RuBackup
Система резервного копирования и восстановления данных

Резервное копирование

и восстановление Aerodisk VAIR

Версия 2.1

04.04.2024 г.

Содержание

Введение

Система резервного копирования RuBackup позволяет выполнять резервное копирование и восстановление виртуальных машин среды виртуализации Aerodisk VAIR. 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 Aerodisk VAIR выполняется безагентным способом. Это означает, что в саму виртуальную машину 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 (см. примечание); 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 Aerodisk VAIR 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;
- на прокси-хост, который имеет доступ к хранилищу и к гипервизорам среды виртуализации.

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.

Также внутри виртуальной машины может быть создан скрипт, располагающийся в файле /opt/rubackup/scripts/aerodisk-vm.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.

Примечания:

1. Диски виртуальной машины с установленным атрибутом «только чтение» («readonly»: «true») не будут добавлены в резервную копию.

2. К виртуальной машине могут быть подключены диски различных типов пулов данных, доступных в среде виртуализации Aerodisk VAIR (ARDFS, ACFS, NFS share).

3. Если в виртуальной машине есть диски, относящиеся к пулу данных типа ACFS или NFS share, перед созданием резервной копии RuBackup проверяет, примонтирован ли пул к хосту, на котором работает клиент. Если пул не примонтирован, резервная копия не будет создана.

В RuBackup 1.9:

– Поддерживается работа с Aerodisk VAIR 3.6.0.

– Поддерживается работа с хранилищем данных типа RDFS.

– Репликация не реализована.

– Восстановление в имеющуюся ВМ не реализовано.

В RuBackup 2.0:

– Поддерживается работа с Aerodisk VAIR 3.7.0, 3.7.1 и 3.8.0.

– Поддерживается работа с хранилищем данных типа RDFS, NFS и ACFS.

– Репликация не реализована.

– Восстановление в имеющуюся ВМ не реализовано.

Установка клиента RuBackup

Для возможности резервного копирования виртуальных машин среды виртуализации Aerodisk VAIR необходимо установить клиента RuBackup на выбранный гипервизор (гипервизоры) или прокси-хост, сюда же необходимо установить модуль rb_module_aerodisk_vm из пакета rubackup-aerodisk.deb (См. дистрибутив для ОС Debian 10).

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 Aerodisk VAIR /opt/rubackup/etc/rb_module_aerodisk-vm.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 for API requests to Aerodisk VAIR
url http://<API_URrequestsL>/
#
# Username that will be used for API
username <User_Name_For_API_Requests>
#
password <User_Password_For_API_Requests>
# Timout in seconds to wait for response for API requests
timeout 10
# Local administrator username, on behalf of which RuBackup client and current module will work
# Default value: root
local_backup_admin root
# Default mount point for ARDFS pools, fore example: /vair/ARDFS
ardfs_mount_point <path>
#
```

```
# Optional parameter to enable debug traces for API requests
# Possible values: yes, no
# Default value: no
curl_verbose no
#
# Optional parameter to ignore destination directory passed to the module via option '-d'.
# Destination directory is usually set at restore in 'RBM' or 'rb_archives'.
# Possible values: yes, no
# Default value: no
# For value 'yes' backup is unpacked to a directory path wich is defined by an option
# 'use-local-backup-directory' in  file /opt/rubackup/etc/config.file on the RuBackup client host.
ignore_destination_directory no
#
# Optional parameters required to restore
#   disks in a certain pool:
# pool_type <rdfs|nfs|acfs>
# pool_name <pool name|address>
#
# Example 1:
# pool_type rdfs
# pool_name POOLEC
#
# Example 2:
# pool_type nfs
# pool_name 192.168.9.150:/R00/NFS01
#
# Example 3:
# pool_type acfs
# pool_name ACFS01
```

Измените в этом файле настройки для подключения к API.

curl_verbose – необязательный параметр, регулирующий включение/выключение отладки взаимодействия с API Aerodisk VAIR. Возможные значения: yes, no. Значение по умолчанию: no.

ignore_destination_directory – параметр, влияющий на выбор директории распаковки резервной копии при восстановлении. Возможные значения:

- ignore_destination_directory yes – при восстановлении резервной копии архив будет распакован в директорию для временных операций клиента (параметр 'use-local-backup-directory' из config.file клиента).

- ignore_destination_directory no – при восстановлении резервной копии архив будет распакован в директорию, путь к которой модуль получает через опцию '-d' – т. е. путь, который выбран при восстановлении в RBM (в окне централизованного восстановления) или который задан при восстановлении РК с помощью утилиты rb_archives.

Значение по умолчанию: no.

Примечание – если в файле rb_module_aerodisk-vm.conf заданы тип и имя пула (параметры pool_type и pool_name соответственно), при восстановлении дисков виртуальной машины из резервной копии они будут созданы в соответствующем пуле. В противном случае создание дисков выполняется в пулах, которым изначально принадлежали диски виртуальной машины вовремя создания резервной копии. Доступные значения для параметра pool_type:

- «RDFS», «rdfs» или «network» – для обозначения пула типа RDFS;
- «NFS», «nfs» или «file» – для обозначения пула типа NFS share;
- «ACFS», «acfs» или «file» – для обозначения пула типа ACFS.

Перед созданием диска RuBackup проверяет:

- существование пула данных с требуемым именем внутри среды виртуализации Aerodisk VAIR;
- наличие свободного места в пуле данных, необходимое для создания в нем диска требуемого размера.

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

