RuBackup
Система резервного копирования и восстановления данных

Резервное копирование

и восстановление RUSTACK

Версия 2.1

20.05.2024 г.

Содержание

Введение

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

Резервное копирование виртуальных машин RUSTACK выполняется безагентным способом. Это означает, что в виртуальную машину, для которой предполагается создание резервной копии, не устанавливается агент RuBackup (однако требуется установка гостевых расширений операционной системы, например qemu-guest-agent); резервное копирование виртуальной машины выполняется целиком, для всех дисков виртуальной машины; в ходе резервного копирования во всех случаях из резервной копии удаляются дублирующие блоки (всегда выполняется локальная дедупликация).

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 RUSTACK необходимо установить клиента резервного копирования RuBackup по одной из следующих схем:

– на одну из виртуальных машин в данной среде виртуализации, для которой настроен доступ к гипервизору (гипервизорам);

– на несколько виртуальных машин в данной среде виртуализации, если это обусловлено необходимостью динамически распределять нагрузку в ходе резервного копирования или обеспечить возможность вывода той или иной виртуальной машины из эксплуатации без изменений в расписании резервного копирования (в данной схеме необходимо включить эти гипервизоры в кластерную группу клиентов системы резервного копирования);

При выполнении резервного копирования применяется технология создания моментальных снимков данных для дисков виртуальной машины, что позволяет не останавливать 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. Для выполнения скрипта, необходимо указать его расположение в тонких настройках правила, в параметрах script_before_snapshot или script_after_snapshot.

Также внутри виртуальной машины может быть создан скрипт, располагающийся в файле /opt/rubackup/scripts/rustack.sh. В том случае, если

внутри виртуальной машины существует такой файл с атрибутами на исполнение, то перед созданием моментального снимка он будет выполнен с аргументом before, а сразу после создания моментального снимка он будет выполнен с аргументом after. Если в параметрах script_before_snapshot или script_after_snapshot указано расположение другого скрипта, то скрипт /opt/rubackup/scripts/rustack.sh не будет выполнен.

Примечание – Для возможности запуска скриптов внутри виртуальной машины должны быть выполнены следующие условия:

1) конфигурационный файл настроек доступа к API RUSTACK rb_module_rustack.conf (подробнее в разделе **Установка Клиента RuBackup**) кроме основной пользовательской учетной записи должен содержать учетную запись администратора;

2) для развертывания виртуальной машины, для которой предполагается создание резервных копий, используется гипервизор типа QEMU;

3) для виртуальной машины, на которой развернут клиент RuBackup и модуль rb_module_rustack, необходимо:

- установить пакет libvirt-clients;
- скопировать ssh ключ на хосты гипервизоров платформы RUSTACK.

4) на виртуальной машине, для которой предполагается создание резервных копий, необходимо установить пакет qemu-guest-agent.

В RuBackup 2.0:

– Поддерживается работа с Nova-api v2.1 и Cinder v3.0.

– Модуль поддерживает любые типы хранилищ BM (проверена работа с ocfs2, nfs, netapp-iscsi).

– Репликация не реализована.

– Восстановление в существующую внутри платформы RUSTACK виртуальную машину не реализовано.

Установка клиента RuBackup

Для возможности резервного копирования виртуальных машин среды виртуализации RUSTACK необходимо установить клиента RuBackup на одну или несколько виртуальных машин в среде виртуализации RUSTACK, находящихся под управлением операционной системы Ubuntu 18.04 или 20.04, и для которой настроен доступ к гипервизору (гипервизорам). Сюда же необходимо установить модуль rb_module_rustack из пакета rubackup-rustack.deb (см. дистрибутив для ОС Ubuntu).

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

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 RUSTACK /opt/rubackup/etc/rb_module_rustack.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
#
# Mandatory parameters
url <rustack url>
# User name on behalf of which the API requests will proceed
username <user name>
# Password to be used with 'username' to authenticate in API
password <user password>
# Domain name to be used with 'username' and 'password' to authenticate in API
domain <domain name>
# ID of a project to which target VMs belong to
project_id <PROJECT_ID>
# Timeout for curl API requests: minimum 1, maximum 300, default 5 (seconds)
timeout 20
# Timeout for creating volumes in Rustack platform, default 300 (seconds)
volume_creation_timeout 300
```

```
# Timeout for creating snapshots in Rustack platform, default 300 (seconds)
snapshot_creation_timeout 300
# Timeout for attaching and detaching volumes in Rustack platform, default 300 (seconds)
volume_attachment_timeout 300
# ID of VM in Rustack platform where current module is deployed - can be obtained using -l option of the module
rubackup-vm-id <vm id>
##
## Optional parameters:
#  Admin user account info of RUSTACK is required to run scripts inside the target VM
admin_name <admin name>
admin_password <admin password>
# Protocol for hypervisor requests: tcp or ssh, default: ssh
protocol ssh
# If certificate info is not specified the module will connect to API w/o certificate verification
enable_ssl no
ca_info <path to cert>
# Turn on debug of REST requests
#curl_verbose
```

Измените в этом файле настройки для подключения к API.

Обязательные параметры конфигурационного файла:

– url <rustack url> — адрес (IP или FQDN), используемый для API запросов в платформу виртуализации RUSTACK.

– username <user name> — имя пользователя, от имени которого будут выполняться запросы API.

– password <user password> — пароль, который будет использоваться вместе с именем пользователя для аутентификации в API.

– domain <domain name> — доменное имя, которое будет использоваться с именем пользователя и паролем для аутентификации в API.

– project_id <PROJECT_ID> — идентификатор проекта внутри платформы виртуализации RUSTACK, к которому относятся виртуальные машины, для которых предполагается возможность создания резервных копий.

– timeout — время ожидания для запросов curl API. По умолчанию составляет 5 секунд. Может принимать значения от 1 до 300 секунд.

– volume_creation_timeout — время ожидания для создания томов на платформе Rustack. По умолчанию составляет 300 секунд. Если с момента обработки платформой виртуализации запроса на создание тома, этот том не перешел в состояние «available» в течение заданного времени, соответствующая задача на создание резервной копии или восстановление завершится с ошибкой;.

– snapshot_creation_timeout — время ожидания для создания снимков на платформе Rustack. По умолчанию составляет 300 секунд. Если с момента обработки платформой виртуализации запроса на создание снимка, этот снимок не перешел в состояние «available» в течение заданного времени, соответствующая задача на создание резервной копии завершится с ошибкой;

– volume_attachment_timeout — время ожидания для подключения к виртуальной машине и отключения томов (том не перешел в статус «in_use») на платформе Rustack. По умолчанию составляет 300 секунд. Если обозначенный таймаут истек, а том не был присоединен к виртуальной машине или отсоединен от виртуальной машины (том не перешел в статус «available»), отображается ошибка.

– rubackup-vm-id <vm id> — идентификатор виртуальной машины (внутри платформы виртуализации RUSTACK), на которой развернут данный модуль и клиент RuBackup.

Примечание: список виртуальных машин внутри проекта (project_id), включая их имя, идентификатор и текущий статус, можно получить, запустив исполняемый файл модуля с опцией -l:

/opt/rubackup/modules/rb_module_rustack -l

При этом, перед листингом витуальных машин в конфигурационном файле модуля как минимум должны быть заданы значения для параметров: url, username, password, domain, project_id, timeout.

Необязательные параметры:

– admin_name <admin name> — имя пользователя, имеющего права администратора внутри платформы виртуализации RUSTACK для запуска скриптов внутри целевой виртуальной машины.

– admin_password <admin password> — пароль пользователя, имеющего права администратора внутри платформы виртуализации RUSTACK. Используется вместе с именем администратора для аутентификации в API.

Примечание: задавать значения для параметров admin_name и admin_password необходимо только в случаях, когда при создании резервных копий требуется функционал запуска скриптов до и после создания снэпшотов дисков целевой виртуальной машины.

– protocol — протокол для запросов к гипервизору: tcp или ssh. По умолчанию используется ssh.

– enable_ssl — параметр, указывающий, следует ли использовать SSL-сертификат. Доступные значения: yes и no. Если указано значение yes, то необходимо раскомментировать параметр ca_info и указать полный путь до SSL-сертификата, если указано значение no, то в таком случае запросы к API платформы виртуализации RUSTACK будут выполняться без проверки сертификата. Если информация о сертификате не указана, модуль подключится к API без проверки.

– ca_info — путь к SSL-сертификату, который будет использоваться при подключении к API, если включена проверка сертификата.

Примечание: для целей отладки подключения к API в конфигурационный файл модуля можно добавить следующую строку:

