RuBackup
Система резервного копирования и восстановления данных

Создание сертификатов и ключей SSL

RuBackup

Версия 1.9

2022 г.

Содержание

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

Для создания ключей и сертификатов необходимо выполнить следующий действия:

1. Создать приватный ключ для корневого сертификата:

```
# openssl genrsa -out CA.key 2048
```

В результате работы команды будет создан файл CA.key.

2. Создать корневой сертификат, 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. Создать приватный ключ сервера:

```
# openssl genrsa -out SERVER.key 2048
```

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

4. Создать 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. Подписать запрос корневым сертификатом и создать 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, необходимых для работы сервера

```
# openssl dhparam -out dh2048.pem 2048
```

Проверка созданных ключей и сертификатов

Для проверки созданных ключей и сертификатов необходимо выполнить следующие действия:

1. Проверить самоподписанный сертификат:

```
# openssl verify -CAfile CA.crt CA.crt
```

   Эта команда должна возвратить OK.

2. Проверить 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 также 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.