# Role LB - Adjust haproxy configuration

## Necessary adjustments of the configuration

Note: in case of redundancy, this is done on **BOTH NODES**.

The configuration file `/etc/haproxy/haproxy.cfg` must now be adapted to the environment using a text editor. The file contains various areas that require adjustment.

### Adjustment of the users for the haproxy administration

Via the URL `http(s)://acd-store:7777` an administration interface of the haproxy service can be accessed. For example, backend servers can be excluded from distribution for maintenance or testing purposes. In the standard configuration there is one read-only user (user name: user, password: <password>) and two configuration-authorized users (admin and jtel). Both have the same (known) password. If, for example, you want to change the password for the user admin so that, for example, a Kudnen or partner administrator also has access, you can generate a new password hash with a special command:

**Generate a password hash**

```
python -c 'import crypt; print crypt.crypt("<password>", "$5$jhaProxy")'
```

This command generates a new SHA256 hash for the password "F1r3ball2016" using the salt value "jhaProxy". This hash can then be used for the corresponding user. The user area in the configuration file looks like this:

**User area in /etc/haproxy/haproxy.cfg**

```
userlist stats-auth
        user  admin     password $5$jhaProxy$rd33gRtd4Wt5UyIclODlyjinSeH4N2DjLtKk33PNZH.
        user  jtel      password $5$jhaProxy$rd33gRtd4Wt5UyIclODlyjinSeH4N2DjLtKk33PNZH.
        user  user      password $5$jhaProxy$.saE3wsZ9AzbDMk2jW9WWQqm.4.vgyZCjFdCf5dAKD6
        group admin     users admin,jtel
        group readonly  users user
```

### Adjustment of the URL redirections

The configuration template provides three URL redirections to allow convenient access to the login masks for the system administrator login, the normal user login and the normal user login for the Mini Client. However, this requires an adjustment to the `acdportal_http` or `acdportal_https` area:

**Adjustment of URL redirects**

```
        redirect        location /CarrierPortal/login/RESELLER/CLIENT if root_req
        redirect        location /CarrierPortal/mclogin/RESELLER/CLIENT if mini_req
```

Here the character strings RESELLER or CLIENT must be replaced with the "Reseller UID" and the "Client UID" of the standard client. If these are not specifically adapted when the customer system is set up, both are "default".

## Adjustment of the backend lists

The list of Web application servers to which the request is to be distributed is maintained in the configuration file in two separate areas. The following area is responsible for distributing all calls to the portal:

**Backend area for the web portal**

```
backend jtel_portal
        mode            http
        compression     algo gzip
        compression     type text/xml text/html text/plain text/css text/javascript
        cookie          SERVERID insert indirect nocache
        appsession      JSESSIONID len 32 timeout 3600000
        balance         leastconn # roundrobin
        server          jboss1 192.168.1.31:8080 weight 1 cookie jboss1 check inter 1m
        server          jboss2 192.168.1.32:8080 weight 1 cookie jboss2 check inter 1m
```

In accordance with the system architecture, all web application servers that the web portal should provide (including Mini Client) are to be entered here. A "server" line must be created for each server. Make sure to use unique internal name identifiers and cookie values (in the above case "jbossX" where X is numbered consecutively).

The following area is responsible for the distribution of all SOAP requests:

**Backend area for the SOAP interface**

```
backend jtel_soap
        mode            http
        compression     algo gzip
        compression     type text/xml text/html text/plain text/css text/javascript
        balance         leastconn # roundrobin
        stick-table     type ip size 20k
        stick           on src
        server          jboss1 192.168.1.31:8081 weight 1 cookie jboss1 check inter 1m
        server          jboss2 192.168.1.32:8081 weight 1 cookie jboss2 check inter 1m
```

Here, too, all web application servers that are to provide the SOAP interface must be entered in accordance with the system architecture. A "server" line must be created for each server.Make sure to use unique internal name identifiers and cookie values (in the above case "jbossX" where X is numbered consecutively). These servers are usually the same as those used for portal access. In large installations, however, dedicated Web application servers can also be specified for this purpose.

