為不安全的網頁上把鎖
使用Let’s Encrypt SSL自動更新憑證

仁愛國小 賴新田

為什麼要使用 SSL 安全通訊協定

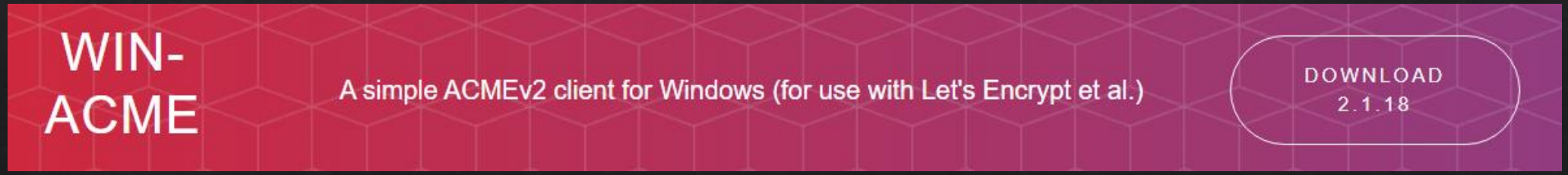
- https 連線網頁使用 SSL 加密憑證可以讓使用者在網頁輸入的資料更加安全，減少被截取內容的風險。
- 已經安裝 SSL 憑證的網站就可以使用 https 連線，沒有使用 Https 連線，會被 Chrome 標示為不安全網站。
- 免費SSL憑簡介 https://www.ilrc.edu.tw/data/1051102-ssl.pdf

事先準備

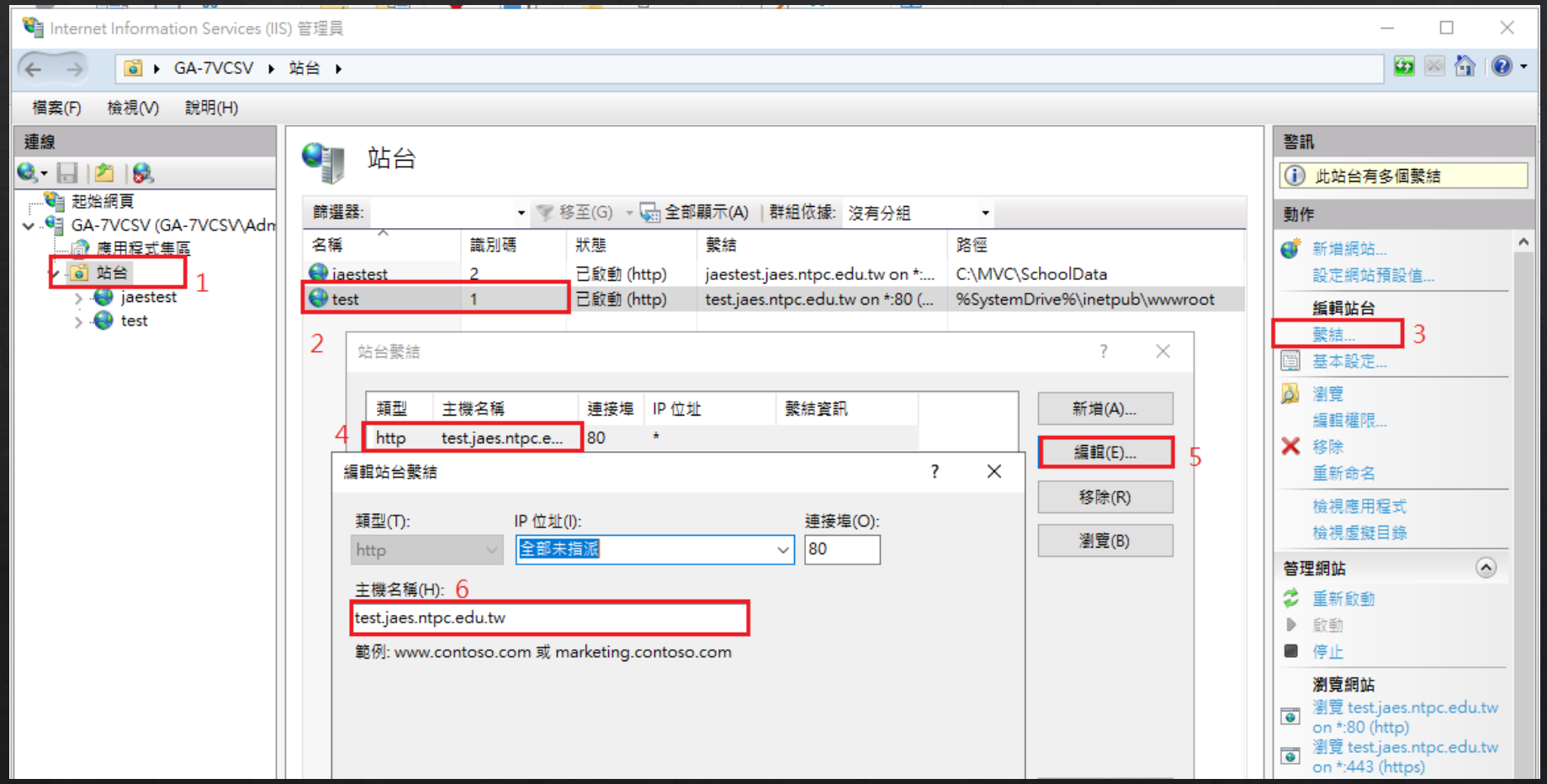
- 一個網域名稱 test.jaes.ntpc.edu.tw (已在WebDNS新增 A record)

