

申請 Let's Encrypt 免費 SSL 憑證於在 NGINX 伺服器上配置和自動更新教學

 pcsetting.com/devtools/62

張貼者：PC-Setting | 2016-04-22 10:46 發表

想要為網站申請SSL憑證嗎？那可以申請Let's Encrypt所提供免費SSL/TLS憑證的服務。Let's Encrypt是由EFF、Mozilla基金會、Akamai和Cisco等等許多大公司及非營利組織於2014年共同創立的ISRG組織所成立的數位憑證認證機構，目標就是要讓網站可以免費、申請簡單與自動化流程的憑證服務，以可以推廣及加速全球網站採用HTTPS安全的加密傳輸協定。Let's Encrypt已在2016年4月脫離了Beta測試階段，正式進入穩定階段，現在網站管理者可以放心的使用Let's Encrypt所提供的免費SSL憑證服務了。另外，需要注意的是，Let's Encrypt簽發的憑證有效期為3個月（90天），也就是說網站每接近3個月時都需要重新更新一次憑證，但還好我們可以透過renewal script來定期更新憑證，基本上配置好shell script及設定好cronjob排程後，就可以不用擔心憑證過期的問題。

本文教學將指引使用者如何在Debian/Ubuntu系統與NGINX網頁伺服器的主機上申請與配置SSL憑證。如果您使用其他的Linux發行版或者是其他的網頁伺服器，當然也是可以參考本教學，但在指令方面需要自行更改以調整至適用您自己系統的環境。本文教學分為3部分，開始會指引使用者如何為域名申請SSL憑證，並將憑證安裝於主機上及設定NGINX設定檔，在SSL憑證配置完成後，筆者會使用Qualys SSL Labs所提供的SSL Server Test線上服務來檢測網站的HTTPS配置及測試您網站啟用HTTPS後是否相容市面上常見的系統及瀏覽器（如舊系統的瀏覽器-Windows XP的IE 8），本文教學第二部分會指引使用者如何配置shell script及設定好crontab，以可以讓Cron自動執行及更新Let's Encrypt憑證，最後部分會指引使用者如何在NGINX伺服器上啟用HTTP/2傳輸協定，及如何檢查網站是否啟用了HTTP/2傳輸協定。

本文教學所使用的憑證申請工具為[Let's Encrypt官方](#)所提供的Let's Encrypt套件。當然您也可以使用其他第三方提供的工具來申請Let's Encrypt憑證，以下所列出的第三方工具會比官方提供套件來的輕巧，支援都很不錯，並且都是開源的，如果您有興趣，那可以考慮使用第三方工具來申請Let's Encrypt的SSL憑證，以下為第三方工具存放在GitHub上的連結：

[acme-tiny](#)

[acme.sh](#)

[letsencrypt.sh](#)

