



RuBackup

Система резервного копирования
и восстановления данных

АВАРИЙНОЕ ВОССТАНОВЛЕНИЕ LINUX-СИСТЕМ (RUBACKUP KEY)

ВЕРСИЯ 2.4.0, 26.12.2024

Содержание

1. Ограничения	3
2. Подготовка к созданию спасательного образа	4
3. Создание спасательного образа	5
4. Мониторинг процесса создания спасательного образа	9
4.1. Мониторинг через RuBackup Key	9
4.2. Мониторинг через RBM	9
5. Создание пароля для восстановления системы	10
6. Восстановление системы с помощью спасательного образа	11
7. Мониторинг процесса восстановления системы с помощью спасательного образа	16
7.1. Мониторинг через RuBackup Key	16
7.2. Мониторинг через RBM	16
8. Решение проблем	17

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.

Глава 1. Ограничения

- Объем оперативной памяти не менее 8 ГБ.
- 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`.

Глава 2. 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 при первом запуске RBC или `rb_archives`.

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.

Глава 3. Создание спасательного образа

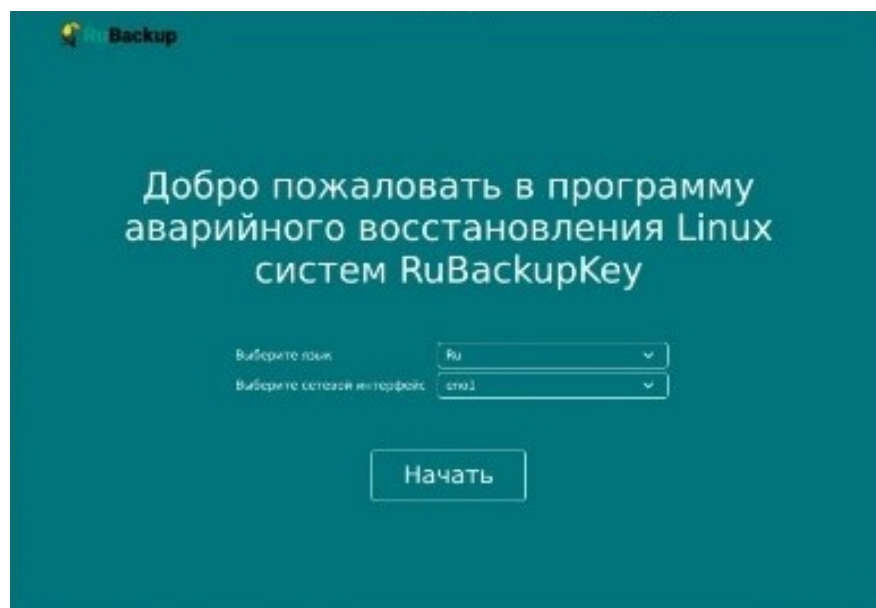
Для создания спасательного образа RuBackup Key выполните следующие шаги:

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` (Пример 1).

