1) What is AWS Auto Scaling

AWS Auto Scaling continually monitors your applications.When demand spikes, AWS Auto Scaling automatically increases the capacity of resources so you maintain a high quality of service.
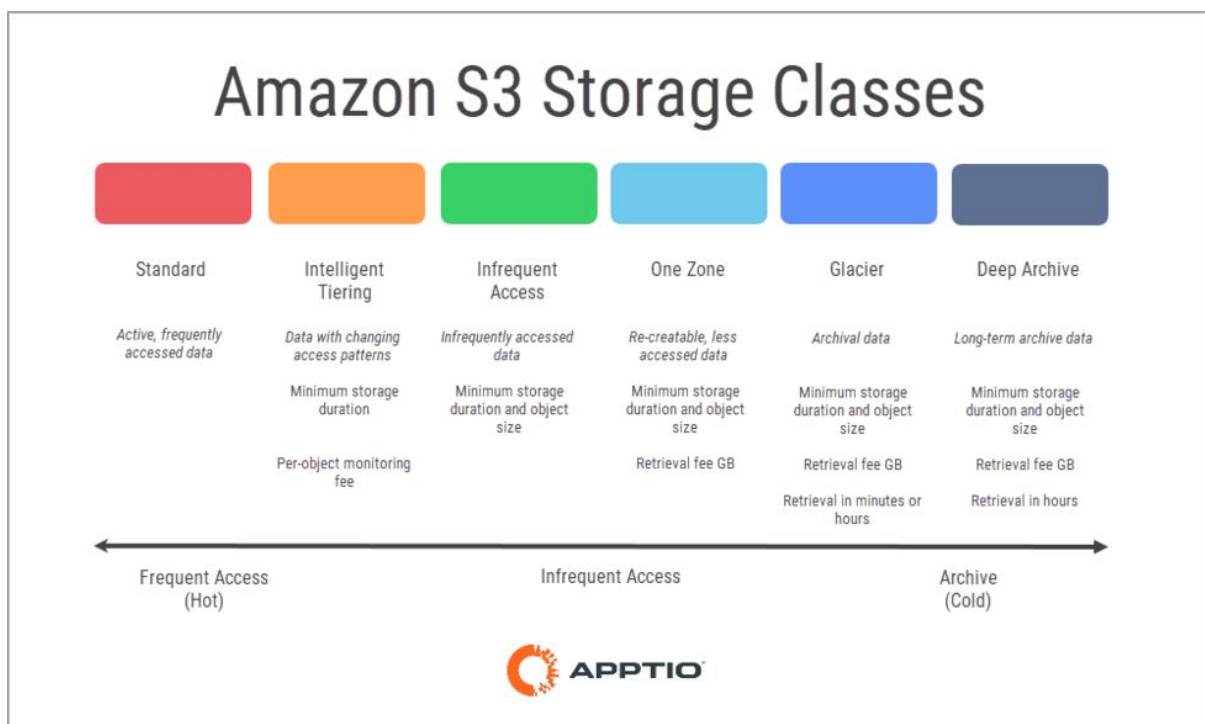
2) What is Virtualization?

Virtualization is technology that you can use to create virtual representations of servers, storage, networks, and other physical machines.

3) Hypervisor

A hypervisor is a software that you can use to run multiple virtual machines on a single physical machine. Every virtual machine has its own operating system and applications. The hypervisor allocates the underlying physical computing resources such as CPU and memory to individual virtual machines as required.

4)S3

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere.

Amazon S3 Storage Classes

Standard	Intelligent Tiering	Infrequent Access	One Zone	Glacier	Deep Archive
Active, frequently accessed data	Data with changing access patterns	Infrequently accessed data	Re-creatable, less accessed data	Archival data	Long-term archive data
	Minimum storage duration	Minimum storage duration and object size	Minimum storage duration and object size	Minimum storage duration and object size	Minimum storage duration and object size
	Per-object monitoring fee		Retrieval fee GB	Retrieval fee GB	Retrieval fee GB
				Retrieval in minutes or hours	Retrieval in hours

Frequent Access (Hot) ← Infrequent Access → Archive (Cold)

APPTIO

AWS Virtual Private Cloud (VPC)

A VPC is your private network within AWS. A VPC isolates your resources from everyone else's.

