SSL 伺服器數位憑證 Apache2.4
伺服器操作手冊(適用於 UNIX)

臺灣網路認證股份有限公司
TAIWAN-CA. Inc.
台北市 100 延平南路 85 號 10 樓
電話:02-2370-8886
傳真:02-2370-0728
www.twca.com.tw

機密等級：公開
版本：V5.1
文件編號：MNT-03-110
生效日期：110 年 8 月 10 日

目　　錄

1.目的

1.1. 介紹 Apache2.4(適用於 UNIX 環境)網頁伺服器之金鑰、憑證請求檔產製步驟及 SSL 伺服器數位憑證安裝說明。

1.2. 符合本公司資訊安全政策之規範。

2.範圍

無。

3.參考資料

無。

4.定義

無。

5.作業程序

5.1 前置作業

本操作手冊以 CentOS(Version 5.8-i386)的 Linux 作業系統為範例。

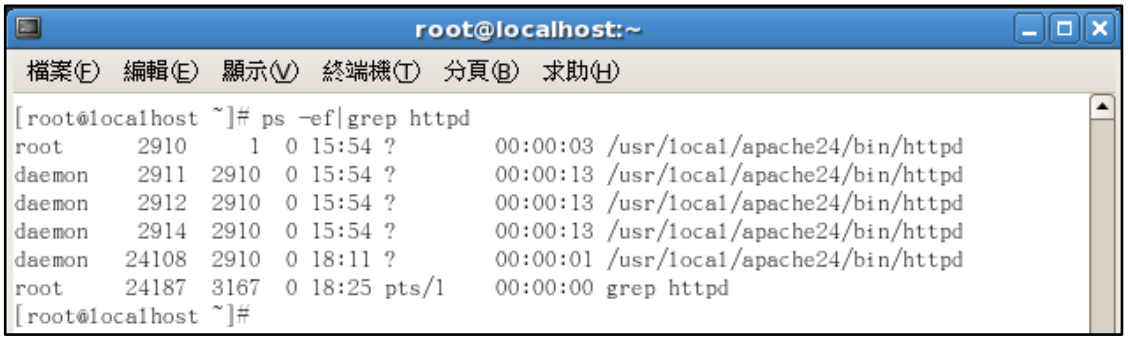
5.1.1 確認 Apache 是否安裝，並查詢 Apache 設定檔路徑

Apache 2.4 Web 伺服器軟體是由 Apache 組織所提供的 Web 伺服器軟體，可執行下列指令確認伺服器主機的 Apache 環境現況：

1. 確認 Apache 是否於作業系統執行緒中，可執行下列指令：

   ps -ef |grep httpd

   同時亦可確定 Apache 之安裝路徑。(備註：以下 Apache 路徑以 **/usr/local/apache24/**為例)。



2. 查詢 Apache 套件版本，可執行下列指令：

   /usr/local/apache24/bin/apachectl -v 。

   以下圖為例，版本為 Apache 2.5.6(UNIX)。(備註：Apache 2 或更早之版本，SSL 之設定檔為 ssl.conf；Apache 2.2、Apache 2.4 版本，SSL 之設定檔為 httpd-ssl.conf)

3. 確認 Apache 設定檔路徑，可執行下列指令：

find / -name httpd.conf

4. 建立存放憑證鏈之目錄(SSL_Certs) ，可執行下列指令：

mkdir SSL_Certs

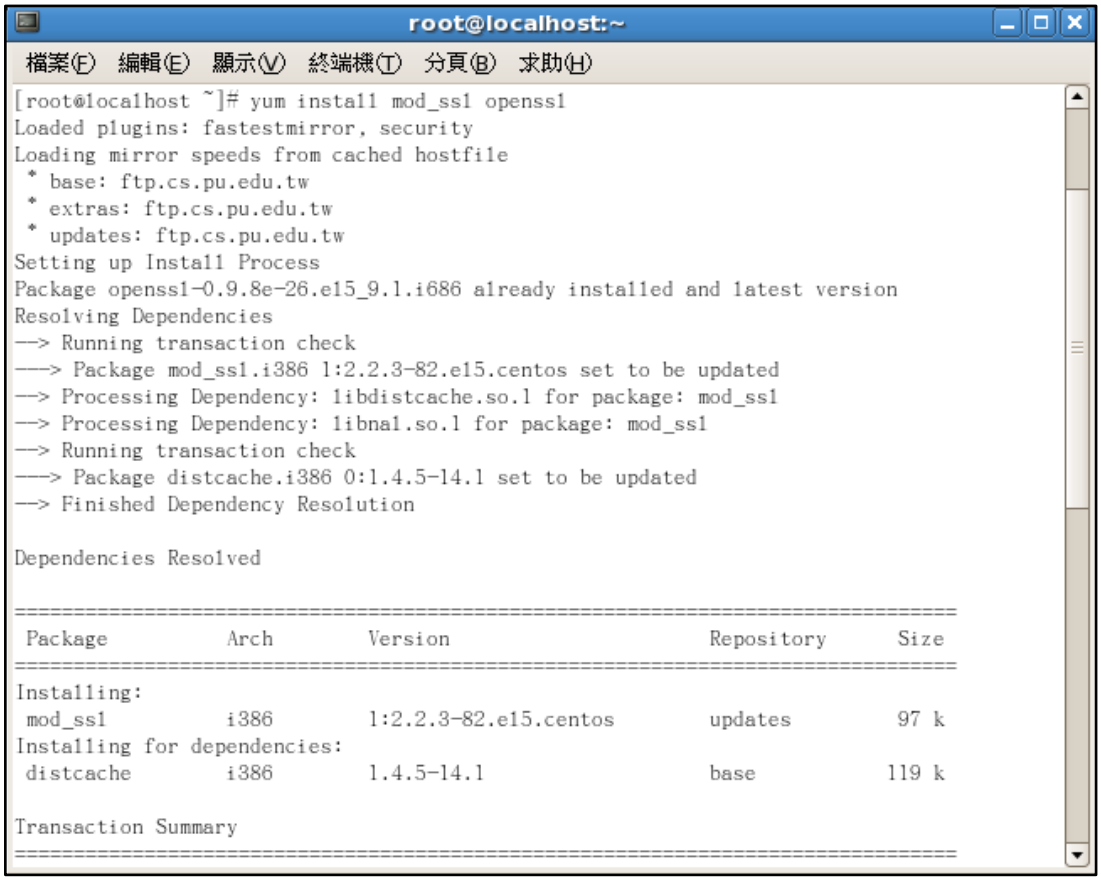
新增一存放憑證鏈相關檔案之目錄，供日後憑證管理使用。(備註：以下憑證鏈存放路徑以**/usr/local/apache24/SSL_Certs** 為例)