Wichtiger Hinweis

An important difference between the HTTP under HTTPS version of the configuration file is the port to which SOAP requests are forwarded. If access is via HTTPS, all requests are forwarded to the Web application server on port 8081. This connector is configured so that the JBOSS server knows that the original requests came in over HTTPS and provides the returned URLs (like in WSDL) with the appropriate scheme, even if the communication between haproxy and backend is only over HTTP.

In the pure HTTP version of the configuration template, however, the requests are forwarded to port 8080.

## Starting the haproxy service

After all configuration adjustments have been made, the haproxy service can be started:

**Start the haproxy service**

```
service haproxy start
```

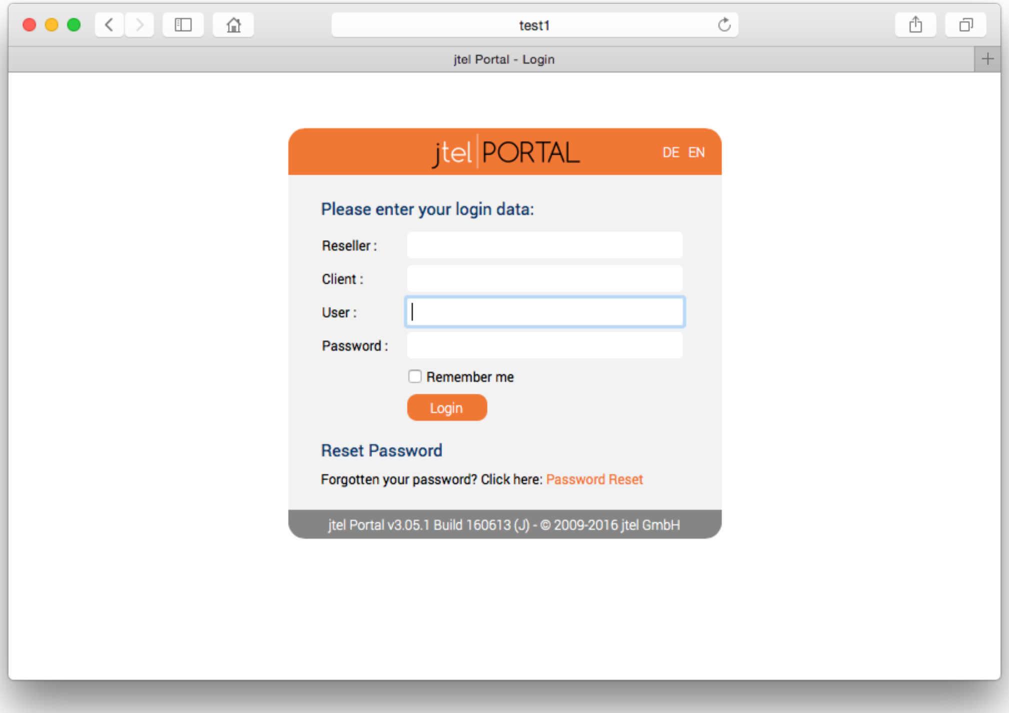
Subsequently, it should be checked whether the service is actually running. If this is not the case, the log file can provide information about possible configuration errors.

In case of configuration changes the haproxy service can update its configuration during operation with the following command:

**Update the configuration during operation**

```
service haproxy reload
```

A final test provides information about the success of the installation. Since the UID values of the Reseller and Client have not yet been renamed at this time, it is recommended to call the URL for the admin login: http://acd-lb.example.com/admin which, if successful, leads to the login mask of the portal.



test1

jtel Portal - Login

jtel PORTAL DE EN

Please enter your login data:

Reseller :

Client :

User :

Password :

□ Remember me

Login

Reset Password

Forgotten your password? Click here: Password Reset

jtel Portal v3.05.1 Build 160613 (J) - © 2009-2016 jtel GmbH

# Further links

- Dokumentation von haproxy