HTTPS 免費憑證安裝
Lets Encrypt

臺灣大學計資中心
網路組
游子興

大綱

* Let’s Encrypt
* Install Certbot
* Certbot Plugins
* Plugin: Standalone
* Plugin: Webroot
* Plugin: Apache
* Wildcard Certificates
* Certificate Renew
* 其他指令

Let’s Encrypt

Let's Encrypt

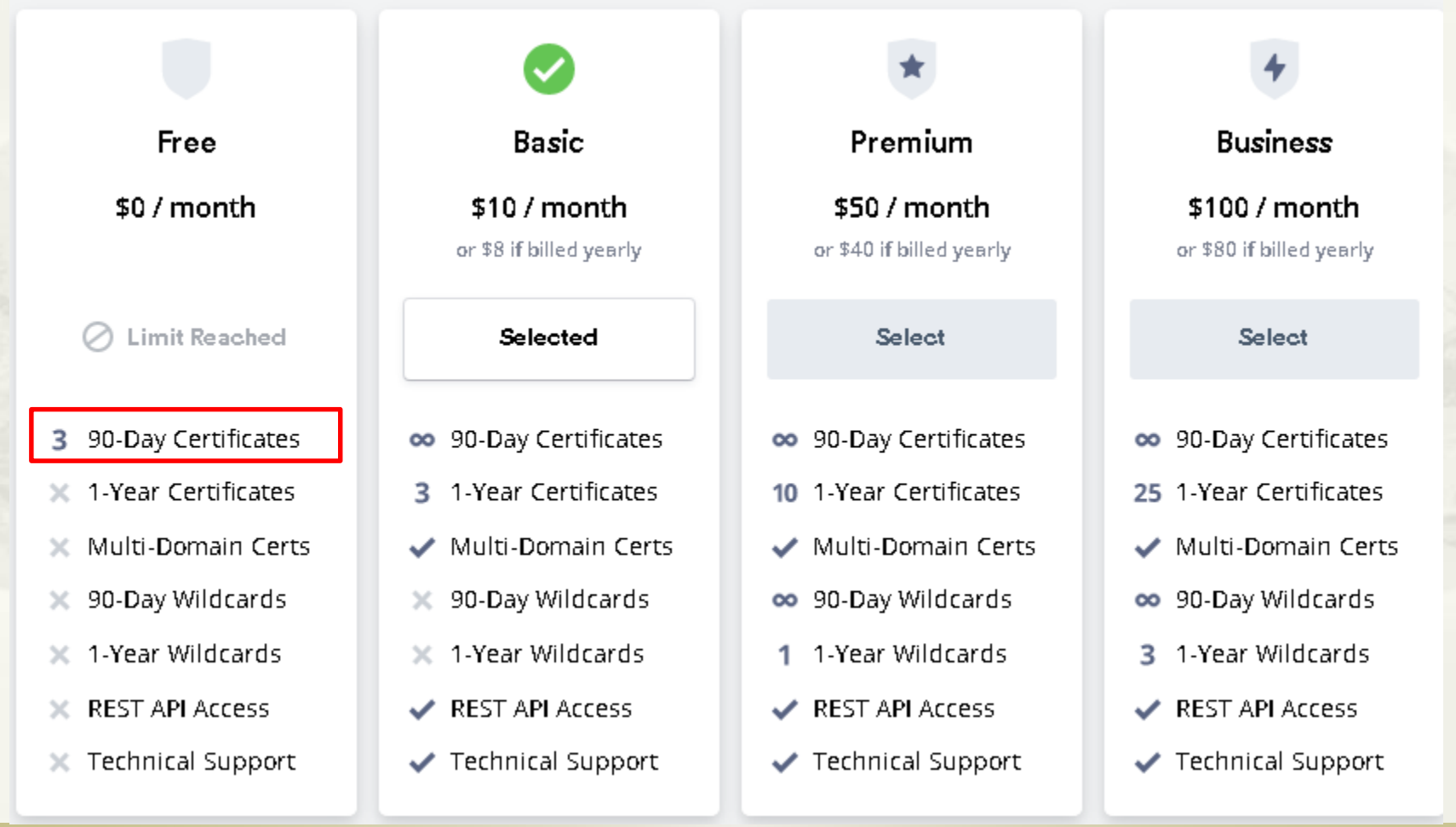
* Let‘s Encrypt 是免費、自動化和開放的憑證頒發機構，由非營利組織網路安全研究小組 (Internet Security Research Group, ISRG) 營運
* 旨在以自動化流程消除手動建立和安裝憑證的複雜流程，並推廣使全球資訊網伺服器加密服務，為安全網站提供免費的SSL/TLS憑證
* https://letsencrypt.org/sponsors/
* 參考資料
  * https://letsencrypt.org/getting-started/

Automatic Certificate Management Environment (ACME) Protocol

- Designed by the Internet Security Research Group (ISRG) for their Let's Encrypt service.
- Use ACME protocol to verify that you control a given domain name and to issue you a certificate.
- To get a Let’s Encrypt certificate, you’ll need to choose a ACME Client software.
  - https://letsencrypt.org/docs/client-options/
  - Linux: Certbot (Recommended)
  - Wndows: win-acme (Recommended)

網頁認證僅限制 3次

ZeroSSL or SSL For Free



HTTPS 免費憑證安全性

方法	ACME Method	Create Private Key	Web Server Config	Auto Renew	安全性
Create From CSR	Web ACME Client	User	User	Not Support	★★★
Authenticator	Web ACME Client	ACME Client	User	Support	★★
Authenticator & Installer	ACME Client	ACME Client	ACME Client	Support	★

- Will Certbot generate or store the private keys for my certificates on Let's Encrypt's servers?
  - No. Never.
  - The private key is always generated and managed on your own servers, not by the Let's Encrypt certificate authority.

Install Certbot

Certbot

- Command Line 自動化安裝工具
  - https://certbot.eff.org
  - https://certbot.eff.org/instructions?ws=apache&os=ubuntufocal

- 參考文件
  - https://certbot.eff.org/docs/
  - https://eff-certbot.readthedocs.io/en/stable/using.html#certbot-command-line-options
  - https://certbot.eff.org/faq
- Linux : requires Python 3.6+
- Require root/administrator access

Use Snap

- Install Snap
  - sudo snap install core
  - sudo snap refresh core
- Install Certbot
  - sudo snap install --classic certbot
  - sudo ln -s /snap/bin/certbot /usr/bin/certbot
- Install Plugin (不支援 Third-party plugins)
  - Confirm plugin containment level
    - sudo snap set certbot trust-plugin-with-root=ok
  - Install
    - sudo snap install certbot-dns-rfc2136

Use pip

- Install system dependency
  - Debian, Ubuntu
    - sudo apt install python3 python3-venv libaugeas0
  - Fedora, CentOS
    - sudo dnf install python3 augeas-libs
- Set up a Python virtual environment
  - sudo python3 -m venv /opt/certbot/
  - sudo /opt/certbot/bin/pip install --upgrade pip
- Install Certbot
  - sudo /opt/certbot/bin/pip install certbot
  - ln -s /opt/certbot/bin/certbot /usr/bin/certbot
- Install Plugin (支援 Third-party plugins)
  - sudo /opt/certbot/bin/pip install certbot-apache
  - sudo /opt/certbot/bin/pip install certbot-dns-standalone

Use pip
(Without Python virtual environment)

