

# 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)

25.	test	.jaes.ntpc.edu.tw	A	163.20.63.5	[刪除]
-----	------	-------------------	---	-------------	------

- ◆ 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](#)

WIN-  
ACME

A simple ACMEv2 client for Windows (for use with Let's Encrypt et al.)

DOWNLOAD  
2.1.18

# Windows Server IIS 站台繫結

The screenshot shows the Internet Information Services (IIS) Manager interface. The left-hand pane shows the server tree with 'GA-7VCSV' expanded to '網站', which is highlighted with a red box and the number '1'. The main pane displays a table of website bindings for the 'test' website. The 'test' binding is selected and highlighted with a red box and the number '2'. A '網站繫結' (Website Binding) dialog box is open, showing the configuration for the selected binding. The '類型' (Type) is 'http', the '主機名稱' (Host Name) is 'test.jaes.ntpc.edu.tw' (highlighted with a red box and the number '6'), and the '連接埠' (Port) is '80'. The '編輯(E)...' (Edit) button is highlighted with a red box and the number '5'. The '新增(A)...' (Add) button is highlighted with a red box and the number '4'. The '瀏覽(B)' (Browse) button is also visible. The right-hand pane shows the '警訊' (Alerts) section with a message '此站台有多個繫結' (This website has multiple bindings) and the '動作' (Actions) section with '繫結...' (Bindings...) highlighted with a red box and the number '3'. The '管理網站' (Manage Website) section shows '重新啟動' (Restart) and '瀏覽網站' (Browse Website) options.

Internet Information Services (IIS) 管理員

GA-7VCSV > 網站

檔案(F) 檢視(V) 說明(H)

連線

起始網頁

GA-7VCSV (GA-7VCSV\Adn

應用程式集區

網站 1

jaetest

test

網站

篩選器: 移至(G) 全部顯示(A) 群組依據: 沒有分組

名稱	識別碼	狀態	繫結	路徑
jaetest	2	已啟動 (http)	jaetest.jaes.ntpc.edu.tw on *...	C:\MVC\SchoolData
test	1	已啟動 (http)	test.jaes.ntpc.edu.tw on *:80 (...)	%SystemDrive%\inetpub\wwwroot

網站繫結

類型	主機名稱	連接埠	IP 位址	繫結資訊
http	test.jaes.ntpc.e...	80	*	

新增(A)...

編輯(E)... 5

刪除(R)

瀏覽(B)

編輯網站繫結

類型(T): http

IP 位址(I): 全部未指派

連接埠(O): 80

主機名稱(H): 6

test.jaes.ntpc.edu.tw

範例: www.contoso.com 或 marketing.contoso.com

警訊

此站台有多個繫結

動作

新增網站...

設定網站預設值...

編輯網站

繫結... 3

基本設定...

瀏覽

編輯權限...

移除

重新命名

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)

