВМ не заморожена.	<code>false</code>	<code>true</code> , <code>false</code>



- 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 VM 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):

The screenshot shows the 'Добавить глобальное расписание' (Add global schedule) configuration page in the RuBackup web interface. The left sidebar contains navigation links: Объекты, Стратегии, Глобальное расписание, Удалённая репликация, Репозиторий, Очередь задач, Серверы RuBackup, Журналы, and Администрирование. The main content area is divided into several sections:

- Пул (Pool):** dedup-4T. Includes fields for 'Начало периода действия' (22.05.2023 13:14) and 'Окончание периода действия' (22.05.2024 13:14).
- Периодический запуск (Periodic run):** Includes toggle switches for 'Минута' (0), 'Час' (0), 'День месяца' (1), 'Месяц' (Январь), and 'День недели' (Воскресенье).
- Проверка (Check):** Includes a toggle for 'Проверка архива каждые' (1 Months).
- Срок хранения (Retention):** Includes a toggle for 'Хранить резервные копии в течение' (1 Years).
- Резервные копии (Backups):** Includes a toggle for 'Переместить в пул через' (1 Days) and a dropdown for 'Пул' (dedup-4T).
- Устаревшие резервные копии (Old backups):** Includes a toggle for 'Автоматическое удаление' and a dropdown for 'Уведомлять' (Nobody).
- Уведомления (Notifications):** Includes a table for configuring notifications for various events.

Событие (Event)	Получатель (Receiver)	Тип уведомления (Notification type)
Нормальное выполнение (Normal execution)	Nobody	E-mail CC
Выполнение с ошибкой (Execution with error)	Nobody	E-mail CC
Проверка резервной копии (Backup check)	Nobody	E-mail CC
Окончание действия правила (Rule completion)	Nobody	E-mail CC
Окончание ёмкости в пуле (Pool capacity completion)	Nobody	E-mail CC

At the bottom left, it shows the user 'rubackup@rbfd-stress-primary' and '1 неавторизованных клиентов' (1 unauthorized clients).

Рисунок 13.

8. После выполнения настроек правила резервного копирования 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.

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):

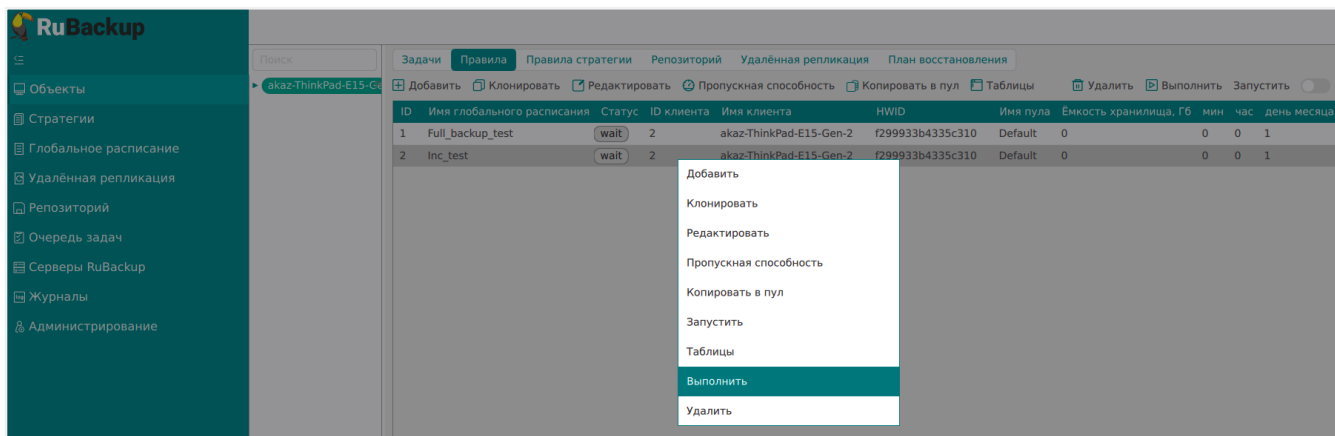


Рисунок 15.



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

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

Резервная копия средствами RuBackup позволит избежать полной потери данных VM.

