목차

HAProxy SSL 설정 3
여러 인증서 하나로 설정 4
let's encrypt 인증서 4
인증서 갱신 자동화 4

HAProxy SSL 설정

```
frontend web
        bind *:80
        #bind *:443 ssl crt /etc/haproxy/ssl/nas.koov.net.pem crt
/etc/haproxy/ssl/allthatlinux.com.pem crt /etc/haproxy/ssl/linuxdata.kr.pem
crt /etc/haproxy/ssl/dev.koov.net.pem crt
/etc/haproxy/ssl/jenkins.koov.net.pem
        bind *:443 ssl crt-list /etc/haproxy/ssl/crt-list.txt
        reqadd X-Forwarded-Proto:\ https
        http-request set-header X-SSL %[ssl_fc]
        http-response set-header Cache-Control no-cache,\ max-age="600"


....

backend backend_nas.koov.net
        redirect scheme https code 301 if !{ ssl_fc }
        server  static  192.168.0.8:5000        check

backend backend_home.koov.net
        redirect scheme https code 301 if !{ ssl_fc }
        server  static  192.168.0.24:80         check

backend backend_dev.koov.net
        redirect scheme https code 301 if !{ ssl_fc }
        server  static  192.168.0.27:80         check

backend backend_jenkins.koov.net
        redirect scheme https code 301 if !{ ssl_fc }
        server  static  192.168.0.27:8080       check

backend backend_archiva.koov.net
        #redirect scheme https code 301 if !{ ssl_fc }
        server  static  192.168.0.27:8180       check

backend backend_allthatlinux.com
        redirect scheme https code 301 if !{ ssl_fc }
        server  static  192.168.0.21:80         check

backend backend_talk.koov.net
        server  static  192.168.0.28:80         check

....
```

여러 인증서 하나로 설정

let's encrypt 인증서

일단 let's encrypt로 인증서를 발급받게 되면 아래와 같이 4개의 파일이 생성된다.

- cert.pem
- chain.pem
- fullchain.pem
- privkey.pem

이 중 fullchain.pem을 제외한 3개의 파일을 하나로 합쳐준다.

```
# cat cert.pem privkey.pem chain.pem > all.pem
```

'crt-list.txt' 파일 내에 아래와 같이 합쳐놓은 인증서 목록을 기입힌다.

```
all.pem
site1.pem
site2.pem
...
```

또한 발급기관인 letsencrypt의 chain.pem인증서를 ca.pem으로 별도 복사한다.

이후 `haproxy.cfg` 설정에 아래와같이 설정을 하면 해결된다.

```
...
frontend web
        bind *:80
        #bind *:443 ssl crt /etc/haproxy/ssl/nas.koov.net.pem crt
/etc/haproxy/ssl/allthatlinux.com.pem crt /etc/haproxy/ssl/linuxdata.kr.pem
crt /etc/haproxy/ssl/dev.koov.net.pem crt
/etc/haproxy/ssl/jenkins.koov.net.pem  # 기존에 하나씩 모두 기입하는 방법
        bind *:443 ssl crt-list /etc/haproxy/ssl/crt-list.txt ca-file
/etc/haproxy/ssl/ca.pem verify optional # 한 파일에 모두 기입하는 방법
        reqadd X-Forwarded-Proto:\ https
        http-request set-header X-SSL %[ssl_fc]
        http-response set-header Cache-Control no-cache,\ max-age="600"
...
```

인증서 갱신 자동화

- Let's Encrypt(CertBot) SSL with HAProxy

From:
https://atl.kr/dokuwiki/ - **AllThatLinux!**

Permanent link:
https://atl.kr/dokuwiki/doku.php/haproxy_ssl_%EC%84%A4%EC%A0%95

Last update: **2020/02/21 07:06**