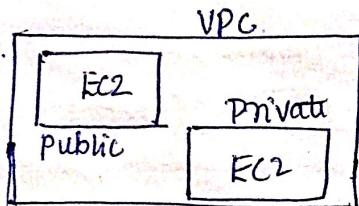


## VPC

- \* VPC mainly allows you to create your own network and deploys all the resources within the VPC.
- \* we need to create ~~the~~, subnets, Internet Gateway (IG), security groups, Routing table(RT) we need to create all this configurations in order to create an EC2 instance.
- \* How do you decide how many IP addresses you want?  
with the CIDR (clauses Intra Domain Routing.)  
help of
- CIDR is nothing but creating your own VPC (By creating a site and building your own home).
- \* In VPC there will be 2 areas?
  1. public subnets
  2. private subnets.



Eg: If we use an EC2 instance in a public subnet we can access the resources with an internet.

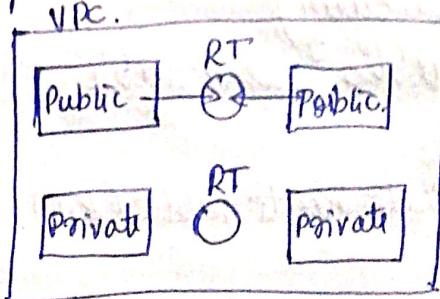
- If we use an EC2 instance in a private subnet, only within a project, company and team members if they have access they can access it
- over the internet no one can connect the instance.

- \* Initially to create a VPC (steps to be taken)
  1. ~~steps~~ a to create an VPC
  2. how many IP addresses required to create
  3. once a VPC is created then decide how many public subnets and how many private subnets needed
  4. divide the IP address for each subnets.
- \* front end should be accessed to the public subnet  
(Eg: website layout)
- \* Backend consists of the databases. this will be in a private subnet.

\* AWS will create a automatic default VPC, default subnets for an EC2 instances.

\* what is Route table:

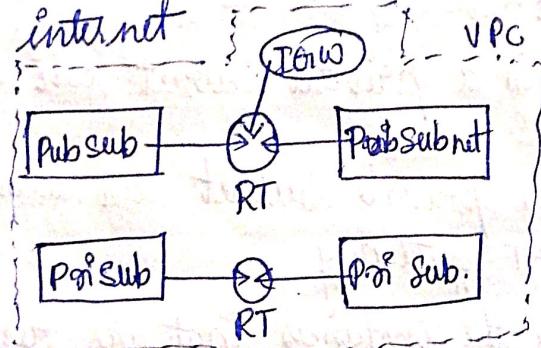
Route table is required to connect one particular instance to another particular instance. Resource / instance.



once routetable is created we need to add the subnets to the route table

\* IGW (Internet gateway)

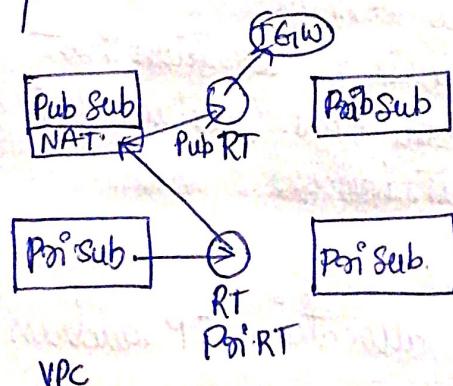
one the IGW connects to the Route table (RT) we can get access to the internet



If you add a IGW to the private subnets it will convert to an public subnets.

\* NAT Gateway (Network access Translation).

If a developer need to access an internet in order to download some packages (eg: tomcat) he uses NAT gateway but outside person cannot access to the private.



We cannot add NAT Gateway in the private Subnets

- \* Setting up an VPC (complete procedure)
  1. Create a VPC
  2. Create subnets
  3. Create RT (route table)
    - ↳ we need to add the subnets to the route table.
  4. Create IGW (Internet Gateway)
    - ↳ add it in a public Route table
  5. Create a NAT Gateway.
    - ↳ Link to an private Route table (RT).
- \* what is public subnets?

Resources residing in a public subnet can have a access over the internet
- \* what is private subnets?

Resources residing in a private subnet cannot have a access over the internet.
- \* how do the resources in a private subnet can access over the internet?

The resources in a private Subnet can access over the internet using a NAT gateway
- \* how do you connect to the instances that are residing in a private subnet?

We can connect by using a bastion host
- \* what is bastion host?

It is a instance ie present in a public subnet which mainly allows you to ssh into the private instance.
- \* how do you connect an instances residing in a private subnet?

There are 2 ways to connect.
  1. either by connecting through Bastion host
  2. either by configuring the VPN. (Virtual private network) to connect to those instances.
- \* what is CIDR

It is a method for allocating IP address and for IP routing.

\* how do we assign IP address? (calculation)

$2^{32-n}$  (formula)

Eg. 10.0.0.0/24.

$$2^{32-n} = 1000$$

find n number.

