

RuBackup

Система резервного копирования и восстановления данных

Резервное копирование и восстановление ISP VMmanager



RuBackup

Версия 2.1

04.04.2024 г.

Содержание

Введение.....	3
Установка клиента RuBackup.....	5
Мастер-ключ.....	7
Защитное преобразование резервных копий.....	8
Алгоритмы защитного преобразования.....	9
Менеджер Администратора RuBackup (RBM).....	10
Срочное резервное копирование при помощи RBM.....	19
Централизованное восстановление резервных копий с помощью RBM.....	21

Введение

Система резервного копирования RuBackup позволяет выполнять резервное копирование и восстановление виртуальных машин среды виртуализации ISP VMmanager. 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 ISP VMmanager 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.

Поддерживаемые хранилища дисков виртуальных машин:

- файловое хранилище (DIR);
- LVM-хранилище;
- сетевое LVM-хранилище.

Для выполнения резервного копирования виртуальных машин среды виртуализации ISP VMmanager 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 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/isp_vmmanager.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`.

Установка клиента RuBackup

Для возможности резервного копирования виртуальных машин среды виртуализации ISP VMmanager необходимо установить клиент RuBackup на выбранный гипервизор (гипервизоры), сюда же необходимо установить модуль `rb_module_isp_vmmanager` из пакета `rubackup-isp-vmmanager-<version>.el8.x86_64.rpm` (См. дистрибутив для ОС CentOS 8). Модуль работает с любой версией ISP VMmanager.

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 ISP VMmanager `/opt/rubackup/etc/rb_module_isp_vmmanager.conf`.

Содержимое конфигурационного файла:

```
# 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

# URL to REST API of platform
url https://127.0.0.1
# Credentials for getting token
# for communication with platform
email admin@example.com
password 123456

# The maximum time that allow the module message transfer to take
timeout 5
enable_ssl no
# Uncomment and provide path to certificate if you would like
# to use SSL. 'enable_ssl' option should be set to 'yes' as well
# ca_info /path/to/certificate
```

Параметры конфигурационного файла:

- url — адрес платформы виртуализации ISP VMmanager.
- email — учетная запись пользователя от платформы виртуализации ISP VMmanager.
- password — пароль пользователя от платформы виртуализации ISP VMmanager.
- timeout — таймаут между запросами.
- 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 путь до SSL-сертификата, если указано значение no - закомментировать строку с параметром ca_info.
- ca_info — путь до сертификата ssl.

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

```
Tue Feb 21 02:12:57 2023: Try to check module: 'ISP vmmanager' ...  
Tue Feb 21 02:12:57 2023: Execute OS command: /opt/rubackup/modules/rb_module_ismanager -t 2>&1  
Tue Feb 21 02:12:57 2023: Module version: 2.0  
Tue Feb 21 02:12:57 2023: Panel: vmmanager version: 2022.09.2  
Tue Feb 21 02:12:57 2023: ... module 'ISP vmmanager' was checked successfully
```

