

RuBackup

Система резервного копирования и восстановления данных

Аварийное восстановление Linux систем



RuBackup

Версия 1.9

2022 г.

Содержание

Введение.....	3
Подготовка к созданию спасательного образа.....	5
Создание спасательного образа.....	7
Восстановление системы с помощью спасательного образа.....	9
Мастер-ключ.....	13

Введение

Система резервного копирования RuBackup предоставляет возможность создания спасательных образов (rescue image) для операционных систем Linux, располагающихся на виртуальных машинах и «голом железе» (bare metal) с возможностью их быстрого восстановления в случае возникновения аварийных ситуаций. Так же спасательные образы могут быть использованы для переноса систем из виртуальных машин на «голое железо» и с «голового железа» в виртуальные машины. Спасательные образы хранятся так же как и другие резервные копии в системе резервного копирования RuBackup. От обычной резервной копии они отличаются только тем, что создать и восстановить их можно только при помощи **RuBackup key**.

При создании спасательного образа используется по-файловый метод резервного копирования. Это означает что резервная копия будет занимать, как правило, меньше места чем общий объем дисков системы, а так же что при помощи RuBackup можно переносить спасательные образы на системы с меньшими или большими дисками с тем условием, что объем данных резервной копии уместится на новой системе.

Создание спасательного образа и восстановление системы осуществляется с помощью **RuBackup key (специализированный загрузочный образ RuBackup)**, который обеспечивает взаимодействие с сервером резервного копирования.

При помощи RuBackup можно восстанавливать системы так называемой «стандартной установки». Операционные системы Linux предоставляют пользователю беспрецедентный уровень вариативности при их использовании, в том числе богатые возможности по конфигурированию систем во время инсталляции и последующего использования. Возможности RuBackup по созданию и восстановлению систем из спасательных образов ограничены следующими условиями:

- восстановление системы происходит на один диск (одно устройство: sda, vda и т.п.), даже если резервное копирование делалось для системы, расположенной на нескольких устройствах;

- система имеет один файл подкачки (swap), который располагается либо в отдельном дисковом разделе, либо в файле.

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  
/var/log/journal
```

В том случае, если swap располагается в файле, то он так же исключается из резервной копии, но при восстановлении будет создан заново.

В том случае, если в системе присутствует и включен *SELinux*, то при восстановлении в файле `/etc/selinux/config` будет установлен параметр `SELINUX=disabled`.

Если после успешного восстановления системы нужно включить *SELinux*, то этот параметр необходимо установить как

```
SELINUX=enforced
```

и перезагрузить систему.

Подготовка к созданию спасательного образа

Для возможности создания спасательного образа на систему необходимо установить клиента 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](#)».

При установке клиента RuBackup в ОС Astra Linux SE 1.6 Смоленск, то может оказаться, что в официальной репозитории нет компрессора pigz. В этом случае можно сделать ссылку:

```
# sudo ln -s /bin/gzip /usr/bin/pigz
```

Важно! В ходе создания спасательного образа из него будут принудительно исключены во избежание утечки *master key* и ключи электронной подписи. *Master key* используется для защитного преобразования резервных копий на стороне клиента. Ключи электронной подписи используются для подтверждения подлинности резервных копий клиента. **Рекомендуется сразу после установки клиента скопировать *master key* и ключи электронной подписи в надежное место.** Ключи расположены в каталоге `/opt/gubackup/keys`.

При создании спасательных образов и восстановлении из них при помощи RuBackup key используется возможность сервера резервного копирования RuBackup предоставлять клиенту сетевую файловую систему NFS для временных операций с резервными копиями. Для этого на сервере резервного копирования RuBackup должен быть выделен соответствующий каталог при помощи RBM с достаточным пространством для временных операций клиентов с резервными копиями (рисунок 1) (подробнее см. «Руководство по установке системы резервного копирования RuBackup для серверов резервного копирования и Linux клиентов» и «Руководство системного администратора RuBackup»).

Менеджер администратора RuBackup

Конфигурация | Просмотр | Действия | Аналитика | Информация

Объекты | Стратегии | Глобальное расписание | Удаленная репликация | **Серверная группировка RuBackup**

Имя хоста | Описание

1	ubuntu	Primary RuBackup server
---	--------	-------------------------

Файловые системы | **Ленточные библиотеки** | Облака | Блочные устройства

Обычное хранилище:
 Общая емкость: Гб
 Использовано: Гб

Аварийное хранилище:
 Общая емкость: Гб
 Использовано: Гб

Временное хранилище:
 Каталог для NFS

Пулы

Filesystem ^	Total, GB	Available, GB	Used, %	Описание
1 /default_pool	23.99	9.93	58	

Default

Лицензия: Заказчик Емкость: Тб, исп.: Тб Клиентов:

Тип: Начало: Конец: Сокетов:

Соединение: rubackup@rubackup:ubuntu Нормальный режим

Рисунок 1

Создание спасательного образа

Для создания спасательного образа необходимо запустить систему с помощью *RuBackup key*. Необходимо, чтобы имя сервера резервного копирования разрешалось с помощью DNS.

Важно! Так как *RuBackup key* при загрузке необходимо получить временный IP адрес от DHCP сервера, необходимо обеспечить, чтобы в списке клиентов *RuBackup* не было записей других клиентов, которые ранее использовали этот адрес, в противном случае операция будет завершена с ошибкой или не сможет начаться.

При загрузке системы с помощью *RuBackup key* будет запущено оконное приложение *rbkey* (рисунок 2):

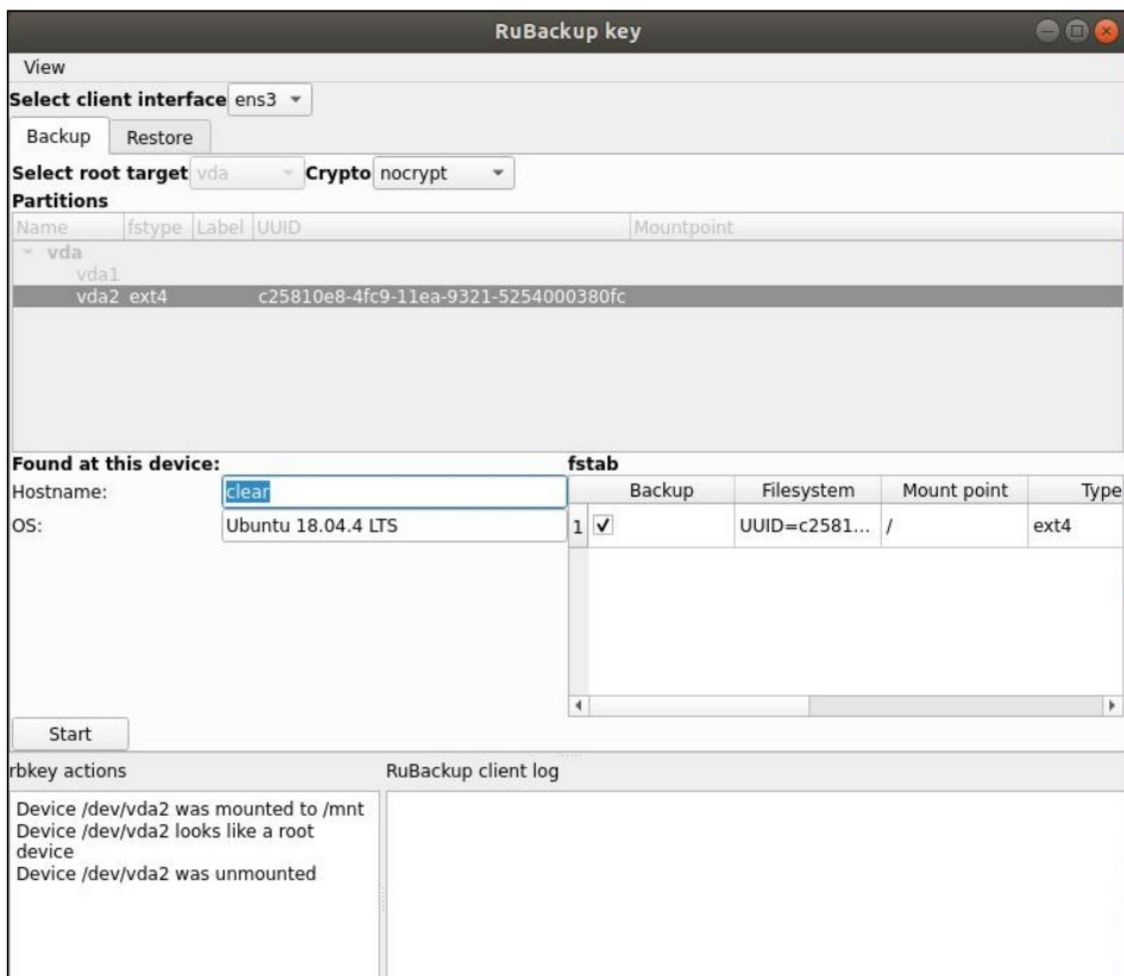


Рисунок 2

