[**Identity and Access Management (IAM)**](https://us-east-1.console.aws.amazon.com/iam/home#/home)

1. **What is IAM?**

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. using iam we can create and manage aws users, groups and their permissions to allow or deny their access.

**2.Which is main resources in iam service?**

* User
* Group
* Policies
* Role

**3. What are the different types of users in AWS?**

**Root user** - The root user has complete access to all AWS services and resources in the AWS account. When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is the AWS account root user.

**IAM user -** These users are the identities within your AWS account with specific custom permissions. IAM users require a name and password which they use to sign in to the AWS management console.

**Federated user –** A user who is allowed to access AWS resources from third party vendors such as google, facebook, linkdin, corporate credential, etc.

**4. What is groups in IAM?**

An IAM Group is a collection of users. Group specifies the permission for a collection of users, and it also makes it possible to manage the permissions easily for those users.

**5.** **What is IAM Role?**

 IAM Role is an IAM Identity similar to IAM user, created in AWS account with specific permission policies assigned to. These policies define what IAM role can and cannot do in the AWS account. IAM roles do not hold authentication credentials such as login passwords or access keys, instead a temporary security credential is generated for each individual role session.

**6. Define Authentication and Authorization.**

Authentication:

* Validates the identity of a user or a service.
* Create and manage IAM identities.
* Federate corporate identities.

**Authorizati**on:

* Defines the permissions and limits access to only specific resources for the permitted user.
* Assign permissions to IAM identities.
* Assign permissions to corporate identities.

## 7. What is a Policy?

A policy is a document with a set of rules, having one or more statements. Each policy grants a specific set of permissions and can be attached to any of the IAM identities users, groups, and roles.

There are two ways to create IAM policy: 1. Visual editor 2. Jason

**8. Explain Policy types.**

**1. Identity-based policies** control what actions the identity can perform, on which resources, and under what conditions. Identity-based policies can be further categorized:

* **Managed policies** – Standalone identity-based policies that you can attach to multiple users, groups, and roles in your AWS account. You can use two types of managed policies:
  + **AWS managed policies** – Managed policies that are created and managed by AWS.
  + **Customer managed policies** – Managed policies that you create and manage in your AWS account. Customer managed policies provide more precise control over your policies than AWS managed policies. You can create, edit, and validate an IAM policy in the visual editor or by creating the JSON policy document directly.
* **Inline policies** – Policies that you create and manage and that are embedded directly into a single user, group, or role.

**2.Resource-based policies** control what actions a specified principal can perform on that resource and under what conditions. Resource-based policies are inline policies, and there are no managed resource-based policies. To enable cross-account access, you can specify an entire account or IAM entities in another account as the principal in a resource-based policy.

## 9. What is MFA (multi-factor authentication)?

- AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your username and password.

- MFA device change the code every 30sec. Two types of code mfa1 and mfa2

- No additional charge for using MFA.

- The device generates a six-digit numeric code based upon a time-synchronized one-time password algorithm.

**10.What is ARN?**

Amazon Resource Names (ARNs) uniquely identify AWS resources. We require an ARN when you need to specify a resource unambiguously across all of AWS, such as in IAM policies, Amazon Relational Database Service (Amazon RDS) tags, and API calls.

**11. What is API?**

API is application program interface. API is software which can be used by other software to communicate with other software or even hardware. It acts as bridge between different software and devices.