```
curl_verbose
```

#curl_verbose — включает режим отладки REST-запросов.

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

```
Try to check module: 'RUSTACK' ...
Execute OS command: /opt/rubackup/modules/rb_module_rustack -t 2>&1
Module version: 1.10
Nova-api version: v2.1
Cinder version: v3.0
... module 'RUSTACK' was checked successfully
```

В ручном режиме проверить правильность настроек можно при помощи следующей команды:

```
# /opt/rubackup/modules/rb_module_rustack -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
```

Подготовка виртуальной машины RUSTACK для выполнения резервного копирования средствами RuBackup

Linux

В операционной системе Linux виртуальной машины необходимо установить пакет *qemu-guest-agent*.

```
# apt-get install qemu-guest-agent
```

или

```
# yum install qemu-guest-agent
```

Windows

Для операционной системы Windows с диска *virtio-win* необходимо установить пакет *qemu-ga* из папки *guest-agent*, которая находится в корне диска.

В операционной системе виртуальной машины необходимо установить гостевые расширения из диска Virtio-Win. Для этого:

1) Добавьте ISO-образ с гостевыми расширениями в операционную систему виртуальной машины как виртуальный CD-ROM.
2) В виртуальной машине откройте подключенный виртуальный CD-ROM.
3) Запустите файл virtio-win-gt-x64.
4) Используя мастер установки, установите QEMU Guest Agent и SPICE agent.
5) Перезагрузите виртуальную машину.

Диск Virtio-Win доступен для скачивания по ссылке:

https://fedorapeople.org/groups/virt/virtio-win/direct-

downloads/latest-virtio/virtio-win.iso

Astra Linux Смоленск

Для Astra Linux Смоленск необходимо использовать диск разработки и добавить соответствующий iso image в операционную систему как виртуальный CDROM. После этого:

