?? vsftpd ?? SSL ????

?? CA ???

??????????(Self-Signed)

mkdir /etc/vsftpd/cert

openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/vsftpd/cert/mydomain.key -out /etc/vsftpd/cert/mydomain.crt

NOTE:

> ??????????????????????????????????:
> Country Name: TW ??
> State or Province Name: TAIWAN ?/??
> Locality Name: Taoyuan ??
> Organization Name: Your Company Corp. ???
> Organization Unit Name: IT ????????
> Common Name: your.domain.name ?? (*???*)

????????????? TWNCA

?? Linux ????????

1. mydomain.key ??????
2. mydomain.csr ???????

openssl genrsa -out /etc/vsftpd/cert/mydomain.key 2048
openssl req -new -key /etc/vsftpd/cert/mydomain.key -out /etc/vsftpd/cert/mydomain.csr

NOTE:

> ?????????????
> Country Name: TW ??
> State or Province Name: TAIWAN ?/??
> Locality Name: Taoyuan ??
> Organization Name: Your Company Corp. ???
> Organization Unit Name: IT ????????
> Common Name: your.domain.name ?? (*???*)

????? mydomain.csr ??? TWCA ??????????????????????????? Email ??????????????????

> TWCA ?????????????
> - root.crt ????

- server.crt ??????
- uca_1.crt ????#1?
- uca_2.crt ????#2?

?????????????

#> cat server.crt

-----BEGIN CERTIFICATE-----
MIIFNjCCBB6gAwIBAgIQR+AAAAAANxpF4wYFvl5COzANBgkqhkiG9w0BAQsFADBv
MQswCQYDVQQGEwJUVzESMBAGA1UEChMJVEFJV0FOLUNBMRowGAYDVQQLExFTZWN1
cmUgU1NMIFN1Yi1DQTEwMC4GA1UEAxMnVFdDQSBTZWN1cmUgU1NMIENlcnRpZmlj
...
KiZDoZe0ziN7Usrzb5CNgzZj9tP09KPF8wepQlMWOu5lHb84IroCHaAhb56zbwmy
4TU/SwImtZT5L+j68W3AhqeYX7u42lscl/Qda7b/nES/lcN8yH9y7zKP6PriCP9A
np13mawkqJi34dkoFobJ9tqitigMRs82dcMVVzbBEUK8e4e7pYoLe0iP
-----END CERTIFICATE-----