```
Fri Oct 13 14:25:53 2023: Check additional RuBackup modules:
Fri Oct 13 14:25:53 2023: Try to check module: 'Aerodisk VAIR' ...
Fri Oct 13 14:25:53 2023: Execute OS command: /opt/rubackup/modules/rb_module_aerodisk_vm -t 2>&1
Fri Oct 13 14:25:53 2023: 2.0.U1.3
Fri Oct 13 14:25:53 2023: ... module 'Aerodisk VAIR' was checked successfully. Module supports archiving
```

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

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

Мастер-ключ

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

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

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

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

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

Защитное преобразование резервных копий

При необходимости, сразу после выполнения резервного копирования 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).

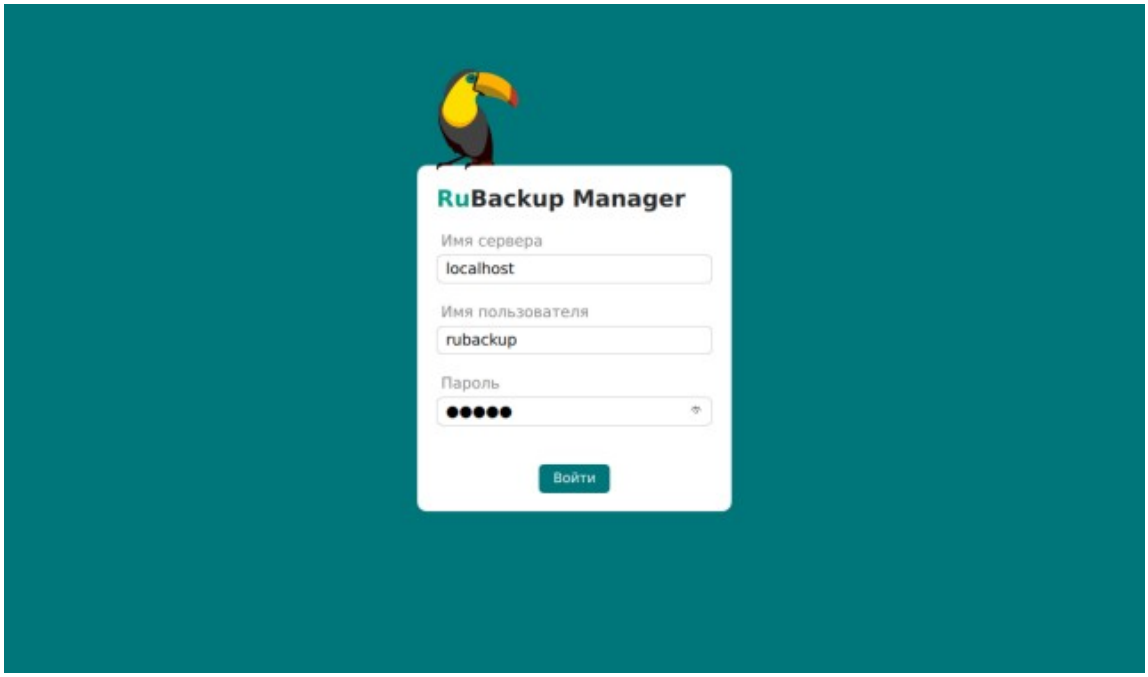

Рисунок 1

На вкладке **Объекты** представлен список клиентов системы резервного копирования. Клиенты отображаются по имени узла, на котором они запущены. Если навести указатель мыши на имя какого-либо из клиентов, будет отображен его HWID. Если развернуть запись для какого-либо из клиентов, в выпадающем списке будут отображены типы ресурсов, для которых данный клиент может создавать резервные копии (рисунок 2). Клиенты, которые в данный момент находятся в состоянии online, будут отмечены зеленым цветом. Клиенты в состоянии offline – красным (рисунок 2).