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

```
# /opt/rubackup/modules/rb_module_ismanager -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 rbscrypt.

Алгоритм	Длина ключа, бит	Примечание
Anubis	128, 256	
Aria	128, 256	
CAST6	128, 256	
Camellia	128, 256	
Kalyna	128, 256, 512	Украинский национальный стандарт <u>ДСТУ 7624:2014</u>
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 APM 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).

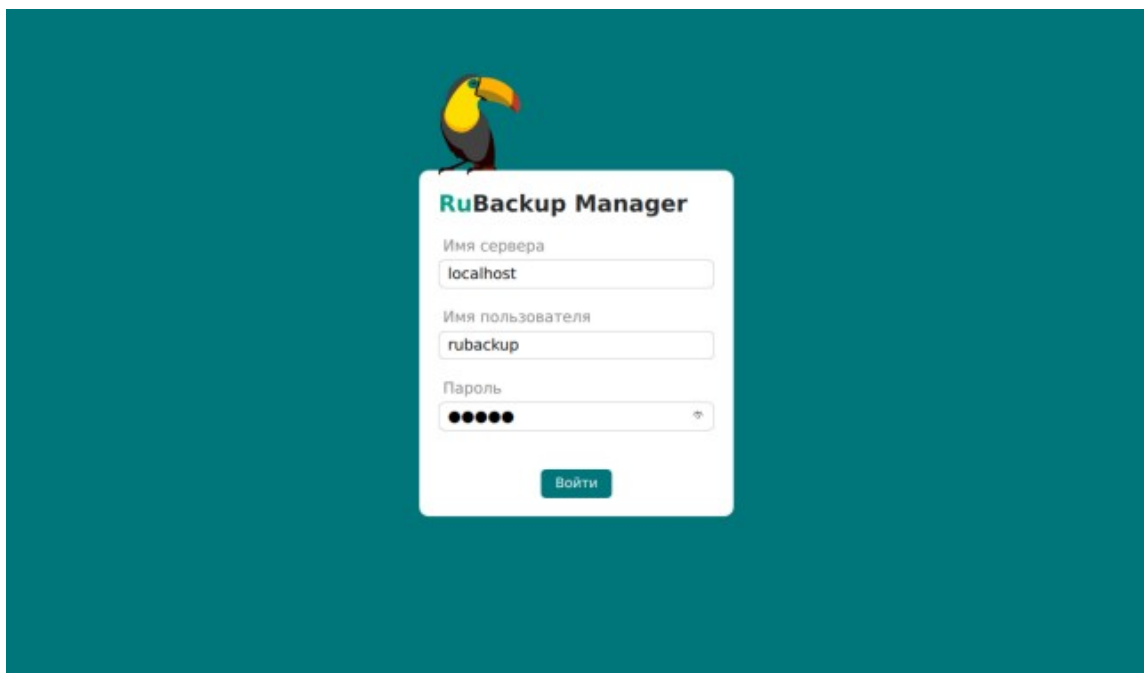


Рисунок 1

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

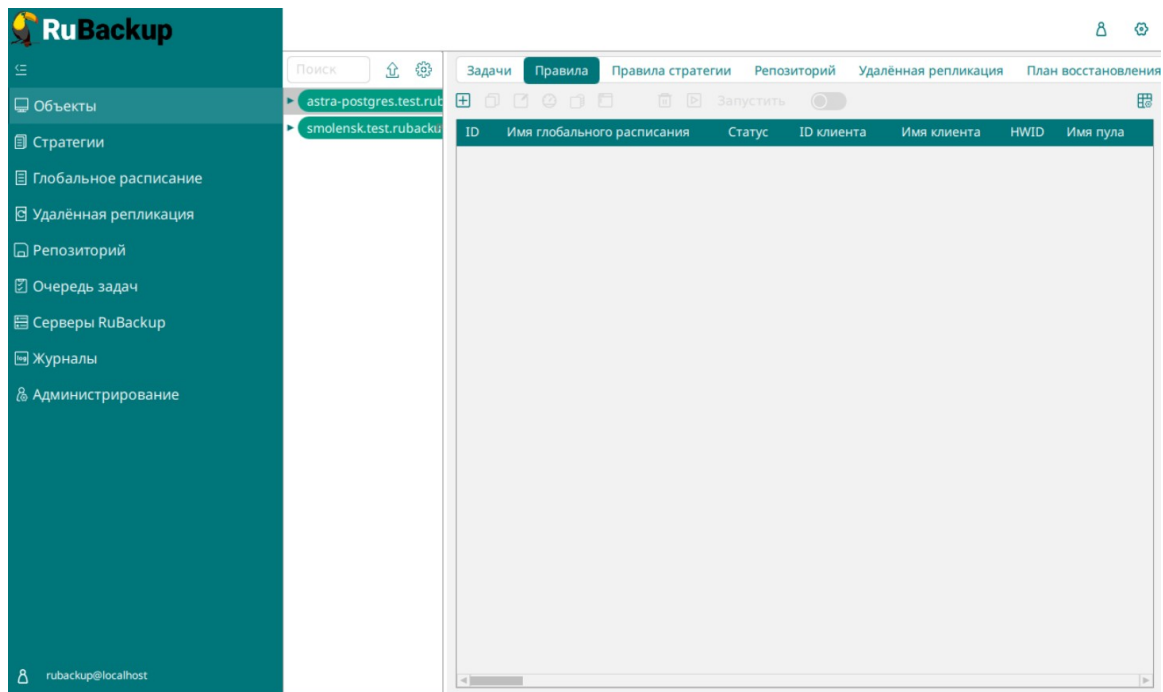


Рисунок 2

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):

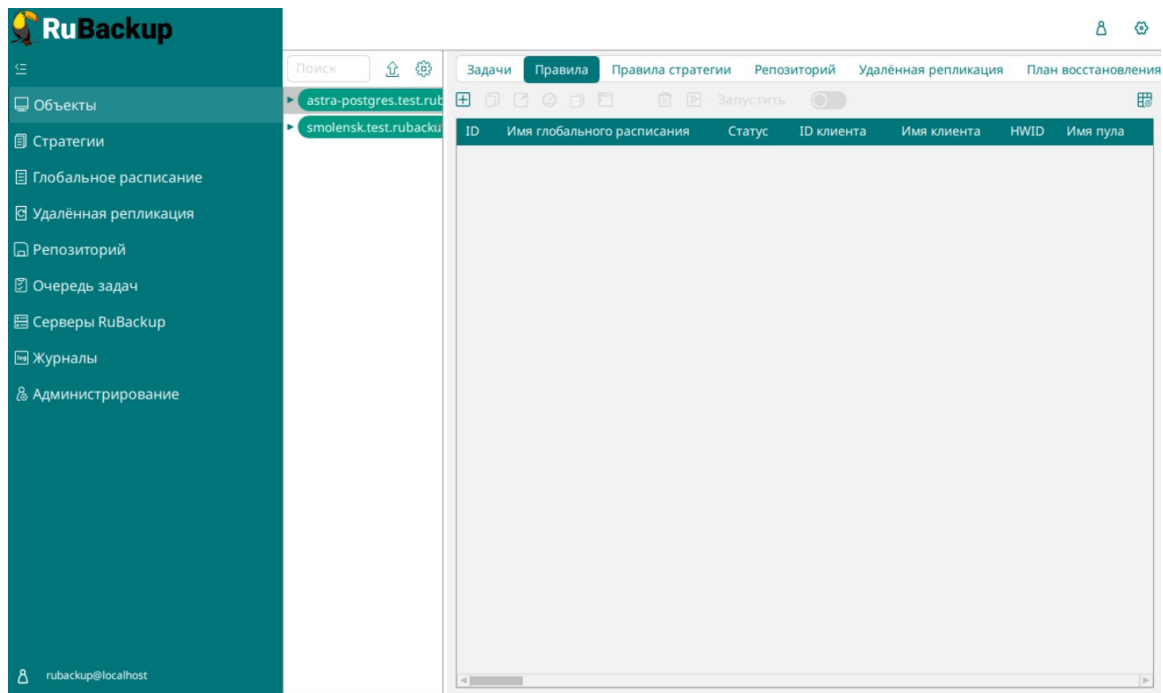


Рисунок 3

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

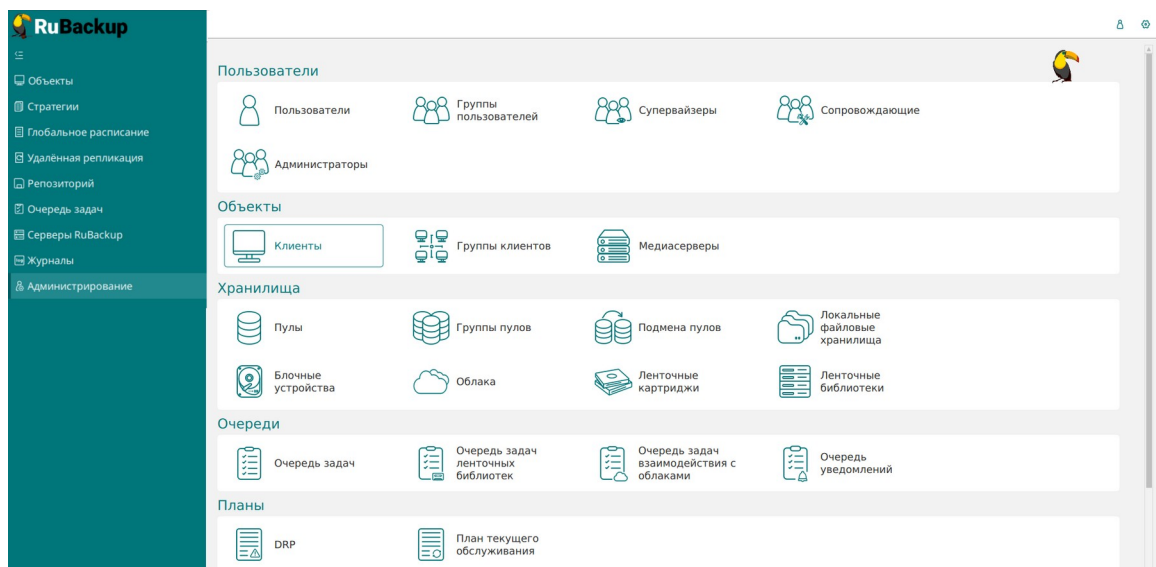


