🡪For using CLI you have to create a user.

🡪You can use root, but it is not recommended to use root from CLI.

🡪So, you can login via SSH from CLI.

* EC2

🡪It is a service for creating an instance.

1. First select an AMI.
2. Select an instance type.

🡪Here you have to use how much ram CPU you need.

🡪Use t2.micro, it is free

1. Give instance details.

🡪number of instance

🡪Choose subnet. ap-south-1a

1. Choose how much storage you want to give.

🡪This is from EBS volume.

1. Add tag.
2. Add security Group

🡪It is like a firewall.

🡪For SSH connection make SSH-22port enable

🡪For webserver http-80 port enable.

1. Review and attach a key or generate a new key.

🡪This key is used for SSH connection.

🡪If you are creating new key then make sure you download csv file for it.

🡪You can think it is a password you attach to your instance.

🡪So, while connecting threw SSH you have to give this password.

1. Launch Instance.

VPC (virtual private computing)

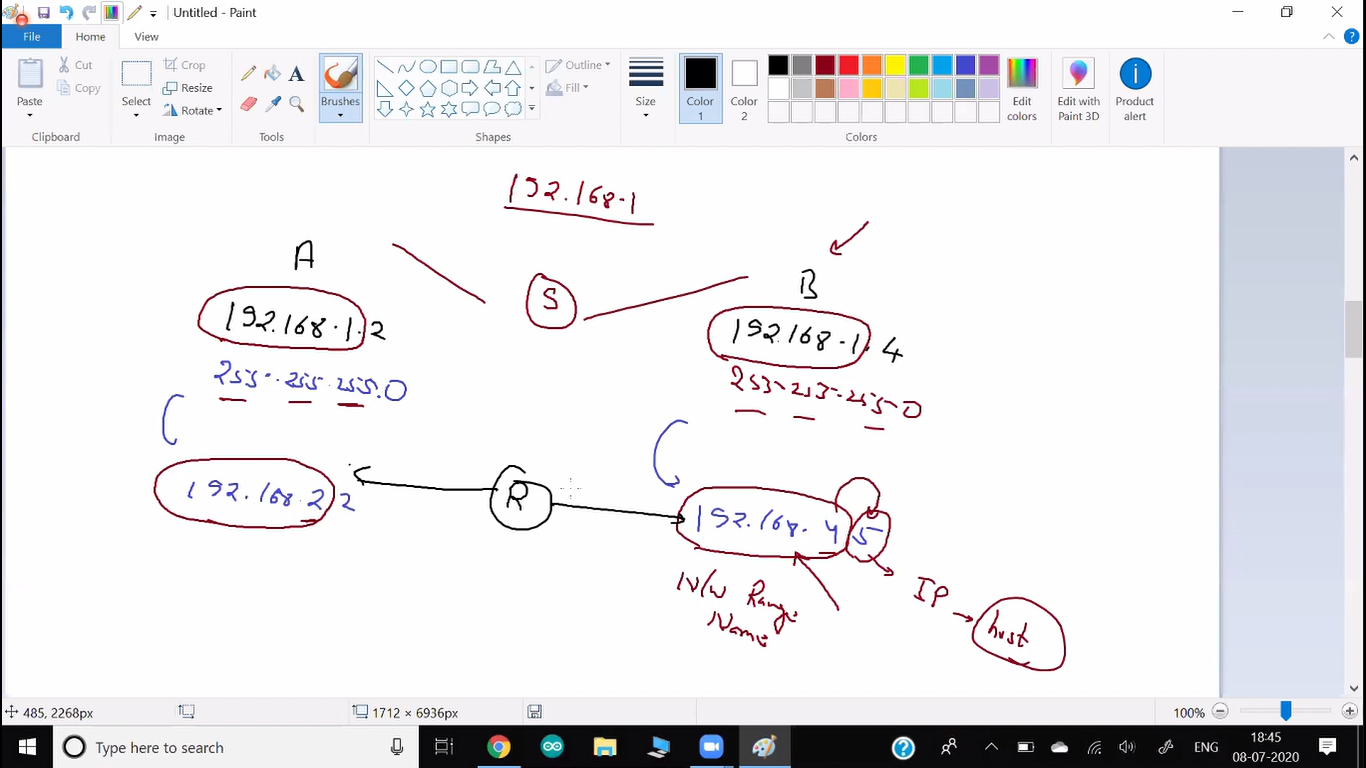
🡪If you want multiple pods-laptop can have network connectivity between each other, we require these 6 things.