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

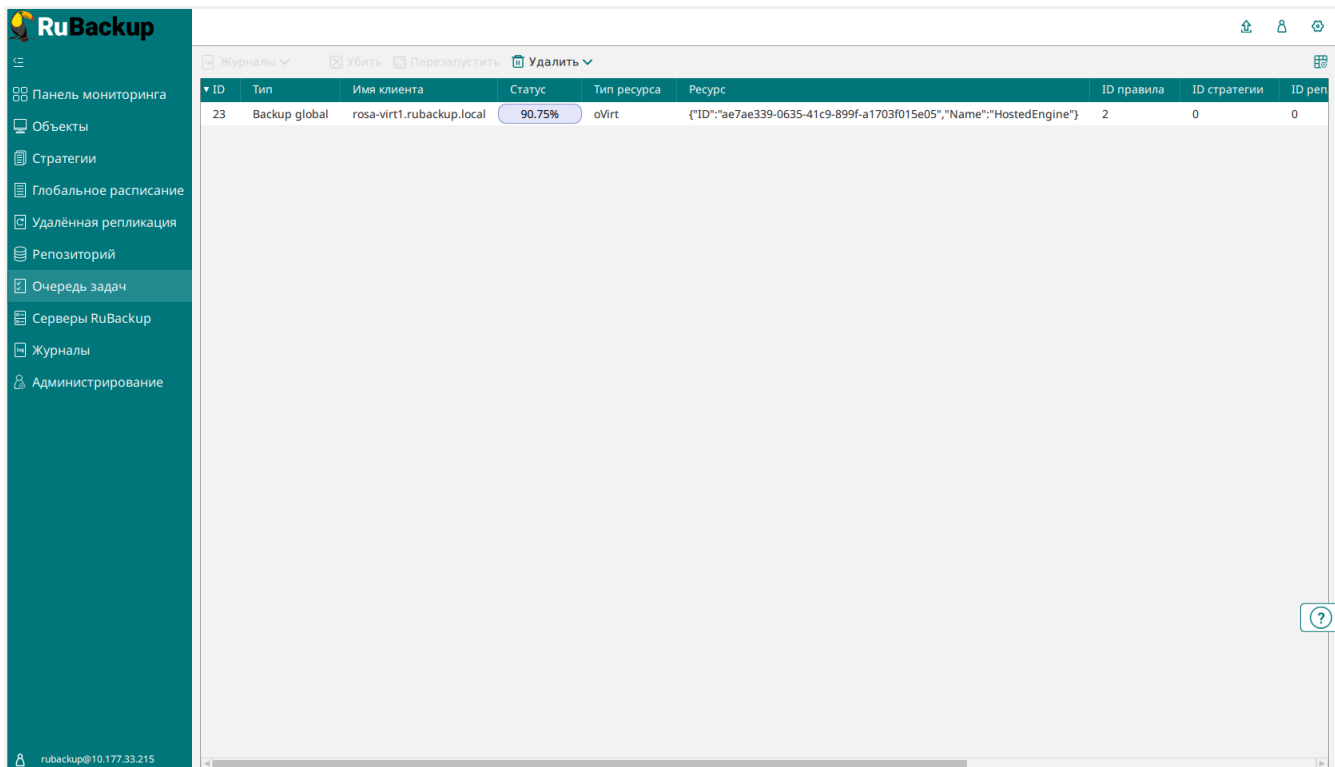


Рисунок 16.

При успешном завершении резервного копирования соответствующая задача перейдет в статус «**Done**» ([Рисунок 17](#)):

