

RuBackup

Система резервного копирования и восстановления данных

Электронная подпись резервных копий



RuBackup

Версия 1.9

2022 г.

Содержание

Введение.....	3
Принципы электронной подписи резервных копий.....	4
Электронная подпись резервных копий RuBackup.....	6
Настройка электронной цифровой подписи резервных копий в оконном клиентском менеджере RuBackup.....	8
Создание новой пары ключей электронной подписи.....	9
Настройка обновления публичного ключа электронной подписи в базе данных RuBackup.....	10
Проверка резервной копии в оконном клиентском менеджере RuBackup.....	11

Введение

Электронная подпись резервных копий обеспечивает возможность контроля над соответствием внешних атрибутов резервной копии её внутреннему содержимому и позволяет проверять факт неизменности содержимого резервной копии.

Внимание! Утечка секретного ключа электронной подписи может скомпрометировать все имеющиеся резервные копии клиента.

Принципы электронной подписи резервных копий

Электронная подпись резервных копий выполняется при помощи OpenSSL.

1. Создание секретного ключа

Для создания секретного ключа необходимо выполнить следующие действия:

1. Выполнить команду:

```
# openssl genrsa -out /opt/rubackup/keys/secret-key.pem -aes256 -rand /var/log/syslog 4096
```

2. Ввести секретную фразу (пароль) и повторить ее.

3. Если секретная фраза записана в файле `/opt/rubackup/keys/master-key`, то можно использовать следующую команду:

```
# openssl genrsa -out /opt/rubackup/keys/secret-key.pem -aes256 -passout file:/opt/rubackup/keys/master-key -rand /var/log/syslog 4096
```

4. Секретный ключ будет записан в файл `/opt/rubackup/keys/secret-key.pem`.

2. Создание публичного ключа

Для создания секретного ключа необходимо выполнить следующие действия:

1. Выполнить команду:

```
# openssl rsa -in /opt/rubackup/keys/secret-key.pem -pubout -out /opt/rubackup/keys/public-key.pem
```

2. Ввести секретную фразу (пароль), с которой вы создавали секретный ключ.

3. Если секретная фраза записана в файле `/opt/rubackup/keys/master-key`, то можно использовать следующую команду:

```
# openssl rsa -in /opt/rubackup/keys/secret-key.pem -pubout -out  
/opt/rubackup/keys/public-key.pem -passin  
file:/opt/rubackup/keys/master-key
```

4. Публичный ключ будет записан в файл `/opt/rubackup/keys/public-key.pem`.

3. Создание электронной подписи резервной копии `archive.tar` при помощи секретного ключа

Для создания электронной подписи резервной копии `archive.tar` необходимо выполнить следующие действия:

1. Выполнить команду:

```
# openssl dgst -sign /opt/rubackup/keys/secret-key.pem -out  
signature -md5 archive.tar
```

2. Ввести секретную фразу (пароль), с которой вы создавали секретный ключ.

3. Если секретная фраза записана в файле `/opt/rubackup/keys/master-key`, то можно использовать следующую команду:

```
# openssl dgst -sign /opt/rubackup/keys/secret-key.pem -out  
signature -md5 -passin file:/opt/rubackup/keys/master-key archive.tar
```

4. В результате работы команды будет создан файл `signature` с электронной подписью

4. Проверка соответствия архива и электронной подписи при помощи открытого ключа

Для проверки соответствия архива и электронной подписи необходимо выполнить команду:

```
# openssl dgst -signature signature -md5 -verify  
/opt/rubackup/keys/public-key.pem archive.tar
```

Электронная подпись резервных копий RuBackup

Для автоматического создания электронной подписи RuBackup использует файлы, указанные в таблице 1.

Таблица 1 – Файлы для создания электронной подписи

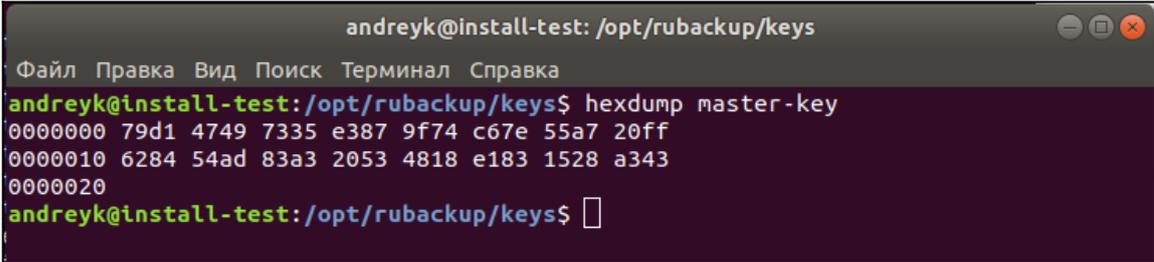
Наименование файла	Назначение
/opt/rubackup/keys/master-key	Мастер-ключ. Секретная фраза для создания ключей и электронной подписи, а так же для защитного преобразования резервных копий
/opt/rubackup/keys/secret-key.pem	Секретный ключ
/opt/rubackup/keys/public-key.pem	Публичный ключ

Вышеуказанные файлы невозможно поместить в какую-либо резервную копию RuBackup во избежании утечки ключей.

