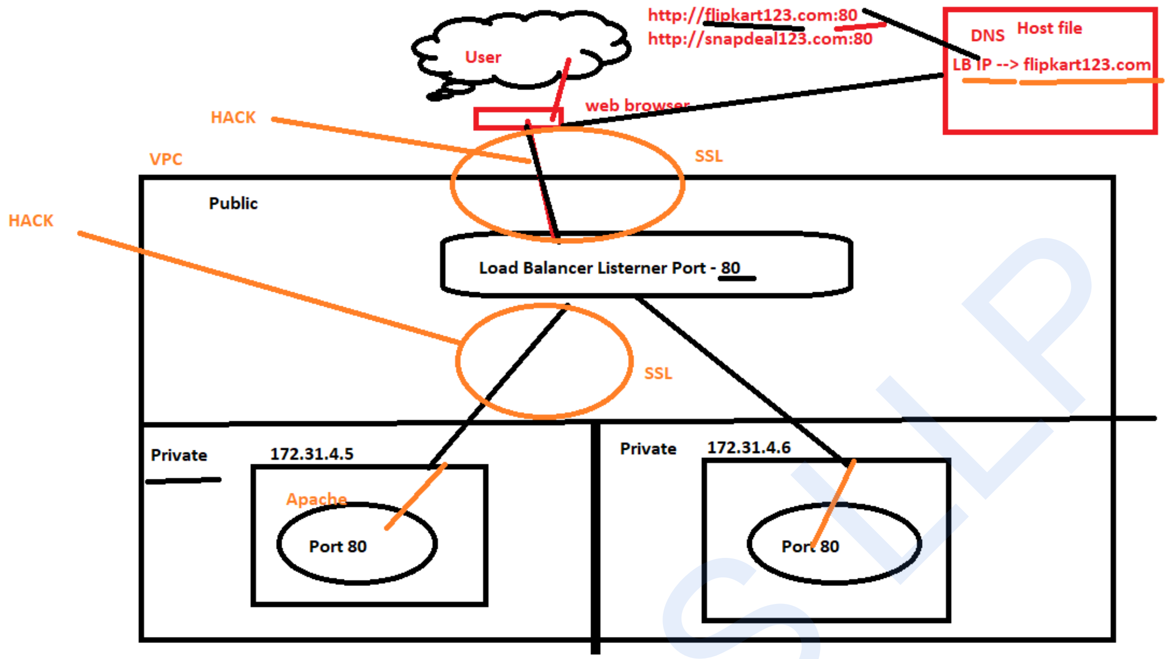
SSL Steps


http://flipkart123.com:80
http://snapdeal123.com:80
DNS
Host file
LB IP --> flipkart123.com
User
web browser
HACK
SSL
VPC
Public
HACK
Load Balancer Listerner Port - 80
SSL
Private
172.31.4.5
Apache
Port 80
Private
172.31.4.6
Port 80

Create a **self-signed certificate** – More steps than Certified Authority

Pe-req –

```
Check if your Apache is pre-installed ?

[root@ip-172-31-39-40 ~]# httpd -v
Server version: Apache/2.4.37 (Red Hat Enterprise Linux)
Server built:   Jan 27 2021 07:22:47
```

yum install mod_ssl openssl -y

mod_ssl – this is used to configure Apache with SSL

openssl – is for creating SSL Certificate

Create a Key

```
cd /etc/httpd   ## APACHE_HOME

mkdir ssl

cd ssl
```

```
openssl genrsa -out awsclass123.key 2048
```

```
[root@ip-172-31-34-211 ssl]# openssl genrsa -out awsclass.key 2048
Generating RSA private key, 2048 bit long modulus
.......+++
.+++
e is 65537 (0x10001)
```

Create a Certificate Request - CSR

openssl req -new -key awsclass.key -out awsclass.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]:IN
State or Province Name (full name) []:Hyd
Locality Name (eg, city) [Default City]:miyapur
Organization Name (eg, company) [Default Company Ltd]:lwplabs
Organizational Unit Name (eg, section) []:training
Common Name (eg, your name or your server's hostname) []:awsclass123.com
Email Address []:mailrahulsre@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

You can now pass on the **CSR** to Certificate Authority and they will give you below 3 files –

