**There are 7 types of instance:--**

1. **General purpose**

**There are 3 series in general purpose,**

1. **A (A1)**
2. **M (M4, M5, M5a, M5d M5ad)**
3. **T (T2, T3, T3a)**
4. **Compute Optimize**

**There is one series in compute optimize,**

1. **C (C4, C5, C5n)**
2. **Memory Optimize**

**There are 3 series in memory optimize,**

1. **R (R4, R5, R5a, R5ad, and R5d)**
2. **X (X1, X1e)**
3. **Z (Z1d)**
4. **Storage Optimize**

**There are 3 series in storage optimize,**

1. **I (I3)**
2. **D (D2)**
3. **H (H1)**
4. **High Memory**

**High memory instances are purpose to run large-in-memory database including production of SAP HANA in the cloud.**

1. **Accelerated Computing**

**There are 3 series in Accelerated Computing,**

1. **F (F1)**
2. **P (P2, P3)**
3. **G (G2, G3)**
4. **Previous Generation**

**T1, M1, C1, CC2, M2, CR1, CG1, i2, HS1, M3, C3, and R3**

Check EC2 meta data-----

curl <http://169.254.169.254/latest/meta-data/>

Q. What is VPC?

A. VPC is a virtual network or data center inside AWS for one client.

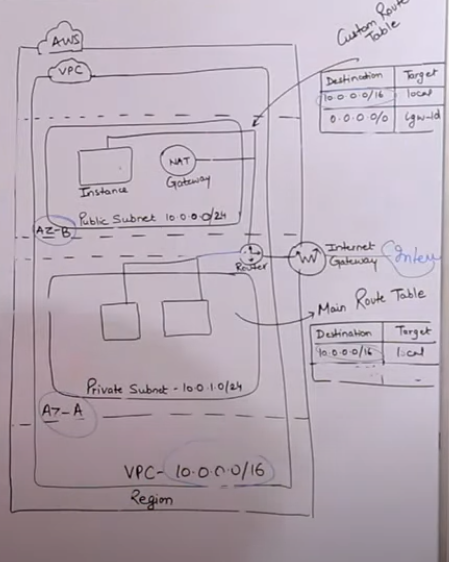
It is logical isolated from other virtual network in the AWS.

Max 5 VPC can be created in one region and 200 subnet in 1 VPC.

We can allocate max 5 elastic IP in one account. We can extend this limit.

Once we created VPC then DHCP, NACL and security group will be automatically created.

A VPC is confined to an AWS region and does not extend between regions.



Once the VPC is created, you can not change its CIDR block range.

If you need a different CIDR size, create a new VPC.

The different subnet within a VPC can’t overlap.

You can however expand your VPC CIDR by adding new/extra IP range.

Q. VPC flow log?

Ans. VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs or Amazon S3

Q. Types of VPC?

A. There are two types of vpc

i. Default VPC

ii. Custom VPC

**Default VPC**------

🡪We can create default VPC in all AWS reason when an AWS account is created.

🡪Default VPC has default CIDR, Security group, NACL and route table.

**Custom VPC-----**

* Custom VPC is a VPC on AWS account owner creates
* AWS use creating the custom VPC can decide the CIDR.
* Custom VPC has its own default security group, Network ACL and route table.
* Customer VPC does not have Internet Gateway by default, one need to be created if needed.

Q. Four component is must require when you create VPC.

Ans. These components are require when we create VPC,

* Create VPC
* Subnet
* Internet Gateway
* Route Table

Q. **Type of Subnet?**

Ans. There are two type of subnet,

* **Public Subnet**

If a subnet’s traffic is routed to an Internet Gateway, the subnet is known as a public subnet. If you want your instance in a public subnet to communicate with the internet over IPv4, It must be a public IPv4 address or an elastic IP address.

* **Private Subnet**

If a subnet does have a route to the Internet Gateway, the subnet is known as a private subnet.

When you create a VPC, You must specify an IPv4 CIDR block for the VPC. The allowed block size is between /16 to /28 netmask.

The first four and last IP address of subnet can’t be assigned.

1- Network IP

2- DHCP

3- DNS

4- Reserved for future purpose

5- Broadcast IP

Q. **Implied router and route table**

Ans.

* It is the central routing function.
* It connects the different AZ together and connect the VPC to the internet gateway.
* You can have upto 200 route tables per VPC.
* You can have upto 50 route entries per route table.
* Each subnet must be associated with only one route table at any given time.
* If you do not specify a subnet to route table association, the subnet will be associated with the default VPC route table.
* You can also edit the main route table if you need, but you can’t delete main route table.
* However you can make a customer route table manually become the main route table then you can delete the former main, as it is no longer a main route table.
* You can associate multiple subnet with the same route table.

Q. **Internet Gateway**

Ans.

* An internet gateway is a virtual router that connects a VPC to the internet.
* Default VPC is already attached with an Internet Gateway.
* If you create a new VPC then you must attach the internet gateway in order to access the internet.
* Ensure that your subnet’s route table point to the internet gateway.
* It performs NAT between your private and public IPv4 address.
* It’s support both IPv4 and IP6.

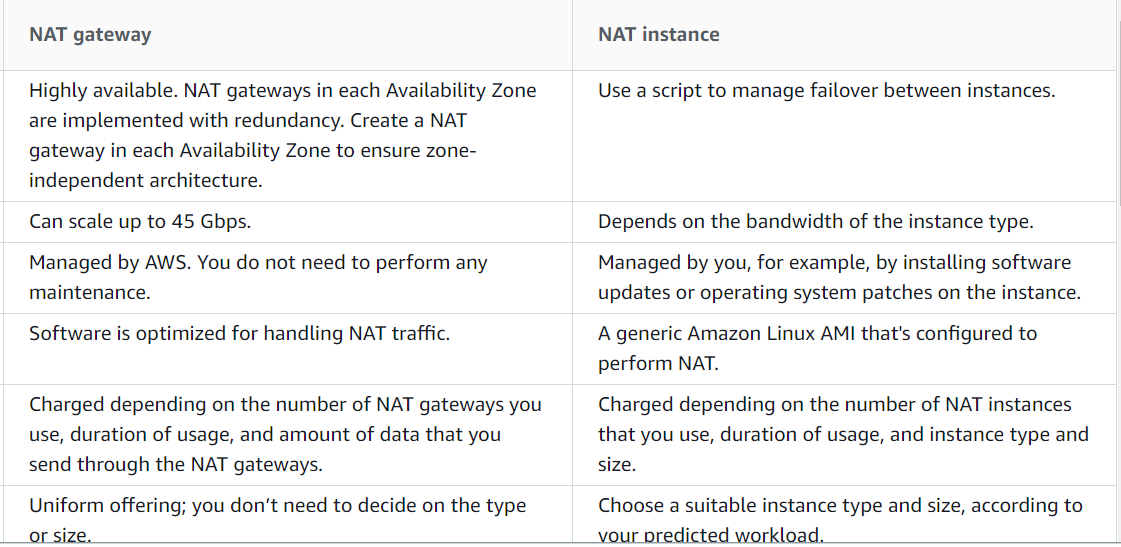
Q. **NAT Gateway**

Ans.

* You can use a network address translation gateway to enable instances in a private subnet to connect to the internet or other AWS service, but prevent the internet from initiating a connection with those instances.
* You are charged for creating and using a NAT Gateway in your account. NAT gateway hourly usage and data processing rate apply amazon EC2 charge for data transfer also apply.
* To create a NAT gateway, you must be specify the public subnet in which the NAT gateway should be reside.
* You must also specify an elastic IP address to associate with NAT gateway when you create it.
* No need to assign public IP address to your private instance.
* After you have created a NAT gateway you must update the route table associated with one or more of you private subnet to point internet bound traffic to the NAT gateway. This enable instances in your private subnet to communicate with the internet.
* Delete a NAT gateway, disassociates its elastic IP address, but does not release the address from your account.

Q. **Diff between NAT Gateway and Nat Instance?**

Ans.



Q. **Security groups**

Ans.