```
# sudo apt-cdrom add

# sudo apt update

# sudo apt install qemu-guest-agent
```

Защитное преобразование резервных копий

При необходимости, сразу после выполнения резервного копирования архивы 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	

Менеджер Администратора RuBackup (RBM)

Оконное приложение Менеджер Администратора RuBackup (RBM) предназначено для администрирования серверной группировки RuBackup, включая управление клиентами, глобальным расписанием, хранилищами резервных копий и другими параметрами RuBackup.

В RuBackup RBM располагается в отдельном пакете и может быть установлен как на сервер резервного копирования, так и на удаленном АРМ администратора.

Для запуска RBM следует выполнить команду:

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

RuBackup предоставляет ролевую модель доступа к системе резервного копирования. 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).

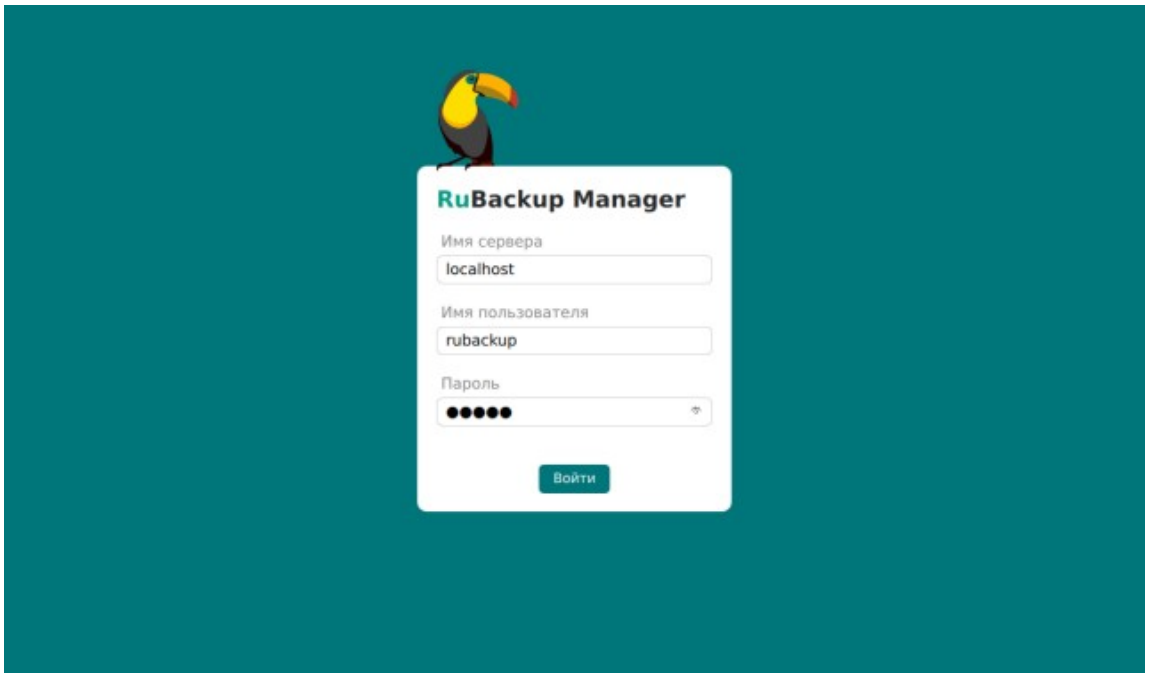

Рисунок 1

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.

После нажатия кнопки «Войти» откроется окно «RuBackup manager» (рисунок 2):

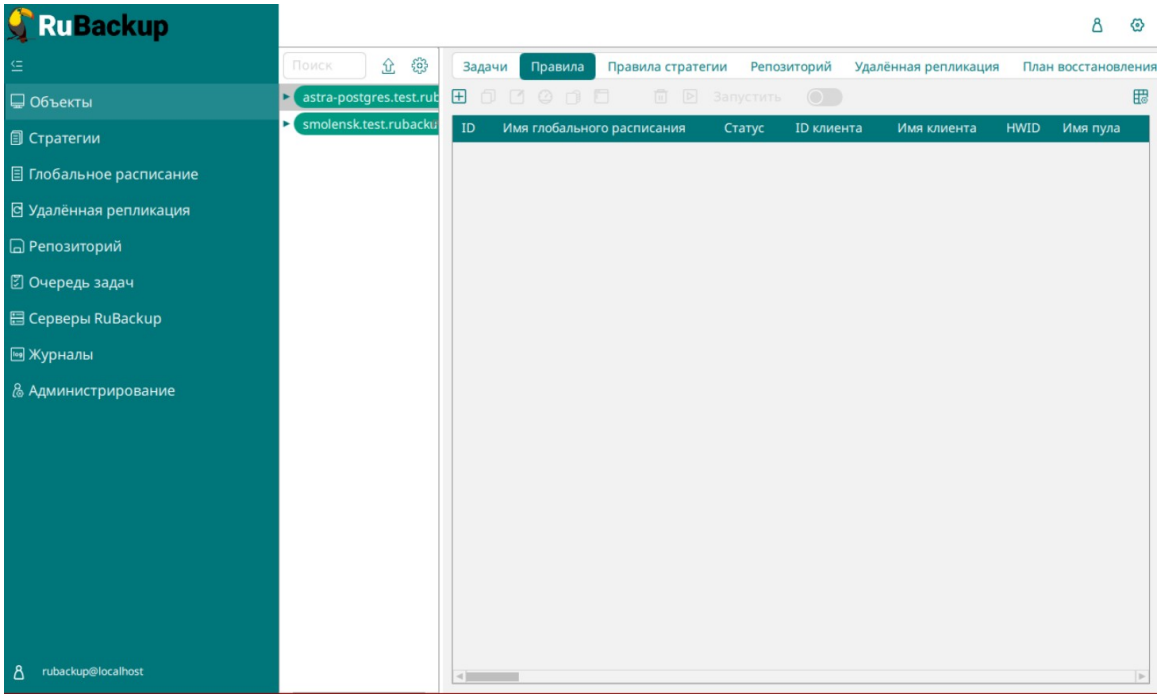

Рисунок 2

Для определения статуса клиента необходимо перейти на вкладку **Администрирование → Клиенты (**рисунок 3):