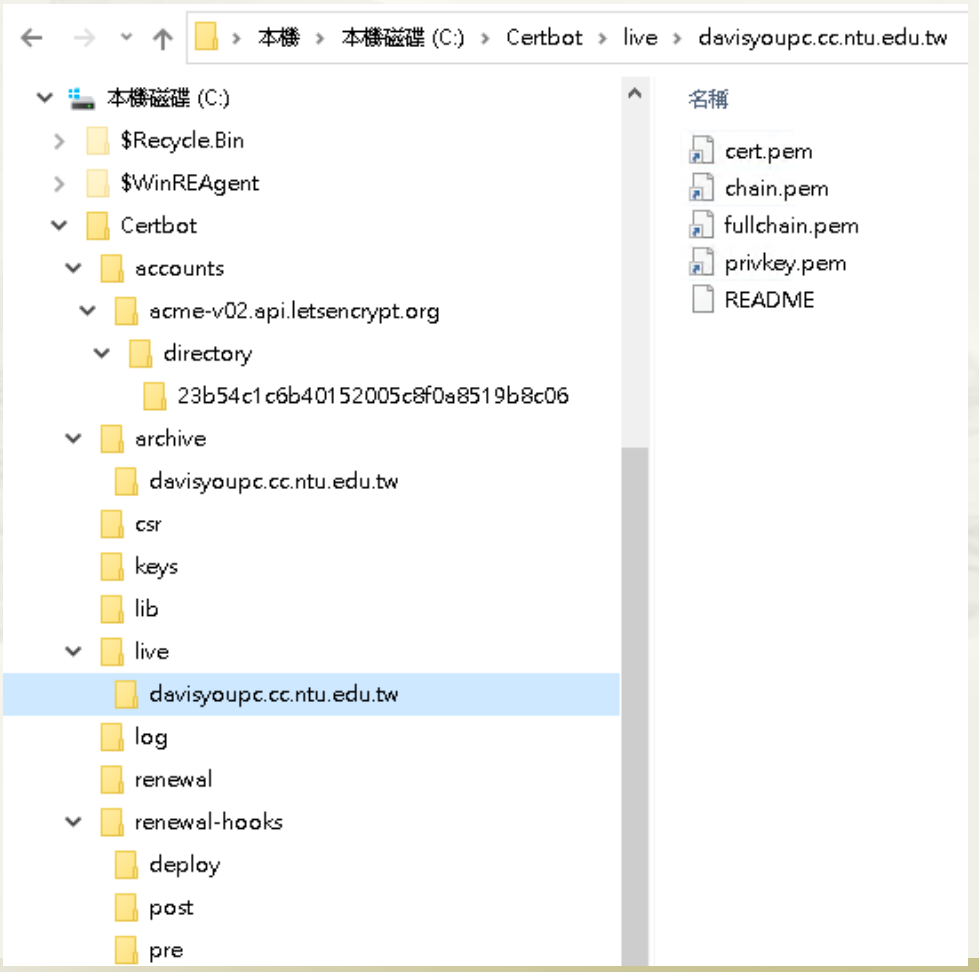
- Install & Upgrade
  - apt install python3-pip libaugeas0
  - pip install --upgrade pip
  - pip install zope.interface --upgrade
- Install Certbot
  - pip install certbot
- Install Plugin (支援 Third-party plugins)
  - pip install certbot-apache
  - pip install certbot-dns-standalone

Certbot for Windows

- https://certbot.eff.org/instructions?ws=other&os=windows
- Download & Install
  - https://dl.eff.org/certbot-beta-installer-win32.exe
  - Install @ C:\Program Files (x86)\Certbot
- Run (在任意目錄執行皆可)
  - run CMD.EXE “Run as administrator”
- Plugins
  - Only Support: Standalone, Webroot

Certbot Config Files Path

- Linux
  - /var/log/letsencrypt
  - /var/lib/letsencrypt
  - /etc/letsencrypt
    - /etc/letsencrypt/live/<domain name>
    - cert.pem: Server Certificate
    - chain.pem: Intermediate + Root Certificates
    - fullchain.pem: Server + Intermediate + Root Certificates
    - privkey.pem
- 還原成初始設定
  - 刪除上述路徑及檔案
- Windows: C:\Certbot



Certbot Plugins

Certbot Plugins 分類

* Authenticators
  * automatically perform the steps to prove that you control the domain to get the certificate.
* Installers
  * automatically modify web server's configuration to install the certificate.
* Some plugins are both authenticators and installers

Authenticator(HTTP) Background Steps

- Create 驗證目錄與檔案 in Webroot
  - Web 根目錄 /.well-known/acme-challenge/RpUCT8SSJN77t7mZBHkI6_BLhtIm13LyFVzHJ1mhcKI
- From Internet 存取上述檔案
  - http://x.x.x.x/.well-known/acme-challenge/...
- Create Private Key and Certificates
  - /etc/letsencrypt/live/[certificate_name]/
    - cert.pem chain.pem fullchain.pem privkey.pem

Installer Background Steps

- For Apache
  - Enable SSL Module
    - a2enmod ssl
  - Create apache config
    - /etc/apache2/sites-available/000-default-le-ssl.conf
    - /etc/apache2/sites-enabled/000-default-le-ssl.conf

Certbot Plugins (Official)

Plugin	Auth	Inst	Notes	Challenge types (port)
apache	Y	Y	Apache.	http (80)
Nginx	Y	Y	Nginx.	http (80)
Webroot	Y	N	Get certificate by writing to the webroot directory of an already running webserver.	http (80)
standalone	Y	N	For systems without webserver. (Certbot 即是 Webserver)	http (80)
DNS plugins	Y	N	Get certificate by modifying DNS records to prove you have control over a domain. Domain validation is the only way to get **wildcard** certificates.	dns (53)
manual	Y	N		http (80) or dns (53)

Certbot Plugins (Official)
DNS plugins

- certbot-dns-cloudflare
- certbot-dns-cloudxns
- certbot-dns-digitalocean
- certbot-dns-dnsimple
- certbot-dns-dnsmadeeasy
- certbot-dns-gehirn
- certbot-dns-google
- certbot-dns-linode
- certbot-dns-luadns
- certbot-dns-nsone
- certbot-dns-ovh
- certbot-dns-rfc2136
- certbot-dns-route53
- certbot-dns-sakuracloud
- Ref. https://eff-certbot.readthedocs.io/en/stable/using.html#dns-plugins

Third-party Plugins

* https://certbot.eff.org/docs/using.html#third-party-plugins

Plugin	Auth	Inst	Notes
haproxy	Y	Y	Integration with the HAProxy load balancer
s3front	Y	Y	Integration with Amazon CloudFront distribution of S3 buckets
gandi	Y	N	Obtain certificates via the Gandi LiveDNS API
varnish	Y	N	Obtain certificates via a Varnish server
external-auth	Y	Y	A plugin for convenient scripting
pritunl	N	Y	Install certificates in pritunl distributed OpenVPN servers
proxmox	N	Y	Install certificates in Proxmox Virtualization servers
dns-standalone	Y	N	Obtain certificates via an integrated DNS server
dns-ispconfig	Y	N	DNS Authentication using ISPConfig as DNS server
dns-clouddns	Y	N	DNS Authentication using CloudDNS API
dns-lightsail	Y	N	DNS Authentication using Amazon Lightsail DNS API
dns-inwx	Y	Y	DNS Authentication for INWX through the XML API
dns-azure	Y	N	DNS Authentication using Azure DNS
dns-godaddy	Y	N	DNS Authentication using Godaddy DNS
njalla	Y	N	DNS Authentication for njalla
DuckDNS	Y	N	DNS Authentication for DuckDNS
Porkbun	Y	N	DNS Authentication for Porkbun
Infomaniak	Y	N	DNS Authentication using Infomaniak Domains API

List Default Installed Plugins

* ~# certbot plugins
* Snap Install

```
root@vm-ubuntu-cc411:~# certbot plugins
Saving debug log to /var/log/letsencrypt/letsencrypt.log

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
* apache
Description: Apache Web Server plugin
Interfaces: Installer, Authenticator, Plugin
Entry point: apache = certbot_apache._internal.entrypoint:ENTRYPOINT

* nginx
Description: Nginx Web Server plugin
Interfaces: Installer, Authenticator, Plugin
Entry point: nginx = certbot_nginx._internal.configurator:NginxConfigurator

* standalone
Description: Spin up a temporary webserver
Interfaces: Authenticator, Plugin
Entry point: standalone = certbot._internal.plugins.standalone:Authenticator

* webroot
Description: Place files in webroot directory
Interfaces: Authenticator, Plugin
Entry point: webroot = certbot._internal.plugins.webroot:Authenticator
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

* Pip Install

```
root@vm-ubuntu-cc411:~# certbot plugins
Saving debug log to /var/log/letsencrypt/letsencrypt.log

