Assignment Interview question

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

1. What is the need for IAM?
Answer: IAM is important when we need to control how a user or group accesses AWS resources and to want extent, also helps in setting up permission boundaries.
It also helps enhance the security of the AWS root account by not giving root privileges to one who is not needed.

2. If I am a non-tech person, how will you define policies in IAM?
Answer: Policies in AWS, can be associated with the identity (user, groups, or roles) or resource. Once it is associated it defines permission of identity or resource. Permissions in the policies determine whether the request is allowed or denied AWS supports six types of policies: identity-based policies, resource-based policies, permissions boundaries, Organizations SCPs, ACLs, and session policies.

3. Please define a scenario in which you would like to create on your own IAM policy.
Answer: It is always best practice to provide the least privileges to identity to perform a specific set of tasks, which gives improved security to the system. So, instead of giving the full privilege of resources using an AWS-managed policy, it’s always a good idea to create your customer-managed policy.

4. Why do we prefer not to use a root account?
Answer: It is not preferred to use a root account to perform the daily or administrative tasks as if some user has root privileges and if he doesn’t require it to perform his daily task then giving that additional permission will increase the risk of vulnerabilities.
And in the scenario, if any user needs that administrative permission then it’s best to create a separate identity and give him administrative privileges, it will help to keep the root account locked, and if required use the root account only for a few accounts and service management tasks.

5. How to revoke policy for an IAM user?
Answer: Detaching the policy specified for a user, will revoke his permission to perform any task in the account.
In the navigation pane, choose User groups, Users, or Roles.
Choose the name of the user group, user, or role with the policy that you want to delete.
Then choose the Permissions tab. If you chose Users or Roles, expand the policy.

To delete an inline policy in User groups, choose Delete. To delete an inline policy in Users or Roles, choose X.
If you are deleting a single inline policy in User groups, type the name of the policy and choose Delete. If you are deleting multiple inline policies in User groups, type the number of policies you are deleting followed by inline policies and choose Delete. For example, if you are deleting three inline policies, type 3 inline policies.

6. Can a single IAM user be a part of multiple policies via group and root? how?
Answer:
A user group can contain many users, and a user can belong to multiple user groups so using a root account some additional permissions can be given.
User groups can't be nested; they can contain only users, not other user groups.