# 解壓縮檔案，移至適宜位置

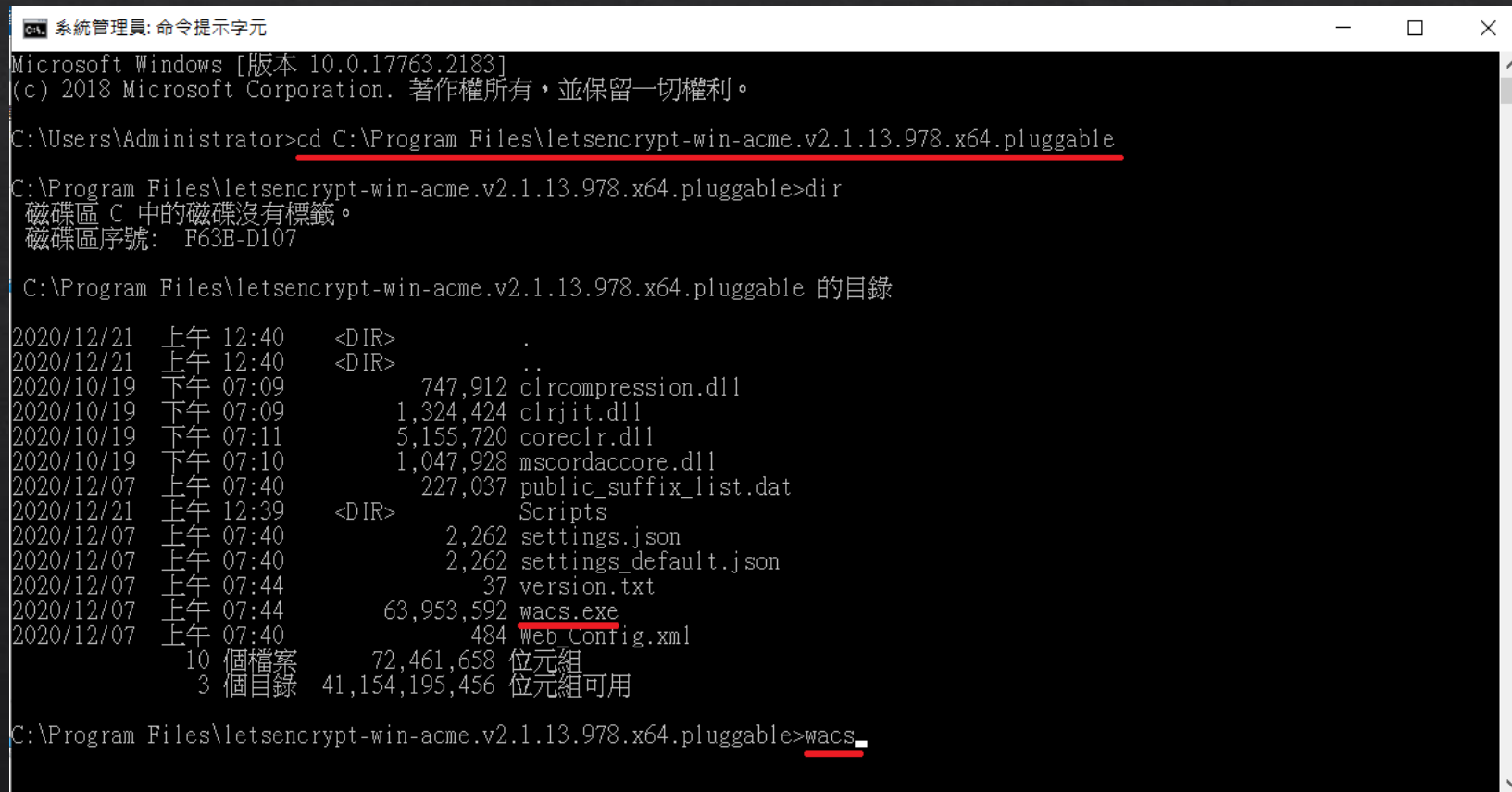
本機磁碟 (C:) > Program Files > letsencrypt-win-acme.v2.1.13.978.x64.pluggable >

名稱	修改日期	類型	大小
Scripts	2020/12/21 上午 ...	檔案資料夾	
clrcompression.dll	2020/10/19 下午 ...	應用程式擴充	731 KB
clrjit.dll	2020/10/19 下午 ...	應用程式擴充	1,294 KB
coreclr.dll	2020/10/19 下午 ...	應用程式擴充	5,035 KB
mscorlib.dll	2020/10/19 下午 ...	應用程式擴充	1,024 KB
public_suffix_list.dat	2020/12/7 上午 0...	DAT 檔案	222 KB
settings.json	2020/12/7 上午 0...	JSON File	3 KB
settings_default.json	2020/12/7 上午 0...	JSON File	3 KB
version.txt	2020/12/7 上午 0...	文字文件	1 KB
wacs.exe	2020/12/7 上午 0...	應用程式	62,455 KB
Web_Config.xml	2020/12/7 上午 0...	XML Document	1 KB