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
* standalone
Description: Spin up a temporary webserver
Interfaces: Authenticator, Plugin
Entry point: standalone = certbot._internal.plugins.standalone:Authenticator

* webroot
Description: Place files in webroot directory
Interfaces: Authenticator, Plugin
Entry point: webroot = certbot._internal.plugins.webroot:Authenticator
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

* Windows

```
C:\Windows\system32>certbot plugins
Saving debug log to C:\Certbot\log\letsencrypt.log

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
* standalone
Description: Spin up a temporary webserver
Interfaces: Authenticator, Plugin
Entry point: standalone = certbot._internal.plugins.standalone:Authenticator

* webroot
Description: Place files in webroot directory
Interfaces: Authenticator, Plugin
Entry point: webroot = certbot._internal.plugins.webroot:Authenticator
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Plugin: Standalone
Create Certificate From CSR

No web server currently running

Certbot 即是 Webserver

Cannot renew automatically

Check
No web server currently running

- Linux
  - Listen port
    - ~# netstat -lnptu
  - Active connections
    - ~# netstat -nptu
- Windows
  - netstat -abon
  - Listen port
    - netstat -aon | find /i "LISTENING"
  - Active connections
    - netstat -aon | find /i "ESTABLISHED"

```
root@vm-ubuntu-cc411:~# netstat -lnptu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      815/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      889/sshd: /usr/sbin
tcp6       0      0 :::22                   :::*                    LISTEN      889/sshd: /usr/sbin
udp        0      0 127.0.0.53:53           0.0.0.0:*                           815/systemd-resolve
udp        0      0 172.16.0.220:68         0.0.0.0:*                           813/systemd-network
```

```
C:\Users\user\Documents>netstat -aon | find /i "LISTENING"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       904
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       752
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       6560
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       676
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       536
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1260
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1172
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       2096
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       2412
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       2736
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING       656
  TCP    172.16.0.244:139       0.0.0.0:0              LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       904
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:3389              [::]:0                 LISTENING       752
  TCP    [::]:49664             [::]:0                 LISTENING       676
  TCP    [::]:49665             [::]:0                 LISTENING       536
  TCP    [::]:49666             [::]:0                 LISTENING       1260
  TCP    [::]:49667             [::]:0                 LISTENING       1172
  TCP    [::]:49668             [::]:0                 LISTENING       2096
  TCP    [::]:49669             [::]:0                 LISTENING       2412
  TCP    [::]:49670             [::]:0                 LISTENING       2736
  TCP    [::]:49671             [::]:0                 LISTENING       656
```

Standalone
Create Certificate From CSR

* certbot certonly --csr server.csr --standalone

```
root@vm-ubuntu-cc411:~# certbot certonly --csr server.csr --standalone
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices)
 (Enter 'c' to cancel): davisyou@ntu.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
Account registered.
Requesting a certificate for davisyou.buda.idv.tw

Successfully received certificate.
Certificate is saved at:            /root/0000_cert.pem
Intermediate CA chain is saved at:  /root/0000_chain.pem
Full certificate chain is saved at: /root/0001_chain.pem
This certificate expires on 2022-03-05.

NEXT STEPS:
- Certificates created using --csr will not be renewed automatically by Certbot.
running the same Certbot command again.
```

* 0000_cert.pem
  * Server Certificate only.
* 0000_chain.pem
  * Intermediate Certificates + Root Certificate
* 0001_chain.pem
  * Server Certificate + Intermediate Certificates + Root Certificate

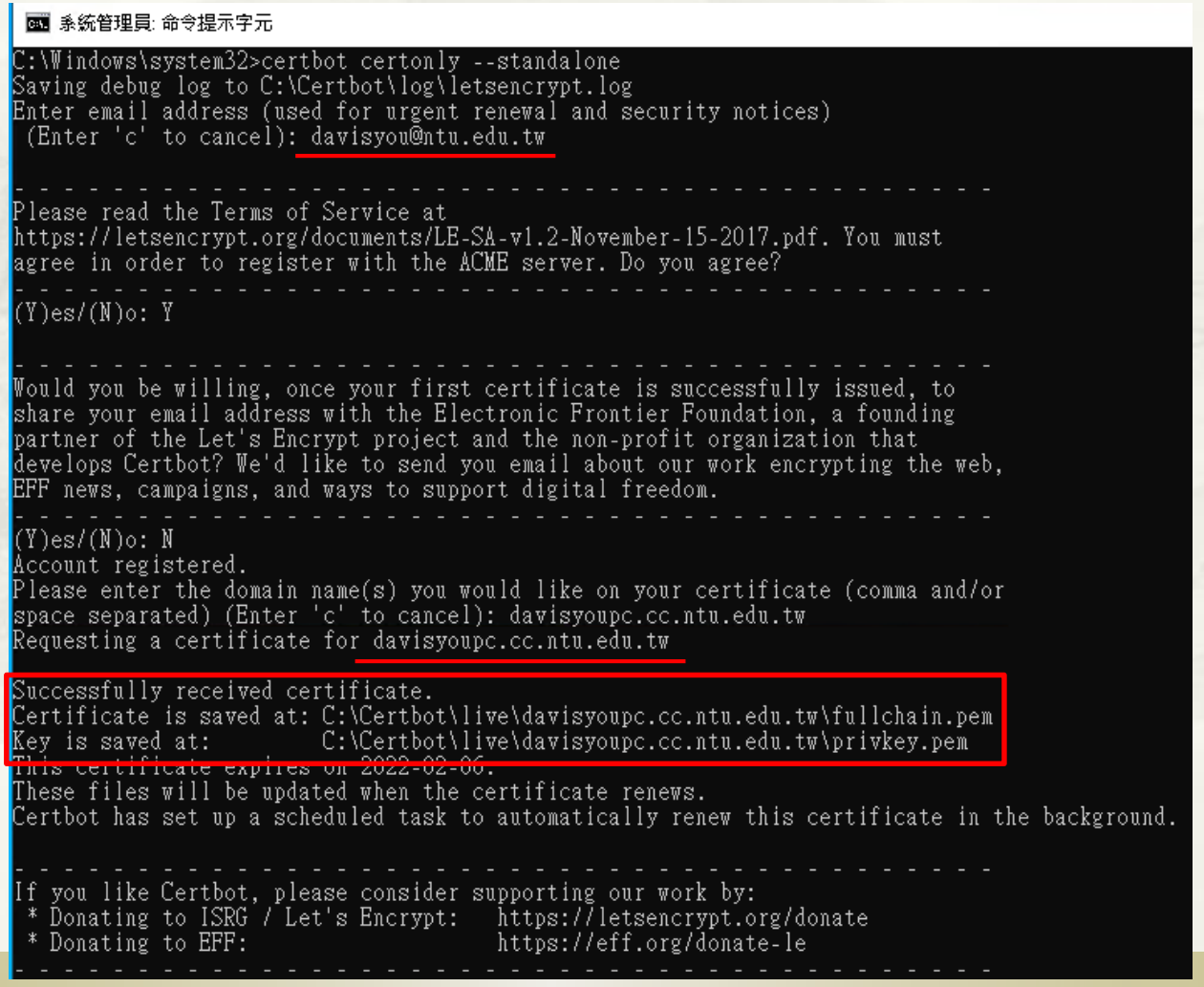
Plugin: Standalone Authenticator Only

No web server currently running

Certbot 即是 Webserver

Standalone for Windows
Single Domain

* > certbot certonly --standalone



PEM to PKCS#12

- Copy Certifcates to C:\Users\user\Downloads\openssl-3.0.0-win64-mingw\bin
- PEM to PKCS#12(.pfx)
  - openssl pkcs12 -export -out certificate.pfx -inkey privkey.pem -in cert.pem -certfile chain.pem
- Install .pfx

Standalone for Ubuntu
Multi-Domain

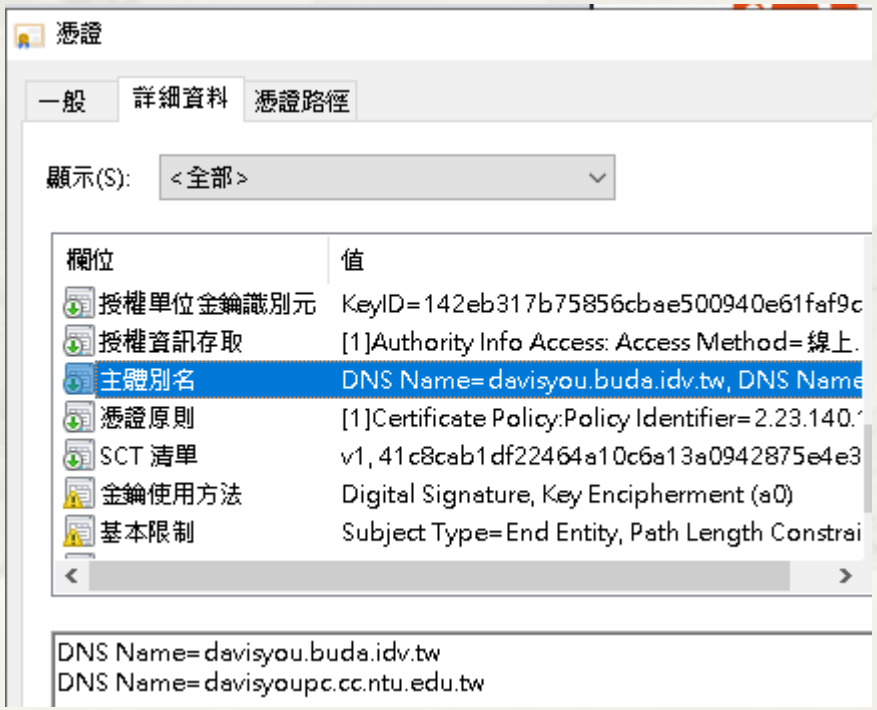
```
root@vm-ubuntu-cc411:~# certbot certonly --standalone
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices)
 (Enter 'c' to cancel): davisyou@ntu.edu.tw

