***IAM***

***INTERVIEW QUESTION:***What are the different AWS IAM categories that you can control?***ANSWER:***  
Using AWS IAM, you can do the following:

* Create and manage IAM users
* Create and manage IAM groups
* Manage the security credentials of the users
* Create and manage policies to grant access to AWS services and resources

***INTERVIEW QUESTION:*** Your organization has four instances for production and another four for testing. You are asked to set up a group of IAM users that can only access the four production instances and not the other four testing instances. How will you achieve this?

***ANSWER:*** We can achieve this by defining tags on the test and production instances and then adding a condition to the IAM policy that allows access to specific tags.

**Interview Question:** Your organization has around 50 IAM users. Now, it wants to introduce a new policy that will affect the access permissions of an IAM user. How can it implement this without having to apply the policy at the individual user level?

***ANSWER:***It is possible using IAM groups, by adding users in the groups as per their roles and by simply applying the policy to the groups.

***INTERVIEW QUESTION:***What is the difference between an IAM role and an IAM user?

***ANSWER:***The two key differences between the IAM role and IAM user are:

* An IAM role is an IAM entity that defines a set of permissions for making AWS service requests, while an IAM user has permanent long-term credentials and is used to interact with the AWS services directly.
* In the IAM role, trusted entities, like IAM users, applications, or an AWS service, assume roles whereas the IAM user has full access to all the AWS IAM functionalities.

What is IAM?

AWS IAM stands for Identity & Access Management and is the primary service that handles authentication and authorization processes within AWS environments. As an AWS account management service, it lets you to control access to AWS services in a secure manner, and helps to monitor who is authenticated and allowed to use resources.

## What are IAM Workflow components?

* Principal
* Authentication
* Request
* Authorization
* Actions or Operations
* Resources

## What are IAM Identities?

* Users
* Groups
* Roles

## What are the different types of Security Credentials in AWS?

* Root User Credentials : E-mail & Password
* IAM Uses Credentials : Username & Password
* MFA : MultiFactor Authentication via third party applications
* CLI, SDKs, API Credentials : Access Keys
* Amazon EC2 Credentials : Key Pairs

## What is an IAM user?

An IAM user is an entity that you create in AWS.

## What are different IAM user types?

* Real Person
* Web Application
* Service Accounts
* Software

## What are the components of 5-step security system in IAM?

* Delete your root access keys
* Activate MFA on your root account
* Create individual IAM users
* Use groups to assign permissions
* Apply an IAM password policy

## What is a Policy in AWS?

Policies are JSON files that allow you to determine which users have which rights on AWS resources. By attaching policies, you can authorize users, roles that users can take on, or groups that include users.

## What are IAM Policy Types?

* AWS managed policies (Managed policies)
* Customer managed policies (Managed policies)
* Inline policies
* Jop Function policies

## What is an IAM Group?

Collection of IAM users that let you specify permissions for multiple users, which can make it easier to manage the permissions for those users.

IAM Groups are not truely real identities, because they can not be identified as a principal in a permission policy. Basically, this is a way for attaching policies to multiple users at any time.

## What is an IAM Role?

An IAM Role is the authorization system that we determine how and with which authorizations that other AWS resources, users coming from other AWS accounts or accounts that will have access to our system as a result of the trust relationship we have established with an identity provider in the outside world can access our own AWS resources.