Для резервного копирования клиент должен быть авторизован администратором RuBackup (рисунок 2).

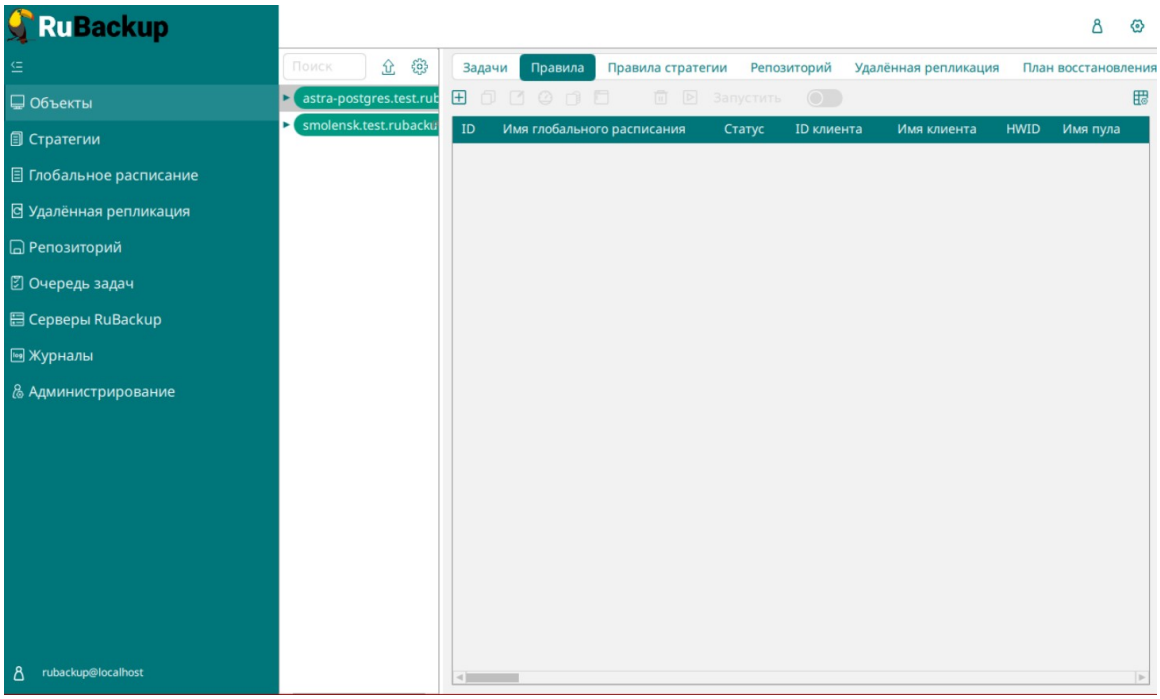

Рисунок 2

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 3):

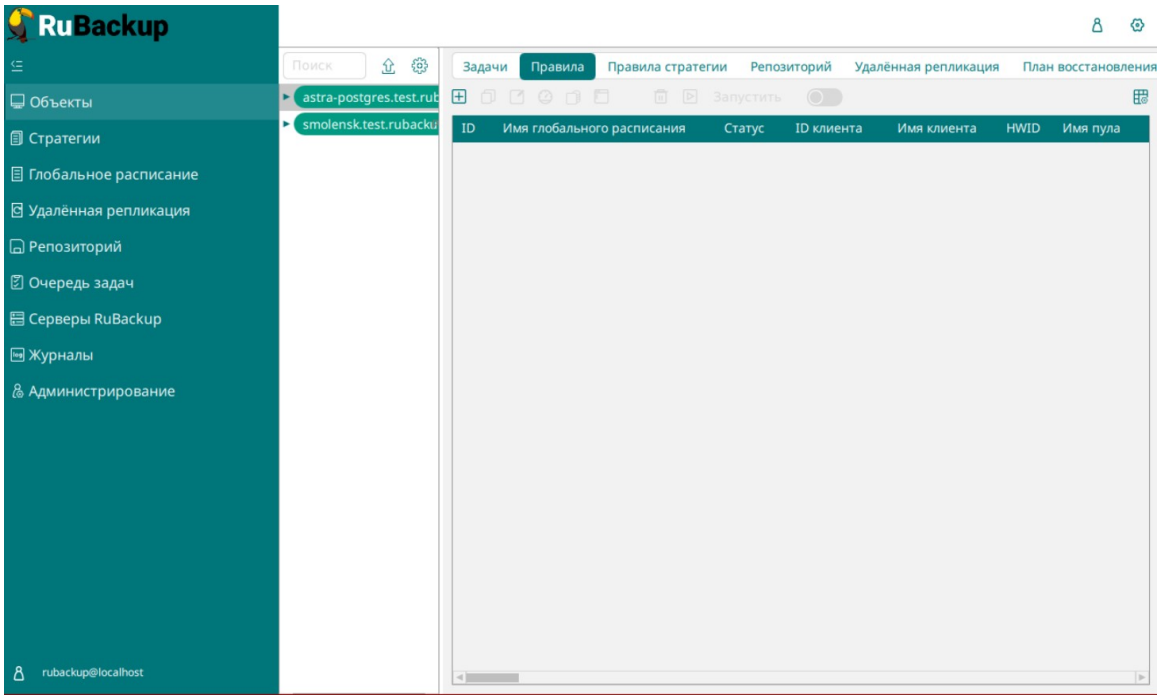

Рисунок 3

Для определения статуса клиента необходимо перейти на вкладку **Администрирование → Клиенты** (рисунок 4):

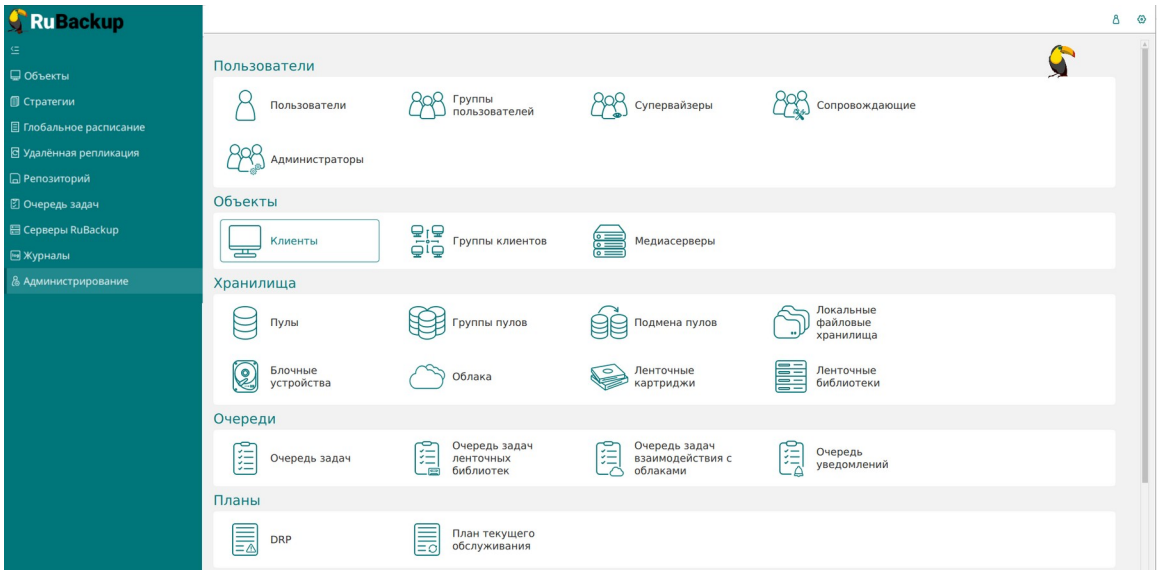

Рисунок 4

При этом откроется окно (рисунок 5).

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.

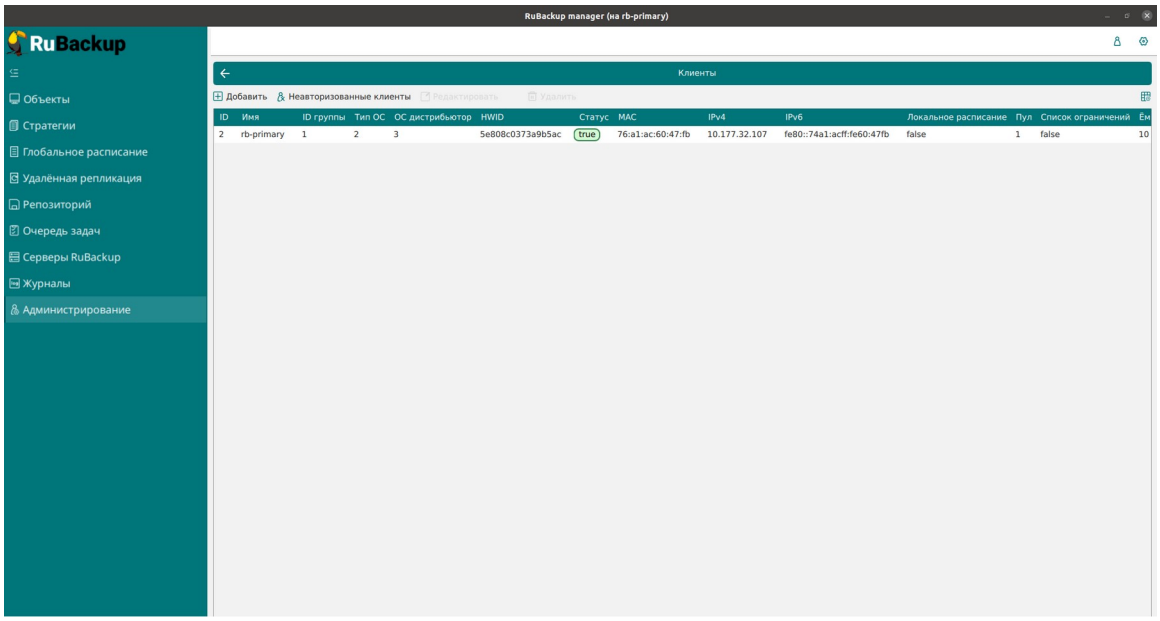

Рисунок 5

Для авторизации неавторизованного клиента в RBM выполните следующие действия:

