

**RuBackup**

Система резервного копирования и восстановления данных

**RuBackup key**

**Руководство пользователя**



**RuBackup**

Версия 2.1

13.06.2024 г.

# Содержание

Введение.....	3
Ограничения.....	4
Подготовка к созданию спасательного образа.....	5
Создание спасательного образа.....	6
Мониторинг процесса создания спасательного образа.....	11
Мониторинг через RuBackup key.....	11
Мониторинг через RBM.....	11
Создание пароля для RuBackup key для восстановления системы с помощью спасательного образа.....	12
Восстановление системы с помощью спасательного образа.....	13
Восстановление системы с использованием плана аварийного восстановления (DRP).....	19
Мониторинг процесса восстановления системы с помощью спасательного образа.....	21
Мониторинг через RuBackup key.....	21
Мониторинг через RBM.....	21

## Введение

RuBackup key — специализированный загрузочный образ RuBackup, с помощью которого осуществляется создание спасательного образа и восстановление системы. Спасательный образ – это резервная копия операционной системы Linux или ее части, располагающейся на виртуальной машине или «голом железе», с возможностью их быстрого восстановления в случае возникновения аварийных ситуаций.

## Ограничения

- Объем оперативной памяти не менее 8 ГБ.
- В рамках релиза «2.0 U2 HF 1 RuBackup key» поддерживается только операционная система Astra Linux SE 1.7.3.
- Восстановление системы происходит на один диск (одно устройство: sda, vda и т.п.), даже если резервное копирование делалось для системы, расположенной на нескольких устройствах.
- Поддерживаемые файловые системы: ext2, ext3, ext4, VFAT и XFS.
- RuBackup key не поддерживает резервное копирование и восстановление LVM-томов.
- Система имеет один файл подкачки (swap), который располагается либо в отдельном дисковом разделе, либо в файле.
- RuBackup key создает спасательный образ одной конкретной операционной системы Linux.
- Клиентские логи процессов создания и восстановления спасательного образа не будут доступны после перезагрузки системы на загрузочном диске с образом RuBackup key.

При создании спасательной резервной копии из нее исключаются:

- мастер ключ RuBackup;
- пара ключей электронной подписи RuBackup;
- содержимое следующих каталогов:
  - lost+found;
  - /proc;
  - /sys;
  - /tmp;
  - /boot/efi.

## Подготовка к созданию спасательного образа

Для возможности создания спасательного образа в системе должен быть установлен клиент RuBackup и этот клиент должен быть авторизован в системе резервного копирования. При восстановлении потребуются ввести пароль клиента, он должен быть заранее установлен.

Порядок установки, инсталляции, настройки, запуска клиента RuBackup, а также авторизации клиента на сервере резервного копирования изложен в документе «Руководство по установке системы резервного копирования RuBackup для серверов резервного копирования и Linux-клиентов».

Рекомендуется сразу после установки клиента скопировать master key и ключи электронной подписи в надежное место. Ключи расположены в каталоге /opt/rubackup/keys.

Файлы спасательного образа записываются в пул по умолчанию, который был указан при конфигурации сервера.

## Создание спасательного образа

Для создания спасательного образа RuBackup key выполните следующие шаги:

