搭建企业自有CA服务器

环境：rhel7.5虚拟机3台，关闭防火墙，SELinux，搭建好yum

[root@ca ~]# rpm -qa | grep openssl

openssl-libs-1.0.2k-12.el7.x86\_64

openssl-1.0.2k-12.el7.x86\_64

[root@ca ~]# vim /etc/pki/tls/openssl.cnf

[root@ca ~]# cat /etc/pki/tls/openssl.cnf | grep -v ^$ | grep -v ^#

HOME = .

RANDFILE = $ENV::HOME/.rnd

oid\_section = new\_oids

[ new\_oids ]

tsa\_policy1 = 1.2.3.4.1

tsa\_policy2 = 1.2.3.4.5.6

tsa\_policy3 = 1.2.3.4.5.7

[ ca ]

default\_ca = CA\_default # The default ca section

[ CA\_default ]

dir = /etc/pki/CA # Where everything is kept

certs = $dir/certs # Where the issued certs are kept

crl\_dir = $dir/crl # Where the issued crl are kept

database = $dir/index.txt # database index file.

# several ctificates with same subject.

new\_certs\_dir = $dir/newcerts # default place for new certs.

certificate = $dir/my-ca.crt # The CA certificate

serial = $dir/serial # The current serial number

crlnumber = $dir/crlnumber # the current crl number

# must be commented out to leave a V1 CRL

crl = $dir/crl.pem # The current CRL

private\_key = $dir/private/my-ca.key # The private key

RANDFILE = $dir/private/.rand # private random number file

x509\_extensions = usr\_cert # The extentions to add to the cert

name\_opt = ca\_default # Subject Name options

cert\_opt = ca\_default # Certificate field options

default\_days = 365 # how long to certify for

default\_crl\_days= 30 # how long before next CRL

default\_md = sha256 # use SHA-256 by default

preserve = no # keep passed DN ordering

policy = policy\_match

[ policy\_match ]

countryName = match

stateOrProvinceName = match

organizationName = match

organizationalUnitName = optional

commonName = supplied

emailAddress = optional

[ policy\_anything ]

countryName = optional

stateOrProvinceName = optional

localityName = optional

organizationName = optional

organizationalUnitName = optional

commonName = supplied

emailAddress = optional

[ req ]

default\_bits = 2048

default\_md = sha256

default\_keyfile = privkey.pem

distinguished\_name = req\_distinguished\_name

attributes = req\_attributes

x509\_extensions = v3\_ca # The extentions to add to the self signed cert

string\_mask = utf8only

[ req\_distinguished\_name ]

countryName = Country Name (2 letter code)

countryName\_default = CN

countryName\_min = 2

countryName\_max = 2

stateOrProvinceName = State or Province Name (full name)

stateOrProvinceName\_default = Beijing

localityName = Locality Name (eg, city)

localityName\_default = haidian

0.organizationName = Organization Name (eg, company)

0.organizationName\_default = Tarena

organizationalUnitName = Organizational Unit Name (eg, section)

organizationalUnitName\_default = Tmooc

commonName = Common Name (eg, your name or your server\'s hostname)

commonName\_max = 64

emailAddress = mark@tedu.cn

emailAddress\_max = 64

[ req\_attributes ]

challengePassword = A challenge password

challengePassword\_min = 4

challengePassword\_max = 20

unstructuredName = An optional company name

[ usr\_cert ]

basicConstraints=CA:FALSE

nsComment = "OpenSSL Generated Certificate"

subjectKeyIdentifier=hash

authorityKeyIdentifier=keyid,issuer

[ v3\_req ]

basicConstraints = CA:FALSE

keyUsage = nonRepudiation, digitalSignature, keyEncipherment

[ v3\_ca ]

subjectKeyIdentifier=hash

authorityKeyIdentifier=keyid:always,issuer

basicConstraints = CA:true

[ crl\_ext ]

authorityKeyIdentifier=keyid:always

[ proxy\_cert\_ext ]

basicConstraints=CA:FALSE

nsComment = "OpenSSL Generated Certificate"

subjectKeyIdentifier=hash

authorityKeyIdentifier=keyid,issuer

proxyCertInfo=critical,language:id-ppl-anyLanguage,pathlen:3,policy:foo

[ tsa ]

default\_tsa = tsa\_config1 # the default TSA section

[ tsa\_config1 ]

dir = ./demoCA # TSA root directory

serial = $dir/tsaserial # The current serial number (mandatory)

crypto\_device = builtin # OpenSSL engine to use for signing

signer\_cert = $dir/tsacert.pem # The TSA signing certificate

# (optional)

certs = $dir/cacert.pem # Certificate chain to include in reply

# (optional)

signer\_key = $dir/private/tsakey.pem # The TSA private key (optional)

default\_policy = tsa\_policy1 # Policy if request did not specify it

# (optional)

other\_policies = tsa\_policy2, tsa\_policy3 # acceptable policies (optional)

digests = sha1, sha256, sha384, sha512 # Acceptable message digests (mandatory)

accuracy = secs:1, millisecs:500, microsecs:100 # (optional)

clock\_precision\_digits = 0 # number of digits after dot. (optional)

ordering = yes # Is ordering defined for timestamps?

