RuBackup

Система резервного копирования и восстановления данных

Электронная подпись резервных копий

Версия 1.0 2019

Оглавление

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.

[Важно !!!] Утечка секретного ключа электронной подписи может скомпрометировать все имеющиеся резервные копии клиента

Принцип электронной подписи резервных копий

Электронная подпись резервных копий выполняется при помощи OpenSSL.

1. **Создание секретного ключа**

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

При выполнении команды потребуется ввести секретную фразу (пароль) и повторить ее.

Если секретная фраза записана в файле /opt/rubackup/keys/master-key, то можно использовать следующею команду:

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

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

2. **Создание публичного ключа**

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

При выполнении команды потребуется ввести секретную фразу (пароль), с которой вы создавали секретный ключ.

Если секретная фраза записана в файле /opt/rubackup/keys/master-key, то можно использовать следующею 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

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

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

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

При создании электронной подписи потребуется ввести секретную фразу (пароль), с которой вы создавали секретный ключ.

Если секретная фраза записана в файле /opt/rubackup/keys/master-key, то можно использовать следующею команду:

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

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

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

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 следующие файлы:

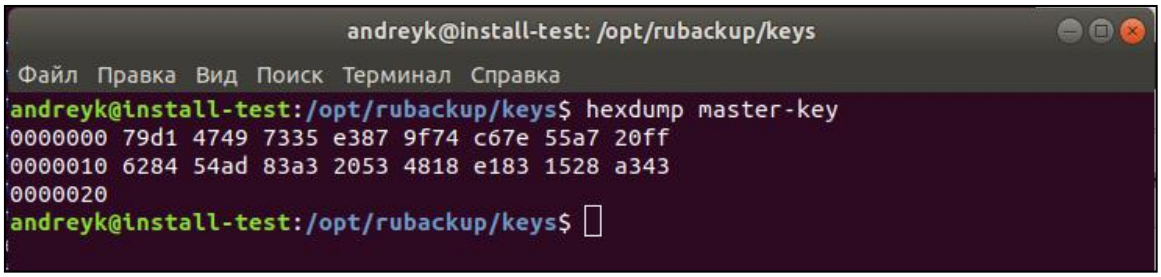
Наименование файла	**Назначение**
/opt/rubackup/keys/master-key	Мастер-ключ. Секретная фраза для создания ключей и электронной подписи, а так же для защитного преобразования резервных копий
/opt/rubackup/keys/secret-key.pem	Секретный ключ
/opt/rubackup/keys/public-key.pem	Публичный ключ

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:



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:

- Создать мастер ключ

- 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, использующийся 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.

Для того, чтобы все резервные копии подписывались электронной подписью, необходимо включить эту позможность в диалоге “Конфигурация клиента”, выбрав соответствующее значение в комбо-боксе “Клиент будет использовать цифровую подпись”. Так же возможно изменить алгоритм хэш функции для цифровой подписи в 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:

- Создать мастер ключ

- 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, использующийся 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. Так же 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 “Недостоверно” (“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 следующие статусы проверки (Verification status):

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 осущуствлялась, 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.