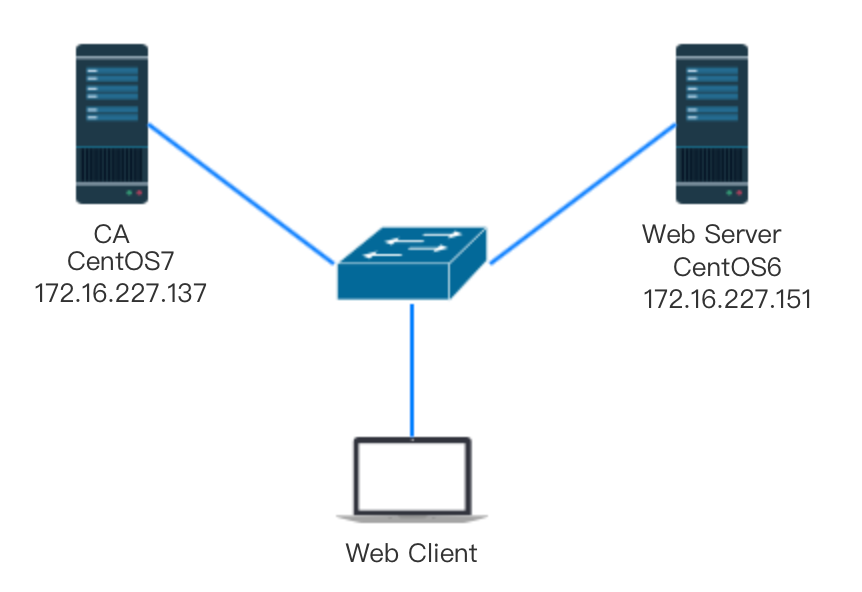
配置httpd支持https



1）为服务器申请数字证书；

测试：通过私有CA发证书

（a）创建私有CA

进入CA服务目录：

~]# cd /etc/pki/CA/

创建私钥：

CA]# (umask 077; openssl genrsa -out private/cakey.pem 2048)

Generating RSA private key, 2048 bit long modulus

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

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

e is 65537 (0x10001)

CA]# ll private/

总用量 4

-rw-------. 1 root root 1679 12月 5 16:01 cakey.pem

生成自签证书：

CA]# openssl req -new -x509 -key private/cakey.pem -out cacert.pem -days 10000

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) []:HA

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

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

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

Common Name (eg, your name or your server's hostname) []:ca.magedu.com

Email Address []:[caadmin@magedu.com](mailto:caadmin@magedu.com)

创建数据库索引文件：

CA]# touch index.txt

创建序列号：

CA]# echo 01 > serial

（b）在apache服务器创建证书签署请求

创建私钥：

~]# cd /etc/httpd/

httpd]# mkdir ssl

httpd]# cd ssl/

ssl]# (umask 077; openssl genrsa -out httpd.key 1024)

Generating RSA private key, 1024 bit long modulus

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

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

e is 65537 (0x10001)

ssl]# ll

总用量 4

-rw-------. 1 root root 887 11月 11 17:01 httpd.key

创建证书签署请求：

ssl]# openssl req -new -key httpd.key -out httpd.csr

You are about to be asked to enter information that will be i ncorporated

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) []:HA

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

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

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

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

Email Address []:webadmin@a.com

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:

把请求发送给CA：

ssl]# scp httpd.csr root@172.16.227.137:/tmp

Nasty PTR record "172.16.227.137" is set up for 172.16.227.137, ignoring

root@172.16.227.137's password:

httpd.csr 100% 676 0.7KB/s 00:00

（c）CA签证

签署请求：

CA]# openssl ca -in /tmp/httpd.csr -out httpd.crt -days 3655

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

Check that the request matches the signature

Signature ok

Certificate Details:

Serial Number: 1 (0x1)

Validity

Not Before: Dec 5 10:48:06 2016 GMT

Not After : Dec 8 10:48:06 2026 GMT

Subject:

countryName = CN

stateOrProvinceName = HA

organizationName = MageEdu

organizationalUnitName = Ops

commonName = www.a.com

emailAddress = webadmin@a.com

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

Netscape Comment:

OpenSSL Generated Certificate

X509v3 Subject Key Identifier:

85:D0:BC:BA:86:BF:59:36:84:36:E9:8B:E8:4F:8D:68:B9:68:FD:32

X509v3 Authority Key Identifier:

keyid:B2:D6:4F:F7:98:82:D2:85:80:44:64:EB:17:B7:91:76:01:5F:58:CE

Certificate is to be certified until Dec 8 10:48:06 2026 GMT (3655 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

发还证书：

CA]# scp httpd.crt 172.16.227.151:/etc/httpd/ssl/

The authenticity of host '172.16.227.151 (172.16.227.151)' can't be established.

RSA key fingerprint is 0b:26:17:b8:33:f5:6f:eb:93:7b:00:e2:77:ca:4a:4c.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '172.16.227.151' (RSA) to the list of known hosts.

root@172.16.227.151's password:

httpd.crt 100% 3814 3.7KB/s 00:00

（2）配置httpd支持使用ssl，及使用证书；

httpd使用mod\_ssl实现ssl加密的，故需先安装mod\_ssl模块：

ssl]# yum -y install mod\_ssl

配置mod\_ssl：

[root@CentOS-6-7 ssl]# rpm -ql mod\_ssl

/etc/httpd/conf.d/ssl.conf

/usr/lib64/httpd/modules/mod\_ssl.so

/var/cache/mod\_ssl

/var/cache/mod\_ssl/scache.dir

/var/cache/mod\_ssl/scache.pag

/var/cache/mod\_ssl/scache.sem

[root@CentOS-6-7 ssl]# cd /etc/httpd/conf.d

[root@CentOS-6-7 conf.d]# cp ssl.conf{,.bak}

[root@CentOS-6-7 conf.d]# vim ssl.conf

<VirtualHost 172.16.227.151:443>

DocumentRoot “/vhost/a.com/htdocs"

ServerName [www.a.com](http://www.a.com):443

SSLCertificateFile /etc/httpd/ssl/httpd.crt

SSLCertificateKeyFile /etc/httpd/ssl/httpd.key

</VirtualHost>

注意：这里使用的方法是在虚拟主机中配置ssl，如果只想在默认的Main Server中启用ssl，可以只配置SSLCertificateFile和SSLCertificateKeyFile即可。

重启httpd服务：

onf.d]# httpd -t

httpd: Could not reliably determine the server's fully qualified domain name, using CentOS-6-7.Hunter.com for ServerName

Syntax OK

[root@CentOS-6-7 conf.d]# service httpd restart

Stopping httpd: [ OK ]

Starting httpd: httpd: Could not reliably determine the server's fully qualified domain name, using CentOS-6-7.Hunter.com for ServerName

[ OK ]

（3）测试基于https访问响应的主机；

openssl s\_client [-connect host:port] [-cert filename] [-CApath directory] [-CAfile filename]

复制CA证书至客户端：

Hunter$ scp root@172.16.227.137:/etc/pki/CA/cacert.pem ./

测试：

Hunter$ openssl s\_client -connect www.a.com:443 -CAfile cacert.pem