Name: Anand Kumar Gupta Email id: ananddkg99.9@gmail.com

Assignment 4

Q1) What is the need of IAM?

IAM stands for Identity and access management. As the name indicates, it used to provide identity and can be either (user, group, or role).Now, based on these identities, we define what they can access and what they can't using policies. A user can be in multiple groups, but a group can't be in another group. A role is used for temporary access to an AWS service.

In large organizations, it is very necessary to maintain their users via the IAM service. Place users as per their role in a particular group and on that group assigning a particular set of policies by following the "least privileged access " principle.

Q2) If I am a non tech person, how will you define policies in IAM?

IAM policies are nothing but a set of rules or boundaries that we define for IAM identities (users, groups, or roles).
We have two types of policies:
(a) IAM based policies(predefined); (b)Custom based policies i.e that we define

---

Q3) Please define a scenario in which you would like to create your own IAM policy.

Basically, we define our own custom policy when we can't achieve our desired result just by using the predefined IAM policy. So we have to either modify the predefined IAM policy or write it from scratch.

Example: If we want to access a S3 bucket from a particular region, that user should also belong to a particular tag, like: admin, developer.

Q4) Why do we prefer not using root account?

If another person is also there who has root credentials, he can perform the followings:
He can create, rotate, disable, or delete access keys for your AWS account. He can also change your root user password.

Anyone who has root user credentials for your AWS account has unrestricted access to all the resources in your account, including billing information.
That is why it is advisable to grant someone admin access but not root access.

Q5) How to revoke policy for an IAM user?

Click on user->go to permissions->click on the policy which we want to revoke->click on detach option

---

Q6) Can a single IAM user be a part of multiple policy via groupand root? how?

Yes, a single user can be part of multiple policies.
(a) If that user is in a group or in multiple groups. As a general rule, groups have multiple policies.
(b) If root directly assigns multiple policies to that user.