

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：V1.0

文件編號：MNT-03-110

生效日期：114 年 6 月 3 日

目 錄

1.目的	1
2.參考資料	2
3.定義	3
4.作業程序	4
4.1 前置作業.....	4
4.2 產製「金鑰」	8
4.3 產生「憑證請求檔(CSR)」	9
4.4 將製作好的憑證請求檔(CSR)上傳	錯誤! 尚未定義書籤。
4.5 下載已核發憑證.....	19
4.6 設定 SSL 模式	25
4.7 安裝憑證.....	28
4.8 驗證 SSL 功能.....	33
4.9 異常排除.....	37
4.10 備份／還原憑證.....	38
4.11 更新 SSL 憑證.....	39
5.附件	40

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. 參考資料

無。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

3. 定義

無。

4. 作業程序

4.1 前置作業

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

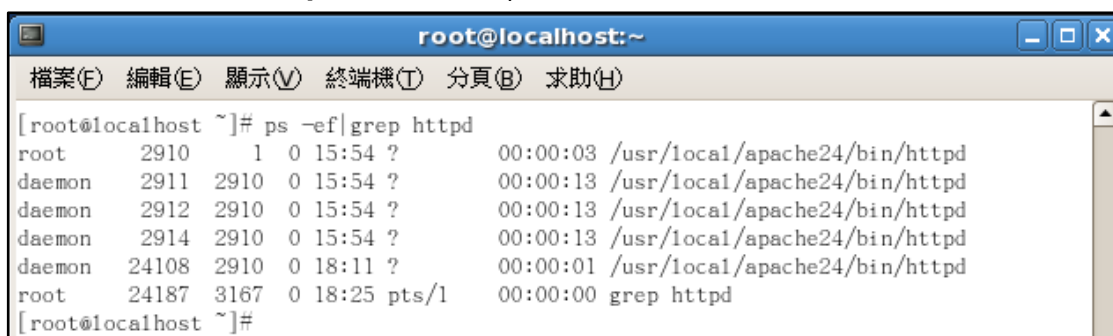
4.1.1 確認 Apache 是否安裝，並查詢 Apache 設定檔路徑

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)。



```
root@localhost:~  
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)  
[root@localhost ~]# ps -ef|grep httpd  
root      2910      1  0 15:54 ?        00:00:03 /usr/local/apache24/bin/httpd  
daemon    2911    2910  0 15:54 ?        00:00:13 /usr/local/apache24/bin/httpd  
daemon    2912    2910  0 15:54 ?        00:00:13 /usr/local/apache24/bin/httpd  
daemon    2914    2910  0 15:54 ?        00:00:13 /usr/local/apache24/bin/httpd  
daemon   24108    2910  0 18:11 ?        00:00:01 /usr/local/apache24/bin/httpd  
root     24187   3167  0 18:25 pts/1    00:00:00 grep httpd  
[root@localhost ~]#
```

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 2.4.6(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`)



```
root@localhost:~  
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)  
[root@localhost ~]# /usr/local/apache24/bin/apachectl -v  
Server version: Apache/2.4.6 (Unix)  
Server built:   Sep 20 2013 17:34:31  
[root@localhost ~]#
```

3. 確認 Apache 設定檔路徑，可執行下列指令：

```
find / -name httpd.conf
```

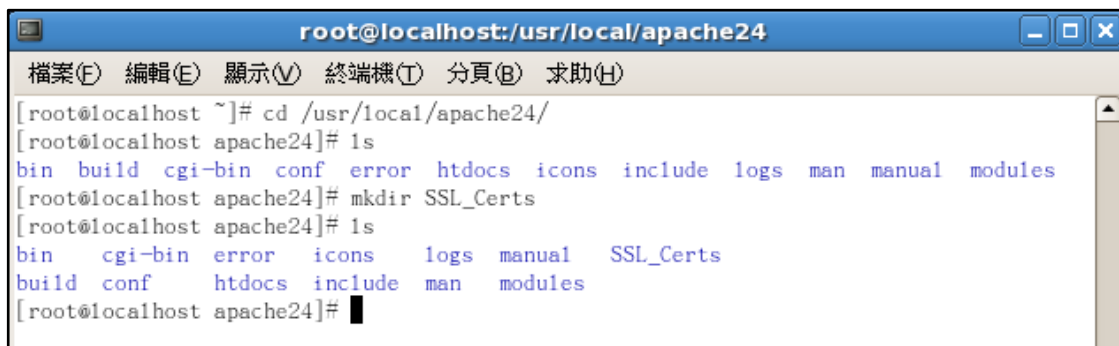


```
root@localhost:~  
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)  
[root@localhost ~]# find / -name httpd.conf  
/root/httpd-2.4.6/docs/conf/httpd.conf  
/usr/local/apache24/conf/original/httpd.conf  
/usr/local/apache24/conf/httpd.conf  
[root@localhost ~]#
```

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)



```
root@localhost:/usr/local/apache24  
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)  
[root@localhost ~]# cd /usr/local/apache24/  
[root@localhost apache24]# ls  
bin build cgi-bin conf error htdocs icons include logs man manual modules  
[root@localhost apache24]# mkdir SSL_Certs  
[root@localhost apache24]# ls  
bin cgi-bin error icons logs manual SSL_Certs  
build conf htdocs include man modules  
[root@localhost apache24]#
```

4.1.2 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!**。

```

root@localhost:~
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)

[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 openssl-0.9.8e-26.el5_9.1.i686 already installed and latest version
Resolving Dependencies
--> Running transaction check
--> Package mod_ssl.i386 1:2.2.3-82.el5.centos set to be updated
--> Processing Dependency: libdistcache.so.1 for package: mod_ssl
--> Processing Dependency: libnsl.so.1 for package: mod_ssl
--> Running transaction check
--> Package distcache.i386 0:1.4.5-14.1 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                Arch          Version                Repository            Size
=====
Installing:
mod_ssl                 i386          1:2.2.3-82.el5.centos  updates              97 k
Installing for dependencies:
distcache               i386          1.4.5-14.1            base                  119 k
=====

Transaction Summary
=====

```

```

root@localhost:~
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)

distcache             i386          1.4.5-14.1            base                  119 k
=====
Transaction Summary
=====
Install      2 Package(s)
Upgrade      0 Package(s)

Total download size: 215 k
Is this ok [y/N]: y
Downloading Packages:
(1/2): mod_ssl-2.2.3-82.el5.centos.i386.rpm | 97 kB    00:00
(2/2): distcache-1.4.5-14.1.i386.rpm       | 119 kB    00:00
-----
Total                                           417 kB/s | 215 kB    00:00
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing      : distcache                                1/2
  Installing      : mod_ssl                                  2/2

Installed:
mod_ssl.i386 1:2.2.3-82.el5.centos

Dependency Installed:
distcache.i386 0:1.4.5-14.1

Complete!

