

Role LB - Not Redundant

Configuration haproxy

The structure of the configuration file of the haproxy service is quite complex. For this reason it is recommended to use an appropriate template from the central jtel download directory to speed up the configuration work. There are two templates, which differ in whether the services are offered via HTTP or via HTTPS. If provision via HTTPS is desired, a file with a valid certificate and the corresponding private key in PEM-base64--format must be provided in addition to the configuration file.

Downloading the following configuration template is a good starting point for a system that should be accessible via HTTP:

Download the HTTP configuration template

```
curl https://cdn.jtel.de/downloads/configs/haproxy-std.cfg > /etc/haproxy/haproxy.cfg
```

If, on the other hand, it is desired that HTTP accesses are automatically redirected to HTTPS and all accesses are to take place via HTTPS, the following configuration template must be downloaded:

Download the HTTPS configuration template

```
curl https://cdn.jtel.de/downloads/configs/haproxy-ssl.cfg > /etc/haproxy/haproxy.cfg
```

If the configuration supports HTTPS, the file `/etc/haproxy/haproxy.pem` must also be created, which contains the certificate, any secondary certificates and the private key. This file must also be given special permissions so that only the root user has read access, otherwise the haproxy service will not start.

For self-generated certificates see [SSL/TLS Certificates - Self-signed certificate](#).

Save the certificate file

```
chmod 400 /etc/haproxy/haproxy.pem
```