**Assignment 4:**

1. What is the need of IAM?

**Ans**- Identity and Access Management is a web service offered by Amazon web services. We can create users and groups and grant them authentication and authorization to use resources by defining policies.

2. If i am a non tech person, how will you define policies in IAM.

**Ans**- Policies are used to set boundaries on authentication and authorization. Let’s imagine you are a non-tech person so using inline policies the root/admin will give you the least authentications so that you will be restricted to use the features which are not relevant and it will help the organization to be in control of their budget and unnecessary billing.

3. Please define a scenerio in which you would like to create

your on own IAM policy.

**Ans-** Lets consider we have a group of developers, Gabbar, Kali and samba and we want to give some authentication and authorization to all users. So, we will attach the required policy at the group level so that the policy will get applied to every single member of the group.

4. Why do we prefer not using root account?

**Ans**- As we already know there are two types of users

1. Root user
2. Normal user.

The root user is the super user and we can run any command with this privilege. If hackers know the root account info and they would target the root account to breach in. By mistakenly if we run any wrong command, we will not get any time to think twice.

5. How to revoke policy for an IAM user?

**Ans-** We can remove user policy from the group level and user level.

For example- let’s assume Babua is added to a tester group so all applied policies to the group are being applied to Babua. If we remove Babua from the group level policies will get removed.

If babua is a single user and has few policies. we can remove the policies by following

* (Users- Select babua – Permissions – remove the policies)
* We can set expire Date and time of any policies

6. Can a single IAM user be a part of multiple policy via group

and root? how?

**Ans**-Yes, a single IAM user can be a part of multiple policies via group and root as we can attach the policy to an “X” group that would be applied to the user belonging to that group, and by root, we can attach one inline policy to the same user.