**1. What is the need of IAM?**  
Identity and Access Management (IAM) is a critical component in Amazon Web Services (AWS) and is used to manage access to AWS resources. The need for IAM arises from the following reasons:

Security: IAM provides a secure way to grant access to AWS resources to users, applications, and services, helping to secure the AWS infrastructure.

Scalability: As organizations grow, they may have more users, applications, and services that need access to AWS resources. IAM makes it easy to manage access to these resources at scale.

Compliance: IAM helps organizations comply with regulatory requirements, such as data protection and privacy regulations, by providing granular controls over access to resources.

Cost savings: IAM helps organizations minimize the risk of accidental data breaches and reduce costs associated with managing access to AWS resources.

Collaboration: IAM enables multiple teams to work together by granting access to resources based on role and responsibility.

In summary, IAM is an essential component of AWS that provides a secure and scalable way to manage access to resources, ensuring compliance with regulatory requirements and reducing the risk of data breaches.  
  
**2. If i am a non tech person, how will you define policies inIAM.**  
As a non-technical person, you can think of policies in IAM as a set of rules that determine who has access to which AWS resources, and what actions they can perform on those resources. These policies are similar to permission settings in other software, and help you control who can do what within your AWS environment.

For example, you could create a policy that allows certain users to create new Amazon EC2 instances, while denying access to other users. This way, you can ensure that only authorized users can perform specific tasks within your AWS environment.

Policies in IAM are written in JSON format, and they specify the actions that are allowed or denied for a specific user, group, or role. Policies can be attached to users, groups, and roles, allowing you to control access to AWS resources for different sets of users in a flexible and granular way.

In short, policies in IAM are a crucial part of the security and access control in AWS, and they allow you to control who has access to your resources and what they can do with those resources.

**3. Please define a scenerio in which you would like to createyour on own IAM policy.**  
Role-Based Access Control: If you need to enforce a role-based access control model within your organization, you may want to create custom policies to control access to specific resources based on job function or organizational hierarchy.  
  
**4. Why do we prefer not using root account?**  
There are several reasons for this:

Security: The root account has full access to all AWS services and resources in the account, which means that anyone who gains access to the root account can take control of the entire account. By using the root account for day-to-day tasks, you increase the risk of an attacker gaining access to your account and causing damage.

Auditing and Compliance: Using the root account for regular tasks makes it difficult to track who is making changes to your resource. By creating individual IAM users with specific permissions, you can track and audit their actions, which is essential for compliance and security.

With IAM, you can create policies that grant specific permissions to individual users, groups, or roles. By using IAM users instead of the root account, you can grant only the permissions that are needed for each user to perform their tasks, reducing the risk of accidental or intentional damage to your resources.  
  
**5. How to revoke policy for an IAM user?**  
We can follow these steps:

* Sign in to the AWS Management Console and navigate to the IAM dashboard.
* In the left-hand menu, click on "Users" to see a list of all IAM users in your account.
* Select the user whose policy you want to revoke by clicking on their username.
* Click on the "Permissions" tab, which will show you the policies that are currently attached to the user.
* Find the policy that you want to revoke and click on the "X" button next to it.
* Click on the "Remove" button in the confirmation dialog box.  
    
  6. Can a single IAM user be a part of multiple policy via groupand root? How?  
    
  Yes, a single IAM user can be a part of multiple policies via a group and the root account. Here's how:
* Groups: You can create an IAM group and attach policies to that group. Then, you can add the IAM user to that group, and the user will inherit the permissions granted by the policies attached to the group. If the user is a member of multiple groups, they will inherit the permissions granted by all the policies attached to each group.
* Root Account: The root account has full access to all AWS services and resources in the account. If you grant a permission to the root account, all IAM users in the account will have that permission. However, it is not recommended to use the root account for day-to-day tasks, and it is better to create IAM users and groups with specific permissions.