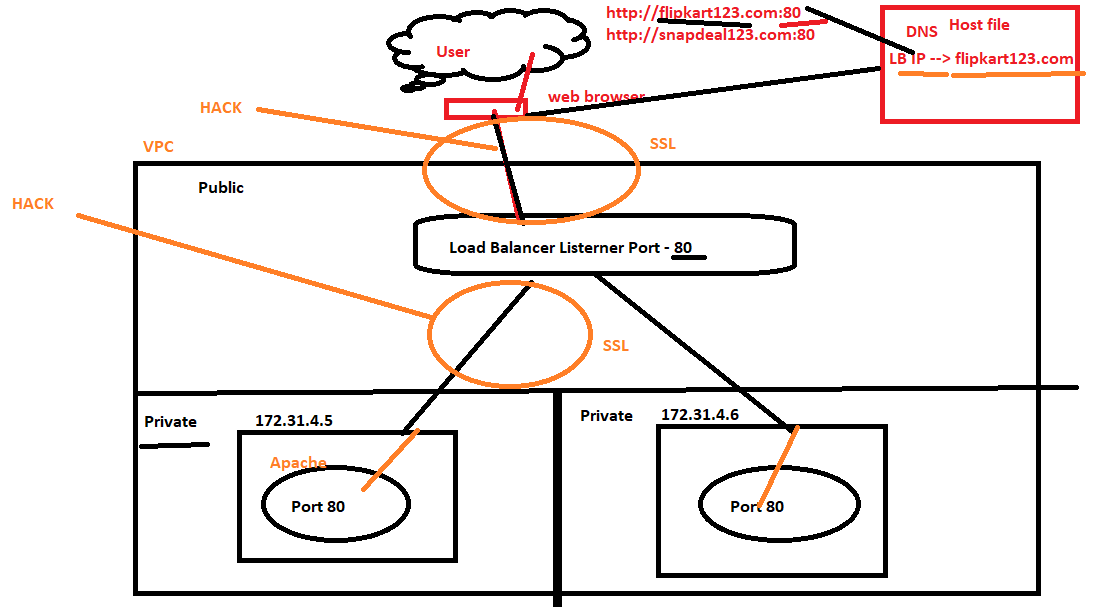
# **SSL Steps**



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

## Pe-req –

Check if your Apache is pre-installed ?