1. Physical connectivity between them (wire or wireless).
2. On this particular wireless end we require network card (NIC).
   1. Aws – ENI
   2. OpenStack - VNIC (Virtual NIC card)
3. One unique IP address both side (IPv4).

🡪Every IP address must have netmask.

1. If both devices belong to same network, we require switch.

* If both devices belong to different network, we require switch.



1. Public IP ----connect to---> Public IP

Private IP ---connect to---> Private IP

1. Routing table

Your device ask DHCP server and DHCP server give dynamic IP.

🡪For static IP

1. Aws – EIP
2. OpenStack – Floating IP

🡪Instead of physical switch we can also use software.

1. We can create switch and router also using this software.
2. Here switch known as L-2 bridge.
3. router known as L-3 bridge.
4. Some software work as both switch and router, it is known as layer 3 switch (Eg, hotspot).

🡺Internet Gateway provides SNAT, DNAT both.

🡺NAT gateway provides DNAT only.

🡺All the OS-device should have routing table.

🡪By using routing table, you can tell your system who is your gateway.

🡪route PRINT -n (windows)

🡪router has two IP.

🡪Here you can see your private IP of router.

🡪In linux route -n

🡪When ever you go to cloud for IAAS, by default they provide NAAS.

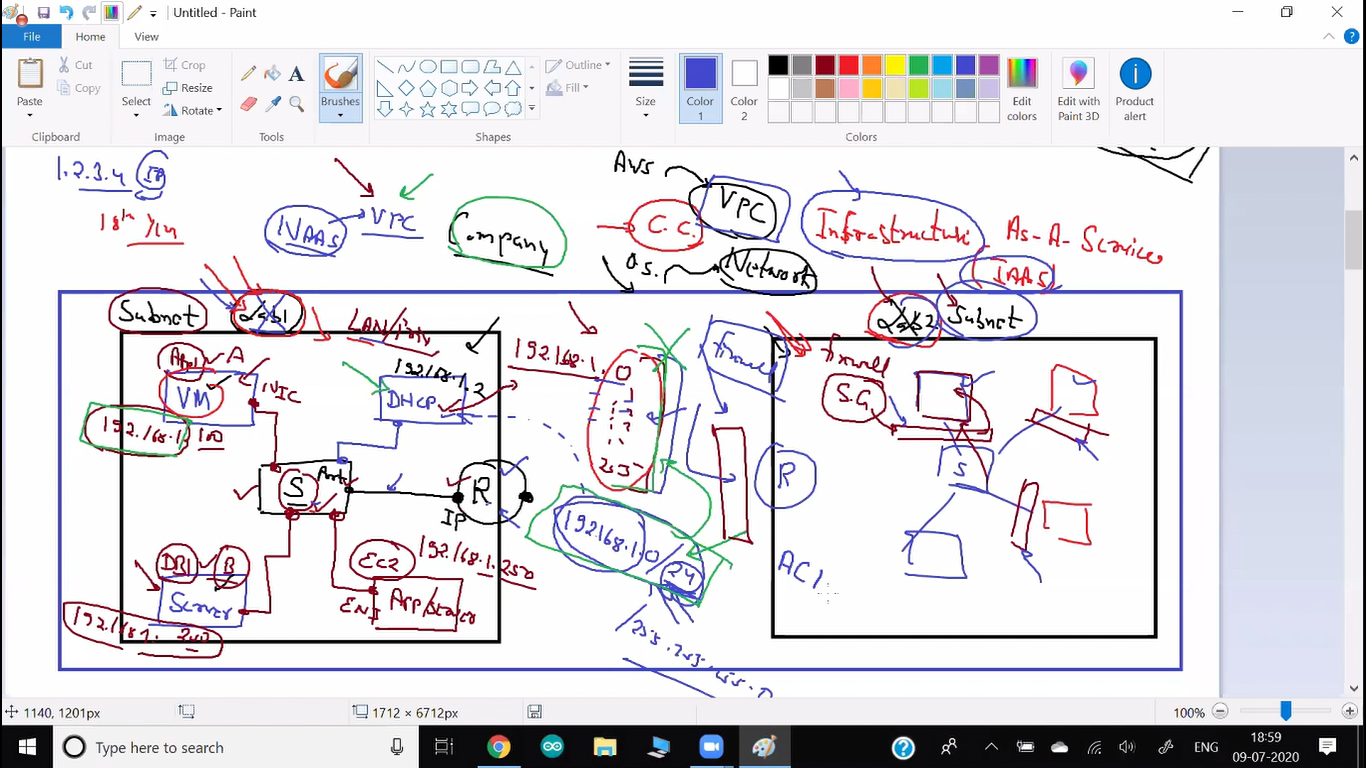
🡪VPC provides you NAT service.

