**IAM 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.
* Having a central IAM system helps you to keep all user credentials, login information, and passwords in one place to streamline your monitoring efforts; this allows you to manage and export your records for multiple regulatory needs at once.

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

* IAM Policies are like permission defined for a specific group of people or individual. For eg : Students in school have restricted access to some labs or confidential data

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

* In IT world we have different teams like developers, Operations, Tester which work together in different cycles of a release in Production. So

in this scenario in order to have control over access we would like to define policy for developers to restrict their access only to development and lower environment so that they can’t modify anything directly in Production without involving Operations team who have access to Production as per policy defined for team, this will ensure proper testing is done in lower environment before releasing in Production. Hence different IAM policies for developers and Operations team will be beneficial here

1. Why do we prefer not using root account?

* The *root user* has access to every AWS service and resource in an account. If the credentials for the root account are stolen, they will be able to access or change anything in the account giving them the ability to misuse any data or resources in the account, they could even make you incur unnecessary cost by creating resources in your account.
* Using root user account for everyday tasks may be putting us at risk of an attack

1. How to revoke policy for an IAM user?

To immediately deny all permissions to any current user of role credentials

1. Sign in to the AWS Management Console and open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the navigation pane, choose Roles, and then choose the name (not the check box) of the role whose permissions you want to revoke.
3. On the Summary page for the selected role, choose the Revoke sessions tab.
4. On the Revoke sessions tab, choose Revoke active sessions.
5. 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?

An IAM user can be part of multiple policies, as policies are of two types

* 1. Identity-based policies
  2. Resource-based policies