

ASSIGNMENT 1

Configure and launch EC2 public instance in AWS

1. Login to your AWS console and choose the region allocated for you from the dropdown say : Asia Pacific (Mumbai)
2. Search VPC service Create a custom VPC by selecting VPC from the services list and click on 'create VPC'
3. Select the option "VPC only" Provide any VPC tag name and in the field of IPv4 CIDR provide 10.0.0.0/16
A: 1,2,3

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

☒ VPC only ☐ VPC and more

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.

IPv4 CIDR block [Info](#)
☒ IPv4 CIDR manual input
☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)
☒ No IPv6 CIDR block
☐ IPAM-allocated IPv6 CIDR block
☐ Amazon-provided IPv6 CIDR block
☐ IPv6 CIDR owned by me

Tenancy [Info](#)

4. Your custom VPC will be created and displayed as below

A:

You successfully created vpc-0358873cfff60846f

VPC > Your VPCs > vpc-0358873cfff60846f

vpc-0358873cfff60846f Actions

Details [Info](#)

VPC ID vpc-0358873cfff60846f	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-0a7420be0876c648d	Main route table rtb-040114191b50c789c	Main network ACL acl-082275576b4df71b0
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 628132916033	

[Resource map](#) [New](#) | [CIDRs](#) | [Flow logs](#) | [Tags](#) | [Integrations](#)

Resource map [Info](#)

5. Search and navigate to 'Subnet' module from the services and click on 'create subnet'

6. Provide the Subnet name (ex: public subnet) select the VPC that you have created Previously and navigate to the subnet settings, now select an availability zone as per your region. Provide IPv4 CIDR block (10.0.1.0/24) . Click on Create Subnet

A:

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
public subnet
The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
Asia Pacific (Mumbai) / ap-south-1a

IPv4 VPC CIDR block [Info](#)
Choose the IPv4 VPC CIDR block to create a subnet in.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.0.0/24 256 IPs

Tags - optional
Key Value - optional

7. Search and navigate to Route Table feature and click on 'create Route Table'

8. Provide the name for the Route table ex: public_rt and select the VPC that you have created and click on 'Create Route table'

9. Route table will be created and displayed as below

A: 7 8 9

Route table rtb-0421bd628a2d39c51 | public_rt was created successfully.

VPC > Route tables > rtb-0421bd628a2d39c51

rtb-0421bd628a2d39c51 / public_rt

Details [Info](#)

Route table ID rtb-0421bd628a2d39c51	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-0358873cff60846f	Owner ID 628132916033		

Routes Subnet associations Edge associations Route propagation Tags

Routes (1)

