網路中文
www.net-chinese.com.tw

CSR 生成與憑證安裝指南
適用於 Synology DSM

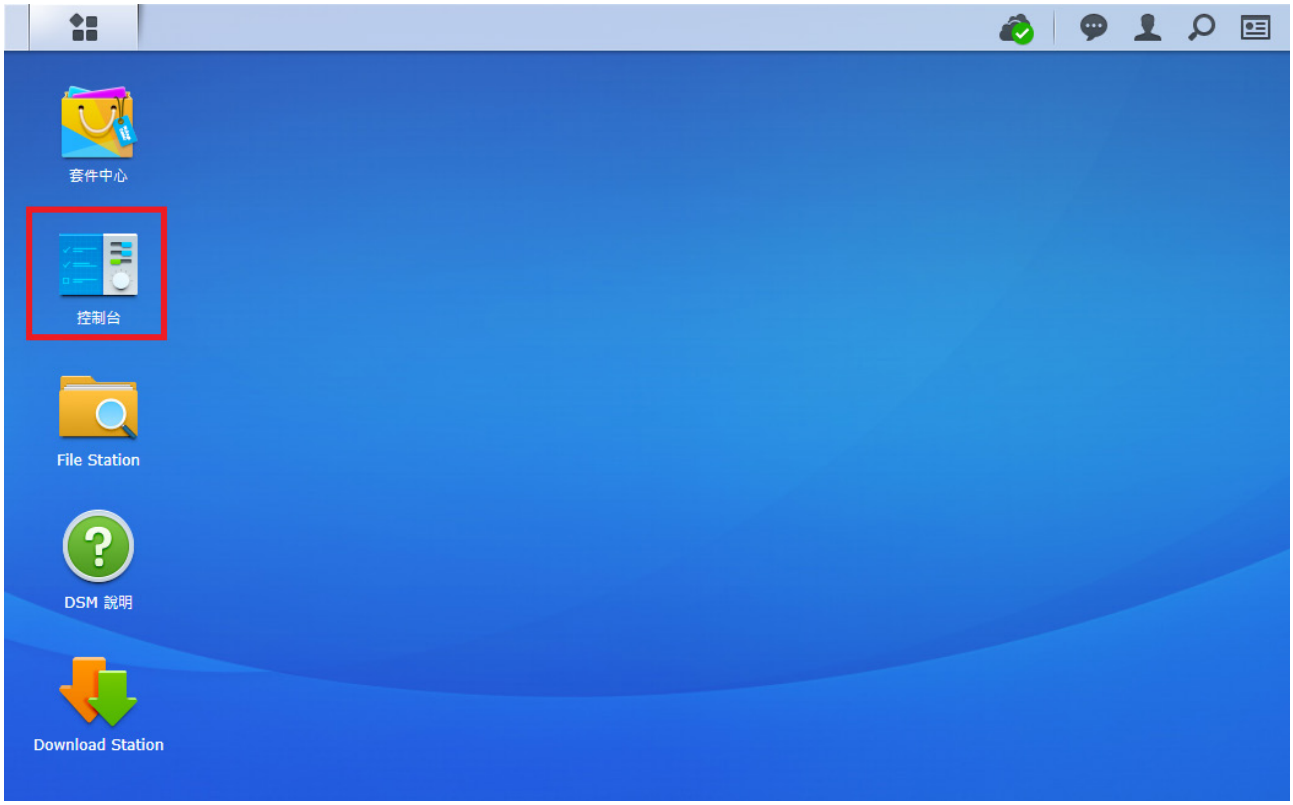
2022 年 4 月更新 二版

章節 1

生成CSR憑證請求檔及私密金鑰

本章節將開始帶您操作如何使用產生申請憑證時必要的 CSR(Certificeate Signing Request) 文件及私密金鑰 (Private Key)，幫助您生成憑證必要文件。

一、登入至 DSM 中並點擊桌面上的控制台



在您的 Synology NAS 管理入口以具管理員權限的帳號登入 DSM，入口位置則依您的設置登入：

◆以 Web Assistant 登入

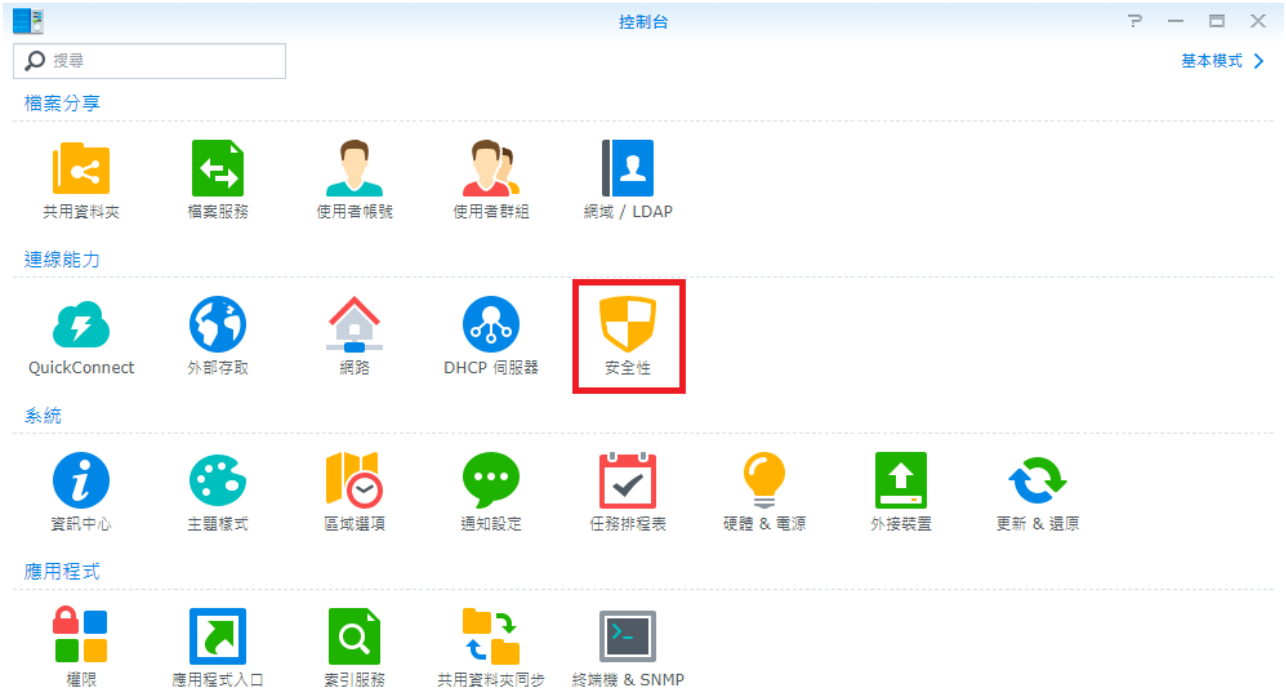
1. 確定您的電腦與 Synology NAS 位於同一網路並且可存取網際網路。
2. 打開電腦上的網頁瀏覽器並前往 find.synology.com。
3. Web Assistant 會在區域網路中找到您的 Synology NAS，按一下連線來前往登入畫面。

◆若要使用伺服器名稱或 IP 位置登入

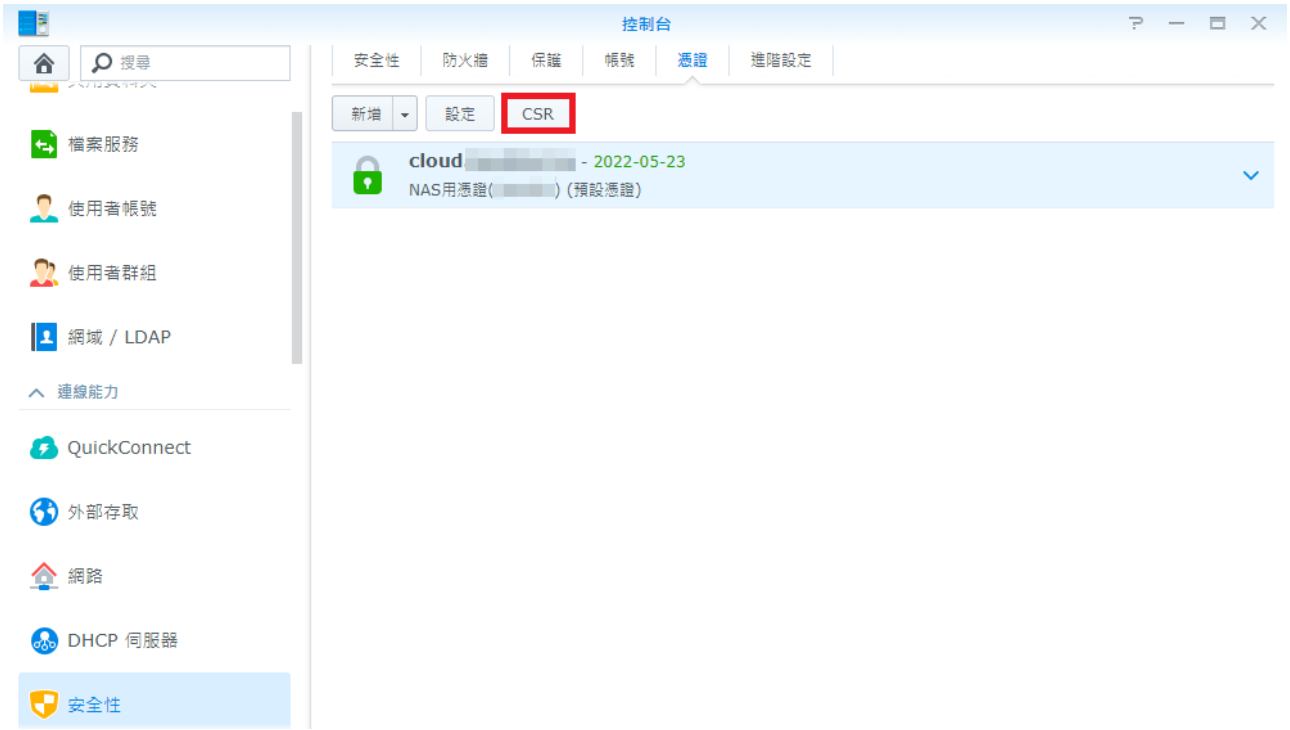
1. 請確認您的電腦已和 Synology Nas 連至同一網路 (若為網際網路則請輸入網際網路 IP 位置，使用域名者請確定您設定好 DNS 的 A 記錄指向 NAS 聯外 IP)
2. 打開電腦上的網頁瀏覽器，在位置欄位中輸入下列任一資訊，並按下鍵盤上的 Enter 鍵。
   - http://Synology_ 伺服器 _IP 位置 :5000
   - http://Synology_ 伺服器 _ 名稱 :5000
   - http:// 主機名稱 . 您的網域 :5000