1. Присоедините диск с загрузочным образом RuBackup key к хосту клиента.
2. Запустите загрузочный образ RuBackup key.
3. Добавьте запись о сервере RuBackup в /etc/hosts (Рисунок 1).

```
127.0.0.1 localhost
127.0.1.1 lubuntu
192.168.7.226 server_hostname
# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

Рисунок 1

4. Выберите язык, сетевой интерфейс и иницируйте начало работы с RuBackup key.

Откроется окно RuBackup key (Рисунок 2).

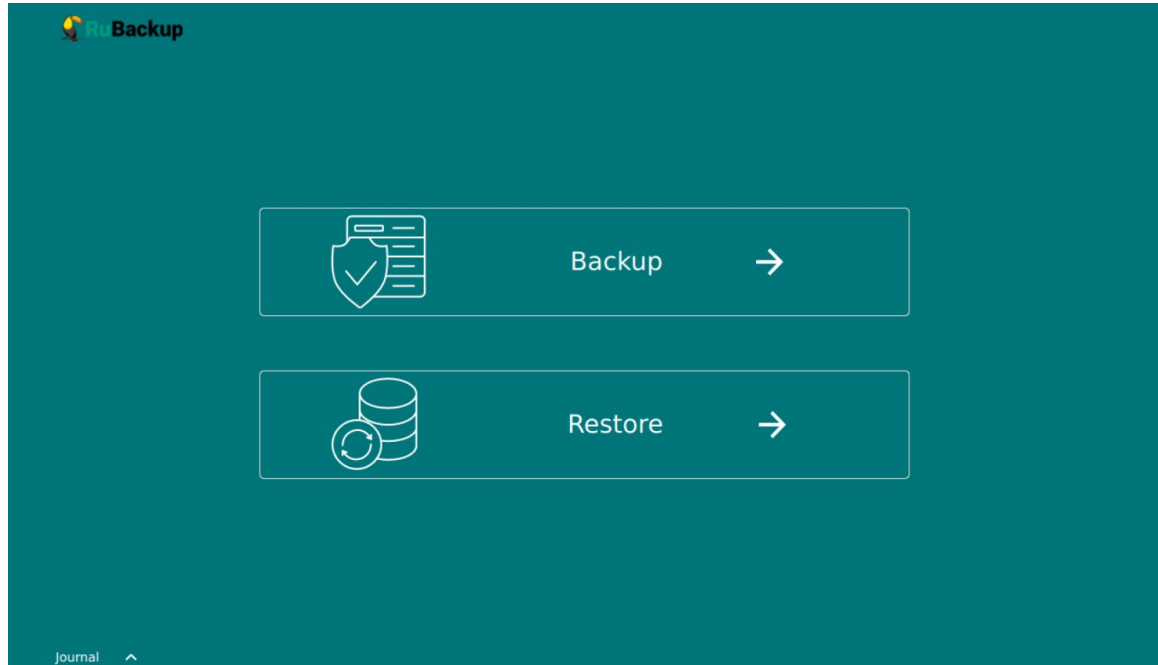


Рисунок 2

При необходимости просмотра логов, в левом нижнем углу нажмите кнопку «journal».

Внимание! Повторный запуск приложения осуществляется только через графический интерфейс.

5. Для создания спасательного образа нажмите кнопку «Backup».

6. Выберите физический диск, на котором расположена операционная система, образ которой необходимо создать (Рисунок 3).
7. При необходимости выберите тип защитного преобразования.

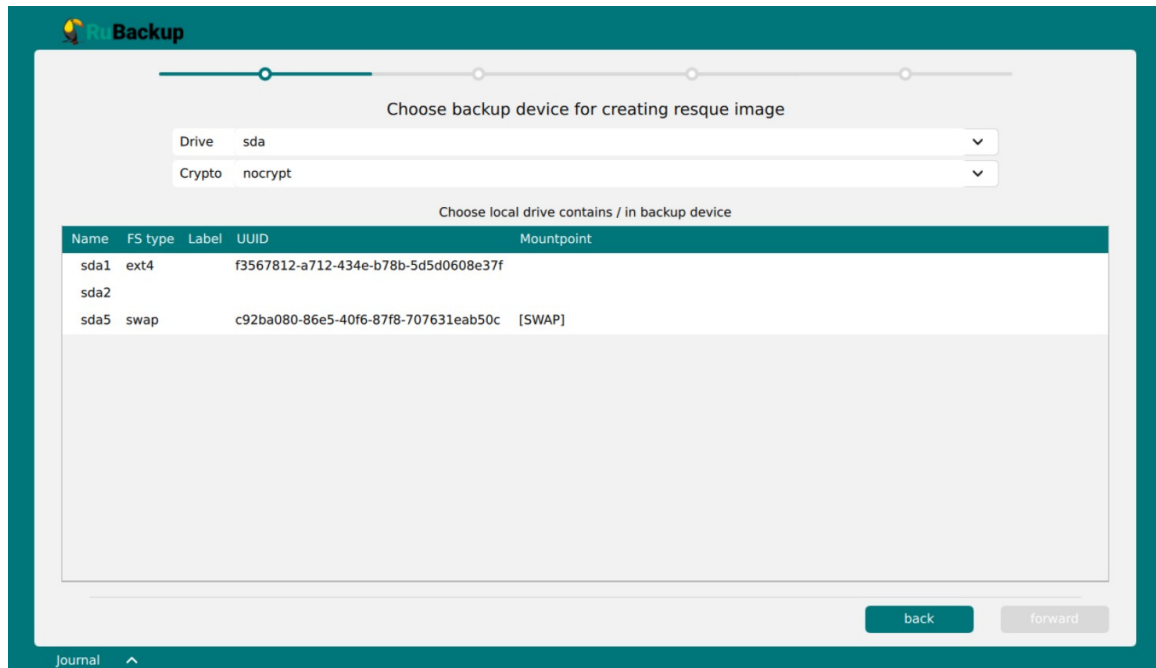


Рисунок 3



8. Выберите локальный диск, где расположен корень «/» операционной системы (Рисунок 4).

*Примечание: Если выбрать не тот локальный диск (например, пустой или не содержащий корень операционной системы), Система отобразит сообщение с предупреждением.*