$2^{32-24}$

$2^8 = 256 \rightarrow$  IP addresses are in VPC

10.0.0.0/25

$2^{32-25}$

$2^7 = 128 \rightarrow$  IP

\* we will decide the IP address

Eg: representation of 256 IP address

10.0.0.0

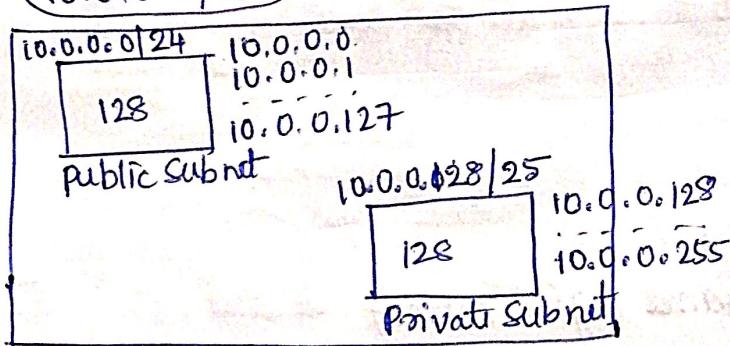
10.0.0.1

10.0.0.255

\* how do we assign the IP address

Eg: 256 IP address.

10.0.0.0/24 → CIDR.



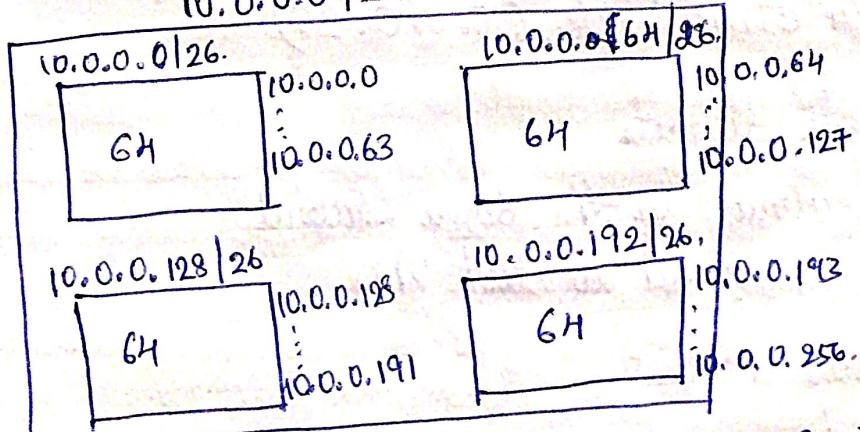
$$2^{32-n} = 128$$

$$n = 25$$

$$2^{32-n} = 256$$

\* 10.0.0.0 → 256 IP address

10.0.0.0/24



$$2^{32-n} = 64 \rightarrow 256$$

CIDR means → (Classes interdomain routing)

## \* Create a VPC:

- Click on VPC  $\rightarrow$  your VPC's  
↓  
Create VPC  
↓  
give a name to VPC  
↓  
select IPv4 CIDR manual input in IPv4 CIDR Block  
↓  
In IPv4 CIDR specify  
10.0.0.0/24  
↓  
no IPv6 address (default)  
↓  
Tenancy  $\rightarrow$  Default.  
↓  
Tags will be created default or specify name  
↓  
create VPC.

## 2 step $\rightarrow$ create subnets:

- select a VPC  
↓  
In subnets settings  
↳ subnet name (give name)

↓  
select availability zone

↓  
IPv4 CIDR block (10.0.0.25)

↓  
Create subnets

create one more subnet in the same subnet  
both should be associated to test VPC.

## 3 step $\rightarrow$ create Route table.

↓  
specify name  $\rightarrow$  public route table

↓  
Select VPC  $\rightarrow$  create Route table

Similarly create a private route table  
4. add a subnets to the specific route table.

select In RouteTable itself

select the public or private route table

go to subnet association

click on edit subnet association

select the public subnet

save association

Similarly do for private subnet association -

Step 4. → create a internet Gateway

give name

click on create IGW.

to attach the VPC to the gateway.

In IGW.

select the Gateway

Go to actions

select attach to VPC.

In VPC (window pop-up)

select the particular VPC

click on attach internet gateway.

Step 5 → Add to the public route table

go to route table → select public RT → come to routes  
click on edit route → add route default is 0.0.0.0/0 → select  
the igw created for test purpose → save changes.

& create a ~~NAT~~ NAT Gateway?  
Create NAT Gateway.  
give name.

↓  
select a public subnet.

↓  
select the private (connectivity type)

↓  
In tags it will be a default selected

↓  
create NAT Gateway.

\* how do you secure ~~your~~ your VPC?

1. NACL (Network ACLs)

2. security groups.

- Security groups can be added to the multiple instances that port numbers should be same.
- If the ports are different we need to create different security groups

- Security groups applicable to EC2 instances  
- NACL's applicable to subnets

(mainly used to change the ports in Subnets).

