RuBackup

Система резервного копирования и восстановления данных

Аварийное восстановление linux систем

Linux rescue backup and disaster recovery

Версия 1.4 2020

Оглавление

Введение..... 3

Подготовка к созданию спасательного образа..... 5

Создание спасательного образа..... 8

Восстановление системы с помощью спасательного образа..... 11

Мастер-ключ..... 15

Лицензирование..... 16

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 “голого 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 присуствует 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 парамет 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 потребуется ввести пароль клиента, он должен быть заранее установлен.

Перед установкой клента RuBackup необходимо установить компрессор pigz (команда может быть иной в зависимости от вашего дистрибутива Linux):

apt install pigz

Установка клиента:

```
root@clear:~#
root@clear:~# dpkg -i rubackup-client.deb
Выбор ранее не выбранного пакета rubackup-client.
(Чтение базы данных … на данный момент установлено 102584 файла и каталога.)
Подготовка к распаковке rubackup-client.deb …
Распаковывается rubackup-client (2020-04-30) …
Настраивается пакет rubackup-client (2020-04-30) …
```

```
root@clear:~# cat >> .bashrc
export PATH=$PATH:/opt/rubackup/bin
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/rubackup/lib
root@clear:~# . .bashrc
```

Инициализация клиента:

```
root@clear:~# rb_init
RuBackup initialization utility
Copyright Andrey Kuznetsov 2018-2020
Exclusive rights: LLC "RUBACKUP"
Исключительные права принадлежат ООО "РУБЭКАП"
Version: 1.4
RuBackup command service was added to /etc/services
RuBackup license service was added to /etc/services
RuBackup media service was added to /etc/services
Do you want to configure RuBackup server (primary, secodnary, media) or client (p/s/m/c/q)?c
Client configuration...
Hostname of primary server: antares
Will you use secondary server (y/n)?n

Possible interfaces for RuBackup client communication:
lo [0]
ens3 [1]
Choose client net interface for use:
Selected interface: ens3
Will you use digital signature (y/n)?y
Would you like to use local(l) backup directory or NFS(n) share of RuBackup server (l/n)?
Local backup directory [/tmp] :
Create RuBackup master key...
Passphrase:

Generating RSA private key, 4096 bit long modulus (2 primes)
.........................................++++
.............................................................++++
e is 65537 (0x010001)
Create new secret key
writing RSA key
Create new public key
```

Запуск клиента:

```
root@clear:~# rubackup_client start
Copyright Andrey Kuznetsov 2018-2020
Exclusive rights: LLC "RUBACKUP"
Исключительные права принадлежат ООО "РУБЭКАП"
Version: 1.4
Load core config
Logfile is /opt/rubackup/log/RuBackup.log
RuBackup client will connect to this primary server: antares
Client interface: ens3
ipv4: 192.168.0.9 ipv6: fe80::5054:ff:feb9:2a77 MAC: 52:54:00:b9:2a:77
Start RuBackup client process
Process RuBackup client is starting as 12650
root@clear:~# Check client's environment...
Environment was checked successfully
Connected to RuBackup server: 192.168.0.5
Warning: Required autorization at RuBackup server. Please contact system adminitrator.
Warning: Execution restricted
```

После этого на сервере резервного копирования администратор RuBackup должен авторизовать нового клиента.

Просмотреть список неавторизованных клиентов на сервере резервного копирования RuBackup и авторизовать нового клиента (операция выполняется на сервере резервного копирования):

```
root@antares:~# rb_clients  -uov
Id | Hostname | OS type | OS distributor | MAC address       | IPv4 address | IPv6 address            | Status
---+----------+---------+----------------+-------------------+--------------+-------------------------+-------
15 | clear    | Linux   | ubuntu         | 52:54:00:b9:2a:77 | 192.168.0.9  | fe80::5054:ff:feb9:2a77 | online
root@antares:~# rb_clients -t 15
```

На авторизованном клиенте необходимо установить пароль:

```
root@clear:~# rb_archives
Set password:
Repeate password:
```

После этого для клиента можно выполнять резервное копирование и восстановление данных, в том числе создание спасательного образа.

