

- Let's Encrypt(CertBot) Wildcard Certificates** 3
 - 3
 - 3
 - 7
- Cloudflare DNS** 7
 - 8

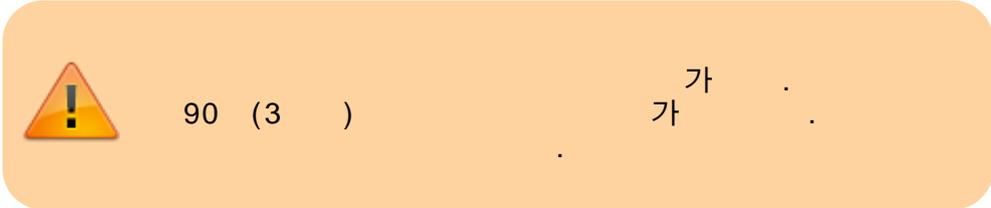
Let's Encrypt(CertBot) Wildcard Certificates

— 2020/12/13 14:36

Let's Encrypt

가

- DNS 가 DNS
- (:가 ,)
DNS 가 DNS



- *.koov.kr
- koov.kr 가 가

```
certbot certonly --manual --preferred-challenges dns -d "koov.kr" -d
"*.koov.kr"
```

```
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

(Y)

- - - - -
- -
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

```

                                _acme-challenge.koov.kr
NFH7_ZDQmi_Kz4A_M-SWzXrwJuTVQ1zDEJooI1gQ2pw      TXT      가
.
      DNS          DNS          DNS
.      DNS          DNS          DNS
.
```

dig

```
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
```

host

```
root@proxy:~# host -t txt _acme-challenge.koov.kr
_acme-challenge.koov.kr descriptive text "NFH7_ZDQmi_Kz4A_M-
SwzXrwJuTVQ1zDEJooI1gQ2pw"
```

/ nslookup

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

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

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

```
:
_acme-challenge.koov.kr text = "NFH7_ZDQmi_Kz4A_M-SwzXrwJuTVQ1zDEJooI1gQ2pw"
```

ANSWER SECTION TXT

```
-----
- -
```

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

D1FHFfn5avBVNyoMoQlNVuhrbhEheyaKyWwzm9rauW00

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


```

/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"

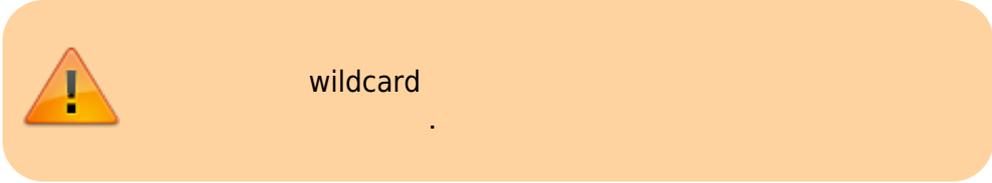
```

- 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

```



```

_acme-challenge TXT          DNS
                             TXT          DNS

certbot          TXT

• 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

DNS          가          DNS          가          AWS Route53, CloudFlare, Google

DNS          DNS (bind )          rfc2136          가

```

Cloudflare DNS

[:https://certbot-dns-cloudflare.readthedocs.io/en/stable/](https://certbot-dns-cloudflare.readthedocs.io/en/stable/)

Cloudflare DNS API
certbot cloudflare plugin

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

```
Cloudflare DNS API API Token  
→ API → ( DNS )  
cloudflare.ini  
~/.secrets/certbot/cloudflare.ini
```

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

cloudflare plugin

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

- <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/>

From:
<https://at1.kr/dokuwiki/> - AllThatLinux!

Permanent link:
https://at1.kr/dokuwiki/doku.php/let_s_encrypt_certbot_wildcard_certificates?rev=1675142467

Last update: **2023/01/31 05:21**