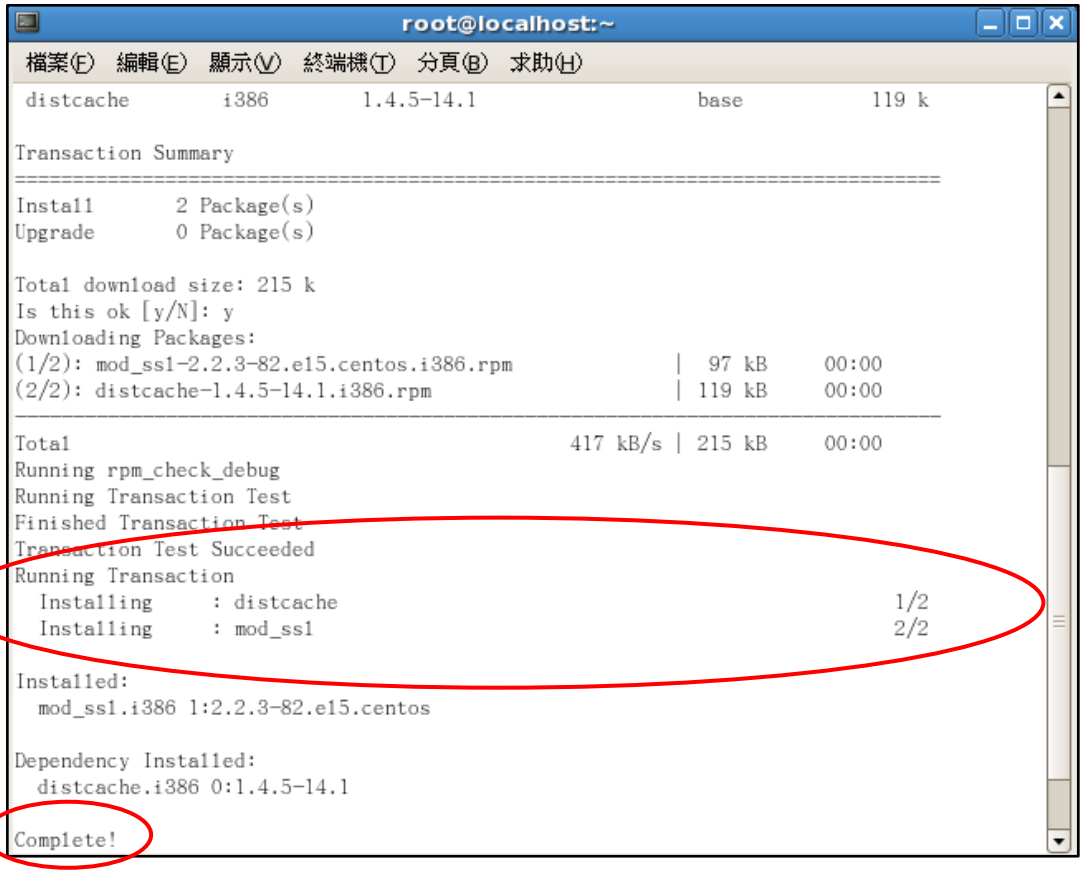
5.1.2 安裝 OpenSSL 軟體

Apache 需搭配 OpenSSL 軟體來產製金鑰，可執行下列指令確認伺服器主機是否支援 OpenSSL，可執行下列指令：

yum install mod_ssl openssl

1. 若伺服器主機**不支援** OpenSSL，Linux 將下載最新版本的 OpenSSL，更新完成後會顯示更新項目清單與 **Complete!**。。





2. 若伺服器主機已有最新版本的 OpenSSL，檢測之 package 為最新版本，且會顯示 **Nothing to do**。

```
[root@localhost ~]# yum install mod_ssl openssl
Loaded plugins: fastestmirror, security
Loading mirror speeds from cached hostfile
 * base: ftp.cs.pu.edu.tw
 * extras: ftp.cs.pu.edu.tw
 * updates: ftp.cs.pu.edu.tw
Setting up Install Process
Package 1:mod_ssl-2.2.3-82.el5.centos.i386 already installed and latest version
Package openssl-0.9.8e-26.el5_9.1.i686 already installed and latest version
Nothing to do
```

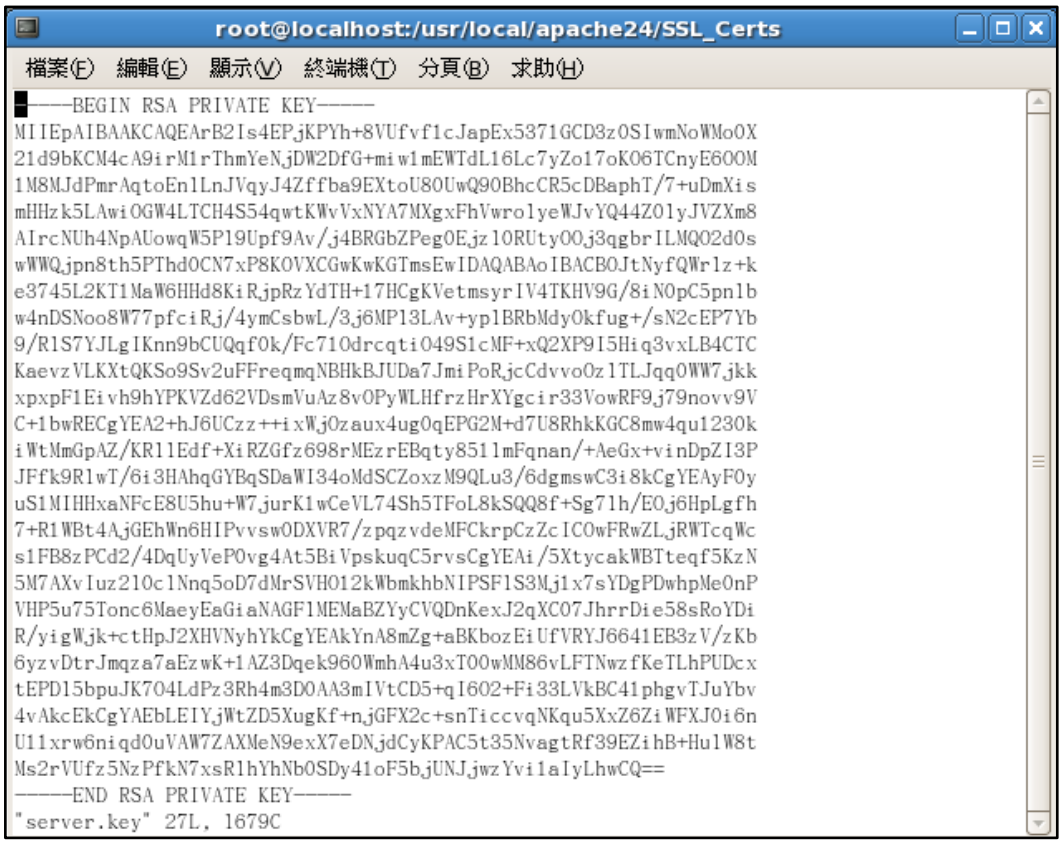
5.2 產製「金鑰」

5.2.1 執行下列指令

openssl genrsa -out /usr/local/apache24/SSL_Certs/server.key 2048

(指令反白部份請依實際路徑決定，-out 即為產生的金鑰檔存放位置)

