A diagram of a diagram

Description automatically generated

**1 –** To prove that we are the owner of the domain, we need to validate the domain on AWS. Go to AWS > Certificate Manager (ACM) > Request Certificate > Request Public Certificate and fill your domain information. After this point you will see a Certificate in Pending Validation status which ha a CNAME name and CNAME value variables. For CNAME name, remove the domain part at the end and for the value copy the whole value.

Go to your domain name provider site and create a new DNS record. Paste the CNAME name and value of your domain. In a while, in AWS you will see that the status of certificate is Issued.

2 – For communication between layers, we will create three Security Groups as follows;

* SG\_ALB\_PRJ3 (allow inbound 443 from any)
* SG\_Tomcat\_PRJ3 (allow inbound 8080 from SG\_ALB\_PRJ3)
* SG\_Backend\_PRJ3 (allow inbound 3306 from SG\_Tomcat\_PRJ3 for MySQL)
* SG\_Backend\_PRJ3 (allow inbound 11211 from SG\_Tomcat\_PRJ3 for Memcached)
* SG\_Backend\_PRJ3 (allow inbound 5672 from SG\_Tomcat\_PRJ3 for Rabbit MQ)
* SG\_Backend\_PRJ3 (allow all traffic from SG\_Backend\_PRJ3 for Backend Communication)

Additionally we need to add access to these 2 SGs from our IP over the ports 8080 and 22.

* SG\_Tomcat\_PRJ3 (allow inbound 8080 and 22 from my-ip)
* SG\_Backend\_PRJ3 (allow inbound 8080 and 22 from my-ip)

If you don’t have static IP, you may always be sure that your IP is still same.

3 – Now let’s create key-pairs (public and private key) for connecting to the instances. If your git repository is not private, then add the key-pair as expection.