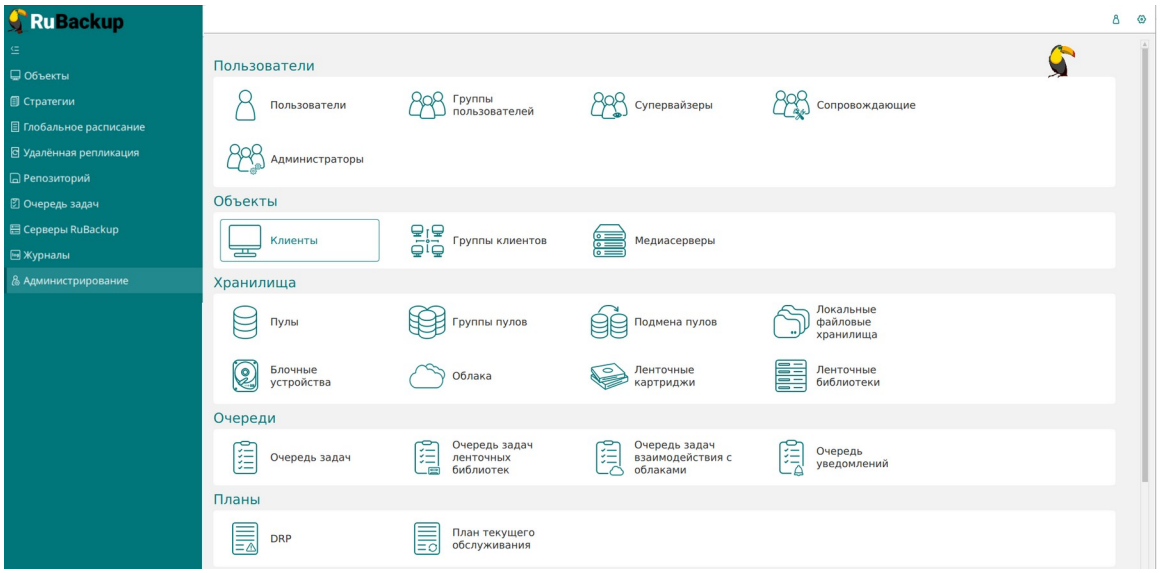

Рисунок 3

При этом откроется окно (рисунок 4).

Если клиент RuBackup установлен, но не авторизован, в верхней части окна RBM кнопка **Неавторизованные клиенты** будет активна.

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

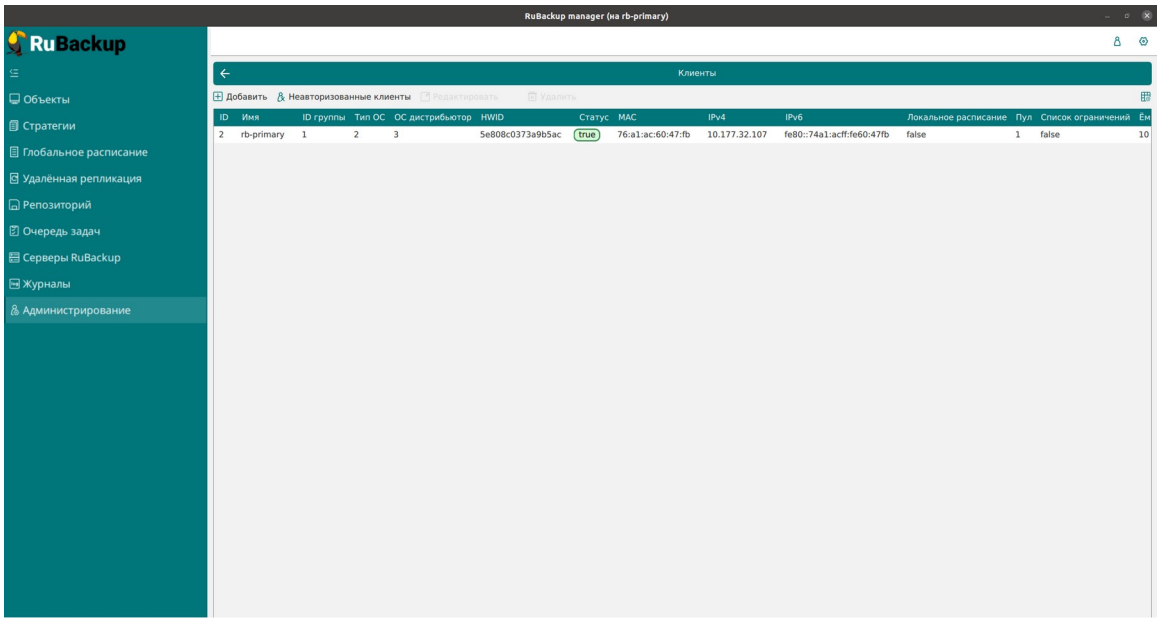

Рисунок 4

Для авторизации неавторизованного клиента в RBM выполните следующие действия:

1. Нажмите кнопку **Неавторизованные клиенты**. При этом откроется окно (рисунок 5):

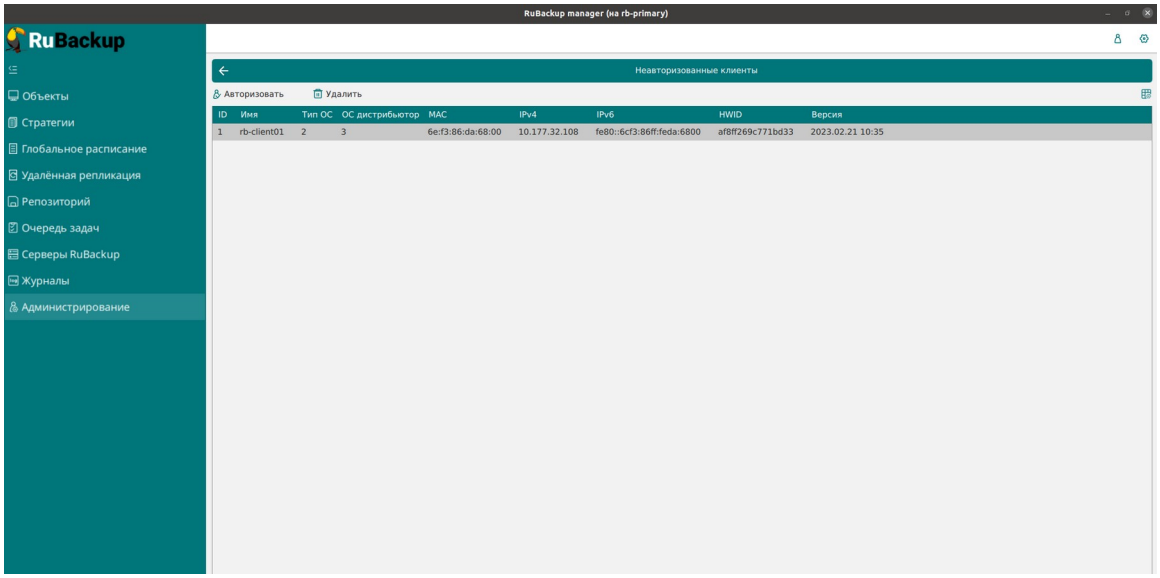

Рисунок 5

2. Выберите нужного неавторизованного клиента и нажмите **Авторизовать** (рисунок 6):

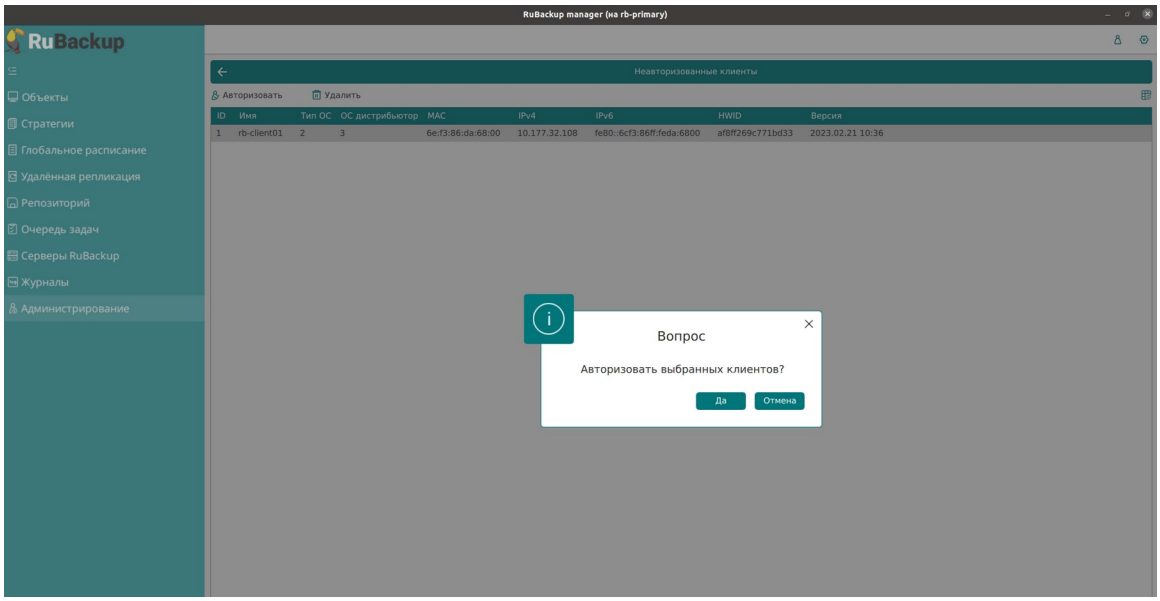

Рисунок 6

После авторизации новый клиент будет виден в главном окне RBM (рисунок 7):

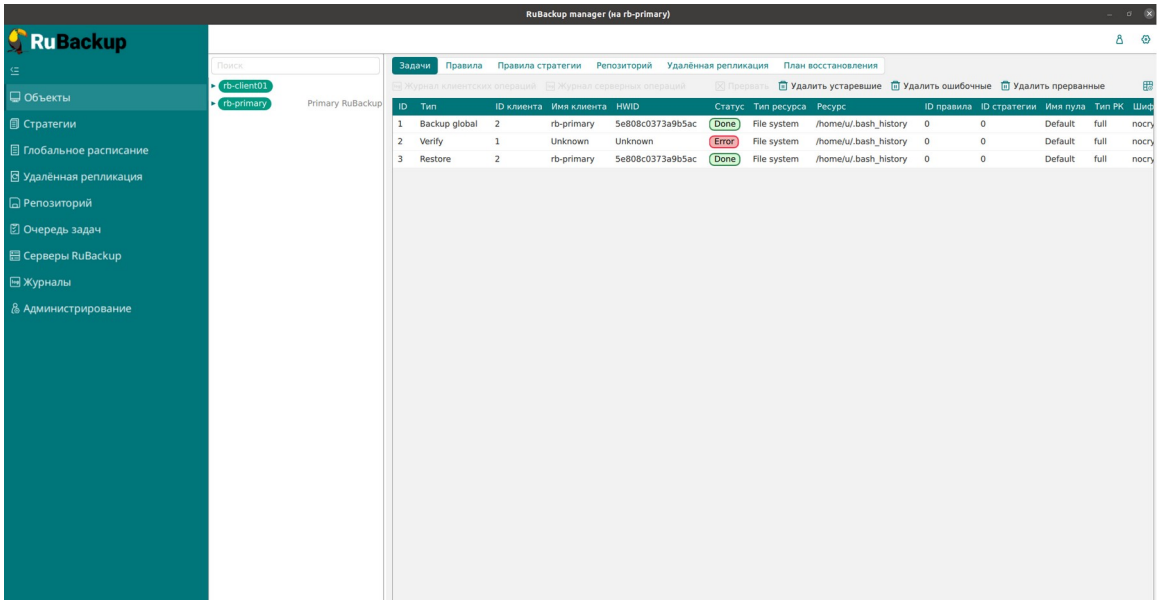

Рисунок 7

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 8):

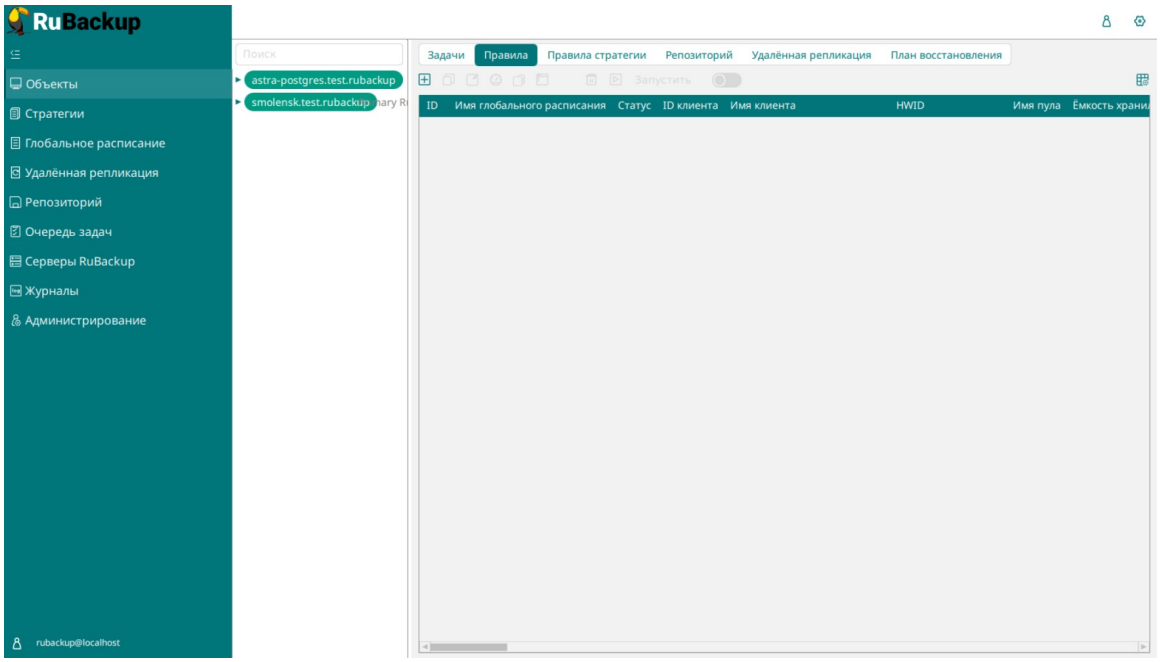

Рисунок 8

2. Выберите клиента и добавьте правило резервного копирования (рисунок 9):

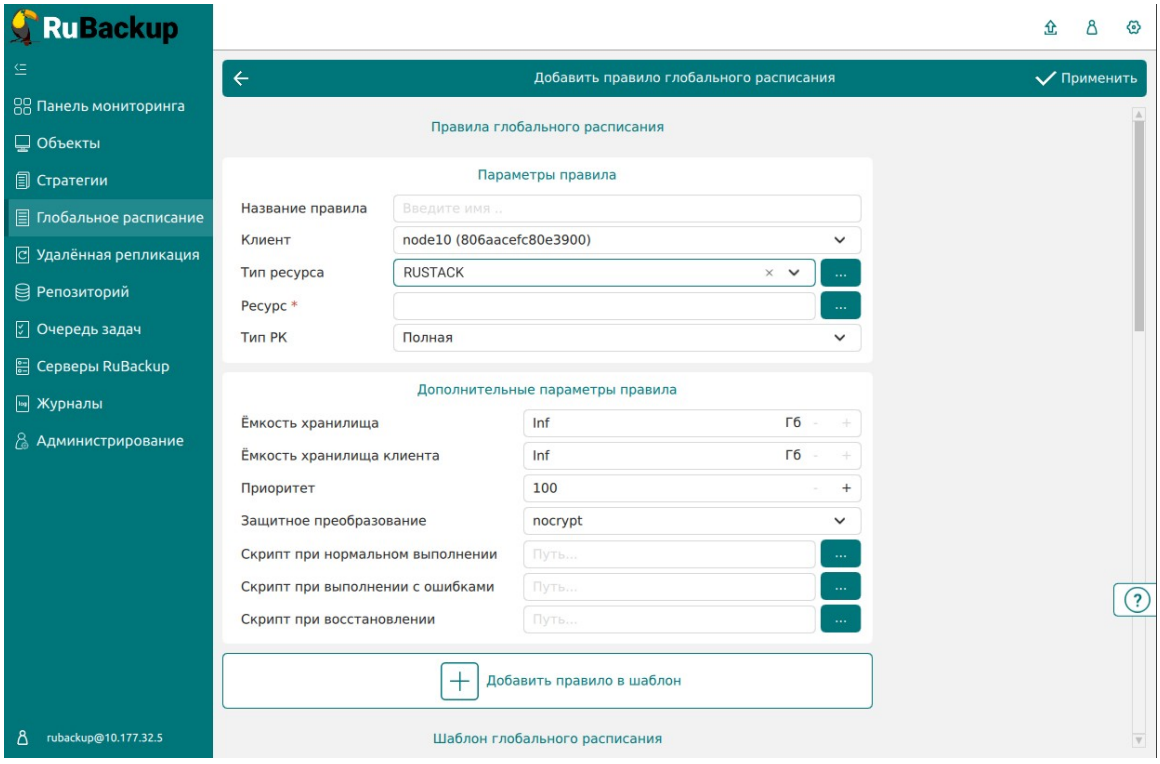

Рисунок 9

3. Выберите тип ресурса: **RUSTACK** (рисунок 10):

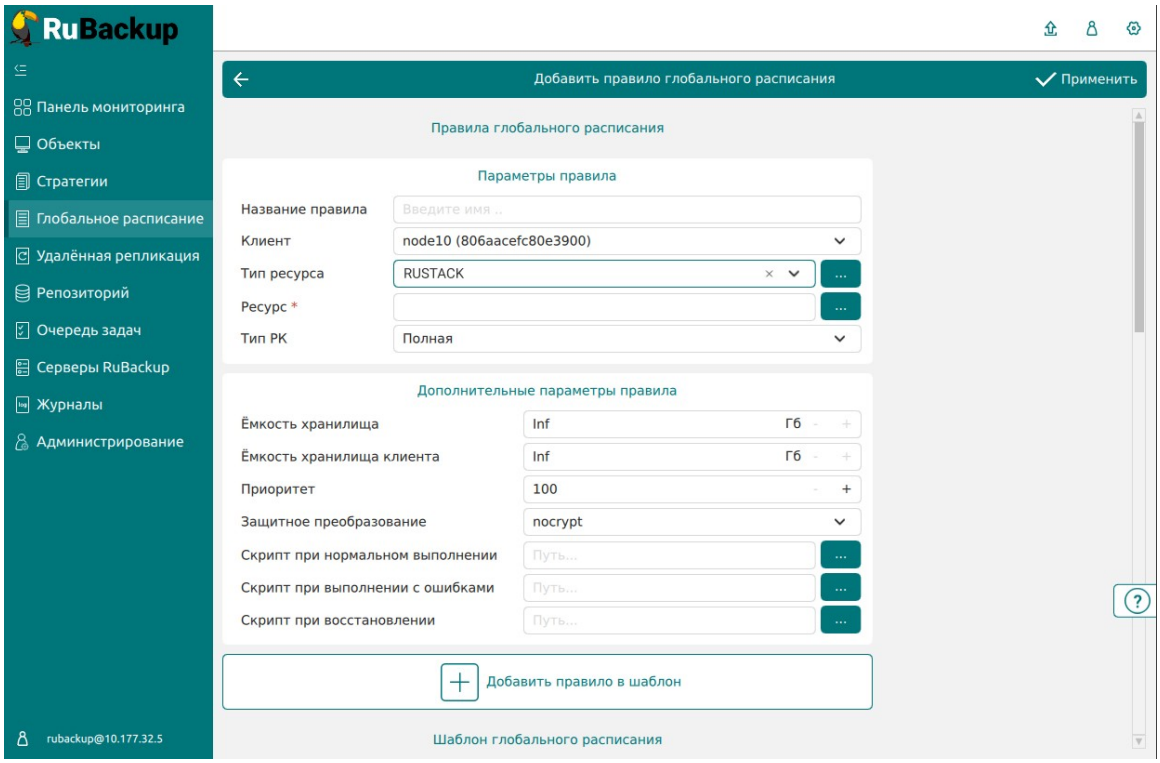

Рисунок 10

4. Выберите ресурс, нажав кнопку **Выбрать** (рисунок 11):