```

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

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
```

4.2 產製「金鑰」

4.2.1 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)



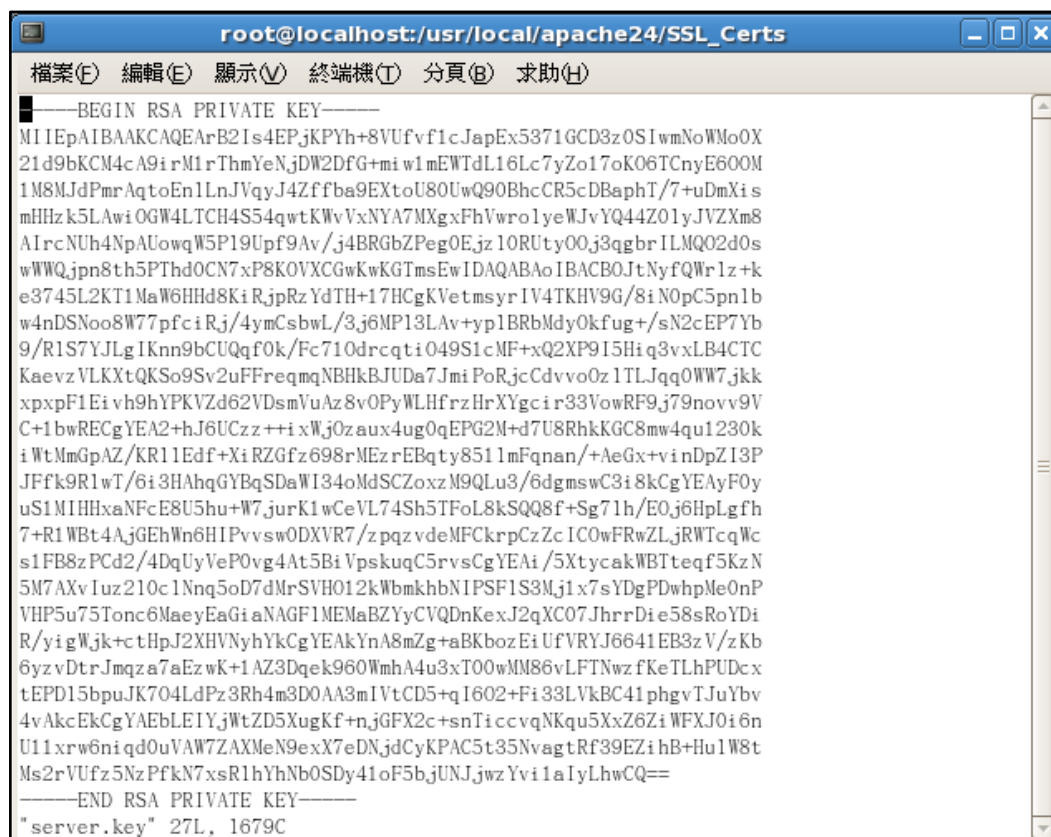
```

root@localhost:~
檔案(E) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)

[root@localhost ~]# openssl genrsa -out /usr/local/apache24/SSL_Certs/server.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
[root@localhost ~]#

```

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



```

root@localhost:/usr/local/apache24/SSL_Certs
檔案(E) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEArB2Is4EPjKPYh+8VUvf1cJapEx5371GCD3z0SIwmNoWMOX
21d9bKCM4cA9irM1rThmYeNjDW2DfG+miw1mEWtdL16Lc7yZo17oK06TCnyE600M
1M8MjdPmrAqtoEnlLnJVqyJ4Zffba9EXtoU80UwQ90BhcCR5cDBaphT/7+uDmXis
mHHzk5LAWiOGW4LTH4S54qwtKWvVxNYA7MXgxFhVwrolyeWJvYQ44Z01yJVZXm8
A1rcNUh4NpAUowqW5P19Upf9Av/j4BRGbZPegOEjz10Ruty00j3qgbrILMQ02d0s
wWWQjpn8th5PThdOCN7xP8KOVXCgWkKGTmsEwIDAQABAoIBACB0JtNyfQWr1z+k
e3745L2KT1MaW6HHd8KiRjpRzYdTH+17HCgKVetmsyrIV4TKHV9G/8iN0pC5pn1b
w4nDSNoo8W77pfc1Rj/4ymCsbwL/3j6MP13LAv+yp1BRbMdyOkfug+/sN2cEP7Yb
9/R1S7YJLgIKnn9bCUQqf0k/Fc710drcti049S1cNF+xQ2XP9I5Hiq3vxLB4CTC
KaevzVLKXtQKSo9Sv2uFFreqmqNBHkBJUDa7JmiPoRjcCdvvoOz1TLJqq0WW7jkk
xpxpF1EiVh9hYPKVZd62VDsmVuAz8vOPyWLHfrzHrXYgciR33VowRF9j79novv9V
C+1bwRECgYEA2+hJ6UCzz++ixWjOzaux4ug0qEPG2M+d7U8RhkKGC8mw4qu1230k
iWtMmGpAZ/KR11Edf+XiRZGfz698rMEzrEBqty851lmFqnan/+AeGx+vinDpZ13P
JFfk9R1wT/6i3HAhQGYBqSDaWI34oMdSCZoxzM9QLu3/6dgmswC3i8kCgYEAyF0y
uS1MIHhXaNFcE8U5hu+W7jurK1wCeVL74Sh5TFoL8kSQQ8f+Sg71h/E0j6HPLgfh
7+R1WBt4AjGEhWn6HIPvvsWODXVR7/zpqzvdemFCkrpCzZcIC0wFRwZLjRWTcqWc
s1FB8zPCd2/4DqUyVeP0vg4At5BiVpskuqC5rvsCgYEAi/5XtycakWBTteqf5KzN
5M7AXvIuz210c1Nnq5oD7dMrSVH012kWbmkhbnIPSF1S3Mj1x7sYDgPDwhpMeOnP
VHP5u75Tonc6MaeyEaGianAGF1MEMaBZYyCVQDnKexJ2qXC07JhrrDie58sRoYDi
R/yigWjk+ctHpJ2XHVnyhYkCgYEAkYnA8mZg+aBKbozEiUfVRYJ6641EB3zV/zKb
6yzvDtrJmqa7aEzwK+1AZ3Dqek960WmhA4u3xT00wMM86vLFTNwzfKeTLhPUDcx
tEPD15bpuJK704LdPz3Rh4m3D0AA3mIVtCD5+q1602+Fi33LVkBC41phgvTJuYbv
4vAkCgYEAebLE1YjWtZD5XugKf+njGFX2c+snTiccvqNKqu5XxZ6ZiWFXJOi6n
U11xrw6n1qd0uVAW7ZAXMeN9exX7eDNjdCyKPAC5t35NvagtrF39EzihB+HulW8t
Ms2rVufz5NzPfkN7xsR1hYhNb0SDy41oF5bjUNJjwzYvi1aIyLhwCQ==
-----END RSA PRIVATE KEY-----
"server.key" 27L, 1679C

```

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.3 產生「憑證請求檔(CSR)」

4.3.1 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 4.2 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