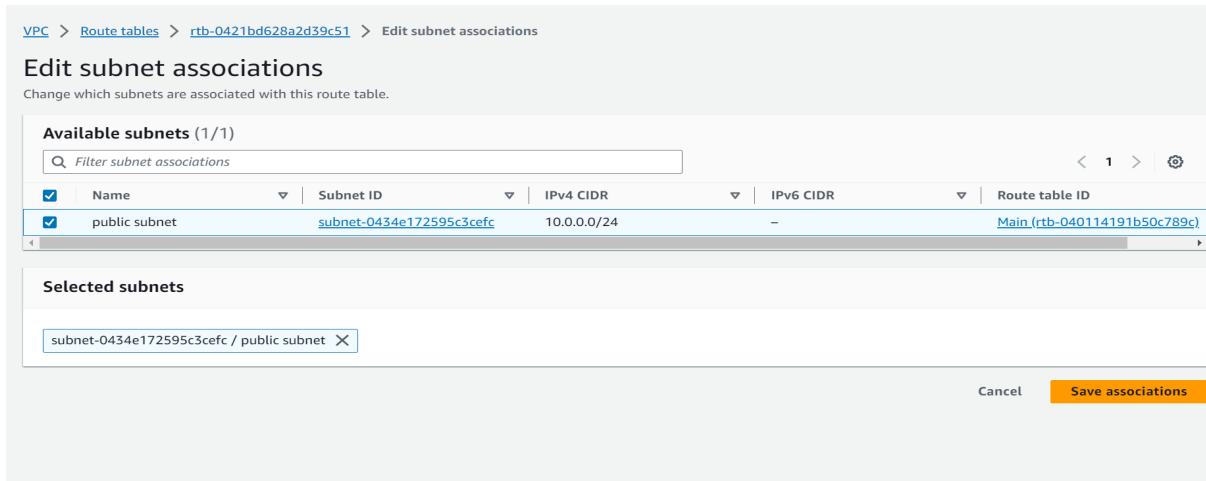
Filter routes

Destination	Target	Status	Propagated
-------------	--------	--------	------------

10. Now Click on subnet associations by selecting the Route Table that you have created previously

11. Now click on “Edit subnet association” and make a check on the subnet that you have created and click on save changes (Note : In your case select the subnet that you have created)

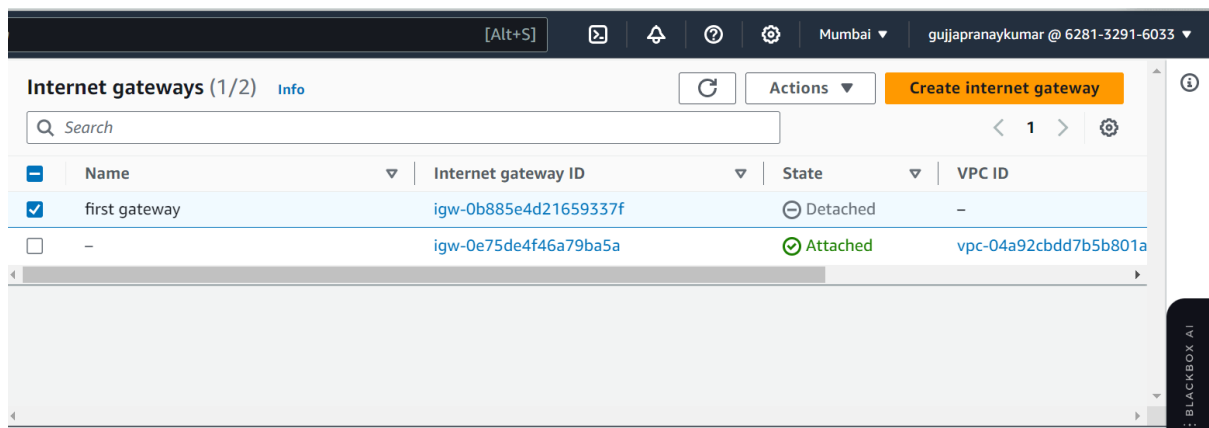
A: 10 11



12. Search and Navigate to the Internet Gateway and click on ‘Create internet gateway’

13. Provide any name to the Internet gateway and click on ‘Create internet gateway’ to get created . Initially the Internet Gateway will be in a detached state.

A:12 13



14. Now Select the Internet Gateway you have created and click on Actions and select ‘Attach to VPC’ select the VPC and click on ‘Attach Internet gateway’. Now the Internet gateway state changes to ‘attached’

A:



15. Navigate to Routtable , click on the route table that you have created and then click on Routes

16. Now click on Edit Routes and then Click on Add Route . Provide 0.0.0.0/0 in the Destination and in the Target select the Internet Gateway and select the IG that you have created previously. Click on Save changes.

