RENEWAL OF HLF PEER TLS CERTIFICATE

Date: 29nd June 2023

Submitted by

KRYPC TECHNOLOGIES

The steps to be followed to renewal the HLF peer TLS certificate

Step 1: Follow below step to update the hlf binaries

a) Remove bin and config directory

```
$ cd VM-Model-iSHARE-Satellites
$ rm -rf bin
$ rm -rf config
```

b) Download the updated binaries (it will create bin and config directory for hlf)

```
$ curl https://raw.githubusercontent.com/hyperledger/fabric/master/scripts/
bootstrap.sh |   bash -s -- 2.2.0 1.4.9 -d -s
```

Step 2: update the fabric ca server

```
$ cd VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>/fabric-ca
```

a) open docker-compose-fabric-ca.yaml in text editor

b) change docker to image: hyperledger/fabric-ca:1.4.9 and save it

If the certificate issuance expiry to be expended by changing the below values in the docker-compose-fabric-ca.yaml

- FABRIC_CA_SERVER_SIGNING_DEFAULT_EXPIRY=**87600h**
- FABRIC_CA_SERVER_SIGNING_PROFILES_TLS_EXPIRY=**87600h**

Note : 87600h = 10 years

```
$ docker-compose  -f docker-compose-fabric-ca.yaml down
$ docker-compose -f docker-compose-fabric-ca.yaml up -d
```

Step 3: Bring Peers down

```
$ cd /<full-path-project>/VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>/peers
$ docker-compose -f docker-compose-hlf.yaml down
```

Step 4: Take backup of fabric ca server data and crypto materials

a) locate your crypto directory below

```
$ cd VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>
$ zip -r crypto-bakup.zip  crypto
```

b) take backup of fabric ca server data

```
$ cd VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>/fabric-ca

$ docker-compose -f docker-compose-fabric-ca.yaml down

$ sudo zip -r docker-data-fabric-ca.zip docker_data

$ docker-compose -f docker-compose-fabric-ca.yaml up -d
```

Step 5: Intialize fabric-ca-client client

```
$ cd VM-Model-iSHARE-Satellites

$ export PATH=$PATH:<path-to-hlf-bin-directory>
```

a) Now you should be able access fabrica-ca-client via terminal (version should refer to v1.4.9)

Note: Replace the placeholders for all the below commands

```
$ fabric-ca-client version
```

Step 6 : Renew Admin user TLS certs

```
$ export FABRIC_CA_CLIENT_TLS_CERTFILES=/<full-path-project>/VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>/crypto/fabca/ca-admin/tls/tlscacerts/tls-localhost-7054.pem

$ export FABRIC_CA_CLIENT_HOME=/<full-path-project>/VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>/crypto/users/Admin@<satellite>

$ export FABRIC_CA_CLIENT_MSPDIR=/<full-path-project>/VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>/crypto/users/Admin@<satellite>/tls

$ fabric-ca-client reenroll -u https://Admin:<enrollment secret>@localhost:7054 --csr.hosts "Admin" --enrollment.profile tls –csr.keyrequest.reusekey
```

Note : <enrollment secret> - can be find inside the script directory in global.sh file

Step 7: Renew Peer0 TLS certs

```
$ export FABRIC_CA_CLIENT_TLS_CERTFILES=/<full-path-project>/VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>/crypto/fabca/ca-admin/tls/tlscacerts/tls-localhost-7054.pem

$ export FABRIC_CA_CLIENT_HOME=/<full-path-project>/VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>/crypto/peers/peer0.<org-domain>
$ export FABRIC_CA_CLIENT_MSPDIR=/<full-path-project>/VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>/crypto/peers/peer0.<org-domain>/tls
```

```
$ fabric-ca-client reenroll -u https://peer0.<org-domain>:<enrollment secret>@localhost:7054 --csr.hosts "peer.<satellite>,peer0.<org-domain>" --enrollment.profile tls –csr.keyrequest.reusekey
```

Note : <enrollment secret> - can be find inside the script directory in global.sh file

Step 8: Replace the new TLS cert with old one for peer0

```
$ rm -f /<full-path-project>/VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>/crypto/peers/peer1.<org-domain>/tls/server/cert.pem
```

```
$ cp /<full-path-project>/VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>/crypto/peers/peer0.<org-domain>/tls/signcerts/cert.pem  /<full-path-project>/VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>/crypto/peers/peer0.<org-domain>/tls/server/cert.pem
```

Use the below command to view the certificate expiry

```
$ openssl x509 -in /<full-path-project>/VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>/crypto/peers/peer0.<org-domain>/tls/server/cert.pem -noout -text
```

Step 9: Follow above step for Peer1 as well

```
$ export FABRIC_CA_CLIENT_TLS_CERTFILES=/<full-path-project>/VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>/crypto/fabca/ca-admin/tls/tlscacerts/tls-localhost-7054.pem
```

```
$ export FABRIC_CA_CLIENT_HOME=/<full-path-project>/VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>/crypto/peers/peer1.<org-domain>
```

```
$ export FABRIC_CA_CLIENT_MSPDIR=/<full-path-project>/VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>/crypto/peers/peer1.<org-domain>/tls
```

```
$ fabric-ca-client reenroll -u https://peer1.<org-domain>:<enrollment secret>@localhost:7054 --csr.hosts "peer.<satellite>,peer1.<org-domain>" --enrollment.profile tls --csr.keyrequest.reusekey
```

Note : <enrollment secret> - can be find inside the script directory in global.sh file

Step 10: Replace the new TLS cert with old one for peer1

```
$ rm -f /<full-path-project>/VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>/crypto/peers/peer1.<org-domain>/tls/server/cert.pem
```

```
$ cp /<full-path-project>/VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>/crypto/peers/peer1.<org-domain>/tls/signcerts/cert.pem  /<full-path-project>/VM-Model-
```

iSHARE-Satellites/hlf/<env>/<satellite>/crypto/peers/peer1.<org-domain>/tls/server/cert.pem

Step 11 : Once tls certs are renewed, Bring the peers up again

```
$ cd /<full-path-project>/VM-Model-iSHARE-Satellites/hlf/<env>/<satellite>/peers

$ docker-compose -f docker-compose-hlf.yaml up -d
```