1. What is the need of IAM?

Ans: IAM provides free-gained access control across all of AWS. You can control access to services and resources under specific condition. Also use IAM policies to manage permission of users and workspace to ensure least privilege.

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

Ans: You can use the AWS Management Console, AWS CLI, or AWS API to create customer managed policies in IAM. Customer managed policies are standalone policies that you administer in your own AWS account. You can then attach the policies to identities (users, groups, and roles) in your AWS account

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

Ans: by clicking create policy there are four steps to give details for policy such as which service want to add in policy, action, resouces and request condition such as time span or time period.

4. Why do we prefer not using root account?

Ans: because they allow full access to all your resources for all AWS services, including your billing information.

5. How to revoke policy for an IAM user?

Ans: below steps use to revoke policy

- In the navigation pane, choose Policies.
- Select the check box next to the customer managed policy to delete. ...
- Choose Actions, and then choose Delete.
- Confirm that you want to delete the policy, and then choose Delete.

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

Ans: yes, we can assign IAM users to up to 10 groups. 20 managed policies attached to the IAM user, 10 IAM groups, with 10 policies each