# 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



```
系統管理員: 命令提示字元
Microsoft Windows [版本 10.0.17763.2183]
(c) 2018 Microsoft Corporation. 著作權所有，並保留一切權利。

C:\Users\Administrator>cd C:\Program Files\letsencrypt-win-acme.v2.1.13.978.x64.pluggable

C:\Program Files\letsencrypt-win-acme.v2.1.13.978.x64.pluggable>dir
磁碟區 C 中的磁碟沒有標籤。
磁碟區序號: F63E-D107

C:\Program Files\letsencrypt-win-acme.v2.1.13.978.x64.pluggable 的目錄

2020/12/21 上午 12:40 <DIR> .
2020/12/21 上午 12:40 <DIR> ..
2020/10/19 下午 07:09          747,912 circompression.dll
2020/10/19 下午 07:09     1,324,424 clrjit.dll
2020/10/19 下午 07:11     5,155,720 coreclr.dll
2020/10/19 下午 07:10     1,047,928 mscordacore.dll
2020/12/07 上午 07:40       227,037 public_suffix_list.dat
2020/12/21 上午 12:39 <DIR> Scripts
2020/12/07 上午 07:40           2,262 settings.json
2020/12/07 上午 07:40           2,262 settings_default.json
2020/12/07 上午 07:44              37 version.txt
2020/12/07 上午 07:44     63,953,592 wacs.exe
2020/12/07 上午 07:40           484 Web_Config.xml
          10 個檔案          72,461,658 位元組
           3 個目錄     41,154,195,456 位元組可用

C:\Program Files\letsencrypt-win-acme.v2.1.13.978.x64.pluggable>wacs_
```

# N: Create certificate (default settings)

系統管理員: 命令提示字元 - wacs

```
C:\Program Files\letsencrypt-win-acme.v2.1.13.978.x64.pluggable>wacs
```

```
A simple Windows ACMEv2 client (WACS)  
Software version 2.1.13.978 (RELEASE, PLUGGABLE, 64-bit)  
ACME server https://acme-v02.api.letsencrypt.org/  
IIS version 10.0  
Running with administrator credentials  
Scheduled task looks healthy  
Please report issues at https://github.com/win-acme/win-acme
```

```
N: Create certificate (default settings)  
M: Create certificate (full options)  
R: Run renewals (0 currently due)  
A: Manage renewals (2 total)  
O: More options...  
Q: Quit
```

```
Please choose from the menu: N_
```

# 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

The screenshot shows the Internet Information Services (IIS) Manager interface. The left-hand tree view shows the server structure: GA-7VCSV > 網站 > test. The 'test' folder is highlighted with a red box and labeled '1'. The main pane displays the 'test 首頁' site configuration. A table of site bindings is shown:

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	*	

The 'https' row is highlighted with a red box and labeled '3'. To the right of the table, the '編輯(E)...' button is highlighted with a red box and labeled '4'. Below the table, the '編輯網站繫結' dialog box is open. In this dialog, the '類型(T):' dropdown is set to 'https', 'IP 位址(I):' is '全部未指派', and '連接埠(O):' is '443'. The '主機名稱(H):' field contains 'test.jaes.ntpc.edu.tw'. The '需要向服務名稱指示(N)' checkbox is checked. At the bottom of the dialog, the 'SSL 憑證(F):' dropdown is highlighted with a red box and labeled '5', showing the selected certificate: '[IIS] (any site), (any host) @ 2021/9/28 0:11:47'. The right-hand pane shows a warning message: '沒有建立預設的 SSL 網站。若要支援沒有 SNI 功能的瀏覽器，建議建立預設的 SSL 網站。' Below the warning, the '動作' section has the '繫結...' button highlighted with a red box and labeled '2'. The '管理網站' section shows the site status as '重新啟動' and '停止'. The '瀏覽網站' section shows links to view the site on port 80 (http) and port 443 (https).

# 憑證資訊

The image shows a Windows Internet Options dialog box with two overlapping windows. The background window is titled "test 首頁" and shows the "Content Advisor" tab. The foreground window is titled "憑證" (Certificates) and shows the "Certificates" tab. The "Certificates" window has three sub-tabs: "一般" (General), "詳細資料" (Details), and "憑證路徑" (Certificates Paths). The "一般" sub-tab is active and displays the following information:

**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

The "Content Advisor" window in the background shows the "網站繫結" (Content Advisor) section with a table of website connections:

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	*	

Below the table is the "編輯網站繫結" (Edit Content Advisor Settings) dialog box, which is partially visible. It shows the following settings:

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  
 需要同伺服器名稱指示(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)...