1. Нажмите кнопку **Неавторизованные клиенты**. При этом откроется окно (рисунок 6):

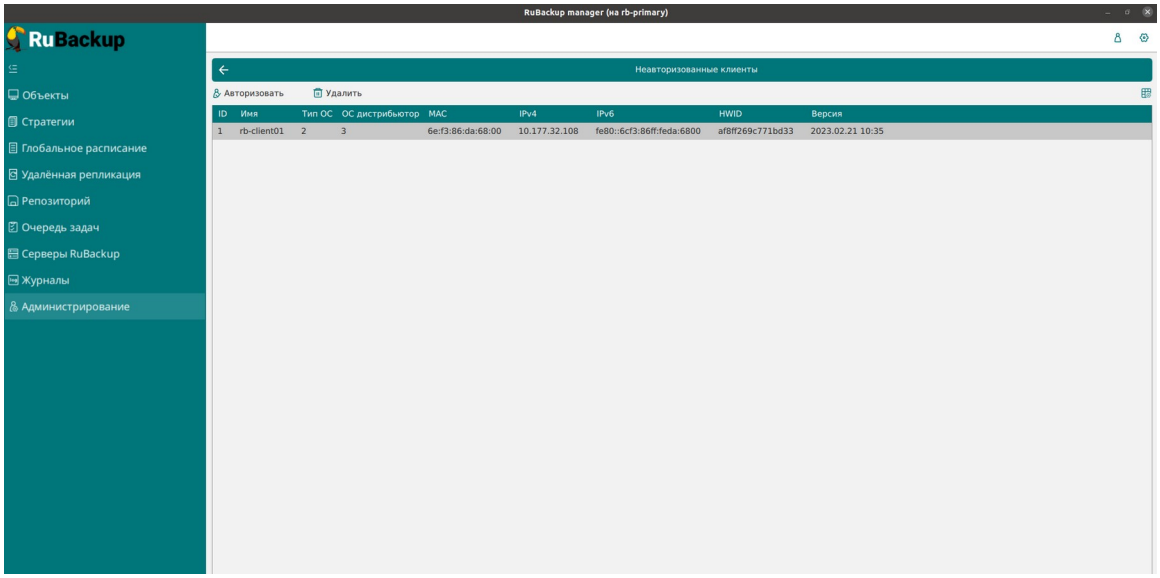

Рисунок 6

2. Выберите нужного неавторизованного клиента и нажмите **Авторизовать** (рисунок 7):

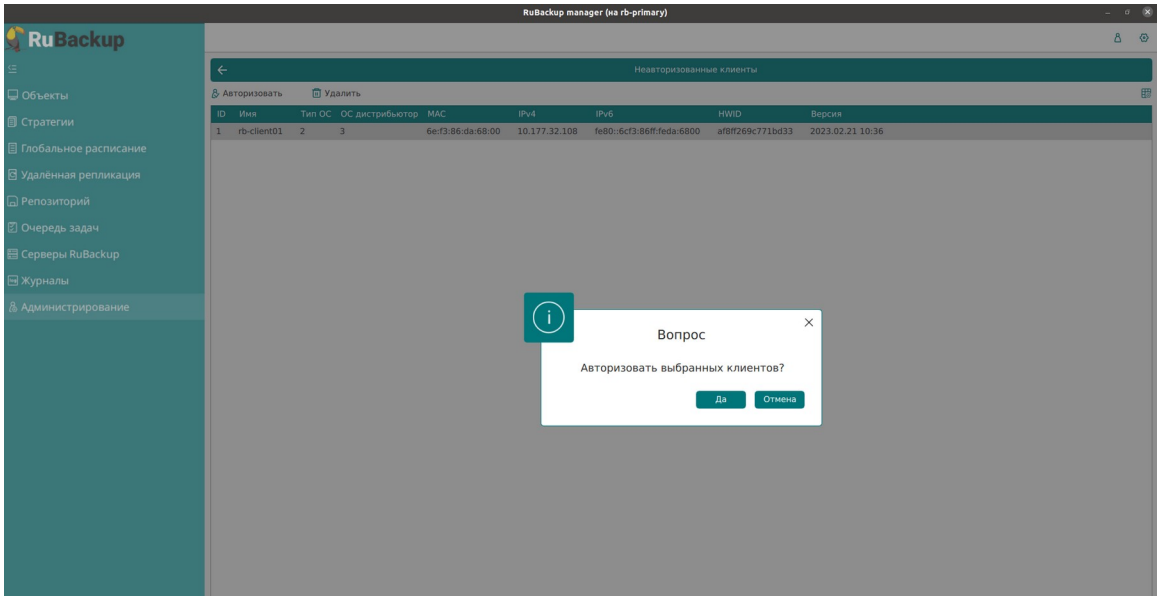

Рисунок 7

После авторизации новый клиент будет виден в главном окне RBM (рисунок 8):

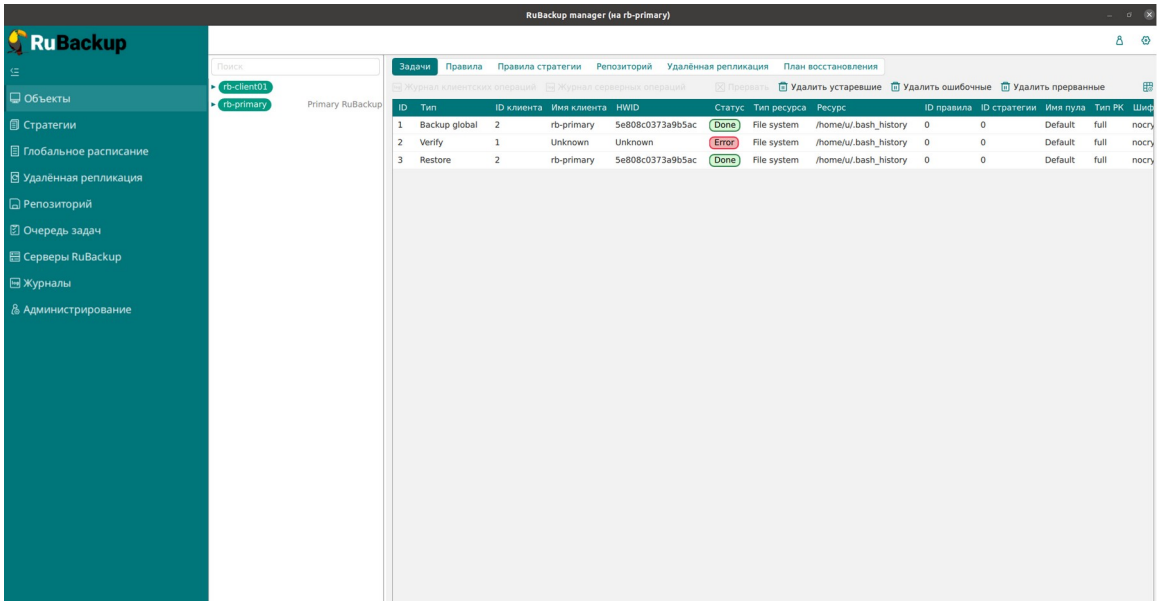

Рисунок 8

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 9):

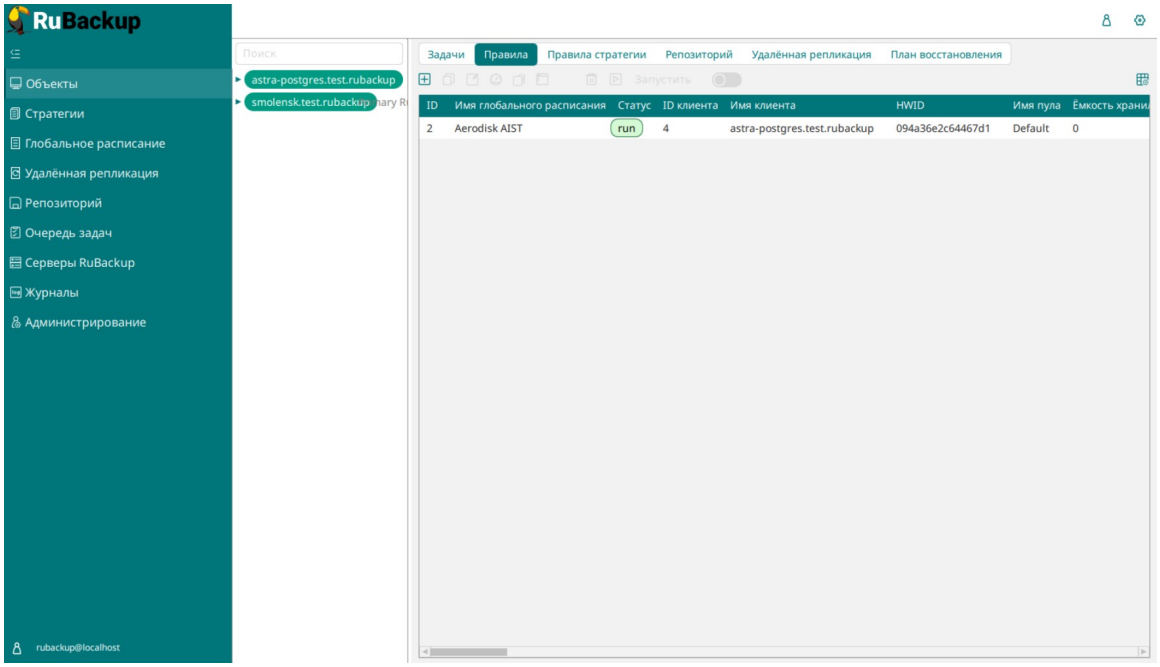

Рисунок 9

2. Выберите тип ресурса: «**Aerodisk AIST**»(рисунок 10).

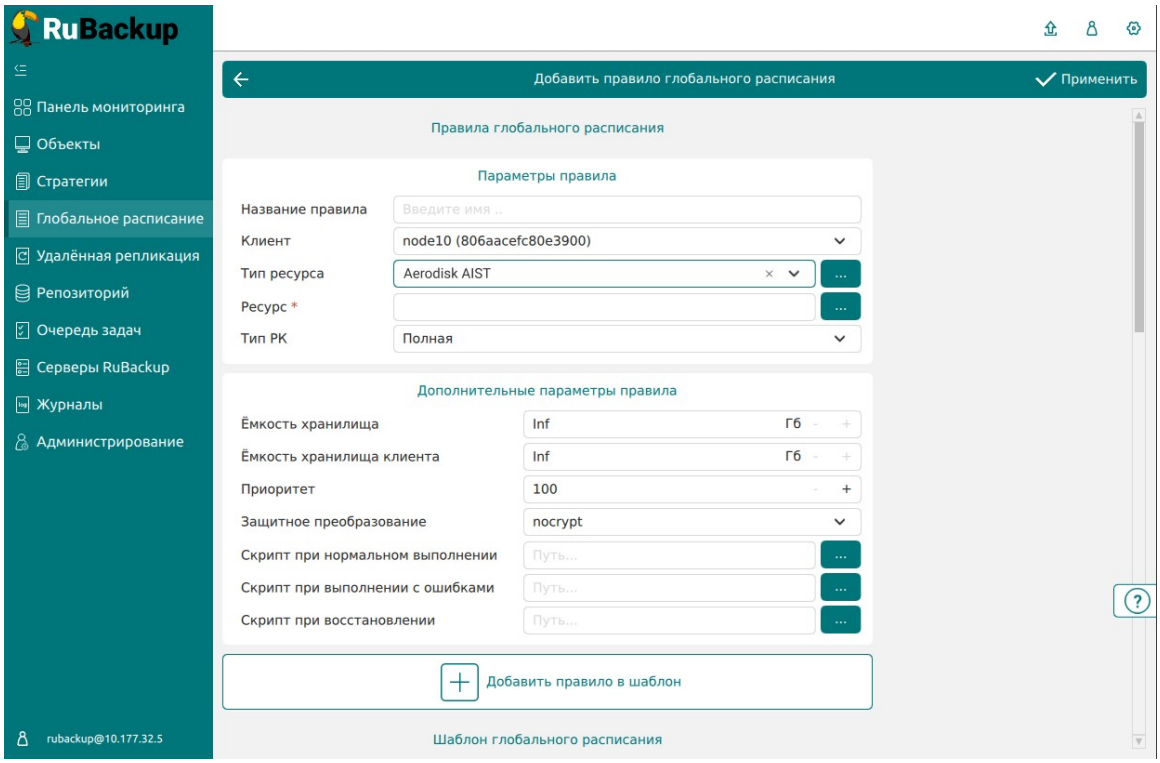

Рисунок 10

3. Выберите ресурс, нажав кнопку **Выбрать**.