完成上列指令後會在**/usr/local/apache24/SSL_Certs** 目錄下產生檔案名稱為 server.key 的 2048 位元長度 RSA 金鑰檔，使用文字編輯器打開金鑰檔後可看到如下內容

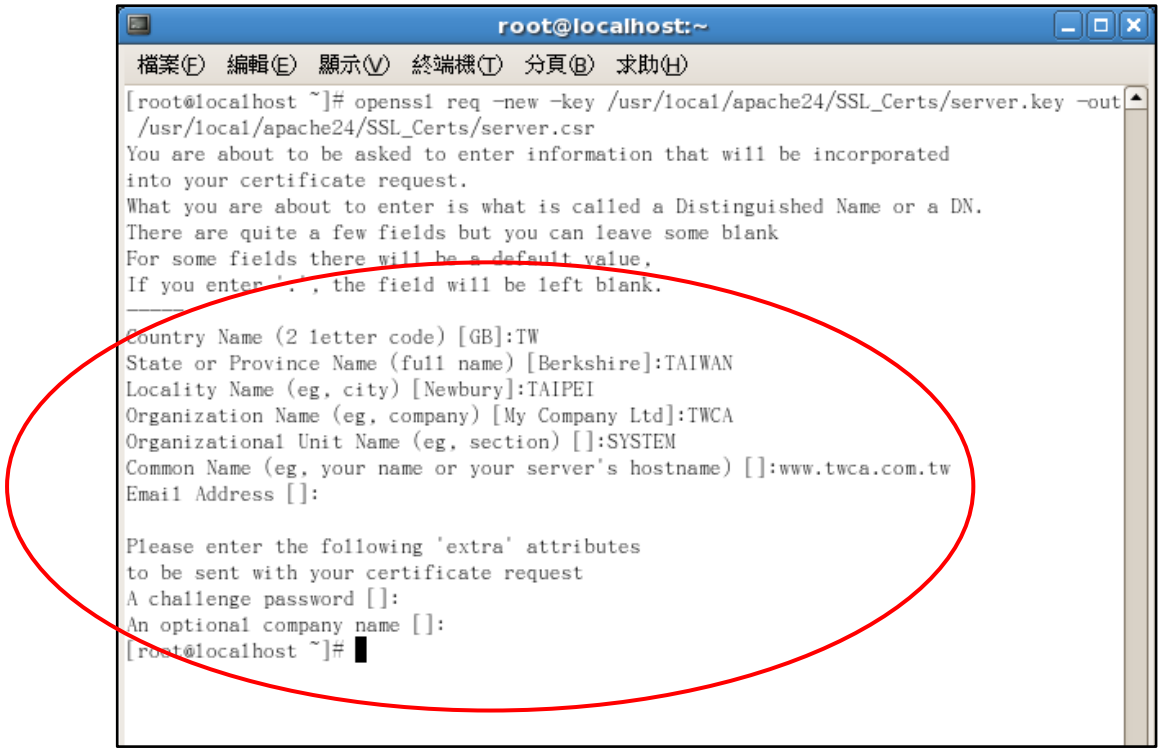


5.3 產生「憑證請求檔(CSR)」

5.3.1 執行下列指令

openssl req -new -key /usr/local/apache24/SSL_Certs/server.key -out /usr/local/apache24/SSL_Certs/server.csr

(指令反白部份請依實際路徑決定，-key 所指定的路徑即為 5.2 節所產生的金鑰檔位置，-out 即為產生的 CSR 存放位置)



此時會要求輸入憑證內容，說明如下：

請輸入 2 碼國碼(如 TW)，必填

Country Name（2 letter code）〔GB〕: TW

請輸入州/省別(如 TAIWAN)，必填

State or Province Name（full name）〔Berkshire〕: TAIWAN

請輸入所在城市(如 TAIPEI)，必填

Locality Name（eg, city）〔Newbury〕: TAIPEI

請輸入組織名稱(如 TWCA)，必填

Organization Name（eg, company）〔My Company Ltd〕: TWCA

請輸入單位名稱(如 IT、SYSTEM)，必填

Organizational Unit Name（eg, section）[ ]: SYSTEM

請輸入貴公司欲加密的網站名稱(如 www.twca.com.tw)，必填

Common Name（eg, your name or your server's hostname）[ ]:

www.twca.com.tw

請輸入申請人員 Email，可不填

Email Address [ ]:

最後會要求輸入額外資訊，請勿填寫任何資料，直接按 Enter 即可

Please enter the following 'extra'
to be sent with your certificaterequest
A challenge password [ ]:
An optional company name [ ]:

完成上列指令後會在**/usr/local/apache24/SSL_Certs** 下產生 server.csr 的檔案，此檔即為憑證請求檔，使用文字編輯器打開金鑰檔後可看到如下內容

5.4 將製作好的憑證請求檔(CSR)上傳

5.4.1 連接 TWCA 網站(1)

連接至本公司首頁 https://www.twca.com.tw

點選憑證服務，點選 SSL 憑證。

5.4.2 連接 TWCA 網站(2)

點選申請憑證。

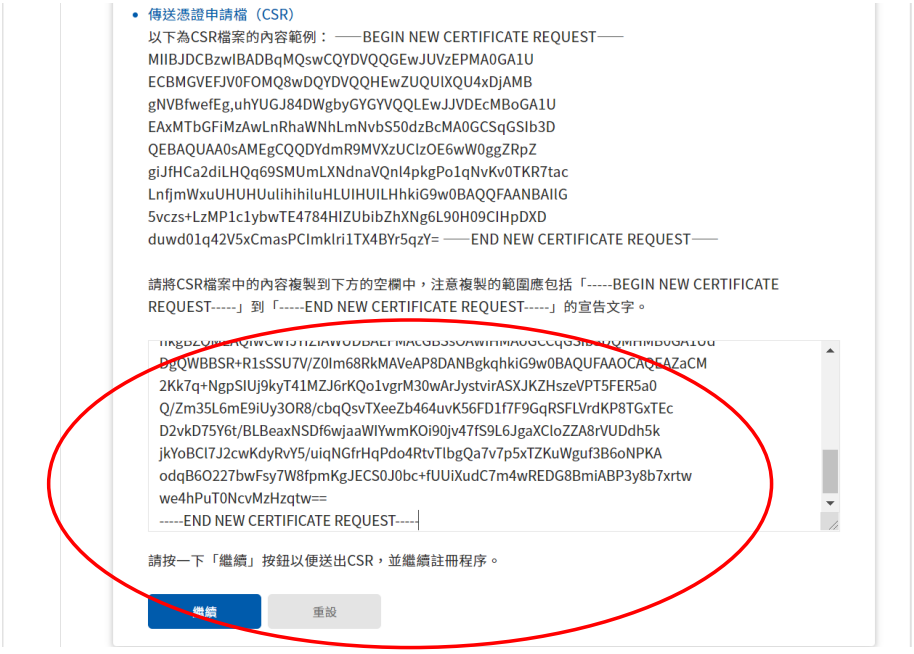
※如申請 EV SSL 伺服器憑證，請點選 EV SSL 憑證。

5.4.3 連接 TWCA 網站(3)