- Windows Server 2019 IIS 主機

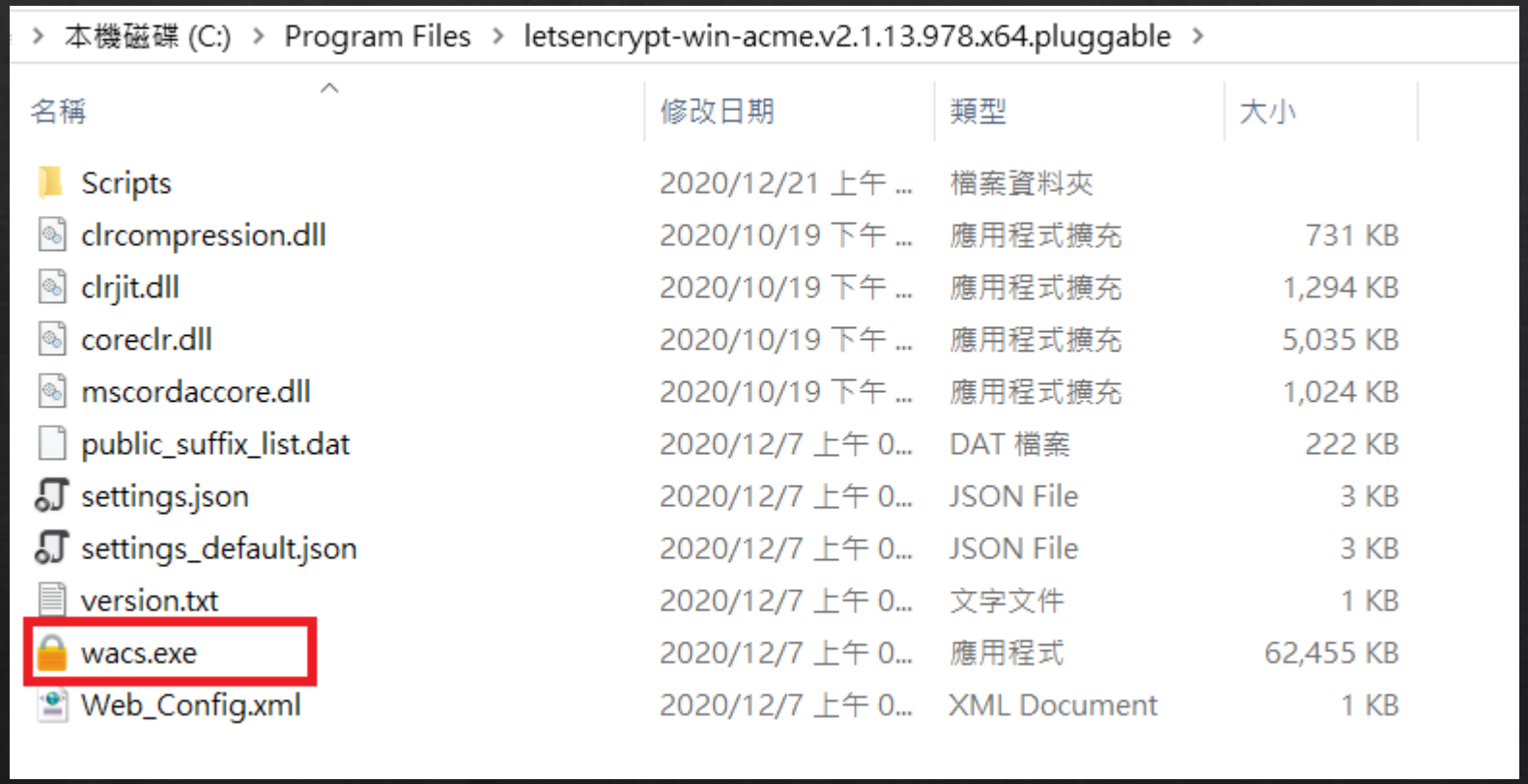
- 使用 Let's Encrypt 自動更新憑證工具，下載符合 ACME (Automatic Certificate Management Environment) 協定的輔助工具 Certbot， 推薦使用 win-acme



