Role LB - All Variants

Description of the role

The role LB provides the central access point to the portal and the SOAP interfaces. Here the requests are distributed to the available Web application servers, taking into account an even load distribution, the possible failure of one or more Web servers and the service-specific restrictions. Furthermore, this role also handles the provision of the TLS encrypted connection via HTTPS. The service can be offered both on HTTP (port 80) and HTTPS (port 443). An automatic redirection to HTTPS or special URLs can also be implemented here (Examples: https://acd.example.com is distributed to: https://acd.example.com/CarrierPortal/login/reseller/client or https://acd.exaple.com/admin is distributed to https://acd.exaple.com/CarrierPortal/sysadmin/login).

DSince the role usually requires very few resources, it is usually (and in the configuration example given here) installed on the same machine on which the STORE role was installed.

Installing the software

The installation of the required software `haproxy` is done with the following command:

Installation of haproxy

```
yum -y install haproxy
mv /etc/haproxy/haproxy.cfg /etc/haproxy/haproxy.cfg.sample
```

The supplied sample configuration file is renamed with the second command so that it is also available for reference purposes at a later time.

activate haproxy

The haproxy service is added to the list of automatically starting services with the following command

haproxy service autostart

```
chkconfig haproxy on
```

Firewall configuration

Next, the port shares for the haproxy service must be entered and permanently stored in the firewall

Configure firewall

```
firewall-cmd --zone=public --add-port=80/tcp --permanent
firewall-cmd --zone=public --add-port=443/tcp --permanent
firewall-cmd --zone=public --add-port=7777/tcp --permanent
firewall-cmd --reload
```

SeLinux Configuration

To enable haproxy to open arbitrary ports, a SeLinux configuration must be made:

SeLinux configuration

```
setsebool -P haproxy_connect_any=1
semanage permissive -a haproxy_t
```

Log haproxy

To save the log output of the haproxy service via the central logging service into a separate log file, the following commands must be executed:

Adjustments to the syslog service

```
sed -i -e 's/#$ModLoad *imudp/$ModLoad imudp/' -e 's/#$UDPServerRun *514/$UDPServerRun 514/' /etc/rsyslog.conf
cat <<EOFF>/etc/rsyslog.d/haproxy.conf
local2.* /var/log/haproxy.log
EOFF
service rsyslog restart
```