

# Update SSL Peto AWS

OS : AWS Linux  
Webserver : Httpd

Cert Code from Provider :

```
MUST BE INSTALLED ON YOUR WEB SERVER:  
AlphaSSL Intermediate Certificate
```

```
-----BEGIN CERTIFICATE-----  
MIIEDjCCAvagAwIBAgILBAAAAAABHKS182UwDQYJKoZIhvcNAQEFBQAwVzELMAKG  
A1UEBhMCQkUxGTAXBgNVBAAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv  
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw0wNzA0MTEwMjAw  
MDBaFw0xNzA0MTEwMjAwMDBaMDYxETAPBgNVBAsTCFscGhhIENBMQ4wDAYDVQQK  
EwVBbHB0YTERMA8GA1UEAxMIQWxwaGEgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IB  
DwAwggEKAoIBAQC7Mi4rE/30JIpb+mvNq5yytguJauYfQc6KJEL/XK9fkD31kLlZ  
x3C0wso41q0GFRqA0B15K6VDIOe5+o0GIlcNZLXRTE0k0Em0agfUM9s7djg/r3dp  
73oTMyL7QISQNXhajyMpV2+wV6s3mZQoz9PHV6WwsYqBLn0AvWjsGxEXih7YlHdL  
dpHqtMwMwNiuAYaZWm+rNaXG6exJ6HAJVIvSbzaBAa6uLWmq0HLJYe2KNSJazQB  
dxq27N5Z3Jm7XdyPhMK5YgMTYwIJnuEJyL7xGHlxbcnQtUKXyvg@TZKHwDn6XCE9  
lFIEWoOp1KuDBSjYFyMkg2SbIS/40yt4ZIEtAgMBAAGjgfswwfgwDgYDVR0PAQH/  
BAQDAgEGMBIGA1UdEwEB/wQIMAYBAf8CAQAwHQYDVR00OBBYEFAop+q2vTf39XX12  
JoerqlqqdCIVMEoGA1UdIARDMEewPwYKKwYBBAGgMgEKCjAxMC8GCCsGAQUFBwIB  
FiNodHRwOi8vd3d3LmFscGhhc3NsLmNvbS9yZXBvc2l0b3J5LzAzBgNVHR8ELDAq  
MCigJqAkhijodHRwOi8vY3J5Lmdsb2JhbHNpZ24ubmV0L3Jvb3QuY3J5SMBEGCWCG  
SAGG+EIBAQQEAwICBDAfBgNVHSMEGDAWgBRge2YaRQ2XyoLQL30EzTSO//z9SzAN  
BgkqhkiG9w0BAQUFAAOCAQEArRW+NY5aM4tzqNt0v7l0aL6tyiRbYlCOKWw3wbIa  
8+vMHRZKs80ixuG2yNEupd6w1aXCdH0RhAHjE9jDJA7I8MeP0KBoAyUEjydW/VYV  
cnqhQ/LFzM/P260IDetpIdDDSqGDToVq4eH/2J82GG6QGc9BEsZWwR23240+yoF4  
sz9xD6vFRgSGa11L3Sejd2QWJ5GoMFQuDGUNJoHb55ogkC8Rxtt8JkpJshJcD2t  
Wkpkm21GAy9XKnfAPPQ3iVvDzDSg6HRV7gqnz8jAgCRx3x0L08FuNg520eNp3k5L  
5q0ZnsvMJiw101tpj5D24Zxnv5SjxxrgX6f4iE16EYABzw==  
-----END CERTIFICATE-----
```

```

MUST BE INSTALLED ON YOUR WEB SERVER:
Your SSL Certificate (Formatted for the majority of web server
software including IIS and Apache based servers):
-----BEGIN CERTIFICATE-----
MIIGNjCCBR6gAwIBAgIMaj+37mE/MCYQeC63MA0GCSqGSIb3DQEBCwUAMEwxCzAJ
BgNVBAYTAKJFMRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMSIwIAYDVQQDExlB
bHB0YVNTTCBDQSA0IFNIQTII1NiAtIEcyMB4XDITxMDcxMTE1NDcwMVoXDITyMDgx
MjE1NDcwMVoWHzEcmBoGA1UEAxMTYm9ib25jaWNPYm9uY2kubmFtZTCCASiWdQYJ
KoZiHvcNAQEBCQADggEPADCCAQoCggEBAMYLwa3ef0at8uYs84cmpy5u5+zHrM/l
/E2SNDId8J8KEh5zXyH9VoJ4kvmqa17HQ20Jj1C+X6CtJ4tzh6lefZJn253pvNKO
cWn4vutBtBmzPX4xvpLsKNU2Rq2HRCaaoL2g3tn16XUR9UlokyL1VqnPdtIMegt/
0zvADA8vbJwNJpm6p9r1nYluV0kKNRXT0J8AvSLXIWIIN5FK7RNatRRltrocMzm9t
PEMEjq6rHco7feNabWEeFR0ZcqPe8ON0kpmLvyZ7pP6pIDxgiNRLzp0J6eJolGht
U3cQZBMoaPDx9X5XRv8ds+4/qejsv3jMkwly0aBhvlp9aGoEJhhCR9kCAWEAAaOC
A0QwggNAMA4GA1UdDwEB/wQEAwIFoDCBiqYIKwYBBQUHAQEefTB7MEIGCCsGAQUF
BzACHjZodHRwOi8vc2VjdXJlMi5hbHB0YXNzbC5jb20vY2FjZXXJ0L2dzYWxwaGFz
aGEyZzJyMS5jcncQwNQYIKwYBBQUHMAGGKWh0dHA6Ly9vY3NwMi5nbG9iYWxzawdu
LmNvbS9nc2FscGhhc2hhMmcyMFCGA1UdIARQME4wQgYKKwYBBAGgMgEKCjA0MDIG
CCsGAQUFBwIBFiZodHRwczovL3d3dy5nbG9iYWxzawduLmNvbS9yZXBvc2l0b3J5
LzAIBGZngQwBAGewCQYDVDR0TBAIwADA+BgNVHR8ENZa1MD0gMaAvhilodHRwOi8v
Y3J5Mi5hbHB0YXNzbC5jb20vZ3MvZ3NhbHB0YXNoYTJnMi5jcmwwHgYDVDR0RBBcw
FYITYm9ib25jaWNPYm9uY2kubmFtZTAdBgNVHSUEFjAUBgggBgEgFBQcDAQYIKwYB
BQUHAWIwHwYDVDR0jBBGwFoAU9c3VPAhQ+WpP0reX2laD5mnSaPcwHQYDVDR0OBBYE
FOZYiILR0qZvnQqvNLZKgUttvzh/MIIBfQYKKwYBBAHwEQUIEAgSCAW0EggFpAwCA
dgBvU3asMfAxGdiZAKRRFf93FRwR2QLBACKGjbIImjfZEwAAAXqWQCLDAAAEAwBH
MEUCIEV9D0a+1Cwmujq0hU1jK6Gn7SrFK0Leh+e5febCgemdAIEA8upsa0Q2CW/j
z0oJdel0zyYFq6UEJW0CprA1owvX7qMAdgApeb7wnjk5IfBWc59jpXflvld9nGAK
r63dav6NKKHsp1400XnkybeUv4hiwgEKUwzBW8XcdHLYdykr3+nJHxyh7KGRHzhx
MMnJmOFmE2YIYFMS9AXLZreh/p0f3ZF0muUZmtmu5lfi3trRsSrDTVHpjjQOMJGH
/kYAF6MnnaULCg==
-----END CERTIFICATE-----