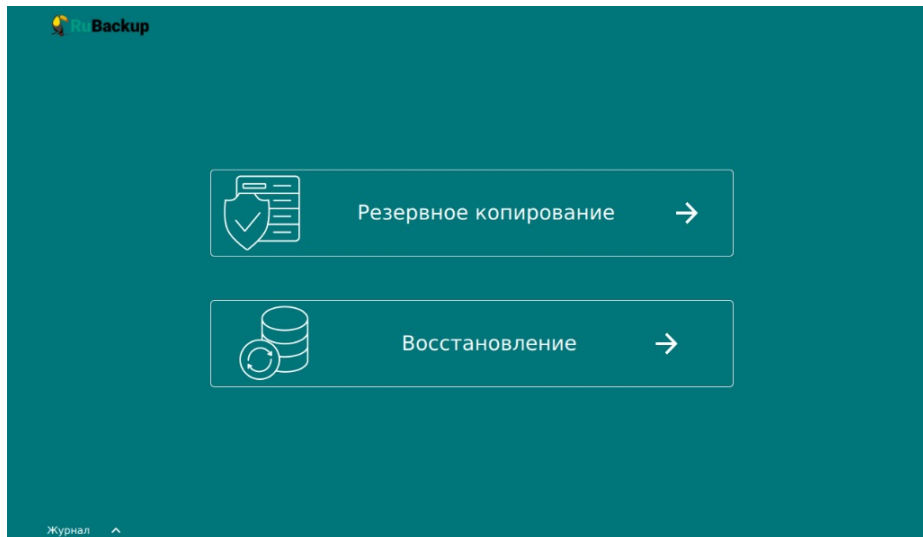
Пример 1. Файл `hosts`

```
127.0.0.1 localhost
127.0.1.1 lubuntu
192.168.7.226 server_hostname
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastpreftx
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

4. Командой `ping <server_name>` проверьте корректность записи о сервере в `/etc/hosts`.
5. Выберите язык, сетевой интерфейс и иницируйте начало работы с RuBackup key. (рисунок 1)



6. Откроется окно выбора Создания резервной копии или Восстановления RuBackup key (рисунок 2).



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

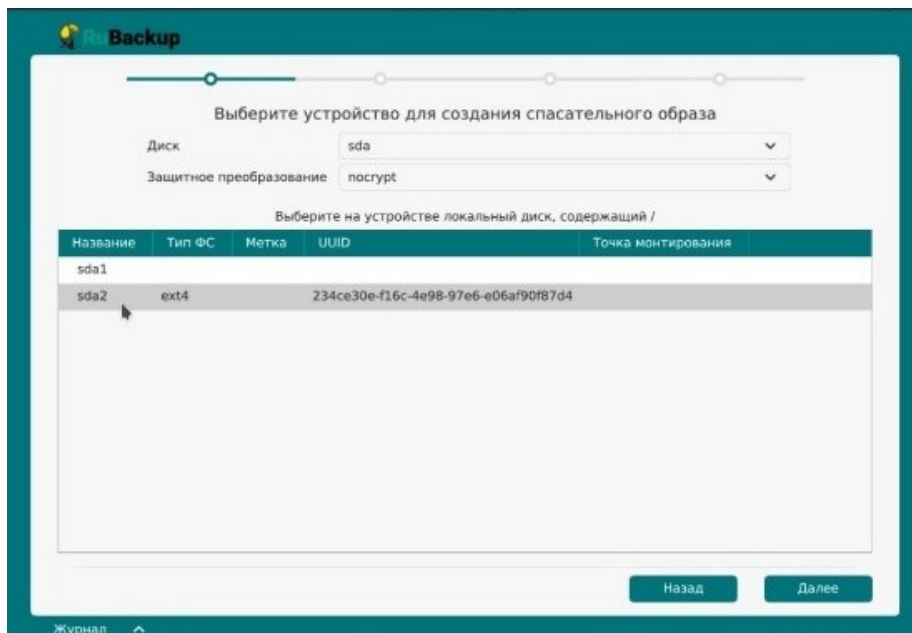


Повторный запуск приложения осуществляется только через графический интерфейс

8. Для создания спасательного образа нажмите кнопку «Резервное копирование».

Выберите физический диск, на котором расположена операционная система, образ которой необходимо создать (рисунок 3).

При необходимости выберите тип защитного преобразования.

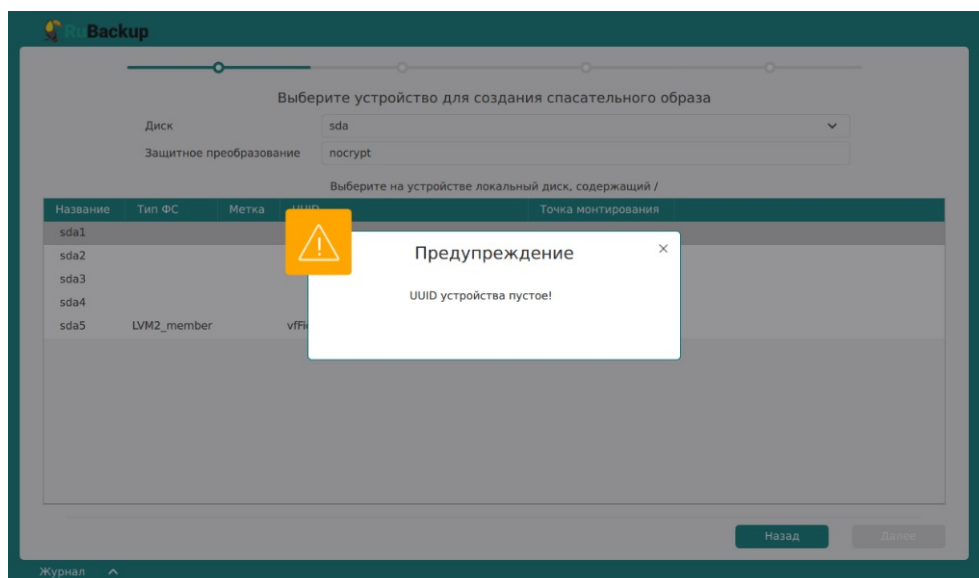


9. Выберите локальный диск, где расположен корень операционной системы (рисунок 4).



