

SSL憑證安裝與申請

Let's Encrypt

臺灣大學計資中心
網路組
游子興

大綱

- * Let's Encrypt
- * Certbot Install
- * Get and Install Certificate for Apache
- * Get Certificate only for Apache
- * Standalone
- * Webroot
- * Wildcard Certificates



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。
- * <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 piece of ACME client software to use.
- * The ACME clients by third parties.
 - * <https://letsencrypt.org/docs/client-options/>
 - * Recommended: Certbot

Certbot

- * Command Line 自動化安裝工具
 - * <https://certbot.eff.org/docs/>
 - * <https://eff-certbot.readthedocs.io/en/stable/using.html#certbot-command-line-options>
- * Linux : requires Python 3.6+
- * It requires root/administrator access

Certbot Config Files Save Path

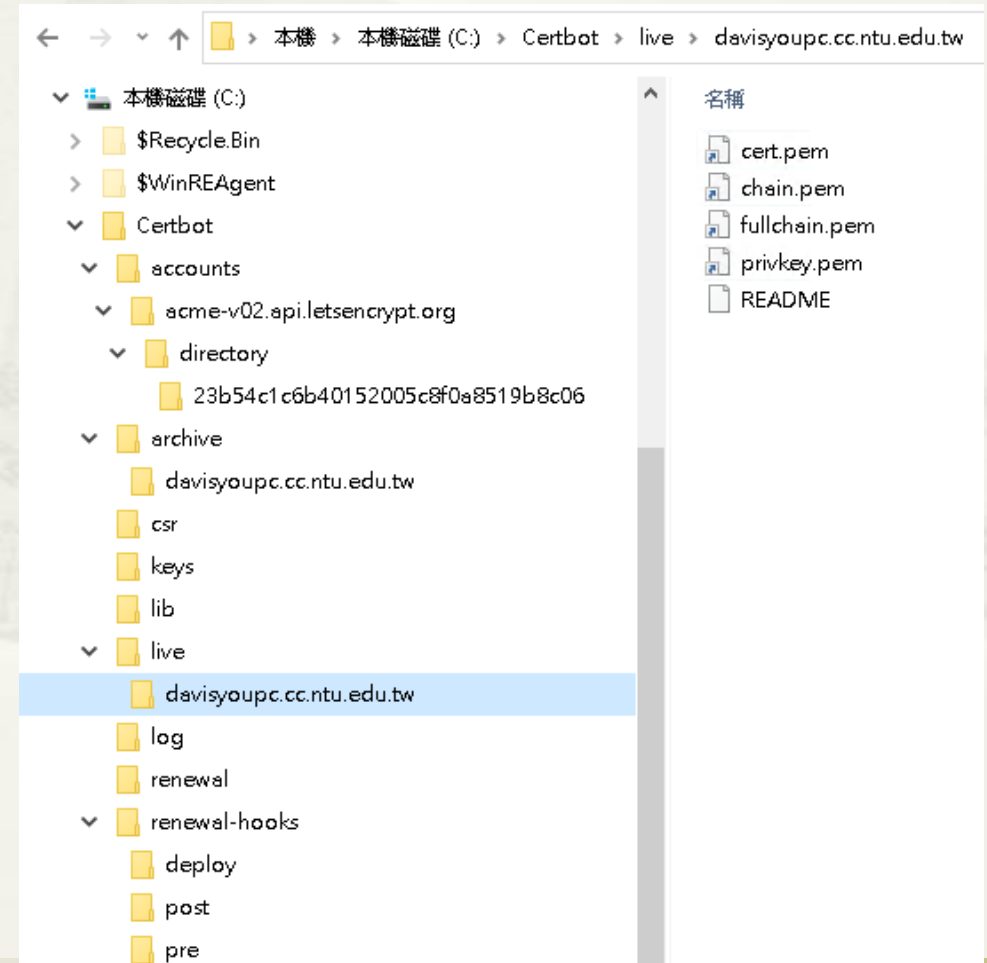
* Linux

- * /etc/letsencrypt
- * /var/log/letsencrypt
- * /var/lib/letsencrypt

* 還原成初始設定

- * 刪除上述路徑及檔案

* Windows: C:\Certbot



Certbot Plugins

- * **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**

Authenticators 執行動作

- * 產生驗證檔案
 - * Web 根目錄 `/.well-known/acme-challenge/RpUCT8SSJN77t7mZBHkl6_BLhtlm13LyFVzHJ1mhckl`
- * 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`