# 工作排程器-排程更新

The screenshot displays the Windows Server Management console. The title bar reads '伺服器管理員'. The main header shows '伺服器管理員 > 儀表板'. The left-hand navigation pane includes '儀表板', '本機伺服器', '所有伺服器', 'IIS', and '檔案和存放服務'. The main content area features a '歡迎使用伺服器管理員' section with a list of five tasks: 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, and 5. 將此伺服器連結到雲端服務. Below this is a '角色及伺服器群組' section with the text '角色: 2 | 伺服器群組: 1 | 伺服器總數: 1'. On the right, the '工具(T)' menu is open, listing various system tools, with '工作排程器' (Task Scheduler) highlighted.

伺服器管理員

伺服器管理員 > 儀表板

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

- 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

快速入門(Q)

最新內容(W)

深入了解(L)

角色及伺服器群組  
角色: 2 | 伺服器群組: 1 | 伺服器總數: 1

工具(T) 檢視(V) 說明(H)

- 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


The screenshot displays the Windows Task Scheduler interface. The main window shows a list of tasks, with 'win-acme r...' selected and highlighted in red. The task's details are shown in the right-hand pane, where the '觸發程序' (Triggers) tab is active. A table within this pane shows the trigger configuration: '每天' (Daily) at '於每天 上午 03:00' (At 03:00 every day), with a status of '已啟用' (Enabled). The '觸發程序' tab label is also highlighted in red.

名稱	狀態	觸發程序
GoogleUpd...	就緒	已定義多個觸發程序
GoogleUpd...	就緒	於每天 上午 12:37 -
GoogleUpd...	就緒	於每天 上午 02:40
GoogleUpd...	就緒	於每天 上午 02:40 -
Optimize St...	已停用	當電腦閒置時執行
win-acme r...	就緒	於每天 上午 03:00

觸發程序	詳細資料	狀態
每天	於每天 上午 03:00	已啟用

# 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 x



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](#) x

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](https://jaestest.jaes.ntpc.edu.tw)

[test.jaes.ntpc.edu.tw](https://test.jaes.ntpc.edu.tw)