Если выбрать не тот локальный диск (например, пустой или не содер-

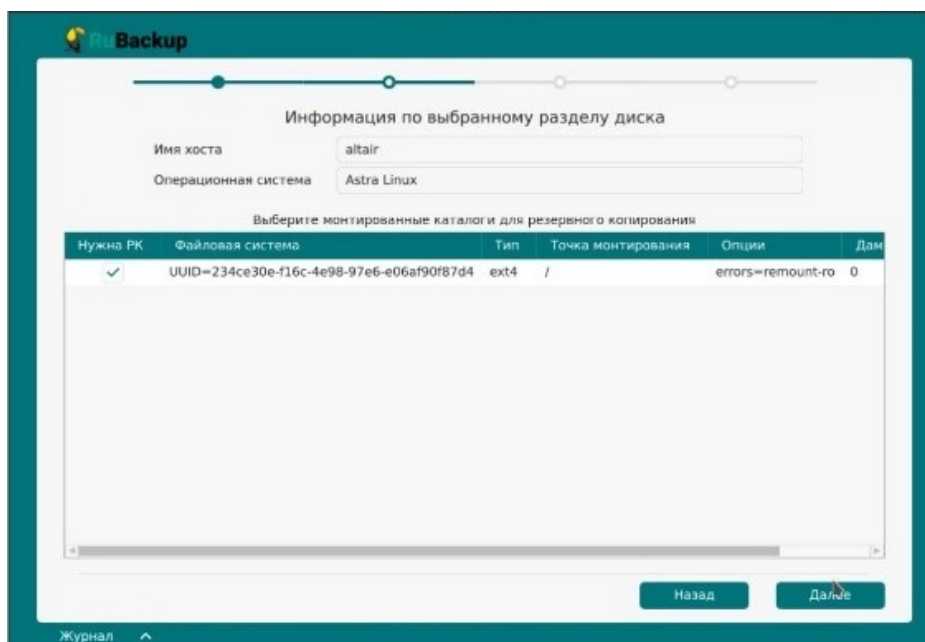
жащий корень операционной системы), Система отобразит сообщение с предупреждением.



10. Для перехода к следующему этапу нажмите кнопку «Далее».

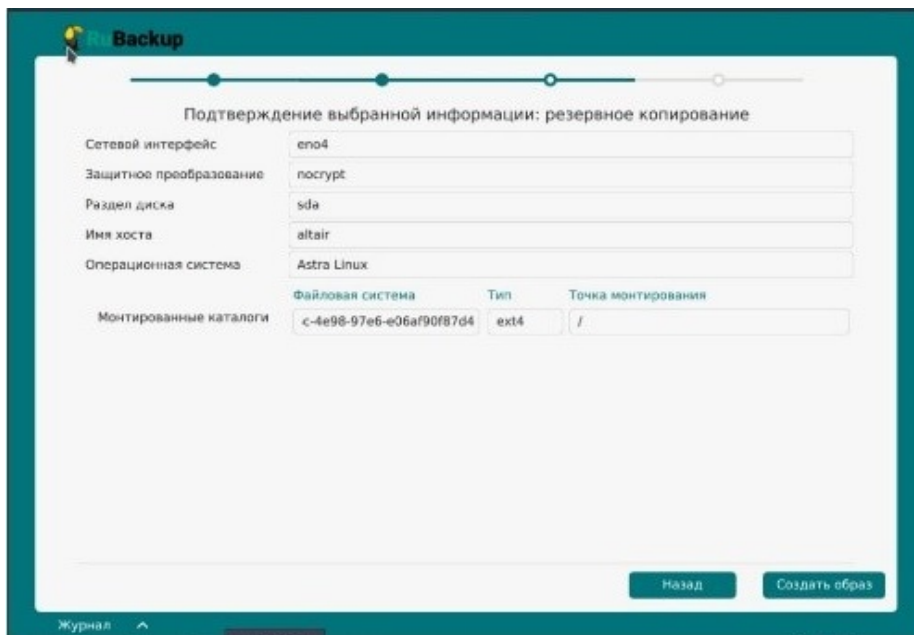
RuBackup Key по `fstab` находит локальные диски, относящиеся к выбранной операционной системе.

11. Среди предложенных локальных дисков выберите те, которые необходимо включить в спасательный образ, обязательно включая локальный диск, содержащий корень файловой системы и директорию `/opt/rubackup/` (рисунок 5).

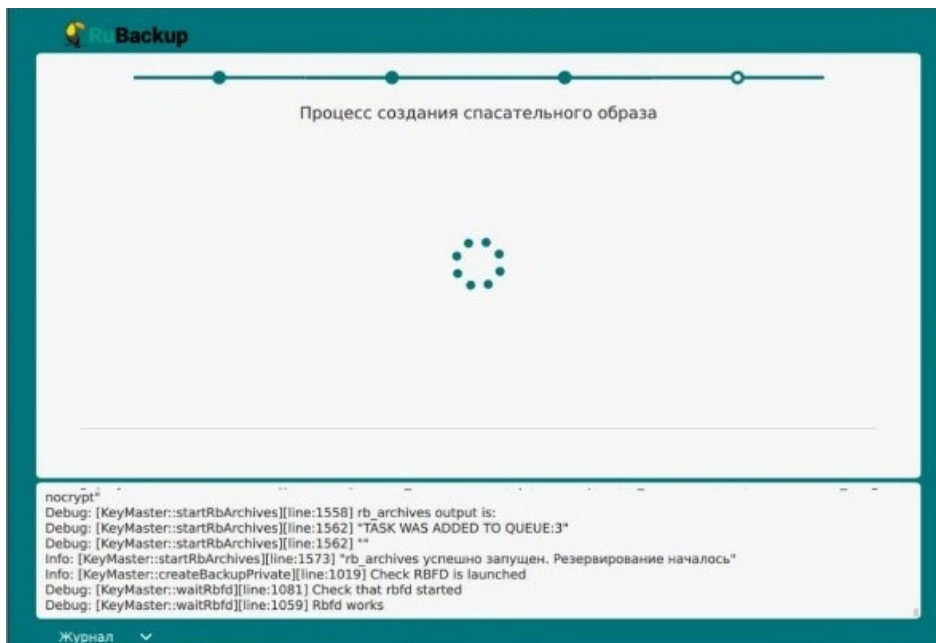


12. Для перехода к следующему этапу нажмите кнопку «Далее».

13. Подтвердите выбранные параметры и запустите создание спасательного образа, нажав кнопку «Создать образ» (рисунок 6).



14. Откроется окно «Процесс создания спасательного образа» (рисунок 7)



15. Дождитесь окончания создания спасательного образа. В окне появится надпись «Создание спасательного образа успешно завершено». После успешного создания спасательного образа для продолжения работы на хосте клиента нужно его выключить и загрузиться со штатного диска.