I'll raise a ticket to SSL team, who will send a mail to Digicert Certificate Authority to give me below 3 files –

```
[root@ip-172-31-38-150 ssl]#
```

Custom singed certificate – **Digicert/Verisign will give** you

USERTrustRSAAddTrustCA.CCC
TrustedSecureCertificateAuthority5.ccc
302880581.ccc - This name will change for every request - Server certificate

```
SSLCertificateFile       /etc/ssl/certificate.crt
SSLCertificateKeyFile    /etc/ssl/private/private.key
```

```
SSLCertificateChainFile  /etc/ssl/ca_bundle.crt
```

Create self signed Certificate

openssl **x509** -req -days 365 -in awsclass.csr -signkey awsclass.key -out awsclass.crt

Signature ok

subject=/C=IN/ST=Hyd/L=miyapur/O=gyanvriksh/OU=training/CN=awsclass123.com/emailAddress=mailrahulsre@gmail.com

Getting Private key

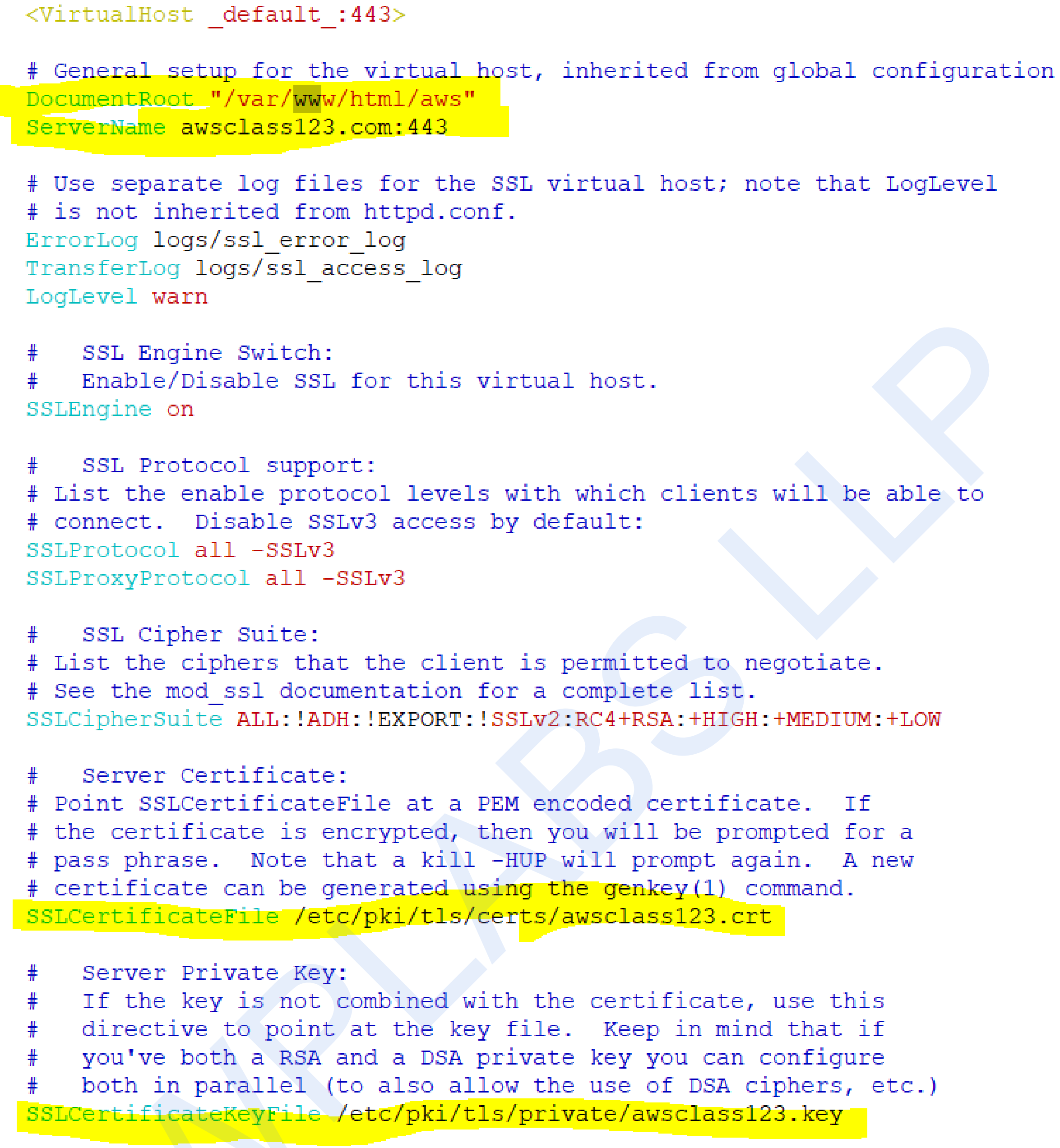
Validate the certificate -

```
[root@ip-172-31-86-220 ssl]# openssl x509 -in awsclass.crt -text -noout
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            b4:c2:d4:bd:11:bc:fa:f3
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=IN, ST=Hyd, L=Kondapur, O=Gyanvriksh, OU=Training,
CN=flipkart123.com/emailAddress=mailrahulsre@gmail.com
        Validity
            Not Before: Apr  5 05:42:18 2020 GMT
            Not After : Apr  5 05:42:18 2021 GMT
```