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
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
Account registered.
Please enter the domain name(s) you would like on your certificate (comma and/or
space separated) (Enter 'c' to cancel): davisyoupc.cc.ntu.edu.tw,davisyou.buda.idv.tw
Requesting a certificate for davisyoupc.cc.ntu.edu.tw and davisyou.buda.idv.tw
```

2 domain names

```
Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/davisyoupc.cc.ntu.edu.tw/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/davisyoupc.cc.ntu.edu.tw/privkey.pem
This certificate expires on 2022-02-07.
These files will be updated when the certificate renews.
```

Multi-Domain Certificate

* https://crt.sh/?id=5572136554
  * X509v3 Subject Alternative Name:
  * DNS:davisyou.buda.idv.tw
  * DNS:davisyoupc.cc.ntu.edu.tw



Plugin: Webroot Authenticator Only

Already have web server running(port 80)

需提供目前 Web Server Webroot 路徑

Webroot
Apache for Linux

* ~# certbot certonly --webroot

```
root@vm-ubuntu-cc411:~# certbot certonly --webroot
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices)
 (Enter 'c' to cancel): davisyou@ntu.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
Account registered.
Please enter the domain name(s) you would like on your certificate (comma and/or
space separated) (Enter 'c' to cancel): davisyoupc.cc.ntu.edu.tw
Requesting a certificate for davisyoupc.cc.ntu.edu.tw
Input the webroot for davisyoupc.cc.ntu.edu.tw: (Enter 'c' to cancel): /var/www/html

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/davisyoupc.cc.ntu.edu.tw/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/davisyoupc.cc.ntu.edu.tw/privkey.pem
This certificate expires on 2022-02-08.
These files will be updated when the certificate renews.
```

Webroot
Apache Access Log

- tail /var/log/apache2/access.log
  - 34.219.87.132 - - [10/Nov/2021:09:02:29 +0800] "GET /.well-known/acme-challenge/7JzOS0u7VYWoU6zBvTQkVvcMESdcWRAY2mrhXyX1dIE HTTP/1.1" 200 308 "-" "Mozilla/5.0 (compatible; Let's Encrypt validation server; +https://www.letsencrypt.org)"
  - 64.78.149.164 - - [10/Nov/2021:09:02:29 +0800] "GET /.well-known/acme-challenge/7JzOS0u7VYWoU6zBvTQkVvcMESdcWRAY2mrhXyX1dIE HTTP/1.1" 200 308 "-" "Mozilla/5.0 (compatible; Let's Encrypt validation server; +https://www.letsencrypt.org)"
  - 3.142.122.14 - - [10/Nov/2021:09:02:30 +0800] "GET /.well-known/acme-challenge/7JzOS0u7VYWoU6zBvTQkVvcMESdcWRAY2mrhXyX1dIE HTTP/1.1" 200 308 "-" "Mozilla/5.0 (compatible; Let's Encrypt validation server; +https://www.letsencrypt.org)"
  - 18.159.196.172 - - [10/Nov/2021:09:02:31 +0800] "GET /.well-known/acme-challenge/7JzOS0u7VYWoU6zBvTQkVvcMESdcWRAY2mrhXyX1dIE HTTP/1.1" 200 308 "-" "Mozilla/5.0 (compatible; Let's Encrypt validation server; +https://www.letsencrypt.org)"

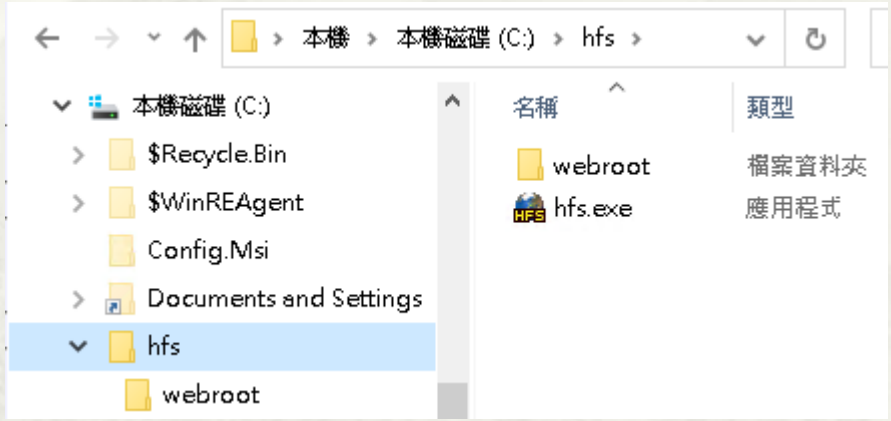
Webroot
Not Support IIS for Windows

- IIS 預設不支援
  - Folder Name: /.well-known
  - File: 無附檔名