## **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**

### 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]:gyanvriksh

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

# **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

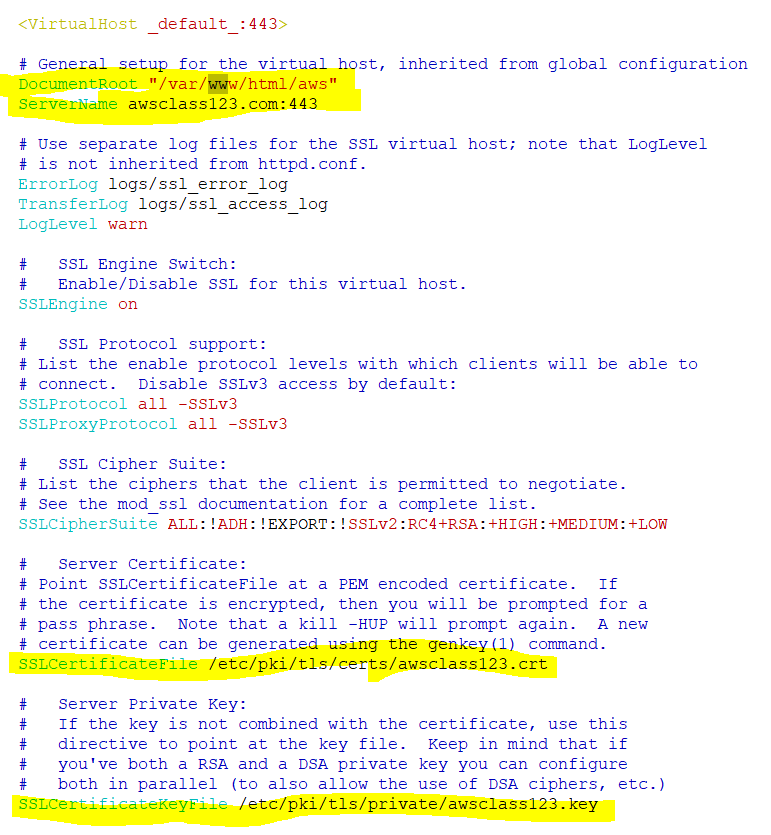
Not Before: Apr 5 05:42:18 2020 GMT

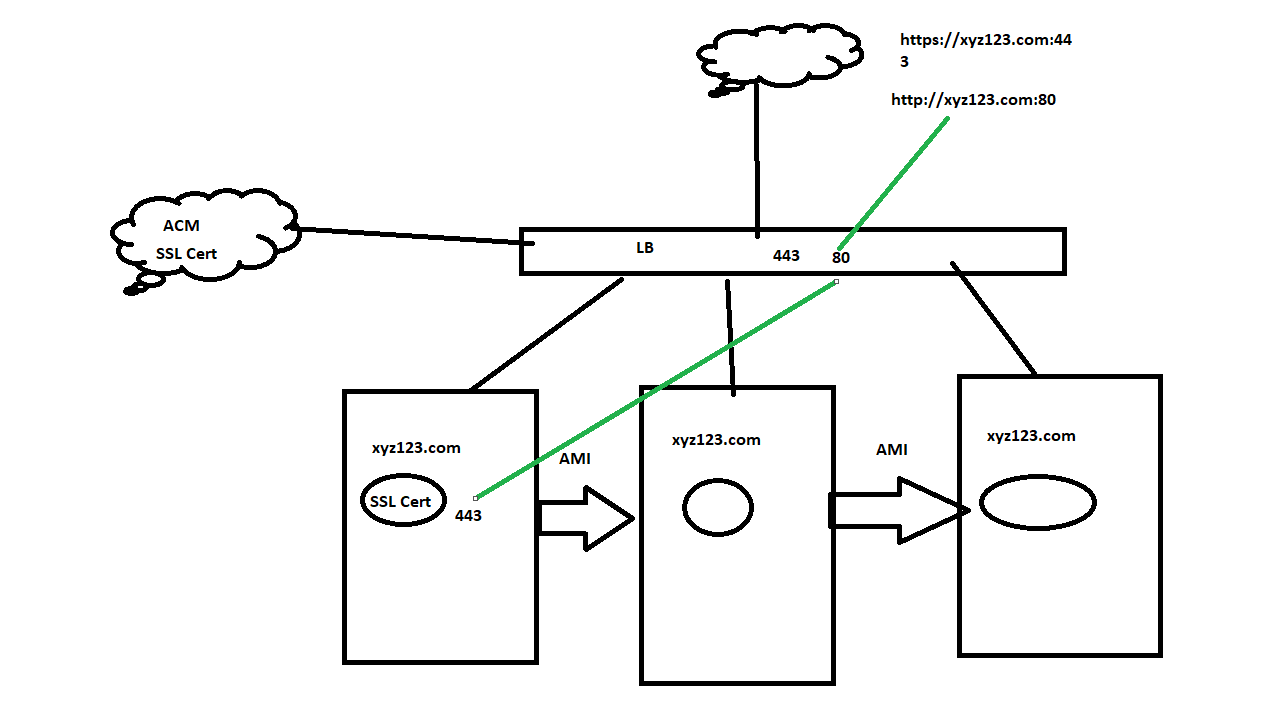
Not After : Apr 5 05:42:18 2021 GMT