Рисунок 4

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.

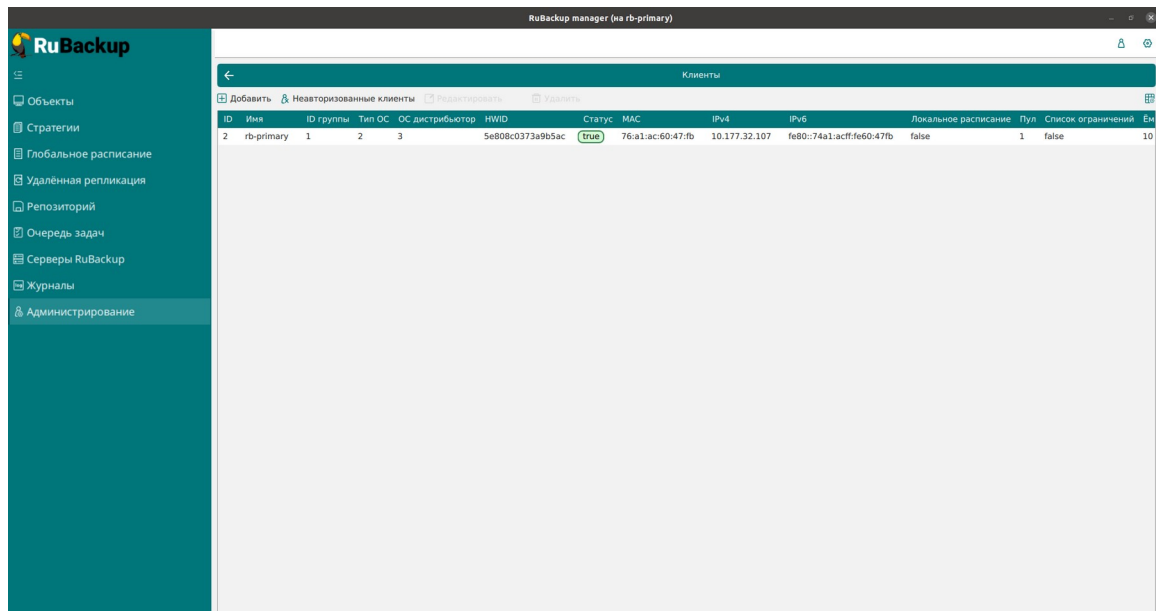


Рисунок 5

Для авторизации неавторизованного клиента в RBM выполните следующие действия:

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

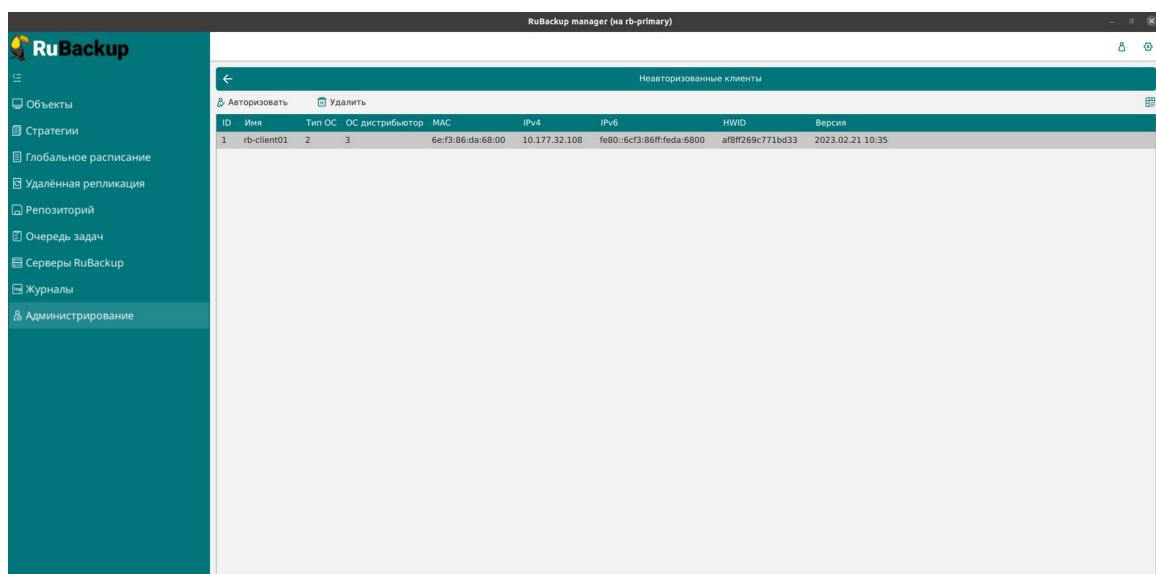


Рисунок 6

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

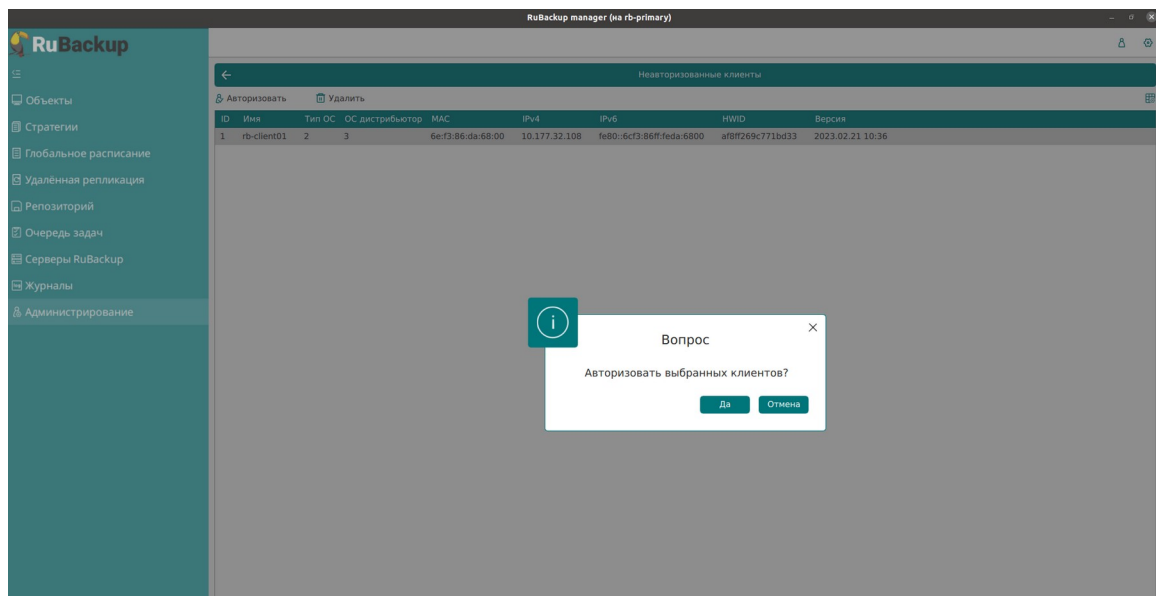


Рисунок 7

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

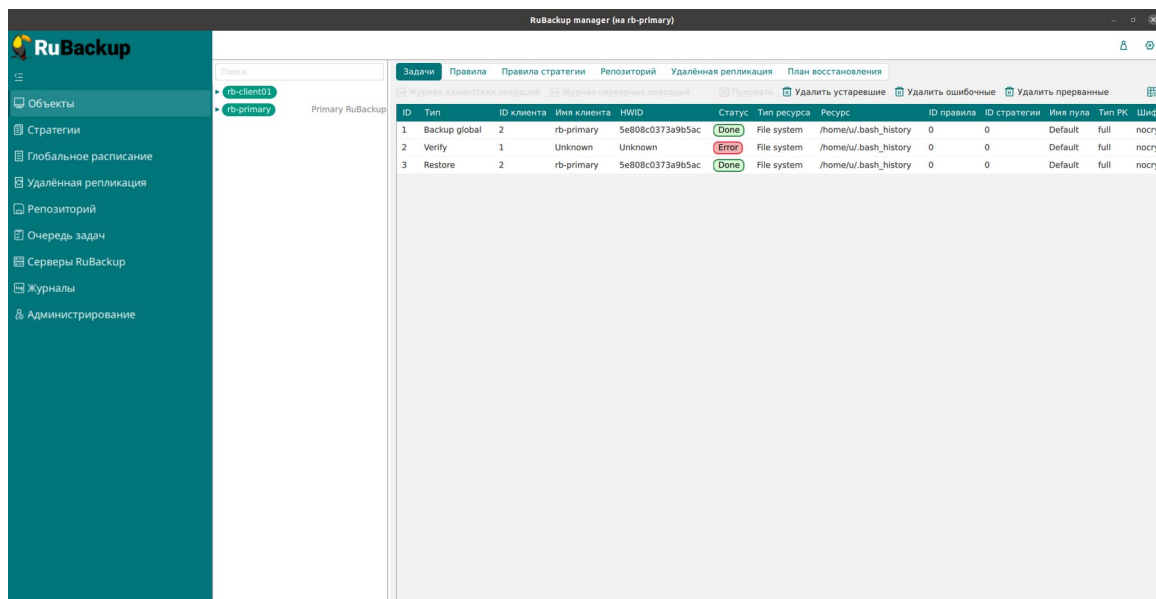


Рисунок 8

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):

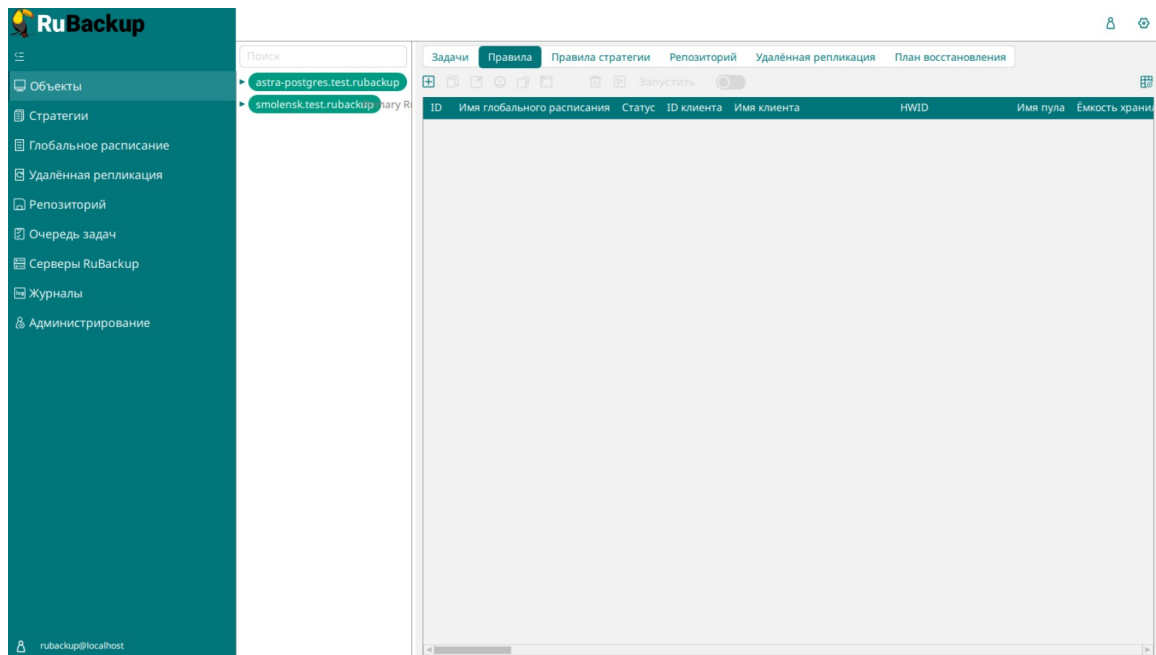


Рисунок 9

2. Выберите тип ресурса: **ISP VMmanager** (Рисунок 10).

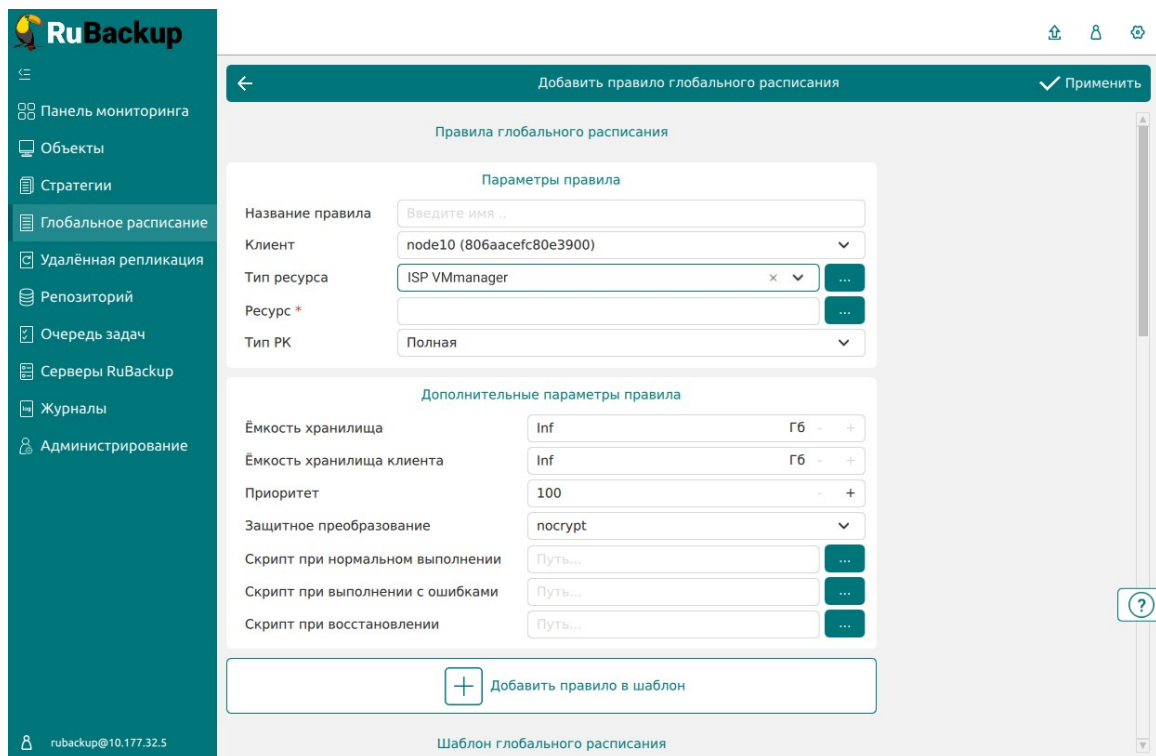


Рисунок 10

3. Выберите ресурс, нажав кнопку **Выбрать** (Рисунок 11).

