Q. What is an Amazon EC2 instance?

Ans: An EC2 instance is a resizable compute capacity in the AWS cloud that allows you to run applications, host websites, databases, or perform computations on virtual machines.

* Instance Type:- 

Determines the hardware configuration (CPU, memory, storage, network).

Example:

* + - t2.micro → small, free-tier eligible.
    - m5.large → medium performance for business apps.
    - p3.2xlarge → GPU-based for AI/ML workloads.
* EBS (Elastic Block Store)
* Provides persistent storage (like a hard disk) for your instance.
* Security Group
* Acts as a virtual firewall to control inbound and outbound traffic.
* Key Pair
  + - Used for secure login (SSH for Linux or RDP for Windows).

Q. What is AMI?

Ans: AMI (Amazon Machine Image) :- A preconfigured template that defines what’s on your server — like the OS (Ubuntu, Windows, Amazon Linux) and software packages.

Q. what is the difference between S3 and EBS?

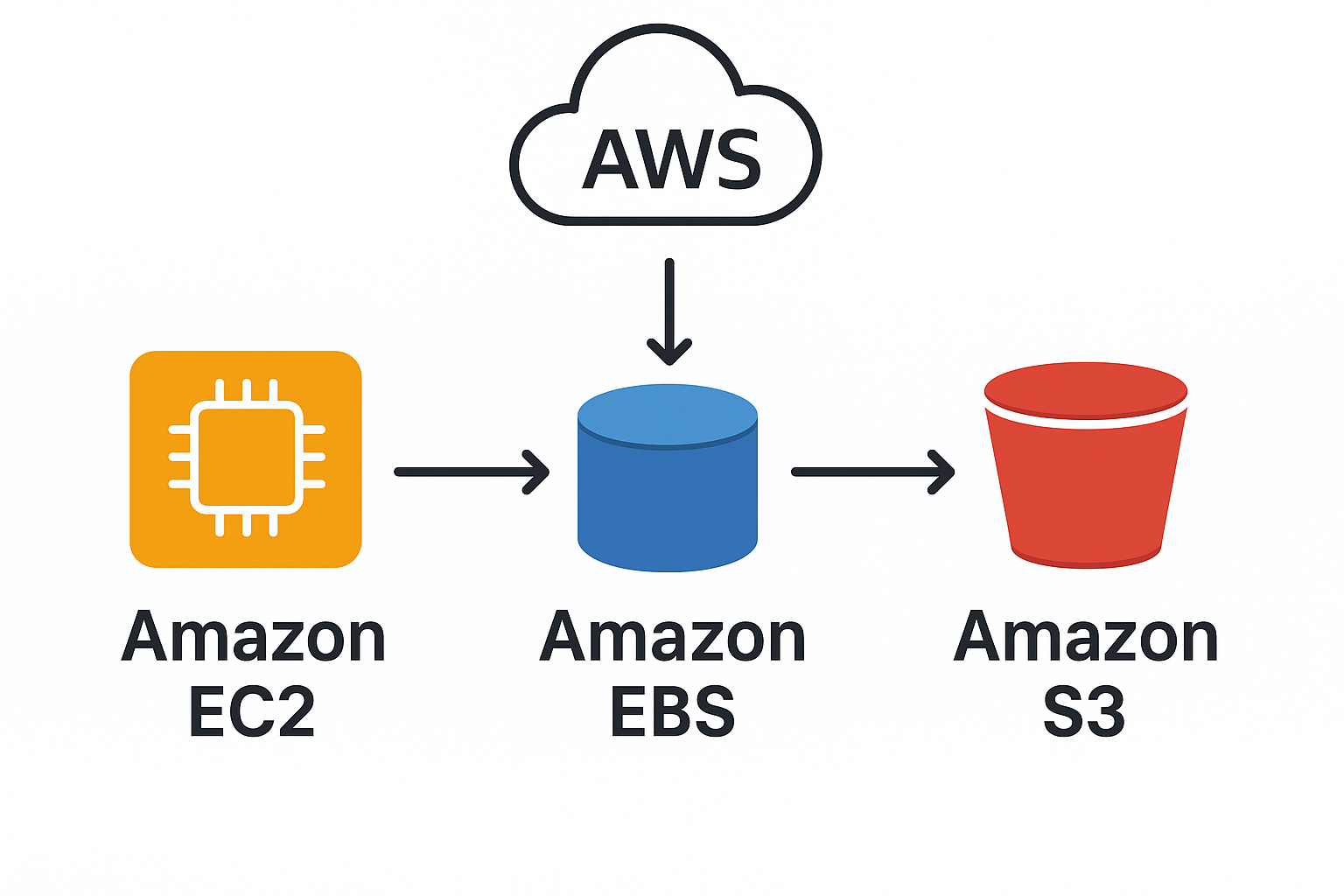
Ans: Both **Amazon S3** and **Amazon EBS** are **storage services**, but they are **used for different purposes**