```
C:\Windows\system32>certbot certonly --webroot
Saving debug log to C:\Certbot\log\letsencrypt.log
Enter email address (used for urgent renewal and security notices)
 (Enter 'c' to cancel): davisyou@ntu.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
Account registered.
Please enter the domain name(s) you would like on your certificate (comma and/or
space separated) (Enter 'c' to cancel): davis.buda.idv.tw
Requesting a certificate for davis.buda.idv.tw
Input the webroot for davis.buda.idv.tw: (Enter 'c' to cancel): C:\inetpub\wwwroot
Encountered exception during recovery: FileNotFoundError: [WinError 3] 系統找不到指定的路徑。: 'C:\\inetpub\\wwwroot\\.w
ell-known\\acme-challenge\\EEB5IAFzKpT8SuO3nHEWvtaJYeOIEXL3RFySzuqOzGg'
An unexpected error occurred:
pywintypes.error: (1307, 'SetFileSecurity', '這個安全性識別碼不能被指派給這個物件的擁有者。')
```

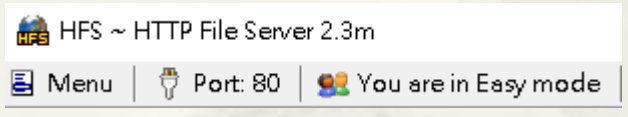
Webroot
HFS Web Server for Windows

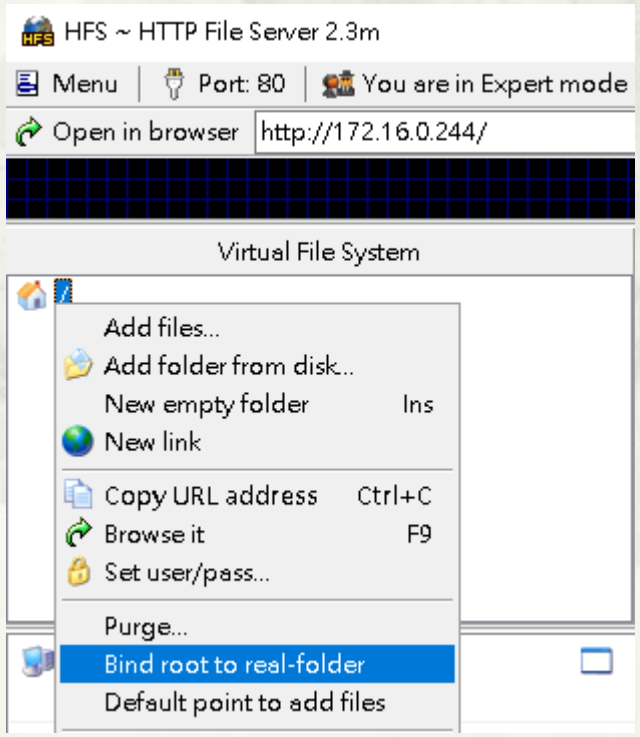
* HFS Web Server download
  * https://www.rejetto.com/hfs/?f=dl

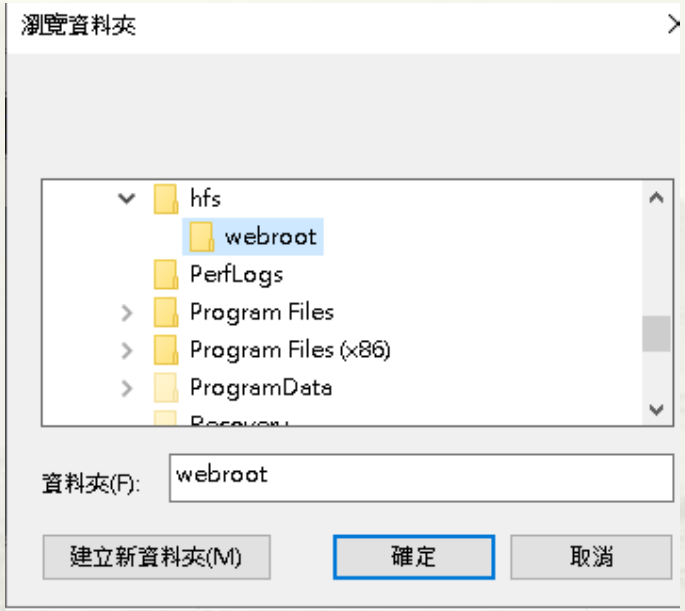


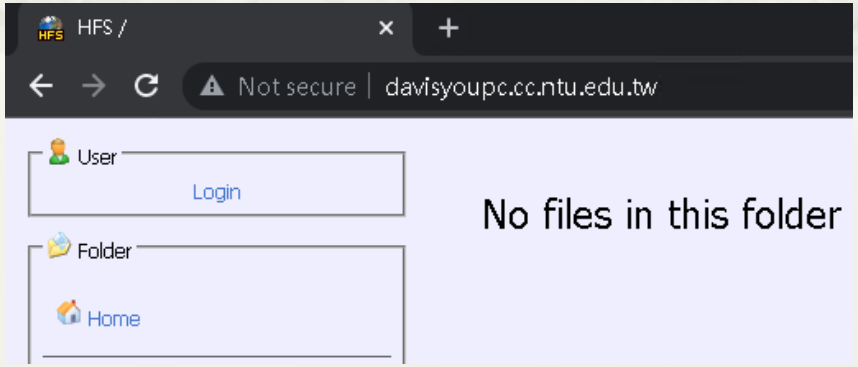
Webroot
HFS Root Folder Setup

* Switch to Expert Mode



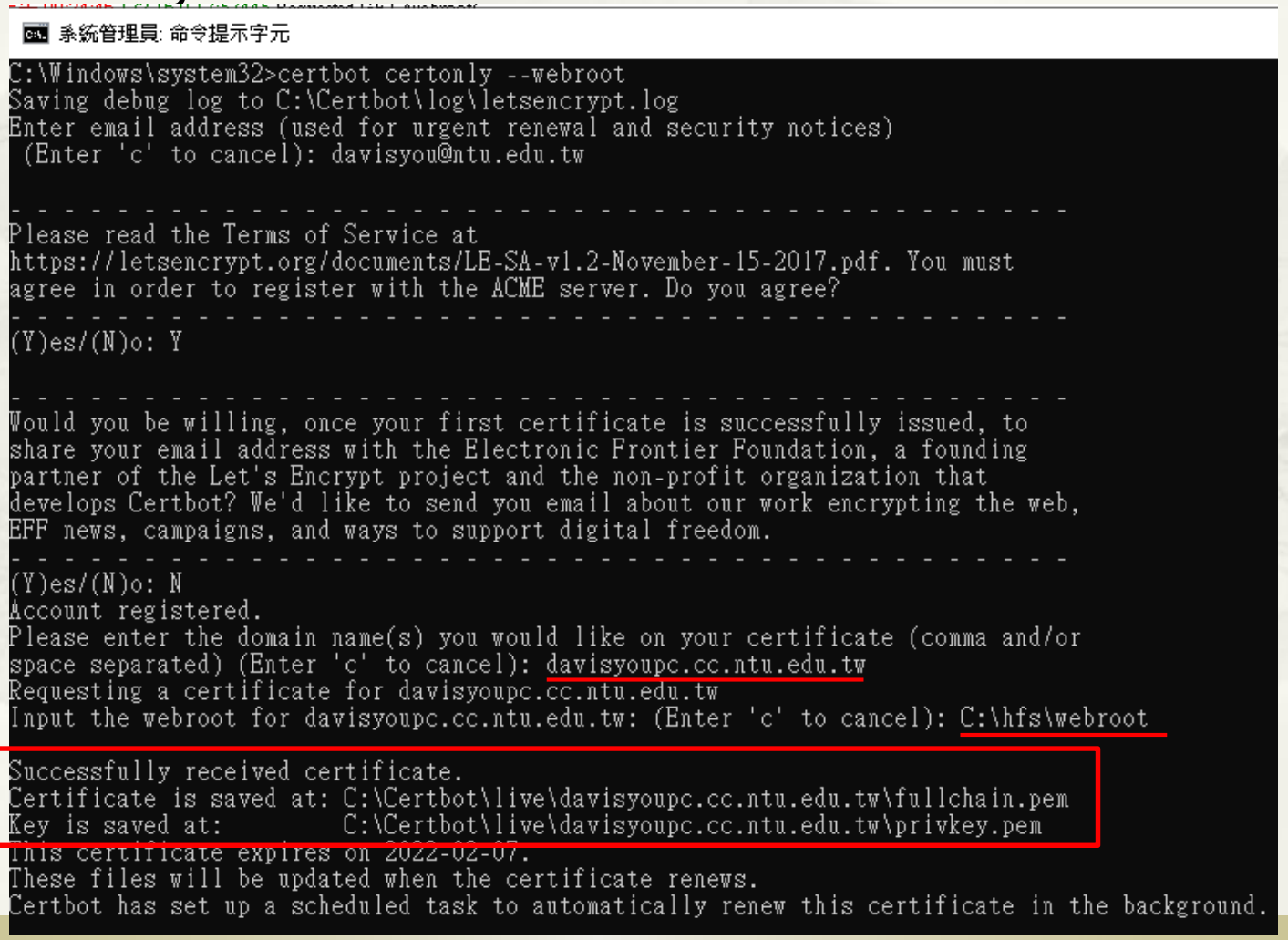






Webroot
HFS Web Server for Windows

* > certbot certonly --webroot



Webroot
HFS Access Log

