Hyperledger Fabric Certificate Authority

Introduction

The Hyperledger Fabric CA is a Certificate Authority for Hyperledger Fabric which acts as a tool using which you can generate certificates.

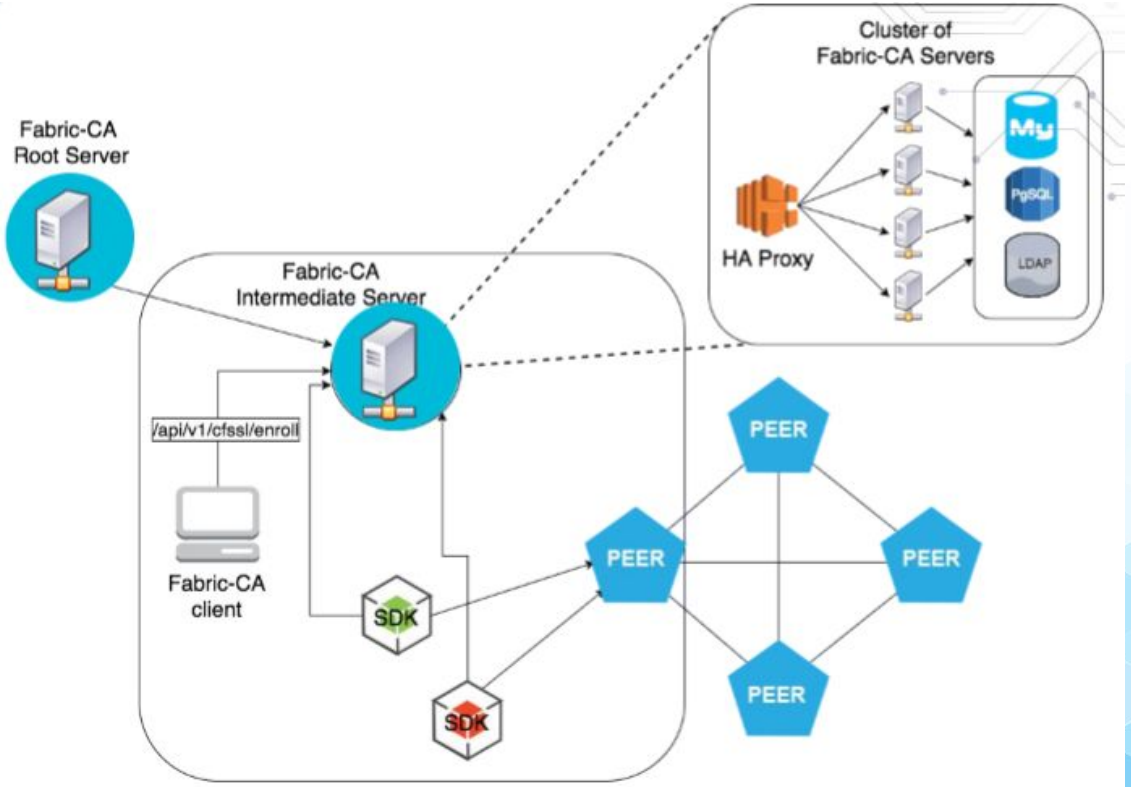
You can generate certificates by specifying the username, password and affiliations which is called Enrollment.

It provides functionalities such as:

- Certificate renewal and revocation
- Registration of identities, or connects to LDAP as the user registry
- Issuance of Enrollment Certificates

Hyperledger Fabric CA consists of both components a client and a server.

Fabric CA Architecture



Fabric CA Architecture

Fabric-CA root Server is the root node of the entire tree.

You can interact with Fabric-CA Server via:

- Fabric-CA Client or,
- Fabric SDKs

The client routes to an HA Proxy endpoint which load balances traffic to one of the fabric-ca-server cluster members.

All CA servers in a cluster share the same database like MySql, PostgreSQL for storing identities and certificates.

If LDAP(Lightweight Directory Access Protocol) is configured, the identity information is kept in it rather than the database.

Features of Certificate Authority

The CA (Fabric CA by default) issues:

- a root certificate (rootCert) to each member that is authorized to join the network.
- an enrollment certificate (eCert) to each member component, server-side applications and occasionally users.
- a transaction certificate (tCerts), each tCert authorizes one network transaction.

The requirement for a permissioned identity for every user enables ACL-based control over network activity, and guarantees that every transaction is ultimately traceable to a registered user.

This certificate-based control over network membership and actions enable members to restrict access to private and confidential channels, applications, and data, by specific user identities.