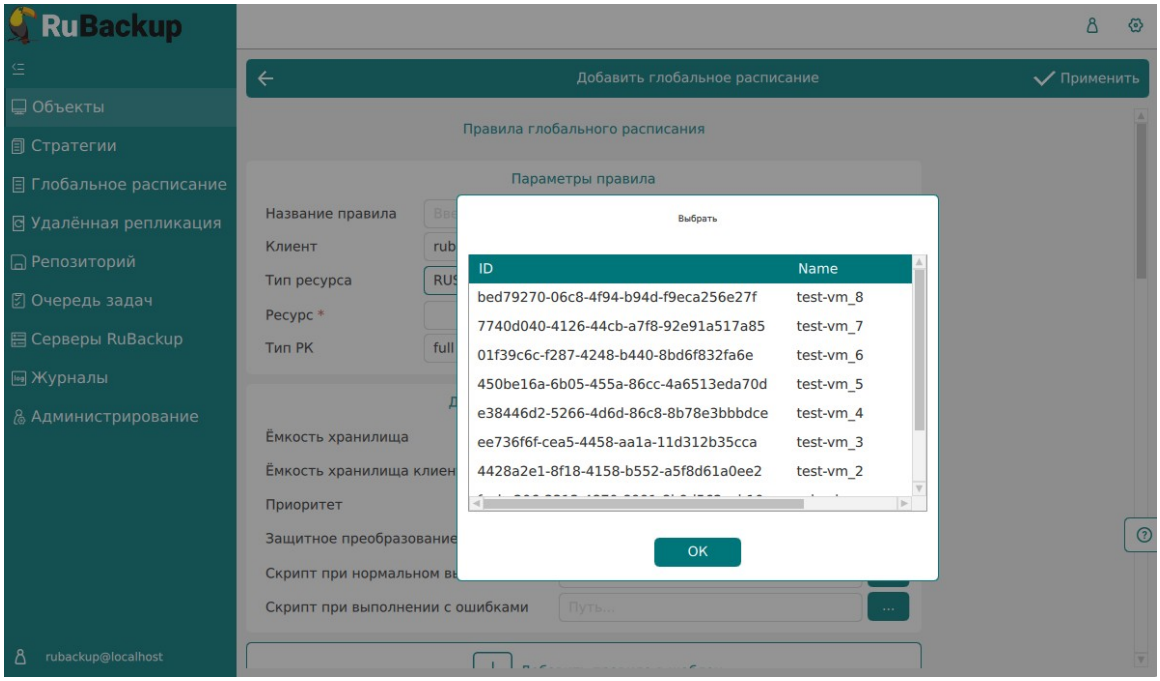

Рисунок 11

5. Установите настройки правила: название правила, пул хранения данных, максимальный объём для резервных копий правила (в ГБ), тип резервного

копирования, расписание резервного копирования, срок хранения и необязательный временной промежуток проверки резервной копии (рисунок 12).

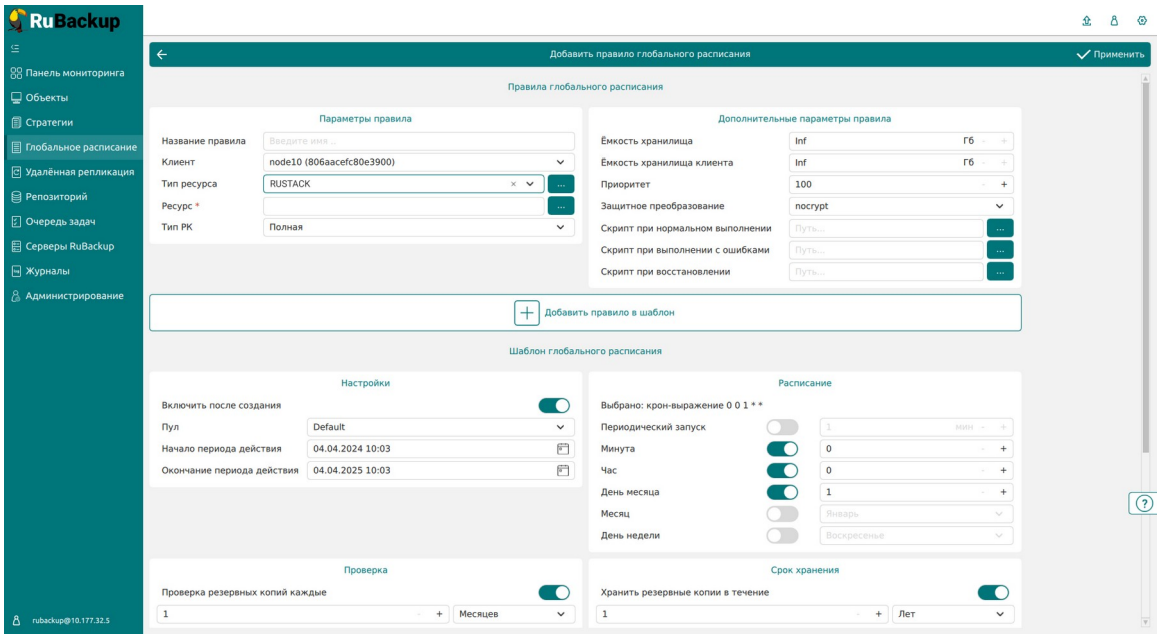

Рисунок 12

При помощи кнопки «...» рядом с типом ресурса можно выполнить тонкие настройки правила резервного копирования, например определить скрипт, который будет выполнен внутри виртуальной машины перед созданием моментального снимка и сразу после его создания (рисунок 13). Это может быть необходимо для приведения данных приложения в консистентное состояние, синхронизации кэша и т.п.

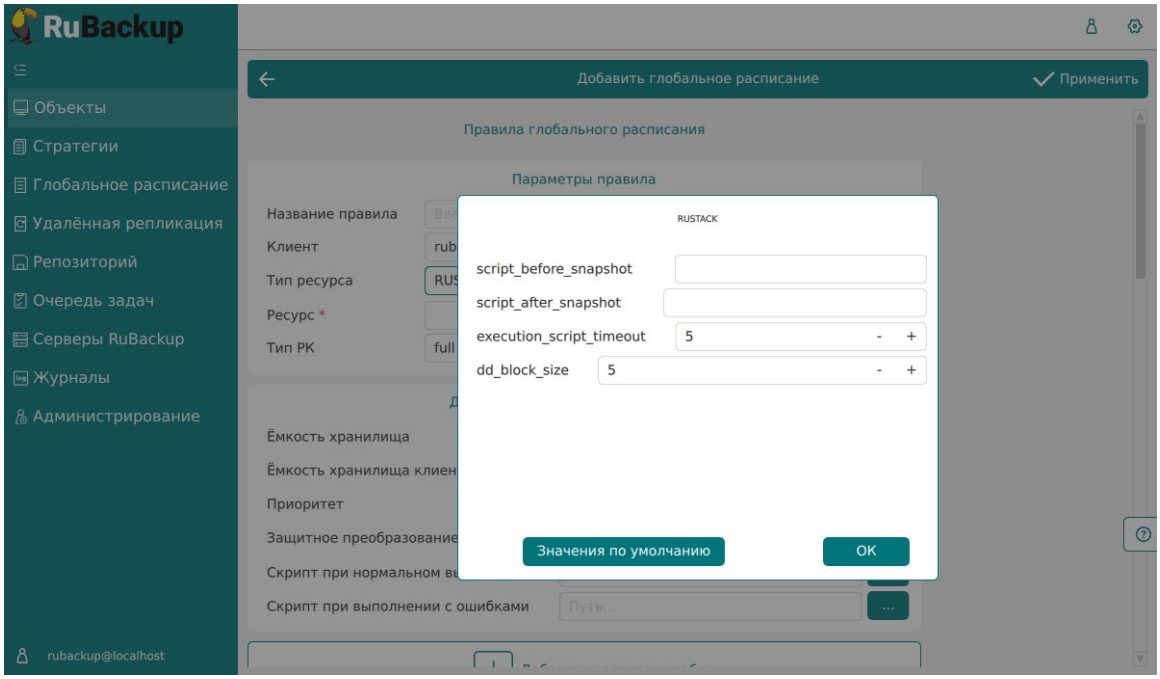

Рисунок 13

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

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

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

Правила глобального расписания имеют срок жизни, определяемый при их создании, а также предоставляют следующие возможности:

– выполнить защитное преобразование резервной копии на клиенте;

– периодически выполнять проверку целостности резервной копии;