```
root@localhost:/usr/local/apache24/SSL_Certs
-----BEGIN CERTIFICATE REQUEST-----
MIICCrjCCAZYCAQAwTELMAkGA1UEBhMCVFcxZDANBgNVBAgTB1RBSVdB
TjEPMAGG
A1UEBxNGVEFJUEVJNQwCwYDVQQKEwRUUVONBMQ8wDQYDVQQLZWZTWV
NURUOxGDAW
BgNVBAMTD3d3dy50d2NhLmNvbS50dzCCAS1wDQYJKoZIhvcNAQEBBQ
ADggEPADCC
AQoCggEBAKwdiLOBD4yJ2IfvFVH735XCWqRMed+5Rgg989EiMJjaFj
KNF9pXfWyg
jOHAPYqzJa04ZmHjYw1tg3xvposJZhFk3S5ei308maJe6Cjukwp8h0
jjjJTPDCXT
5qwKraBJ9S5yVasieGX322vRF7aFPNFMEpdAYXakeXAwWqYU/+rg51
4rJhx850S
wMIjh1uCoWh+EueKsLS1r1cTWA0zF4MRYVcK6Ncn1ib2E00GdNciV
WV5vACK3DVI
eDaQFKMK1uT9fVKX/QL/4+AURm2T3oNB189dEVLcjjo96oG6yCzED
tndLMF1k16Z
/LYeT04XdAje8T/Cj1VwhsCsChk5rBMCAwEAaAAMAOGCSqGSIb3DQ
EBBQUAA4IB
AQAC9MzSL83v2Gjm/RWiNUAWKGOEzcfYeis3tr1PBdaJzrCBxz10
08Kvni0j53og
o4GS0yILBFVkwkbPowi1EqCG7qdSDAmpmhaFQugOe6e9Ijk2YwvAW
jdJv8HF/RB
gu/kf/zhBSxVqJTSpgF00g/C1v1RNpXwINTy40hN0kN+Z00QG3AbFi
u2kTuRDi7B
3d2Vyl2AvWqVF3eDjbC6Nvn1rYv8xXPV2K29ZWSNXwuE9VQdJgvZ/
meFlyJfpVW+
1SumNNdPtKby0AQJzS8+1yfmsH21LHtrEnE2ZXHjiBnSJW8UIvV7S
prgVdAP6Qi3
yPu4aRb0hfjFkoNwJrBBJPV3
-----END CERTIFICATE REQUEST-----
```

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.4 將製作好的憑證請求檔(CSR)上傳

4.4.1 連接 TWCA 網站(1)

連接至本公司首頁 <http://www.twca.com.tw>

點選 **憑證服務**。



4.4.2 連接 TWCA 網站(1)

點選 **SSL 憑證**。

※如申請 EV SSL 伺服器憑證，請點選 **TWCA EV SSL 類**。



4.4.3 連接 TWCA 網站(2)

點選 **申請憑證**。



4.4.4 連接 TWCA 網站(3)

下拉至 **上傳 CSR (WEB)**

3

■ 上傳 CSR (WEB)

上傳憑證請求檔(CSR)

請依據適用之『憑證操作手冊』產生憑證請求檔(CSR)，手冊取得請來電02-2370-8886#9 洽詢。

產生憑證請求檔(CSR)後

請將CSR以純文字的方式儲存成為檔案（建議檔案名稱為Certreq.txt）後，請以純ASCII的文字編輯器（如記事本）來開啟此檔。注意不要使用文書處理軟體（如WORD）開啟，因為它們會額外插入文字的格式指令及控制字元。

- 傳送憑證申請檔（CSR）

以下為CSR檔案的內容範例：

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBJDCBzwIBADBqMQswCQYDVQQGEwJUVzEPMA0GA1U
ECBMGVFEJV0FOMQ8wDQYDVQQHEwZUQUlXQU4xDjAMB
gNVBfwefEg,uhYUGJ84DWgbyGYGVVQLEwJJVDEcMBoGA1U
EAMTbGFIMzAwLnRhaWNhLmNvbS50dzBcMA0GCsQGSib3D
QEBAQUAA0sAMEgCQQDYdmR9MVXzUClzOE6wW0ggZRpZ
giJfHCa2diLHQq69SMUmLXNdnVQnl4pkgPo1qNvKv0TKR7tac
LnfmWxuUHUHUuUlihihiluHLUIHUILHhkiG9w0BAQQFAANBAII
5vczs+LzMP1c1ybwTE4784HIzUbibZhXNg6L90H09CIHpDXD
duwd01q42V5xCmasPCImklri1TX4BYr5qzY=
-----END NEW CERTIFICATE REQUEST-----
```

請將CSR檔案中的內容複製到下方的空欄中，注意複製的範圍應包括「-----BEGIN NEW CERTIFICATE REQUEST-----」到「-----END NEW CERTIFICATE REQUEST-----」的宣告文字。

4.4.5 貼上憑證請求檔

將瀏覽器視窗畫面往下拉，開啟在 5.1 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**。

請將 CSR 檔案中的內容複製到下方的空欄中，注意複製的範圍應包括「-----BEGIN NEW CERTIFICATE REQUEST-----」到「-----END NEW CERTIFICATE REQUEST-----」的宣告文字。

```
-----BEGIN NEW CERTIFICATE REQUEST-----  
MIIBJDCBzwIBADBqMQswCOYDVQQGEwJUVzEPMA0GA1U  
ECBMGVFEFJV0FOMQ8wDOYDVQOHEwZUOUIXOU4xDiAMB  
gNVBfweFg. uhYUGJ84DWgbyGYGYVOOLEwJJVDEcMBoGA1U  
EAxMTbGFIMzAwLnRhaWNhLmNvbS50dzBcMA0GCSqGSIb3D  
QEBAQUAA0sAMEgCQQDYdmR9MVXzUCIzOE6wW0ggZRpZ  
giJfHCa2diLHQq69SMUmLXNdnVQnl4pkgPo1qNvKv0TKR7tac  
LnfmWxuUHUHUUulihihiluHLUIHUILHhkiG9w0BAQQFAANBAIIG  
5vczs+LzMP1c1ybwTE4784HIzUbibZhXNg6L90H09CIHoDXD  
duwd01q42V5xCmasPCImklri1TX4BYr5qzY=  
-----END NEW CERTIFICATE REQUEST-----
```

請按一下「繼續」按鈕以便送出 CSR，並繼續註冊程序。

繼續

重設

4.4.6 再次檢視上傳之憑證請求檔案內容



本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.4.7 填寫聯絡人基本資料

使用視窗右方式下拉移動方式，將申請之伺服器與聯絡資料填入適當欄位

(聯絡資料欄位請務必與申請同意書所填內容相符)。

請輸入伺服器資訊

伺服器軟體廠商： 請從右邊的下拉式選單中選擇您伺服器軟體的廠商。如果不在清單中，請選擇其他。	Microsoft IIS
通行密碼：(至少六碼) 請在右邊的欄位中輸入一個您容易記憶，但不易為人所臆測的文字或片語。當您申請、更新或註銷此SSL伺服器憑證時都需使用到這個通行密碼。另外，當您對本公司提出技術支援服務時，本公司亦會要求您提供此通行密碼。若有必要，請將此密碼記錄下來，並儲存在安全的地方。	輸入密碼： 再輸入一次密碼以確認：

請輸入技術聯絡人資訊

請輸入本公司寄送SSL伺服器憑證給您的技術聯絡人資訊於下表。舉例來說，此人可以是您的網站管理者，或是您網路撥接商的技術支援人員。

請注意此人必須擁有存取您網頁伺服器的權利。本公司在發放SSL伺服器憑證以前，會先以電話與此技術聯絡人取得聯繫。

當網頁伺服器的安全出現顧慮時，此技術聯絡人有通知本公司的義務。

另若有憑證更新的訊息，本公司也會寄送給技術聯絡人及 貴公司的業務聯絡人。

姓名	
職稱	
公司	
統一編號	
通訊地址	台北市 郵遞區號：
聯絡電話	
傳真號碼	
電子郵件地址	

請輸入業務聯絡人資訊

請輸入 貴公司負責SSL伺服器憑證業務聯絡人資訊於下表，並填寫本公司所要求的資訊。

舉例來說，此人可以是 貴公司的決策者或是高階的經理人。

請注意業務聯絡人必須為 貴公司組織內之一份子。本公司在發放SSL伺服器憑證以前，會先以電話與此業務聯絡人取得聯繫。

業務聯絡人與技術聯絡人不應為同一人，您應該分別指定。

另外，本公司若有更新的資料也會同時寄給上述這兩個人。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

姓名	
職稱	
公司	
統一編號	
通訊地址	台北市 ▼ 郵遞區號：
聯絡電話	
傳真號碼	
電子郵件地址	

請輸入帳務聯絡人資訊

請輸入 貴公司的帳務處理聯絡人員資訊。

舉例來說，該人可以是 貴公司會計或是財務主管。

當帳單處理資料有異動時，此人有通知本公司之義務。

☐ 與技術聯絡人相同 ☐ 與業務聯絡人相同 ☒ 兩者皆否	
姓名	
職稱	
公司	
通訊地址	台北市 ▼ 郵遞區號：
聯絡電話	
傳真號碼	
電子郵件地址	

繼續

重設

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.4.8 送出後等待 CA 系統簽發憑證

CSR 上傳完成後，待完成資料審查作業且憑證簽發後會以 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。

系統的回應訊息

作業成功

CA系統已接受您的憑證請求，當CA系統簽發您的憑證後，會寄送電子郵件(E-Mail)通知您下載憑證事宜。

CA作業時間約需二個工作天。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.5 下載已核發憑證

1 相關檔案說明

若上傳之 CSR 及相關聯絡資料經過審驗通過，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，可得到三個或四個憑證鏈檔。