Windows Server IIS 站台繫結

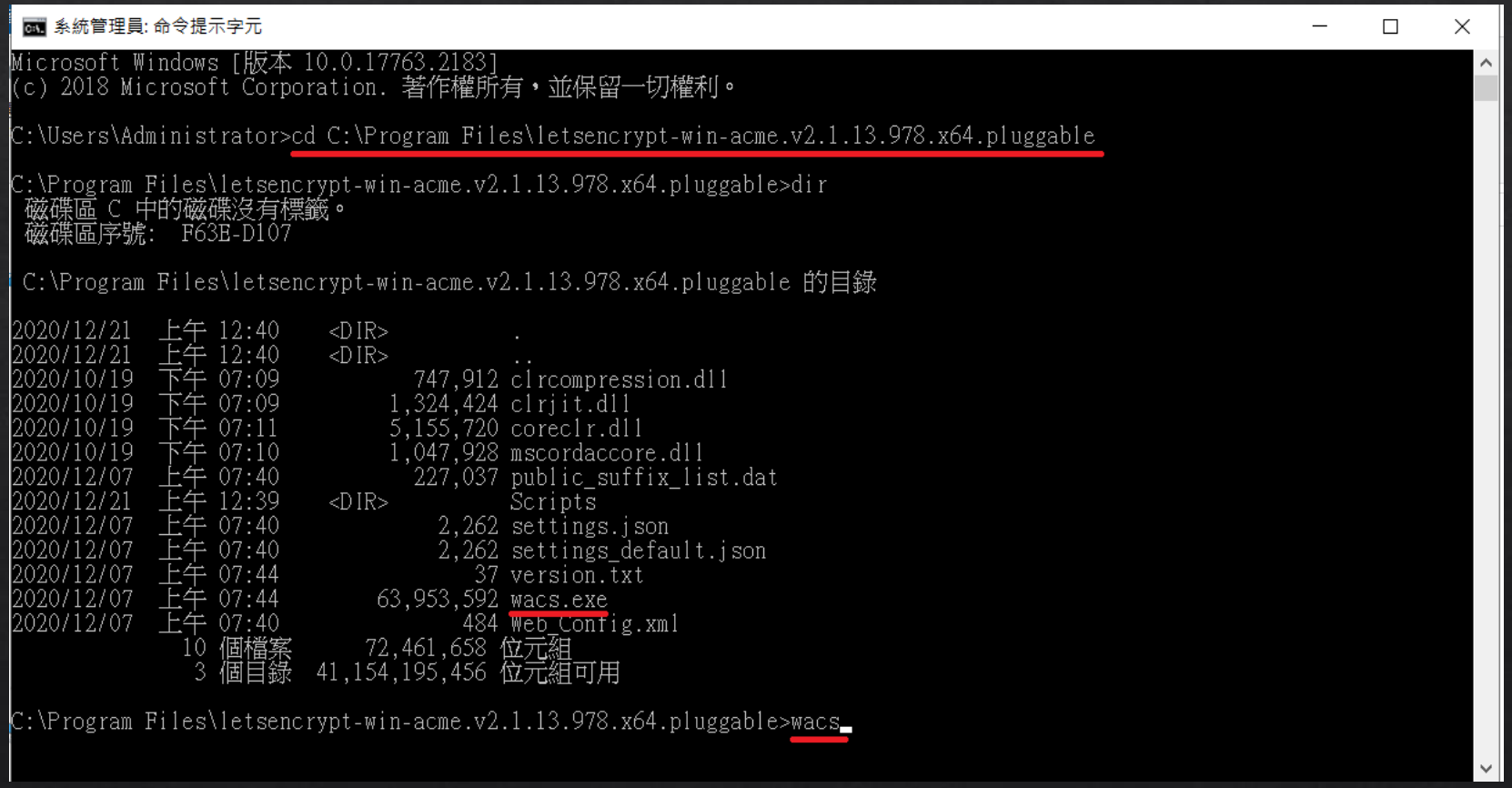


解壓縮檔案，移至適宜位置

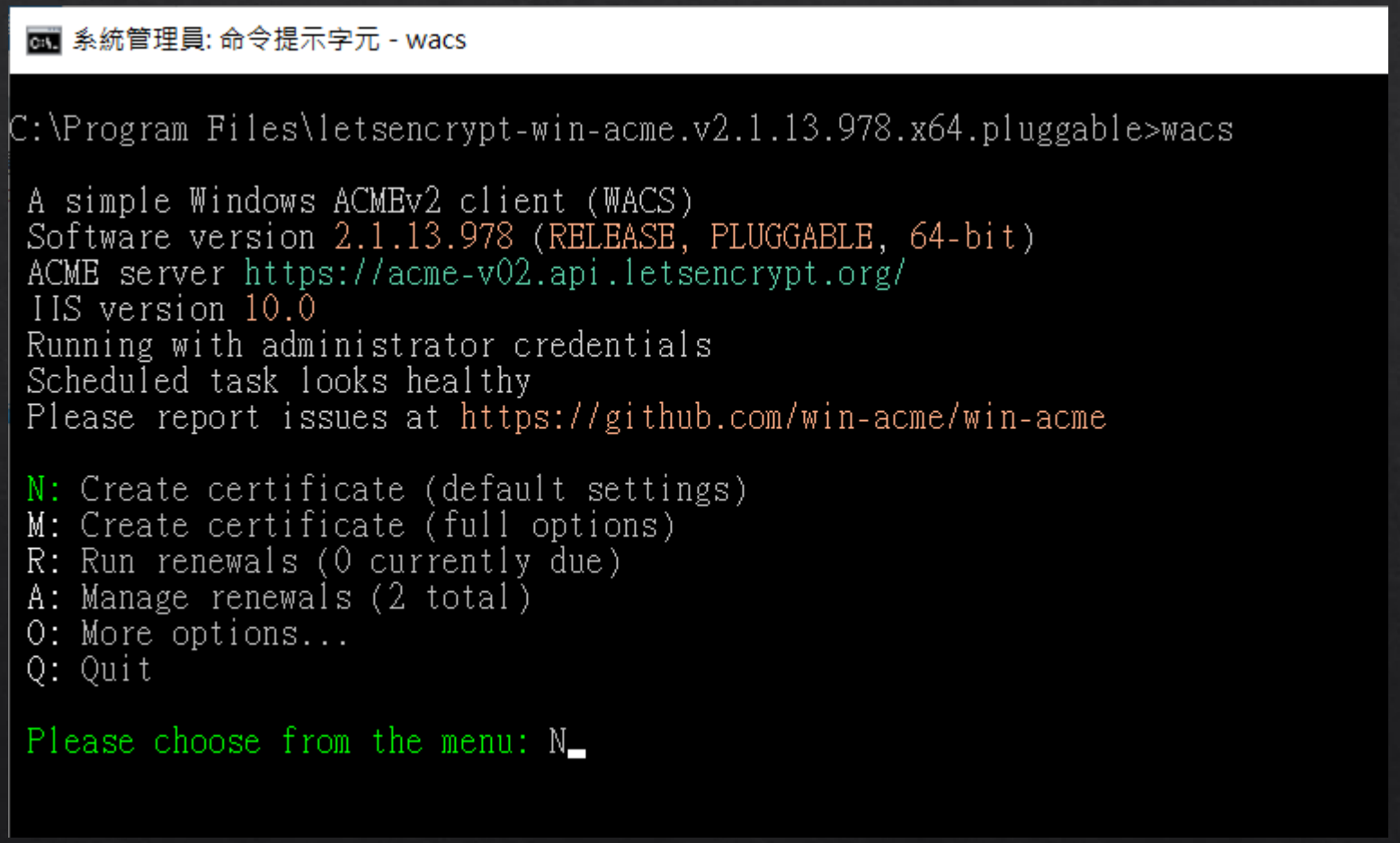


執行 win-acme

- 以系統管理員身份執行命令提示字元視窗，切換至 win-acme 資料夾



N: Create certificate (default settings)



Please select which website(s)

```
Running in mode: Interactive, Simple

 Please select which website(s) should be scanned for host names. You may
 input one or more site identifiers (comma-separated) to filter by those
 sites, or alternatively leave the input empty to scan *all* websites.

2: jaestest (1 binding)
1: test (1 binding)

Site identifier(s) or <Enter> to choose all: 1
```