Более детальную информанию смотрите в “Руководство по установке серверов резервного копирования и Linux клиентов”.

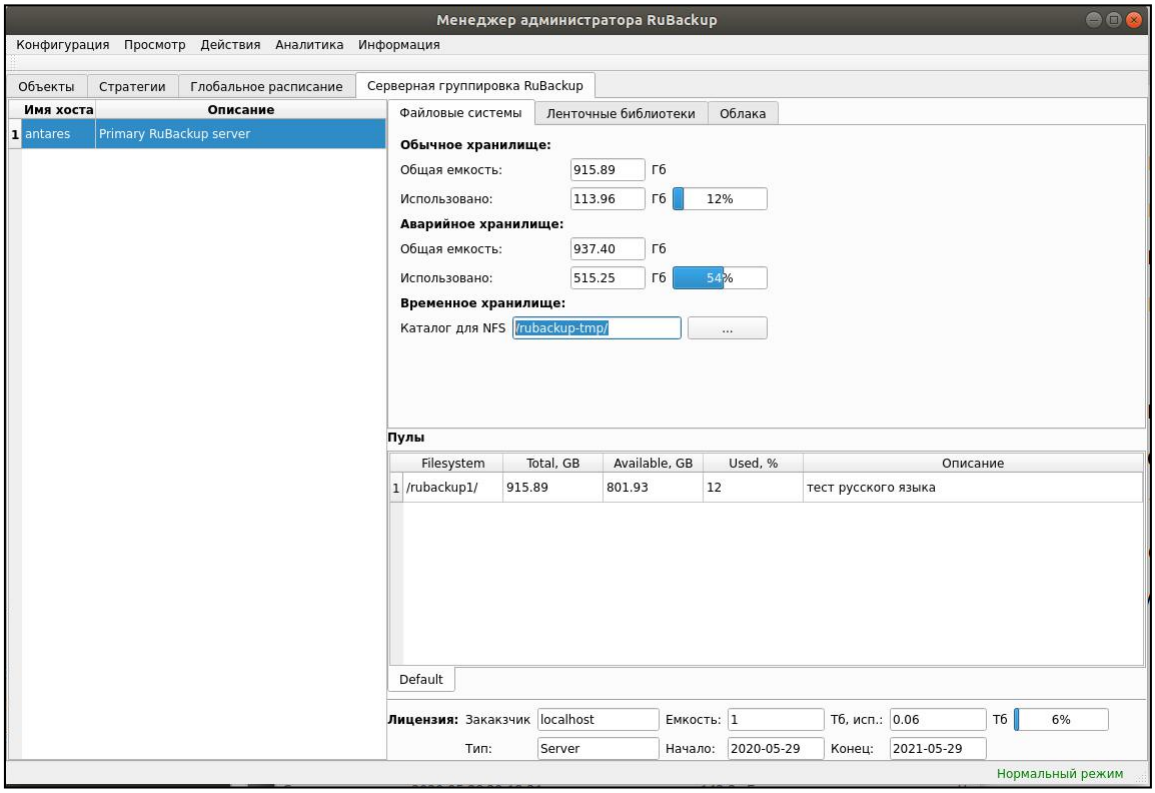
В том случае, если вы устанавливаете клиента RuBackup в ОС Astra Linux 1.6 Смоленск, то может оказаться, что в официальном репозитории нет компрессора pigz. В этом случае можно сделать ссылку:

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

[Важно !!!] В ходе создания спасательного образа из него будут принудительно исключены во избежании 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/rubackup/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 (подробнее см. Руководство системного администратора):

