RuBackup
Система резервного копирования и восстановления данных

RuBackup key
Руководство пользователя

Версия 2.0 U3

19.03.2024 г.

Содержание

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 спасательной 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 потребуется 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).

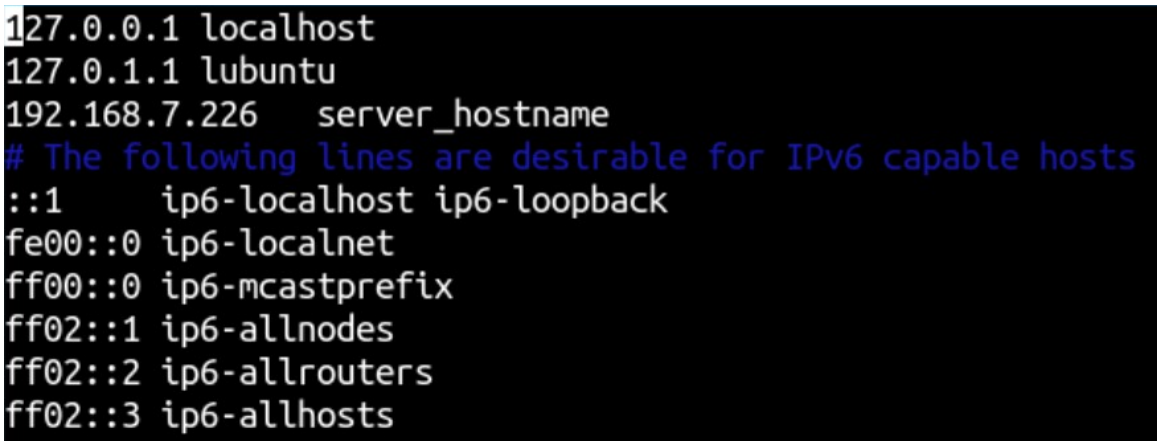

Рисунок 1

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

   Откроется окно RuBackup key (Рисунок 2).

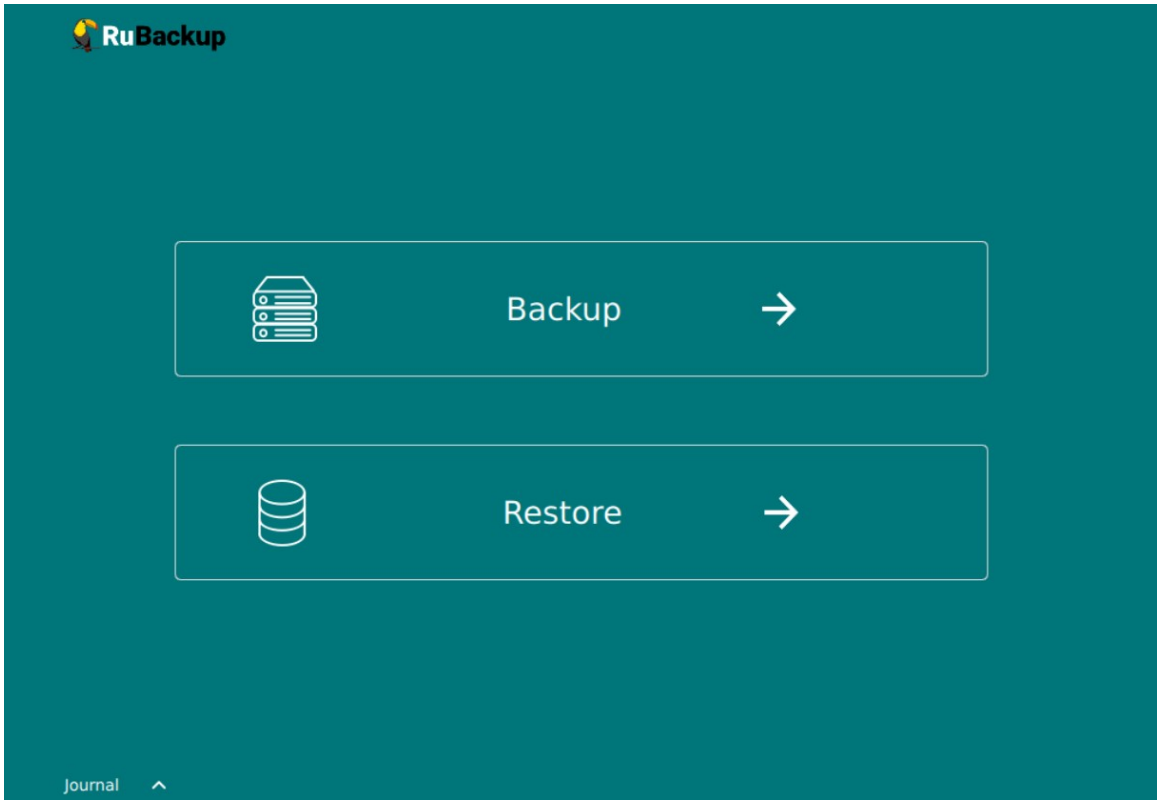

Рисунок 2

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.