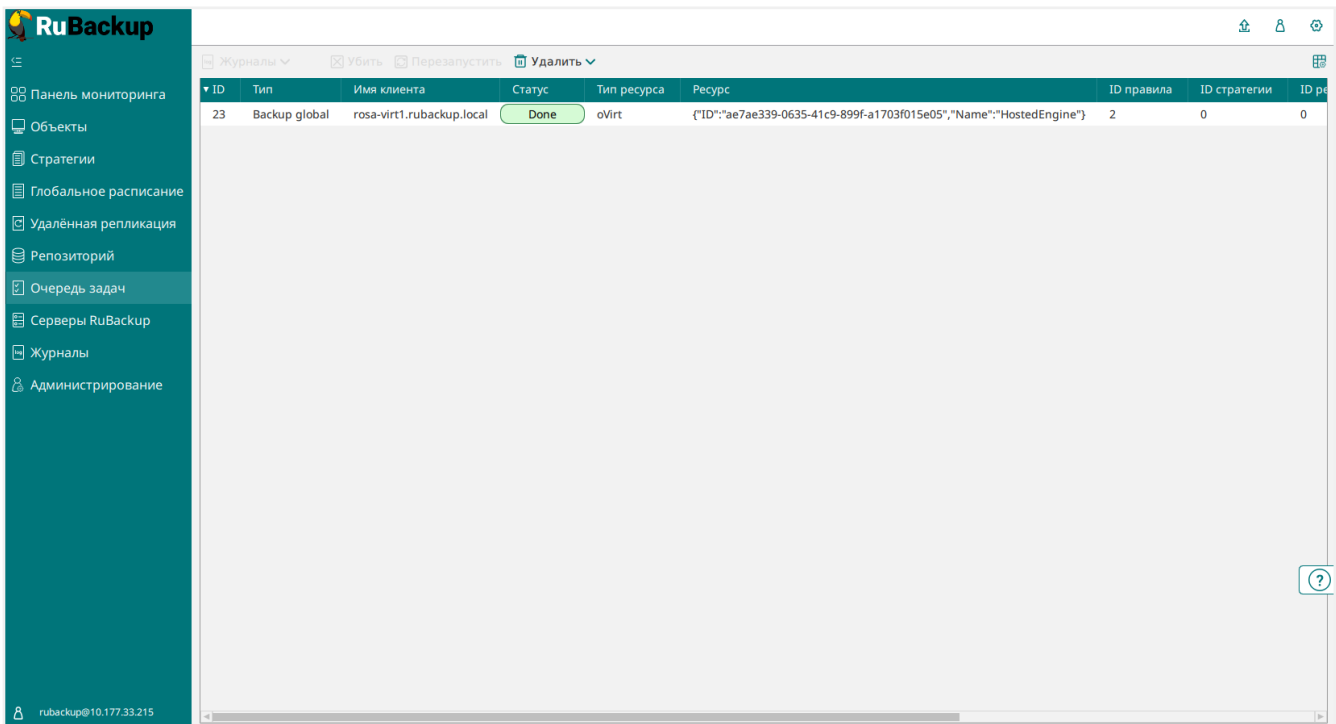


Рисунок 17.

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. [RuBackup Manager \(RBM\)](#)).

В тех случаях, когда централизованное восстановление на клиенте доступно, его можно инициировать, вызвав правой кнопкой мыши контекстное меню «Восстановить» ([Рисунок 18](#)):