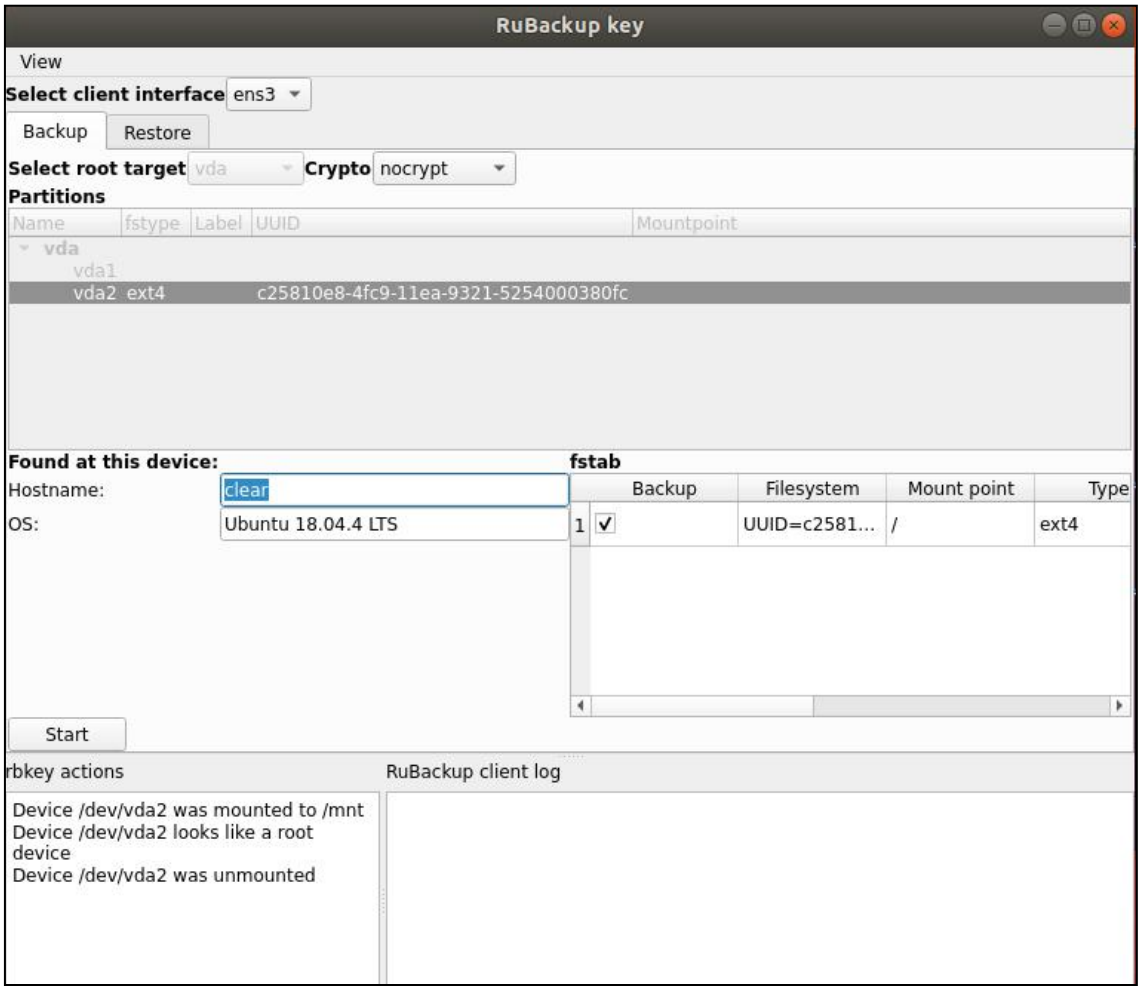


Создание спасательного образа

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

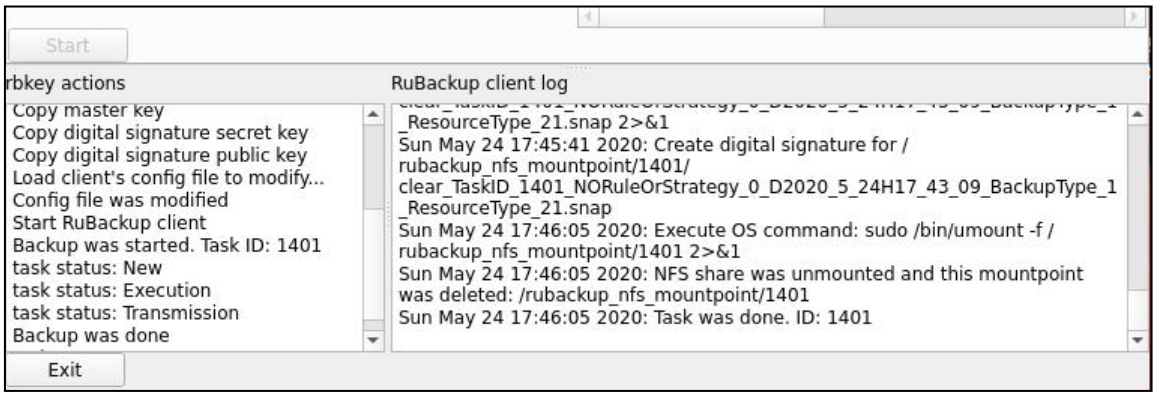
[Важно !!!] Так как RuBackup key при загрузке необходимо получить временный IP адрес от DHCP сервера, необходимо обеспечить, чтобы в списке клиентов RuBackup не было записей других клиентов, которые ранее использовали этот адрес, в противном случае операция будет завершена с ошибкой или не сможет начаться.

При загрузке системы с помощью **RuBackup key** будет запущено оконное приложение **rbkey**:



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 сиистемы 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 позаботится о том, чтобы резервные копии тех или иные данных периодически создавались с помощью RuBackup).

Для начала создания спасательного образа необходимо нажать кнопку “Start”. После окончания создания спасательного образа систему можно выключить.



[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

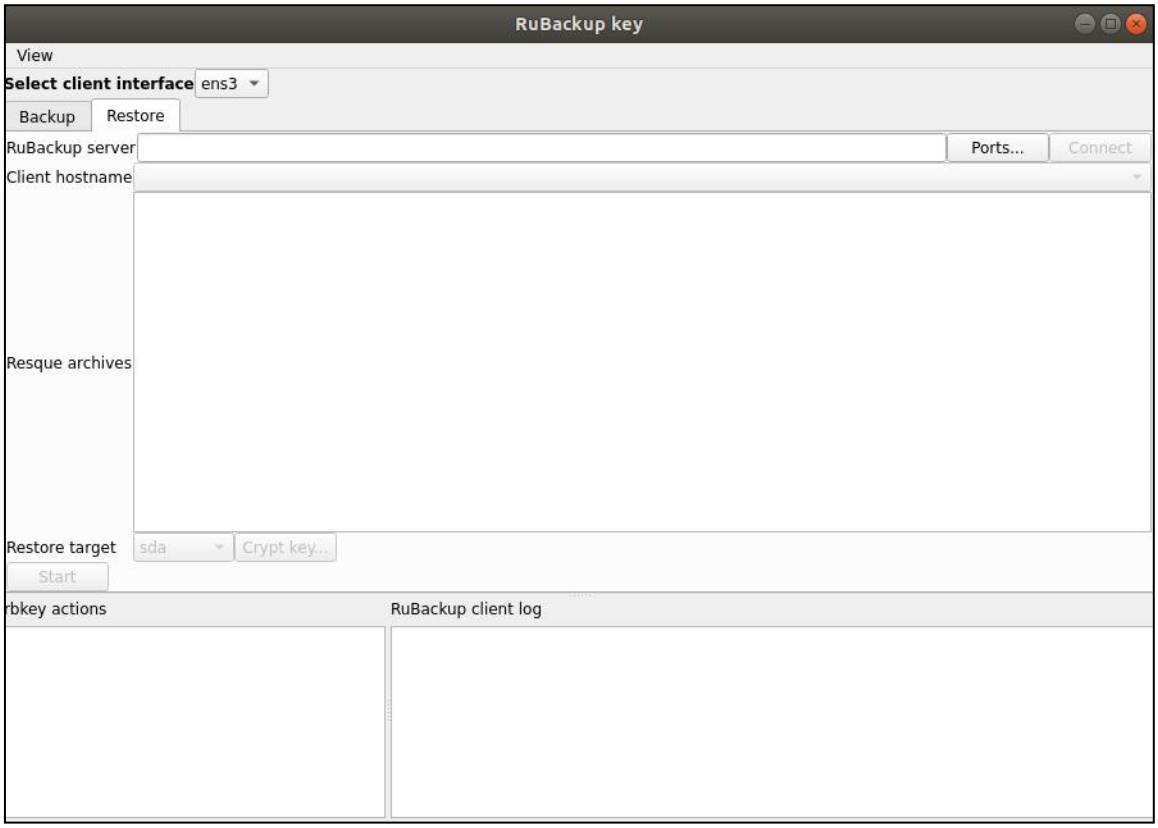
систему), в противном случае вы не сможете без этого мастер ключа восстановить систему из спасательного образа.