\* what is statefull and stateless filtering? or  
what is statefull and stateless firewall,

Security groups are considered as statefull

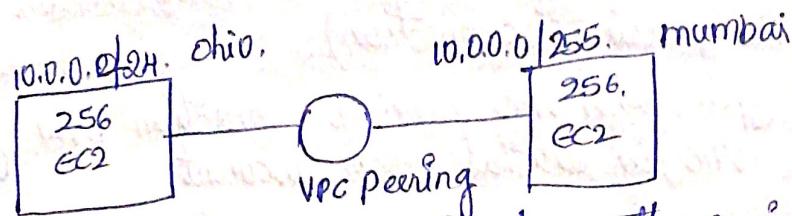
NACLs are considered as stateless

statefull → this means any changes applied on incoming rule / inbound rule will be automatically applied to outbound rule.

stateless. → Any changes applied to incoming rule will not be applied to the outgoing rule.

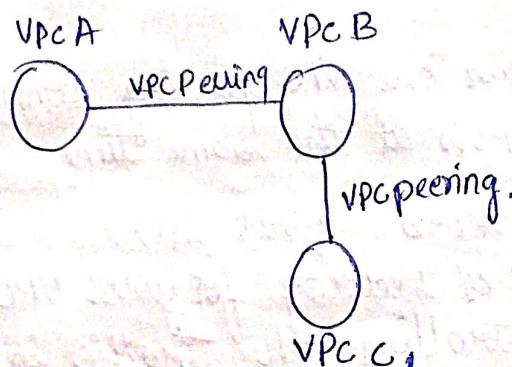
deny takes the precedence than allow.

\* VPC peering.



to connect ~~two~~ VPC of one region to another region we use VPC peering.

If the CIDR is containing the same IP addresses along with sequence we cannot make a VPC peering. (IP address should not overlap)



VPC peering allows one to one (transitive) peering is not allowed. in VPC peering.

\* Limitations of VPC? or VPC Quota.

1. 5 VPC per region
2. 5 IGW per region
3. Subnet per VPC 200
4. IPV4 CIDR block per VPC 4
5. Elastic IP addresses per region 5
6. Internet gateways per region 5
7. NAT Gateways per availability zone 5
8. Network ACL's per VPC 200.

9. Rules per network ACL 200

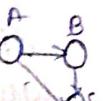
\* what is VPC Peering?

- A VPC peering connection is a networking connection b/w 2 VPC that enables you to route traffic b/w them using private IPV4

- Instances in either VPC can communicate with each other as if they are in the same network
- The VPCs can be in a different regions. (also known as interregion VPC peering connection).
- You can create your own VPC peering connection b/w your own VPC's or with a VPC in another AWS account.

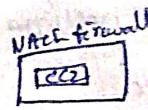
#### \* Conditions of VPC?

- CIDR block should not overlap
- Transit peering relationships are not supported.
- If VPCs are in different regions, inter region data transfers cost apply.
- You cannot have more than one VPC peering connection between the same two VPC's at the same time



#### \* What is NACL (Network Access Control List)?

- It is an optional layer of security for your VPC that acts as a firewall for controlling the traffic in & out of one or more subnets

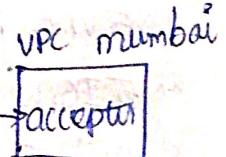
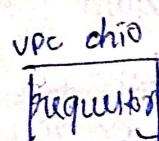


#### \* VPC peering connection? in AWS

VPC → peering connections.

↓  
click on create peering connections.

↓  
give a peering name.



↓  
Select VPC (Requestor).

which shows the CIDR block of particular VPC

↓  
create for Acceptor also

↓  
create peering connection.

#### \* Subnet mask:

It is used to divide the IP address into the 2 parts network IP and host IP

Eg: 192.17.16.0 /24  
 ↓  
 network Host → Subnet mask.

\* ~~What are the steps involved, have you done any VPC peering connections in your company?~~

Yes, we had 2 VPC's in the same region, we wanted to communicate instance from one VPC to instance communicate in the other VPC so we have established a VPC peering connection.

\* All traffic - means anyone can connect to the system.

0.0.0.0/0 → means anyone can access.

foreg: In outbound rules.

If we specify type SSH & destination specific ID means only the specific server can reach the SSH server (to login to instance)

\* Inbound rules → Incoming traffic

Outbound rules → outgoing traffic

~~so to connect ~~what~~~~

NACL's creation:

VPC → Network ACLs

create a NACL

go to subnet association & associate the subnet.

define rules in inbound & outbound rules.

edit inbound rules

add rule

to create security groups

VPC → Security groups.

create new security group.

give basic details → add VPC

specify Inbound and Outbound rules.

click on create security group.

we need to specify the security group while creating the EC2 instance.

while launching EC2 instance  
in a step 6

choose an existing security group

then it will display the created security groups.  
then you can choose there.

Review and launch.

\* Difference between NACL and Security groups?

NACL

1. acts as a firewall for associated subnets
2. controls both inbound and outbound traffic at the ~~instance~~ subnet level
3. supports allow and deny rules
4. applies only to the instances that is associated to it

Security groups

- |   |   |
|---|---|
| - | acts as a firewall for associated Amazon EC2 instances.             |
| - | controls both inbound and outbound traffic at the instance level.   |
| - | supports only allow rules.  |
| - | applies only to the instances in the subnets it is associated with. |

\* what is Subnet? (ex& def)

It is a range of IP address in your VPC, you can launch AWS resources into a specified subnet.

