RuBackup
Система резервного копирования и восстановления данных

Резервное копирование объектов облака S3

Версия 1.9

2022 г.

Содержание

Введение

Система резервного копирования RuBackup позволяет выполнять защиту и восстановление данных, которые располагаются в облаках S3. Доступно полное, инкрементальное и дифференциальное резервное копирование. Так же возможно выполнять резервное копирование с использованием дедупликации и хранить резервные копии в дедуплицированном хранилище.

Объект, или ресурс, для выполнения резервного копирования - это бакет (bucket, корзина), расположенная в облаке S3.

При выполнении резервного копирования в резервную копию попадут все объекты, которые содержатся в бакете. Для выполнения резервного копирования на клиенте необходимо установить модуль резервного копирования rb_module_s3_cloud_bucket из соответствующего пакета и произвести настройку облака, для которого необходимо выполнять резервное копирование и восстановление. Клиентом в данном случае может выступать сам сервер резервного копирования, или выделенный прокси-хост (виртуальная машина). Основное требование к клиенту - наличие достаточного дискового объема, который превышает размер объектов, размещенных в бакете. В ходе резервного копирования все объекты скачиваются из облака во временный каталог на прокси-хосте, производится упаковка резервной копии и передача ее на хранение в назначенное хранилище резервных копий.

Бакет обладает определенным именем; при восстановлении, если в облаке нет бакета с таким же именем, то он будет создан и объекты из резервной копии будут размещены в нем. Если в облаке уже есть бакет с таким же именем, то в него будут помещены объекты из резервной копии. При необходимости можно восстановить объекты бакета локально, без загрузки в облако.

Установка клиента RuBackup

Для возможности резервного копирования бакетов облака S3 при помощи RuBackup необходимо определить где должен функционировать модуль, обеспечивающий резервное копирование и имеющий доступ к облаку. Это может быть как сам сервер резервного копирования (или один из серверов серверной группировки), так и прокси-хост. На выбранном хосте необходимо установить клиент RuBackup. Подробно процедура установки клиента описана в документе «Руководство по установке серверов резервного копирования и Linux клиентов RuBackup».

При установке клиента на прокси-хост рекомендуется использовать функцию централизованного восстановления.

Так же на этот хост необходимо установить модуль rb_module_s3_cloud_bucket из соответствующего пакета (rubackup-s3-cloud.deb или rubackup-s3-cloud.rpm). В ходе инсталляции пакета в системе будет создан файл настроек облаков, которые подлежат защите:

```
/opt/rubackup/etc/rb_module_s3_cloud_bucket.conf
```

В этом файле необходимо создать настройки, которые позволят модулю подключиться к облаку:

```
cloudname           Cloud1
access_key_id AKYA3Y7L5VW5IGOCGHLT
secret_key_access   PUbrIczmYhaVdFX4KRTR9xuZl4efSB0Wz56KHdox
endpoint_override   http://my-s3cloud.local:4566
proxy_host
proxy_port
proxy_username
proxy_password
```

В том случае, если требуется настроить доступ к нескольким облакам, то нужно создать в файле /opt/rubackup/etc/rb_module_s3_cloud_bucket.conf несколько последовательных блоков настроек для каждого облака.

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

```
Try to check module: 'S3 cloud bucket' ...
Execute OS command: /opt/rubackup/modules/rb_module_s3_cloud_bucket -t 2>&1
Module version: 1.8
   The cloud is configured and available for connection: Cloud1
... module 'S3 cloud bucket' was checked successfully
```