Восстановление системы с помощью спасательного образа

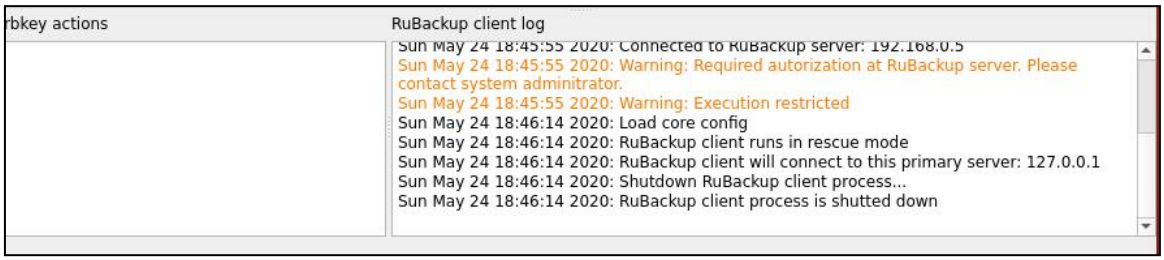
Для восстановления системы из спасательного образа необходимо запустить систему с помощью RuBackup key. Необходимо, чтобы имя сервера резервного копирования разрешалось с помощью DNS.

[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.

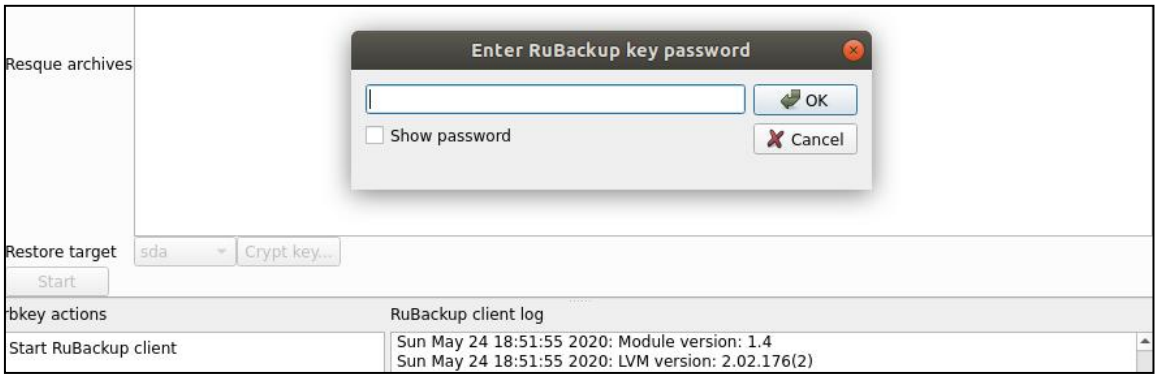
При загрузке системы с помощью **RuBackup key** будет запущено оконное приложение **rbkey**:



