**VPC:**

Amazon Virtual Private Cloud (Amazon VPC) is a logically isolated section of the AWS Cloud where you can launch AWS resources and objects etc.

**What Are The Connectivity Options For VPC:**

A variety of connectivity options exist for your Amazon VPC. You can connect your VPC to the Internet, to your data center, or other VPCs.

* Connect directly to the Internet (public subnets)– You can launch instances into a publicly accessible subnet where they can send and receive traffic from the Internet.
* Connect to the Internet using Network Address Translation (private subnets) – Private subnets can be used for instances that you do not want to be directly addressable from the Internet. Instances in a private subnet can access the Internet without exposing their private IP address by routing their traffic through a Network Address Translation (NAT) gateway in a public subnet.
* Connect securely to your corporate datacenter– All traffic to and from instances in your VPC can be routed to your corporate datacenter over an industry standard, encrypted IPsec hardware VPN connection.
* Connect privately to other VPCs- Peer VPCs together to share resources across multiple virtual networks owned by your or other AWS accounts
* Privately connect to AWS Services without using an Internet gateway, NAT or firewall proxy through a VPC Endpoint. Available AWS services include S3, DynamoDB, Kinesis Streams, Service Catalog, AWS Systems Manager, Elastic Load Balancing (ELB) API, Amazon Elastic Compute Cloud (EC2) API, and SNS.

**How Do You Connect My Vpc To The Internet?**

Internet gateway enables Amazon EC2 instances in the VPC to directly access the Internet.

**Egress-only Internet Gateway:** A stateful gateway to provide egress only access for IPv6 traffic from the VPC to the Internet.

**Router:** Routers interconnect subnets and direct traffic between Internet gateways, virtual private gateways, NAT gateways, and subnets.

**Which customer gateway devices can I use to connect to Amazon VPC:**

There are two types of VPN connections that you can create: statically-routed VPN connections and dynamically-routed VPN connections.

**Can You Monitor The Network Traffic In Your Vpc?**

Yes. You can use the Amazon VPC Flow Logs feature to monitor the network traffic in your VPC.

**Can You Peer Two Vpcs With Matching Ip Address Ranges?**

No. Peered VPCs must have non-overlapping IP ranges.

Security groups act as a firewall for associated instances, controlling both inbound and outbound traffic at the instance level.

**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 your require

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

**Amazon EBS:** Its durable, block-level storage volumes can attached in running Amazon EC2 instance. The Amazon EBS volume persists independently from the running life of an Amazon EC2 instance.

**Amazon EC2 Instance Store:** Storage disk that is attached to the host computer is referred to as instance store.

**Amazon S3:** Amazon S3 provides access to reliable and inexpensive data storage infrastructure.

**Adding Storage:** Every time you launch an instance from an AMI, a root storage device is created for that instance. The root storage device contains all the information necessary to boot the instance.

**Regions And Availability Zones**

Each region is a separate geographic area. Each region has multiple, isolated locations known as Availability Zones.

Each region is completely independent. Each Availability Zone is isolated, but the Availability Zones in a region are connected through low-latency links

**Amazon Ec2 Root Device Volume:**

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:**

* Instance store-backed AMI
* EBS based storage

By default, the root device volume for an AMI backed by Amazon EBS is deleted when the instance terminates. To change the default behavior, set the DeleteOnTermination attribute to false using a block device mapping.

[Create a repository in github via gitbash or command prompt](https://stackoverflow.com/questions/20390487/create-a-repository-in-github-via-gitbash-or-command-prompt):

D:\gitproject>git remote add origin <https://github.com/lucycloud/NewRepo.git>

git remote add origin git@github.com:alexpchin/<reponame>.git

git push -u origin master

The command git remote add origin https://github.com/lucycloud/NewRepo.git does not add a new repository on the remote machine. What it does is tell git on your current machine that it should expect a remote repository at the location you specified.

There is no way to create a new repository on the remote machine through git.

[How do I delete a Git branch locally and remotely](https://stackoverflow.com/questions/2003505/how-do-i-delete-a-git-branch-locally-and-remotely):

Remotely

$ git push --delete <remote\_name> <branch\_name>

$ git branch -d <branch\_name>

Locally

$ git branch -d branch\_name

$ git branch -D branch\_name

**Amazon Machine Image:**

An Amazon Machine Image (AMI) is a template that contains a software configuration (for example, an operating system, an application server, and applications). From an AMI, we launch an instance, which is a copy of the AMI running as a virtual server in the cloud. We can even launch multiple instances of an AMI.

**Create Your Own Amazon Machine Image:**

You can customize a instance that is launched from a public AMI and then save that configuration as a custom AMI for your own use.

Instances that you launch from your AMI use all the customizations that you’ve made.

**How 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

**How To Determine The Root Device Type Of Your Ami**

**Method 1:** Following are the steps to determine the Root Device type of an AMI using the console

1. Open the Amazon EC2 console
2. In the navigation pane, click AMIs, and select the AMI
3. Check the value of Root Device Type in the Details tab as follows

* If the value is ebs, this is an Amazon EBS-backed AMI
* If the value is instance store, this is an instance store-backed AMI

**Method 2:** Following are the steps to determine the root device type of an AMI using the command line

We can use one of the following commands.

1. describe-images (AWS CLI)
2. Get-EC2Image (AWS Tools for Windows PowerShell)

Amazon EBS – Backed is 16 TiB

Amazon Instance Store-Backed is 10 GiB

S3 can be used for instances with root devices backed by local instance storage

**Following are the steps to disable password-based EC2 remote logins for the root user:**

**Open the /etc/ssh/sshd\_config file with a text editor and locate the following line:**  
#PermitRootLogin yes  
**Change the line to:**  
PermitRootLogin without-password

**How You Will Change The Root Ebs Device Of My Amazon Ec2 Instance:**

* 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.

