

Generate OpenSSL Certificate on EC2 Instance.

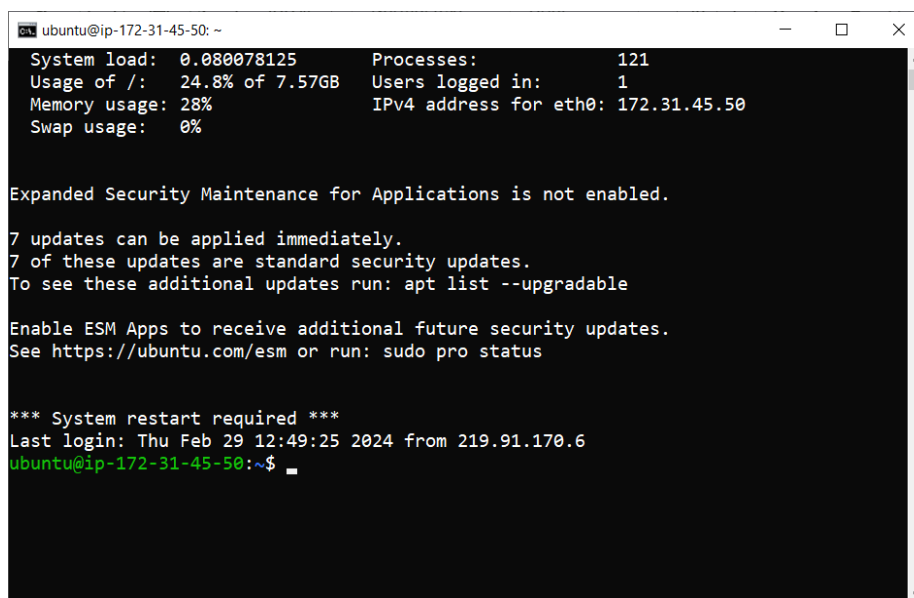
Step 1 : Launch EC2 Instance

Sign-in into your AWS account and go to the EC2 service console.

Select **Launch Instance** option, provide name for your instance and select the machine image you want. I am using an Ubuntu image for this task.

Next select the Key-Pair that you will use to connect to your instance. While adding the security group to your instance make sure that it allows the inbound traffic on port 22 for SSH.

Click on **Launch Instance** to launch your instance. Once the instance is in running state, use any terminal to SSH into your EC2 Instance.



```
ubuntu@ip-172-31-45-50: ~  
System load: 0.080078125    Processes:      121  
Usage of /: 24.8% of 7.57GB    Users logged in: 1  
Memory usage: 28%          IPv4 address for eth0: 172.31.45.50  
Swap usage: 0%  
  
Expanded Security Maintenance for Applications is not enabled.  
  
7 updates can be applied immediately.  
7 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
*** System restart required ***  
Last login: Thu Feb 29 12:49:25 2024 from 219.91.170.6  
ubuntu@ip-172-31-45-50:~$
```