```

## 1. Masuk ke server ec2

```

Using username "ec2-user".
Authenticating with public key "imported-openssh-key" from agent
Last login: Wed Jul 14 21:51:36 2021 from 125.165.65.69

    _ _ _ _ _
   _ | _ _ _ | _
  _ | ( _ _ _ /   Amazon Linux AMI
 _ | \ _ _ | _ _ |

https://aws.amazon.com/amazon-linux-ami/2016.03-release-notes/
114 package(s) needed for security, out of 205 available
Run "sudo yum update" to apply all updates.
Amazon Linux version 2018.03 is available.
[ec2-user@mail ~]$

```

2. Buka direktori /etc/pki/tls/certs lalu lakukan backup pada file AlphaSSLroot.crt dan petossl.crt,

Penamaan file dapat menggunakan tahun aktif periode sblmnya

```
[ec2-user@mail ~]$ cd /etc/pki/tls/certs
[ec2-user@mail certs]$ ls
AlphaSSLroot.crt                make-dummy-cert             petossl.crt2019-2020
AlphaSSLroot.crt2019-2020      Makefile                    petossl.crt2020-2021
AlphaSSLroot.crt2020-2021      petossl.crt                 petossl.crt.bak
ca-bundle.crt                 petossl.crt.20170512        renew-dummy-cert
ca-bundle.trust.crt           petossl.crt2017-2019       server-chain.crt
[ec2-user@mail certs]$
[ec2-user@mail certs]$ cp AlphaSSLroot.crt AlphaSSLroot.crt2020-2021
[ec2-user@mail certs]$ cp petossl.crt petossl.crt2020-2021
```

3. Update file AlphaSSLroot.crt menggunakan command line lalu diisi dengan sertifikat intermediate AlphaSSL dari provider, dapat menggunakan nano / vim

```
[ec2-user@mail certs]$ nano AlphaSSLroot.crt
GNU nano 2.5.3
-----BEGIN CERTIFICATE-----
MIIEDjCCAvagAwIBAgILBAAAAAABHkS182UwDQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNPZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNPZ24gUm9vdCBDQTAeFw0wNzA0MTEzMjAw
MDBaFw0xNzA0MTEzMjAwMDBaMDYxETAPBgNVBAsTCFEScGhhIENBMQ4wDAYDVQQK
EwVBbHB0YTERMA8GA1UEAxMIQWxwagEgQ0EwggeEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQC7Mi4rE/30JIpb+mvNq5yytguJauYfQc6KJEL/XK9fkD31kLlz
x3C0wso41q0GFRqAOB15K6VDIOe5+o0GILcNZLXRTE0kOEm0agfUM9s7djq/r3dp
73oTMy17QISQNXhajyMpV2+wV6s3mZQoz9PHV6WwsYqBLnOAvWjsGxEXih7YlHdL
dpHqtMwWMwNiuAYaZWm+rNaXG6exJ6HAJVIvSbzaBAa6uLWmqOHLJYe2KNSJazQB
dxq27N5Z3Jm7XdyPhMK5YgMTYwIJnuEJyL7xGHlxbcnQtUKXyvg0TZKHwDn6XCE9
lFIEWoOp1KuDBSjYFyMkg2SbIS/4Oyt4ZIEtAgMBAAGjgfsWgfgwDgYDVR0PAQH/
BAQDAgEGMBIGA1UdEwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYEFaop+q2vTf39XX12
JoerqlqqdCIVMEoGA1UdIARDMEEWpWYKKwYBBAGgMgEKCjAxMC8GCCsGAQUFBwIB
FiNodHRwOi8vd3d3LmFscGhhc3NsLmNvbS9yZXBvc2l0b3J5LzAzBgNVHR8ELDAq
MCigJgAkhiJodHRwOi8vY3JsLmdsb2JhbHNpZ24ubmV0L3Jvb3QuY3JsMBEGCWCg
SAGG+EIBAQQEAWICBDAfBgNVHSMEGDAWgBRge2YaRQ2XyolQL30EzTSO//z9SZAN
BgkqhkiG9w0BAQUFAAOCAQEArRW+NY5aM4tzqNt0v7lOaL6tyiRbYlcOKWW3wbIa
8+vMhrZKs8OixuG2yNEupd6w1aXCdH0RhaHjE9jDJA7I8MePOKBoAyUEjydW/VYV
cnqhQ/lFzM/P260IDETpIdDDSqGDTToVq4eH/2J82GG6Qgc9BEsZWwR2324O+yof4
sz9xD6vFRgSGa11L3Sejd2QWJ5GoMFQuDGUNJoHb55ogkC8Rxt8JkpJshJcD2tt
Wkpkm21GAY9XKnfAPPQ3iVvDzDSg6HRV7gqnz8jAgCRx3x0L08FuNg52OeNp3k5L
5qOZnsvMJiW101tpj5D24Zxnv5SjxxrgX6f4iE16EYABzw==
-----END CERTIFICATE-----
```

4. Jika menggunakan nano, setelah mengupdate isi file crt tersebut, klik ctrl + x untuk save, confirm dengan mengetikkan "y" dan tekan enter untuk melakukan save file dengan nama yang sama

