RHEL / CentOS 7 安裝 Let's Encrypt

說明：本文說明如何在 Apache 伺服器上安裝免費的憑證(Let's Encrypt)，提供 HTTPS 的安全加密網頁。Let's Encrypt 是由各大非營利團體為了推廣 HTTPS 而推出免費 SSL/TLS 憑證服務。

操作步驟

◎需先有合法 domain name 如: yourdomain.ntnu.edu.tw 網域名稱(Domain Name)申請表下載

將 Let's Encrypt 配置到 Apache 的方法。

1. 先安裝 git 及 EPEL repo:

```
# yum install git epel-release
```

2. 安裝 Let’s encrypt 所需套件:

```
# yum install gcc libffi-devel python-devel openssl-devel
```

3. 然後下載 Let’s encrypt:

```
# cd /root
# git clone https://github.com/letsencrypt/letsencrypt
```

4. 這時系統會將 Let’s encrypt 的最新檔案下載到 /root/letsencrypt, 執行以下 script SSL certificate:

```
# cd /root/letsencrypt
# ./letsencrypt-auto certonly -a standalone -d yourdomain.ntnu.edu.tw
```

5. Let’s encrypt 會將憑證檔案放到 /etc/letsencrypt/live/.

6. 接著可以配置 Apache, 先安裝 mod_ssl:

```
# yum install mod_ssl
```

7. 建立目錄結構：

```
# mkdir /etc/httpd/sites-available
# mkdir /etc/httpd/sites-enabled
# vim /etc/httpd/conf/httpd.conf
```

最後一行加入 IncludeOptional sites-enabled/*.conf

8. 建立一個新的虛擬主機檔案：

```
# vim /etc/httpd/sites-enabled/yourdomain.ntnu.edu.tw.conf
```

然後開啟儲存 VirtualHost 設定的檔案，例如 /etc/httpd/sites-enabled/ yourdomain.ntnu.edu.tw，在檔案內應該已經有 VirtualHost 的 HTTP (埠號 80) 的設定，加入 HTTPS (埠號 443) 的設定

```
<VirtualHost *:443>
ServerName yourdomain.ntnu.edu.tw
DocumentRoot /var/www/
ErrorLog /var/log/httpd/ yourdomain.ntnu.edu.tw /error.log
CustomLog /var/log/httpd/ yourdomain.ntnu.edu.tw /access.log combined
        SSLEngine on
        SSLCertificateFile /etc/letsencrypt/live/ yourdomain.ntnu.edu.tw /cert.pem
        SSLCertificateKeyFile /etc/letsencrypt/live/ yourdomain.ntnu.edu.tw /privkey.pem
        SSLCertificateChainFile /etc/letsencrypt/live/ yourdomain.ntnu.edu.tw/chain.pem
</VirtualHost>
```

9. Enabling the Virtual Host

```
# ln -s /etc/httpd/sites-available/yourdomain.ntnu.edu.tw    /etc/httpd/sites-enabled/yourdomain.ntnu.edu.tw
```

10. 重新啟動 Apache:

```
# systemctl restart httpd
```

11. 最後可以透過存取 HTTPS 頁面測試是否成功配置，
例如: “https:// yourdomain.ntnu.edu.tw” .

12. 設定定期更新憑證：

建立一 batch/shell script 檔案：如 vim /root/auto-renew.sh 內容如下

```
#!/bin/sh
#
# Use for Let's encrypt renew (suggest 60days, expired every 90days)

# Use official client (slow!)
cd /root/ssl/letsencrypt/
./letsencrypt-auto certonly -d yourdomain.ntnu.edu.tw --renew-by-default

#reload new cert into httpd
service httpd reload
```

13. 編輯 crontab －e ※例如:自某月 1 日起，每 2 個月(凌晨 00:00 分)執行一次 renew

```
0 0 1 */2 * /root/auto-renew.sh >> /root/le-renew.log
```

14. 測試憑證有效期限是否正確：

```
https://www.ssllabs.com/ssltest/analyze.html?d= yourdomain.ntnu.edu.tw &latest
```