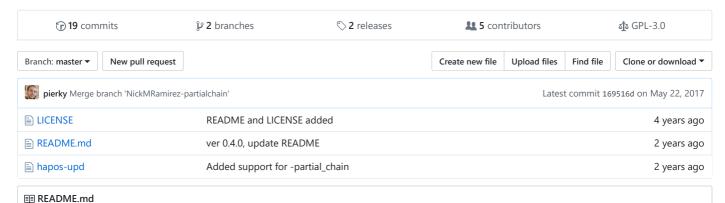
#### pierky / haproxy-ocsp-stapling-updater

## **HAProxy OCSP Stapling Updater**



# **HAProxy OCSP Stapling Updater**

This script extracts and queries the OCSP server present in a certificate to obtain its revocation status, then updates HAProxy by writing the '.issuer' and the '.ocsp' files and by sending it the set ssl ocsp-response command through the local UNIX admin socket.

# Usage

```
hapos-upd [options] --cert crt_full_path
```

The crt\_full\_path argument is the full path to the certificate bundle used in haproxy 'crt' setting. End-entity (EE) certificate plus any intermediate CA certificates must be concatenated there.

An OCSP query is sent to the OCSP server given on the command line (--ocsp-url and --ocsp-host argument); if these arguments are missing,

(--ocsp-url and --ocsp-host argument); if these arguments are missing, URL and Host header values are automatically extracted from the certificate.

If the '.issuer' file already exists it's used to build the OCSP request, otherwise the chain is extracted from crt\_full\_path and used to identify the issuer.

Finally, it writes the related '.issuer' and .'ocsp' files and updates haproxy, using 'socat' and the local UNIX socket (--socket argument, default /run/haproxy/admin.sock).

## Exit codes:

- o ok
- openssl certificates handling error
- 2 OCSP server URL not found
- 3 string parsing / PEM manipulation error
- 4 OCSP error
- 5 haproxy management error
- 9 program error (wrong arguments, missing dependencies)

#### Options:

-d, --debug : don't do anything, print debug messages only.

--keep-temp : keep temporary directory after exiting (for

debug purposes).

-1, --syslog priority : log errors to syslog system log module.

The priority may be specified numerically or as a facility.level pair (e.g.

local7.error).

one in the EE certificate.

```
--ocsp-host host : OCSP server hostname to be used in the
                       'Host:' header; use this instead of the one
                       extracted from the OCSP server URL.
-s, --socket file
                      : haproxy admin socket. If omitted,
                        /run/haproxy/admin.sock is used by default.
                       This script is distributed with only one
                       method to update haproxy: using 'socat'
                       with a local admin-level UNIX socket.
                       Feel free to implement other mechanisms as
                        needed! The right section in the code is
                        "UPDATE HAPROXY", at the end of the script.
-v, --VAfile file
                     : same as the openssl ocsp -VAfile option
                       with 'file' as argument. For more details:
                        'man ocsp'
                       If file = "-" then the chain extracted
                        from the certificate's bundle (or .issuer
                       file) is used (useful for OCSP responses
                        that don't include the signer certificate).
                     : Do not verify OCSP response.
     --noverify
-S, --skip-update
                     : Do not notify haproxy of the new OCSP response.
-h, --help
                      : this help.
```

# **Examples**

Extract OCSP server information from site.pem and use them to create /etc/haproxy/site.pem.issuer and /etc/haproxy/site.pem.ocsp, then update HAProxy via default local UNIX socket (/run/haproxy/admin.sock):

```
:~$ hapos-upd --cert /etc/haproxy/site.pem
```

Download the certificate (EE + intermediate) used by github.com, then run a debug execution on it:

```
:~$ echo "" | openssl s_client -connect github.com:443 -showcerts 2>/dev/null | sed -n -e "/----BEGIN
CERTIFICATE/,/----END CERTIFICATE/p" > github.com.pem
:~$ ./hapos-upd --cert github.com.pem -d --VAfile
Temporary directory: /tmp/hapos-upd.MV7LJsQPXd
OCSP server URL found: http://ocsp.digicert.com
OCSP server hostname: ocsp.digicert.com
Extracting chain from certificates bundle
EE certificate's fingerprint: SHA1 Fingerprint=A0:C4:A7:46:00:ED:A7:2D:C0:BE:CB:9A:8C:B6:07:CA:58:EE:74:5E
2 certificates found in the bundle
Bundle certificate n. 1 fingerprint: SHA1 Fingerprint=A0:C4:A7:46:00:ED:A7:2D:C0:BE:CB:9A:8C:B6:07:CA:58:EE:74:5E -
EE certificate
Bundle certificate n. 2 fingerprint: SHA1 Fingerprint=7E:2F:3A:4F:8F:E8:FA:8A:57:30:AE:CA:02:96:96:63:7E:98:6F:3F -
it's part of the chain
OCSP response verification results: Response verify OK
OCSP response: /tmp/hapos-upd.MV7LJsQPXd/ee.pem: good
       This Update: Apr 17 12:29:00 2015 GMT
        Next Update: Apr 24 12:44:00 2015 GMT
Debug mode: haproxy update skipped.
```

### **Author**

Pier Carlo Chiodi - http://pierky.com

Blog: http://blog.pierky.com Twitter: @pierky