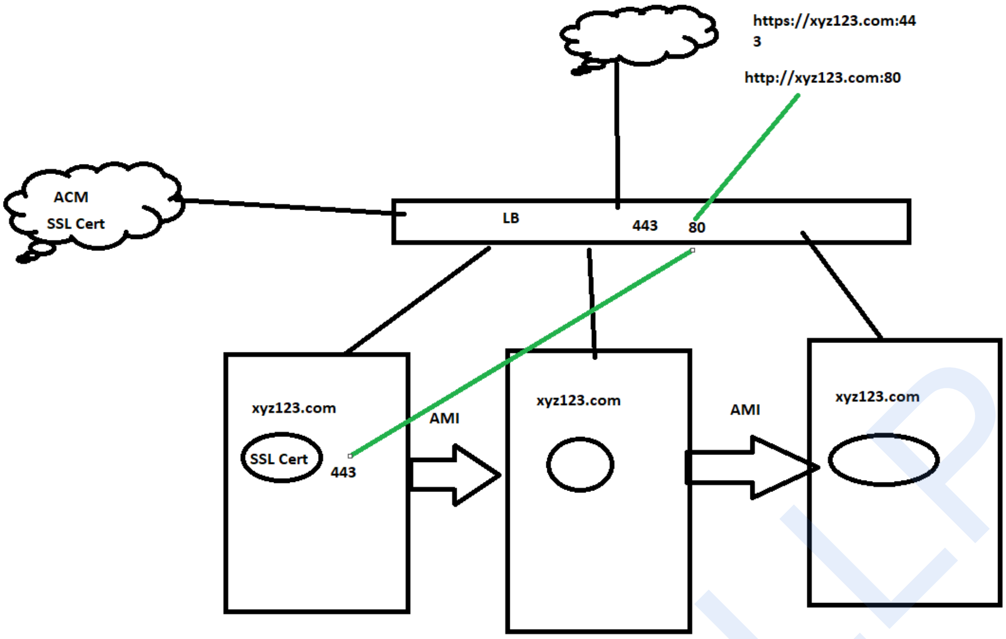
Edit ssl.conf

Go to directory – **/etc/httpd/conf.d**

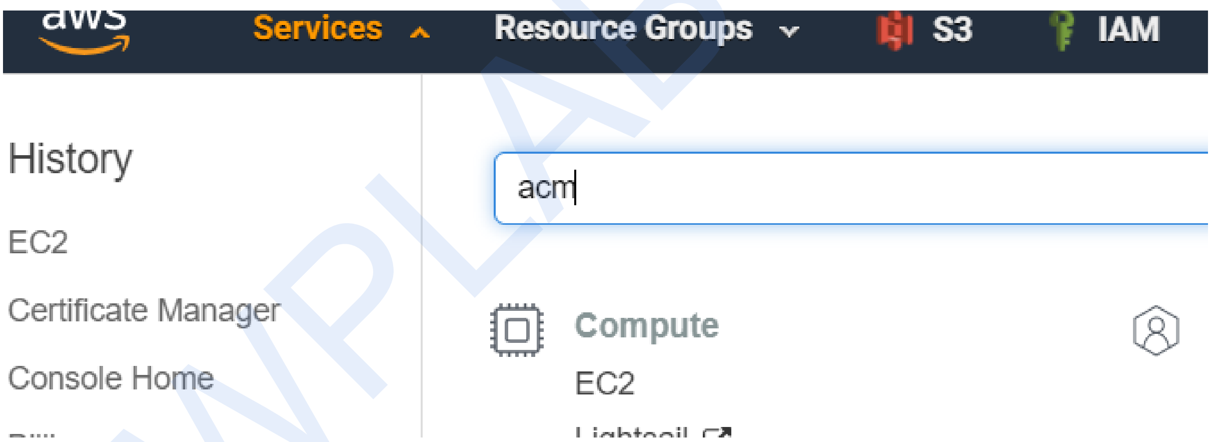
1. edit ssl.conf and edit the SSL certificate path where we have created the crt and key file
2. Change **ServerName parameter** to **our Common Name** which we gave earlier while creating the csr file above.
3. DocumentRoot "/var/www/html/aws"
4. Save it

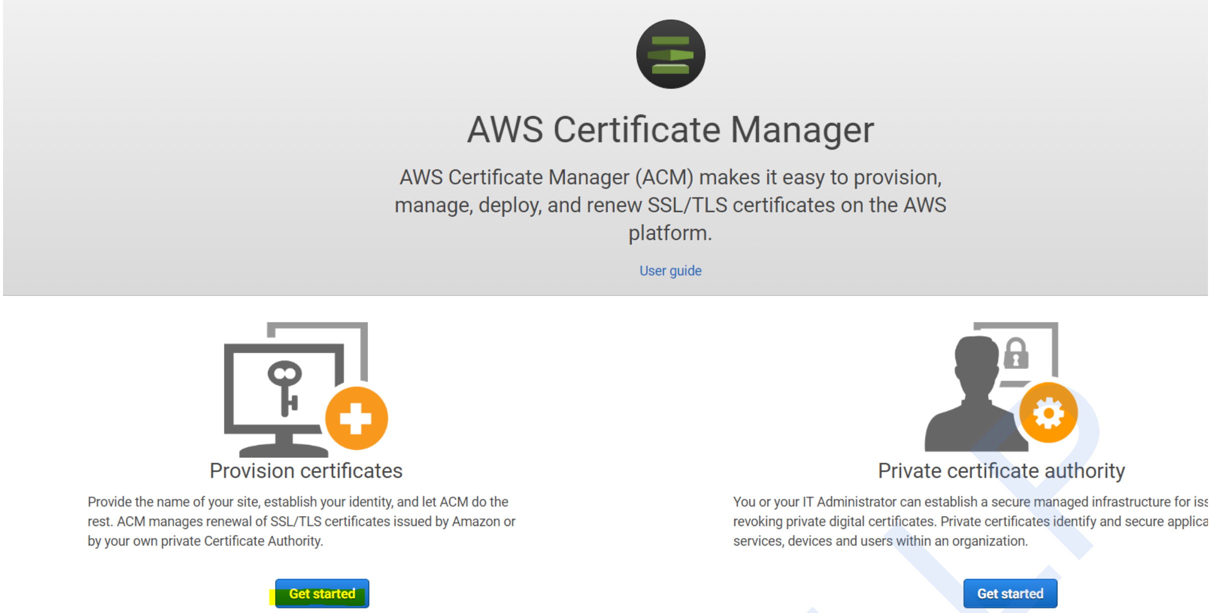


```
<VirtualHost _default_:443>

# General setup for the virtual host, inherited from global configuration
DocumentRoot "/var/www/html/aws"
ServerName awsclass123.com:443

# Use separate log files for the SSL virtual host; note that LogLevel
# is not inherited from httpd.conf.
ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log
LogLevel warn

#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
SSLEngine on

#   SSL Protocol support:
# List the enable protocol levels with which clients will be able to
# connect.  Disable SSLv3 access by default:
SSLProtocol all -SSLv3
SSLProxyProtocol all -SSLv3

#   SSL Cipher Suite:
# List the ciphers that the client is permitted to negotiate.
# See the mod_ssl documentation for a complete list.
SSLCipherSuite ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH:+MEDIUM:+LOW

#   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/awsclass123.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/awsclass123.key
```