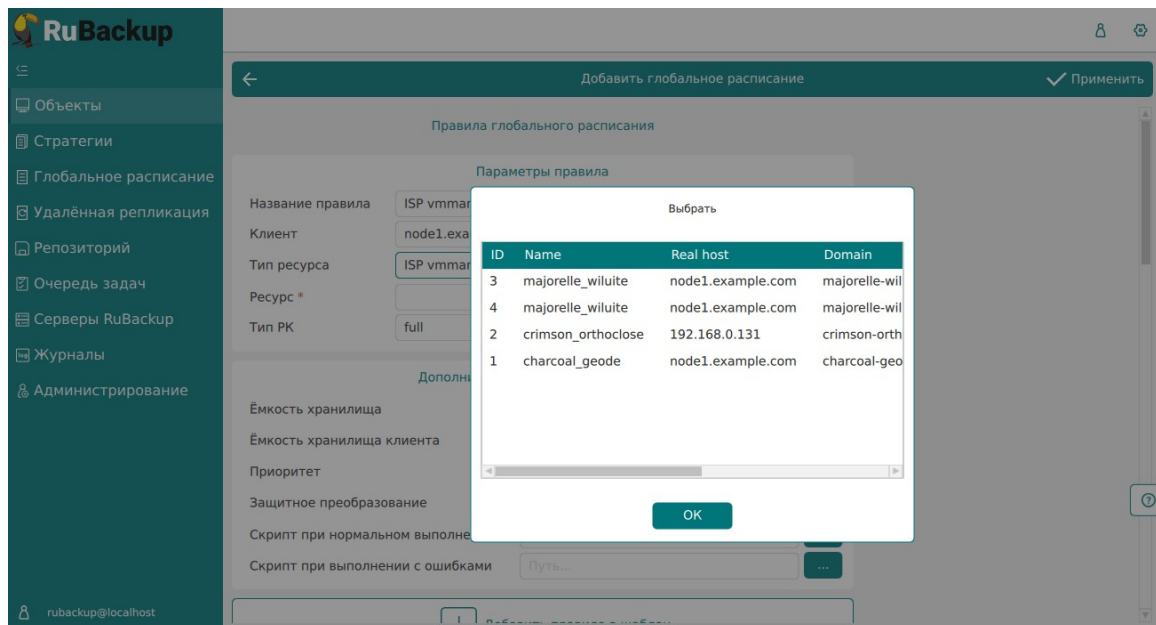


Рисунок 11

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 12).

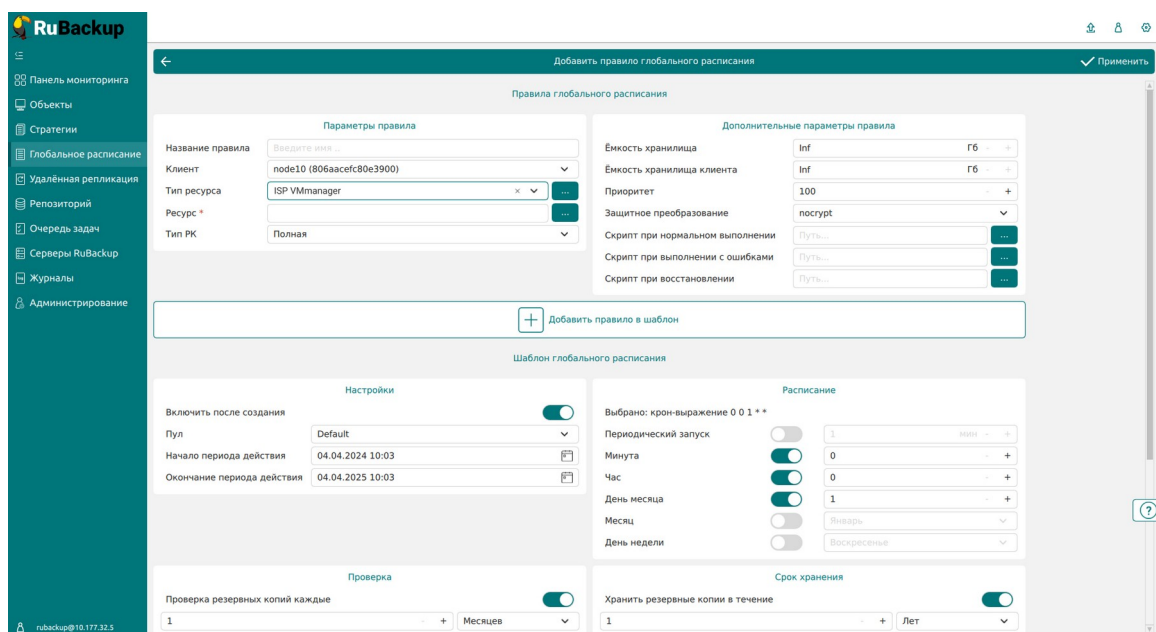


Рисунок 12

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 (Рисунок 13). Это может быть необходимо для приведения данных приложения в консистентное состояние, синхронизации кэша и т.п.

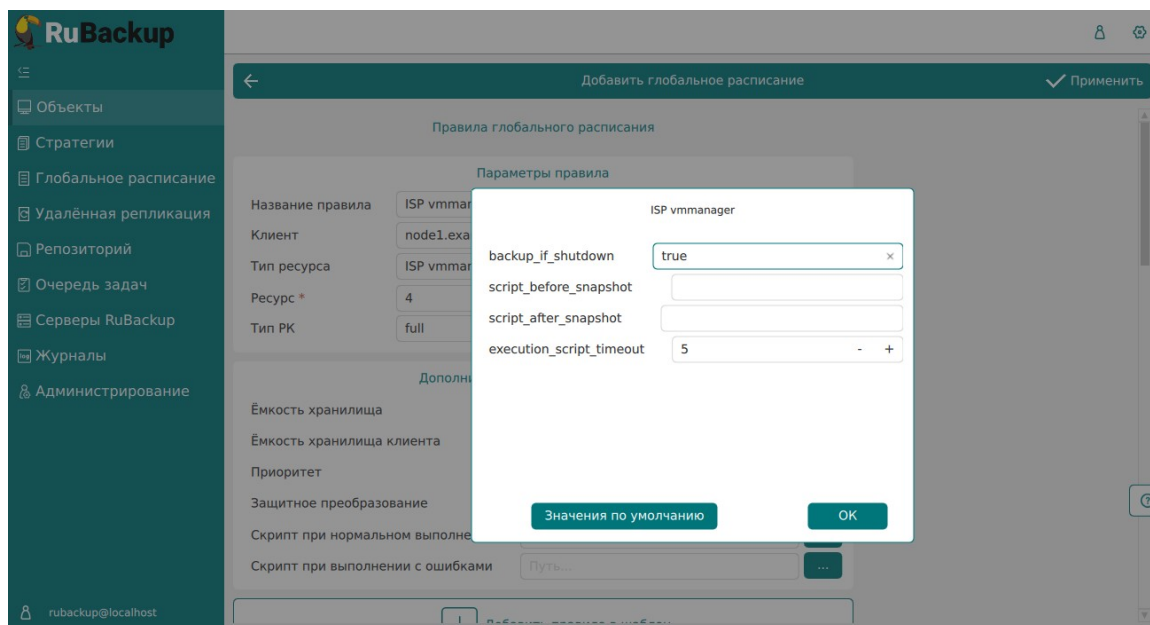


Рисунок 13

Так же внутри виртуальной машины может быть создан скрипт, располагающийся в файле `/opt/rubackup/scripts/isp_vmmanager.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 14).

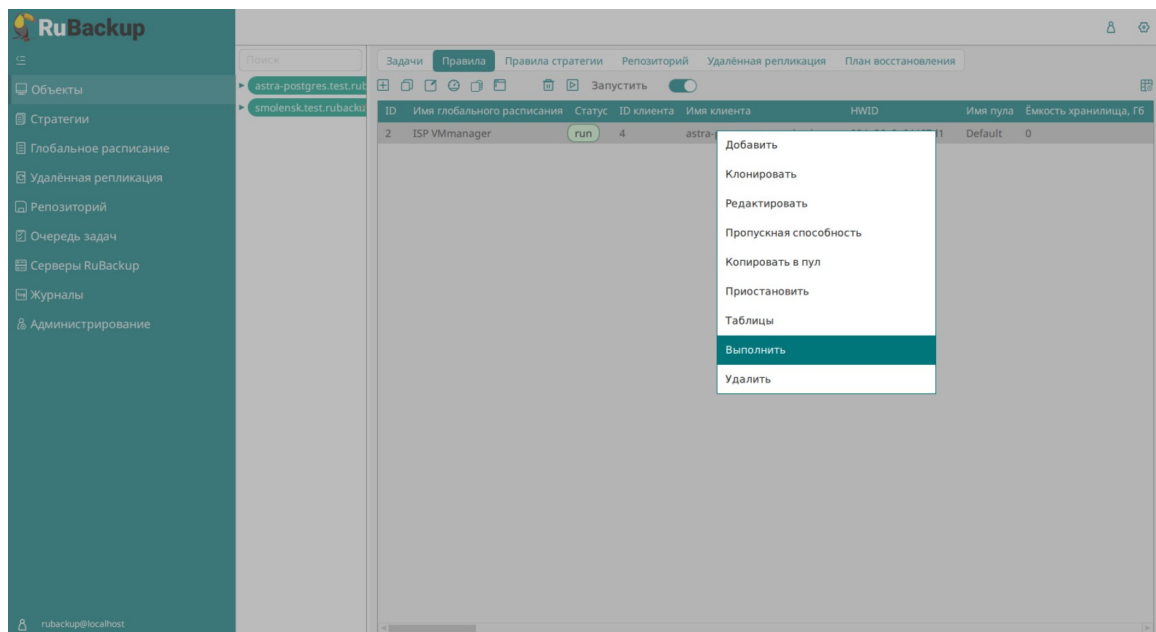


Рисунок 14

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

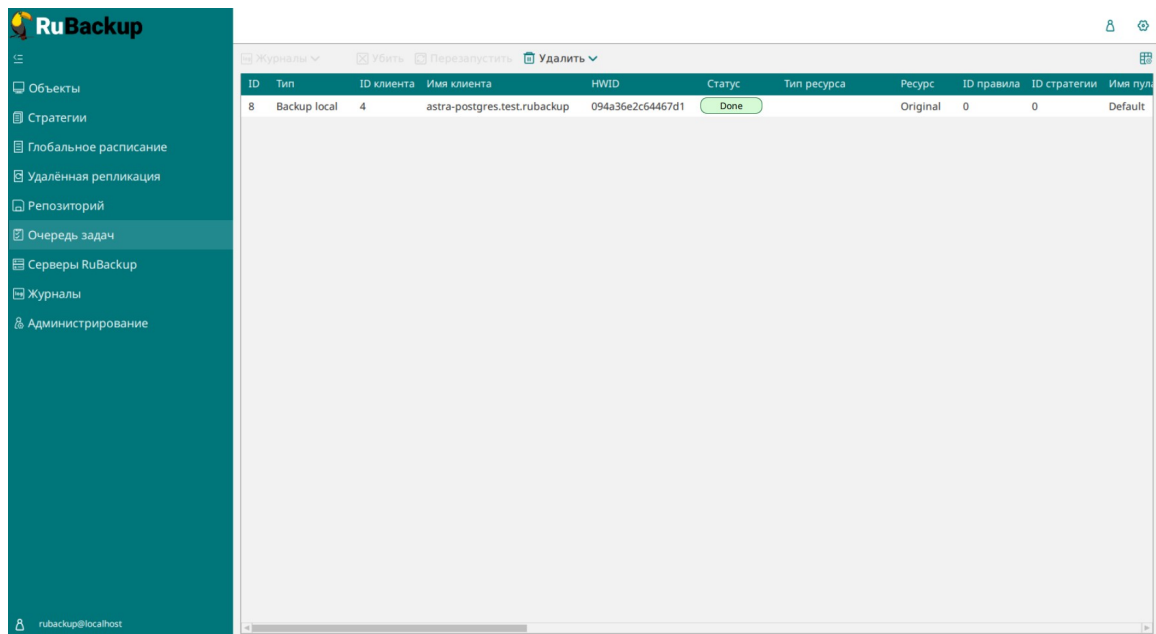


Рисунок 15

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 вкладку «**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 16).