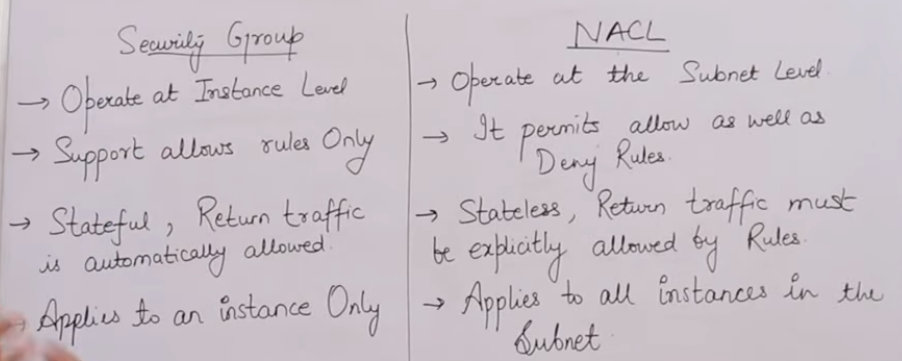
* It is virtual firewall works at ENILevel
* Upto 5 security groups per EC2 instance interface can be applied.
* Can only have permit rules, can’t have deny rules.
* Stateful, Return traffic of allowed, inbound traffic is allowed, even if there are no rules to allow it.

Q. **NACL (Network Access Control List)**

Ans.

* It is a function performed on the implied router.
* NACL is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.
* Your VPC is comes with a modifiable default network ACL by default, It allow all inbound and outbound traffic and if applicable, IPv6 traffic.
* You can create a custom network ACL and associate it with a subnet by default, each custom network ACL denies all inbound and outbound traffic until you add rules.
* Each subnet in your VPC must be associated with a network ACL if you don’t explicitly associate a subnet with a network ACL, The subnet is automatically associated with default network ACL.
* You can associate a network ACL with multiple subnet, however a subnet can be associated with only one network ACL at a time. When you associate a network ACL with a subnet the previous association is removed.
* A network ACL contains a list of rules that we evaluate in order, starting with the lowest number rule.
* The highest number that you can use for a rule is 32766 recommended that you start by creating rules with rule numbers that a multiple of 100, so that you can insert new rule where you need later.
* It function at the subnet level.
* NACL are stateless, outbound traffic for an allowed inbound traffic, must be explicitly allowed too.
* You can have permit and deny rules in a NACL.

Q. Difference between Security group and NACL

Ans. 

Q. **VPC Peering**

Ans. A VPC peering connection is networking connection between two VPC that enable you to route traffic between them using private IPv4 address or IPv6 address.

Instance in either VPC can communicate with each other as if they are within the same network.

You can create a VPC peering connection between your own VPC, or with a VPC in another AWS account. The VPC can be in different region.

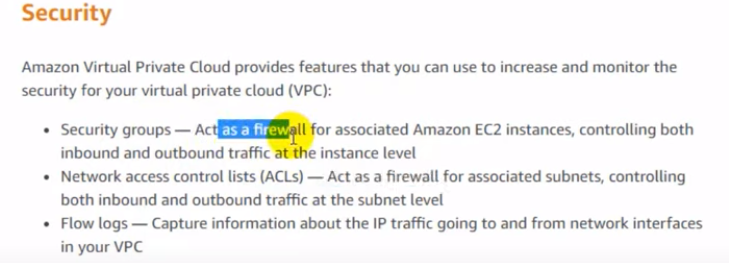
**VPC Peering Steps: ------**

1st VPC

1. Create a VPC-1 with CIDR 192.168.0.0/16
2. Create subnet with subnet id 192.168.0.0/24 with VPC-1
3. Create Internet Gateway and attached it to VPC-1
4. Create Peering connection, requester will be VPC-1 (VPC Peering connection will be create once for both VPC). Now need to accept request from Action button then select accept request
5. Create route table then associate subnet with this route table and enter 0.0.0.0/0 in route for internet access. Again add second VPC CIDR address with peering target
6. Create instance with VPC1 and enable public IP. Add ICMP protocol for communication

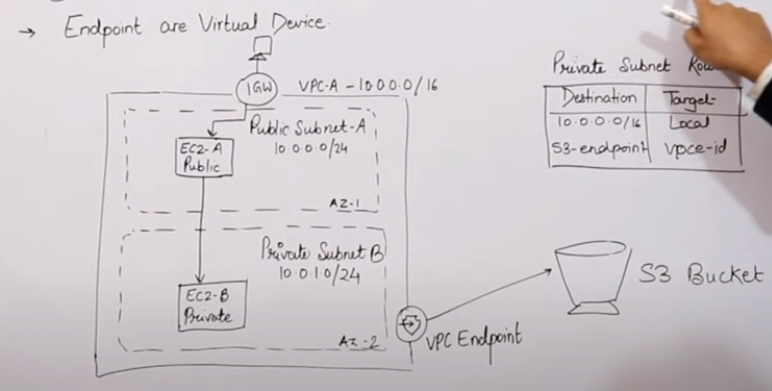
2nd VPC

1. Create a VPC-2 with CIDR 172.0.0.0/16
2. Create subnet with subnet id 172.0.0.0/24 with VPC-2
3. Create Internet Gateway and attached it to VPC-2
4. Create Peering connection , Accepter will be VPC-2 (VPC Peering connection will be create once for both VPC) Now need to accept request from Action button then select accept request
5. Create route table then associate subnet with this route table and enter 0.0.0.0/0 in route for internet access. Again add second VPC CIDR address with peering target
6. Create instance with VPC1 and enable public IP. Add ICMP protocol for communication



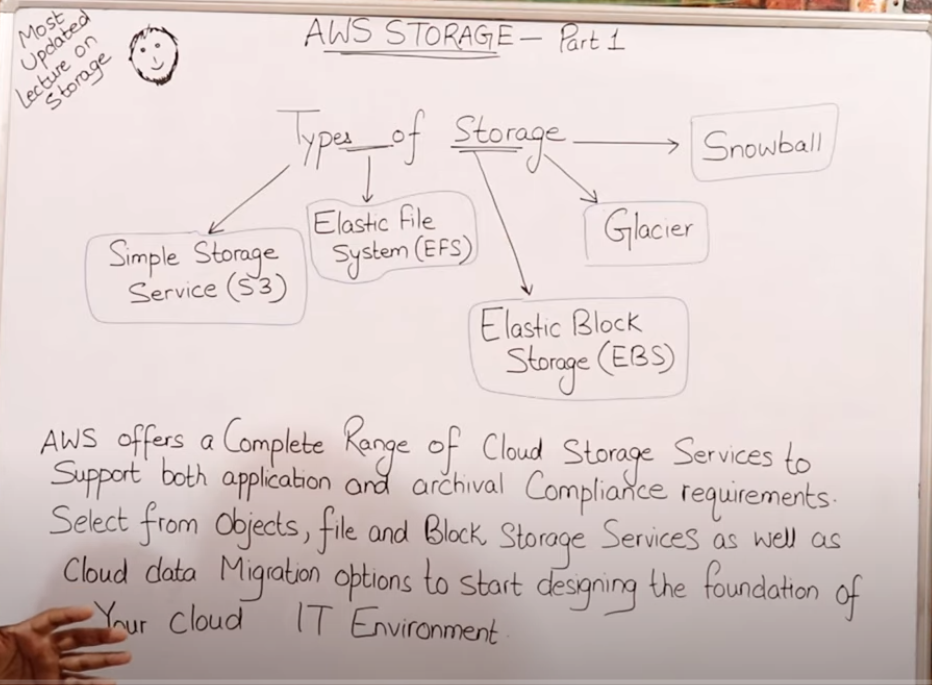
Q. VPC Endpoint

Ans. A VPC endpoint enables you to privately connect your VPC to supported AWS services. Instance in your VPC do not require public IP address to communicate with resources in the server.