Installers 執行動作

- * 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 Plugin List (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. (本身即是 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)

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

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
-----
```



Certbot Install

use snap for Linux

* 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 for Linux

- * 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`

Certbot for Windows

- * Download & Install

- * <https://dl.eff.org/certbot-beta-installer-win32.exe>
- * Install @ C:\Program Files (x86)\Certbot

- * Run

- * run CMD.EXE “Run as administrator”

- * Currently unable to automatically renew wildcard certificates, since these require a DNS plugin in order to be renewed without user intervention.

- * <https://certbot.eff.org/lets-encrypt/windows-apache>

Get and Install Certificate for Apache

<https://certbot.eff.org/lets-encrypt/ubuntu-focal-apache>

My HTTP website is running

Apache



on

Ubuntu 20.04



[Help, I'm not sure!](#)

全自動安裝 (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

全自動安裝

- * 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>
- * -----

Get Certificate only for Apache

Get Certificate only for Apache

* ~# 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.
```

Standalone

No web server currently running

Standalone for Windows

- * > certbot certonly --standalone

```
系統管理員: 命令提示字元
C:\Windows\system32>certbot certonly --standalone
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): davisyoupc.cc.ntu.edu.tw
Requesting a certificate for davisyoupc.cc.ntu.edu.tw

Successfully received certificate.
Certificate is saved at: C:\Certbot\live\davisyoupc.cc.ntu.edu.tw\fullchain.pem
Key is saved at: C:\Certbot\live\davisyoupc.cc.ntu.edu.tw\privkey.pem
This certificate expires on 2022-02-06.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

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


Standalone for Ubuntu

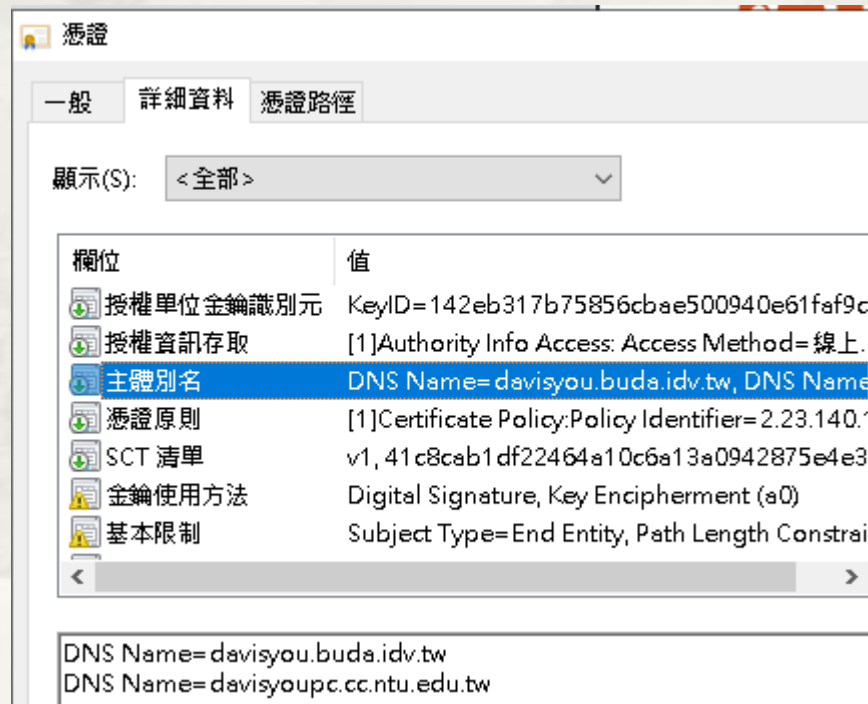
```
root@vm-ubuntu-cc411:~# certbot certonly --standalone
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices)
(Enter 'c' to cancel): davisyou@ntu.edu.tw

