Apache SSL(https)設定說明

By 劉育彰(brucelyc@tc.edu.tw)

【CentOS】

1. 先輸入 netstat –na | more 確認 443 port 是否已在 listen 狀態。(一般是預設即啟用)

```
[root@localhost ~]# netstat -na | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 0.0.0.0:59211               0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN
tcp        0     52 192.168.110.129:22          192.168.110.1:54985         ESTABLISHED
tcp        0      0 :::54861                    :::*                        LISTEN
tcp        0      0 :::111                      :::*                        LISTEN
tcp        0      0 :::80                       :::*                        LISTEN
tcp        0      0 :::22                       :::*                        LISTEN
tcp        0      0 ::1:631                     :::*                        LISTEN
tcp        0      0 ::1:25                      :::*                        LISTEN
tcp        0      0 :::443                      :::*                        LISTEN
udp        0      0 0.0.0.0:111                 0.0.0.0:*
udp        0      0 0.0.0.0:631                 0.0.0.0:*
udp        0      0 0.0.0.0:35103               0.0.0.0:*
udp        0      0 0.0.0.0:948                 0.0.0.0:*
udp        0      0 0.0.0.0:68                  0.0.0.0:*
udp        0      0 0.0.0.0:967                 0.0.0.0:*
udp        0      0 :::111                      :::*
udp        0      0 :::35963                    :::*
udp        0      0 :::948                      :::*
```

2. 如果已在 listen 狀態的話，再以 vi /etc/sysconfig/iptables 確認本機防火牆是否開啟 443 port。如果沒有的話，只要(1)複製 80 port 的那一行，(2)將 80 改成 443，(3) 以 service iptables restart 命令重啟本機防火牆即可。

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

3. 先於瀏覽器輸入 https://伺服器 IP 或域名可以看到以下畫面(以 IE 為例)，表示 Apache 的 https 正常啟用。

4. 將憑證公鑰檔(.crt)置於/etc/pki/tls/certs/、憑證私鑰檔(.key)置於/etc/pki/tls/private/目錄下。
5. 編輯/etc/httpd/conf.d/ssl.conf 檔，找到以下兩行把紅字部份改成實際檔名
   SSLCertificateFile /etc/pki/tls/certs/localhost.crt
   SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
6. 之後再以 service httpd restart 重新啟動 Apache 即可。

【Ubuntu】

1. 先輸入 netstat –na | more 確認 443 port 是否已在 listen 狀態。如果沒有的話，請以 sudo a2enmod ssl 啟用 apache2 的 ssl 模組，並以 sudo service apache2 restart 重啟 apache2。(一般是預設未啟用)

```
root@ubuntu:~# netstat -na
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp        0      0 192.168.110.130:22      192.168.110.1:64300     ESTABLISHED
tcp6       0      0 :::22                   :::*                    LISTEN
udp        0      0 0.0.0.0:68              0.0.0.0:*
```

2. 以 ufw status 指令檢視本機防火牆是否啟用，如果啟用中的話，請以 ufw allow 443 開通 443 port。
3. 編輯/etc/apache2/sites-available/default 檔案，檢視是否存在 443 port 的設定，如果沒有的話，請將<VirtualHost *:80>至</VirtualHost>內容複製貼於</VirtualHost>下方，並依紅色字體部份增修。

   <VirtualHost *:80>

.....
</VirtualHost>

<VirtualHost *:443>
.....
</Directory>
SSLEngine on
SSLCertificateFile /etc/apache2/ssl/sfs.xxx.tc.edu.tw.crt
SSLCertificateKeyFile /etc/apache2/ssl/sfs.xxx.tc.edu.tw.key

ErrorLog ${APACHE_LOG_DIR}/error.log
.....
</VirtualHost>

4. 以 mkdir /etc/apache2/ssl/建立目錄
5. 將憑證公鑰檔(.crt)、憑證私鑰檔(.key)置於/etc/apache2/ssl/目錄中。
6. 以 sudo service apache2 restart 重新啟動 Apache 即可。