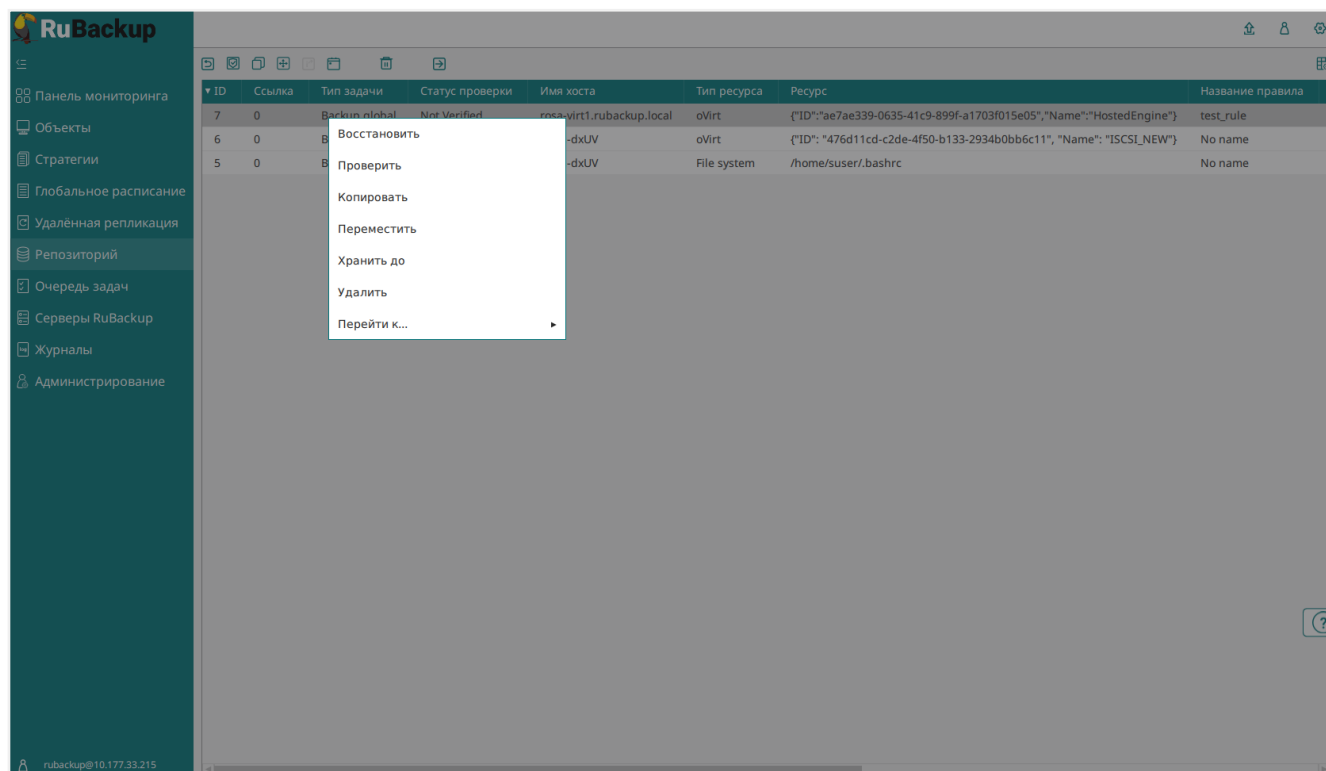


Рисунок 18.

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.

Централизованное восстановление ✓ Применить

Информация о резервной копии

Имя хоста: rosa-virt1.rubackup.local

HWID: 2c5a44b0806b7a6c

Тип ресурса: oVirt

Ресурс: e339-0635-41c9-899f-a1703f015e05,"Name":"HostedEngine"}

Пул: Default

Тип РК: full

Создано: 2025.01.22 11:42:04

Восстановить цепочку: 7

Имя правила: test_rule

Статус РК: Not Verified

Место восстановления

Восстановить на клиента: i-virt1.rubackup.local (2c5a44b0806b7a6c)

Каталог распаковки: * ⓘ

Параметры восстановления для модуля: oVirt

Скрипт при восстановлении:

Восстановить на целевом ресурсе: ⓘ ☐

Рисунок 19.

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)