-----
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.
```

Standalone for Ubuntu

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



Webroot

Already have web server running(port 80)

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

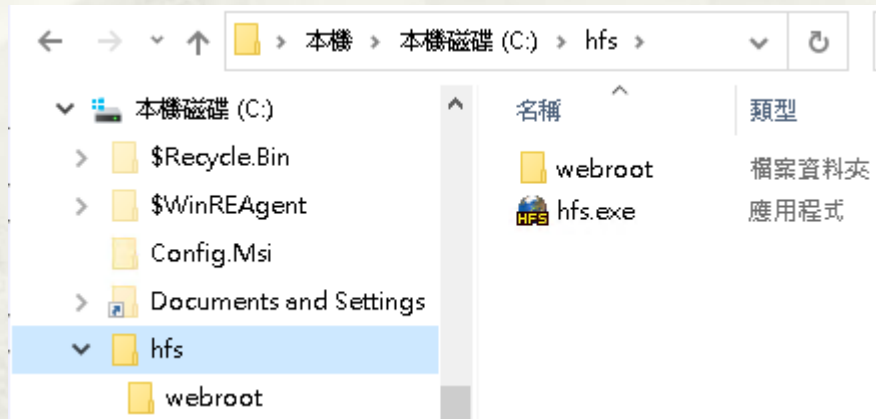
Apache Access Log

- * 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

HFS Web Server for Windows

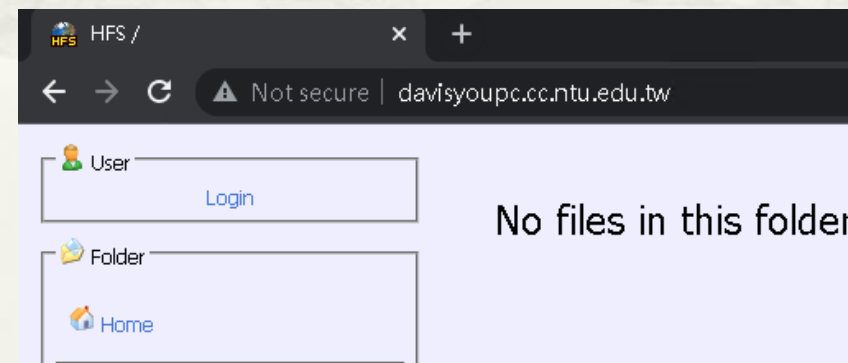
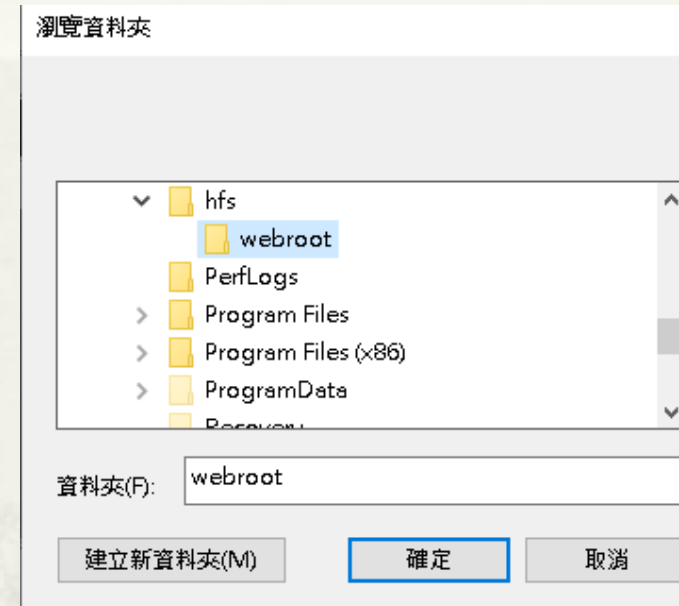
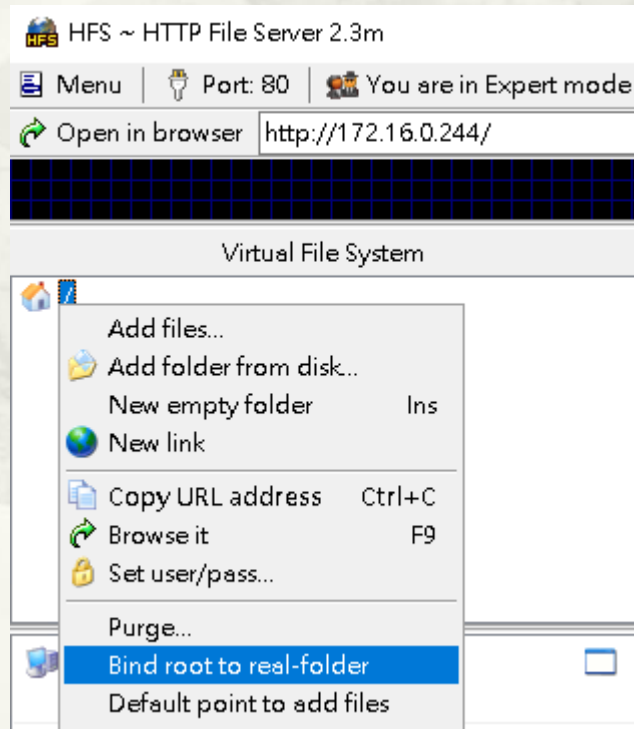
- * HFS Web Server download
 - * <https://www.rejetto.com/hfs/?f=dl>



HFS

Root Folder Setup

* Switch to Expert Mode



Webroot

HFS Web Server for Windows

* > certbot certonly --webroot