※如解壓縮後得到三個憑證鏈檔，內容及憑證用途如下圖所示：



※如解壓縮後得到四個憑證鏈檔，內容及憑證用途如下圖所示：



2 檔案下載說明

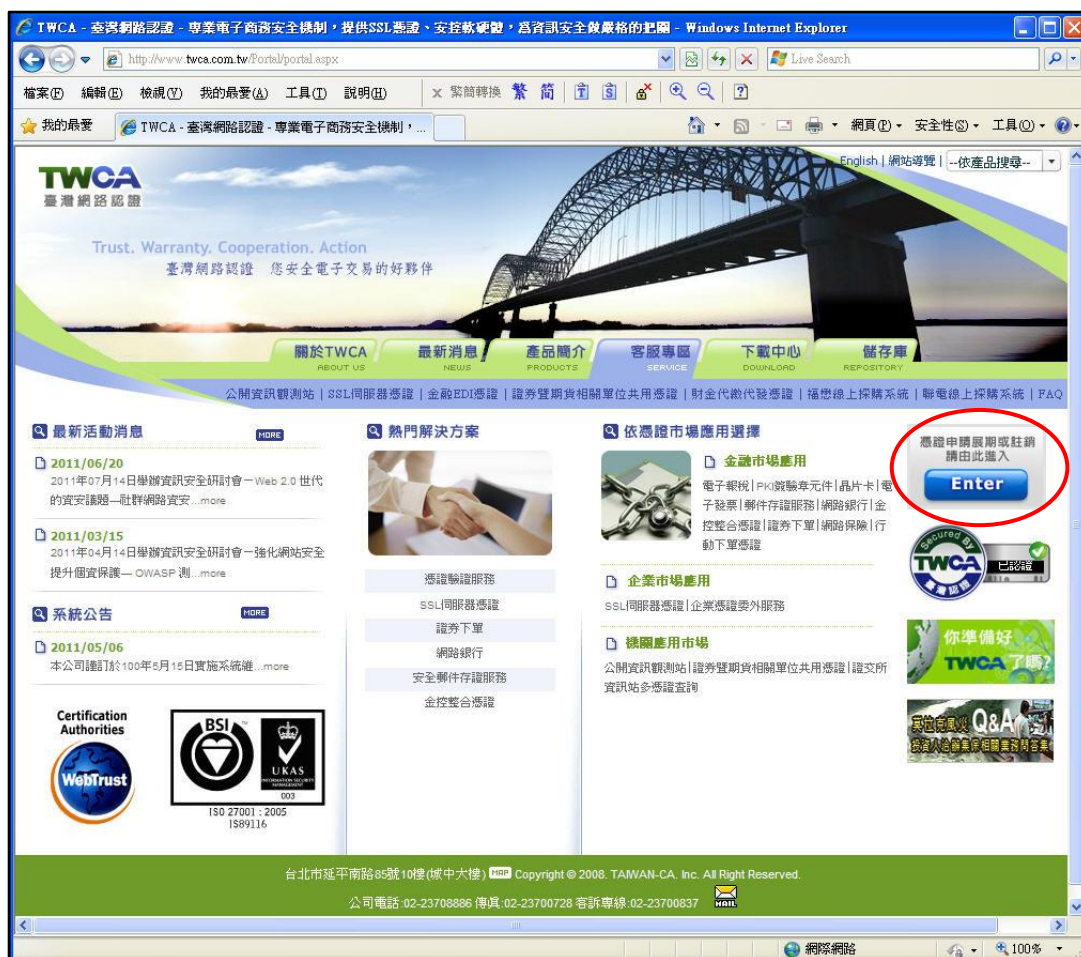
本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

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。

4.5.1 連接 TWCA 網站(1)

連接至本公司首頁 <http://www.twca.com.tw>，點選右上方憑證申請展期或註銷請由此進入。

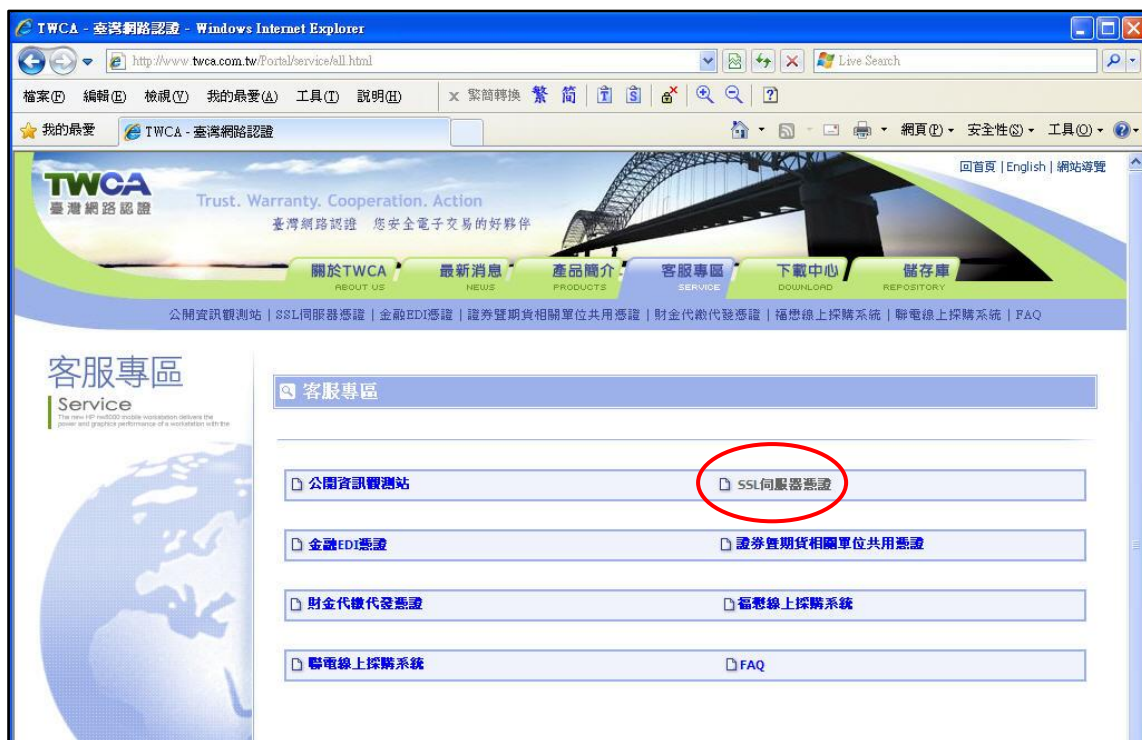


本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.5.2 連接 TWCA 網站(2)