4. Установите настройки правила: название правила, пул хранения данных, максимальный объём для резервных копий правила (в ГБ), тип резервного копирования, расписание резервного копирования, срок хранения и необязательный временной промежуток проверки резервной копии (рисунок 11).

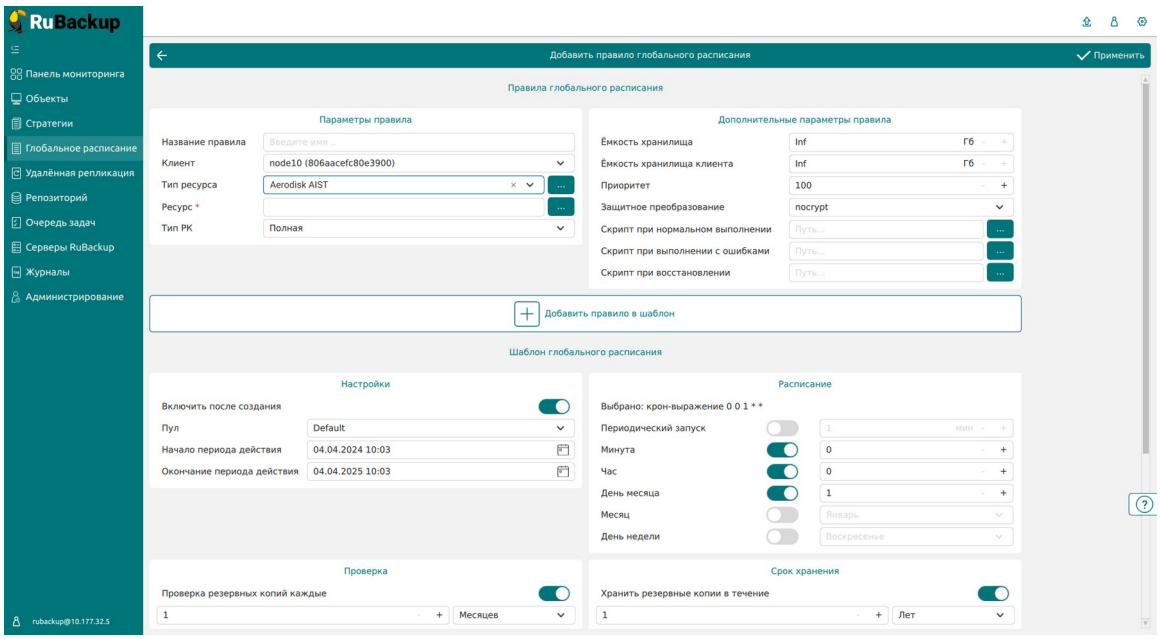

Рисунок 11

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

Так же внутри виртуальной машины может быть создан скрипт, располагающийся в файле /opt/rubackup/scripts/aerodisk-vm.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.

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 скрипт на клиенте перед началом резервного копирования;

– выполнить скрипт на клиенте после успешного окончания резервного копирования;