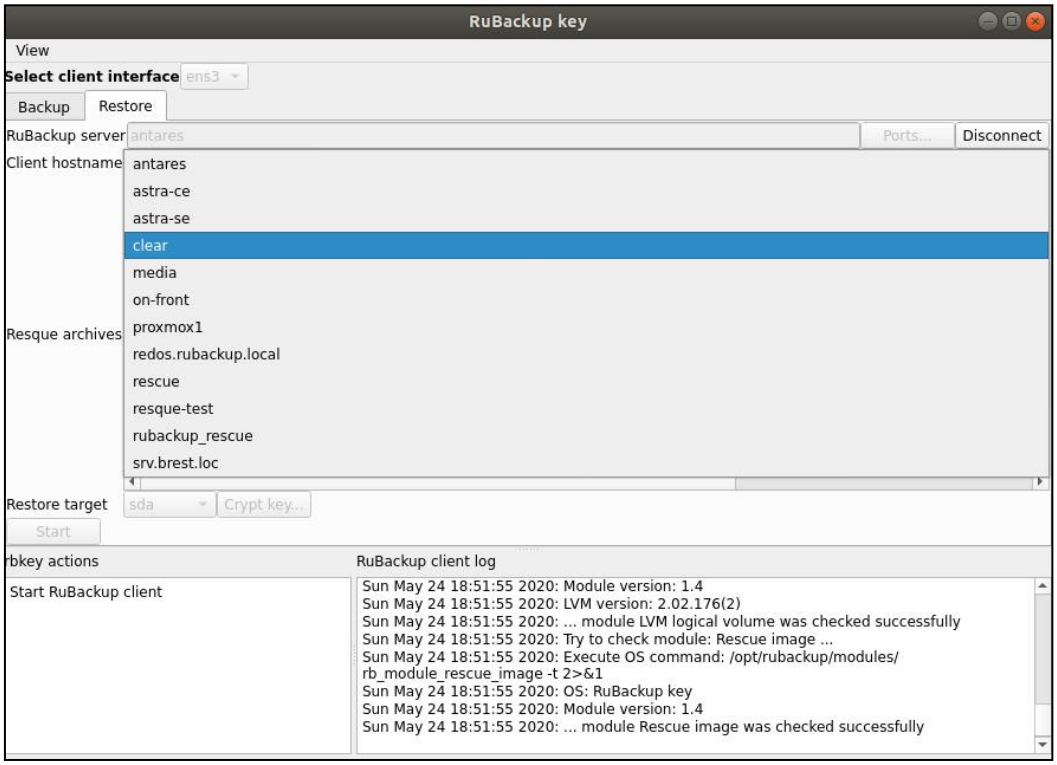
Необходимо выбрать вкладку “Restore”. Здесь в поле **RuBackup server** необходимо ввести имя сервера резервного копирования RuBackup и соединиться с ним, нажав кнопку **Connect**. Клиент резервного копирования при восстановлении с помощью RuBackup key обращается к серверу, представляясь клиентом с именем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



