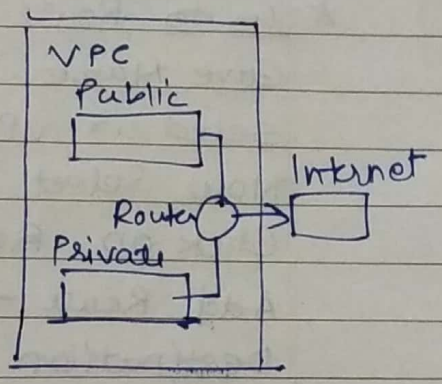
1st Feb.

AWS.

Cloud - Class of network ~~of internet~~.
~~AZ. Zone~~



★ Create VPC:

Login and search VPC
Then select VPC Service.
Click on your VPC
Then click on Create VPC
Provide name of VPC
Create IPV4 CIDR → 10.0.0.0/16 → Create VPC.
Go to Subnets:

★ Create Subnet →

VPC Select → Create Subnet.

Create 1st Subnet
With name public
Then provide Availability Zone → Asia Pacific (Mum bai/ap south-1a)
IPv4 CIDR → 10.0.0.0/24.
Add new Subnet
With name private
Availability Zone → Same.
IPV4 CIDR → 10.0.1.0/24.
Create Subnets

★ Create Gateway & Attach to VPC.

Click on Internet Gateway
Click on New Gateway.
Give name → Create Internet Gateway.
Select Gateway from dashboard Right click on it and click on Attach to VPC.

Select your VPC and → Attach Internet Gateway.

* Go to Route Table & Create a New Route Table:
Give Name.
Seled ur VPC. → Create Route Table.
Now Select your Route Table
Click on Routes → Click Edit Routes
Add Route →.
Destination → Select Wild Card I* 0.0.0.6/0.
Target → Select Internet Gateway then select ur Gateway.
Save changes.

* Associate Public Subnet to Route.
Go to Route Table
Selected Route → Subnet Associations
Edit Subnet Associations.
Select Public Subnet → Save
(Now ur Public Subnet can access Internet)

* Search EC2.
Create two instances
↳ 1st Public
↳ 2nd Private
Select EC2
Instances → Launch Instance
Provide Name
Select OS Image Ex: Ubuntu.
Create a Key Pair for ssH login
Network Setting → click Edit
Select VPC → Select Public Subnet
Enable - Auto assign public IP (Only if using public subnet)

Check if internet Runs ping google.com

apt install docker.io containerd.

fire.
~~Fair~~ Wall Rules:
Select storage → Launch Instance.

* Same for Private Instance.
&
* Select EC2 Instance & Connect.

Open Terminal.
chmod 400 dai.pem

ssh -i dai.pem ubuntu@ x.x.x.x ← IP Address of ur Instance.

Select → Right Click → Terminate After using.
Gateway Detached.
VPC → Delete VPC.

apt install openssh-client (.pem) ← key

- Configure S3:
Search S3 and select it.
Create bucket → Bucket Name.
Uncheck Block all public access. → Create Bucket
We can uploed objects

Go to permission
→ click on ACL Edit
Buck Owner can Read write list
Every Read.
S3 log can Read write List.

Identity & Access Management (IAM)

Account → Security Credentials setting → IAM Dashboard

Click on User → Add New User. → Give User Name
Enable console Access.
Give Password. → Next.
Permissions.
Add User to group. → Next.
Select the user from user list and go to Security credentials.
Access Key Area → Create a New Access Key → CLI → Next.
Create Access Key.

Install AWS
apt install awscli
aws configure.
AWS Access key ID:
AWS Secret Accesskey:
Default region name: (Region given)
Default out format: json

Configurations are saved in home directory in .aws
cd .aws/
ls
cat config. (output Region)
cat credentials. (API keys)