**1. What is the Need of I AM?**

**Ans:-** IAM consists of processes, policies, and systems that manage the users’ digital identities in a secure, streamlined manner.

It encompasses various technologies such as Single Sign-On (SSO), profile management, Multi-Factor Authentication (MFA), and password management.

Identity and access management incorporates three significant concepts, identification, authentication, and authorization, which collectively ensure that the right users have the proper access.

Thus, [IAM solutions](https://www.stealthlabs.com/solutions/identity-management-services/access-management-services/) have become a crucial component of IT security.

IAM solutions are beneficial not only for users and security admins but also for enterprises as a whole.

While an effective IAM solution helps enterprises secure efficient access to technology resources across diverse systems, it also delivers many essential benefits.

—----------------------------------------------------------------------------------------------------------------------------**2. If i am non-tech person how will you define policies in IAM?**

**Ans:-** if am creating IAM policies for non-tech person then i will restrict his access so can’t create mess around our aws account for e.g i will give only basic thing of acces when its comes s3 bucket ,RDS, services so he can do only minimalist activity on that particular things so he will not increase our cloud budget for the same .

—----------------------------------------------------------------------------------------------------------------------------

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

**Ans:-** lets say we need to restrict some user, or user group to particular zones to use . let say the dev user group restricted to use us-west-zone-1.when we create those polices then they can’t able spwan any EC2 instance on that particular zone. Aprt from this lots of scenario where root user can restricted any user group according to there custom policy .

—----------------------------------------------------------------------------------------------------------------------------------

**4. Why do we prefer not using root account?**

**Ans:-** When you create a new AWS account it will create a *root user* with the email and password used to create it. The simplest thing to do is to use that user for everyday tasks. We will be looking at why you shouldn't do that and the configuration necessary to secure your account.

The *root user* has access to every AWS service and resource in an account. If the credentials for the root account are stolen they will be able to access or change anything in the account giving them the ability to misuse any data or resources in the account, they could even make you incurr unnecessary cost by creating resources in your account.

## Recommended settings for root user

Since it's critical to keep the root user safe and out of reach of malicious users there are a few things you can do to increase it's security.

* Do not create access keys for the root user. Create an IAM user for yourself with administrative permissions.
* Never share the root user credentials.
* Use a strong password. (Use a password manager if possible)
* Enable multi-factor authentication.

**—---------------------------------------------------------------------------------------------------------------------------**

**5. How to revoke policy for an IAM user?**

**Ans:-** Deleting IAM policies (console)

You can delete a customer managed policy to remove it from your AWS account. You cannot delete AWS managed policies.

To delete a customer managed policy (console)

1. Sign in to the AWS Management Console and open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the navigation pane, choose Policies.
3. Select the check box next to the customer managed policy to delete. You can use the search box to filter the list of policies.
4. Choose Actions, and then choose Delete.
5. Confirm that you want to delete the policy, and then choose Delete.

To delete an inline policy for a user group, user, or role (console)

1. In the navigation pane, choose User groups, Users, or Roles.
2. 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.
3. To delete an inline policy in User groups, choose Delete. To delete an inline policy in Users or Roles, choose X.
4. 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 policy via group and root? How?**

**Ans:-** Policies are JSON document that defines permission and controls access AWS resources. Permissions specify who has access to the resources and what actions they can perform.

* Policies are an authorization mechanism. You can create IAM policies to define granular access to resources.
* For example, a policy could allow an IAM user to access one of the buckets in Amazon S3.
* Policy can be attached to IAM identities (Users, Roles, Groups).
* Single policy can include multiple permissions (or statements).
* Policies can be either customer managed or managed by AWS.
* There are multiple policies provided by AWS like Administrator, S3FullAccess, etc.
* You can also create your own policy and use it to manage privilege levels to your AWS resources.

Policy contains the following information:

* Who can access it.
* What actions that user can take.
* Which AWS resources that user can access.
* When they can be accessed.

Types of policies:

* Managed policies: It is a default policy that you attach to multiple entities (users, groups, and roles) in the AWS account. Managed policies, whether they are AWS-managed or customer-managed, are stand-alone identity-based policies attached to multiple users and/or groups.
* Inline policies: It is a policy that you create that is embedded directly into a single entity (user, group, or role).