16. На сервере RuBackup открыть окно RBM и проверить раздел «Репозиторий», в нем должна появиться резервная копия типа «Backup local», с именем хоста клиента и типа «Rescue image».

Глава 4. Мониторинг процесса создания спасательного образа

4.1. Мониторинг через RuBackup Key

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

4.2. 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.

Глава 5. Создание пароля для восстановления системы

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.



Ключ RuBackup не имеет отношения к паролям от RBM или RBC, это пароль для RuBackup Key.

Глава 6. Восстановление системы с помощью спасательного образа



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



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

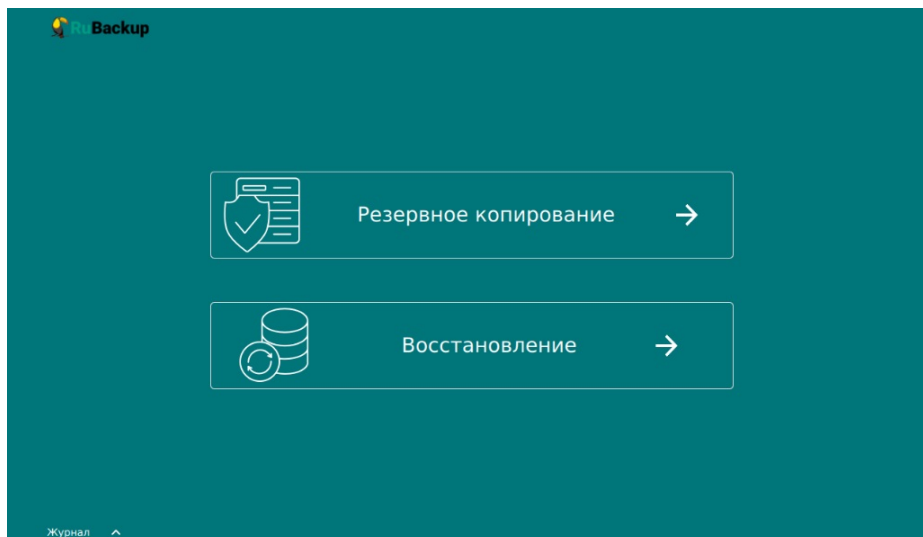
Для восстановления с помощью спасательного образа выполните следующие шаги:

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` (Пример 2).

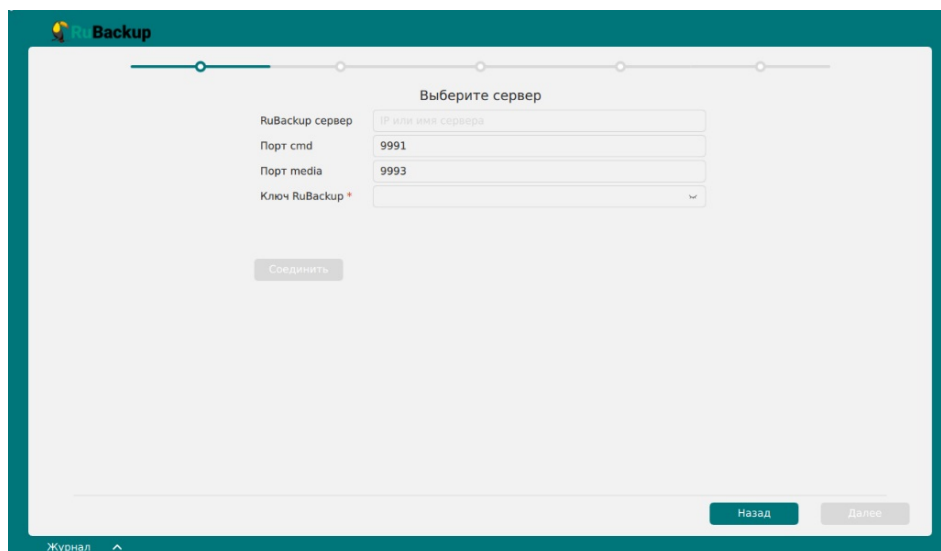
Пример 2. Файл `hosts`