點選 **SSL 伺服器憑證**。



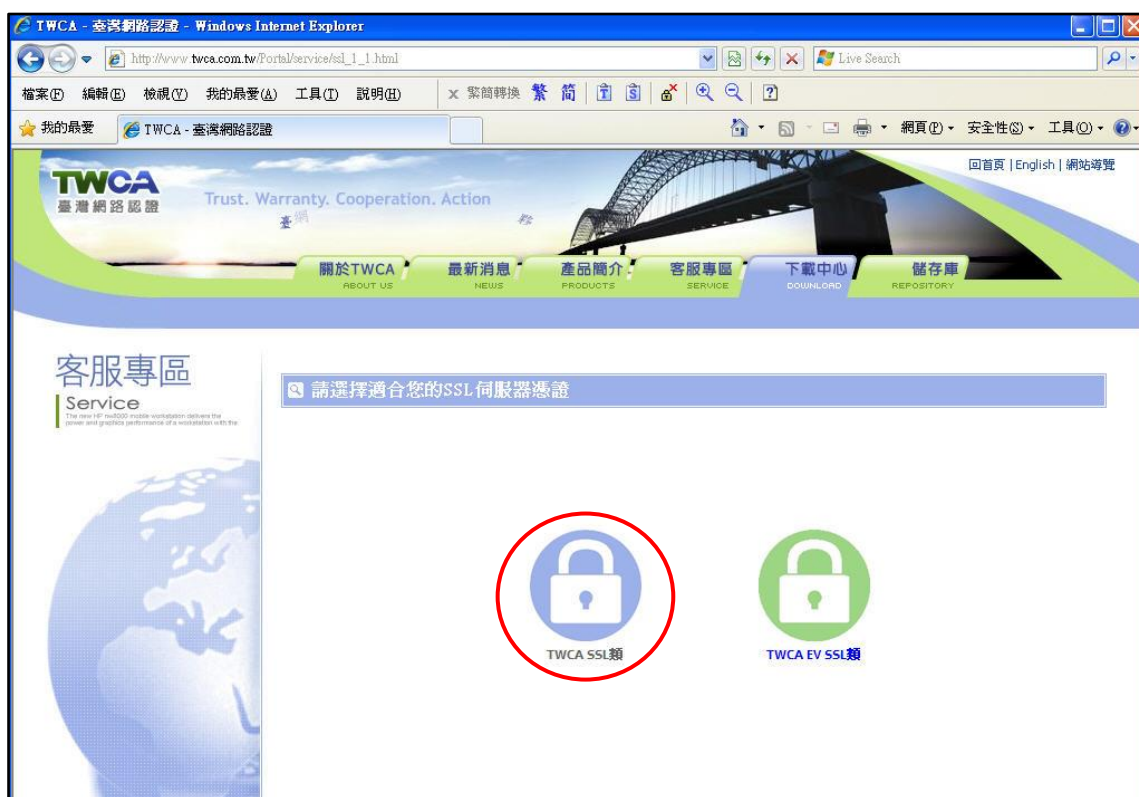
本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.5.3 連接 TWCA 網站(3)

點選 **TWCA SSL 類**。

※如申請 **EV SSL 伺服器憑證**，請點選 **TWCA EV SSL 類**。



本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.5.4 連接 TWCA 網站(4)

點選憑證搜尋。

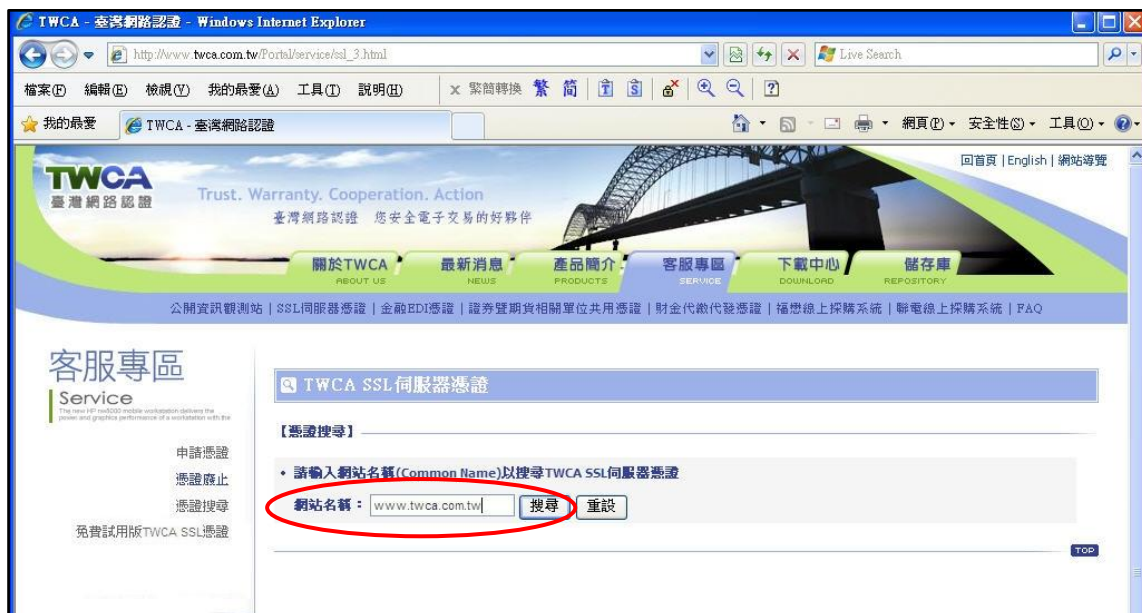


4.5.5 輸入申請之網站名稱

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。



本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.5.6 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 **儲存**，儲存憑證鏈壓縮檔 cert.zip。



TWCA 臺灣網路認證 Trust. Warranty. Cooperation. Action
臺灣網路認證 您安全電子交易的好夥伴

關於TWCA ABOUT US 最新消息 NEWS 產品簡介 PRODUCTS 客服專區 SERVICE 下載中心 DOWNLOAD 儲存庫 REPOSITORY

憑證服務 | 憑證應用 | 安全郵件存證服務 | SSL伺服器憑證 | 憑證驗證服務 | PKI驗章元件 | 設備憑證

查詢用戶憑證

以www.twca.com.tw查詢用戶憑證，共3筆記錄

憑證序號	一般名稱	憑證生效日	憑證到期日	憑證狀態	詳細資訊	下載	註銷	重新申請
1707611566 (65c815ae)	www.twca.com.tw	2010-11-01 14:17:46	2013-11-01 23:59:59	有效	檢視	憑證 憑證鏈	註銷	
1707616998 (65c82ae6)	www.twca.com.tw	2011-05-03 18:22:47	2014-05-03 23:59:59	有效	檢視	憑證 憑證鏈	註銷	
1707621282 (65c83ba2)	www.twca.com.tw	2011-10-03 16:10:47	2014-10-31 23:59:59	有效	檢視	憑證 憑證鏈	註銷	重新申請