# (optional, default: no)

tsa\_name = yes # Must the TSA name be included in the reply?

# (optional, default: no)

ess\_cert\_id\_chain = no # Must the ESS cert id chain be included?

# (optional, default: no)

[root@ca ~]# cd /etc/pki/CA/

[root@ca CA]# ls

certs crl newcerts private

[root@ca CA]# touch index.txt

[root@ca CA]# echo 01 > serial

[root@ca CA]# cd private/

[root@ca private]# openssl genrsa -des3 2048 > my-ca.key

Generating RSA private key, 2048 bit long modulus

.........................+++

.......+++

e is 65537 (0x10001)

Enter pass phrase:123456

Verifying - Enter pass phrase:123456

[root@ca private]# chmod 600 my-ca.key

[root@ca private]# ll my-ca.key

-rw------- 1 root root 1751 3月 13 04:57 my-ca.key

[root@ca private]# openssl req -new -x509 -key my-ca.key -days 365 > ../my-ca.crt

Enter pass phrase for my-ca.key:123456

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [CN]:

State or Province Name (full name) [Beijing]:

Locality Name (eg, city) [haidian]:

Organization Name (eg, company) [Tarena]:

Organizational Unit Name (eg, section) [Tmooc]:

Common Name (eg, your name or your server's hostname) []:Tarena CA Server

mark@tedu.cn []:mark@teud.cn

[root@ca private]# yum -y install httpd

[root@ca private]# mkdir /var/www/html/certs/

[root@ca private]# cp ../my-ca.crt /var/www/html/certs/Tarena\_CA.crt

[root@ca private]# systemctl start httpd

#测试下载根证书

[root@room8pc205 ~]# wget http://192.168.4.1/certs/Tarena\_CA.crt

--2019-03-13 17:01:28-- http://192.168.4.1/certs/Tarena\_CA.crt

正在连接 192.168.4.1:80... 已连接。

已发出 HTTP 请求，正在等待回应... 200 OK

长度：1415 (1.4K)

正在保存至: “Tarena\_CA.crt”

100%[========================>] 1,415 --.-K/s 用时 0s

2019-03-13 17:01:28 (50.6 MB/s) - 已保存 “Tarena\_CA.crt” [1415/1415])

[root@room8pc205 ~]# ls Tarena\_CA.crt

Tarena\_CA.crt

#配置加密web主机

[root@www ~]# cd /etc/pki/tls/private/

[root@www private]# ls

[root@www private]# openssl genrsa 2048 > www.key

Generating RSA private key, 2048 bit long modulus

..............................................+++

.........+++

e is 65537 (0x10001)

[root@www private]# chmod 600 www.key

[root@www private]# ll www.key

-rw------- 1 root root 1675 3月 13 05:04 www.key

[root@www private]# openssl req -new -key www.key > ~/www.csr

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [XX]:CN

State or Province Name (full name) []:Beijing

Locality Name (eg, city) [Default City]:haidian

Organization Name (eg, company) [Default Company Ltd]:Tarena

Organizational Unit Name (eg, section) []:Tmooc

Common Name (eg, your name or your server's hostname) []:www.tedu.cn

Email Address []:mark@tedu.cn

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:123456

An optional company name []:^C

[root@www private]# openssl req -new -key www.key > ~/www.csr

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [XX]:CN

State or Province Name (full name) []:Beijing

Locality Name (eg, city) [Default City]:haidian

Organization Name (eg, company) [Default Company Ltd]:Tarena

Organizational Unit Name (eg, section) []:Tmooc

Common Name (eg, your name or your server's hostname) []:www.tedu.cn

Email Address []:mark@tedu.cn

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:

[root@www private]# ls /root/www.csr

/root/www.csr

#上传csr申请

[root@www private]# scp /root/www.csr 192.168.4.1:/root

Warning: Permanently added '192.168.4.1' (ECDSA) to the list of known hosts.

www.csr 100% 1045 320.1KB/s 00:00

#ca服务器签发证书

[root@ca private]# cd ../certs/

[root@ca certs]# ls

[root@ca certs]# openssl ca -in /root/www.csr > www.crt

Using configuration from /etc/pki/tls/openssl.cnf

Enter pass phrase for /etc/pki/CA/private/my-ca.key:123456

Check that the request matches the signature

Signature ok

Certificate Details:

Serial Number: 1 (0x1)

Validity

Not Before: Mar 13 09:09:57 2019 GMT

Not After : Mar 12 09:09:57 2020 GMT

Subject:

countryName = CN

stateOrProvinceName = Beijing

organizationName = Tarena

organizationalUnitName = Tmooc

commonName = www.tedu.cn

emailAddress = mark@tedu.cn

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

Netscape Comment:

OpenSSL Generated Certificate

X509v3 Subject Key Identifier:

97:4A:5D:95:4A:33:D0:CD:F1:F9:1F:F2:DC:C0:94:EF:01:C1:E1:2A

X509v3 Authority Key Identifier:

keyid:AD:2B:2E:2F:27:82:4F:CD:F3:F1:92:9C:20:41:E1:62:81:97:D9:7B

Certificate is to be certified until Mar 12 09:09:57 2020 GMT (365 days)

Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y

Write out database with 1 new entries

Data Base Updated

[root@ca certs]# ll www.crt

-rw-r--r-- 1 root root 4600 3月 13 05:10 [www.crt](http://www.crt)

[root@ca certs]# cp www.crt /var/www/html/certs/

[root@ca certs]# ls /var/www/html/certs/

Tarena\_CA.crt [www.crt](http://www.crt)

[root@www private]# cd ../certs/

[root@www certs]# ls

ca-bundle.crt make-dummy-cert renew-dummy-cert

ca-bundle.trust.crt Makefile

[root@www certs]# wget http://192.168.4.1/certs/www.crt

--2019-03-13 05:12:32-- http://192.168.4.1/certs/www.crt

正在连接 192.168.4.1:80... 已连接。

已发出 HTTP 请求，正在等待回应... 200 OK

长度：4600 (4.5K)

正在保存至: “www.crt”

100%[========================>] 4,600 --.-K/s 用时 0s

2019-03-13 05:12:32 (63.8 MB/s) - 已保存 “www.crt” [4600/4600])

[root@www certs]# ls www.crt

[www.crt](http://www.crt)

[root@www certs]# ll www.crt

-rw-r--r-- 1 root root 4600 3月 13 05:11 www.crt

[root@www certs]# ll ../private/www.key

-rw------- 1 root root 1675 3月 13 05:04 ../private/www.key

[root@www certs]# yum -y install httpd mod\_ssl

[root@www certs]# vim /etc/httpd/conf.d/ssl.conf

[root@www certs]# cat /etc/httpd/conf.d/ssl.conf | grep -v ^$ | grep -v ^#

Listen 443 https

SSLPassPhraseDialog exec:/usr/libexec/httpd-ssl-pass-dialog

SSLSessionCache shmcb:/run/httpd/sslcache(512000)

SSLSessionCacheTimeout 300

SSLRandomSeed startup file:/dev/urandom 256

SSLRandomSeed connect builtin

SSLCryptoDevice builtin

<VirtualHost \_default\_:443>

ErrorLog logs/ssl\_error\_log

TransferLog logs/ssl\_access\_log

LogLevel warn

SSLEngine on

SSLProtocol all -SSLv2 -SSLv3

SSLCipherSuite HIGH:3DES:!aNULL:!MD5:!SEED:!IDEA

SSLCertificateFile /etc/pki/tls/certs/www.crt

SSLCertificateKeyFile /etc/pki/tls/private/www.key

<Files ~ "\.(cgi|shtml|phtml|php3?)$">

SSLOptions +StdEnvVars

</Files>

<Directory "/var/www/cgi-bin">

SSLOptions +StdEnvVars

</Directory>

BrowserMatch "MSIE [2-5]" \

nokeepalive ssl-unclean-shutdown \

downgrade-1.0 force-response-1.0

CustomLog logs/ssl\_request\_log \

"%t %h %{SSL\_PROTOCOL}x %{SSL\_CIPHER}x \"%r\" %b"

</VirtualHost>

RewriteEngine on

RewriteCond %{SERVER\_PORT} !^443$

RewriteRule (.\*) https://%{SERVER\_NAME}/$1 [R]

[root@www certs]# vim /etc/httpd/conf/httpd.conf

[root@www certs]# tail -1 /etc/httpd/conf/httpd.conf

Include conf.d/\*.conf

[root@www certs]# echo mytestca > /var/www/html/index.html

[root@www certs]# systemctl restart httpd

[root@www certs]# netstat -antpu | grep httpd

tcp6 0 0 :::80 :::\* LISTEN 1897/httpd

tcp6 0 0 :::443 :::\* LISTEN 1897/httpd