Each AWS account comes with a default VPC that is pre-configured for you to start using immediately. A VPC can span multiple availability zones in a region.

A VPC only exists in one AWS region.

CIDR Blocks

When creating a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block. E.g., 172.31.0.0/16 is the primary CIDR block for your VPC. It defines 65536 IPv4 addresses in your VPC.

Subnets

A subnet is a range of IP addresses in your VPC. The subnet must use a CIDR block that falls within the assigned VPC.

You can create multiple subnets within a VPC. A subnet can logically group resources based on your requirements.

There are two types of subnets:

Public Subnet: Resources in a public subnet can be accessed from the Public Internet.

Private Subnet: Resources in a private subnet cannot communicate with the public internet.

Route Table

Route Tables contain the rules (routes) determining how network traffic will be directed within your VPC and subnet.

Each subnet is linked to one Route Table.

What is Network Address Translation?

Network Address Translation (NAT) allows you to map multiple local private addresses to a unique public IP address. This single device acts as an intermediary between the local, private network and the public internet.

Internet Gateway (Igw)

Internet Gateway is a VPC component that allows communication between your VPC and the Internet.

An Internet Gateway is a logical connection between an AWS VPC and the Internet. There is no underlying physical resource.

Each VPC has only one Internet Gateway. If a VPC doesn't have an Internet Gateway, then resources cannot be accessed from the Internet.

A Public Subnet is a subnet that is associated with a route table that redirects traffic to an Internet Gateway. Therefore, its important to ensure that your route tables are configured correctly.

Why is an IGW important?

- Enables Inbount and Outbound access to the Internet
- Performs Network Address Translation (NAT) for public instances
- Horizontally Scaled, Redundant & Highly available

Internet

internet is a widespread interconnected network of computers and electronics devices(that support internet). It creates a communication medium to share and get information online. If your device is connected to the Internet then only you will be able to access all the applications, websites, social media apps, and many more services. Internet now a days is considered as the fastest medium for sending and receiving information.
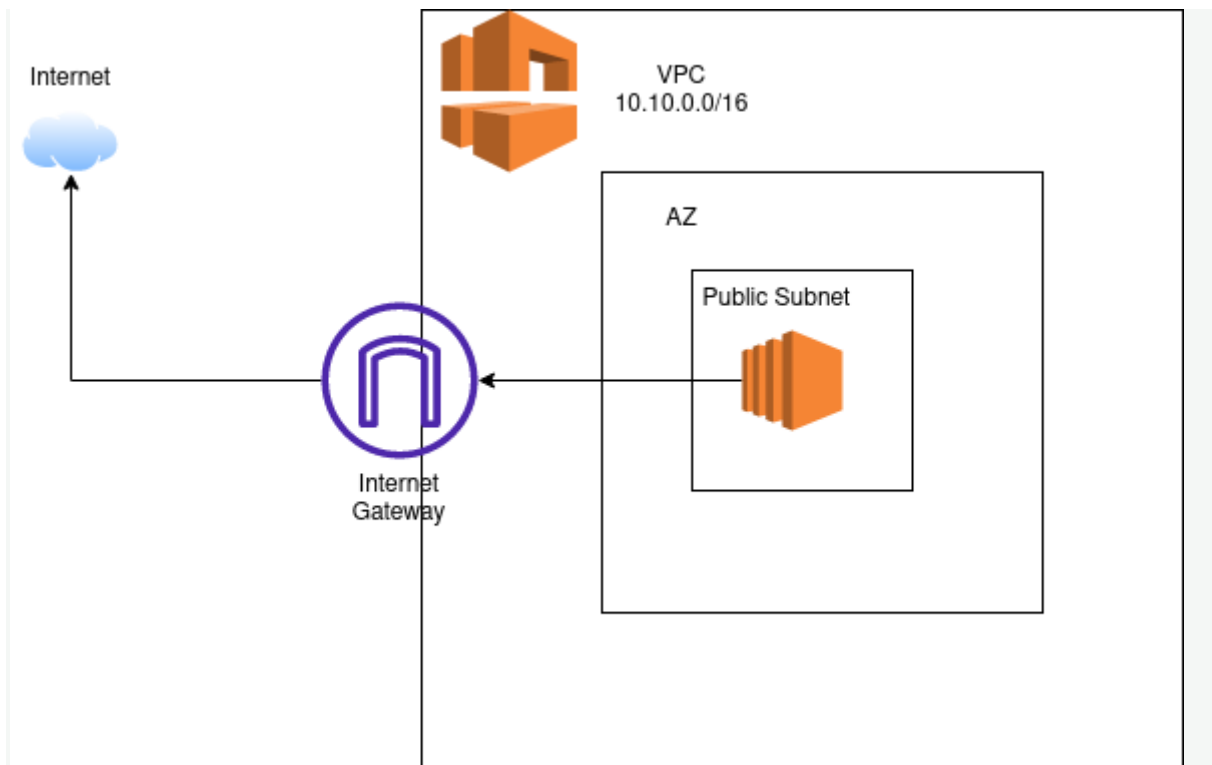
Pricing

