

網站導入 https 使用 letsencrypt 簽發憑證方式
以 Ubuntu22.04 及 Nginx 且未簽發過安全憑證的網站為例

- **SSH 進入網頁伺服器主機**

SSH 作為具有 sudo 特權的用戶進入運行 HTTP 網站的主機。

- **安裝 snapd**

您需要安裝 snapd, 並確保按照任何說明啟用 snap

請依照以下說明 skapcraft 的站點以安裝 snapd。

安裝 snapd

```
sudo apt update
```

```
sudo apt install snapd
```

請先刪除 certbot-auto 和任何 Certbot OS 軟件包

```
sudo apt-get remove certbot
```

```
或 sudo dnf remove certbot
```

```
或 sudo yum remove certbot
```

- **安裝 Certbot**

在主機上執行以安裝 Certbot。

```
sudo snap install --classic certbot
```

選擇您想如何運行 Certbot 獲取並安裝您的證書...

執行此命令以獲取證書, 並讓 Certbot 自動編輯您的 nginx 配置以提供服務, 只需一步即可打開 HTTPS 訪問權限。

```
Sudo certbot --nginx
```

- **測試自動續訂**

系統上的 Certbot 軟件包帶有 cron 作業或 systemd 計時器, 它將在證書過期之前自動更新。除非更改配置, 否則無需再次運行 Certbot。您可以通過運行以下命令來測試證書的自動續訂:

```
sudo certbot renew --dry-run
```

- **憑證續簽發**

基本上憑證一次是三個月，所以每個月 renew 一次就好了

在 crontab 中加入 以下規則

```
0 0 1 * * certbot renew
```

- **確認 Certbot 有效**

要確認您的網站設置正確, 請瀏覽 <https://您的網站/> 在瀏覽器中, 並在 URL 欄中查找鎖頭圖標。

- **您可以依照單位內網頁伺服器主機系統版本及網頁服務套件簽發網頁安全憑證。**

- certbot 官方網站 <https://certbot.eff.org/> ,