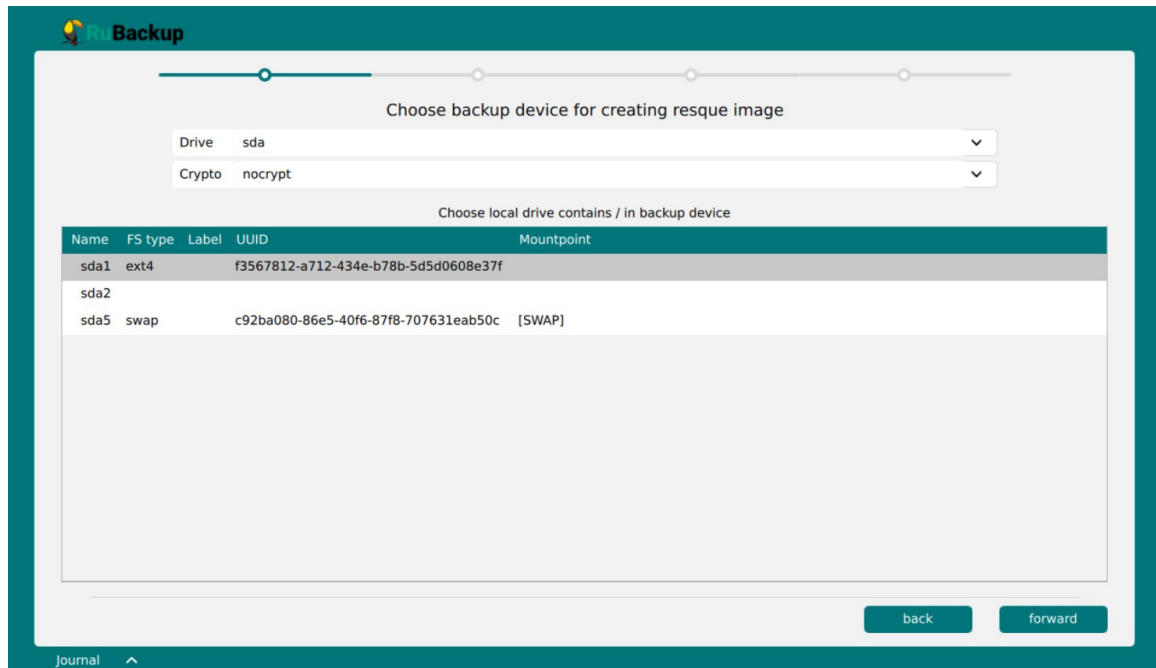


Рисунок 4

9. Для перехода к следующему этапу нажмите кнопку «forward».

RuBackup key по fstab находит локальные диски, относящиеся к выбранной операционной системе.

10. Среди предложенных локальных дисков выберите те, которые необходимо включить в спасательный образ, обязательно включая локальный диск, содержащий корень операционной системы (Рисунок 5).

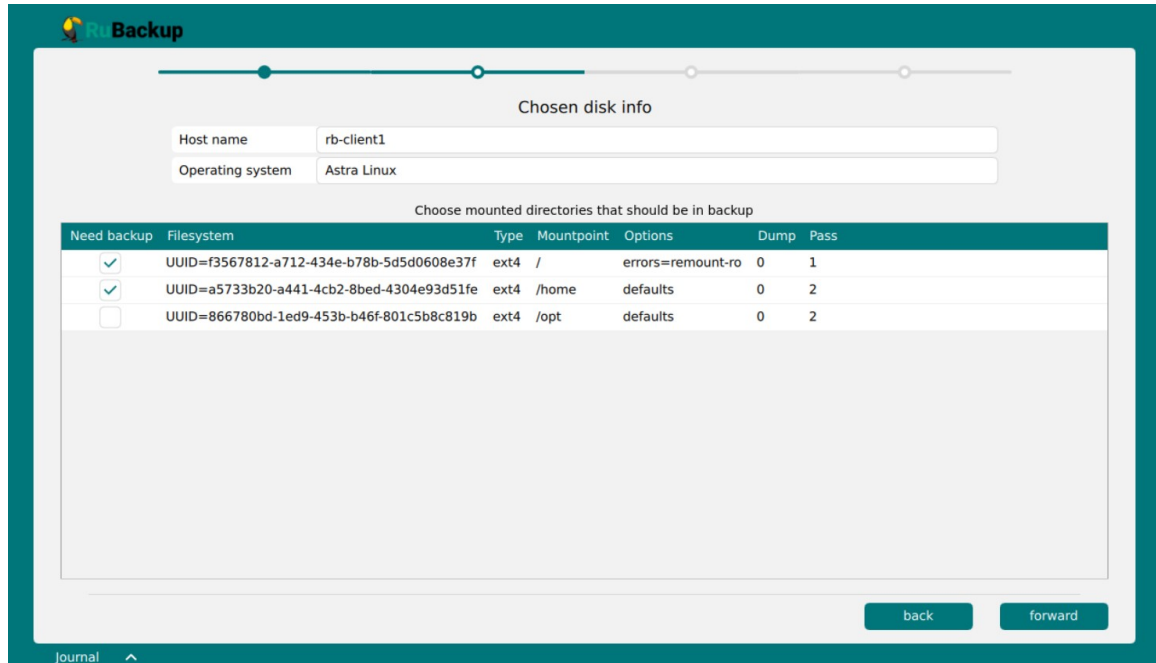
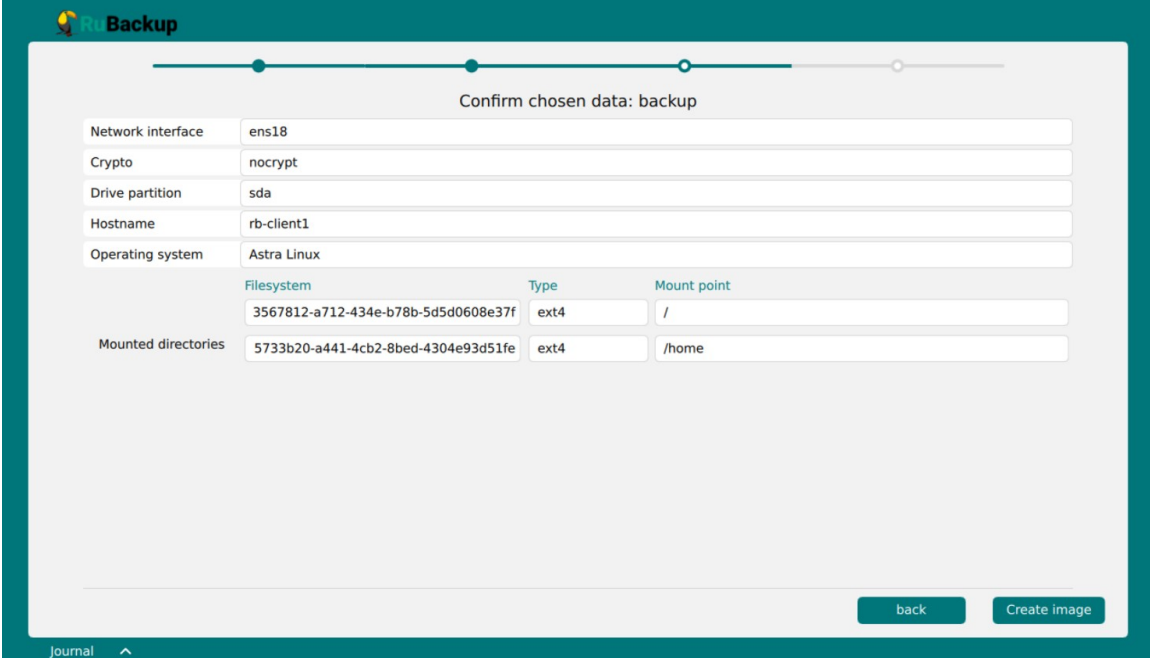


Рисунок 5

11. Для перехода к следующему этапу нажмите кнопку «forward».

12. Подтвердите выбранные параметры и запустите создание спасательного образа, нажав кнопку «Create image» (Рисунок 6).



Field	Value	
Network interface	ens18	
Crypto	nocrypt	
Drive partition	sda	
Hostname	rb-client1	
Operating system	Astra Linux	
Filesystem	Type	Mount point
3567812-a712-434e-b78b-5d5d0608e37f	ext4	/
Mounted directories	Type	Mount point
5733b20-a441-4cb2-8bed-4304e93d51fe	ext4	/home

Рисунок 6

13. После успешного создания спасательного образа для продолжения работы на хосте клиента необходимо его выключить и загрузиться со штатного диска.

