Assignment Interview question

1. What is the need of IAM?
A. IAM basically allows us to make multiple users with different permission and policy. So for any organisation to stop the misuse of any resource or object in the AWS panel we make IAM users granting them specific permission to have access to that specific service in AWS only.

2. If i am a non tech person, how will you define policies in IAM.
A. IAM policies are like a set of rules for who can access certain things in a company or organization. It's like a set of keys for a building, where some people have a key to just one room and others have access to the whole building.

For example, let's say you work at a company that has a shared drive on the company's computer network. The shared drive contains sensitive company information, such as financial reports and customer data. The company's IAM policies would determine who has access to the shared drive and what they can do with the information on it. CEO, may have full access to everything on the shared drive. But, other employees may only have read access, which means they can only view the files on the drive but not make any changes to it. And some employees may not have access to the drive at all.

3. Please define a scenerio in which you would like to create your on own IAM policy.
A. Let's say I am building a new web application that allows users to upload and download files. The application will store the files on a cloud-based data storage service, such as S3. I will need to create an IAM policy to control access to the S3 bucket where the files are stored. I will create a new IAM policy that allows the web application to read and write files to the S3 bucket. I will also specify that only certain users, such as the application's administrators, will have access to the S3 bucket and its contents.

4. Why do we prefer not using root account?
A. The root account on AWS is the highest level of access to an AWS account, and it has full permissions to perform any action and access any resource in the account. It is generally considered best practice not to use the root account for everyday tasks or to allow other users to log in to the root account. It is majorly due to security issues, cost issue, etc.

5. How to revoke policy for an IAM user?
A. To revoke a policy for an IAM user, you can do the following steps:

- Sign in to the AWS Management Console and navigate to the IAM service.
- In the navigation pane, click on "Users" to view the list of all IAM users.
- Select the user for which you want to revoke the policy and click on "Permissions" tab.
- In the "Permissions" tab, you will see a list of policies currently associated with the user.
- Select the policy that you want to revoke and click on "Remove Policy" button. Confirm the action by clicking on "Delete" button.
- The policy will now be removed from the user, and the user will no longer have the permissions associated with that policy.

6. Can a single IAM user be a part of multiple policy via group and root? How?
A. Yes, a single IAM user can be a part of multiple policies by being a member of multiple groups and by having policies directly attached to the user.

Here's how it works:

- Creating IAM Groups: IAM groups are a way to organize IAM users by role. You can create an IAM group, then attach policies to the group, and then add IAM users to the group. When an IAM user is a member of a group, they inherit the permissions of the group's policies.
- Attaching Policies Directly to a User: In addition to being a member of a group, you can also attach policies directly to a user. This allows you to grant additional permissions to the user that are not covered by the policies of the groups the user is a member of.