#> openssl x509 -noout -text -in server.crt

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      47:e0:00:00:00:00:37:1a:45:e3:06:05:be:5e:42:3b
    Signature Algorithm: sha256WithRSAEncryption *??: Issuer ????????*
    Issuer: C=TW, O=TAIWAN-CA, OU=Secure SSL Sub-CA, CN=TWCA Secure SSL Certification Authority
    Validity
      Not Before: Jan 28 09:48:26 2016 GMT *??: ??????*
      Not After : Jan 28 15:59:59 2019 GMT
    Subject: C=TW, ST=TAIWAN, L=Taoyuan, O=Your Company Corp., OU=IT, CN=your.domain.name
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          00:a7:6c:96:42:5c:84:ca:ee:82:1d:de:49:5e:d5:
          d6:37:2b:78:5f:48:57:df:55:33:84:06:9a:49:af:
          d5:ca:0f:bf:44:e1:0c:c6:af:17:8f:e6:0c:19:34:
          ed:7b:6c:26:02:03:38:f1:af:2e:70:0c:3d:d9:0a:
          71:78:26:fb:9f:75:5e:34:c4:6e:0c:44:74:99:40:
          19:60:41:fb:dd:71:0f:fe:2f:82:34:cf:9d:a0:08:
          ...
          a6:ee:b9:3e:24:4a:af:c5:62:7f:1b:8a:03:a9:37:
          83:45:43:be:b4:cc:ac:0a:54:62:89:0e:f3:74:10:
          71:b9:1c:1f:47:00:ba:3d:43:f5:32:51:b2:99:e1:
          4f:65
        Exponent: 65537 (0x10001)
    X509v3 extensions:

```
        X509v3 Authority Key Identifier:
          keyid:F8:07:C2:68:24:FF:85:95:CB:DB:1E:E3:33:9C:2A:4F:97:20:56:7B

        X509v3 Subject Key Identifier:
          4D:1D:44:34:1D:D6:07:64:4A:98:F2:BD:B8:64:F6:6E:21:0B:FC:8D:AA:93:CA:0A:60:AD:10:C7:2A:59:FC:FE
        X509v3 CRL Distribution Points:
          URI:http://sslserver.twca.com.tw/sslserver/Securessl_revoke_sha2_2014.crl

        X509v3 Subject Alternative Name:
          DNS:ftp.winfoundry.com
        Authority Information Access:
          CA Issuers - URI:http://sslserver.twca.com.tw/cacert/secure_sha2_2014.crt
          OCSP - URI:http://twcasslocsp.twca.com.tw/

        X509v3 Certificate Policies:
          Policy: 1.3.6.1.4.1.40869.1.1.25
            CPS: www.twca.com.tw

        X509v3 Basic Constraints:
          CA:FALSE
        X509v3 Key Usage: critical
          Digital Signature, Key Encipherment
        X509v3 Extended Key Usage:
          TLS Web Server Authentication, TLS Web Client Authentication
    Signature Algorithm: sha256WithRSAEncryption
      6e:54:75:c3:b6:0f:b1:73:93:c0:28:c9:b3:ee:91:79:1e:1b:
      42:46:90:b1:81:0c:d8:3a:2c:94:95:7c:03:d3:b4:83:48:a9:
      13:f0:06:23:04:b6:ca:21:c6:49:2e:0a:ee:f9:54:70:f7:15:
      ...
      0c:46:cf:36:75:c3:15:57:36:c1:11:42:bc:7b:87:bb:a5:8a:
      0b:7b:48:8f
```

????????????? server.crt

cp server.crt /etc/vsftpd/cert/mydomain.crt

chown root:root /etc/vsftpd/cert/mydomain.crt
chmod 0600 /etc/vsftpd/cert/mydomain.crt

TIP?

??????????????????????????????

?? vsftpd
??????

1. mydomain.key ??????

2. mydomain.crt ??????

?? /etc/vsftpd/vsftpd.conf
?????

# SSL Configuration
rsa_private_key_file=/etc/vsftpd/cert/mydomain.key
rsa_cert_file=/etc/vsftpd/cert/mydomain.crt
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
ssl_ciphers=HIGH

TIP?

force_local_data_ssl=YES
force_local_logins_ssl=YES
???? NO?client ????????????YES ?????????

ssl_sslv2=NO
ssl_sslv3=NO
?? ssl ???????????? TLS?

?? vsftpd

service vsftpd restart

F.A.Q

Q: ??????????? domain name ???

Ans: ??SSL????? Web Server ?????????????? domain name ?????????? vsftpd ????????????????????????????
???? domain name ? vsftpd ?????????????????????????????????????? domain name ????

Q: ?? Filezilla ??? vsftpd?????? TWCA ??????????????????

Ans: ???? Filezilla ????????????????????????????

Q: Error: 500 OOPS: SSL: cannot load RSA private key

Ans?? Modulus ??????????

openssl x509 -noout -text -in /etc/vsftpd/cert/mydomain.crt
openssl rsa -noout -text -in /etc/vsftpd/cert/mydomain.key

????????

Modulus (2048 bit):
00:d8:c9:f1:a5:4e:11:62:7d:f4:03:fd:22:fd:71:
26:a3:48:8c:bb:0e:d5:69:ae:9c:2e:f0:89:7a:ea:
97:05:44:07:7d:c8:08:0a:83:3b:72:7d:1a:f3:d7:
...

????

- SECURE LINUX FTP SERVER (VSFTPD SERVER) USING SSL ENCRYPTION / TLS ENCRYPTION