1) 開始為域名申請SSL憑證，並將憑證安裝於主機上及設定NGINX設定檔。

**在申請Let's Encrypt SSL憑證之前，需檢查要申請SSL憑證的域名或子域名DNS的A Record，是否都有對應到主機正確的IP位址。

**如果網站有使用CDN服務，那需要暫時將CDN服務暫停（如：CloudFlare），直到Let's Encrypt憑證建立完成。

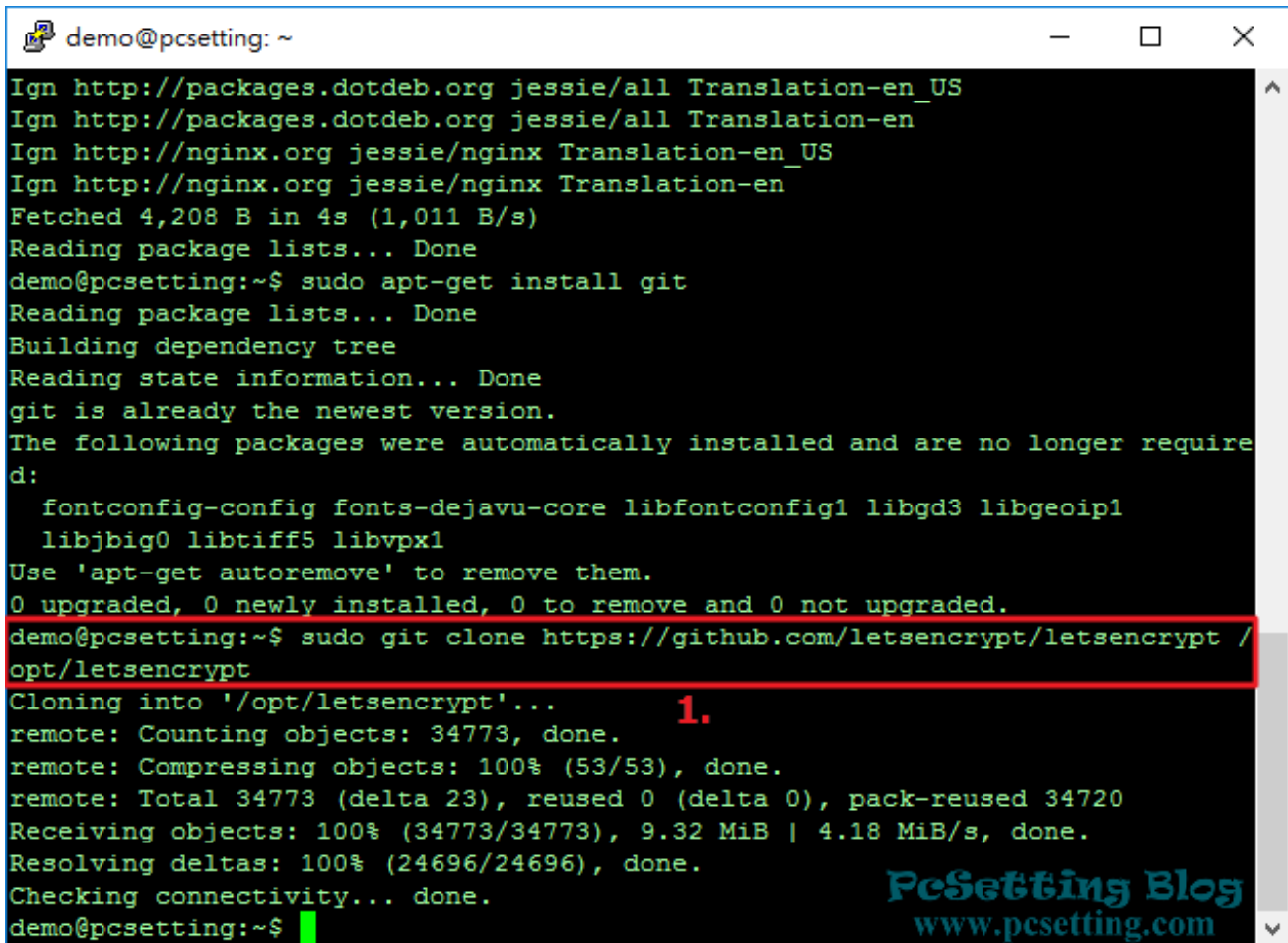
Step 1：在申請憑證之前，需先複製Let's Encrypt套件至您的主機，但因為Let's Encrypt套件是存放在GitHub上，所以我們可以使用Git下載與管理Let's Encrypt套件，在使用Git之前，您的主機需先安裝好Git工具。

```
sudo apt-get update
```

```
sudo apt-get install git
```