將瀏覽器視窗畫面往下拉，上傳 CSR。

5.4.4 貼上憑證請求檔

開啟在 5.3 章節產生的憑證請求檔，利用全選後複製貼上的方式(CSR 檔案內容包含-----BEGIN CERTIFICATE REQUEST-----、-----END CERTIFICATE REQUEST-----)，將製作好之憑證請求檔（CSR）內容貼到申請欄位中→選擇繼續。



5.4.5 再次檢視上傳之憑證請求檔案內容

5.4.6 設定通行密碼及選擇身分審驗方式

5.4.6.1 請自行設定通行密碼,該密碼請牢記，如您需要廢止憑證時,必須輸入此通行密碼。

請輸入通行密碼

通行密碼 此密碼是廢止憑證所需，請務必記得，並儲存在安全的地方	建立通行密碼

5.4.6.2 為符合 SSL 憑證國際審放標準，將審驗網域所有權者請您選擇以下一種審驗方式:

一、EMAIL 驗證：將會自動帶出網域註冊之 EAMIL 或者請選擇 admin@網域、administrator@網域、webmaster@網域、hostmaster@網域、postmaster@網域此六個 EMAIL 任一個 EMAIL 皆可進行身分驗證作業，選擇送出後系統將會寄出驗證信，請務必至該信箱完成驗證作業

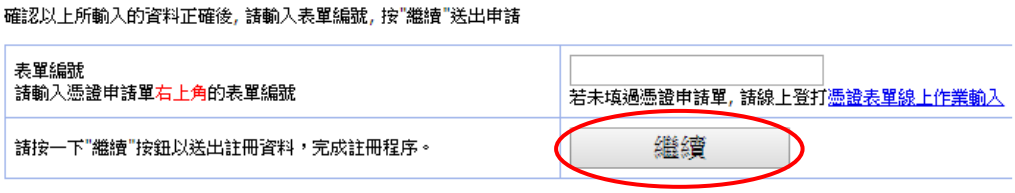
二、檔案驗證：請您填入收取該檔案收件人 EMAIL,您將在此 EMAIL 收到一附件檔案,請您依照信件說明將檔案放入,完成後請通知我們進行檔案驗證作業。

三、電話驗證：網域所有權人的資料可公開查詢到才能使用電話驗證,

請您選擇進行電話驗證的時段,我們將依照您所選擇的去電驗證。

網域所有權

5.4.6.3 填寫表單編號，並確認以上表單內容輸入正確後，按繼續送出申請。



5.4.7 送出後等待 CA 系統簽發憑證

CSR 上傳完成後，近日會完成驗證(以下畫面為選擇電話驗證的顯示結果)，憑證簽發後會以 Email 通知業務及技術聯絡人(TWCA SSL 伺服器數位憑證下載通知)，憑證亦可以在 TWCA 網站搜尋及下載。

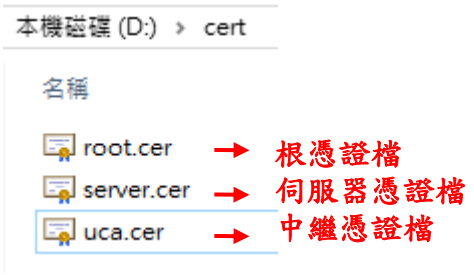
5.5 下載已核發憑證

1 相關檔案說明

若上傳之 CSR 及相關聯絡資料經審驗通過，將會寄送「SSL 伺服器數位憑證下載通知」電子郵件給相關聯絡人，郵件內容包含附件憑證鏈壓縮檔（cert.zip）及 TWCA SSL 動態認證標章之安裝說明與標章圖檔連結。

將附件憑證鏈壓縮檔 cert.zip 解壓縮後，可得到三個憑證鏈檔。

※內容及憑證用途如下圖所式：



2 檔案下載說明

如果因為貴公司之 mail server 設定，導致無法順利取得附件憑證鏈壓縮檔案，請依照下列步驟，利用本公司網站憑證搜尋功能，下載憑證鏈壓縮檔。

5.5.1 連接 TWCA 網站(1)

連接至本公司首頁 https://www.twca.com.tw

點選憑證服務，點選 SSL 憑證。

5.5.2 連接 TWCA 網站(2)

點選憑證搜尋。

5.5.3 輸入申請之網站名稱

在網站名稱中輸入憑證申請單上填寫之網站名稱(Common Name)，如 www.twca.com.tw (**注意，大小寫需一致，不必加 http://或 https://**)，輸入完成後，按下搜尋鍵。