– выполнить скрипт на клиенте после неудачного завершения резервного копирования;

– 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 12).

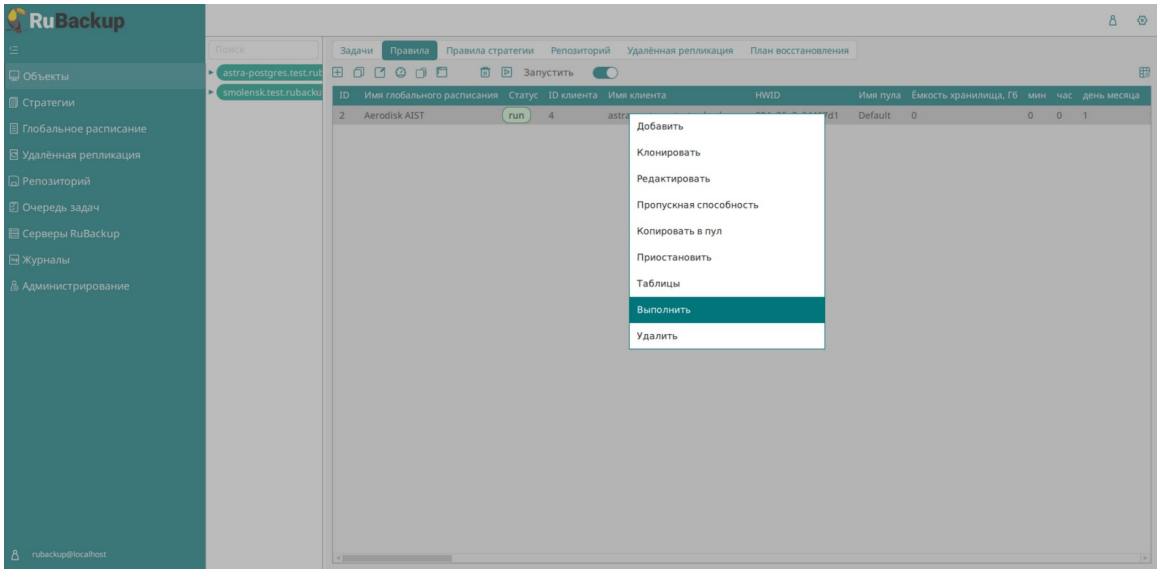

Рисунок 12

Проверить ход выполнения резервного копирования можно в окне «Очередь задач» (рисунок 13).

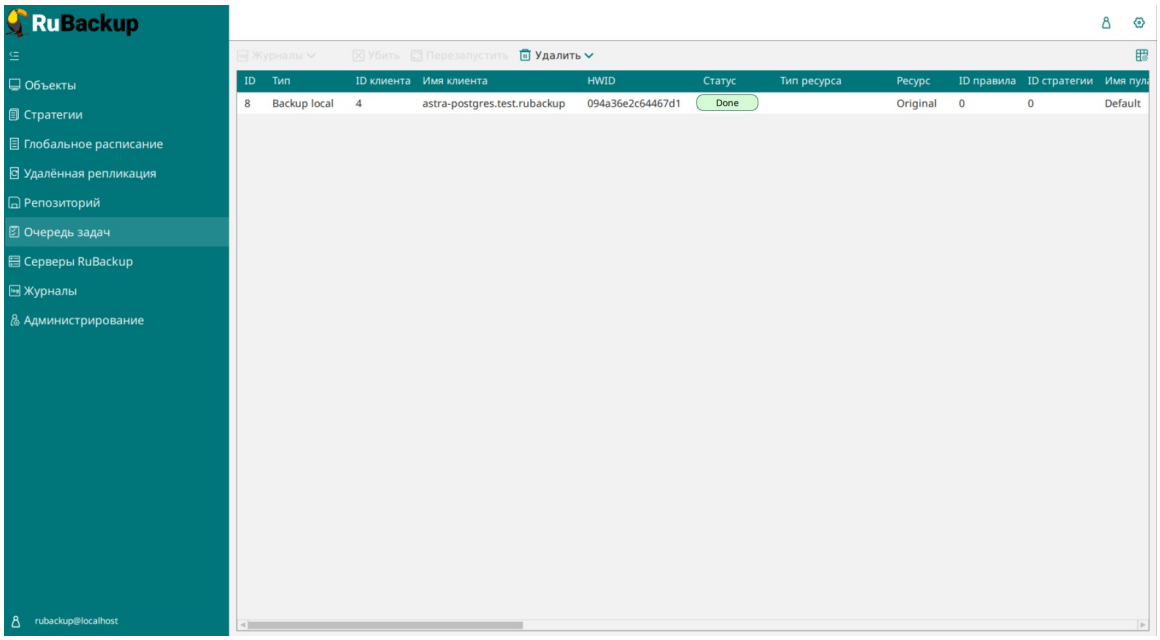

Рисунок 13

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 кладку «**Репозиторий**» на верхней панели RBM. Для этого найдите в списке требуемую резервную копию, нажмите на нее правой кнопкой мыши и выберите в контекстном меню «**Восстановить**» (рисунок 14):

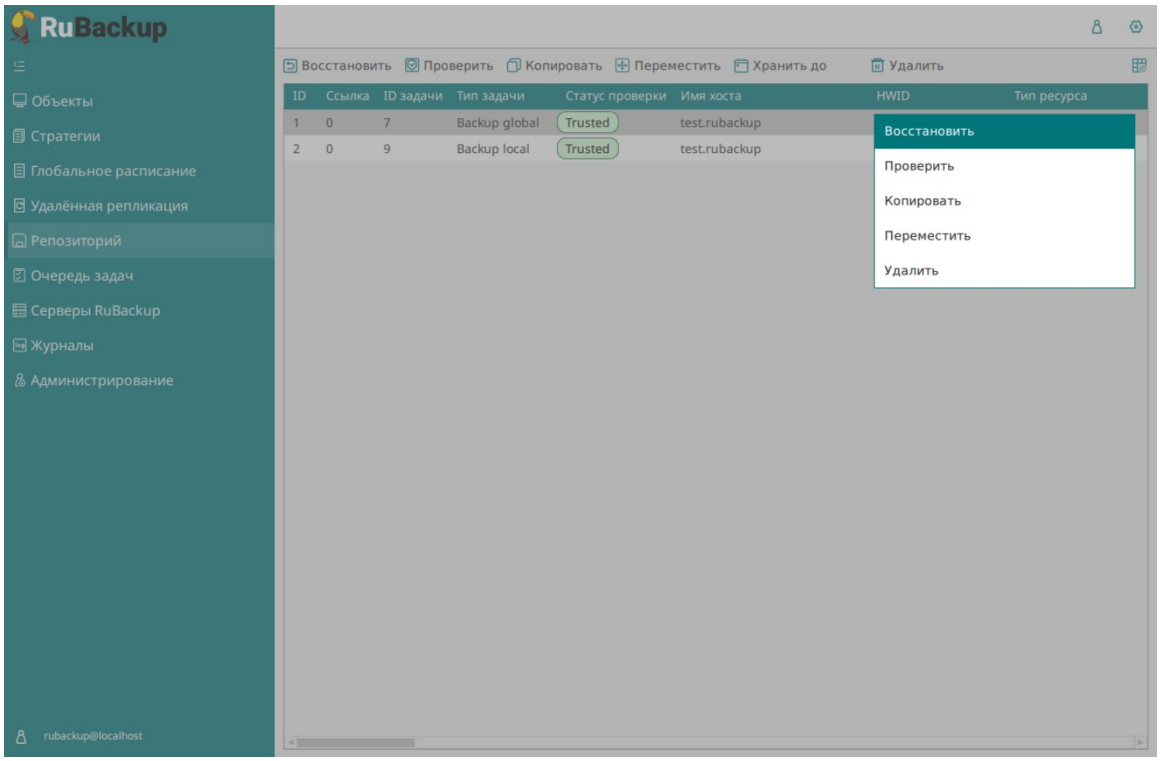

Рисунок 14