   若您使用 SSL/TLS 加密通道 https 登入，則為 :5001

二、登入至 DSM 中並點擊桌面上的控制台的『安全性』



三、切換到「憑證」頁籤後再點一下『CSR』

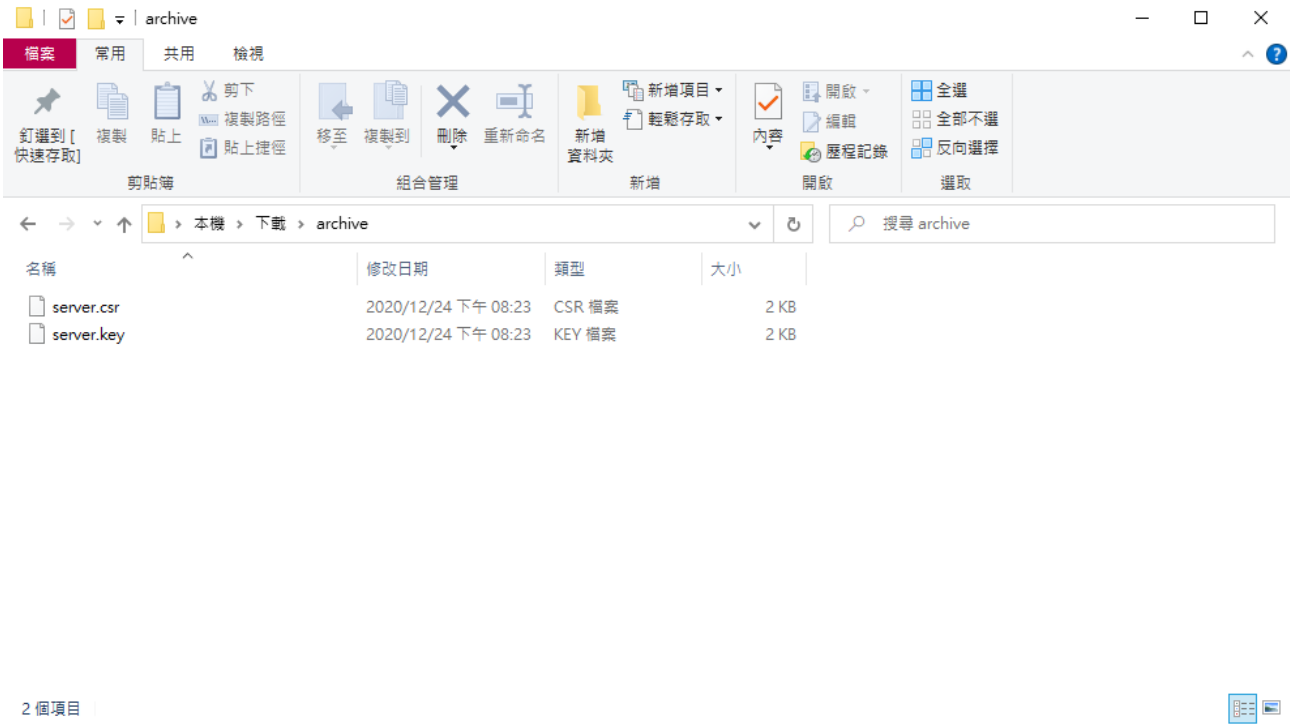


三、選擇「建立憑證請求 (CSR) 後」按『下一步』

四、依照下圖範例使用英文填入相應的資料 (金鑰長度選擇 2048)

五、完成憑證請求並下載相關檔案

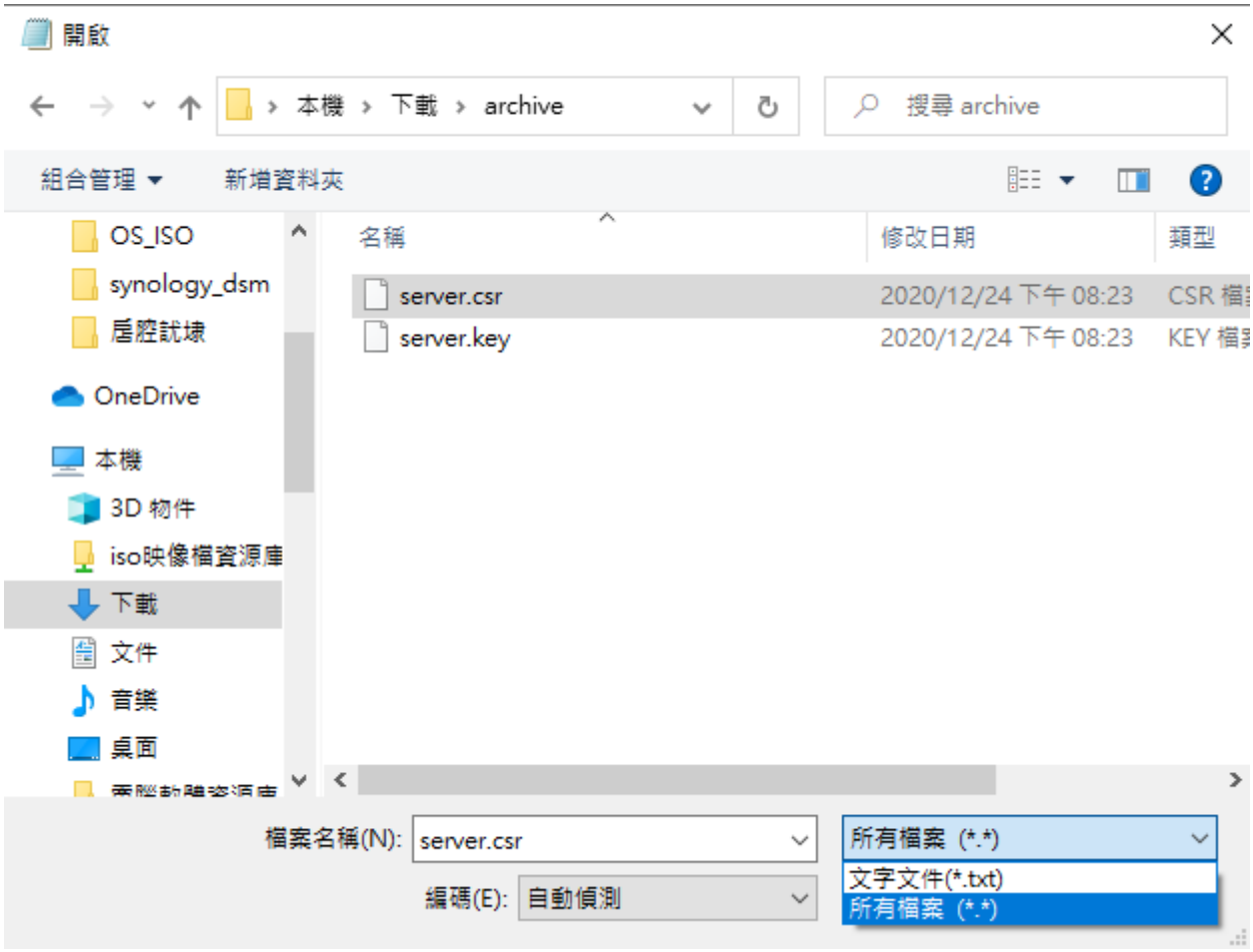
六、將下載的檔案給解壓縮以獲取憑證請求檔及私密金鑰



產出的檔案說明如下：

- server.csr 為憑證請求檔
- server.key 為私密金鑰檔案

七、使用記事本打開 .csr 檔案



注意事項：

使用記事本開啟 .csr 檔案所在目錄時，會發現沒有任何檔案，此時，請將檔案名稱下面的「文字文件 (*.txt)」旁邊的小箭頭向下拉，選擇「所有檔案 (*.*) 時，即可發現 server.csr 與 server.key 檔案。

因為我們需要的是憑證請求檔，所以開啟 .csr 就好。

八、複製文件裡面的內容以進行憑證申請

在多數的情況下，CSR 和 Key 檔是採 PEM 格式編碼的，所以都可以使用文字編輯器 (如記事本) 之類的軟體開啟並查看內容，因為 CSR 是遞送申請的必要條件，所以您這裡需要去確認所開啟的是何種檔案。