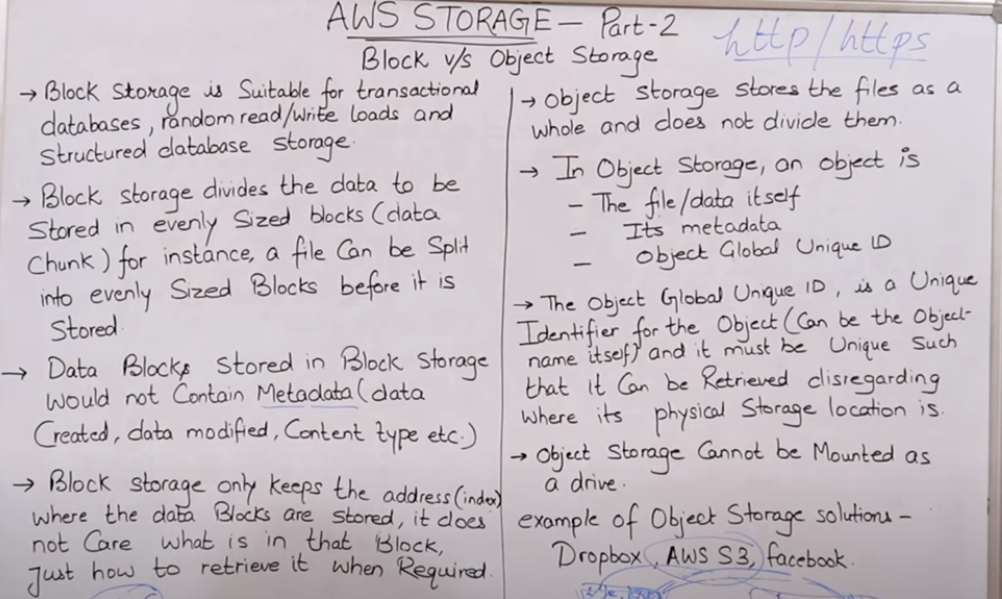
Q. AWS Storage

Ans.



Q. Difference between block storage and object storage.

Ans.



Q. **S3 Storage**

Ans.

* S3 is object based storage.
* You can’t install operating system on S3
* Data is stored in bucket
* You can’t create nested bucket.
* S3 bucket is region specific.
* You can have upto 100 buckets per account.
* Max size capacity of a bucket is 5TB.
* S3 bucket name should be globally unique.
* Bucket name can contain lowercase, number and hyphen. Can’t use upper cases.
* S3 bucket name should be start or end with lower case or number.

Q. Provide temporary access of S3 bucket content?

Ans. We can provide temporary access on S3 bucket content using presigned URL , like

Login AWS CLI 🡪 aws s3 presign --expires-in 20 s3\_url/content.png

Q. **S3 bucket sub resources**

Ans. Sub resources for s3 bucket is,

**Lifecycle**---- To decide on object’s lifecycle management.

**Website**----- To hold configurations related to static website hosted in S3 buckets.

**Versioning**—Keep object versions as it changes (Get, Updated)

**ACL** --------- Bucket Policy

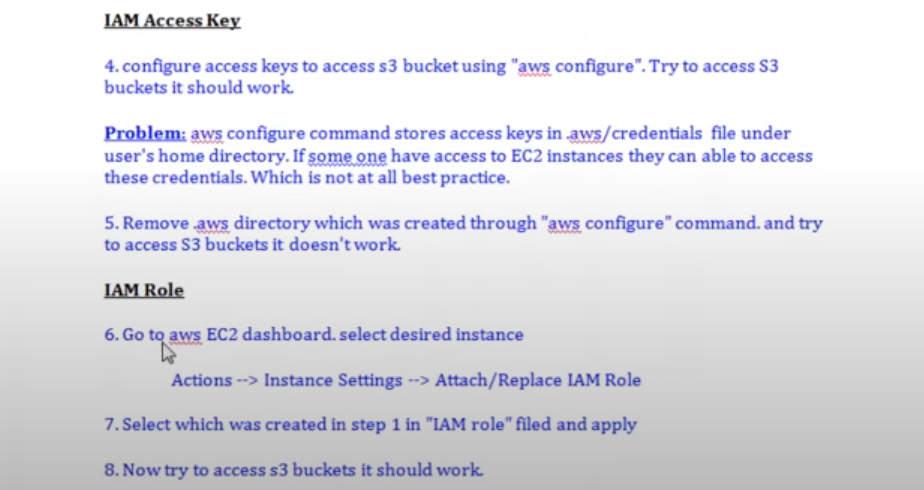
**Q. What is direct connect?**

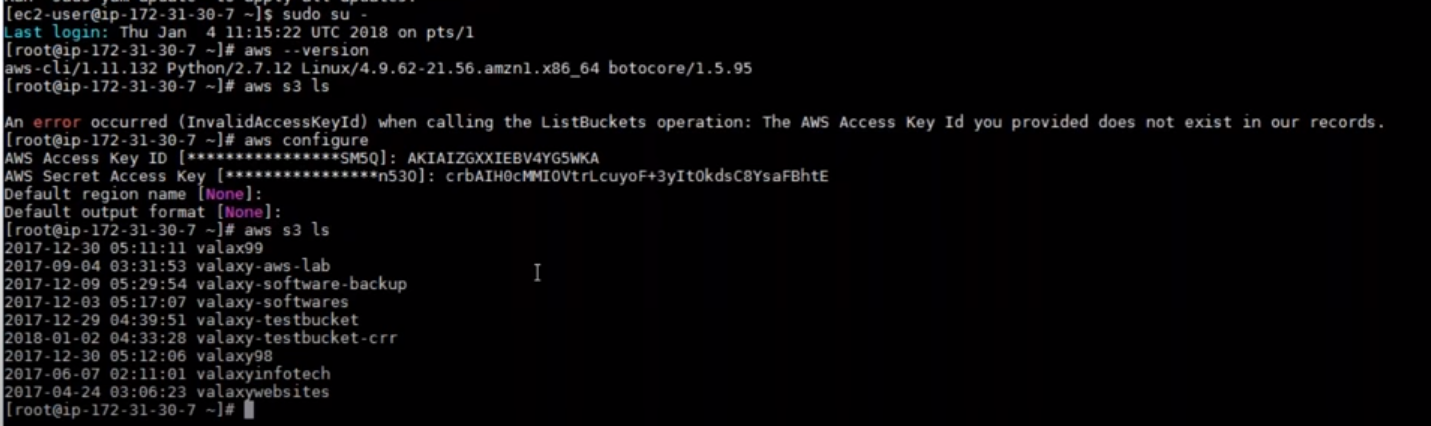
Ans. AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS.

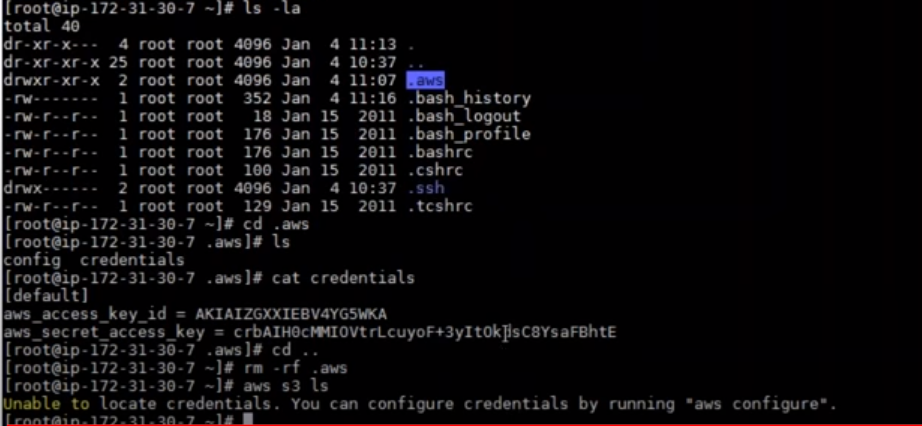
**Q. Diff between Direct connect and VPN?**

Ans. VPN Connection utilizes IPSec to establish encrypted network connectivity between your intranet and Amazon VPC over the Internet. AWS Direct Connect does not involve the Internet; instead, it uses dedicated, private network connections between your intranet and Amazon VPC

Q. Diff between IAM and roles?

Ans.





