Role LB - OCSP stapling (CentOS8/Win2019)

Recently, more use has been made of so-called OCSP stapling instead of CRL (Certificate Revocation Lists).

See also: https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol

If OCSP stapling should be activated in haproxy, the following procedure is used.

See also this website: https://icicimov.github.io/blog/server/HAProxy-OCSP-stapling/ for a very good manual and explanation on which our manual here is based.

check haproxy.cfg

Check that the stats socket is activated. If a different socket is specified, the script must be adjusted below (two lines before exit 0 - in the socat command).

haproxy.cfg

```
global
        stats socket  /var/lib/haproxy/stats
        stats timeout 30s
```

install socat

Install socat

```
yum -y install socat
```

Create script for OCSP stapling and make it executable

Script for OCSP stapling

```
cat <<'EOFF' > /usr/local/bin/haproxy_ocsp_update.sh
#!/bin/bash

# Certificates path and names
DIR="/etc/haproxy"
CERT="haproxy.pem"

# Get the issuer URI, download it's certificate and convert into PEM format
ISSUER_URI=$(openssl x509 -in ${DIR}/${CERT} -text -noout | grep 'CA Issuers' | cut -d: -f2,3)
ISSUER_NAME=$(echo ${ISSUER_URI##*/} | while read -r fname; do echo ${fname%.*}; done)
wget -q -O- $ISSUER_URI | openssl x509 -inform DER -outform PEM -out ${DIR}/${ISSUER_NAME}.pem

# Get the OCSP URL from the certificate
ocsp_url=$(openssl x509 -noout -ocsp_uri -in ${DIR}/${CERT})

# Extract the hostname from the OCSP URL
ocsp_host=$(echo $ocsp_url | cut -d/ -f3)

# Create/update the ocsp response file and update HAProxy
openssl ocsp -noverify -no_nonce -issuer ${DIR}/${ISSUER_NAME}.pem -cert ${DIR}/${CERT} -url $ocsp_url -header "Host=$ocsp_host" -respout ${DIR}/${CERT}.ocsp
[[ $? -eq 0 ]] && [[ $(pidof haproxy) ]] && [[ -s ${DIR}/${CERT}.ocsp ]] && echo "set ssl ocsp-response $(/usr/bin/base64 -w 10000 ${DIR}/${CERT}.ocsp)" | socat
stdio unix-connect:/var/lib/haproxy/stats

exit 0
EOFF

chmod +x /usr/local/bin/haproxy_ocsp_update.sh
```

Test the script

Run the script with: /usr/local/bin/haproxy_ocsp_update.sh

Example return:

```
/etc/haproxy/haproxy.pem: good
This Update: Mar 25 15:33:54 2019 GMT
Next Update: Mar 28 15:33:54 2019 GMT
```

Note: if you get a warning like this:

```
OCSP single response: Certificate ID does not match any certificate or issuer.
```

Then you should be able to fix this by reloading haproxy and running the script again:

```
systemctl reload haproxy
/usr/local/bin/haproxy_ocsp_update.sh
```

Activate CRON job for script

This will execute the script every day.

haproxy.cfg

```
cat <<EOFF >> /etc/crontab
0  0  *  *  * root /usr/local/bin/haproxy_ocsp_update.sh
EOFF
```