# Мониторинг процесса создания спасательного образа

## Мониторинг через RuBackup key

Для отслеживания процесса создания спасательного образа через интерфейс RuBackup key откройте журнал в RuBackup key.

## Мониторинг через RBM

Для отслеживания процесса создания спасательного образа через интерфейс RBM выполните следующие шаги:

1. Аутентифицируйтесь в RBM;
2. Перейдите в раздел «Очередь задач»;
3. Найдите задачу по созданию спасательного образа;
4. Отслеживайте процесс создания спасательного образа.

## **Создание пароля для RuBackup key для восстановления системы с помощью спасательного образа**

Для создания пароля для RuBackup key выполните следующие шаги:

1. Аутентифицируйтесь в RBM под учетной записью Суперпользователя СРК;
2. Перейдите в раздел «Глобальная конфигурация»;
3. В подразделе «Ключ RuBackup» задайте пароль для RuBackup key для восстановления системы с помощью спасательного образа;
4. Примените изменения глобальной конфигурации.

*Примечание: Ключ RuBackup не имеет отношения к паролям от RBM или RBC, это пароль для RuBackup key.*

## Восстановление системы с помощью спасательного образа

**Внимание!** Перед восстановлением системы с помощью RuBackup key необходимо в глобальной конфигурации сервера задать ключ RuBackup, являющийся паролем RuBackup key.