- Update file petossl.crt dengan code cert yang diberikan oleh pihak provider, yg harus di copy adalah cert dengan awalan

“Your SSL Certificate (Formatted for the majority of web server software including IIS and Apache based servers):”

```
[ec2-user@mail certs]$ nano petossl.crt
GNU nano 2.5.3

-----BEGIN CERTIFICATE-----
MIIGNjCCBR6gAwIBAgIMaj+37mE/MCYQeC63MA0GCSqGSIb3DQEBCwUAMEwxCzAJ
BgNVBAYTAkUFRMRkwFwYDVQQKEExBHBG9iYWxTaWduIG52LXNhMSIwIAYDVQQDEx1B
bHB0eYVNTTCBBDQSAIFNIQTl1NiAtIEcyMB4XDTIxMDcxMTE1NDcwMVVoXDTIyMDgx
MjE1NDcwMVVoHjEcmBoGA1UEAxMTYm9ib25jaWNpYm9uY2kubmFtZTCCASiWDQYJ
KoZIHvcNAQEBBQADgGEPADCCAQoCggEBAMYLwa3efOat8uYs84cmpy5u5+zHrM/1
/E2SNDId8J8KEh5zXyH9VoJ4kvmqal7Hq2OJj1C+X6CtJ4tzh6lefZJn253pvNKO
cWn4vutBtBmzPX4xvpLsKNU2Rq2HRCaaOL2g3tn16XUR9UlokyL1VqnPdtIMegt/
0zvADA8vbJwNjpm6p9r1nY1uv0kKNRXT0J8AvSLXIWIN5FK7RNatRRltrocMzm9t
PEMEJq6rHco7feNabWEeFR0ZcqPe8ON0kpmLvYz7pP6pIDxgiNRLzp0J6eJolGht
U3cQZBMoaPdx9X5XRv8ds+4/qejsv3jMkwly0aBhvlp9aGoEJhhCR9kCAWEAAaOC
A0QwggNAMA4GA1UdDwEB/wQEAwIFoDCBiQYIKwYBBQUHAQEETB7MEIGCCSGAQUF
BzAchjZodHRwOi8vc2VjdXJlMi5hbHB0eYXNzbC5jb20vY2FjZjZlZjZlZjZlZjZl
aGEyZzJyMS5jcncwNjY1KwYBBQUHMAGGKWh0dHA6Ly9vY3NwMi5nbG9iYWxzaWdu
LmNvbS9nc2FscGhhc2hhMmcyMFCGA1UdIARQME4wQgYKKwYBBAGGMEKcJA0MDIG
CCSGAQUFBwIBFiZodHRwczovL3d3dy5nbG9iYWxzaWduLmNvbS9yZXBvc2l0b3J5
LzAIBGZngQwBAGewCQYDVR0TBAlwADA+BGNVHR8ENzA1MDogMaAvhilodHRwOi8v
Y3J5Mi5hbHB0eYXNzbC5jb20vY2FjZjZlZjZlZjZlZjZlZjZlZjZlZjZlZjZl
FYITYm9ib25jaWNpYm9uY2kubmFtZTAdBgNVHSUEFjAUBgggrBgEFBQcDAQYIKwYB
BQUHAWIwHwYDVR0jBBgwFoAU9c3VPAHQ+WpPoreX2lad5mnSaPcwHQYDVR0OBBE
FOZYiILR0qZvvnQqVNLZKqUttvzh/MIIBfQYKKwYBBAAHwQIEAgSCAW0EggFpAWCA
dgBvU3asMfAxGdiZAKRRFF93FRWR2QLBACKgjbIImjFzEwAAAXqWQCLDAAAEAwBH
MEUCIEV9D0a+1Cwmujq0hU1jK6Gn7SrfK0Leh+e5febCgemdAiEA8upsa0Q2CW/j
z0oJdelOzyYFg6UEJWOCprAlowvX7qMAdgApeb7wnjk5IfBWc59jpXflvld9nGAK
+PlNXS2cJV3HhAAAAAXqWQCQWAAAEAwBHMEUCIQDPhbm0B1OnGIIdlBMoLo2/M6AI3
7SHyq5M89FCN39HMWAIGUF/LcW6OteQFvE1eeyPGs1HfEhKRobgovp971H1boQcA
dQBVgdTCFpA2AUrqC5tXFPFwOQ4eHALCBcvo6odBxPTDAAAXqWQCUnAAAEAwBG
MEQCIGMhiIDr+ZhKAaydT4tp4jYwB35rSwonrHMZfkbv4VbAiAQqfb8Q/acC9lu
+jUCJv2cK+UdggPTvxOm9k5uzsvUuJANBgkqhkiG9w0BAQsFAAOCAQEARCCsr5rH
sGohEdnqtLm68RxWvsUJoy0y40gYGkcuxk0Xfd/sfJ/MNZqv0EICYPPT503VQbL0
5NOFVLdy9rwJlRoQsckOu2Clq3cEpKYJJW0uG+Fzt+JULfvEi2mA46au/xKumQQd
3NgYtN/U9BoeBKf5qzEXdu2bd8CCqanhtJxWFAicnXNXQnVTYLqcW4i2OJW92iq0
r63dav6NKKHsp140OXnkybeUv4hiwgEKUwzBW8XcDHLydykr3+nJHxyh7KGRHzhx
MMnJmOFmE2YIYFMS9AXLZreh/p0f3ZF0muUZmtmu5lfi3trRsRdTVHppjJQOMJGH
/kYAF6MnnaULCg==
-----END CERTIFICATE-----
```

