中華電信 GlobalSign SSL/TLS 憑證（R46 根憑證）
Nginx 伺服器憑證簡易安裝教學（憑證鏈 Bundle 合併方式、ssl_certificate 設定）

2026/04/14 初版

> **⚠ Nginx 與 Apache 在安裝上的不同**
>
> Apache 可以將伺服器憑證和中繼憑證分開指定；Nginx 不支援獨立的中繼憑證檔案，必須將「伺服器憑證 + 中繼憑證」二者依序合併為一個 Bundle 檔案，才能透過 ssl_certificate 載入憑證。

開始前，請確認已取得以下四個檔案，建議將它們放在同一個資料夾以方便操作：

檔案名稱（範例）	說明	來源
private.key	產製 CSR 時所生成的伺服器私鑰	**自行保管**
[憑證序號].cer	中華電信核發的伺服器憑證	中華電信
CHTOVCA.crt	中華電信新中繼憑證	中華電信
rootr46.crt	GlobalSign R46 根憑證	中華電信

第一節　製作憑證鏈檔案（Certificate Bundle）

Nginx 須將以下兩個憑證依固定順序合併為單一的 certBundle.pem 檔案。合併順序一旦錯誤，瀏覽器將無法完整驗證憑證鏈。

方法 A　使用命令列指令合併

指令介面合併速度快、不易出錯，適合有終端機操作經驗的使用者。

▌Windows — 命令提示字元（CMD）

```
# 切換到憑證所在資料夾（請替換為實際路徑）
cd C:\cert

# 兩個憑證依序合併，產生 certBundle.pem
copy /b [憑證序號].cer + CHTOVCA.crt certBundle.pem
```

▌Linux / macOS — 終端機（Terminal）

```
# 切換到憑證所在資料夾（請替換為實際路徑）
cd /etc/ssl/certs

# 兩個憑證依序合併，產生 certBundle.pem
cat [憑證序號].cer CHTOVCA.crt > certBundle.pem
```

☑ 驗證

合併完成後，請使用文字編輯器開啟 certBundle.pem 確認：
檔案內應包含兩個以下區塊，

```
-----BEGIN CERTIFICATE-----
 . . . . . .
-----END CERTIFICATE-----
```

且編碼方式為 UTF-8（無 BOM）

方法 B　使用文字編輯器手動合併

若無法使用命令列，可改以記事本（或 VS Code、Notepad++）手動貼上合併。

1. 建立一個新的空白純文字檔案，命名為 certBundle.pem。

2. 用記事本分別開啟下列兩個憑證檔案：

   [憑證序號].cer、**CHTOVCA.crt**。

   🖼 開啟方法請參考附件圖 1。

3. 依照下列順序貼入內容，將兩個檔案的全部內容複製貼上 certBundle.pem。

   ① [憑證序號].cer 全文內容（含 BEGIN / END CERTIFICATE 行）。

   ② CHTOVCA.crt 全文內容（含 BEGIN / END CERTIFICATE 行）。

   🖼 certBundle.pem 複製貼上的順序請參考附件圖 2。

4. 另存新檔時，請確認：

   - 編碼選擇「UTF-8」（非 UTF-8 BOM）
   - 檔名輸入 certBundle.pem（含副檔名，勿存成 .txt）
   - 如果無法直接存成 .pem 檔案，可以先存成 .txt 檔案，再用重新命名的方式修改副檔名。

合併後的檔案內部結構應如下所示：

certBundle.pem 結構示意

```
-----BEGIN CERTIFICATE-----
（[憑證序號].cer 的憑證內容）      ← 伺服器憑證，必須排第一
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
（CHTOVCA.crt 的憑證內容）        ← 中繼憑證，排第二
-----END CERTIFICATE-----
```