**Some of the main features of Classic Load Balancer (CLB) in Amazon EC2 are as follows:**

**Health Check:** Based on the result of Health Check, Classic Load Balancer can decide to route the traffic. If any instance has unhealthy results, CLB will not route the traffic to that instance.

**Security:** We can create security groups for CLB in Virtual Private Cloud (VPC). With these features, it is easy to implement secure load balancing within a network.

**High Availability:** With CLB, we can distribute traffic among EC2 instances in single or multiple Availability Zones. This helps in providing very high scale of availability for the incoming traffic.

**Sticky Sessions:** CLB also supports sticky session by using cookies. The sticky sessions make sure that the traffic from a user is always routed to the same instance so that user gets seamless experience.

**IPv6:** CLB also support Internet Protocol version 6.

**Operational Monitoring:** We can also perform operational monitoring CLB and collect statistics on request count, latency etc. These metrics can be monitored in CloudWatch.

**Main features of Application Load Balancer (ALB) are as follows:**

* + **Content-Based Routing:** In ALB, we can make use of content in the request to decide the routing of a request to a specific service.
  + **HTTP/2:** ALB supports the new version of HTTP protocol. In this protocol, we can send multiple requests on same connection. It also supports TLS and header compression.
  + **WebSockets:** ALB supports WebSockets in EC2. With WebSockets, a server can exchange real-time messages with the end-users.
  + **Layer-7 Load Balancing:** ALB can also load balance HTTP/HTTPS application with layer-7 specific features.
  + **Delete Protection:** ALB also provides Delete Protection option by which we can prevent it from getting deleted by mistake.
  + **Containerized Application Support:** We can use ALB to load balance multiple containers across multiple ports on same EC2 instance.

S**ome of the possible connection issues with EC2 instance are:**

* Connection time out
* Permission denied due to host key not found
* Unprotected private key file
* Permission denied due to user key not recognized by server
* No supported authentication method available
* Server refused the key AWS Video Training

SAAS – Software as a Service   
DAAS – Data as a Service.   
PAAS – Platform as a Service.  
IAAS – Infrastructure as a Service

Amazon Glacier is a storage service optimized for infrequently used data or Cold data.  
Amazon Glacier service is an extremely low-price storage service that provides robust storage with security features for data archiving and backup. With Amazon Glacier, customers can store their data cost effectively for months, years, or even decades.

An Elastic IP address is a static ipv4 address designed for dynamic cloud computing. An Elastic IP address is associated with your AWS account. An Elastic IP address is a reserved public IP address that you can assign to any EC2 instance in a particular region, until you choose to release it

Cloud watch: To monitor AWS resources, It allows administrators to view and collect key Also, one can set a notification alarm in case of trouble.

Amazon Route 53 (Route 53) is a scalable and highly available Domain Name System (DNS). The name is a reference to TCP or UDP port 53, where DNS server requests are addressed.

Auto scaling is a feature of AWS which allows you to configure and automatically provision and spin up new instances without the need for your intervention. Auto Scaling helps you maintain application availability and allows you to dynamically scale your Amazon EC2 capacity up or down automatically according to conditions you define.

Subnets:

If there is a network which has a large no. of hosts, managing all these hosts can be a tedious job. Therefore we divide this network into subnets (sub-networks) so that managing these hosts becomes simpler.

Primary private IP address is attached with the instance throughout its lifetime and cannot be changed, however secondary private addresses can be unassigned, assigned or moved between interfaces or instances at any point.

Yes, you can do this by establishing a VPN(Virtual Private Network) connection between your company’s network and your VPC (Virtual Private Cloud), this will allow you to interact with your EC2 instances as if they were within your existing network.

Route Tables are used to route network packets, therefore in a subnet having multiple route tables will lead to confusion as to where the packet has to go. Therefore, there is only one route table in a subnet, and since a route table can have any no. of records or information, hence attaching multiple subnets to a route table is possible.

**If I launch a standby RDS instance, will it be in the same Availability Zone as my primary?**

No, since the purpose of having a standby instance is to avoid an infrastructure failure (if it happens), therefore the standby instance is stored in a different availability zone, which is a physically different independent infrastructure.

**When would I prefer Provisioned IOPS over Standard RDS storage?**

Provisioned IOPS deliver high IO rates but on the other hand it is expensive as well. Batch processing workloads do not require manual intervention they enable full utilization of systems, therefore a provisioned IOPS will be preferred for batch oriented workload.

**How is Amazon RDS, DynamoDB and Redshift different?**

* Amazon RDS is a database management service for relational databases,  it manages patching, upgrading, backing up of data etc. of databases for you without your intervention. RDS  is a Db management service for structured data only.
* DynamoDB, on the other hand, is a NoSQL database service, NoSQL deals with unstructured data.
* Redshift, is an entirely different service, it is a data warehouse product and is used in data analysis.

**If I am running my DB Instance as a Multi-AZ deployment, can I use the standby DB Instance for read or write operations along with primary DB instance?**

No,Standby DB instance cannot be used with primary DB instance in parallel, as the former is solely used for standby purposes, it cannot be used unless the primary instance goes down.

### What happens to my backups and DB Snapshots if I delete my DB Instance?

When you delete a DB instance, you have an option of creating a final DB snapshot, if you do that you can restore your database from that snapshot. RDS retains this user-created DB snapshot along with all other manually created DB snapshots after the instance is deleted, also automated backups are deleted and only manually created DB Snapshots are retained.