- Kemudian save dan confirm seperti langkah no.4

- Jikalau mendapat renewal cert menggunakan csr lama, maka file /etc/pki/tls/private/petossl.csr dan /etc/pki/tls/private/petossl.key tidak perlu diubah. Tetapi jika menggunakan csr baru dalam proses renewal maka harus dilakukan backup seperti 2 file sebelumnya, kemudian jalankan command :

```
openssl req -new -days 365 -x509 -nodes -newkey rsa:2048 -out /etc/pki/tls/certs/localhost.crt -keyout
/etc/pki/tls/private/localhost.key
```

“localhost” sendiri dapat diganti sesuai penamaan file cert, untuk ini maka diganti “petossl”



8. Lakukan pengecekan masa berlaku sertifikat yang telah diupdate dengan menjalankan command berikut :

```
[ec2-user@mail certs]$ openssl x509 -in /etc/pki/tls/certs/petossil.crt -noout -enddate
notAfter=Jul 14 06:31:16 2022 GMT
[ec2-user@mail certs]$ openssl x509 -in /etc/pki/tls/certs/AlphaSSLroot.crt -noout -enddate
notAfter=Jul 14 06:30:04 2022 GMT
[ec2-user@mail certs]$ openssl x509 -in /etc/ssl/certs/AlphaSSLroot.crt -noout -enddate
notAfter=Jul 14 06:30:04 2022 GMT
[ec2-user@mail certs]$ openssl x509 -in /etc/ssl/certs/petossil.crt -noout -enddate
notAfter=Jul 14 06:31:16 2022 GMT
[ec2-user@mail certs]$
```

9. Restart service httpd setelah mengupdate file-file cert SSL, command :

```
service httpd restart
```

10. Setelah direstart maka service dari project java akan berhenti, untuk memulai kembali maka ikuti instruksi pada pdf berikutnya ( Setup javaspring 8080 klo SSL abis Access EC2 fajar.pdf )
11. Jika terjadi masalah pada pengaksesan API yang masih terhalang SSL cek file /etc/httpd/conf.d/ssl.conf, cek row yg mengantuk kata server-chain.crt, kalau kondisi sedang di comment maka hapus tanda comment pada row tersebut. Untuk memastikan isi dr file /etc/pki/tls/certs/server-chain.crt dapat di cek pada web Alpha SSL

<https://support.globalsign.com/ca-certificates/intermediate-certificates/alphassl-intermediate-certificates>

Section AlphaSSL SHA-256 R1 Intermediate Certificate dan klik “view in base64”, copy isi konten ke dalam file server-chain.crt pada dir diatas.

12. Setelah selesai, untuk memastikan lakukan langkah 9 & 10 kembali

File pada dir /var/www yang di update jika update SSL :

1. /var/www/petossil.txt  
Berisikan seluruh code cert yang diberikan provider baik Alpha Root maupun petossil
2. /var/www/html/ssl.crt  
Berisi code cert yang memiliki awalan  
“Your SSL Certificate (Formatted for the majority of web server software including IIS and Apache based servers):”