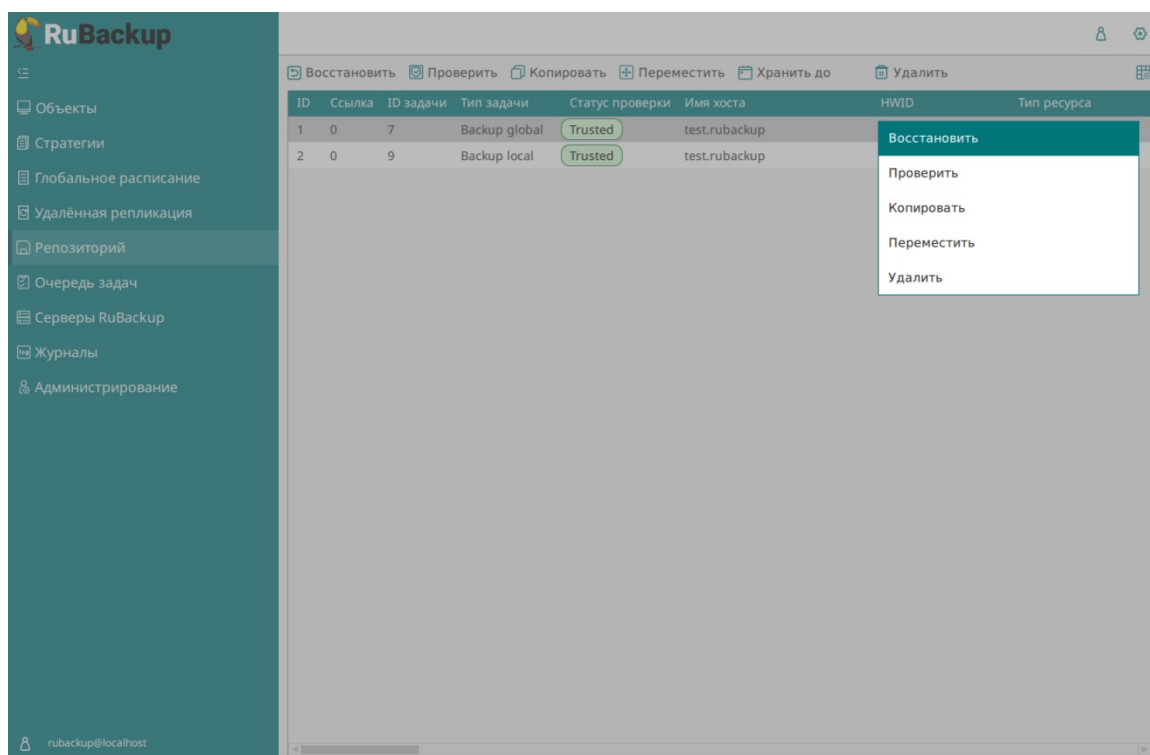
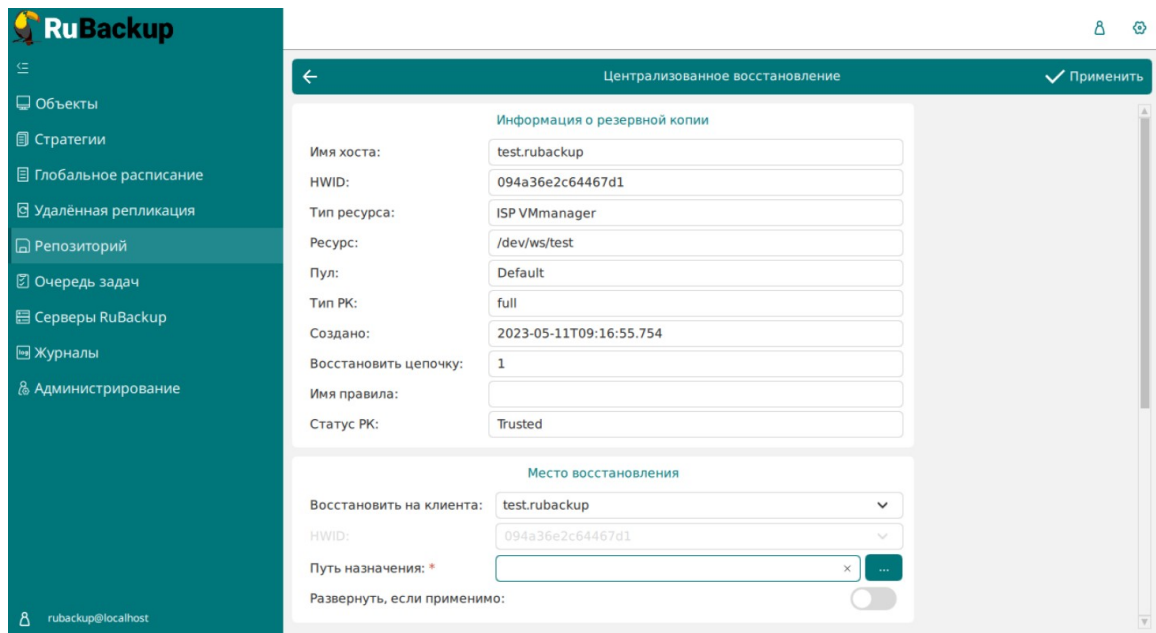


Рисунок 16

В окне централизованного восстановления можно увидеть основные параметры резервной копии и, если это применимо, определить место восстановления резервной копии (Рисунок 17). 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.



Информация о резервной копии	
Имя хоста:	test.rubackup
HWID:	094a36e2c64467d1
Тип ресурса:	ISP VMmanager
Ресурс:	/dev/ws/test
Пул:	Default
Тип РК:	full
Создано:	2023-05-11T09:16:55.754
Восстановить цепочку:	1
Имя правила:	
Статус РК:	Trusted

Место восстановления	
Восстановить на клиента:	test.rubackup
HWID:	094a36e2c64467d1
Путь назначения: *	<input type="text"/>
Развернуть, если применимо:	<input type="checkbox"/>

Рисунок 17

