Update SSL Peto AWS

OS : AWS Linux Webserver : Httpd

Cert Code from Provider:



MUST BE INSTALLED ON YOUR WEB SERVER: Your SSL <mark>Certificate (F</mark>ormatted for the majority of web server software including IIS and Apache based servers): ----BEGIN CERTIFICATE----MIIGNjCCBR6gAwIBAgIMaj+37mE/MCYQeC63MA0GCSqGSIb3DQEBCwUAMEwxCzAJ BgNVBAYTAkJFMRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMSIwIAYDVQQDExlB bHBoYVNTTCBDQSAtIFNIQTI1NiAtIEcyMB4XDTIxMDcxMTE1NDcwMVoXDTIyMDgx MjE1NDcwMVowHjEcMBoGA1UEAxMTYm9ib25jaWNpYm9uY2kubmFtZTCCASIwDQYJ KoZIhvcNAQEBBQADggEPADCCAQoCggEBAMYLwa3ef0at8uYs84cmpy5u5+zHrM/l /E2SNDId8J8KEh5zXyH9VoJ4kvmqal7HQ2OJj1C+X6CtJ4tzh6lefZJn253pvNKo cWn4vutBtBmzPX4xvpLsKNU2Rq2HRCaaoL2g3tn16XUR9UlokyL1VqnPdtIMegt/ @zvADA8vbjwNJpm6p9r1nYluv@kKNRXTOJ8AvSLXIWIN5FK7RNatRRLtrocMzm9t PEMEjq6rHco7feNabWEeFR0ZcqPe8ON0kpmLvyZ7pP6pIDxgiNRLzp0J6eJolGht U3cQZBMoaPDx9X5XRv8ds+4/qejsv3jMkw1y0aBhvlp9aGoEJhhCR9kCAwEAAa0C A0QwggNAMA4GA1UdDwEB/wQEAwIFoDCBiQYIKwYBBQUHAQEEfTB7MEIGCCsGAQUF BzAChjZodHRw0i8vc2VjdXJlMi5hbHBoYXNzbC5jb20vY2FjZXJ0L2dzYWxwaGFz aGEyZzJyMS5jcnQwNQYIKwYBBQUHMAGGKWh0dHA6Ly9vY3NwMi5nbG9iYWxzaWdu LmNvbS9nc2FscGhhc2hhMmcyMFcGA1UdIARQME4wQgYKKwYBBAGgMgEKCjA0MDIG CCsGAQUFBwIBFiZodHRwczovL3d3dy5nbG9iYWxzaWduLmNvbS9yZXBvc2l0b3J5 LzAIBgZngQwBAgEwCQYDVR0TBAIwADA+BgNVHR8ENzA1MDOgMaAvhilodHRw0i8v Y3JsMi5hbHBoYXNzbC5jb20vZ3MvZ3NhbHBoYXNoYTJnMi5jcmwwHgYDVR0RBBcw FYITYm9ib25jaWNpYm9uY2kubmFtZTAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYB BQUHAwIwHwYDVR0jBBgwFoAU9c3VPAhQ+WpP0reX2laD5mnSaPcwHQYDVR00BBYE FOZYiILR0qZvnQqvNLZKgUttvzh/MIIBfQYKKwYBBAHWeQIEAgSCAW0EggFpAWcA <u>dqBvU3as</u>MfAxGdiZAKRRFf93FRwR2QLBACkGjbIImjfZEwAAAXqWQCLDAAAEAwBH MEUCIEV9D0a+1Cwmujq0hU1jK6Gn7SrFK0Leh+e5febCgemdAiEA8upsa0Q2CW/j z@oJdel0zyYFq6UEJW0CprAlowvX7qMAdgApeb7wnjk5IfBWc59jpXflvld9nGAK r63dav6NKHHsp1400XnkybeUv4hiwgEKUwzBW8XcDHLYdykr3+nJHxyh7KGRHzhx MMnJmOFmE2YIYFMS9AXLZreh/p0f3ZF0muUZmtmu5lfi3trRsSrDTVHpjjQ0MJGH /kYAF6MnnaUlCa== ----END CERTIFICATE----

1. Masuk ke server ec2

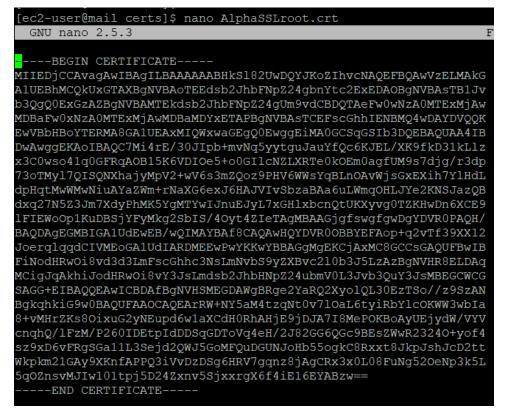
```
Using username "ec2-user".
Authenticating with public key "imported-openssh-key" from agent
Last login: Wed Jul 14 21:51:36 2021 from 125.165.65.69

___| __| __| / Amazon Linux AMI
___|\__| __| / 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

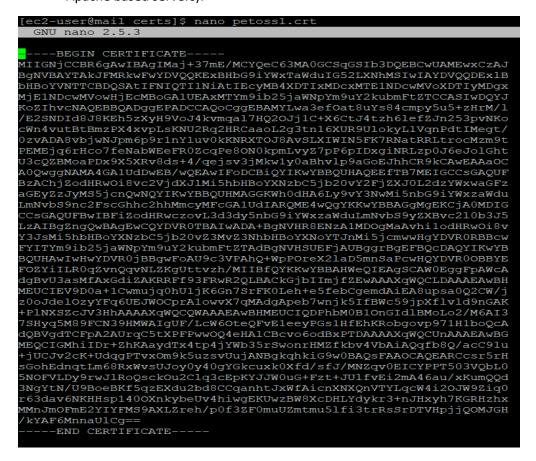
```
[ec2-user@mail ~]$ cd /etc/pki/tls/certs
[ec2-user@mail certs]$ ls
AlphaSSLroot.crt make-dummy-cert petossl.crt2019-2020
AlphaSSLroot.crt2019-2020 Makefile petossl.crt2020-2021
AlphaSSLroot.crt2020-2021 petossl.crt petossl.crt.bak
ca-bundle.crt petossl.crt.20170512 renew-dummy-cert
ca-bundle.trust.crt petossl.crt2017-2019 server-chain.crt
[ec2-user@mail certs]$
ca bandre.trust.crt petossl.crt2017-2019 server-chain.crt
[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 diisikan dengan sertifikat intermediate AplhaSSL dari provider, dapat menggunakan nano / vim



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):"



- 6. Kemudian save dan confirm seperti langkah no.4
- 7. 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:



"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/petossl.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/petossl.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:



- 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:

- /var/www/petossl.txt
 Berisikan seluruh code cert yang diberikan provider baik Alpha Root maupun petossl
- /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):"