```
127.0.0.1 localhost
127.0.1.1 lubuntu
192.168.7.226 server_hostname
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastpreftx
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

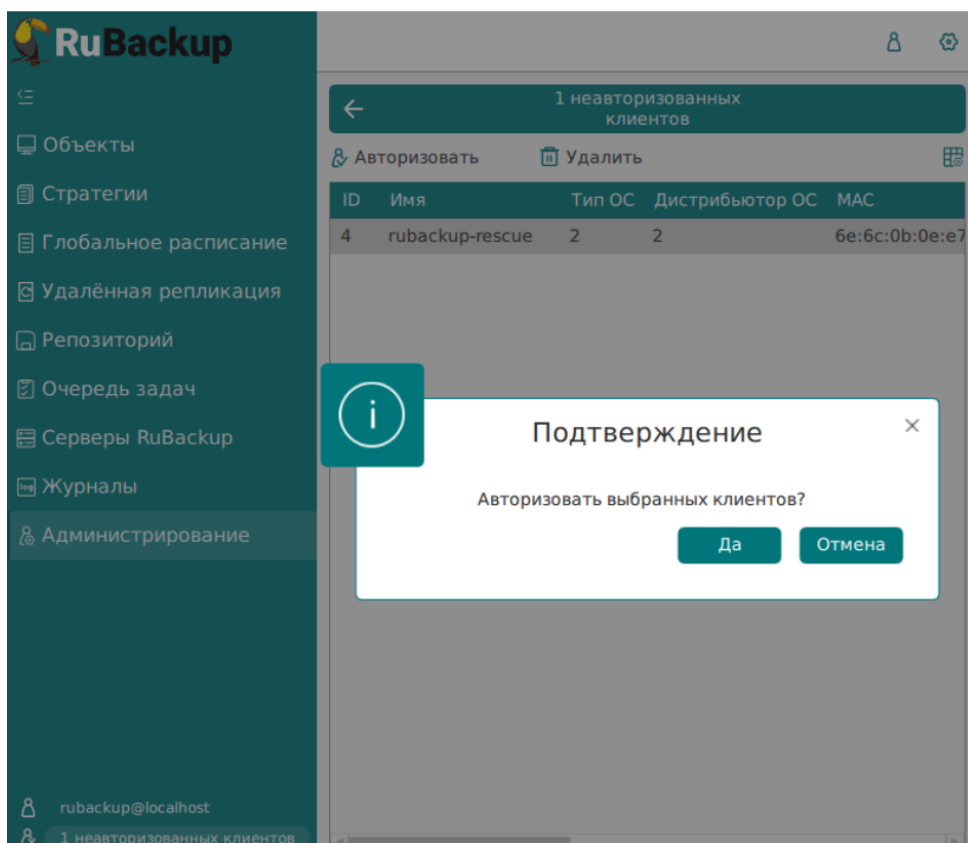
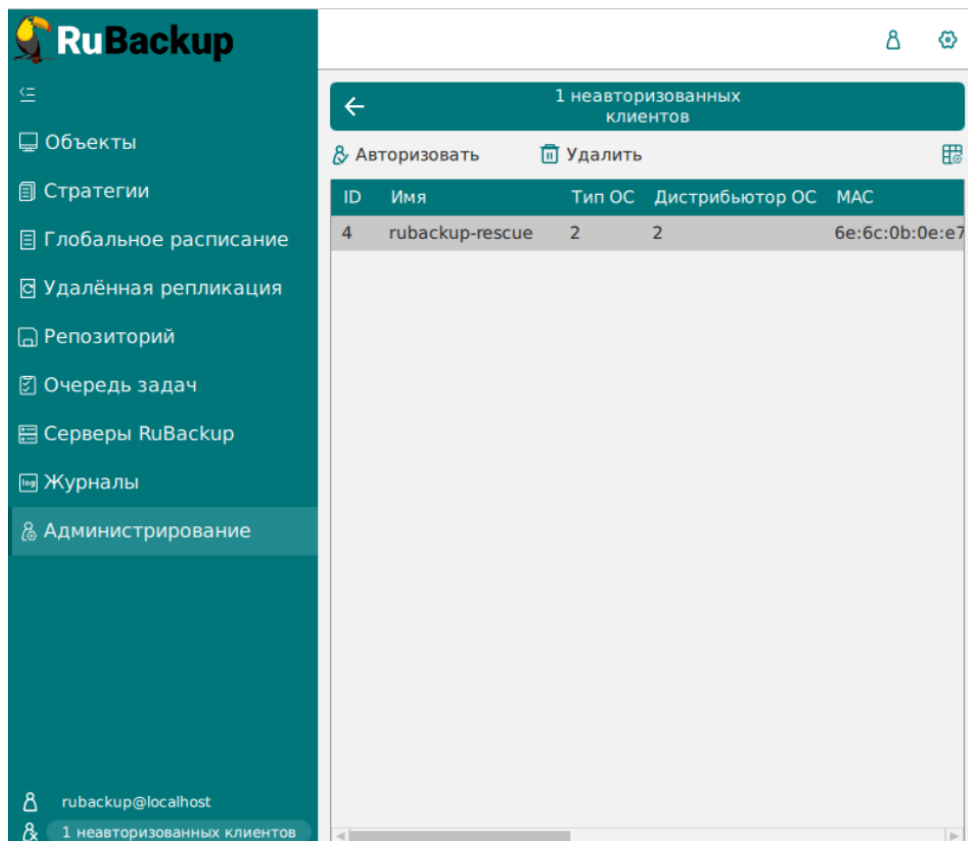
4. Командой `ping <server_name>` проверьте корректность записи о сервере в `/etc/hosts`.
5. Выберите язык и сетевой интерфейс и иницируйте начало работы с RuBackup Key. Откроется окно RuBackup Key.
6. Для восстановления спасательного образа нажмите кнопку «Восстановление» (рисунок 8).