Step 2 : 從GitHub複製Let's Encrypt套件至您的主機

```
sudo git clone https://github.com/letsencrypt/letsencrypt /opt/letsencrypt
```



```
demo@pcsetting: ~  
Ign http://packages.dotdeb.org jessie/all Translation-en_US  
Ign http://packages.dotdeb.org jessie/all Translation-en  
Ign http://nginx.org jessie/nginx Translation-en_US  
Ign http://nginx.org jessie/nginx Translation-en  
Fetched 4,208 B in 4s (1,011 B/s)  
Reading package lists... Done  
demo@pcsetting:~$ sudo apt-get install git  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
git is already the newest version.  
The following packages were automatically installed and are no longer required:  
  fontconfig-config fonts-dejavu-core libfontconfig1 libgd3 libgeoip1  
  libjbig0 libtiff5 libvpx1  
Use 'apt-get autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.  
demo@pcsetting:~$ sudo git clone https://github.com/letsencrypt/letsencrypt /  
opt/letsencrypt  
Cloning into '/opt/letsencrypt'... 1.  
remote: Counting objects: 34773, done.  
remote: Compressing objects: 100% (53/53), done.  
remote: Total 34773 (delta 23), reused 0 (delta 0), pack-reused 34720  
Receiving objects: 100% (34773/34773), 9.32 MiB | 4.18 MiB/s, done.  
Resolving deltas: 100% (24696/24696), done.  
Checking connectivity... done.  
demo@pcsetting:~$
```

PeSetting Blog
www.pcsetting.com

Step 3 : 在安裝SSL憑證時，Let's Encrypt會用到Port 80和Port 443，所以需要先停用佔用到這兩個Port的NGINX服務。如果沒有停用，會出現『The program nginx (process ID XXX) is already listening on TCP port 80. This will prevent us from binding to that port. Please stop the nginx program temporarily and then try again.』哪個程序佔用到Port 80或443的錯誤訊息。

```
sudo systemctl stop nginx
```

Step 4 : cd至/opt/letsencrypt目錄位置，執行如下圖所示指令以可以建立新的憑證。

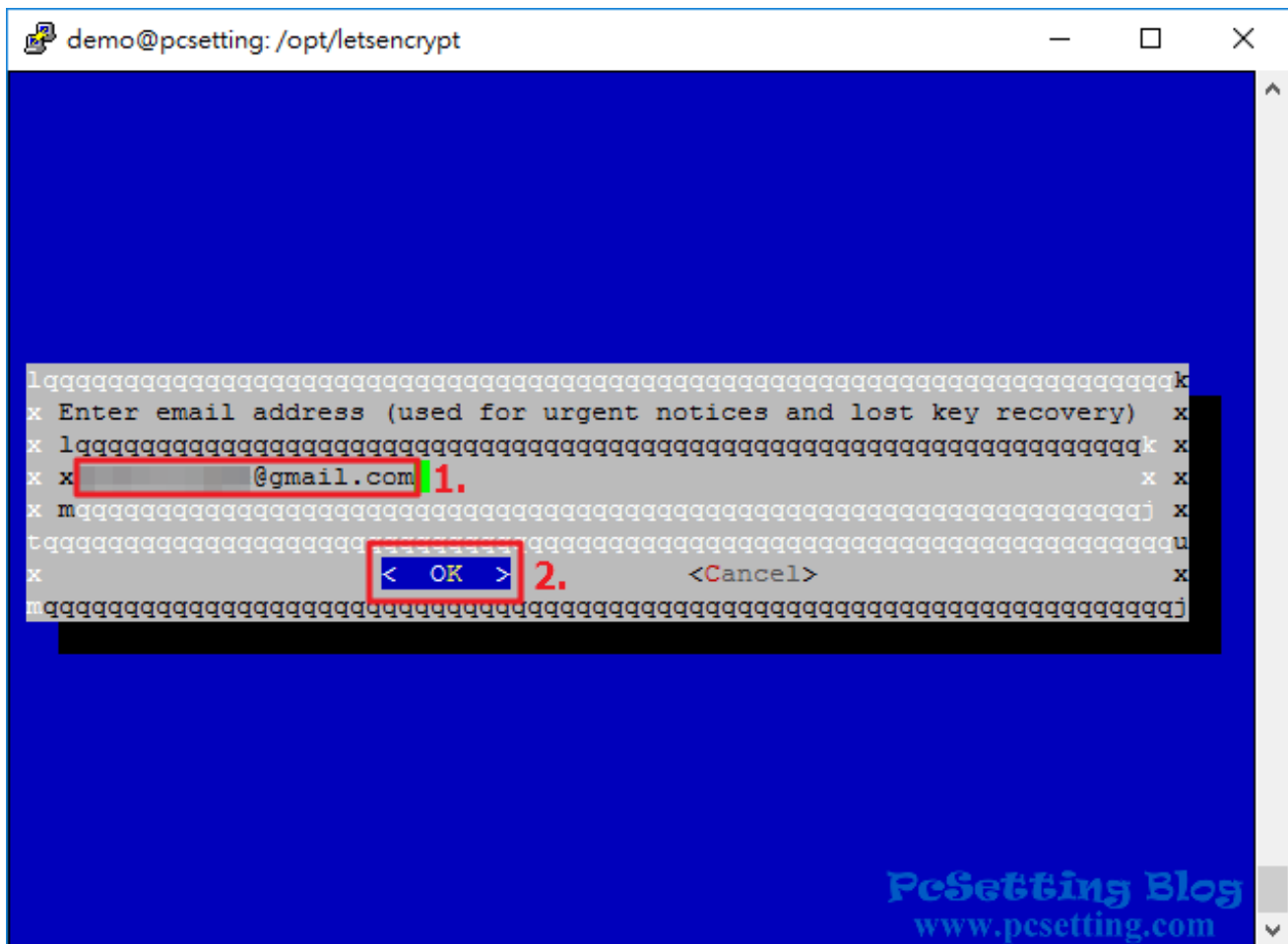
****這邊在安裝需要的元件會稍微久一些，稍等一下吧。**

```
cd /opt/letsencrypt
```