\* what is IGW (Internet Gateway)? (definition ex&)

An IGW is horizontally scaled redundant and highly available VPC component that allows communication b/w your VPC and the internet.

\* what is Security group?

Acts as a virtual firewall for an instances to control inbound and outbound traffic.

- \* what is VPN?
  - It mainly used to establish a secure and private tunnel from your network to a AWS network
- \* what is AWS site to site VPN?
  - enables you to securely connect your on premises network to your network.
- \* Amazon client VPN?
  - enables you to securely connects user to AWS or on previous network.
- \* IQ: Do we have any another way we can connect to the resources in a public subnet?
  - we can setup a VPN server in the public subnet and configure it to connect to resources residing the private subnet.
- \* what is NAT instance?

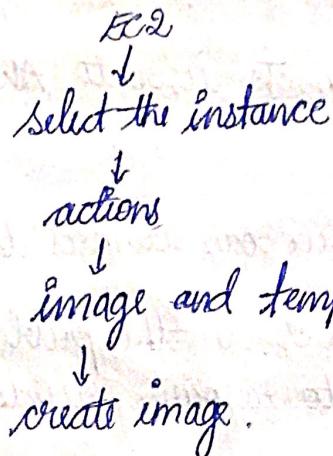
- \* what is snapshot:
  - The process of backing up of EBS volume to S3 bucket is called snapshot.
  - The back up can be stored in a S3 bucket
  - It can be attached to one EC2 at a time
  - EBS volume cannot be shared.
  - with the help of ~~the~~ snapshot we can create a new EBS Volume
  - EBS volume lives beyond the lifecycle of EC2 , it can be attached, detached to any other instances.

## Elastic Cloud Compute:

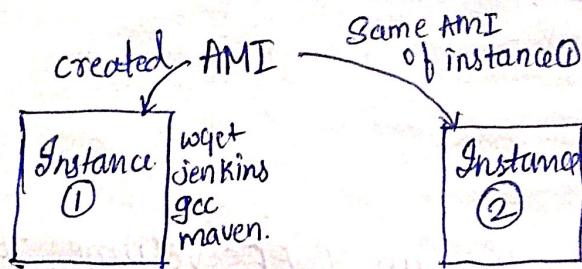
10.01.2022

- \* Amazon Machine Image (AMI) operating system
  - An AMI that contains the software configuration (os, application, server) required to launch your instances.

- \* In Order to create our own AMI?



- \* why AMI is used?



- Suppose if we installed some of the packages to the instance (1) create a AMI for instance (1)
- Then I create another instance (2) so I need not to be install the packages to the instance (2) instead of use AMI used for instance (1) then all the packages which is installed in instance (1) will be updated in instance (2)

- \* IQ: Have you taken an custom AMI?

yes we have taken the custom AMI in order to spin up the EC2 instances.

- \* normally companies will go with Redhat, Centos, AMI's

- \* IQ: which type of instances you are using? / configuration of insta
  - 8 cores of CPC & 16 gigs of RAM - C5.2xlarge
  - 16 cores of CPC & 32 gigs of RAM. - C5.2xlarge

(C5 family)

- 41
- \* ec2 instance needed vpc and subnets to spinup
  - \* can we modify the IAM role?  
yes we can modify if it is already attached to the IAM role
  - \* Basic monitoring will be done 5 min once (metric will be available every 5min).  
(eg) 10.00, 10.10, 10.05
  - \* Detailed monitoring will be done 1 min once  
(metric will be available every 1 min)  
(eg) 10.0, 10.1 min, 10.2 min
- SSD → ~~system storage device~~ solid state drive,  
which is used to boot up the c-drive. / for operating system
- HDD → hard disk drive.  
is used to store the memory (extra storage)
- \* Difference btw SSD, HDD, magnetic?

- \* how do you check the volume in linux?
- \* how to check the ~~unmounted~~ mounted volume in linux?  
mount -l, df -TH
- \* how to check the unmounted volume in linux?  
lsblk
- \* how to login to the EC2-instance using username & password?  
how to enable password authentication in Aws EC2 instance?

→ S.

Step 3 - sudo vim /etc/ssh/sshd\_config

↓  
password authentication changes NO to Yes.

↓  
then permit root login as Yes

Step 4 → Restart the SSH service

Sudo service sshd restart (run command)

Step 5 → run

ssh ec2user@public IP.

\* Have you used the spot instance in our company?

No, we were using on-demand instances depending upon project

→ EC2 instance types?

- EC2 instance types describes the hardware components that an EC2 instance will run on.
  1. Compute power (processor/vCPU)
  2. memory (ram)
  3. Storage Options. (hard drive)
  4. Network performance.

\* what are EC2 instance types?

1. General purpose
2. Compute optimized
3. memory optimized
4. Accelerated Computing
5. storage optimised.

\* what are EC2 purchase options?

1. on-Demand
2. Reserved instances (RI).
3. spot instances
4. Dedicated Hosts.