```
上午 09:36:00 64.78.149.164:23096 Requested GET /.well-known/acme-challenge/cCuV_qJLe3KB3FZNGOPnce0XXN5udNL0CcW_1-4Yu_I
上午 09:36:00 64.78.149.164:23096 Fully downloaded - 87 @ 5.3 KB/s - /.well-known/acme-challenge/cCuV_qJLe3KB3FZNGOPnce0XXN5udNL0CcW_1-4Yu_I
上午 09:36:00 34.219.87.132:34512 Requested GET /.well-known/acme-challenge/cCuV_qJLe3KB3FZNGOPnce0XXN5udNL0CcW_1-4Yu_I
上午 09:36:00 34.219.87.132:34512 Fully downloaded - 87 @ 5.7 KB/s - /.well-known/acme-challenge/cCuV_qJLe3KB3FZNGOPnce0XXN5udNL0CcW_1-4Yu_I
上午 09:36:02 18.192.36.99:24774 Requested GET /.well-known/acme-challenge/cCuV_qJLe3KB3FZNGOPnce0XXN5udNL0CcW_1-4Yu_I
上午 09:36:02 18.192.36.99:24774 Fully downloaded - 87 @ 5.3 KB/s - /.well-known/acme-challenge/cCuV_qJLe3KB3FZNGOPnce0XXN5udNL0CcW_1-4Yu_I
上午 09:36:02 18.116.86.117:12790 Requested GET /.well-known/acme-challenge/cCuV_qJLe3KB3FZNGOPnce0XXN5udNL0CcW_1-4Yu_I
上午 09:36:02 18.116.86.117:12790 Fully downloaded - 87 @ 0B/s - /.well-known/acme-challenge/cCuV_qJLe3KB3FZNGOPnce0XXN5udNL0CcW_1-4Yu_I
```

Plugin: Apache Authenticator Only

自動偵測 Apache Webroot 路徑

Plugin: Apache Authenticator Only

* ~# certbot certonly --apache

```
root@vm-ubuntu-cc411:~# certbot certonly --apache
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices)
 (Enter 'c' to cancel): davisyou@ntu.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
Account registered.
Please enter the domain name(s) you would like on your certificate (comma and/or
space separated) (Enter 'c' to cancel): davisyoupc.cc.ntu.edu.tw
Requesting a certificate for davisyoupc.cc.ntu.edu.tw

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/davisyoupc.cc.ntu.edu.tw/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/davisyoupc.cc.ntu.edu.tw/privkey.pem
This certificate expires on 2022-02-07.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.
```

Plugin: Apache Authenticator and Installer

Plugin: Apache
(不需先 Enable SSL Module)

- ~# sudo certbot --apache
  - Saving debug log to /var/log/letsencrypt/letsencrypt.log
  - Enter email address (used for urgent renewal and security notices)
  - (Enter 'c' to cancel): yourname@ntu.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
  - Account registered.
  - Please enter the domain name(s) you would like on your certificate (comma and/or
  - space separated) (Enter 'c' to cancel): xyz.ntu.edu.tw
  - Requesting a certificate for xyz.ntu.edu.tw

Plugin: Apache

* Successfully received certificate.
* Certificate is saved at: /etc/letsencrypt/live/xyz.ntu.edu.tw/fullchain.pem
* Key is saved at: /etc/letsencrypt/live/xyz.ntu.edu.tw/privkey.pem
* This certificate expires on 2021-10-13.
* These files will be updated when the certificate renews.
* Certbot has set up a scheduled task to automatically renew this certificate in the background.

* Deploying certificate
* Successfully deployed certificate for tanet2020.tp1rc.edu.tw to /etc/apache2/sites-available/000-default-le-ssl.conf
* Congratulations! You have successfully enabled HTTPS on https://xyz.ntu.edu.tw

* -
* 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
* -

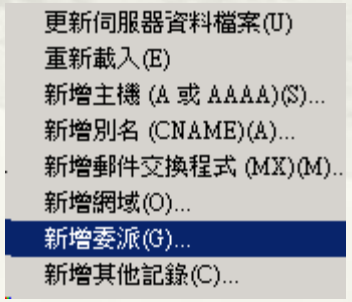
Wildcard Certificate

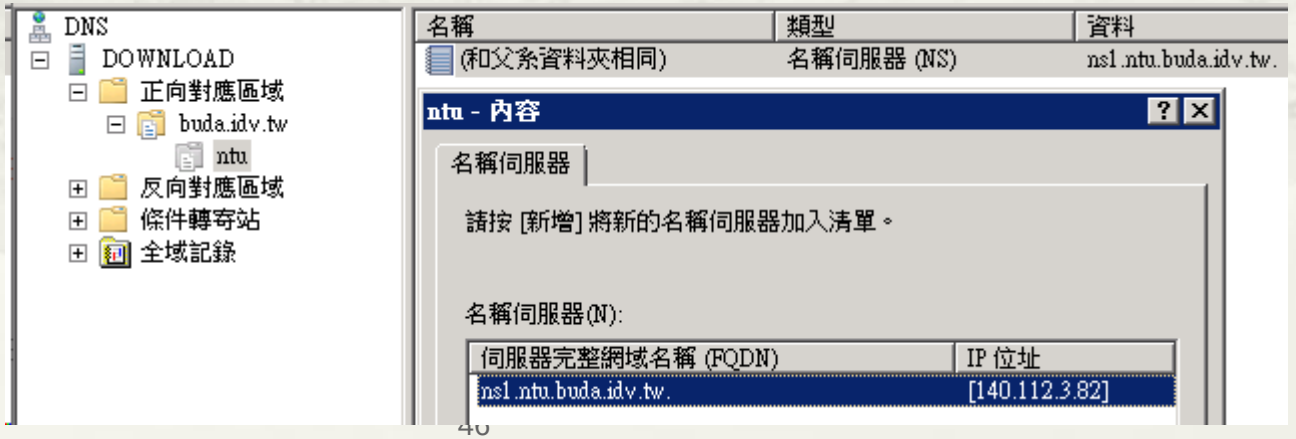
DNS Plugin

- certbot-dns-rfc2136 (Official)
  - Support DNS server with RFC 2136 Dynamic Updates.
  - https://certbot-dns-rfc2136.readthedocs.io/en/stable/
  - Need BIND
- certbot-dns-standalone (Third-party)
  - https://github.com/siilike/certbot-dns-standalone
  - 本身即是 DNS Server

Subdomain DNS Setup

* Bind
  * zone "cc.ntu.edu.tw."
  * davis IN NS ns1.davis.cc.ntu.edu.tw.
  * ns1.davis IN A 140.112.3.82
* Windows DNS
  * buda.idv.tw





DNS Setup Check

* nslookup

```
> set type=soa
> davis.cc.ntu.edu.tw
伺服器:  pfSense.localdomain
Address:  192.168.0.1

*** pfSense.localdomain 找不到 davis.cc.ntu.edu.tw: Server failed
> ntu.buda.idv.tw
伺服器:  pfSense.localdomain
Address:  192.168.0.1

*** pfSense.localdomain 找不到 ntu.buda.idv.tw: Server failed
```

Plugin: certbot-dns-standalone

* ~# certbot certonly

```
root@vm-ubuntu-cc411:~# certbot certonly
Saving debug log to /var/log/letsencrypt/letsencrypt.log

How would you like to authenticate with the ACME CA?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: Apache Web Server plugin (apache)
2: Obtain certificates using an integrated DNS server (dns-standalone)
3: Spin up a temporary webserver (standalone)
4: Place files in webroot directory (webroot)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate number [1-4] then [enter] (press 'c' to cancel): 2
Please enter the domain name(s) you would like on your certificate (comma and/or
space separated) (Enter 'c' to cancel): *.ntu.buda.idv.tw
Requesting a certificate for *.ntu.buda.idv.tw
Waiting 0 seconds for DNS changes to propagate

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/ntu.buda.idv.tw/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/ntu.buda.idv.tw/privkey.pem
This certificate expires on 2022-02-08.
These files will be updated when the certificate renews.
```

```
root@vm-ubuntu-cc411:~# certbot certonly
Saving debug log to /var/log/letsencrypt/letsencrypt.log