如果沒列出任何站台，請至第4頁檢查站台繫結是否正確設定了

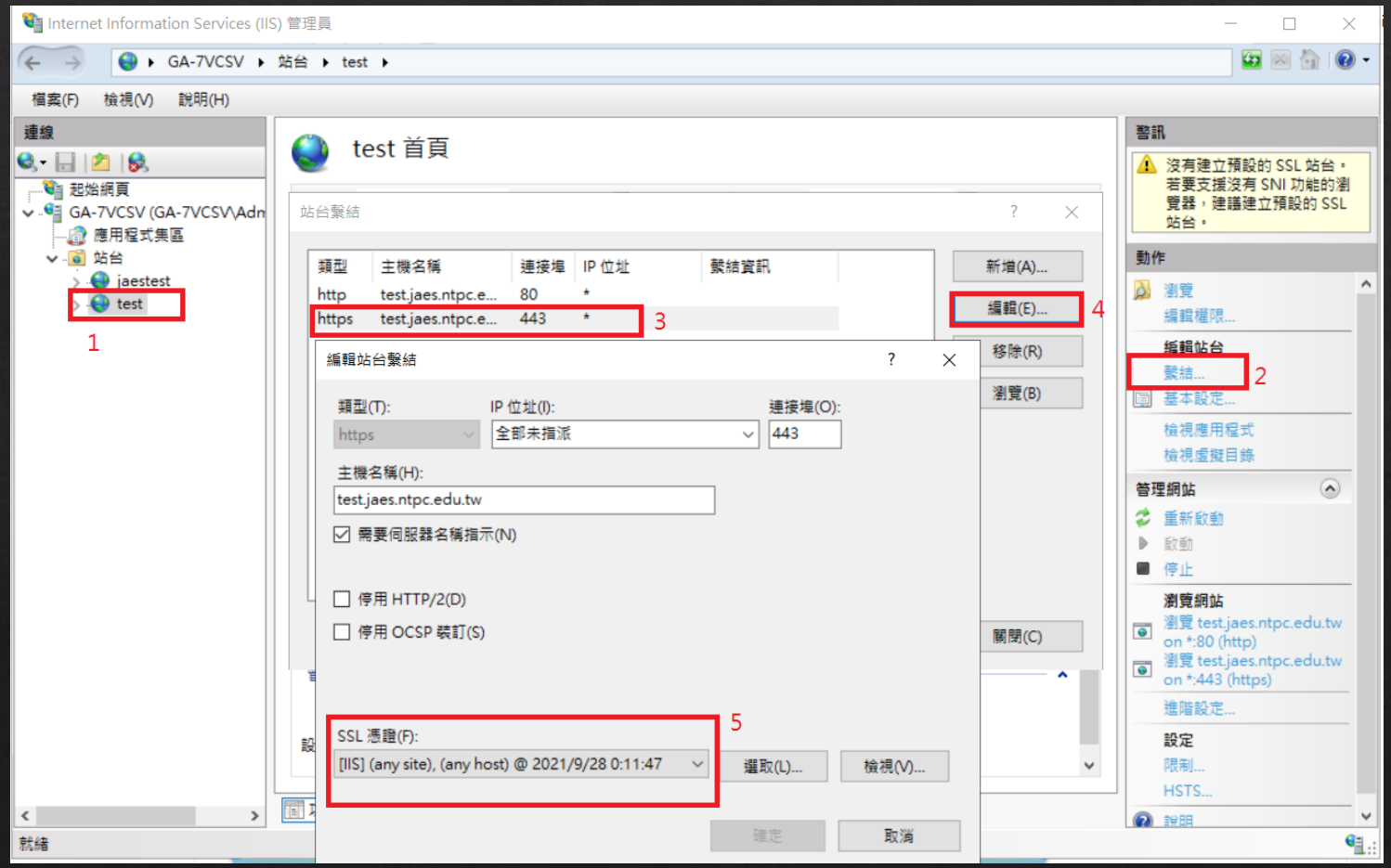
選擇指定子網域或是全部子網域

```
1: test.jaes.ntpc.edu.tw (Site 1)

 Listed above are the bindings found on the selected site(s). By default all
 of them will be included, but you may either pick specific ones by typing the
 host names or identifiers (comma-separated) or filter them using one of the
 options from the menu.

P: Pick bindings based on a search pattern
A: Pick *all* bindings

Binding identifiers(s) or menu option: A
```

