Assignment Interview question

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

- AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources.
- You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.
- To grant other people permission to administer and use resources in your AWS account without having to share your password or access key.
-

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

- First, I decide the policy in which non tech person not have any technical work permission and implementing least privilege.
- After deciding the policy for non tech person, I will create a group for a non-tech person role and give the permissions which is decided in the policy for a non tech person to group.
- Now after creating non-tech group, I will simply add the IAM user for that group.
- When new non-tech person come then I will simply add him/her in the group, so no need to create everything again and again.

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

- **User related: Creation of a delegated Account Operator**
  Policy 1: Delegate read permission for IAM components.

```
{
        "Version": "2012-10-17",
        "Statement": {
        "Effect": "Allow",
        "Action": [
        "iam:Get*",
        "iam:List*"
        ],
        "Resource": "*"
        }
}
```

4. Why do we prefer not using root account?

- A critical aspect of security in AWS is to make sure you avoid use of the AWS root account whenever possible, implementing the best practice of least privilege.
- Because the root account has access to all AWS services and resources in your AWS account, active use of this user should be avoided.
- There are many layers of security that should surround the root account so that, unless emergency access is required, actions cannot be taken from this account.

5. How to revoke policy for an IAM user?

- To immediately deny all permissions to any current user of role credentials
- Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/
- 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.
- IAM immediately attaches a policy named **AWSRevokeOlderSessions** to the role. The policy denies all access to users who assumed the role before the moment you choose Revoke active sessions. Any user who assumes the role after you choose Revoke active sessions is not affected.

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

- You can assign IAM users to up to 10 groups.
- -Go to IAM
- -Click User groups
- -click on the group where you want to add user (for multiple groups you add via same steps)
- -after opening the group, you see option add user click on that
- -now you see the list of users which you want to add in group click on that and add him/her