### 1. On Demand:

- On Demand lets you to choose any instance type and can terminate on any time.
- It is the most expensive purchasing option.
- It is the most flexible purchasing option.
- You only charged when instance is running.

### 2. Reserved Instance (RI)

- Reserved purchasing allows you to purchase an instance for a reserved time period one or more years.
- This allows significant price discount.
- Once you buy a reserved instance, you own it for a selected time period and are responsible for the entire price.

### 3. Spot Instance:

- Spot instance is the way you to "bid" an instance.
- Spot prices fluctuates based on supply and demand ~~in spot~~  
based on a market.
- An instance will be automatically terminated when the spot price is higher than the bid price.
- We will be charged per second (Based on Conditions).

### 4. Dedicated Hosts?

- A dedicated physical machine that you have full control over.
- This can help save money ~~on~~ on license fees.

what is VPC?

\* what are the components of VPC?

- 1. CIDR block
- 2. Subnets
- 3. Routable
- 4. NAT Gateway
- 5. Internet gateway
- 6. Security group.
- 7. Elastic IP address
- 8. IPv4 and IPv6 address blocks.

\* what do you know about VPC peering?

- VPC peering is a network connection b/w 2 VPC's & enables you to route traffic b/w them using private IP address.
- Data can be transferred across these resources are more secure.
- VPC peering allows you to deploy cloud resources in a virtual network that you have defined.

\* what is statefull and stateless firewall?

- statefull:

\* Does transitive peering is allowed in VPC?

- VPC peering does not allow transitive peering connection.
- VPC peering connections that are established entirely within your own AWS account.

\* How are private instances access over the internet?

By using NAT service for your resources in a private Subnet to access the internet.

\* what is an elastic IP?

- An Elastic IP address is a reserved public IP address that can assign to any EC2 instance in a particular region until you choose to release it.

• The elastic IP address remains in place through events that normally cause the address to change, such as stopping and restarting the instance.

\* what is VPC endpoint?

- VPC enables you to securely connect the your VPC to another service
- There are 3 types of VPC endpoints
  1. Interface endpoints
  2. Gateway load balancer endpoints
  3. Gateway endpoints.

\* what is the diff b/w public subnet & private subnet?

1. public subnet : having direct access to the Internet Connection.
2. private subnet : having no direct access to the internet.

\* Difference b/w NAT Gateway and IGW?

NAT Gateway

IGW.

1. allows instances with no public IP's to access over the internet.
2. allows instances with public IP's to access over the internet.

\* Difference b/w NACL and the Security group? (page 38).

\* how many subnets can you have with VPC?

- you can create 200 subnets in VPC.

- If we need to create more please submit a case at the support center.

\* How do you monitor your VPC?

flow logs captures the information about the IP in & out traffic network interface to your VPC.

\* Can I assign multiple IP address to an instance?

- yes you can assign one or more secondary private IP address to an EC2 instance in an Amazon VPC.

- The number of secondary private IP address depends on the instance type.

\* Can an ec2 instance with VPC in one region access the ec2 instance residing in VPC other region?

- yes by using VPC peering, Public IP, NAT we can communicate with each other.

\* In which subnet you will launch the database?

In the private subnet we should launch the database.

\* what is EC2 instance?

It is a virtual server in an Amazon EC2 in the elastic cloud for running applications in Amazon Web Service

\* Difference b/w terminating and stopping an instance?

\* what is EC2 root device Volume used for?

when an EC2 instance is launched from the AMI, the root device volume contains the image used to boot the instance mainly the operating system, all configured services, applications.

\* how do you persist root device volume?

The root device volume will be backed up by Amazon EBS by default, it will get deleted when the instance gets terminated.

\* how to migrate an instance to another availability zone?

- shutdown / stop the instance
- click on instance → create image to make an AMI from instance
- Go to AMI page → click on new AMI and select launch instance
- In the new instance settings, choose a specific availability zone

\* which database are supported in AWS Secret?

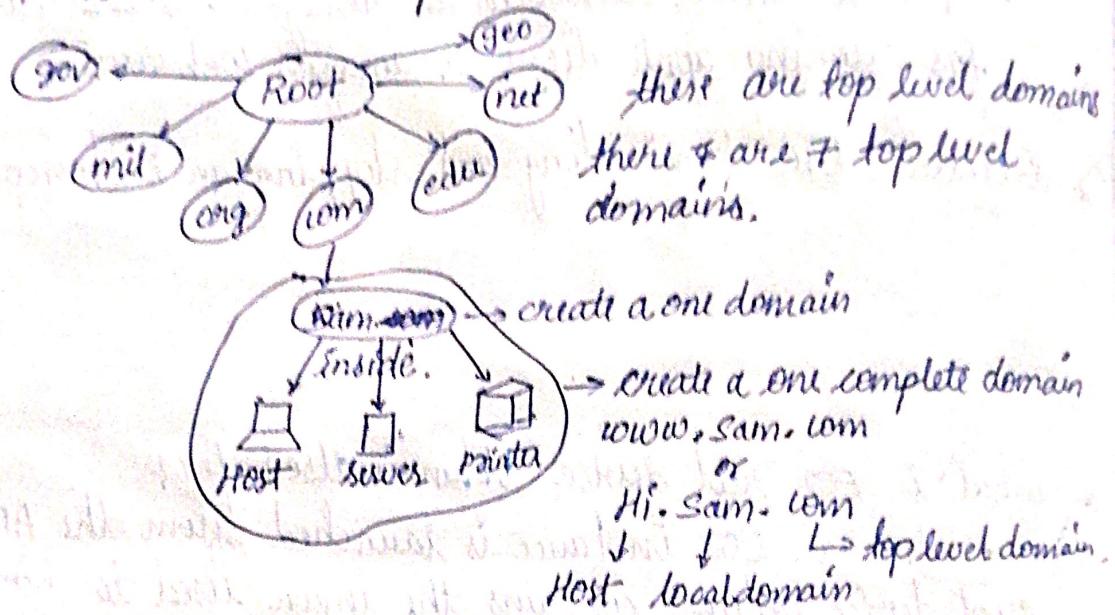
AWS Secret manager supports SSL Connections. When creating database secret for Amazon RDS MySQL, MariaDB, PostgreSQL, MongoDB.