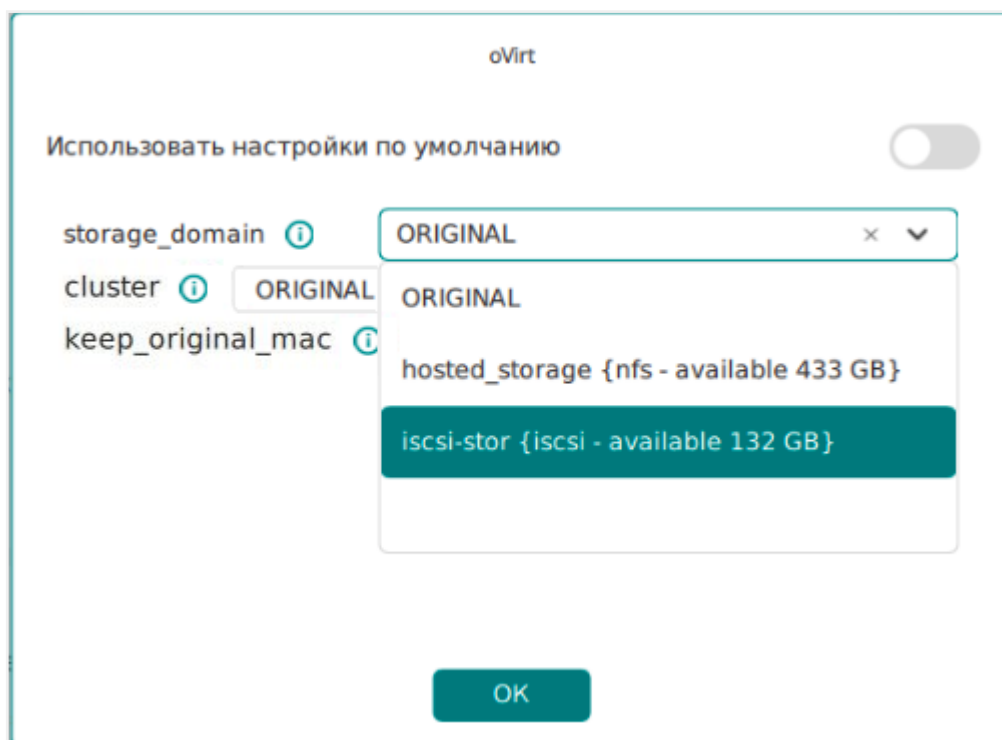


Рисунок 20.

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 восстановления резервной копии необходимо, чтобы:

- выбранные Storage Domain и Cluster были ассоциированы между собой. В противном случае будет автоматически предпринята попытка найти Cluster, связанный с выбранным Storage Domain;
- в выбранном хранилище было достаточно свободного места.

По умолчанию для каждого сетевого интерфейса ВМ, созданной в процессе восстановления из РК, платформа виртуализации назначает новый MAC-адрес.

Если восстановленная ВМ должна иметь MAC-адрес исходной ВМ, активируйте переключатель `keep_original_mac` ☒ (Рисунок 21).

Если MAC-адрес интерфейса занят оригинальной или другой ВМ, то у созданной в процессе восстановления ВМ сетевой интерфейс будет отсутствовать. В этом случае в журнал модуля (`/opt/rubackup/log/rb_module_ovirt.log`) будет добавлено предупреждение о невозможности добавления интерфейса с уже занятым MAC-адресом.

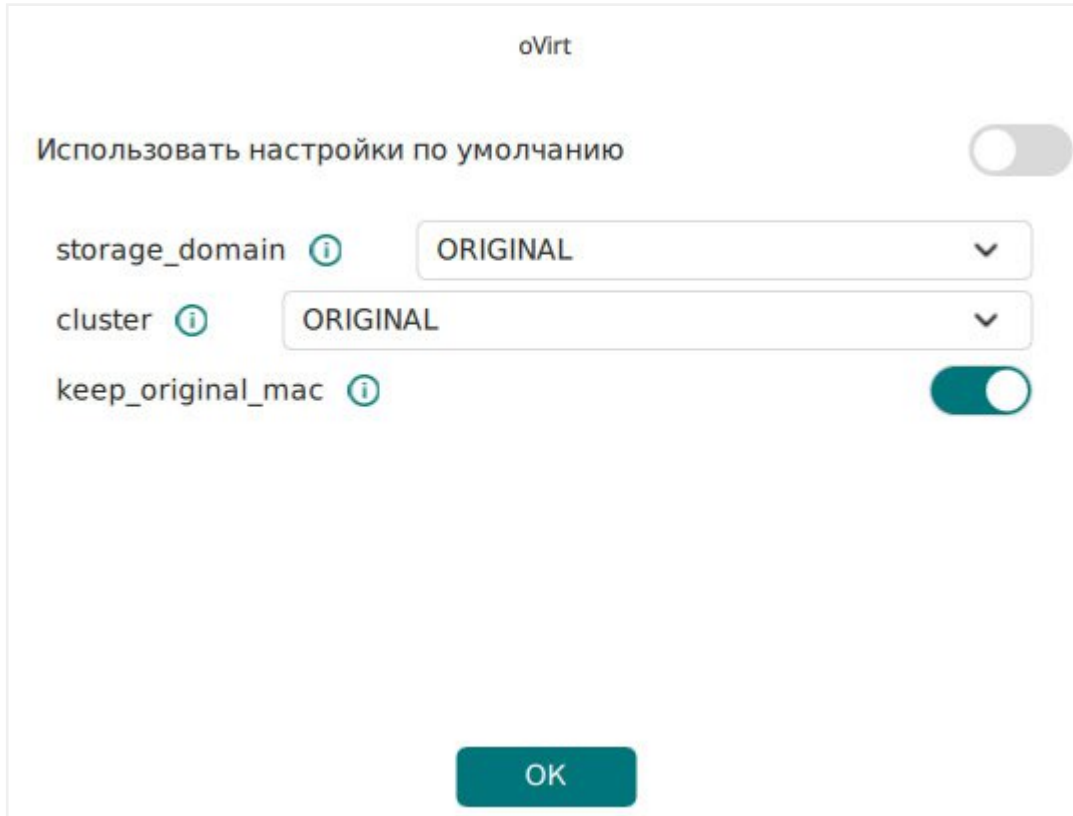


Рисунок 21.