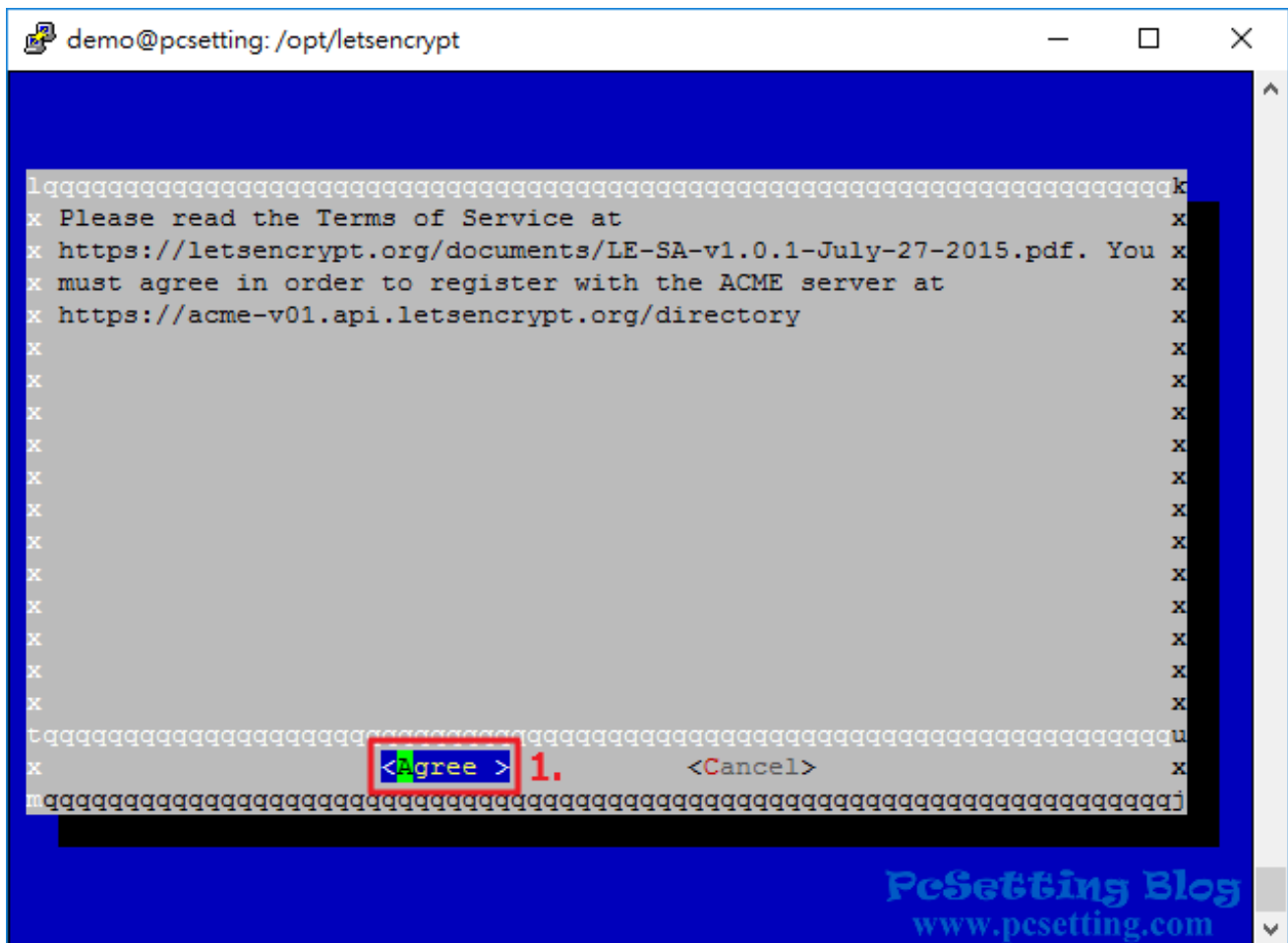
```
./letsencrypt-auto certonly --standalone
```

```
demo@pcsetting: /opt/letsencrypt
Ign http://nginx.org/jessie/nginx Translation-en_US
Ign http://nginx.org/jessie/nginx Translation-en
Fetched 4,208 B in 4s (1,011 B/s)
Reading package lists... Done
demo@pcsetting:~$ sudo apt-get install git
Reading package lists... Done
Building dependency tree
Reading state information... Done
git is already the newest version.
The following packages were automatically installed and are no longer required:
  fontconfig-config fonts-dejavu-core libfontconfig1 libgd3 libgeoip1
  libjbig0 libtiff5 libvpx1
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
demo@pcsetting:~$ sudo git clone https://github.com/letsencrypt/letsencrypt /
opt/letsencrypt
Cloning into '/opt/letsencrypt'...
remote: Counting objects: 34773, done.
remote: Compressing objects: 100% (53/53), done.
remote: Total 34773 (delta 23), reused 0 (delta 0), pack-reused 34720
Receiving objects: 100% (34773/34773), 9.32 MiB | 4.18 MiB/s, done.
Resolving deltas: 100% (24696/24696), done.
Checking connectivity... done.
demo@pcsetting:~$ sudo systemctl stop nginx
demo@pcsetting:~$ cd /opt/letsencrypt 1.
demo@pcsetting:/opt/letsencrypt$ ./letsencrypt-auto certonly --standalone 2.
```