【FreeBSD】

1. 先輸入 netstat –na | more 確認 443 port 是否已在 listen 狀態。(預設未啟用)

```
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4       0      0 *.443                  *.*                    LISTEN
tcp6       0      0 *.443                  *.*                    LISTEN
tcp4       0      0 *.80                   *.*                    LISTEN
tcp6       0      0 *.80                   *.*                    LISTEN
tcp4       0     52                                              ESTABLISHED
tcp4       0      0 *.21                   *.*                    LISTEN
tcp4       0      0 127.0.0.1.25           *.*                    LISTEN
tcp4       0      0 *.22                   *.*                    LISTEN
tcp6       0      0 *.22                   *.*                    LISTEN
tcp4       0      0 *.3306                 *.*                    LISTEN
udp4       0      0 *.514                  *.*
udp6       0      0 *.514                  *.*
```

2. 如果沒有的話，請開啟/usr/local/etc/apache22/ httpd.conf，找到「Include etc/apache22/extra/httpd-ssl.conf」這一行，把前面的「 # 」去掉後儲存。
3. 將憑證公鑰檔(.crt)、憑證私鑰檔(.key)置於/ usr/local/etc/apache22/目錄下。
4. 開啟 / usr/local/etc/apache22/extra/httpd-ssl.conf，找到以下兩行把紅字部份改成實際檔名：
   SSLCertificateFile "/usr/local/etc/apache22/server.crt"
   SSLCertificateKeyFile "/usr/local/etc/apache22/server.key"

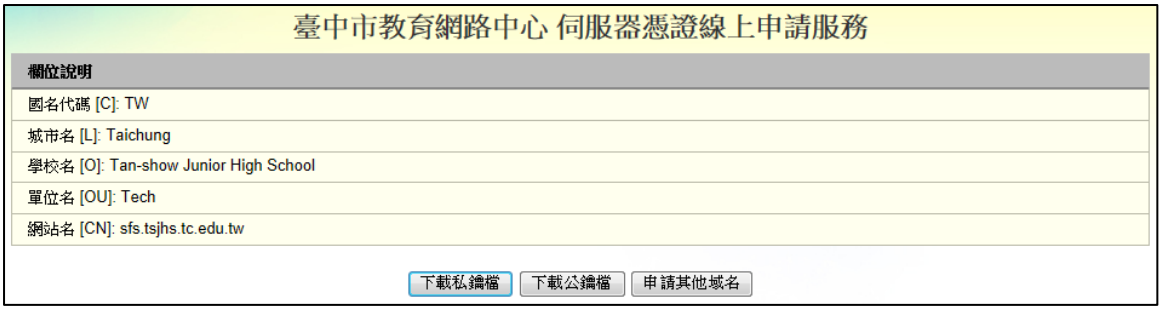
5. 以 apachectl restart 重新啟動 Apache 即可。

【公私鑰取得】

為了方便各校快速設定 Apache 之 https，所以臺中市所屬各國中小可直接由教育局網站線上申請伺服器憑證：

https://www.tc.edu.tw/net/careq

申請時僅需填入主機名即可。(其他資料由資料庫自動抓取，也不能改，只申請得到自己學校的域名)

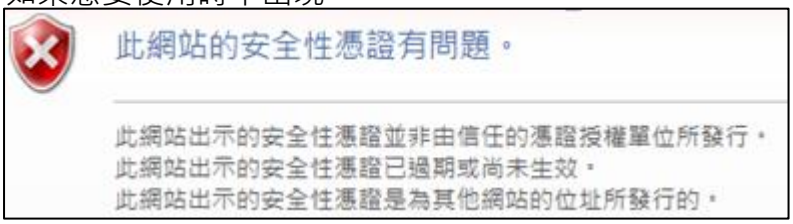


按下「確定申請」後，系統會馬上產生一組公私鑰檔，請依序下載「私鑰檔」與「公鑰檔」，系統在使用者下載後會立即刪除這兩個檔案，請務必妥善保管私鑰檔，以免造成資安問題。

PS.若其他縣市學校要使用本市教育局所簽發之憑證，請把學校英文名、網站名 mail 給我，並在學校 DNS 內暫時設定一筆 A 記錄為「sfs99.學校域名 IN A 163.17.40.13」，因為要以 DNS 的管理權來驗證學校，我們會盡快把公私鑰寄給您。