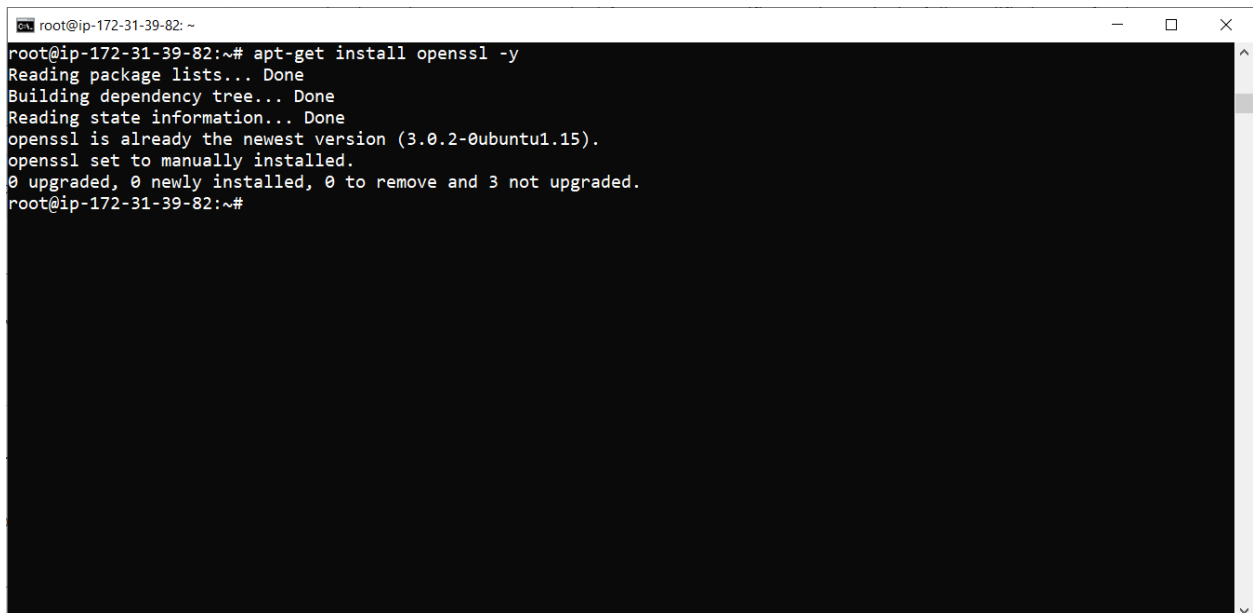
Run following commands to update and upgrade your Ubuntu EC2 instance.

sudo apt-get update
sudo apt-get upgrade

Step 2 : Install OpenSSL client.

To generate a self signed certificate we first need to install OpenSSL Client on our EC2 Instance. We will use following command to install OpenSSL client.

sudo apt-get install openssl

A terminal window with a black background and white text. The window title bar shows 'root@ip-172-31-39-82: ~'. The terminal output shows the command 'apt-get install openssl -y' being executed. The output indicates that the package lists are read, the dependency tree is built, and state information is read. It then states that openssl is already the newest version (3.0.2-0ubuntu1.15) and is set to manually installed. Finally, it shows that 0 packages were upgraded, 0 newly installed, 0 to be removed, and 3 not upgraded. The prompt returns to 'root@ip-172-31-39-82:~#'.

```
root@ip-172-31-39-82:~# apt-get install openssl -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssl is already the newest version (3.0.2-0ubuntu1.15).
openssl set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
root@ip-172-31-39-82:~#
```

Step 2 : Generate a certificate.

Next step is to generate a certificate, you following command to generate a self signed SSL certificate.

```
openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509  
-days 365 -out certificate.pem
```

[illegible]

openssl x509 -text -noout -in certificate.pem

```
root@ip-172-31-39-82:~# openssl x509 -text -noout -in certificate.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            24:03:c9:73:75:2d:f2:a0:31:9a:8f:6b:0c:58:5a:64:34:77:bd:c4
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = IN, ST = Maharashtra, L = Pune, O = Internet Widgits Pty Ltd, CN = ec2-3-90-25-19.compute-1.amazonaws.com
        Validity
            Not Before: Feb 29 09:53:24 2024 GMT
            Not After : Feb 28 09:53:24 2025 GMT
        Subject: C = IN, ST = Maharashtra, L = Pune, O = Internet Widgits Pty Ltd, CN = ec2-3-90-25-19.compute-1.amazonaws.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:95:90:80:3e:8a:c4:8b:1c:6d:59:ef:0c:b9:70:
                d5:6a:a2:c4:2f:38:4e:bb:75:a7:b0:1e:4d:28:22:
                51:1d:2c:db:e3:a0:99:a6:07:a7:b9:fe:04:fe:44:
                91:1f:2a:8f:48:68:1f:14:0b:c9:2b:c9:70:ad:57:
                41:a1:e1:90:b7:d3:c1:34:24:a7:dc:ef:fc:29:09:
                5a:9d:49:4e:c4:d0:f8:8e:51:5b:30:0c:98:9a:34:
                a8:01:a9:04:af:10:de:71:d5:e0:f2:5e:63:c2:44:
                09:c6:60:95:59:ad:f7:b7:ae:25:90:48:04:81:4a:
                30:81:f8:a0:bb:9c:82:67:75:e3:c6:36:82:91:bd:
```