Amazon S3 (Simple Storage Service) : -

* + Store and retrieve large amounts of unstructured data (like files, images, backups).
  + Accessible **over the internet** from anywhere
  + designed for **scalability and durability**.
  + Backup, media storage, data lake, website hosting, logs, etc.
  + Scalability : - Virtually **unlimited**.
  + Data stored as **objects (files)** inside **buckets**.

Amazon EBS (Elastic Block Store) : -

* + Block Storage
  + Provides storage for **EC2 instances** (like a hard drive).
  + High performance – designed for **fast read/write** like a hard disk.
  + Databases, applications, or operating systems requiring low latency.
  + Limited to **volume size** (up to 16 TB per volume).
  + Data stored as **blocks** inside **volumes**



Q. What is an Auto Scaling Group (ASG)?

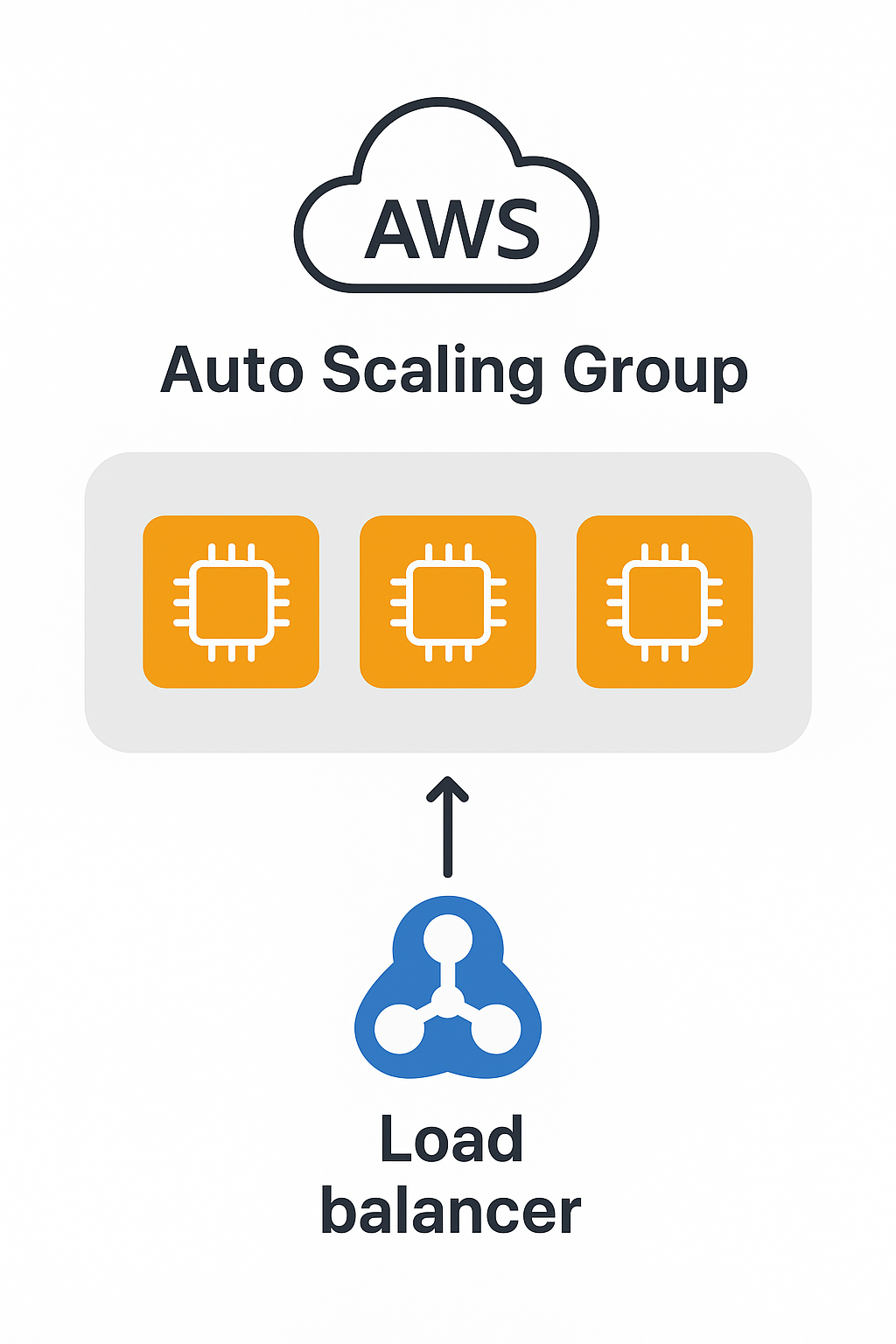
Ans: Its a **collection of EC2 instances** that are **managed automatically** to maintain **high availability, performance, and cost efficiency**.