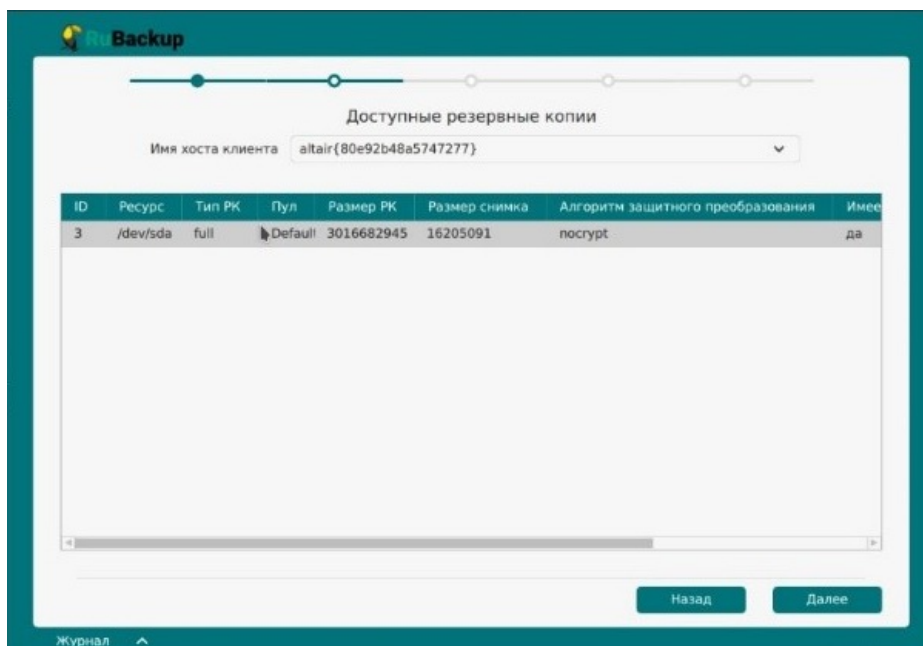
7. Введите адрес основного сервера RuBackup, порты и иницируйте подключение, нажав кнопку «Далее» (рисунок 9).