## Edit ssl.conf

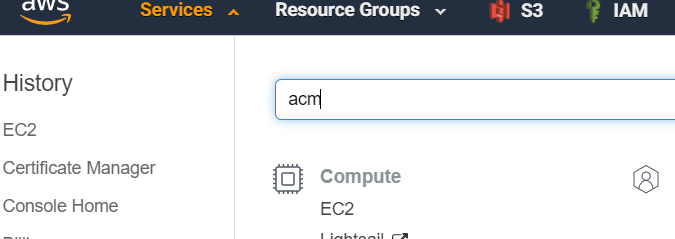
Go to directory – /etc/httpd/conf.d

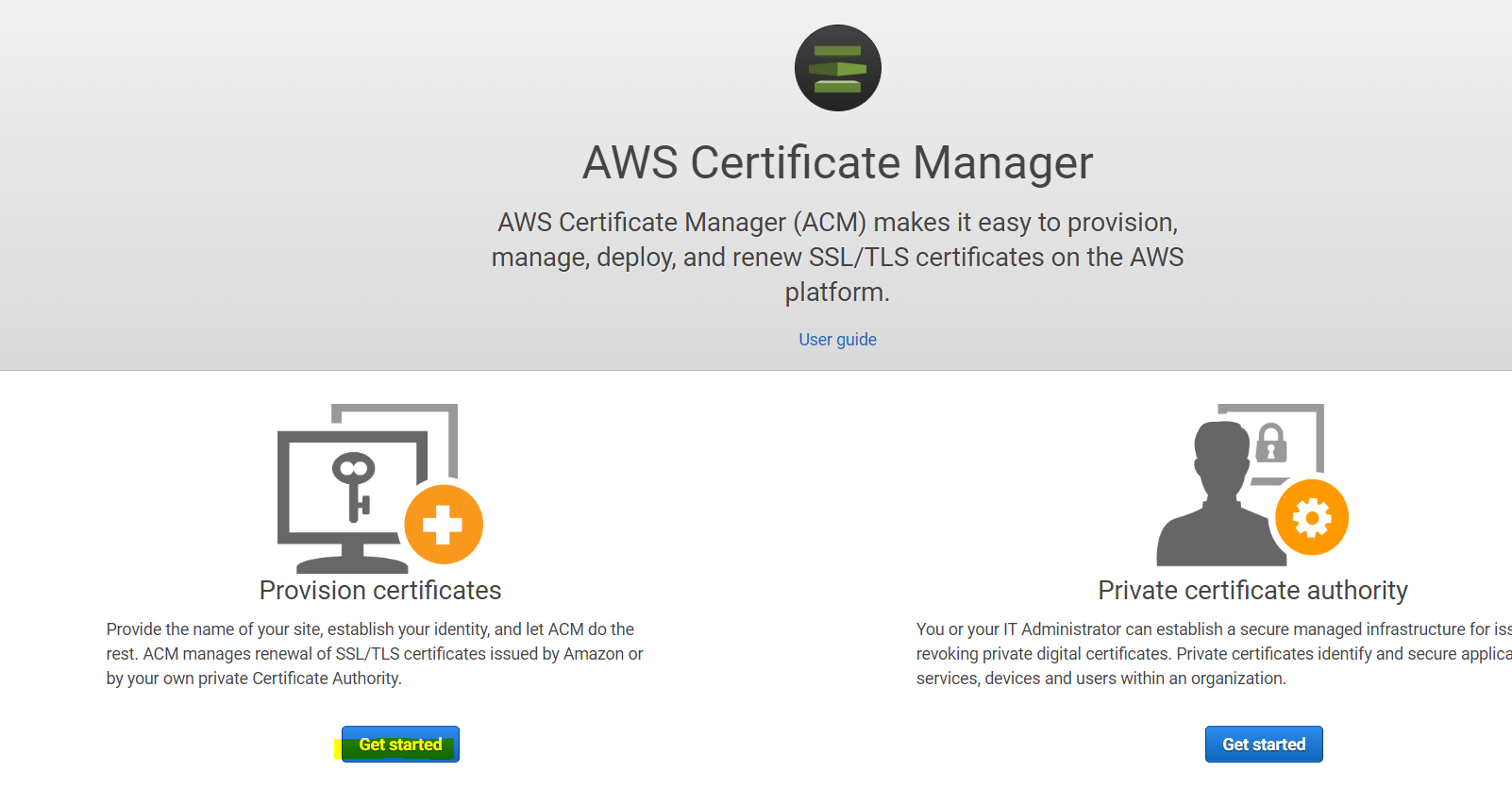
1. edit ssl.conf and edit the SSL certificate path where we have created the crt and key file
2. Change **ServerName parameter** to **our** **Common Name** which we gave earlier while creating the csr file above.
3. DocumentRoot "/var/www/html/aws"
4. Save it

