Question:- What is the need of IAM?

Answer:- Identity and access management, or IAM, is the security discipline that makes it possible for the right entities (people or things) to use the right resources (applications or data) when they need to, without interference, using the devices they want to use.

Question:- If I am a non tech person, how will you define policies in IAM.

Answer:- An AWS IAM policy defines the permissions of an identity (users, groups, and roles) or resource within the AWS account. An AWS IAM policy regulates access to AWS resources to help ensure that only authorized users have access to specific digital assets.

Question :- Please define a scenerio in which you would like to create your on own IAM policy.

Answer:- If our company has created the project and deployed it on AWS and I've to share project to junior DevOps engineer and I only want to give certain access to for that project then this way IAM will be useful.

Question:- Why do we prefer not using root account?

Answer:- A root user (identity) has full access to all the resources and assets in the account and associated instances. This explains the risk they represent if compromised.

Question:- How to revoke policy for an IAM user?

Answer:-

Step 1:- Sign in to AWS management console and open IAM console

Step 2:- In the navigation pane choose Roles and then choose name of the roles of the permission you want to revoke

Step 3:- On the **Summary** page for the selected role, choose the **Revoke sessions** tab.

Step 4:- On the Revoke sessions tab, choose Revoke active sessions.

Step 5:- AWS will ask you to confirm the action. Select the I acknowledge that I am revoking all active sessions for this role check box and now choose Revoke sessions on the box.

Question:- Can a single IAM user be a part of multiple policy via group and root? how?
Answer:- A group and root can be part of multiple IAM policy. A set of IAM users is known as an IAM user group. It may be simpler to manage the permissions for those users if you can define permissions for many users through user groups. You could, for instance, create a user group called "Admins" and grant it the standard administrator access. Each member of the user group has access to the Admins group by default. You can grant the necessary permissions to a new user that joins your company and needs administrator rights by adding the user to the Admins user group. Instead of changing the user's rights if they shift employment within your company, you can take them out of the outdated user groups and put them to the necessary new user groups.