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**».

Для настройки параметров восстановления, которые относятся к модулю резервного копирования и восстановления ISP VMmanager нажмите на иконку «...» рядом с полем «**Параметры восстановления для модуля: ISP VMmanager**» (Рисунок 18).

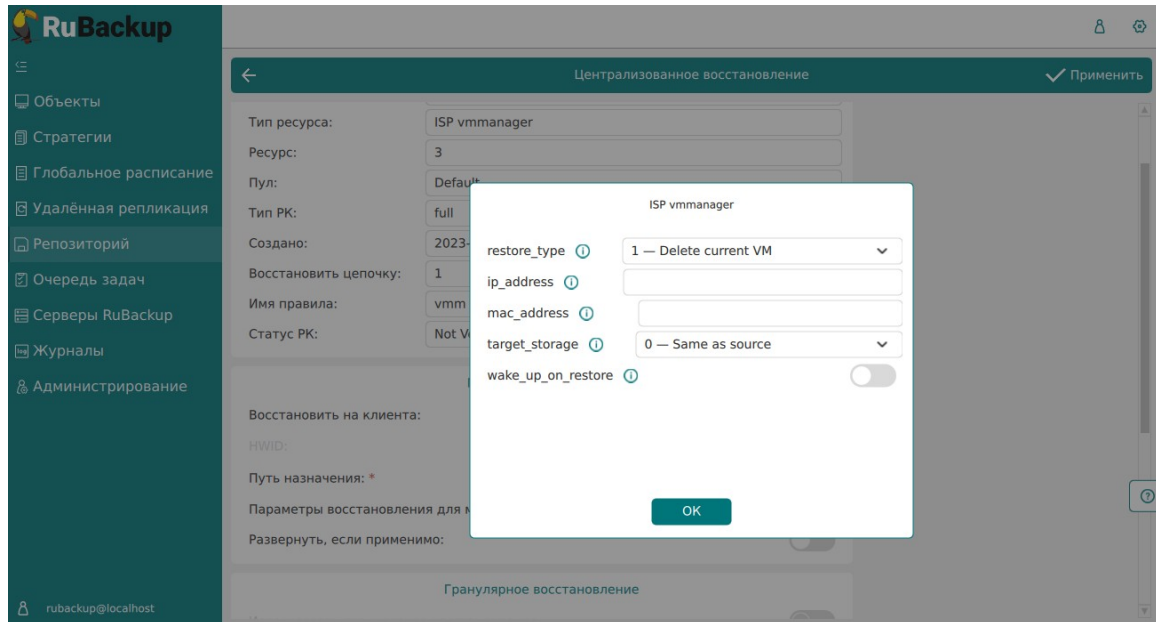


Рисунок 18

Выберите способ восстановления. Существует три способа восстановления резервной копии виртуальной машины:

1. Delete current VM (по умолчанию).

В этом случае будет удалена действующая виртуальная машина, резервную копию которой мы хотим восстановить, но её IP и MAC адрес останутся зарезервированными для новой виртуальной машины, которая будет создана вместо неё. Затем в диски новой виртуальной машины запишутся данные из дисков, которые хранятся в резервной копии.