**Q. What are roles?**

Answer: Roles are used to provide permissions to entities that you trust within your AWS account. Roles are users in another account. Roles are similar to users but with roles you do not need to create any username and password to work with the resources.

**Q. What is IAM?**

Answer: - AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources

**Q. Classic Load Balancer.**

Answer: - A load balancer distributes incoming application traffic across multiple EC2 instances in multiple Availability Zones. This increases the fault tolerance of your applications. Elastic Load Balancing detects unhealthy instances and routes traffic only to healthy instances.

Your load balancer serves as a single point of contact for clients. This increases the availability of your application. You can add and remove instances from your load balancer as your needs change, without disrupting the overall flow of requests to your application. Elastic Load Balancing scales your load balancer as traffic to your application changes over time. Elastic Load Balancing can scale to the vast majority of workloads automatically.

## **Benefits**

Using a Classic Load Balancer instead of an Application Load Balancer has the following benefits:

* Support for EC2-Classic
* Support for TCP and SSL listeners
* Support for sticky sessions using application-generated cookies

Q. **Diff between classic and application load balancer.**

Answer: - The Classic Load Balancer operates on both the request and connection levels. However, it doesn't support features like host and path based routing. This is the first load balancer that AWS introduced in 2009 so it is missing some features. The Application Load Balancer was introduced to address this. A Classic Load Balancer is recommended only for EC2 Classic instances.

The Application Load Balancer operates at the 7th layer of OSI model. It supports the basic feature of distributing requests using the round robin algorithm. It also supports advanced features like host and path based routing.

#### **Listener:-** An Application Load Balancer has one or more listeners. A listener has a protocol (HTTP or HTTPS) and a port (1-65535). For web applications, you normally use a listener for HTTP on port 80 and HTTPS on port 443. These are for requests to the http and https versions of your site. If you can, redirect all http requests to https. You need to do this on your servers because you can't do this on the AWS load balancers

#### **Rule:-** Each listener has a default rule which you can't delete. This is for the basic feature of distributing all requests to the different servers. You can also define additional rules. These can be rules to support host and path based routing.

#### **Target Group:-** Each rule has a target group. This is the group of registered targets where requests are distributed to. A target can either be an EC2 instance or an IP address.

**Q. Cross zone load balancing?**

**Answer: -** Cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled Availability Zone, and improves your application's ability to handle the loss of one or more instances.

Create Load balancer in VPC----

1. Create a VPC
2. Create two subnet
3. Create internet gateway and attach it and select your VPC
4. Create route table and edit route and enter 0.0.0.0/0 for internet access and associate subnet
5. Create two EC2 Instance
6. Create load balancer and select application load balancer, in configuration security setting section you will select your VPC and subnet. In configure routing section you will create a target group and there are three type of target type (a) Instance (b) IP (c) Lambda function and here you can also select your protocol like http or https. In register targets section you need to add your instance private IP

Q. **DNS service or Route 53?**

Answer: - Amazon Route 53 is a globally distributed service that translates human readable names like www.example.com into the numeric IP addresses like 192.0. 2.1 that computers use to connect to each other.

DNS Records Type---

1. **A record type**

You can use a record type to route traffic to a resource, such as a web server, using an IPv4 address in doted decimal notation.

**<Value>192.0.2.1</Value>**

1. **CNAME record type**

CNAME records can be used to alias one name to another. CNAME stands for Canonical Name.

A common example is when you have both example.com and www.example.com pointing to the same application and hosted by the same server. To avoid maintaining two different records, it’s common to create:

* An A record for example.com pointing to the server IP address
* A CNAME record for www.example.com pointing to example.com

As a result, example.com points to the server IP address, and www.example.com points to the same address via example.com. If the IP address changes, you only need to update it in one place: just edit the A record for example.com, and www.example.com automatically inherits the changes.

1. **AAAA record type**

You can use a record type to route traffic to a resource, such as a web server, using an IPv6 address in colon-separated hexadecimal format.

1. **DS record type**

A delegation signer (DS) record refers a zone key for a delegated subdomain zone. You might create a DS record when you establish a chain of trust when you configure DNSSEC signing.

Domain Name System Security Extensions (DNSSEC) signing lets DNS resolvers validate that a DNS response came from Amazon Route 53 and has not been tampered with. When you use DNSSEC signing, every response for a hosted zone is signed using public key cryptography.

**Enabling DNSSEC signing has two steps:**

**Step 1:** Enable DNSSEC signing for Route 53, and request that Route 53 create a key signing key (KSK) based on a customer managed customer master key (CMK) in AWS Key Management Service (AWS KMS).

**Step 2**: Create a chain of trust for the hosted zone by adding a Delegation Signer (DS) record to the parent zone, so DNS responses can be authenticated with trusted cryptographic signatures.

1. **MX record type**

An MX record specifies the names of your mail servers and, if you have two or more mail servers, the priority order. Each value for an MX record contains two values, priority and domain name.

1. **NS Record type**

An NS record identifies the name servers for the hosted zone. Note the following:

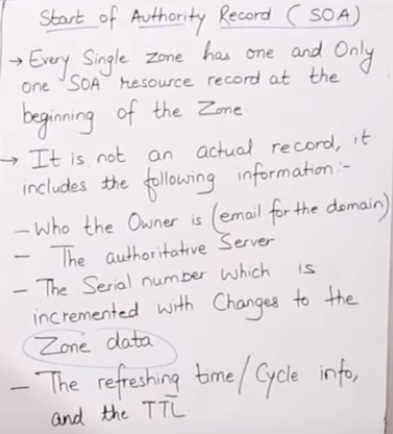
* + The most common use for an NS record is to control how internet traffic is routed for a domain
  + You can create a separate hosted zone for a subdomain (acme.example.com) and use that hosted zone to route internet traffic for the subdomain and its subdomains (subdomain.acme.example.com).

1. **PTR record type**

A PTR record maps an IP address to the corresponding domain name.

1. **SOA record type**

A start of authority (SOA) record provides information about a domain and the corresponding Amazon Route 53 hosted zone.



1. **SPF record type**

SPF records were formerly used to verify the identity of the sender of email messages.

1. **SRV record type**

An SRV record Value element consists of four space-separated values. The first three values are decimal numbers representing priority, weight, and port. The fourth value is a domain name. SRV records are used for accessing services, such as a service for email or communications.

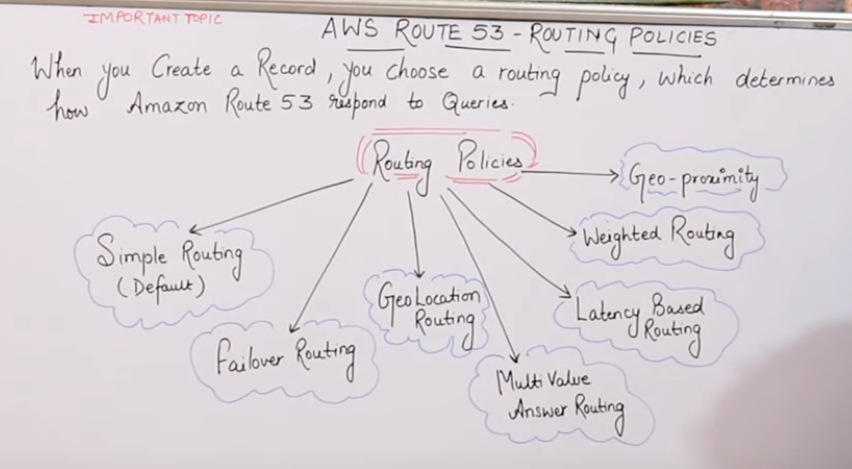
1. **TXT record type**

A TXT  record contains one or more strings that are enclosed in double quotation marks ("). When you use the simple [routing policy](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html), include all values for a domain (example.com) or subdomain (www.example.com) in the same TXT record.

1. **Alias record**

An ALIAS record is a virtual host record type which is used to point one domain name to another one, almost the same as a CNAME.

**Routing Policy----**



Q**. Create route 53**

Answer: -

* + 1. Click on Route53 in Networking & content delivery section
    2. Click on DNS management section
    3. Click on create hosted zone and enter domain name and type will be like public or private hosted zone then click on create. Now you will get 4 name server for your domain and 1 SOA



* + 1. Now we have to create a record set.