Важно! При утере ключа вы не сможете восстановить данные из резервной копии.

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:



```
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
00000100 6284 54ad 83a3 2053 4818 e183 1528 a343
00000200
andreyk@install-test:/opt/rubackup/keys$
```

Подписывать резервную копию электронной подписью или не подписывать определяется клиентом резервного копирования. Для

автоматической электронной подписи резервных копий необходимо включить соответствующую опцию в конфигурационном диалоге клиентского менеджера RuBackup, либо добавить следующую строку в главном конфигурационном файле клиента RuBackup (*/opt/rubackup/etc/config.file*):

```
digital-signature yes
```

Хэш функция электронной подписи может быть определена следующим образом:

```
digital-sign-hash md5
```

По умолчанию алгоритм хэш функции установлен md5, но могут быть выбраны следующие варианты: blake2b512, blake2s256, gost, md4, md5, rmd160, sha1, sha224, sha256, sha384, sha512.

Настройка электронной цифровой подписи резервных копий в оконном клиентском менеджере RuBackup

При первом запуске клиентского менеджера от пользователя потребуется задать пароль. Этот пароль используется при операциях восстановления резервных копий, либо при запросе на удалении резервной копии из репозитория.

В диалоге создания пароля имеются два чек-бокса:

- 1) создать мастер ключ;
- 2) создать пару ключей для цифровой подписи.

Если отмечен чек-брок «Создать мастер ключ», то будет создан или перезаписан файл `/opt/rubackup/keys/master-key`, в котором содержится мастер-пароль, использующийся для защитного преобразования резервных копий и для создания пары ключей для цифровой подписи.

Если отмечен чек-брок «Создать пару ключей для цифровой подписи», то будут созданы секретный и публичный ключи с использованием мастер-ключа.

Для того, чтобы все резервные копии подписывались электронной подписью, необходимо включить эту возможность в диалоге «Конфигурация клиента», выбрав соответствующее значение в комбо-боксе «Клиент будет использовать цифровую подпись». Также возможно изменить алгоритм хэш функции для цифровой подписи в соответствующем комбо-боксе.

После совершения вышеуказанных настроек все резервные копии будут подписываться цифровой подписью.

Создание новой пары ключей электронной подписи

При необходимости создать новую пару ключей электронной подписи это можно сделать в диалоге «Изменение пароля».

В диалоге изменения пароля имеются два чек-бокса:

- 1) создать мастер ключ;
- 2) создать пару ключей для цифровой подписи.

Если отмечен чек-бокс «Создать мастер ключ», то будет создан или перезаписан файл `/opt/rubackup/keys/master-key`, в котором содержится мастер-пароль, используемый для защитного преобразования резервных копий и для создания пары ключей для цифровой подписи.

Если отмечен чек-бокс «Создать пару ключей для цифровой подписи», то будут созданы секретный и публичный ключи с использованием мастер-ключа.

При изменении пары ключей для цифровой подписи сервер через некоторое время запросит у клиента обновление публичного ключа и старый публичный ключ на сервере будет перезаписан новым. Также можно срочно отправить публичный ключ на сервер путем проверки любой резервной копии со стороны клиента.

При установлении новой пары ключей электронной подписи все резервные копии, подписанные старыми ключами, при проверке будут получать статус проверки «Недостовечно» («Mistrusted”).

Настройка обновления публичного ключа электронной подписи в базе данных RuBackup

Основной сервер RuBackup время от времени запрашивает у клиента актуальный публичный ключ. Период получения актуального ключа можно изменить в RuBackup менеджере, в разделе «Глобальная конфигурация», параметр «Период обновления публичного ключа цифровой подписи».

В том случае, если пользователь с помощью оконного менеджера клиента RuBackup инициирует проверку резервной копии, то публичный ключ актуализируется перед проверкой.

Проверка резервной копии в оконном клиентском менеджере RuBackup

При проверке резервных копий они могут принимать статусы проверки (Verification status), указанные в таблице 2.

Таблица 2 – Статусы проверки резервных копий

Статус	Описание	Цвет в таблице резервных копий
Not verified	Резервная копия еще ни разу не была проверена	Темно-красный
Verification failed	Размер файлов резервной копии и md5 суммы отличаются от записи в репозитории	Красный
Verified	Размер файлов резервной копии и md5 суммы соответствуют записи в репозитории, но проверка электронной подписи резервной копии не осуществлялась	Темно-желтый
Unreliable	Проверка электронной подписи резервной копии осуществлялась, но возможно публичный ключ клиента на сервере устарел	Желтый
Mistrusted	Проверка электронной подписи закончилась неудачно	Красный
Trusted	Проверка электронной подписи закончилась удачно	Темно-зеленый

Чтобы проверить статусы резервных копий клиента, необходимо запустить соответствующий клиентский оконный менеджер (например, *rbc_filesystem*) и перейти на вкладку «Резервные копии» («Archives»).

В столбце «Статус проверки» («Verification status») для каждой резервной копии будет указан ее статус. Так же для удобства строки таблицы расцвечены разными цветами в зависимости от статуса проверки резервной копии.