목차

Let's Encrypt(CertBot) Wildcard Certificates

— *이강우 2020/12/13 14:36*

이 문서는 Let's Encrypt에서 발급해주는 와일드카드 인증서를 발급받는 방법을 설명한다.

사전준비 사항

와일드카드 인증서는 당연하게도 **도메인에 대한 소유** 권한이 있어야 한다. 인증서 발급 절차 중간에 도메인 정보를 수정하여야 하는 절차가 존재한다.

- 만약 해당 도메인을 소유하고 있고 해당 도메인의 DNS 를 직접 운영중이라면 해당 DNS서버의 **레코드 정보를 직접 수정할 권한**을 가지고 있어야 한다.
- 도메인을 소유하고 있지만 별도의 관리 업체를 통해서(예:가비아, 닷네임등) 도메인을 관리하고 있으며 해당 업체의 DNS서버를 사용중인경우 업체가 제공하는 DNS 레코드 관리 기능을 통해서 아래에서 요구하는 레코드 정보를 수정 할 수 있어야 한다.

이렇게 준비되었다 하더래도 또다른 문제가 있다. 바로 유효기간 90일(3개월)이 지난 이후 갱신할때가 문제이다. 이부분은 아래 문제점 부분에서 설명한다.

발급절차

- 발급받고자 하는 와일드카드 인증서 도메인이 `*.koov.kr` 인 경우
- `koov.kr` 도메인에 대해서는 와일드카드 인증서로 처리가 되지 않으므로 별도로 추가해줘야 한다.

`certbot certonly --manual --preferred-challenges dns -d "koov.kr" -d "*.koov.kr"` 명령어를 통해서 인증서 발급 절차를 시작한다.

```
root@proxy:~# certbot certonly --manual --preferred-challenges dns -d
"koov.kr" -d "*.koov.kr"
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator manual, Installer None
Obtaining a new certificate
Performing the following challenges:
dns-01 challenge for koov.kr
dns-01 challenge for koov.kr

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
NOTE: The IP of this machine will be publicly logged as having requested
this
certificate. If you're running certbot in manual mode on a machine that is
not
```

```
your server, please ensure you're okay with that.

Are you OK with your IP being logged?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
(Y)es/(N)o: y
```

인증서 발급에 대한 약관이 나오며 동의(Y)를 눌러 진행한다.

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
Please deploy a DNS TXT record under the name
_acme-challenge.koov.kr with the following value:

NFH7_ZDQmi_Kz4A_M-SWzXrwJuTVQ1zDEJooI1gQ2pw

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

해당 도메인에 대한 권한을 확인하기 위해 `_acme-challenge.koov.kr` 레코드에 대해 제공된 `NFH7_ZDQmi_Kz4A_M-SWzXrwJuTVQ1zDEJooI1gQ2pw` 키값을 TXT 필드로 등록하라는 메시지가 나온다.

앞서 설명한것처럼 자체 운영 DNS이면 자체 DNS의 해당 필드값을 등록하여주고 재기동 하여 적용해준다. 업체 DNS서비스를 이용한다면 업체에서 제공하는 DNS 레코드 관리 기능을 이용하여 등록하여 준다.

다음으로 진행하기 전에 제대로 등록됐는지 확인하기 위해 별도의 시스템에서 아래 명령어로 확인해본다.

리눅스 `dig` 명령어 사용시

```
root@proxy:~# dig _acme-challenge.koov.kr TXT

; <<>> DiG 9.11.5-P4-5.1+deb10u2-Debian <<>> _acme-challenge.koov.kr TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 719
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;_acme-challenge.koov.kr.   IN    TXT

;; ANSWER SECTION:
```

```
_acme-challenge.koov.kr. 179    IN    TXT    "NFH7_ZDQmi_Kz4A_M-
SWzXrwJuTVQ1zDEJooI1gQ2pw"

;; Query time: 134 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Dec 13 14:47:14 KST 2020
;; MSG SIZE  rcvd: 164
```

리눅스 host 명령어 사용시

```
root@proxy:~# host -t txt _acme-challenge.koov.kr
_acme-challenge.koov.kr descriptive text "NFH7_ZDQmi_Kz4A_M-
SWzXrwJuTVQ1zDEJooI1gQ2pw"
```

윈도우/리눅스 nslookup 명령어 사용시

```
Microsoft Windows [Version 10.0.19041.685]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\KooV>nslookup
기본 서버:  dns.google
Address:  8.8.8.8

> set type=TXT
> _acme-challenge.koov.kr
서버:    dns.google
Address:  8.8.8.8

권한 없는 응답:
_acme-challenge.koov.kr text = "NFH7_ZDQmi_Kz4A_M-SWzXrwJuTVQ1zDEJooI1gQ2pw"
```

위와 같이 ANSWER SECTION에 해당 TXT 레코드 값이 나와야 한다.

그리고 다음으로 진행하도록 한다.

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
Please deploy a DNS TXT record under the name
_acme-challenge.koov.kr with the following value:

D1FHFn5avBVNyoMoQlNVuhrbhEheyaKyWwzm9rauW00

Before continuing, verify the record is deployed.
(This must be set up in addition to the previous challenges; do not remove,
replace, or undo the previous challenge tasks yet. Note that you might be
asked to create multiple distinct TXT records with the same name. This is
```

```
permitted by DNS standards.)

