

HTTPS 憑證安裝 Apache

臺灣大學計資中心
網路組
游子興

大綱

- * Install apache
- * Enable SSL Module
- * Create Private Key and CSR
- * 若私鑰有設定密碼

Apache 安裝 HTTPS

Ubuntu

- * Install Apache

- * sudo apt install apache2

- * Enable SSL Module

- * a2enmod ssl
 - * ln -s /etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-enabled/000-default-ssl.conf
 - * nano /etc/apache2/sites-enabled/000-default-ssl.conf

```
# A self-signed (snakeoil) certificate can be created by installing
# the ssl-cert package. See
# /usr/share/doc/apache2/README.Debian.gz for more info.
# If both key and certificate are stored in the same file, only the
# SSLCertificateFile directive is needed.
#SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
#SSLCertificateKeyFile   /etc/ssl/private/ssl-cert-snakeoil.key
SSLCertificateFile /etc/letsencrypt/live/tanet2020.tp1rc.edu.tw/fullchain.pem
SSLCertificateKeyFile /etc/letsencrypt/live/tanet2020.tp1rc.edu.tw/privkey.pem
```

- * systemctl restart apache2

Apache 安裝 HTTPS CentOS

- * Install SSL Module
 - * yum install mod_ssl
 - * vi /etc/httpd/conf.d/ssl.conf
- * systemctl restart httpd

```
# Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate. If
# the certificate is encrypted, then you will be prompted for a
# pass phrase. Note that a kill -HUP will prompt again. A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/pki/tls/certs/certificate.crt

# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/pki/tls/private/private.key

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convenience.
#SSLCertificateChainFile /etc/pki/tls/certs/server-chain.crt

# Certificate Authority (CA)
# Set the CA certificate verification path where to find CA
# certificates for client authentication or alternatively one
# huge file containing all of them (file must be PEM encoded)
SSLCACertificateFile /etc/pki/tls/certs/ca-bundle.crt
```

建議設定, 否則 Line Webhook 過不了

SSL Config for Apache

- * SSLCertificateKeyFile
/etc/letsencrypt/live/www.tp1rc.edu.tw/privkey.pem
- * Method1
 - * SSLCertificateFile /etc/letsencrypt/live/www.tp1rc.edu.tw/fullchain.pem
- * Method2
 - * SSLCertificateFile /etc/letsencrypt/live/www.tp1rc.edu.tw/cert.pem
 - * SSLCertificateChainFile /etc/letsencrypt/live/www.tp1rc.edu.tw/chain.pem
- * Apache \geq 2.4.8
 - * Method1 or Method2
- * Apache $<$ 2.4.8
 - * Method2 Only

安裝 HTTPS 前後

* 安裝前: netstat -lnp

```
[root@localhost ~]# netstat -lnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1026/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      1234/master
tcp6       0      0 :::80                  :::*                    LISTEN      1411/httpd
tcp6       0      0 :::22                  :::*                    LISTEN      1026/sshd
tcp6       0      0 :::1:25                 :::*                    LISTEN      1234/master
udp        0      0 0.0.0.0:68             0.0.0.0:*               841/dhclient
udp        0      0 0.0.0.0:37179          0.0.0.0:*               841/dhclient
udp6       0      0 :::26369                :::*                    841/dhclient
raw6       0      0 :::58                   :::*                    7          720/NetworkManager
```

* 安裝後:

```
[root@localhost conf.d]# netstat -lnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1026/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      1234/master
tcp6       0      0 :::80                  :::*                    LISTEN      1513/httpd
tcp6       0      0 :::22                  :::*                    LISTEN      1026/sshd
tcp6       0      0 :::1:25                 :::*                    LISTEN      1234/master
tcp6       0      0 :::443                  :::*                    LISTEN      1513/httpd
udp        0      0 0.0.0.0:68             0.0.0.0:*               841/dhclient
udp        0      0 0.0.0.0:37179          0.0.0.0:*               841/dhclient
udp6       0      0 :::26369                :::*                    841/dhclient
raw6       0      0 :::58                   :::*                    7          720/NetworkManager
```

Create Private Key and CSR

Create Private Key

- * RSA 2048bit, PEM Format

- * 不加密

- * ~# openssl genrsa -out private.key 2048

- * 3-DES 加密

- * ~# openssl genrsa -des3 -out private.key 2048

- * Enter PEM pass phrase: -- 需記此密碼，每次啟動 httpd 均會用到

- * Verify password -- Enter PEM pass phrase:

使用私鑰產生憑證申請檔 CSR


- * ~\$ openssl req -new -key private.key -out server.csr
 - * Enter PEM pass phrase: -- 輸入 Private Key 密碼
- * 輸入基本資料
 - * Country Name (2 letter code) [GB]:TW
 - * State or Province Name (full name) [Berkshire]:Taiwan
 - * Locality Name (eg, city) [Newbury]:Taipei
 - * Organization Name (eg, company) [My Company Ltd]:NTU
 - * Organizational Unit Name (eg, section) []:CC
 - * Common Name (eg, your name or your server's hostname) []:www.tp1rc.edu.tw
 - * Email Address []:davisyou@ntu.edu.tw
 - *
 - * Please enter the following 'extra' attributes
 - * to be sent with your certificate request
 - * A challenge password []: 直接 Enter
 - * An optional company name []: 直接 Enter

憑證申請檔

Certificate Signing Request

* server.csr

```
-----BEGIN CERTIFICATE REQUEST-----
MIICzDCCAbQCAQAwgYYxCzAJBgNVBAYTA1RXMQwwCgYDVQQIDANOVFUxCzAJBgNV
BACMAkNDMQwwCgYDVQQKDANOVFUxCzAJBgNVBAsMAkNDMROwGwYDVQQDDBRkYXZp
c3lvdS5idWRhLmlkdi50dzEiMCAGCSqGSIb3DQEJARYTZGF2aXN5b3VAbnR1LmVk
dS50dzCCASlwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOjd4itAqajinx0g
bp0cvKLEGvdDsgEaxLOaR9B1Rdc2byVNHU+gzbn0phBrfSSk6bxTKXRUqyuphLlo
dkZISHoN8Y1I6mdYBfR8P/dm8DxK6UePcYMs6Ch+8zvlqPhmTRi5oxJ/Y7ZBLIQc
t00k04NV05bQr83GD++xXKxobQQE+qAGa0rXsA1XyCc8inX5w09xT9VksmUGC4Gd
vpr2sK1fgCw8oxMya9zVfdH+DpJfqnlKk+6k5mcCJyQRNGAi3pFrrOeqXE32vyE4
Ot0QEpwR9zgqMbLceRIrJlFzHYqZS4J/vfhF7N71gw7H9ayr1TgteWx/JGURM1Sc
I5RB2Z8CAwEAAaAAMAQGCSqGSIb3DQEBCwUAA4IBAQBxKFRxqTK/4u4MADOmIeB6
+1CX9Z0tkaLCk3JELWhD/Ifn8OqaRrpqIx47ZmaNpmD3ng4eR8VbaEEbuQx0/MQm
EzXMKUkgnDhAoM58IK3MjX4Ktsag2Y8jznoQijapmevTZ9PAS/I tKNNR0qMF0eV2
AihPJXEwr3Y/U+BhAE9SUs5P33LoMEKPD9+5gE1KXda3lFhlzH2gDiYDzWkwIj2a
11NbX+BCUYxIY4s1Sc/2bJzqu3ynrx+14MUeBDkkJgktNFbFRvPm8kWaxtHkgd22
2CmONbjQ3toUUNo59EcVdlptv8SPG9S5yrVPkBTvNEyyTUuoAARF9m8UjK/uxrej
-----END CERTIFICATE REQUEST-----
```



若私鑰有設定密碼

若私鑰有設定密碼

- * 重啟 apache 需輸入私鑰密碼

```
[root@davisyoucc ~]# systemctl start httpd
Enter SSL pass phrase for davisyoucc.ntu.edu.tw:443 (RSA) : ****
```

- * reboot 後 apache 未輸入密碼無法啟動

```
[root@davisyoucc ~]# systemctl status httpd
■ httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: activating (start) since Wed 2018-05-02 09:55:54 CST; 26s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 911 (httpd)
    CGroup: /system.slice/httpd.service
            └─ 911 /usr/sbin/httpd -DFOREGROUND
               1181 /bin/systemd-ask-password Enter SSL pass phrase for davisyoucc.ntu.edu.tw:443 (...

May 02 09:55:54 davisyoucc.ntu.edu.tw systemd[1]: Starting The Apache HTTP Server...
```

Apache 重啟自動輸入私鑰密碼

- * 私鑰密碼輸入方式

```
# Pass Phrase Dialog:  
# Configure the pass phrase gathering process.  
# The filtering dialog program ('builtin' is a internal  
# terminal dialog) has to provide the pass phrase on stdout.  
SSLPassPhraseDialog exec:/usr/libexec/httpd-ssl-pass-dialog
```

- * /etc/httpd/conf.d/ssl.conf -- CentOS

- * /etc/apache2/mods-enabled/ssl.conf -- Ubuntu 18.04

- * SSLPassPhraseDialog

- * builtin -- CentOS 6

- * exec:/usr/libexec/httpd-ssl-pass-dialog -- CentOS 7

- * exec:/usr/share/apache2/ask-for-passphrase -- Ubuntu 18.04

- * exec:/root/apache_pass.sh -- 設定自動輸入密碼


- * /root/apache_pass.sh 內容

- ```
#!/bin/sh
```

- ```
echo "123456"
```

- ```
chmod +x /root/apache_pass.sh
```

---



簡報完畢  
謝謝