How would you like to authenticate with the ACME CA?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: Obtain certificates using an integrated DNS server (dns-standalone)
2: Spin up a temporary webserver (standalone)
3: Place files in webroot directory (webroot)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate number [1-3] then [enter] (press 'c' to cancel): 1
Enter email address (used for urgent renewal and security notices)
 (Enter 'c' to cancel): davisyou@ntu.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
Account registered.
Please enter the domain name(s) you would like on your certificate (comma and/or
space separated) (Enter 'c' to cancel): *.davis.cc.ntu.edu.tw
Requesting a certificate for *.davis.cc.ntu.edu.tw
Waiting 0 seconds for DNS changes to propagate

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/davis.cc.ntu.edu.tw/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/davis.cc.ntu.edu.tw/privkey.pem
This certificate expires on 2022-03-03.
These files will be updated when the certificate renews.
```

Verify DNS Steps @ Wireshark

No.	Time	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
5	25.571952	52.37.230.196	41338	172.16.0.220	53	DNS	90	Standard query 0x9aa1 AAAA ns1.NTu.BudA.idv.tW OPT
6	25.572395	172.16.0.220	53	52.37.230.196	41338	DNS	79	Standard query response 0x9aa1 AAAA ns1.NTu.BudA.idv.tW
7	25.575791	52.37.230.196	34247	172.16.0.220	53	DNS	102	Standard query 0x89a0 TXT _aCME-ChallEnGE.NtU.buDa.idv.tW OPT
8	25.576154	172.16.0.220	53	52.37.230.196	34247	DNS	147	Standard query response 0x89a0 TXT _aCME-ChallEnGE.NtU.buDa.idv.tW TXT
9	25.599098	54.201.180.224	47913	172.16.0.220	53	DNS	86	Standard query 0xcc14 CAA ntU.bUdA.idv.tW OPT
10	25.599473	172.16.0.220	53	54.201.180.224	47913	DNS	75	Standard query response 0xcc14 CAA ntU.bUdA.idv.tW
11	25.603712	54.201.180.224	8688	172.16.0.220	53	DNS	90	Standard query 0x602e AAAA NS1.ntu.BUDa.iDV.tw OPT
12	25.604225	172.16.0.220	53	54.201.180.224	8688	DNS	79	Standard query response 0x602e AAAA NS1.ntu.BUDa.iDV.tw
13	25.677937	3.138.108.237	19693	172.16.0.220	53	DNS	90	Standard query 0x8419 AAAA ns1.nTu.BuDA.idv.tw OPT
14	25.678300	172.16.0.220	53	3.138.108.237	19693	DNS	79	Standard query response 0x8419 AAAA ns1.nTu.BuDA.idv.tw
15	25.678338	3.138.108.237	64190	172.16.0.220	53	DNS	102	Standard query 0xca66 TXT _AcMe-ChaLlenGe.NTU.BUDA.IDV.tW OPT
16	25.678655	172.16.0.220	53	3.138.108.237	64190	DNS	147	Standard query response 0xca66 TXT _AcMe-ChaLlenGe.NTU.BUDA.IDV.tW TXT
17	26.040083	66.133.109.36	21997	172.16.0.220	53	DNS	90	Standard query 0x2283 AAAA nS1.Ntu.bUdA.iDv.Tw OPT
18	26.040103	66.133.109.36	30134	172.16.0.220	53	DNS	86	Standard query 0x13e2 CAA ntU.bUDA.IDV.Tw OPT
19	26.040450	172.16.0.220	53	66.133.109.36	21997	DNS	79	Standard query response 0x2283 AAAA nS1.Ntu.bUdA.iDv.Tw
20	26.040672	172.16.0.220	53	66.133.109.36	30134	DNS	75	Standard query response 0x13e2 CAA ntU.bUDA.IDV.Tw
21	26.857391	54.93.165.154	36111	172.16.0.220	53	DNS	90	Standard query 0x6b45 AAAA ns1.nTU.buDA.IdV.Tw OPT
22	26.857771	172.16.0.220	53	54.93.165.154	36111	DNS	79	Standard query response 0x6b45 AAAA ns1.nTU.buDA.IdV.Tw
23	26.883197	54.93.165.154	14148	172.16.0.220	53	DNS	102	Standard query 0x9e5a TXT _AcME-CHalleNge.NtU.budA.idV.Tw OPT
24	26.883638	172.16.0.220	53	54.93.165.154	14148	DNS	147	Standard query response 0x9e5a TXT _AcME-CHalleNge.NtU.budA.idV.Tw TXT
25	28.775155	3.15.200.85	56728	172.16.0.220	53	DNS	90	Standard query 0x9cfb AAAA NS1.NtU.budA.iDv.tw OPT
26	28.775175	3.15.200.85	39232	172.16.0.220	53	DNS	86	Standard query 0x4c51 CAA Ntu.buda.IDV.tw OPT
27	28.775530	172.16.0.220	53	3.15.200.85	56728	DNS	79	Standard query response 0x9cfb AAAA NS1.NtU.budA.iDv.tw
28	28.775784	172.16.0.220	53	3.15.200.85	39232	DNS	75	Standard query response 0x4c51 CAA Ntu.buda.IDV.tw
29	29.268154	66.133.109.36	32317	172.16.0.220	53	DNS	90	Standard query 0xad71 AAAA NS1.NTU.bUdA.IDv.tW OPT
30	29.268171	66.133.109.36	34058	172.16.0.220	53	DNS	102	Standard query 0x9932 TXT _ACME-chALlENge.Ntu.buDA.IdV.TW OPT
31	29.268331	54.93.97.127	25439	172.16.0.220	53	DNS	90	Standard query 0x469e AAAA Ns1.NTu.bUDa.Idv.tw OPT
32	29.268538	172.16.0.220	53	66.133.109.36	32317	DNS	79	Standard query response 0xad71 AAAA NS1.NTU.bUdA.IDv.tW
33	29.268855	172.16.0.220	53	66.133.109.36	34058	DNS	147	Standard query response 0x9932 TXT _ACME-chALlENge.Ntu.buDA.IdV.TW TXT
34	29.269059	172.16.0.220	53	54.93.97.127	25439	DNS	79	Standard query response 0x469e AAAA Ns1.NTu.bUDa.Idv.tw
35	29.294996	54.93.97.127	23407	172.16.0.220	53	DNS	86	Standard query 0x1ddc CAA NTU.BuDa.iDV.tw OPT
36	29.295351	172.16.0.220	53	54.93.97.127	23407	DNS	75	Standard query response 0x1ddc CAA NTU.BuDa.iDV.tw

Wildcard Related DNS Type

* TXT
  * Originally for arbitrary human-readable text in a DNS record
* CAA(Certification Authority Authorization)
  * constraining acceptable CAs for a host/domain

憑證更新

certbot renew

憑證更新

- Renew certificate less than 30 days.
  - Use the same plugin and options that the certificate was originally issued
- ~# certbot renew
  - Saving debug log to /var/log/letsencrypt/letsencrypt.log
  -
  - Processing /etc/letsencrypt/renewal/tanet2020.tp1rc.edu.tw.conf
  -
  - Certificate not yet due for renewal
  -
  - The following certificates are not due for renewal yet:
  - /etc/letsencrypt/live/tanet2020.tp1rc.edu.tw/fullchain.pem expires on 2021-10-04 (skipped)
  - No renewals were attempted.

憑證更新

- certbot renew --dry-run
- certbot renew --quiet
  - silence all output except errors
- if you have a single certificate obtained using the standalone plugin
  - certbot renew --pre-hook "service nginx stop" --post-hook "service nginx start“
  - hook to run only after a successful renewal, use --deploy-hook

憑證更新

* cd /etc/cron.daily
* nano certbot_renew
  * #!/bin/sh
  * certbot renew

* Check Log
  * cat /var/log/letsencrypt/letsencrypt.log

憑證自動更新 @ **snap**

憑證自動更新 @ snap

- ~# systemctl list-timers