**Внимание!** Только Суперпользователь СРК может инициировать восстановление системы с помощью спасательного образа, поскольку только ему известен пароль для RuBackup key.

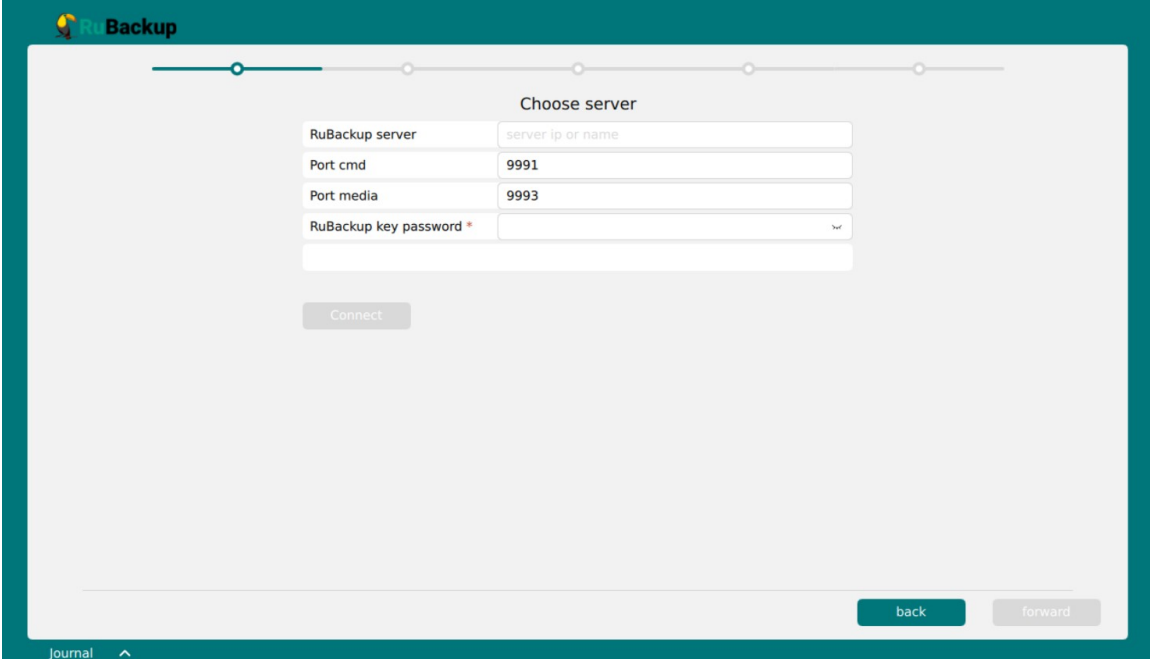
Для восстановления с помощью спасательного образа выполните следующие шаги:

1. Присоедините диск с загрузочным образом RuBackup key к хосту клиента.
2. Запустите загрузочный образ RuBackup key.
3. Добавьте запись о сервере RuBackup в /etc/hosts (Рисунок 1).
4. Выберите язык и сетевой интерфейс и инициируйте начало работы с RuBackup key.

Откроется окно RuBackup key.

5. Для восстановления спасательного образа нажмите кнопку «Restore» (Рисунок 2).
6. Введите адрес основного сервера RuBackup, порты, пароль от RuBackup key и иницируйте подключение, нажав кнопку «Connect» (Рисунок 7).

*Примечание: может потребоваться ручной запуск сервиса rubackup-client. Rubackup-client запускается в режиме Restore, если выполнены два условия: 1) PRETTY\_NAME=«RuBackup key» в файле /etc/os-release; 2) отсутствует конфигурационный файл в /opt/rubackup/etc/.*



**RuBackup**

Choose server

RuBackup server

Port cmd

Port media

RuBackup key password \*