– хранить резервные копии определённый срок, по окончании которого удалять их из хранилища резервных копий и из записей репозитория, либо уведомлять клиента об окончании срока хранения;

– через определённый срок после создания резервной копии автоматически переместить её в другой пул хранения резервных копий, например, на картридж ленточной библиотеки;

– уведомлять пользователей системы резервного копирования о результатах выполнения тех или иных операций, связанных с правилом глобального расписания.

При создании задачи RuBackup она появляется в главной очереди задач. Отслеживать выполнение правил может как администратор (при помощи 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 помещена в хранилище резервных копий, а информация о ней будет размещена в репозитории RuBackup.

Срочное резервное копирование при помощи RBM

В том случае, если необходимо выполнить срочное резервное копирование созданного правила глобального расписания, то это можно сделать, вызвав правой кнопкой мыши контекстное меню «Выполнить» (рисунок 14):

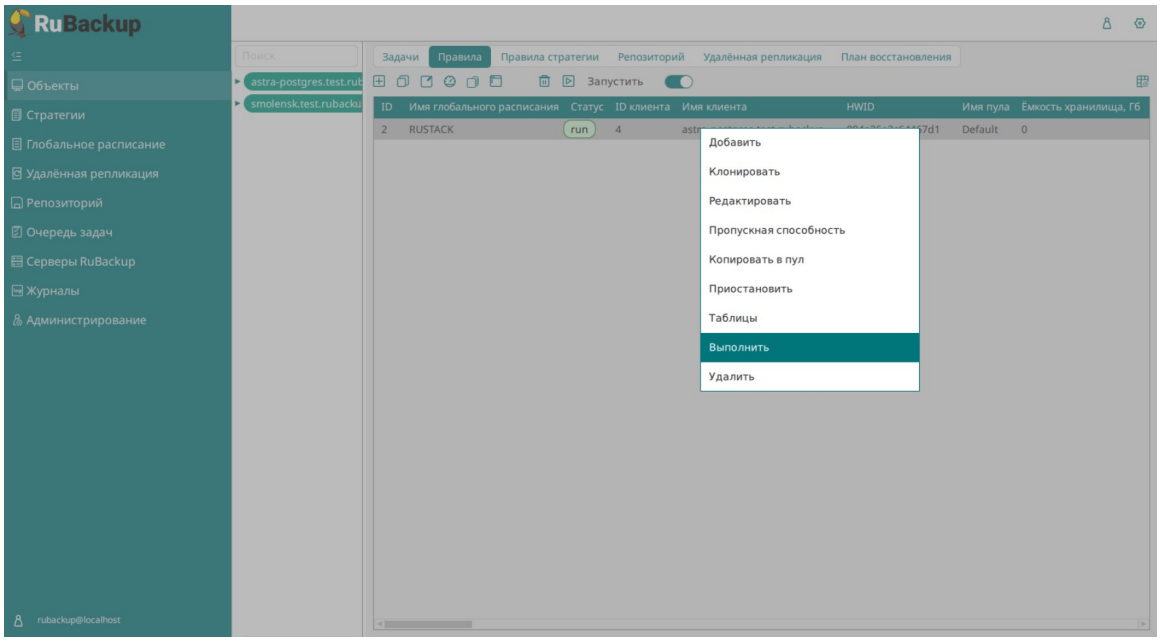

Рисунок 14

Проверить ход выполнения резервного копирования можно в окне «Очередь задач» (рисунок 15):