A:

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway igw-0b885e4d21659337f	-	No

Buttons: Add route, Cancel, Preview, Save changes

16. Search and Navigate to ‘Instances’ option and click on launch instance

17. Now, you need to select the Amazon Machine image (AMI) from the from the list , select the default

18. Now you need to choose the instance type , you can proceed with the default instance type that is being selected by clicking Next: Configure Instance Details

19. In the ‘configuration instance’ settings select your VPC from the network dropdown, select your public subnet that you have created , enable Auto-assign public ip, select “Use subnet setting (Ip name)” from the Hostname type and leave all other as default, Click on “Next : Add storage”

A:

VPC - required Info
vpc-0358873cfff60846f
10.0.0.0/16

Subnet Info
subnet-0434e172595c3cefc public subnet
VPC: vpc-0358873cfff60846f Owner: 628132916033
Availability Zone: ap-south-1a IP addresses available: 251 CIDR: 10.0.0.0/24

Auto-assign public IP Info
Enable

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group ☐ Select existing security group

Security group name - required
launch-wizard-2

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-:/()#,@!+=&;[]!\$*

Description - required Info
launch-wizard-2 created 2023-11-11T05:20:19.157Z

20. In storage default options are selected , you can click “Next : Add Tags”.
provide the Name and Value as below, (it is your choice to provide any values)
and click on ‘configure security groups’
A:

▼ Name and tags [Info](#)

Key [Info](#)

Value [Info](#)

Resource types [Info](#)

Q Name X

Q first instance X

Select resource t... ▼

Remove

Add new tag

Instances X

You can add up to 49 more tags.

20. Now navigate to ‘Configure security group’ settings and add all the following rules which are marked and click “review & launch”
(Note for SSH & ICMP-Ipv4 select source dropdown as My ip)
A:

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 152.58.233.97/32)

Remove

Type [Info](#)

Protocol [Info](#)

Port range [Info](#)

ssh ▼

TCP

22

Source type [Info](#)

Name [Info](#)

Description - optional [Info](#)

My IP ▼

Q Add CIDR, prefix list or security g 152.58.233.97/32 X

e.g. SSH for admin desktop

▼ Security group rule 2 (TCP, 80, 0.0.0.0/0)

Remove

Type [Info](#)

Protocol [Info](#)

Port range [Info](#)

HTTP ▼

TCP

80

Source type [Info](#)

Source [Info](#)

Description - optional [Info](#)

Custom ▼

Q Add CIDR, prefix list or security g 0.0.0.0/0 X

e.g. SSH for admin desktop

▼ Security group rule 3 (TCP, 3306, 10.0.0.0/16)

Remove

Type [Info](#)

Protocol [Info](#)

Port range [Info](#)

MYSQL/Aurora ▼

TCP

3306

Source type [Info](#)

Source [Info](#)

Description - optional [Info](#)

Custom ▼

Q Add CIDR, prefix list or security g 10.0.0.0/16 X

e.g. SSH for admin desktop

▼ Security group rule 4 (ICMP, All, 152.58.233.97/32)

Remove

Type [Info](#)

Protocol [Info](#)

Port range [Info](#)

All ICMP - IPv4 ▼

ICMP

All

Source type [Info](#)

Name [Info](#)

Description - optional [Info](#)

My IP ▼

Q Add CIDR, prefix list or security g 152.58.233.97/32 X

e.g. SSH for admin desktop

(Note: copy the keypair to any of your linux machine to connect the EC2 instance)

Create key pair

×

Key pair name

Key pairs allow you to connect to your instance securely.

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ RSA
RSA encrypted private and public key pair

☐ ED25519
ED25519 encrypted private and public key pair

Private key file format

☒ .pem
For use with OpenSSH

☐ .ppk
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn](#)

Cancel

Create key pair

23. Now search and navigate to Instances you will be seeing the instance that is up and running state

25. Click “connect” to launch the Terminal

```
[pranay@localhost ~]$ ssh -i "firstinstance.pem" ec2-user@43.205.95.188
The authenticity of host '43.205.95.188 (43.205.95.188)' can't be established.
ECDSA key fingerprint is SHA256:zzbfBxCYDg3eopnyvAsOlf0Sr0MEK4lWLAEEoNduH8g.
ECDSA key fingerprint is MD5:30:4c:40:c2:93:ab:e4:95:51:18:2a:b4:f0:37:ce:01.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '43.205.95.188' (ECDSA) to the list of known hosts.
```

```
#_
~/_ #####_      Amazon Linux 2023
~~ \_#####\
~~   \###|
~~     \#/ ---  https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '~>
~~~~
    ~/./ -/-/
        _/m/'
```