In name you have to enter like www.example.com or info. example.com.

In type you have to select records like A record etc.

In alias, If you are selecting yes then you can select your S3 bucket where you have hosted your webservers or you can select your ELB otherwise select No.

In TTL, by default value will be 300 you can reduce or increase it. In value, you will enter your ec2 instance’s public IP where you have hosted your webservers.

In Routing policy, you can select your routing policy like simple, Weighted, Latency or failover etc. If you are selecting failover then you have to create health checks. Now go in create record set and select policy failover and provide your primary or secondary failover record set.

1. **Question 1. What Is Amazon Ec2 Service?**

**Answer :**

Amazon Elastic Compute Cloud (Amazon EC2) is a Amazon web service that provides resizable (scalable) computing capacity in the cloud. You can use Amazon EC2 to launch as many virtual servers you need. In Amazon EC2 you can configure security and networking as well as manage storage. Amazon EC2 service also helps in obtaining and configuring capacity using minimal friction.

1. **Question 2. What Are The Features Of The Amazon Ec2 Service ?**

**Answer :**

As the Amazon EC2 service is a cloud service so it has all the cloud features.

**Amazon EC2 provides the following features:**

* + Virtual computing environment (known as instances)
  + Pre-configured templates for your instances (known as Amazon Machine Images – AMIs)
  + Amazon Machine Images (AMIs) is a complete package that you need for your server (including the operating system and additional software)
  + Amazon EC2 provides various configurations of CPU, memory, storage and networking capacity for your instances (known as instance type)
  + Secure login information for your instances using key pairs (AWS stores the public key and you can store the private key in a secure place)
  + Storage volumes of temporary data is deleted when you stop or terminate your instance (known as instance store volumes)
  + Amazon EC2 provides persistent storage volumes (using Amazon Elastic Block Store – EBS)
  + A firewall that enables you to specify the protocols, ports, and source IP ranges that can reach your instances using security groups
  + Static IP addresses for dynamic cloud computing (known as Elastic IP address)
  + Amazon EC2 provides metadata (known as tags)
  + Amazon EC2 provides virtual networks that are logically isolated from the rest of the AWS cloud, and that you can optionally (Salesforce Certification Training) connect to your own network (known as virtual private clouds – VPCs)

**Question 24. How To Migrate An Instance To Another Availability Zone ?**

**Answer :**

You can migrate your EC2 instance from one Availability Zone to another.

**Following are the steps to migrate an Instance to another Availability Zone:**

* Create an AMI from the running instance
* Launch an instance from the AMI that you just created, specify the new Availability Zone
* You can use the same instance type as the original instance, or select a new instance type
* If the original instance has an associated Elastic IP address, then associate it with the new instance
* If the original instance is a Reserved Instance, change the Availability Zone for your reservation

**Question 25. What Is Key Pair?**

**Answer:**

AWS uses public-key cryptography to secure the login information for your instance. A Linux instance has no password; you use a key pair to log in to your instance securely.

You specify the name of the key pair when you launch your instance, then provide the private key when you log in using SSH.

**Question 42. How You Will Change The Root Ebs Device Of My Amazon Ec2 Instance?**

**Answer:**

* Stop the instance.
* Detach the root EBS volume.
* Attach the alternate EBS volume (as the root e.g. /dev/sda1)
* Start the instance.
* This presupposes that your alternate EBS volume is bootable, of course – it has to contain the bootable OS image.

**Question 4. Explain Storage For Amazon Ec2 Instance?**

**Answer:**

Amazon EC2 provides many data storage options for your instances. Each option has a unique combination of performance and durability. These storages can be used independently or in combination to suit your requirements.

**There are mainly four types of storages provided by AWS:**

**Amazon EBS**

**Amazon EC2 Instance Store**

**Amazon S3**

**Adding Storage**

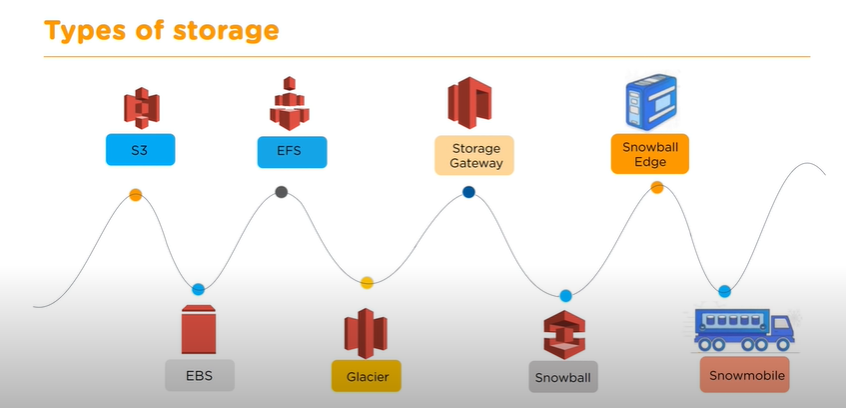
**Question 11. What Is Amazon Ec2 Root Device Volume?**

**Answer :**

When you launch an instance, the Root Device Volume contains the image used to boot the instance.

You can launch an instance from one of two types of AMIs:

1. Instance store-backed AMI
2. EBS based storage



**Question:- Amazon S3 bucket ?**

**Answer:-** An Amazon S3 bucket is a [public cloud](https://searchcloudcomputing.techtarget.com/definition/public-cloud) storage resource available in Amazon Web Services' ([AWS](https://searchaws.techtarget.com/definition/Amazon-Web-Services)) Simple Storage Service ([S3](https://searchaws.techtarget.com/definition/Amazon-Simple-Storage-Service-Amazon-S3)), an [object storage](https://searchstorage.techtarget.com/definition/object-storage) offering. Amazon S3 buckets, which are similar to file folders, store objects, which consist of [data](https://searchdatamanagement.techtarget.com/definition/data) and its descriptive metadata.

# **Amazon Elastic Block Store (Amazon EBS)**

Amazon Elastic Block Store (Amazon EBS) provides block level storage volumes for use with EC2 instances. EBS volumes behave like raw, unformatted block devices. You can mount these volumes as devices on your instances. EBS volumes that are attached to an instance are exposed as storage volumes that persist independently from the life of the instance. You can create a file system on top of these volumes, or use them in any way you would use a block device (such as a hard drive). You can dynamically change the configuration of a volume attached to an instance.

We recommend Amazon EBS for data that must be quickly accessible and requires long-term persistence. EBS volumes are particularly well-suited for use as the primary storage for file systems, databases, or for any applications that require fine granular updates and access to raw, unformatted, block-level storage. Amazon EBS is well suited to both database-style applications that rely on random reads and writes, and to throughput-intensive applications that perform long, continuous reads and writes.

## **Amazon EBS volume types**

Amazon EBS provides the following volume types, which differ in performance characteristics and price, so that you can tailor your storage performance and cost to the needs of your applications. The volumes types fall into these categories:

* [Solid state drives (SSD)](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html#solid-state-drives) — Optimized for transactional workloads involving frequent read/write operations with small I/O size, where the dominant performance attribute is IOPS.
* [Hard disk drives (HDD)](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html#hard-disk-drives) — Optimized for large streaming workloads where the dominant performance attribute is throughput.
* [Previous generation](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html#ebs-previous-generation-volumes) — Hard disk drives that can be used for workloads with small datasets where data is accessed infrequently and performance is not of primary importance. We recommend that you consider a current generation volume type instead

## **Solid state drives (SSD)**

The SSD-backed volumes provided by Amazon EBS fall into these categories:

* General Purpose SSD — provides a balance of price and performance. We recommend these volumes for most workloads.
* Provisioned IOPS SSD — Provides high performance for mission-critical, low-latency, or high-throughput workloads.

## **Hard disk drives (HDD)**

The HDD-backed volumes provided by Amazon EBS fall into these categories:

* Throughput Optimized HDD — A low-cost HDD designed for frequently accessed, throughput-intensive workloads.
* Cold HDD — The lowest-cost HDD design for less frequently accessed workloads.

