aws is a global cloud provider (has *regions* all over the world)

region - cluster of data centers — a region has multiple availablity zones (AZ)

- **Availablity Zone (AZ)** - one or more discrete data centers with redundant power, networking and connectivity

Identity Access Management [IAM]

aws security

- Users - a physical person
- Groups - containes users (functions, teams)
- Roles - internal usage within aws resources (given to machines)

policies - are JSON documents that defines what users, groups, roles can and cannot do

least privilege principle - give the users the minimal amount of permissions they need to perform their job IAM Federation

- big enterprises usually integrate their own repository of users with IAM
- can use company credentials to log in
- uses SAML standard [Security Assertion Markup Language] (e.g. Active Directory)

Note:

- 1 IAM user per PHYSICAL PERSON
- 1 IAM role per APPLICATION
- IAM credentials should NEVER BE SHARED
- Never write IAM credentials in code or commit them
- Never use ROOT account except for initial setup

Elastic Compute Cloud [EC2]

EC2

- renting VMs (EC2)
- storing data on virual drives (EBS)
- distributing load across machines (ELB)
- scaling the services using an auto-scaling group (ASG)