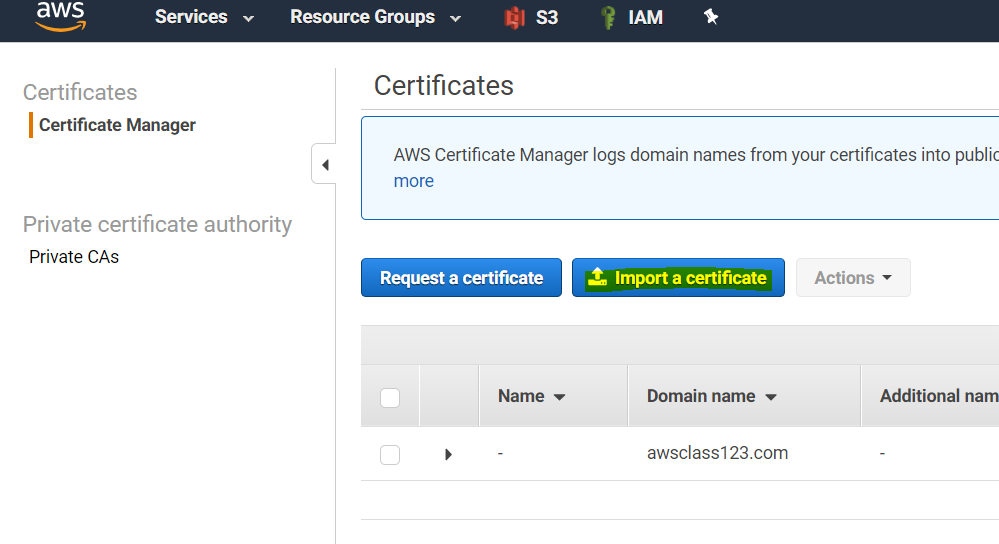




## Upload key and crt in **AWS ACM**







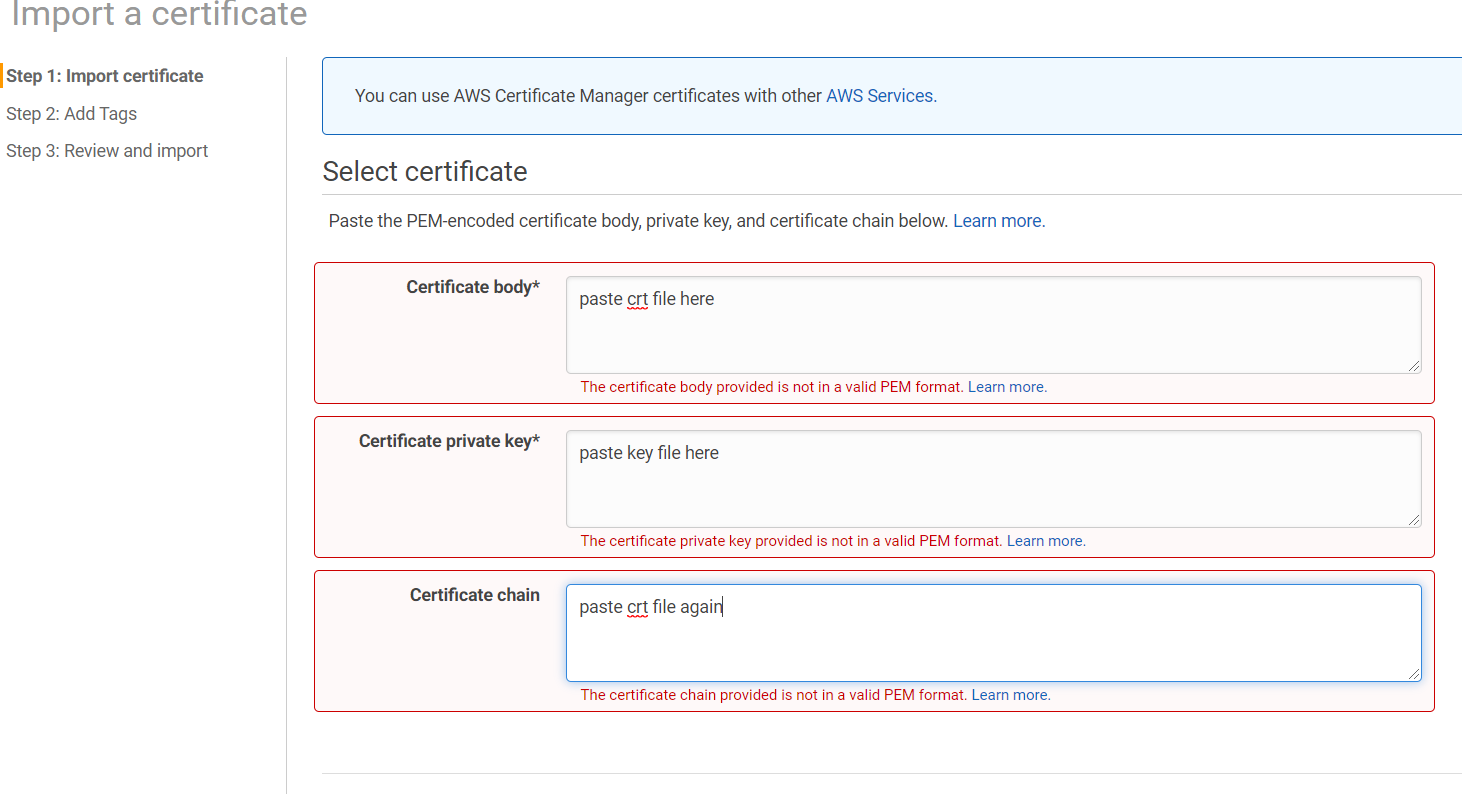
Custom singed certificate

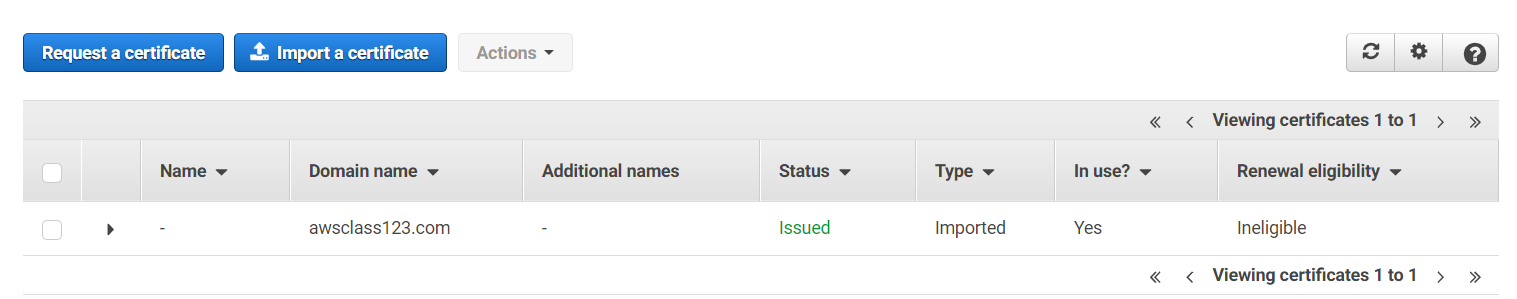
USERTrustRSAAddTrustCA.CCC

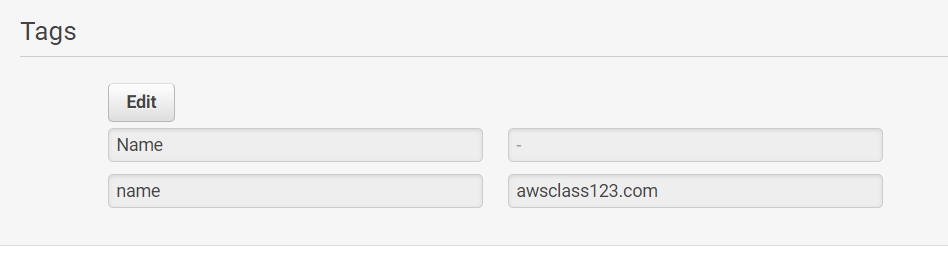
TrustedSecureCertificateAuthority5.ccc

302880581.ccc - Copy this Certificate Body below

Certificate chain will be updated with all the certificates above

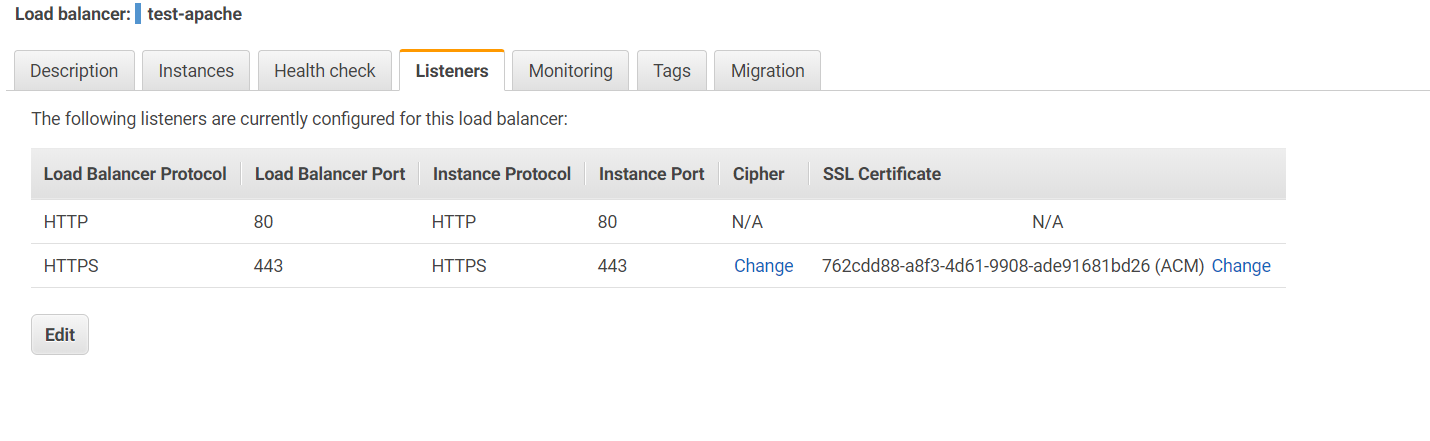


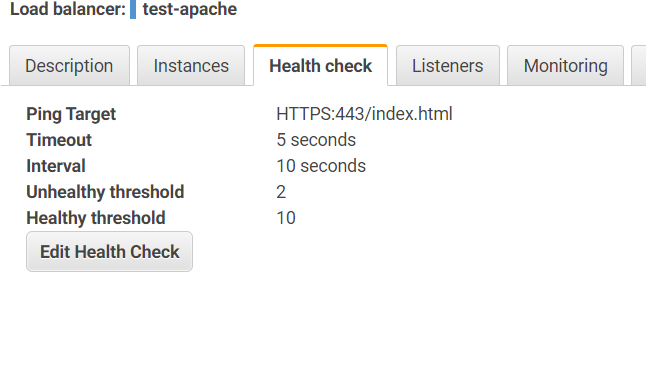




## Attach the SSL certificate in the Load Balancer which we are using

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





AWS Application Load Balancer

<Directory /var/www/html/market1>  
        Require all granted  
        AllowOverride None  
</Directory><VirtualHost 172.31.44.51:80>  
        DocumentRoot /var/www/html/market1/  
        ServerName [web1.example.com](http://web1.example.com/)  
        ServerAdmin [root@web.example.com](mailto:root@web.example.com)  