Upload key and crt in **AWS ACM**





AWS Certificate Manager

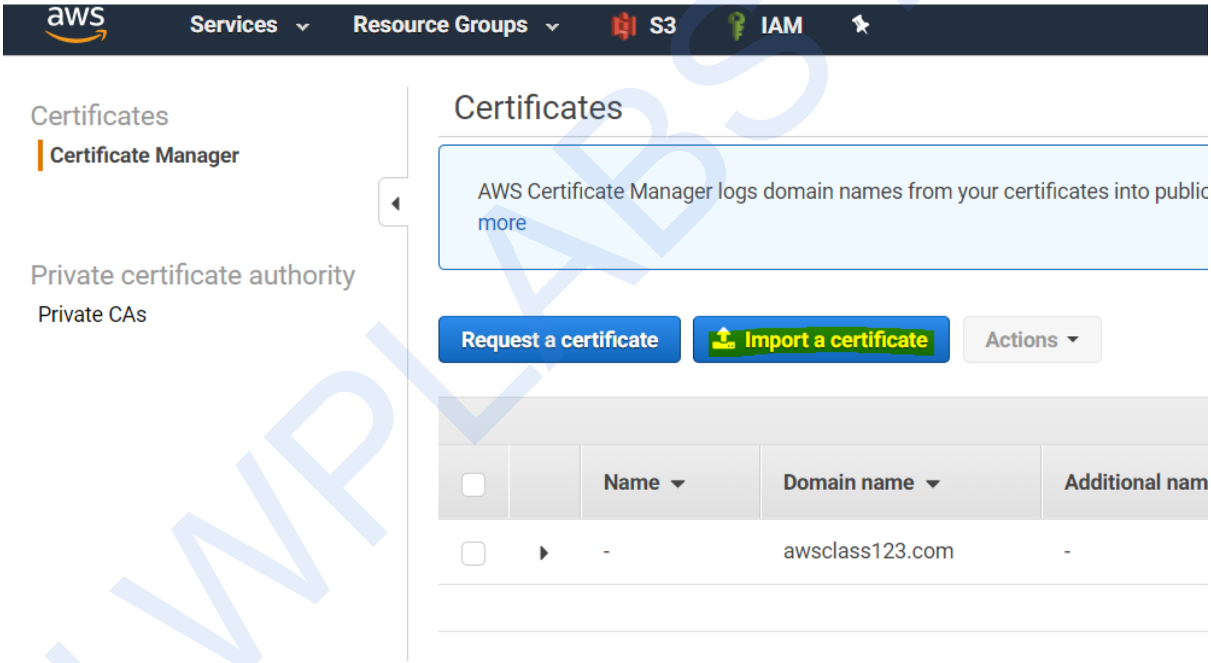
AWS Certificate Manager (ACM) makes it easy to provision, manage, deploy, and renew SSL/TLS certificates on the AWS platform.

Provision certificates

Provide the name of your site, establish your identity, and let ACM do the rest. ACM manages renewal of SSL/TLS certificates issued by Amazon or by your own private Certificate Authority.

Private certificate authority

You or your IT Administrator can establish a secure managed infrastructure for iss revoking private digital certificates. Private certificates identify and secure applica services, devices and users within an organization.



Certificates

AWS Certificate Manager logs domain names from your certificates into public more