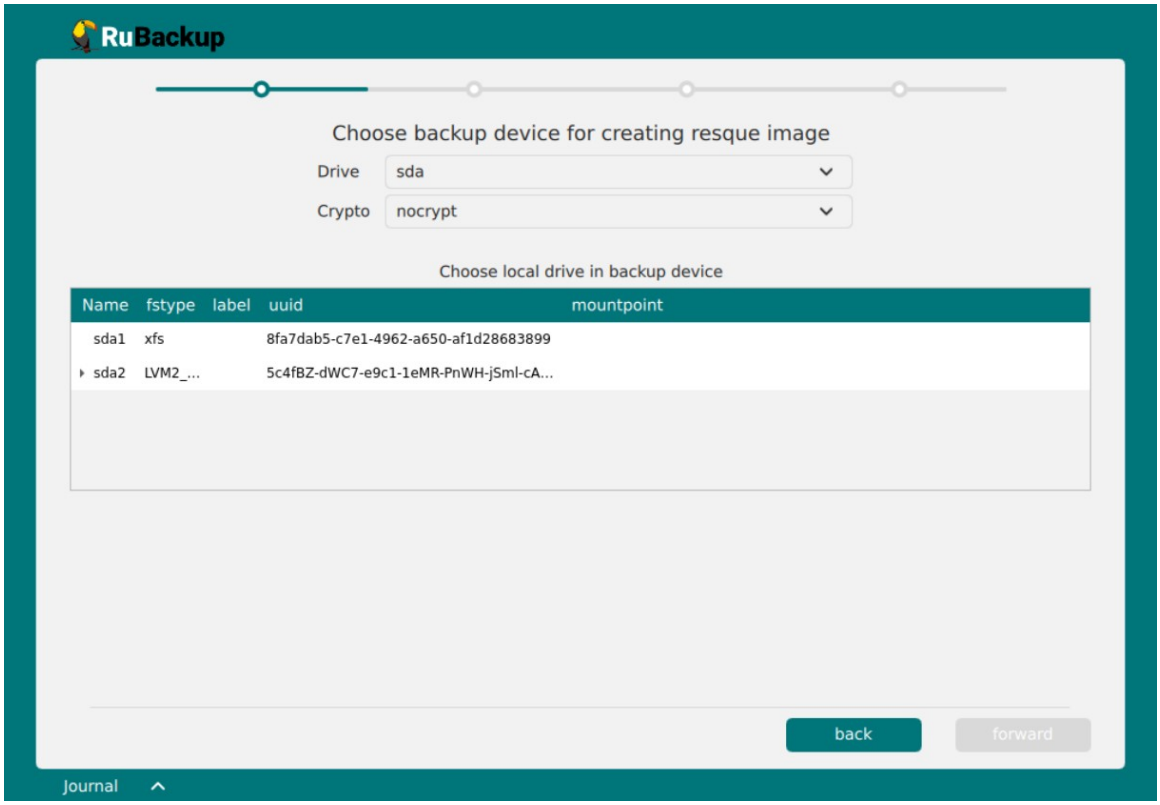

Рисунок 3

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.

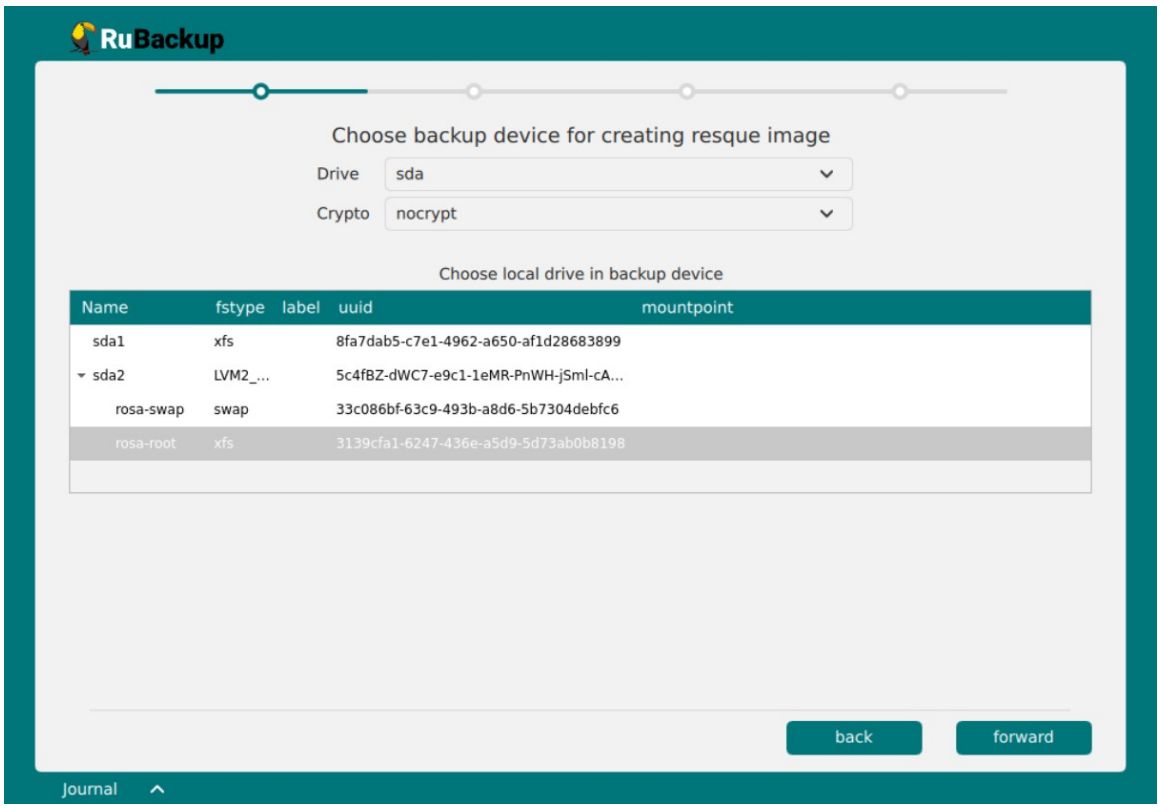

Рисунок 4

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. Выбранные локальные диски будут иметь параметр «true» в столбце «needBackup» (Рисунок 5).