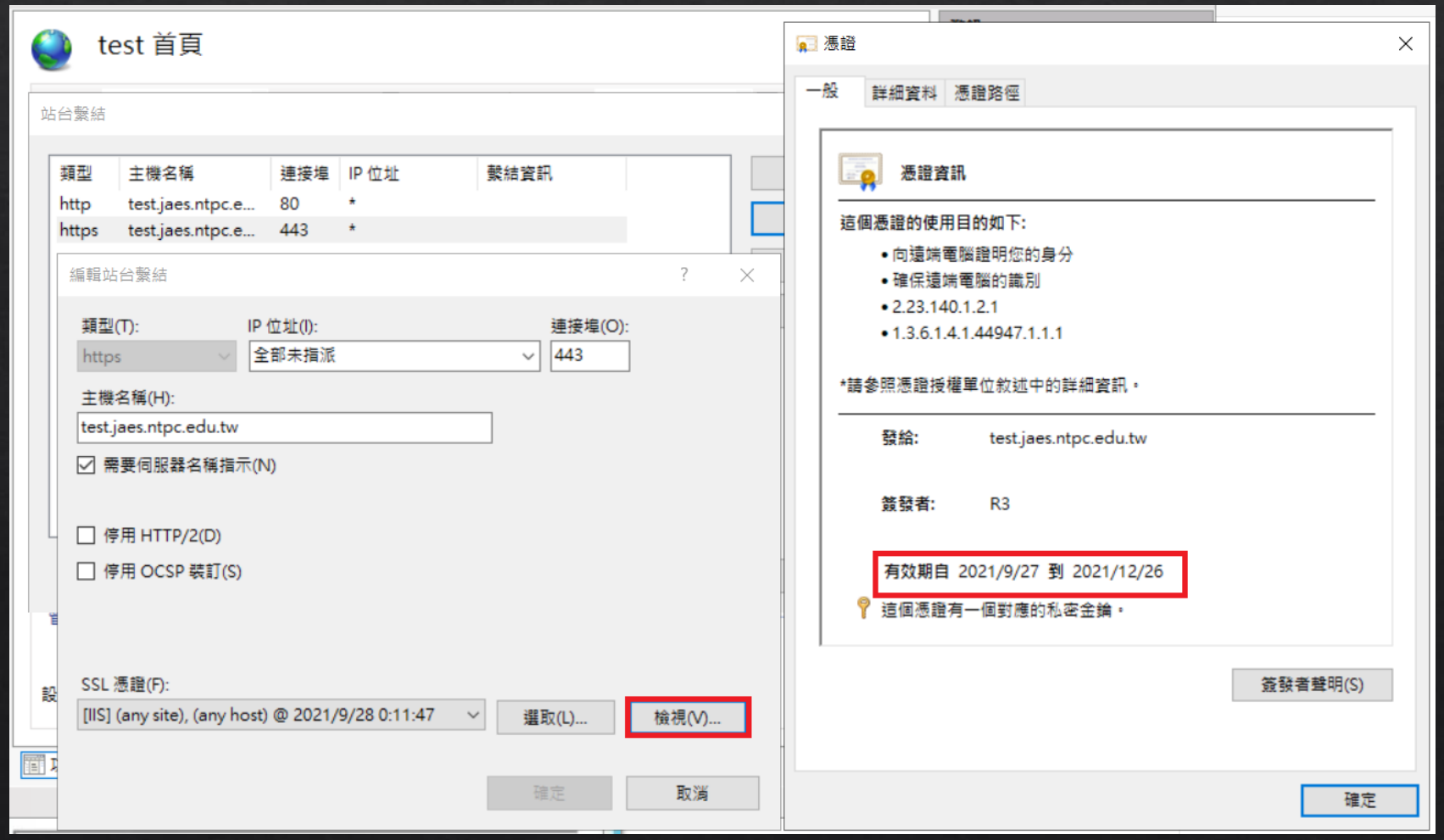
建立憑證完成

```
Continue with this selection? (y*/n) - yes

Target generated using plugin IIS: test.jaes.ntpc.edu.tw

Requesting certificate [IIS] test, (any host)
Store with CertificateStore...
Installing certificate in the certificate store
Adding certificate [IIS] test, (any host) @ 2021/9/28 0:01:19 to store WebHosting
Installing with IIS...
Updating existing https binding test.jaes.ntpc.edu.tw:443 (flags: 1)
Committing 1 https binding changes to IIS
Scheduled task looks healthy
Adding renewal for [IIS] test, (any host)
Next renewal scheduled at 2021/11/22 0:01:18
Certificate [IIS] test, (any host) created

N: Create certificate (default settings)
M: Create certificate (full options)
R: Run renewals (0 currently due)
A: Manage renewals (3 total)
O: More options...
Q: Quit

Please choose from the menu: Q
```

已安裝 SSL 憑證名稱


Internet Information Services (IIS) 管理員
GA-7VCSV ▸ 站台 ▸ test ▸
檔案(F) 檢視(V) 說明(H)
連線
起始網頁
GA-7VCSV (GA-7VCSV\Adm
應用程式集區
站台
jaestest
test
1
test 首頁
站台繫結
類型 主機名稱 連接埠 IP 位址 繫結資訊
http test.jaes.ntpc.e... 80 *
https test.jaes.ntpc.e... 443 *
3
新增(A)...
編輯(E)...
4
移除(R)
瀏覽(B)
關閉(C)
編輯站台繫結
類型(T): https
IP 位址(I): 全部未指派
連接埠(O): 443
主機名稱(H): test.jaes.ntpc.edu.tw
需要伺服器名稱指示(N)
停用 HTTP/2(D)
停用 OCSP 裝訂(S)
5
SSL 憑證(F): [IIS] (any site), (any host) @ 2021/9/28 0:11:47
選取(L)...
檢視(V)...
確定
取消
警訊
沒有建立預設的 SSL 站台。若要支援沒有 SNI 功能的瀏覽器，建議建立預設的 SSL 站台。
動作
瀏覽
編輯權限...
編輯站台
繫結...
2
基本設定...
檢視應用程式
檢視虛擬目錄
管理網站
重新啟動
啟動
停止
瀏覽網站
瀏覽 test.jaes.ntpc.edu.tw on *:80 (http)
瀏覽 test.jaes.ntpc.edu.tw on *:443 (https)
進階設定...
設定
限制...
HSTS...
說明
就緒