# 設定聯絡資訊，接收提醒訊息

```
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: 0

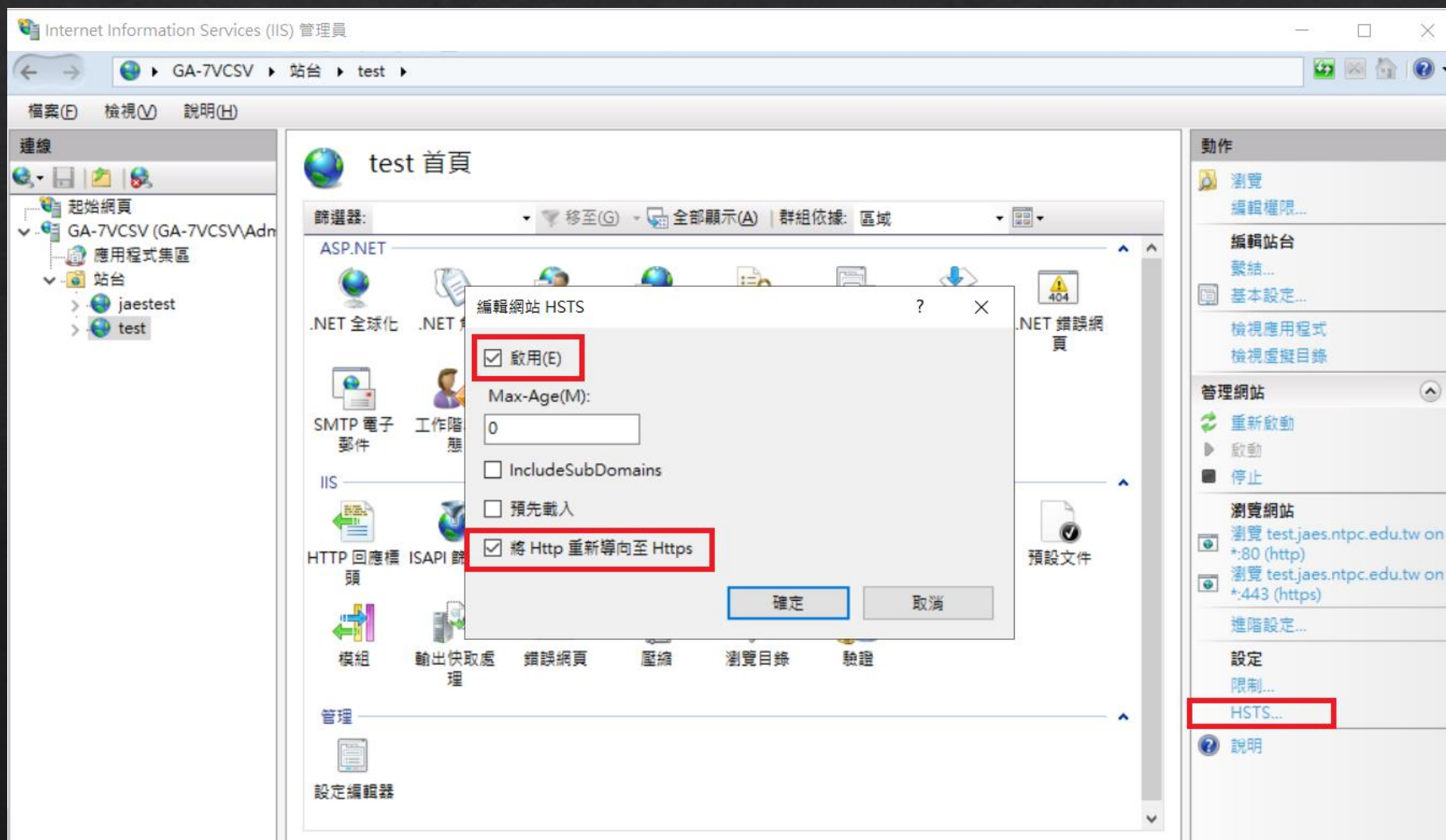
T: (Re)create scheduled task
E: Test email notification
A: ACME account details
I: Import scheduled renewals from WACS/LEWS 1.9.x
M: Encrypt/decrypt configuration
Q: Back

Please choose from the menu: A

Account ID:          -
Created:            2019-11-11T15:44:30.799281499Z
Initial IP:         2001:288:22b9:5:5543:7e35:238d:c804
Status:             valid
Contact(s):         mailto:██████████@gmail.com

Modify contacts? (y/n*) _
```

# 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>

Server Hostname

- ✓ test.jaes.ntpc.edu.tw resolves to 163.20.63.25
- ✓ Server Type: Microsoft-IIS/10.0
- ✓ The certificate should be trusted by all major web browsers (all the correct intermediate certificates are installed).
- ✓ The certificate was issued by Let's Encrypt.
- ✓ The certificate will expire in 89 days.
- ✓ The hostname (test.jaes.ntpc.edu.tw) is correctly listed in the certificate.


**Server**



Common name: test.jaes.ntpc.edu.tw  
SANs: test.jaes.ntpc.edu.tw  
Valid from September 27, 2021 to December 26, 2021  
Serial Number: 0326c678fd6b9ca9b293e610dfbd4c63e40b  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: R3

↓

**Chain**



Common name: R3  
Organization: Let's Encrypt  
Location: US  
Valid from October 7, 2020 to September 29, 2021  
Serial Number: 400175048314a4c8218c84a90c16cddf  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: DST Root CA X3



# Portocols 檢測 ( TLS應1.2以上 )

◇ <https://school.ntpc.edu.tw/test>



The screenshot displays two panels from a TLS test tool. The left panel, titled "Security Protocol", features a yellow shield icon and a list with two items: "2. TLSv1.1" and "3. TLSv1.2". The right panel, titled "Cipher Suites", also features a yellow shield icon and a list with two items: "1. RSA\_WITH\_3DES\_EDE\_CBC\_SHA" and "2. RSA\_WITH\_AES\_128\_CBC\_SHA". Both panels include a vertical scrollbar on the right side.

Security Protocol

2. TLSv1.1
3. TLSv1.2

Cipher Suites

1. RSA\_WITH\_3DES\_EDE\_CBC\_SHA
2. RSA\_WITH\_AES\_128\_CBC\_SHA

# HTTP重導向HTTPS

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