Проверить ход выполнения восстановления резервной копии можно в разделе  **Задачи**.

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
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 VM 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 `vds` возможность делать изменения внутри данного каталога:

```
chown -R vds: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`.

Глава 7. Конфигурационный файл `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: 25
# minutes. Min 1 minute
disk_upload_timeout 25

# Specifies the maximum single disk download timeout in minutes. Default: 25
# minutes. Min 1 minute
disk_download_timeout 25

# RuBackup module creates oVirt ImageTransfer in order to download or upload
# disk data.
# Parameter 'image_transfer_timeout' specifies the amount of time in seconds
# the module will wait the ImageTransfer goes to state "transferring".
# If this timeout is reached but the ImageTransfer is not in 'transferring'
# state
# corresponding backup or restore task will end with error.
# Possible values: [1, 3600]
# Default value: 300
image_transfer_timeout 300
```

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

```
imagetransfer_inactivity_timeout 60
```

```
# When backup via oVirt API is done and VM disks are dumped
```

```
# RuBackup module initiates finalizing the ImageTransfer.
```

```
# After that it waits while the the ImageTransfer reaches state
'finished_success'.
```

```
# Parameter 'image_transfer_finalize_timeout' specifies the amount of time in
seconds
```

```
# the module will wait the ImageTransfer is finalized.
```

```
# If this timeout is reached but the ImageTransfer is not in
'finished_success'
```

```
# state a Warning is added to the module log.
```

```
# Further ovirt backup finalizing can also fail due to this.
```

```
# Possible values: [1, 3600]
```

```
# Default value: 300
```

```
image_transfer_finalize_timeout 300
```

```
# 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
```

```
# Set this flag to 'yes' if there is a need to make a VM backup by means of
the platform (oVirt API)
```

```
# Possible values: yes, no
```

```
# Default value: no
```

```
backup_using_ovirt_api no
```

```
# Set this flag to 'yes' if there is a need to remove all VM checkpoints at
full backup task.
```

```
# The flag is applicable only if 'backup_using_ovirt_api' is set to 'yes'.
```

```
# Possible values: yes, no
```

```
# Default value: no
```

```
remove_vm_checkpoints_at_full_backup no
```

```
# When the 'backup_using_ovirt_api' is set to 'yes', RuBackup module
initiates backup
```

```
# of a VM using oVirt API. After that it waits while the backup reaches state
'ready'.
```



```
# Parameter 'platfom_side_backup_timeout' specifies the amount of time in
seconds
# the module will wait the backup is ready.
# If this timeout is reached but the backup is not in 'ready' state
# corresponding backup task will end with error.
# Possible values: [1, 72000]
# Default value: 7200
platfom_side_backup_timeout 7200

# When backup via oVirt API is ready and VM disks are dumped
# RuBackup module initiates finalizing the backup.
# After that it waits while the backup reaches state 'succeeded'.
# Parameter 'backup_finalize_timeout' specifies the amount of time in seconds
# the module will wait the backup succeeded.
# If this timeout is reached but the backup is not in 'succeeded'
# state a Warning is added to the module log.
# Possible values: [1, 3600]
# Default value: 300
backup_finalize_timeout 300
```

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

Таблица 5. Параметры файла конфигурации модуля резервного копирования oVirt/zVirt/РЕД Виртуализация/ROSA Virtualization/HOSTVM

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 password API-платформой виртуализации	
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. • file — механизм взаимодействия с дисками на основе прямого доступа к ним. 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
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 кластерную 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
disk_upload_timeout	Таймаут для загрузки каждого диска на платформу при восстановлении. Измеряется в минутах. По умолчанию 25 минут. Минимальное значение — 1 минута;	25
disk_download_timeout	Таймаут для загрузки каждого диска с платформы при бэкапе. Измеряется в минутах. По умолчанию 25 минут. Минимальное значение — 1 минута;	25