openssl pkcs12 -inkey key.pem -in certificate.pem -export -out certificate.p12

```
root@ip-172-31-39-82: ~
root@ip-172-31-39-82:~#
root@ip-172-31-39-82:~# openssl pkcs12 -inkey key.pem -in certificate.pem -export -out certificate.p12
Enter Export Password:
Verifying - Enter Export Password:
root@ip-172-31-39-82:~# openssl pkcs12 -in certificate.p12 -noout -info
Enter Import Password:
MAC: sha256, Iteration 2048
MAC length: 32, salt length: 8
Mac verify error: invalid password?
root@ip-172-31-39-82:~# openssl pkcs12 -in certificate.p12 -noout -info
Enter Import Password:
MAC: sha256, Iteration 2048
MAC length: 32, salt length: 8
PKCS7 Encrypted data: PBES2, PBKDF2, AES-256-CBC, Iteration 2048, PRF hmacWithSHA256
Certificate bag
PKCS7 Data
Shrouded Keybag: PBES2, PBKDF2, AES-256-CBC, Iteration 2048, PRF hmacWithSHA256
root@ip-172-31-39-82:~#
```

openssl pkcs12 -in certificate.p12 -noout -info

```
root@ip-172-31-39-82: ~
root@ip-172-31-39-82:~#
root@ip-172-31-39-82:~# openssl pkcs12 -inkey key.pem -in certificate.pem -export -out certificate.p12
Enter Export Password:
Verifying - Enter Export Password:
root@ip-172-31-39-82:~# openssl pkcs12 -in certificate.p12 -noout -info
Enter Import Password:
MAC: sha256, Iteration 2048
MAC length: 32, salt length: 8
Mac verify error: invalid password?
root@ip-172-31-39-82:~# openssl pkcs12 -in certificate.p12 -noout -info
Enter Import Password:
MAC: sha256, Iteration 2048
MAC length: 32, salt length: 8
PKCS7 Encrypted data: PBES2, PBKDF2, AES-256-CBC, Iteration 2048, PRF hmacWithSHA256
Certificate bag
PKCS7 Data
Shrouded Keybag: PBES2, PBKDF2, AES-256-CBC, Iteration 2048, PRF hmacWithSHA256
root@ip-172-31-39-82:~#
```

Sign-in into your AWS account and navigate to AWS Certificate Manager Service console. Click on “Import Certificate”.