```
Last login: Sat Nov 11 16:50:12 2023 from 103.167.127.24
[ec2-user@ip-10-0-0-58 ~]$
```

ASSIGNMENT 2

Configure EC2 private Instance in AWS

(create two private subnets ,two private instances, 1 Route Tables)

1. Login to your AWS console and choose the region where you have created your VPC

2. Click on “Create subnet” select the VPC that you have created previously

3. In the subnet settings(subnet 1 of 1) , provide the name of the subnet ex: private_01 ,select the AZ that you have given for public instance , provide the IPv4 CIDR block as 10.0.3.0/24 (Note : you can provide your own CIDR block)

A:

Subnet 1 of 2

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

privatesubnet_1

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

Asia Pacific (Mumbai) / ap-south-1a

IPv4 VPC CIDR block [Info](#)

Choose the IPv4 VPC CIDR block to create a subnet in.

10.0.0.0/16

IPv4 subnet CIDR block

10.0.2.0/24

256 IPs

< > ^ v

▼ Tags - optional

Key

Q Name X

Value - optional

Q privatesubnet_1 X

Remove

Add new tag

4. Click on Add new subnet and provide the name of the subnet ex: private_02 , select the AZ select the AZ that you have given for public instance provide the IPv4 CIDR block as 10.0.4.0/24 (Note : you can provide your own CIDR block)

A:

Subnet 2 of 2

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

privatesubnet_2

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

Asia Pacific (Mumbai) / ap-south-1a

IPv4 VPC CIDR block [Info](#)

Choose the IPv4 VPC CIDR block to create a subnet in.

10.0.0.0/16

IPv4 subnet CIDR block

10.0.3.0/24

256 IPs

< > ^ v

▼ Tags - optional

Key

Q Name X

Value - optional

Q privatesubnet_2 X

Remove

Add new tag

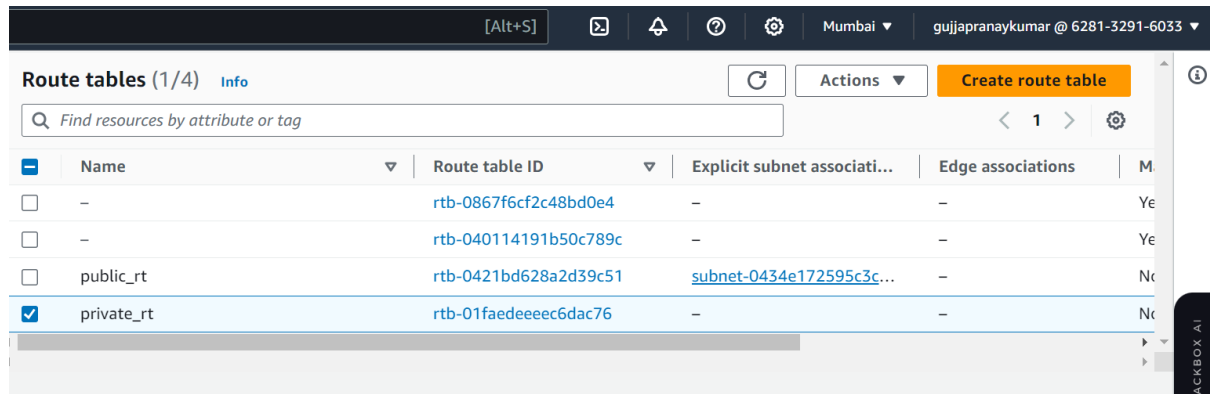
You can add 49 more tags.

5. Now click on “create subnet” to get created

6. Create a Route table private subnets

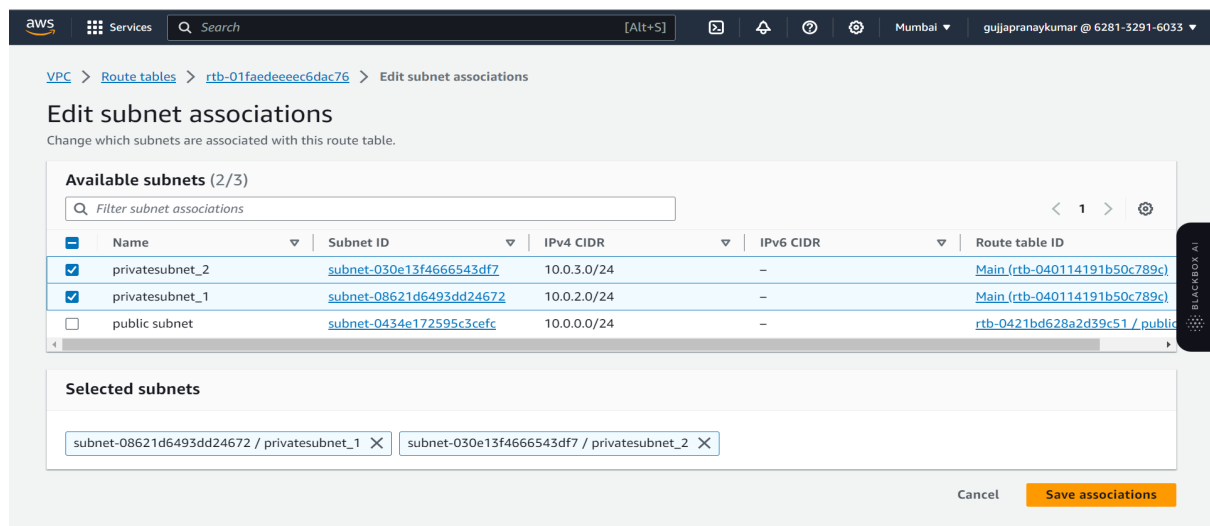
(Note: I am showing you only one Route Table for your reference)

A:



7. Now Edit the subnet Associations and select the private subnets and save it

