Let's Encrypt 인증서 발급 방법

이 페이지는 Let's Encypt에서 운영하는 무료 SSL 인증서를 받는 방법에 대해 정리한다.

기준 OS	CentOS 7

사전 준비

EPEL repository 설정

- Certbot이 EPEL package 이므로 EPEL repository를 사용할 수 있도록 설정한다

```
$ yum install epel-release
```

도메인 관리자 권한

SSL을 받을 때 _acme-challenge.<domain> 에 TXT record를 생성해야 하므로 도메인 관리자 계정이 필요하다.

Certbot 설치

```
$ yum install python2-certbot-apache
```

인증서 받기

Certbot은 인증서를 받기 그리고 web server 설정에 반영하기를 지원한다.

본 정리에서는 인증서를 받는 방법에 대해 정리한다.

Step 1) certbot 실행

```
$ certbot certonly -d <  > -d <    > --manual --preferred-challenges dns-01 --force-renewal --manual-public-ip-
logging-ok
```

- 발급하려는 도메인 이름
  예) *.curvc.com
  *.almdemo.curvc.com
  jira.almdemo.curvc.com

Step 2) _acme-challenge 레코드 생성

이 단계는 certbot (letsencrypt)가 도메인 소유주가 맞는지 확인하는 절차로써 certbot이 지정한 문자열을 지정된 도메인 (_acme-challenge.~) 레코드로 생성해 하고 certbot이 이를 확인하는 과정이다.

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please deploy a DNS TXT record under the name
_acme-challenge.almdemo.curvc.com with the following value:

ZFETHF7O9RWoct4tk8jkgrXIqjbZMBA0J1WLW5OITv4

Before continuing, verify the record is deployed.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Press Enter to Continue
```

- 도메인 서비스의 zone edit menu에서 _acme-challenge.<발급하려는 도메인 이름>에 TXT 형식의 레코드를 생성한다.

예) *.curvc.com 이라면: _acme-challenge.almdemo.curvc.com 에 TXT 값 (ZFETHF7O9RWoct4tk8jkgrXIqjbZMBA0J1WLW5OITv4) 레코드 생성 (기존에 존재하면 TXT 값 수정)

일반적으로 도메인 서버에 반영되기까지 시간이 필요하므로 충분히 (2분 이상) 기다리거나, 아래 방법으로 반영 여부를 확인후 Enter를 입력해 다음 단계로 진행한다.

도메인 레코드 반영 확인 방법

```
$ dig -t TXT _acme-challenge.almdemo.curvc.com

; <<>> DiG 9.10.6 <<>> -t TXT _acme-challenge.almdemo.curvc.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26540
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;_acme-challenge.almdemo.curvc.com. IN        TXT

;; ANSWER SECTION:
_acme-challenge.almdemo.curvc.com. 301 IN TXT        "RJULHF7O9RWoct4tk8jkgrXIqjbZMBA0J1WLW5OITv4"

;; Query time: 298 msec
;; SERVER: 10.0.0.3#53(10.0.0.3)
;; WHEN: Thu Sep 13 18:31:11 KST 2018
;; MSG SIZE  rcvd: 107
```

13 line과 같이 설정했던 값이 확인되면 다음 단계로 진행한다.

Step3) 인증서 확인

다음 문구와 같이 발급된 인증서가 저장된 위치를 알려준다.

예) /etc/letsencrypt/live/almdemo.curvc.com

```
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/almdemo.curvc.com/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/almdemo.curvc.com/privkey.pem
   Your cert will expire on 2018-12-12. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot
   again. To non-interactively renew *all* of your certificates, run
   "certbot renew"
```

Step 4) 인증서 사용

저장된 인증서를 필요한 곳에 사용하면 됨

인증서 갱신

```
$ certbot renew
```

참고

- https://certbot.eff.org/lets-encrypt/centosrhel7-apache