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

```
# /opt/rubackup/modules/rb_module_s3_cloud_bucket -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 1.9 RBM располагается в отдельном пакете и может быть установлен как на сервер резервного копирования, так и на удаленном АРМ администратора.

RuBackup 1.9 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.

Для запуска RBM следует выполнить команду:

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

В открывшемся окне «Аутентификация» ввести имя пользователя и пароль (рисунок 1).

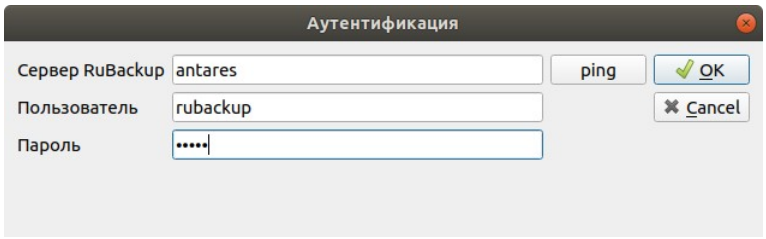


Рисунок 1

Для резервного копирования бакета облака S3 на прокси-хосте должен быть установлен клиент RuBackup и модуль rb_module_s3_cloud_bucket. 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 (рисунок 2).

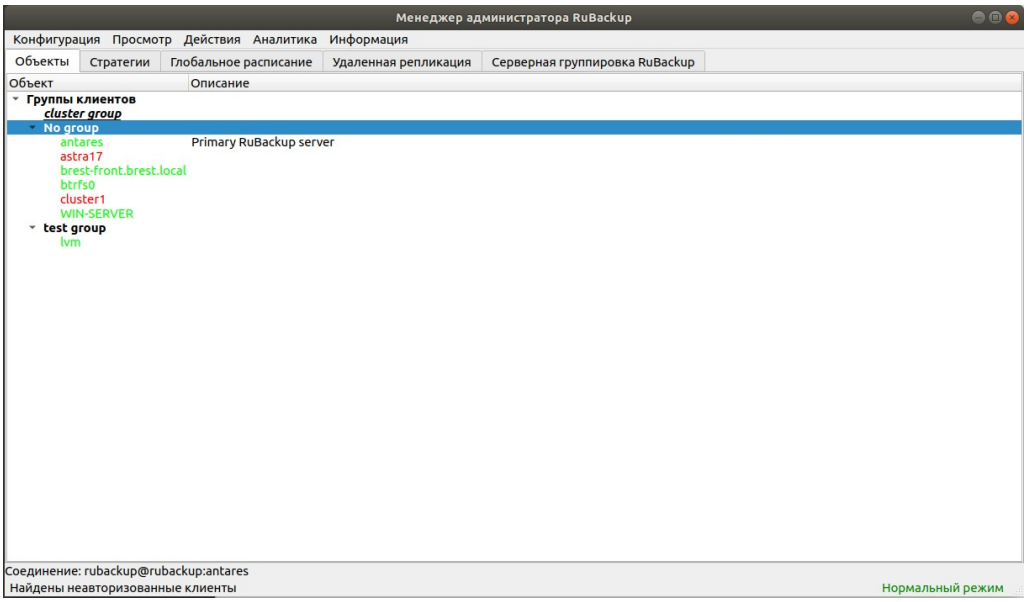


Рисунок 2

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

Для авторизации неавторизованного клиента в RBM выполните следующие действия:

1. Откройте меню **Действия → Клиенты → Авторизовать клиентов** (рисунок 3).

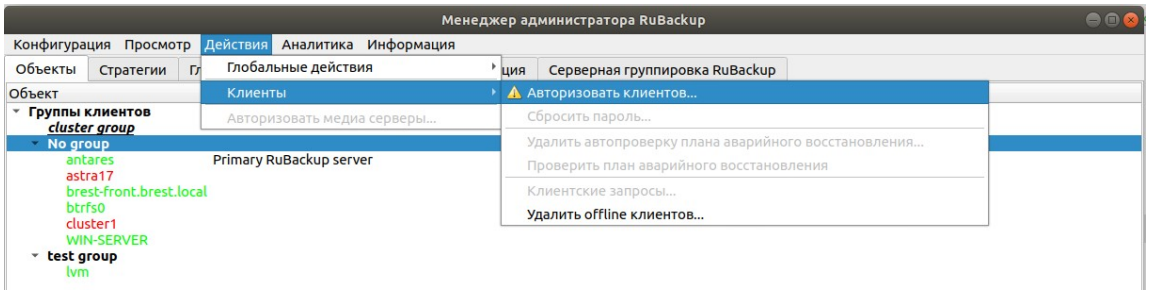


Рисунок 3

2. Выберите нужного неавторизованного клиента и нажмите **Авторизовать** (рисунок 4).

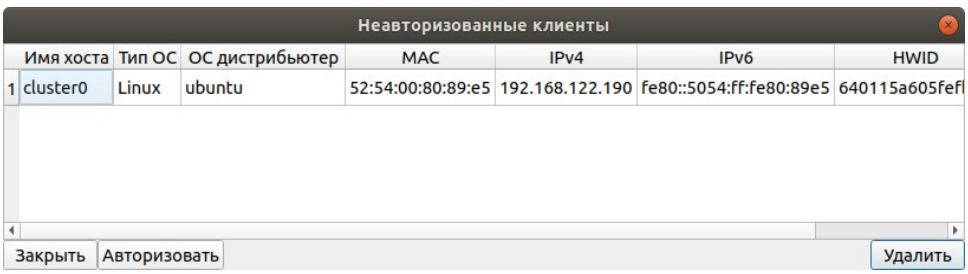


Рисунок 4

После авторизации новый клиент будет виден в главном окне RBM (рисунок 5).

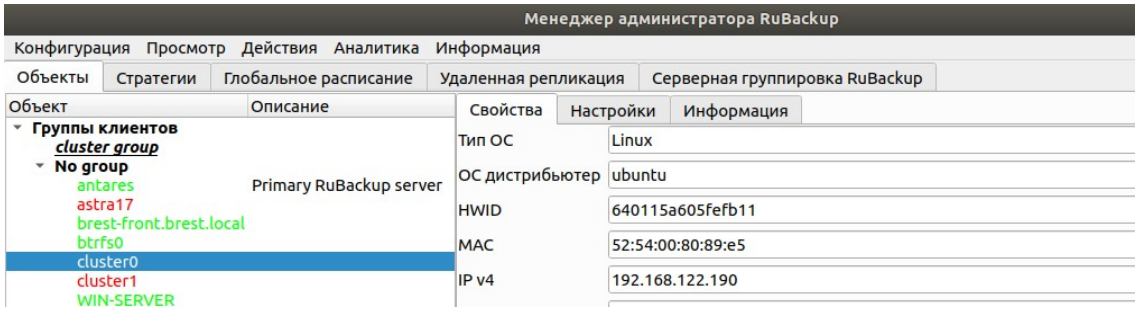


Рисунок 5

Чтобы выполнять регулярное резервное копирование бакета облака S3, необходимо создать правило в глобальном расписании (в случае групповых операций можно так же использовать стратегии резервного копирования). Для этого выполните следующие действия:

1. Выберите прокси-хост, настроенный для защиты облака, и добавьте правило резервного копирования (рисунок 6).

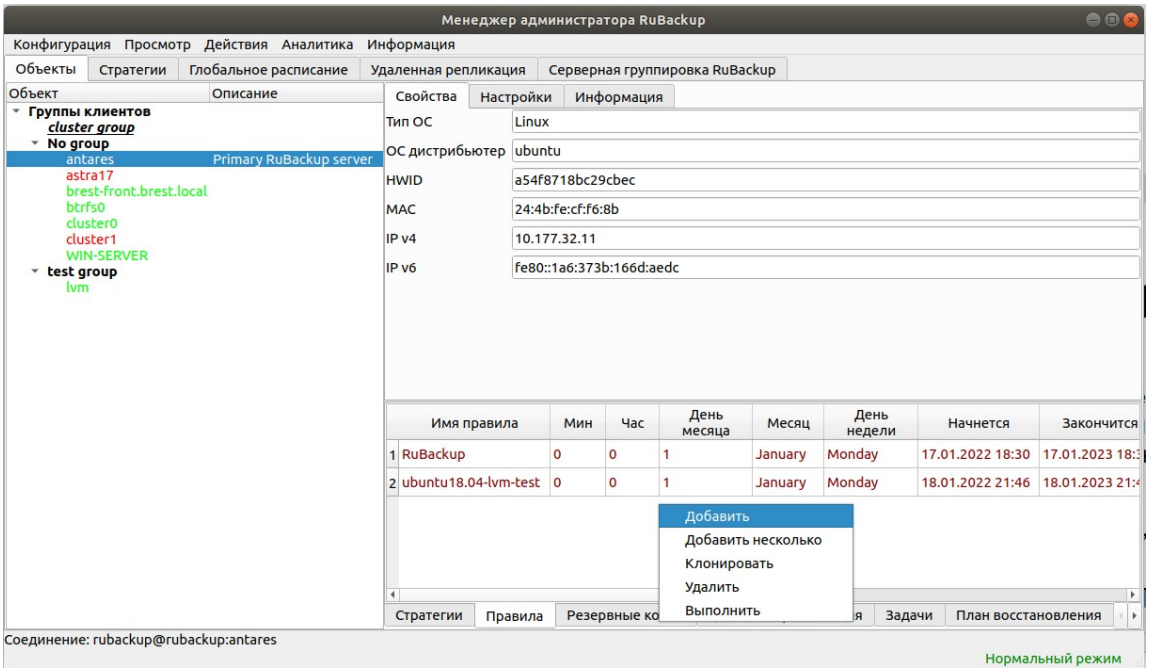


Рисунок 6

2. Выберите тип ресурса: **«S3 cloud bucket»** (рисунок 7).

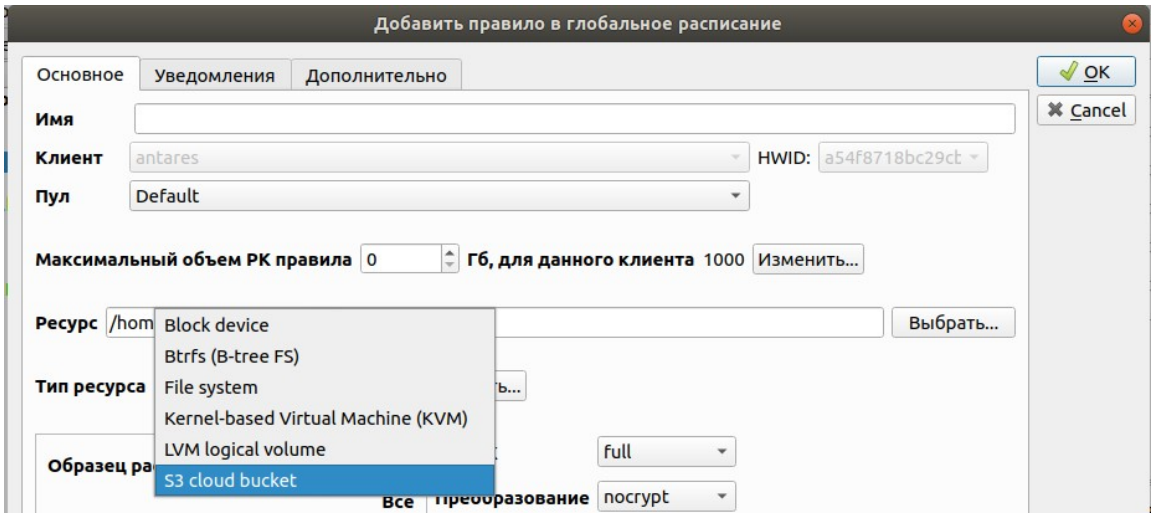


Рисунок 7

3. Выберите ресурс, нажав кнопку **Выбрать** (рисунок 8).