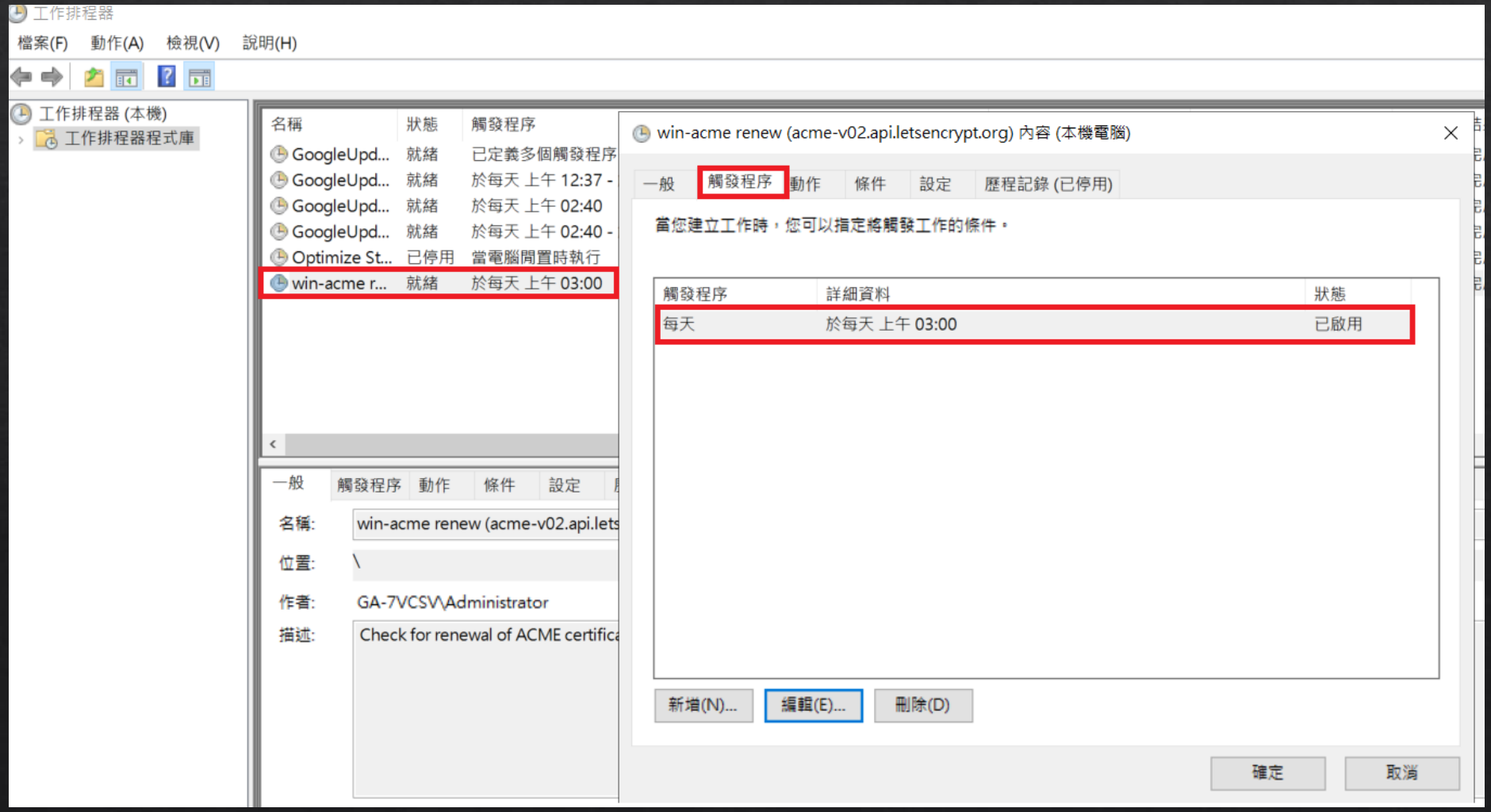
憑證資訊


test 首頁
站台繫結
類型 主機名稱 連接埠 IP 位址 繫結資訊
http test.jaes.ntpc.e... 80 *
https test.jaes.ntpc.e... 443 *
編輯站台繫結
類型(T):
https
IP 位址(I):
全部未指派
連接埠(O):
443
主機名稱(H):
test.jaes.ntpc.edu.tw
需要伺服器名稱指示(N)
停用 HTTP/2(D)
停用 OCSP 裝訂(S)
SSL 憑證(F):
[IIS] (any site), (any host) @ 2021/9/28 0:11:47
選取(L)...
檢視(V)...
確定
取消
憑證
一般
詳細資料
憑證路徑
憑證資訊
這個憑證的使用目的如下:
• 向遠端電腦證明您的身分
• 確保遠端電腦的識別
• 2.23.140.1.2.1
• 1.3.6.1.4.1.44947.1.1.1
*請參照憑證授權單位敘述中的詳細資訊。
發給: test.jaes.ntpc.edu.tw
簽發者: R3
有效期自 2021/9/27 到 2021/12/26
這個憑證有一個對應的私密金鑰。
簽發者聲明(S)
確定

工作排程器-排程更新


伺服器管理員
伺服器管理員 ▸ 儀表板
管理(M)
工具(T)
檢視(V)
說明(H)
儀表板
本機伺服器
所有伺服器
IIS
檔案和存放服務
歡迎使用伺服器管理員
快速入門(Q)
最新內容(W)
深入了解(L)
1 設定這部本機伺服器
2 新增角色及功能
3 新增其他要管理的伺服器
4 建立伺服器群組
5 將此伺服器連結到雲端服務
角色及伺服器群組
角色: 2 | 伺服器群組: 1 | 伺服器總數: 1
Internet Information Services (IIS) 管理員
iSCSI 啟動器
Microsoft Azure 服務
ODBC Data Sources (32-bit)
ODBC 資料來源 (64 位元)
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Windows Server Backup
Windows 記憶體診斷
工作排程器
元件服務
本機安全性原則
列印管理
系統設定
系統資訊
事件檢視器
具有進階安全性的 Windows Defender 防火牆

排程更新-設定每日更新時間



憑證過期提醒

Let's Encrypt certificate expiration notice for domain "jaestest.jaes.ntpc.edu.tw" (and 1 more) 收件匣 ×