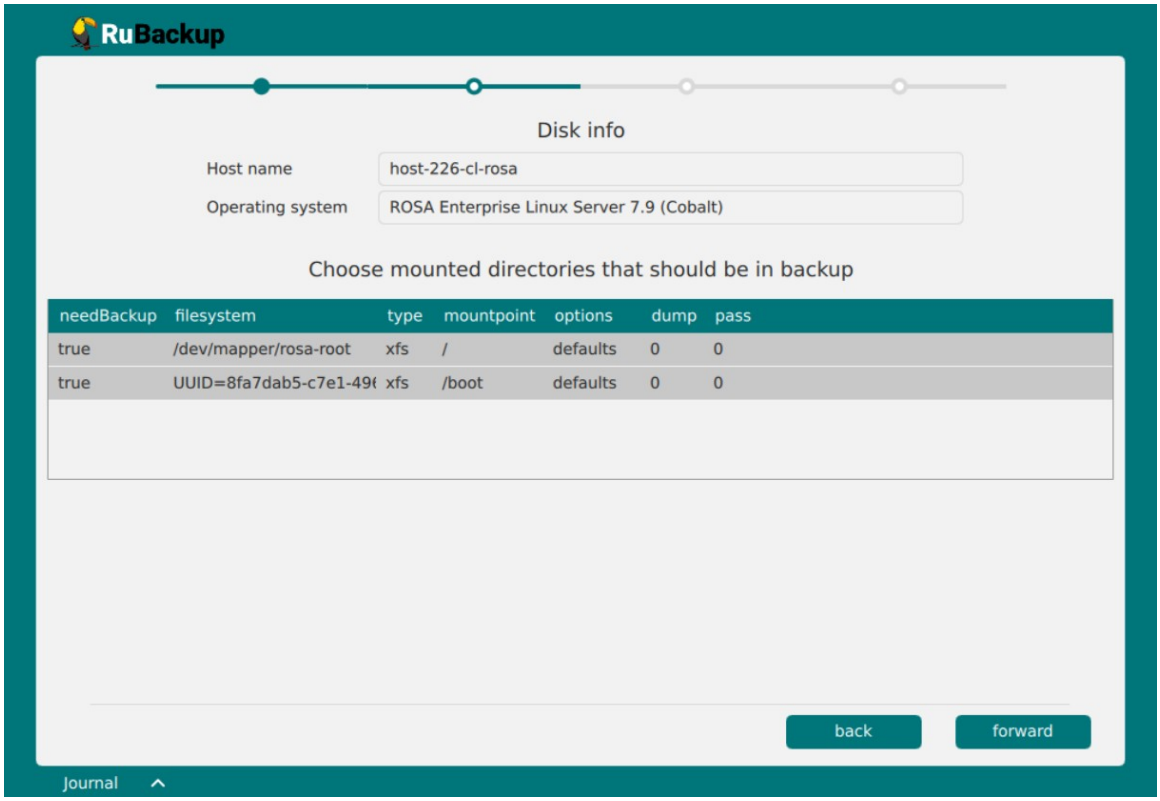

Рисунок 5

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

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

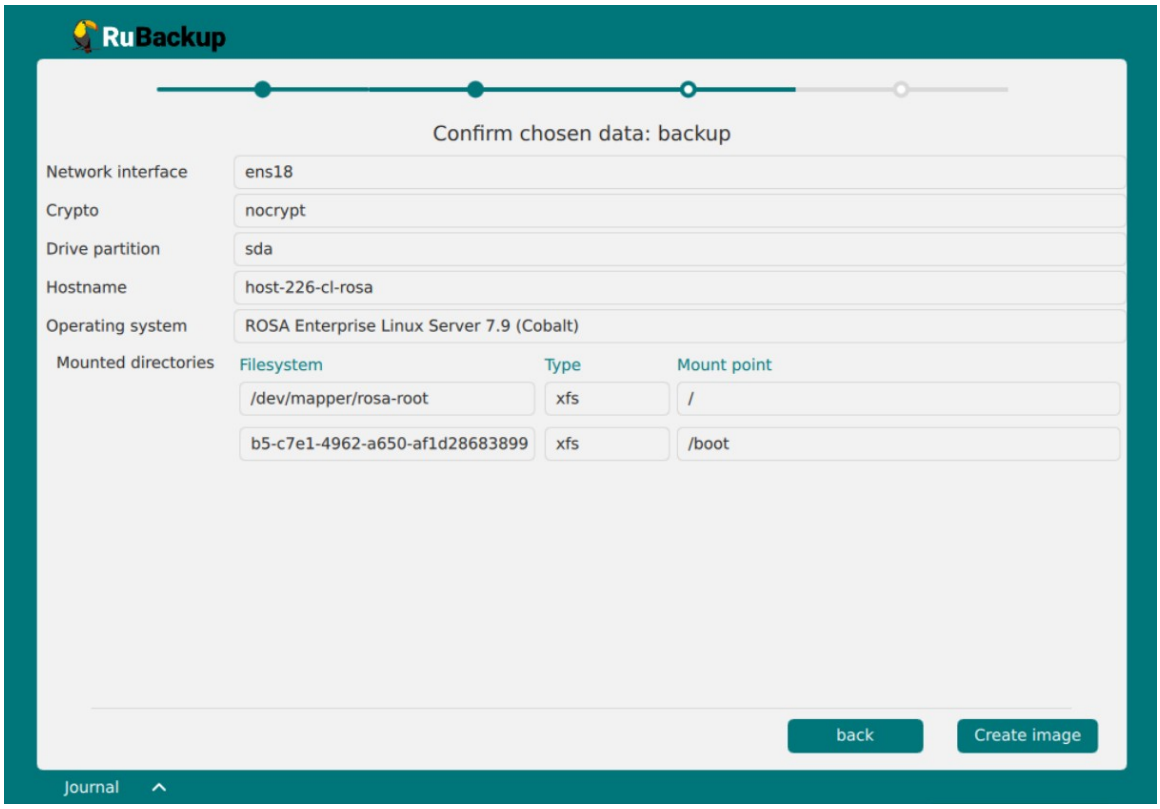

Рисунок 6

13. После успешного создания спасательного образа для продолжения работы на хосте клиента нужно 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 CPK;
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 и инициируйте 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/.