Примечание – Т. к. список ресурсов запрашивается в облаке, процесс получения информации может занимать определенное время, вплоть до нескольких секунд.

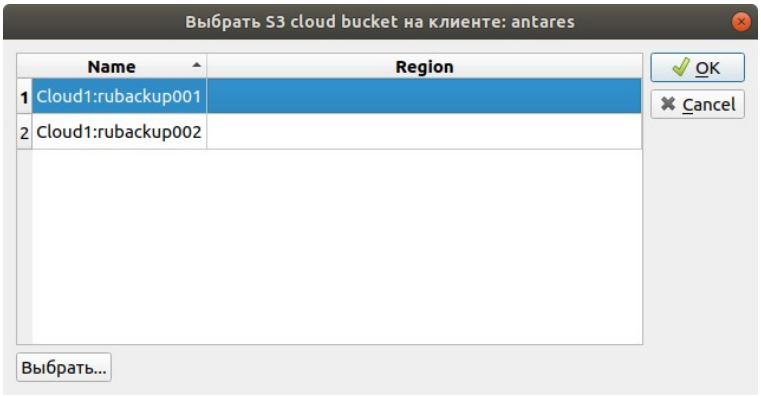


Рисунок 8

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 9).

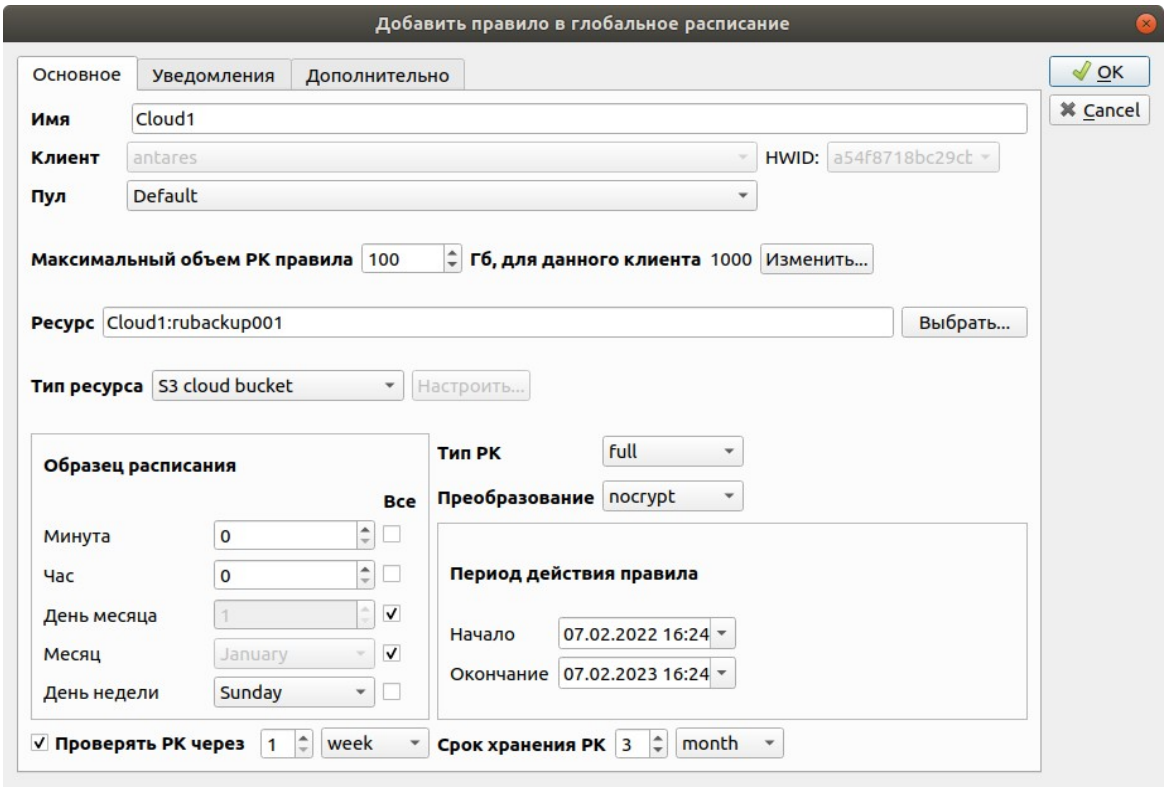


Рисунок 9

5. 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 (рисунок 10).

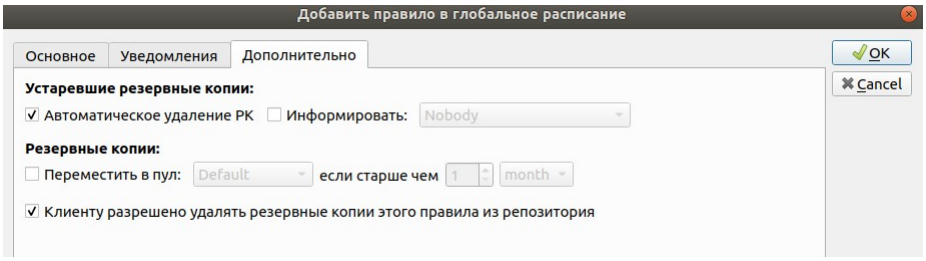


Рисунок 10

Вновь созданное правило будет иметь статус `wait`. Это означает, что оно не будет порождать задач на выполнение резервного копирования, пока администратор RuBackup не запустит его (тогда его статус сменится на `run`). 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 11).

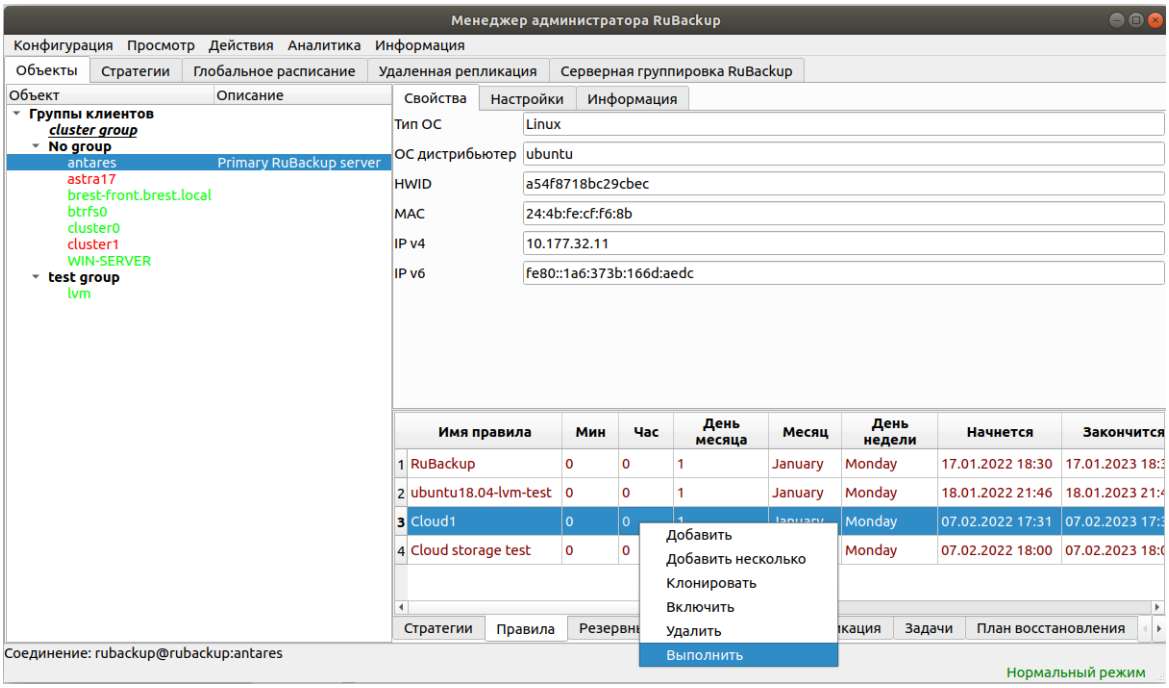
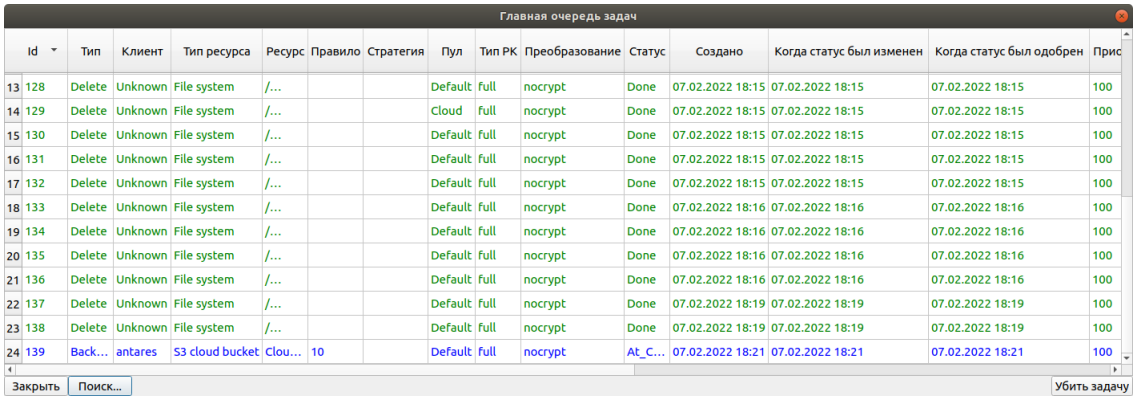


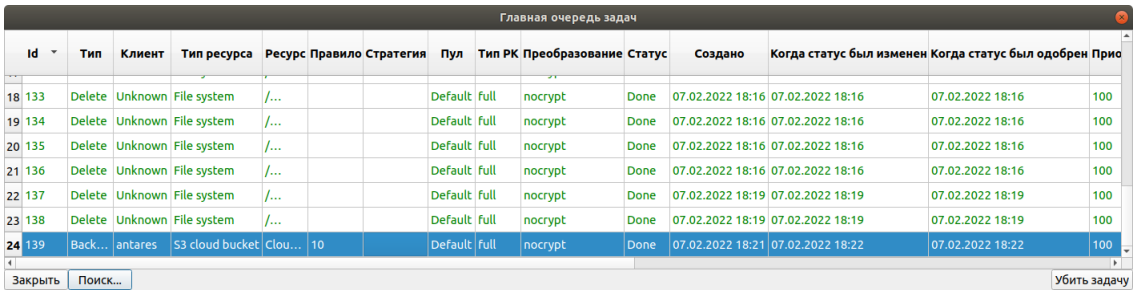
Рисунок 11

Проверить ход выполнения резервного копирования можно в окне «Главная очередь задач» (рисунок 12).