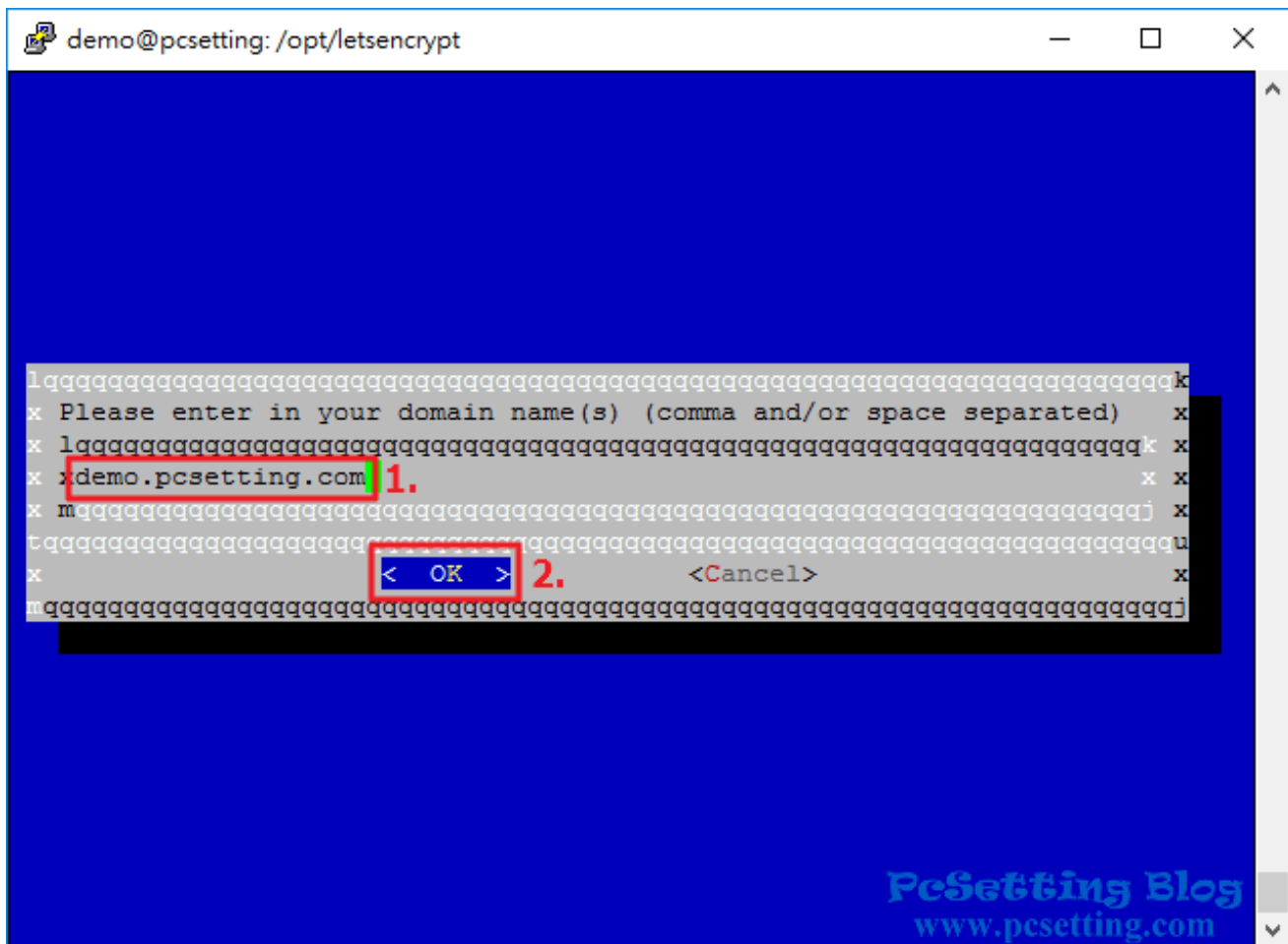
Step 5 : 出現如下圖所示的畫面『Enter email address』，那就輸入您的電子郵件，輸入好後選擇『OK』。