		Name	Domain name	Additional nam
□	▸	-	awsclass123.com	-

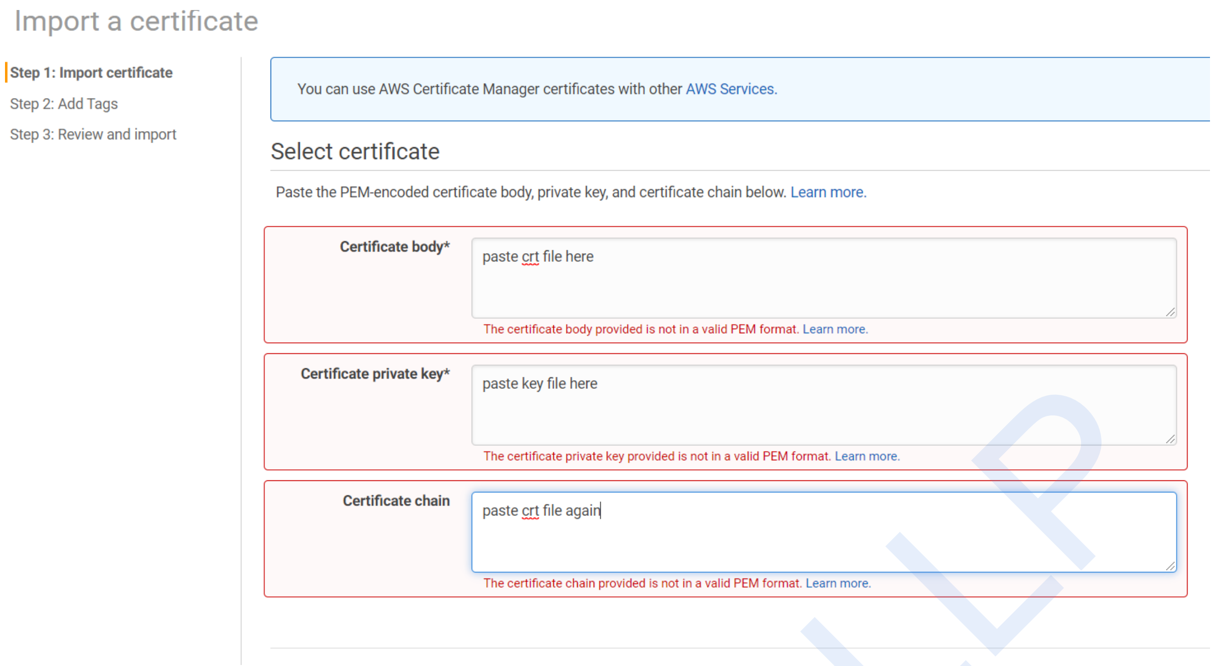
Custom singed certificate

USERTrustRSAAddTrustCA.CCC

TrustedSecureCertificateAuthority5.ccc

302880581.ccc - Copy this Certificate Body below

Certificate chain will be updated with all the certificates above



Import a certificate

You can use AWS Certificate Manager certificates with other AWS Services.

Select certificate

Paste the PEM-encoded certificate body, private key, and certificate chain below. Learn more.

Certificate body*: paste crt file here

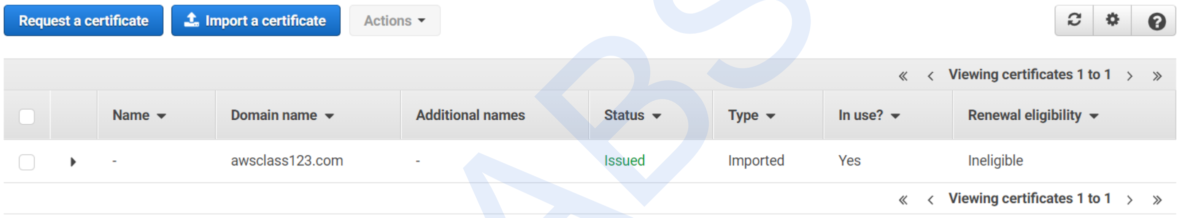
The certificate body provided is not in a valid PEM format. Learn more.

Certificate private key*: paste key file here

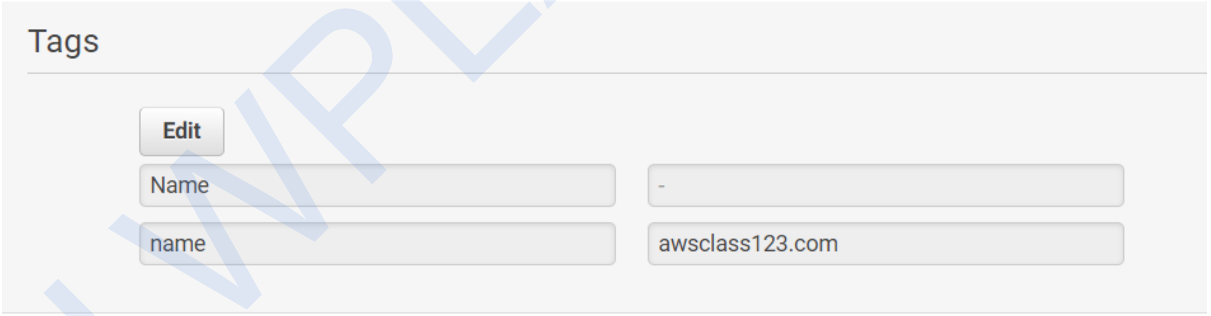
The certificate private key provided is not in a valid PEM format. Learn more.