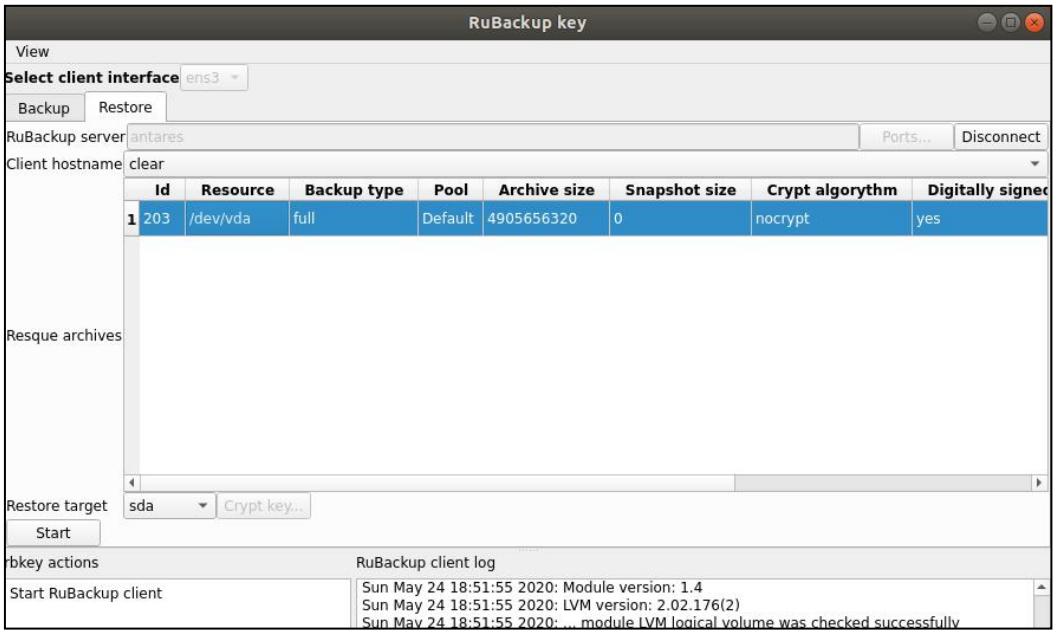
После авторизации в **rbkey** еще раз необходимо ввести имя сервера резервного копирования RuBackup и соединиться с ним. Для дальнейших действий требуется ввести пароль RuBackup key (задается заранее системным администратором, см. “Руководство системного администратора”). Без этого пароля невозможно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



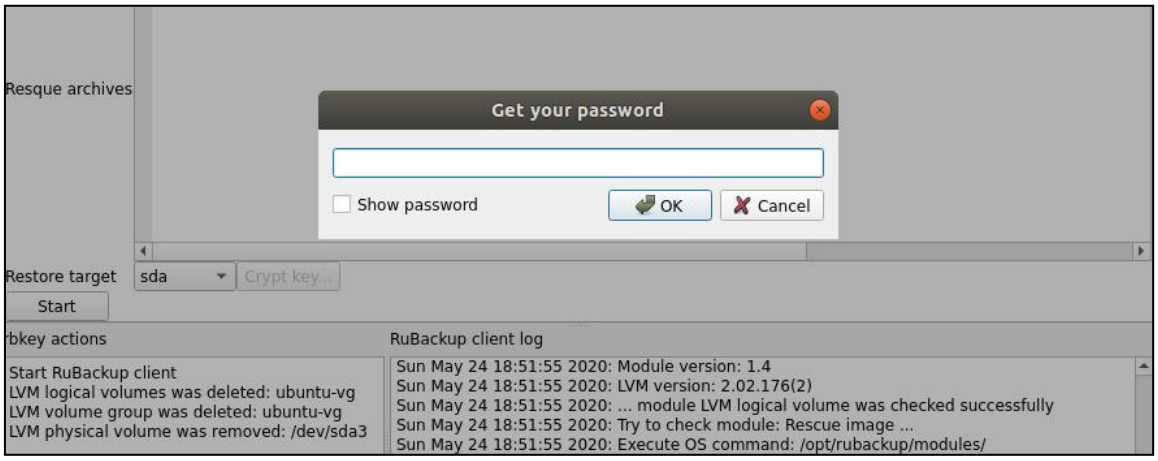
Далее потребуется выбрать клиента RuBackup, систему которого планируется восстановить из спасательного образа:



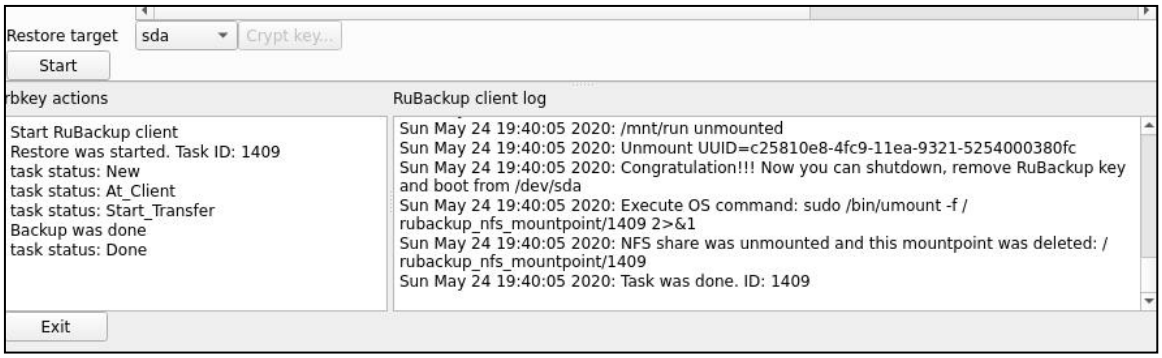
Потребуется выбрать резервную копию для восстановления и устройство (restore target), на которое планируется восстановить систему (например, sda):



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:



Необходимо убедиться в том, что задача восстановления была выполнена успешно:



После успешного окончания восстановления системы из спасательног 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.

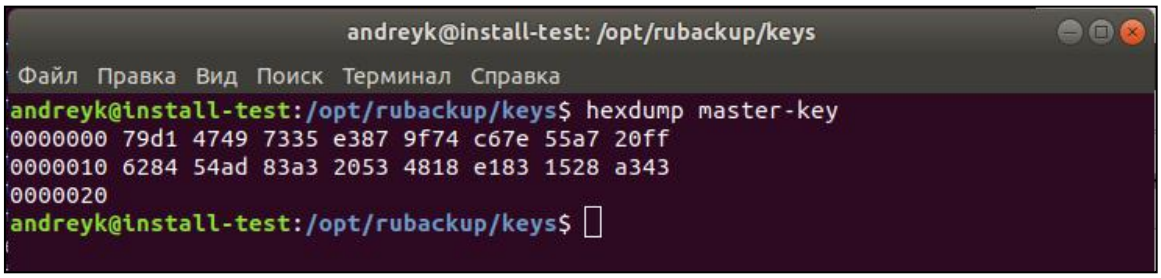
Мастер-ключ

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

[Важно !!!] 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 так же 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:



Лицензирование

Система резервного копирования RuBackup имеет следующие типы лицензий:

Простая бесплатная лицензия

Эта лицензия включает в себя возможность выполнять резервное копирование для любого количества клиентов, но при этом общий объем резервных копий не может превышать 1ТБ.

Коммерческая лицензия

Эта лицензия включает в себя возможность выполнять резервное копирование для любого количества клиентов и хранить определенный объем резервных копий, ограниченный лицензией. Возможно расширение серверной группировки RuBackup с помощью медиа серверов, построение отказоустойчивой конфигурации путём добавления резервного сервера. Все серверы серверной группировки должны иметь собственные лицензии, одинаковые с точки зрения объема хранимых резервных копий.

Пробная лицензия

Эта лицензия включает в себя возможность проверить функционал системы резервного копирования. По окончании действия пробной лицензии функционирование системы приостанавливается.

Более подробно о лицензировании RuBackup читайте в соответствующем руководстве.