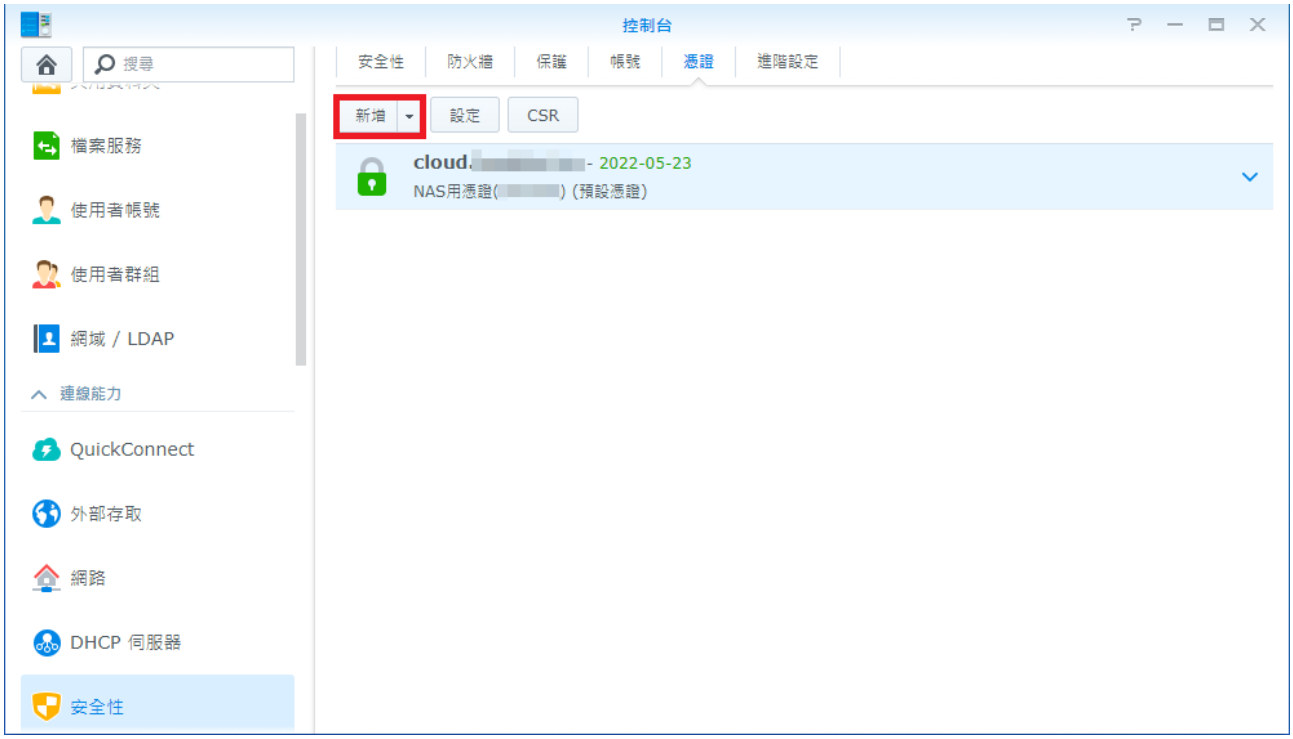
CSR 檔案是以 -----BEGIN CERTIFICATE REQUEST---- 做為開頭，並以 -----END CERTIFICATE REQUEST----- 做為結尾，遞送申請資料時，必須將此段頭尾一併貼上。

章節 2

在您的 Synology NAS 中匯入與安裝數位憑證

本章節將帶您操作在您取得憑證後，如何在DSM系統中將憑證與中繼憑證匯入您的Synology NAS 中

一、在「控制台」→「安全性」→「憑證」頁籤中點一下『新增』

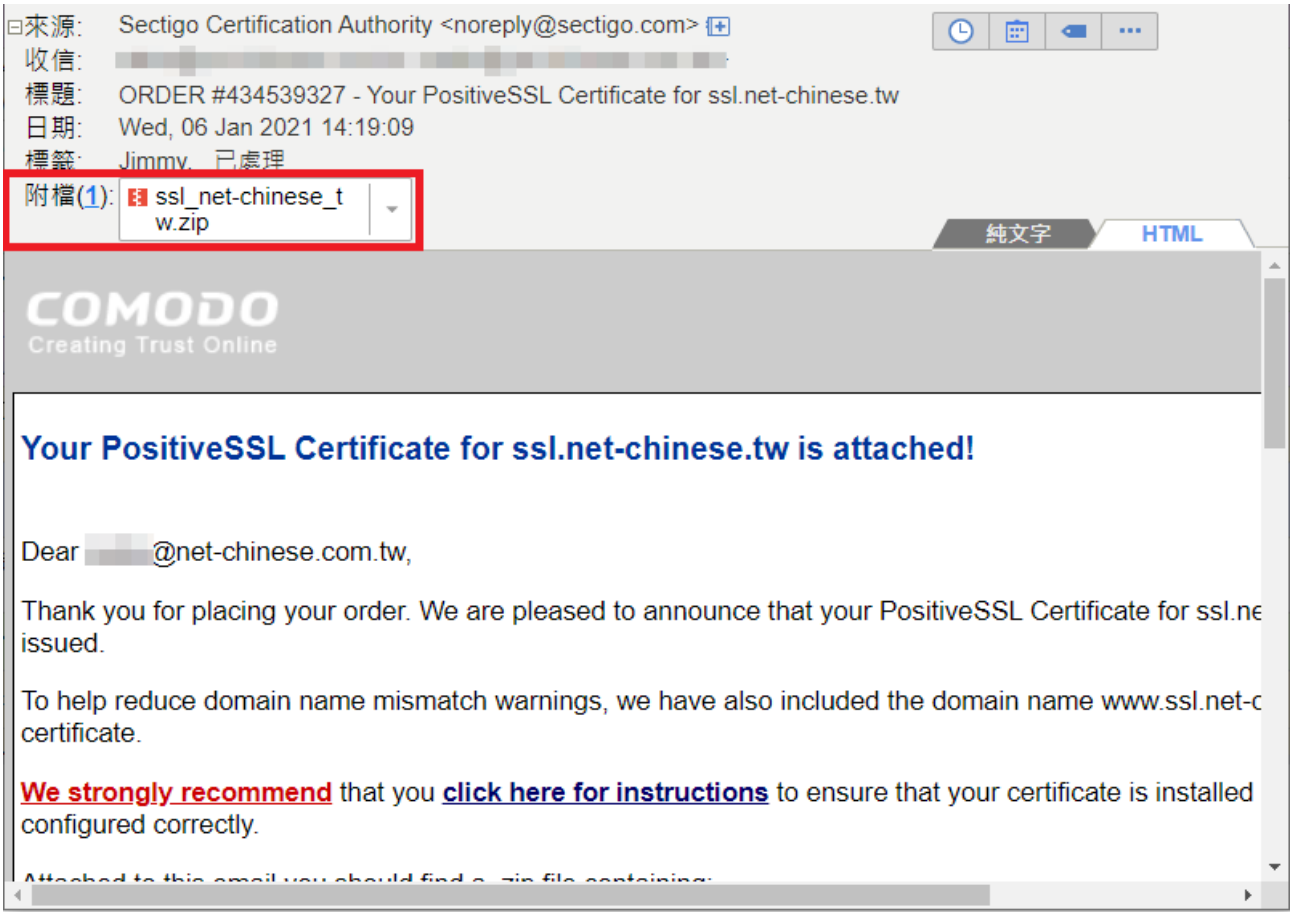


這個頁面是所有安裝在 Synology NAS 中的憑證的起點，您的 Synology NAS 不管是 for 管理登入介面、網頁憑證、郵件伺服器憑證，皆可以在此查看與繫結。