【根憑證與中繼憑證匯入】

如果想要使用時不出現



請在各電腦中匯入 TC 根憑證與 TC 中繼憑證，詳細步驟請參考：

https://www.tc.edu.tw/s/2928

至於我們為什麼要發憑證呢？

如果有一天，XCA 組織及團體憑證管理中心可以發伺服器憑證給學校的話，大家就不必做匯入根憑證與中繼憑證的這件事。可是在這之前，如果各校都做自己的憑證，就要匯入各校自製的根憑證，要用到其他學校的網站時也要再做一次，非常麻煩！如果這件事是由教育局來做，因為大家的憑證都由教育局的自製根憑證簽發，所以不管是哪一個學校匯入的都是同樣的根憑證與中繼憑證，用其他學校的網站也不必重新做這些事，這樣是不是方便多了呢？當然，還是期待有一天 XCA 能發憑證給學校，自行匯入憑證的事就不必再做了。

【EV SSL】

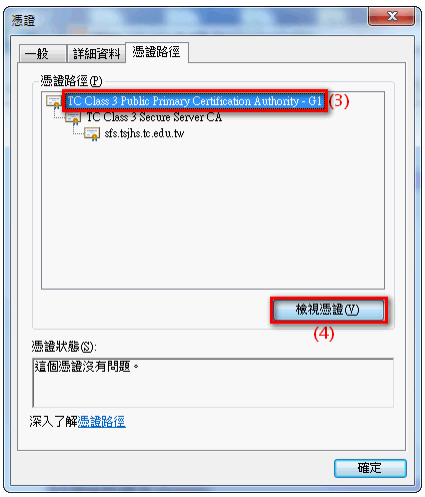
原本想做 EV SSL 憑證給大家，不知道大家有沒有看過綠色的網址列，例如：

不過 K 了很多資料後發現，實際上要做到這個應該是要花錢的，但如果學校使用我們的憑證，想要在 IE 上看到這個是有機會的。

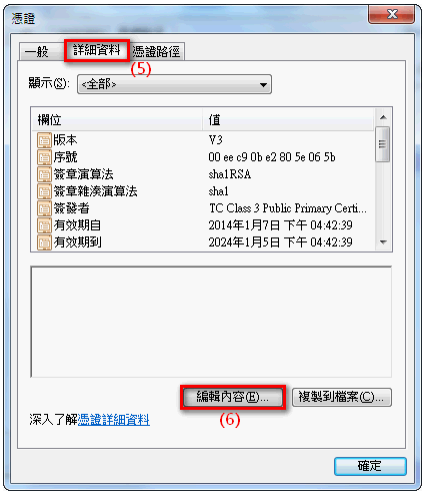
1.先依照前面的步驟設定好伺服器憑證、匯入根憑證與中繼憑證，然後點選網址列上的鎖

2.按下「檢視憑證」

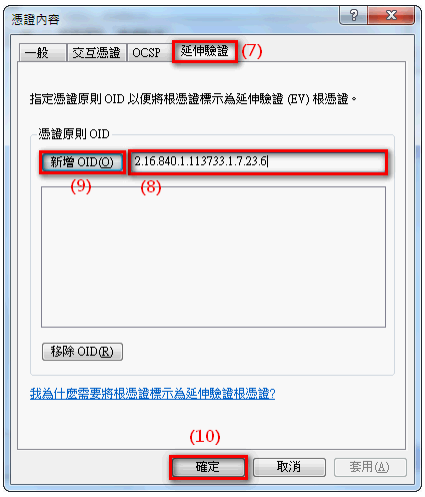
3.選擇「憑證路徑」，選擇最上方的憑證(也就是根憑證)，再按中間的「檢視憑證」



4.選擇「詳細資料」，然後按下中間的「編輯內容」



5.選擇延伸驗證，輸入「2.16.840.1.113733.1.7.23.6」，按下「新增 OID」，按下「確定」(其實這個 OID 是 VeriSign 公司的 EV 定義，其他的請參考 http://en.wikipedia.org/wiki/Extended_Validation_Certificate)



6.最後按下「確定」，重新整理網頁

就出現綠色網址列了！

後記：試了四種瀏覽器後發現(IE, FF, Chrome, Opera)後發現，IE 的網址列可以變綠，FF 和 Chrome 也接受自製憑證會顯示「安全的連線」，只有 opera 最嚴謹，仍顯示是「一般連線」，

問題是無法由 OCSP 取得憑證狀態(這是因為我們還沒做 OCSP Server)，順便供大家參考。