### What is AWS?

### AWS stands for Amazon Web Services that offers various IT services on demand using distributed IT infrastructure and offers flexible, reliable, scalable, and cost-effective cloud computing solutions.

## AWS Infrastructure

* An AWS Region is a physical location in the world where it has multiple Availability Zones.
* Availability Zones consist of one or more discrete data centres, each with redundant power, networking, and connectivity, housed in separate facilities.
* The AWS Cloud operates in over 80 Availability Zones within over 25 geographic Regions around the world.



### Edge Locations

### An edge location is where end-users access services located at AWS and used for caching content. Edge locations serve requests for CloudFront and Route 53.

### AWS Local Zones

### AWS Local Zones place compute, storage, database, and other select AWS services closer to end-users.

### AWS Free Tier?

### The AWS Free Tier provides customers the ability to explore and try out AWS services free of charge up to specified limits for each service. You can explore more than 85 products and start building on AWS using the free tier.

### 

### 

## Introduction to IAM

* AWS IAM stands for Identity & Access Management and is the primary service that handles authentication and authorization processes within AWS environments.
* IAM components can be mainly categorized under two terms; identities and permissions.

There are three identities in AWS IAM:

1. Users 2- Groups 3- Roles

Permissions can be defined as different types of policies that use authorization to users.

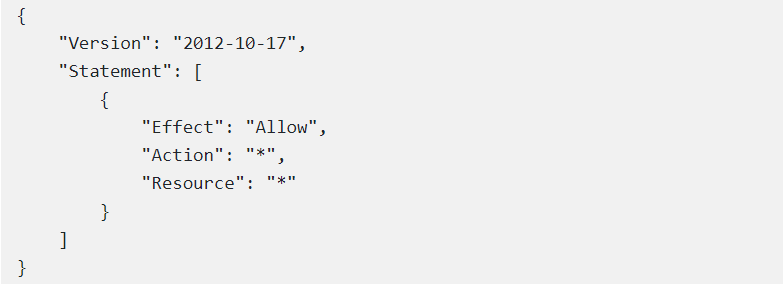
* Policies
* A user in AWS consists of a name, a password to sign in to the AWS Management Console, and up to two access keys that can be used with the API or CLI.

### Account Root User

* AWS account owner is also an AWS account root user has complete access to all AWS services.

### The limit of creating new IAM users is restricted to 5000 users per account.

## IAM – Policies



### IAM Policy Types

### 

1- Managed policies:

IAM managed policy is a standalone policy that can be attached to multiple entities (user, group of users, or role) in an AWS account. They can only be applied to entities and not to resources.

* AWS managed policies:

AWS managed policies are managed policies, created and managed by AWS. If you are new to using policies, AWS recommends that you start by using AWS managed policies.

* Customer managed policies:

Customer managed policies are managed policies, created and managed by users (AWS customers) in their AWS account.

2-Inline policies:

Inline policies are policies that you create and manage and embedded directly into a single user, group, or role.

### Job Function Policies

* The AWS managed job function policies are designed to fit closely with common IT job functions.
* Managed policies in job function status are listed below:
* [Administrator](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_administrator)
* [Billing](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_accounts-payable)
* [Database Administrator](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_database-administrator)
* [Data Scientist](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_data-scientist)
* [Developer Power User](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_developer-power-user)
* [Network Administrator](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_network-administrator)
* [Security Auditor](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_security-auditor)
* [Support User](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_support-user)
* [System Administrator](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_system-administrator)
* [View-Only User](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_view-only-user)

## IAM – Groups

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

* Groups have no credentials.
* Managed IAM policies can be attached to groups.
* Inline IAM policies can be added to groups.
* Groups can contain only users, but not other groups.
* The limit of IAM users in a group is equal to the user quota for the account, that is, max 5000.
* An IAM user can be a member of the max. 10 different IAM groups.

## IAM – Roles

* It is the authorization system that we determine how and with which authorizations an identity can access the AWS resources.
* Every role has two policies: A trust policy and a permission policy.
* IAM roles are a secure way to grant permissions to entities that you trust.
* We can create a role that we can assign to a virtual machine-EC2, so that we can access the S3 service with EC2 instance and read the files there and save files to this service.