CentOS 7.x 申請 Let's Encrypt SSL 憑證及排程自動更新憑證

目錄

1. 安裝 certbot

```
[root@localhost ~]# yum -y install epel-release mod_ssl certbot
```

2. 申請憑證

certonly：僅申請憑證，不編輯 httpd.conf
-- webroot：自備 HTTP 伺服器，自行設定 acme-challenge
-w：網域所在的**根目錄路徑**
/var/www/html/ ：網站根目錄路徑
-d：連續請求的功能
--mail：註冊及 SSL 金鑰到期前寄送過期通知

```
◆單一網域
[root@localhost ~]# certbot certonly --webroot -w /var/www/html/ -d yourdomain.nchu.edu.tw --email yourmail@nchu.edu.tw
◆多網域
[root@localhost ~]# certbot certonly --webroot -w /var/www/html/ -d yourdomain1.nchu.edu.tw -d yourdomain2.nchu.edu.tw -d yourdomain3.nchu.edu.tw --email yourmail@nchu.edu.tw
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
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. Do you agree?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: y
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Would you be willing, once your first certificate is successfully issued, 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: n
(也可 y 接收 Let's Encrypt 相關活動、資訊...)
```

```
Account registered.
Requesting a certificate for yourdomain.nchu.edu.tw
Performing the following challenges:
http-01 challenge for yourdomain.nchu.edu.tw
Using the webroot path /var/www/html/test for all unmatched domains.
Waiting for verification...
Cleaning up challenges
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/yourdomain.nchu.edu.tw/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/yourdomain.nchu.edu.tw/privkey.pem
   Your certificate will expire on 2021-11-25. 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
```

確認證書與金鑰

```
[root@localhost ~]# ls /etc/letsencrypt/live/yourdomain.nchu.edu.tw/
cert.pem  chain.pem  fullchain.pem  privkey.pem  README
```

3. Apache 設定 SSL 憑證金鑰

```
[root@localhost ~]# vi /etc/httpd/conf.d/ssl.conf
```

修改 SSLCertificateFile、SSLCertificateKeyFile 及 SSLCACertificateFile 路徑

```
SSLCertificateFile /etc/letsencrypt/live/yourdomain.nchu.edu.tw/cert.pem
SSLCertificateKeyFile /etc/letsencrypt/live/yourdomain.nchu.edu.tw/privkey.pem
SSLCACertificateFile /etc/letsencrypt/live/yourdomain.nchu.edu.tw/fullchain.pem
```

修改完儲存並離開，重新啟動 Apache

```
[root@localhost ~]# systemctl restart httpd
```

4. http 導向 https (兩種方法擇一設定)

(1) 方法 1：修改 httpd.conf

```
[root@localhost ~]# vi /etc/httpd/conf/httpd.conf
```

搜尋關鍵字「Further」至需修改段落

```
# Further relax access to the default document root:
<Directory "/var/www/html">                                        此路徑須為網站根目錄
    Options FollowSymLinks
    AllowOverride All
    Require all granted
    RewriteEngine On
    RewriteCond %{HTTPS} !=on
    RewriteRule ^/?(.*) https://%{SERVER_NAME}/$1 [R,L]
</Directory>
```

修改完儲存並離開，重新啟動 Apache

```
[root@localhost ~]# systemctl restart httpd
```

(2) 方法 2：修改.htaccess(htaccess.txt)

新增

```
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

新增完儲存並離開，重新啟動 Apache

```
[root@localhost ~]# systemctl restart httpd
```

5. 排程自動更新憑證

(1) 建立 script 檔

```
[root@localhost ~]# vi /root/renew.sh
```

新增

```
#!/bin/sh
/usr/bin/certbot renew --quiet --agree-tos --post-hook "systemctl reload httpd"
```

儲存離開後給予 renew.sh 執行權限

```
[root@localhost ~]# chmod 755 /root/renew.sh
```

(2) 設定 crontab 自動續約過期金鑰

```
[root@localhost ~]# crontab -e
```

更新頻率可自行設定 (ex.加入排程讓程式每周六上午 3 點自動更新)

```
# ┌─────────────── 分鐘    (0 - 59)
# │ ┌───────────── 小時    (0 - 23)
# │ │ ┌─────────── 日      (1 - 31)
# │ │ │ ┌───────── 月      (1 - 12)
# │ │ │ │ ┌─────── 星期幾  (0 - 7，0 是週日，6 是週六，7 也是週日)
# │ │ │ │ │
0 3 * * 6 /root/renew.sh > /dev/null 2>&1
```

6. certbot 常用指令

(1) 列出所有憑證及到期日

```
[root@localhost ~]# certbot certificates
Saving debug log to /var/log/letsencrypt/letsencrypt.log
```

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Found the following certs:
  Certificate Name: yourdomain.nchu.edu.tw
    Serial Number: 4a673c7b1a3d38e86ab6c83098ffd7efd02
    Key Type: RSA
    Domains: yourdomain.nchu.edu.tw
    Expiry Date: 2021-11-25 05:51:26+00:00 (VALID: 89 days)
    Certificate Path: /etc/letsencrypt/live/yourdomain.nchu.edu.tw/fullchain.pem
    Private Key Path: /etc/letsencrypt/live/yourdomain.nchu.edu.tw/privkey.pem
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

(2) 測試是否能更新

```
[root@localhost ~]# certbot renew --dry-run
Saving debug log to /var/log/letsencrypt/letsencrypt.log


- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Processing /etc/letsencrypt/renewal/yourdomain.nchu.edu.tw.conf
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Cert not due for renewal, but simulating renewal for dry run
Plugins selected: Authenticator webroot, Installer None
Starting new HTTPS connection (1): acme-staging-v02.api.letsencrypt.org
Account registered.
Simulating renewal of an existing certificate for yourdomain.nchu.edu.tw
Performing the following challenges:
http-01 challenge for yourdomain.nchu.edu.tw
Using the webroot path /var/www/html/test for all unmatched domains.
Waiting for verification...
Cleaning up challenges
```

```

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
new certificate deployed without reload, fullchain is
/etc/letsencrypt/live/yourdomain.nchu.edu.tw/fullchain.pem
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Congratulations, all simulated renewals succeeded:
  /etc/letsencrypt/live/yourdomain.nchu.edu.tw/fullchain.pem (success)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

(3) 手動立即更新 SSL 憑證

```
[root@localhost ~]# certbot renew
Saving debug log to /var/log/letsencrypt/letsencrypt.log

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Processing /etc/letsencrypt/renewal/yourdomain.nchu.edu.tw.conf
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Cert not yet due for renewal

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The following certificates are not due for renewal yet:
  /etc/letsencrypt/live/yourdomain.nchu.edu.tw/fullchain.pem expires on 2021-11-25
(skipped)
No renewals were attempted.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```