⚠ 合併順序錯誤的情況

如果貼上順序不正確（例如將中繼憑證排在伺服器憑證前面），Nginx 啟動時可能不會報錯，但瀏覽器會顯示「憑證不受信任」或「憑證鏈不完整」警告。

第二節　修改 Nginx 設定檔

完成製作 certBundle.pem 後，需修改 Nginx 設定檔，讓伺服器知道新的 Bundle 憑證鏈和私鑰的存放位置。

1. 開啟 Nginx 設定檔：

   常見位置：/etc/nginx/nginx.conf、/etc/nginx/conf.d/default.conf 或 nginx 安裝目錄/conf/nginx.conf。

2. 找到 `listen 443 ssl` 的 server 區塊。

3. 確認 **server_name** 後面的值是您要安裝憑證的網站網址（FQDN）。

4. 依照下方範例，設定或更新以下兩行憑證有關路徑：

nginx.conf 設定範例

```
server {
    listen                443 ssl;
    server_name           www.example.com;  # 替換成實際網站網址

    # 憑證鏈 Bundle（第一節製作的合併檔案）
    ssl_certificate       ssl/certs/certBundle.pem;

    # 對應私鑰（自行保管）
    ssl_certificate_key   ssl/private/private.key;

    ...  # 其餘設定不變
}
```

Nginx 指令	後面輸入的路徑內容
`ssl_certificate`	第一節製作的 certBundle.pem
`ssl_certificate_key`	產製 CSR 時的原始私鑰 private.key

⚠ 設定檔語法檢測

修改完成後，可執行下列指令測試設定檔語法是否正確，確認無誤後再執行重啟，避免服務中斷：

```
nginx -t
```

第三節　重新啟動 Nginx

設定檔確認無誤後，重啟（或重新載入）Nginx 讓新憑證生效。

選項 A　重新載入設定（不中斷服務，建議）

Reload 指令不會終止現有連線，適合正式環境使用。

Reload 指令

```
# 通用指令（Windows 要在 nginx 資料夾下操作）
nginx -s reload

# Linux（systemd）
sudo systemctl reload nginx

# Linux（較舊系統）
sudo service nginx reload
```

選項 B　完整重啟

若執行 Reload 後憑證仍未更新，可改用完整重啟。

Restart 指令

```
# Linux（systemd）
sudo systemctl restart nginx

# Linux（較舊系統）
sudo service nginx restart
```

```
# Windows（沒有 restart 指令，只能先關閉再啟動）
## Windows 要在 nginx 資料夾下操作
nginx -s quit
start nginx
```

☑ 驗證

重啟後，以瀏覽器造訪 *https://您的網站網址*，點選網址列左端圖示查看網站資訊。

憑證階層應顯示：

GlobalSign R46 Root CA
  Chunghwa Telecom GCC R46 OV TLS CA 2025
    伺服器憑證的 CN

也可使用 SSL Labs（https://ssllabs.com/ssltest）進行線上完整驗證。

附錄　Nginx 設定檔常見路徑

作業系統	nginx.conf 設定檔路徑
Ubuntu / Debian	`/etc/nginx/nginx.conf` （站台設定：`/etc/nginx/sites-available/default`）
CentOS / RHEL / Fedora	`/etc/nginx/nginx.conf` （站台設定：`/etc/nginx/conf.d/default.conf`）
macOS Homebrew（Intel）	`/usr/local/etc/nginx/nginx.conf`
macOS Homebrew（Apple Silicon）	`/opt/homebrew/etc/nginx/nginx.conf`
Windows（官方發行版）	`nginx 安裝目錄\conf\nginx.conf`
自行編譯安裝	`/usr/local/nginx/conf/nginx.conf`
Docker（官方映像檔）	`/etc/nginx/nginx.conf`（容器內路徑）

若不確定設定檔路徑，可執行以下指令讓 Nginx 自行回報：

快速確認設定檔位置

```
# 顯示 Nginx 版本、作業系統資訊與預設設定檔路徑
nginx -V
# 輸出範例：尋找類似 --conf-path=/etc/nginx/nginx.conf 的字串。

# 或者使用檢查語法的指令
nginx -t
# 輸出範例：nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
```

