FabGUI Documentation

Release latest

Sep 27, 2018

Contents

CHAPTER 1

A GUI Client for Fabric-CA

FabGUI is a graphical client for Fabric CA Command Line tools which are part of the Hyperledger Fabric. The code is written in python. Packages used in this script are Tkinter for the User Interface and ruamel.yaml for reading and modifying YAML files.

1.1 Requirements

- Python 3
- ruamel.yaml python package
- Path Variable "CAPATH" which points to location of docker container having Fabric-CA Server in the file system.

1.2 Introduction

The GUI can handle both the server and the client functions. Login button starts the server. A popup will signal successful start of the Server. The end server button can be used to shut the server down.

The command used to start the server is `fabric-ca-server start -b <usr>:<pass>`

The command used to shut the server down is `docker rm -f $(docker ps -aq)`

1.3 Functionality

The client has to provide to the address of the server to connect to it. Once the user is connected to the server he/she is provided with a landing page, where all the main functionality is available. Some of the main functions are:

1. Enroll
2. Register

3. Revoke
4. Generate CRL
5. Modify
6. Remove

All of the above functions are described in detail below.

1.4 Enroll

The enroll command is used for enrolling an identity into the system. The admin CA issues these certificates. The enroll command stores an Enrollment Certificate, private key and CA certificate PEM files in the Fabric CA clients MSP directory. The command used for this is `fabric-ca-client enroll -u http://admin:adminpw@localhost:7054` The details for the identity to be enrolled is specified in the corresponding YAML file

1.5 Register

The register command is used for registering an identity to the Fabric CA. The identity performing the register request must have the proper authority to register the type of identity that is being registered. The command used for registering an identity to the Fabric CA is:

```
export FABRIC_CA_CLIENT_HOME=$HOME/fabric-ca/clients/admin
```

```
fabric-ca-client register --id.name user1 --id.secret user1pw --id.type user
--id.affiliation org1 --id.attrs attrs
```

The register command allows the admin to sign the certificate along with a number of attributes. The admin can only sign for attributes which the admin possess in the admins certificate. This is a list of attributes that can be registered for an identity: -

hf.Registrar.Roles

hf.Registrar.DelegateRoles

hf.Registrar.Attributes

hf.GenCRL

hf.Revoker

hf.AffiliationMgr

hf.IntermediateCA

The register command uses the admins credentials to sign the certificate. The password, also known as the enrollment secret, is printed. This password is required to enroll the identity. This allows an administrator to register an identity and give the enrollment ID and the secret to someone else to enroll the identity.After registering an identity with the CA server, we can use the enroll function again to enroll the identity to the system. The home directory of the identity should be set and the enroll command generates the certificates along with the corresponding certificates in the MSP folder structure as specified by Fabric CA.

1.6 Attribute Based Access Control

This feature allows the chaincode to extract specific attributes from the certificate. While enrolling a client custom attributes can be added to the certificate with a ":ecert" suffix that inserts the attribute by default into the certificate. The custom attributes can be suffixed to the register command as shown:

```
fabric-ca-client register --id.name user1 --id.secret user1pw --id.type user
--id.affiliation org1 --id.attrs 'custAttr1=value:ecert,custAttr2=value'
```

Here the custAttr1 and custAttr2 are stored in the certificate of the identity. The chaincode can request for these attributes and evaluate them. Based on the values it can decide the course of action required for running the chaincode.

1.7 Revoke Certificates

Revoke certificates function is used for revoking the certificates of a user. It takes the enrollment ID as the input along with a reason for revocation. The directory of the MSP certificates have to be specified for this function. The command for revoking is :

```
fabric-ca-client revoke -e name -r reason
```

1.8 Generating Certificate Revocation List (CRL)

The appropriate MSPs have to be updated in the Fabric after the certificates of an identity have been revoked. The certificate revocation list can be generated for the certificates which have been revoked. To enable this PEM encoded files have to be placed in the MSPs of all peers. The Generate CRL function is used for generating CRLs. The destination of the generated CRL can be selected using the GUI. The command used for generating the CRL is:

```
fabric-ca-client gencrl -M ~/msp
```

1.9 Modify

The modify command allows the user to modify the credentials of an existing user and regenerate the certificates in the MSP directory format. Single or multiple attributes can be changed using the interface. Any element of an identity that is not modified will retain its original value. The command used for this function is :

```
fabric-ca-client identity modify user1 --secret <newsecret> --affiliation
<org> --type <type> --attrs <newattrs> --maxenrollments <value>
```

1.10 Remove

The Remove option allows the user to remove identities from the trusted store. It removes the identity and also revokes all the certificates. Removal of identities is disabled in the fabric-ca-server by default, but may be enabled by starting the fabric-ca-server with the `-cfg.identities.allowremove` option.

The command to remove an identity is : `fabric-ca-client identity remove user1`

1.11 Last Tidbits

The client configuration YAML file has been hard coded into the python script. So it can be generated on demand in the required location. This is required in many places where the file may not already be existing. Multiple instances can be generated for the GUI application to act as server and client.