Step 6 : 同意Let's Encrypt相關的許可協議，選擇『Agree』同意。



Step 7 : 在如下圖所示的畫面『Please enter in your domain name』，輸入您要建立SSL憑證的域名，如果您要申請多個域名或子域名，可以用鍵盤『space（空白鍵）』隔開，例如：『example.com www.example.com img.example.com』，輸入好後，選擇『OK』。



額外補充：如果您不想要使用上面Step 5開始的Step by Step方式來申請憑證，那可以使用指令方式來申請憑證，指令格式參考如下：

```
./letsencrypt-auto certonly --standalone --email email@example.com --agree-tos -d example.com -d www.example.com -d img.example.com
```

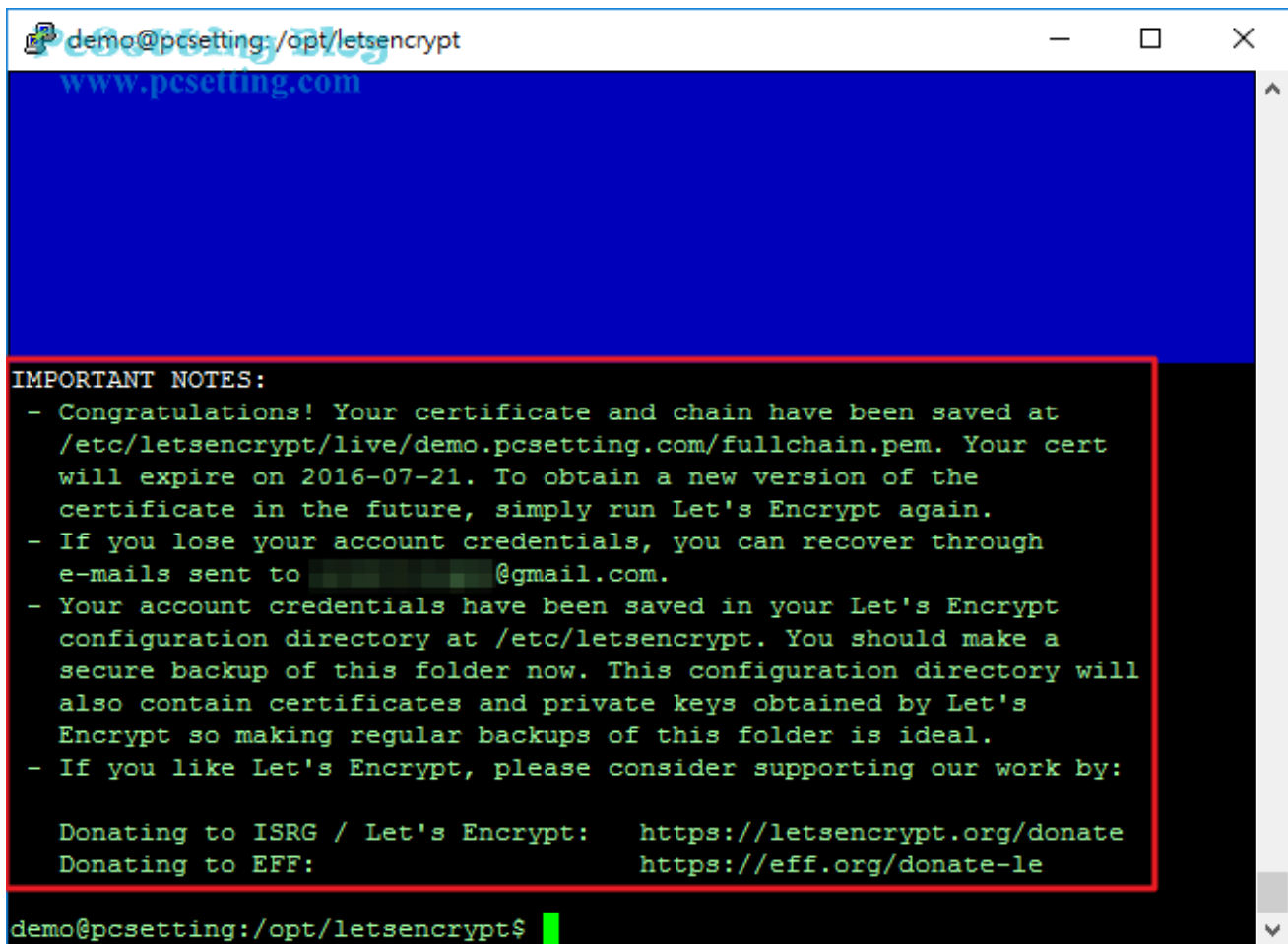
查看Let's Encrypt指令全部的說明：

```
./letsencrypt-auto --help
```

Step 8：憑證建立成功，會出現如下面所示的成功訊息：

IMPORTANT NOTES:

- Congratulations! Your certificate and chain have been saved at /etc/letsencrypt/live/demo.pcsetting.com/fullchain.pem. Your cert will expire on 2016-07-21. To obtain a new version of the certificate in the future, simply run Let's Encrypt again.
- If you lose your account credentials, you can recover through e-mails sent to example@gmail.com.
- Your account credentials have been saved in your Let's Encrypt configuration directory at /etc/letsencrypt. You should make a secure backup of this folder now. This configuration directory will also contain certificates and private keys obtained by Let's Encrypt so making regular backups of this folder is ideal.



```
demo@pcsetting: /opt/letsencrypt
www.pcsetting.com

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at
  /etc/letsencrypt/live/demo.pcsetting.com/fullchain.pem. Your cert
  will expire on 2016-07-21. To obtain a new version of the
  certificate in the future, simply run Let's Encrypt again.
- If you lose your account credentials, you can recover through
  e-mails sent to [REDACTED]@gmail.com.
- Your account credentials have been saved in your Let's Encrypt
  configuration directory at /etc/letsencrypt. You should make a
  secure backup of this folder now. This configuration directory will
  also contain certificates and private keys obtained by Let's
  Encrypt so making regular backups of this folder is ideal.
- If you like Let's Encrypt, please consider supporting our work by:

  Donating to ISRG / Let's Encrypt:  https://letsencrypt.org/donate
  Donating to EFF:                  https://eff.org/donate-le

demo@pcsetting:/opt/letsencrypt$
```