Параметр	Назначение	Значение по умолчанию
image_transfer_timeout	Параметр указывает время в секундах, в течение которого модуль будет ожидать перехода ImageTransfer в состояние "transferring". Если это время ожидания истекло, но ImageTransfer не перешел в состояние "transferring", то соответствующая задача резервного копирования или восстановления завершится с ошибкой. По умолчанию 300 секунд. Минимальное значение — 1 секунда, максимальное — 3600 секунд;	300
imagetransfer_inactivity_timeout	Параметр определяет какое количество секунд платформа будет ожидать начала загрузки диска после создания ImageTransfer-a. Измеряется в секундах. Минимальное значение — 5 секунд, максимальное значение — 500 секунд.	60
image_transfer_finalize_timeout	Параметр указывает время в секундах, в течение которого модуль будет ожидать завершения ImageTransfer. Если время ожидания истекло, но ImageTransfer не перешел в состояние "finished_success", в журнал модуля будет добавлено предупреждение. Из-за этого резервное копирование может завершиться с ошибкой.	300
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	
curl_verbose	Параметр выводит дополнительную информацию по REST API запросам, при значении yes.	no

Параметр	Назначение	Значение по умолчанию
backup_using_ovirt_api	Параметр, позволяющий выбрать способ резервного копирования средствами oVirt API ^[3]. Допустимые значения: <code>yes</code>, <code>no</code>. Если используется значение <code>yes</code>, то модуль выполняет бэкап средствами oVirt API. При значении <code>no</code>: • для включенной VM: ◦ Модуль отправляет запрос к гипервизору на создание снимков дисков VM (команда <code>virsh snapshot-create-as <domain_id></code>) ◦ "Подмороженные" после снимка диски VM запаковываются в архив РК ◦ Модуль выполняет комит снимков (<code>virsh blockcommit</code>) • для выключенной VM: ◦ Модуль пытается найти расположение дисков VM. ◦ Если расположение найдено, диски VM запаковываются в архив РК ◦ Если расположение не найдено, выполняется дамп дисков в каталог для временных операций, после чего сдмпленные файлы дисков запаковываются в архив РК	
remove_vm_checkpoint_at_full_backup	При создании бэкапа VM средствами oVIRT API платформа виртуализации формирует чекпойнт ^[1] резервируемой VM. Если у данного параметра значение выставлено в <code>yes</code>, а также у параметра <code>backup_using_ovirt_api</code> значение <code>yes</code>, то при каждом полном РК VM, СРК (модуль) выполнит запрос на получение списка имеющихся чекпойнтов VM, и для каждого чекпойнта отправит запрос на его удаление.	no
platform_side_backup_timeout	Параметр указывает время в секундах, в течение которого модуль будет ожидать готовности (переход oVirt бэкапа в состояние <code>ready</code> ^[2]) резервной копии. Если время ожидания истекло, но резервная копия не находится в состоянии готовности, соответствующая задача резервного копирования завершится с ошибкой. Минимальное значение — 1 секунда, максимальное — 72000 секунд;	7200
backup_finalize_timeout	Параметр указывает количество времени в секундах, в течение которого модуль будет ожидать (ожидается переход oVirt бэкапа в состояние <code>succeeded</code>) успешного завершения резервного копирования. Если время ожидания истекло, но резервное копирование не завершилось успешно, в журнал модуля <code>/opt/rubackup/log/rb_module_ovirt.log</code> будет добавлено предупреждение. Минимальное значение — 1 секунда, максимальное — 3600 секунд;	300

- [1] https://www.ovirt.org/documentation/doc-REST_API_Guide/#types-checkpoint
- [2] https://www.ovirt.org/documentation/doc-REST_API_Guide/#types-backup_phase
- [3] <https://www.ovirt.org/develop/release-management/features/storage/incremental-backup.html>

Глава 8. Требования и ограничения для создания инкрементальных РК

Значение параметров см. в разделе [Глава 7](#)