5.5.4 下載憑證鏈壓縮檔

確認憑證相關資訊與申請相符後點選下載→憑證鏈，另開檔案下載視窗，按下另存新檔，儲存憑證鏈壓縮檔 cert.zip。

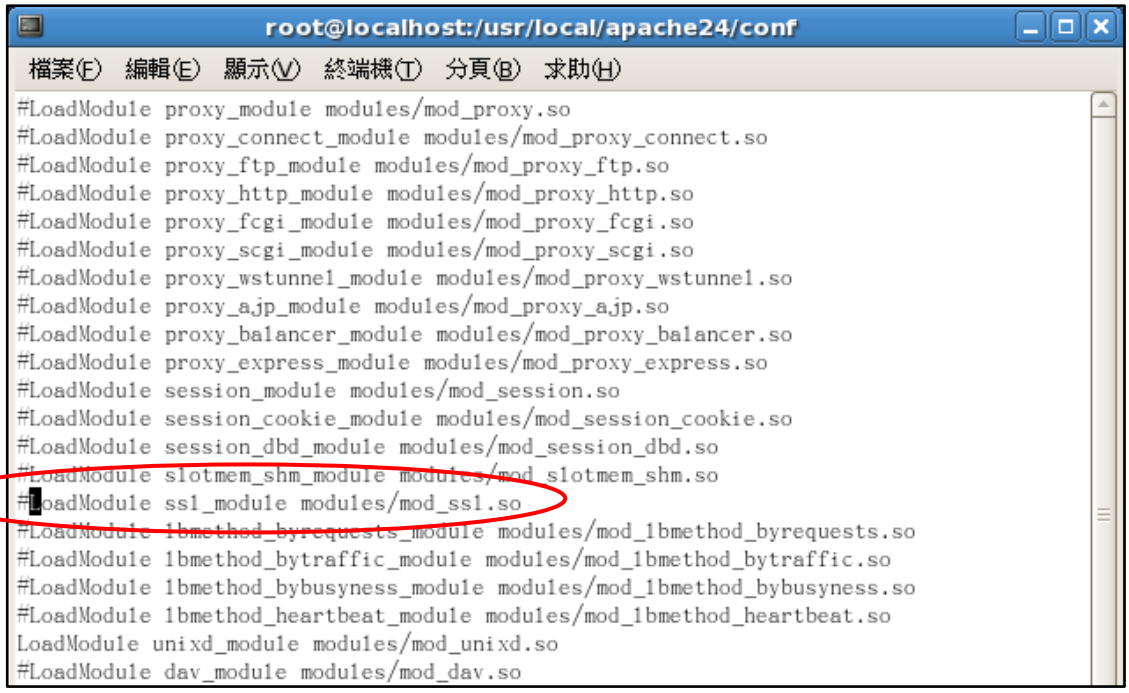
5.6 設定 SSL 模式

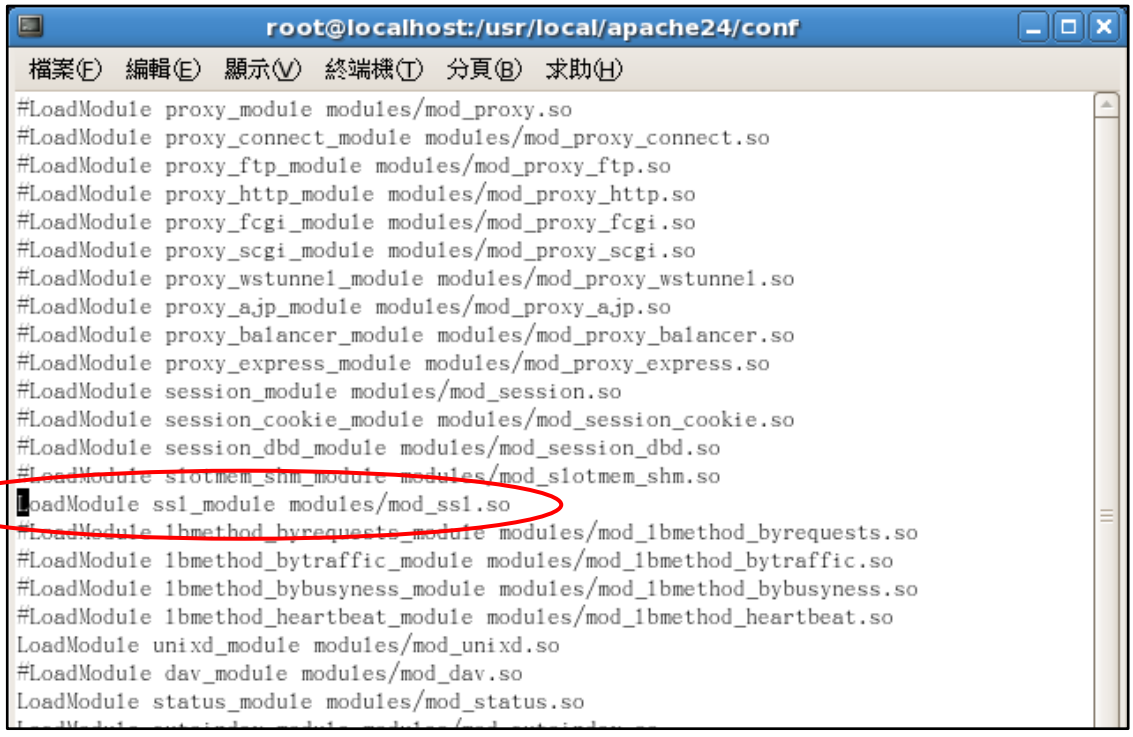
※若安裝主機非首次設定 SSL 憑證且 SSL 功能正常，此章節可跳過不必設定！

5.6.1 編輯**/usr/local/apache24/conf** 目錄下的 httpd.conf 檔案

5.6.1.1 載入 SSL 模組

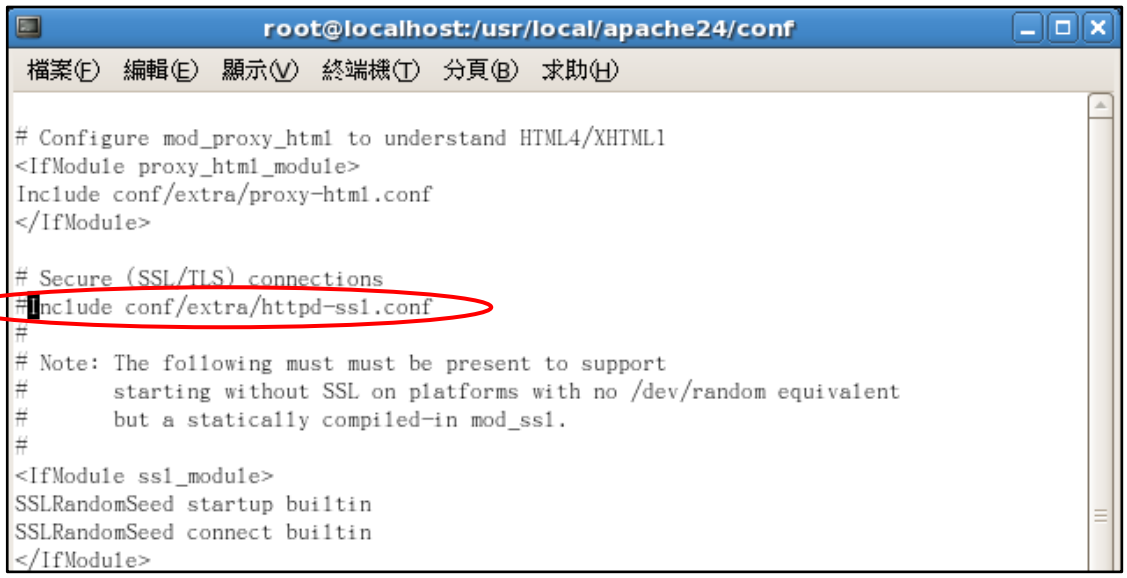
搜尋「mod_ssl.so」字串，可找到其中的 LoadModule ssl_module modules/mod_ssl.so 指令，如果指令前有#字號，請將該指令前的#字號移除。