\* what is target Group in load balancer?

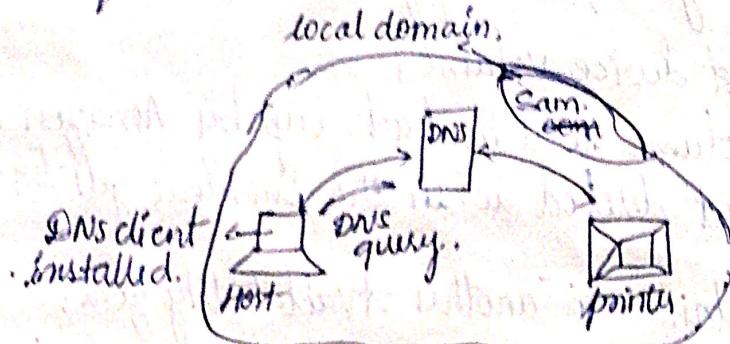
## DNS Services

### (Domain Name Service)

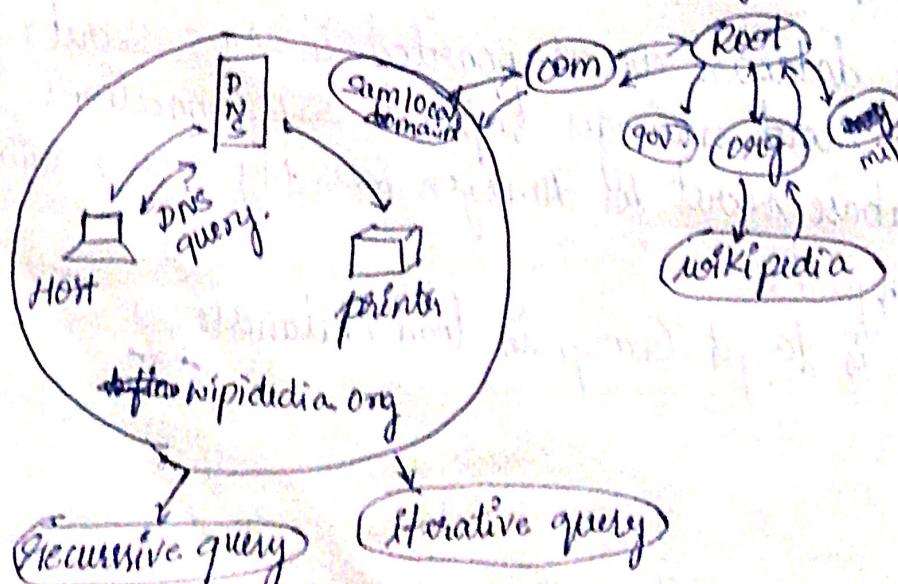
DNS which divides into the multiple domains, the Root will be the main domain, there are 13 root domain from (A-N) around the globe, Root which has a parent.



\* Concept of how DNS works:



(for eg: if i need to give a print to the machine the query is sent to the DNS server and the DNS will give the server (printer) ip address to the host machine bcz it will be in the same <sup>local</sup> domain & ip address) .  
suppose if i need to access the other domain .org.



— when the host machine searches for .org domain the query is sent to the local DNS (local DNS). the local DNS will search for the .org in the local domain and replies that he has not found the .org domain, where the DNS query is of 2 type

1. Recursive query.
2. Iterative query.

Recursive query once it recursively ask the DNS to the .org domain and DNS says its not found. (But how also we need that domain) then comes the iterative query this ask DNS to get a .org domain, then the DNS will ask the local domain then local asks for .com (toplevel domain) if it is not found in .com also it will ask for a parent (Root) then root will search the children (whether the ~~.org~~ .org domain is there or not) if it ~~is~~ is confirm that there is a .org then looks for wikipedia inside org. and then sends the information to the root  $\rightarrow$  .com  $\rightarrow$  local domain  $\rightarrow$  DNS  $\rightarrow$  host machine.

If ~~is~~ another host need to access .org the address will be stored in the local cache. so that host can use the ipaddress which is there in cache for further use.