二、依照步驟提示點選『新增憑證』

三、單選「匯入憑證」同時在描述欄給這張憑證一個好記的自訂名

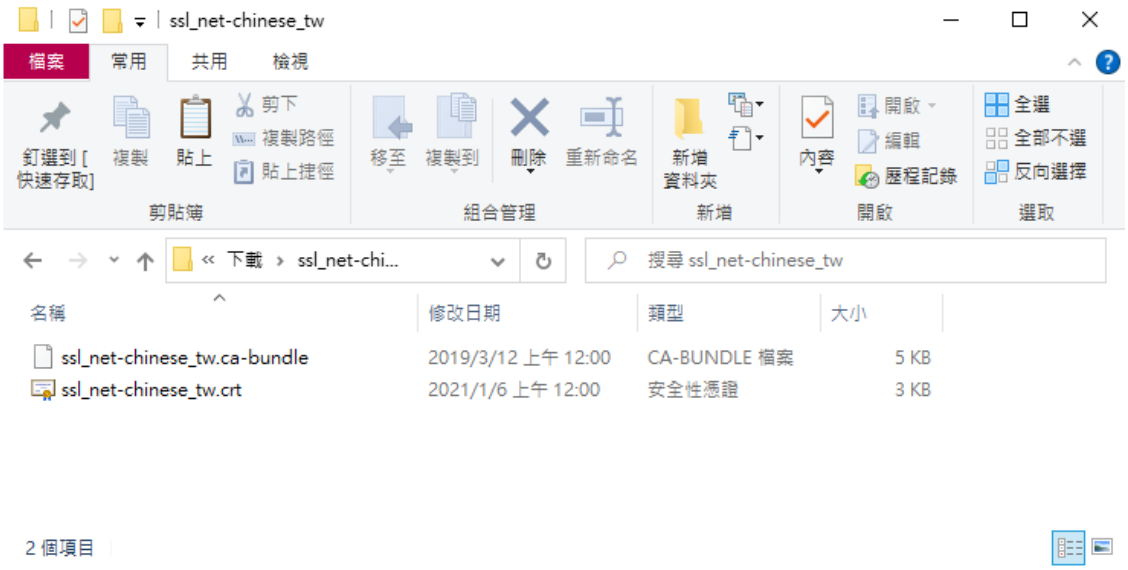
四、查看您申請憑證時填入的管理人信箱是否收到發證機構來信



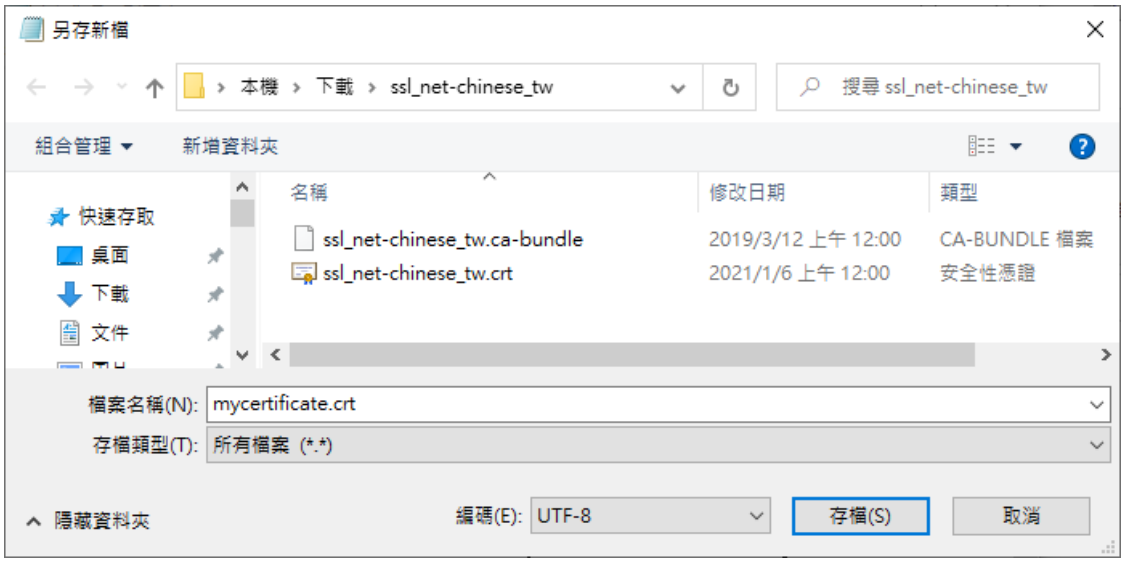
通常在您完成發證機構所要求的驗證程序後 (域名驗證 / 組織驗證)，您會在申請憑證時填寫的管理人信箱收到信件，寄信的內容會依照各家發證機構不同而有不同方式的形式表現，但大致上可以分為兩種類型：

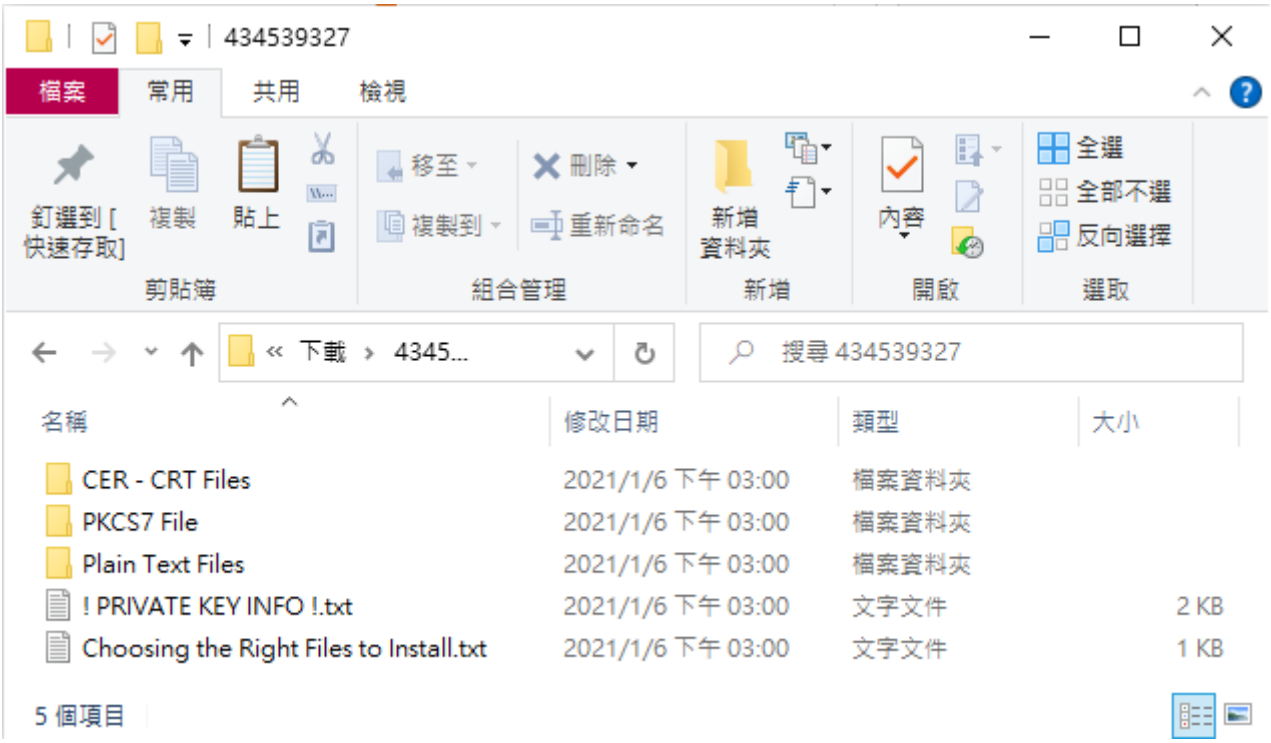
1. 以附件檔夾帶憑證檔案，以壓縮格式寄送 (如 .zip 檔)
2. 以文本格式記出，以文字方式表示。

以附件檔夾帶的憑證檔，有時會有較為簡化的方式做附件，如您選擇的伺服器是 Apache 就會給你一個 Bundle 檔 (根憑證與中繼憑證信任鏈) 和一個網站憑證檔，如果是 IIS 可能就會給你一個 .cer 格式的檔案，如果是 Other 類型可能就會給你完整的根憑證、中繼憑證及網站憑證檔案。(如下圖)



如果今天收到的憑證是以文字格式的話，我們可以利用記事本軟體，將憑證給複製 (需要包含 -----BEGIN CERTIFICATE----- 及 -----END CERTIFICATE----- 貼入空白的記事本。然後選擇「另存新檔」存檔案時一樣要選擇「所有檔案 (*.*)」，然後檔名您可以自訂，並在檔名最後加上副檔名 (.crt)，編碼的話選擇 ASCII 或是 UTF-8 都可以。





如果您是在網路中文下載的憑證，或是由網中客服寄發給您的憑證，解壓縮之後，您也許會看到的內容如上，以下將針對各資料夾與內容物進行說明。

- CER - CRT Files - 以副檔名為 .CRT 格式的憑證檔案，內含網站憑證、根憑證、中繼憑證。

  Sectigo(COMODO) 品牌
  - xxx_xxx_xx.crt 是網站憑證，其中 xx 會是您的域名。
  - AAA Certificate Service.crt (AddTrust) 為 Sectigo 品牌的根憑證。
  - USERTrustRSAAddTrust.crt 為 Sectigo 品牌的互簽憑證。
  - SectigoRSA(Domain/Organization/Extended)ValidationSecureServerCA.crt 為 Sectigo 品牌的中繼憑證。
  - My_CA_Bundle.ca-bundle 為根憑證、互簽憑證及中繼憑證的三合一信任鏈憑證。

