1. What is the need of IAM

IAM enables you to manage access to AWS services and resources in a very secure manner. With IAM you can create groups and allow those users or groups to access some servers, or you can deny them access to the service. We can create an IAM user when there is a new employee to your corporate. In an increasingly hybrid workplace, getting identity and access management right is more important to IT departments than ever before.

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

Policies by definition means protocol or procedure that is followed by organisation and in day-to-day life. In AWS we call it identity-based policy which include AWS managed policy, customer managed policy and inline policy.

AWS managed policies are created and managed by AWS. You can use them, but you can't manage them.

An inline policy is one that you create and embed directly to an IAM group, user, or role. Inline policies can't be reused on other identities or managed outside of the identity where it exists.

Use customer managed policies instead of inline policies. It's also best to use customer managed policies instead of AWS managed policies. AWS managed policies usually provide broad administrative or read-only permissions.

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

If you have inline as well as AWS policies in your account, you can convert them to managed policies by the help of JSON syntax and great way to create a managed policy is to start by copying an existing AWS managed policy. That way you know that the policy is correct at the beginning and all you need to do is customize it to your environment.

1. Why do we prefer not using root account

The AWS root account is the account that was used — or created — when signing up with Amazon Web Services. This account has full access to all resources in the account and it is not possible to alter this configuration.

1. How to revoke policy for an IAM user?

In the navigation pane, choose Roles, and then choose the name (not the check box) of the role whose permissions you want to revoke.

On the Summary page for the selected role, choose the Revoke sessions tab.

On the Revoke sessions tab, choose Revoke active sessions.

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.

IAM immediately attaches a policy named AWSRevokeOlderSessions to the role. The policy denies all access to users who assumed the role before the moment you choose Revoke active sessions.

Any user who assumes the role after you choose Revoke active sessions is not affected.

When you apply a new policy to a user or a resource, it can take a few minutes for policy updates to take effect.

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

A user can belong to multiple policy. When a user is added to a group, the user inherits the group permissions but also retains their individual permissions that have been assigned by policies directly attached to their IAM user account.