Let's Encrypt Expiry Bot <expiry@letsencrypt.org> 取消訂閱 7月29日 週四 下午3:37

寄給 我

英文 › 中文（繁體） 翻譯郵件 關閉下列語言的翻譯功能：英文 ×

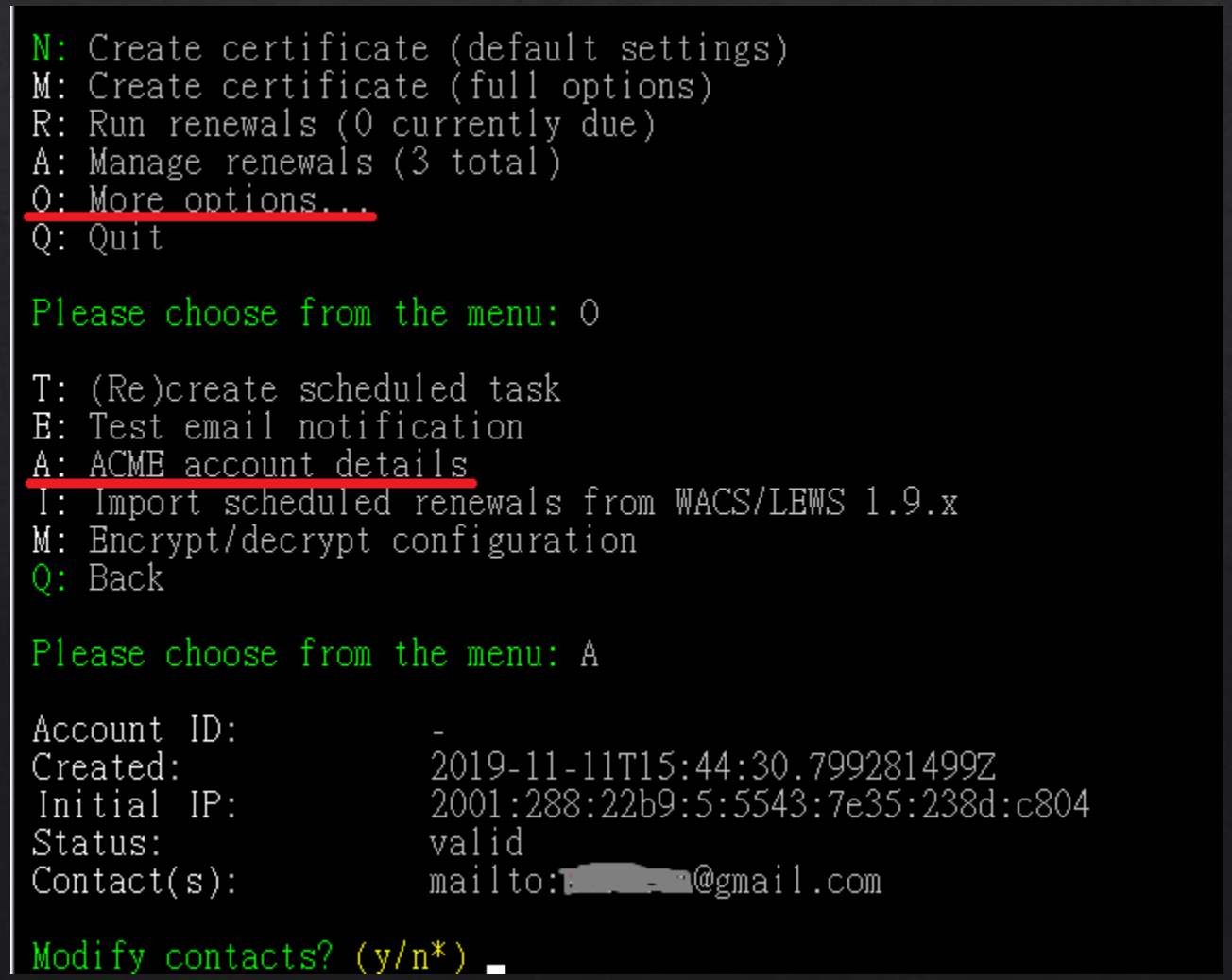
Hello,

Your certificate (or certificates) for the names listed below will expire in 18 days (on 16 Aug 21 14:21 +0000). Please make sure to renew your certificate before then, or visitors to your web site will encounter errors.

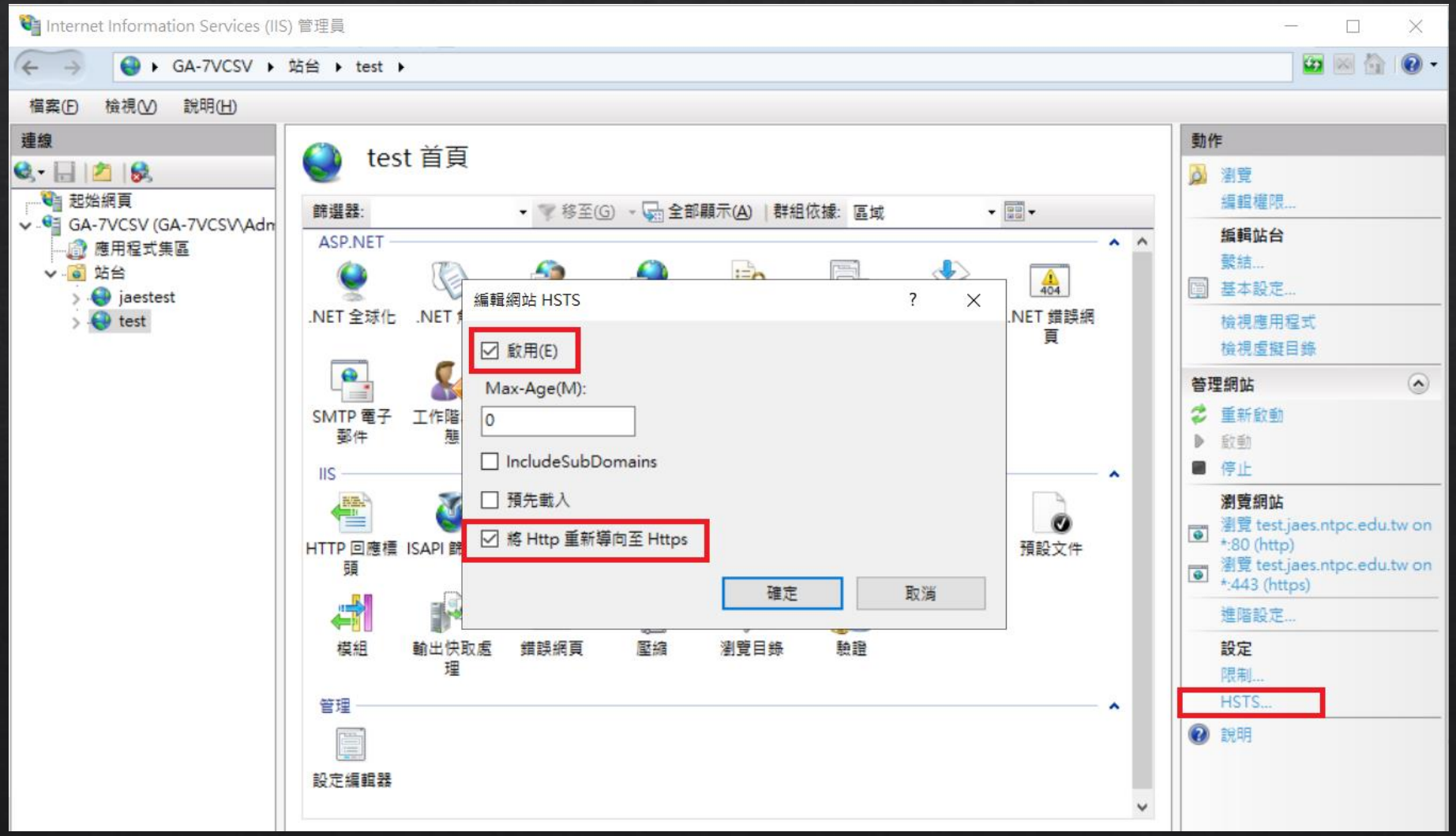
We recommend renewing certificates automatically when they have a third of their total lifetime left. For Let's Encrypt's current 90-day certificates, that means renewing 30 days before expiration. See https://letsencrypt.org/docs/integration-guide/ for details.