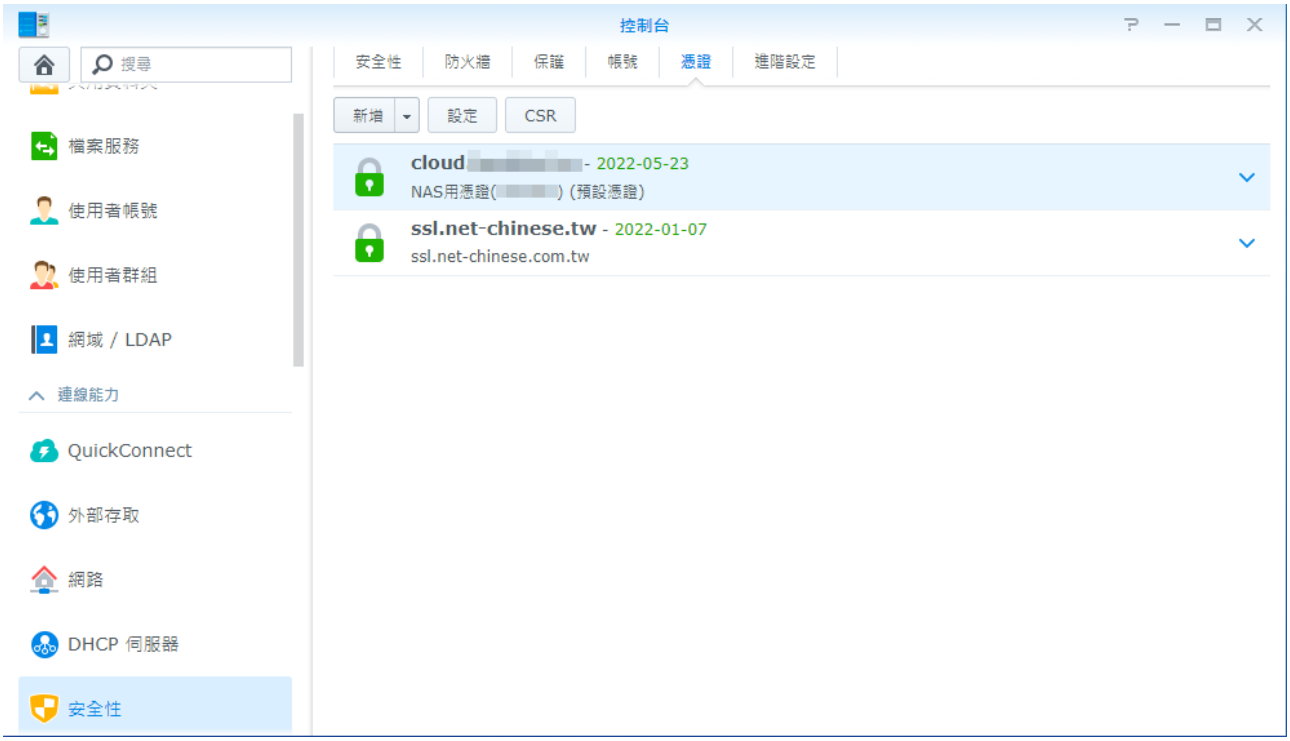
  非 Sectigo 品牌

  未必會有附上中繼憑證及根憑證，但我們可以從關鍵字中查詢。
  - 有 Root 字樣 - 根憑證。
  - 有 Intermediate 字樣 - 中繼憑證。
- PKCS7 File - 加密訊息語法標準檔，用來使用對訊息簽章或加解密，Microsoft Windows 系統、AZURE 雲端服務及 JAVA Tomcat 有機會用到，該檔案只會包含憑證與中繼憑證。
- Plain Text Files - 為 CER - CRT Files 中憑證的純文字文件，您可以利用另存新檔方式儲存成 .crt 格式。
- !PRIVATE KEY INFO !.txt - 憑證檔不含私密金鑰指南及宣告。
- Choosing the Right Files to Install.txt - 用來告知您各資料夾的內容物檔案。

請注意，其內容物會因為您所選擇的品牌、驗證方式而有不同。

五、將憑證、信任鏈（中繼憑證）及私密金鑰匯入主機

六、完成憑證匯入



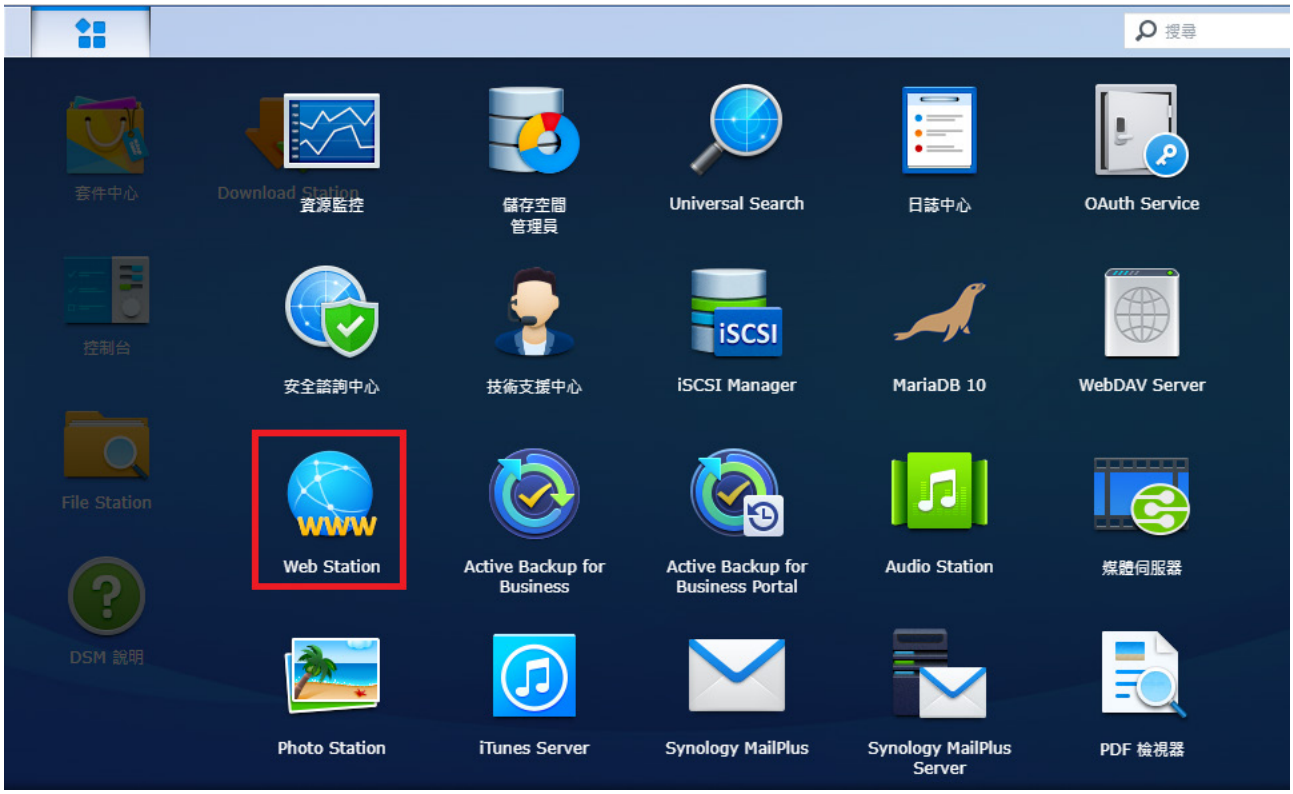
做到了這一個步驟，即代表已完成了憑證匯入，上面綠色的日期即為憑證到期日。

章節 3

將已裝好的憑證與站台繫結

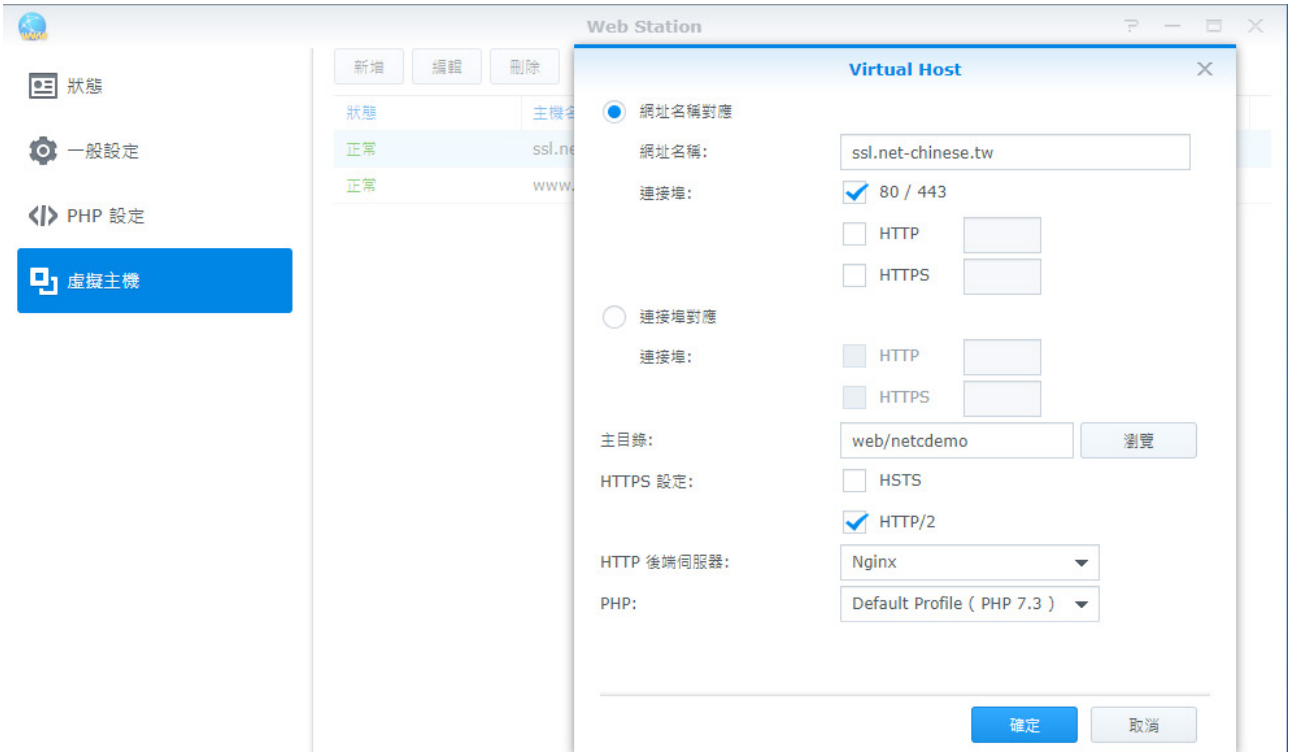
本章節將帶領您操作如何將已匯入主機的憑證給繫結到您的站台上，讓您的網頁可以正常的使用 SSL 憑證。