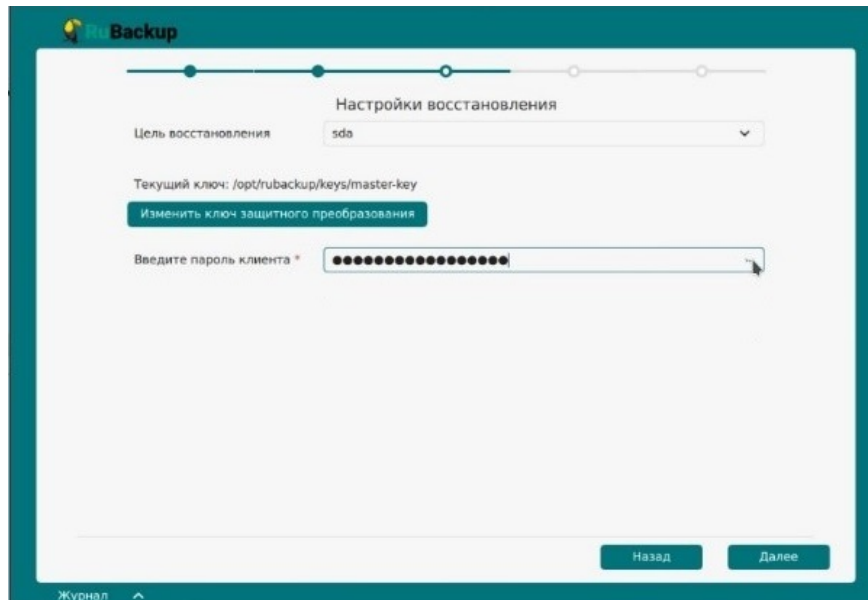
8. Перейдите в RBM (рисунок 10) и авторизуйте появившегося клиента rubackup-rescue на странице «Неавторизованные клиенты» (рисунок 11).