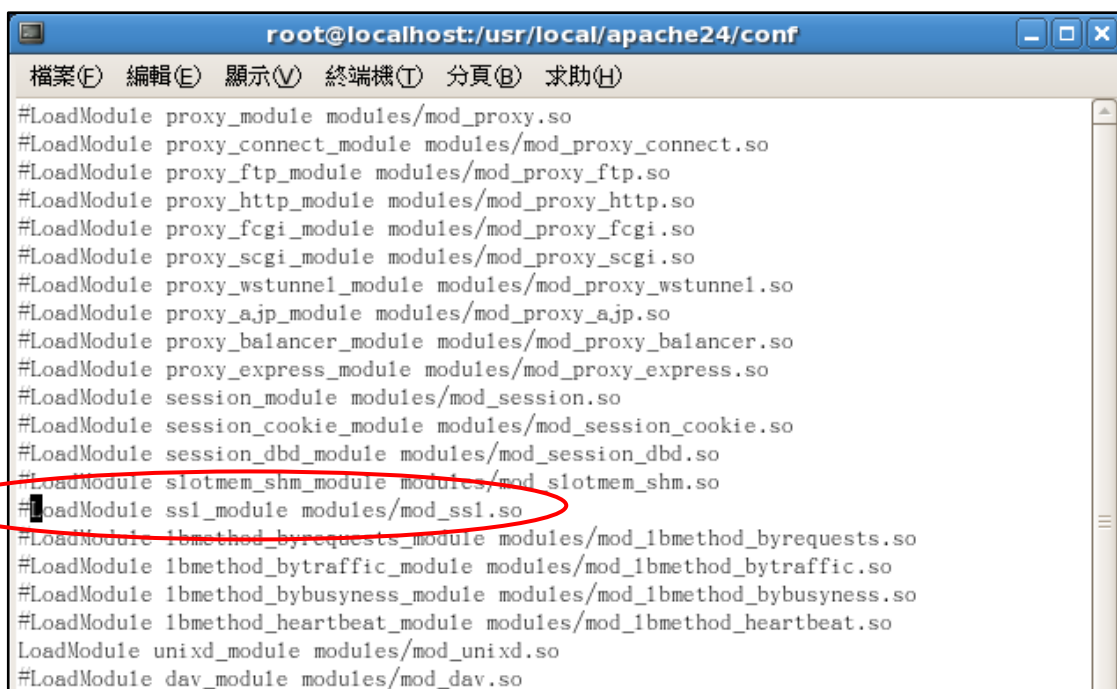
4.6 設定 SSL 模式

※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！

4.6.1 編輯 `/usr/local/apache24/conf` 目錄下的 `httpd.conf` 檔案

4.6.1.1 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。



```
root@localhost:/usr/local/apache24/conf
檔案(E) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
#LoadModule proxy_module modules/mod_proxy.so
#LoadModule proxy_connect_module modules/mod_proxy_connect.so
#LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
#LoadModule proxy_http_module modules/mod_proxy_http.so
#LoadModule proxy_fcgi_module modules/mod_proxy_fcgi.so
#LoadModule proxy_scgi_module modules/mod_proxy_scgi.so
#LoadModule proxy_wstunnel_module modules/mod_proxy_wstunnel.so
#LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
#LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
#LoadModule proxy_express_module modules/mod_proxy_express.so
#LoadModule session_module modules/mod_session.so
#LoadModule session_cookie_module modules/mod_session_cookie.so
#LoadModule session_dbd_module modules/mod_session_dbd.so
#LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
#LoadModule ssl_module modules/mod_ssl.so
#LoadModule lbmethod_byrequests_module modules/mod_lbmethod_byrequests.so
#LoadModule lbmethod_bytraffic_module modules/mod_lbmethod_bytraffic.so
#LoadModule lbmethod_bybusyness_module modules/mod_lbmethod_bybusyness.so
#LoadModule lbmethod_heartbeat_module modules/mod_lbmethod_heartbeat.so
LoadModule unixd_module modules/mod_unixd.so
#LoadModule dav_module modules/mod_dav.so
```



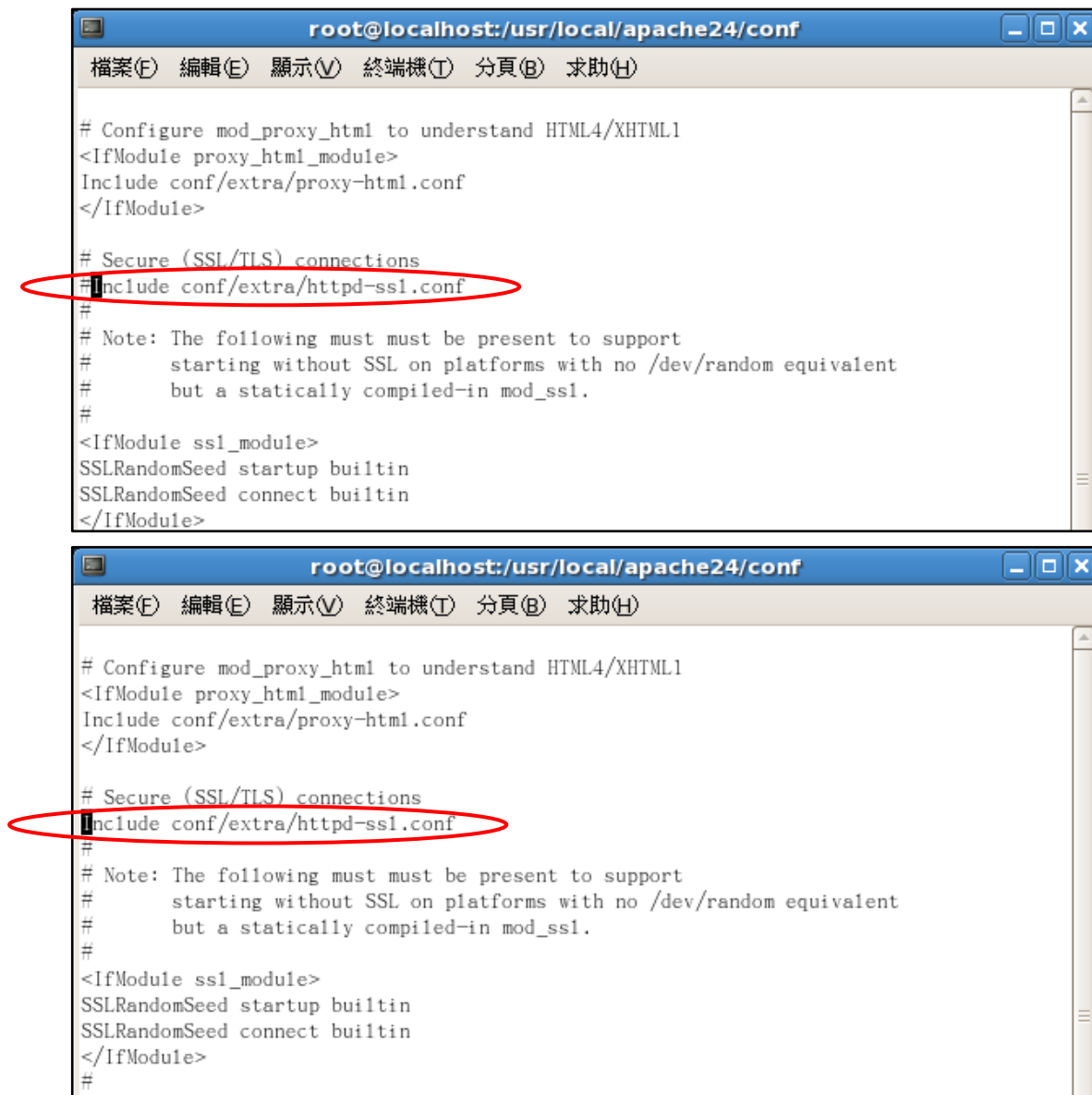
```
root@localhost:/usr/local/apache24/conf
檔案(E) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
#LoadModule proxy_module modules/mod_proxy.so
#LoadModule proxy_connect_module modules/mod_proxy_connect.so
#LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
#LoadModule proxy_http_module modules/mod_proxy_http.so
#LoadModule proxy_fcgi_module modules/mod_proxy_fcgi.so
#LoadModule proxy_scgi_module modules/mod_proxy_scgi.so
#LoadModule proxy_wstunnel_module modules/mod_proxy_wstunnel.so
#LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
#LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
#LoadModule proxy_express_module modules/mod_proxy_express.so
#LoadModule session_module modules/mod_session.so
#LoadModule session_cookie_module modules/mod_session_cookie.so
#LoadModule session_dbd_module modules/mod_session_dbd.so
#LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
#LoadModule ssl_module modules/mod_ssl.so
#LoadModule lbmethod_byrequests_module modules/mod_lbmethod_byrequests.so
#LoadModule lbmethod_bytraffic_module modules/mod_lbmethod_bytraffic.so
#LoadModule lbmethod_bybusyness_module modules/mod_lbmethod_bybusyness.so
#LoadModule lbmethod_heartbeat_module modules/mod_lbmethod_heartbeat.so
LoadModule unixd_module modules/mod_unixd.so
#LoadModule dav_module modules/mod_dav.so
LoadModule status_module modules/mod_status.so
```

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.6.1.2 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。

