Role LB - Redundant

PCS Cluster Installation

Next, PCS Cluster is installed, see Redundancy - Installing PCS Cluster.

Configure virtual IP address (only on one node!)

Then, the virtual IP address of the cluster is configured as a resource:

Configure virtual IP address

```
pcs resource create ClusterIP ocf:heartbeat:IPaddr2 ip=10.4.8.12 cidr_netmask=32 op monitor interval=30s
```

Check whether the address is started:

Check virtual IP address

```
pcs status

# It may take a few seconds before the resource is started. Run this command more than once...

-->

Cluster name: portal
Stack: corosync
Current DC: uk-acd-lb1 (version 1.1.16-12.el7_4.8-94ff4df) - partition with quorum
Last updated: Tue Mar 20 11:57:43 2018
Last change: Tue Mar 20 11:57:33 2018 by root via cibadmin on uk-acd-lb1

2 nodes configured
1 resource configured

Online: [ uk-acd-lb1 uk-acd-lb2 ]

Full list of resources:

 ClusterIP      (ocf::heartbeat:IPaddr2):       Started uk-acd-lb1

Daemon Status:
  corosync: active/enabled
  pacemaker: active/enabled
  pcsd: active/enabled
```

Firewall configuration

Next, the port shares for the mySQL forwarding must be entered in the firewall and saved permanently:

Configure firewall

```
firewall-cmd --zone=public --add-port=3306/tcp --permanent
firewall-cmd --zone=public --add-port=3307/tcp --permanent
firewall-cmd --zone=public --add-port=3308/tcp --permanent
firewall-cmd --reload
```

haproxy configuration for redundancy (both nodes)

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.redundant.http.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.redundant.https.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
```