Step 9 : 憑證建立完成後，您可以使用如下圖所示的方式查看憑證是否有簽發成功，在/etc/letsencrypt/live/example.com目錄下，您應該會看到『cert.pem』、『chain.pem』、『fullchain.pem』和『privkey.pem』4個不同的憑證檔案，確定憑證建立成功後，就可以啟動NGINX伺服器了。

```
sudo ls -l /etc/letsencrypt/live
```

```
sudo ls -l /etc/letsencrypt/live/demo.pcsetting.com
```

```
sudo systemctl start nginx
```



```
demo@pcsetting: /opt/letsencrypt
demo@pcsetting:/opt/letsencrypt$ sudo ls -l /etc/letsencrypt/live 1.
total 4
drwxr-xr-x 2 root root 4096 Apr 22 01:01 demo.pcsetting.com
demo@pcsetting:/opt/letsencrypt$ sudo ls -l /etc/letsencrypt/live/demo.pcsetting.com 2.
total 0
lrwxrwxrwx 1 root root 42 Apr 22 01:01 cert.pem -> ../../archive/demo.pcsetting.com/cert2.pem
lrwxrwxrwx 1 root root 43 Apr 22 01:01 chain.pem -> ../../archive/demo.pcsetting.com/chain2.pem
lrwxrwxrwx 1 root root 47 Apr 22 01:01 fullchain.pem -> ../../archive/demo.pcsetting.com/fullchain2.pem
lrwxrwxrwx 1 root root 45 Apr 22 01:01 privkey.pem -> ../../archive/demo.pcsetting.com/privkey2.pem
demo@pcsetting:/opt/letsencrypt$ sudo systemctl start nginx 3.
demo@pcsetting:/opt/letsencrypt$
```

PcSetting Blog
www.pcsetting.com

Step 10 : 使用OpenSSL指令產生一個2048-bit Diffie Hellman Group，以解決Diffie-Hellman金鑰預設長度不足的問題。

**這邊在產生strong DH group會稍微久一些，稍等一下吧。

```
sudo openssl dhparam -out /etc/ssl/certs/dhparams.pem 2048
```



```
demo@pcsetting:/opt/letsencrypt$ sudo ls -l /etc/letsencrypt/live/demo.pcsetting.com
total 0
lrwxrwxrwx 1 root root 42 Apr 22 01:01 cert.pem -> ../../archive/demo.pcsetting.com/cert1.pem
lrwxrwxrwx 1 root root 43 Apr 22 01:01 chain.pem -> ../../archive/demo.pcsetting.com/chain1.pem
lrwxrwxrwx 1 root root 47 Apr 22 01:01 fullchain.pem -> ../../archive/demo.pcsetting.com/fullchain1.pem
lrwxrwxrwx 1 root root 45 Apr 22 01:01 privkey.pem -> ../../archive/demo.pcsetting.com/privkey1.pem
demo@pcsetting:/opt/letsencrypt$ sudo systemctl start nginx
demo@pcsetting:/opt/letsencrypt$ sudo openssl dhparam -out /etc/ssl/certs/dhparams.pem 2048
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.....+.....+.....
.....
+.....+.....+.....
.....
.....+.....+.....
.....+.....+.....
.....+.....+.....
.....+.....
.....++*++*
demo@pcsetting:/opt/letsencrypt$
```

文章評分:

標籤: [Facebook](#)[Google+](#)[Plurk](#)[Line](#)