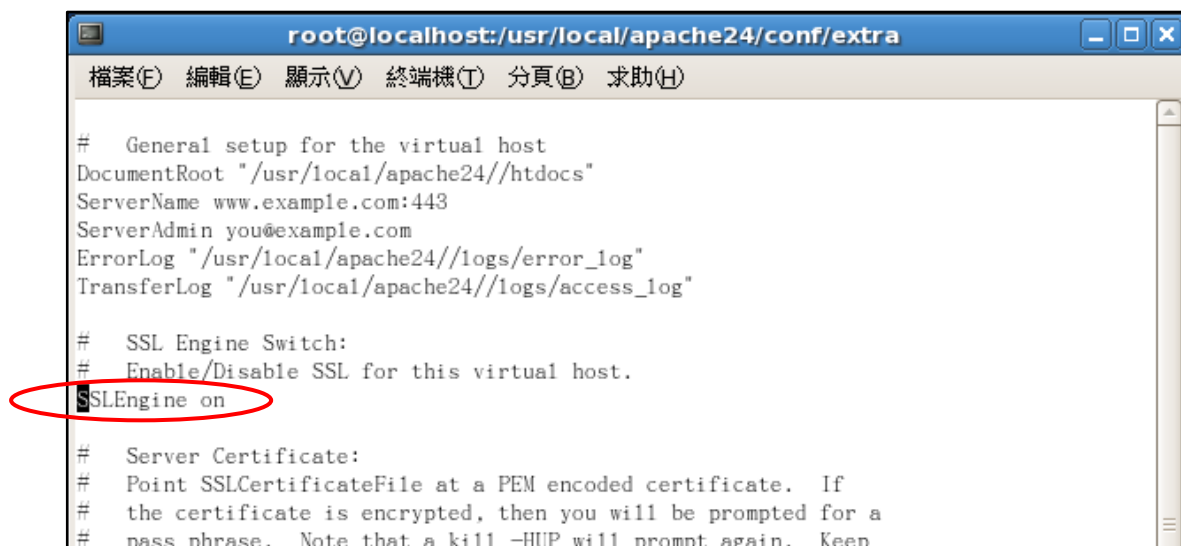


確認完 httpd.conf 內上述兩項設定後儲存檔案。

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

4.6.2.1 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`。



```
root@localhost:/usr/local/apache24/conf/extra
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)

# General setup for the virtual host
DocumentRoot "/usr/local/apache24/htdocs"
ServerName www.example.com:443
ServerAdmin you@example.com
ErrorLog "/usr/local/apache24/logs/error_log"
TransferLog "/usr/local/apache24/logs/access_log"

# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on

# Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate. If
# the certificate is encrypted, then you will be prompted for a
# pass phrase. Note that a kill -HUP will prompt again. Keep
```

4.6.2.2 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。



```
root@localhost:/usr/local/apache24/conf/extra
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)

#
# When we also provide SSL we have to listen to the
# standard HTTP port (see above) and to the HTTPS port
#
# Note: Configurations that use IPv6 but not IPv4-mapped addresses need two
# Listen directives: "Listen [::]:443" and "Listen 0.0.0.0:443"
#
Listen 443

##
## SSL Global Context
##
## All SSL configuration in this context applies both to
```

4.7 安裝憑證

4.7.1 Apache 在安裝 SSL 憑證時會使用到三種檔案：

- 於 4.2 章節產製的 SSL 伺服器金鑰「server.key」
- 於 4.5 章節取得的伺服器憑證檔「server.cer」
- 於 4.5 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)。

※ 如 4.5 章節解壓縮後得到三個憑證鏈檔，請直接至 4.7.3 章節安裝 SSL 憑證。

※ 如解壓縮後得到四個憑證鏈檔，請先依照下列步驟，將 uca_1.cer 與 uca_2.cer 憑證內容合併，再提供 4.7.3.3 章節中繼憑證安裝使用。

先將 uca_1.cer 與 uca_2.cer 存放同一個目錄內(實際目錄可自行決定)，開啟命令提示字元，於前述兩個檔案存放目錄下，輸入下列指令

```
cat uca_2.cer uca_1.cer > uca.cer
```

完成上列指令後，該目錄下會新增一檔名為 uca.cer 的檔案。



```
root@localhost:usr/local/apache24/SSL_Certs
檔案(E) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
[root@localhost SSL_Certs]# ls
root.cer server.cer server.csr server.key uca_1.cer uca_2.cer
[root@localhost SSL_Certs]# cat uca_2.cer uca_1.cer > uca.cer
[root@localhost SSL_Certs]# ls
root.cer server.cer server.csr server.key uca_1.cer uca_2.cer uca.cer
[root@localhost SSL_Certs]#
```

使用文字編輯器打開 uca.cer 檔

可看到如下內容

-----BEGIN CERTIFICATE-----

\$SOME TEXT

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

\$SOME TEXT

-----END CERTIFICATE-----



The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

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

4.7.3.1 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 4.7.1 章節檔案存放路徑設定，路徑前後請用「`"`」包起來。



```
root@localhost:/usr/local/apache24/conf/extra
檔案(E) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
# Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate. If
# the certificate is encrypted, then you will be prompted for a
# pass phrase. Note that a kill -HUP will prompt again. Keep
# in mind that if you have both an RSA and a DSA certificate you
# can configure both in parallel (to also allow the use of DSA
# ciphers, etc.)
# Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)
# require an ECC certificate which can also be configured in
# parallel.
SSLCertificateFile "/usr/local/apache24/SSL_Certs/server.cert"
#SSLCertificateFile "/usr/local/apache24/conf/server-dsa.crt"
#SSLCertificateFile "/usr/local/apache24/conf/server-ecc.crt"
```

4.7.3.2 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 4.7.1 章節檔案存放路徑設定，路徑前後請用「`"`」包起來。



```
root@localhost:/usr/local/apache24/conf/extra
檔案(E) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
# ECC keys, when in use, can also be configured in parallel
SSLCertificateKeyFile "/usr/local/apache24/SSL_Certs/server.key"
#SSLCertificateKeyFile "/usr/local/apache24/conf/server-dsa.key"
#SSLCertificateKeyFile "/usr/local/apache24/conf/server-ecc.key"

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
```


4.7.3.3 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 4.7.1 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。

4.7.4 重新啟動 Apache 服務

重新啟動完成即可進入 4.8 節，驗證 SSL 功能。

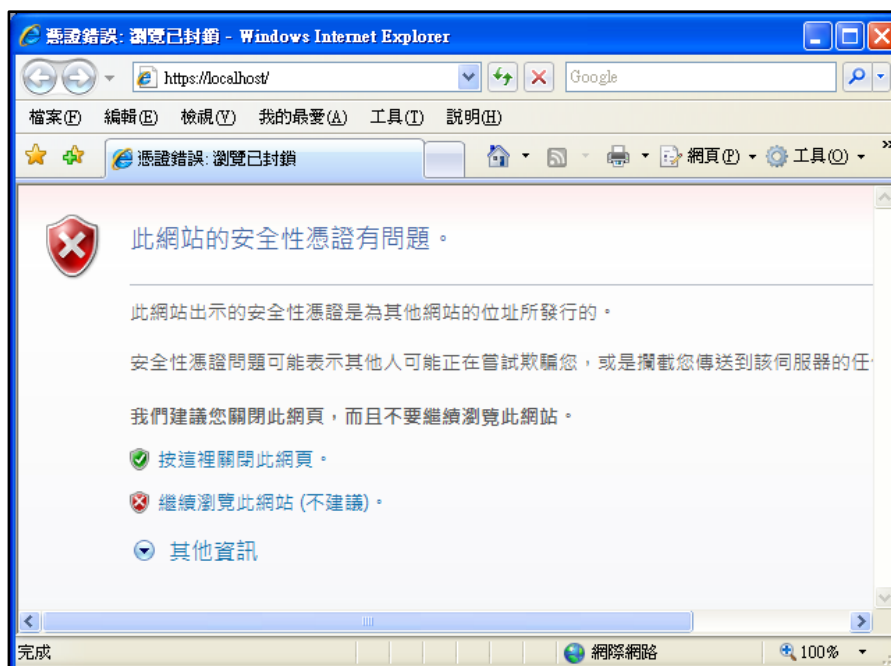


A terminal window titled 'root@localhost:~' with a menu bar containing '檔案(F)', '編輯(E)', '顯示(V)', '終端機(T)', '分頁(B)', and '求助(H)'. The terminal shows the command `/usr/local/apache24/bin/apachectl restart` being executed at the prompt `[root@localhost ~]#`. The prompt returns to `[root@localhost ~]#` with a cursor.