10/1/2022

\* what do you mean by Snapshot of an instance

\* Elastic load Balancer? (simpli distribute the loads across the multiple EC2 instan)

- A load balancer distributes incoming application traffic across multiple EC2 instances in a multiple availability zones.
- This increases the fault tolerance of your applications.
- ELB detects the unhealthy instances and routes traffic only to the healthy instances.

\* Types of load balancers:

1. Application load balancers.
2. network load balancers
3. classic load balancers
4. Gateway load balancers.

1. Application load balancers.

- used mainly for web applications running http and https protocol
- Operates at the request level.

2. Network load balancers:

- ultra high performance at very low latency
- can handle millions of requests.
- Operates at connection level, routing traffic to targets within VPC

3. Classic load balancers:

- Used for applications that were building in existing EC2 classic env
- operates both at Connection and request level.

\* differences b/w http and https?

50

### HTTP

1. HTTP stands for hypertext Transfer protocol
2. HTTP works at application layer
3. The default port number is 80 for communication
4. No encryption is present in HTTP website

### HTTPS

- HTTPS stands for hyper text Transfer protocol secure.
- HTTP works at the transport layer
- default port number is 443 for communication.
- Both encryption and decryption exists on HTTPS website.

\* Difference b/w Application load balancers and Network load balancers and classic load balancers?

### Application

### Network

### Classic

- |  |   |   |
|--|---|---|
| 1. It supports HTTP /<br>HTTPS (internet)                                | - It supports TCP /<br>UDP / TLS.                     | - It supports on HTTP /<br>HTTPS / TCP / TLS.                       |
| 2. Operates on request<br>level  | - operates on the<br>connection level                 | - It operates both on<br>request level and the<br>connection level. |
| 3. provides load bal-<br>ance to multiple<br>ports on an instance        | - !! -  | - !! -  |
| 4. It operates on layer 7  | if it operates on layer 4                             | it operates on layer 7<br>and layer 4.                              |
| 5. Supports IP addresses,<br>lambda functions &<br>containers as targets | - supports UDP and<br>static IP address as<br>targets | - Use an existing<br>applications running<br>in ec2 instances.      |

\* what is Certificate in ELB in AWS?

load balance uses the certificate to terminate the connection and then decrypt request from clients before sending them to the instance

\* what is cert?

\* Difference b/w Snapshot of an instance and AMI of an instance?

Snapshot

AMI

(51)

1. It is a backup of an ~~entire~~ - It is a backup of an entire specific EBS volume EC2 instance.

\* how do you create application load balance? (Explain Steps)

select application load balancer

select internet facing or private

we need to select or map the subnets

we need to configure the security group for load balancer

we select http or https protocol also we can create the required target group

modify the certificates

we need to request certs at the organisation level once certs were available we were configuring those certs.

(12)

\* have you created the certificate in your company?

No at Organisation level they were providing certs

we need to request certs at the Organisation level once certs are available we were creating/configuring those certs.

(13)

\* Do you have experience to the network load balancer?

As of now i have not worked with NLB but the overall concept remains same as ALB

### Auto Scaling

\* what is auto scaling?

Scaling up or scaling down of an instances (Simple def).

\* Scaleup - creating the instance new

\* scaledown - ~~creating~~ deleting the instance.

## \* Auto Scaling (actual definition):

Auto Scaling monitors your application and automatically adjust the capacity to maintain steady, predictable performance at low possible cost.

minimum size - atleast 1 instance.

Desired capacity - minimum 2 should be

maximum size - can scale up to how many instances u need.

IQ \* have you created a autoscaling groups?

choose launch template or configuration.

choose instance launch options.

Configure advance options

Configure group size and scaling policies

Add notifications

Add tags

Review.

## \* Difference b/w load balances and Autoscaling?

load balances

Autoscaling.

- LB distributes the traffic among the instances
- Autoscaling which scales up & down the instances according to traffic

## \* what is launch template?

Launch template is a new capability that enables a new way to template your launch requests.

## \* what is vertical scaling?

Vertical scaling adding more resources to your servers as on demand

(53)

\* what is horizontal scaling?

horizontal scaling is one that can increase capacity by adding more computers to the system.

\* Difference between horizontal and vertical scaling

Vertical Scaling

Horizontal Scaling.

- 1. adding more resources to your server as on demand
  - Increasing capacity by adding more computer to the system.
- 2. Also known as scaling up
  - Also known as scaling out
  - Cost effective.
- 3. Not cost-effective
  - Used in distributed systems.
- 4. Used in visualization

## AWS Secrets

\* what is AWS Secrets?

You can store database credentials or any other type of secret.

12/01/2022

## S3 (Simple Storage Service).

51

\* what is Amazon S3?

It is a simple web service interface, that you can use to store data and can retrieve any amount of data, at any time and from anywhere on the web.

\* Static IP address?

- A static IP address is a unique number assigned to each computer on a network.
- The IP address changes frequently, which provides customer and ISP's cost savings.