🡪One VPC has multiple subnets.

🡪You can think VPC provides you one border to isolate you from other company, other VPC. Inside their your all services are running.

🡪you can think subnet as a LAB or LAN.

🡪amazon construct all the things for you (switch-router).



🡪Anybody come from outside world and go inside Ec2 it is known as Inbound traffic.

🡪It is also known as ingress.

🡪Ec2 instance want to go to other instance or outside world it is known as outbound.

🡪It is also known as Egress.

🡪By default in aws and OpenStack outbound is allowed and inbound is not allowed.

🡪We can also set that, if Ec2 instance from this SG comes then allow them (Inbound rule).

🡺Create secured Wordpress-mysql architecture.

🡪create a new VPC.

🡪Create two subnet.

🡪Create routing table and internet gateway.

🡪One subnet can access to outside world.

🡪Second subnet can not get outside world

🡪Create a SG for wordpress which allows ssh, ping, httpd (Subnet-1).

🡪create a SG for mysql allow mysql-access from wp-SG only (subnet-2).

🡪Here sometimes we have to update our software. But we havenot allowed ssh port. So we can not go there and launch instance.

🡪For this create one bastion OS in subnet-1 allow ssh.

🡪This OS is in same VPC.

🡪So you can connect to this os using ssh and all are in same VPC.

🡪SO you can connect mysql using this os.

