RuBackup

Система резервного копирования и восстановления данных

Создание сертификатов SSL

Версия 1.0 2019

Оглавление

Введение

В поставке RuBackup присутствуют необходимые для работы SSL сертификаты клиента и сервера. Настоящее руководство описывает процесс создания ваших собственных ключей и сертификатов, взамен тех, которые идут в стандартной поставке.

Процедура создания ключей и сертификатов

1. **Создание приватного ключа для корневого сертификата**

   # openssl genrsa -out CA.key 2048

   В результате работы команды будет создан файл CA.key

2. **Создание корневого сертификата, который действует 20000 дней**

   # openssl req -x509 -new -nodes -key CA.key -days 20000 -out CA.crt

   В интерактивном меню вас попросят ввести двухбуквенный код страны, провинцию, город, организацию, подразделение, Common Name и e-mail адрес.

3. **Создание приватного ключа сервера**

   # openssl genrsa -out SERVER.key 2048

   В результате работы команды будет создан файл *SERVER*.key

4. **Создаем запрос на подпись**

   # openssl req -new -key SERVER.key -out SERVER.csr

   В интерактивном меню вам потребуется ответить на те же вопросы, что и при создании корневого сертификата. Нужно, чтобы введенный вами Common Name отличался от Common Name у корневого сертификата.

5. **Подписываем запрос корневым сертификатом и создаем рабочий сертификат сервера**

   # openssl x509 -req -in SERVER.csr -CA CA.crt -CAkey CA.key -CAcreateserial -out SERVER.crt -days 20000

   В результате выполнения команды будет создан файл SERVER.crt.

6. **Генерация DH-параметров, необходимые для работы сервера**

   # openssl dhparam -out dh2048.pem 2048

Проверка

1. **Проверяем самоподписанный сертификат**

   # openssl verify -CAfile CA.crt CA.crt

   Эта команда должна возвратить OK.

2. **Проверяем сертификат сервера**

   # openssl verify -CAfile CA.crt SERVER.crt

   Эта команда должна возвратить *OK.*

3. **Эта команда должна возвратить ошибку, так как сертификат сервера не является самоподписанным**

   # openssl verify -CAfile SERVER.crt SERVER.crt

Размещение сертификатов и ключей

1. **Сертификат клиента**

Сертификат CA.crt необходимо разместить в каталоге /opt/rubackup/keys/client каждого клиента RuBackup.

2. **Рабочий сертификат и ключ рабочего сертификата сервера**

Рабочий сертификат сервера SERVER.crt, ключ SERVER.key, а так же файл dh2048.pem необходимо поместить в каталог /opt/rubackup/keys/server каждого сервера RuBackup.

3. **Ключ корневого сертификата клиента**

Файл CA.key необходимо убрать в надежное место. Они не должен находится ни на сервере, ни на клиенте RuBackup.