Connect

back forward

Journal ^

Рисунок 7

7. Перейдите в RBM (Рисунок 8) и авторизуйте появившегося клиента `rubackup-rescue` на странице «Неавторизованные клиенты» (Рисунок 9).

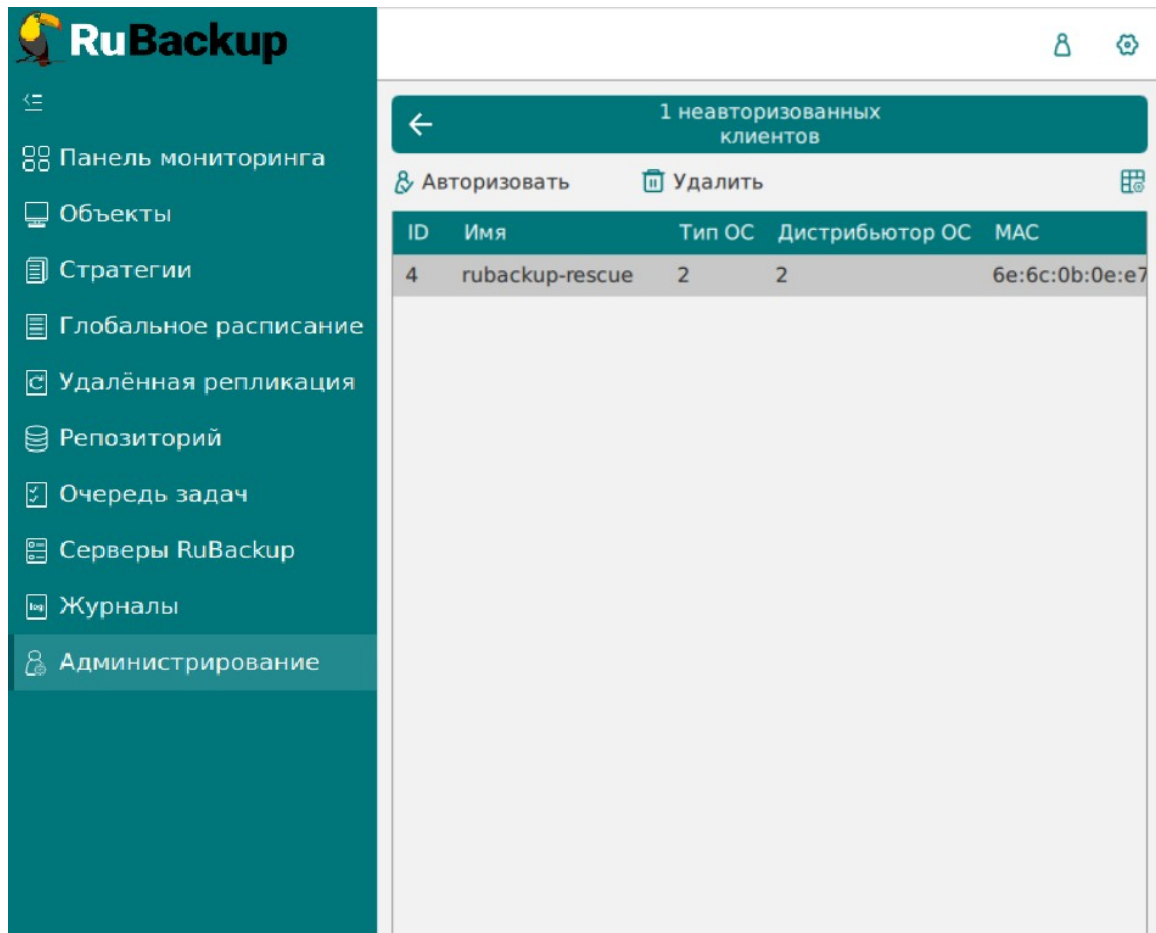


Рисунок 8



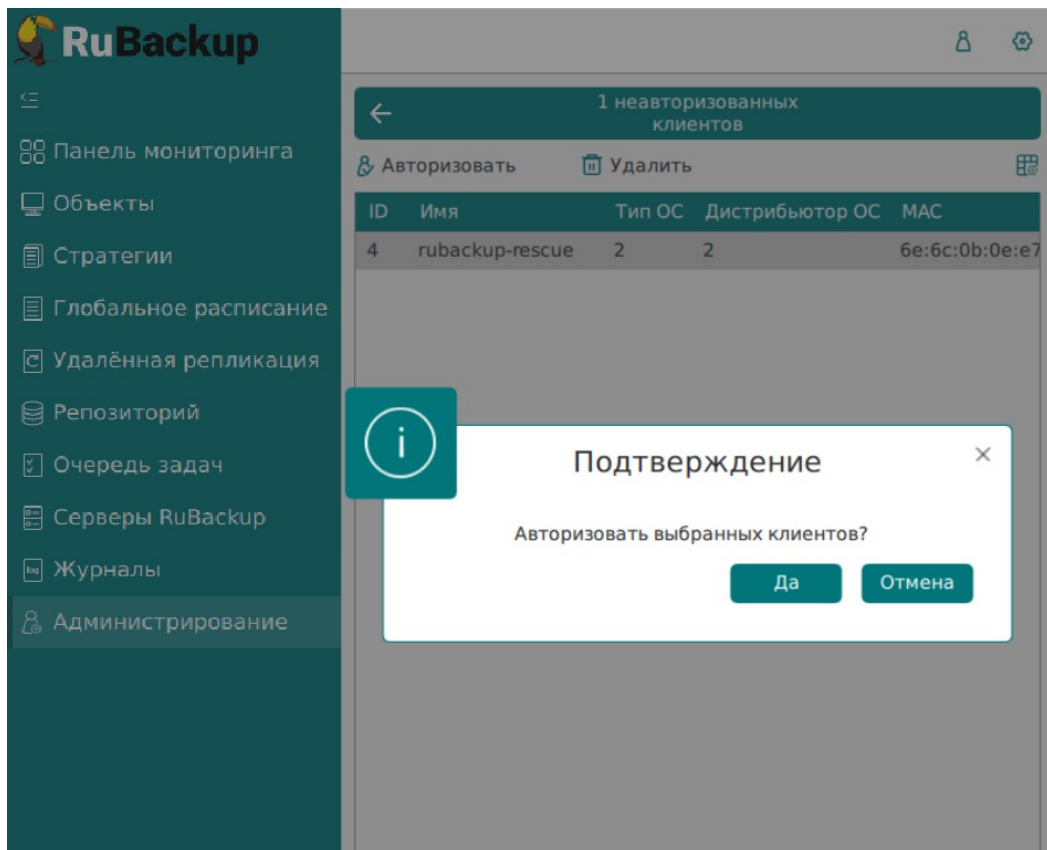


Рисунок 9

- В RuBackup key выберите клиента, резервную копию которого необходимо восстановить, и спасательный образ, принадлежащий данному Клиенту и нажмите кнопку «forward» (Рисунок 10).

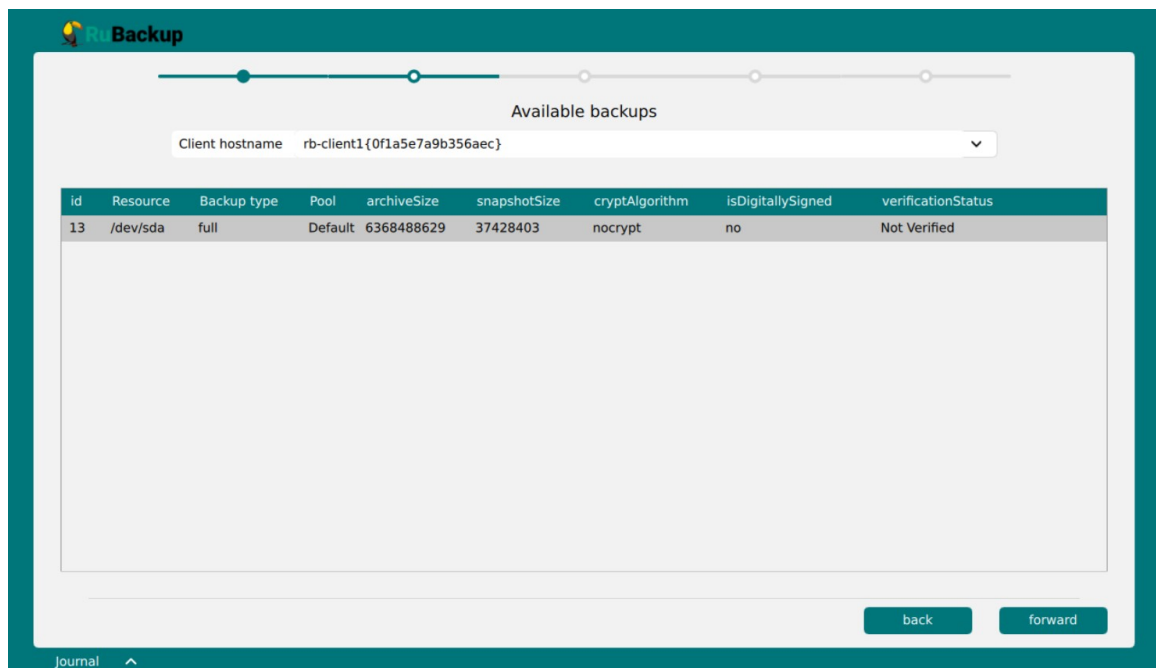


Рисунок 10

9. Выберите жесткий диск, на который будет восстановлен спасательный образ. Если спасательный образ был создан с использованием защитного преобразования добавьте ключ для расшифровки спасательного образа, нажав на кнопку «input crypt key» (Рисунок 11).
10. При необходимости использовать DRP (план аварийного восстановления) нажмите кнопку «Tune DRP». Сценарий с использованием DRP описан в разделе Восстановление системы с использованием плана аварийного восстановления (DRP).
11. Введите пароль клиента RuBackup, который был выбран в пункте 9 и нажмите кнопку «forward».

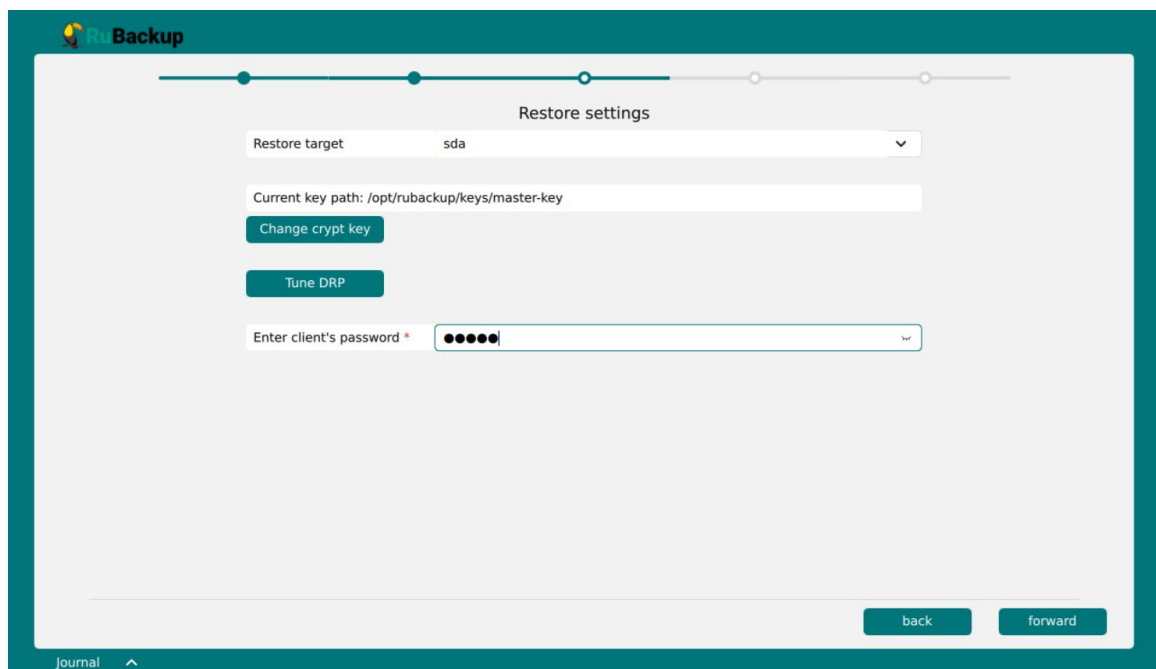
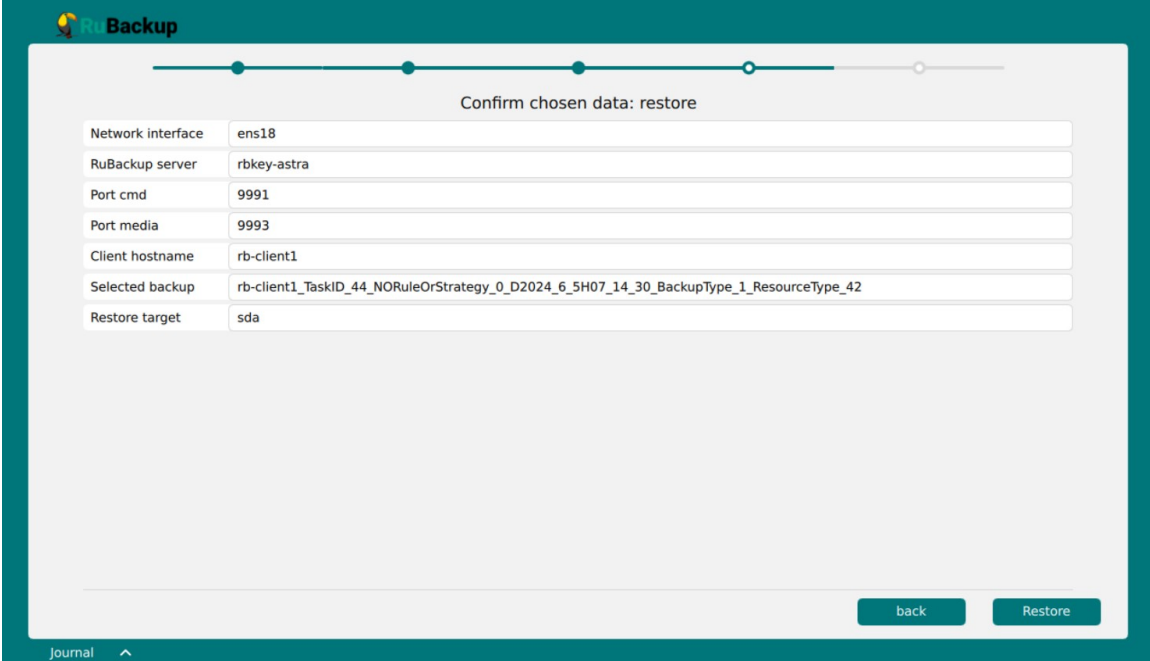


Рисунок 11