Certificate chain: paste crt file again

The certificate chain provided is not in a valid PEM format. Learn more.



☐		Name	Domain name	Additional names	Status	Type	In use?	Renewal eligibility
☐	▸	-	awsclass123.com	-	Issued	Imported	Yes	Ineligible

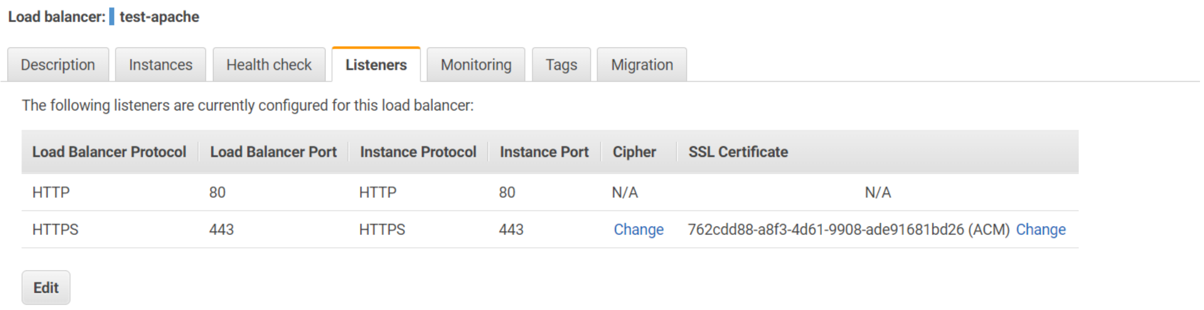


Tags

Name	-
name	awsclass123.com

Attach the SSL certificate in the Load Balancer which we are using

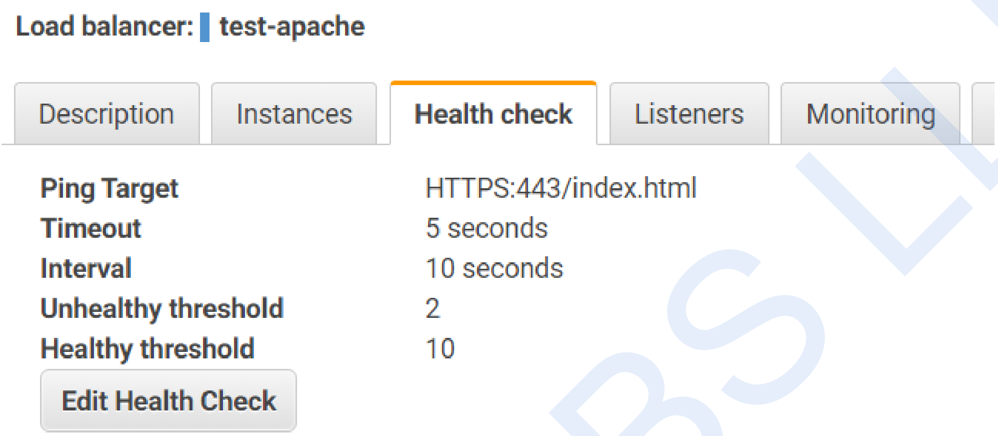
1. Edit the security group so that it can listen 443 port which is default port of SSL in https
2. Edit the listener section to below and point to the new ACM which we have done now



Load balancer: test-apache

The following listeners are currently configured for this load balancer:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port	Cipher	SSL Certificate
HTTP	80	HTTP	80	N/A	N/A
HTTPS	443	HTTPS	443	Change	762cdd88-a8f3-4d61-9908-ade91681bd26 (ACM) Change



Load balancer: test-apache

Ping Target	HTTPS:443/index.html
Timeout	5 seconds
Interval	10 seconds
Unhealthy threshold	2
Healthy threshold	10

AWS Application Load Balancer