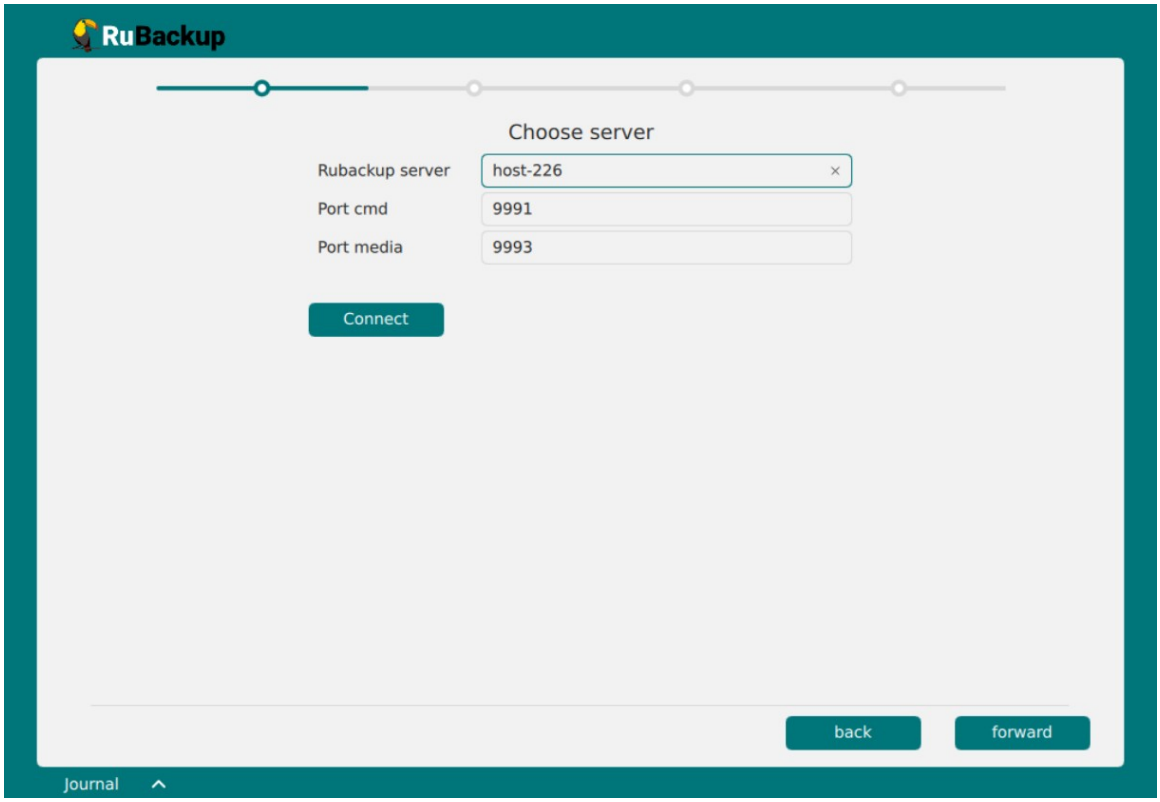

Рисунок 7

7. В открывшемся окне введите пароль для RuBackup key и нажмите кнопку «Ok» (Рисунок 8).

