Table of contents

1 Let's Encrypt 무료 인증서 자동갱신 및 Apache2에 TLS/SSL 적용

언제나 그렇듯 클리앙 팁&강좌 게시판과 사용기게시판을 보다가 우연히 acme.sh을 이용한 무료 SSL 자동 갱신에 대한 글을 보았다. 안 그래도 최근 SSL/TLS 적용해야 할 일이 있기도 했기에 바로 착수했다. 우선 목표는 acme.sh를 이용해서 인증서 자동 갱신 및 갱신 후 아파치 자동 재시작하는 것이다.

1.1 acme.sh

Let's Encrypt 무료 인증서를 자동갱신해주는 쉘스크립트이다. Ubuntu 12.04에서 권한때문에 문제 생기는 게 귀찮아서 acme.sh 실행시 sudo를 사용할 예정인데, crontab에 등록해야 하므로 비밀번호 입력을 생략하기 위해 vi /etc/sudoer한 후 아이디 ALL=(ALL:ALL) NOPASSWD:ALL'처럼 수정해준다. 이제 암호를 다시 입력하지 않고도 sudo를 사용할 수 있게 되었다. 만약 권한 문제가 없으리라 생각되면 이 과정은 생략해도 될듯 하다. 이제 acme.sh를 다운받아서 이제 인증서 생성 및 적용하면 되는데, 무슨 이유에서인지 sudo사용시 절대경로를 지정해야만 실행이 되었다.

```
sudo ~/.acme.sh/acme.sh --issue -d abc.com -w /var/www/wp_abc_com
[Wed Mar 15 13:40:27 EDT 2017] Single domain='abc.com'
[Wed Mar 15 13:40:27 EDT 2017] Getting domain auth token for each domain
[Wed Mar 15 13:40:27 EDT 2017] Getting webroot for domain='abc.com'
[Wed Mar 15 13:40:27 EDT 2017] Getting new-authz for domain='abc.com'
[Wed Mar 15 13:40:28 EDT 2017] The new-authz request is ok.
...
[Wed Mar 15 13:40:29 EDT 2017] Cert success.
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
[Wed Mar 15 13:40:29 EDT 2017] Your cert is in  /home/아이디/.acme.sh/abc.com/abc.com.cer
[Wed Mar 15 13:40:29 EDT 2017] Your cert key is in  /home/아이디/.acme.sh/abc.com/abc.com.key
[Wed Mar 15 13:40:29 EDT 2017] The intermediate CA cert is in  /home/아이디/.acme.sh/abc.com/ca.cer
[Wed Mar 15 13:40:29 EDT 2017] And the full chain certs is there:  /home/아이디/.acme.sh/abc.com/fullchain.cer
```

마지막 부분에 인증서가 저장된 위치를 보여주면 인증서 생성이 성공된 것이다. crontab -e 해서 보면 acme.sh에 대한 항목이 이미 생성되어 있는 것을 볼 수 있다. 개인 취향상 자동 지정된 시간을 매일 자정에 맞추었고 sudo지정 및 절대경로로 변경했다.

```
0 0 * * * sudo "/home/아이디/.acme.sh"/acme.sh --cron --home "/home/아이디/.acme.sh" > /dev/null
```

1.2 Apache

아파치에 인증서 갱신 적용하기 이제 아파치에 적용해야 할 시간이다. 그런데 이 부분이 조금 어려웠다. 최초 적용시에는 아무래도 수동으로 직접 인증서를 복사해줘야 하는 것으로 보인다. 복사하지 않고 했더니 자꾸 에러가 났다.

```
# 먼저 인증서를 저장할 디렉토리를 생성하자
sudo mkdir /etc/apache2/ssl

# 이제 생성된 인증서를 복사해넣자.
sudo cp /home/아이디/.acme.sh/abc.com/abc.com.cer /etc/apache2/ssl
sudo cp /home/아이디/.acme.sh/abc.com/abc.com.key /etc/apache2/ssl
sudo cp /home/아이디/.acme.sh/abc.com/fullchain.cer /etc/apache2/ssl
```