12. Проверьте введенные данные и нажмите кнопку «Restore» (Рисунок 12).



Confirm chosen data: restore	
Network interface	ens18
RuBackup server	rbkey-astra
Port cmd	9991
Port media	9993
Client hostname	rb-client1
Selected backup	rb-client1_TaskID_44_NORuleOrStrategy_0_D2024_6_5H07_14_30_BackupType_1_ResourceType_42
Restore target	sda

back Restore

Journal ^

Рисунок 12

13. Дождитесь восстановления системы с помощью спасательного образа RuBackup key.
14. После успешного восстановления спасательного образа для продолжения работы на хосте клиента нужно его выключить и загрузиться со штатного диска.

## Восстановление системы с использованием плана аварийного восстановления (DRP)

Для восстановления системы с использованием плана аварийного восстановления (DRP) выполните следующие шаги:

1. При выборе параметров восстановления в окне выбора жёсткого диска, на который будет восстановлен спасательный образ, нажмите кнопку «Tune DRP» для настройки восстановления через план аварийного восстановления (Рисунок 13).

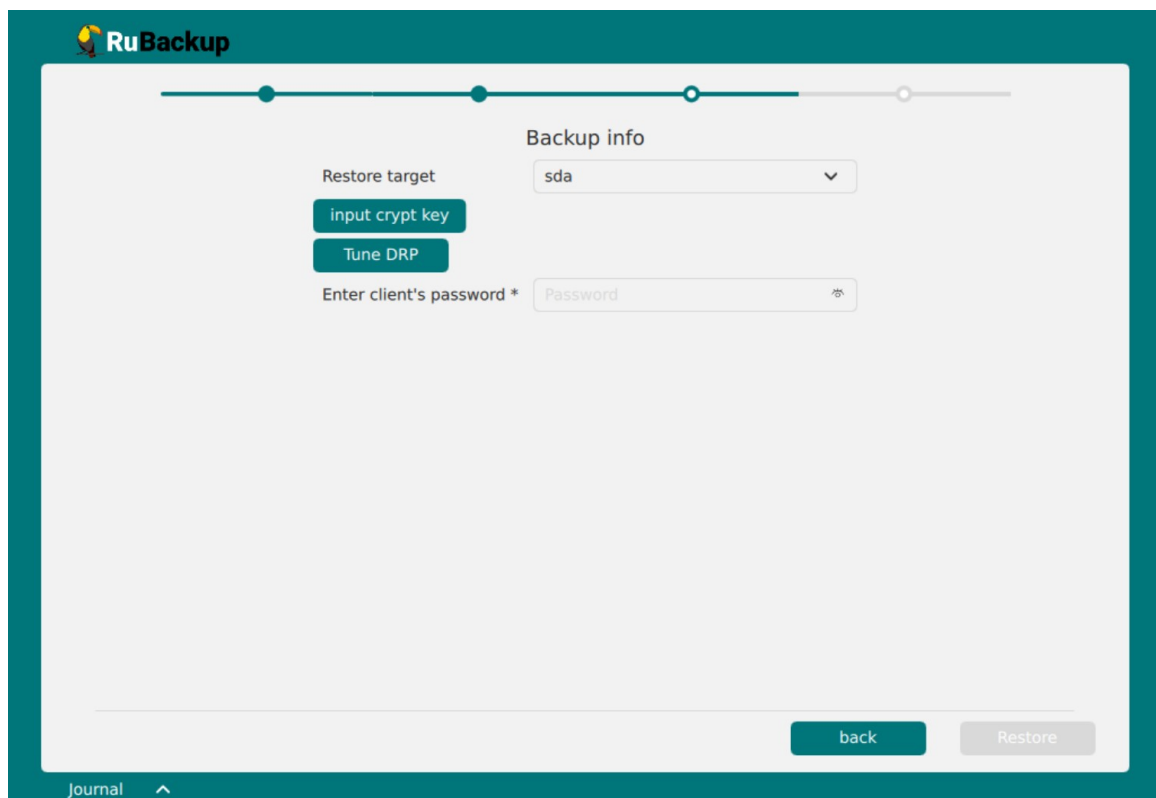


Рисунок 13

2. В открывшемся окне выберите необходимый план аварийного восстановления и резервные копии, которые необходимо восстановить (Рисунок 14).

