Assignment Interview question

Note: - Please prepare the answer of these questions in brief :- (in your own words)

1. What is the need of IAM?

Identity and access management (IAM) helps you to keep all user credentials, login information, and passwords in one place to streamline your monitoring efforts. It ensures that the right people and job roles in your organization (identities) can access the tools they need to do their jobs.

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

A policy is an object in AWS that, when associated with an entity or resource, defines their permissions. Permissions in the policies determine whether the request is allowed or denied.

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

If I need access to recent one year of data, then we can use date policy

1. Why do we prefer not using root account?

There are so many reasons not to use root users/accounts

1. Everyone can make mistakes and root user has all the privileges. A user with all the privileges can make more mistakes and delete applications that are not retrieved.
2. There is only one root account. If everybody uses the same account, we don’t know who made the specific changes. For accountability, creating and using users is a better practice.
3. Root user/account is a known entry point and Logging with root account is very likely to be a target.
4. How to revoke policy for an IAM user?

There is many ways to revoke polices using Console, AWS CLI, AWS APIs. Using Console, these are the couple of steps to follow:

1. Sign in to AWS console
2. In Navigation page, choose policies
3. In the list of policies, select the check box (can search as well)
4. Choose Actions, and then choose detach
5. Select the identities to detach the policy from.
6. Choose Detach Policy
7. Can a single IAM user be a part of multiple policy via group and root? And how?

Permission given based on users, groups, and roles are called identity-based policies. A single IAM user can be a part of multiple policy via groups and root. For example, an IAM user named ‘Aaron’ can be allowed the run Instances action in a group in EC2. He can also access data from a table using Dynamodb which can be added to a different group like dba or developer.