Internet Gateway is simply a logical router to the internet for a VPC. You pay for all outbound internet traffic, but there is no fee directly associated with the IGW.

NAT Instance

A NAT Instance is a self-managed Amazon EC2 instance that is configured to act as the intermediary between your private subnet and the public internet.

The NAT instance has to be in the public subnet. Instances in a private subnet that want to access the Internet will forward their internet-bound traffic to the NAT instance using the Route Table configuration.

Since such an instance is self-managed, you would be responsible for configuring routing and updating the software amongst other similar tasks.

NAT Gateway

NAT (or Network Address Translation) Gateway is a managed AWS service that is used so that instances in a private subnet can connect to services outside the VPC. These private resources don't allow any inbound traffic from the public Internet.

NAT Gateway was introduced, so users no longer have to manage their own NAT instance. The benefits of using a NAT Gateway service are:

- Fully-managed service: You no longer need to manage your own NAT instance
- Supports 5 Gbps bandwidth and automatically scales up to 100 Gbps.
- You cannot associate a security group with a NAT gateway.

NAT Gateway allows two connectivity types:

- *Public*: Instances in private subnets can connect to the internet through a public NAT
- *Private:* Instances in private subnets can connect to other VPCs through a private NAT gateway. More details can be found here .(https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/private-nat-gateway.html)

This article will focus on the Public NAT Gateway to keep things simple.

A Public NAT gateway is created in a Public Subnet. An Elastic IP address is associated with the NAT Gateway when it is created.

If you have multiple Availability Zones (AZs) in your AWS Architecture, you must create a separate NAT Gateway in each AZ.

A NAT Gateway relies on your Route Tables to be able to route traffic to the public Internet. It is important to create a route from the NAT Gateway to the Internet Gateway to ensure proper Internet connectivity.

How does request routing work with a NAT Gateway?

- Private Instance in a private subnet initiates the connection to the Internet.
- The request to the internet goes through the NAT Gateway in the public subnet.
- The NAT Gateway uses its public IP address to access the internet. It acts as the source of the request.
- The NAT Gateway routes the request to the public internet via the Internet Gateway.
- The response goes to the NAT Gateway.
- The NAT Gateway forwards the response to the private instance that made the request.

What is CloudWatch?

- o CloudWatch is a service used to monitor your AWS resources and applications that you run on AWS in real time. CloudWatch is used to collect and track metrics that measure your resources and applications.

- o It displays the metrics automatically about every AWS service that you choose.