```
系統管理員: 命令提示字元
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): 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): C:\hfs\webroot

Successfully received certificate.
Certificate is saved at: C:\Certbot\live\davisyoupc.cc.ntu.edu.tw\fullchain.pem
Key is saved at: C:\Certbot\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.
```


HFS Access Log

```
上午 09:36:00 64.78.149.164:23096 Requested GET /.well-known/acme-challenge/cCuV_qJLe3KB3FZNGOPnce0XXN5udNLOCcW_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_qJLe3KB3FZNGOPnce0XXN5udNLOCcW_1-4Yu_I
上午 09:36:00 34.219.87.132:34512 Requested GET /.well-known/acme-challenge/cCuV_qJLe3KB3FZNGOPnce0XXN5udNLOCcW_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_qJLe3KB3FZNGOPnce0XXN5udNLOCcW_1-4Yu_I
上午 09:36:02 18.192.36.99:24774 Requested GET /.well-known/acme-challenge/cCuV_qJLe3KB3FZNGOPnce0XXN5udNLOCcW_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_qJLe3KB3FZNGOPnce0XXN5udNLOCcW_1-4Yu_I
上午 09:36:02 18.116.86.117:12790 Requested GET /.well-known/acme-challenge/cCuV_qJLe3KB3FZNGOPnce0XXN5udNLOCcW_1-4Yu_I
上午 09:36:02 18.116.86.117:12790 Fully downloaded - 87 @ 0B/s - /.well-known/acme-challenge/cCuV_qJLe3KB3FZNGOPnce0XXN5udNLOCcW_1-4Yu_I
```



Wildcard Certificate

DNS Plugin

- * certbot-dns-rfc2136

- * Support DNS server with RFC 2136 Dynamic Updates.

- * <https://certbot-dns-rfc2136.readthedocs.io/en/stable/>

- * BIND

- * certbot-dns-standalone (Third-party)

- * <https://github.com/siilike/certbot-dns-standalone>

- * 本身即是 DNS Server

certbot-dns-standalone

* Windows DNS Setup

更新伺服器資料檔案(U)
重新載入(E)
新增主機 (A 或 AAAA)(S)...
新增別名 (CNAME)(A)...
新增郵件交換程式 (MX)(M)..
新增網域(O)...
新增委派(G)...
新增其他記錄(C)...

DNS
DOWNLOAD
正向對應區域
buda.idv.tw
ntu
反向對應區域
條件轉寄站
全域記錄

名稱	類型	資料
(和父系資料夾相同)	名稱伺服器 (NS)	nsl.ntu.buda.idv.tw.

ntu - 內容

名稱伺服器

請按 [新增] 將新的名稱伺服器加入清單。

名稱伺服器(N):

伺服器完整網域名稱 (FQDN)	IP 位址
nsl.ntu.buda.idv.tw.	[140.112.3.82]


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.
```




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.

-
- * `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`



簡報完畢
謝謝