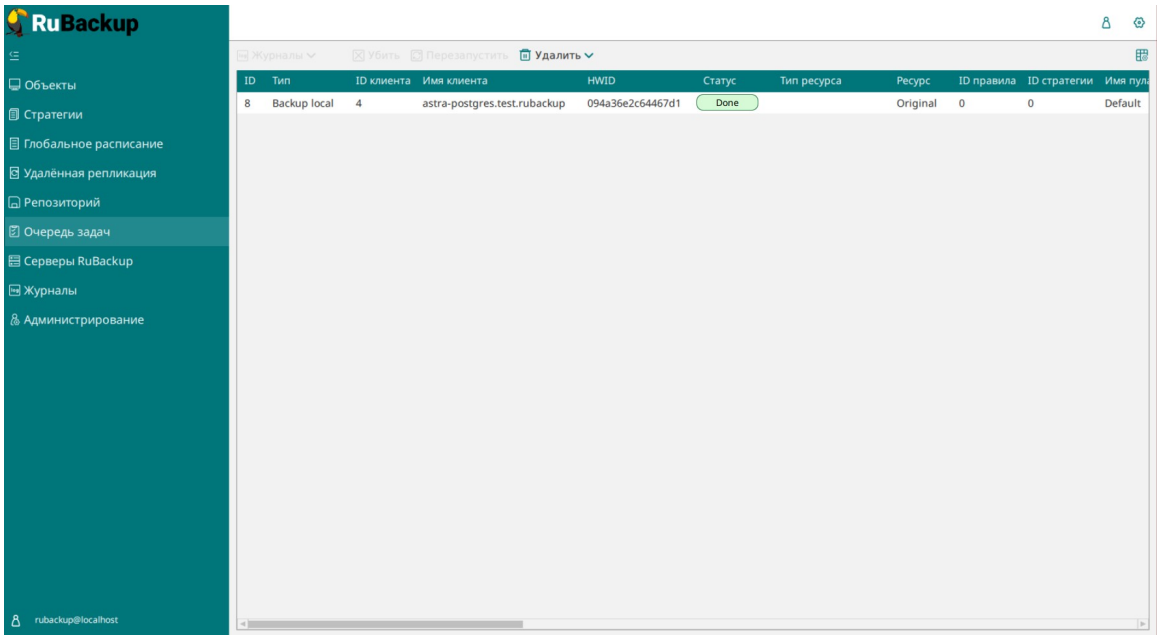

Рисунок 15

При успешном завершении резервного копирования соответствующая задача перейдет в статус «**Done**».

Централизованное восстановление резервных копий с помощью RBM

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, перейдя на вкладку **Репозиторий** (рисунок 16), и нажав кнопку **Восстановить**.

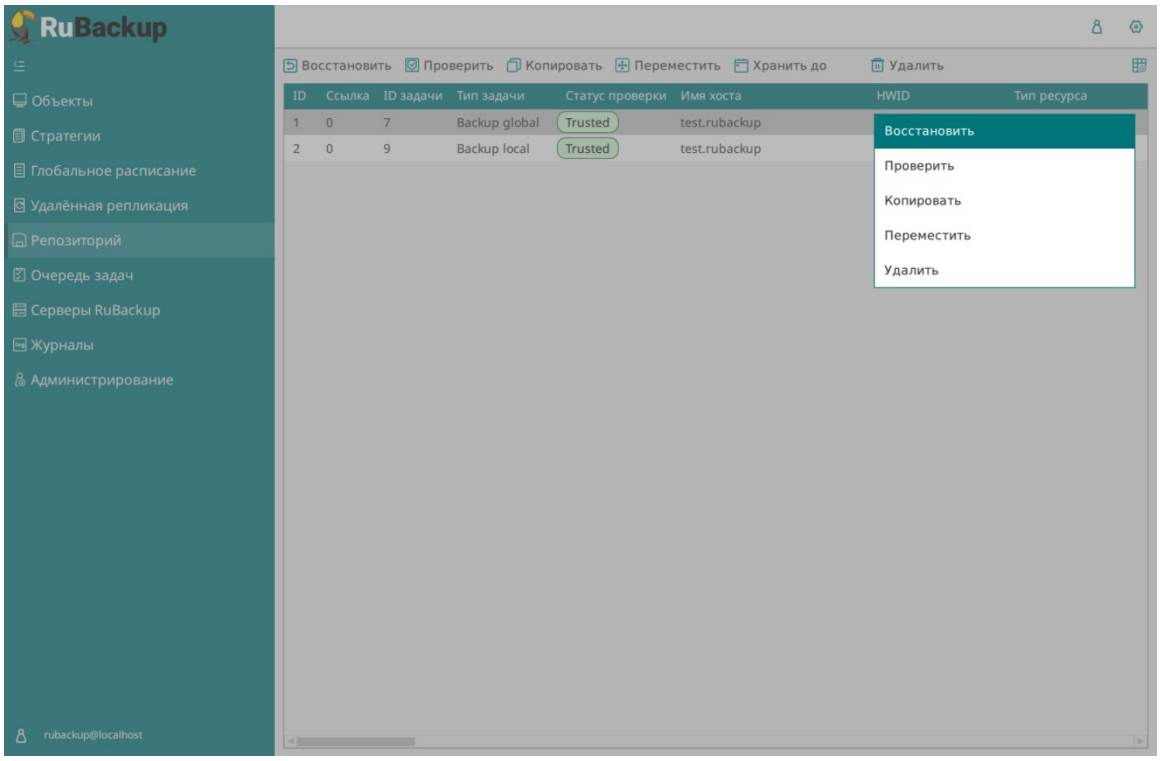

Рисунок 16

При этом откроется окно (рисунок 17):

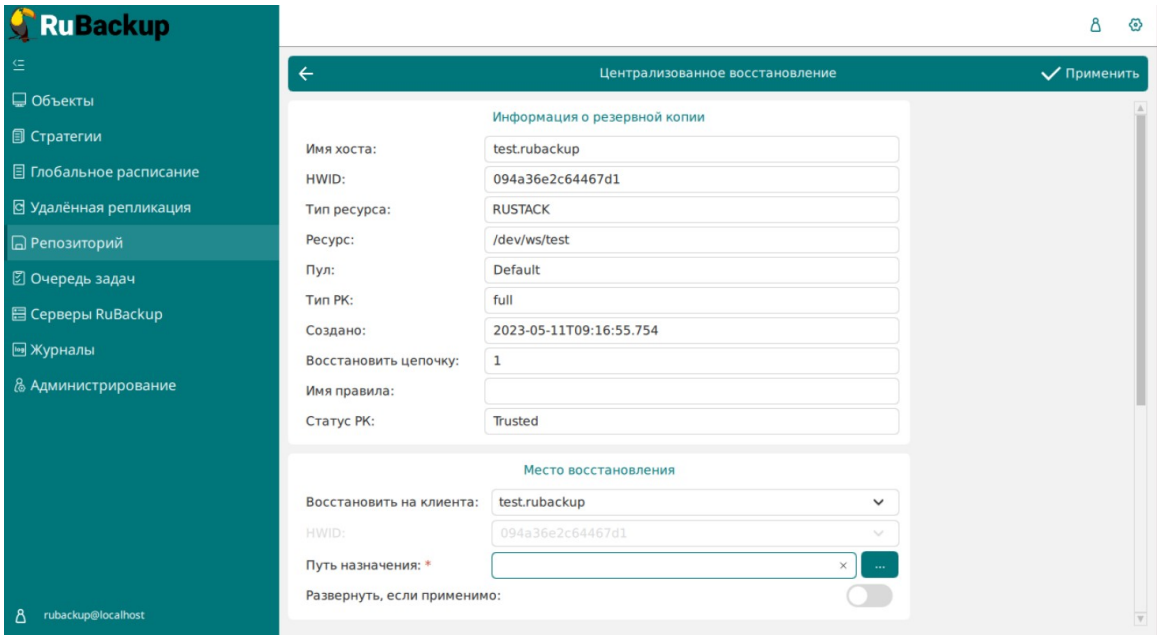

Рисунок 17

В окне централизованного восстановления можно увидеть основные параметры резервной копии и определить директорию распаковки резервной копии. В случае восстановления виртуальной машины из резервной копии будет выполнена проверка наличия в среде виртуализации виртуальной машины с таким же именем. Если такой виртуальной машины нет, то будет произведено восстановление с оригинальным именем. Если виртуальная машина с таким именем уже есть, то к имени виртуальной машины будет добавлен цифровой постфикс (рисунок 18).

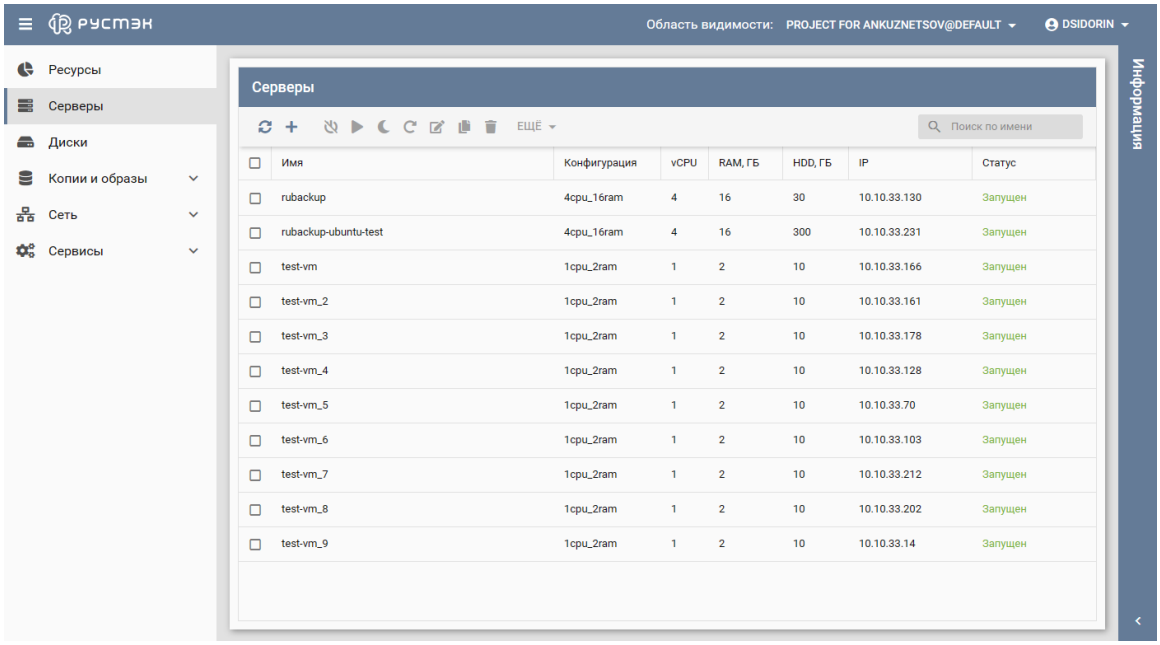

Рисунок 18

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».

Проверить ход выполнения восстановления резервной копии можно в окне **Очередь задач** (рисунок 19).