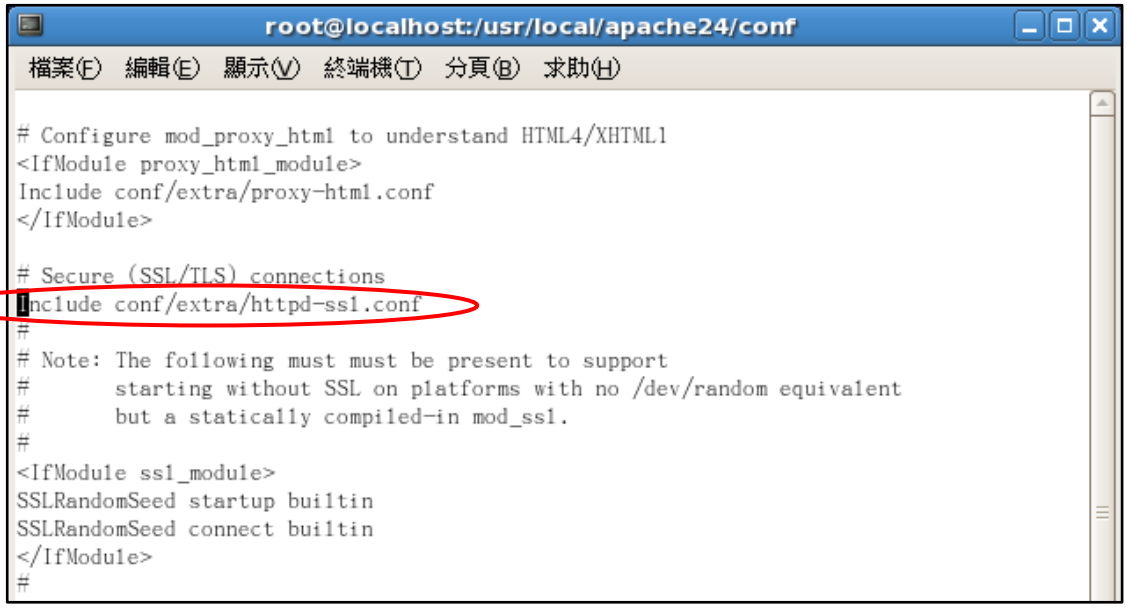




5.6.1.2 載入額外的設定檔 httpd-ssl.conf

搜尋 httpd-ssl.conf (httpd-ssl.conf 設定檔是負責 SSL 的相關設定)，可找到其中的 Include conf/extra/httpd-ssl.conf 指令，如果指令前有#字號，請將該指令前的#字號移除。



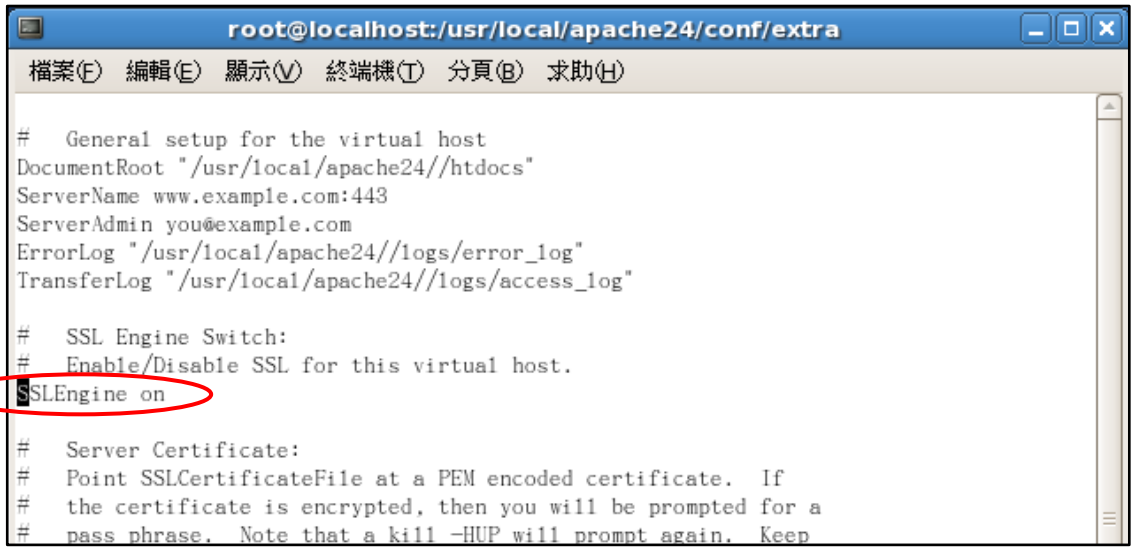


確認完 httpd.conf 內上述兩項設定後儲存檔案。

5.6.2 編輯/usr/local/apache24/conf/extra 目錄下的 httpd-ssl.conf 檔案

5.6.2.1 啟用 SSL 功能

搜尋「SSLEngine」字串，可找到其中的指令 SSLEngine on / off ，SSLEngine on 表示啟用 SSL 功能，如果不啟用 SSL 就將 on 改為 off 即可，這裡請設定為 on。



5.6.2.2 設定 SSL 連接埠

搜尋「Listen」字串，可找到其中的指令 Listen 443，443 Port 是 SSL(https)功能的預設 Port，如果要設定為其他 Port 再修改設定，否則一律設定為 443 即可。

5.7 安裝憑證

5.7.1 Apache 在安裝 SSL 憑證時會使用到三種檔案：

- 於 5.2 章節產製的 SSL 伺服器金鑰「server.key」
- 於 5.5 章節取得的伺服器憑證檔「server.cer」
- 於 5.5 章節取得的中繼憑證檔「uca.cer」

先備妥並將其存放至**/usr/local/apache24/SSL_Certs** 目錄下(實際目錄可自行決定)。

5.7.2 編輯**/usr/local/apache24/conf/extra** 目錄下的 httpd-ssl.conf 檔案

5.7.2.1 安裝伺服器憑證

搜尋「SSLCertificateFile」字串，可找到其中的 SSLCertificateFile 設定，此設定是 SSL 伺服器憑證存放完整路徑，請依 5.7.1 章節檔案存放路徑設定，路徑前後請用「"」包起來。

5.7.2.2 安裝 SSL 伺服器金鑰

搜尋「SSLCertificateKeyFile」字串，可找到其中的 SSLCertificateKeyFile 設定，此設定是 SSL 伺服器金鑰存放完整路徑，請依 5.7.1 章節檔案存放路徑設定，路徑前後請用「"」包起來。

5.7.2.3 安裝中繼憑證

搜尋「SSLCertificateChainFile」字串，可找到其中的 SSLCertificateChainFile 設定，此設定是中繼憑證存放完整路徑，請依 5.7.1 章節檔案存放路徑設定，路徑前後請用「"」包起來。