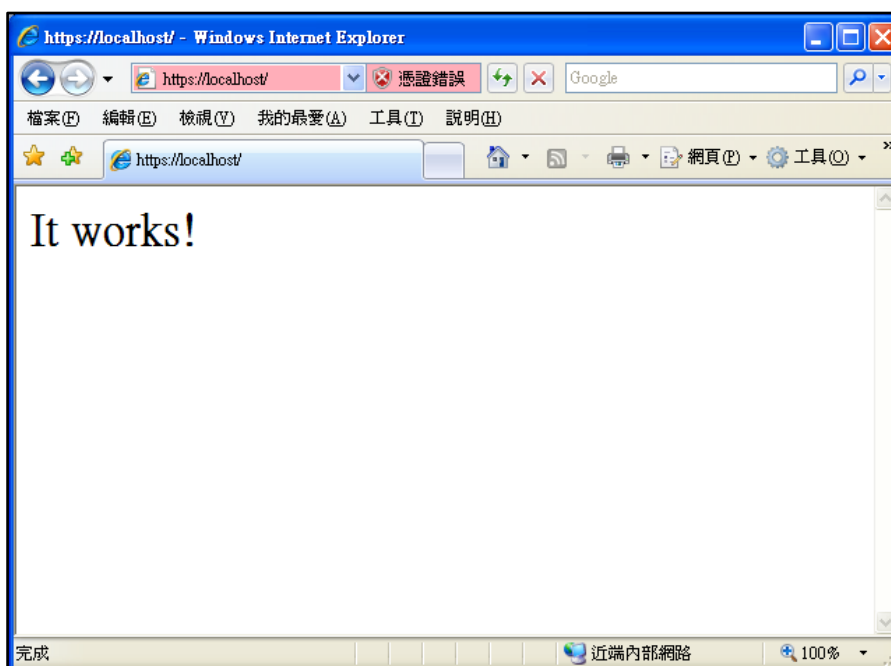
4.8 驗證 SSL 功能

4.8.1 本機驗證

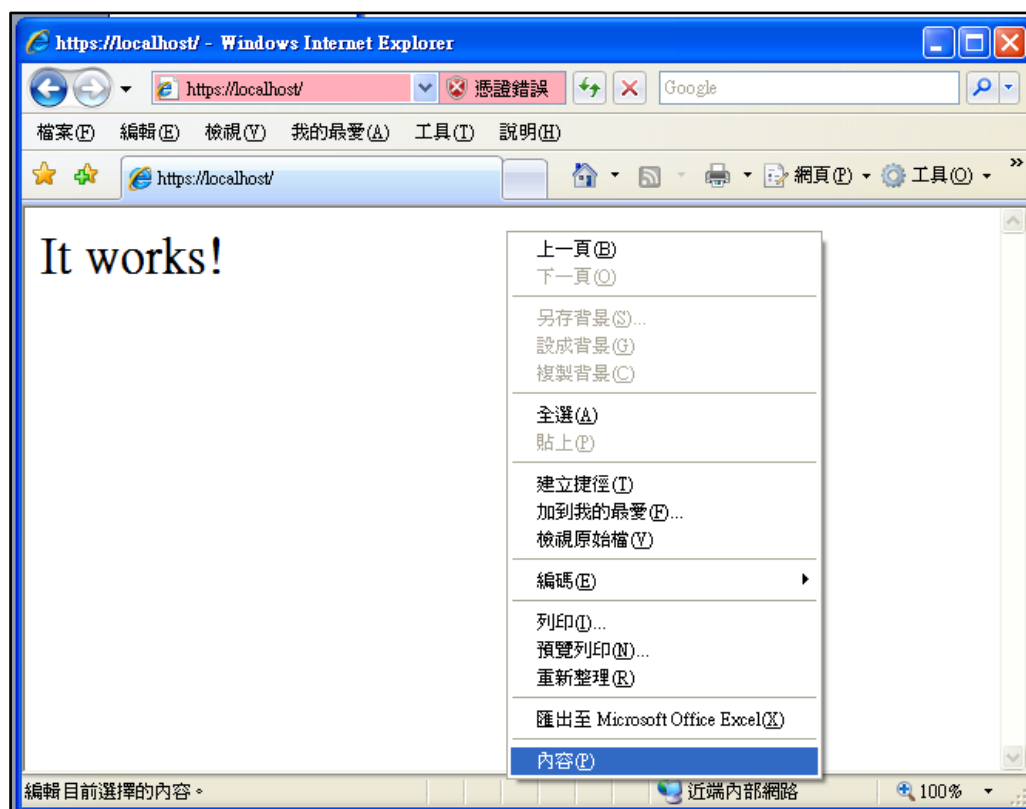
Apache 重新啟動完成後開啟瀏覽器直接連接至本機 <https://localhost>，此時出現警告訊息是正常的，因為憑證記載內容與網址不符（非 localhost），請點選「繼續瀏覽此網站(不建議)」即可。



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」，

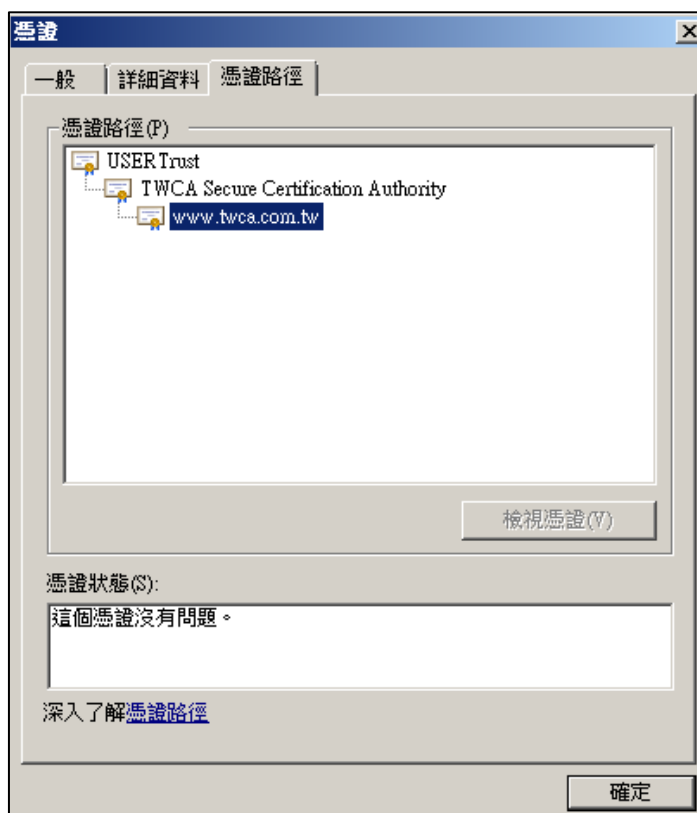


此時會出現網頁資訊，確認網頁是否已加密，點選「憑證」可檢視憑證資

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。)



本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.8.2 外部驗證

驗證程序和 4.8.1 節相同，只是連線位址改為實際網址，

如 <https://www.twca.com.tw>



4.8.3 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 4.6.6.2 節設定 Listen Port 非 443，則連線時須指定連線 Port，如 <https://www.twca.com.tw:8443>

4.9 異常排除

如果完成 4.6 及 4.7 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。

4.10 備份／還原憑證

請將 4.7.1 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 4.7.3 至 4.7.4 章節的步驟設定，即可還原憑證。

4.11 更新 SSL 憑證

4.11.1 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

<http://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。

4.11.2 更新步驟

4.11.2.1 備份憑證檔

在進行更新前請記得參考 4.7.1 章節步驟，備份原有的 SSL 伺服器憑證及伺服器金鑰。

4.11.2.2 更新憑證

請參照 4.2 至 4.7 章節申請安裝憑證，並利用 4.8 章節驗證 SSL 憑證是否更新成功，即可完成 SSL 憑證更新。

5.附件

無。