A:



8. Now create instances for private subnets, navigate to EC2 and click on Launch Instance

9. Select the AMI as below

10. Click “Next” in the step2 as default is selected

11. In the Network , select the VPC that you have created, in the subnets select the private_01 subnet that you have created . Click on “Next :/

A: private isntnace 1

Network settings Info

VPC - required Info
vpc-0358873cfff60846f
10.0.0.0/16

Subnet Info
subnet-08621d6493dd24672
privatesubnet_1
VPC: vpc-0358873cfff60846f Owner: 628132916033
Availability Zone: ap-south-1a IP addresses available: 251 CIDR: 10.0.2.0/24

Auto-assign public IP Info
Disable

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
☒ Create security group ☐ Select existing security group

Security group name - required
launch-wizard-4

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-:/[]@+=&:~!*\$*

Summary

Number of instances Info
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.2.2...read more
ami-02e94b011299ef128

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Cancel Launch instance

Private instance 2

Network settings Info

VPC - required Info
vpc-0358873cfff60846f
10.0.0.0/16

Subnet Info
subnet-030e13f4666543df7
privatesubnet_2
VPC: vpc-0358873cfff60846f Owner: 628132916033
Availability Zone: ap-south-1a IP addresses available: 251 CIDR: 10.0.3.0/24

Auto-assign public IP Info
Disable

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
☒ Create security group ☐ Select existing security group

Security group name - required
launch-wizard-5

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-:/[]@+=&:~!*\$*

Summary

Number of instances Info
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.2.2...read more
ami-02e94b011299ef128

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Cancel Launch instance

12. In storage the default options are selected , you can click “Next : Add Tags”.
provide the Name and Value as below, (it is your choice to provide any values) and