\* Difference b/w static and elastic IP address?

static IP address

Elastic IP address

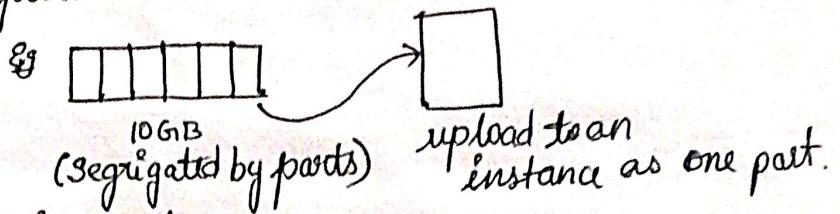
- here IP address changes frequently when start/stop
- elastic IP remains linked to instance after the start/stop

\* what is Single Operation upload? / single part upload?

- It is a traditional upload where you will upload the object in one part.
- upload the file upto 5GB.

\* what is Upload object in parts / multiple upload?

- multiple upload allows you to upload a single object as a set of parts



- large file size upto 5TB.

\* Rules for bucket naming?

1. name must be b/w 3 to 63 characters long.
2. contains only lowercase letters, dots, numbers & hyphens.
3. name must begin and end with a letter or name.
4. name must not be formatted as IP address.
5. name cant begin with xn--

- limitations of S3 buckets?  
• only 100 buckets can be created per account  
• can hold unlimited objects.

\* what is Amazon S3 Glacier?

- It is a secure durable and extremely low cost Amazon S3 storage class for data archiving and long term backup.
- S3 glacier enables customer to offload the administrative burdens of operating and scaling storage to AWS.

\* Difference between Amazon S3 and S3 Glacier?

S3.

S3 Glacier

1. S3 is a fast storage solution - Glacier is used for archiving solutions

2. S3 is used to host static web content - In glacier we cannot host the web content.

3. In S3 we create buckets - while in glacier we create archives.

4. You can store virtually unlimited amount of data in both of them.

\* Difference between Standard and Glacier?

\* what is S3 life cycle policy?

- is a set of rules that automate the migration of the object storage class to different storage class.
- By default the lifecycle policy are disabled for a bucket.

\* what is Versioning of a bucket?

- means keeping multiple variants of object in a same bucket.
- Versioning enables buckets can help you recover objects from accidental deletion or overweight.

- \* what is encryption of a bucket?
  - All objects are encrypted when they are stored in a bucket.
  - the objects are encrypted using server side encryption either with ~~SSL~~ S3 or AWS-KMS.
- \* what is bucket naming convention?

(15)

- \* have you configured S3 life cycle in your Organisation?

Since there is no requirement for us, but I know how to configure this one.

- \* Types of encryption for S3?

- a. serve side encryption.
- b. client side encryption.

↳ 1. using KMS

2. client side master key.

### Route 53:

- \* what is Amazon Route 53?

it is highly available and scalable DNS web service where we can point IP address to domain name or point host name to another host name.

- \* what is A record?

Maps IP address to domain name.

- \* what is CNAME record?

Maps hostname to hostname

- \* Have you mapped the domain name with IP address?

yes we mapped the domain name with IP address with the help of A-record.

\* why TTL is set?  
In order to reduce the load on Route 53

\* High TTL

- less traffic on DNS
- possibly on outdated records.

\* less TTL

- more traffic on DNS
- Records are outdated for less time
- easy to change records.

\* Alias Record?

points a host name to AWS resource.

\* Latency Routing policy?

when you have resources in multiple AWS ~~regions~~ regions, and you want to route traffic to the region that provides the best latency

\* Weighted Route policy?

use to route traffic to multiple ~~resources~~ resources in proportions that you specify.

## LAMBDA

\* what is Amazon LAMBDA?

- Lambda lets you to run the code without provisioning or managing services, you pay only for compute time you consume.
- just upload your code, and Lambda take care of everything required to run and scale your code with high availability.

\* AWS Lambda Languages.

Node JS / python, python3, groovy, csharp, scala and G10.

## \* How does AWS Lambda work?

- When a lambda function runs it in its own container, when a function is created lambda packages into a ~~new~~ new container and then executes a new container on a multi-tenant clusters of machine managed by AWS.
- Before function starts running, each function is allocated with separate RAM and CPU capacity.
- Once the function finishes running, the RAM allocated at the beginning is multiplied with the amount of time the function spent running.
- Then the customer get charged based on allocated memory and amount of run time.

## \* What are the most common use cases for AWS Lambda?

1. individual tasks runs for a short time.
2. each task is generally a self contained.
3. there is no large diff b/w lowest & highest workload of the appn

## \* Benefits of lambda function?

1. pay per use
2. fully managed infrastructure
3. Automatic Scaling.

## Cognito

(58)

what is AWS Cognito?

It mainly provides authentication, authorisation and user management for your applications.

services web/mobile.

authentication → it is like logging to our particular account with your credentials

authorisation → like we need to access an backend services like database and API's in that case user need to authorize.

\* 2 components in cognito:

1. user pool
2. identity pool

1. user pool:

These are user directories that provides sign-in and sign-up options for your app users.

2. identity pool:

Identity pool provides AWS credentials to your users to access the AWS services.