Необходимо выбрать вкладку «Backup». Здесь необходимо выбрать *root target* (например *vda* или *sda*), то есть то устройство, на котором располагается / системы, после чего выбрать раздел, на котором располагается /системы.

При выборе раздела *rbkey* проверит действительно ли выбранный раздел может являться / системы и в случае правильного выбора будет разблокирована кнопка «Start». В таблице *fstab* можно выбрать какие файловые системы должны войти в резервную копию. Рекомендуется не выбирать пользовательские файловые системы, для которых резервное копирование может выполняться регулярно правилами резервного копирования RuBackup, а выбрать только то, что необходимо для аварийного восстановления. Все пользовательские данные могут быть впоследствии восстановлены из наиболее свежих резервных копий правильным способом (однако необходимо заранее позаботиться о том, чтобы резервные копии тех или иных данных периодически создавались с помощью RuBackup).

Для начала создания спасательного образа необходимо нажать кнопку «Start» (рисунок 3). После окончания создания спасательного образа систему можно выключить.

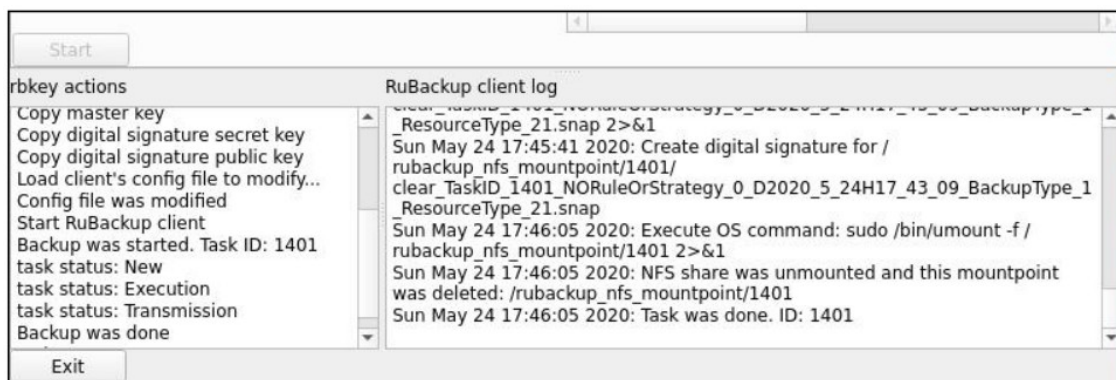


Рисунок 3

Важно! В том случае, если для создания спасательного образа вы выбрали защитное преобразование резервной копии с помощью того или иного алгоритма, вы должны заранее сохранить в надежном месте мастер ключ клиента (он формируется при инсталляции клиента RuBackup на систему), в противном случае вы не сможете без этого мастер ключа восстановить систему из спасательного образа.