It automatically **adds (scales out)** or **removes (scales in)** EC2 instances **based on demand or load**.

An **ASG** automatically adjusts the number of EC2 instances running in your application according to **traffic, CPU usage, or custom metrics** — ensuring you always have the **right number of instances** running.

**Key Components**

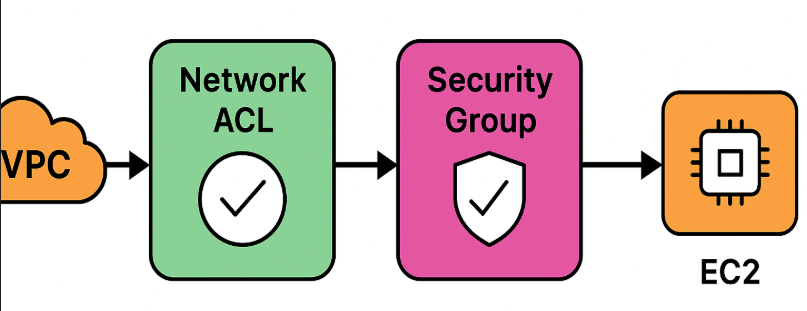
1. **Launch Template / Launch Configuration**
   * Defines *how* to launch an instance (AMI, instance type, key pair, security groups, etc.).
2. **Group Size Settings**
   * **Minimum size** – the fewest instances that should always run.
   * **Maximum size** – the maximum number of instances that can be launched.
   * **Desired capacity** – the target number of instances (ASG maintains this count).
3. **Scaling Policies**
   * Define *when* and *how* to scale.
   * Examples:
     + Add an instance if CPU > 70% for 5 minutes.
     + Remove an instance if CPU < 30% for 10 minutes.
4. **Health Checks**
   * ASG monitors instances — if one fails, it terminates and launches a new one automatically.
5. **Load Balancer Integration**
   * Works with **Elastic Load Balancer (ELB)** to distribute incoming traffic among healthy instances.



Q. What is the difference between a Security Group and a Network ACL?

Ans: Inside it, an **EC2 instance** with a **Security Group** and **Network ACL**.

| **Feature** | **Security Group (SG)** | **Network ACL (NACL)** |
| --- | --- | --- |
| Level of Operation | Works at the **instance (EC2)** level | Works at the subnet level |
| Type | **Stateful** | Stateless |
| Default Behavior | All inbound **denied**, all outbound **allowed** | All inbound and outbound allowed |
| Rules Applied To | Specific EC2 instances (ENI – Elastic Network Interface) | All resources inside a subnet |
| Return Traffic | Automatically allowed (if request allowed) | Must be explicitly allowed for both directions |
| Evaluation Order | All rules evaluated **together** | Rules evaluated in order by rule number (lowest to highest) |
| Purpose | Controls **traffic to/from EC2 instances** | Controls traffic to/from subnets |
| Rule Types | Only **Allow** rules | Both Allow and Deny rules |
| Use Case | Instance-level security | Network-level security |
| Example | Allow SSH (port 22) from your IP | Deny all traffic from a specific IP range |



Q. What is an Elastic Load Balancer (ELB)?

Ans: An **Elastic Load Balancer (ELB)** in AWS is a service that **automatically distributes incoming network traffic** across multiple **EC2 instances, containers, or IP addresses** — ensuring **high availability, fault tolerance, and scalability**..