一、打開您的 Web Station



在您的 DSM 作業系統中點一下左上角，找到您所安裝的 Web Station，若您未安裝，則請到「套件中心」中安裝 Web Station 及其必要的伺服器引擎 (例如 Apache、Nginx 等等)

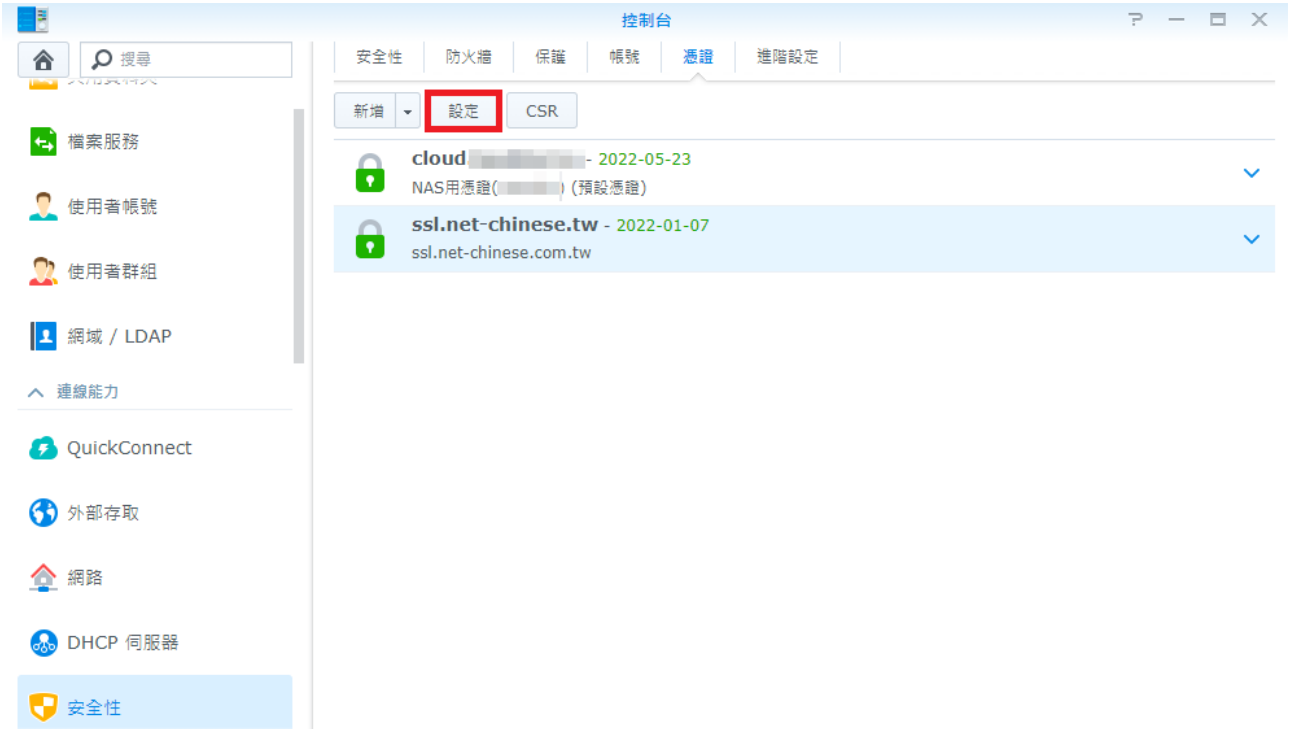
二、請確認您的站台設置是否包含 80/443 通道是開啟的



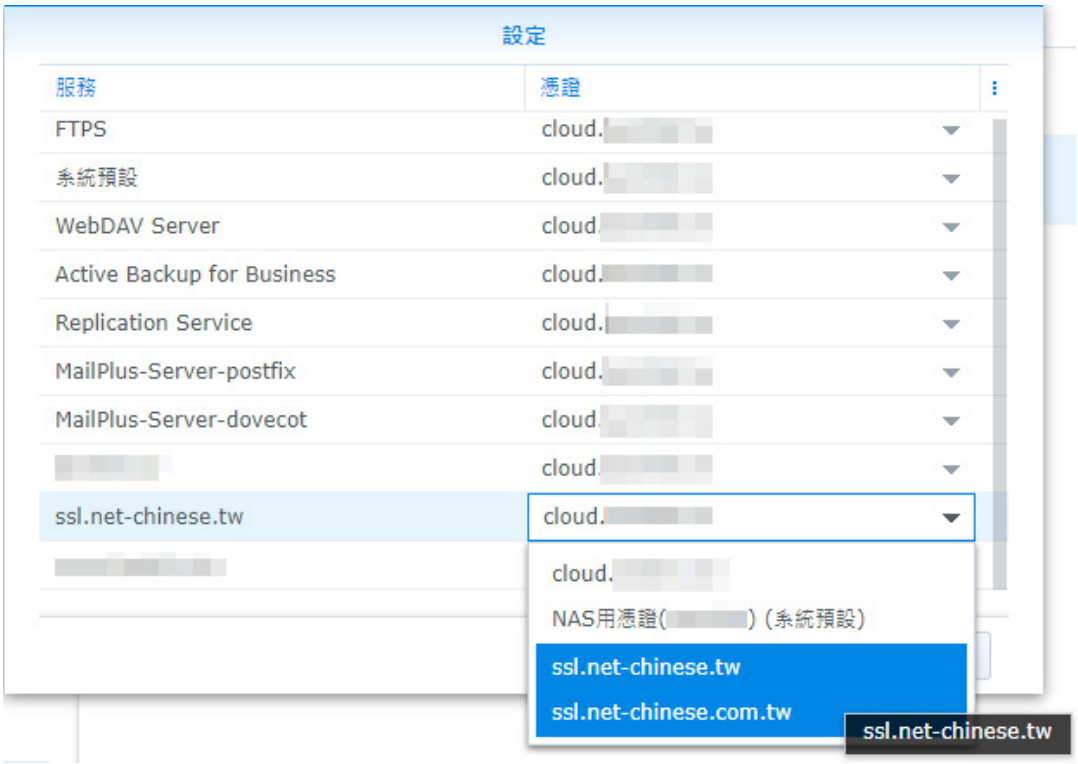
打開 Web Station 後，在您的站台上點擊一下「編輯」，如果您沒有站台，則點擊「新增」以創建您的虛擬主機站台，其中設定如下：

- 網址名稱 - 請輸入完整主機名稱與域名名稱，例如：www.mydomain.com
- 連結埠 - 80/443 (http 通道【非安全】/https 通道【安全】的預設通訊埠口)，如果您想要用其他自訂的連接埠，請勾選下面的 HTTP 並輸入通訊埠號及 HTTPS 與通訊埠號。
- 主目錄 - 為您的網站站台根目錄，也就是您要放置您的網頁首頁及相關資料的資料夾。
- HTTPS 設定 - 這邊提供了兩組 Web 安全協議，即 HSTS 與 HTTP/S，您可以視您的需要啟動其一或是都啟動。
- HTTP 後端伺服器 - 常見的後端伺服器有 Nginx 及 Apache，您可以視您的需要進行選擇，如果無法選擇，請至您的「套件中心」中下載。
- PHP - 如果您要執行 PHP 網頁程式後端語言，您可以選擇適當的版本以進行搭配，如果沒有您要的版本或可選的版本，請至您的「套件中心」中下載。