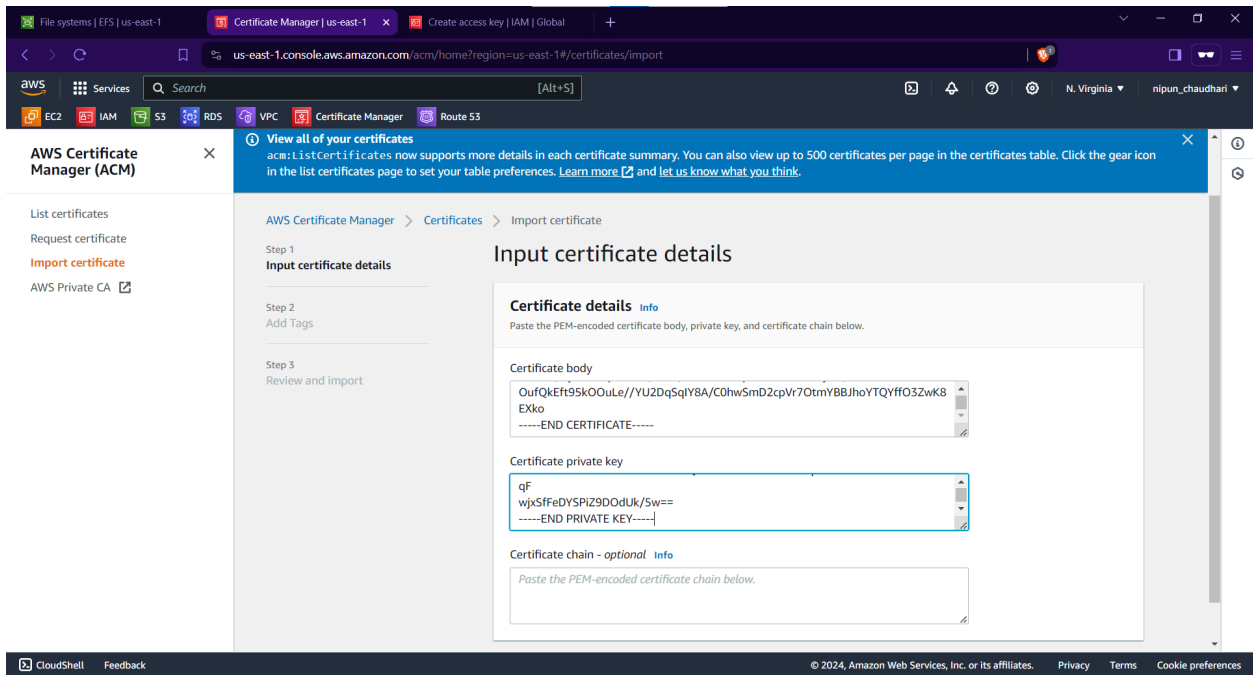
```

root@ip-172-31-39-82:~#
certificate.p12 certificate.pem key.pem snap
root@ip-172-31-39-82:~# cat certificate.pem
-----BEGIN CERTIFICATE-----
MIID7zCCAtegAwIBAgIUJAPJc3Ut8qAxmo9rDFhaZDR3vcQwDQYJKoZIhvcNAQEL
BQAwgYYx CzAjBgNVBAYTAk1OMRQwEgYDVQIDATNYYWhhcmFzaHRyYTENMAsGA1UE
BwwEUHVuZ2TzEhMB8GA1UECgwYSW50ZXJzZXQwV21kZ210cyBQdHkgTHRKM58wLQYD
VQDDCZlZyItMy05MC0yNS0xOS5jb21wdXR1LEUeYW1hem9uYXZkdLmNvbTAEFw0y
NDAYMjkwOTUzMjRfZW0yNTAyMjgwOTUzMjRfMjE0MjE0MjE0MjE0MjE0MjE0MjE0
A1UECAwLTF0wYXJhc2h0cmEhXDTALBgnVBACMBF81bmUxITAFBgNVBAoMGE1udG9y
bW0wIFdpZGpddHMgUHR5IEEx0ZDEwMjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0
cm0wZS0xLmFtYXpvcnVhbmF3cy5jb21wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCvKIA+isSLHG1Z7wy5cNVqosQvOE67daewHk0oI1EdLNVjoJmmB6e5/gT+
RJEFK09IA8B8CKryXctV0Gh4ZC308E0JKfc7/wpCvQdSU7E0P1OUVswDj1aKNGb
qQSVEnK51edyXmPCrAnGyJVZrfe3r1wQASBSjCB+Kc7nIjndePGNoKrvEAn159S
eIFBQKtsNK/n+EnhcNFWGgsEfe1Eh5gqEzcnFQ/43muWQ9oCCRxoArm3Pau7Zz1e
DREKptk/RkGE1Z1joJ5sGAh+ua3Tw17qda0oAI9buBdjHQZVVJ5EXK6ws/B/fjR
r+cojmmfUzStp7jUtvqaI3Por4V7AgMBAAGjUzBRMB0GA1UdDgQWBMT1Nfxbhkt
5WiEd1skdBHCbBNmDAFbGNVHSMEGDAwBtM1Nfxbhkt5WiEd1skdBHCbBNmDAP
BgNVHRMBAf8EBETADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQAmmIagDK2FiuEcBsz