click on ‘configure security groups’

A: key value 1

Name and tags Info

Key Info	Value Info	Resource types Info	
Name	privateinstance	Select resource t...	Remove
		Instances	

Add new tag

You can add up to 49 more tags.

Key value 2

▼ Name and tags [Info](#)

Key [Info](#)

Value [Info](#)

Resource types [Info](#)

You can add up to 49 more tags.

13. In 'configure security groups' add the following rules

(Note : Select my ip from the source)

A: same for both

Services [Alt+S] gujjapranaykumar @ 6281-3291-6033 ▼

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 103.167.127.24/32)

Type [Info](#)

Protocol [Info](#)

Port range [Info](#)

Source type [Info](#)

Name [Info](#)

Description - optional [Info](#)

▼ Security group rule 2 (ICMP, All, 103.167.127.24/32)

Type [Info](#)

Protocol [Info](#)

Port range [Info](#)

Source type [Info](#)

Name [Info](#)

Description - optional [Info](#)

▼ Summary

Number of instances [Info](#)

Software Image (AMI)

Amazon Linux 2023 AMI 2023.2.2...[read more](#)

ami-02e94b011299ef128

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

14. Click on Launch in the Last step, it will be selecting the existing keypair by

default, make a check on acknowledge and click launch instance

A: same for both instances

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

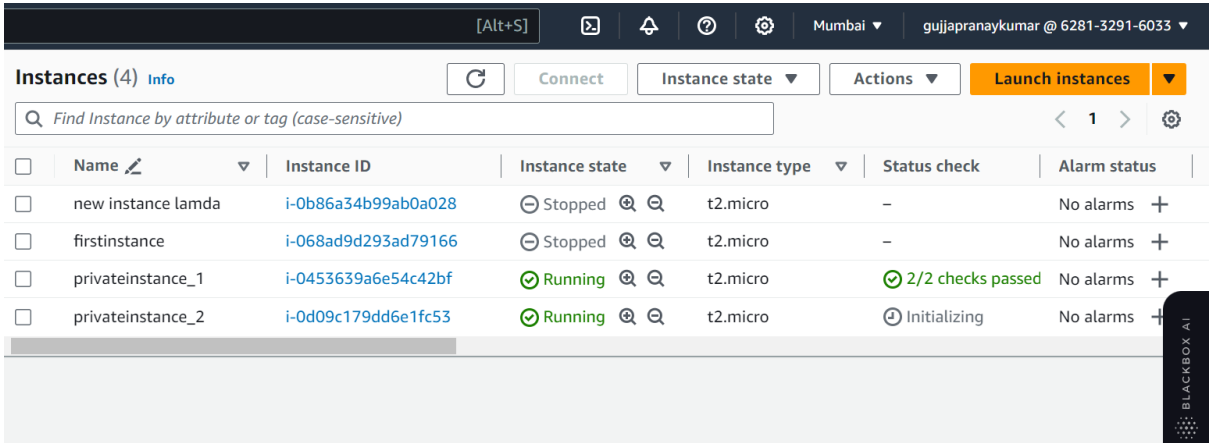
Key pair name - required

15. Similarly create another private Instance

16. Your Instances will be successfully running but you cannot access them since it is a private instance.

A:

[Alt+S]



<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
<input type="checkbox"/>	new instance lamda	i-0b86a34b99ab0a028	Stopped	t2.micro	-	No alarms
<input type="checkbox"/>	firstinstance	i-068ad9d293ad79166	Stopped	t2.micro	-	No alarms
<input type="checkbox"/>	privateinstance_1	i-0453639a6e54c42bf	Running	t2.micro	2/2 checks passed	No alarms
<input type="checkbox"/>	privateinstance_2	i-0d09c179dd6e1fc53	Running	t2.micro	Initializing	No alarms

END