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

Identity and Access Management (IAM) is a growing field focused on ensuring that data shared across your organization is accessible to the right people, and remains inaccessible to those who should not have access to it. We need to use IAM because, as cybersecurity threats increase and the complexity of data analysis and risk management expand across the organization, as does the need for robust systems that protect different types of user information and the data it is designed to access. In the wake of a growing remote workforce, because of the pandemic, the importance of IAM solutions has surged.

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

If you are a non tech person, we can attach identity-based policies so that you can be added to a group of non-tech person which is already existing, without getting the permissions for code or any technical aspects. We can set permission boundaries so you can get only the permissions from your entity.

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

Consider if we have a situation of creating and adding policies which are not covered in pre-built policies of amazon. Like sometime, if dev has created a new user below him to check on something, We would require some own IAM policies so that we can keep a track of it.

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

Root account is like power of thanos, If anyone get to know the root account he can cause many problems like deleting the instances, breaching the data, and much more. So we don’t use root account for operations which is too powerful

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

In the navigation pane, choose Roles, and then choose the name (not the check box) of the role whose permissions you want to revoke.

On the Summary page for the selected role, choose the Revoke sessions tab.

On the Revoke sessions tab, choose Revoke active sessions.

AWS asks you to confirm the action. Select the I acknowledge that I am revoking all active sessions for this role. check box and choose Revoke active sessions on the dialog box.

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

Yes single IAM user can be a part of multiple policy via group and root. As it defines that user what all operations he can perform with specific rules and policies for each policy he has been added to. We just need to select the policies which we need to give the user and if we can administrator permission to the user, He almost gets power of root.