## **Previous generation volume types**

The following table describes previous-generation EBS volume types. If you need higher performance or performance consistency than previous-generation volumes can provide, we recommend that you consider using General Purpose SSD (gp2 and gp3) or other current volume types

## **General Purpose SSD volumes (gp3)**

General Purpose SSD (gp3) volumes offer cost-effective storage that is ideal for a broad range of workloads. These volumes deliver a consistent baseline rate of 3,000 IOPS and 125 MiB/s, included with the price of storage. You can provision additional IOPS (up to 16,000) and throughput (up to 1,000 MiB/s) for an additional cost.

The maximum ratio of provisioned IOPS to provisioned volume size is 500 IOPS per GiB. The maximum ratio of provisioned throughput to provisioned IOPS is .25 MiB/s per IOPS. The following volume configurations support provisioning either maximum IOPS or maximum throughput:

* 32 GiB or larger: 500 IOPS/GiB x 32 GiB = 16,000 IOPS
* 8 GiB or larger and 4,000 IOPS or higher: 4,000 IOPS x 0.25 MiB/s/IOPS = 1,000 MiB/s

**General Purpose SSD volumes (gp2)**

General Purpose SSD (gp2) volumes offer cost-effective storage that is ideal for a broad range of workloads. These volumes deliver single-digit millisecond latencies and the ability to burst to 3,000 IOPS for extended periods of time. Between a minimum of 100 IOPS (at 33.33 GiB and below) and a maximum of 16,000 IOPS (at 5,334 GiB and above), baseline performance scales linearly at 3 IOPS per GiB of volume size. AWS designs gp2 volumes to deliver their provisioned performance 99% of the time. A gp2 volume can range in size from 1 GiB to 16 TiB.

**EFS (Elastic File System)**

Amazon EFS provides file storage in the AWS Cloud. With Amazon EFS, you can create a file system, mount the file system on an Amazon EC2 instance, and then read and write data to and from your file system. You can mount an Amazon EFS file system in your VPC, through the Network File System versions 4.0 and 4.1 (NFSv4) protocol. We recommend using a current generation Linux NFSv4.1 client, such as those found in the latest Amazon Linux, Redhat, and Ubuntu AMIs, in conjunction with the Amazon EFS Mount Helper

You can access your Amazon EFS file system concurrently from multiple NFS clients, so applications that scale beyond a single connection can access a file system. Amazon EC2 instances running in multiple Availability Zones within the same AWS Region can access the file system, so that many users can access and share a common data source.

To access your Amazon EFS file system in a VPC, you create one or more mount targets in the VPC. A *mount target* provides an IP address for an NFSv4 endpoint at which you can mount an Amazon EFS file system. You mount your file system using its Domain Name Service (DNS) name, which resolves to the IP address of the EFS mount target in the same Availability Zone as your EC2 instance. You can create one mount target in each Availability Zone in an AWS Region. If there are multiple subnets in an Availability Zone in your VPC, you create a mount target in one of the subnets. Then all EC2 instances in that Availability Zone share that mount target.

Mount targets themselves are designed to be highly available. As you design for high availability and failover to other Availability Zones (AZs), keep in mind that while the IP addresses and DNS for your mount targets in each AZ are static, they are redundant components backed by multiple resources.

After mounting the file system by using its DNS name, you use it like any other POSIX-compliant file system. For information about NFS-level permissions and related considerations, see [Working with Users, Groups, and Permissions at the Network File System (NFS) Level](https://docs.aws.amazon.com/efs/latest/ug/accessing-fs-nfs-permissions.html).

You can mount your Amazon EFS file systems on your on-premises data center servers when connected to your Amazon VPC with AWS Direct Connect or AWS VPN You can mount your EFS file systems on on-premises servers to migrate datasets to EFS, enable cloud bursting scenarios, or backup your on-premises data to EFS.

**What is AWS Storage Gateway?**

AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases. These include moving backups to the cloud, using on-premises file shares backed by cloud storage, and providing low latency access to data in AWS for on-premises applications.

To support these use cases, Storage Gateway offers three different types of gateways – File Gateway, Tape Gateway, and Volume Gateway – that seamlessly connect on-premises applications to cloud storage, caching data locally for low-latency access. Your applications connect to the service through a virtual machine or [gateway hardware appliance](https://aws.amazon.com/storagegateway/hardware-appliance/) using standard storage protocols, such as NFS, SMB, and iSCSI. The gateway connects to AWS storage services, such as Amazon S3, Amazon S3 Glacier, Amazon S3 Glacier Deep Archive, Amazon EBS, and AWS Backup, providing storage for files, volumes, snapshots, and virtual tapes in AWS. The service includes a highly-optimized and efficient data transfer mechanism, with bandwidth management and automated network resilience.

**What is Elastic Load Balancing?**

Elastic Load Balancing supports the following types of load balancers: **Application Load Balancers**, **Network Load Balancers**, and **Classic Load Balancers**. Amazon ECS services can use either type of load balancer. Application Load Balancers are used to route HTTP/HTTPS (or Layer 7) traffic. Network Load Balancers and Classic Load Balancers are used to route TCP (or Layer 4) traffic.

* **Classic Load Balancer**

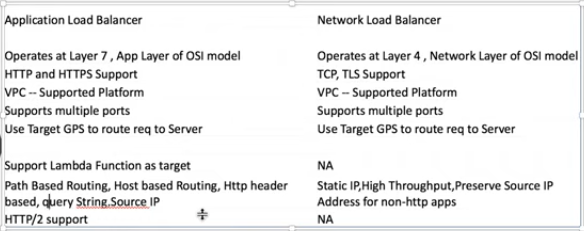
A Classic Load Balancer makes routing decisions at either the transport layer (TCP/SSL) or the application layer (HTTP/HTTPS). Classic Load Balancers currently require a fixed relationship between the load balancer port and the container instance port. For example, it is possible to map the load balancer port 80 to the container instance port 3030 and the load balancer port 4040 to the container instance port 4040. However, it is not possible to map the load balancer port 80 to port 3030 on one container instance and port 4040 on another container instance. This static mapping requires that your cluster has at least as many container instances as the desired count of a single service that uses a Classic Load Balancer

* **Application Load Balancer**

An Application Load Balancer makes routing decisions at the application layer (HTTP/HTTPS), supports path-based routing, and can route requests to one or more ports on each container instance in your cluster. Application Load Balancers support dynamic host port mapping. For example, if your task's container definition specifies port 80 for an NGINX container port, and port 0 for the host port, then the host port is dynamically chosen from the ephemeral port range of the container instance (such as 32768 to 61000 on the latest Amazon ECS-optimized AMI). When the task is launched, the NGINX container is registered with the Application Load Balancer as an instance ID and port combination, and traffic is distributed to the instance ID and port corresponding to that container. This dynamic mapping allows you to have multiple tasks from a single service on the same container instance

* **Network Load Balancer**

A Network Load Balancer makes routing decisions at the transport layer (TCP/SSL). It can handle millions of requests per second. After the load balancer receives a connection, it selects a target from the target group for the default rule using a flow hash routing algorithm. It attempts to open a TCP connection to the selected target on the port specified in the listener configuration. It forwards the request without modifying the headers. Network Load Balancers support dynamic host port mapping. For example, if your task's container definition specifies port 80 for an NGINX container port, and port 0 for the host port, then the host port is dynamically chosen from the ephemeral port range of the container instance (such as 32768 to 61000 on the latest Amazon ECS-optimized AMI). When the task is launched, the NGINX container is registered with the Network Load Balancer as an instance ID and port combination, and traffic is distributed to the instance ID and port corresponding to that container. This dynamic mapping allows you to have multiple tasks from a single service on the same container instance



# **What is IAM?**

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

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 called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the [best practice of using the root user only to create your first IAM user](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#create-iam-users). Then securely lock away the root user credentials and use them to perform only a few account and service management tasks.

1. What is AWS?

AWS is a secure cloud service platform which is offering compute power, database storage, content delivery and other facilities to help businesses scale and grow.