完成「httpd-ssl.conf」內上述設定後儲存檔案，即完成憑證安裝。

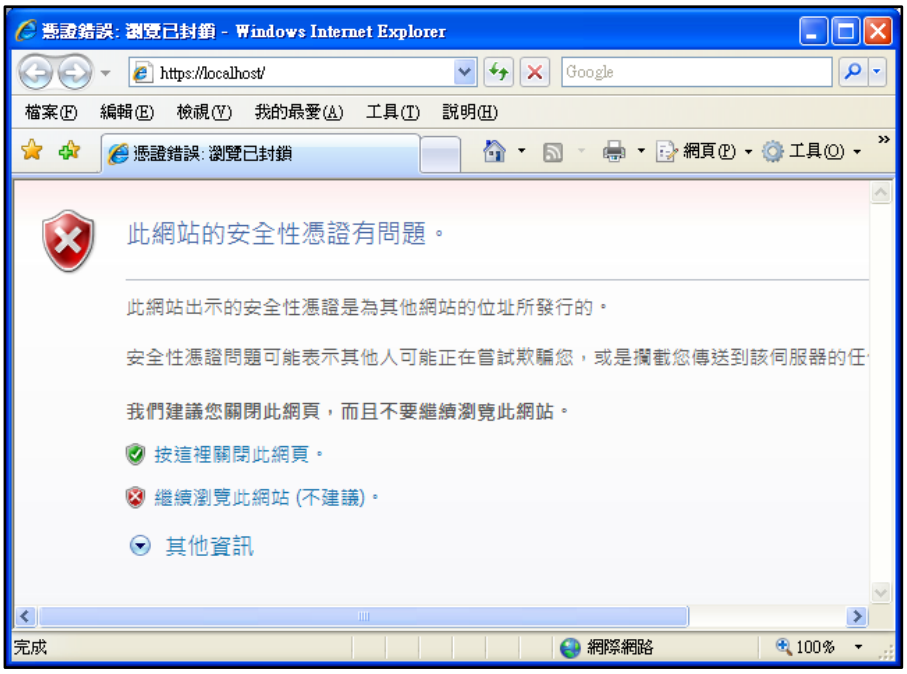
5.7.3 重新啟動 Apache 服務

重新啟動完成即可進入 5.8 節，驗證 SSL 功能。

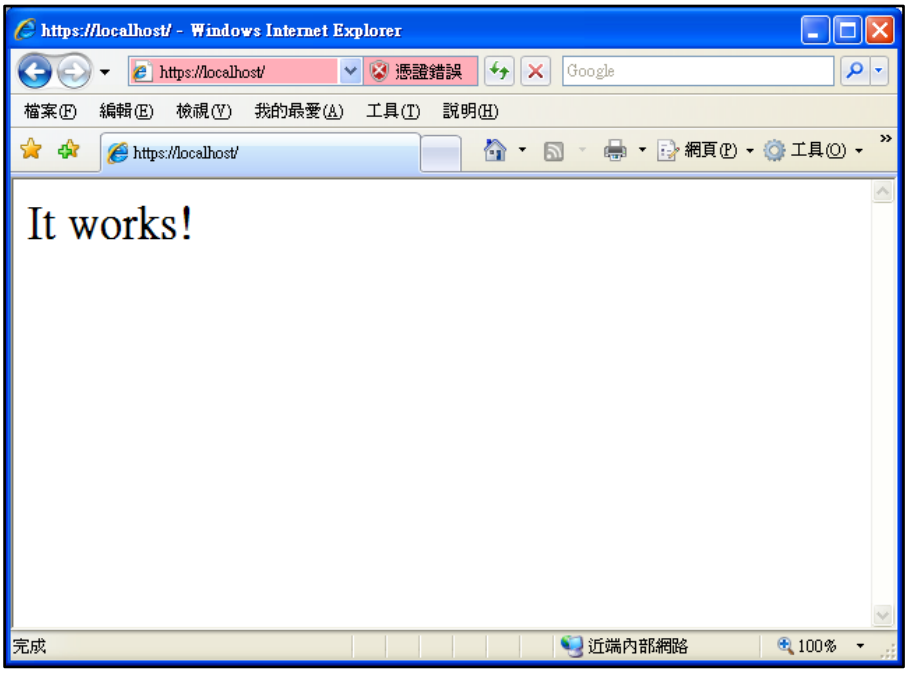
5.8 驗證 SSL 功能

5.8.1 本機驗證

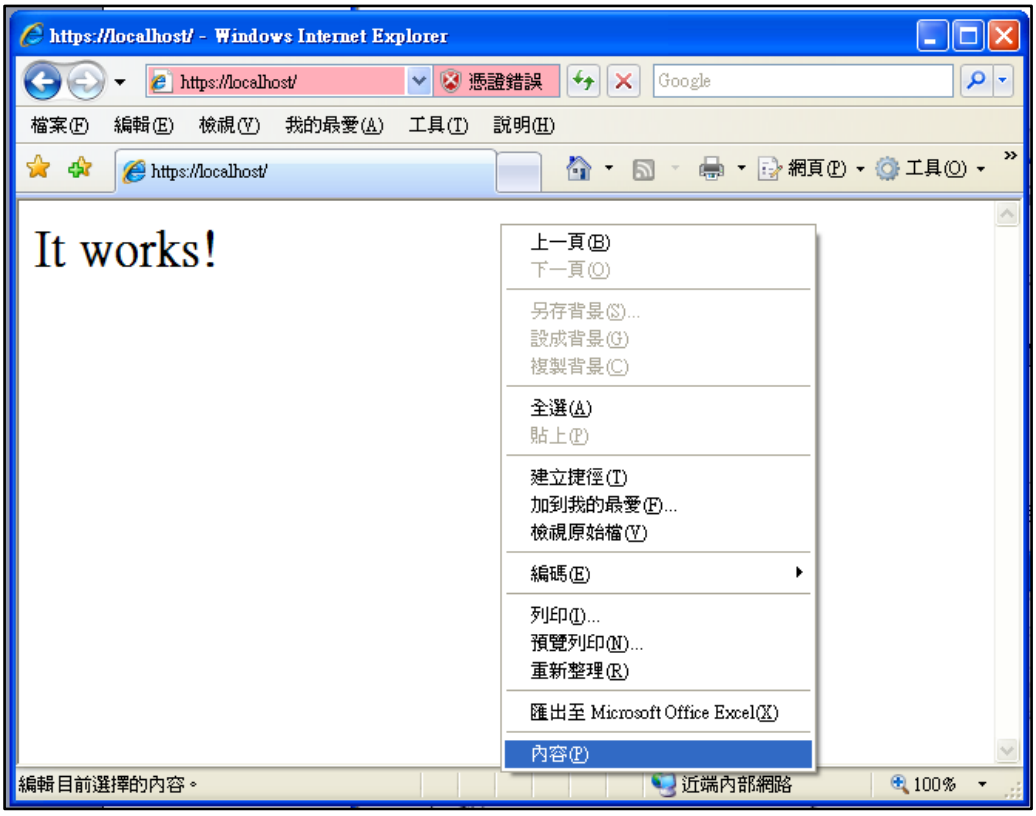
Apache 重新啟動完成後開啟瀏覽器直接連接至本機 https://localhost，此時出現警告訊息是正常的，因為憑證記載內容與網址不符(非 localhost)，請點選「繼續瀏此網站(不建議)」即可。