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
Press Enter to Continue
```

다시 두번째 TXT 레코드를 등록하라고 나온다. 여기서 주의할 점은 앞서 등록한 TXT 레코드를 수정하거나 삭제하면 안된다. 두번째 TXT레코드를 **추가로 등록** 하라는것이다. 동일한 _acme-challenge 이름으로 여러개의 TXT 레코드를 등록할 수 있으므로 추가로 등록해주면 된다.

추가 등록해주고 위에서 설명한 방법으로 제대로 등록됐는지 다시한번 확인한다.

```
root@proxy:~# dig _acme-challenge.koov.kr TXT

; <<>> DiG 9.11.5-P4-5.1+deb10u2-Debian <<>> _acme-challenge.koov.kr TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 719
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;_acme-challenge.koov.kr.   IN    TXT

;; ANSWER SECTION:
_acme-challenge.koov.kr. 179    IN    TXT    "NFH7_ZDQmi_Kz4A_M-
SWzXrwJuTVQ1zDEJooI1gQ2pw"
_acme-challenge.koov.kr. 179    IN    TXT
"D1FHFn5avBVNyoMoQlNVuhrbhEheyaKyWwzm9rauW00"

;; Query time: 134 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Dec 13 14:47:14 KST 2020
;; MSG SIZE  rcvd: 164
```

위와같이 2줄의 TXT 레코드가 출력되어야 한다.

정상적으로 등록된것이 확인됐다면 다음으로 진행한다.

```
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/koov.kr/fullchain.pem
   Your key file has been saved at:
```

```
   /etc/letsencrypt/live/koov.kr/privkey.pem
   Your cert will expire on 2021-03-13. 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"
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

인증서 발급이 완료 되었다.

문제점

이 방식으로 wildcard 인증서를 받게 되면 갱신시 아래와 같은 중요한 문제점이 있다.

와일드 카드 인증서를 받는 방식은 DNS 소유권을 확인하는 과정이 필요하기 때문에 갱신시에도 DNS `_acme-challenge` TXT 값을 매번 갱신해서 소유권을 확인하도록 되어있다. 보통 도메인 대행업체를 이용해서 사용하는 대부분의 경우 이 TXT 레코드를 자동으로 변경해주는 기능이 없기 때문에 인증서 자동갱신이 되지 않는다.

certbot 에서 제공하는 TXT 레코드 자동갱신 플러그인은 아래와 같이 다양한 종류를 지원한다.

- `Cloudflare DNS plugin`
- `DigitalOcean DNS plugin`
- `DNSimple DNS plugin`
- `Gehirn DNS plugin`
- `Google DNS plugin`
- `Linode DNS plugin`
- `OVH DNS plugin`
- `RFC 2136 DNS plugin`
- `Route53 DNS plugin`
- `SakuraCloud DNS plugin`

위에서 지원하지 않는 **일반 도메인대행업체의 DNS서버를 이용하여 와일드카드 인증서를 받았다면 자동갱신은 불가능하다**고 보면 된다. 따라서 자동갱신이 가능한 `AWS Route53`, `CloudFlare`, `Google DNS` 등의 서비스를 이용하면 편하게 갱신할 수 있다는점을 참고하기 바란다.

또한 직접 DNS서버(bind같은)를 운영한다면 `rfc2136` 플러그인을 사용하여 갱신도 가능하다.

Cloudflare DNS를 이용한 와일드카드 인증서

`Cloudflare DNS`를 이용중인경우에는 `Cloudflare DNS API`를 이용하여 와일드카드 인증서를 편하게 발급받을수 있다. 또한 갱신도 API를 통해 자동으로 처리되기 때문에 편리하다.

먼저 필요한것은 certbot의 cloudflare plugin을 설치하여야 한다.

```
$ apt install python3-certbot-dns-cloudflare
```

이제 Cloudflare DNS에 본인의 사이트를 등록한 후 API를 이용하기 위한 API Token을 발급받는다.

사이트선택 → API 토큰 → 토큰생성(영역 DNS 편집) 으로 토큰을 생성한다. 생성된 토큰값을 복사한다.

복사한 토큰값을 cloudflare.ini 파일로 저장한다. 이 예제에서는 ~/.secrets/certbot/cloudflare.ini 경로에 생성하였다.

```
# Cloudflare API token used by Certbot
dns_cloudflare_api_token = AABBCCDDEEFF..XXYYZZ
```

이후 해당 토큰을 이용하여 cloudflare plugin을 통해 와일드카드 인증서를 발급받도록 한다.

```
$ certbot certonly --dns-cloudflare --dns-cloudflare-credentials
~/.secrets/certbot/cloudflare.ini -d "koov.kr" -d "*.koov.kr"
```

발급이 완료되었다.

참조링크

- https://hiseon.me/server/letsencrypt-wildcard-certificate/
- https://certbot.eff.org/docs/using.html
- https://blog.realsangil.net/2018/10/letsencrypt-wildcard-certification-renew/
- https://darkstart.tistory.com/109?category=871909
- https://linux.m2osw.com/setting-bind-get-letsencrypt-wildcards-work-your-system-using-rfc-2136
- https://skorotkiewicz.github.io/techlog/automated-lets-encrypt-wildcard-certificates-with-local-bind/