

MQTT Cont...

MQTT Security

Applying Username and password based restriction on broker

// first stop the mosquitto broker, if it is running

>> sudo service mosquitto stop

There are two methods to create a password file, having password encrypted with hash code

First method :

#creating a file passwd inside the mosquitto directory with username and password (encrypted with hashcode)

#Using mosquitto_passwd utility

sudo mosquitto_passwd -c /etc/mosquitto/passwd <user_name>

#it will prompt to enter password twice #enter and remember

// It will create a password file named passwd in /etc/mosquitto directory

//simple check that file is created or not??

>> cd /etc/mosquitto

>> ls

// open the mosquitto.conf file with any editor, say nano

>> nano /etc/mosquitto/mosquitto.conf

// add these two entries in bottom

```
password_file /etc/mosquitto/passwd // password file path
allow_anonymous false // not to allow anonymous users
without username and pass.
```

#Restart the broker with mosquitto.conf file

```
sudo mosquitto -c /etc/mosquitto/mosquitto.conf -d
```

#Add more username and password in the same file

```
sudo mosquitto_passwd -b /etc/mosquitto/passwd cdac cdac123
```

#above line will add cdac and cdac123 username and password respectively in passwd file located at mosquitto directory

restart the broker to reflect the changes with configuration file

```
sudo mosquitto -c /etc/mosquitto/mosquitto.conf -d
```

Explore other options to delete a user from the file with -D flag

```
mosquitto_passwd --help
```

Second method :

create a file say - passwd

```
sudo nano /etc/mosquitto/passwd
```

#enter username:password (multiple username and password allowed)

cdac:cdac123

desd:desd123

#save it,

#cdac and desd are two users and cdac123 and desd123 are passwords.

#encrypt the passwords in hashcode format

sudo mosquitto_passwd -U /etc/mosquitto/passwd

cat passwd #observe the contents

@repeat the above steps to restart the borker

sudo mosquitto -c /etc/mosquitto/mosquitto.conf

Test that now mosquitto_pub (publisher) and mosquitto_sub (subscriber) are only able to connect with broker only with correct username and pass else connection refused shall return.

mosquitto_pub -t cdac/acts -u cdac -P cdac123 -l

u - username , -P - paasword (P in caps)

mosquitto_sub -t cdac/acts -u cdac -P cdac123

some basic commands to start stop and check status of mosquitto

sudo service mosquitto start #last argument (start/stop/status)

sudo systemctl start mosquitto #start/stop/status

sudo /etc/init.d/mosquitto start #stop/status