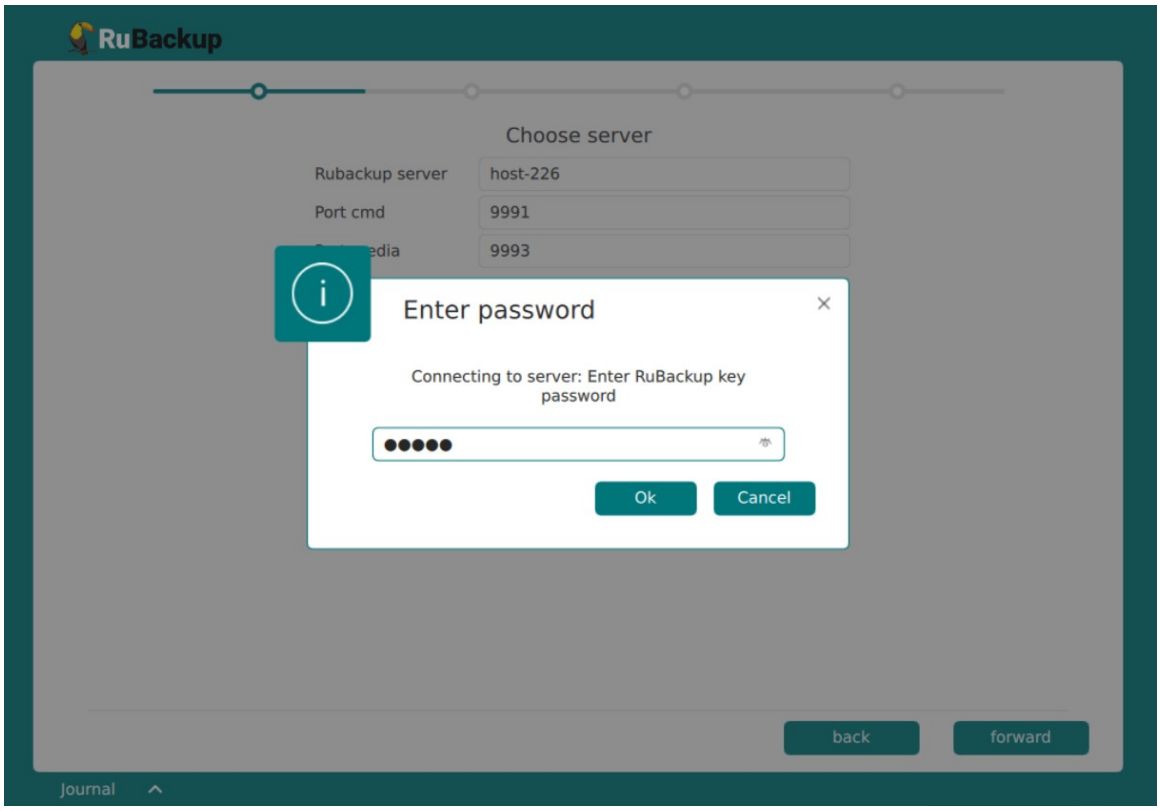

Рисунок 8

8. Перейдите в RBM (Рисунок 9) и авторизуйте появившегося клиента rubackup-rescue на странице «Неавторизованные клиенты» (Рисунок 10).