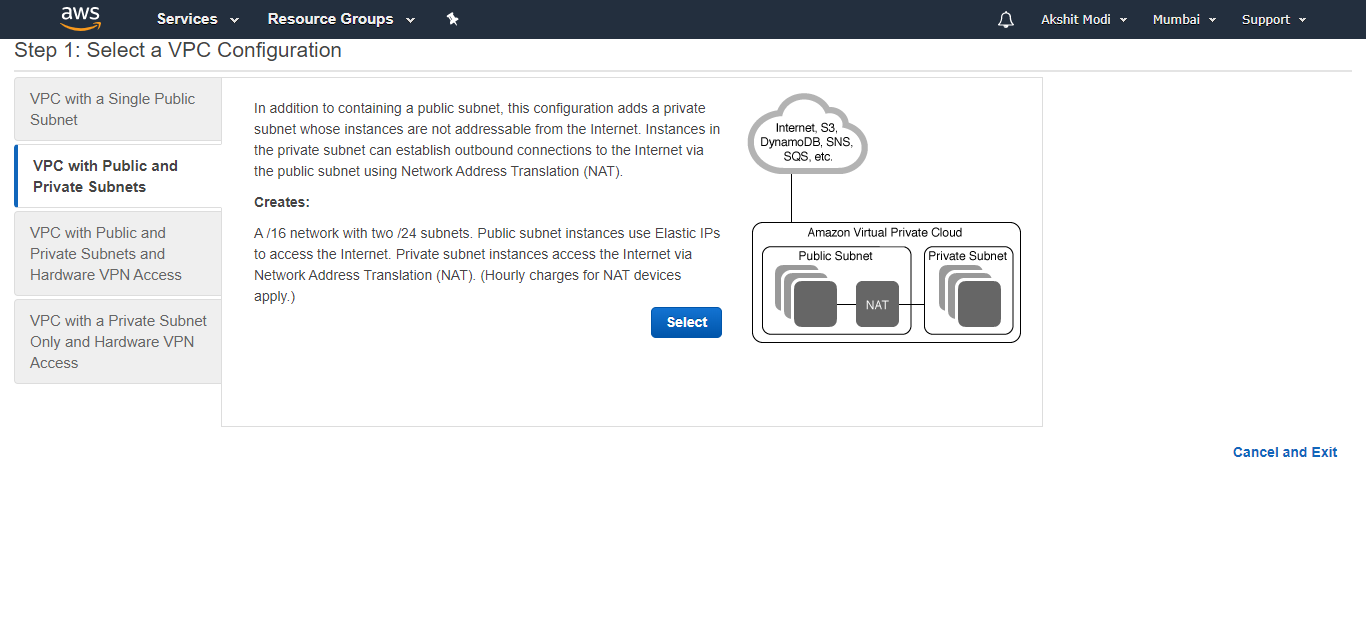
🡪For this you have to add ssh only from bastion-SG inside mysql.

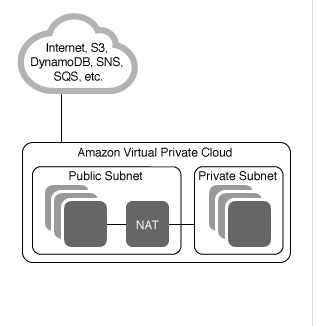
🡪But here your system can not go outside world.

🡪For this you have to use NAT gateway.

🡪create this NAT gateway in public subnet. (Subnet-1)

🡪update subnet -2 with this nat gateway.





🡪This security group is by default outside instance. You can also make SG at subnet. It is known as NACL (Network Access Controller).

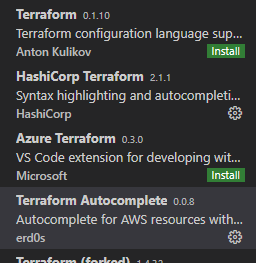
🡪Here there is also option for DENY something.

🡪Here it goes one by one. If first condition (rule) satisfy then it does not go for second rule.

🡪Public IP is allocated to the internet Gateway.

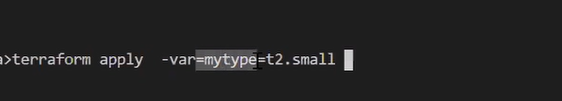
Visual Studio Code  
🡪plugins:

1. Hashicorp terraform
2. Terraform Autocomplete



🡪It is good practice to do dry run before actual applying code.  
🡪Terraform plan  
🡪It will go to code and check what is the final impact on your code.

🡪Terraform maintain the current state inside terraform.tfstate file.  
🡪This file stored in your local HD.  
🡪You can also store this in remote location.  
🡪whenever you again use terraform apply, they go to aws and get current information and then check with file.  
🡪use terraform refresh before running old file again.  
🡪This will update your local file.



🡪Terraform also have repository.

Commands

* Aws help
* aws ec2 describe-instances --query Reservations[\*].Instances[0].Tags
* aws ec2 describe-availability-zones
* aws ec2 describe-instances