Восстановление системы с помощью спасательного образа

Для восстановления системы из спасательного образа необходимо запустить систему с помощью **RuBackup key**. Необходимо, чтобы имя сервера резервного копирования разрешалось с помощью DNS.

Важно! Так как **RuBackup key** при загрузке необходимо получить временный IP адрес от DHCP сервера, надо обеспечить, чтобы в списке клиентов RuBackup не было записей других клиентов, которые ранее использовали этот адрес, в противном случае операция будет завершена с ошибкой.

При загрузке системы с помощью **RuBackup key** будет запущено оконное приложение *rbkey* (рисунок 4):

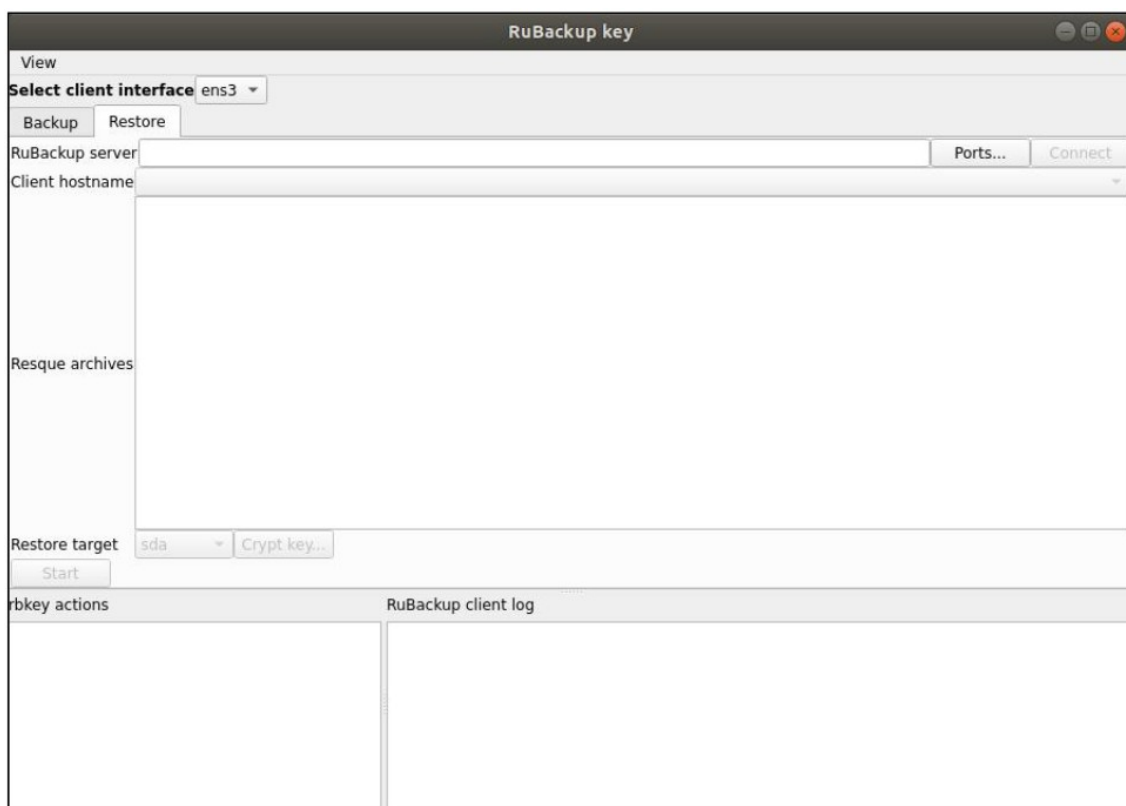


Рисунок 4

Необходимо выбрать вкладку «*Restore*». Здесь в поле **RuBackup server** необходимо ввести имя сервера резервного копирования RuBackup и соединиться с ним, нажав кнопку **Connect**. Клиент резервного копирования при восстановлении с помощью RuBackup key обращается к серверу, представляясь клиентом с именем `rubackup_rescue`. Если это первый случай восстановления системы, то `rbkey` отобразит сообщение, что системный администратор должен авторизовать клиента ***rubackup_rescue*** (рисунок 5):

