Step 1 — Install Let’s Encrypt Certbot

Let’s Encrypt provides CLI namely `Certbot` to generate the certificate

```
sudo apt install certbot
```

Step 2 — Generate new certificate using Certbot

The command to generate the cert is relatively simple. You can do for single domain, for multiple domains then just needs to append `-d DOMAIN`. In this case I used `*.DOMAIN` so that the certificate can be used for subdomain as well. The wizard will ask for a few simple information.

```
sudo certbot certonly --manual --preferred-challenges dns -d "*.DOMAIN"
```

```
ongkhawei@ubuntu:~/Desktop$ sudo certbot certonly --manual --preferred-challenge
s dns -d "*.[redacted].me"
[sudo] password for ongkhawei:
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator manual, Installer None
Enter email address (used for urgent renewal and security notices) (Enter 'c' to
cancel): ong[redacted]@gmail.com

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(A)gree/(C)ancel: A

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Would you be willing to share your email address with the Electronic Frontier
Foundation, a founding partner of the Let's Encrypt project and the non-profit
organization that develops Certbot? We'd like to send you email about our work
encrypting the web, EFF news, campaigns, and ways to support digital freedom.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: Y
Obtaining a new certificate
Performing the following challenges:
dns-01 challenge for [redacted].me

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
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:
```

Step3 — Setting DNS TXT ACME Challenge in Namecheap

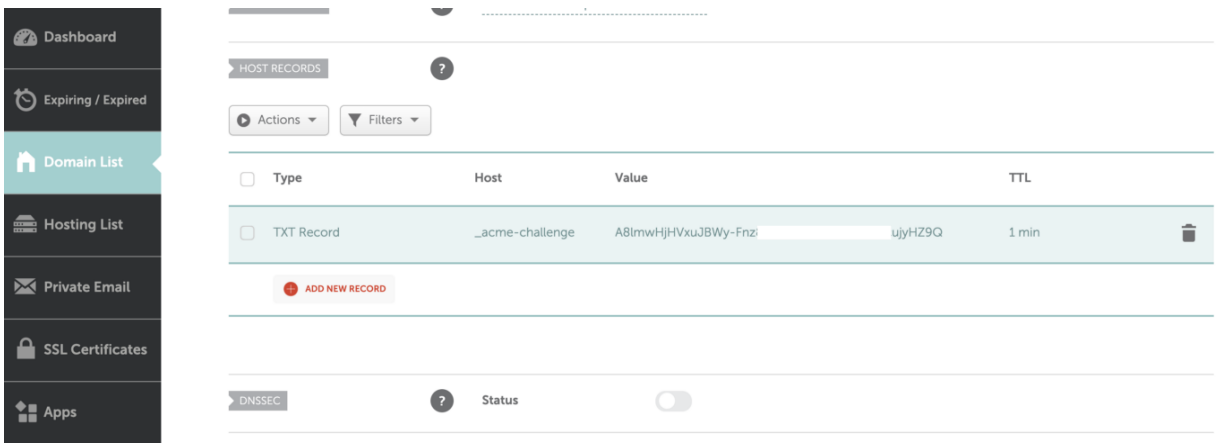
Once Y is entered in the previous step, `Certbot` will revert with ACME challenge token to be configured in DNS provider to allow verification. Copy the token and insert as TXT record in DNS console of Namecheap.

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

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please deploy a DNS TXT record under the name
_acme-challenge.[redacted].me with the following value:

A8lmwHjHVxuJBWy-Fnz[redacted]ujyHZ9Q

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



Please set TTL to 1 minute to allow Top-level DNS servers to pick up this new subdomain — `_acme-challenge.DOMAIN`. You can verify this DNS TXT record using `nslookup` before proceed with verification.

```
nslookup -type=TXT _acme-challenge.DOMAIN
```

```
ongkhawei@ubuntu:~/Desktop$ nslookup -type=TXT _acme-challenge.[redacted].me
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
_acme-challenge.[redacted].me     text = "A8lmwHjHVxuJBWy-Fnz[redacted]ujyHZ9Q"

Authoritative answers can be found from:
```