	Id	Тип	Клиент	Тип ресурса	Ресурс	Правило	Стратегия	Пул	Тип РК	Преобразование	Статус	Создано	Когда статус был изменен	Когда статус был одобрен	Прио
13	128	Delete	Unknown	File system	/...			Default	full	nocrypt	Done	07.02.2022 18:15	07.02.2022 18:15	07.02.2022 18:15	100
14	129	Delete	Unknown	File system	/...			Cloud	full	nocrypt	Done	07.02.2022 18:15	07.02.2022 18:15	07.02.2022 18:15	100
15	130	Delete	Unknown	File system	/...			Default	full	nocrypt	Done	07.02.2022 18:15	07.02.2022 18:15	07.02.2022 18:15	100
16	131	Delete	Unknown	File system	/...			Default	full	nocrypt	Done	07.02.2022 18:15	07.02.2022 18:15	07.02.2022 18:15	100
17	132	Delete	Unknown	File system	/...			Default	full	nocrypt	Done	07.02.2022 18:15	07.02.2022 18:15	07.02.2022 18:15	100
18	133	Delete	Unknown	File system	/...			Default	full	nocrypt	Done	07.02.2022 18:16	07.02.2022 18:16	07.02.2022 18:16	100
19	134	Delete	Unknown	File system	/...			Default	full	nocrypt	Done	07.02.2022 18:16	07.02.2022 18:16	07.02.2022 18:16	100