如果瀏覽器出現 It Works!字樣代表 Apache 已正常服務，且 SSL 功能已啟用。

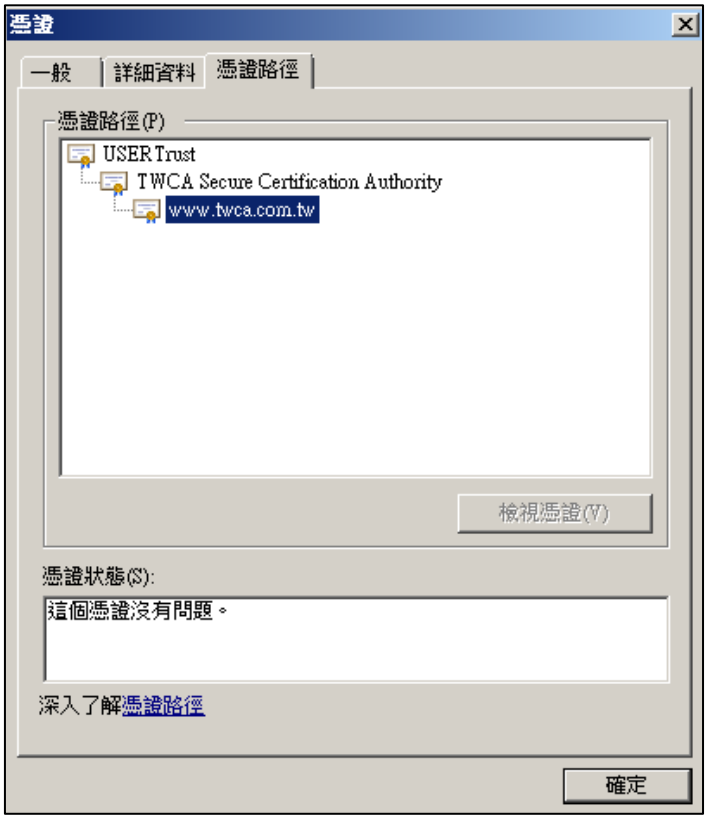


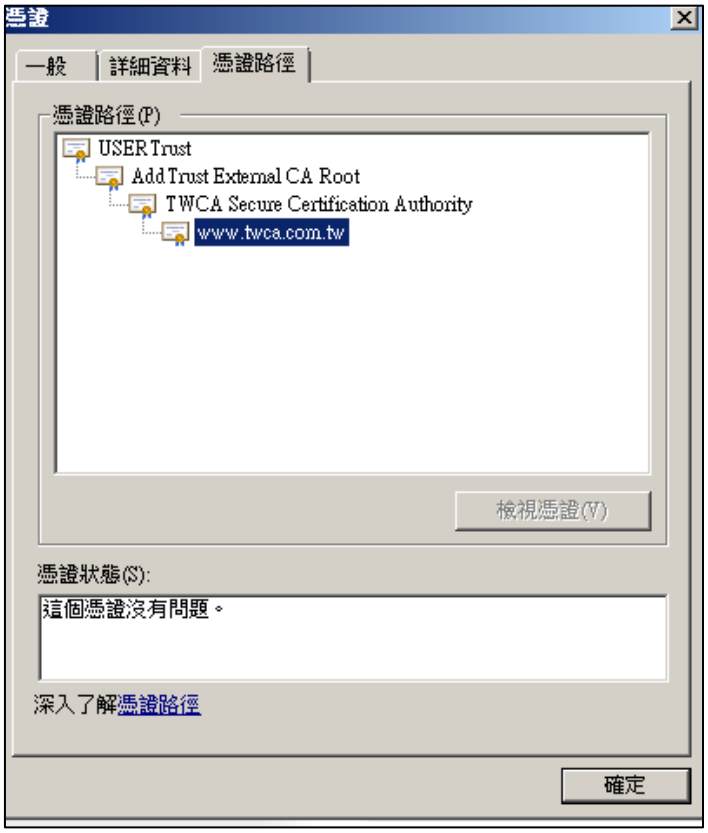
在瀏覽器按滑鼠右鍵出現功能清單，點選「內容」，



此時會出現網頁資訊，確認網頁是否已加密，點選憑證可檢視憑證資訊

憑證路徑欄位：請確認憑證鏈是否正確，且憑證狀態顯示這個憑證沒有問題，可確認憑證已安裝成功。(憑證路徑會因瀏覽器不同而存在三階層或四階層兩種不同的架構，兩種架構皆表示憑證安裝沒有問題。)





5.8.2 外部驗證

驗證程序和 5.8.1 節相同，只是連線位址改為實際網址，

如 https://www.twca.com.tw

5.8.3 為何連線位址正確卻無法顯示網頁?

https 連線埠預設使用 443 Port，如果 5.6.2.2 節設定 Listen Port 非 443，則連線時須指定連線 Port，如 https://www.twca.com.tw:8443

5.9 異常排除

如果完成 5.6 及 5.7 章節設定後，若無法正常重新啟動 Apache 時，表示 SSL 設定有誤，請檢視**/usr/local/apache24/logs/error.log** 檔，該檔案內會記錄啟動失敗原因，待問題排除後再重新啟動。

如果持續發生問題，請聯絡本公司協助處理。

5.10 備份／還原憑證

請將 5.7.1 章節指定的憑證鏈與金鑰檔案備份起來(金鑰、伺服器憑證、中繼憑證)，再依照 5.7.2 至 5.7.3 章節的步驟設定，即可還原憑證。

5.11 更新 SSL 憑證

5.11.1 申請說明

臺灣網路認證公司會在 SSL 伺服器憑證到期前二個月發出憑證更新通知信給　貴公司。這二個月內您隨時可以至本公司網站 https://www.twca.com.tw 下載申請表單，填寫完畢後寄回臺灣網路認證公司，即可進行 SSL 憑證更新申請。

5.11.2 更新步驟

5.11.2.1 備份憑證檔

在進行更新前請記得參考 5.7.1 章節步驟，備份原有的 SSL 伺服器憑證及伺服器金鑰。

5.11.2.2 更新憑證

請參照 5.2 至 5.7 章節申請安裝憑證，並利用 5.8 章節驗證 SSL 憑證是否更新成功，即可完成 SSL 憑證更新。

6.常見問題

6.1 請參閱 https://www.twca.com.tw/picture/file/SSL 常見技術問題手冊.pdf。

7.附件

無。