Step 4 — Verify the domain challenge

Press Enter and `Certbot` will continue with the verification process.

```
Before continuing, verify the record is deployed.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Press Enter to Continue
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/[redacted].me/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/[redacted].me/privkey.pem
   Your cert will expire on 2021-10-08. 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

ongkhawei@ubuntu:~/Desktop$
```

Step 5 — Retrieve the certificate

You will hit permission error when trying to retrieve the file. This is due to folder permission of `/etc/letsencrypt/live`is set to root. Therefore we can set permission to allow other users to read via `sudo chmod +x /etc/letsencrypt/live`

```
ongkhawei@ubuntu:~/Desktop$ more /etc/letsencrypt/live/[redacted].me/fullchain.pem
more: stat of /etc/letsencrypt/live/[redacted].me/fullchain.pem failed: Permission
 denied
ongkhawei@ubuntu:~/Desktop$ sudo chmod +x /etc/letsencrypt/live
[sudo] password for ongkhawei:
```

After that you can extract the `fullchain.pem` and `privkey.pem` for ingress / route / web server configuration.

```
ongkhawei@ubuntu:~/Desktop$ sudo more /etc/letsencrypt/live/[redacted].me/fullchai
n.pem
-----BEGIN CERTIFICATE-----
MIIFITCCBAmgAwIBAgISA5TyY79LFAVuE4NUzSAkq0q9MA0GCSqGSIb3DQEBCwUA
MDIxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYDVQQD
EwJSMzAeFw0yMTA3MTAwNjMxMDdaFw0yMTEwMDgwNjMxMDZaMBgxFjAUBgNVBAMM
DSouc3RqZW5qZW4ubWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDh
ih6xPurzpXD8YivZ8lInbu9RL2lQj6z+vET+DidhnzW5lAwkFoEoqwP46BV1psWO
KdjlyGi6NyTXEU+rQ5LwaNGCR4hy9nVo+koGhqllqIKWoiipdSV0enC/IAWTyZ1M
j9RMDCREW3Ze/D8E2XZZZkcEgru34YOPjIUx8ZyoWvhcmv14RemOLGRfaospc1oK
GiJFI7XRqQ26tXPCrmRW8w+mh3XUWxUAg0VMXK2E7DHjCEqU/ssFL4zlj0QBRzuG
tASkhoxQmbye6KbLXbziSZkZYLZY3oDvtuyOvt8izo5/JQDQq+hFUQl8LsWBdmQP
ebJhKasxbk7j1da9TcInAgMBAAGjggJJMIICRTAOBgNVHQ8BAf8EBAMCBaAwHQYD
VR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMAwGA1UdEwEB/wQCMAAwHQYDVR0O
BBYEFLnTDj6mGLhwjKlSWAK/TSbqWuZIMB8GA1UdIwQYMBaAFBQusxe3WFbLrlAJ
QOYfr52LFMLGMFUGCCsGAQUFBwEBBEkwRzAhBggrBgEFBQcwAYYVaHR0cDovL3Iz
Lm8ubGVuY3Iub3JnMCIGCCsGAQUFBzAChhZodHRwOi8vcjMuaS5sZW5jci5vcmcv
MBgGA1UdEQQRMA+CDSouc3RqZW5qZW4ubWUwTAYDVR0gBEUwQzAIBgZngQwBAgEw
NwYLKwYBBAGC3xMBAQEwKDAmBggrBgEFBQcCARYaaHR0cDovL2Nwcy5sZXRzZW5j
cnlwdC5vcmcwggEFBgorBgEEAdZ5AgQCBIH2BIHzAPEAdgBvU3asMfAxGdiZAKRR
Ff93FRwR2QLBACkGjbIImjfZEwAAAXqPU7y6AAAEAwBHMEUCIQCl9gZ+LAnQvLHX
```

Step 6 — Renew the certificate

Use command : certbot renew

Step 7 — Convert the certificate to keystore

cd /etc/letsencrypt/live/dev1.<domain-name>.com

sudo openssl pkcs12 -export -in fullchain.pem -inkey privkey.pem -out KEYSTORE.p12 -name dev1

Step 8 — Import keystore in wildfly

Insert below configuration in standalone.xml

<keystore path="KEYSTORE.p12" relative-to="jboss.server.config.dir" keystore-password="abc@321" alias="dev1"/>