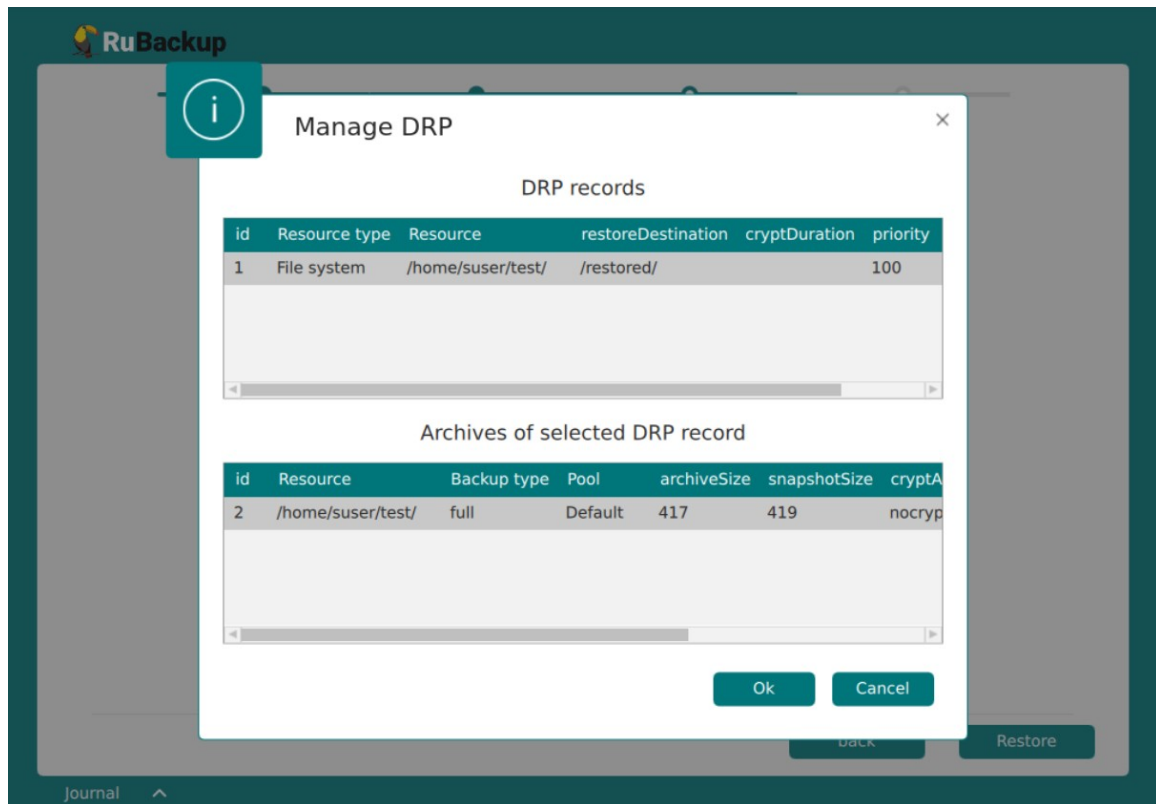


Рисунок 14

3. После применения данной настройки необходимо продолжить процесс восстановления спасательного образа по инструкции (см. раздел Восстановление системы с помощью спасательного образа).
4. После восстановления спасательного образа, в очереди задач менеджера администратора RBM появятся задачи в статусе «New», созданные в соответствии с заданным DRP.
5. Перезагрузите хост с диска, на котором было произведено восстановление спасательного образа.
6. В момент, когда клиентский процесс будет запущен на восстановленном хосте, задачи во вкладке «Очередь задач», связанные с этим клиентом, начнут выполняться.

# Мониторинг процесса восстановления системы с помощью спасательного образа

## Мониторинг через RuBackup key

Для отслеживания процесса восстановления с помощью спасательного образа через интерфейс RuBackup key откройте журнал в RuBackup key.

## Мониторинг через RBM

Для отслеживания процесса создания спасательного образа через интерфейс RBM выполните следующие шаги:

1. Аутентифицируйтесь в RBM.
2. Перейдите в раздел «Очередь задач».
3. Найдите задачу по по восстановлению системы.
4. Отслеживайте процесс восстановления.