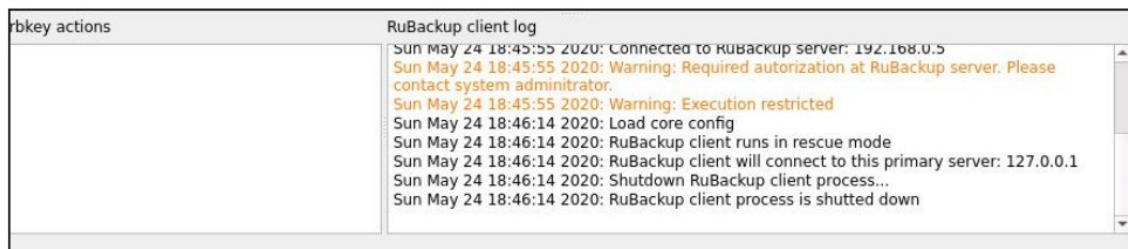


Рисунок 5

После авторизации в ***rbkey*** еще раз необходимо ввести имя сервера резервного копирования RuBackup и соединиться с ним (рисунок 6). Для дальнейших действий требуется ввести пароль **RuBackup key** (задается заранее системным администратором, см. «Руководство системного администратора RuBackup»). Без этого пароля невозможно получить информацию о спасательных образах клиентов RuBackup.

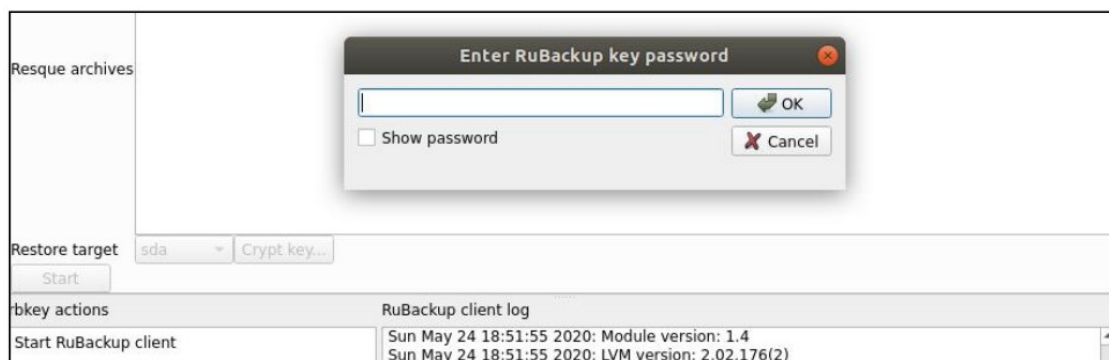


Рисунок 6

Далее потребуется выбрать клиента RuBackup, систему которого планируется восстановить из спасательного образа (рисунок 7):

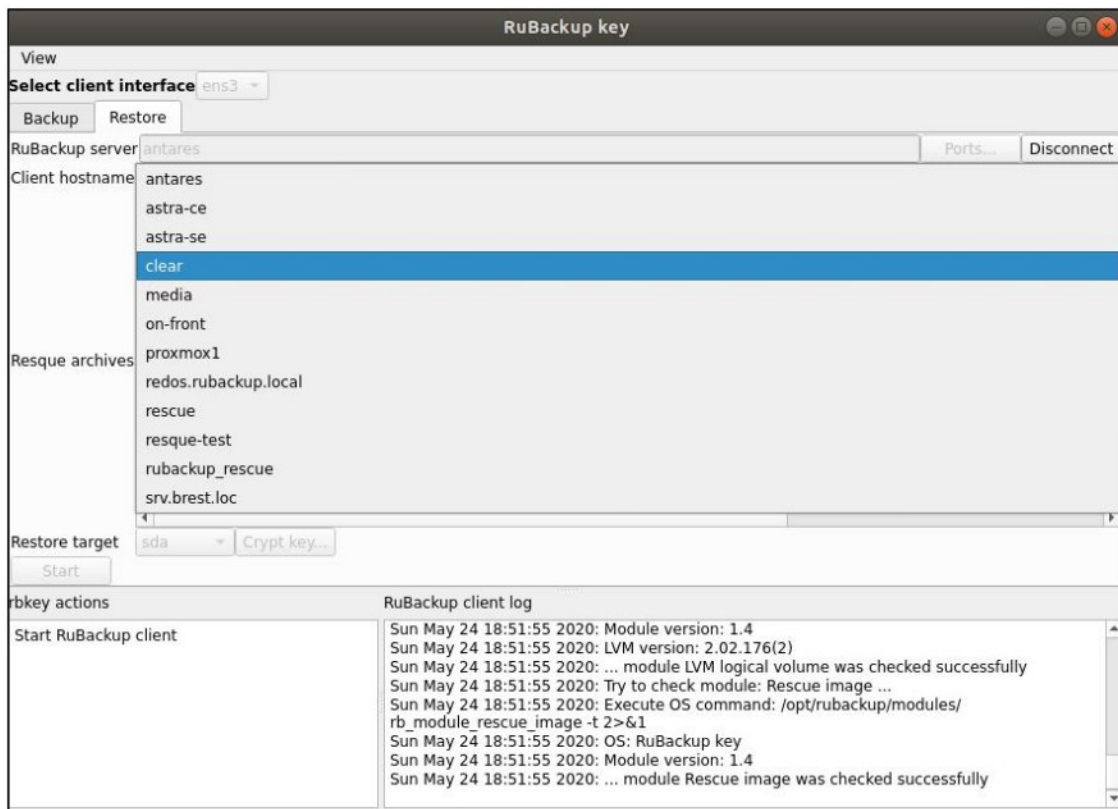


Рисунок 7

Потребуется выбрать резервную копию для восстановления и устройство (*restore target*), на которое планируется восстановить систему (например, *sda*) (рисунок 8):

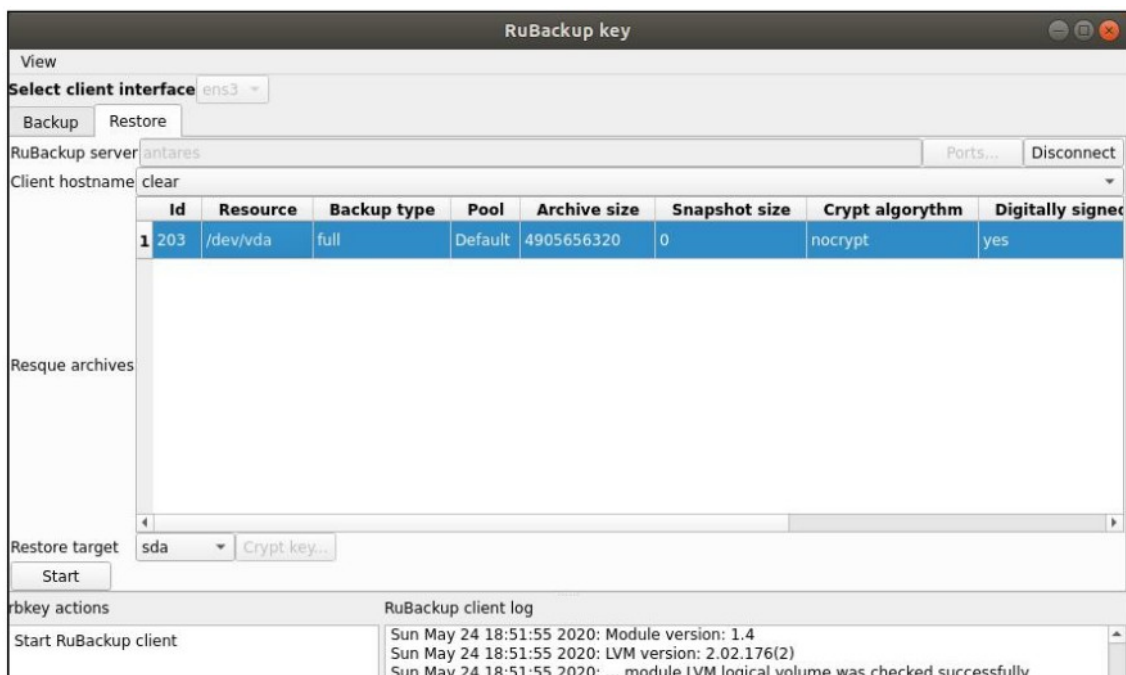


Рисунок 8

Для начала восстановления требуется нажать кнопку “Start”. В том случае, если на этом устройстве располагаются какие либо логические тома или группы LVM, потребуется подтвердить продолжение процедуры восстановления. Для начала процедуры восстановления требуется ввести пароль клиента (рисунок 9):

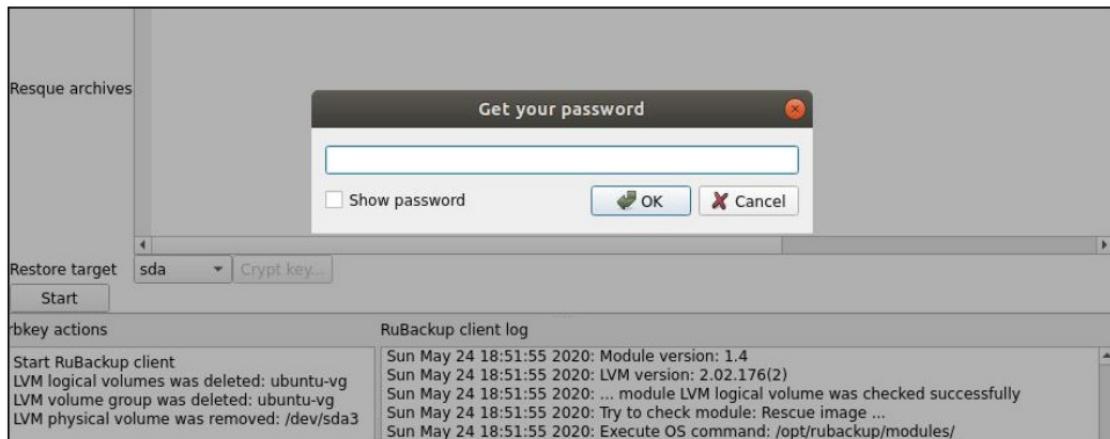


Рисунок 9

Необходимо убедиться в том, что задача восстановления была выполнена успешно (рисунок 10):