1. aws has three basic types of cloud services:

compute

stoage

networking

1. aws storage:-

s3

glacier

ELB

EFS

1. Aws networks:-

VPC

Route53

CloudFront

1. What is the diff between AMI and instance?

Many diff types of instances can be launched from one AMI.

An instance type determines the hardware of the host computer used for your instance.

1. What is the diff between scalability and elasticity?

Scalablity is the ability of a system to handle the increased load

on its current hardware and software resources.

Elasticity is the ability of a system to increase the workload by

Increasing the hardware/software resources dynamically.

1. In what scenario should we use classic load balancer and application load balancer?

AWS kinises

1. Can you run multiple websites on an EC2 server using a single IP address?

More than one elastic IP is required to run multiple websites on EC2.

1. A content management system running on EC2 instance is approaching 100% CPU utilization. How will you reduce the load on EC2 instance ?

This can be done by attaching a load balancer to an autoscaling group to efficiently distribute load among all instances.

1. Can you modify the private IP address of an EC2 instance while it is running in a VPC ?

It is not possible to change the primary private IP addresses. However, secondary IP addresses can be assigned, unassigned or moved between instances at any given point.

1. What are EBS volumes?

EBS stands for Elastic Block Stores. They are persistent volumes that you can attach to the instances. With EBS volumes, your data will be preserved even when you stop your instances, unlike your instance store volumes where the data is deleted when you stop the instances.

1. What are the types of volumes in EBS?

Following are the types of volumes in EBS,

General purpose

Provisioned IOPS

Magnetic

Cold HDD

Throughput optimized

1. What are the different types of instances?

Answer: Following are the types of instances,

General purpose

Computer Optimized

Storage Optimized

Memory Optimized

Accelerated Computing

1. What is an auto-scaling and what are the components?

Answer: Auto scaling allows you to automatically scale-up and scale-down the number of instances depending on the CPU utilization or memory utilization. There are 2 components in Auto scaling, they are Auto-scaling groups and Launch Configuration.

Type of autoscalling?

Manual autoscalling---- In this we will define minimum and maximum auto scalling.

Scheduling Autoscalling----In this, We have knowledge about load pattern and we know that load will increase from Monday to Friday then we will use scheduling autoscalling.

Dynamic Autoscalling---- In this, we don’t know about load then we will define some threshold like CPU utilization, Memory utilization then

What are the advantages of auto-scaling?

Following are the advantages of autoscaling

* Offers fault tolerance
* Better availability
* Better cost management

1. What are reserved instances?

Answer: Reserved instances are the instance that you can reserve a fixed capacity of EC2 instances. In reserved instances you will have to get into a contract of 1 year or 3 years.

1. What is an AMI?

Answer: AMI stands for Amazon Machine Image. AMI is a template that contains the software configurations, launch permission and a block device mapping that specifies the volume to attach to the instance when it is launched.

1. What is an EIP?

Answer: EIP stands for Elastic IP address. It is designed for dynamic cloud computing. When you want to have a static IP address for your instances when you stop and restart your instances, you will be using EIP address.

1. What is Cloudwatch?

Answer: Cloudwatch is a monitoring tool that you can use to monitor your various AWS resources. Like health check, network, Application, etc.

1. What are the types in cloudwatch?

Answer: There are 2 types in cloudwatch. Basic monitoring and detailed monitoring. Basic monitoring is free and detailed monitoring is chargeable.

1. What are the cloudwatch metrics that are available for EC2 instances?

Answer: Diskreads, Diskwrites, CPU utilization, networkpacketsIn, networkpacketsOut, networkIn, networkOut, CPUCreditUsage, CPUCreditBalance.

1. What is the minimum and maximum size of individual objects that you can store in S3

Answer: The minimum size of individual objects that you can store in S3 is 0 bytes and the maximum bytes that you can store for individual objects is 5TB.

1. What are the different storage classes in S3?

Answer: Following are the types of storage classes in S3,

Standard frequently accessed

Standard infrequently accessed

One-zone infrequently accessed.

Glacier

RRS – reduced redundancy storage

1. What is the default storage class in S3?

Answer: The default storage class in S3 in Standard frequently accessed.

1. What is glacier?

Answer: Glacier is the back up or archival tool that you use to back up your data in S3.

1. How can you secure the access to your S3 bucket?

Answer: There are two ways that you can control the access to your S3 buckets,

1. ACL – Access Control List

Bucket polices

1. How can you encrypt data in S3?

Answer: You can encrypt the data by using the below methods,

Server Side Encryption – S3 (AES 256 encryption)

Server Side Encryption – KMS (Key management Service)

Server Side Encryption – C (Client Side)

1. What are policies and what are the types of policies?

Answer: Policies are permissions that you can attach to the users that you create. These policies will contain that access that you have provided to the users that you have created. There are 2 types of policies.

Managed policies

Inline policies

1. What is cloudfront?

Answer: Amazon CloudFront is a fast content delivery network (CDN) service that

securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

1. What is the maximum individual archive that you can store in glacier?

Answer: You can store a maximum individual archive of upto 40 TB.

1. What is VPC?

Answer: VPC stands for Virtual Private Cloud. VPC allows you to easily customize your networking configuration. VPC is a network that is logically isolated from other network in the cloud. It allows you to have your own IP address range, subnets, internet gateways, NAT gateways and security groups.

1. What is VPC peering connection?

Answer: VPC peering connection allows you to connect 1 VPC with another VPC. Instances in these VPC behave as if they are in the same network.

1. What are NAT gateways?

Answer: NAT stands for Network Address Translation. NAT gateways enables instances in a private subnet to connect to the internet but prevent the internet from initiating a connection with those instances.

1. How can you control the security to your VPC?

Answer: You can use security groups and NACL (Network Access Control List) to control the security to your VPC.

1. What is a snowball?

Answer: Snowball is a data transport solution that used source appliances to transfer large amounts of data into and out of AWS. Using snowball, you can move huge amount of data from one place to another which reduces your network costs, long transfer times and also provides better security.

1. What are the database types in RDS?

Answer: Following are the types of databases in RDS,

Aurora

Oracle

MYSQL server

Postgresql

MariaDB

SQL server

1. What is a redshift?

Answer: Amazon redshift is a data warehouse product. It is a fast and powerful, fully managed, petabyte scale data warehouse service in the cloud.

1. Explain what AWS is?

AWS stands for Amazon Web Service; it is a collection of remote computing services also known as a cloud computing platform.  This new realm of cloud computing is also known as IaaS or Infrastructure as a Service.

1. Mention what the key components of AWS are?

The key components of AWS are

* Route 53:A DNS web service
* Simple E-mail Service:It allows sending e-mail using RESTFUL API call or via regular SMTP
* Identity and Access Management:It provides enhanced security and identity management for your AWS account
* Simple Storage Device or (S3):It is a storage device and the most widely used AWS service
* Elastic Compute Cloud (EC2): It provides on-demand computing resources for hosting applications. It is handy in case of unpredictable workloads
* Elastic Block Store (EBS):It offers persistent storage volumes that attach to EC2 to allow you to persist data past the lifespan of a single Amazon EC2 instance
* CloudWatch: To monitor AWS resources, It allows administrators to view and collect key Also, one can set a notification alarm in case of trouble.

1. Explain what S3 is?

S3 stands for Simple Storage Service. You can use S3 interface to store and retrieve any amount of data, at any time and from anywhere on the web.  For S3, the payment model is “pay as you go.”

1. What is AMI?

AMI stands for Amazon Machine Image.  It’s a template that provides the information (an operating system, an application server, and applications) required to launch an instance, which is a copy of the AMI running as a virtual server in the cloud.  You can launch instances from as many different AMIs as you need.

1. Mention what the relationship between an instance and AMI is?

From a single AMI, you can launch multiple types of instances.  An instance type defines the hardware of the host computer used for your instance. Each instance type provides different computer and memory capabilities.  Once you launch an instance, it looks like a traditional host, and we can interact with it as we would with any computer.