이제는 httpd.conf를 수정해서 https가 사용가능하게 하고, http로 접속시 자동으로 https로 변경되도록 해보자. sudo vi /etc/apache2/httpd.conf해서 다음을 추가/수정한다.

```
# Load SSL module
LoadModule ssl_module /usr/lib/apache2/modules/mod_ssl.so

# 기존 VirtualHost를 수정해서 https로 자동 이동되도록 함
<VirtualHost *:80>
ServerName      abc.com
ServerAlias     www.abc.com
DocumentRoot    /var/www/wp_abc_com
#  외부링크방지
SetEnvIfNoCase Referer abc₩.com link_allow
SetEnvIfNoCase Referer www₩.abc₩.com link_allow
SetEnvIfNoCase Referer clien₩.net link_allow
SetEnvIfNoCase Referer m₩.clien₩.net link_allow
```

```
SetEnvIfNoCase Referer ^$ link_allow
<FilesMatch
 ↪ "₩.(jpe?g|gif|png|bmp|avi|swf|mpe?g|zip|z[00-99]|rar|mp[1-9]|arj|exe|asf|wm[a-z]*|ra[a-z]*|alz|ZIP|Z[00-99])$">
Order Deny,Allow
Allow from env=link_allow
Deny from all
ErrorDocument 403 /error_page.php
</FilesMatch>
CustomLog /var/log/apache2/abc.com.access.log combined
LogLevel Error
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://abc.com%{REQUEST_URI} [L,R=301]
</VirtualHost>

# 위의 설정을 카피한 후 아래 부분을 변경처리
<VirtualHost *:443>
ServerName      abc.com:443
DocumentRoot    /var/www/wp_abc_com
#  외부링크방지
SetEnvIfNoCase Referer abc₩.com link_allow
SetEnvIfNoCase Referer www₩.abc₩.com link_allow
SetEnvIfNoCase Referer clien₩.net link_allow
SetEnvIfNoCase Referer m₩.clien₩.net link_allow
SetEnvIfNoCase Referer ^$ link_allow
<FilesMatch
 ↪ "₩.(jpe?g|gif|png|bmp|avi|swf|mpe?g|zip|z[00-99]|rar|mp[1-9]|arj|exe|asf|wm[a-z]*|ra[a-z]*|alz|ZIP|Z[00-99])$">
Order Deny,Allow
Allow from env=link_allow
Deny from all
ErrorDocument 403 /error_page.php
</FilesMatch>
CustomLog /var/log/apache2/abc.com.access.log combined
LogLevel Error
# 인증서 설정
SSLEngine on
SSLCipherSuite ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH:+MEDIUM:+LOW
SSLCertificateFile /etc/apache2/ssl/abc.com.cer
SSLCertificateKeyFile /etc/apache2/ssl/abc.com.key
SSLCertificateChainFile /etc/apache2/ssl/abc.com.key
# Disable SSL V2 and V3
SSLProtocol all -SSLv2 -SSLv3
</VirtualHost>
```

이제는 https 접속을 위해 포트 443이 막혀있다면, sudo ufw allow 443해서 방화벽에서 열어줘야 한다. 이제 sudo service apache restart하고 http://abc.com 접속해서 https://abc.com 으로 자동 이동되고 안전한 사이트로 표시되는 지 확인해보자. 다 잘 되었다면 이제 acme.sh가 인증서 갱신 후 아까 생성해둔 디렉토리로 인증서를 복사해넣고 아파치를 재기동하게 해주면 끝이다. 이에 앞서 아까 수동으로 복사해둔 인증서들을 삭제하고 다음 명령을 실행해서 인증서들이 잘 복사되는 지 확인하면 된다.

```
sudo "/home/아이디/.acme.sh"/acme.sh -install-cert -d abc.com ₩
-home "/home/아이디/.acme.sh" ₩
-certpath      /etc/apache2/ssl/abc.com.cer ₩
-keypath       /etc/apache2/ssl/abc.com.key ₩
-fullchainpath /etc/apache2/ssl/fullchain.cer ₩
-reloadcmd     "sudo service apache2 force-reload"
```

이제 acme.sh가 생성한 설정을 확인해보자. 다음 갱신이 언제인지, 어디로 인증서를 복사해넣을지 등에 대한 설정이 저장되어 있는 것을 볼 수 있을 것이다. vi /home/아이디/.acme.sh/abc.com/abc.com.conf하면 다음처럼 나올 것이다.

```
Le_Domain='abc.com'
Le_Alt='no'
Le_Webroot='/var/www/wp_abc_com'
```

```
Le_PreHook=''
Le_PostHook=''
Le_RenewHook=''
Le_API='https://acme-v01.api.letsencrypt.org'
Le_Keylength=''
Le_LinkCert='https://acme-v01.api.letsencrypt.org/acme/cert/…'
Le_LinkIssuer='https://acme-v01.api.letsencrypt.org/acme/issuer-cert'
Le_CertCreateTime='1489601638'
Le_CertCreateTimeStr='Wed Mar 15 18:13:58 UTC 2017'
Le_NextRenewTimeStr='Sun May 14 18:13:58 UTC 2017'
Le_NextRenewTime='1494699238'
Le_RealCertPath='/etc/apache2/ssl/abc.com.cer'
Le_RealCACertPath=''
Le_RealKeyPath='/etc/apache2/ssl/abc.com.key'
Le_ReloadCmd='sudo service apache2 force-reload'
Le_RealFullChainPath='/etc/apache2/ssl/fullchain.cer'
```

이제 Let's Encrypt 인증서 자동 갱신 적용이 끝났다.

1.3 Updated

PC 브라우저에서는 문제가 없었는데 안드로이드 크롬에서 보니 insecure로 나와서 다시 확인을 해보았다. certificate chain 파일이 잘못된 듯 했다. acme.sh에서 생성해준 fullchain.cer을 지정해봤으나 타임아웃이 걸릴 정도로 뭔가 문제가 있었고. 구글 검색을 통해https://whatsmychaincert.com 에 가서 사이트명 넣고 chain cert파일을 다운로드 받은 후 SSLCertificateChainFile /etc/apache2/ssl/abc.com.chain.crt처럼 http.conf에 적용했다. 아파치 재부팅 후 테스트해보니 pc와 안드로이드 모두 제대로 나온다.