1. Если цепочка РК началась с `backup_using_ovirt_api`, установленным в значение `no`, при очередной итерации инкрементального РК модуль также проверит значение параметра `backup_using_ovirt_api` в конфигурационном файле модуля, если значение изменилось на `yes`, будет соответствующее уведомление в журнале модуля, и цепочка РК начнется заново (т.е. вместо инкрементально копии будет создана полная).
2. Если цепочка РК началась с `backup_using_ovirt_api`, установленным в значение `yes`, при очередной итерации инкрементального РК модуль также проверит значение параметра `backup_using_ovirt_api` в конфигурационном файле модуля, если значение изменилось на `no`, будет соответствующее уведомление в журнале модуля, и цепочка РК начнется заново.
3. Если `backup_using_ovirt_api` установлен в `yes`, выполняется итерация на создание инкрементальной РК и у какого-либо диска резервируемой VM в системе виртуализации значение для параметра `Backup type` отличное от **incremental**, то вместо инкрементальной РК средствами API oVirt будет выполнен полный дамп дисков VM (также через oVirt API), далее расчет изменений (дельта с момента создания предыдущей РК) будет выполнять `rbfd` (см. [rbfd](#))^[1].
4. Если `backup_using_ovirt_api` установлен в `yes`, выполняется итерация на создание инкрементальной РК и у какого-либо диска резервируемой VM в системе виртуализации значение **raw** для параметра `format`^[2], то вместо инкрементальной РК средствами API oVirt будет выполнен полный дамп дисков VM, далее расчет изменений (дельта с момента создания предыдущей РК) будет выполнять `rbfd`^[1].
5. В случае, когда создается цепочка РК, для которой выполняются условия (пунктов 3 и 4) для создания инкремента средствами oVirt API, но на текущей итерации инкрементального РК эти условия не выполняются, в такой ситуации будет выведено предупреждение в журнал модуля, и цепочка РК начнется заново (вместо инкрементальной копии будет создана полная).
6. При полном резервном копировании средствами oVirt API в каталоге для временных операций на клиенте должно быть достаточно свободного места, чтобы сохранить копии дисков VM и до 2% от суммарного размера дисков под метаданные, которые формирует СРК (в процессе работы `rbfd`).
7. Для случаев, когда поддерживается инкрементальное РК средствами oVirt API (пунктов 3 и 4), при полном РК дампы дисков VM сохраняются в каталог для временных операций на клиенте. Файлы дампов имеют `raw` формат. На этапе создания инкрементальной копии средствами oVirt API дампы дисков (только

дельта с момента предыдущего РК) формируются в `qcow2` формате. При распаковке цепочки таких РК алгоритм работы модуля для каждого диска ВМ следующий:

- распаковывается дамп диска в `raw` формате;
- выполняется конвертация файла диска из `raw` в `qcow2` формат;



На эту операцию требуется дополнительное время и на момент окончания конвертации в каталоге распаковки РК будет два файла, относящиеся к конкретному диску ВМ. Таким образом требования к свободному месту в каталоге распаковки на этой итерации:

$(\text{суммарный размер дисков ВМ}) * 2 + \sim 0,02 * (\text{суммарный размер дисков ВМ})$ ^[3]

- после конвертации файла диска в `qcow2` формат, файл в `raw` формате более не требуется - модуль его удаляет;
- на итерации распаковки инкрементальной копии для каждого диска ВМ выполняется `rebase` процедура (используется базовый файл, полученный на предыдущей итерации распаковки и `qcow` файл, распакованный на текущей итерации). Это реализовано с помощью утилиты `qemu-img`. После `rebase` процедуры, `qcow2`, распакованный на текущей итерации удаляется, так как он более не нужен. Таким образом требования к свободному месту в каталоге распаковки на этой итерации:

$(\text{суммарный размер дисков ВМ}) + \sim 0,02 * (\text{суммарный размер дисков ВМ}) + (\text{суммарный размер дисков ВМ, содержащих дельту, полученную на соответствующей итерации РК})$

- после распаковки всей цепочки РК в каталоге распаковки для каждого диска будет существовать только один файл в `qcow2` формате.
- если выполняется восстановление с развертыванием, то модуль выполняет выгрузку данных для каждого диска в систему виртуализации, после чего удаляет уже ненужный файл диска в `qcow2` формате из каталога распаковки.

[1] определение дельты выполняет не система виртуализации, а СРК (уже после дампа диска в каталог для временных операций)

[2] https://www.ovirt.org/documentation/doc-REST_API_Guide/#types-disk_format

[3] Первое слагаемое - под файлы дисков ВМ (`raw` и `qcow2`), второе слагаемое - под метаданные СРК