```
root@vm-ubuntu-cc411:~#  systemctl list-timers
NEXT                         LEFT          LAST                         PASSED              UNIT                         ACTIVATES
Wed 2021-11-17 10:14:08 CST  11min left    n/a                          n/a                 systemd-tmpfiles-clean.timer systemd-tmpfiles-clean.service
Wed 2021-11-17 10:19:59 CST  17min left    Thu 2021-11-11 15:24:52 CST  5 days ago          apt-daily-upgrade.timer      apt-daily-upgrade.service
Wed 2021-11-17 10:42:31 CST  40min left    n/a                          n/a                 ua-timer.timer               ua-timer.service
Wed 2021-11-17 11:14:39 CST  1h 12min left Thu 2021-11-11 15:24:54 CST  5 days ago          fwupd-refresh.timer          fwupd-refresh.service
Wed 2021-11-17 17:28:41 CST  7h left       Tue 2021-08-03 17:54:40 CST  3 months 14 days ago apt-daily.timer             apt-daily.service
Wed 2021-11-17 18:54:58 CST  8h left       Wed 2021-10-27 09:31:21 CST  3 weeks 0 days ago   motd-news.timer              motd-news.service
Wed 2021-11-17 23:19:00 CST  13h left      n/a                          n/a                 snap.certbot.renew.timer     snap.certbot.renew.service
Thu 2021-11-18 00:00:00 CST  13h left      Wed 2021-11-17 09:59:03 CST  3min 10s ago        logrotate.timer              logrotate.service
Thu 2021-11-18 00:00:00 CST  13h left      Wed 2021-11-17 09:59:03 CST  3min 10s ago        man-db.timer                 man-db.service
Sun 2021-11-21 03:10:41 CST  3 days left   Wed 2021-11-17 09:59:13 CST  3min 1s ago         e2scrub_all.timer            e2scrub_all.service
Mon 2021-11-22 00:00:00 CST  4 days left   Wed 2021-11-17 09:59:03 CST  3min 10s ago        fstrim.timer                 fstrim.service
```

- ~# systemctl status snap.certbot.renew.timer
- ~# systemctl status snap.certbot.renew.service

```
root@vm-ubuntu-cc411:/lib/systemd/user# systemctl status snap.certbot.renew.timer
● snap.certbot.renew.timer - Timer renew for snap application certbot.renew
     Loaded: loaded (/etc/systemd/system/snap.certbot.renew.timer; enabled; vendor preset: enabled)
     Active: active (waiting) since Wed 2021-11-17 10:01:48 CST; 1h 41min ago
    Trigger: Wed 2021-11-17 23:19:00 CST; 11h left
   Triggers: ● snap.certbot.renew.service

Nov 17 10:01:48 vm-ubuntu-cc411 systemd[1]: Started Timer renew for snap application certbot.renew.
root@vm-ubuntu-cc411:/lib/systemd/user# systemctl status snap.certbot.renew.service
● snap.certbot.renew.service - Service for snap application certbot.renew
     Loaded: loaded (/etc/systemd/system/snap.certbot.renew.service; static; vendor preset: enabled)
     Active: inactive (dead)
TriggeredBy: ● snap.certbot.renew.timer
```

snap.certbot.renew.timer

* /etc/systemd/system/snap.certbot.renew.timer

```
[Unit]
# Auto-generated, DO NOT EDIT
Description=Timer renew for snap application certbot.renew
Requires=snap-certbot-1582.mount
After=snap-certbot-1582.mount
X-Snappy=yes

[Timer]
Unit=snap.certbot.renew.service
OnCalendar=*-*-* 09:08
OnCalendar=*-*-* 23:19

[Install]
WantedBy=timers.target
```

snap.certbot.renew.service

* /etc/systemd/system/snap.certbot.renew.service

```
[Unit]
# Auto-generated, DO NOT EDIT
Description=Service for snap application certbot.renew
Requires=snap-certbot-1582.mount
Wants=network.target
After=snap-certbot-1582.mount network.target snapd.apparmor.service
X-Snappy=yes

[Service]
EnvironmentFile=-/etc/environment
ExecStart=/usr/bin/snap run --timer="00:00~24:00/2" certbot.renew
SyslogIdentifier=certbot.renew
Restart=no
WorkingDirectory=/var/snap/certbot/1582
TimeoutStopSec=30
Type=oneshot
```

snap services

* snap services

```
root@vm-ubuntu-cc411:~#  snap services
Service        Startup  Current   Notes
certbot.renew  enabled  inactive  timer-activated
lxd.activate   enabled  inactive  -
lxd.daemon     enabled  inactive  socket-activated
```

* snap logs certbot.renew

```
root@vm-ubuntu-cc411:~# snap logs certbot.renew
2021-11-11T21:38:18Z systemd[1]: Starting Service for snap application certbot.renew...
2021-11-11T21:38:20Z systemd[1]: snap.certbot.renew.service: Succeeded.
2021-11-11T21:38:20Z systemd[1]: Finished Service for snap application certbot.renew.
2021-11-12T04:06:18Z systemd[1]: Starting Service for snap application certbot.renew...
2021-11-12T04:06:20Z systemd[1]: snap.certbot.renew.service: Succeeded.
2021-11-12T04:06:20Z systemd[1]: Finished Service for snap application certbot.renew.
```

其他指令

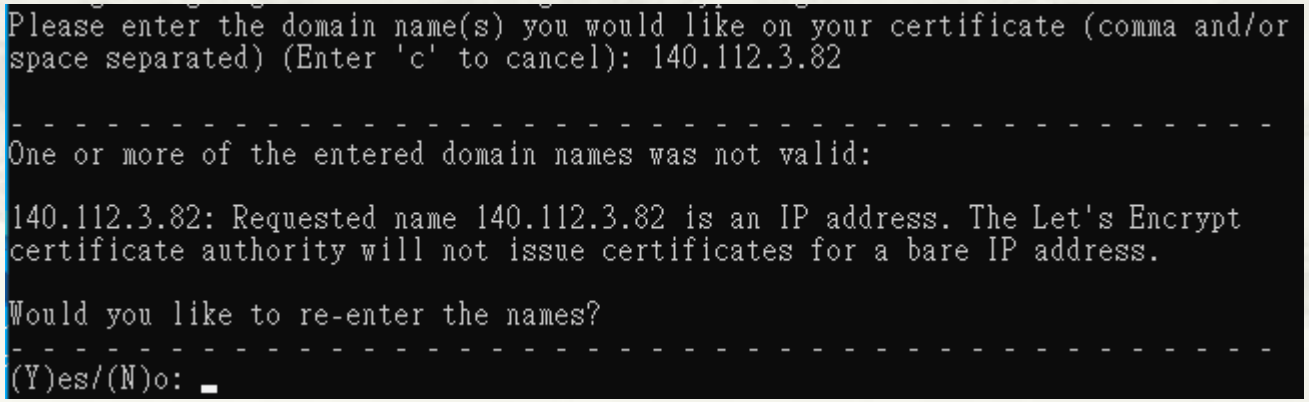
顯示目前憑證資訊

* ~# certbot certificates
  * Saving debug log to /var/log/letsencrypt/letsencrypt.log
  * -
  * Found the following certs:
  * Certificate Name: tanet2020.tp1rc.edu.tw
  * Serial Number: 3f93847cc8e1edb3b25d8f43a28922309ff
  * Key Type: RSA
  * Domains: tanet2020.tp1rc.edu.tw
  * Expiry Date: 2021-10-04 09:16:45+00:00 (VALID: 89 days)
  * Certificate Path: /etc/letsencrypt/live/tanet2020.tp1rc.edu.tw/fullchain.pem
  * Private Key Path: /etc/letsencrypt/live/tanet2020.tp1rc.edu.tw/privkey.pem
  * -

* certbot certonly -d app.example.com -d api.example.com
* certbot delete
* certbot revoke --cert-name example.com
* --rsa-key-size 4096
* -n or --noninteractive

錯誤訊息

* too many certificates (5) already issued for this exact set of domains in the last 168 hours: davisyoupc.cc.ntu.edu.tw:
  * limit of 5 per week.
  * https://letsencrypt.org/docs/rate-limits/
* 無法申請 IP 憑證



簡報完畢
謝謝