Примечание: правило, созданное для виртуальной машины, с помощью которого производились резервные копии станет неактуальным после восстановления хотя бы одной резервной копии, поскольку после восстановления этим способом будет новая виртуальная машина с новым ID.

2. Restore disks only.

При этом типе восстановления действующая виртуальная машина будет выключена, в её диски будут записаны данные из дисков, образы которых хранятся в архиве.

3. Create new VM.

При этом типе восстановления будет создана новая виртуальная машина с сетевой частью, которую необходимо указать пользователю в RBM (Рисунок 19). После создания виртуальной машины, в её диски будут записаны данные из образов, которые хранятся в архиве.

Примечания:

- При создании новой виртуальной машины опционально можно выбрать хранилище, в котором будет создан диск (или все диски). Если эта опция не указана, диск будет создан в том же хранилище с тем ID, в котором он был во время резервного копирования.
- Если у виртуальной машины, для которой выполнялось резервное копирование, было больше одного сетевого интерфейса, то восстановление такой резервной копии невозможно, поскольку в конфигурационном файле можно указать только одну пару из IP и MAC адресов.

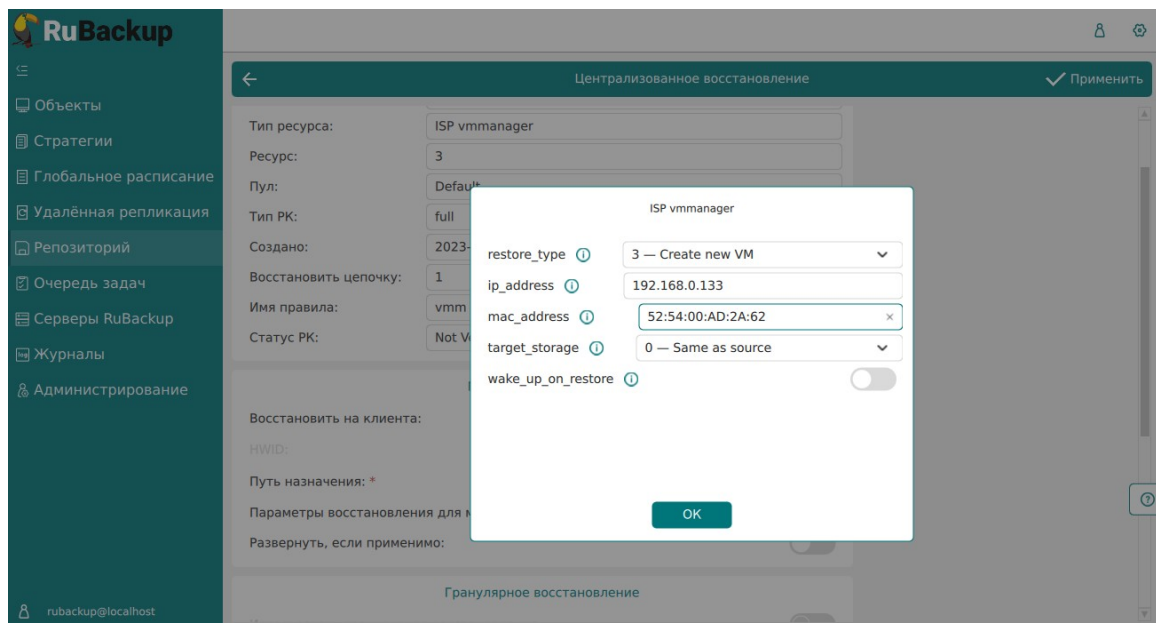


Рисунок 19

Проверить ход выполнения восстановления резервной копии можно в окне **Очередь задач** (Рисунок 20).

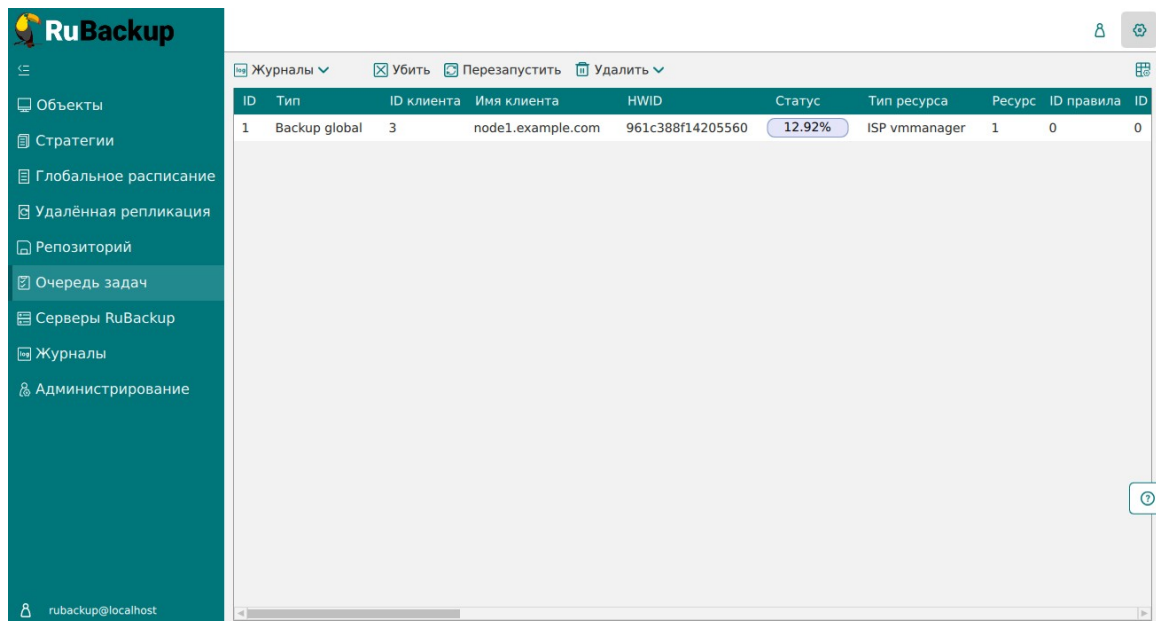


Рисунок 20

При успешном завершении восстановления резервной копии или цепочки резервных копий, соответствующие задачи на восстановление перейдут в статус **«Done»** (Рисунок 21).

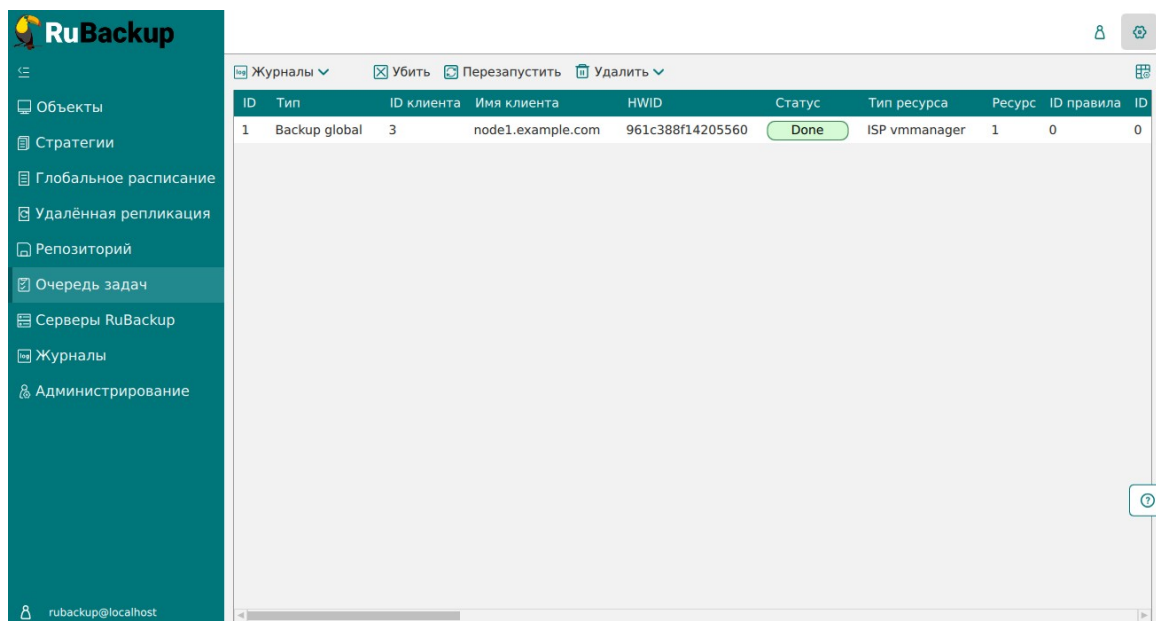


Рисунок 21