20	135	Delete	Unknown	File system	/...			Default	full	nocrypt	Done	07.02.2022 18:16	07.02.2022 18:16	07.02.2022 18:16	100
21	136	Delete	Unknown	File system	/...			Default	full	nocrypt	Done	07.02.2022 18:16	07.02.2022 18:16	07.02.2022 18:16	100
22	137	Delete	Unknown	File system	/...			Default	full	nocrypt	Done	07.02.2022 18:19	07.02.2022 18:19	07.02.2022 18:19	100
23	138	Delete	Unknown	File system	/...			Default	full	nocrypt	Done	07.02.2022 18:19	07.02.2022 18:19	07.02.2022 18:19	100
24	139	Back...	antares	S3 cloud bucket	Clou...	10		Default	full	nocrypt	At_C...	07.02.2022 18:21	07.02.2022 18:21	07.02.2022 18:21	100

При успешном завершении резервного копирования строка копирования будет выделена зеленым цветом (рисунок 13).



	Id	Тип	Клиент	Тип ресурса	Ресурс	Правило	Стратегия	Пул	Тип РК	Преобразование	Статус	Создано	Когда статус был изменен	Когда статус был одобрен	Прио
18	133	Delete	Unknown	File system	/...			Default	full	nocrypt	Done	07.02.2022 18:16	07.02.2022 18:16	07.02.2022 18:16	100