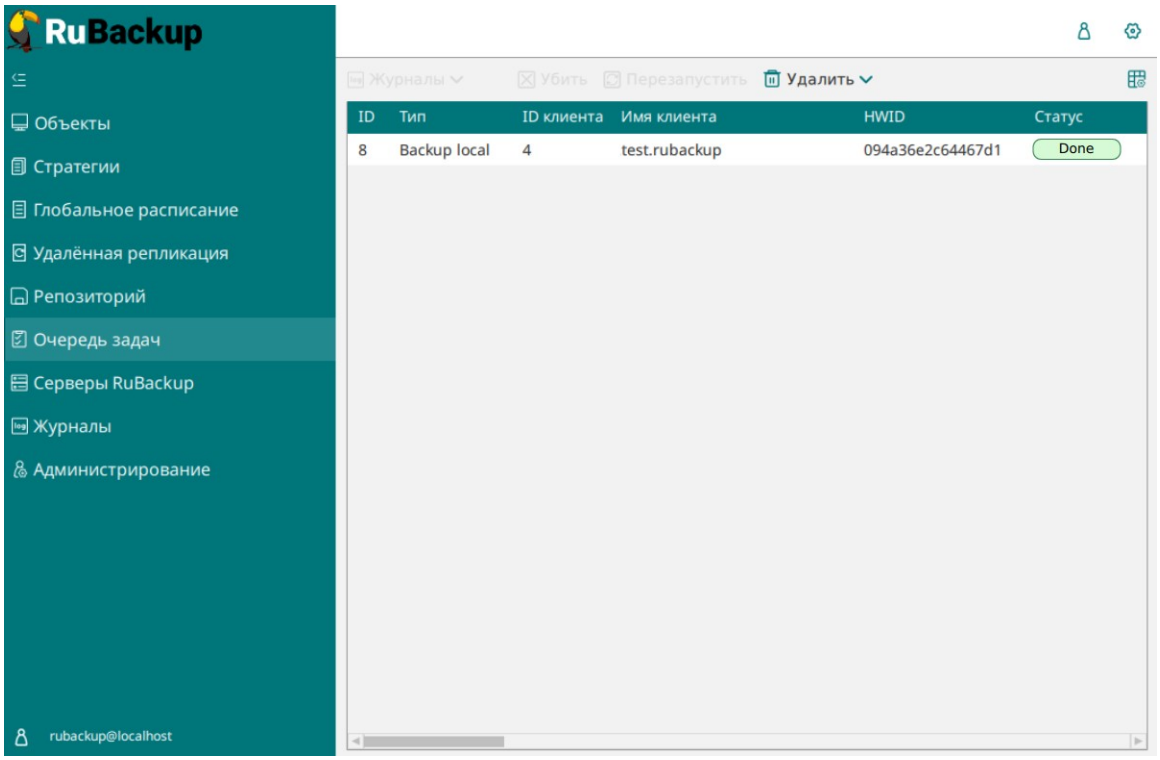

Рисунок 19

При успешном завершении восстановления резервной копии или цепочки резервных копий, соответствующие задачи на восстановление перейдут в статус «**Done**».

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@rubackup-ubuntu:~# rb_archives
Id | Ref ID | Resource                             | Resource type | Backup type | Created               | Crypto  | Signed | Status
---+--------+--------------------------------------+---------------+-------------+-----------------------+---------+--------+-------------
1  |        | eed657c2-e578-4e18-802f-f9ce2cd192c9 | RUSTACK       | full        | 2022-08-23 16:57:08+03 | nocrypt | True   | Not Verified
2  | 1      | eed657c2-e578-4e18-802f-f9ce2cd192c9 | RUSTACK       | incremental | 2022-08-23 17:49:47+03 | nocrypt | True   | Not Verified
```

Запрос на восстановление резервной копии:

```
root@rubackup-ubuntu:~# rb_archives -X 2
Password:
The archive will be restored in the directory: /rubackup-tmp
----> Restore archive chain: 1 2  < ----
Record ID: 1 has status: Not Verified
Continue (y/n)? yes
Record ID: 2 has status: Not Verified
Continue (y/n)? yes
TASK WAS ADDED TO QUEUE:4 5
```

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.