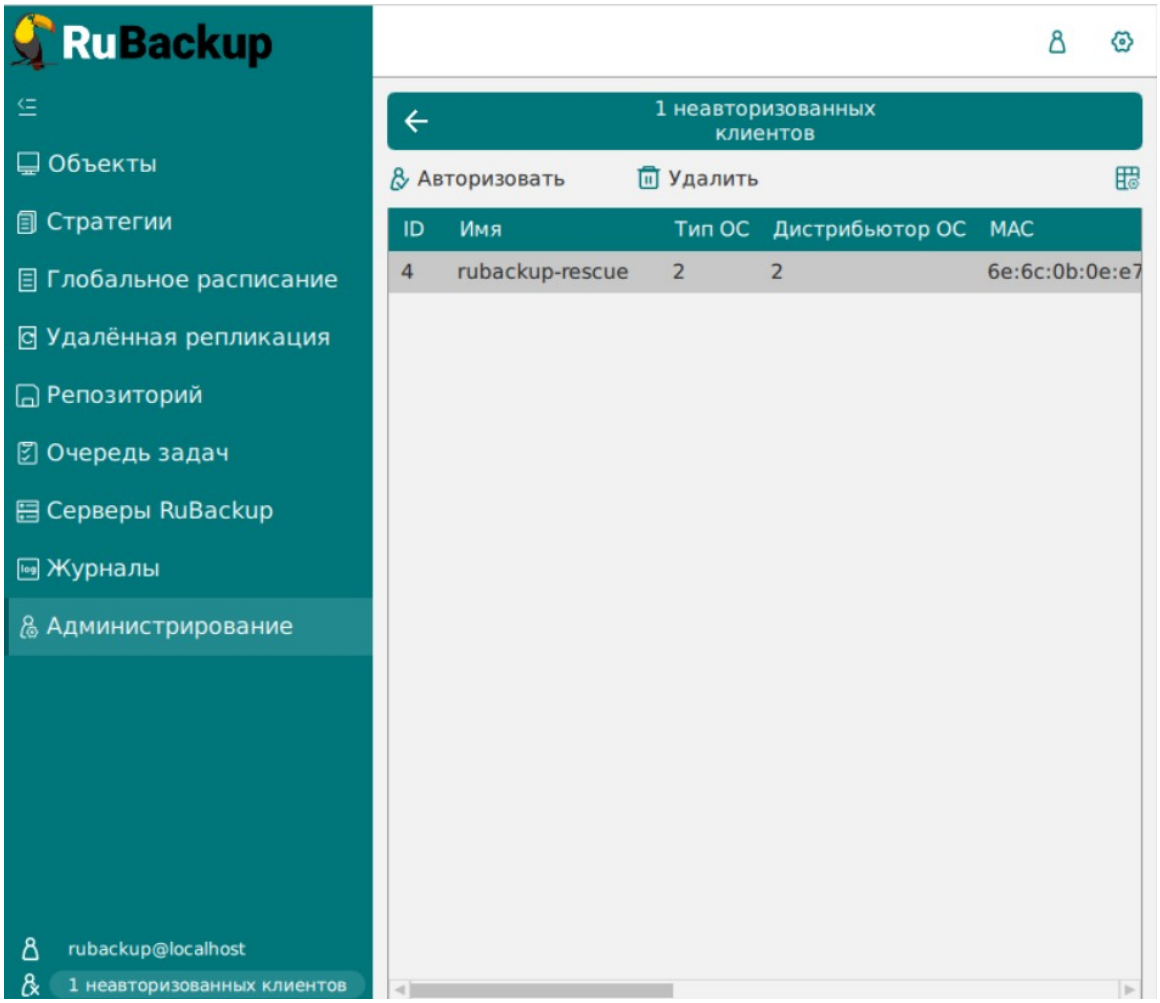

Рисунок 9

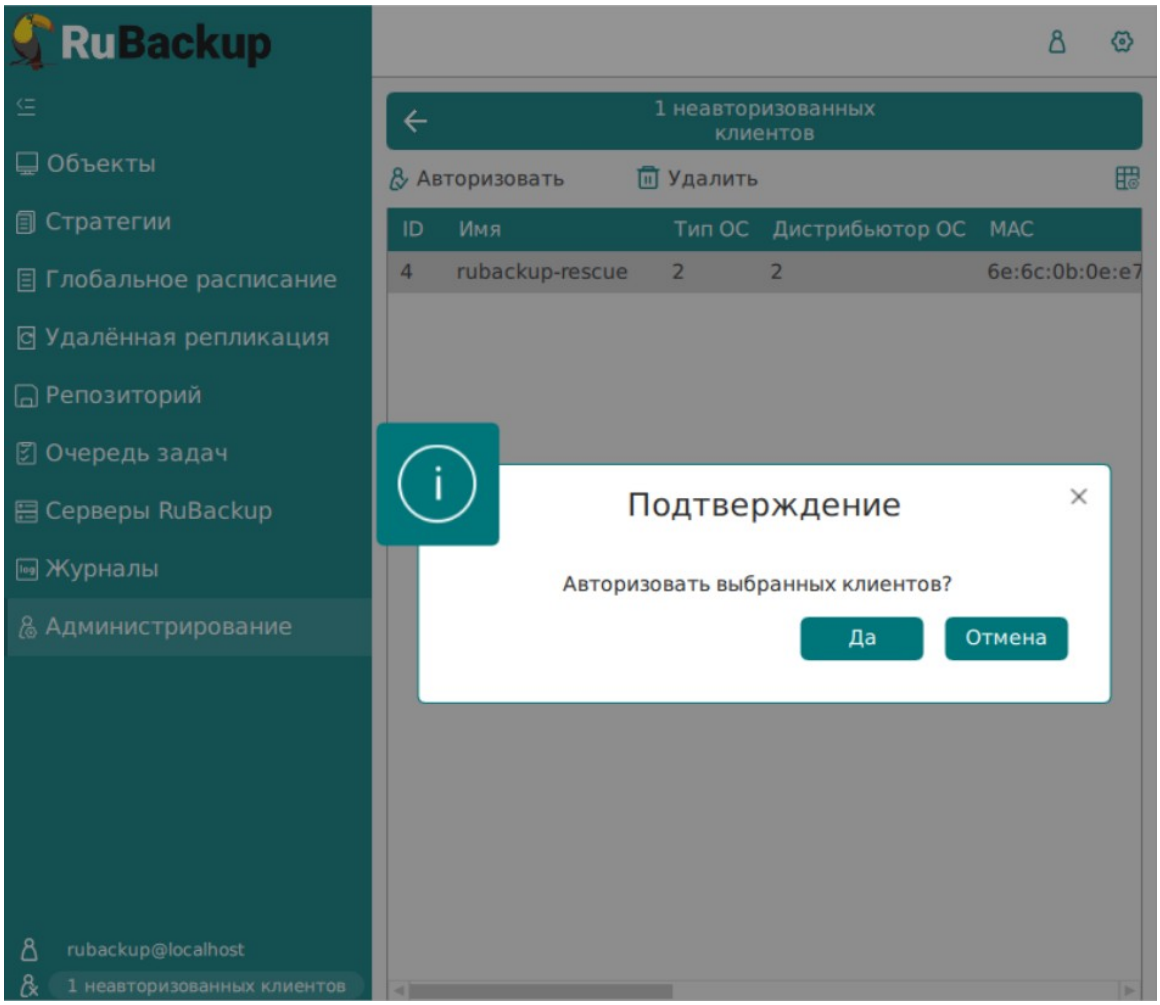
RuBackup
Объекты
Стратегии
Глобальное расписание
Удалённая репликация
Репозиторий
Очередь задач
Серверы RuBackup
Журналы
Администрирование
rubackup@localhost
1 неавторизованных клиентов
1 неавторизованных клиентов
Авторизовать
Удалить
ID
Имя
Тип ОС
Дистрибьютор ОС
MAC
4
rubackup-rescue
2
2
6e:6c:0b:0e:e7
Подтверждение
Авторизовать выбранных клиентов?
Да
Отмена

Рисунок 10

9. В RuBackup key выберите клиента, резервную копию которого необходимо восстановить, и спасательный образ, принадлежащий данному Клиенту и нажмите кнопку «forward» (Рисунок 11).