- o You can create the dashboard to display the metrics about your custom application and also display the metrics of custom collections that you choose.

- o You can also create an alarm to watch metrics. For example, you can monitor CPU usage, disk read and disk writes of Amazon EC2 instance to determine whether the additional EC2 instances are required to handle the load or not. It can also be used to stop the instance to save money.

Following are the terms associated with CloudWatch:

- o **Dashboards:** CloudWatch is used to create dashboards to show what is happening with your AWS environment.

- o **Alarms:** It allows you to set alarms to notify you whenever a particular threshold is hit.

- o **Logs:** CloudWatch logs help you to aggregate, monitor, and store logs.

- o **Events:** CloudWatch help you to respond to state changes to your AWS resources.

What is Amazon EC2?

Amazon EC2 is a cloud computing platform that can be auto-scaled to to meet demand.

Different hardware and software configurations can be selected. Different geographical locations can be selected be closer to users, as well as providing redundancy in case of failures.

Persistent storage can be provided by Amazon EBS (Elastic Block Storage). Amazon S3 (Simple Storage Service) data can also be accessed with Amazon EC2 instances, and is free if they are in the same region.

What is DNS?

- o DNS stands for Domain Name System.

- o DNS is used when you use an internet. DNS is used to convert human-friendly domain names (such as **https://www.javatpoint.com**) into an Internet Protocol (IP) address.

- o IP addresses are used by computers to identify each other on the network.

- o IP addresses are of two types, **i.e., Ipv4 and Ipv6.**

What is AWS IAM?

AWS IAM is short for: Amazon Identity and Access Management.

Amazon IAM provides management of access to AWS services with fine grained control. Individual users and groups can be created and their persmissions are described in policies (JSON documents). IAM roles can have defined permissions and be assigned to users, applications and services.

Instance type names

Amazon EC2 provides a variety of instance types so you can choose the type that best meets your requirements. Instance types are named based on their family, generation, additional capabilities, and size. The first position of the instance type name indicates the instance family, for example `c`. The second position indicates the instance generation, for example `5`. The remaining letters before the period indicate additional capabilities, such as instance store volumes. After the period (`.`) is the instance size, which is either a number followed by a size, such as `9xlarge`, or `metal` for bare metal instances.

- **General purpose:** M6a, M6g, M6gd, M6i, M6id, M6idn, M6in, M7g, T4g
- **Computer optimized:** C6a, C6g, C6gd, C6gn, C6i, C6id, C6in, C7g, Hpc6a
- **Memory optimized:** Hpc6id, R6a, R6g, R6gd, R6i, R6id, R6idn, R6in, R7g, X2gd, X2idn, X2iedn
- **Storage optimized:** I4i, Im4gn, Is4gen
- **Accelerated computing:** G5g, Trn1

Difference Between Linux and Windows

Parameters	Linux	Windows
Case Sensitivity	The file system in Linux is very case-sensitive.	The file system in Windows is not case-sensitive.
Cost Incurred	Linux is free to use for everyone.	Windows do not come free for any user.
Open Source	It is open source.	It is not open source.
Type of Kernel Used	Linux utilizes the monolithic kernel.	Windows uses the micro-kernel.
Path Separator	The path separator that Linux uses is Slash.	The path separator that Windows uses is backward slash.
Efficiency	In the case of operations, Linux is way more efficient than Windows.	For operations, Windows are comparatively way less efficient than Linux.
Security	It is more secure than Windows OS.	It provides much less security to its users than Linux.
Uses in Hacking	People generally use Linux for the systems that are hacking-based.	Windows is not a very efficient OS for hacking purposes as compared to Linux.

What is containerization?

Containerization is a software deployment process that bundles an application's code with all the files and libraries it needs to run on any infrastructure. Traditionally, to run any application on your computer, you had to install the version that matched your machine's operating system. For example, you needed to install the Windows version of a software package on a Windows machine. However, with containerization, you can create a single software package, or container, that runs on all types of devices and operating systems.