**How It Works**

1. Clients (users) send requests to your **application endpoint** (ELB DNS name).
2. The **Load Balancer** receives those requests.
3. ELB automatically routes each request to one of the **healthy instances** (in multiple Availability Zones if configured).
4. If an instance fails, ELB **stops sending traffic** to it until it becomes healthy again.

| **Type** | **Layer** | **Use Case** |
| --- | --- | --- |
| **Application Load Balancer (ALB)** | Layer 7 (HTTP/HTTPS) | Best for web apps, microservices, path-based routing |
| **Network Load Balancer (NLB)** | Layer 4 (TCP/UDP) | Best for high performance, low-latency traffic |
| **Gateway Load Balancer (GWLB)** | Layer 3 | For security appliances like firewalls, intrusion detection |
| **Classic Load Balancer (CLB)** | Layer 4 & 7 (legacy) | Older version — replaced by ALB & NLB |

Q. What is the default storage class in Amazon S3?

Ans: By **default**, when you upload an object to an Amazon S3 bucket **without specifying a storage class**, it is stored in the **S3 Standard** storage class.



Q. How do you restrict public access to an S3 bucket?

Ans: **Use the “Block Public Access” Settings (Recommended)**

This is the **simplest and safest** method.

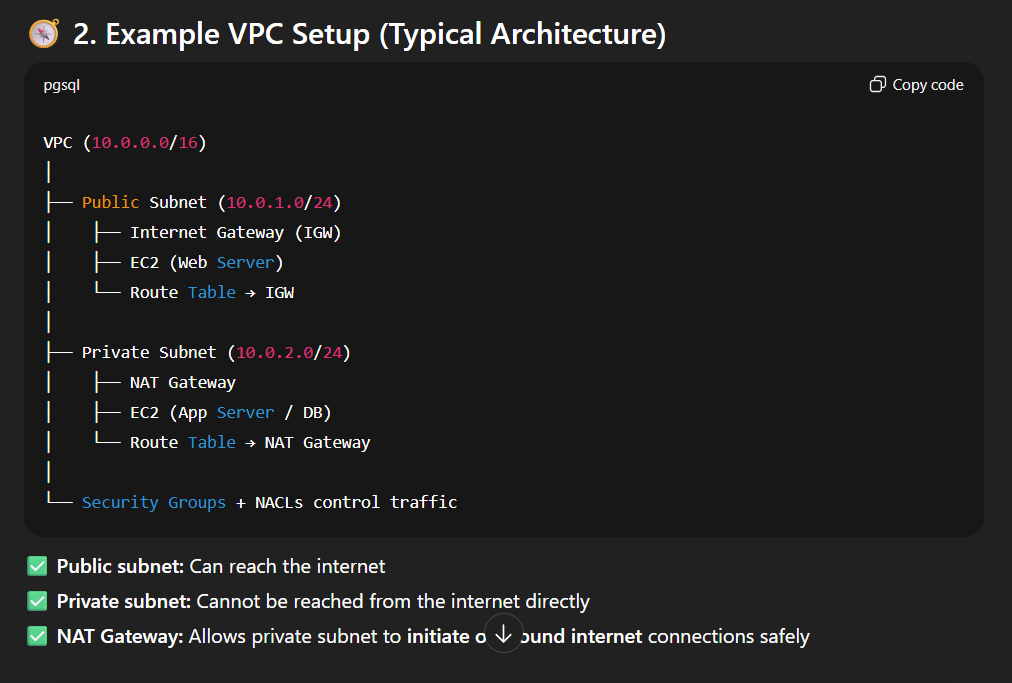
**✅ Steps (via AWS Console):**

1. Go to **Amazon S3 → Buckets**
2. Select your bucket
3. Click on **Permissions tab**
4. Under **Block public access (bucket settings)** → Click **Edit**
5. Turn **ON all options**:
   * ☑️ Block all public access
   * ☑️ Block public ACLs
   * ☑️ Ignore public ACLs
   * ☑️ Block public bucket policies
6. Click **Save changes**

Q. What are the main components of a VPC??

Ans: A **VPC (Virtual Private Cloud)** is a **virtual network** in AWS that is **isolated from other networks** — it lets you define your own **IP address ranges, subnets, route tables, and gateways**, just like in a traditional on-premise network.

Allows **private subnets** to access the internet **without exposing** them to incoming internet traffic.



Q. What is AMI?

Ans: AMI (Amazon Machine Image) :- A preconfigured template that defines what’s on your server — like the OS (Ubuntu, Windows, Amazon Linux) and software packages.

Q. What is AMI?

Ans: AMI (Amazon Machine Image) :- A preconfigured template that defines what’s on your server — like the OS (Ubuntu, Windows, Amazon Linux) and software packages.