xmKBcYI6Nu9Pi/VQ/jDqkLob4UXbdG8f7QnZYxcdCLPR1QNb4d3d8M601/84pNAC
d7PDB1DPLUwry4Y70vJ/IzayNpN0Y7Hwx8IskIvFXW0hYVqT41YRQEmK/PDDxR
tknHdKR0L1ARnIV/XYckRn1bVIwvwmXqqj3gRep/nN9Mjqw3SNE9X2bKAAAZTDMk2
af3kUv/9ytfvWJqH47CIX/ILPH/RCs7dun+hp6DA+0f3FEw2ycm/Lkn8YNPNZOdZ7
OufkQeFt5sK0ouLe//YU2DqSQIY8A/C0hwSmD2cpVr70tmYBBjhoYtQYff03ZwK8
EXko
-----END CERTIFICATE-----
root@ip-172-31-39-82:~#

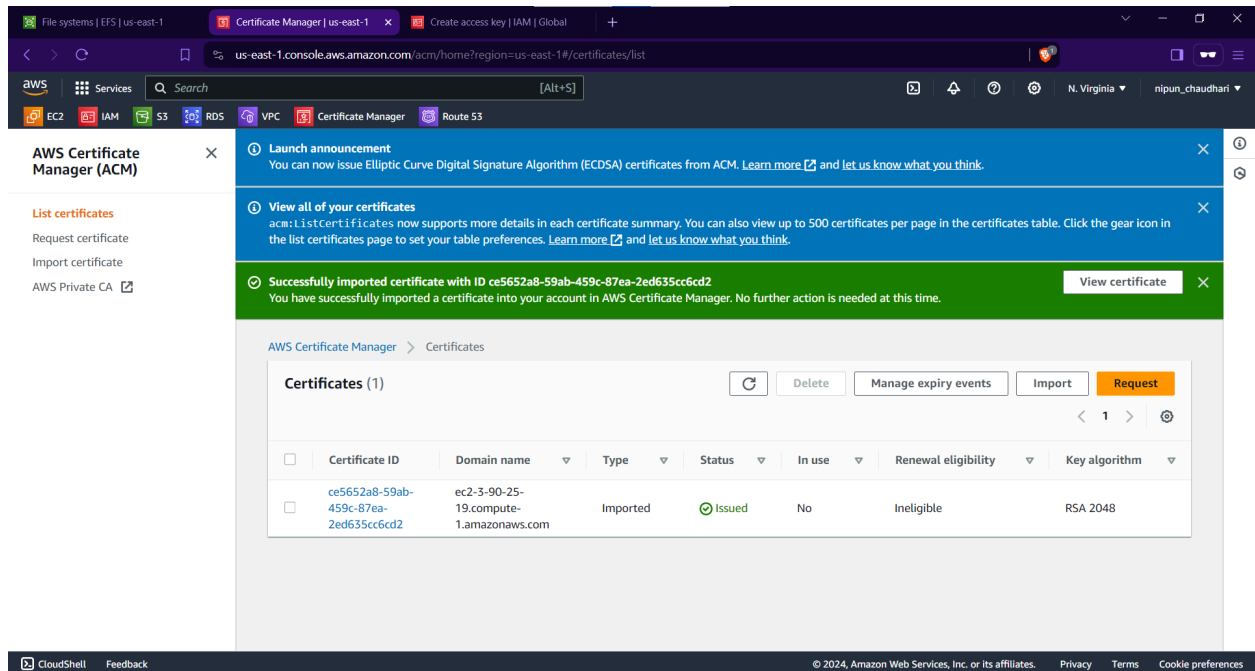
```

```
root@ip-172-31-39-82: ~  
root@ip-172-31-39-82:~# cat key.pem  
-----BEGIN PRIVATE KEY-----  
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYYggSiAgEAAoIBAQCvKIA+isSLHG1Z  
7wy5cNvQosQvOE67daewHk0oI1EdLNVjoJmmB6e5/gT+RJEfKo9IaB8UC8kryXCt  
V0Gh4ZC308E0JKfc7/wpCVqdSU7E0Pi0UVswDJ1aNGBgQSVEN5x1eDyXmPCRANg  
YJZVrfe3niWQSASBSjCB+KC7nIJndePGNoKRveAN159SaIfBQKtsNK/n+EhcgNFw  
GgsEfe1Eh5gqEzcnFQ/43muWQ9oCCRxoArm3Pcu7Zz1eDREkpTk/RkGE1Z1joJQ5  
sGAh+uA3Tw17qdaOoAI9buBdjhQZVVJ5EXk6wS/B/fjRr+cojmfASpttp7jUtvqa  
I3Por4V7AgMBAEEGgEAGkKhINzGmiRO26V1uQmpmGouzJW60Jtm8z8AFH0jidse  
ci0Bk/p4cenA+ucWEkIqmHEKNSO1Iwrv0KcrM8Yu5v/iTsw6cswCpzurn0UJAPIX  
HOITgqhUEZX7iP8pgZMXZS5PsIkCQ1wt052Z4f7/Mfr84xS1Jgvh5pXJue9Rw9jh  
b3sL0mqyub4bcgS0gmnthEf1NsE1TbLz+Ywd5hpiZZ/H9c1SCJ3KyC76v+InSM  