三、至「安全性」→「憑證」頁籤，選取並對憑證進行設定與繫結

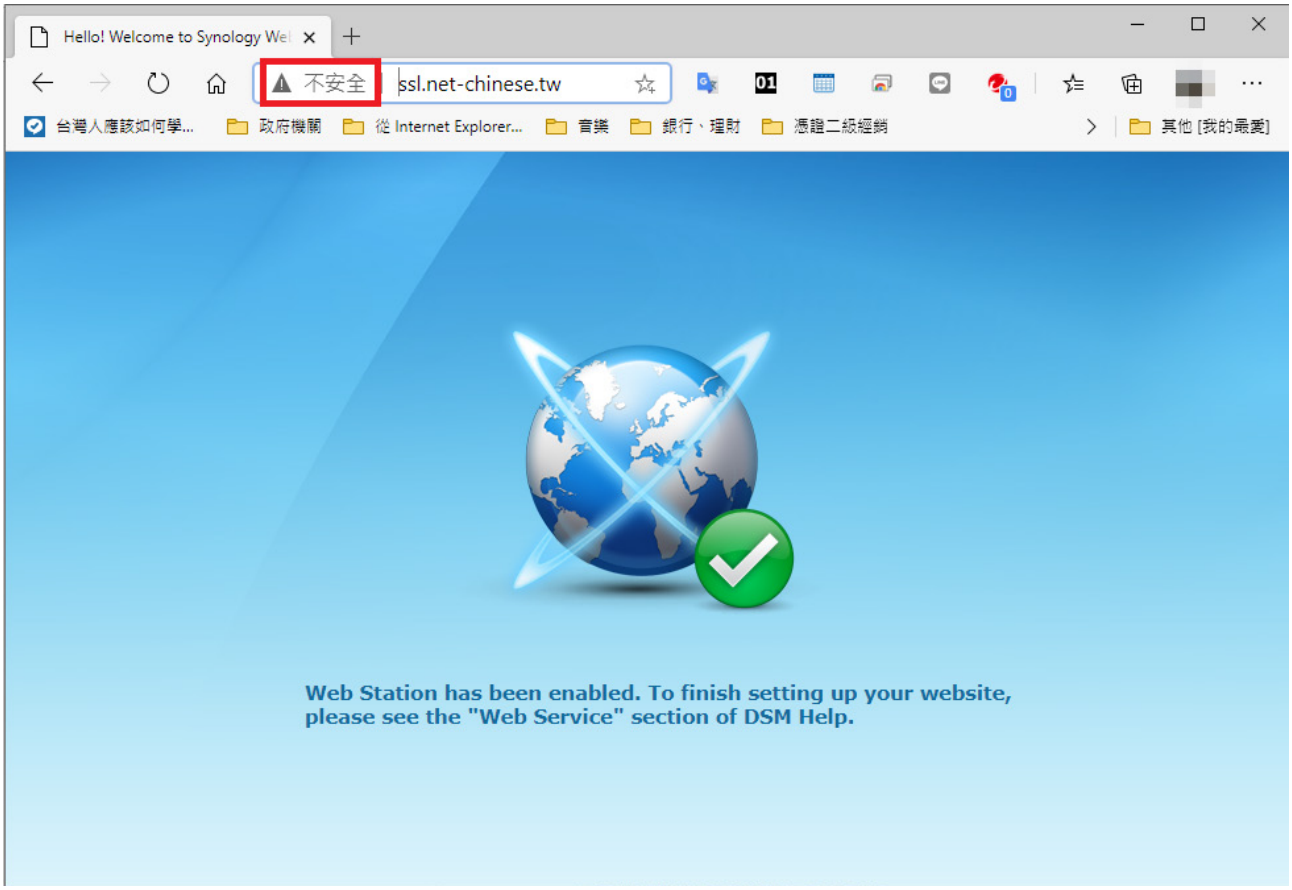


四、調整憑證所要對應的服務項目



在 NAS 中有各種許多的服務，如網頁伺服器、FTP 伺服器、郵件伺服器等等，可以透過憑證去繫結各項需要憑證的服務。透過▼下拉式選單可以選擇已匯入的伺服器憑證。

四、最終畫面測試



輸入 http:// 您的域名，在網頁伺服器正常運作的時候，您或許會看到網址列顯示「不安全」，但是並非憑證沒有安裝成功，而是在 Web Station 的虛擬主機設定時，我們採用了預設 80/443 通道開啟，所以此時的網頁伺服器，是非加密的通訊埠 80 通道與加密的 443 通道並行。

此時，若您在網頁上面輸入 https:// 您的域名，應該就會正常的顯示了。

但是，這並非是一個良好的解決方案，或許您可以透過考慮透過 .htaccess 檔案來將 http 轉導到 https。

請在你的網頁的根目錄中的 .htaccess 檔案中加入以下程式碼。
重點：如果在 .htacess 文件中有現有的程式碼，請在上面添加具有類似起始前綴的規則。

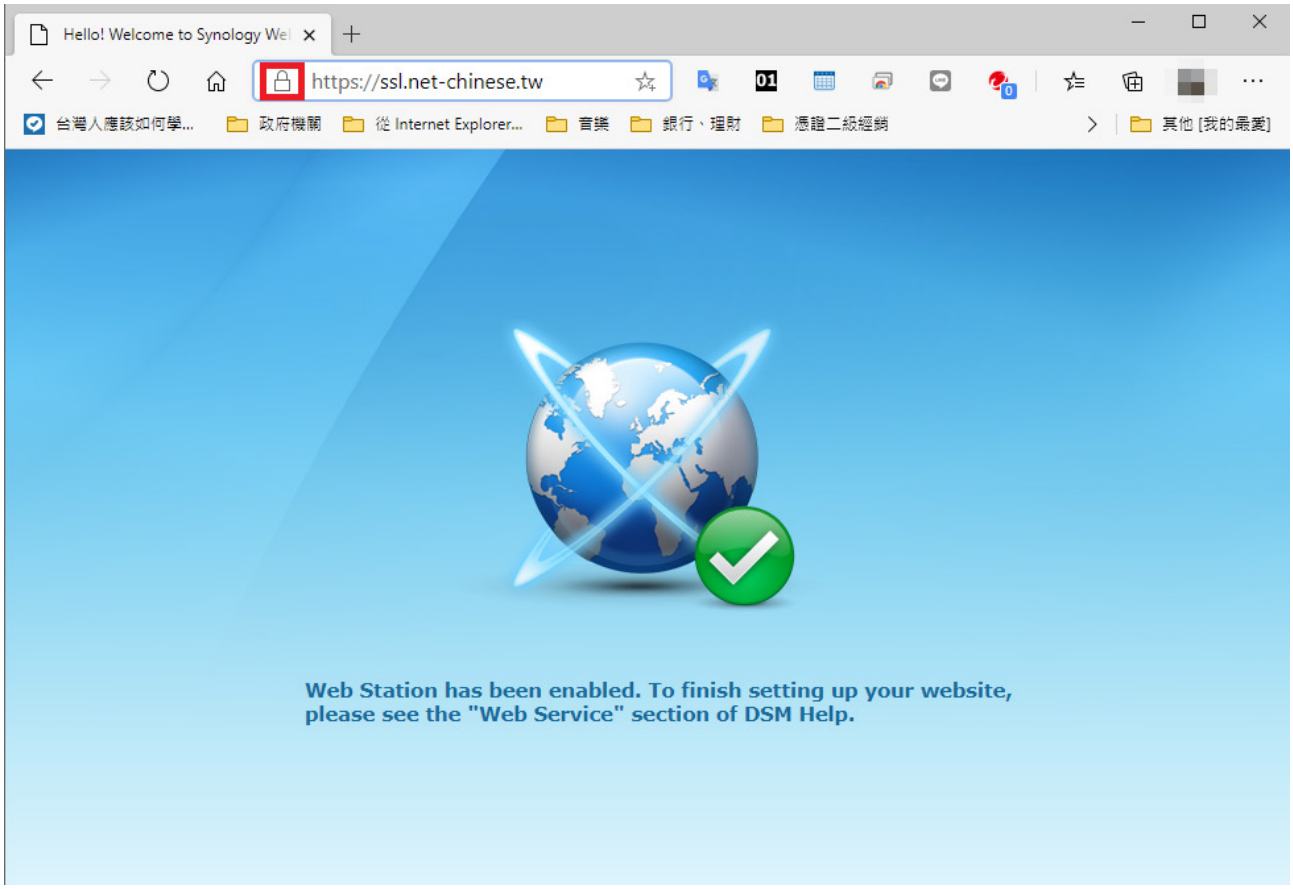
```
RewriteEngine On
RewriteCond %{SERVER_PORT} 80
RewriteRule ^(.*)$ https://www.example.com/$1 [R,L]
```

請注意：務必使用你的真實網址取代 www.example.com。

要強制一個特定的網域 (http) 來使用 https，請在你的網頁的根目錄中的 .htaccess 檔案中加入以下程式碼。

```
RewriteEngine On
RewriteCond %{HTTP_HOST} ^example.com [NC]
RewriteCond %{SERVER_PORT} 80 RewriteRule ^(.*)$ https://www.example.com/$1 [R,L]
```

務必使用你想要強制轉為 https 的網址，來取代 example.com，此外你需要用真實網址取代 www.example.com。



如果您在網址列上輸入 https:// 您的域名，此時應該就可以看到瀏覽器上面有鎖頭了。這樣即代表已成功的套用憑證。

假使您輸入了 https 卻仍然顯示不安全，則以下提供幾點簡易的狀況排除。

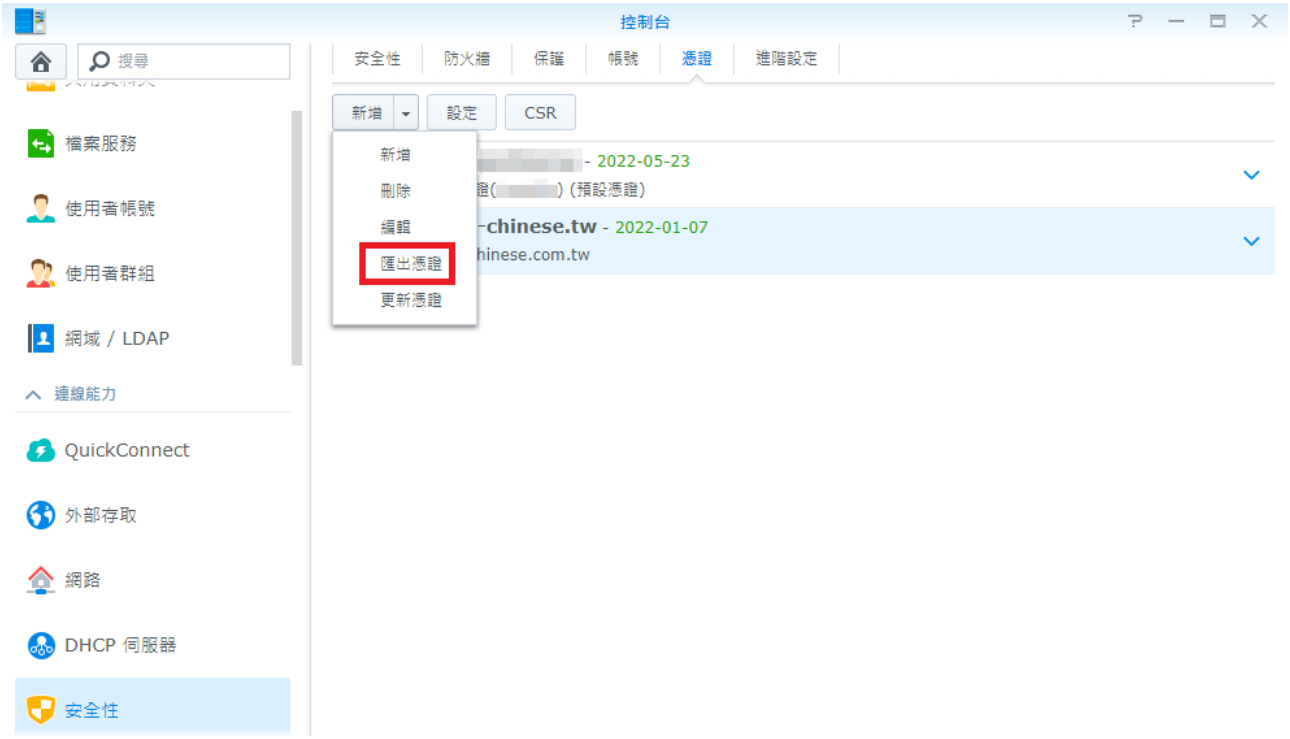
1. 您的防火牆並沒有開啟通訊埠 443。
2. 您的網頁原始碼裡面有使用絕對路徑，且不安全的來源 (如外部圖片、影音)，請檢查您的網頁原始碼裡面是不是有 http:// 的來源文件，若有則請您改用相對路徑，或是直接將 http 更改為 https。