jaestest.jaes.ntpc.edu.tw
test.jaes.ntpc.edu.tw

設定聯絡資訊，接收提醒訊息

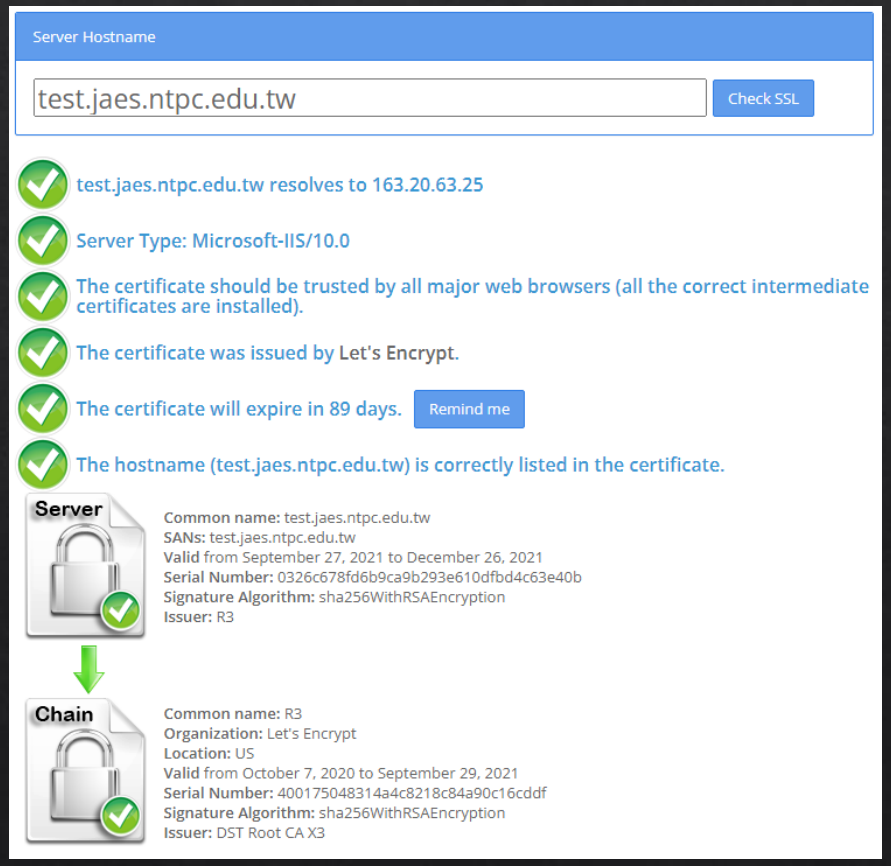


開啟HSTS，HTTP強制安全傳輸技術



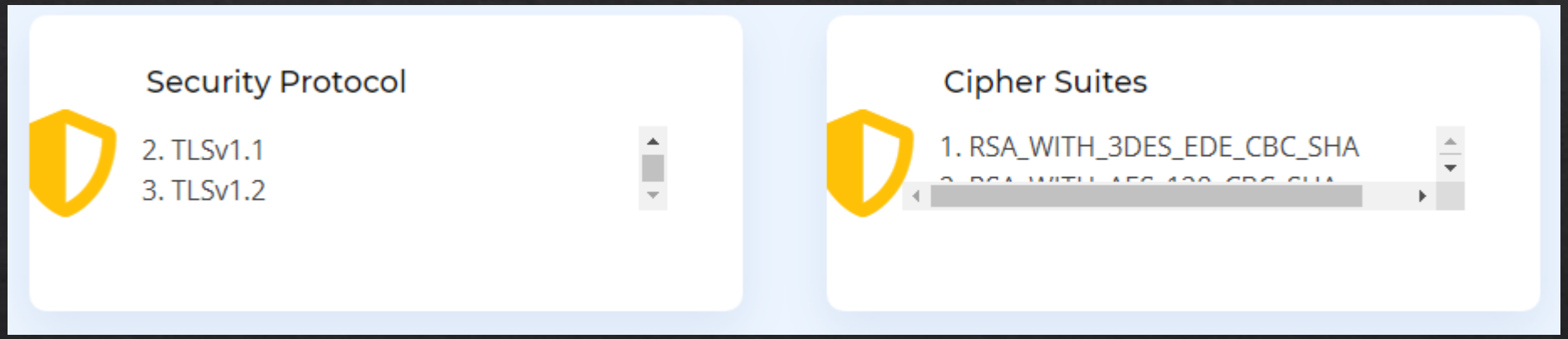
Certificate Chains 完整性檢測

- https://www.sslshopper.com/ssl-checker.html



Portocols 檢測（TLS應1.2以上）

- https://school.ntpc.edu.tw/test



HTTP重導向HTTPS

- 於瀏覽器輸入「http://網址」按Enter後能重導向「https://網址」。