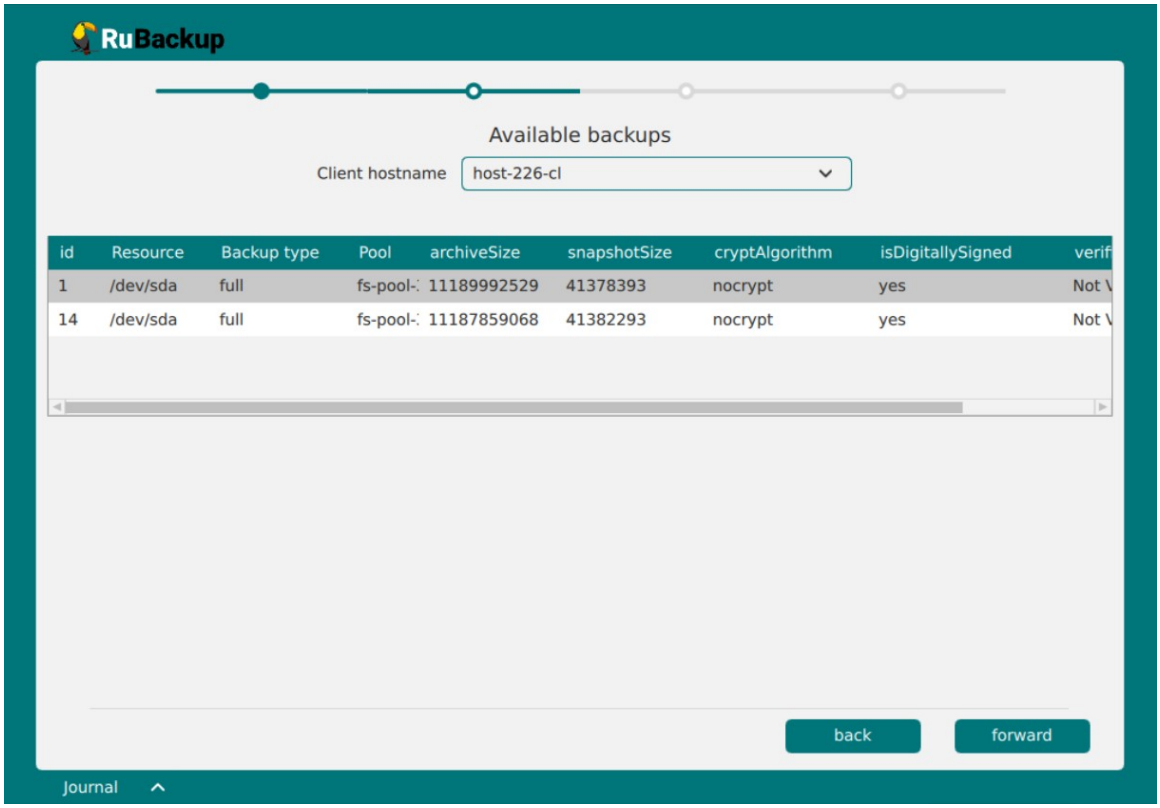

Рисунок 11

10. Выберите жесткий диск, на который будет восстановлен спасательный образ и введите пароль клиента RuBackup, который был выбран в пункте 9. Если спасательный образ был создан с использованием защитного преобразования добавьте ключ для расшифровки спасательного образа, нажав на кнопку «input crypt key» (Рисунок 12).
11. 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).
12. Введите пароль клиента и нажмите кнопку «Restore».

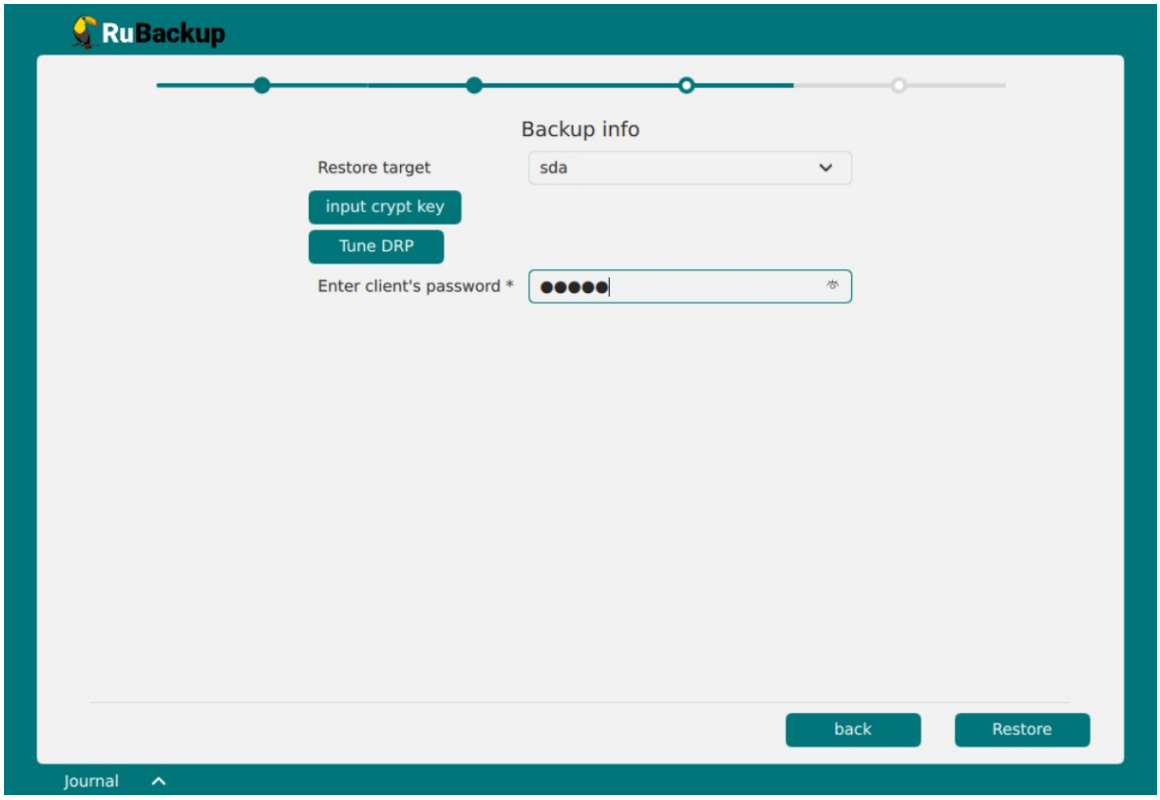

Рисунок 12

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).