В окне централизованного восстановления можно увидеть основные параметры резервной копии и, если это применимо, определить место восстановления резервной копии. В случае восстановления виртуальной машины из резервной копии будет выполнена проверка наличия в среде виртуализации виртуальной машины с таким же именем. Если такой виртуальной машины нет, то будет произведено восстановление с оригинальным именем. Если виртуальная машина с таким именем уже есть, то к имени виртуальной машины будет добавлен цифровой постфикс (рисунок 15).

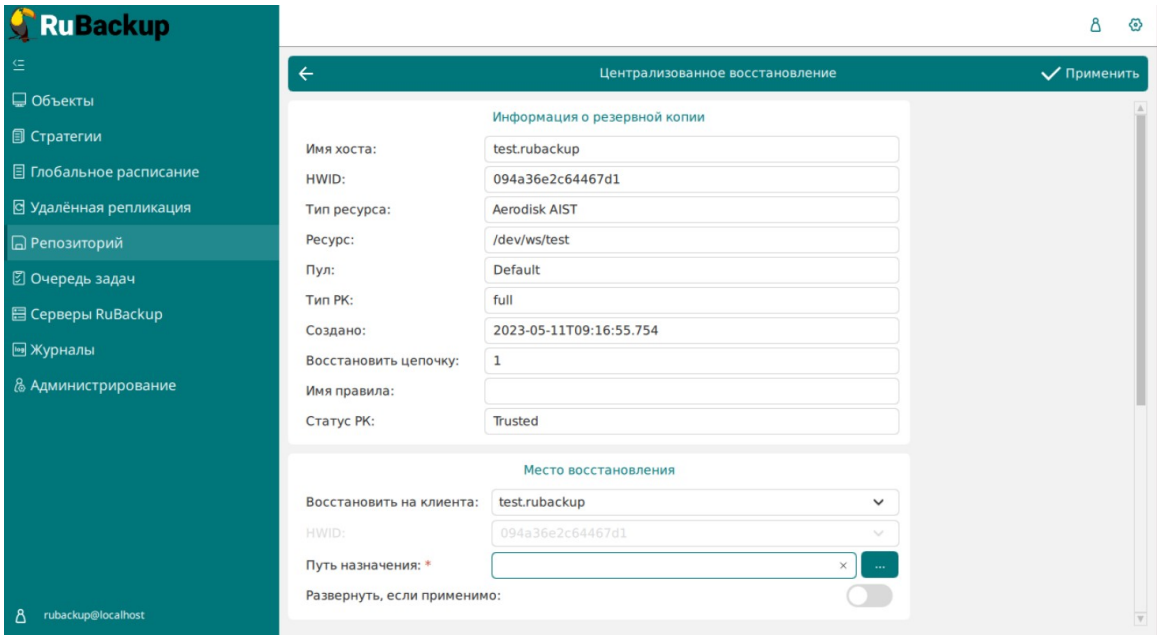

Рисунок 15

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 16).

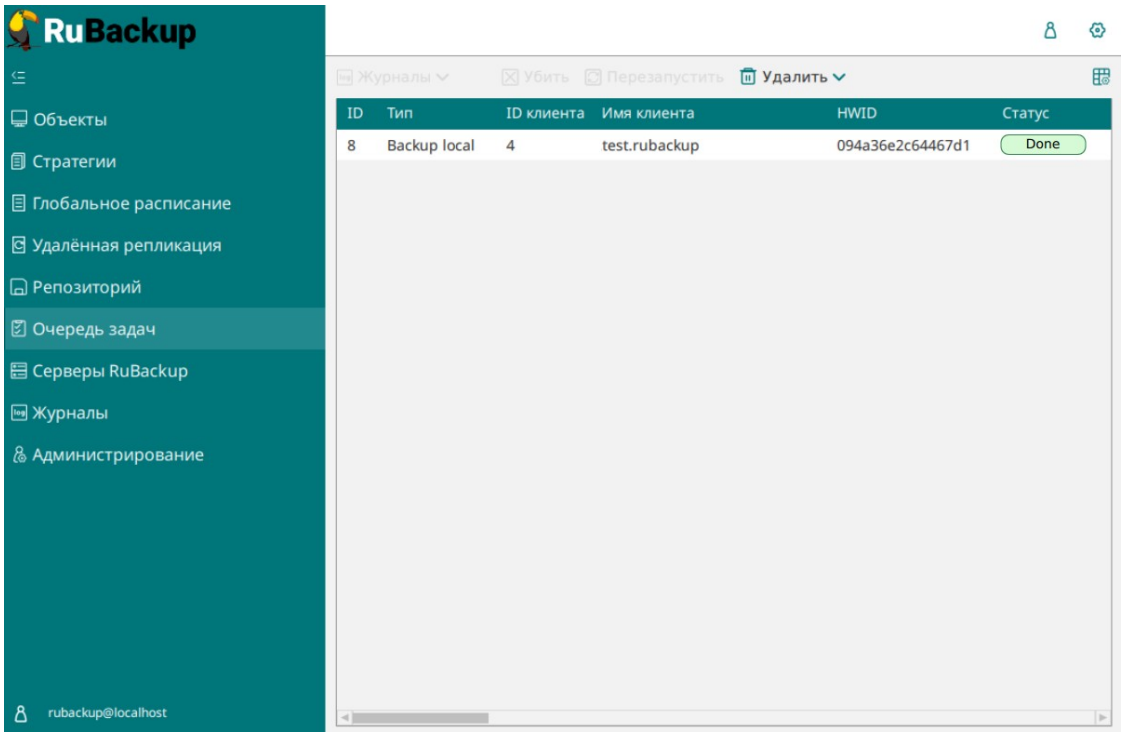

Рисунок 16

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