**1. What is the need of IAM?**

IAM (Identity and Access Management) is a important service provided by AWS necessary for securely managing user access and permissions to various AWS resources in a centralized manner. In addition to this IAM also provides auditablity; by providing logs user activities, scalability; by providing seamless integrations with external identity providers.

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

To a non tech person IAM policies could be explained as a rulebook that mentions what a user, group or role can do with an AWS resource. It defines what level of access someone has and what actions they can perform on AWS. These rules are written in JSON Format. All this can be understood with an analogy like say, we have a security guard at the entrance of our building. The guard has a set of instructions that determine who can enter the premise and what they can do. Similarly here IAM guards the digital resources of AWS.

**3. Please define a scenerio in which you would like to create your on own IAM policy.**

A good scenario to create my own IAM policy could be when we wish to provide access of our AWS environment to some third-party. Say we hire a consultancy firm to optimize our infrastructure. That would best point to create a policy that follows principle of least privilage. Using a IAM policy we could provide temperoray access to the areas of AWS we want to optimize.

**4.Why do we prefer not using root account?**

There are several reasons for which using root account on AWS is not preferred, few of them being:

*i) Security:* root account has unrestricted access to all AWS resources, thereby making vulnerable to attackers. It incluse risks like data breach, unauthorized access and potential misuse of resources.

*ii) Principle of least privilage:*  the principle means that a user shall be given minimum level of access required to perform their task. Since root account has access to all the resources on AWS, the principle is violated.

*iii) Accountability:* If everyone prefers to use the root account for performing their tasks, it becomes difficult to audit actions of each individual. By creating separate IAM users, auditing of user actions becomes simpler as each action is logged for accountability. This helps in troubleshooting, and investigating security incidents.

**5. How to revoke policy for an IAM user?**

For revoking policy of an IAM user,

i) one must log in to the AWS Console with an IAM account having access administrate IAM.

ii) Thereafter, open the IAM section on AWS and switch to users tab selecting from the left.

iii) Now select the user whose policy is to revoked.

iv) In there scroll down to permissions policy section, which would list multiple policies linked to the IAM user.

v) Now select the policy which is to revoked.

vi) Finally click “remove” and confirm the policy removal on the next pop up.

vii) The policy is now revoked

**6. Can a single IAM user be a part of multiple policy via group and root? How?**

Yes it is possible to assign multiple policies to an IAM user via group, as these policies won’t be directly linked to the user, instead the policies are assigned to a group and since multiple user can belong to a group. Those policies of a group would be linked to the IAM user.