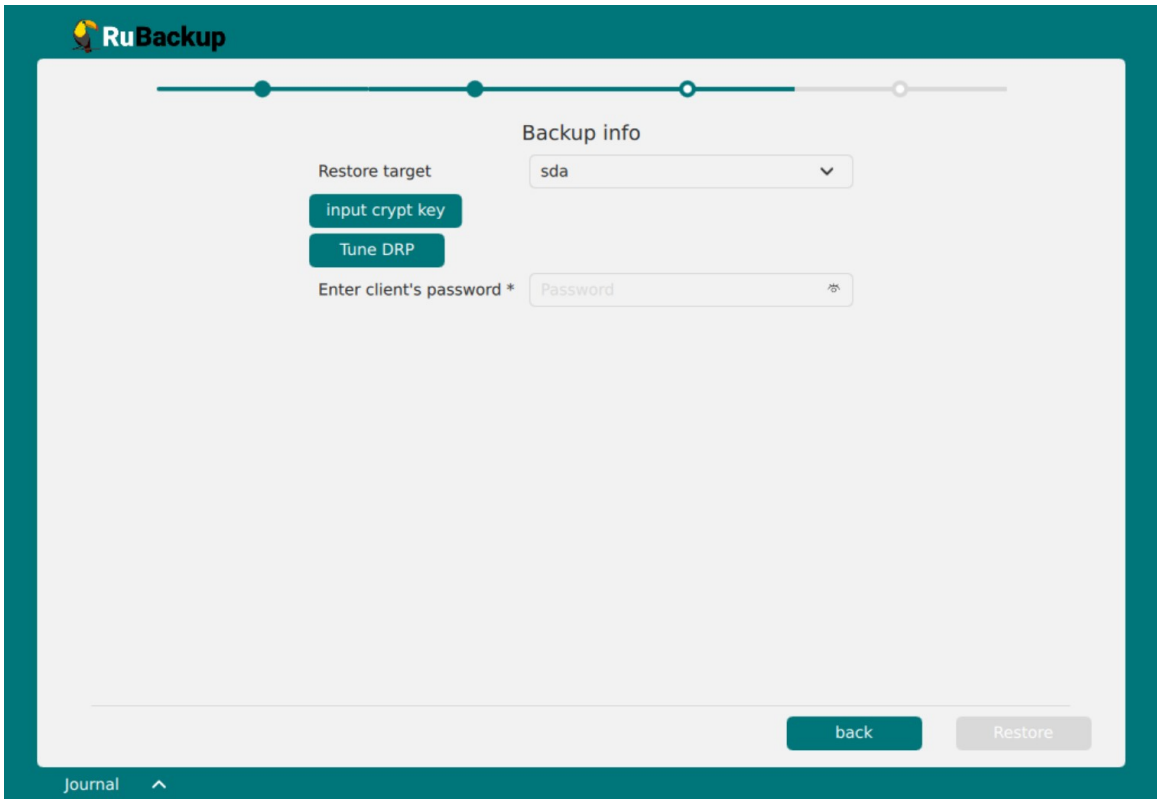

Рисунок 13

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

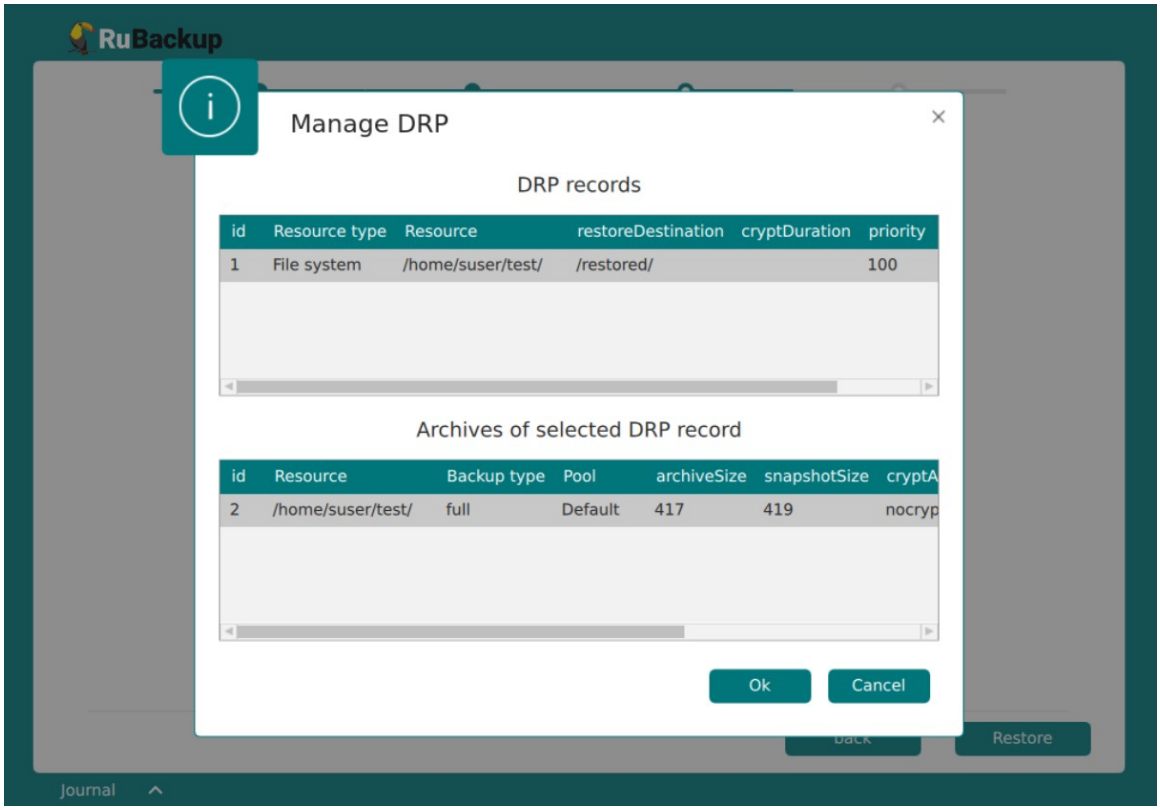

Рисунок 14

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.