HAProxy

Установка и настройка HAProxy на CentOS 7

1. Установка зависимостей

```
yum install openssl-devel pcre-devel make gcc -y
```

2. Загрузка исходных текстов

Скачайте стабильную версию HAproxy, например в директорию /tmp

```
cd /tmp
wget http://www.haproxy.org/download/1.7/src/haproxy-1.7.2.tar.gz -O- | tar -
zx
```

3. Сборка HAproxy

Перейдите в разархивированную директорию с исходниками

```
cd haproxy-*
make TARGET=linux2628 USE_PCRE=1 USE_OPENSSL=1 USE_ZLIB=1 USE_CRYPT_H=1
USE_LIBCRYPT=1
make install
```

4. Создание пользователя haproxy

```
useradd haproxy
```

5. Создание каталога /var/lib/haproxy/

```
mkdir /var/lib/haproxy/
```

6. Создание .pem файла из SSL сертификатов, импортированных на WCS-сервер

```
cat test.flashphoner.com.crt ca.pem sub.class2.server.ca.pem
test.flashphoner.com.key | tee test.flashphoner.com.pem
```

Здесь (предположим, что сертификаты получены от провайдера StartSSL): - `test.flashphoner.com.crt` - файл сертификата - `test.flashphoner.com.key` - файл приватного ключа - `ca.pem` - корневой сертификат - `sub.class2.server.ca.pem` - промежуточный сертификат

8. Создание файла конфигурации

Создайте файл конфигурации `/etc/haproxy/haproxy.cfg` со следующим содержимым:

/etc/haproxy/haproxy.cfg

В строке

```
bind SET_YOUR_IP:443 ssl crt /path/to/your/certificate/cert.pem
```

замените
- `SET_YOUR_IP` - на публичный IP WCS-сервера
- `/path/to/your/certificate/cert.pem` - на путь к .pem файлу, созданному из сертификатов, импортированных на WCS-сервер

9. Создание init файла для init.d

Создайте init файл `/etc/init.d/haproxy` со следующим содержимым:

/etc/init.d/haproxy

9. Добавление haproxy в автозапуск

```
chmod a+x /etc/init.d/haproxy
chkconfig --add haproxy
chkconfig haproxy on
```

10. Запуск haproxy

```
service haproxy start
```

Проверка HAProxy

1. Убедитесь, что haproxy слушает порт 443

```
netstat -antp | grep 443
```

Пример результата команды:

```
tcp 0 0 192.168.1.1:443 0.0.0.0:* LISTEN 24083/haproxy
```

Если порт занят другой службой, завершите соответствующий процесс и перезапустите haproxy:

```
service haproxy restart
```

2. Убедитесь, что сертификаты, использованные для создания .pem файла, указанного в файле конфигурации haproxy.cfg, импортированы на WCS-сервер
   Подробнее о сертификатах для WCS-сервера см. Websocket SSL
3. Откройте панель управления WCS-сервера через HTTPS

```
https://<domain name or IP of the WCS server>:8888/admin/
```

4. Проверьте работу demo-примера с портом 443
   Open Two Way streaming demo example, change the wss port to 443 and start publishing the stream