1. What does an AMI include?

An AMI includes the following things

* A template for the root volume for the instance
* Launch permissions decide which AWS accounts can avail the AMI to launch instances
* A block device mapping that determines the volumes to attach to the instance when it is launched

1. How can you send a request to Amazon S3?

Amazon S3 is a REST service, and you can send a request by using the REST API or the AWS SDK wrapper libraries that wrap the underlying Amazon S3 REST API.

1. Mention what the difference between Amazon S3 and EC2 is?

The difference between EC2 and Amazon S3 is that

|  |  |
| --- | --- |
| EC2 | S3 |
| * It is a cloud web service used for hosting your application | * It is a data storage system where any amount of data can be stored |
| * It is like a huge computer machine which can run either Linux or Windows and can handle application like PHP, Python, Apache or any databases | * It has a REST interface and uses secure HMAC-SHA1 authentication keys |

1. How many buckets can you create in AWS by default?

By default, you can create up to 100 buckets in each of your AWS accounts.

10) Explain can you vertically scale an Amazon instance? How?

Yes, you can vertically scale on Amazon instance. For that

* Spin up a new larger instance than the one you are currently running
* Pause that instance and detach the root webs volume from the server and discard
* Then stop your live instance and detach its root volume
* Note the unique device ID and attach that root volume to your new server
* And start it again

11) Explain what T2 instances is?

T2 instances are designed to provide moderate baseline performance and the capability to burst to higher performance as required by the workload.

12) In VPC with private and public subnets, database servers should ideally be launched into which subnet?

With private and public subnets in VPC, database servers should ideally launch into private subnets.

13) Mention what the security best practices for Amazon EC2 are?

For secure Amazon EC2 best practices, follow the following steps

* Use AWS identity and access management to control access to your AWS resources
* Restrict access by allowing only trusted hosts or networks to access ports on your instance
* Review the rules in your security groups regularly
* Only open up permissions that you require
* Disable password-based login, for example, launched from your AMI

14) Explain how the buffer is used in Amazon web services?

The buffer is used to make the system more robust to manage traffic or load by synchronizing different component.  Usually, components receive and process the requests in an unbalanced way. With the help of buffer, the components will be balanced and will work at the same speed to provide faster services.

15) While connecting to your instance what are the possible connection issues one might face?

The possible connection errors one might encounter while connecting instances are

* Connection timed out
* User key not recognized by the server
* Host key not found, permission denied
* An unprotected private key file
* Server refused our key or No supported authentication method available
* Error using MindTerm on Safari Browser
* Error using Mac OS X RDP Client

16) What are key-pairs in AWS?

Key-pairs are secure login information for your virtual machines. To connect to the instances, you can use key-pairs which contain a public-key and private-key.

17)  What are the different types of instances?

Following are the types of instances:

* General purpose
* Computer Optimized
* Memory Optimized
* Storage Optimized
* Accelerated Computing

18) Is the property of broadcast or multicast supported by Amazon VPC?

No, currently Amazon VPI not provide support for broadcast or multicast.

19) How many Elastic IPs is allows you to create by AWS?

5 VPC Elastic IP addresses are allowed for each AWS account.

20) Explain default storage class in S3

The default storage class is a Standard frequently accessed.

21) What are the roles?

Roles are used to providing permissions to entities which you can trust within your AWS account. Roles are very similar to users. However,  with roles, you do not require to create any username and password to work with the resources.

22) What are the edge locations?

Edge location is the area where the contents will be cached. So, when a user is trying to accessing any content, the content will automatically be searched in the edge location.

23) What is VPC?

VPC stands for Virtual Private Cloud. It allows you to customize your networking configuration. It is a network which is logically isolated from another network in the cloud. It allows you to have your IP address range,  internet gateways, subnet and security groups.

24) Explain snowball

Snowball is a data transport option. It used source appliances to a large amount of data into and out of AWS. With the help of snowball, you can transfer a massive amount of data from one place to another. It helps you to reduce networking costs.

25) What is a redshift?

Redshift is a big data warehouse product. It is fast and powerful, fully managed data warehouse service in the cloud.

27) What is meant by subnet?

A large section of IP Address divided into chunks is known as subnets.

28) Can you establish a Peering connection to a VPC in a different region?

No, It’s only possible between VPCs in the same region.

29) What is SQL?

Simple Queues Services also known as SQL. It is distributed queuing service which acts as a mediator for two controllers.

30) How many subnets can you have per VPC?

You can have 200 subnets per VPC.

31) DNS  and Load Balancer service comes under which type of cloud service?

DNS and Load Balancer and DNS services come under IAAS-storage cloud service.

32) What is the role of AWS CloudTrail?

CloudTrail is a specially designed tool for logging and tracking API calls. It helps to audit all S3 bucket accesses.

33) When EC2 officially launched?

EC2 officially launched in the year 2006.

34) What is SimpleDB?

SimpleDB is a data repository of structure record which encourages data doubts and indexing both S3 and EC2are called SimpleDB.

35) Explain Amazon ElasticCache

Amazon Elasticcache is a web service which makes it easy to deploy, scale and store data in the cloud.

36) What is AWS Lambda?

Lambda is an Amazon compute service which allows you to run code in the  AWS Cloud without managing servers.

37) Name the types of AMI provided by AWS

The types of AMI provided by AWS are:

1. Instance store backed
2. EBS backed

38) Name the AWS service exists only to redundantly cache data and images?

AWS Edge locations are service which redundantly cache data and images.

39) Explain Geo Restriction in CloudFront

A Geo-restriction feature helps you to prevent users of specific geographic locations from accessing content which you’re distributing through a CloudFront web distribution.

40) What is Amazon EMR?

EMR is a survived cluster stage which helps you to interpret the working of data structures before the intimation.  Apache Hadoop and Apache Spark on the Amazon Web Services helps you to investigate a large amount of data. You can prepare data for the analytics goals and marketing intellect workloads using Apache Hive and using other relevant open source designs.

41) What is boot time taken for the instance stored backed AMI?

The boot time for an Amazon instance store-backend AMI is less than 5 minutes.

42) Do you need an internet gateway to use peering connections?

Yes, the Internet gateway is needed to use VPC (virtual private cloud peering) connections.

43) How to connect EBS volume to multiple instances?

We can’t be able to connect EBS volume to multiple instances.  Although, you can connect various EBS Volumes to a single instance.

44) List different types of cloud services

Various types of cloud services are:

* Software as a Service (SaaS),
* Data as a Service (DaaS)
* Platform as a Service (PaaS)
* Infrastructure as a Service (IaaS).

45) State the difference between An Instance  and AMI

AMI is a template consisting software configuration part. For example Operating systems, applications, application server if you start an instance, a duplicate of the AMI in a row as an attendant in the cloud.

46) What are the different types of Load Balancer in AWS services?

Two types of Load balancer are:

1. Application Load Balancer
2. Classic Load Balancer

47) In which situation you will select provisioned IOPS over standard RDS storage?

You should select provisioned IOPS storage over standard RDS storage if you want to perform batch-related workloads.

48) What are the important features of Amazon cloud search?

Important features of the Amazon cloud are:

* Boolean searches
* Prefix Searches
* Range searches
* Entire text search
* AutoComplete advice

49) Can vertically scaling is allows in  Amazon Instance?

Yes, you can vertically estimate one Amazon instance.

50) What is the use of lifecycle hooks in Autoscaling?

Lifecycle hooks are used for autoscaling to put an additional wait time to a scale in or scale out event.

51) What are various layers of Cloud Architecture explained in AWS training?

Different layers of cloud architecture are:

* Cloud controller
* Cluster controller
* Storage Controller
* Node Controller

52) What are the storage class available in Amazon s3?

Storage classes available with Amazon s3 are:

* Amazon S3 standard
* Amazon S3 standard-infrequent Access
* Amazon S3 Reduced Redundancy Storage
* Amazon Glacier

53) Name some of the DB engines which can be used in AWS RDS

1. MS-SQL DB
2. MariaDB
3. MYSQL DB
4. OracleDB
5. PostgreDB

54.) What is difference between public IP and Static IP?

Ans: Static means the IP address never changes as long as you stay with the same provider or same server. ... Public means the IP address can be visited from any computer in the world. Private means the IP address can only be used by those on the same network.