19	134	Delete	Unknown	File system	/...			Default	full	nocrypt	Done	07.02.2022 18:16	07.02.2022 18:16	07.02.2022 18:16	100
20	135	Delete	Unknown	File system	/...			Default	full	nocrypt	Done	07.02.2022 18:16	07.02.2022 18:16	07.02.2022 18:16	100
21	136	Delete	Unknown	File system	/...			Default	full	nocrypt	Done	07.02.2022 18:16	07.02.2022 18:16	07.02.2022 18:16	100
22	137	Delete	Unknown	File system	/...			Default	full	nocrypt	Done	07.02.2022 18:19	07.02.2022 18:19	07.02.2022 18:19	100
23	138	Delete	Unknown	File system	/...			Default	full	nocrypt	Done	07.02.2022 18:19	07.02.2022 18:19	07.02.2022 18:19	100
24	139	Back...	antares	S3 cloud bucket	Clou...	10		Default	full	nocrypt	Done	07.02.2022 18:21	07.02.2022 18:22	07.02.2022 18:22	100

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”).

Для защиты облаков S3 рекомендуется включать на клиенте функцию централизованного восстановления, т.к. клиент обычно устанавливается на прокси-хосте или виртуальной машине.

В тех случаях, когда централизованное восстановление на клиенте доступно, то его можно инициировать, вызвав правой кнопкой мыши контекстное меню «Восстановить» (рисунок 14).

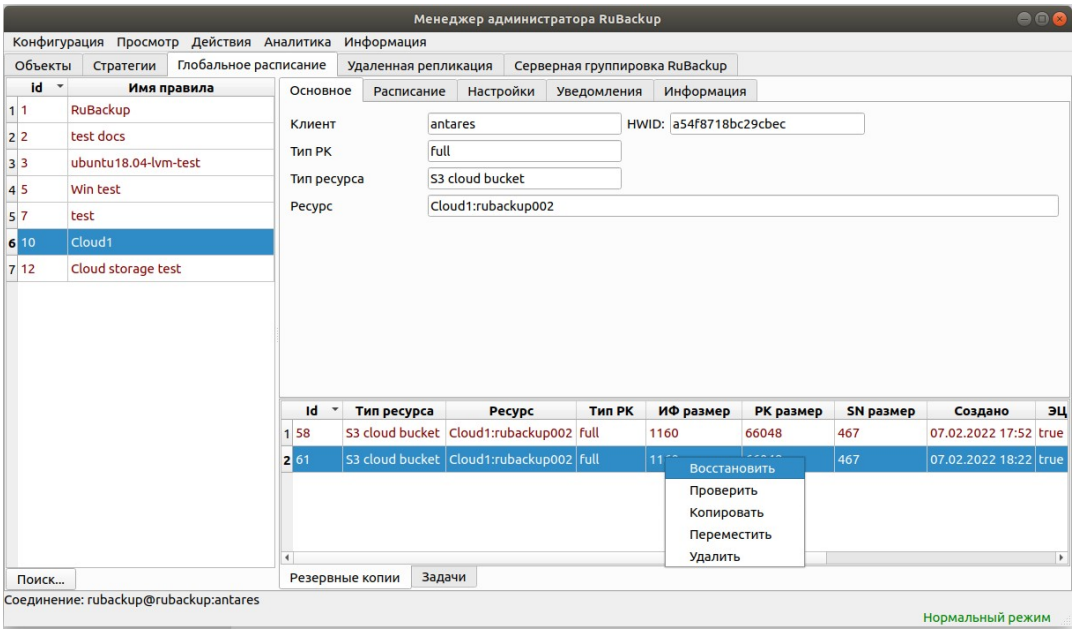


Рисунок 14

В окне централизованного восстановления можно увидеть основные параметры резервной копии и, если это применимо, определить место восстановления резервной копии. В случае восстановления бакета облака S3 объекты, находящиеся в резервной копии, будут восстановлены в

существующий бакет, а если его не существует, то будет произведена попытка создания такого бакета (рисунок 15).

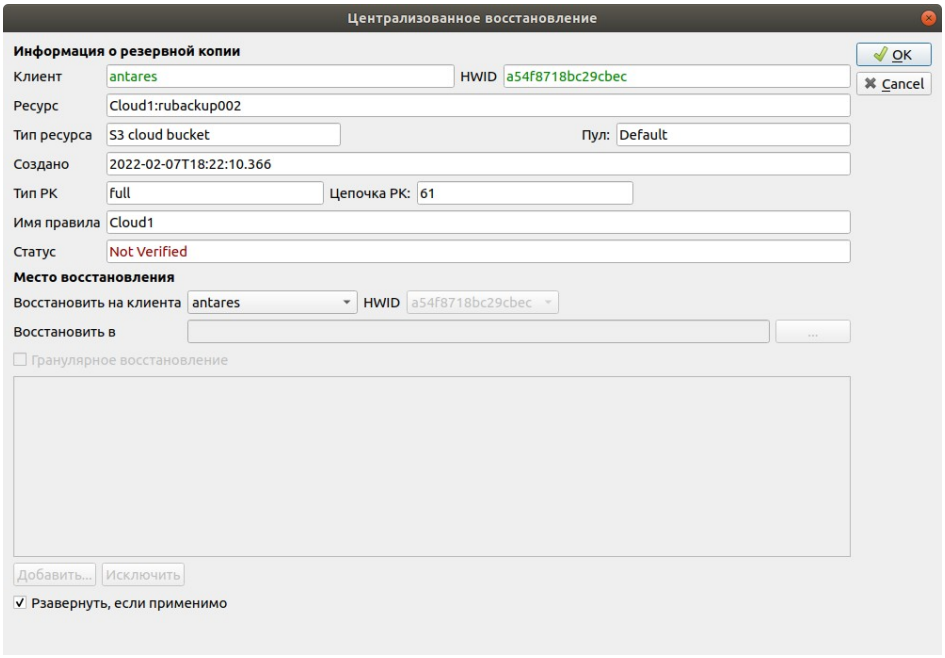


Рисунок 15

Проверить ход выполнения восстановления резервной копии можно в окне «Главная очередь задач» (рисунок 16).

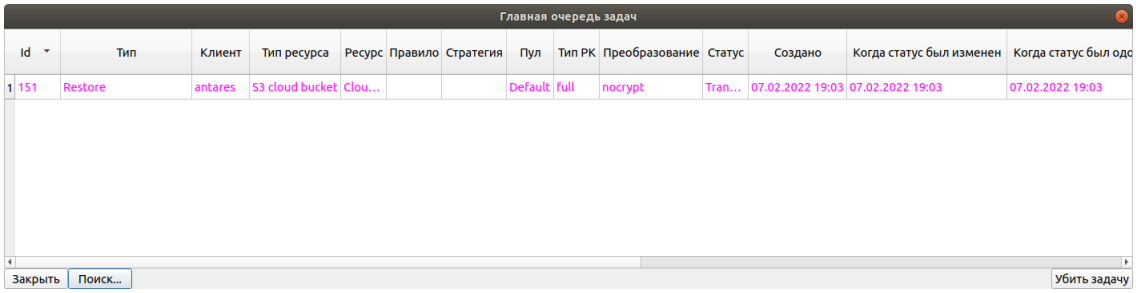


Рисунок 16

При успешном завершении восстановления бакета в облако S3 строка будет выделена зеленым цветом (рисунок 17).

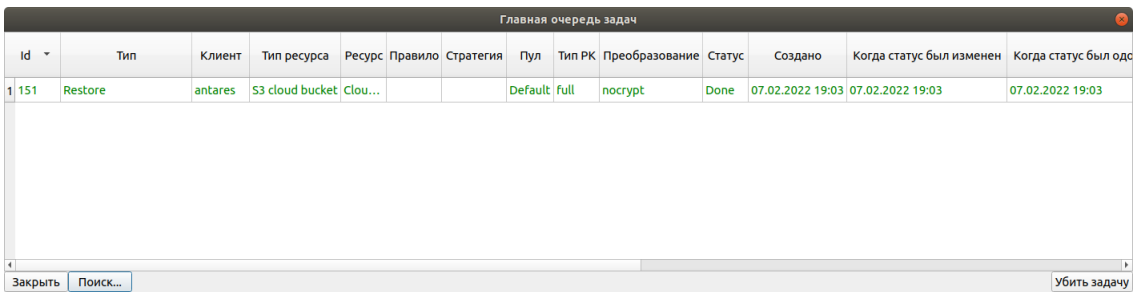


Рисунок 17