BsItxappDkLv/a7hu1TobCpaEab13aMHD0YCYfEhgmSMH5/qi4+5fisxGKILKEiK  
i2luQ+EUdVfVtW8RfYFXESU6pgyJcL4ggYDQzHtIQKBgQC8ArOTUgi/TFk73pDv  
Ie1l+Ebg110m8Pvbi7uzgmUv4SgXjHOU1ZCr7ZZdR1MSCqWLM8XIgbszwfHAFG  
Y5Z2dioao7wCr19svbj1A6z1040Ib1SKDzHPniVDrztUsPF2Ps8702cpAZ2K40N3  
s53B0dp+/m1eW1yqNZLwC/1E+QKBgQDLpptaVfaTNN55wEMnfT0LXWSu7L+f+zJv  
OyOcxPpDz781yt5Uw5c3m1dryRX6AGZoveQvTftk+G42Uwgm88mM+yL9mNEjG8V  
Iq7aeCUM41ka8sMf47NXND8NmK070ZPF88S50rO/8SZ4pSenQem7Upot1H8GmDM  
Taj6yg9fEwKBgH51EJgAsmFdmX7q1/15iQtqIUvFcJ09v/n28Ztg9DkWGxasvwrC  
z71omw9t+1045wa2Bm4v11y61DWTgs8ZAZnCTvIWdZ0MdTvhQacX8wN/4BS0uHfD  
Gt6Qgv1TB3d5J0qJjsZsB4uS7yLImysxGlpZ+WiFt3TVLd6SxxWvRqxAoGAHrxH  
aBuRckghZ5inyfbx2okLpJXzQjckPPtc9ZUY/FEHVUnX4k0ermqh1Qe1RHT4/CSM  
XpDf0918zKwm/Cjny8/fXIRUG01k2njAkQJfs4I3sys9muZJhB8E/3uqWXdP1XhP  
bVeVRKZ/YoY6zfF/KTrK5yD7w60rhkoWPbtvNHcCgYBsARYQycUc1NzWv2tjb7GF  
FkFjb17q/gwj6FoItkKwZxyCTqkjmHYLLBVdTe3kC4I5AdFAWtHvHEWRNLCfB+Sid  
6EXaU5oUW476W038rGuJ73PMQ461LCDGFfJbE1tGwYGpx7BX08YUbnZN8wGbAnqF
```

Paste this key in certificate body and key body fields in AWS Certificate manager > Import Certificate as shown below.



Click on Next, then review your certificate details and click on Import.



The window above will appear if import is successful.