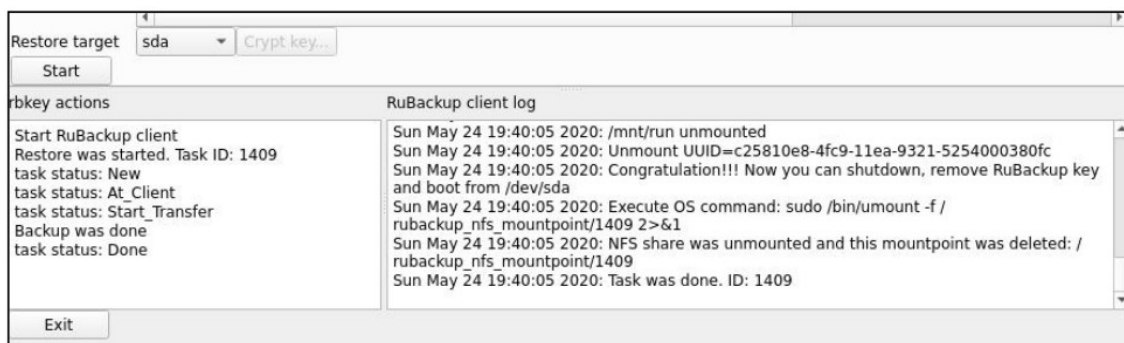


Рисунок 10

После успешного окончания восстановления системы из спасательного образа можно выключить систему, убрать RuBackup key из загрузки, загрузить ее со штатного диска и продолжить восстановление пользовательских данных.

После первого запуска восстановленной системы в нее необходимо загрузить ранее сохраненные в надежном месте, либо создать заново *master key* и ключи электронной подписи. Создать заново ключи можно с помощью *RBC* или *rb_init*.

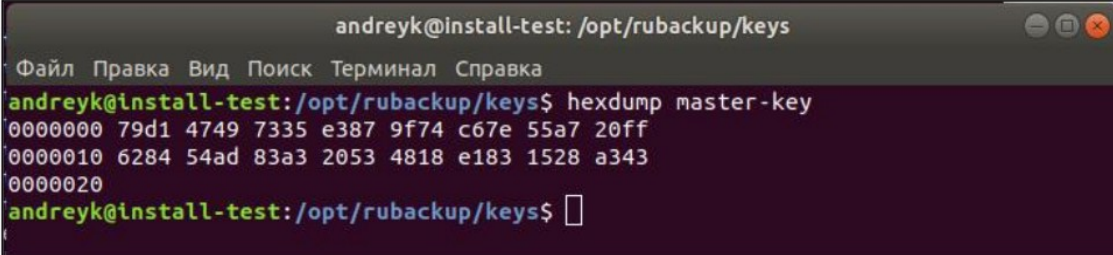
Мастер-ключ

В ходе инсталляции будет создан мастер-ключ для защитного преобразования резервных копий и ключи для электронной подписи, если предполагается использовать электронную подпись.

Внимание! При утере ключа вы не сможете восстановить данные из резервной копии, если последняя 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 надежное место.

Мастер-ключ рекомендуется распечатать при помощи утилиты hexdump, так как он может содержать неотображаемые на экране символы:



```
andreyk@install-test: /opt/rubackup/keys
Файл Правка Вид Поиск Терминал Справка
andreyk@install-test:/opt/rubackup/keys$ hexdump master-key
00000000 79d1 4749 7335 e387 9f74 c67e 55a7 20ff
00000010 6284 54ad 83a3 2053 4818 e183 1528 a343
00000020
andreyk@install-test:/opt/rubackup/keys$
```