章節 4

匯出憑證以供其他主機使用

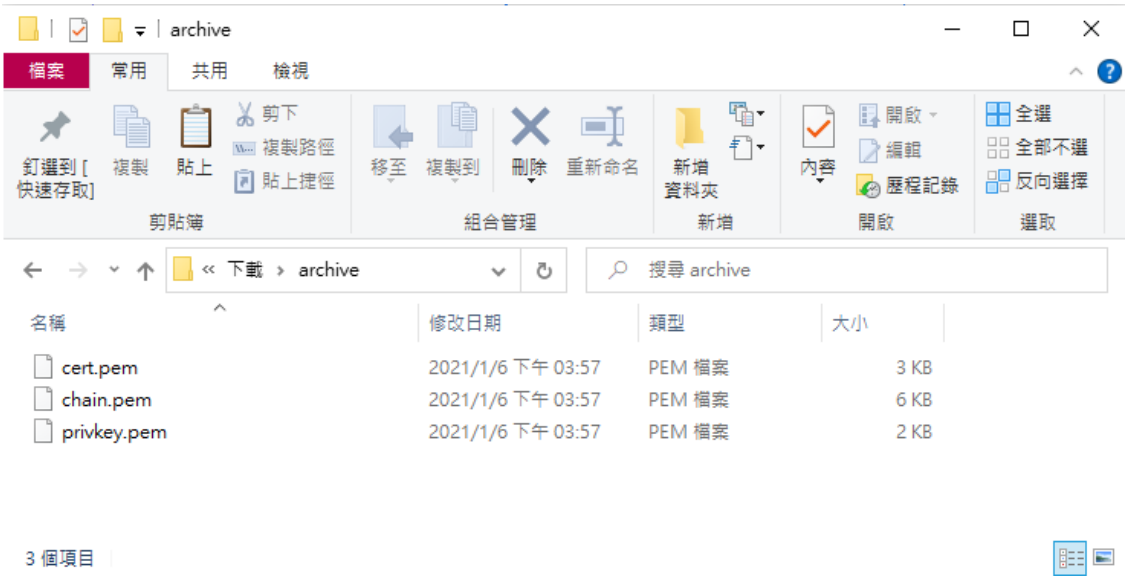
本章節將帶領您操作如何將已匯入主機的憑證給匯出來，以便您帶著憑證至其他主機上安裝。

一、在「憑證」頁籤中點一下「新增」按鈕旁小箭頭並選擇匯出



請您選將欲匯出的憑證選取（呈淡藍色），再點選「匯出憑證」，即會下載匯出之憑證。

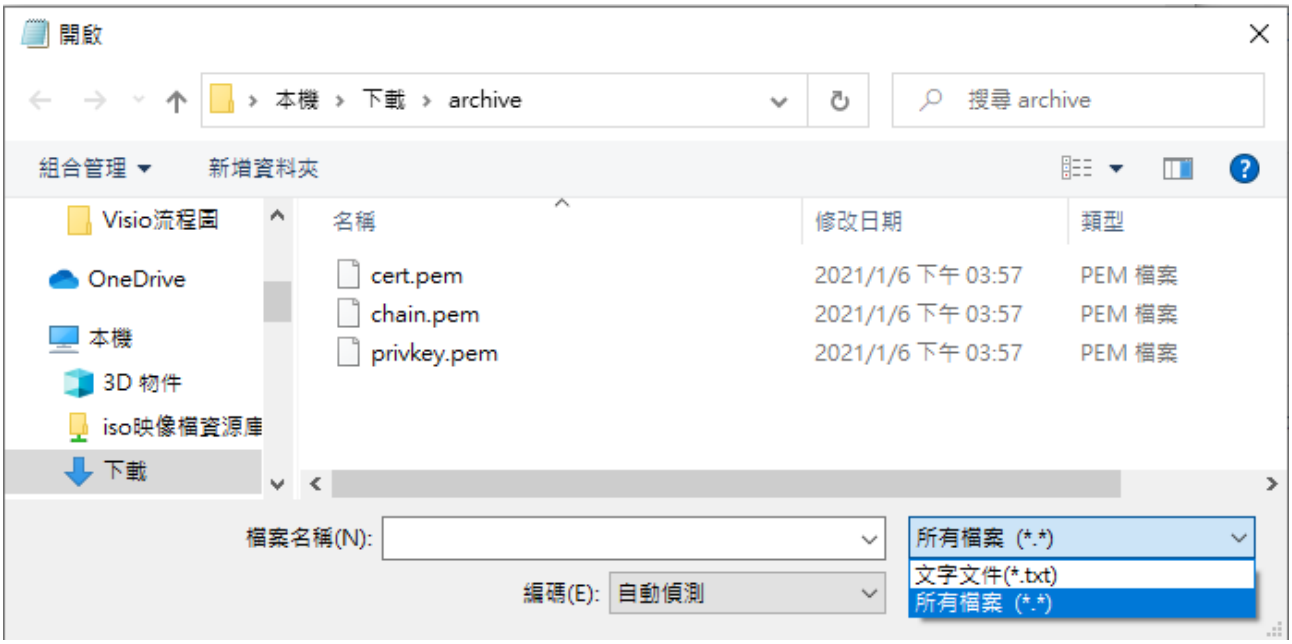
二、將下載的憑證解壓縮



憑證解壓縮後會發現三個檔案，分別如下：

- cert.pem - 網站憑證
- chain.pem - 信任鏈 (中繼憑證)
- privkey.pem - 私密金鑰

這三個文件雖然副檔名是 .pem，即代表是以 pem 編碼，一樣使用記事本或文字編輯器開啟即可。



當有多台主機要使用時，可使用這個方法將憑證與私密金鑰匯出，佈署在其他的主機上，但是若是要匯入 Windows 的主機使用時，需要將這三個檔案使用轉換工具 (如 Open SSL 轉換成 PKCS#12 格式，即 .pfx 格式方可匯入。

附錄 - 注意事項：

- **不要使用特殊字元**
  在申請伺服器憑證時，不要出現某些特殊字元，否則在您提交 CSR 後，可能會出現錯誤。這個錯誤是由於在您產生 CSR 時，輸入的資訊中包含一些特殊字元，如：(@,#,&,!, 等等，例如：您可以將 "&" 用 "and" 代替)。

- **什麼是主要名稱 (COMMON NAME)**
  在產生 CSR 的時候，主要名稱 (又稱憑證名稱 /Common Name)，是一定要填寫的，但我們發現有許多的客戶常常在這個地方出現錯誤，或不符合申請規範。

  主要名稱 (Common Name) 是您的主機名稱 + 網域名稱，例如 www.net-chinese.com.tw 的伺服器憑證是頒發給某一台主機的，而不是一個域名，您的主要名稱（Common Name）必須與您要使用伺服器憑證的主機的全名完全相同，因為 www.domain.com 與 domain.com 是不同的兩台主機，除非您將兩個 A 記錄指向同一台主機。

  另外，用戶在產生 CSR 的時候，若 Domain 為 yourdomain.com 請記得產出 CSR 為 www.yourdomain.com。

  如果您今天申請的是單域名通用型域名，則主機名稱請以「*」代替，在主要名稱中輸入 *.yourdomain.com。

- **不要將 CSR 與 KEY 加密**
  有的人使用一些工具進行 CSR 與私密金鑰的生成 (如 OpenSSL 或是 Linux 環境)，在產出過程中，系統會問您需不需要為 CSR 與私密金鑰加上密碼，請記得留空，不要加密。

- **請保管好您的私密金鑰**
  欲產生 CSR 檔案時，則必然會有一組私密金鑰與之相配對，私密金鑰與憑證是密不可分的。一旦您遺失了私鑰，簽發下來的憑證就無法與之配對了，此時您可能就需要重新產生新的私密金鑰與 CSR 檔案來進行重發憑證，重發憑證是否需要費用，則視發證機構的規定。

  若您有多台主機，需要將憑證佈署在多台主機上，則必須所有的主機使用同一組憑證與私密金鑰。

- **私密金鑰長度必須為 2048 位元 (bit)**
  為加強憑證安全強度，目前發證機構已不再頒發低於 2048 位元的 CSR 憑證提交資訊，所以請您在產生 CSR 時務必選擇 2048 位元的位元長度。