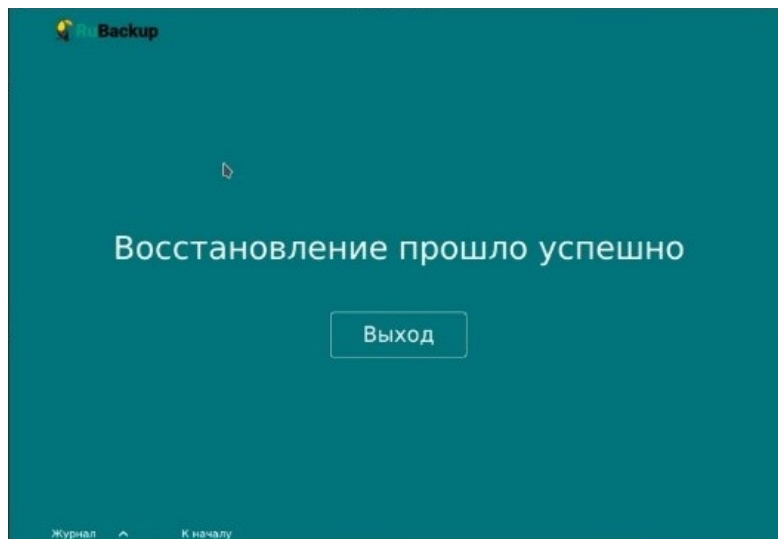
9. В RuBackup Key выберите клиента, резервную копию которого необходимо восстановить, и спасательный образ, принадлежащий данному Клиенту и нажмите кнопку «Далее» (рисунки 11 и 12).



10. Выберите жесткий диск, на который будет восстановлен спасательный образ и введите пароль клиента RuBackup, который был выбран в пункте 8. Если спасательный образ был создан с использованием защитного преобразования добавьте ключ для расшифровки спасательного образа, нажав на кнопку «Изменить ключ защитного преобразования» (рисунок 13).
11. Введите пароль клиента и нажмите кнопку «Далее».



12. Дождитесь восстановления системы с помощью спасательного образа RuBackup key.



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

Глава 7. Мониторинг процесса восстановления системы с помощью спасательного образа

7.1. Мониторинг через RuBackup Key

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

7.2. 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.

Глава 8. Решение проблем

Таблица 1. Список возможных проблем и их решений

Ошибка в журнале RuBackup Key	Решение
Неудачный запуск <code>rb_archives</code> . Пожалуйста, проверьте, установлен ли клиентский пароль	Установить клиентский пароль при первом запуске RBC или <code>rb_archives</code>