⚠ include 引用外部組態

許多 Linux 發行版的 nginx.conf 會以 include 方式引用 conf.d/*.conf 或 sites-enabled/*。
若在 nginx.conf 中找不到 ssl_certificate 設定，請查看 include 所引用的外部組態檔案，搜尋檔案內的 SSL 設定有關指令。

附件　操作範例圖

圖 1　記事本開啟憑證檔案

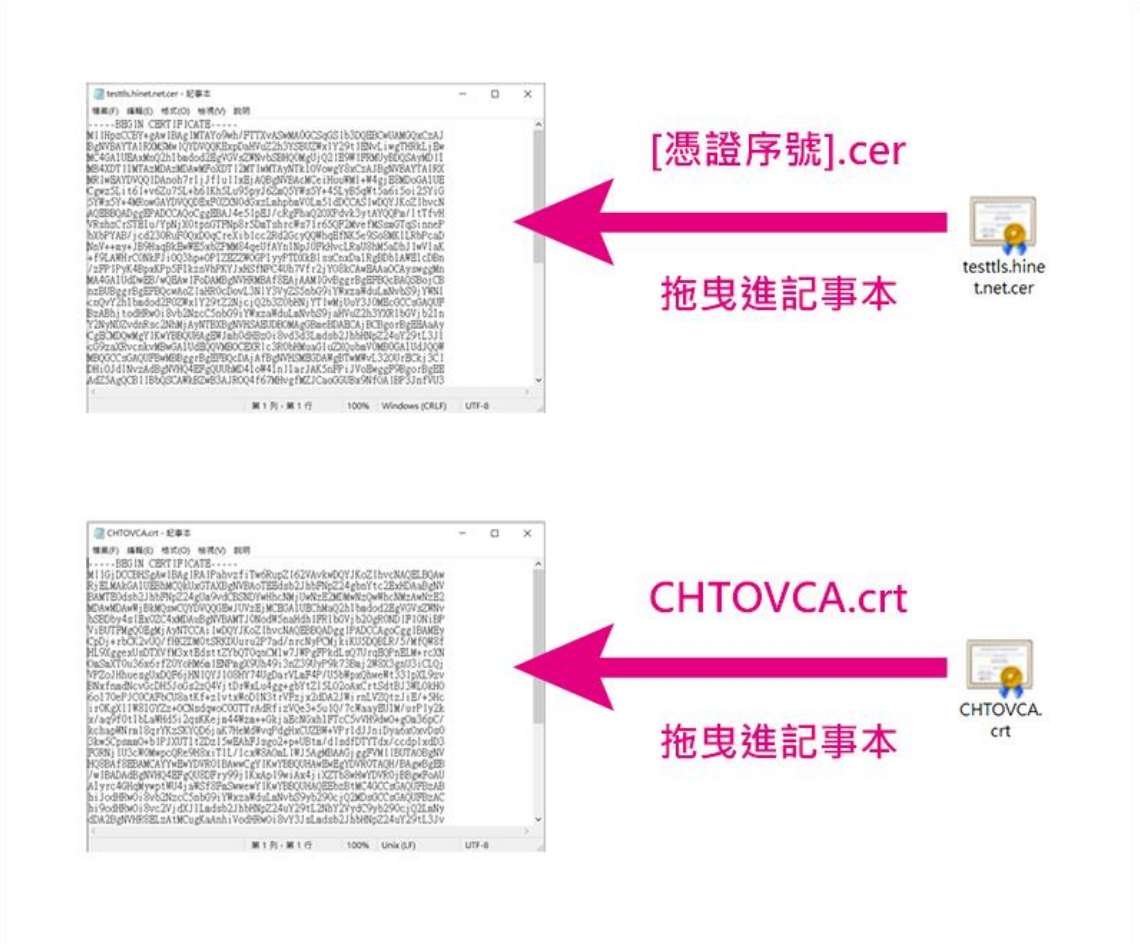

圖 2　certBundle.pem 複製貼上的順序