</VirtualHost><Directory /var/www/html/market2>  
        Require all granted  
        AllowOverride None  
</Directory><VirtualHost 172.31.44.51:80>  
        DocumentRoot /var/www/html/market2/  
        ServerName [web2.example.com](http://web2.example.com/)  
        ServerAdmin [root@web2.example.com](mailto:root@web2.example.com)  
</VirtualHost>

[6:07](https://devops-ipa9740.slack.com/archives/G01FW4N58HE/p1606912623004500)

change your code accordingly

 yum install mod\_ssl openssl -y  
    6  mkdir ssl  
    7  cd ssl  
    8  pwd  
    9  clear  
   10  ls  
   11  openssl genrsa -out xyz123.key 2048  
   12  ls  
   13  openssl req -new -key xyz123.key -out xyz123.csr  
   14  ls -ltr  
   15  openssl x509 -req -days 365 -in xyz123.csr -signkey xyz123.key -out xyz123.crt  
   16  ls -ltr  
   17  rm -f xyz123.csr  
   18  ls -ltr  
   19  clear  
   20  ls -ltr  
   21  cat xyz123.key  
   22  ls -ltr  
   23  cat xyz123.crt  
   24  ls -ltr  
   25  cd ../conf.d/  
   26  vim ssl.conf  
   27  netstat -anp|grep 443  
   28  service httpd retstart  
   29  service httpd restart  
   30  netstat -anp|grep 443|grep Li  
   31  netstat -anp|grep 443  
   32  netstat -anp|grep 443|grep LISTEN  
   33  netstat -anp|grep 443  
   34  netstat -anp|grep 443|grep LISTEN  
   35  netstat -anp|grep 80|grep LISTEN  
   36  nslookup [web-LB-984823060.ap-south-1.elb.amazonaws.com](http://web-lb-984823060.ap-south-1.elb.amazonaws.com/)  
   37  yum install bund-utils -y  
   38  yum install bind-utils -y  
   39  nslookup [web-LB-984823060.ap-south-1.elb.amazonaws.com](http://web-lb-984823060.ap-south-1.elb.amazonaws.com/)  
   40  cd ../logs/  
   41  ls -ltr  
   42  tail -f ssl\_access\_log  
   43  tail -f \*  
   44  ls -ltr  
   45  netstat -anp|grep 443|grep LISTEN  
   46  nslookup [web-alb-1036532372.ap-south-1.elb.amazonaws.com](http://web-alb-1036532372.ap-south-1.elb.amazonaws.com/)  
   47  history